



Ressourcesinformatiques

Windows Server 2016

Infrastructure réseau

Jérôme BEZET-TORRES



Nicolas
BONNET

Fichiers complémentaires
à télécharger



Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>. Saisissez la référence ENI
de l'ouvrage **RI16WINR** dans la zone de recherche et validez.
Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Chapitre 1 Généralités

1. Comment est organisé ce livre ?	11
2. Le gestionnaire de serveur	12
2.1 Création d'un groupe de serveurs	20
2.2 Installation d'un rôle à distance	23
2.3 Suppression d'un groupe de serveurs	23
3. Serveur en mode installation minimale	24
3.1 Installation de rôles avec une installation en mode Core	32
3.2 Configuration avec sconfig	35
4. Serveur Nano	39
5. Hyper-V	40
5.1 Prérequis matériels	40
5.2 Les machines virtuelles sous Hyper-V	41
5.3 La mémoire dynamique avec Hyper-V	42
5.4 Le disque dur des machines virtuelles	44
5.5 Les points de contrôle dans Hyper-V	47
5.6 Gestion des réseaux virtuels	49

Chapitre 2

Installation et configuration d'Hyper-V

1. Le bac à sable.	51
1.1 Configuration nécessaire	51
1.2 Installation de Windows Server 2016	52
2. Création des machines virtuelles.....	53
2.1 Schéma de la maquette	59
2.2 Méthode Classique	62
2.2.1 Création et paramétrage de la VM	62
2.2.2 Installation du système d'exploitation	67
2.2.3 Configuration post-installation.....	70
2.3 Machine virtuelle PAR-DC02	73
2.4 Machine virtuelle PAR-SRV1.....	74
2.5 Machine virtuelle PAR-SRV2.....	74
2.6 Machine virtuelle CL10-01.....	75
2.7 Machine virtuelle CL10-02.....	75
2.8 Machine virtuelle SRV-RTR	75
2.9 Les captures instantanées.....	76
2.10 Méthode Différentielle.....	77
2.10.1 Configuration de PowerShell.....	77
2.10.2 Configuration d'Hyper-V.....	78
2.10.3 Création des disques parents	79
2.11 Création et paramétrage de la VM PAR-DC01.....	81
2.12 Machine virtuelle PAR-DC02	82
2.13 Machine virtuelle PAR-SRV1.....	83
2.14 Machine virtuelle PAR-SRV2.....	84
2.15 Machine virtuelle SRV-RTR	85
2.16 Machine virtuelle CL10-01 et 02	86
2.17 Configuration mémoire dynamique	87
2.18 Création d'un point de contrôle	88
2.19 Configuration Post-installation.....	88

Chapitre 3

Prévoir, planifier et implémenter l'adressage IP

1. Planifier l'adressage IPv4.....	89
1.1 Les adresses IPv4.....	89
1.1.1 Principe de fonctionnement.....	90
1.1.2 Le binaire.....	91
1.1.3 Numération pondérée.....	92
1.1.4 Système binaire.....	92
1.2 Conversion binaire/décimale.....	93
1.2.1 Binaire/décimale.....	93
1.2.2 Conversion décimale/binaire.....	93
1.3 Les classes d'adresses IPv4.....	94
1.3.1 Classe A.....	95
1.3.2 Classe B.....	95
1.3.3 Blocs d'adresses C.....	96
1.3.4 Adresses spéciales.....	96
1.3.5 En résumé.....	97
1.4 Adressage privé/public IPv4.....	98
1.5 Le CIDR.....	99
2. Les sous-réseaux.....	99
2.1 L'avantage du sous-réseau.....	100
2.2 Comment calculer un sous-réseau ?.....	100
2.2.1 Méthode à utiliser.....	100
2.2.2 Sous-réseaux à masques variables VLSM.....	102
3. Configurer et maintenir IPv4.....	106
3.1 Configuration et contrôle en DOS.....	106
3.1.1 La commande netsh.....	106
3.1.2 La commande ipconfig.....	107
3.1.3 La commande ping.....	108
3.1.4 La commande tracert.....	109

4 _____ Windows Server 2016

Infrastructure réseau

3.2	Configuration et contrôle en PowerShell	110
3.2.1	La commande Test-Connection	110
3.2.2	La commande Test-Netconnection	111
3.2.3	La commande New-NetIPAddress	112
3.2.4	La commande Set-DnsClientServerAddress	112
3.3	Commandes PowerShell utiles	113
4.	Implémentation du protocole IPv6	114
4.1	Le protocole IPv6	114
4.1.1	Un format hexadécimal	114
4.1.2	Comprendre le format binaire	115
4.1.3	Conversions hexadécimales	116
4.1.4	Représentation d'une adresse IPv6	116
4.1.5	Règle n° 1 : omission des zéros en début de segment	118
4.1.6	Règle n° 2 : omission des séquences composées uniquement de zéros	119
4.2	Longueur de préfixe IPv6	120
4.3	Types d'adresses IPv6	121
4.3.1	Adresses locales uniques IPv6	121
4.3.2	Adresses globales unicast IPv6	122
4.3.3	Adresses de lien local IPv6	122
4.3.4	Équivalence IPv4/IPv6	123
4.3.5	Sous-réseaux et IPv6	123
5.	Les mécanismes de transitions IPv4 - IPv6	125
5.1	Technologie ISATAP	125
5.1.1	Un routeur ISATAP	126
5.2	Technologie 6to4	127
5.3	Technologie Teredo	128
5.4	Le PortProxy	130

Chapitre 4

Implémentation d'un serveur DHCP

1. Introduction	131
2. Rôle du service DHCP	131
2.1 Fonctionnement de l'allocation d'une adresse IP	132
2.2 Utilisation d'un relais DHCP.....	133
3. Installation et configuration du rôle DHCP	133
3.1 Ajout d'une nouvelle étendue	136
3.2 Configuration des options dans le DHCP.....	141
3.3 Réserve de bail DHCP	144
3.4 Mise en place des filtres	147
4. Base de données DHCP	159
4.1 Présentation de la base de données DHCP	159
4.2 Sauvegarde et restauration de la base de données	160
4.3 Réconciliation et déplacement de la base de données	161
5. Haute disponibilité du service DHCP	166

Chapitre 5

Configuration et maintenance de DNS

1. Introduction	175
2. Installation de DNS	175
2.1 Vue d'ensemble de l'espace de noms DNS	176
2.2 Séparation entre DNS privé/public	177
2.3 Déploiement du DNS.....	177
3. Configuration du rôle.....	178
3.1 Composants du serveur	178
3.2 Requêtes effectuées par le DNS.....	179
3.3 Enregistrement de ressources du serveur DNS.....	185
3.4 Fonctionnement du serveur de cache	189

6 _____ Windows Server 2016

Infrastructure réseau

4.	Configuration des zones DNS	189
4.1	Vue d'ensemble des zones DNS	189
4.2	Zones de recherche directes et zones de recherche inversée ..	191
4.3	Délégation de zone DNS	191
5.	Configuration du transfert de zone	192
5.1	Présentation du transfert de zone	192
5.2	Sécurisation du transfert de zone	201
6.	Gestion et dépannage du serveur DNS	202
7.	Implémenter la sécurité des serveurs DNS	204
7.1	Implémenter DNSSEC	205
7.2	Le verrouillage du cache DNS	213
7.3	Le pool de sockets DNS	214
8.	La stratégie de réponses pour un serveur DNS	214
8.1	Scénarios d'utilisations	215
8.2	Les objets DNS correspondants	215
8.3	Configuration et gestion des stratégies DNS	216

Chapitre 6 IPAM

1.	Présentation	221
2.	Les spécifications d'IPAM	222
3.	Les fonctionnalités d'IPAM	223
4.	Les nouveautés apportées par Windows Server 2016	224
4.1	Gestion améliorée des adresses IP	224
4.2	Gestion du service DNS améliorée	224
5.	Déploiement d'IPAM et configuration	225
5.1	Installation	225
5.2	Administration	226
5.3	Configuration	228

Chapitre 7

Configuration de l'accès distant

1. Introduction	231
2. Composants d'une infrastructure de service d'accès réseau	231
2.1 Présentation du rôle Services de stratégie et accès réseau	232
2.2 Authentification et autorisation réseau	233
2.3 Méthodes d'authentification	233
2.4 Vue d'ensemble de la PKI	234
2.5 Intégration du DHCP avec routage et accès distant	235
3. Configuration de l'accès VPN	236
3.1 Les connexions VPN	236
3.2 Protocoles utilisés pour le tunnel VPN	236
3.3 Présentation de la fonctionnalité VPN Reconnect	237
3.4 Configuration du serveur	238
3.5 Présentation du kit CMAK	238
4. Vue d'ensemble des politiques de sécurité	239
5. Présentation du Web Application Proxy et du proxy RADIUS	240
6. Support du routage et accès distant	242
6.1 Configuration des logs d'accès distant	242
6.2 Résolution des problèmes du VPN	243
7. Routage et protocoles	243
7.1 La translation d'adresse NAT	244
7.2 Protocole de routage RIP	245
7.3 Le protocole BGP	246
8. Configuration de DirectAccess	248
8.1 Présentation de DirectAccess	248
8.2 Composants de DirectAccess	248
8.3 La table de stratégie de résolution de noms	249
8.4 Prérequis pour l'implémentation de DirectAccess	250
9. Présentation du rôle Network Policy Server	251

8 _____ Windows Server 2016

Infrastructure réseau

10. Configuration du serveur RADIUS	251
10.1 Notions sur le client RADIUS	251
10.2 Stratégie de demande de connexion	252
11. Méthode d'authentification NPS	252
11.1 Configurer les templates NPS	252
11.2 L'authentification	253
12. Surveillance et maintenance du rôle NPS	254

Chapitre 8

Optimisation des services de fichiers

1. Introduction	255
2. Le système DFS	255
2.1 Présentation de l'espace de noms DFS	256
2.2 La réplication DFS	264
2.3 Fonctionnement de l'espace de noms	270
2.4 La déduplication de données	271
2.5 Scénarios DFS	278
3. Configuration de l'espace de noms	280
3.1 Mise en place du service DFS	280
3.2 Optimisation d'un espace de noms	281
4. Configuration et support de DFS-R	282
4.1 Fonctionnement de la réplication	282
4.2 Processus de réplication initial	282
4.3 Support du système de réplication	283
4.4 Opérations sur la base de données	284
5. BranchCache	285
5.1 Présentation de BranchCache	285
5.1.1 Fonctionnement de BranchCache	286
5.1.2 Gestion de BranchCache	288

5.2	Les différents modes de cache	290
5.2.1	Mode de cache hébergé BranchCache	290
5.2.2	Mode de cache distribué BranchCache	292
5.3	Déployer BranchCache	293

Chapitre 9

Hyper-V et Software Defined Networking

1.	Introduction	313
2.	Les fonctionnalités réseau	313
2.1	NIC Teaming	314
2.1.1	Configuration d'un hôte Hyper-V	315
2.1.2	Configuration d'une machine virtuelle	315
2.2	Amélioration du protocole SMB	316
2.2.1	Améliorations introduites avec SMB 3.0 sous Windows Server 2012 R2	317
2.2.2	Améliorations introduites avec SMB 3.1.1 avec Windows Server 2016	317
2.3	La Qualité de Service QoS	318
2.4	Partage du trafic entrant (RSS, Receive Side Scaling)	322
3.	Les fonctionnalités réseau avancées	323
3.1	Les fonctionnalités réseau avancées présentes depuis Windows Server 2012 et R2	325
3.2	Les nouveautés avec Server 2016	331
3.3	Hyper-V et les containers	332
4.	Le Software Defined Networking SDN	332
4.1	Introduction	332
4.2	Le cloud	333
4.3	Déploiement du SDN	334
4.4	Les avantages de la virtualisation de réseaux	337
4.4.1	Encapsulation générique de routage	338

10 _____ Windows Server 2016

Infrastructure réseau

4.5	Le contrôleur de réseau	340
4.5.1	Déploiement d'un contrôleur de réseau	341
4.5.2	Le pare-feu avec le Network Controller	350
4.5.3	Software Load Balancing (SLB)	351
4.5.4	Passerelle RAS	351
Index		353

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 2016. 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.

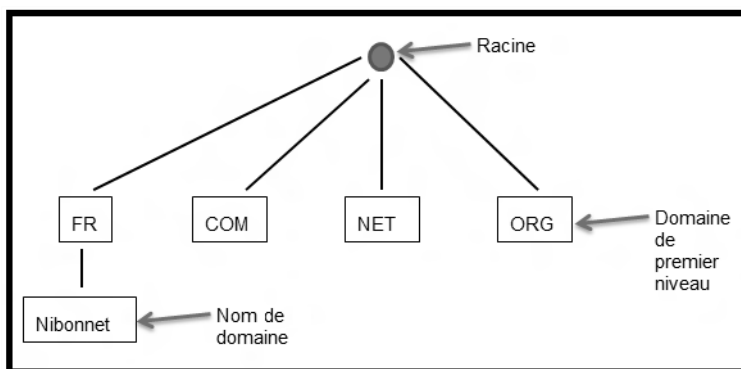
2.1 Vue d'ensemble de l'espace de noms DNS

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

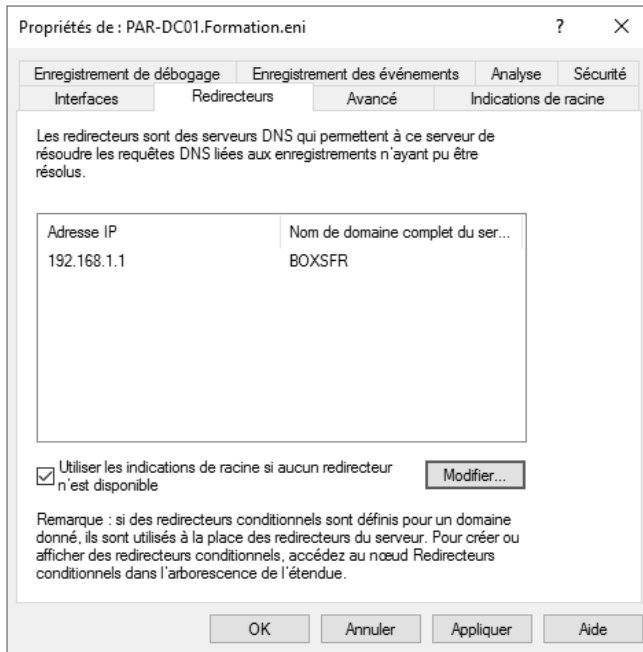
3.2 Requêtes effectuées par le DNS

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.nibonnet.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 `nibonnet`. L'interrogation de ce dernier permet la résolution du nom `www.nibonnet.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.nibonnet.fr`. Il envoie la demande à son serveur DNS. N'ayant pas autorité sur la zone `nibonnet.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**.