

vBook

livre &  
vidéo



# Windows Server 2012 R2



livre

Administration avancée



vidéo

Sécurité de l'infrastructure  
avec les GPO

2 H 40 de vidéo

Jérôme BEZET-TORRES

Thierry DEMAN



Freddy ELMALEH



Sébastien NEILD

Maxence VAN JONES

Téléchargement

[www.editions-eni.fr](http://www.editions-eni.fr)



Les éléments à télécharger sont disponibles à l'adresse suivante :  
**<http://www.editions-eni.fr>**  
Saisissez la référence ENI de l'ouvrage **EI12WINA** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

## Chapitre 1 Introduction

- 1. Introduction . . . . . 13
- 2. Les différentes éditions de Windows Server 2012 . . . . . 13
- 3. Les grands axes de Windows Server 2012 . . . . . 15
  - 3.1 Un meilleur contrôle de l'information . . . . . 15
  - 3.2 Une meilleure protection du système d'information . . . . . 16
  - 3.3 Une plate-forme évolutive . . . . . 18

## Chapitre 2 Domaine Active Directory

- 1. Introduction . . . . . 21
- 2. Présentation du service d'annuaire Microsoft :  
Active Directory Domain Services . . . . . 21
  - 2.1 Définition d'un domaine Active Directory . . . . . 22
  - 2.2 Fonctionnalités de l'Active Directory sous Windows Server 2012 . . . 23
    - 2.2.1 Installation d'un annuaire Active Directory . . . . . 23
    - 2.2.2 Présentation de l'audit lié au service d'annuaire . . . . . 42
    - 2.2.3 Contrôleur de domaine en lecture seule . . . . . 51
    - 2.2.4 Stratégies de mot de passe et de verrouillage  
de compte granulaire . . . . . 61
    - 2.2.5 Active Directory en tant que service Windows . . . . . 66
    - 2.2.6 Clonage d'un contrôleur de domaine  
Active Directory virtualisé . . . . . 69
    - 2.2.7 Cliché instantané de l'Active Directory . . . . . 72
    - 2.2.8 Les comptes de service administrés . . . . . 75
    - 2.2.9 La corbeille Active Directory . . . . . 84
    - 2.2.10 Autres spécificités de Windows Server 2008 R2 et 2012 . . . . . 92

3.	Les stratégies de groupe . . . . .	95
3.1	Détection des liens lents . . . . .	96
3.2	Le format ADMX . . . . .	97
3.3	Journaux d'événements. . . . .	98
3.4	Paramètres de stratégies de groupe à connaître. . . . .	99
3.5	La console Gestion des stratégies de groupe . . . . .	100
3.6	Les objets GPO Starter . . . . .	108
4.	Les autres composants Active Directory . . . . .	109
4.1	Active Directory Lightweight Directory Services (ou AD LDS) . . . . .	109
4.2	Active Directory Federation Services (ou AD FS) . . . . .	110
4.3	Active Directory Rights Management Services (ou AD RMS) . . . . .	111
4.4	Active Directory Certificate Services (ou AD CS) . . . . .	111

## Chapitre 3

### Architecture distribuée d'accès aux ressources

1.	Introduction . . . . .	115
2.	Description de DFS . . . . .	115
3.	Installation . . . . .	117
3.1	Le module d'espace de noms . . . . .	118
3.2	Le module de réplication . . . . .	118
3.3	La console d'administration . . . . .	118
3.4	Le cas des contrôleurs de domaine . . . . .	119
3.5	La procédure d'installation graphique . . . . .	119
4.	Configuration du service DFS . . . . .	128
4.1	Les différents types de racines distribuées . . . . .	128
4.1.1	Les racines autonomes . . . . .	128
4.1.2	Les racines de noms de domaine . . . . .	134
4.2	La création des liaisons DFS et cibles DFS . . . . .	141
4.3	La réplication . . . . .	142
4.3.1	Les filtres de réplication . . . . .	142
4.3.2	La mise en place graphique de la réplication . . . . .	142
4.3.3	La topologie de réplication . . . . .	154

5.	Configuration avancée	154
5.1	Les méthodes de classement	154
5.1.1	La configuration au niveau des racines DFS	154
5.1.2	La configuration au niveau des liaisons DFS	156
5.1.3	La configuration au niveau des cibles DFS	156
5.2	La délégation d'administration	157
6.	L'administration de DFS avec PowerShell	158
6.1	Gestion des racines	158
6.2	Gestion des cibles (dossiers) et des accès	160
7.	L'utilisation de DFS et les bons usages	161
8.	Interaction avec d'autres composants	162
8.1	Les espaces de noms DFS : détection du site par les clients DirectAccess	162
8.2	La réplication DFS supporte les volumes sur lesquels la déduplication est activée	162
8.3	DFS dispose d'un fournisseur WMI complet (Espaces de noms et Réplication)	163
9.	BranchCache	165
9.1	L'installation du BranchCache	165
9.2	La configuration des partages	173
9.3	La configuration des clients	174

## Chapitre 4 Haute disponibilité

1.	Introduction	181
2.	Les choix d'architecture	182
2.1	Les différentes architectures	182
2.2	La haute disponibilité, nirvana de votre infrastructure ?	184
3.	La répartition de charge (Cluster NLB)	186
3.1	Pré-requis pour NLB	186
3.2	Créer une ferme NLB	187
3.3	Configurer la ferme	190
3.4	Exemple : ferme Web IIS	192
3.5	Mise à niveau d'une ferme NLB	193

# 4 --- Windows Server 2012

Administration avancée

4.	Le cluster à basculement . . . . .	194
4.1	Validation de votre cluster . . . . .	197
4.2	Mise en œuvre du cluster . . . . .	198
4.2.1	Configurer le réseau pour le cluster . . . . .	199
4.2.2	Configurer le stockage pour le cluster . . . . .	199
4.2.3	Configurer le quorum pour le cluster . . . . .	201
4.2.4	L'installation du cluster . . . . .	202
4.2.5	Mise en place d'un cluster de fichiers . . . . .	210
4.2.6	Cas particuliers . . . . .	214
4.3	Migration de Windows Server 2008 à 2012 . . . . .	216
4.4	Configuration d'un cluster à basculement en multisite . . . . .	217
4.5	Mise à jour adaptée aux clusters à basculement . . . . .	218

## Chapitre 5

### Mise en place des services réseau d'entreprise

1.	Introduction . . . . .	223
2.	L'implémentation d'un système d'adressage IP . . . . .	223
2.1	Le choix de l'architecture réseau . . . . .	224
2.1.1	La zone DNS . . . . .	224
2.1.2	La classe réseau . . . . .	225
2.2	L'installation d'un serveur DHCP . . . . .	225
2.2.1	Définition . . . . .	225
2.2.2	L'installation . . . . .	225
2.2.3	La configuration . . . . .	226
2.2.4	Les réservations . . . . .	239
3.	La mise en place des systèmes de résolutions de nom . . . . .	241
3.1	La résolution DNS . . . . .	241
3.1.1	Définition . . . . .	241
3.1.2	L'installation . . . . .	241
3.1.3	Les différents types de zones . . . . .	242
3.1.4	Les différents types de répliquions . . . . .	243
3.1.5	Les zones de recherche inversée . . . . .	244
3.1.6	La zone GlobalNames dite GNZ . . . . .	244
3.1.7	Les tests et vérifications . . . . .	245
3.1.8	Les différents types d'enregistrement . . . . .	246
3.1.9	Les bons usages . . . . .	247

- 3.1.10 DNSSEC . . . . . 247
- 3.1.11 L'administration de DNS avec PowerShell . . . . . 263
- 3.2 La résolution WINS . . . . . 266
  - 3.2.1 Définition . . . . . 266
  - 3.2.2 L'installation . . . . . 267
  - 3.2.3 La configuration . . . . . 267
  - 3.2.4 La réplication entre serveurs WINS . . . . . 267
  - 3.2.5 Quand et pourquoi utiliser WINS ? . . . . . 268
- 4. La mise en place de la quarantaine réseau . . . . . 268
  - 4.1 La préparation de l'environnement commun aux différents types de quarantaine . . . . . 268
  - 4.2 La mise en place de NAP via DHCP . . . . . 277
  - 4.3 La mise en place de NAP via IPsec . . . . . 279
    - 4.3.1 Installation du service Autorité HRA . . . . . 279
    - 4.3.2 Configuration du système de validation (HRA) . . . . . 283
    - 4.3.3 Définition des règles de sécurité de connexion . . . . . 285
  - 4.4 La mise en place de NAP sur 802.1x . . . . . 289
  - 4.5 Conclusion . . . . . 298

**Chapitre 6**  
**Les évolutions du réseau**

- 1. La console IPAM . . . . . 299
  - 1.1 Les avantages de cette solution . . . . . 300
  - 1.2 L'architecture IPAM . . . . . 300
  - 1.3 L'installation . . . . . 301
  - 1.4 La configuration initiale . . . . . 305
  - 1.5 Les groupes utilisés par IPAM . . . . . 313
  - 1.6 Les tâches d'administration courantes . . . . . 314
  - 1.7 Les limites à prendre en compte . . . . . 315
- 2. Le protocole IPv6 . . . . . 315
  - 2.1 Tableau d'équivalence IPv4 et IPv6 . . . . . 316
  - 2.2 Les commandes principales . . . . . 317
  - 2.3 La configuration de DHCP v6 . . . . . 318
    - 2.3.1 Configuration du client DHCPv6 sur le serveur DHCP . . . . . 319
    - 2.3.2 Configuration du service DHCPv6 . . . . . 320

# 6 --- Windows Server 2012

Administration avancée

2.4	La configuration DNS v6 de la zone de recherche inverse . . . . .	325
2.5	TEREDO . . . . .	331
2.6	ISATAP . . . . .	331
3.	L'association de cartes réseau en équipe (Teaming) . . . . .	331
4.	Les nouveautés de SMBv3 . . . . .	336
4.1	Présentation des différentes nouveautés . . . . .	336
4.2	Pratique : mise en place du mode Multicanal . . . . .	337
4.2.1	Les pré-requis . . . . .	337
4.2.2	Les commandes PowerShell . . . . .	337
4.3	Remarques . . . . .	340

## Chapitre 7

### Services Bureau à distance

1.	Introduction . . . . .	341
2.	Mise en œuvre des Services Bureau à distance . . . . .	344
2.1	Administration à distance . . . . .	346
2.2	Installation des services Bureau à distance . . . . .	350
2.2.1	Pré-requis . . . . .	351
2.2.2	Installation Démarrage rapide . . . . .	352
2.2.3	Installation Déploiement standard . . . . .	358
2.2.4	Installation en PowerShell . . . . .	361
2.3	Présentation du Gestionnaire des services Bureau à distance . . . . .	363
3.	Configuration . . . . .	368
3.1	Propriétés du déploiement . . . . .	368
3.2	Configuration d'une collection de sessions . . . . .	369
3.2.1	Installation d'un logiciel sur un serveur de sessions . . . . .	376
3.2.2	Maintenance d'un serveur de sessions . . . . .	376
3.2.3	Amélioration de l'expérience utilisateur sur un serveur de sessions . . . . .	377
3.3	Configuration d'une collection de bureaux virtuels . . . . .	380
3.3.1	Ajout de bureaux virtuels à une collection - Création d'un bureau virtuel . . . . .	386
3.4	Déployer des applications avec RemoteApp . . . . .	386

4.	Configuration avancée	391
4.1	Configuration de l'Accès Web des services Bureau à distance	391
4.2	Configuration de la Passerelle des services Bureau à distance	395
4.3	Configuration du Gestionnaire de licences des services Bureau à distance	407
4.4	RemoteFX	412
4.4.1	RemoteFX pour un hôte de virtualisation des services Bureau à distance	412
4.4.2	RemoteFX pour un hôte de session Bureau à distance	415
4.4.3	RemoteFX utilisé pour la redirection USB	416

## Chapitre 8 Accès distant

1.	Introduction	417
2.	Principe de l'accès distant	417
2.1	Accès par téléphone	418
2.1.1	Généralités sur les connexions Dial-up	418
2.1.2	Avantages et inconvénients des connexions Dial-up	418
2.2	Accès via Internet	419
2.2.1	Généralités sur les VPN	419
2.2.2	Les différents types de VPN proposés sous Windows Server 2012	421
2.2.3	Avantages et inconvénients du VPN	422
2.2.4	DirectAccess, le "VPN-Killer"	423
2.2.5	Quoi de neuf avec Windows Server 2012 ?	424
3.	Mettre en place un accès sécurisé à travers Internet	425
3.1	Mise en place d'une liaison VPN	425
3.1.1	Installation du rôle Accès à distance	426
3.1.2	Configuration des fonctionnalités VPN	430
3.2	Gestion de la sécurité des accès	437
3.3	Gestion de l'authentification RADIUS	445
3.4	Implémentation de DirectAccess derrière un pare-feu	449
3.5	Supervision des connexions	453



## **Chapitre 9** **Application Internet**

1.	Mettre en place un serveur Intranet/Internet . . . . .	457
1.1	Présentation d'IIS 8. . . . .	457
1.1.1	Présentation générale . . . . .	457
1.1.2	Architecture héritée . . . . .	458
1.1.3	Administration . . . . .	459
1.1.4	Nouveautés incluses avec IIS 8 dans Windows Server 2012 . . . . .	460
1.2	Installation du rôle Serveur Web (IIS) en mode Windows Server minimal . . . . .	461
1.2.1	Installation par défaut . . . . .	461
1.2.2	Installation complète . . . . .	461
1.3	Installation du rôle Serveur Web (IIS) en mode graphique . . . . .	462
2.	Créer un site Web . . . . .	466
2.1	Création et configuration d'un site . . . . .	466
2.2	Utilisation des en-têtes d'hôte . . . . .	471
2.3	Mise en place d'une DMZ . . . . .	473
2.4	Implémentation du CPU Throttling . . . . .	475
3.	Monter un site FTP avec isolation des utilisateurs . . . . .	477
3.1	Installation du rôle Serveur FTP . . . . .	477
3.2	Configuration de l'isolation des utilisateurs . . . . .	478
3.3	Configuration de la restriction des tentatives de connexion . . . . .	483

## **Chapitre 10** **Réduire la surface d'attaque**

1.	Introduction . . . . .	485
2.	Principes du serveur Core . . . . .	485
2.1	Restrictions liées à une installation minimale . . . . .	485
2.2	Installation minimale . . . . .	486
3.	Configurer localement un serveur Core . . . . .	488
3.1	Sconfig . . . . .	488
3.2	Configurer le temps . . . . .	489
3.3	Paramètres régionaux . . . . .	490
3.4	Résolution de l'écran . . . . .	490
3.5	Économiseur d'écran . . . . .	491

- 3.6 Nom du serveur . . . . . 492
- 3.7 Gestion des pilotes . . . . . 492
- 3.8 Configuration réseau . . . . . 493
- 3.9 Activation de Windows . . . . . 494
- 3.10 Gestion du rapport d'erreurs . . . . . 495
- 3.11 Configurer le fichier de pagination . . . . . 496
- 3.12 Joindre un domaine . . . . . 497
- 3.13 Cérer les journaux d'événements . . . . . 497
- 4. Gestion à distance . . . . . 498
  - 4.1 Activation du bureau à distance . . . . . 498
  - 4.2 Activation de WinRM . . . . . 499
- 5. Sécuriser le serveur Core . . . . . 501
  - 5.1 Gestion du pare-feu . . . . . 501
  - 5.2 Gestion automatique des mises à jour . . . . . 502
  - 5.3 Sauvegarder le serveur . . . . . 503
  - 5.4 Sécurisation du stockage avec BitLocker . . . . . 504
- 6. Mise en place d'un serveur Core et des applications associées . . . . . 506
  - 6.1 Installation des rôles et des fonctionnalités . . . . . 506
    - 6.1.1 Les rôles réseau . . . . . 507
    - 6.1.2 Le rôle serveur de fichiers . . . . . 509
    - 6.1.3 Le rôle serveur d'impression . . . . . 510
  - 6.2 Service d'annuaire (AD) . . . . . 511
  - 6.3 Exécuter des applications 32 bits . . . . . 511
- 7. Souplesse de la gestion du mode Core . . . . . 512
  - 7.1 Passage du Mode GUI au mode Core . . . . . 512
  - 7.2 Passage du Mode Core au mode GUI . . . . . 514
  - 7.3 Utilisation des fonctionnalités à la demande . . . . . 515

**Chapitre 11**  
**Consolider vos serveurs**

- 1. Introduction . . . . . 517

2.	Pourquoi consolider ?	517
2.1	Virtuel versus Physique	518
2.1.1	Optimisation des coûts	518
2.1.2	Les limites de la virtualisation	519
2.2	De nouvelles problématiques	520
2.2.1	Environnement mutualisé	521
2.2.2	Sauvegarde	522
2.3	Préparer son déploiement	524
2.3.1	Pré-requis	524
2.3.2	Méthodologie	525
2.3.3	Déterminer les serveurs et les applications propices à la virtualisation	526
2.3.4	Respect des meilleures pratiques	528
3.	Déployer Hyper-V	530
3.1	Installation	530
3.1.1	Installation du rôle Hyper-V	530
3.1.2	Configuration du rôle	530
3.1.3	Configuration des réseaux virtuels	531
3.1.4	Configuration du stockage	532
3.2	Création et configuration d'une machine virtuelle	534
3.2.1	Dynamic Memory	535
3.2.2	Resource Metering	537
3.3	Gestion de la haute disponibilité avec Hyper-V	539
3.3.1	Live migration	539
3.3.2	Réplicas Hyper-V	540
3.4	SCVMM 2012 SP1	543
3.5	Mises à jour Windows	551

## Chapitre 12

### Déploiement des serveurs et postes de travail

1.	Introduction	555
2.	Préparer son déploiement en choisissant bien sa stratégie	555
2.1	Définir le périmètre	556
2.2	Gestion des licences	557
2.3	Choix de l'édition et du type d'installation	558

3.	Créer et déployer	558
3.1	Microsoft Deployment Toolkit (MDT 2012)	559
3.2	Lite Touch	567
3.3	WDS	574
4.	Aller plus loin	578
4.1	Microsoft Application Compatibility Toolkit	578
4.2	Environnement à la demande	579
4.3	ImageX	579
4.4	DISM (Deployment Image Servicing and Management)	580
4.5	Zero touch avec SCCM 2012 SP1	581
4.6	Joindre le domaine sans réseau	581
4.7	En cas de problème	582

## Chapitre 13 Sécuriser votre architecture

1.	Introduction	583
2.	Principe de moindre privilège	583
2.1	Les différents types de compte	584
2.2	Le contrôle d'accès utilisateur	586
2.3	Gérer vos groupes à l'aide des groupes restreints	591
2.4	AppLocker ou le contrôle de l'application	593
2.5	Assistant configuration de la sécurité	601
2.6	Le contrôle d'accès dynamique	612
2.6.1	Principe du contrôle d'accès dynamique)	612
2.6.2	Terminologie	613
2.6.3	Méthodes de mise en œuvre et pré-requis	614
2.6.4	Étude d'un exemple et analyse des besoins	614
2.6.5	Pour aller plus loin...	628
3.	Délégation d'administration	631
3.1	Approche de la délégation d'administration	631
3.2	Délégation de comptes utilisateur	631
4.	Sécurisation du réseau	640
4.1	Network Access Protection	640
4.2	Le pare-feu Windows	640
4.3	Le chiffrement IPsec	651

## Chapitre 14

### Cycle de vie de votre infrastructure

1. Introduction . . . . .	655
2. Gestion des sauvegardes . . . . .	655
2.1 Windows Server Backup . . . . .	656
2.1.1 Installation de Windows Server Backup . . . . .	657
2.1.2 Création d'une sauvegarde complète planifiée . . . . .	658
2.1.3 Création de la sauvegarde planifiée d'un (or de plusieurs) dossier(s) . . . . .	662
2.1.4 Outils associés à WSB et sauvegardes uniques . . . . .	664
2.1.5 Les clichés instantanés . . . . .	666
2.2 Restauration de données . . . . .	670
2.2.1 Restauration des fichiers et/ou de dossiers . . . . .	670
2.2.2 Restauration de l'état du système . . . . .	672
2.3 Grappe RAID . . . . .	675
2.4 Nouveau système de fichiers . . . . .	676
2.4.1 Resilient File System (ReFS) . . . . .	676
2.4.2 Déduplication des données . . . . .	678
3. Gestion des mises à jour . . . . .	684
3.1 Présentation de WSUS . . . . .	684
3.2 Installation de WSUS . . . . .	685
3.3 Utilisation de WSUS . . . . .	689

## Chapitre 15

### Se préparer pour le futur

1. Après Windows Server 2012 et Windows 8 . . . . .	695
2. Le calendrier attendu . . . . .	696

Index . . . . .	697
-----------------	-----

# Chapitre 5

## Mise en place des services réseau d'entreprise

### 1. Introduction

Ce chapitre est consacré à la définition et la configuration des composants nécessaires au bon fonctionnement d'un réseau d'entreprise basé sur Windows Server 2012.

Les composants IP, DNS, DHCP, WINS, ainsi que la mise en place de la quarantaine réseau sur DHCP, IPsec et 802.1x seront abordés.

### 2. Le choix de l'infrastructure réseau

La mise en place de toute architecture réseau passe par l'analyse des réseaux existants. Il est souvent difficile de modifier l'ensemble en une seule fois. La migration se fait donc souvent en implémentant un nouvel adressage réseau et une cohabitation avec les réseaux existants. La modification de l'adressage IP est souvent vue comme coûteuse, n'apportant que peu d'avantages supplémentaires.

C'est souvent lors du déplacement ou de la création d'un site qu'il est facile voire nécessaire de repenser l'adressage IP et de planifier un nouveau système.

Le changement d'un domaine DNS est encore plus compliqué, surtout lorsque ce domaine DNS sert de support à un domaine Active Directory. Dans ce cas, une migration représente une étude particulière qui sort du cadre de cette présentation.

## 2.1 Le choix de l'architecture réseau

Deux points précis sont à étudier à ce niveau :

- Le choix de la zone DNS.
- Le choix de la classe réseau.

### 2.1.1 La zone DNS

Deux aspects sont importants lors du choix de la zone DNS.

Le nom choisi pour la zone DNS doit correspondre à l'intégralité de l'entité (entreprise, groupe, etc.) que l'on souhaite gérer. Ce nom doit pouvoir être accepté par toutes les entités dépendantes qui vont se retrouver dans cette zone. Le problème est beaucoup plus politique que technique !

Si une entité n'est pas dans ce cadre, cela veut dire qu'une zone DNS spécifique doit lui être affectée.

Si la zone DNS doit être utilisée sur Internet, le domaine DNS sera forcément public et enregistré, c'est-à-dire utilisant une extension reconnue de type **.fr**, **.com**, **.info**...

Pour un réseau interne, le domaine peut être public ou privé. Le choix le plus courant est alors d'utiliser un domaine DNS local avec une extension inconnue sur Internet. L'extension **.local** est très souvent utilisée sous la forme **masociete.local**. Le découpage entre ce qui est interne ou externe est plus facile à réaliser. Ce choix est maintenant à déconseiller, car les fournisseurs de certificats ont décidé, en accord avec les grands éditeurs, de ne plus distribuer à partir du 1<sup>er</sup> Janvier 2014 de certificats comportant des noms appartenant à des domaines DNS non vérifiables. Ceci a une conséquence directe pour la configuration de nombreux serveurs Exchange qui possèdent ce type de certificats. Mais, il est probable que certains serveurs Web visibles à la fois en Intranet et en Internet utilisaient ce type de fonctionnalité.

En revanche, l'utilisation du même nom de domaine sur le réseau interne et sur Internet suppose des serveurs DNS différents pour ne rendre visible sur Internet que ce qu'il est souhaitable de montrer. Cela entraîne une double administration des zones DNS. Cette solution est plus complexe.

Pour les nouvelles installations, la préconisation sera :

- soit d'utiliser un domaine qui a une extension reconnue (et disponible à l'enregistrement) telle que **.org**, **.net**, **.info**.
- soit de définir un sous-domaine du domaine public déjà utilisé, sous la forme **ad.masociete.fr**.

Dans les deux cas, l'obtention d'un certificat public ne posera aucun problème.

### 2.1.2 La classe réseau

Pour tous les réseaux internes, le choix se portera évidemment toujours sur les classes réseaux privées. Si l'on ne peut pas toujours modifier l'intégralité des réseaux existants pour des raisons souvent historiques, on peut au moins créer tous les nouveaux réseaux en suivant cette règle.

La classe du réseau se choisit en fonction du nombre de machines présentes sur le réseau, du nombre de sites, etc. Un réseau de classe C (192.168.0.X) représente souvent un bon choix initial. Il est toujours possible de changer de classe, de réseau ou même surtout d'utiliser plusieurs réseaux en fonction des besoins.

L'usage de TCP/IP v6 n'est pas encore bien développé mais deviendra nécessaire dans les deux ou trois années qui suivent, principalement sur Internet. Sur le réseau local, il reste encore de nombreux logiciels qui ne sont pas compatibles, mais ceci devrait évoluer très rapidement ! Le réseau IPv6 est étudié dans le chapitre Les évolutions du réseau.

## 2.2 L'installation d'un serveur DHCP

Si le service DHCP permet de mettre en place rapidement le réseau choisi, il permet aussi de modifier rapidement et globalement une série de paramètres. Les entreprises n'utilisant aucun service DHCP sont maintenant très rares.

Parmi les nombreux composants de Windows Server 2012, le service DHCP est un rôle.

### 2.2.1 Définition

Le protocole DHCP (*Dynamic Host Configuration Protocol*) a pour but de fournir une adresse IP et un masque de sous-réseau à tout périphérique réseau (station, serveur ou autre) qui en fait la demande. Selon la configuration, d'autres paramètres tout aussi importants seront transmis en même temps : les adresses IP de la route par défaut, des serveurs DNS à utiliser, des serveurs WINS et le suffixe de domaine pour ne citer que les principaux.

DHCP est souvent réservé aux stations, aux imprimantes et ne devrait servir qu'exceptionnellement aux serveurs.

### 2.2.2 L'installation

Comme pour tous les composants Windows, l'installation peut se faire graphiquement ou par commande PowerShell sans avoir besoin d'insérer le moindre média.

Installation via PowerShell :

```
Install-WindowsFeature DHCP
```



**Remarque**

Attention, le service sera démarré immédiatement et configuré en démarrage automatique ! En revanche, l'installation du composant DHCP par PowerShell n'installe que le service DHCP. Il faut lancer la commande indiquée ci-dessous pour installer l'outil d'administration.

```
Install-WindowsFeature RSAT-DHCP
```

Le service doit être démarré pour que DHCP soit accessible et configurable.

Pour que le service DHCP commence à distribuer des adresses, il est indispensable de configurer et d'activer une étendue.

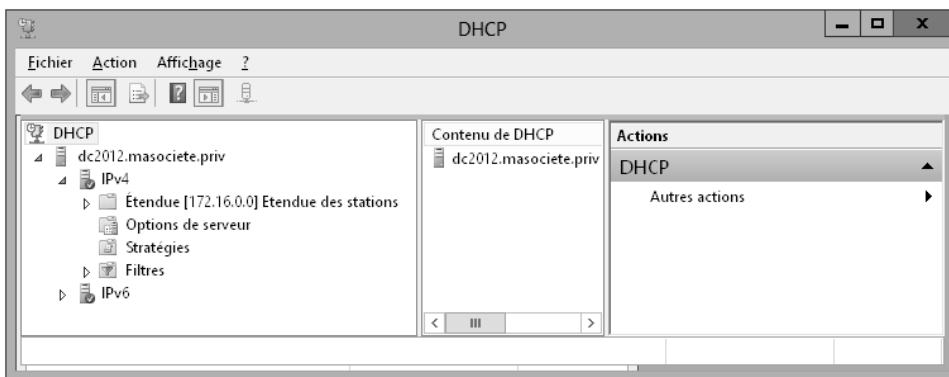
Attention, si le serveur qui héberge DHCP fait partie d'une forêt Active Directory, il doit en plus avoir été autorisé par des administrateurs membres du groupe **Administrateurs de l'entreprise** ou ayant reçu les droits d'administration DHCP.

Le service DHCP, comme les autres services réseau de référence (DNS, WINS), devrait toujours être installé sur des serveurs disposant d'adresses IP fixes.

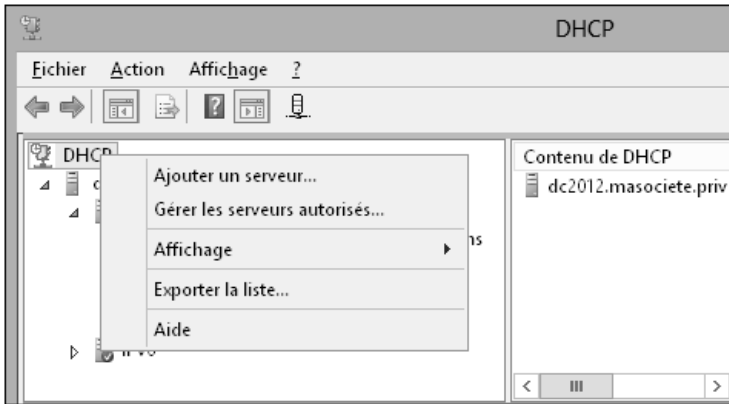
### 2.2.3 La configuration

La console d'administration DHCP se trouvera sur tout serveur où le rôle DHCP a été installé par l'interface graphique et sur tout serveur où le composant d'administration a été ajouté spécifiquement.

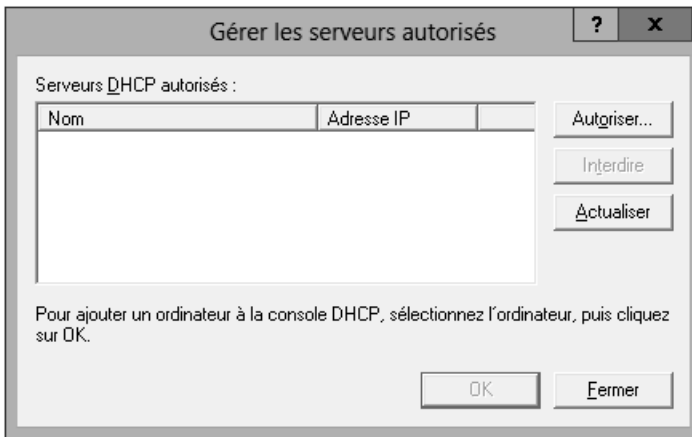
Si le serveur local héberge le rôle DHCP, le serveur apparaît automatiquement dans la console.



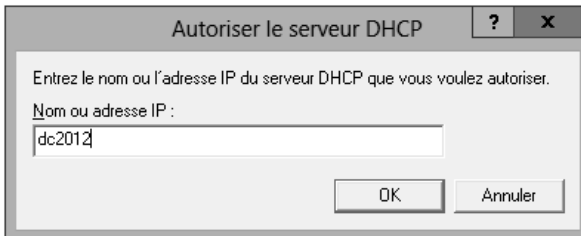
- Si le serveur n'héberge pas le rôle DHCP ou n'est pas celui souhaité, utilisez le bouton droit pour ajouter un serveur spécifique ou le sélectionner parmi les serveurs autorisés.



► Pour autoriser un serveur DHCP, utilisez l’option **Gérer les serveurs autorisés**.

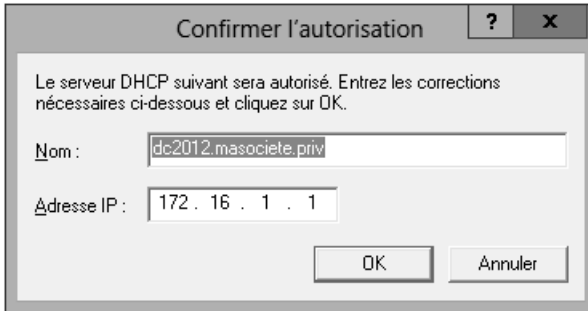


► Cliquez sur le bouton **Autoriser**, et saisissez le nom ou l’adresse IP.

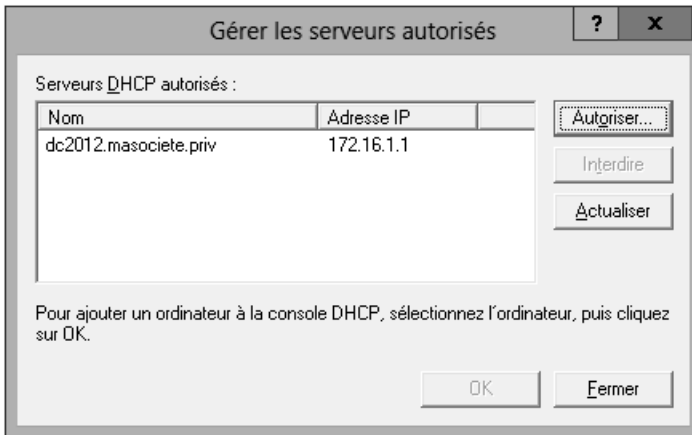


Dans une forêt Active Directory, seuls les serveurs DHCP qui ont été autorisés par les administrateurs de l'entreprise ont le droit d'émettre des adresses IP à partir des étendues actives.

- ▣ Confirmez l'adresse et le nom proposés en cliquant sur le bouton **OK**.



- ▣ Fermez la fenêtre des serveurs autorisés en cliquant sur **Fermer**.



Les serveurs autorisés apparaissent avec une flèche verte.