

DNS (Domain Name System)

Système de gestion des noms de domaines

L' **ICANN** est un organisme qui gère la liste des **Top Level Domain (TLD)**

Il existe une TLD par pays
(*.fr pour France, .it pour Italie, .de pour l'Allemagne, etc.*)
et quelques TLD générales (*.com, .net, .org, .mil, .biz...*)

L'**ICANN** délègue la gestion de chaque TLD à un organisme (**registry**).

DNS (Domain Name System)

Système de gestion des noms de domaines

Les **registry** doivent tenir à jour la liste des domaines définis sur sa ou ses TLD.

AFNIC tient le registre des *.fr*

VeriSign tient le registre des
.com/.net/.org/.name/.info/.biz.

Chaque **registry** peut gérer comme bon lui semble l'attribution des noms de domaine sur sa TLD.

Les **registry** ont un **rôle technique**

DNS (Domain Name System)

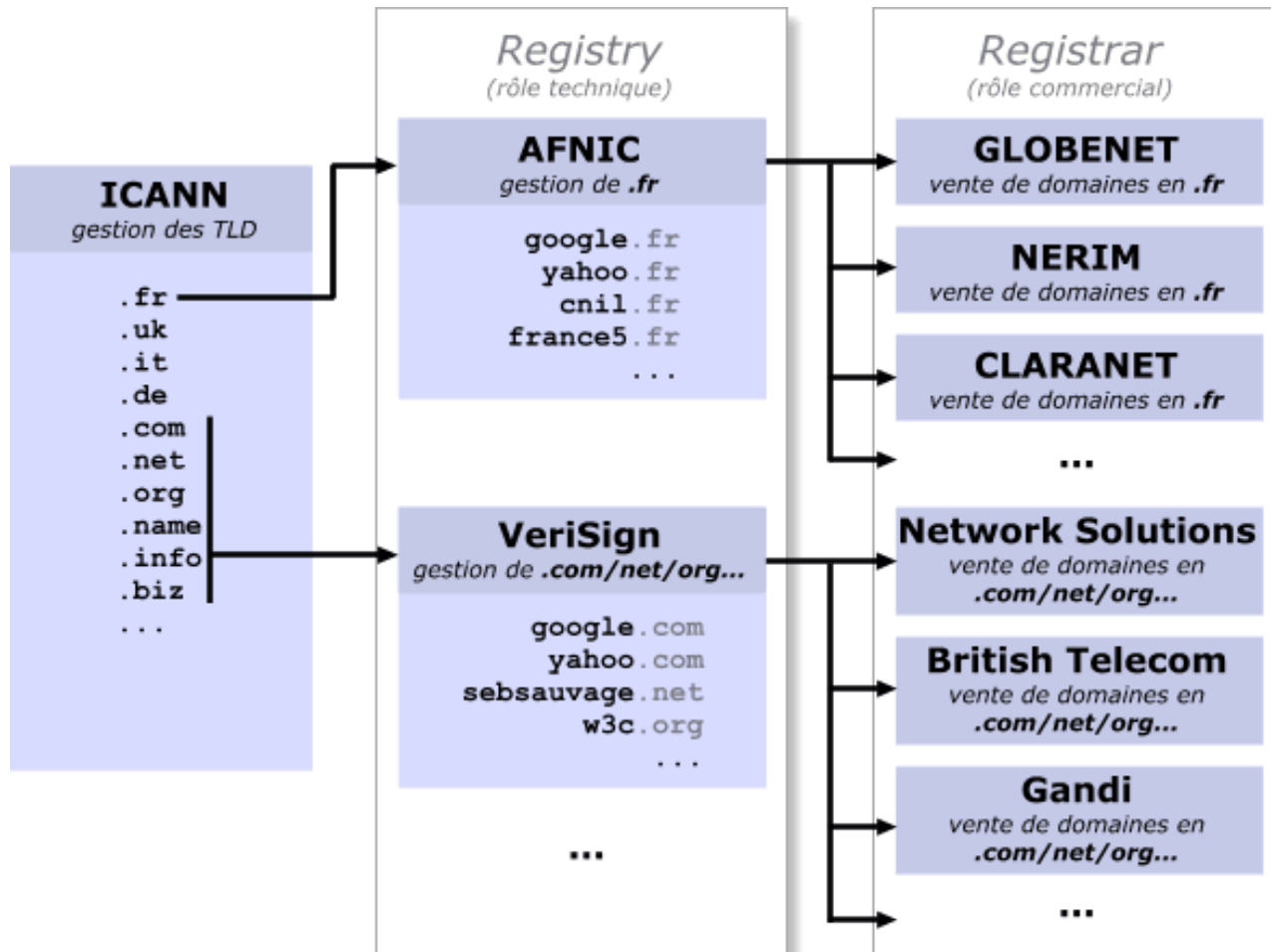
Système de gestion des noms de domaines

Chaque **registry** autorise des **registrars** à vendre des noms de domaine.

Les **registrars** ont un **rôle commercial**.

DNS (Domain Name System)

Système de gestion des noms de domaines



DNS (Domain Name System)

Système de gestion des noms de domaines

Chaque pays possède un **TLD** qui correspond à son code pays ISO

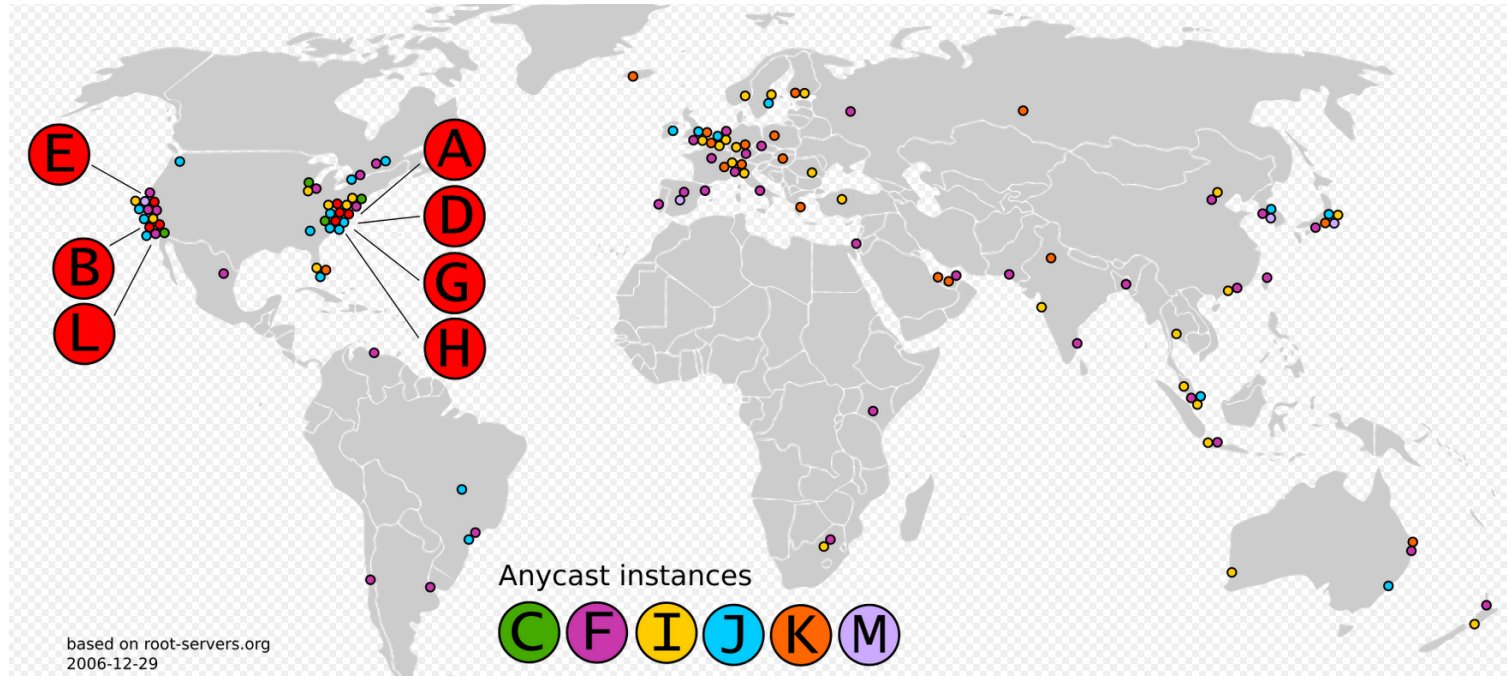
(fr=France, it=Italie, de=Allemagne, uk=Grande-Bretagne, ca=Canada, pl=Pologne, be=Belgique, etc.).

On les appelle **ccTLD** (*Country-code TLD*)

La gestion de ces **TLD** repose sur des **serveurs racines** (appelés ***DNS root servers***).

DNS (Domain Name System)

Système de gestion des noms de domaines

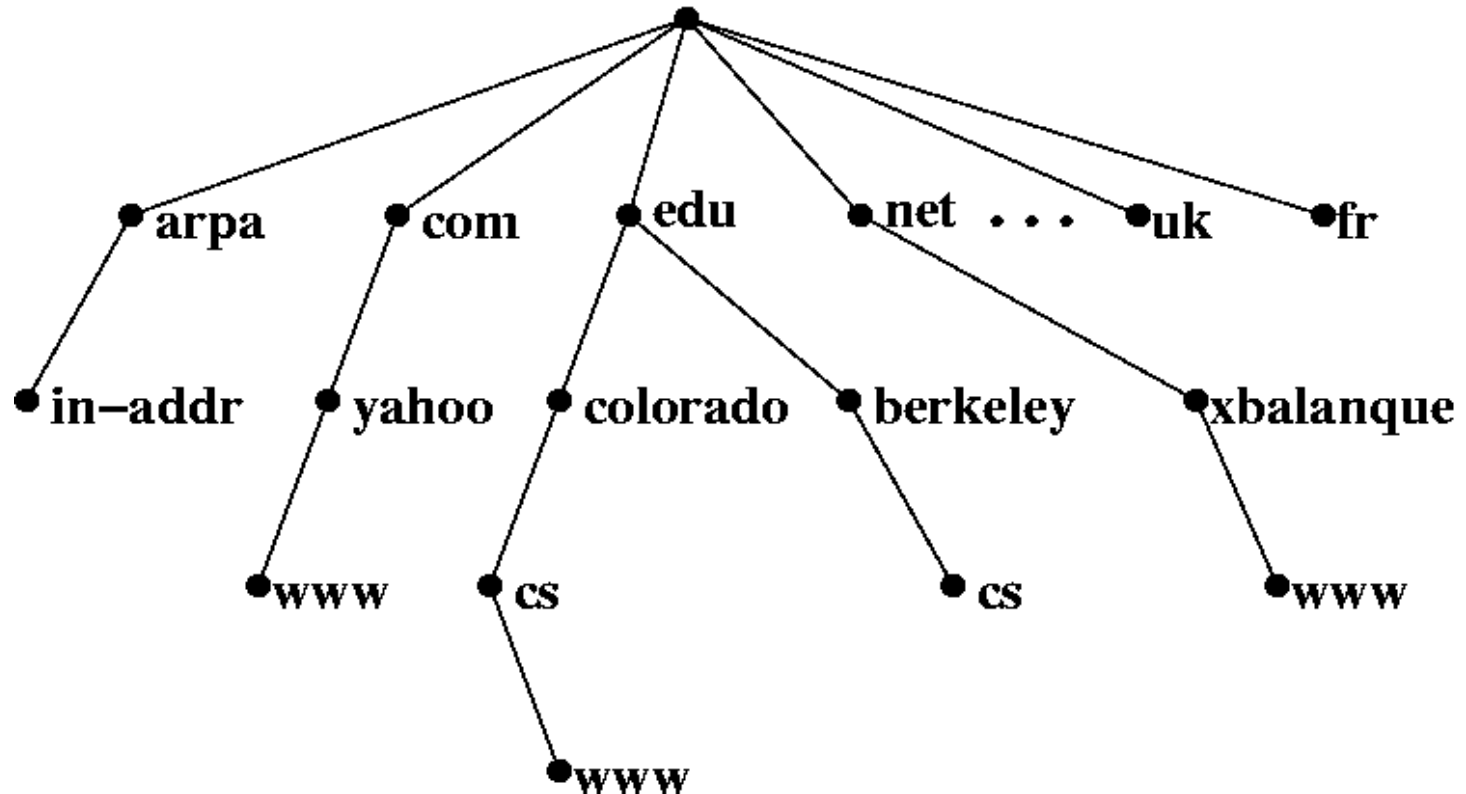


DNS (Domain Name System)

Lettre	adresse IPv4	adresse IPv6	Ancien nom	Société	Localisation	Sites	Logiciel
A	198.41.0.4	2001:503:BA3E::2:30	ns.internic.net	VeriSign	trafic distribué par anycast	6	BIND
B	192.228.79.201	2001:478:65::53	ns1.isi.edu	USC-ISI ^(en)	Marina Del Rey, Californie, États-Unis	1	BIND v4
C	192.33.4.12		c.psi.net	Cogent Communications	trafic distribué par anycast	6	BIND
D	128.8.10.90		terp.umd.edu	Université Maryland du	College Park, Maryland, États-Unis	1	BIND
E	192.203.230.10		ns.nasa.gov	NASA	Mountain View, Californie, États-Unis	1	BIND
F	192.5.5.241	2001:500:2f:f	ns.isc.org	ISC	trafic distribué par anycast	49	BIND
G	192.112.36.4		ns.nic.ddn.mil	Defense Information Systems Agency ^(en)	trafic distribué par anycast	6	BIND
H	128.63.2.53	2001:500:1::803f:235	aos.arl.army.mil	United States Army Research Laboratory ^(en)	Aberdeen ^(en) , Maryland, États-Unis	1	NSD
I	192.36.148.17	2001:7fe::53	nic.nordu.net	Autonomica ^(en)	trafic distribué par anycast	34	BIND
J	192.58.128.30	2001:503:C27::2:30		VeriSign	trafic distribué par anycast	70	BIND
K	193.0.14.129	2001:7fd::1		RIPE-NCC	trafic distribué par anycast	18	NSD
L	199.7.83.42	2001:500:3::42		ICANN	trafic distribué par anycast	7	NSD
M	202.12.27.33	2001:dc3::35		WIDE ^(en)	trafic distribué par anycast	6	NSD BIND

DNS (Domain Name System)

Système de gestion des noms de domaines



DNS (Domain Name Service) = service TCP/IP

Permet la correspondance entre un nom de domaine qualifié FQDN (*Fully Qualified Domain Name*) et une adresse IP

Exemple : `www.google.fr` = `74.125.230.82`

Domaine Inverse

Résolution d'une adresse IP en nom de domaine avec l'ajout d'un domaine spécial **in-addr.arpa** à la fin

Exemple : réseau 10.1.0.0. Adresse inverse : 1.10.in-addr.arpa
réseau 192.168.1.0 Adresse inverse : 1.168.192.in-addr.arpa

Délégation

Transfert de responsabilité dans l'administration d'une zone DNS avec autorité pour les serveurs de la zone de la résolution de noms

Zone primaire et zone secondaire

Transfert de zones entre serveur maître (primaire) et un autre serveur (secondaire), chacun ayant autorité sur la zone.

Vis-à-vis d'un client, l'un ou l'autre répond en fonction de la vitesse du réseau

Scénarios possibles

- **Serveur cache**
- **Serveur primaire (maître)**
- **Serveur secondaire (esclave)**
- **Serveur stub**

Serveur cache

But : Effectuer des requêtes DNS pour se rappeler de la réponse pour la prochaine requête

Avantages : Réduction de la bande passante
Réduction du temps de latence

Serveur primaire (maître)

But : Contenir des **enregistrements DNS** d'un nom de domaine enregistré

Un ensemble d'enregistrements DNS pour un nom de domaine est appelé une « **zone** »

Le nom de domaine peut être imaginaire, mais seulement sur un réseau local fermé, non connecté à Internet

Serveur secondaire (esclave)

But : Contenir une copie des zones configurées sur le serveur maître

Avantages :

- Recommandé sur les réseaux importants**
- Assure la disponibilité de la zone DNS si le serveur maître n'est pas disponible**

Serveur stub

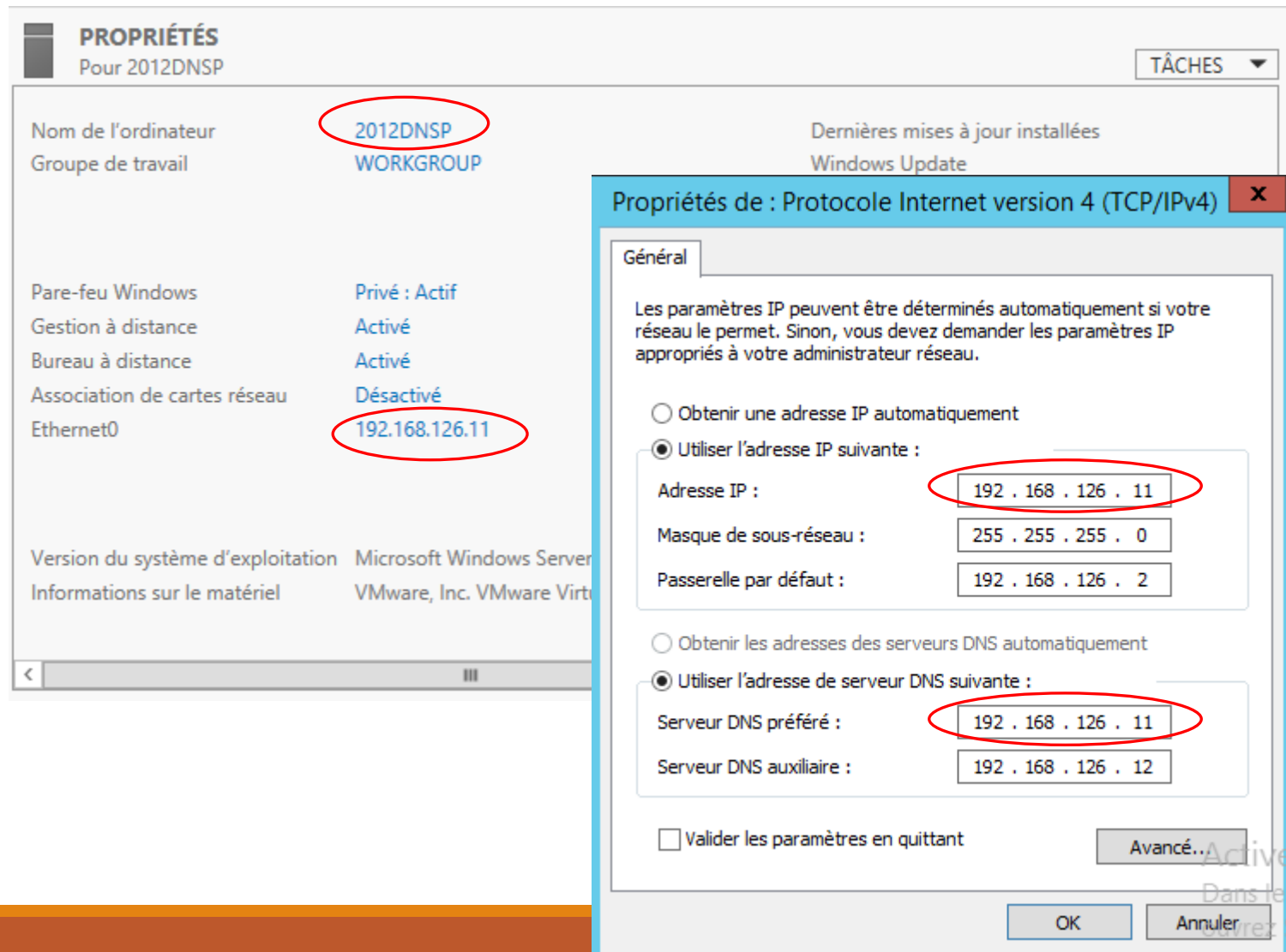
But : Idem que le serveur esclave, mais copie uniquement les données du serveur et pas les données de l'hôte

Enregistrements DNS

But : mapper nom d'hôte / adresse IP et adresse IP / nom d'hôte

Enregistrements	Mappages
SOA (Start Of Authority)	Serveur DNS de la zone principale / Adresse IP
NS (Name Server)	Serveurs DNS / Adresses IP
A	Hôte / Adresse IP v4
AAAA	Hôte / Adresse IP v6
PTR (PoinTeR)	Adresse IP / Hôte (recherche inversée)
CNAME (Canonical NAME)	Hôte / Hôte (alias)
MX (Mail eXchanger)	Serveur de messagerie / Adresse IP

Pré-configuration : nom Netbios + adressage IP



Installation du rôle DNS

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES RÔLES DE SERVEURS

SERVEUR DE DESTINATION
2012DNSP

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

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

Rôles

- ☐ Accès à distance
- ☐ Expérience Windows
- ☐ Hyper-V
- ☐ Serveur d'application
- ☐ Serveur de télécopie
- ☐ Serveur DHCP
- ☒ **Serveur DNS**
- ☐ Serveur Web (IIS)
- ☐ Services AD DS
- ☐ Services AD FS (Activ)
- ☐ Services AD LDS (Act)
- ☐ Services AD RMS (Ac)
- ☐ Services Bureau à dis
- ☐ Services d'activation

Ajouter les fonctionnalités requises pour Serveur DNS ?

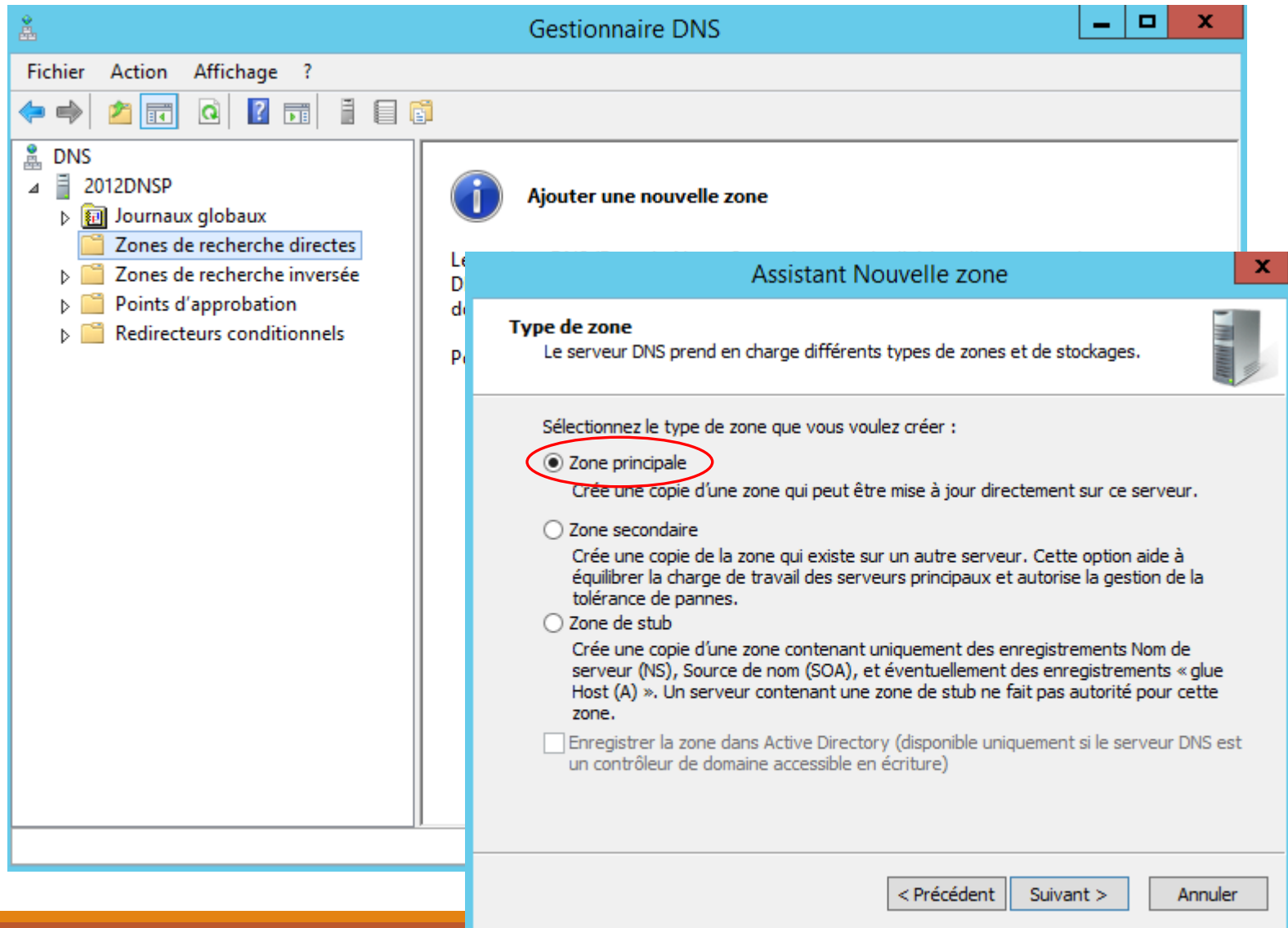
Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.

- ▲ Outils d'administration de serveur distant
 - ▲ Outils d'administration de rôles
 - [Outils] Outils du serveur DNS

☒ Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités Annuler

Configuration zone primaire (principale)



Configuration zone primaire (principale)

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 :

cd.local.dns

☐ Utiliser un fichier existant :

Pour utiliser ce fichier, il doit être situé dans le répertoire %SystemRoot%\System32\DNS

Assistant Nouvelle zone

Mise à niveau dynamique

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

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour dynamiquement leurs enregistrements de ressources avec un serveur DNS. 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 par n'importe quel client.

⚠ Cette option peut mettre en danger la sécurité de vos données car les mises à jour dynamiques non sécurisées 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 pour cette zone. Vous devez mettre à jour ces enregistrements manuellement.

Assistant Nouvelle zone

Fin de l'Assistant Nouvelle zone

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

Nom : cd.local

Type : Zone principale standard

Type de recherche : Directe

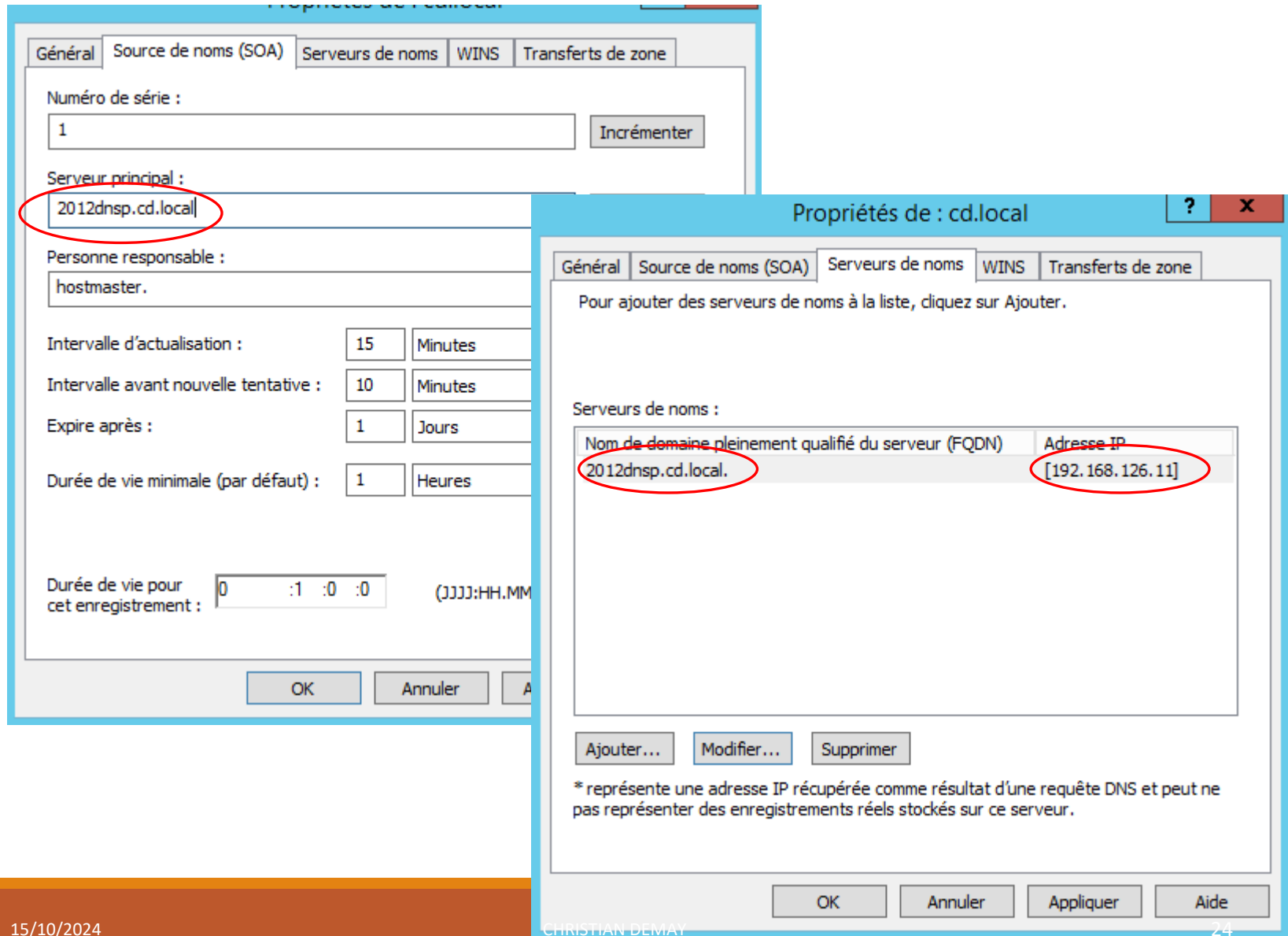
Nom de fichier : cd.local.dns

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent Suivant > Annuler

Configuration des enregistrements SOA et NS



Configuration zone de recherche inversée

The image displays three overlapping screenshots of the 'Assistant Nouvelle zone' (New Zone Wizard) in Windows DNS Manager, illustrating the steps to create an IPv4 reverse lookup zone.

First Screenshot (Left): The 'Type de zone' (Zone Type) screen. It explains that the DNS server handles different zone types and storage. The instruction is to 'Sélectionnez le type de zone que vous voulez créer :'. The 'Zone principale' (Primary zone) option is selected and circled in red. Other options include 'Zone secondaire' (Secondary zone), 'Zone de stub' (Stub zone), and an unchecked checkbox for 'Enregistrer la zone d'un contrôleur de domaine' (Register the zone of a domain controller).

Second Screenshot (Middle): The 'Nom de la zone de recherche inversée' (Reverse lookup zone name) screen. It explains that a reverse lookup zone translates IP addresses into DNS names. The instruction is to 'Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6'. The 'Zone de recherche inversée IPv4' (IPv4 reverse lookup zone) option is selected and circled in red. The 'Zone de recherche inversée IPv6' (IPv6 reverse lookup zone) option is also visible. Navigation buttons '< Précédent' and 'Suivant >' are at the bottom.

Third Screenshot (Right): The 'Nom de la zone de recherche inversée' (Reverse lookup zone name) screen, continuing from the previous step. It instructs to 'Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.' The 'ID réseau' (Network ID) option is selected and circled in red. A text box contains the IP address '192.168.126'. Below this, it explains that the network ID is the part of the IP address that belongs to the zone and should be entered in its normal order. An example is given: 'L'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.' The 'Nom de la zone de recherche inversée' (Reverse lookup zone name) option is also visible, with a text box containing '126.168.192.in-addr.arpa'.

Configuration zone de recherche inversée

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 :

126.168.192.in-addr.arpa.dns

☐ Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez que le chemin est correct : %SystemRoot%\system32\dns sur c

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 les mises à jour dynamiques d'enregistrement de ressources n'importe quel client.

⚠ Cette option peut mettre en danger la sécurité de vos données. Les mises à jour dynamiques non sécurisées 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 autorisées pour cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent

Assistant Nouvelle zone

Fin de l'Assistant Nouvelle zone

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

Nom : 126.168.192.in-addr.arpa

Type : Zone principale standard

Type de recherche : Inversée

Nom de fichier : 126.168.192.in-

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent Terminer Annuler

Configuration des enregistrements SOA et NS

Propriétés de : 126.168.192.in-addr.arpa

Général Source de noms (SOA) Serveurs de noms WINS-R Transferts de zone

Numéro de série : Incrémenter

Serveur principal : 2012dnsp.cd.local

Personne responsable :

Intervalle d'actualisation : Minutes

Intervalle avant nouvelle tentative : Minutes

Expire après : Jours

Durée de vie minimale (par défaut) : Heures

Durée de vie pour cet enregistrement : : : : (JJJJ:HH:MM:SS)

OK Annuler

Modifier l'enregistrement de serveur de noms

Entrez un nom de serveur et une ou plusieurs adresses IP. Ces informations sont nécessaires pour identifier le serveur de noms.

Nom de domaine complet (FQDN) du serveur : 2012dnsp.cd.local. Résoudre

Adresses IP de cet enregistrement NS :

Adresse IP	Validé
< Cliquez ici pour ajouter une adresse... >	
✓ 192.168.126.11	OK

Supprimer Monter Descendre

OK Annuler

Configuration de la zone secondaire

Assistant Nouvelle zone

Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

- ☐ Zone principale
Crée une copie d'une zone qui peut être mise à jour directement.
- ☒ Zone secondaire
Crée une copie de la zone qui existe sur un autre serveur. Cela permet d'équilibrer la charge de travail des serveurs principaux et d'augmenter la tolérance de pannes.
- ☐ Zone de stub
Crée une copie d'une zone contenant uniquement des enregistrements de serveur (NS), Source de nom (SOA), et éventuellement Host (A) ». Un serveur contenant une zone de stub ne peut pas être le maître d'une zone.

☐ Enregistrer la zone dans Active Directory (disponible uniquement si un contrôleur de domaine accessible en écriture est configuré).

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

Le nom de la zone spécifie la partie autorité. Il peut s'agir du nom de domaine complet ou d'une partie du nom de domaine. Le nom de zone n'est pas le nom du serveur.

Nom de la zone :

Serveurs DNS maîtres
La zone secondaire est copiée à partir d'un ou de plusieurs serveurs DNS.

Spécifiez les serveurs DNS à partir desquels vous voulez copier la zone. Les serveurs sont contactés dans l'ordre indiqué.

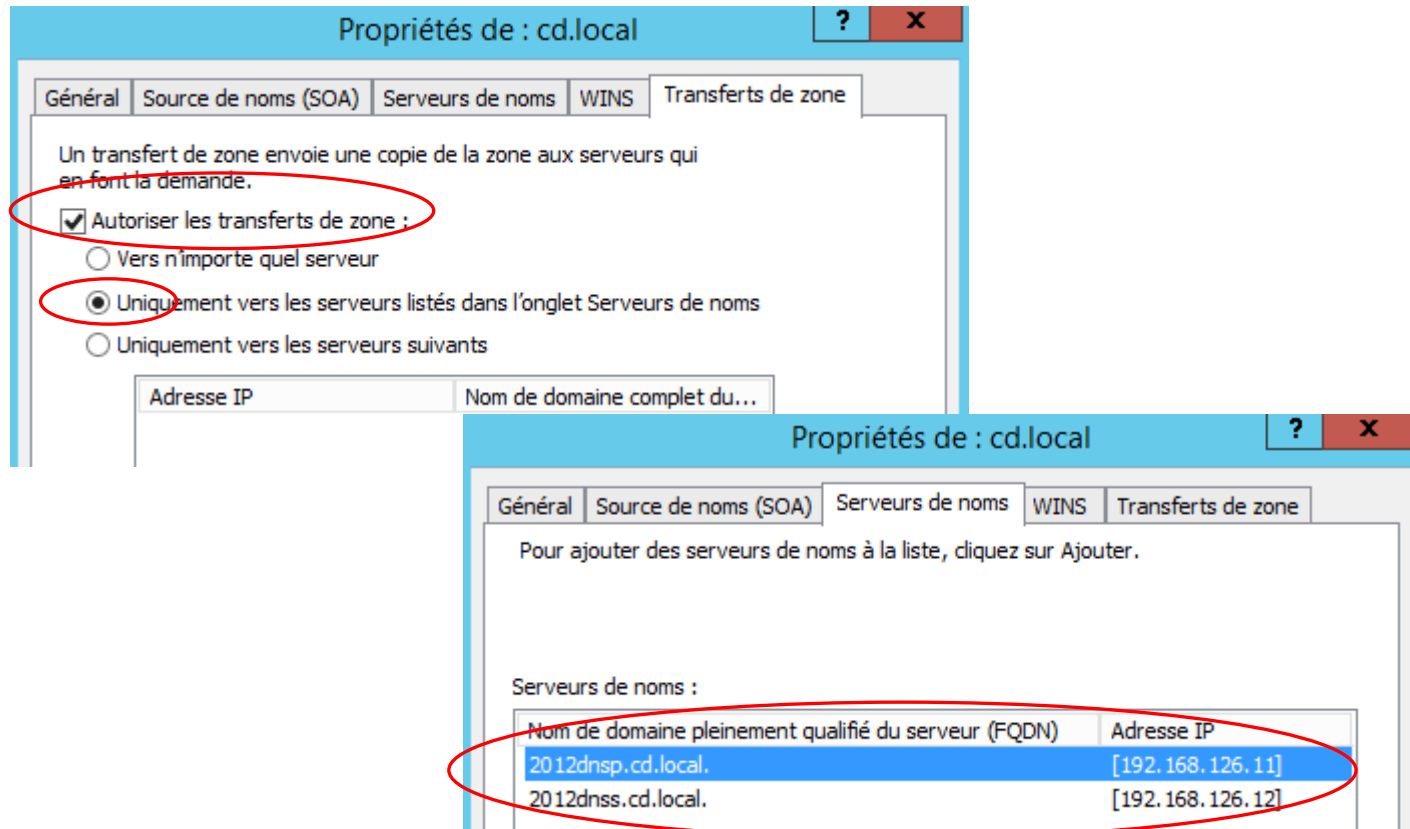
Serveurs maîtres :

Adresse IP	Nom de domaine ...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		
192.168.126.11	2012dnsp.cd.local	OK

Supprimer Monter Descendre

< Précédent Suivant > Annuler

Paramétrage transfert de zone sur serveur primaire

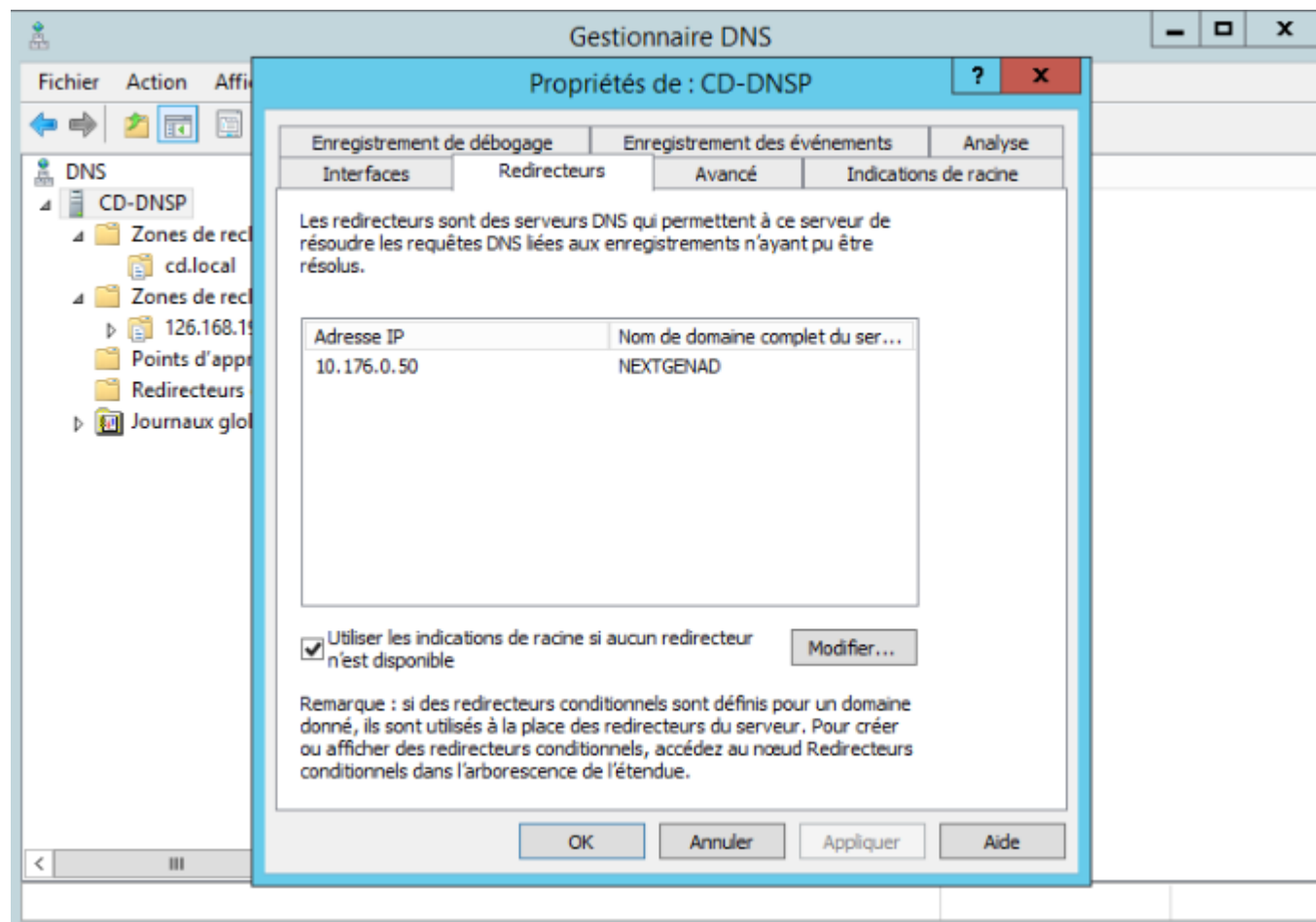


Transfert de la zone sur serveur secondaire

The screenshot shows the Windows DNS Manager console. The left pane displays the hierarchy: DNS > 2012DNSS > Zones de recherche directe > cd.local. The right pane shows a list of DNS records for the cd.local zone.

Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
_udp			
(identique au dossier parent)	Source de nom (SOA)	[29], 2012dnsp.cd.local., h...	statique
(identique au dossier parent)	Serveur de noms (NS)	2012dnsp.cd.local.	statique
(identique au dossier parent)	Serveur de noms (NS)	2012dnss.cd.local.	statique
(identique au dossier parent)	Hôte (A)	192.168.126.10	statique
2012AD	Hôte (A)	192.168.126.10	statique
2012dnsp	Hôte (A)	192.168.126.11	statique
2012dnss	Hôte (A)	192.168.126.12	statique
win10	Hôte (A)	192.168.126.15	statique

Les redirecteurs



Configuration de l'AD-DS sans DNS

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SERVEUR CIBLE
2012AD

Configuration de déploiement...
Options du contrôleur de...
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration...
Installation
Résultats

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

Niveau fonctionnel de la forêt : Windows Server 2012 R2

Niveau fonctionnel du domaine : Windows Server 2012 R2

Spécifier les fonctionnalités de contrôleur de domaine

☐ Serveur DNS (Domain Name System)

☒ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)

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

Mot de passe :

Confirmer le mot de passe :

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

< Précédent Suivant > Installer Annuler

Intégration de l'AD-DS dans le DNS

