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'entre 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 1er 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.

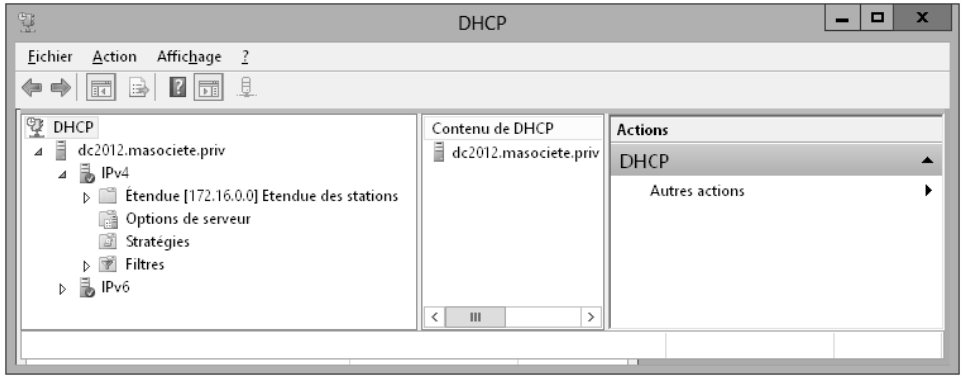
Attention, si le serveur qui héberge DHCP fait partie d'une forêt Active Directory, il doit en plus avoir été autorisé par des administrateurs membres du groupe **Administrateurs de l'entreprise** ou ayant reçu les droits d'administration DHCP.

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

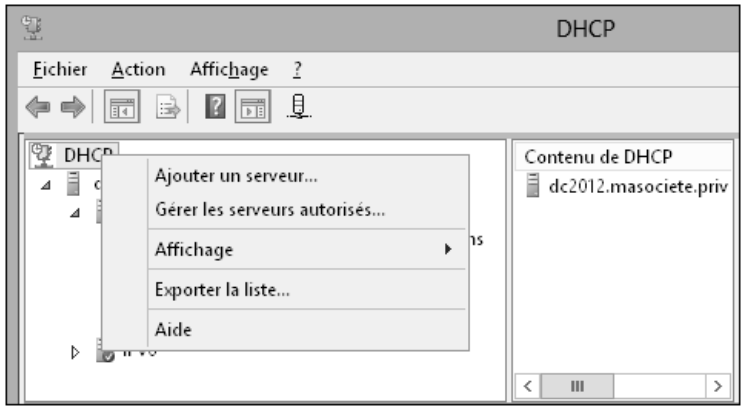
2.2.3 La configuration

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.

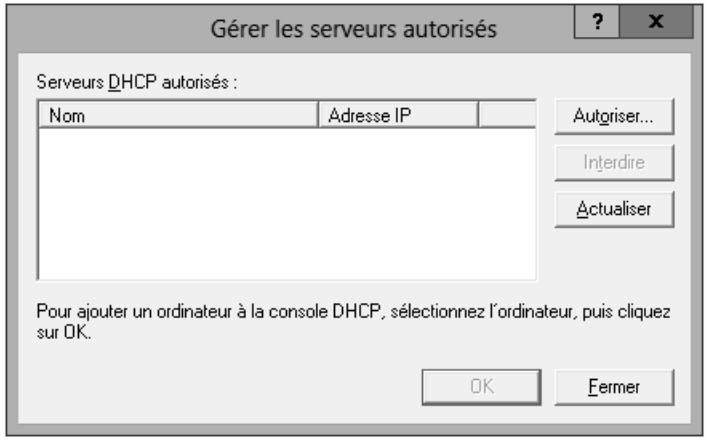
Si le serveur local héberge le rôle DHCP, le serveur apparaît automatiquement dans la console.



- 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**.

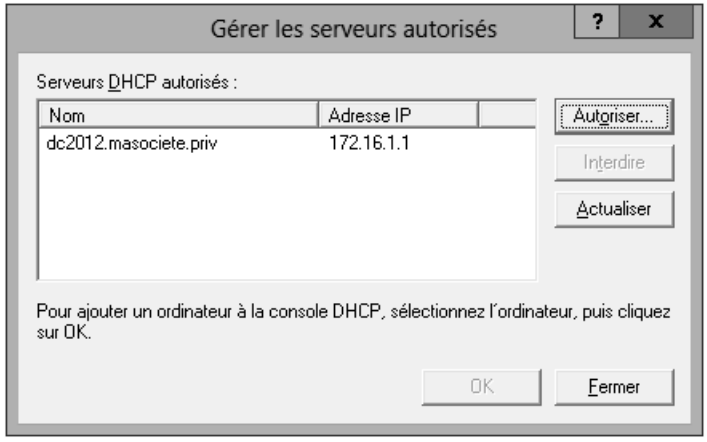


- Cliquez sur le bouton **Autoriser**, et saisissez le nom ou l'adresse IP.

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.