



Ressourcesinformatiques



+ QUIZ

Version en ligne

OFFERTE !

pendant 1 an

Windows Server 2019

Infrastructure réseau



Jérôme
BEZET-TORRES



Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>. Saisissez la référence ENI
 de l'ouvrage **RI19WINR** dans la zone de recherche et validez.
 Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

Chapitre 1 Généralités

1. Comment est organisé ce livre ?	11
2. Windows en tant que service.	12
2.1 La terminologie.	12
2.2 L'évolution.	12
2.3 Les anneaux de déploiement	13
2.3.1 Windows 10	13
2.3.2 Windows Server	14
2.4 Windows Server 2019.	15
2.4.1 Les nouveautés	16
2.4.2 Les suppressions	17
2.4.3 Comment retrouver le canal d'exécution LTSC ou SAC ?	18
3. Le gestionnaire de serveur	19
3.1 Création d'un groupe de serveurs	28
3.2 Installation d'un rôle à distance	31
3.3 Suppression d'un groupe de serveurs	31
4. Serveur en mode installation minimale	32
4.1 Installation de rôles avec une installation en mode Core	40
4.2 Configuration avec sconfig	43
5. Serveur Nano	47

6. Hyper-V.....	48
6.1 Prérequis matériels	48
6.2 Les machines virtuelles sous Hyper-V.....	49
6.3 La mémoire dynamique avec Hyper-V	50
6.4 Le disque dur des machines virtuelles	52
6.5 Les points de contrôle dans Hyper-V	55
6.6 Gestion des réseaux virtuels.....	57

Chapitre 2

Installation et configuration d'Hyper-V

1. Le bac à sable.....	59
1.1 Configuration nécessaire	59
1.2 Installation de Windows Server 2019	60
2. Création des machines virtuelles.....	61
2.1 Schéma de la maquette	67
2.2 Méthode classique	70
2.2.1 Création et paramétrage de la VM	70
2.2.2 Installation du système d'exploitation	75
2.2.3 Configuration post-installation.....	78
2.3 Configuration des autres machines virtuelles.....	81
2.3.1 Machine virtuelle PAR-DC02	81
2.3.2 Machine virtuelle PAR-SRV1.....	82
2.3.3 Machine virtuelle PAR-SRV2.....	82
2.3.4 Machine virtuelle CL10-01.....	82
2.3.5 Machine virtuelle CL10-02.....	83
2.3.6 Machine virtuelle SRV-RTR	83
2.4 Les captures instantanées.....	84
2.5 Méthode différentielle	85
2.5.1 Configuration de PowerShell.....	85
2.5.2 Configuration d'Hyper-V.....	86
2.5.3 Création des disques parents	87

2.6	Paramétrage des machines virtuelles	88
2.6.1	Création et paramétrage de la VM PAR-DC01	88
2.6.2	Machine virtuelle PAR-DC02	89
2.6.3	Machine virtuelle PAR-SRV1	90
2.6.4	Machine virtuelle PAR-SRV2	91
2.6.5	Machine virtuelle SRV-RTR	92
2.6.6	Machines virtuelles CL10-01 et CL10-02	93
2.7	Configuration de la mémoire dynamique	95
2.8	Création d'un point de contrôle	96
2.9	Configuration post-installation	96

Chapitre 3

Prévoir, planifier et implémenter l'adressage IP

1.	Planifier l'adressage IPv4	97
1.1	Les adresses IPv4	97
1.1.1	Principe de fonctionnement	98
1.1.2	Quel système utiliser ?	99
1.1.3	Numération pondérée	100
1.1.4	Système binaire	100
1.2	Conversion entre binaire et décimal	101
1.2.1	Conversion binaire/décimal	101
1.2.2	Conversion décimal/binaire	101
1.3	Les classes d'adresses IPv4	102
1.3.1	Classe A	103
1.3.2	Classe B	103
1.3.3	Blocs d'adresses C	104
1.3.4	Adresses spéciales	104
1.3.5	En résumé	105
1.4	Adressage privé/public IPv4	106
1.5	Le CIDR	107

4 _____ Windows Server 2019

Infrastructure réseau

2. Les sous-réseaux	107
2.1 L'avantage du sous-réseau	108
2.2 Comment calculer un sous-réseau ?	108
2.2.1 Méthode à utiliser.	108
2.2.2 Sous-réseaux à masques variables VLSM	110
3. Configurer et maintenir IPv4.	114
3.1 Configuration et contrôle en DOS	114
3.1.1 La commande netsh	114
3.1.2 La commande ipconfig	115
3.1.3 La commande ping	116
3.1.4 La commande tracert	117
3.2 Configuration et contrôle en PowerShell	118
3.2.1 La commande Test-Connection	118
3.2.2 La commande Test-NetConnection	119
3.2.3 La commande New-NetIPAddress	120
3.2.4 La commande Set-DnsClientServerAddress	120
3.2.5 Commandes PowerShell utiles	121
4. Implémentation du protocole IPv6	122
4.1 Le protocole IPv6	122
4.1.1 Un format hexadécimal	122
4.1.2 Comprendre le format binaire	123
4.1.3 Conversions hexadécimales	124
4.1.4 Représentation d'une adresse IPv6	124
4.1.5 Règle n° 1 : omission des zéros en début de segment.	126
4.1.6 Règle n° 2 : omission des séquences composées uniquement de zéros	127
4.2 Longueur de préfixe IPv6	128
4.3 Types d'adresses IPv6	129
4.3.1 Adresses locales uniques IPv6	129
4.3.2 Adresses globales unicast IPv6	130
4.3.3 Adresses de lien local IPv6	130
4.3.4 Équivalence IPv4/IPv6	131
4.3.5 Sous-réseaux et IPv6	131

5. Les mécanismes de transition IPv4-IPv6	133
5.1 Technologie ISATAP	133
5.1.1 Présentation	133
5.1.2 Un routeur ISATAP	134
5.2 Technologie 6to4	135
5.3 Technologie Teredo	136
5.4 Le PortProxy	138

Chapitre 4

Implémentation d'un serveur DHCP

1. Introduction	139
2. Rôle du service DHCP	139
2.1 Fonctionnement de l'allocation d'une adresse IP	140
2.2 Utilisation d'un relais DHCP	141
3. Installation et configuration du rôle DHCP	141
3.1 Ajout d'une nouvelle étendue	144
3.2 Configuration des options dans le DHCP	149
3.3 Réserve de bail DHCP	152
3.4 Mise en place des filtres	155
4. Base de données DHCP	167
4.1 Présentation de la base de données DHCP	167
4.2 Sauvegarde et restauration de la base de données	168
4.3 Réconciliation et déplacement de la base de données	169
5. Haute disponibilité du service DHCP	174

Chapitre 5

Configuration et maintenance de DNS

1. Introduction	183
2. Installation de DNS	183
2.1 Vue d'ensemble de l'espace de noms DNS	184

6 _____ Windows Server 2019

Infrastructure réseau

2.2	Séparation entre DNS privé/public	185
2.3	Déploiement du DNS	185
3.	Configuration du rôle	186
3.1	Composants du serveur	186
3.2	Requêtes effectuées par le DNS	187
3.3	Enregistrement de ressources du serveur DNS	193
3.4	Fonctionnement du serveur de cache	197
4.	Configuration des zones DNS	197
4.1	Vue d'ensemble des zones DNS	197
4.2	Zones de recherche directes et zones de recherche inversée	199
4.3	Délégation de zone DNS	199
5.	Configuration du transfert de zone	200
5.1	Présentation du transfert de zone	200
5.2	Sécurisation du transfert de zone	209
6.	Gestion et dépannage du serveur DNS	210
7.	Implémenter la sécurité des serveurs DNS	212
7.1	Implémenter DNSSEC	213
7.2	Le verrouillage du cache DNS	221
7.3	Le pool de sockets DNS	222
8.	La stratégie de réponses pour un serveur DNS	222
8.1	Scénarios d'utilisations	223
8.2	Les objets DNS correspondants	223
8.3	Configuration et gestion des stratégies DNS	224

Chapitre 6

IPAM

1.	Présentation	229
2.	Les spécifications d'IPAM	230
3.	Les fonctionnalités d'IPAM	231

4. Les nouveautés apportées par Windows Server 2019.....	232
4.1 Gestion améliorée des adresses IP	232
4.2 Gestion du service DNS améliorée	232
5. Déploiement d'IPAM et configuration	233
5.1 Installation	233
5.2 Administration	234
5.3 Configuration	236

Chapitre 7

Configuration de l'accès distant

1. Introduction	239
2. Composants d'une infrastructure de service d'accès réseau	239
2.1 Présentation du rôle Services de stratégie et accès réseau	240
2.2 Authentification et autorisation réseau	241
2.3 Méthodes d'authentification	241
2.4 Vue d'ensemble de la PKI	242
2.5 Intégration du DHCP avec routage et accès distant	243
3. Configuration de l'accès VPN	244
3.1 Les connexions VPN	244
3.2 Protocoles utilisés pour le tunnel VPN	244
3.3 Présentation de la fonctionnalité VPN Reconnect	245
3.4 Configuration du serveur	246
3.5 Présentation du kit CMAK	246
4. Vue d'ensemble des politiques de sécurité	247
5. Présentation du Web Application Proxy et du proxy RADIUS	248
6. Support du routage et accès distant	250
6.1 Configuration des logs d'accès distant	250
6.2 Résolution des problèmes du VPN	251
7. Routage et protocoles	251
7.1 La traduction d'adresse NAT	252
7.2 Le protocole de routage RIP	253

8 _____ Windows Server 2019

Infrastructure réseau

7.3	Le protocole BGP	254
8.	Configuration de DirectAccess	256
8.1	Présentation de DirectAccess	256
8.2	Composants de DirectAccess	256
8.3	La table de stratégie de résolution de noms	257
8.4	Prérequis pour l'implémentation de DirectAccess	258
9.	Présentation du rôle Network Policy Server	259
10.	Configuration du serveur RADIUS	259
10.1	Notions sur le client RADIUS	259
10.2	Stratégie de demande de connexion	260
11.	Méthode d'authentification NPS	260
11.1	Configurer les templates NPS	260
11.2	L'authentification	261
11.3	Surveillance et maintenance du rôle NPS	262

Chapitre 8

Optimisation des services de fichiers

1.	Introduction	263
2.	Le système DFS	263
2.1	Présentation de l'espace de noms DFS	264
2.2	La réplication DFS	272
2.3	Fonctionnement de l'espace de noms	278
2.4	La déduplication de données	279
2.5	Scénarios DFS	286
3.	Configuration de l'espace de noms	288
3.1	Mise en place du service DFS	289
3.2	Optimisation d'un espace de noms	289
4.	Configuration et support de DFS-R	290
4.1	Fonctionnement de la réplication	290
4.2	Processus de réplication initial	290
4.3	Support du système de réplication	291

4.4	Opérations sur la base de données.	292
5.	BranchCache.	293
5.1	Présentation de BranchCache	293
5.1.1	Fonctionnement de BranchCache.	295
5.1.2	Gestion de BranchCache	296
5.2	Les différents modes de cache	298
5.2.1	Mode de cache hébergé BranchCache	298
5.2.2	Mode de cache distribué BranchCache	300
5.3	Déployer BranchCache.	301

Chapitre 9 Hyper-V et Software Defined Networking

1.	Introduction	321
2.	Les fonctionnalités réseau	321
2.1	NIC Teaming	322
2.1.1	Configuration d'un hôte Hyper-V.	323
2.1.2	Configuration d'une machine virtuelle	323
2.2	Amélioration du protocole SMB	324
2.2.1	Améliorations introduites avec SMB 3.0 sous Windows Server 2012 R2.	325
2.2.2	Améliorations introduites avec SMB 3.1.1 sous Windows Server 2016	325
2.3	La qualité de service (QoS).	326
2.4	Partage du trafic entrant (RSS, Receive Side Scaling)	330
3.	Les fonctionnalités réseau avancées	331
3.1	Les fonctionnalités réseau avancées présentes depuis Windows Server 2012 et R2	333
3.2	Les nouveautés avec Windows Server 2016	339
3.3	Hyper-V et les containers.	340
4.	Le SDN (Software Defined Networking)	340
4.1	Introduction	340
4.2	Le cloud	341

4.3	Déploiement du SDN	342
4.4	Les avantages de la virtualisation de réseaux	345
4.4.1	Encapsulation générique de routage	346
4.5	Le contrôleur de réseau	348
4.5.1	Déploiement d'un contrôleur de réseau	349
4.5.2	Le pare-feu avec le Network Controller	358
4.5.3	Software Load Balancing (SLB)	359
4.5.4	Passerelle RAS	359
5.	Les nouveautés de Windows Server 2019	
	au sein du Software Defined Networking (SDN)	360
5.1	Réseaux chiffrés	360
5.2	L'audit de pare-feu SDN	361
5.3	Peering de réseau virtuel	362
5.3.1	Les avantages de l'homologation des réseaux	362
5.3.2	Les contraintes	363
5.3.3	Connectivité	363
5.3.4	Chaînage de services	364
5.3.5	Passerelles et connectivité locale	364
5.3.6	Surveillance	365
5.4	Contrôle de sortie	365
	Index	367



Chapitre 5

Configuration et maintenance de DNS

1. Introduction

Le rôle DNS est avec Active Directory un point essentiel. En effet, il permet la résolution de nom en adresse IP. L'arrêt du service DNS empêcherait toute résolution et donc un risque de dysfonctionnement au niveau des applications souhaitant accéder à des ressources partagées (application accédant à une base de données par exemple).

2. Installation de DNS

Comme pour Active Directory ou DHCP, DNS est un rôle dans Windows Server 2019. Il existe deux manières de l'installer : procéder à l'ajout du rôle depuis la console **Gestionnaire de serveur** ou en effectuant une promotion d'un serveur en contrôleur de domaine.

DNS (*Domain Name System*) est un système basé sur une base de données distribuée et hiérarchique. Cette dernière est séparée de manière logique. Ainsi, les noms publics (editions-eni.fr) sont accessibles par n'importe qui quelle que soit sa position géographique.

Il est naturellement plus facile de retenir un nom de domaine ou un nom de poste qu'une adresse IP, de plus l'implémentation d'IPv6 favorise l'utilisation d'un nom plutôt que d'une adresse IP.

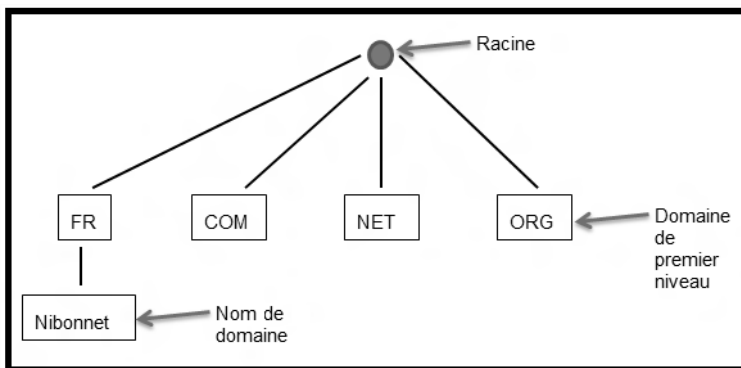
2.1 Vue d'ensemble de l'espace de noms DNS

DNS est construit sur un système hiérarchique. Le serveur racine permet de rediriger les requêtes vers les serveurs DNS juste en dessous de lui. Il est représenté par un point. On trouve en dessous les différents domaines de premier niveau (fr, net, com...). Chacun de ces domaines est géré par un organisme (AFNIC pour le .fr), IANA (*Internet Assigned Numbers Authority*) gère pour sa part les serveurs racines.

Au second niveau se trouvent les noms de domaine qui sont réservés par les entreprises ou les particuliers (editions-eni). Ces noms de domaine sont réservés chez un fournisseur d'accès qui peut également héberger votre serveur web ou tout simplement vous fournir un nom de domaine.

On trouve sur chaque niveau des serveurs DNS différents qui ont autorité sur leur zone. Le serveur racine contient uniquement l'adresse et le nom des serveurs de premier niveau. Il en est de même pour tous les serveurs de chaque niveau.

Il est possible pour une entreprise ou un particulier de rajouter pour le nom de domaine qu'il a réservé des enregistrements ou des sous-domaines (par exemple mail.nibonnet.fr, qui me permet de transférer tout mon trafic mail vers mon routeur, plus précisément à destination de mon adresse IP publique).



Chaque serveur DNS ne peut résoudre que les enregistrements de sa zone. Le serveur de la zone FR peut résoudre l'enregistrement nibonnet, mais il ne sait pas résoudre le nom de domaine shop.nibonnet.fr.

2.2 Séparation entre DNS privé/public

Un système DNS est composé de deux parties, le DNS privé qui a pour charge la résolution de noms DNS dans un réseau local ainsi que le serveur DNS sur les réseaux publics qui résout lui les noms DNS accessibles sur Internet (serveurs web...).

Il est ainsi nécessaire de choisir la politique souhaitée pour les deux serveurs. L'espace de noms interne (privé) peut ainsi être identique à l'espace de noms externe (public). Chaque serveur possède bien sûr ses propres enregistrements. Ce type de solution est valable pour des tailles de réseau restreintes. Il est fréquent de trouver un espace de noms interne différent de l'externe. L'espace de noms se trouve ainsi complètement séparé en deux parties bien distinctes. Enfin une solution hybride consiste à définir au niveau des DNS privés des sous-domaines de l'espace public.

2.3 Déploiement du DNS

Lors de la mise en place d'une solution DNS, il est important de prendre en compte certains paramètres. Dans un premier temps, il est nécessaire de connaître le nombre de zones DNS configurées sur un serveur ainsi que le nombre approximatif d'enregistrements (ceci afin de fractionner si besoin les enregistrements en plusieurs zones). Par la suite, il est également nécessaire de savoir le nombre de serveurs à installer et à configurer, ceci en fonction évidemment du nombre de clients qui communiquent avec les serveurs. Il est utile d'installer un serveur supplémentaire dans le cas où le nombre de postes client est important, ceci afin de pouvoir éviter la surcharge des serveurs. De plus, l'ajout d'un serveur permet également la continuité de service si le premier serveur venait à subir un dysfonctionnement. Il est nécessaire de connaître le positionnement des serveurs, il est fréquent de trouver au minimum un serveur DNS par localisation (si le réseau de l'entreprise s'étend sur quatre agences, soit quatre réseaux locaux reliés par des liaisons WAN, il est judicieux d'avoir au moins quatre serveurs DNS). Ceci est évidemment assujéti à la taille du site.

Enfin, d'autres interrogations peuvent apparaître, comme l'intégration ou non dans Active Directory. Lors de la création d'une zone, le stockage de cette dernière peut être réalisé de deux manières :

- **Utilisation d'un fichier texte** : l'ensemble des enregistrements est stocké dans un fichier. Ce dernier peut évidemment être modifié à l'aide d'un éditeur de texte.
- **Active Directory** : les enregistrements DNS sont contenus dans la base de données Active Directory. Pour procéder à une modification, il est nécessaire d'accéder à la console DNS. Néanmoins l'intégration de la zone à Active Directory nécessite que le rôle DNS soit installé sur le contrôleur de domaine, sans quoi il est impossible d'effectuer l'opération. Cette dernière offre un véritable bénéfice aux administrateurs. En effet, en plus de sécuriser les mises à jour dynamiques, la réplication s'effectue en même temps que celle d'Active Directory. Les administrateurs n'ont donc plus que celle-ci à gérer.

3. Configuration du rôle

Une fois installé, il est nécessaire de procéder à la configuration du rôle. Dans le cas d'une installation lors de la promotion du serveur en contrôleur de domaine, la création de la zone s'opère automatiquement.

3.1 Composants du serveur

Une solution DNS est constituée de plusieurs composants. Les serveurs DNS, pour commencer, ont pour fonction de répondre aux requêtes de leurs clients mais d'assurer également l'hébergement et la gestion d'une ou plusieurs zones. Ces dernières contiennent plusieurs enregistrements de ressources. Les serveurs DNS publics gèrent également des zones et des enregistrements de ressource. Néanmoins ces derniers ne concernent que les ressources qui doivent être accessibles depuis Internet. Enfin les clients DNS ont eux la fonction d'envoyer au serveur DNS les différentes requêtes de résolution

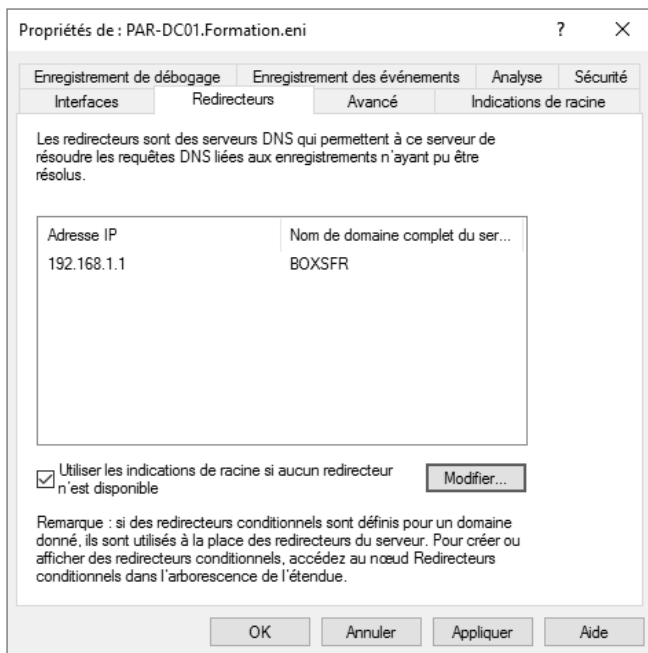
3.2 Requêtes effectuées par le DNS

Une requête permet de demander une résolution à un serveur DNS. Ainsi ce dernier peut apporter deux types de réponses, celles faisant autorité et celles ne faisant pas autorité. Un serveur fournit une réponse faisant autorité si la demande concerne une ressource présente dans une zone sur laquelle il a autorité. Dans le cas contraire, il ne peut répondre au client. Il utilise donc un redirecteur ou des indications de racines afin d'obtenir cette réponse. Deux types de requêtes peuvent donc être utilisés, itératif ou récursif.

Avec les requêtes itératives, le poste client envoie à son serveur DNS une requête afin de résoudre le nom `www.editions-eni.fr` par exemple. Le serveur interroge le serveur racine. Ce dernier le redirige vers le serveur ayant autorité sur la zone FR. Il peut ainsi connaître l'adresse IP du serveur DNS ayant autorité sur la zone `editions-eni`. L'interrogation de ce dernier permet la résolution du nom `www.editions-eni.fr`. Le serveur DNS interne répond à la demande qu'il a reçue au préalable de son client.

Avec les requêtes récursives, le poste client souhaite résoudre le nom `www.editions-eni.fr`. Il envoie la demande à son serveur DNS. N'ayant pas autorité sur la zone `editions-eni.fr`, le serveur a besoin d'un serveur externe pour effectuer la résolution. La demande est donc transmise au redirecteur configuré par l'administrateur (le serveur DNS du FAI qui possède un cache plus important par exemple). Si la réponse n'est pas contenue dans son cache, le serveur DNS du FAI effectue une requête itérative puis transmet la réponse au serveur qui lui a transmis la demande. Ce dernier peut maintenant répondre à son client.

La capture ci-dessous montre la configuration d'un redirecteur :

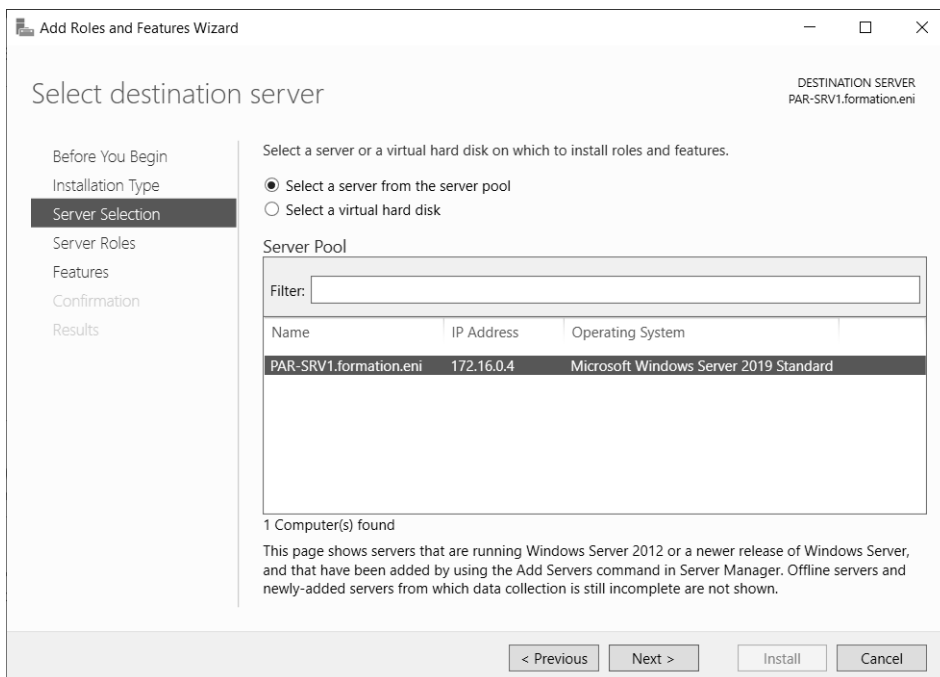


Pour toute demande sur laquelle le serveur n'a pas autorité, le redirecteur est utilisé. Dans certains cas (approbation de forêt AD, etc.), il est nécessaire que la demande de résolution qui va être envoyée à un autre serveur DNS soit redirigée en fonction du nom de domaine (pour le domaine eni.fr envoyer la demande à SRVDNS1). Le redirecteur conditionnel permet d'effectuer cette modification et d'aiguiller les requêtes vers le bon serveur si la condition (nom de domaine) est validée.

Par exemple un redirecteur conditionnel peut être un moyen pour permettre à un administrateur de donner la possibilité de résoudre un nom de domaine par exemple **Formatica.msft**. Dans cet exemple, on installe le service DNS sur un serveur membre du domaine **Formation.eni**.

- Ouvrez une session en tant qu'administrateur du domaine.
- Lancez la console **Gestionnaire de serveur** puis cliquez sur le lien **Ajouter des rôles et des fonctionnalités**.

- Un assistant se lance, cliquez sur **Suivant**.
- Dans les fenêtres **Sélectionner le type d'installation** et **Sélectionner le serveur de destination**, cliquez sur **Suivant** en laissant la valeur par défaut.



- Cochez le rôle **Serveur DNS** puis cliquez sur **Ajouter des fonctionnalités**.
- Cliquez trois fois sur **Suivant** puis sur **Installer**.
- Fermez la fenêtre une fois l'opération terminée.
- Lancez la console **DNS** depuis les Outils d'administration puis déroulez **PAR-SRV1**.
- Effectuez un clic droit sur **Zones de recherche directes** puis sélectionnez **Nouvelle zone**.
- Dans la fenêtre de bienvenue, cliquez sur **Suivant**.
- Vérifiez que **Zone principale** est coché puis cliquez sur **Suivant**.

■ Dans le champ **Nom de la zone**, saisissez **Formatica.msft** puis cliquez sur **Suivant**.

La zone ne peut pas être intégrée à Active Directory car le serveur n'est pas un contrôleur de domaine.

Un fichier est donc créé, ce dernier contient tous les enregistrements de la zone.

■ Cliquez sur **Suivant** dans la fenêtre **Fichier zone**.

■ Laissez coché **Ne pas autoriser les mises à jour dynamiques** puis cliquez sur **Suivant**.

■ Cliquez sur **Terminer** pour effectuer la création de la zone.

■ Développez la zone **Formatica.msft** puis effectuez un clic droit sur la zone.

■ Dans le menu contextuel, sélectionnez **Nouvel hôte (A ou AAAA)**.

■ Saisissez **www** dans le champ **Nom** puis **172.16.0.97** dans le champ **Adresse IP**.