

Travaux pratiques

- La société NEXTINFO souhaite créer un service informatique dédié avec un domaine Active Directory. Pour ce faire, elle fait appel à vos services afin d'installer les contrôleurs de domaine et configurer les composants principaux du réseau tels que DNS, DNSSEC, DHCP et IPAM.
- INFOLIVE est une nouvelle filiale. Les postes clients de la société NEXTINFO devront être en mesure de résoudre des noms de machines hébergeant des ressources dans le domaine de cette filiale.
- Le service DHCP devra être configuré afin de permettre le basculement vers un serveur DHCP de secours en cas de panne.
- Pour finir, la société NEXTINFO souhaite mettre en place un serveur central de gestion d'adresses IP.

Pour réaliser les TP suivants, vous aurez besoin de mettre en place les machines virtuelles suivantes qui hébergeront les rôles ci-dessous :

- **DC-01** : contrôleur du domaine Nextinfo.priv, serveur DNS et DHCP
 - Adresse IP : 192.168.0.100
 - Masque de sous-réseau : 255.255.255.0
- **DC-02** : contrôleur du domaine Nextinfo.priv, serveur DNS et DHCP
 - Adresse IP : 192.168.0.101
 - Masque de sous-réseau : 255.255.255.0
- **IPAM-01** : serveur IPAM pour le domaine Nextinfo.priv
 - Adresse IP : 192.168.0.103
 - Masque de sous-réseau : 255.255.255.0
- **CLIENT1** : client DNS & DHCP
 - Adresse IP : 192.168.0.104
 - Masque de sous-réseau : 255.255.255.0
- **INFODC-01** : contrôleur du domaine infolive.local, serveur DNS
 - Adresse IP : 192.168.0.105
 - Masque de sous-réseau 255.255.255.0

1. Installer et configurer le service DNS

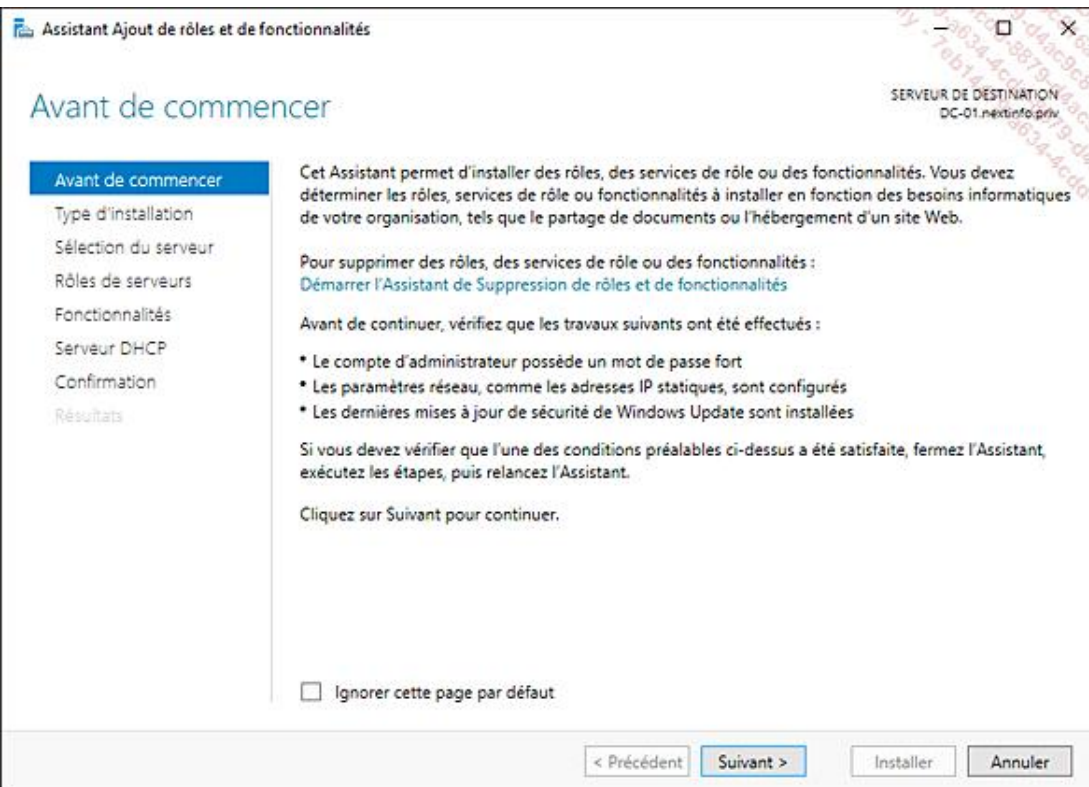
Ce TP permet d'installer et de configurer les principales options du rôle de serveur DNS. À ce stade, le domaine Nextinfo.priv n'est pas encore créé.

Installer le rôle de serveur DNS

- **Étape 1** : sur le serveur **DC-01**, ouvrez le Gestionnaire de serveur et cliquez sur **Ajouter des rôles et des fonctionnalités**.



→ **Étape 2** : cliquez sur **Suivant** :



→ **Étape 3** : cliquez sur **Suivant** :

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le type d'installation

SÉVEUR DE DESTINATION
DC-01.néxinfo.priv

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DHCP

Confirmation

Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

☒ **Installation basée sur un rôle ou une fonctionnalité**
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

☐ **Installation des services Bureau à distance**
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent Suivant > Installer Annuler

→ **Étape 4** : cliquez sur **Suivant** :

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SÉVEUR DE DESTINATION
DC-01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez 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 :

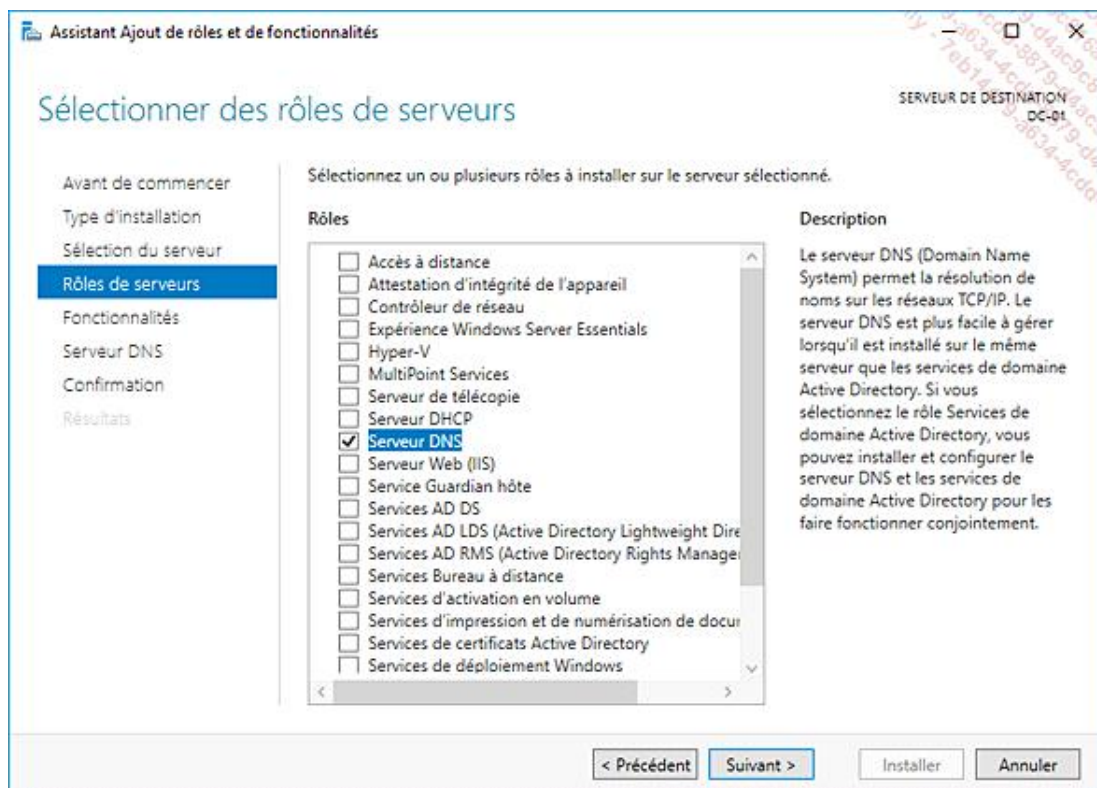
Nom	Adresse IP	Système d'exploitation
DC-01	192.168.0.15	Microsoft Windows Server 2016 Datacenter

1 ordinateur(s) trouvé(s)

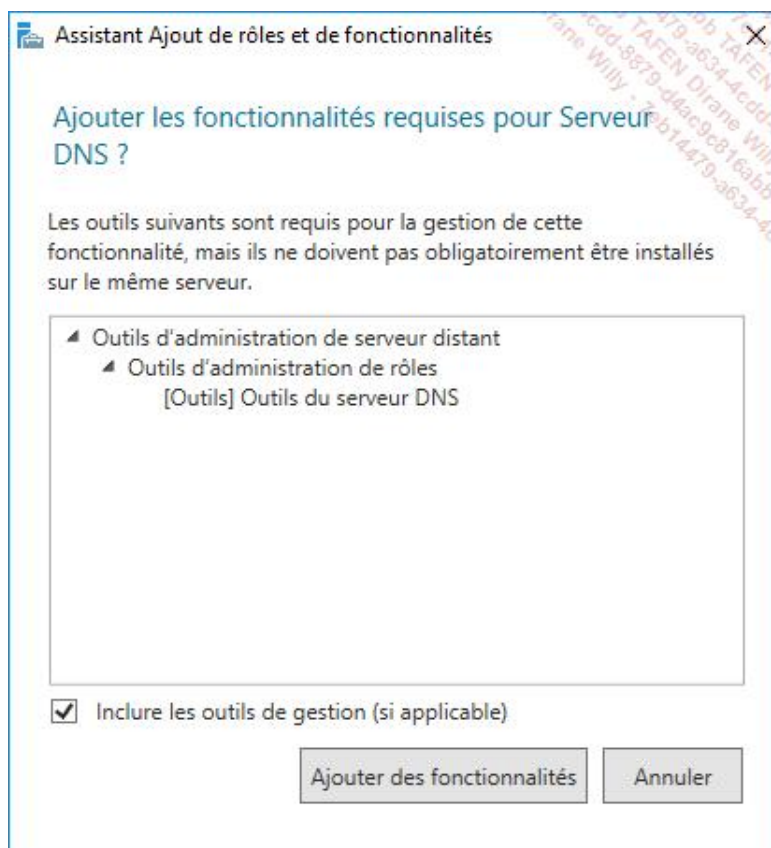
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète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

< Précédent Suivant > Installer Annuler

→ **Étape 5** : cochez la case correspondant au rôle de **Serveur DNS** :



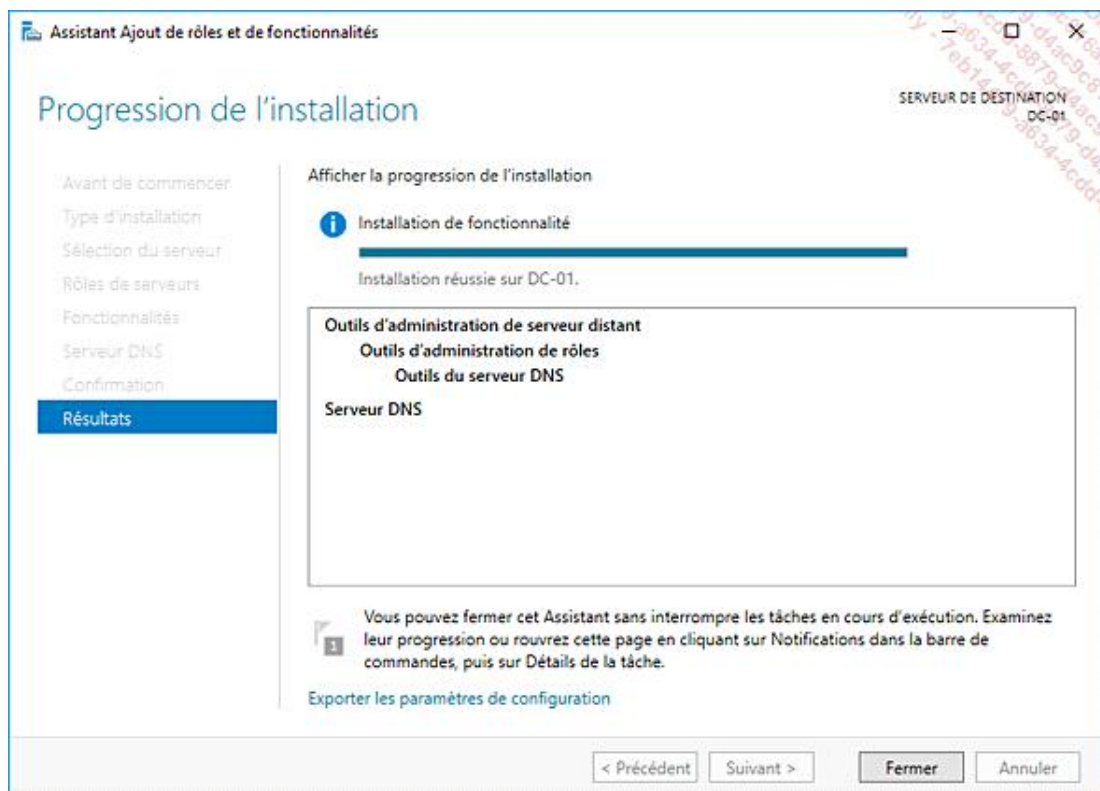
→ **Étape 6** : cliquez sur **Ajouter des fonctionnalités** :



→ **Étape 7** : cliquez trois fois sur **Suivant**.

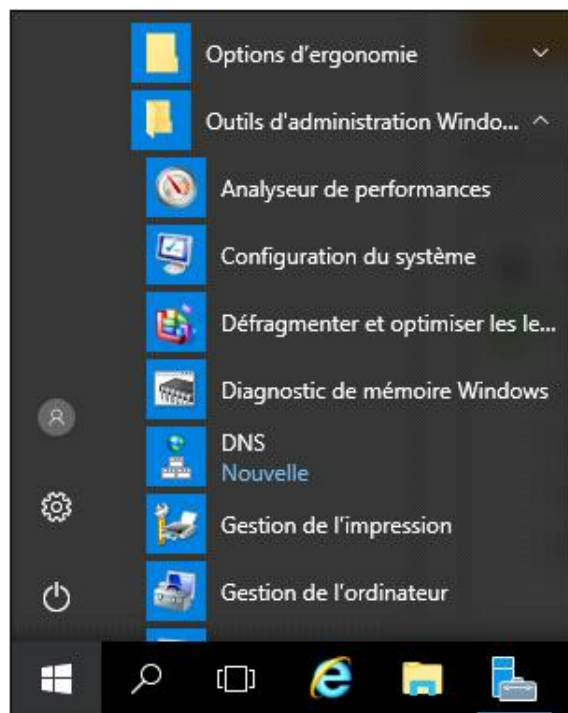
→ **Étape 8** : cliquez sur **Installer**.

→ **Étape 9** : cliquez sur **Fermer** lorsque l'installation est terminée :

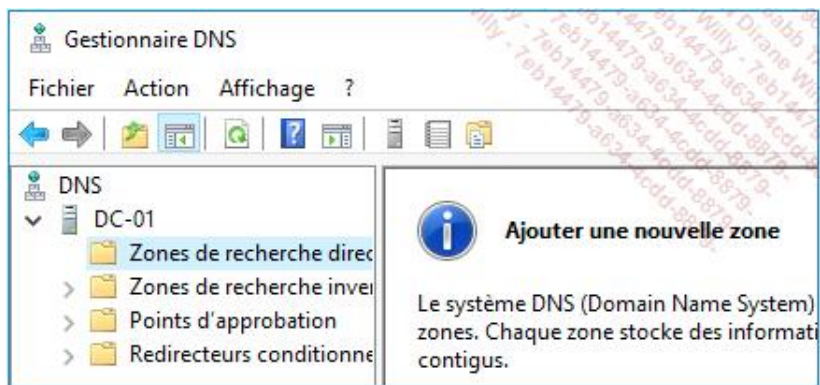


Créer des zones de recherche DNS

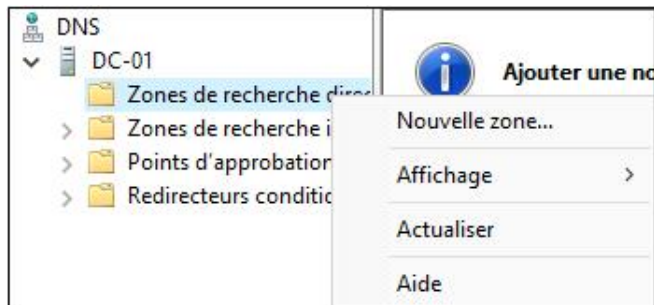
→ **Étape 1** : allez dans le menu Démarrer de Microsoft Windows Server 2016 et cliquez sur **DNS** :



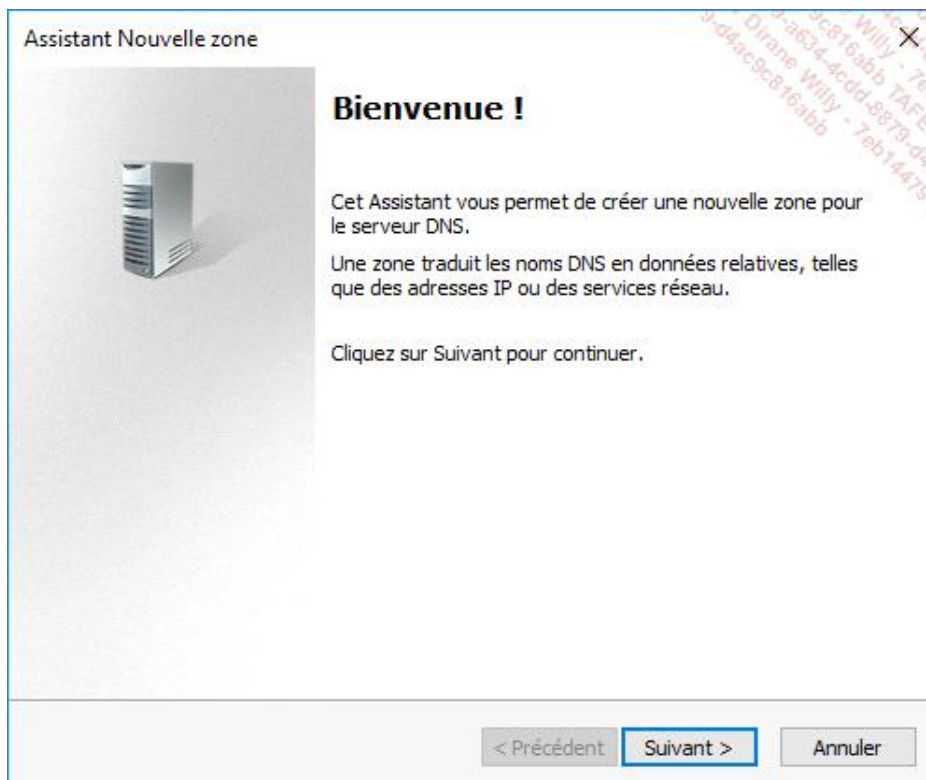
→ **Étape 2** : développez l'arborescence de la console et sélectionnez **Zones de recherche directes** :



→ **Étape 3** : affichez le menu contextuel et cliquez sur **Nouvelle zone...** :



→ **Étape 4** : cliquez sur **Suivant** :



→ **Étape 5** : sélectionnez **Zone principale** et cliquez sur **Suivant** :

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

→ **Étape 6** : tapez comme nom de zone **nextinfo.priv** et cliquez sur **Suivant** :

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 :

nextinfo.priv

< Précédent Suivant > Annuler

→ **Étape 7** : laissez les options par défaut et cliquez sur **Suivant** :

Assistant Nouvelle zone

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

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

☒ Créer un nouveau fichier nommé :

nextinfo.priv.dns

☐ Utiliser un fichier existant :

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

< Précédent Suivant > Annuler


→ **Étape 8** : cochez la case **Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées** et cliquez sur **Suivant** :

Assistant Nouvelle zone

Mise à niveau dynamique
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

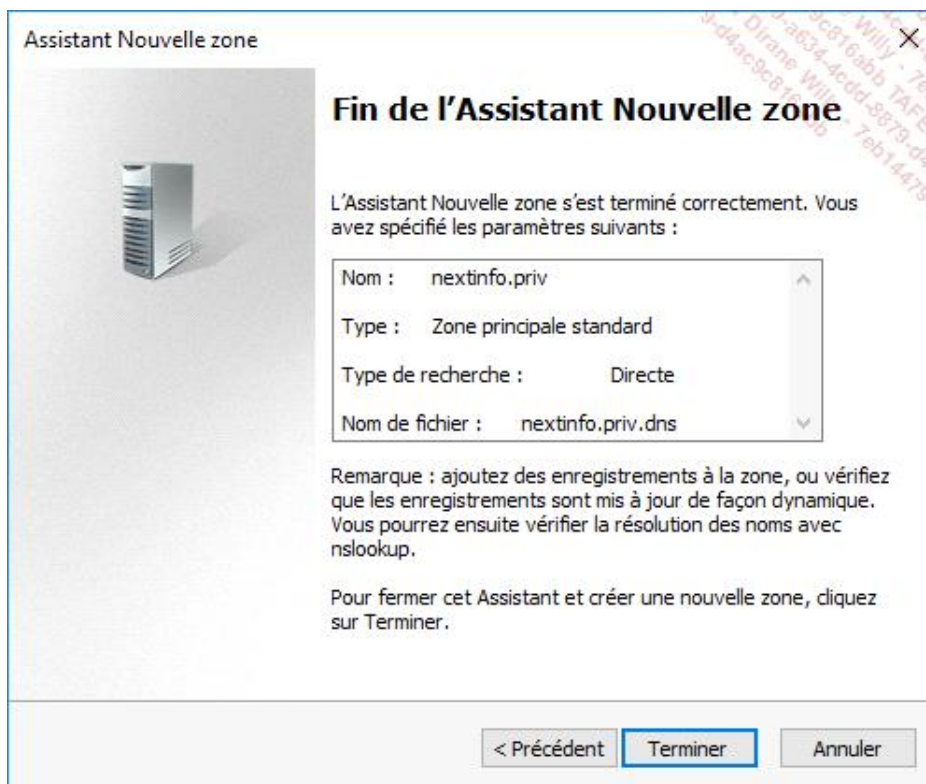
☐ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

☒ Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

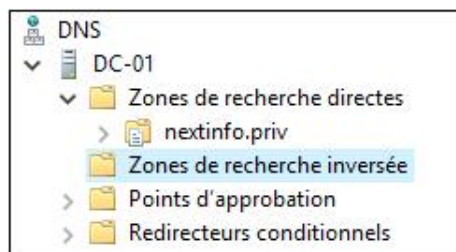
☐ Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent Suivant > Annuler

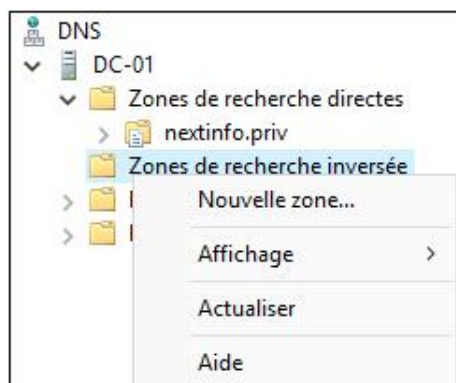
→ **Étape 9** : cliquez sur **Terminer** :



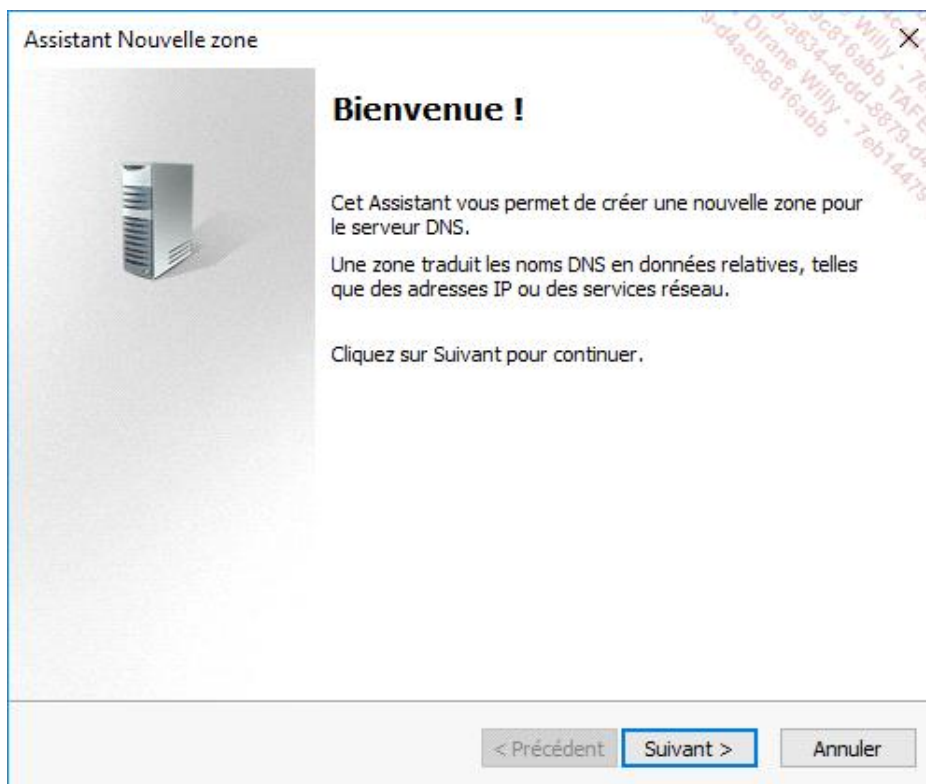
→ **Étape 10** : dans l'arborescence de la console DNS, sélectionnez **Zones de recherche inversée** :



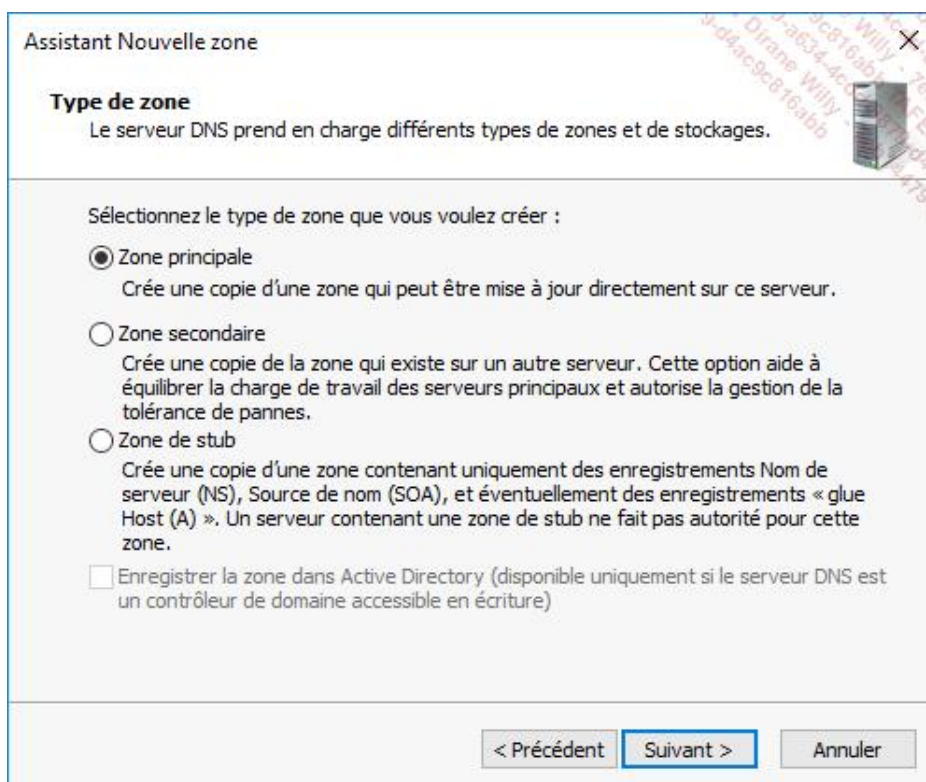
→ **Étape 11** : affichez le menu contextuel et cliquez sur **Nouvelle zone...** :



→ **Étape 12** : cliquez sur **Suivant** :



→ **Étape 13** : cliquez sur **Suivant** :



→ **Étape 14** : sélectionnez **Zone de recherche inversée IPv4** et cliquez sur **Suivant** :

Assistant Nouvelle zone

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

☐ Zone de recherche inversée IPv6

< Précédent Suivant > Annuler

→ **Étape 15** : entrez l'ID réseau **192.168.0** et cliquez sur **Suivant** :

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 .0

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 :

0.168.192.in-addr.arpa

< Précédent Suivant > Annuler

→ **Étape 16** : cliquez sur **Suivant** :

Assistant Nouvelle zone

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

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

☒ Créer un nouveau fichier nommé :

0.168.192.in-addr.arpa.dns

☐ Utiliser un fichier existant :

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

< Précédent Suivant > Annuler


→ **Étape 17** : cochez la case **Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées** et cliquez sur **Suivant** :

Assistant Nouvelle zone

Mise à niveau dynamique
Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

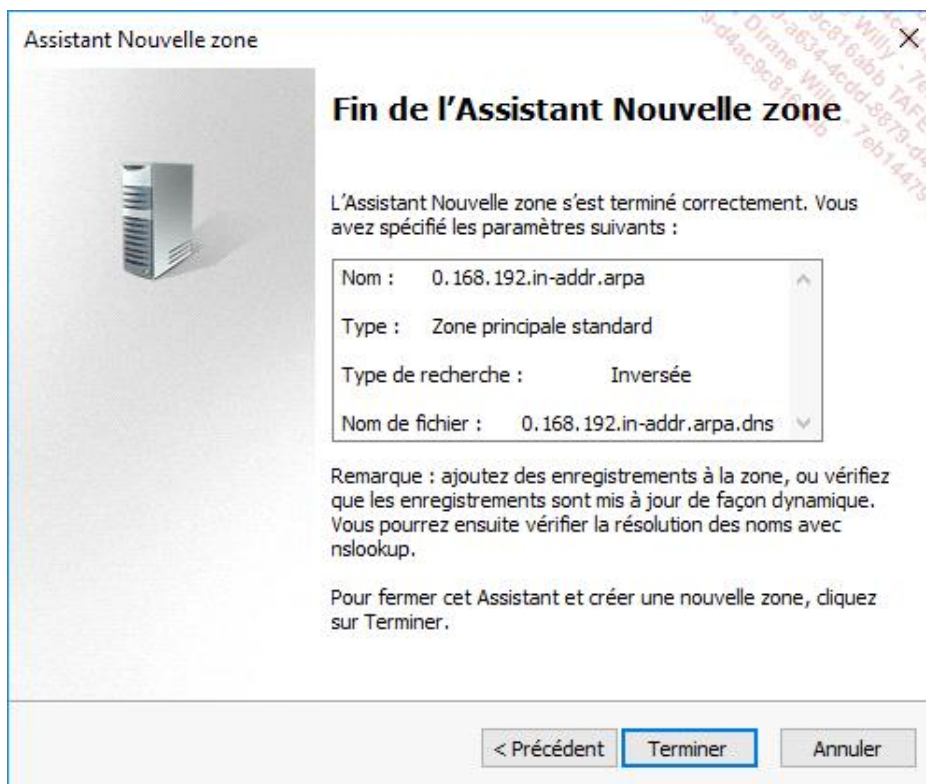
☐ N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)
Cette option n'est disponible que pour les zones intégrées à Active Directory.

☒ Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.
 Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

☐ Ne pas autoriser les mises à jour dynamiques
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

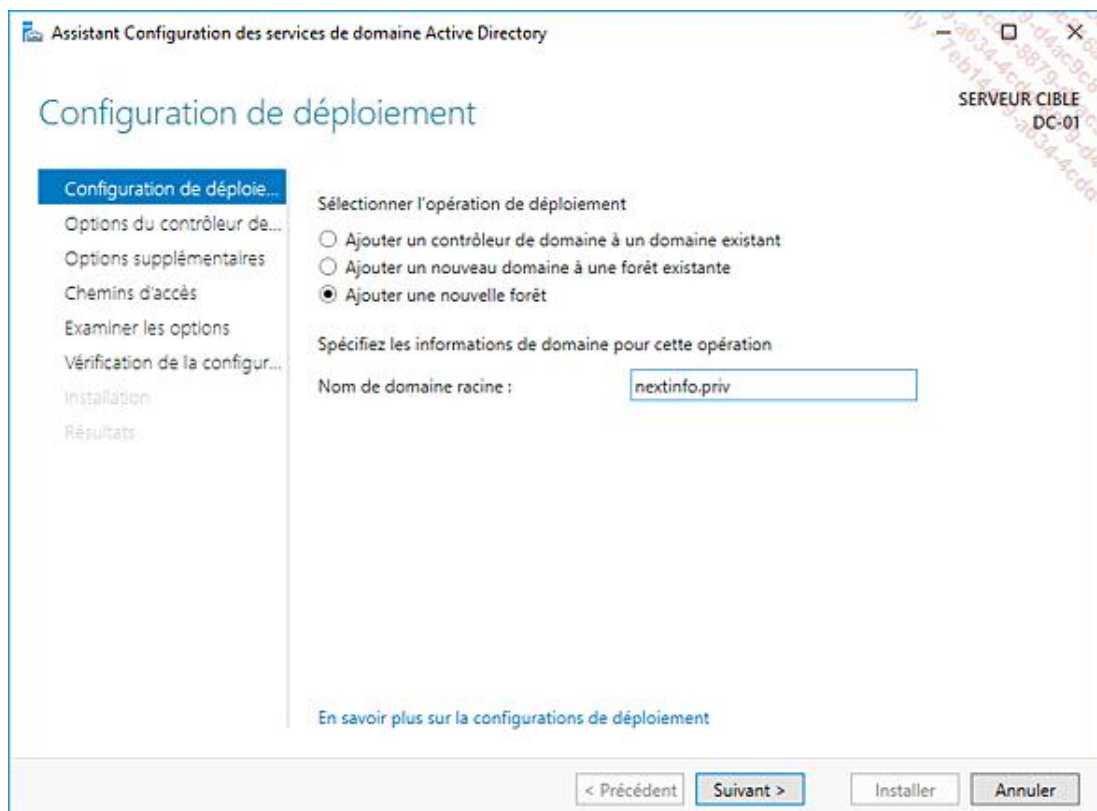
< Précédent Suivant > Annuler

→ **Étape 18** : cliquez sur **Terminer** :

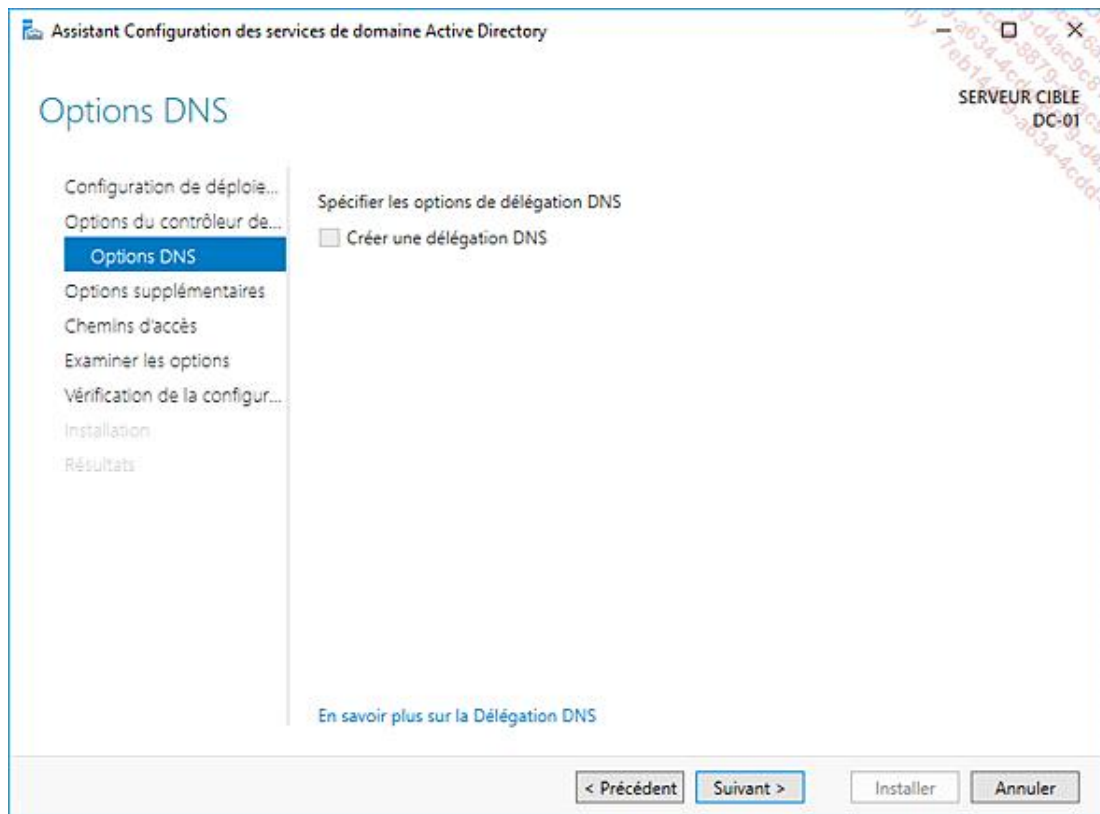


➔ À ce stade, les zones de recherche directe et inversée pour le domaine Nextinfo.priv sont créées (sous forme de fichier .dns car ces zones ne sont pas intégrées à Active Directory). Vous pouvez désormais installer le rôle services AD DS avant de passer au TP suivant.

➔ **Étape 19** : ajoutez le rôle services AD DS pour créer une nouvelle forêt dont le domaine racine sera **nextinfo.priv** :



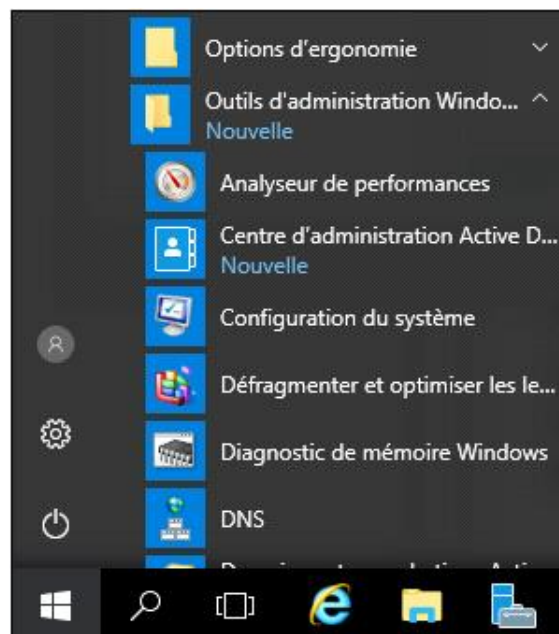
- **Étape 20** : décochez la case **Créer une délégation DNS** et indiquez les informations de connexion du compte **Administrateur** local du serveur :



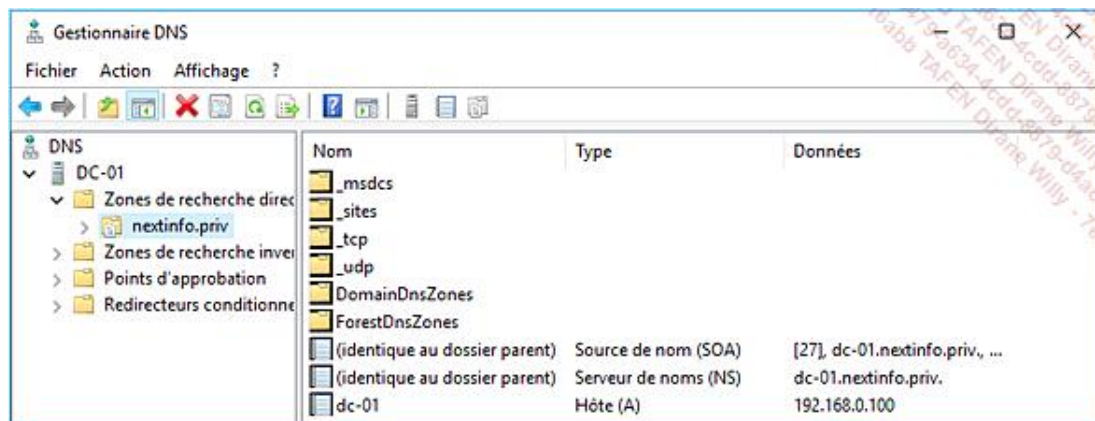
- Renseignez les différentes fenêtres afin de pouvoir installer Active Directory.

Intégrer une zone à Active Directory

- **Étape 1** : une fois que le domaine Active Directory est installé, dirigez-vous dans le menu **Démarrer** et cliquez sur **DNS** :



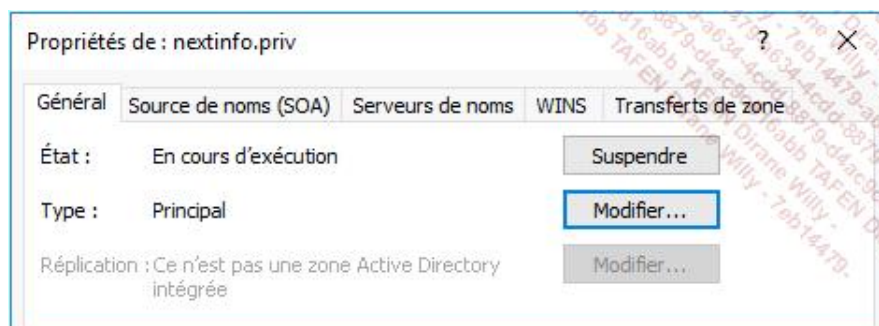
- **Étape 2** : développez l'arborescence afin de sélectionner la zone de recherche directe **nextinfo.priv** :



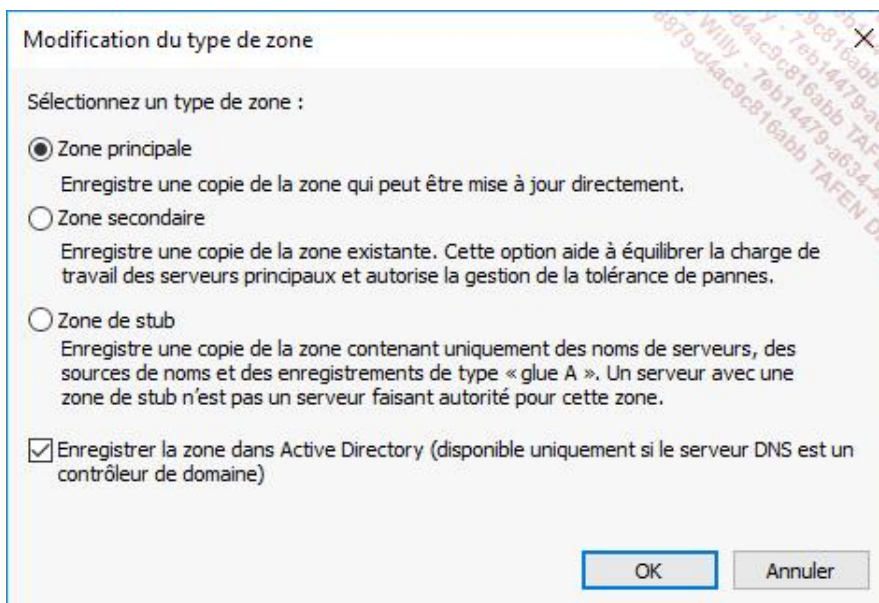
→ **Étape 3** : affichez le menu contextuel et cliquez sur **Propriétés** :



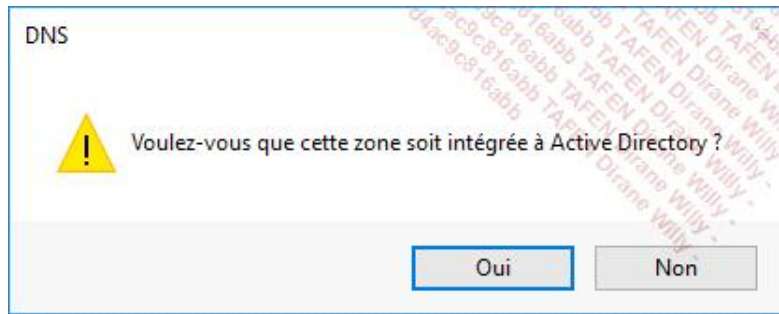
→ **Étape 4** : cliquez sur **Modifier...** :



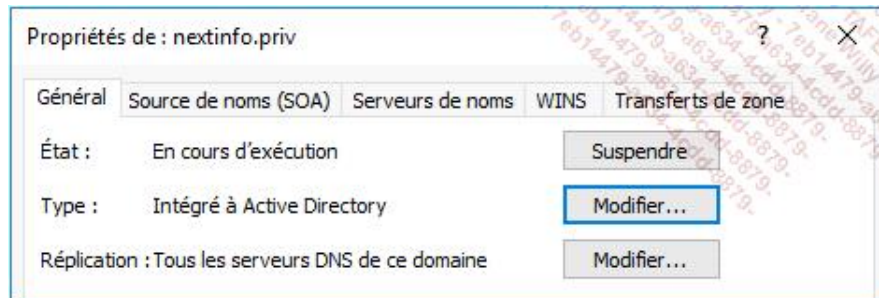
→ **Étape 5** : cochez la case **Enregistrer la zone dans Active Directory** et cliquez sur **OK** :



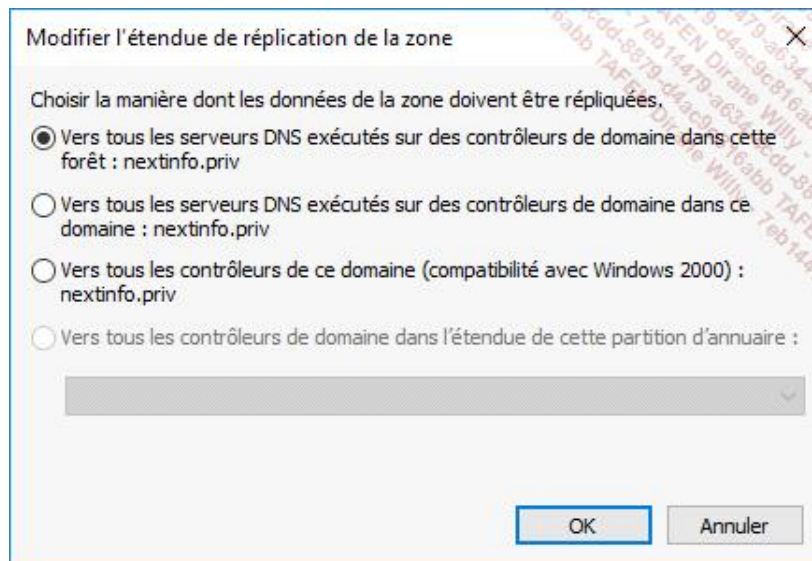
→ **Étape 6** : cliquez sur **Oui** :



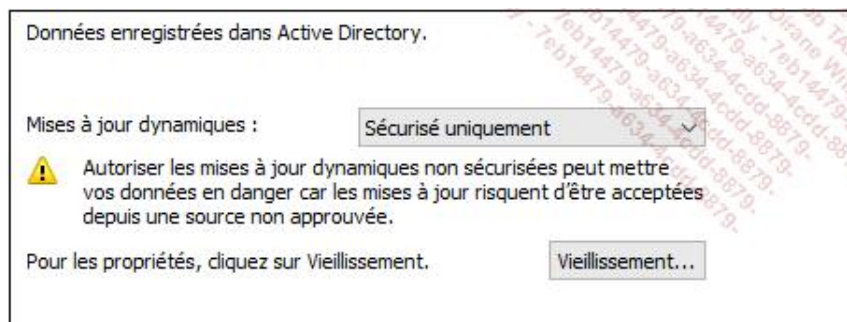
→ **Étape 7** : dans les propriétés de la zone, cliquez à nouveau sur **Modifier...** dans la section **Réplication** cette fois-ci :



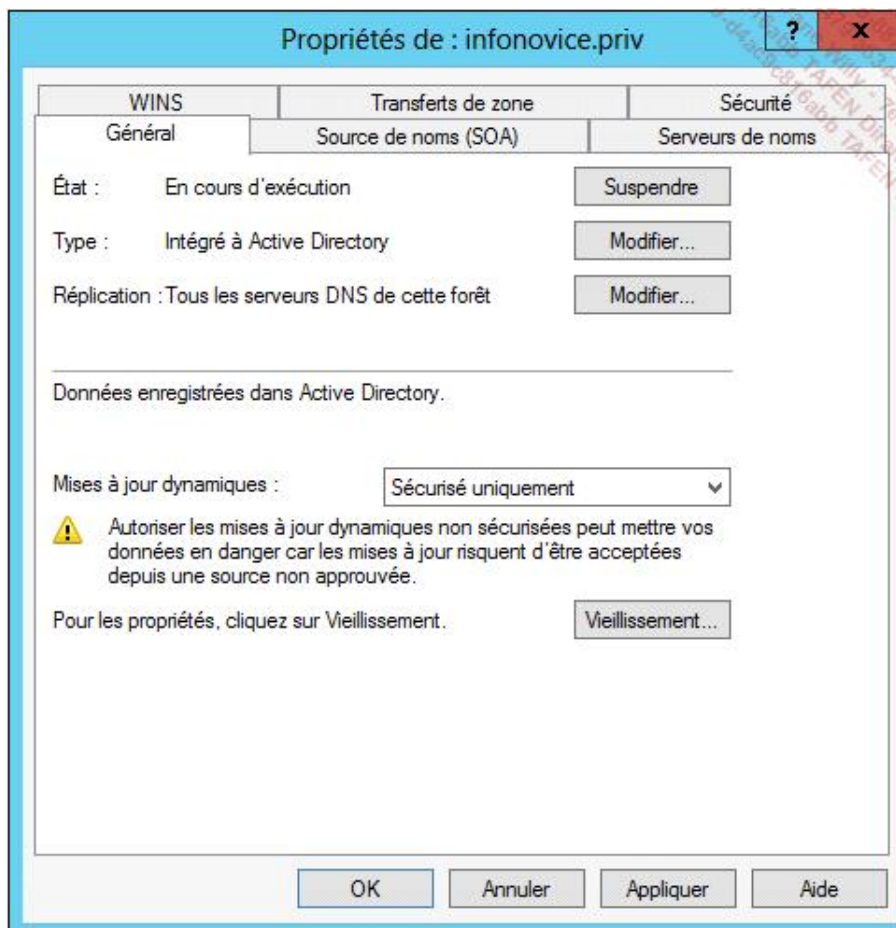
→ **Étape 8** : cochez la case **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : nextinfo.priv** et cliquez sur **OK** :



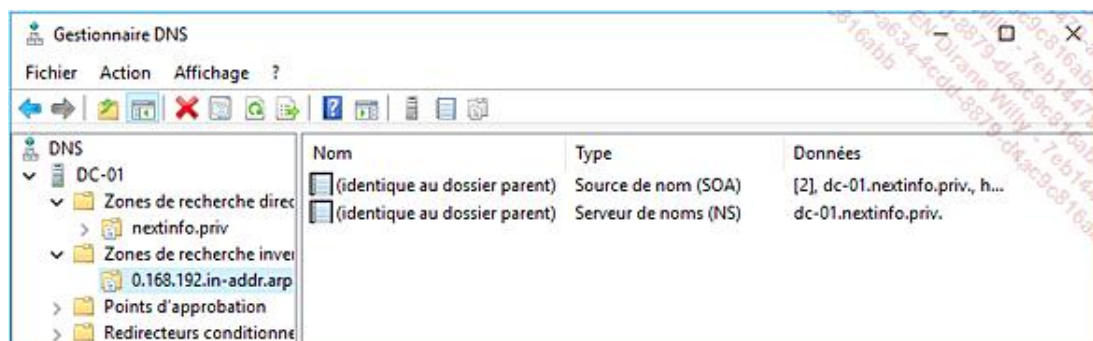
→ **Étape 9** : dans les propriétés de la zone, sélectionnez des mises à jour dynamiques **Sécurisé uniquement** :



→ **Étape 10** : cliquez sur **OK** :

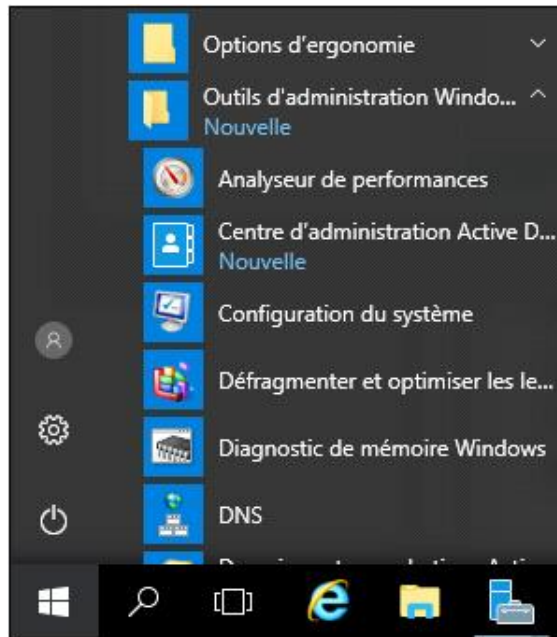


→ **Étape 11** : répétez les étapes 1 à 9 en sélectionnant la zone de recherche inversée **0.168.192.in-addr.arpa** :

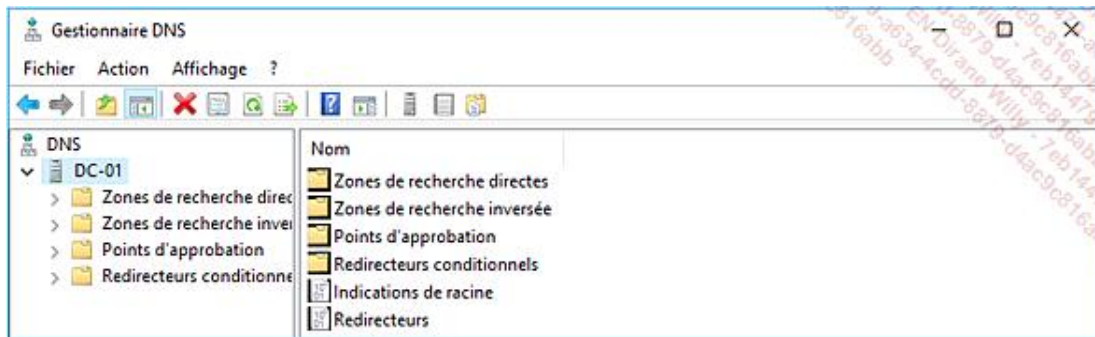


Configurer le nettoyage automatique des zones

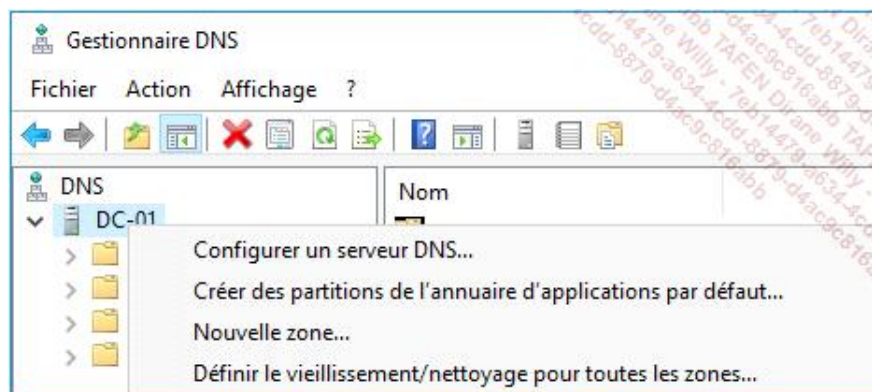
→ **Étape 1** : ouvrez le menu **Démarrer** et cliquez sur **DNS** :



→ **Étape 2** : développez l'arborescence de la console et sélectionnez le serveur DNS **DC-01** :



→ **Étape 3** : affichez le menu contextuel et cliquez sur **Définir le vieillissement/nettoyage pour toutes les zones...** :



→ **Étape 4** : cochez la case **Nettoyer les enregistrements de ressources obsolètes** et cliquez sur **OK** :

Vieillessement de serveur/Propriétés de nettoyage

☒ Nettoyer les enregistrements de ressources obsolètes

Intervalle de non-actualisation

La durée entre la plus récente réactualisation d'un datage d'enregistrement et le moment auquel le horodatage peut être réactualisé.

Intervalle de non-actualisation : jours

Intervalle d'actualisation

La durée entre le moment auquel un horodatage d'enregistrement peut être réactualisé au plus tôt et le moment auquel un enregistrement peut être nettoyé au plus tôt. L'intervalle d'actualisation doit être plus long que le délai maximal d'actualisation des enregistrements.

Intervalle d'actualisation : jours

OK Annuler

→ **Étape 5** : cochez la case **Appliquer ces paramètres aux zones existantes intégrées à Active Directory** et cliquez sur **OK** :

Vieillessement de serveur/Confirmation de nettoyage

Paramètres par défaut pour les nouvelles zones intégrées à Active Directory :

Nettoie les ressources périmées : Activé

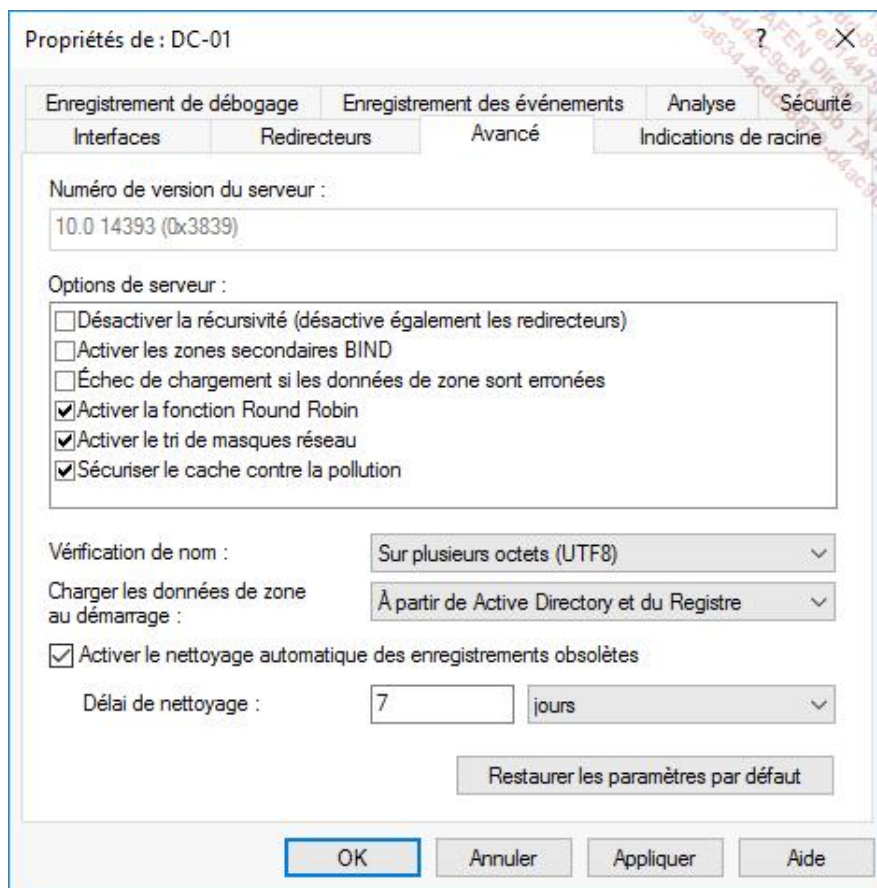
☒ Appliquer ces paramètres aux zones existantes intégrées à Active Directory

OK Annuler

→ **Étape 6** : affichez de nouveau le menu contextuel sur le serveur DNS puis cliquez sur **Propriétés** :

Exporter la liste...
Propriétés
Aide

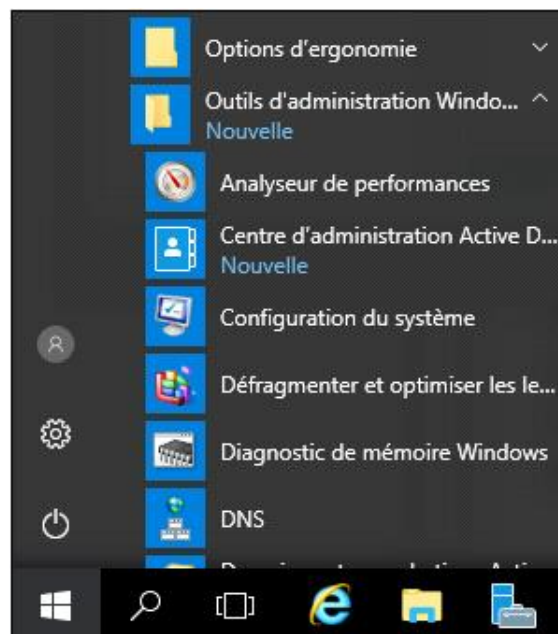
→ **Étape 7** : sélectionnez l'onglet **Avancé**, cochez la case **Activer le nettoyage automatique des enregistrements obsolètes** et cliquez sur **OK** :



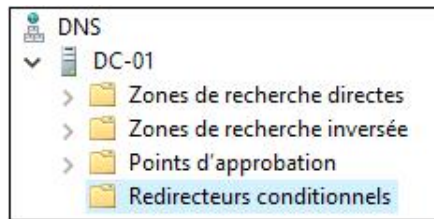
Le nettoyage automatique des enregistrements DNS pour toutes les zones est désormais activé. Ce paramètre sera effectif pour toutes les nouvelles zones DNS qui seront créées par la suite.

Configurer un redirecteur conditionnel

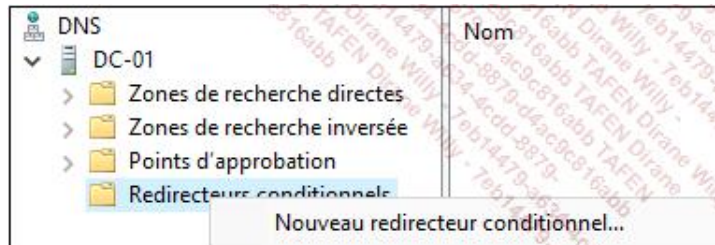
→ **Étape 1** : depuis le menu **Démarrer** cliquez sur **DNS** :



→ **Étape 2** : développez l'arborescence de la console et sélectionnez le conteneur **Redirecteurs conditionnels** :



→ **Étape 3** : affichez le menu contextuel et cliquez sur **Nouveau redirecteur conditionnel...** :



→ **Étape 4** : tapez le nom DNS du domaine Active Directory de la société INFOLIVE, soit *infolive.local*, dans le champ **Domaine DNS**. Ensuite, tapez l'adresse IP d'un serveur DNS du domaine *infolive.local*, soit *192.168.0.105* et cliquez sur **OK** :

Nouveau redirecteur conditionnel

Domaine DNS :

Adresses IP des serveurs maîtres :

Adresse IP	Nom de domaine compl...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		
192.168.0.105	<Tentative de résolutio...	Validation en cours...

☐ Stocker ce redirecteur conditionnel dans Active Directory, et le répliquer comme suit :
 Tous les serveurs DNS de cette forêt

Délai d'expiration des requêtes de redirection (en secondes) :

Le nom de domaine complet du serveur n'est pas disponible si les entrées et les zones de recherche inversée appropriées ne sont pas configurées.

→ **Étape 5** : sur le serveur DNS du domaine *infolive.local* **INFODC-01**, créez un enregistrement DNS de type CNAME nommé *fichiers* et d'adresse IP *192.168.0.105* :

infodc-01	Hôte (A)	192.168.0.105	statique
fichiers	Alias (CNAME)	192.168.0.105	

→ **Étape 6** : connectez-vous sur le poste client **CLIENT1** et tapez la commande DOS suivante : **ping**

fichiers.infolive.local

```
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping fichiers.infolive.local

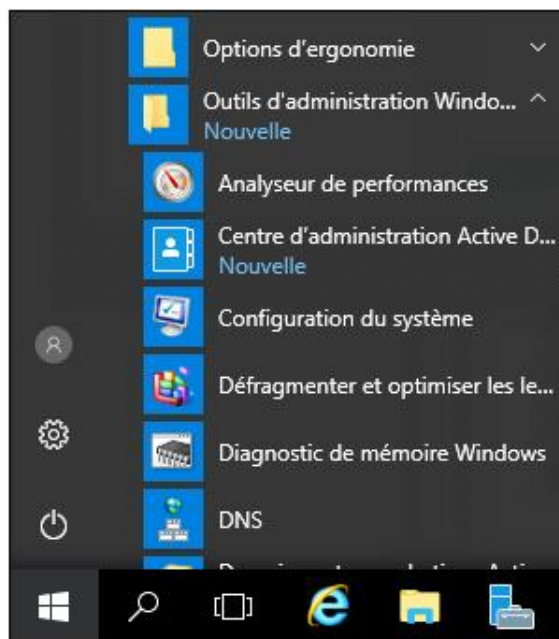
Envoi d'une requête 'ping' sur infodc-01.infolive.local [192.168.0.105] avec 32 octets de données :
Réponse de 192.168.0.105 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.105 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.105 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.105 : octets=32 temps<1ms TTL=128
```

Le poste client obtient la résolution de l'alias fichiers *infolive.local* car la redirection conditionnelle redirige toutes les requêtes DNS à destination du serveur DNS du domaine *infolive.local*. Les postes clients du domaine *Nextinfo.priv* pourront ainsi obtenir la résolution des noms FQDN associés aux différents services hébergés dans une autre forêt.

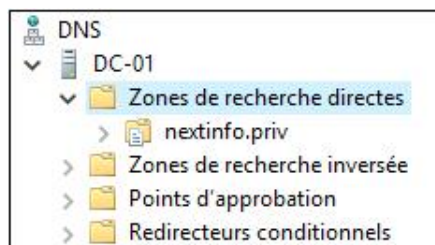
2. Configurer le service DNS avec DNSSEC

Signer une zone avec DNSSEC

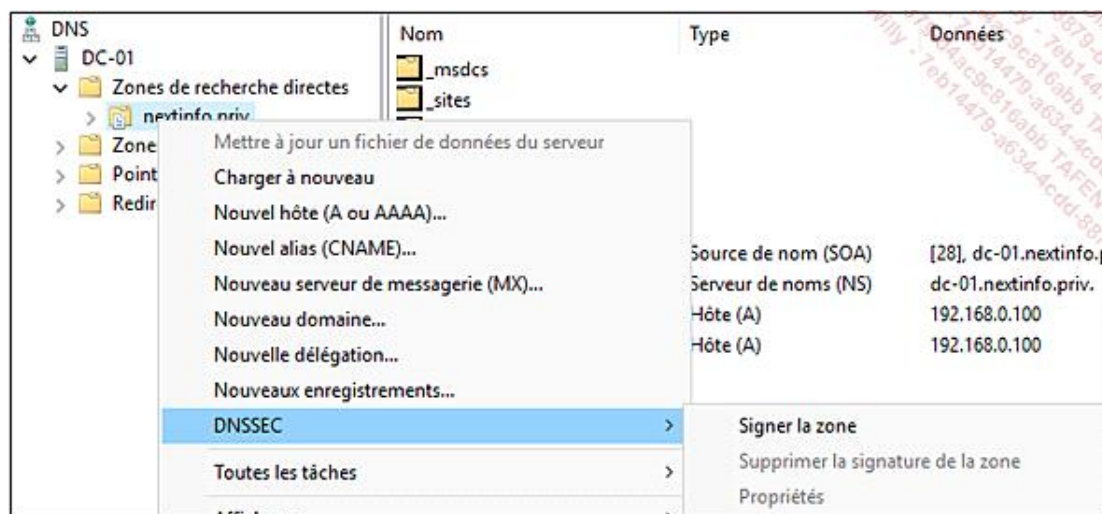
→ **Étape 1** : ouvrez le menu **Démarrer** et cliquez sur **DNS** :



→ **Étape 2** : développez l'arborescence de la console et sélectionnez la zone **nextinfo.priv** :



→ **Étape 3** : affichez le menu contextuel et cliquez sur **DNSSEC** puis **Signer la zone** :



→ **Étape 4** : cliquez sur **Suivant** :



→ **Étape 5** : cochez la case **Personnalisez les paramètres de signature de zone** et cliquez sur **Suivant** :

Assistant Signature de zone

Options de signature
Le serveur DNS prend en charge trois options de signature.

Choisissez l'une des options disponibles pour signer la zone :

☒ Personnalisez les paramètres de signature de zone.
Signe la zone avec un jeu de paramètres de signature de zone.

☐ Signer la zone à l'aide des paramètres d'une zone existante.
Signe la zone à l'aide des paramètres d'une zone signée existante.
Nom de la zone :

☐ Utiliser les paramètres pour signer la zone.
Signe la zone à l'aide des paramètres par défaut.

< Précédent **Suivant >** Annuler

→ **Étape 6** : cochez la case **Le serveur DNS DC-01 est le maître des clés** et cliquez sur **Suivant** :

Assistant Signature de zone

Maître des clés
Choisissez un maître des clés pour cette zone.

Le maître des clés est un serveur DNS qui génère et gère les clés de chiffrement d'une zone protégée DNSSEC. Tout serveur DNS faisant autorité et qui héberge une copie principale de la zone peut être le maître des clés.

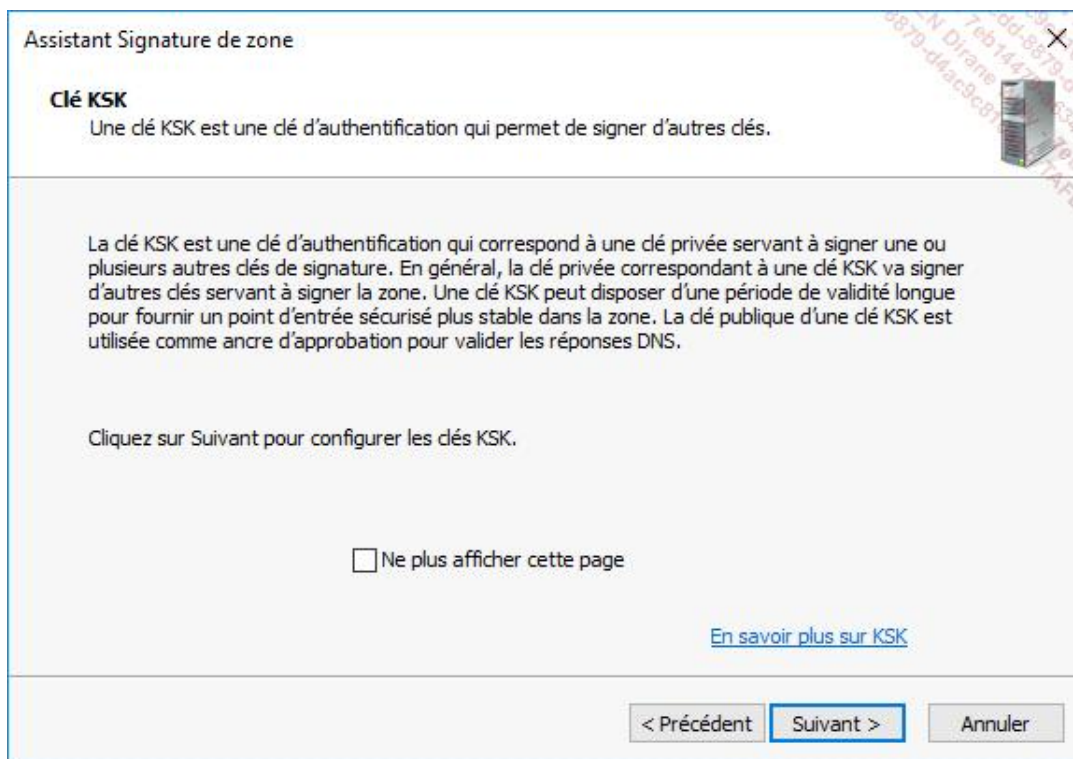
Par défaut, le serveur DNS en cours d'utilisation est choisi en tant que maître des clés. Vous pouvez également spécifier un autre serveur DNS comme maître des clés pour cette zone.

☒ Le serveur DNS DC-01 est le maître des clés.

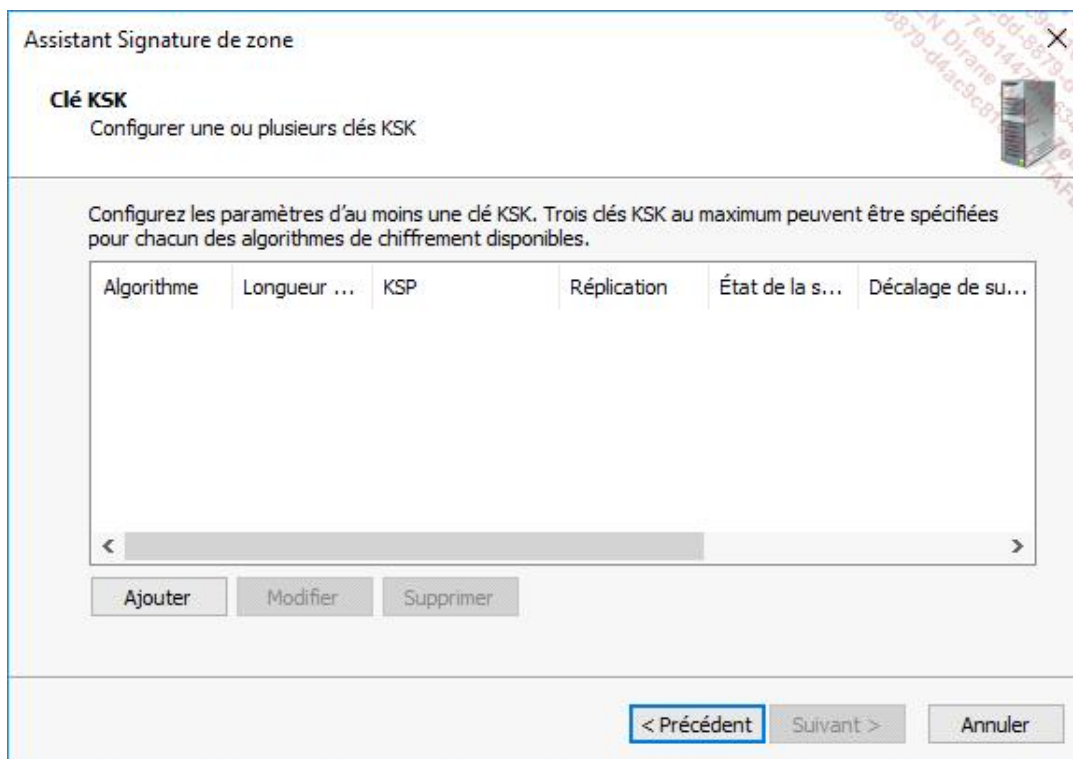
☐ Sélectionner un autre serveur primaire en tant que maître des clés :

< Précédent **Suivant >** Annuler

→ **Étape 7** : cliquez sur **Suivant** :



→ **Étape 8** : cliquez sur **Ajouter** :



→ **Étape 9** : vérifiez les paramètres de la clé d'authentification (KSK) puis cliquez sur **OK** :

Nouvelle clé KSK

GUID
GUID : {00000000-0000-0000-0000-000000000000}

Génération de clé

☒ Générer de nouvelles clés de signature.
☐ Utiliser des clés pré-générées

Utiliser cette clé comme clé active :
Utiliser cette clé comme clé de secours :

Propriétés de clé

Algorithme de chiffrement : RSA/SHA-256
Longueur de clé (bits) : 2048
Sélectionnez un fournisseur de stockage de clé pour générer et stocker des clés : Microsoft Software Key Storage Prov
Période de validité de la signature du RRSET DNSKEY (heures) : 168
☒ Répliquer cette clé privée vers tous les serveurs DNS faisant autorité pour cette zone.
(Applicable uniquement aux zones intégrées Active Directory)

Substitution de clé

☒ Activer la substitution automatique
Fréquence de substitution (jours) : 755
Reporter la première substitution de (jours) : 0

OK Annuler

→ **Étape 10** : cliquez sur **Suivant** :

Assistant Signature de zone

Clé KSK
Configurer une ou plusieurs clés KSK

Configurez les paramètres d'au moins une clé KSK. Trois clés KSK au maximum peuvent être spécifiées pour chacun des algorithmes de chiffrement disponibles.

Algorithme	Longueur ...	KSP	Réplication	État de la s...	Décalage de su...
RSA/SHA-256	2048	Microsoft Softw...	Activé	Activé	0

< >

Ajouter Modifier Supprimer

< Précédent Suivant > Annuler

→ **Étape 11** : cliquez sur **Suivant** :

Assistant Signature de zone

Clé ZSK
Une clé ZSK est une clé d'authentification qui permet de signer les données de la zone.

La clé ZSK est une clé d'authentification qui correspond à une clé privée servant à signer les données d'une zone. En général, les clés ZSK sont plus souvent substituées que les clés KSK.

Cliquez sur Suivant pour configurer les clés ZSK.

☐ Ne plus afficher cette page

[En savoir plus sur ZSK](#)

< Précédent **Suivant >** Annuler

→ **Étape 12** : cliquez sur **Ajouter** :

Assistant Signature de zone

Clé ZSK
Configurer une ou plusieurs clés ZSK

Configurez les paramètres d'au moins une clé ZSK. Trois clés ZSK au maximum peuvent être spécifiées pour chacun des algorithmes de chiffrement disponibles.

Algorithme	Longueur ...	KSP	État de la s...	Décalage de su...	Fréquence de
<div style="border: 1px solid black; height: 100px; margin-bottom: 5px;"></div> <div style="display: flex; justify-content: space-between; border-top: 1px solid black;"> < > </div>					

Ajouter Modifier Supprimer

< Précédent **Suivant >** Annuler

→ **Étape 13** : vérifiez les paramètres de la clé d'authentification (ZSK) puis cliquez sur **OK** :

Nouvelle clé ZSK

GUID

GUID : {00000000-0000-0000-0000-000000000000}

Propriétés de clé

Algorithme de chiffrement : RSA/SHA-256

Longueur de clé (bits) : 1024

Sélectionnez un fournisseur de stockage de clé pour générer et stocker des clés : Microsoft Software Key Storage Prov

Période de validité de la signature DNSKEY (heures) : 168

Période de validité de la signature DS (heures) : 168

Période de validité des enregistrements de zones (heures) : 240

Substitution de clé

☒ Activer la substitution automatique

Fréquence de substitution (jours) : 90

Reporter la première substitution de (jours) : 0

OK Annuler

→ **Étape 14** : cliquez sur **Suivant** :

Assistant Signature de zone

Clé ZSK

Configurer une ou plusieurs clés ZSK

Configurez les paramètres d'au moins une clé ZSK. Trois clés ZSK au maximum peuvent être spécifiées pour chacun des algorithmes de chiffrement disponibles.

Algorithme	Longueur ...	KSP	État de la s...	Décalage de su...	Fréquence de
RSA/SHA-256	1024	Microsoft Softw...	Activé	0	90

< >

Ajouter Modifier Supprimer

< Précédent Suivant > Annuler

→ **Étape 15** : cochez la case **Utiliser NSEC3** puis cliquez sur **Suivant** :

Assistant Signature de zone

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

➤ Les paramètres d'itérations et de sel (*salt*) permettent de limiter les attaques par dictionnaire ou brute-force dans le but de décrypter le chiffrement.

➔ **Étape 16** : cochez la case **Activer la mise à jour automatique des ancres d'approbation lors de la substitution de la clé (RFC 5011)** et cliquez sur **Suivant** :

Assistant Signature de zone

Ancres 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

➔ **Étape 17** : cliquez sur **Suivant** deux fois :

Assistant Signature de zone

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

Algorithme de génération d'enregistrements DS : SHA-1 et SHA-256

Durée de vie (TTL) des enregistrements DS (secondes) : 3600

Durée de vie (TTL) des enregistrements DNSKEY (secondes) : 3600

Période d'interrogation de la délégation sécurisée (heures) : 12

Prise d'effet de la signature (heures) : 1

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

< Précédent Suivant > Annuler

→ **Étape 18** : cliquez sur **Terminer** :

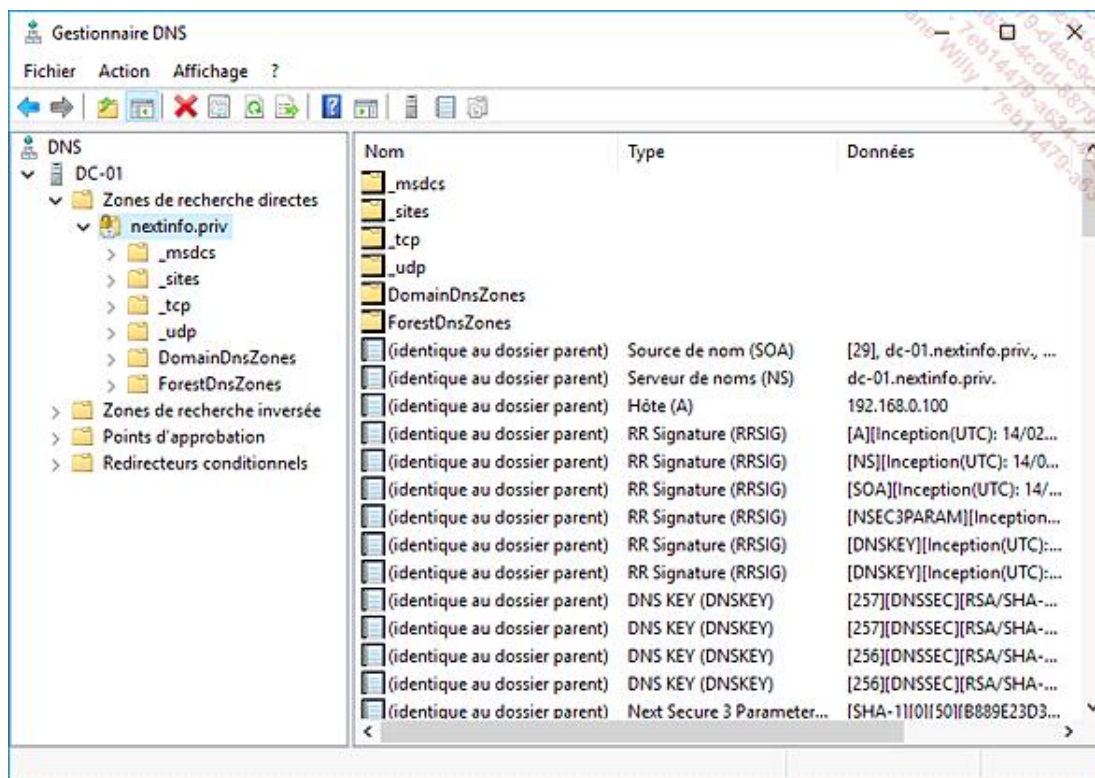
Assistant Signature de zone

Signature de la zone
Les paramètres de la zone ont été appliqués et le processus de signature a débuté.

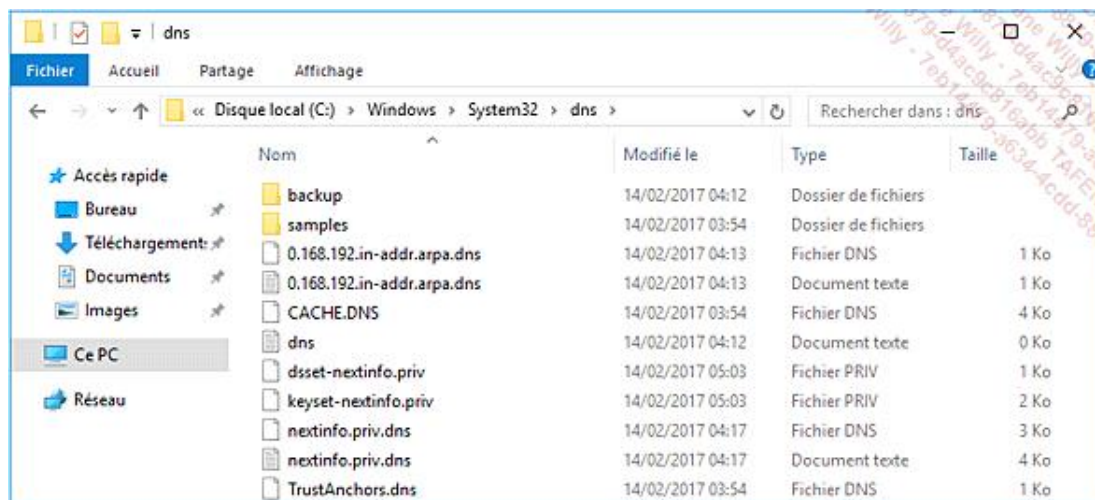
La zone a été correctement signée. Cliquez sur Terminer pour fermer l'Assistant.

< Précédent Terminer Annuler

→ **Étape 19** : vérifiez que la zone sélectionnée porte bien un petit logo en forme de cadenas indiquant que la zone est signée, puis que les enregistrements **RRSIG**, **DNSKEY** et **NSEC3** ont bien été créés :

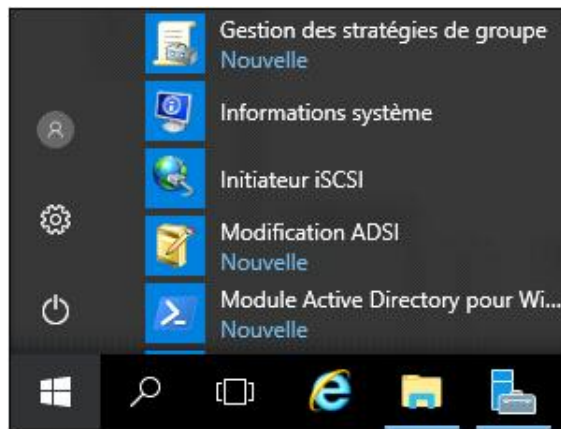


→ **Étape 20** : on peut constater qu'après la signature de la zone, deux fichiers ont été créés dans le répertoire **%SYSTEMROOT%\System32\dns** : **dsset-nextinfo.priv** et **keyset-nextinfo.priv**.

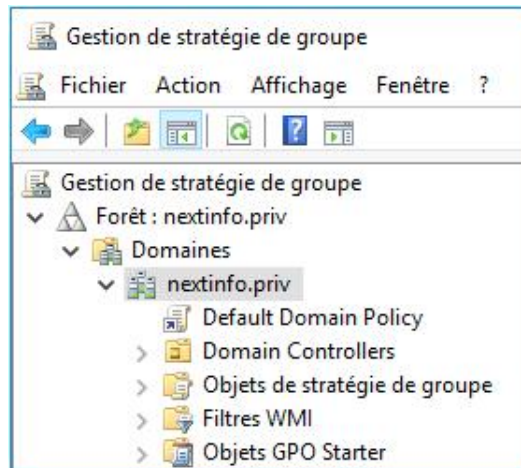


Configurer la table NRPT des clients DNS

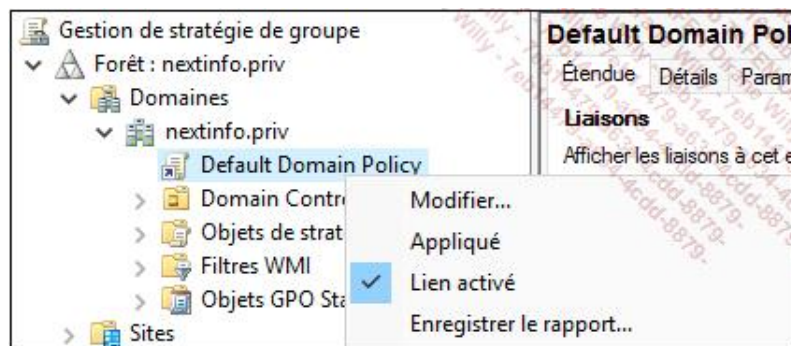
→ **Étape 1** : dans le menu **Démarrer** de Microsoft Windows Server 2016, cliquez sur l'icône **Gestion des stratégies de groupes** :



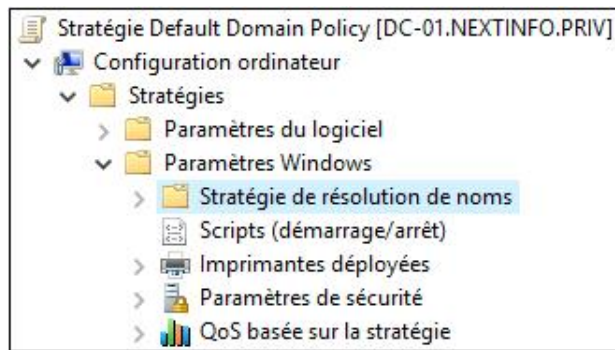
- **Étape 2** : développez l'arborescence et sélectionnez l'objet de stratégie de groupe (GPO), nommé **Default Domain Policy** :



- **Étape 3** : affichez le menu contextuel et cliquez sur **Modifier...** :



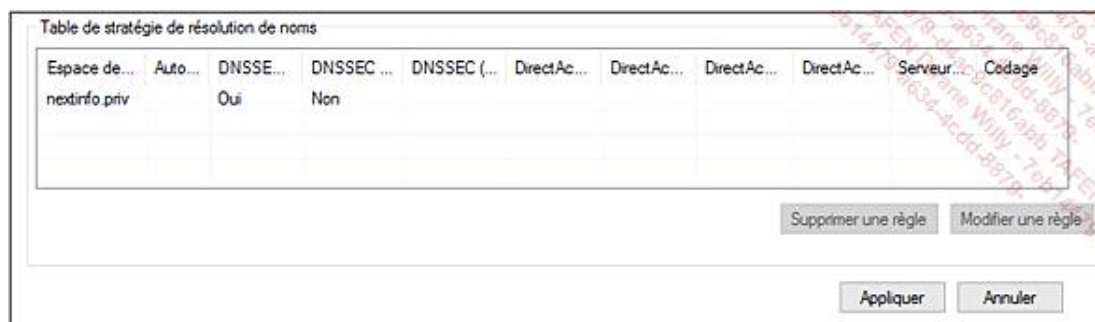
- **Étape 4** : développez l'arborescence de la console et sélectionnez le nœud suivant : **Configuration ordinateur\Stratégies\Paramètres Windows\Stratégie de résolution de noms** :



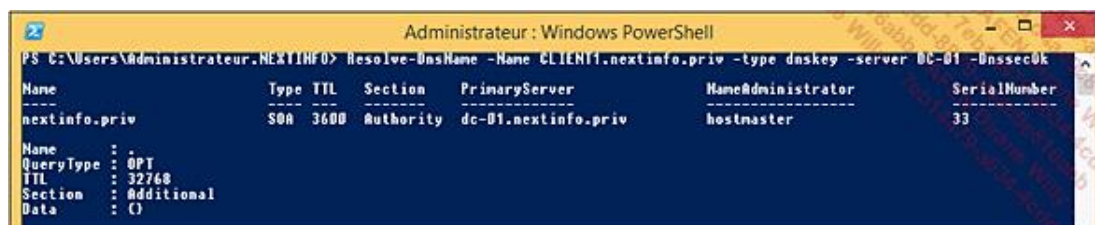
→ **Étape 5** : remplissez la règle de stratégie de résolution de noms afin d'alimenter la table NRPT et cliquez sur **Créer** :

- Dans le champ **À quelle partie de l'espace de noms s'applique cette règle ?**, sélectionnez **Nom de domaine complet** dans la liste déroulante, puis tapez **nextinfo.priv**.
- Dans l'onglet **DNSSEC**, cochez les cases **Activer DNSSEC dans cette règle** et **Demander aux clients DNS de vérifier que les données de nom et d'adresse ont été validées par le serveur DNS**.

→ **Étape 6** : vérifiez que la règle créée précédemment figure bien dans la table de stratégie de résolution de noms (NRPT), et cliquez sur **Appliquer** :



- **Étape 7** : fermez l'éditeur de gestion des stratégies de groupe et exécutez la commande DOS `gpupdate /force`.
- **Étape 8** : connectez-vous sur le poste **CLIENT1**, ouvrez une fenêtre DOS et exécutez la commande `gpupdate /force`. Cette opération a pour but d'actualiser les stratégies de sécurité du domaine.
- **Étape 9** : toujours sur **CLIENT1**, ouvrez une fenêtre PowerShell et tapez la commande `Resolve-dnsname -name CLIENT1.nextinfo.priv -type dnskey -server DC-01 -dnssecok`. On interroge ainsi des enregistrements DNSSEC de la zone *nextinfo.priv*.



3. Installer et configurer le service DHCP

Ce TP a pour but d'installer et de configurer les principales options du rôle de serveur DHCP. À ce stade, le domaine *Nextinfo.priv* doit être créé.

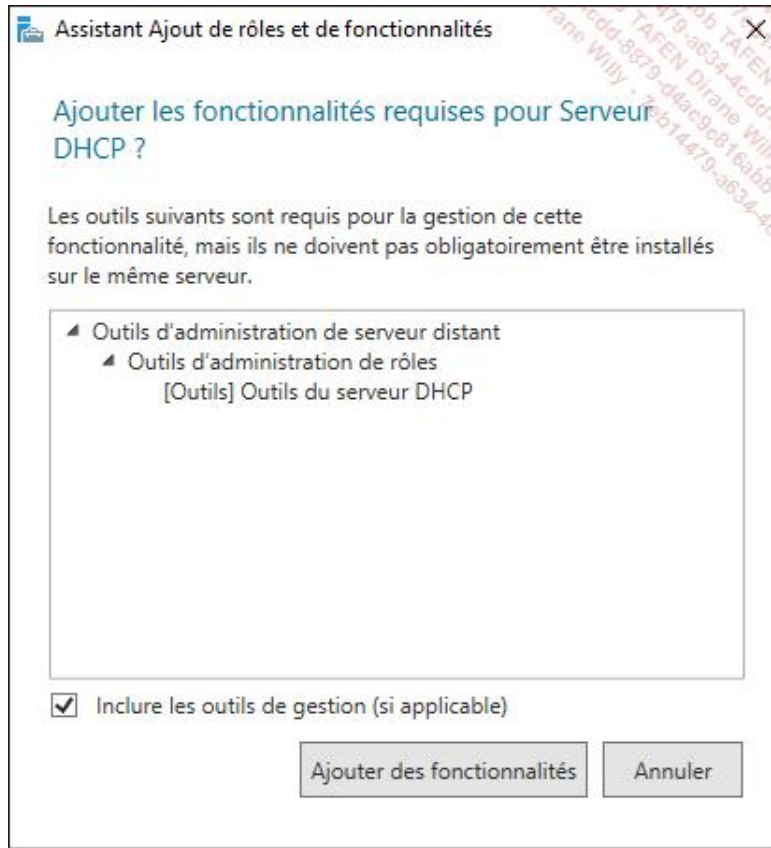
Installer le rôle de serveur DHCP

- **Étape 1** : sur le serveur **DC-01**, ouvrez le Gestionnaire de serveur et cliquez sur **Ajouter des rôles et des fonctionnalités**.

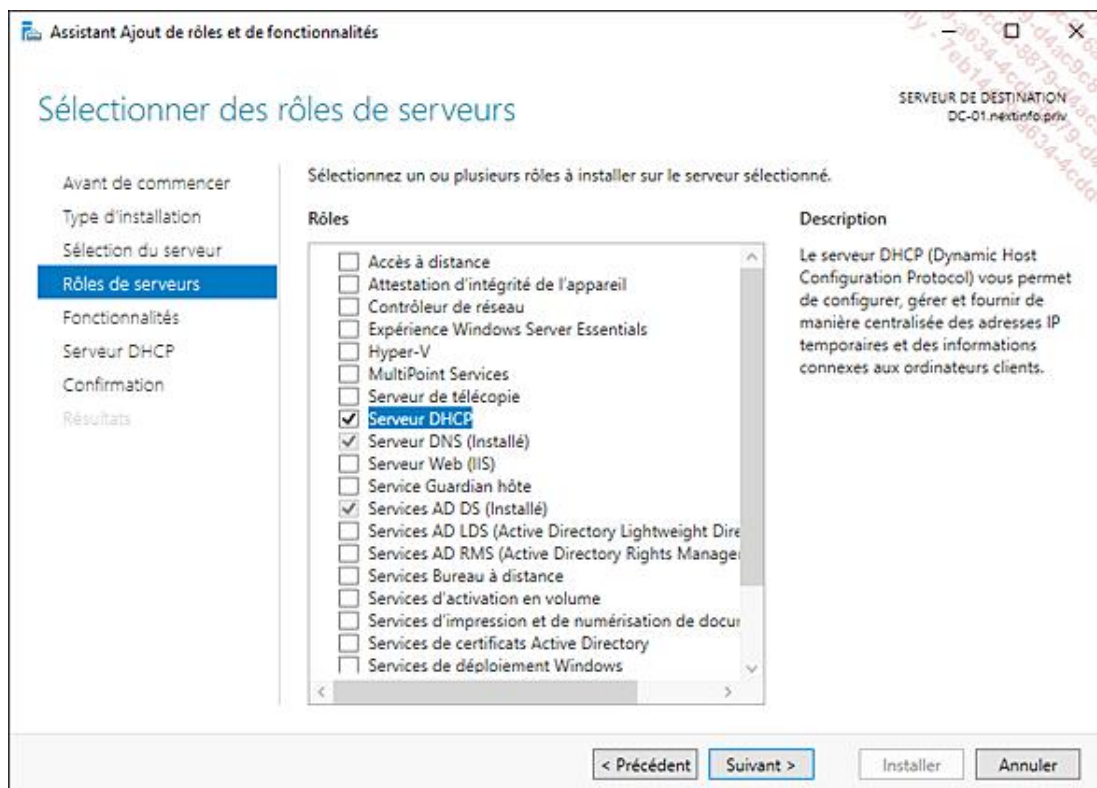


- **Étape 2** : cliquez sur **Suivant** dans la fenêtre **Avant de commencer**.

- **Étape 3** : cliquez sur **Suivant** à l'étape **Sélectionner le type d'installation**.
- **Étape 4** : cliquez sur **Suivant** à l'étape **Sélectionner le serveur de destination**.
- **Étape 5** : dans la fenêtre **Sélectionner des rôles de serveurs**, cochez la case correspondant au rôle de **Serveur DHCP**.
- **Étape 6** : cliquez sur **Ajouter des fonctionnalités** :

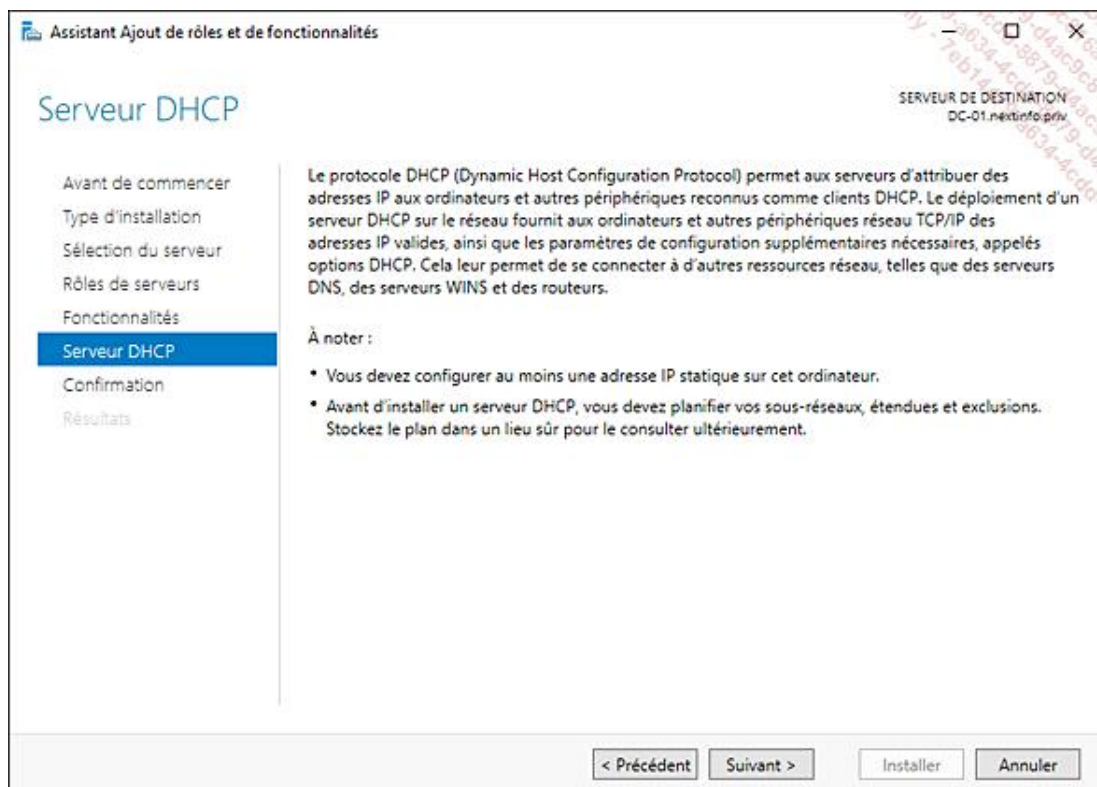


- **Étape 7** : cliquez sur **Suivant** :

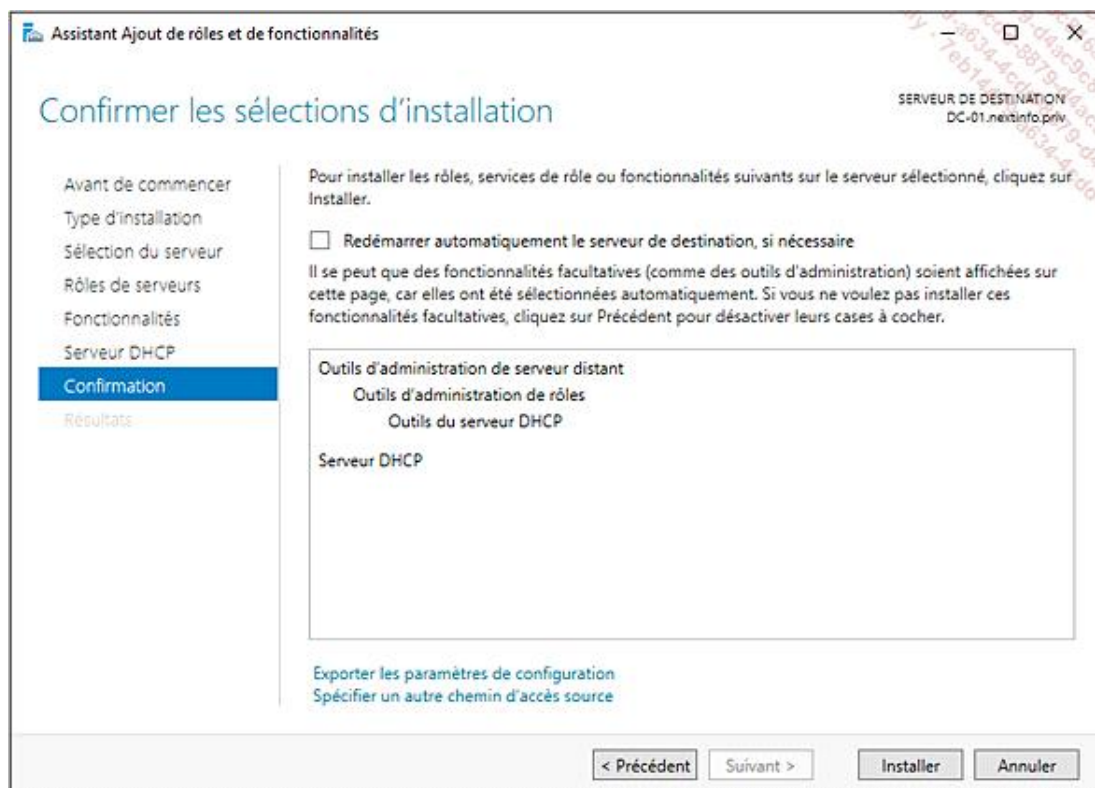


→ **Étape 8** : cliquez sur **Suivant** à l'étape **Sélectionner des fonctionnalités**.

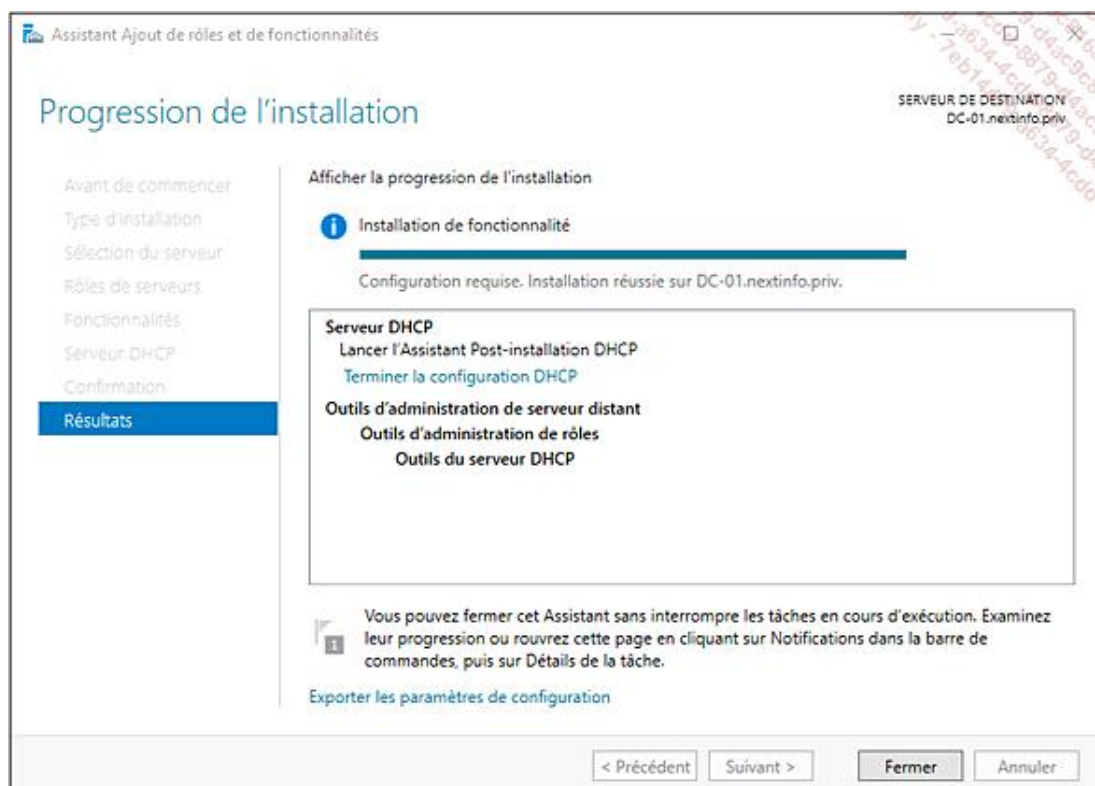
→ **Étape 9** : cliquez sur **Suivant** :



→ **Étape 10** : cliquez sur **Installer** :



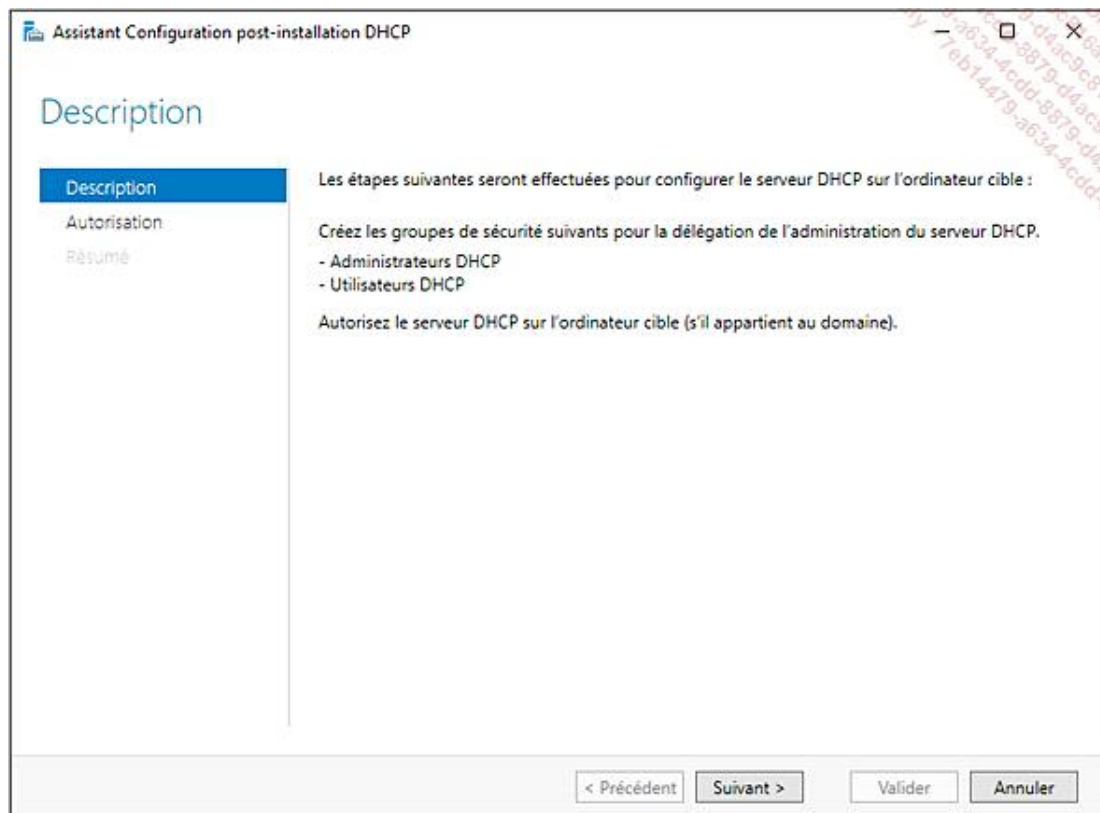
→ **Étape 11** : cliquez sur **Fermer** :



→ **Étape 12** : dans le tableau de bord de la console **Gestionnaire de serveur**, cliquez sur le panneau de signalisation jaune avec le point d'exclamation et cliquez sur **Terminer la configuration DHCP** :



→ **Étape 13** : cliquez sur **Suivant** :



→ **Étape 14** : cliquez sur **Valider** pour autoriser le serveur DHCP dans Active Directory :

Assistant Configuration post-installation DHCP

Autorisation

Description

Autorisation

Résumé

Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.

☒ Utiliser les informations d'identification de l'utilisateur suivant

Nom d'utilisateur :

☐ Utiliser d'autres informations d'identification

Nom d'utilisateur :

☐ Ignorer l'autorisation AD

< Précédent Suivant > Valider Annuler

→ **Étape 15** : cliquez sur **Fermer** :

Assistant Configuration post-installation DHCP

Résumé

Description

Autorisation

Résumé

L'état des étapes de configuration post-installation est indiqué ci-dessous :

Création des groupes de sécurité	Terminé
Redémarrez le service Serveur DHCP sur l'ordinateur cible pour que les groupes de sécurité soient effectifs.	
Autorisation du serveur DHCP	Terminé

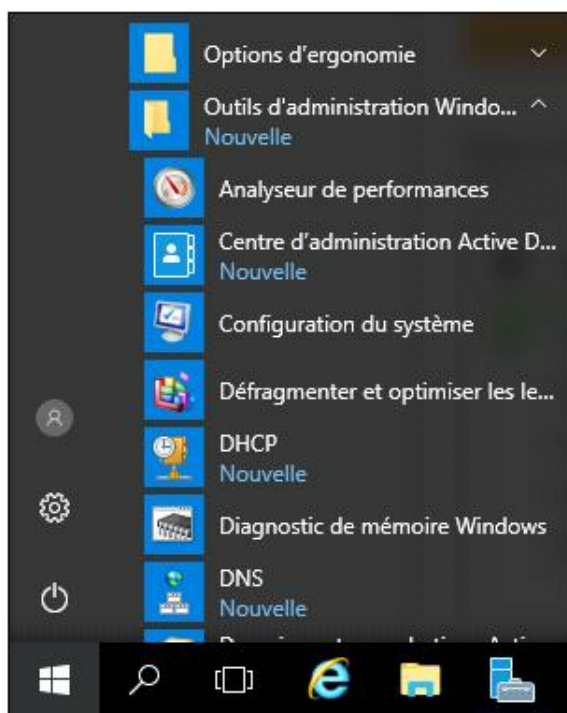
< Précédent Suivant > **Fermer** Annuler

➤ Le service DHCP est désormais installé et autorisé dans Active Directory pour la distribution d'adresses IP sur le réseau.

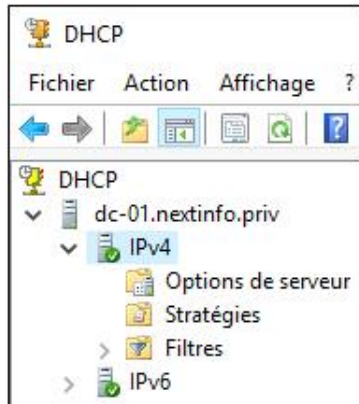
→ **Étape 16** : répétez les étapes 1 à 15 pour installer le rôle de serveur DHCP sur le serveur **DC-02**.

Créer une nouvelle étendue DHCP - IPv4

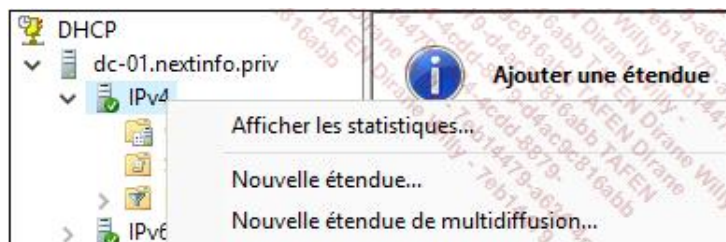
→ **Étape 1** : ouvrez le menu **Démarrer** du serveur **DC-01** et cliquez sur l'icône **DHCP** :



→ **Étape 2** : développez l'arborescence de la console et sélectionnez le protocole **IPv4** :



→ **Étape 3** : affichez le menu contextuel et cliquez sur **Nouvelle étendue...** :



→ **Étape 4** : dans la fenêtre **Assistant Nouvelle étendue**, cliquez sur **Suivant**.

→ **Étape 5** : dans le champ **Nom**, tapez **Etendue DHCP NEXTINFO**, puis dans le champ **Description**, tapez **Serveur : DC-01** :

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 :

Description :

< Précédent **Suivant >** Annuler

→ **Étape 6** : dans le champ **Adresse IP de début**, tapez **192.168.0.150**, puis dans le champ **Adresse IP de fin**, tapez **192.168.0.250** et cliquez 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 :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< Précédent **Suivant >** Annuler

→ **Étape 7** : dans la section **Ajout d'exclusions et de retard**, cliquez sur **Suivant**.

→ **Étape 8** : laissez la durée du bail DHCP par défaut et cliquez sur **Suivant** :

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

→ **Étape 9** : cochez la case **Oui, je veux configurer ces options maintenant** et cliquez sur **Suivant** :

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

→ **Étape 10** : dans le champ **Adresse IP**, tapez l'adresse de la passerelle par défaut qui sera configurée pour tous les clients DHCP, puis cliquez sur **Ajouter** et cliquez sur **Suivant** :

Assistant Nouvelle étendue

Routeur (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 :

192.168.0.254	Ajouter
	Supprimer
	Monter
	Descendre

< Précédent Suivant > Annuler

→ **Étape 11** : cliquez sur **Suivant** :

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 : nextinfo.priv

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 :	Ajouter
	192.168.0.100	Supprimer
		Monter
		Descendre

Résoudre

< Précédent Suivant > Annuler

→ **Étape 12** : cliquez sur **Suivant** :

Assistant Nouvelle étendue

Serveurs WINS

Les ordinateurs fonctionnant avec Windows peuvent utiliser les serveurs WINS pour convertir les noms NetBIOS d'ordinateurs en adresses IP.

Entrer les adresses IP ici permet aux clients Windows d'interroger WINS avant d'utiliser la diffusion pour s'enregistrer et résoudre les noms NetBIOS.

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

Pour modifier ce comportement pour les clients DHCP Windows, modifiez l'option 046, type de nœud WINS/NBT, dans les options de l'étendue.

< Précédent **Suivant >** Annuler

→ **Étape 13** : cochez la case **Oui, je veux activer cette étendue maintenant** et cliquez sur **Suivant** :

Assistant Nouvelle étendue

Activer l'étendue

Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.

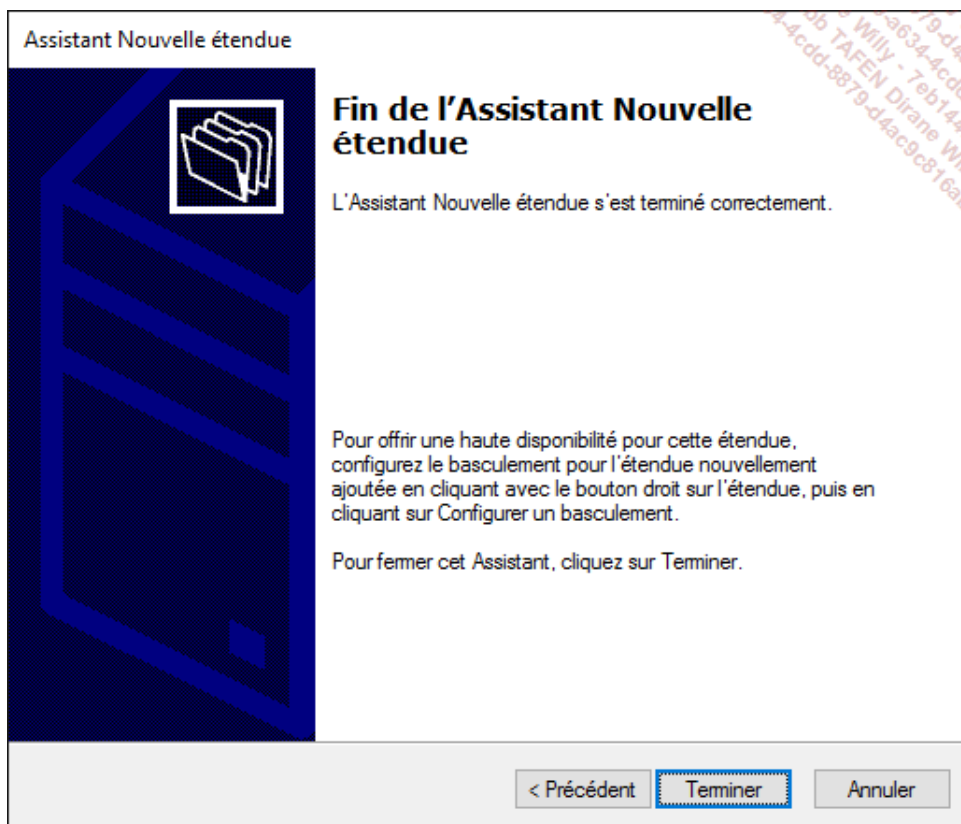
Voulez-vous activer cette étendue maintenant ?

☒ **Oui, je veux activer cette étendue maintenant**

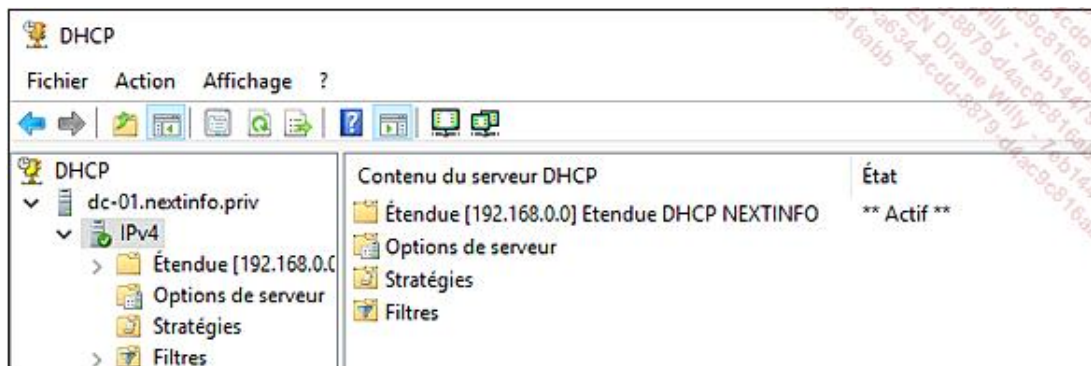
☐ Non, j'activerai cette étendue ultérieurement

< Précédent **Suivant >** Annuler

→ **Étape 14** : cliquez sur **Terminer** :

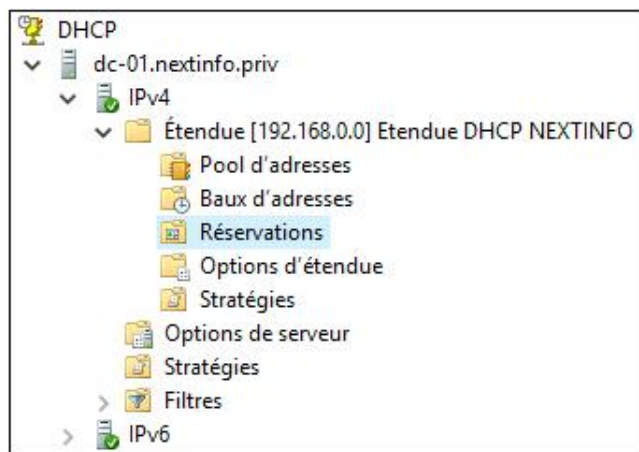


→ **Étape 15** : vérifiez dans la console que l'étendue créée précédemment apparaît avec un état **Actif** :

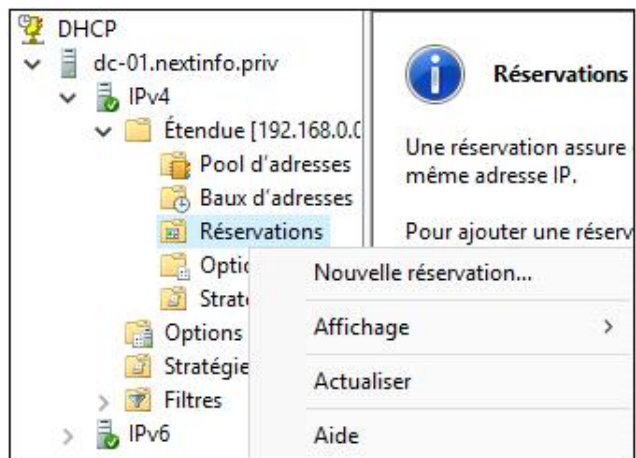


Créer une réservation DHCP

→ **Étape 1** : développez l'arborescence de la console et sélectionnez le dossier **Réservations** :

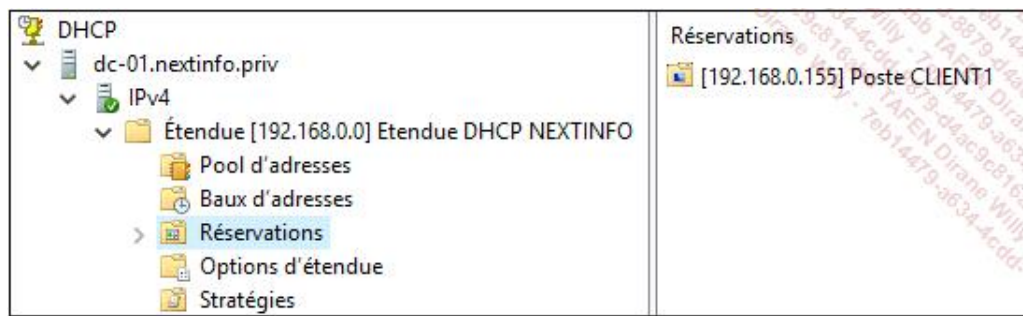


→ **Étape 2** : affichez le menu contextuel et cliquez sur **Nouvelle réservation** :



→ **Étape 3** : tapez le nom de réservation **Poste CLIENT1**, l'adresse IP **192.168.0.155**, l'adresse MAC correspondante à la carte réseau de votre machine virtuelle CLIENT1 et la description **IP CLIENT1** puis cliquez sur **Ajouter**, puis sur **Fermer** :

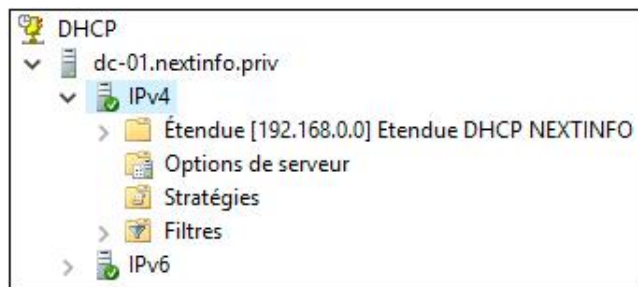
→ **Étape 4** : vérifiez que la réservation d'adresse IP pour le poste CLIENT1 apparaît :



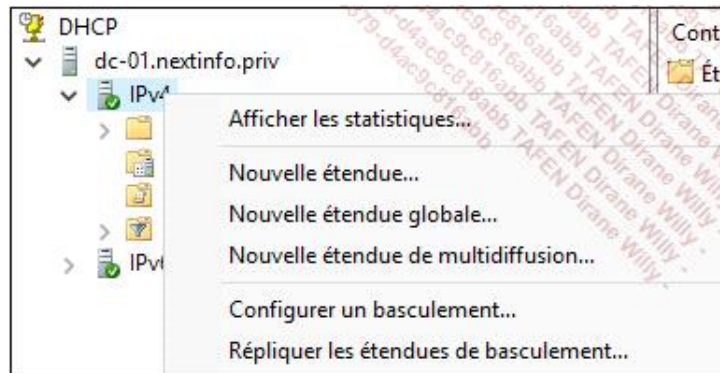
- **Étape 5** : connectez-vous sur le poste **CLIENT1** et assurez-vous que la carte réseau est configurée pour recevoir une adresse IP automatiquement. Tapez ensuite la commande **ipconfig /renew**.
- **Étape 6** : tapez la commande **ipconfig**, et vérifiez que l'adresse IP est bien **192.168.0.155**.

4. Installer et configurer la haute disponibilité du service DHCP

- **Étape 1** : ouvrez le menu **Démarrer** du serveur **DC-01** et cliquez sur l'icône **DHCP**.
- **Étape 2** : développez l'arborescence et sélectionnez le protocole **IPv4** :



- **Étape 3** : affichez le menu contextuel et cliquez sur **Configurer un basculement....**



- **Étape 4** : cliquez sur **Suivant** :



→ **Étape 5** : cliquez sur **Ajouter un serveur** :

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

- **Étape 6** : cochez la case **Ce serveur DHCP autorisé**, sélectionnez le serveur DHCP **dc-02.nextinfo.priv** et cliquez sur **OK** :

Ajouter un serveur

Sélectionnez un serveur que vous voulez ajouter à votre console.

☐ Ce serveur :

☐ **Ce serveur DHCP autorisé :**

Nom	Adresse IP
dc-01.nextinfo.priv	192.168.0.100
dc-02.nextinfo.priv	192.168.0.101

- **Étape 7** : vérifiez qu'un serveur partenaire est bien sélectionné et cliquez sur **Suivant** :

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

☐ Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

< Précédent **Suivant >** Annuler

→ **Étape 8** : cochez la case **Activer l'authentification du message** et tapez un mot de passe dans le champ **Secret partagé**. Cliquez ensuite sur **Suivant**.

Configurer un basculement

Créer une relation de basculement

Créer une relation de basculement avec le partenaire dc-02.nextinfo.priv

Nom de la relation : dc-01.nextinfo.priv-dc-02.nextinfo.priv

Délai de transition maximal du client (MCLT) : 1 heures 0 minutes

Mode : Équilibrage de charge

Pourcentage d'équilibrage de charge

Serveur local : 50 %

Serveur partenaire : 50 %

☐ Intervalle de basculement d'état : 60 minutes

☒ Activer l'authentification du message

Secret partagé :

< Précédent Suivant > Annuler

- **Étape 9** : vérifiez les informations du résumé et cliquez sur **Terminer**.
- **Étape 10** : assurez-vous de la réussite de chaque étape du basculement, puis cliquez sur **Fermer** :

Configurer un basculement

Progression de la configuration du basculement.

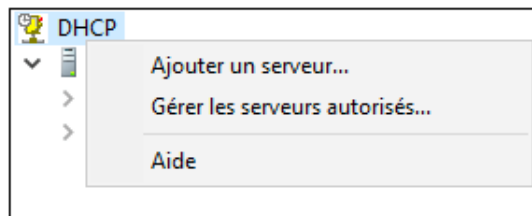
Le journal ci-dessous montre la progression des diverses tâches de configuration du basculement, ainsi que les erreurs rencontrées.

Ajouter des étendues sur le serveur partenaireRéussite
 Désactiver des étendues sur le serveur partenaireRéussite
 Création de la config. du basculement sur le serveur partenaireRéussit
 Création de la configuration du basculement sur le serveur hôteRéussi
 Activer des étendues sur le serveur partenaireRéussite
 Réussite de la configuration du basculement.

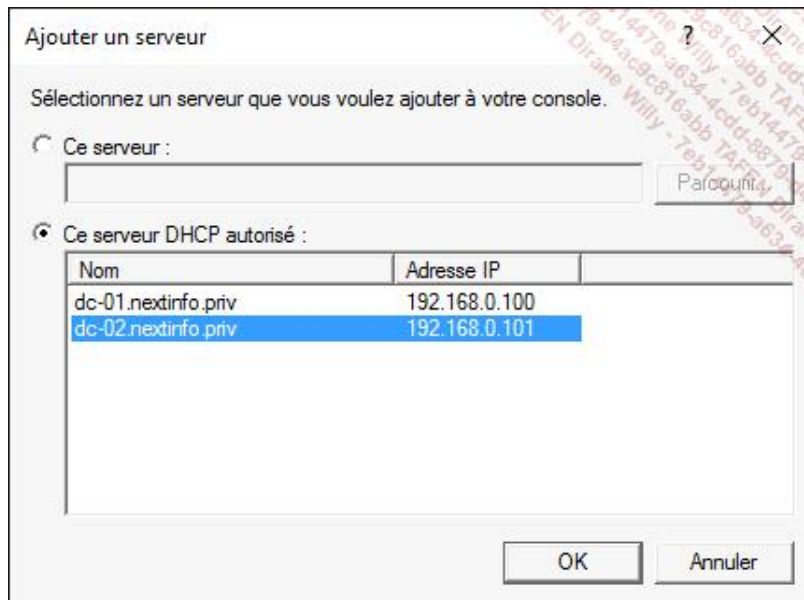
< >

Fermer

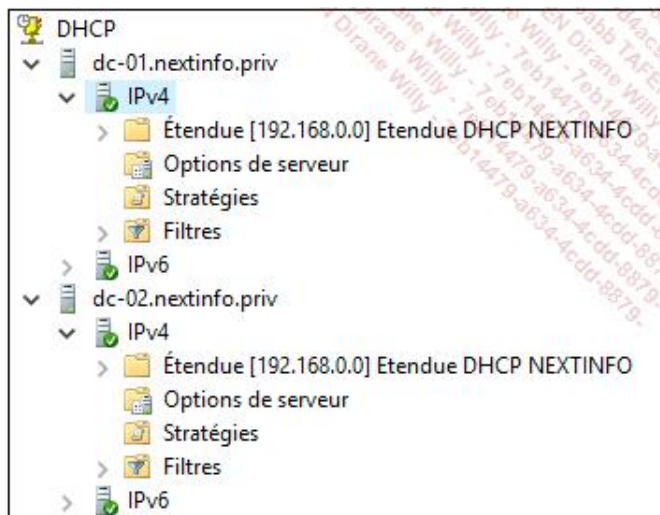
- **Étape 11** : dans l'arborescence de la console, sélectionnez DHCP et cliquez sur **Ajouter un serveur...** :



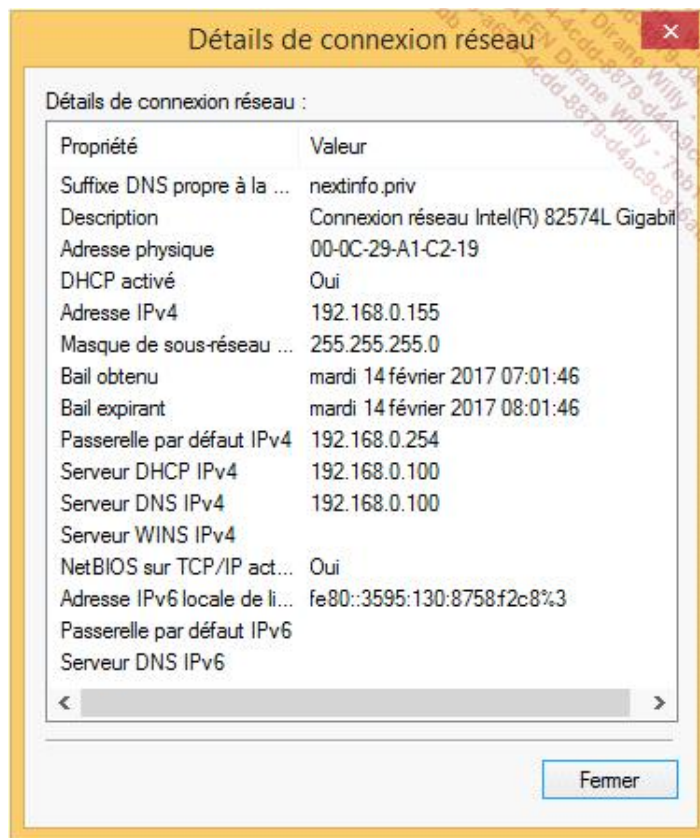
- **Étape 12** : cochez la case **Ce serveur DHCP autorisé**, sélectionnez le serveur **dc-02.nextinfo.priv** et cliquez sur **OK** :



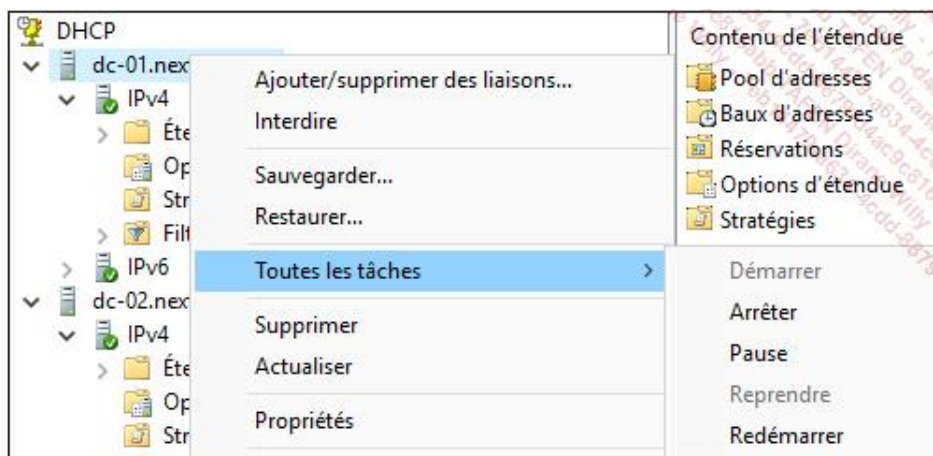
- **Étape 13** : développez l'arborescence du serveur **dc-02.nextinfo.priv** jusqu'au protocole **IPv4** afin de vérifier que l'étendue créée sur le serveur **DC-01** a bien été répliquée :



- **Étape 14** : ouvrez une session sur le poste **CLIENT1**, puis affichez les détails de connexion de la carte réseau. Identifiez et mémorisez l'adresse IP du **serveur DHCP IPv4** :



→ **Étape 15** : basculez sur le serveur **DC-01**, puis dans la console DHCP, arrêtez le service sur le serveur **dc-01.nextinfo.priv** :



→ **Étape 16** : basculez de nouveau sur le poste **CLIENT1** et exécutez consécutivement les commandes DOS suivantes **ipconfig /release** puis **ipconfig /renew**.

```
C:\Users\Administrateur.NEXTINFO>ipconfig /renew

Configuration IP de Windows

Carte Ethernet Ethernet0 :

Suffixe DNS propre à la connexion. . . : nextinfo.priv
Adresse IPv6 de liaison locale. . . . : fe80::3595:130:8758:f2c8%3
Adresse IPv4. . . . . : 192.168.0.155
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.0.254

C:\Users\Administrateur.NEXTINFO>
```

→ **Étape 17** : affichez les propriétés de la carte réseau pour constater que le serveur DHCP IPv4 a bien basculé sur le serveur DHCP de secours hébergé sur le serveur dc-02.nextinfo.priv (192.168.0.101) :

