République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la
Recherche Scientifique

Université Abderrahmane Mira Bejaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de L'obtention du diplôme de master professionnel en Administration et sécurité des réseaux

Thème :

Mise en œuvre d'une infrastructure réseau sous Windows server 2012 R2

Cas d'étude : Entreprise Portuaire de Bejaia

Réalisé par :

CHILLA Oumennoune Yasmine.

MAOUCHE Amel.

Devant le jury :

Président : *Mme BOUTRID Samia.*

Examinateur : *Mme KHOULALENE Nadjet.*

Encadreur : *Mr BOUKERRAM Abdellah.*

Co-Encadreur: *Mr OMAR Mawloud.*

Encadreur de stage: Mr *BETACHE Idir.*

Promotion : 2015/2016.

Dédicaces

Ce modeste travail est dédié :

A nos chers parents qui nous ont soutenus et encouragés

tout au long de notre cursus.

A nos frères et sœurs

A nos enseignants

A nos ami(e)s

A toutes les personnes qui nous ont apportés de l'aide.

REMERCIEMENTS

En préambule à ce mémoire nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette année universitaire.

Nous tenons à remercier Mr BOUKERRAM ainsi que Mme AIT KACI AZZOU, BOUKERRAM qui, en tant qu'encadreur et Co-encadreur se sont toujours montrés à l'écoute.

Nous remercions sincèrement Mr MEKHOUKH Fares qui ne nous a lésé d'aucune information, qui a été très disponible tout au long de la rédaction de ce mémoire, Sans oublier les membres de la commission du jury qui évalueront notre travail.

Enfin, nous adressons nos plus sincères remerciements à nos parents et ami(e)s, pour leur soutien et encouragements tout au long de la réalisation de ce projet.

Merci à tous et à toutes.

Glossaire

DHCP: **D**ynamic **H**ost **C**onfiguration **P**rotocol.

DNS: **D**omain **N**ame **S**ystem.

GPO: **G**roup **P**olicies **O**bject.

GUI: **G**raphical **U**ser **I**nterface.

IDS: **I**ntrusion **D**etection **S**ystem.

IP: **I**nternet **P**rotocol.

IPAM: **IP** **A**ddress **M**anagement.

IPS: **I**ntrusion **P**revention **S**ystem.

ISCSI: **I**nternet **S**mall **C**omputer **S**ystem **I**nterface.

LAN: **L**ocal **A**rea **N**etwork.

MAC: **M**edia **A**cces **C**ontrol.

NT: **N**ew **T**echnology.

OS: **O**perating **S**ystème.

PKI: **P**ublic **K**ey **I**nfrastructure.

RAID: **R**edundant **A**rray of **I**ndependent **D**isks.

ReFS : **R**esilient **F**ile **S**ystem.

RIS: **R**emote **I**nstallation **S**ervices.

SQL: **S**tructured **Q**uery **L**anguage.

TCP: **T**ransmission **C**ontrol **P**rotocol.

VPN: **V**irtual **P**rivate **N**etwork.

VM: **V**irtual **M**achine.

WAN: **W**ide **A**rea **N**etwork.

WIMAX: **W**orldwide **I**nteroperability for **M**icroware **A**ccess.

WS: **W**indows **S**erver.

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

De nos jours, les réseaux informatiques sont devenus un atout incontournable voire indispensable au sein d'une entreprise quel que soit son secteur d'activité.

On compte désormais sur les services offerts par les réseaux pour le fonctionnement de l'outil informatique. Les systèmes d'information sont au centre des différentes entités métiers et doivent fonctionner pleinement et en permanence pour garantir l'efficacité de l'entreprise. A tous les niveaux, les réseaux, les terminaux utilisateurs, les serveurs d'application, les données, constituent autant de maillons sensibles dont la disponibilité et la qualité de service conditionnent le bon fonctionnement de l'entreprise et les problèmes liés aux réseaux informatiques doivent donc être réduits au minimum.

L'administrateur réseau a le souci de mettre en place des moyens de contrôle des accès, et pour cela, il doit résoudre à la fois la simplicité pour l'utilisateur, fiabilité des mécanismes, le niveau de sécurité élevé le tout en utilisant le plus possible les ressources mises à sa disposition.

C'est dans ce cadre que s'inscrit notre travail dont les objectifs fixés sont :

- Administration d'un réseau LAN (soit le réseau de l'EPB).
- Mise à niveau et configuration des serveurs du réseau.
- Solutions de sécurité : tolérance aux pannes et gestion des PKI.

Organisation du mémoire :

Le premier chapitre donne un bref aperçu sur les réseaux informatiques ainsi que le modèle adéquat pour une entreprise telle que celle de l'EPBejaia, puis une explication des différentes fonctionnalités d'un administrateur réseaux suivie des outils d'administration à savoir Microsoft SQL Server, Active Directory et Windows server. Nous avons egalement établi une étude comparative des différents OS Serveur.

Dans le deuxième chapitre nous présentons l'infrastructure informatique de « EPBejaïa », nous consacrerons une part à la présentation de l'entreprise, l'organisation humaine et la place du centre informatique, et une autre part à l'étude

des principaux aspects du réseau local, les besoins et les faiblesses de l'entreprise. Nous terminons avec une proposition de solutions d'amélioration.

La réalisation fera l'objet du troisième chapitre dans lequel nous définirons les outils que nous avons utilisés et nous aborderons les configurations et la mise en œuvre des solutions proposées.

Enfin, nous conclurons ce travail en résumant les points forts de ce travail, suivi de perspectives futures.

Chapitre I :

Les réseaux, administration et sécurité

Introduction

Le besoin de communication et de partage a poussé les entreprises à s'orienter vers les réseaux informatiques et travailler d'avantage pour les améliorer. Dans ce premier chapitre nous allons aborder le concept des réseaux informatiques, ensuite nous allons passer aux multiples tâches d'un administrateur réseau ainsi qu'aux différents outils d'administration.

I.1 Réseau informatique d'entreprise

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs ordinateurs en vue d'échanger, de partager des données, des ressources ou des informations. En d'autres termes c'est une infrastructure de communication reliant des équipements informatiques (ordinateur, concentrateur, commutateur, routeur, imprimante...) permettant de partager des ressources communes. Il est caractérisé par un aspect physique (câble véhiculant des signaux électriques) et un aspect logique (les logiciels qui réalisent les protocoles). [1]

I.1.1 Les objectifs du réseau informatique

Les objectifs d'un réseau sont classiquement les suivants :

- **Le partage de ressources :** Rendre accessible à une communauté d'utilisateurs des programmes, des données et des équipements informatiques indépendamment de leur localisation.
- **La Fiabilité :** Permettre le fonctionnement même en cas de problèmes matériels (sauvegardes, duplication ...).
- **La réduction des coûts :** Aujourd'hui, l'architecture la plus répondue en entreprise est celle du client/serveur qui est plus économique, plus souple et permettant un déploiement facile. [1]

I.1.2 Les modèles de réseaux

Il existe deux modes de communication dans les réseaux : le modèle client-serveur et le modèle Pair-à-Pair :

❖ Le modèle Pair-à-Pair (Peer to Peer)

Dans ce modèle, tous les ordinateurs ont le même rôle. Ils sont équipés d'un logiciel (assimilé à un logiciel client-serveur) et peuvent communiquer et échanger entre eux. [2]

- **Avantages**
  - ✓ Les réseaux Postes à Postes sont faciles et pas cher à installer.
  - ✓ Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.

- **Inconvénients**
  - ✓ Le système devient ingérable lorsque le nombre de postes augmente.
  - ✓ Les outils de sécurité sont très limités.

Ils conviennent pour les petites structures (moins de quinze postes) avec des utilisateurs compétents pour administrer eux-mêmes leur propre machine. [3]

❖ Le modèle client-serveur

Un serveur est un ordinateur (équipé d'un logiciel serveur) dont le rôle est de répondre aux requêtes envoyées par des ordinateurs clients (équipés d'un logiciel client).

1. Le client envoie une requête au serveur.
2. Le serveur traite la requête et retourne une réponse. [2]

- **Avantage**

Le réseau Client/serveur réuni deux avantages complémentaires, l'indépendance et la centralisation :

- ✓ L'indépendance : Les stations peuvent travailler en mode autonome et ouvrir des sessions locales.
- ✓ La centralisation : L'administration du réseau est réalisée par un administrateur ou un super utilisateur qui gère le réseau et qui a tous les droits : La standardisation des installations et des mises à jour des applications sur un très grand nombre de postes, permet d'uniformiser la configuration d'un grand nombre de postes, la planification du réseau, son évolution, sa croissance, ses changements, la stratégie de sécurité, les sauvegardes ...

Dans un réseau client-serveur, avec des serveurs d'applications et de fichiers, et une configuration standardisée pour les stations clientes, il est très facile de changer une machine en panne. C'est « l'interchangeabilité » qui limite la durée d'une panne pour l'utilisateur. Toutefois, une organisation en client-serveur requiert des machines dédiées et très performantes.

- **Inconvénients**

Les serveurs deviennent les points faibles du réseau (panne, piratage…) et doivent être protégés rigoureusement, avec un système RAID par exemple. [4]

I.1.3Adressage réseau

De manière générale, les adresses forment une notion importante en communication et sont un moyen d'identification. Dans un réseau informatique, une adresse IP est un identifiant unique attribué à chaque interface avec le réseau IP et associé à une machine (routeur, ordinateur, etc.). C'est une adresse unicast utilisable comme adresse source ou comme destination.

Une adresse IP est décomposée en deux parties : une partie de l'adresse identifie le réseau (netid) auquel appartient l'hôte et une partie identifie le numéro de l'hôte (hostid) dans le réseau.

Il existe deux versions pour les adresses IP :

- ✓ Version 4 : les adresses sont codées sur 32 bits - Elle est généralement notée avec quatre nombres compris entre 0 et 255, séparés par des points.
- ✓ Version 6 : les adresses sont codées sur 128 bits - Elle est généralement notée par groupes de 4 chiffres hexadécimaux séparés par ':'.

On distingue deux situations pour assigner une adresse IP à un équipement :

- ✓ **De manière statique :** l'adresse est fixe et configurée le plus souvent manuellement puis stockée dans la configuration de son système d'exploitation.
- ✓ **De manière dynamique :** l'adresse est automatiquement transmise et assignée grâce au protocole DHCP. [5]

I.1.3.1 Protocole DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau permettant d'assigner automatiquement des informations TCP/IP aux ordinateurs clients. Chaque client DHCP se connecte au serveur central DHCP, lequel renvoie la configuration réseau du client, y compris l'adresse IP, la passerelle et les serveurs DNS.

Le DHCP permet donc de configurer automatiquement les paramètres réseaux d'une machine. Ses avantages :

- Simplifier l'installation d'un grand nombre de machines.
- Grande souplesse pour les utilisateurs mobiles. Ils peuvent passer d'un réseau à un autre sans avoir à modifier leur paramètre réseau.
- Reconfiguration complète d'un réseau (changement de classe d'IP, etc.) très simple. Une seule machine à modifier qui le serveur DHCP.
- Centralisation de la base effectuant la correspondance entre adresses IP et MAC

I.1.3.2 Serveur DNS

DNS (Domain Name System, système de noms de domaine) est un système de noms pour les ordinateurs et les services réseau organisé selon une hiérarchie de domaines. Le système DNS est utilisé dans les réseaux TCP/IP tels qu'Internet pour localiser des ordinateurs et des services à l'aide de noms conviviaux. Lorsqu'un utilisateur entre un nom DNS dans une application, les services DNS peuvent résoudre ce nom en une autre information qui lui est associée, par exemple une adresse IP. C'est une sorte de base de données dynamique, globalement distribuée, cohérente, évolutive et fiable. Ses avantages :

1. Existence d'un cache DNS qui accélère la recherche des noms.
2. Possibilité d'en avoir plusieurs sur différents serveurs afin de garantir son service en cas d'arrêt d'un des serveurs (Installation maitre sur un serveur principal et esclave sur les autres).
3. Facilité de mise en place.

4. Une entreprise peut disposer de son propre DNS. [6]

I.2 Administration réseau

L'administration des systèmes et des réseaux consiste à contrôler, coordonner et surveiller les différentes ressources mises en œuvre afin de fournir des services opérationnels aux utilisateurs : ces ressources sont les équipements, le réseau, les services sont ceux offerts par les différents serveurs, les applications, Internet, etc...

L'administration du réseau est appliquée en suivant une politique, c'est-à-dire des objectifs à atteindre, cette politique spécifie des actions à long, moyen et court terme :

- Une stratégie, plan des actions à entreprendre à long terme, de quelques mois à un ou deux ans.
- Une tactique, plan d'exécution pour atteindre les objectifs à moyen terme, de quelques jours à un a deux mois
- Un fonctionnement opérationnel, pour gérer le réseau en continu, à court terme, de quelques minutes à quelques heures

I.2.1 Fonctionnalité

Elles sont regroupées en cinq grandes classes :

1. **Gestion des anomalies :** Elle recouvre la détection des anomalies, l'identification et la correction des fonctionnements anormaux. Ces défauts font qu'un système n'atteint pas ses objectifs ; ils sont temporaires ou permanent.

2. **Gestion de la comptabilité :** C'est une activité qui peut être complexe car elle doit prendre en considération les Informations des utilisateurs sur le cout encourus ou les ressources utilisée.

3. **Gestion des performances :** Cette activité analyse le trafic, le fonctionnement du réseau (débit, temps de réponse) et utilise ces informations pour régler le système en déterminant de nouvelle procédure d'acheminement.

4. **Gestion de la configuration et des noms :** Elle permet de gérer les composants des systèmes et des les designers par leur adresse physique ou leur

nom (adresse logique), ceux-ci sont consignés dans différents fichier répartis dans les systèmes interconnectés et leur mise à jour doit en garder la cohérence.

5. **Gestion de la sécurité :** Elle droit répondre à deux types de problèmes : Garantir les abonnés (les utilisateurs) et le réseau lui-même contre les intrusions volontaires et involontaires. Pour cela elle comporte la création, suppression et contrôle des mécanismes de services de sécurité et le compte rendu d'événements relatifs à la sécurité. [7]

I.2.2 Les outils d'administration

I.2.2.1 Microsoft SQL serveur

SQL Server est un produit Microsoft utilisé pour gérer et stocker des informations. Techniquement, SQL Server est un « système de gestion de base de données relationnelle » (SGBDR), ce terme signifie deux choses. Tout d'abord, que les données stockées dans SQL Server seront logées dans une « base de données relationnelle", et deuxièmement, que SQL Server est un ensemble de « système de gestion », et pas seulement une base de données. SQL lui-même représente Structured Query Language. Ceci est le langage utilisé pour gérer et administrer le serveur de base de données. [8]

I.2.2.2 Windows server

Windows Server fait référence à tout type d'instance de serveur qui est installé, exploité et géré par l'un de la famille Windows Server des systèmes d'exploitation. Il fournit la même capacité, les caractéristiques et le mécanisme de fonctionnement d'un système d'exploitation de serveur standard et est basé sur l'architecture Windows NT. [9]

I.2.2.3 Active Directory

Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone, etc.) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données, etc.

Le service Active Directory permet une gestion centralisée. Cela donne la possibilité d'ajouter, de retirer et de localiser les ressources facilement, il offre aussi des mécanismes de sécurité pour protéger ses informations.

Il est donc un outil destiné aux utilisateurs mais dans la mesure où il permet une représentation globale de l'ensemble des ressources et des droits associés il constitue également un outil d'administration et de gestion du réseau. Il fournit à ce titre des outils permettant de gérer la répartition de l'annuaire sur le réseau, sa duplication, la sécurisation et le partitionnement de l'annuaire de l'entreprise. [10]

I.3 Les Os serveur

Un système d'exploitation serveur, est un système d'exploitation spécialement conçu pour fonctionner sur les serveurs , qui sont des ordinateurs spécialisés qui opèrent au sein d' une architecture client / serveur pour répondre aux demandes des ordinateurs clients sur le réseau.

Les OS (Operating Système) serveur aident à activer et faciliter les rôles de serveurs typiques tels que : serveur Web, serveur de messagerie, serveur de fichiers, serveur de base de données, serveur d'applications et serveur d'impression. Ci-dessous sont présentés les différents systèmes d'exploitation orientés serveur et leurs distributions les plus courantes [11] :

L'OS	Les distributions les plus courantes
Linux	• Slackware (commercial ou téléchargement gratuit). • Redhat (commercial ou téléchargement gratuit). • Suse (commercial). • Debian (gratuit). • Mandrake.
BSD (La *Berkeley Software Distribution*)	• Open BSD (gratuit). • FreeBSD (gratuit). • NetBSD (gratuit). • BSDi (commercial).
Sun Microsystems	• Solaris/SunOS (commercial, gratuit pour une utilisation non commerciale).
Windows	• Windows NT. • Windows serveur 2000. • Windows serveur 2003. • Windows serveur 2003 R2. • Windows serveur 2008. • Windows serveur 2008 R2. • Windows 2012. • Windows 2012 R2.

Tableau I-1 : les différents OS serveur.

I.3.1 La famille Windows serveur

Nous aborderons dans ce qui suit les versions les plus récentes de Windows serveur :

- **Définition du WS 2003**

Windows Server 2003 est un système d'exploitation orienté serveur développé par Microsoft. Présenté le 24 avril 2003 comme le successeur de Windows Server 2000. Une version évoluée intitulée Windows Server 2003 R2 a été finalisée le 6 décembre 2005. Le 14juillet2015, Microsoft cesse de le supporter, ce qui signifie l'arrêt de la publication de correctifs de sécurité.

- **Définition du WS 2008**

Il est considéré comme le successeur de Windows Server 2003. Les administrateurs bénéficient d'un environnement serveur d'avantage sécurisé et fiable car il s'appuie sur les points forts du système d'exploitation Windows Server 2003 et sur les innovations de Windows Server 2003 R2. Cependant, Windows Server 2008 est bien plus qu'une version perfectionnée des systèmes d'exploitation précédents. Il a été conçu pour offrir aux entreprises la plateforme la plus efficace pour prendre en charge des applications, des réseaux et des services Web. Il existe cinq éditions stables :

- ✓ Edition Standard.
- ✓ Edition Enterprise.
- ✓ Edition Datacenter.
- ✓ Edition Web.
- ✓ Edition Itanium.

- **Définition du WS 2012**

Windows Server 2012 est un système d'exploitation serveur complet, polyvalent et puissant qui se base sur les améliorations que Microsoft a apportées à Windows server 2008 R2. Windows server 2012 et Windows 8 partagent un certain nombre de caractéristiques car ils font partie du même projet de développement. Ces fonctionnalités partagent une base de code commune qui couvre de nombreux domaines du système d'exploitation, notamment la gestion, la sécurité, le réseau et le stockage. Il existe quatre éditions :

- ✓ Edition Standard.
- ✓ Edition Foundation.
- ✓ Edition Essentials.
- ✓ Edition Datacenter.

Windows server 2012 inclut des améliorations dans ce qui suit :

- **Interface utilisateur graphique (GUI)** : Windows Server 2012 a été créé avec le Metro langage de conception de sorte qu'il a le même aspect que Windows 8. Les administrateurs peuvent basculer entre *Server Core* et le *serveur avec* les options *de* l'*interface graphique* sans une réinstallation complète.
- **Gestion des adresses** : Windows Server 2012 a un rôle de gestion d'adresses IP (IPAM) pour découvrir, le suivi et la gestion de l'espace d'adressage IP du réseau.
- **Migration de stockage** : Migration de stockage en direct est autorisé et le stockage partagé ne seront plus nécessaires pour la machine virtuelle (VM) la migration lors de l' utilisation d' Hyper-V Replica.
- **Hyper-V** : Hyper-V 3.0 offre un commutateur extensible évolutif virtuel qui permet à un réseau virtuel pour étendre ses fonctionnalités de façons qui étaient difficiles ou impossibles à obtenir dans les versions précédentes.
- **Système** de **fichiers** : Ajout de ReFS (Resilient File System) pour les serveurs de fichiers. [8]

I.3.2 Comparaison des versions de Windows Server

Le tableau ci-dessous arbore les différentes fonctionnalités proposées dans les versions Windows server :

Fonctionnalités		Serveur 2003	Serveur 2008/2008 R2	Server 2012	Server 2012 R2
Identité et accès	Service Active Directory	✓	✓	✓	✓
	Contrôle d'accès dynamique			✓	✓
	Virtualisation d'active Directory			✓	✓
Virtualisation	Migration dynamique sans partage			✓	✓
	Réplica Hyper-V			✓	✓
	Clustering Hyper-V		✓	✓	✓
Stockage	Migration du stockage dynamique			✓	✓
	Qualité de service du stockage				✓
Mise en réseau	Virtualisation de réseau Hyper-V			✓	✓
	Gestion des adresses IP			✓	✓
Automatisation et gestion	Windows PowerShell	✓	✓	✓	✓

Tableau I-2 : Comparaison des versions Windows Server.

D'après le Tableau, la version de Windows Server qui présente le plus de fonctionnalités et de stabilité est la version Windows server 2012 R2 suivi de Windows Server 2012.

Conclusion

Dans ce chapitre nous avons présenté les notions et les aspects élémentaires des réseaux informatiques d'entreprise, l'administration réseau et système et les différents OS serveurs.

Le réseau informatique de l'EPB, sur lequel est focalisé notre travail se présente dans le chapitre qui suit.

Chapitre II :

Etude du réseau LAN : Infrastructure de l'EPB

Introduction

Une bonne compréhension de l'environnement informatique de l'entreprise aide à déterminer la portée de notre projet. Il est essentiel de disposer d'informations précises sur l'infrastructure réseau et les problèmes qui ont une incidence sur le fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement.

II.1 Présentation de l'entreprise portuaire de Bejaia

Le port de Bejaïa est un port Algérien se situant dans la région de Kabylie dans le nord du pays. Il est notamment consacré au commerce international et aux hydrocarbures.

Il joue un rôle très important dans les transactions internationales vu sa situation géographique qui se résume comme suit :

- Délimité au Nord par la route national N°9.
- Au sud par les jetées de fermeture et du large sur une largeur de 2750 m.
- A l'est par la jetée Est.
- A l'ouest par la zone industrielle de Bejaia.

II.2 Missions de l'EPB

La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentielles portuaires de Bejaïa, dans le but de promouvoir les échanges extérieurs du pays.

- Traiter, dans les meilleures conditions de délais, de coût et de sécurité, l'ensemble des passagers, des marchandises et des navires.
- La gestion et l'exploitation des infrastructures et des superstructures portuaires.
- La manutention et l'acconage des marchandises en transit par le port de Bejaia.
- Le transit des passagers et leurs véhicules par la gare maritime.
- Mise à disposition d'infrastructures nécessaires aux activités relatives aux hydrocarbures (exportation pétrole et de cabotage national des produits raffinés et gaz de pétrole liquéfié).
- Le pilotage, le remorquage et le lamanage des navires dans les limites de la zone de pilotage dans le port de Bejaia.

II.3 Organisation de l'entreprise

Les différentes structures de l'EPB sont présentées dans l'organigramme ci-dessus :

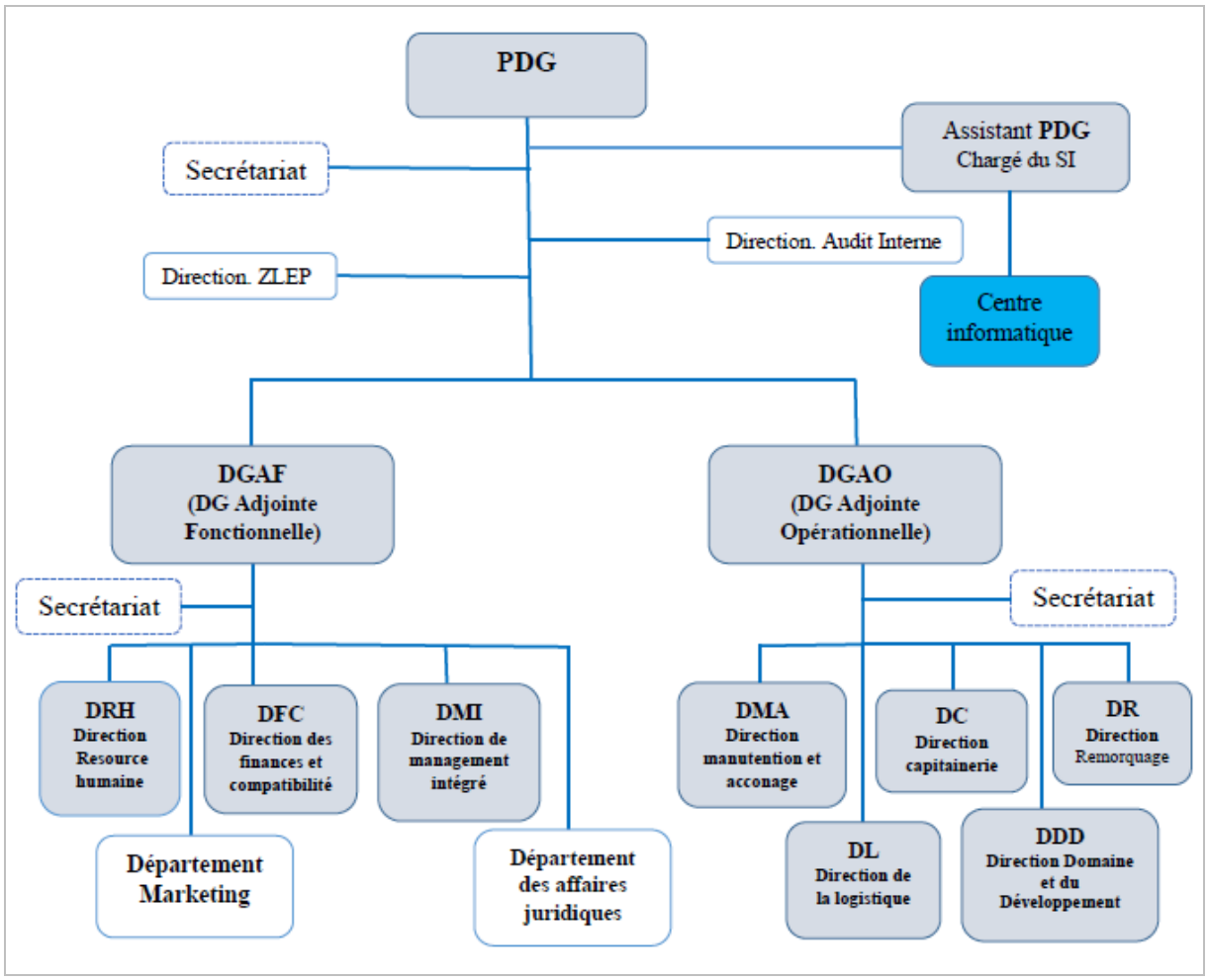


Figure II-1 : Organigramme général de l'EPB.

II.4 Le Centre informatique

II.4.1 Présentation du centre informatique

Le centre informatique est une structure de l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'entreprise portuaire de Bejaïa, et cela en mettant en place les logiciels et l'infrastructure nécessaire pour la gestion du système d'information.

L'EPB déploie des systèmes d'informations pour accroitre la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces

systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs. Le réseau local de l'entreprise apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

II.4.2 L'organisation humaine

Le centre informatique se compose de trois départements sous la coupe de l'assistant du PDG chargé du SI, chaque département est structuré en services comme le montre l'organigramme suivant :

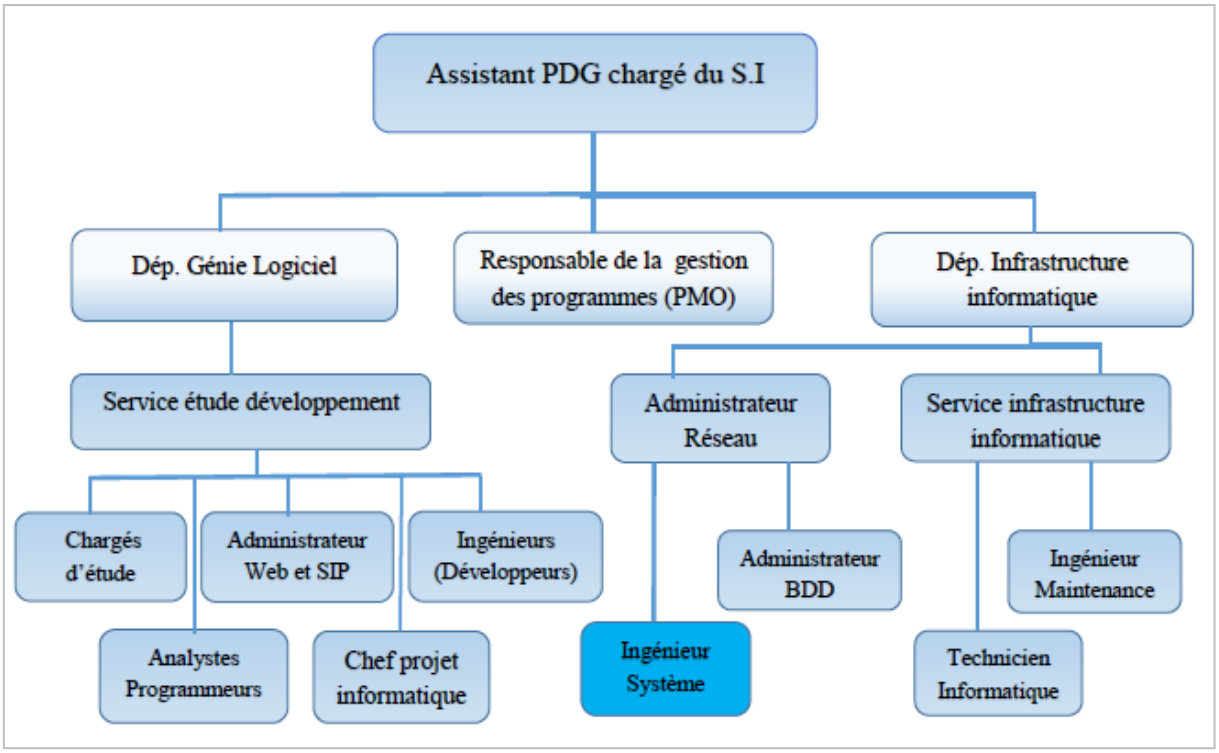


Figure II-2 : Organigramme du centre informatique.

II.5 Le réseau local de l'EPB

Le réseau local de l'EPB permet aux différents postes de travail de s'échanger des informations, de se connecter vers l'extérieur et d'utiliser des applications hébergées en interne nécessaire a l'exécution des taches quotidiennes des employées. Le réseau du port de Bejaia s'étend du port pétrolier (N16) aux ports 13 et 18 (port à bois).

II.5.1 Architecture du réseau local actuel de l'entreprise

L'architecture du réseau LAN de l'entreprise est représentée dans la figure ci-dessous :

Figure II-3 : Architecture actuelle du réseau local de L'EPB.

- **Connexion internet :** L'entreprise portuaire de Bejaia est dotée de deux connexions internet, Icosnet et Algérie télécom en utilisant l'accès haut débit sans fil WIMAX (Worldwide Interoperabilite for Microware Access) qui est une solution alternative pour le déploiement des réseaux haut-débit, l'entreprise se connecte à Internet sans-fil à partir d'un poste fixe qui communique par ondes hertziennes via une antenne-relais appelée station de base.

- **Sécurité internet :** L'Internet représente un canal non sécurisé pour l'échange d'informations conduisant à un risque élevé d'intrusion, deux serveurs proxy sont mis en place pour sécuriser le LAN et filtrer les paquets échangés

ainsi définir les règles d'accès à internet et de deux pare feu logiciels de types ISA2004 y sont intégrés pour gérer les stratégies d'accès et les règles de routage qui détermine la manière dont le client accède à internet.

- **Salle machine :** Ou les activités du port se rattachent à cette salle, qui rassemble tous les serveurs nécessaires pour répondre aux attentes des utilisateurs afin d'aboutir à un réseau qui accompagne la croissance de l'entreprise. En plus des switches elle comporte les différents serveurs :

  - **Serveur de base de données SQL SERVEUR 2005 & MY SQL :** pour stocker, extraire, géré les données, les mises à jour dans une base de données.

  - **Serveur de contrôleur de domaine (active directory Windows serveur 2003) :** L'objectif principal d'*Active Directory* est de stocker les données et gérer les interactions entre l'utilisateur et le domaine, y compris les processus d'ouverture de session, l'authentification et les recherches dans l'annuaire.

  - **Serveur de contrôleur de domaine en redondance (active directory Windows serveur 2003) :** la réplication permet au service d'annuaire Active Directory de conserver des réplicas de données de l'annuaire sur un autre contrôleur de domaine, ce qui garantit la disponibilité et l'efficacité de l'annuaire pour tous les utilisateurs.

  - **Serveur de sauvegarde des données :** Il a pour rôle de sauvegarder en continue les données générer par l'entreprise. Si un employé efface par erreur un document ou qu'il y a un disfonctionnement d'un ordinateur, un ordinateur est en mesure de rétablir le premier fichier.

  - **Serveur Application/fichier :** mettre à disposition des ressources applicatives à distance, sans prise en compte de l'environnement du poste utilisateur : c'est le serveur d'application qui fait tourner les applications qui sont accessibles simplement via un navigateur internet.

- **Un serveur de messagerie électronique :** est un serveur qui, connecté à Internet, permet à ses utilisateurs d'envoyer et de recevoir des courriers électroniques.

➢ **Parc informatique :** L'entreprise dispose d'un parc de 200 PC et 142 imprimantes répartis à travers l'ensemble des directions.

L'EPB se base sur l'utilisation des produits Microsoft sous licence. Elle utilise comme système d'exploitation pour les ordinateurs : Windows XP et Seven mais pour les serveurs : Windows Server 2003 qui ne répond plus aux nouveaux besoins. [12]

II.6 Critiques du réseau

➢ Plateforme Windows serveur dépassée :

L'entreprise dispose à ce jour de serveurs exploitant le système Windows serveur 2003 bien que Microsoft ait marqué la fin de son support total en juillet 2015, il n'y aurait donc plus aucune mise à jour de logiciel ni aucun correctif de sécurité pour cette plate-forme. Le fait de rester sous Windows Server 2003 après cette date ne sera pas sans conséquences. Les conséquences de la fin de vie de Windows Server 2003 :

✓ Toutes les applications s'exécutant sur cette plate-forme seront de plus en plus exposées aux failles de sécurité, puisque les nouvelles vulnérabilités ne seront plus corrigées.

✓ L'entretien d'un matériel obsolète peut s'avérer très onéreux : les pièces sont de plus en plus difficiles à obtenir.

✓ Une infrastructure IT branlante affectera la capacité à offrir des services de valeur fiables aux employés et aux clients.

✓ Des risques potentiels liés à la non-conformité avec les nouveaux standards et réglementations en vigueur.

➢ **Serveurs physiques archaïques :**

- ✓ Incompatibilité des nouvelles plateformes sachant que la plus part sont de l'architecture 64 bits, avec les processeurs 32 bits des Serveurs physiques.

➢ **Pare-feu Isa serveur 2004 n'est plus supporté :**

- ✓ Fin de support en juillet 2009.
- ✓ Fonctionnalités limitées et basique.
- ✓ Protection obsolète contre les nouvelles menaces.
- ✓ Control de flux entrant et sortant restreint.

➢ **Réseau plat (non segmenté) :**

Le réseau se présente sous une architecture plate et sans cloisonnement ce qui peut provoquer :

- ✓ Surcharge et congestion du réseau local
- ✓ Risques considérable d'intrusions

➢ **Adressage statique**

La configuration de réseaux de taille importante peut devenir assez longue et complexe. Cela peut devenir une source d'erreur et de complexité supplémentaire quand la taille du réseau grandit.

➢ **Sécurité**

Les utilisateurs ont des droits d'administrateur ce qui augmentent les actions et les risques potentiels liés à la sécurité des données de l'entreprise.

➢ **Messagerie**

Messagerie externe : la messagerie dépend d'internet ce qui peu causer des risques d'intrusions et de bugs ainsi que des problèmes de disponibilité en cas de coupure d'internet.

II.7 Description des besoins

Ce tableau représente les besoins de mise à niveau :

Projets d'améliorations	Observation
Mise à niveau des contrôleurs de domaines	• Migration vers une nouvelle plateforme Active directory (système et paramétrage réseaux) sur deux contrôleurs. • Création de nouveaux rôles sur le premier contrôleur. • Création de nouvelles sessions contrôlables organisées selon les organigrammes des structures de l'entreprise. • Mise en place de règles de contrôle d'accès. • Mise en place de stratégies de groupes. • Gestion des partages. • Paramétrage du deuxième contrôleur pour la tolérance aux pannes.
Mise en place d'un nouveau serveur de BDD en redondance	• Système et paramétrage des réseaux. • Allocation des espaces disques et installation de l'ensemble des BDD de l'entreprise. • Gestion des contrôles d'accès.
Mise à niveau des différents serveurs	• Serveur d'application. • Serveur de fichier. • Serveur de sauvegarde.
Mise à niveau du système d'adressage	• Revoir le système d'adressage IP du réseau

Tableau 2-1 : Analyse des besoins de l'EPB.

II.8 Améliorations réalisées

L'architecture du réseau LAN de l'entreprise après les améliorations est représentée dans la figure ci-dessous :

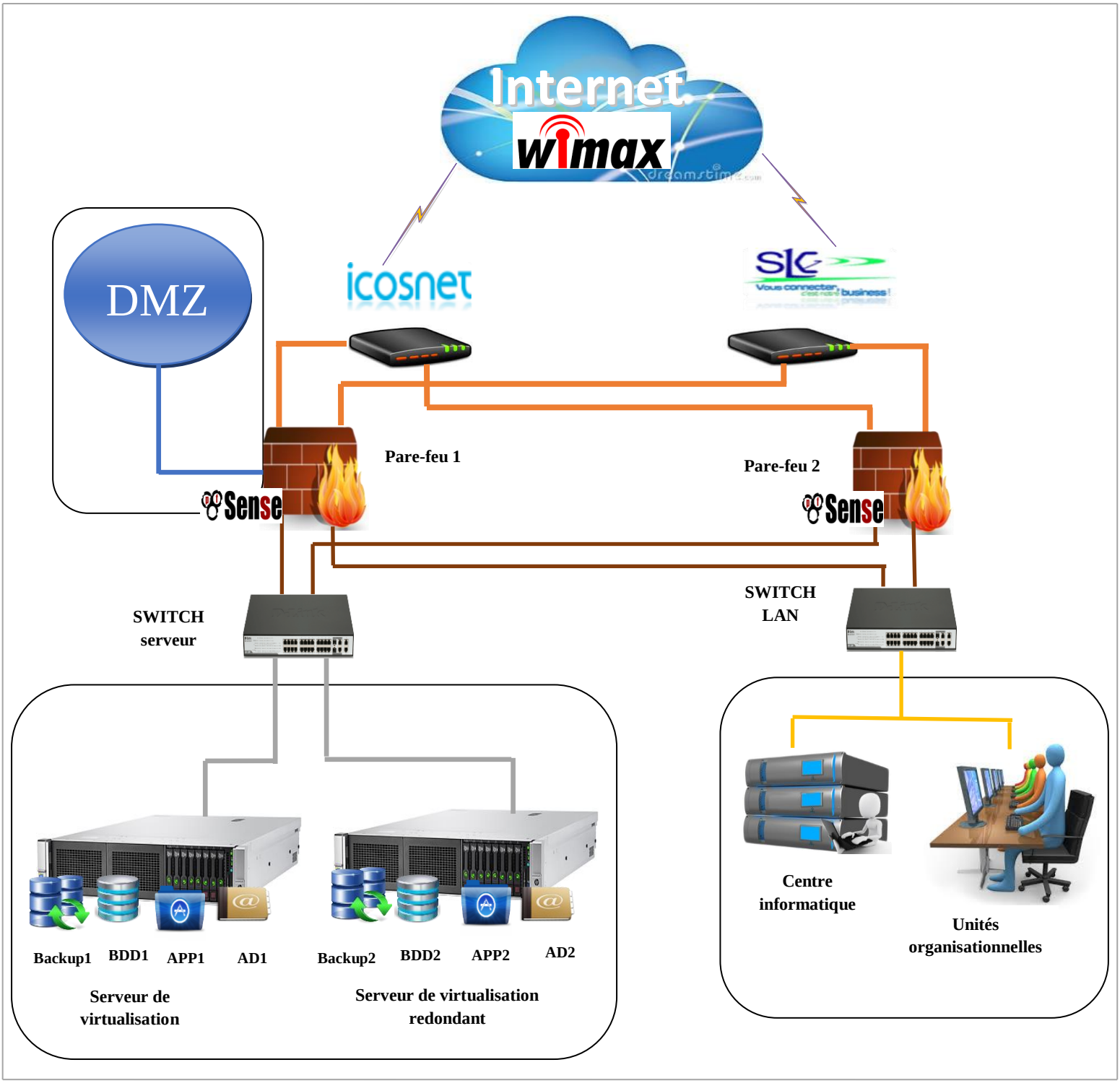


Figure II-4 : Nouvelle architecture du réseau local de L'EPB.

➢ Consolidation des serveurs

Par l'acquisition de nouveaux serveurs dernières génération (HP ProLiant G9) et en y intégrant une solution de virtualisation VmwareEsxi. Dans le but d'optimiser les ressources de la salle serveur les améliorations suivantes ont été apportées :

- ✓ Mise en place d'un serveur redondant pour chaque serveur afin d'assurer la disponibilité et la tolérance aux pannes.
- ✓ Amélioration de la politique de stockage : Configuration des RAID pour une Meilleure gestion du Stockage et garantir la disponibilité des données.
- ✓ Facilité de déploiement de nouvelles machines et optimisation de la consommation des ressources matérielles.
- ✓ Facilité de maintenance et d'accès aux données.
- ✓ Réduction de la consommation d'énergie.
- ✓ Possibilités de test, de retour en arrière lors des configurations grâce aux snapshots.

➢ Pare-feu Pfsense (Packet Filter Sense)

Est un routeur/pare-feu qui possède un nombre conséquent de fonctionnalités ce qui fait de cet outil une solution fiable pour les entreprises, ses avantages :

- ✓ Meilleure gestion de l'utilisation d'internet.
- ✓ Extension de la protection en incluant les IPS/IDS et Outils de supervision réseau.
- ✓ Surveillance du réseau en temps réel et génération de rapports journaliers.
- ✓ Fonctionnalités proxy avancées et optimisation de la bande passante.
- ✓ Garantir la disponibilité des services et la reprise d'activité même en cas de défaillance (tolérance aux pannes failover).
- ✓ Equilibrage de la charge des connexions internet.
- ✓ Contrôle total des flux entrants et sortants.
- ✓ Solution de protection complète et approuvée.

➢ Segmentation

La segmentation est principalement utilisée afin d'augmenter les performances globales du réseau et améliorer sa sécurité, elle permet aussi la réduction de la taille des domaines de diffusion et du temps de réponse, la réduction de la charge globale de la circulation (congestion) et une meilleure répartition des ressources sur le réseau.

II.9 les solutions proposées

Suite aux problèmes de sécurité liés à Windows server 2003 et afin de satisfaire les besoins cités précédemment, et de répondre aux critiques, nous avons opté pour une solution d'administration qui est une mise à niveau des serveurs vers WS 2012 R2, qui permettra à l'EPB de faire évoluer, gérer ses infrastructures plus efficacement et de répondre aux besoins des entités grâce à ses nouvelles fonctionnalités et d'offrir une plateforme performante et économique qui associe haute disponibilité et administration simplifiée des infrastructures multi-serveurs.

Nous avons proposé différentes solutions basées sur les fonctionnalités de Windows server 2012 afin de pallier les problèmes rencontrés au sein de l'entreprise :

- **Mise en œuvre des services réseaux avancées :**
  - Configuration des fonctionnalités avancées de DHCP.
  - Configuration des services RIS.
  - Mise en place d'un server DHCP redondant.
  - Configuration des paramètres avancés de DNS.

- **Mise à niveau du contrôleur de domaine Active Directory Domain Services (AD DS) :** Il permet de gérer les comptes utilisateurs ainsi que les ressources mais également la prise en charge des applications utilisant les annuaires, notre travail consistera en partie à réaliser les points suivants :
  - Configuration de relation d'approbation AD DS.
  - Surveiller et établir la continuité de service pour les services de domaine.
  - Mettre en œuvre et gérer les GPOs.
  - Gérer les paramètres utilisateurs avec les GPOs.
  - Création des profils itinérants.
  - Mise en œuvre d'un deuxième contrôleur de domaine pour la tolérance aux pannes.
  - Configuration et surveillance de la réplication AD DS.

- **Mise en œuvre de l'autorité de certification Active Directory Certificate Services (AD CS) :** AD CS permet de gérer l'utilisation des certificats de manière centralisée et sécurisée. Nous allons mettre en place quelques services proposés par AD CS tels que :
  - Mise en œuvre des infrastructures à clé publique (PKI).
  - Déploiement des autorités de certification AD CS.
  - Déploiement et gestion des modèles de certificats.
  - Mise en œuvre de la distribution de certificats et de la révocation.
  - Gestion de la récupération de certificats.

- **Mise en œuvre des services de fichiers avancés :**
  - Configuration du stockage iSCSI sous Windows Server 2012.
  - Configuration de BranchCache.
  - Gestion et contrôle du partage.
  - Ajout des clichés instantanés.

- **Mise en œuvre de la reprise en cas de panne :**
  - Mise en œuvre d'une solution de sauvegarde (Backup).

Conclusion

Ce chapitre nous a permis de cerner le fonctionnement du service informatique de l'EPB, il est indispensable de disposer d'information précise sur l'infrastructure réseau et les problèmes qui ont une incidence sur le fonctionnement de ce dernier.

En vue de palier aux problèmes rencontrés lors de cette étude, nous avons proposé quelques solutions liées au réseau de l'EPB que nous allons développer dans le chapitre qui suit.

Chapitre III :

Réalisation

Introduction

Nous consacrons ce chapitre à la partie mise en œuvre et configuration, pour commencer nous allons présenter les différents outils que nous avons utilisés dans la réalisation de notre travail, puis décrire les différentes étapes suivies lors de l'installation et configuration des services proposées par Windows serveur 2012 R2.

III.1 La famille d'Active Directory

Microsoft a regroupé les fonctionnalités d'annuaire et a crée une famille de services connexes qui comprend notamment.

- Active directory Certificats Services (AD CS)

AD CS fournit les fonctions nécessaires pour emmètre et révoquer les certificats numériques des utilisateurs, des ordinateurs clients et des serveurs. Ces services font appel aux autorités de certification (CA, Certificat Authority) chargées de confirmer l'identité des utilisateurs et des ordinateurs puis d'emmètre des certificats pour confirmer ces identités. Les domaines disposent d'une autorité de certification racine d'entreprise, c'est-à-dire des serveurs de certification situés à la base des hiérarchies de certification pour les domaines et les serveurs de certification les plus fiables de l'entreprise.

- Active directory Domain Server (AD DS)

Les services AD DS procurent les services d'annuaire essentiels à l'établissement d'un domaine, y compris le magasin de données qui stocke les informations sur les objets du réseau, et les met à disposition des utilisateurs. Les services AD DS font appel aux contrôleurs de domaine pour gérer l'accès aux ressources du réseau. Une fois que les utilisateurs s'authentifient en se connectant à un domaine, leurs informations d'identification stockées peuvent être exploitées pour accéder aux ressources du réseau

- Active directory Federation Services (AD FS)

Les services AD FS font appel à des agents Web pour donner aux utilisateurs un accès aux applications Web et aux proxys, hébergés en interne, qui gèrent l'accès client. Une fois les services AD FS configurés, les utilisateurs emploient leur identité numérique pour s'authentifier sur le Web et accéder aux applications Web hébergées en interne à l'aide d'un navigateur Web. [6]

- Active directory Lightweight Directory Services (AD LDS)

Les services AD LDS fournissent un magasin de données pour les applications fonctionnant avec l'annuaire qui n'ont pas besoin d'être déployées sur des contrôleurs de domaines. Ce service ne fonctionne pas comme un service de système d'exploitation et il peut être utilisé autant dans des environnements de domaine que de groupe de travail. Chaque application qui s'exécute sur un serveur dispose de son propre magasin de données implémenté via les services AD LDS. [13]

- Active Directory Rights Mangement Services (AD RMS)

Les services AD RMS procurent une couche destinée à protéger les informations d'une organisation et qui peu s'étendre hors de l'entreprise, protégeant ainsi les messages électroniques, les documents et les pages Web de l'intranet, contre tout accès non autorisé. Les services AD RMS exploitent d'une part un service de certification qui émet des certificats de comptes de droits qui identifient les utilisateurs, groupes et services approuvés, d'autre part un service de licences qui donne un accès aux informations protégées aux utilisateurs, aux groupes et aux services autorisés et enfin un service de journalisation qui surveille et dépanne les services AD RMS. [6]

III.2 Structure d'Active Directory

- **Domaine :** Un domaine regroupe des ordinateurs, des périphériques, des utilisateurs. C'est une sorte de zone sécurisée, sur laquelle on ne peut pénétrer que quand on a été authentifié par le Contrôleur de Domaine. L'administrateur est le seul à pouvoir accorder des permissions sur les objets de son domaine. Sauf autorisation accordée explicitement, il ne gère rien en dehors de son domaine.

Un domaine étant une organisation logique d'objets, il peut aisément s'étendre sur plusieurs emplacements physiques. [14]

- **Arbre ou arborescence :** Est un ensemble de domaines appartenant à une même hiérarchie de nom DNS ou le domaine racine est le premier domaine créé, non renommable et non supprimable et l'ajout d'un nouveau domaine se fait en créant un domaine feuille à un domaine existant de l'arborescence. Le nom complet (DNS) du nouveau domaine est obtenu en concaténant son nom au nom du domaine parent.

- **Notion de foret et d'arborescence de domaines :** Chaque domaine Active Directory a un nom de domaine DNS, dans notre cas ça sera EPB.AD. On appelle foret un ou plusieurs domaines partageant les mêmes données d'annuaire. Les noms de domaine de cette forêt peuvent être non contigus ou contigus dans la hiérarchie d'attribution des noms DN. [6]

  Lorsque les domaines ont une structure de noms contiguë, on dit qu'ils sont dans la même arborescence de domaine. La figure ci-dessous illustre l'arborescence de domaine de l'EPB. La racine de domaine EPB.AD a trois domaines enfants : *DGAO.EPB.AD*, *DGAF.EPB.AD* et *DG.EPB.AD.* Ces domaines ont, à leur tour, des sous-domaines.

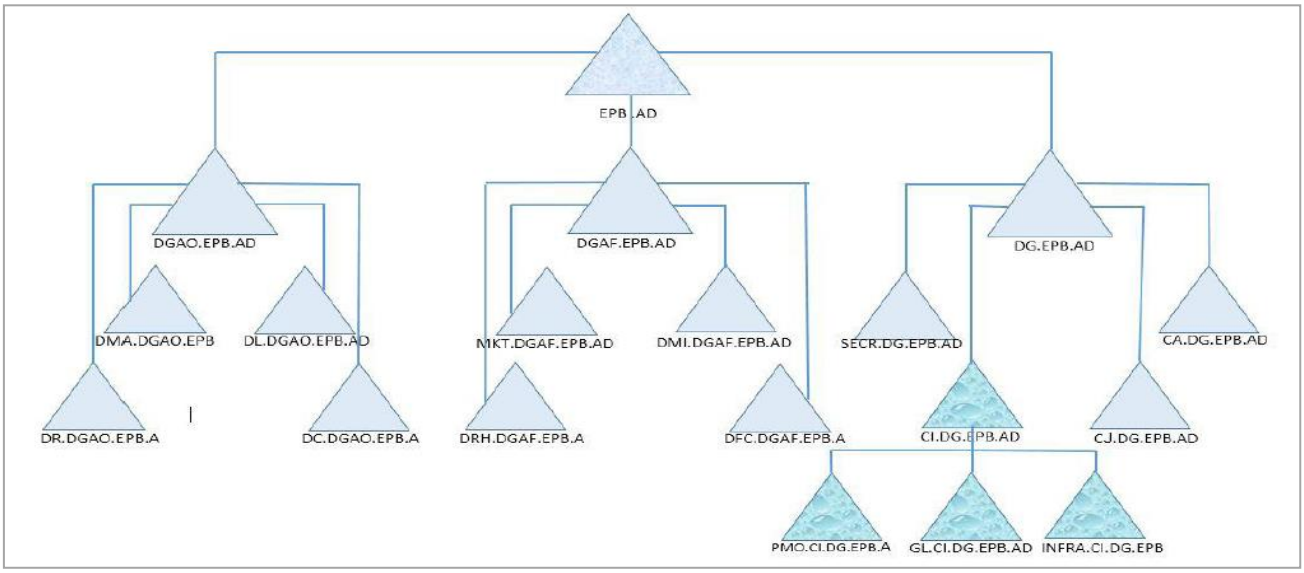


Figure III-1 : Arboresence de l'EPB.

- **Unité d'organisation (UO) :** Est un « container » pouvant contenir des utilisateurs, des ordinateurs, des groupes, ... et d'autres unités d'organisation. Une unité d'organisation doit être utilisée quand on souhaite déléguer des pouvoirs ou appliquer une stratégie particulière à un sous-ensemble des objets du domaine.

  Il est possible de donner tout ou une partie des droits d'administration sur les objets d'une UO à certains utilisateurs. En créant une unité d'organisation regroupant les ordinateurs du domaine, on peut déléguer leur gestion à un utilisateur qui n'aura pas de droit sur les comptes utilisateurs. [6]

III.3 Avantage d'active Directory

- La base de données d'AD est distribuée ce qui lui améliore la tolérance aux pannes.
- Son mode de fonctionnement multi-maître permet de conserver une gestion centralisée.
- Offre une administration de toutes les ressources du réseau d'un point unique. Un administrateur peut se connecter sur n'importe quel ordinateur pour gérer les ressources de tout ordinateur du réseau.
- Le nombre de types d'objets disponibles dans un Active Directory n'est pas limité. [9]

III.4 Réalisation

III.4.1 Table d'adressage

Afin de mener à bien notre projet, nous allons commencer par présenter la table d'adressage adéquate au réseau de l'EPB. [12]

	Adresse	**Masque**	**Passerelle**
DC01	10.0.0.198	255.255.255.0	172.16.103.252
DNS 1	10.0.0.198		
DC02	10.0.0.197	255.255.255.0	172.16.103.252
DNS 2	10.0.0.197		
Parefeu 1	172.16.103.254		
Parefeu 2	172.16.103.253		
Lan	172.16.100.0	255.255.252.0	

Tableau III-1 : Tableau d'adressage.

III.4.2 Mise en œuvre des services réseaux et du contrôleur de domaine AD DS

Etape 1 : Installation de Windows server 2012 R2

Windows Server 2012 R2 est la dernière version de Windows orientée serveur. L'installation de ce système d'exploitation est très classique et ressemble à celle de Windows 8. Les différents écrans sont aussi très proches de Windows Server 2008/R2.

Le premier démarrage se fait sur l'écran Gestionnaire de serveur, son design est très différent des anciennes versions de Windows Server mais les fonctions sont conservées, voire améliorées. Celui-ci nous donne la possibilité d'ajouter des rôles, surveiller l'état de notre serveur ou encore gérer ses fonctionnalités.

Figure III-2 : Gestionnaire de serveur.

Pour commencer, il faudra configurer notre serveur local, pour cela nous cliquons sur Configurer ce serveur local, cette étape nous permet de définir les propriétés du serveur :

Nom de l'ordinateur : SrDC01 pour le premier serveur qui fera office de contrôleur de domaine.

Ethernet0 : 10.0.0.198 que nous avons attribué à notre serveur.

Figure III-3 : Configuration du serveur Local.

Etape 2 : Création du contrôleur de domaine et DNS

Active Directory utilise le système DNS (Domain Name System). DNS est un service internet standard qui organise les groupes d'ordinateurs en domaines. Les domaines DNS sont organisés selon une structure hiérarchique. Les différents niveaux de la hiérarchie identifient les ordinateurs, les domaines organisationnels et les domaines de premier niveau. DNS est également utilisé pour faire correspondre les noms d'hôtes à des adresses IP numériques. Par le biais de DNS, une hiérarchie de domaine Active Directory peut également être définie à l'échelle de l'internet ou bien être séparés de l'internet et demeurer privée.

Avant de promouvoir le serveur en tant que contrôleur de domaine dans notre domaine, il faut installer le rôle « **Service de domaine Active Directory** ».

- Dans le Gestionnaire de serveur, nous avons sélectionné « **Ajouter des rôles et des fonctionnalités** ».
- Au niveau des rôles, choisir « **Service AD DS** » qui correspond au service de domaine Active Directory en cochant la case. Une fenêtre va apparaître pour indiquer que d'autres éléments requis par AD DS doivent être installés, cliquer sur « **Ajouter des fonctionnalités** ».

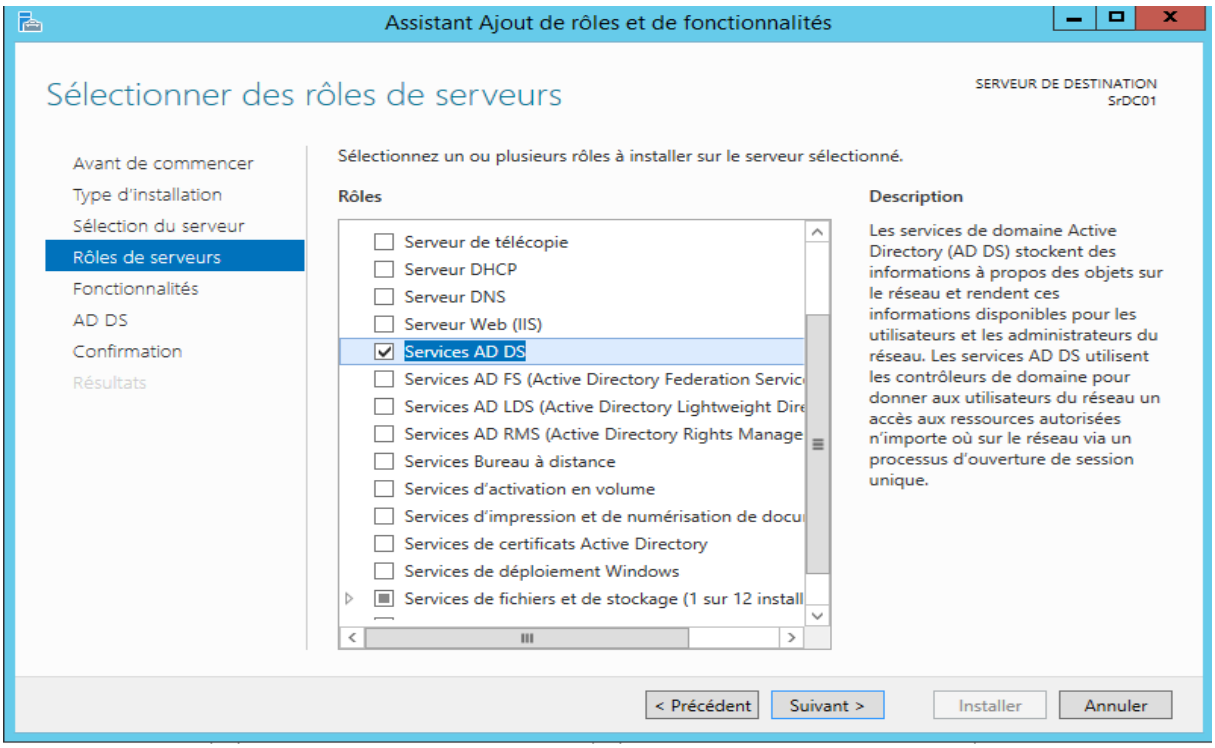


Figure III-4 : Ajout du service AD DS.

Une fois les fonctionnalités d'AD DS installées, le serveur va redémarrer automatiquement. Nous devons promouvoir ce serveur en tant que contrôleur de domaine, sinon le domaine ne sera pas créé.

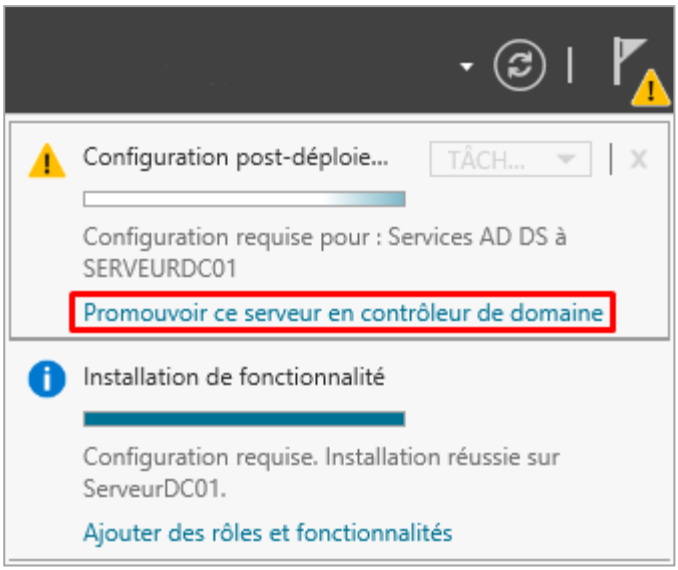


Figure III-5 : Promotion du serveur en contrôleur de domaine.

Vu que nous souhaitons créer un nouveau domaine, nous devons déployer une nouvelle forêt en cochant sur « **Ajouter une nouvelle forêt** » et en spécifiant le nom de notre domaine appelé « **EPB.AD** ».

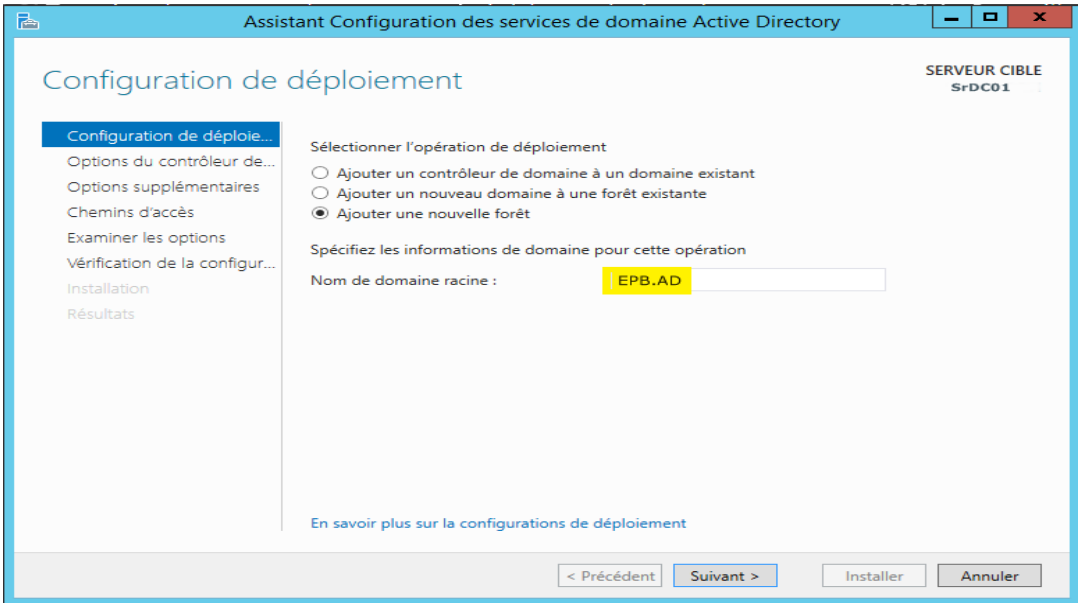


Figure III-6 : Création du domaine EPB.AD.

L'étape suivante consiste à choisir le niveau fonctionnel de la forêt ou du domaine pour cela nous avons choisi l'option « Windows serveur 2008 R2 » ce choix dépend du parc informatique correspondant au réseau de l'entreprise majoritairement sous Windows 7.

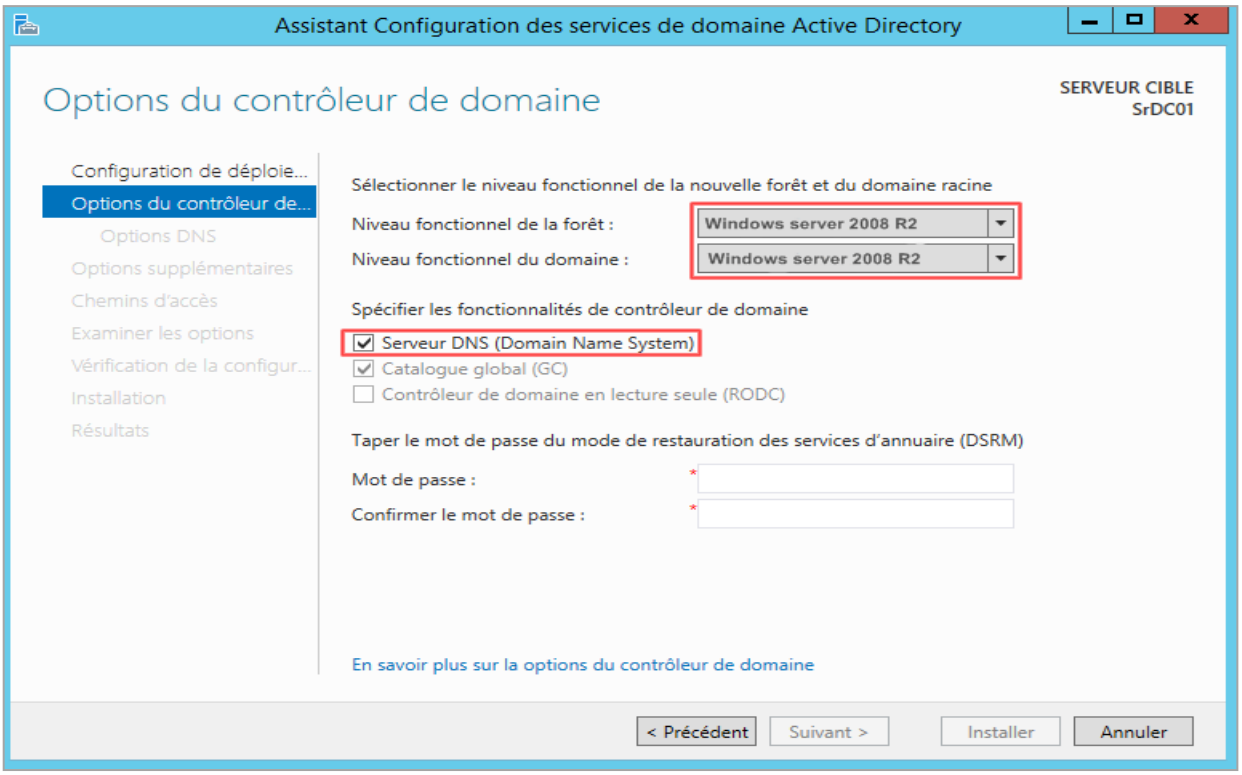


Figure III-7 : Sélection du niveau fonctionnel de la forêt et du domaine.

Lorsque nous installons les services de domaine Active Directory (AD DS), celui-ci nous donne la possibilité d'installer et de configurer automatiquement un serveur DNS. La zone DNS résultante est intégrée à AD DS contrôlé par le serveur SrDC01.

Après configuration, le serveur redémarre automatiquement. A présent, les outils de gestion d'active Directory sont présents dans le menu Outils, notre domaine est créé et l'ouverture d'une session s'effectue avec le compte d'administrateur du domaine « EPB\Administrateur ».

Figure III-8 : Ouverture de la session Administrateur.

Etape 3 : Installation et configuration du service DHCP

Pour que les PC des utilisateurs et les serveurs communiquent nous devons leur donner une adresse IP, un masque de sous réseau, une passerelle et un serveur DNS qui est obligatoirement un DNS de Active Directory.

Le faire manuellement réclamera du travail : gestion d'un inventaire, paramétrage manuel et cela engendrera des erreurs (conflits d'adresse, mauvaise adresse, etc).

L'idéal serait d'utiliser un serveur DHCP afin de palier aux problèmes cité ci-dessus, pour cela nous avons procédé comme suit :

- Dans l'assistant de gestion des rôles, Ajouter le rôle DHCP.

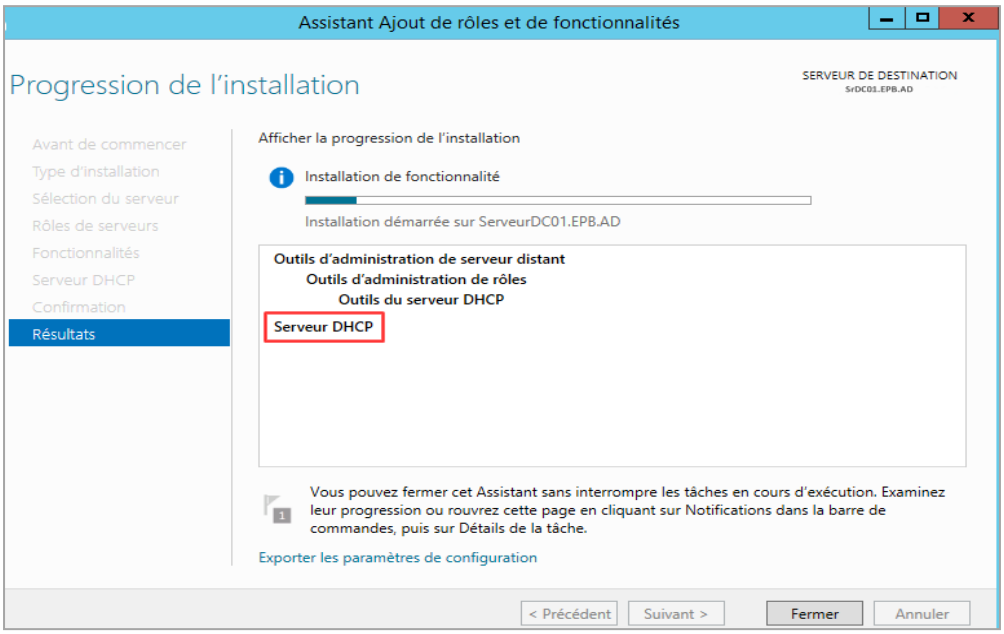


Figure III-9 : Installation du serveur DHCP.

Après quelques minutes le rôle est installé, l'écran final nous invite à commencer la configuration de DHCP

- Création de nos étendues DHCP à l'aide de la console d'administration DHCP qui a été lancée depuis le menu Outils du gestionnaire de serveur.

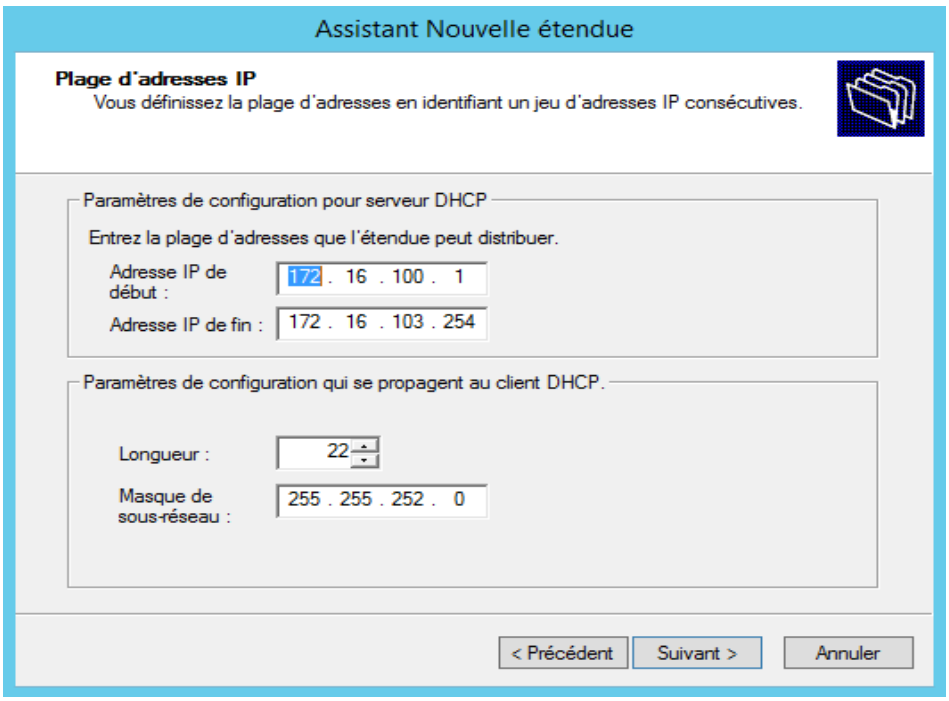


Figure III-10 : Création des étendues DHCP.

Lors de la création de Notre étendu, nous avons défini les plages d'adresses que l'étendue peut distribuer aux Hôtes clients

@IP début : 172.16.100.1

@IP fin : 172.16.103.254

Masque : 255.255.252.0, sa longueur : 22.

- Ajouter d'éventuelles exclusions afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses (imprimante, webcam IP, PC en adresse fixe, serveur…).

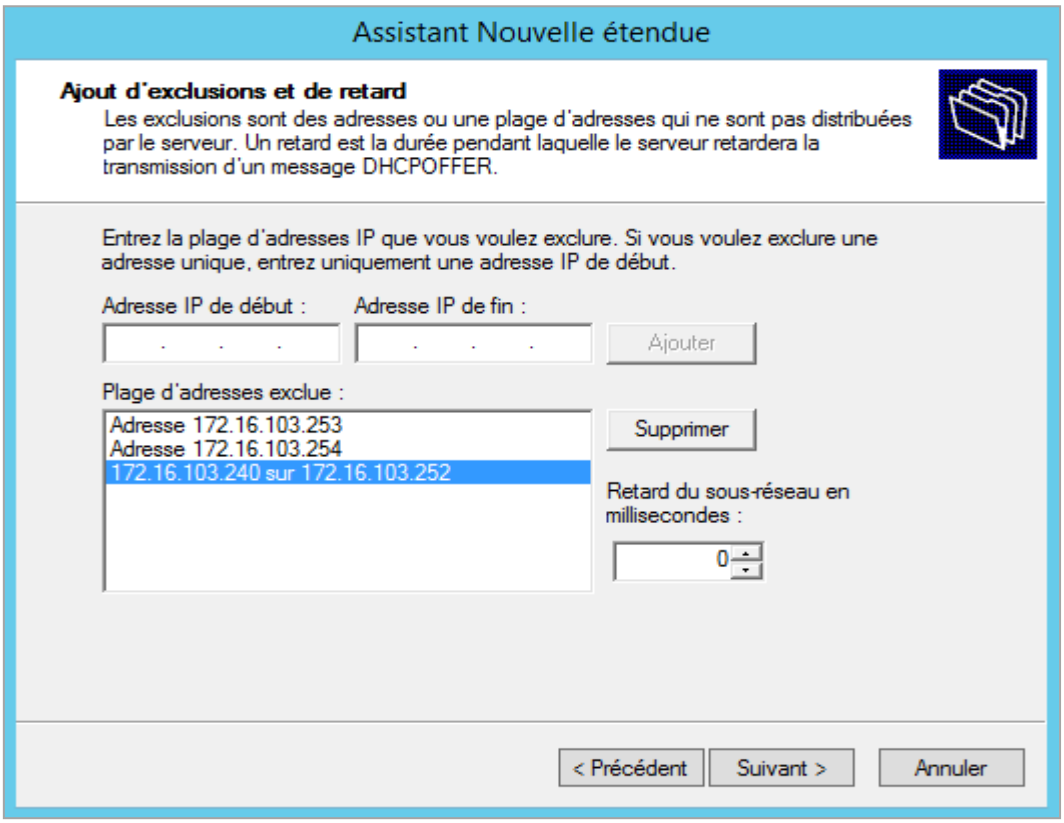


Figure III-11 : Ajout d'exclusion DHCP.

Concernant le réseau de l'EPB :

L'@ 172.16.103.253 : Adresse IP fixe pour le Firewall 1.

L'@ 172.16.103.254 : Adresse IP fixe pour le Firewall 2.

De 172.16.103.240 à 172.16.103.252 : Pool d'adresse réservé aux serveurs.

Etape 4 : Promotion du deuxième contrôleur de domaine

L'installation d'un deuxième contrôleur de domaine s'inscrit dans une politique dite de « haute disponibilité » en cas de panne de notre Serveur contrôleur de domaine SrDC01 le serveur SrDC02 prends le relai et cela sans que les utilisateurs se rendent compte de se basculement.

L'installation du rôle AD DS se fait de la même manière que SrDC01 à la différence que lors de la promotion de SrDC02, nous choisissons l'option « ajouter un contrôleur de domaine a un domaine existant ».

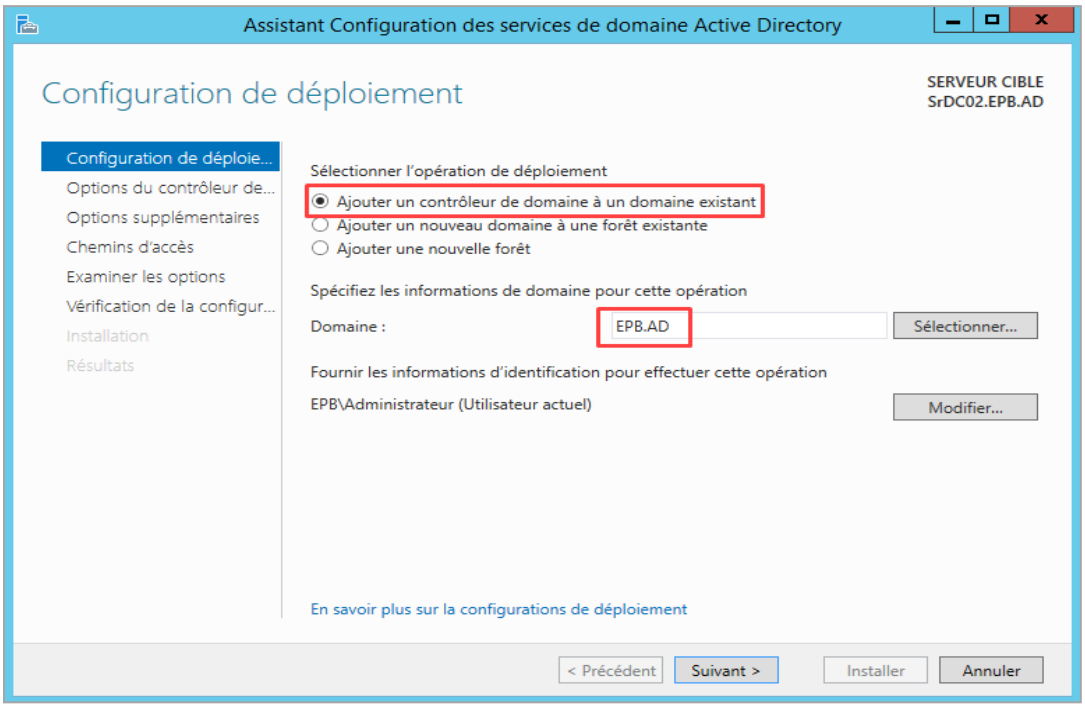


Figure III-12 : Ajout d'un contrôleur de domaine à un domaine existant.

Dans les « options supplémentaires » nous devons sélectionner le premier contrôleur de domaine *SrDC01* afin d'indiquer au second contrôleur *SrDC02*, d'où il devra répliquer les services d'annuaire d'Active Directory.

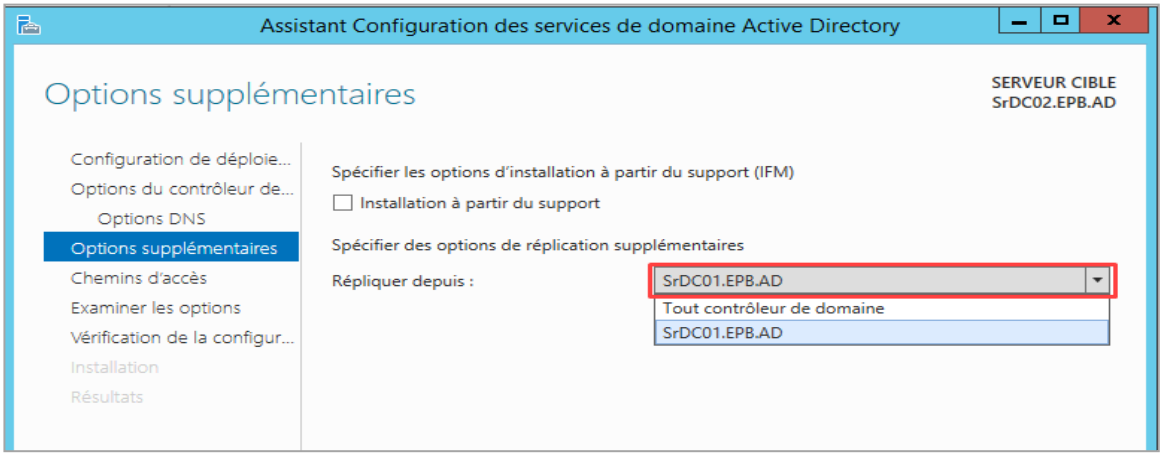


Figure III-13 : Spécification du contrôleur de domaine à répliquer.

Une fois le serveur redémarré, se positionner sur la fenêtre « site et services Active Directory » afin de vérifier si les deux serveurs sont présents. Dès lors, nous pouvons sélectionner les paramètres des deux contrôleurs, puis choisir « Répliquer » maintenant.

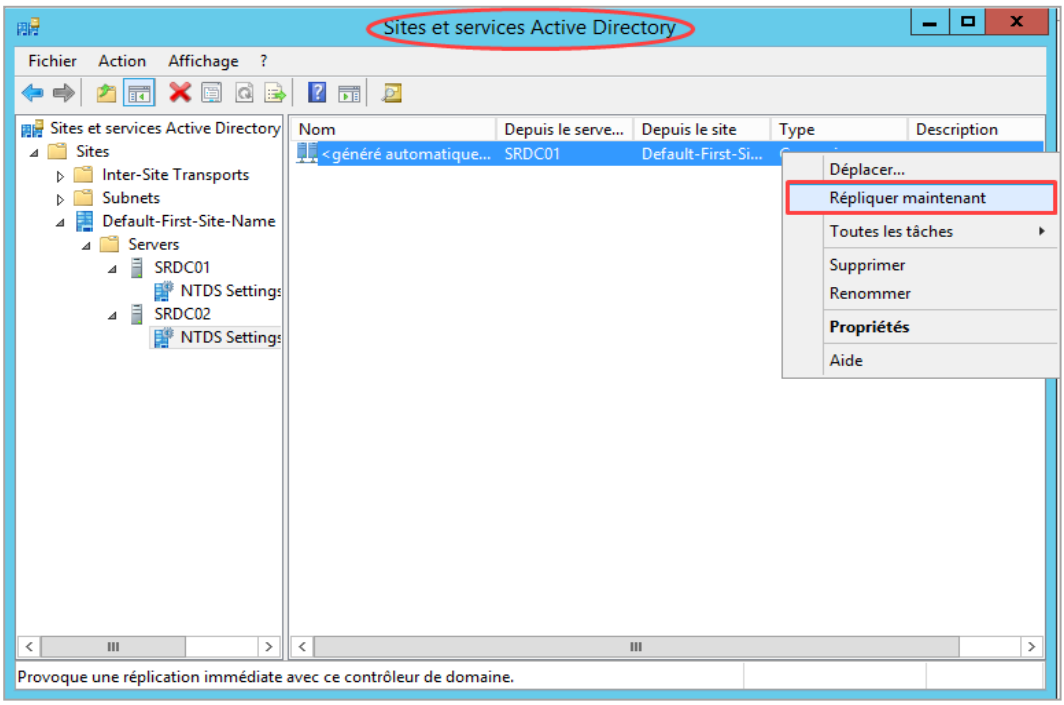


Figure III-14 : Réplication du serveur SrDC01 sur SrDC02.

Etape5 : Répartition des rôles FSMO entre les deux contrôleurs de domaines

Le rôle FSMO (Flexible Single Master Opérations) a pour objectif de répartir l'ensemble des maitres d'opération qui sont tous hébergés sur SrDC01, pour cela nous allons déplacer une partie des rôles du serveur SrDC01 à destination de SrDC02. Les rôles FSMO sont au nombre de cinq, ces cinq rôles ne sont pas forcément à mettre sur la même machine, il est intéressant pour des raisons de performances ou tout simplement de distribution de charge de pouvoir répartir ces rôles.

Figure III-15 : Affichage des rôles FSMO.

Sur le serveur qui doit récupérer les rôles (SrDC02) nous allons exécuter sur l'Invité de commandes la commande suivante : « ntdsutil »

Le prompt devient « **ntdsutil** », nous saisissons la commandes « **rôles** » pour passer en mode « **fsmo maintenance** ». Ce mode propose notamment des commandes permettant de faire le transfert de chacun des rôles. La commande « **connections** » permet d'ouvrir un outil qui permet d'établir une connexion avec un contrôleur de domaine. Puis nous saisissons « **connect to server** » suivit du nom du serveur pour se connecter au DC.

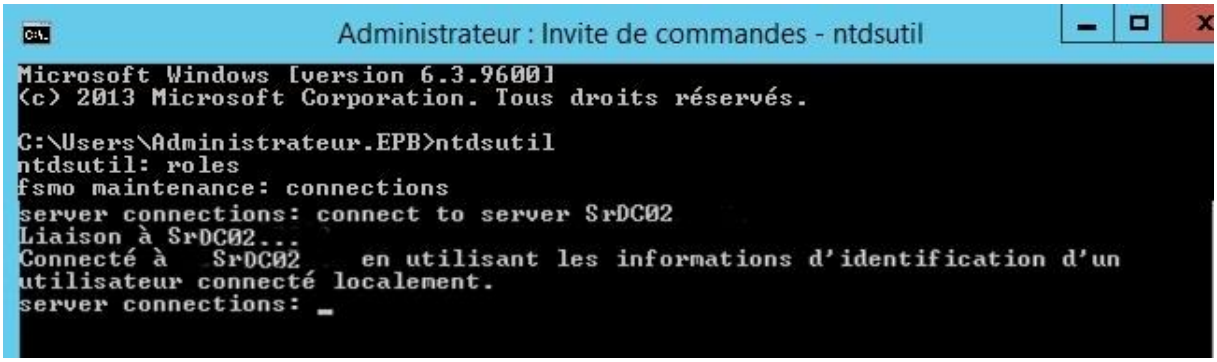


Figure III-16 : Connexion au serveur SrDC02.

Pour commencer, nous allons prendre le rôle « Maître d'attribution de noms », appelé aussi « **naming master** ». Pour cela nous exécutons la commande : **seize naming master,** une confirmation nous sera demandée, un clique sur « **Oui** » pour confirmer la prise de rôle.

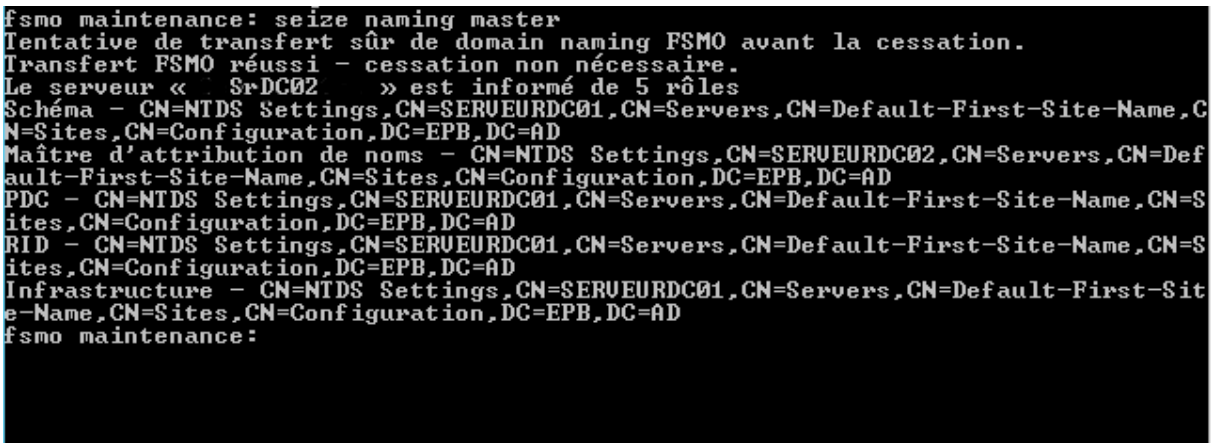


Figure III-17 : Configuration du rôle « maître d'attribution de nom ».

Une fois cette étape achevée, un récapitulatif concernant les 5 rôles est affiché et permet de vérifier si SrDC02 est bien le nouveau naming master.

Passons au Maître RID, appelé aussi RID master**.** Saisir la commande suivante **: seize RID master.** Comme pour le rôle précédent, la fenêtre de confirmation apparaît. Nous n'avons qu'à cliquer sur oui.

Pour finir, nous vérifions tout de même que les rôles soient bien pris par le contrôleur SrDC02. Pour cela, toujours dans l'**Invite de commandes** et à l'aide de la commande **netdom query fsmo**.

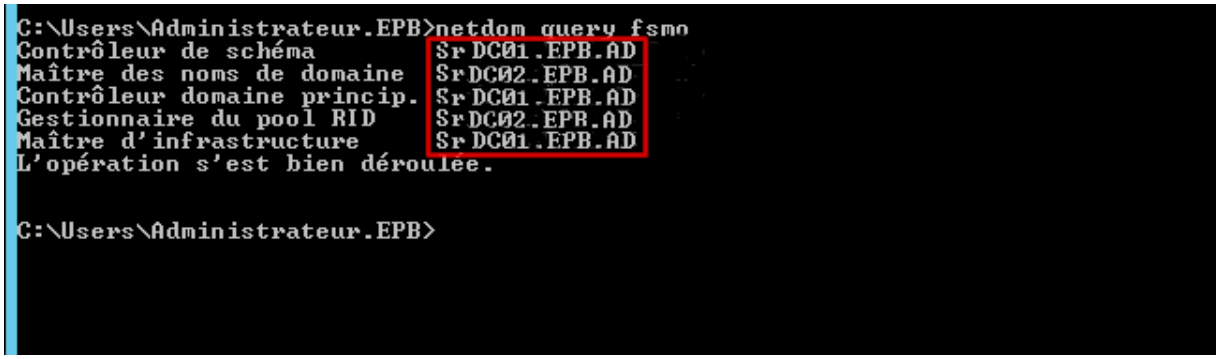


Figure III-18 : Résumé de la configuration FSMO.

On peut voir « **SrDC02** » et « **SrDC01** » se partageant les rôles FSMO.

Etape 6 : Configuration du DHCP Failover.

La fonctionnalité de failover DHCP est nouvelle depuis Windows Server 2012, elle permet d'assurer la disponibilité du service DHCP et améliorer la fiabilité du réseau.

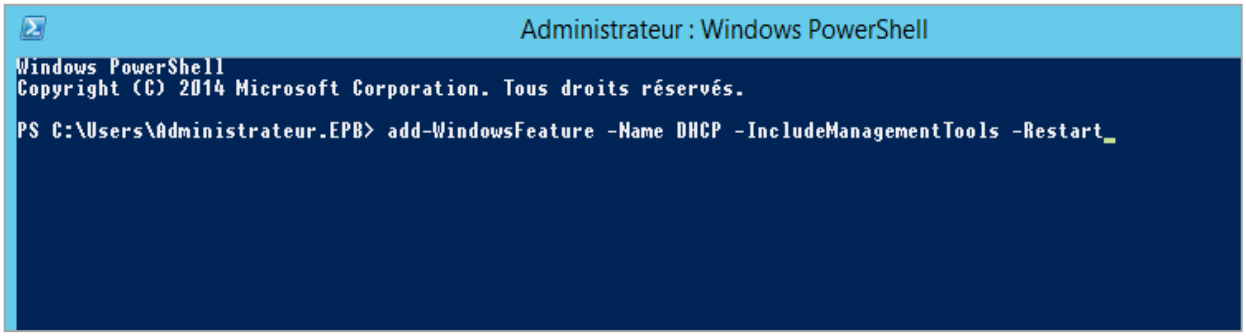
Le basculement de serveurs DHCP inclus deux modes de fonctionnement :

– **Actif/passif :** Un serveur actif, un second serveur de secours

– **Actif/actif :** Les deux serveurs sont actifs et une répartition de charge est effectuée. Les serveurs se répartissent les clients et synchronisent les informations liées aux baux entre eux.

La première étape consiste à créer un serveur DHCP sur notre serveur SrDC02, la procédure est la suivante :

- Installation du service DHCP surSrDC02.



III-19 : Installation du service DHCP sur SrDC02 depuis le PowerShell.

Le résultat s'affichera sur le gestionnaire de serveur :

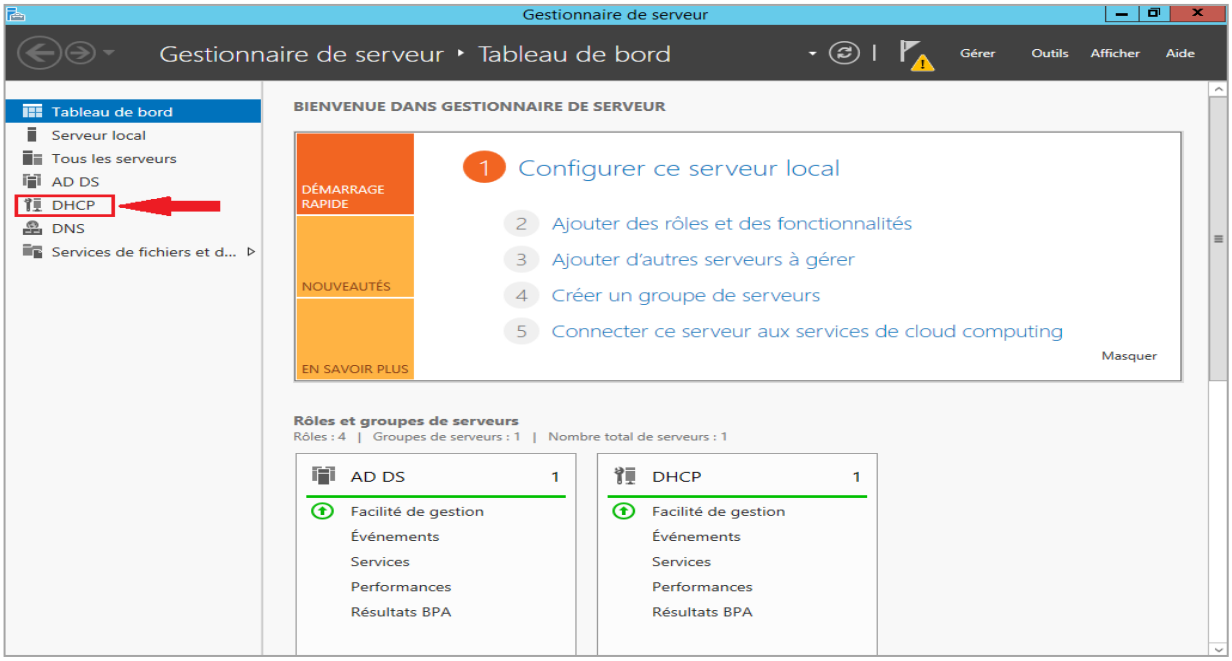


Figure III-20 : L'ajout du service DHCP sur le gestionnaire de serveur.

Afin de configurer un basculement, sur la console d'administration DHCP qui se trouve sous « Outils d'administration ».

- Sur le serveur DHCP qui contient l'étendue à répliquer, sélectionné « Configurer un basculement ».

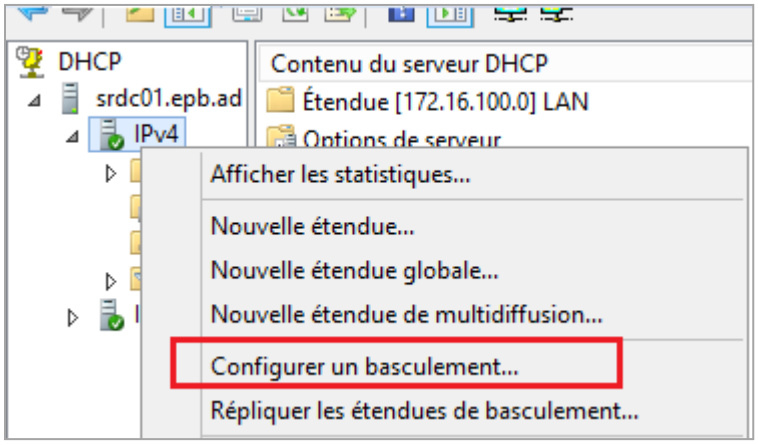


Figure III-21 : Configuration d'un basculement.

- Après avoir sélectionné un serveur partenaire qui est le serveur SrDC02, nous devons configurer les paramètres de la relation de basculement.

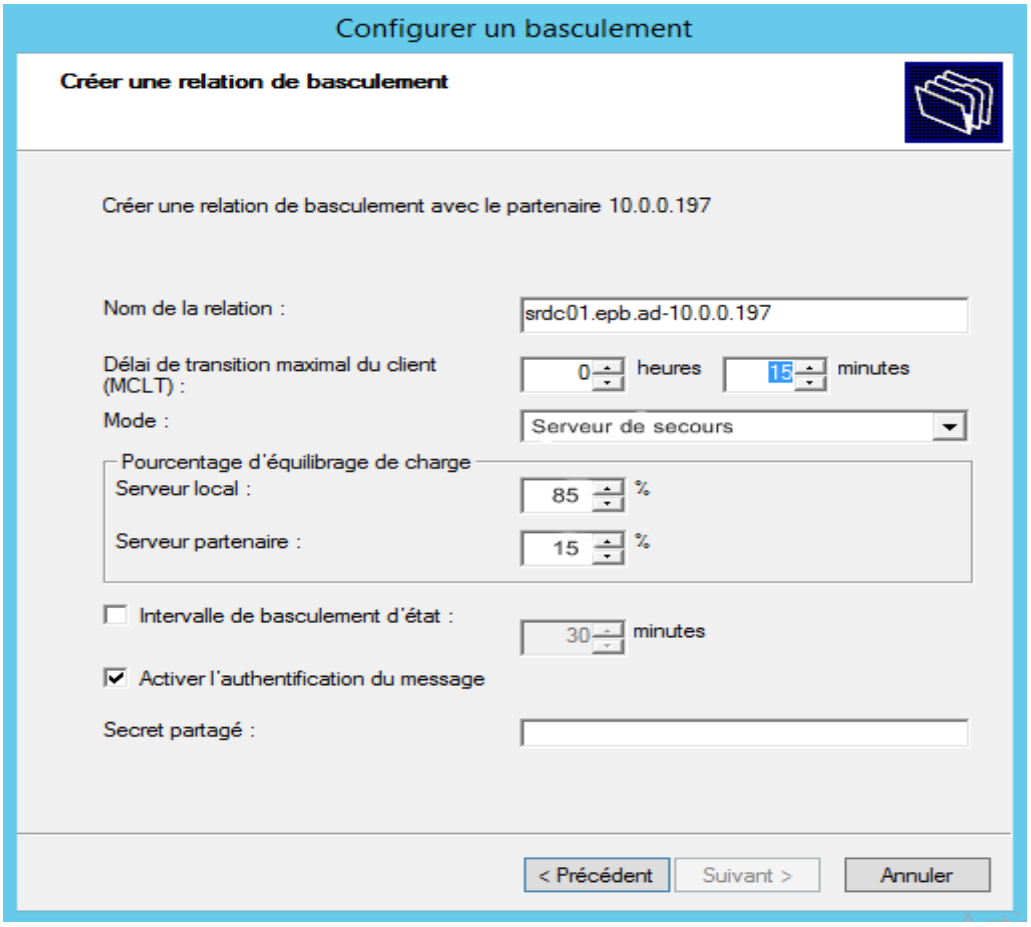


Figure III-22 : configuration des paramètres de la relation de basculement.

Le champ « **Nom de la relation** » : reprend tout simplement le nom des deux serveurs qui entrent dans la relation de Failover.

Le champ « **Délai de transition maximal du client** » ou « **MCLT** » : correspond au temps pendant lequel on autorise la prolongation du bail du client. Dans notre cas, nous l'avons fixé à 15 minutes.

Le choix du mode est essentiel puisqu'il définit le mode de fonctionnement des serveurs. Si l'on prend « **Équilibrage de charge** » nous entrons dans le mode actif/actif. Si l'on opte pour le second choix qui est « **Serveur de secours** » on passe en mode actif/passif, les données du serveur primaire sont répliquées sur le secondaire afin qu'il soit en mesure de prendre le relais en cas de panne du primaire. Nous avons choisi le mode « **Serveur de secours** ».

L'option « **Intervalle de basculement d'état** » : définit le temps d'attente du serveur de secours après avoir perdu la communication avec le serveur primaire afin de passer à l'état actif. En mode équilibrage de charge cette option devient inutile car le serveur de secours est déjà en activité.

L'authentification du message sera utilisée pour chiffrer les échanges entre les deux serveurs DHCP concernés. Ainsi, les échanges de configuration entre ces deux derniers ne transiteront pas en clairs sur le réseau.

- Après avoir validé cette étape, la configuration du basculement est désormais terminée.

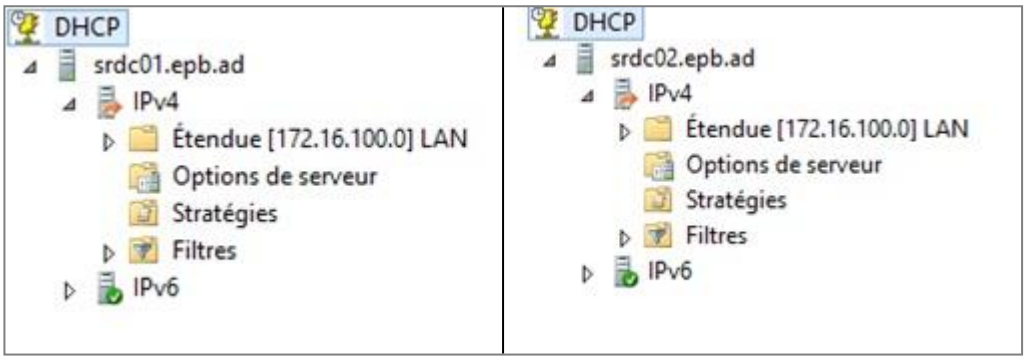


Figure III-23 : Résultat du basculement.

Etape7 : Mise en œuvre des services d'installation à distance RIS.

Le service RIS permet d'installer automatiquement des postes clients vierges (sans SE) à distance, ainsi les intégrées au domaine parent et leur fournir les paramétrages IP.

Le service RIS contient deux serveurs, un serveur de déploiement et l'autre de transport et il s'installe à partir de l'assistant d'ajout de rôle en cliquant sur le service de déploiement Windows.

Une fois l'installation effectuée, nous nous dirigeons vers les « services de déploiement Windows » dans le menu outil d'administration, sur les **services de déploiement Windows** nous faisons un clique droit puis **Configurer le serveur.**

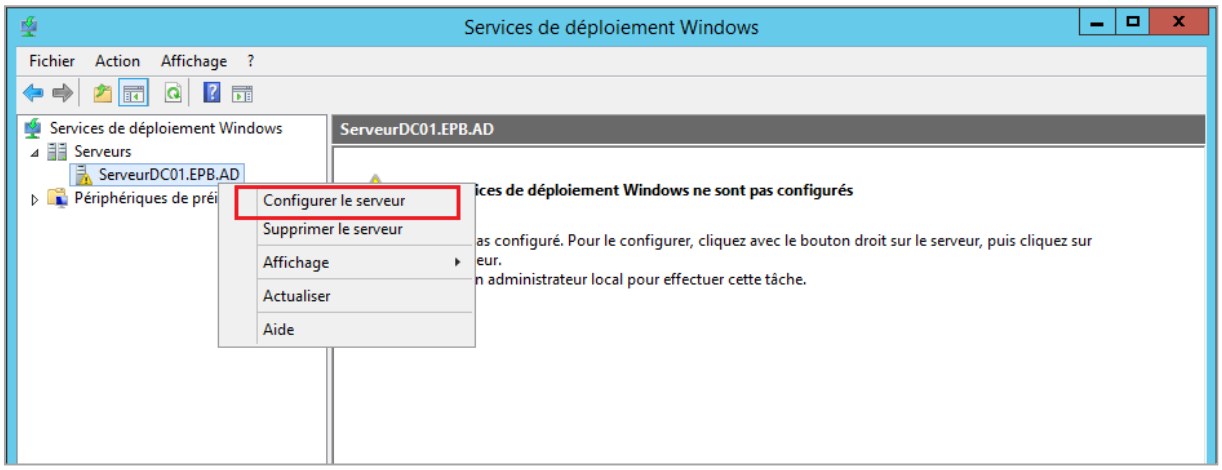


Figure III-24 : Configuration du serveur pour le déploiement des services Windows.

Sur la fenêtre « Installation des options », sélectionné « Intégré avec Active Directory ».

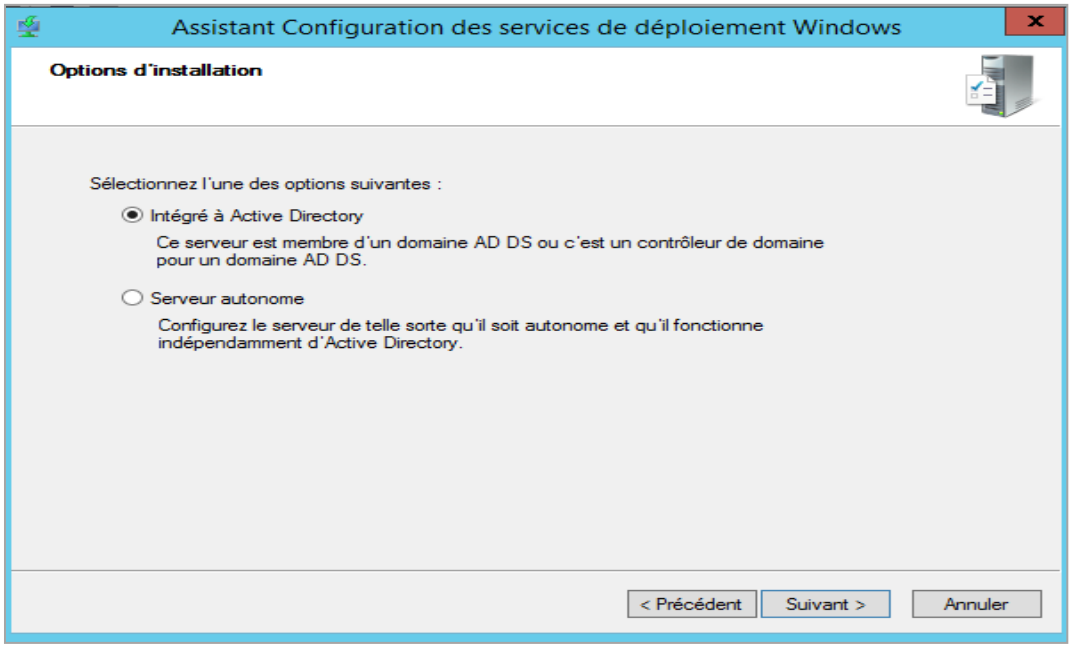


Figure III-25 : Intégration du RIS au domaine.

L'étape qui suit consiste à sélectionner l'emplacement où on souhaite conserver les images Windows et les fichiers de configuration. Ainsi nous avons terminé la configuration des services de déploiement Windows.

Etape8 : Organisation des clients AD en unités organisationnelles

Nous allons commencer à peupler notre Active Directory. Pour ce faire nous devons lancer la console Utilisateurs et ordinateurs Active Directory. On peut la lancer depuis le Gestionnaire de serveur puis sous la rubrique AD DS.

Nous allons créer une unité organisationnelle afin d'y mettre l'ensemble des utilisateurs et groupes pour cela on se place dans l'arbre à la hauteur de notre domaine EPB.AD et sur le menu, nous choisissons l'option « Unité d'organisation ».

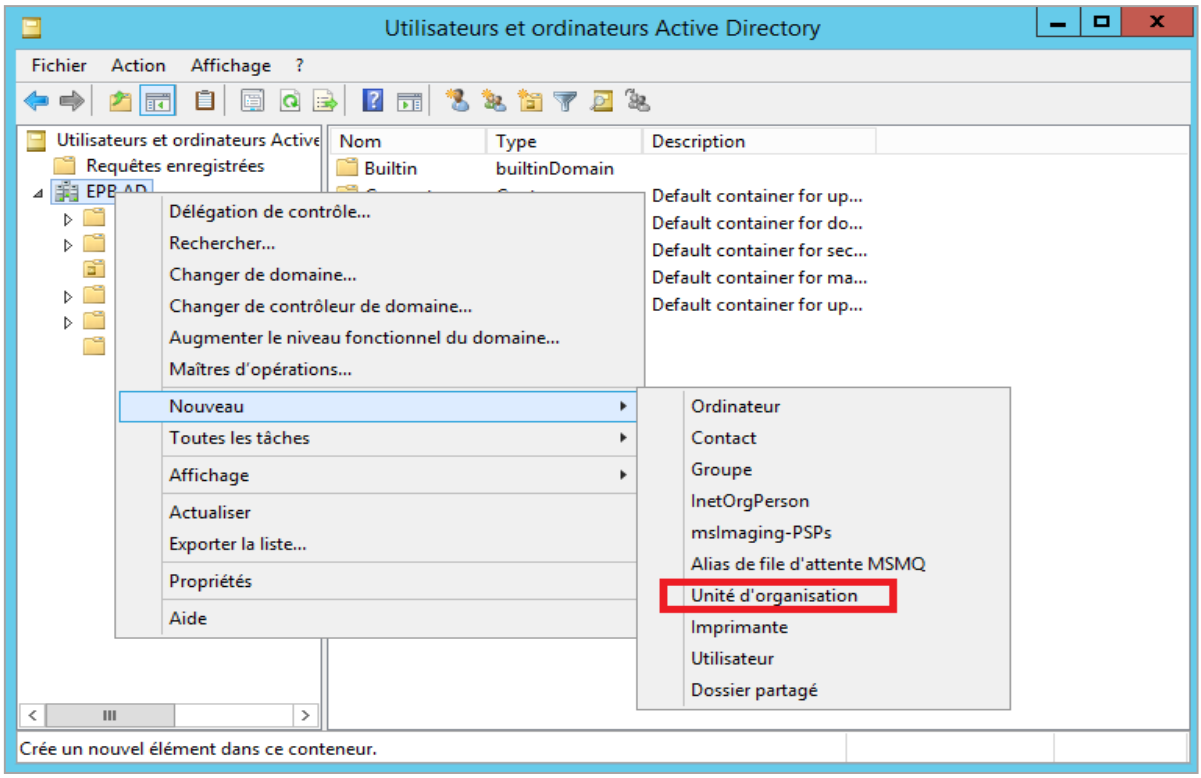


Figure III-26 : Création d'une unité d'organisation.

Après avoir créé les unités organisationnelles relatives à notre entreprise, nous pouvons créer les premiers utilisateurs et commencer à peupler nos unités. Nous répétons la même procédure pour tous les nouveaux utilisateurs.

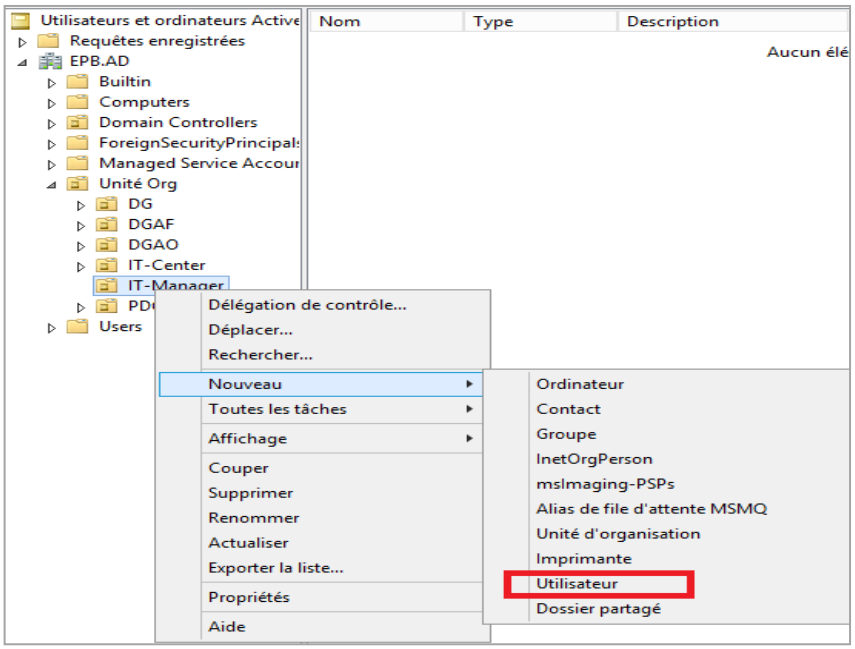


Figure III-27 : Ajout d'utilisateurs.

Pour chaque UO, nous avons créé des comptes utilisateurs avec un identifiant unique de la forme P.NOM@EPB.AD.

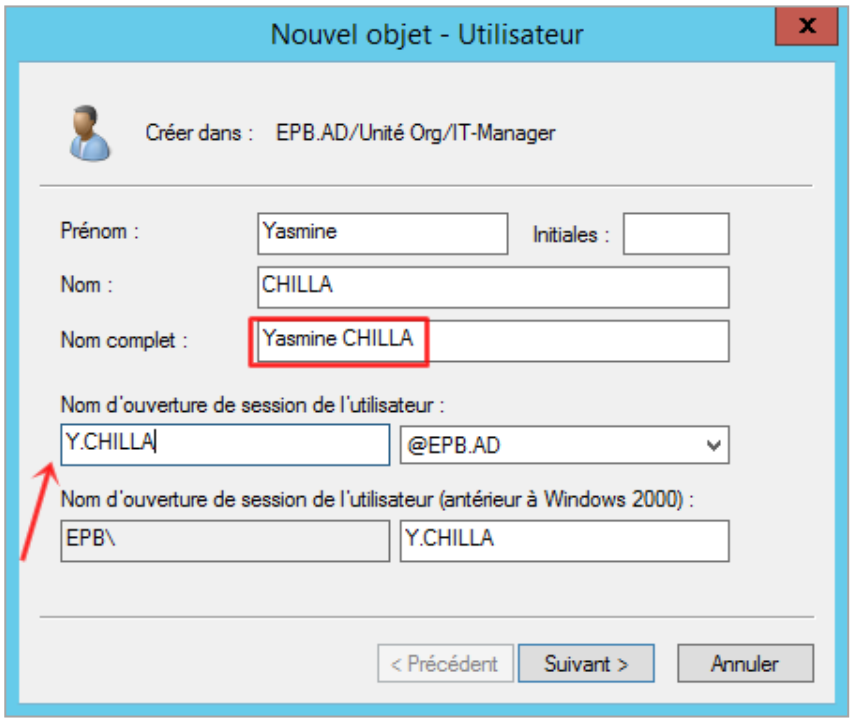


Figure III-28 : Création des sessions utilisateur.

Etape 9 : Mise en œuvre des Group Policy Organisation (GPO)

Les stratégies de groupe, aussi appelées GPO, sont des outils de configuration permettant de modifier un ensemble de paramètres s'appliquant à des configurations "utilisateur" ou à des configurations "ordinateur" membres d'un domaine Active Directory (AD DS), ils présentent plusieurs avantages dont : la réduction des coûts, le contrôle des configurations, la conservation des utilisateurs productifs, le renforcement de la sécurité et la gestion des droits d'accès aux ressources.

Après avoir installé Active Directory, mis en place notre domaine dans une nouvelle forêt et créé nos unités d'organisation, nous allons mettre en place nos GPO.

La première étape consiste à modifier le « default domaine Policy » dans le menu « Gestion de stratégie de groupe » celle-ci représente la GPO par défaut de notre domaine, il suffit de faire un clic droit et de modifier comme la figure ci-dessous l'indique :

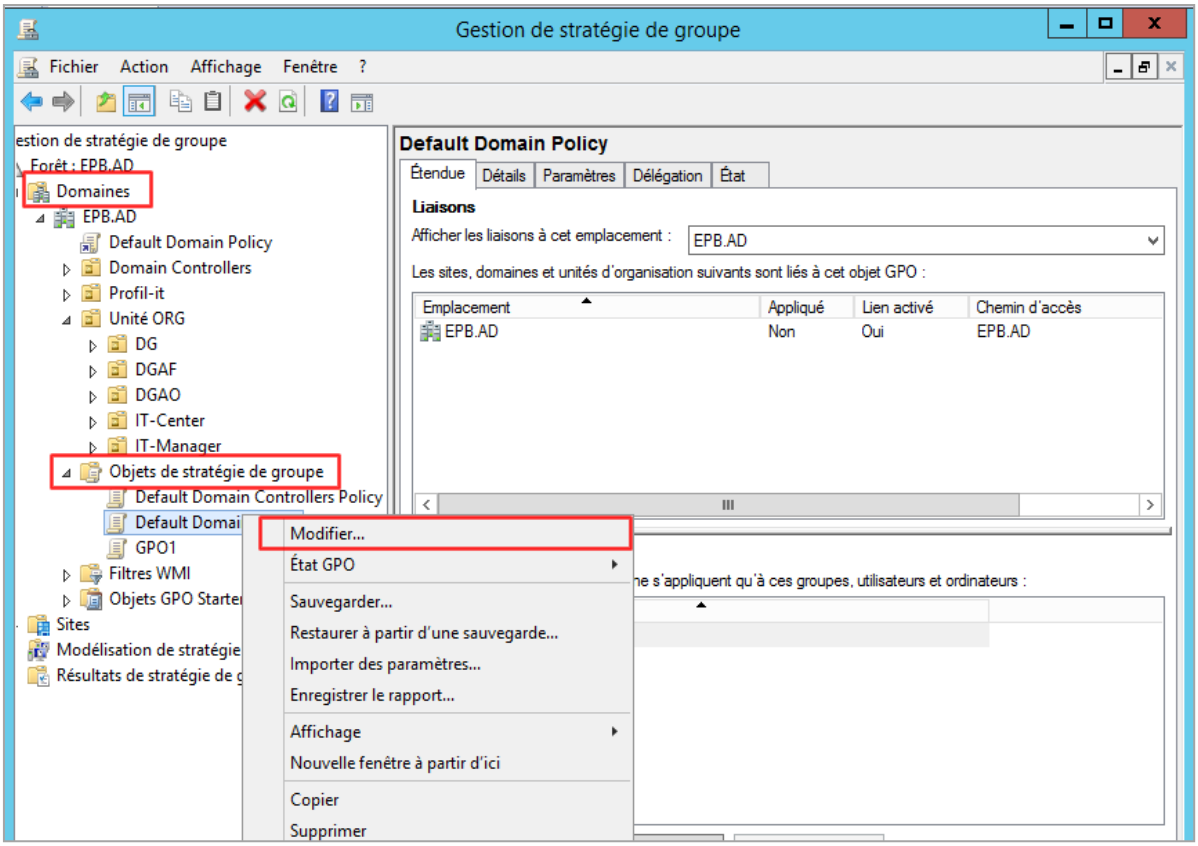


Figure III-29 : Modification de la stratégie de groupe par défaut.

a) Configuration ordinateur

Arrivé à la fenêtre « Editeur de gestion des stratégies de groupes » nous remarquons qu'il y'a deux types de configuration : ordinateur et utilisateurs, nous commencerons par les configurations ordinateurs :

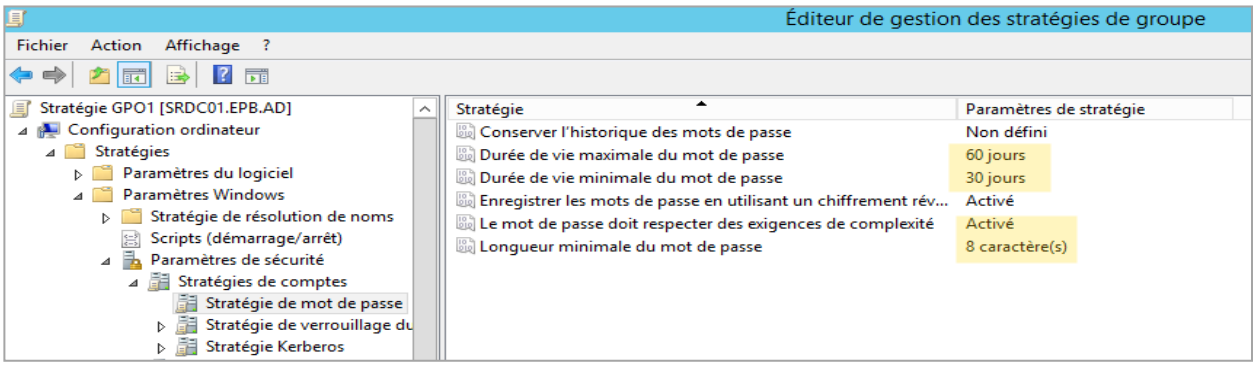


Figure III-30 : Configuration d'une GPO ordinateur.

La configuration ordinateur s'applique au démarrage de l'ordinateur et est valable pour tous les utilisateurs qui ouvrent une session. Elle s'applique seulement si le site Active Directory, le domaine, ou l'UO auquel est liée la GPO contient des objets ordinateurs.

Prenons exemple les stratégies de mot de passe, se trouvant dans les paramètres Windows de la configuration Ordinateur, la stratégie est définie sur plusieurs paramètres soient :

– **Conserver l'historique des mots de passe** : Afin qu'un utilisateur évite de reprendre un ancien mot de passe.

–**Durée de vie minimale de mot de passe** : Ce qui permet d'empêcher un utilisateur de changer successivement plusieurs fois son mot de passe. Cela pourrait lui permettre de dépasser la limite de l'historique des mots de passe et de redéfinir son mot de passe initial.

– **Appliquer l'âge maximal de mot de passe** : Le temps ou l'utilisateur gardera un mot de passe reste valide avant qu'il ne soit obligé de le changer.

–**Le mot de passe doit respecter des exigences de complexité** : Indiquer si oui ou non le mot de passe doit respecter ces exigences (conseillé par sécurité).

–**Appliquer la longueur minimale du mot de passe** : Chiffre entier pour définir la longueur minimale que doit faire le mot de passe.

b) Configuration utilisateur

La configuration utilisateur s'applique à l'ouverture de session et « suit » l'utilisateur quelque soit l'ordinateur sur lequel il se connecte. Elle s'applique seulement si le site Active Directory, le domaine, ou l'UO auquel est liée la GPO contient des objets utilisateurs.

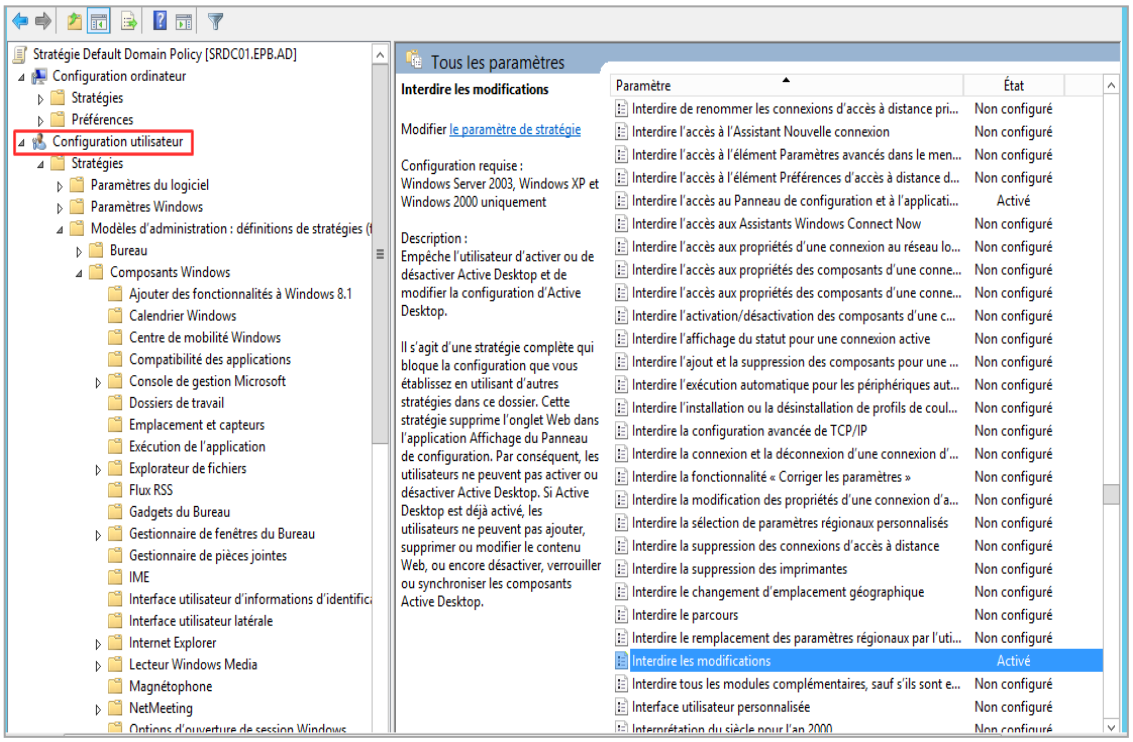


Figure III-31 : Configuration d'une GPO utilisateur.

Nous pouvons faire différents paramétrages liés aux utilisateurs, comme interdire l'accès au panneau de configuration, interdire la suppression des imprimantes et bien d'autres.

C) Configuration d'une GPO pour une UO

Pour créer une GPO propre à une unité d'organisation, dans le menu « Gestion de stratégie de groupe » choisir l'unité organisationnelle puis nous n'avons plus qu'à faire une clique droite--> « Créer un objet GPO dans ce domaine et lier ici… ».

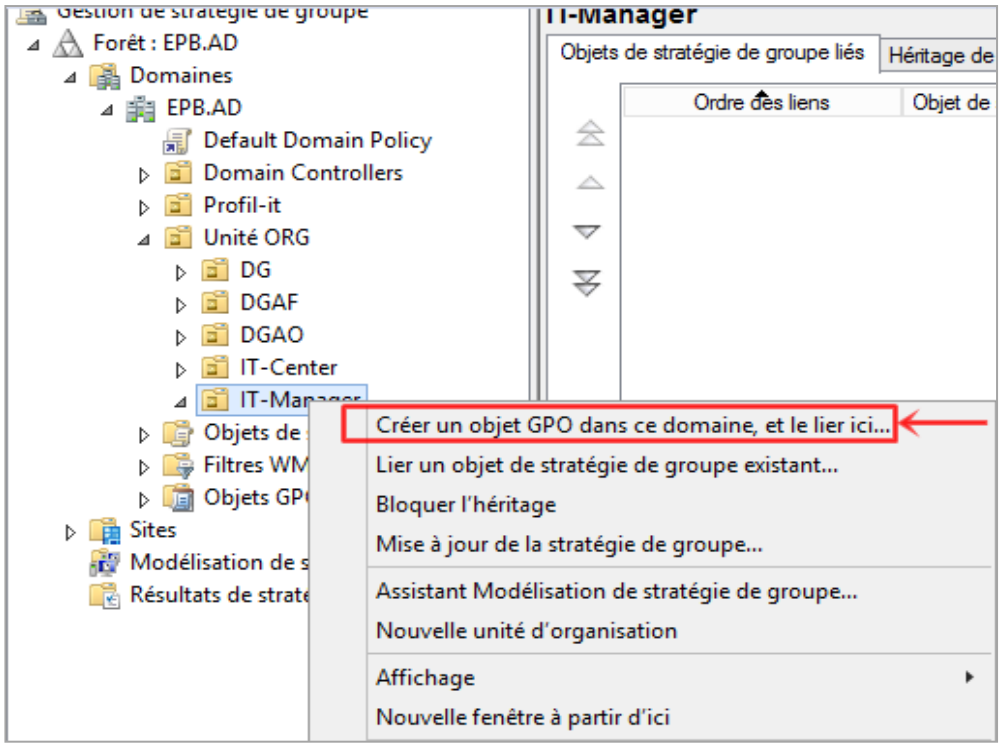


Figure III-32 : Création d'une GPO pour une UO.

Une fenêtre s'ouvre nous permettant de nommer notre GPO. Dans cet exemple, nous avons choisi le nom GPO-Manager pour l'unité organisationnelle IT-Manager

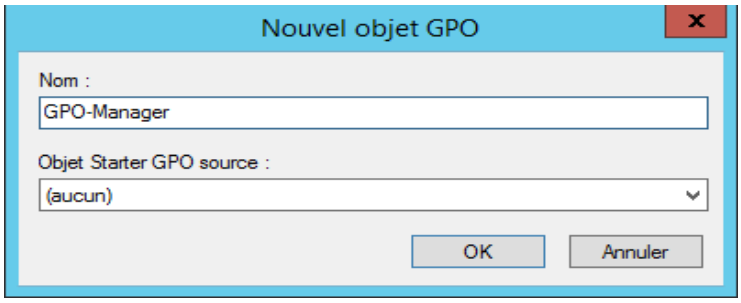


Figure III-33 : Création d'une nouvel GPO.

Le GPO est maintenant visible dans l'unité d'organisation « IT-Manager ». Nous n'avons plus qu'à la modifier comme nous l'avons fait précédemment pour la « Policy default objet ».

Etape10 : Création des profils itinérants

En entreprise, ce n'est pas rare que les utilisateurs changent de bureaux, utilisent l'ordinateur du collègue ou changent de service, les utilisateurs sont amenés à utiliser différentes machines. De ce fait, la disposition sur une machine à l'autre ne sera pas la même et les données ne seront pas les mêmes si l'utilisateur stocke du contenu sur sa machine. En effet, les profils itinérants vont stocker leurs informations sur notre serveur SrDC01, pour cela, il est nécessaire de créer sur le serveur, un répertoire qui accueillera tous les profils utilisateurs. Une fois cela fait, dans les propriétés du dossier Choisir « *Partage avancé* », cocher la case « *Partager le dossier* » et vérifier que le « *noms de groupes ou d'utilisateurs* » est bien positionné sur *Tout le monde*, puis indiquer *Autorisé* sur la valeur *Contrôle total.*

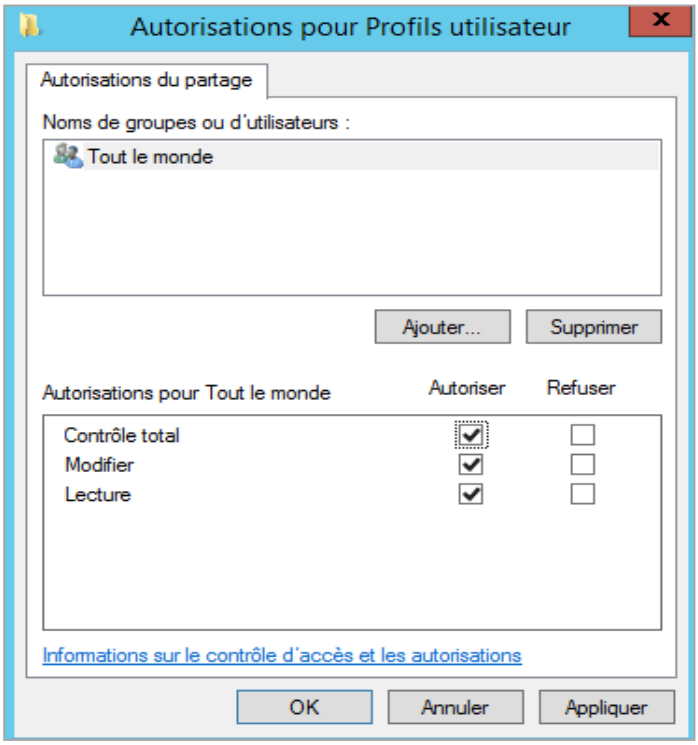


Figure III-34 : Autorisation pour profils utilisateur.

Ensuite, dans la console Utilisateurs et Ordinateurs Active Directory et dans les propriétés d'un utilisateur, choisir l'onglet Profil -> Chemin du profil. Nous devons renseigner l'adresse du dossier partagé sous la forme : \\Serveur\Dossier\%username%.

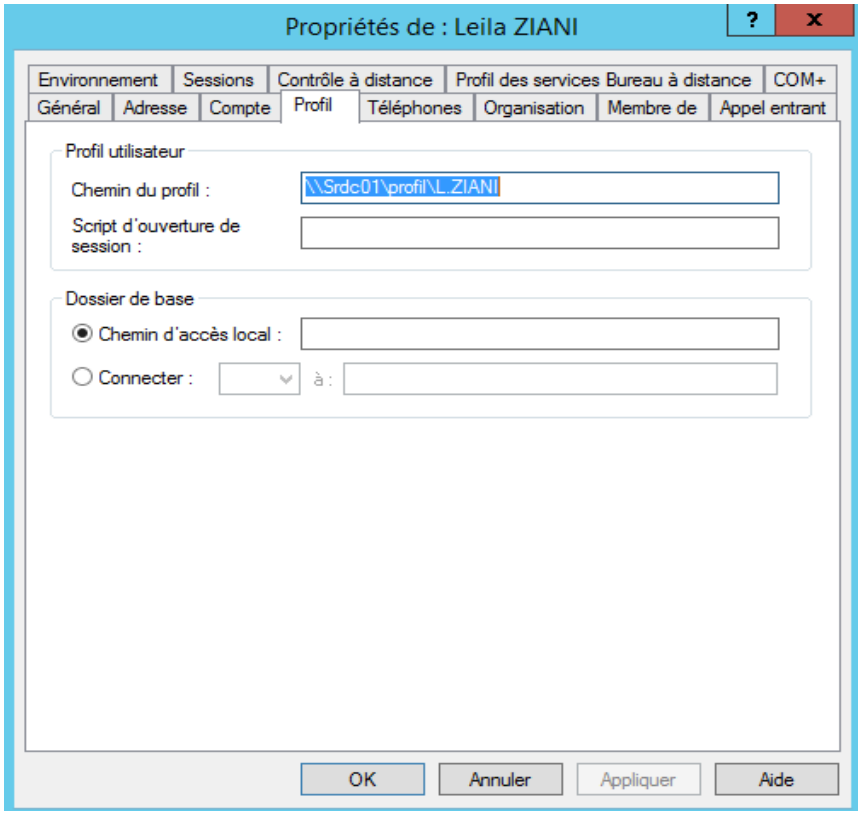


Figure III-35 : Spécification du profil de l'utilisateur.

L'opération est à faire sur chaque compte utilisateur. Le dossier utilisateur sera situé sur le serveur, et sera synchronisé à chaque ouverture et fermeture de session.

III.4.3 Mise en œuvre de l'autorité de certification Active Directory Certificat Services (AD CS)

Les services de certificats Active Directory (AD CS) fournissent des services personnalisables pour l'émission et la gestion de certificats qui sont utilisés dans les systèmes de sécurité logiciels employant des technologies de clé publique.

Dans cette partie, nous allons créer une autorité de certification racine d'entreprise (liée à l'Active Directory) et nous modifierons les stratégies de groupe pour que les clients de l'Active Directory reçoivent automatiquement le certificat de notre autorité de certification racine. Ainsi, notre autorité sera reconnue par les ordinateurs clients et aucun avertissement ne s'affichera concernant nos certificats SSL, notre serveur SRDC01 sera l'hébergeur de la PKI, pour y parvenir nous devons passer par les étapes suivantes :

Etape1 : Installation et configuration de l'autorité de certification racine d'entreprise

Après l'installation du « Services de certificats Active Directory » sur le gestionnaire de serveur, et avoir cocher la case « Autorité de certification » pour configurer ce rôle. La figure suivante présente un résumé des configurations post installation.

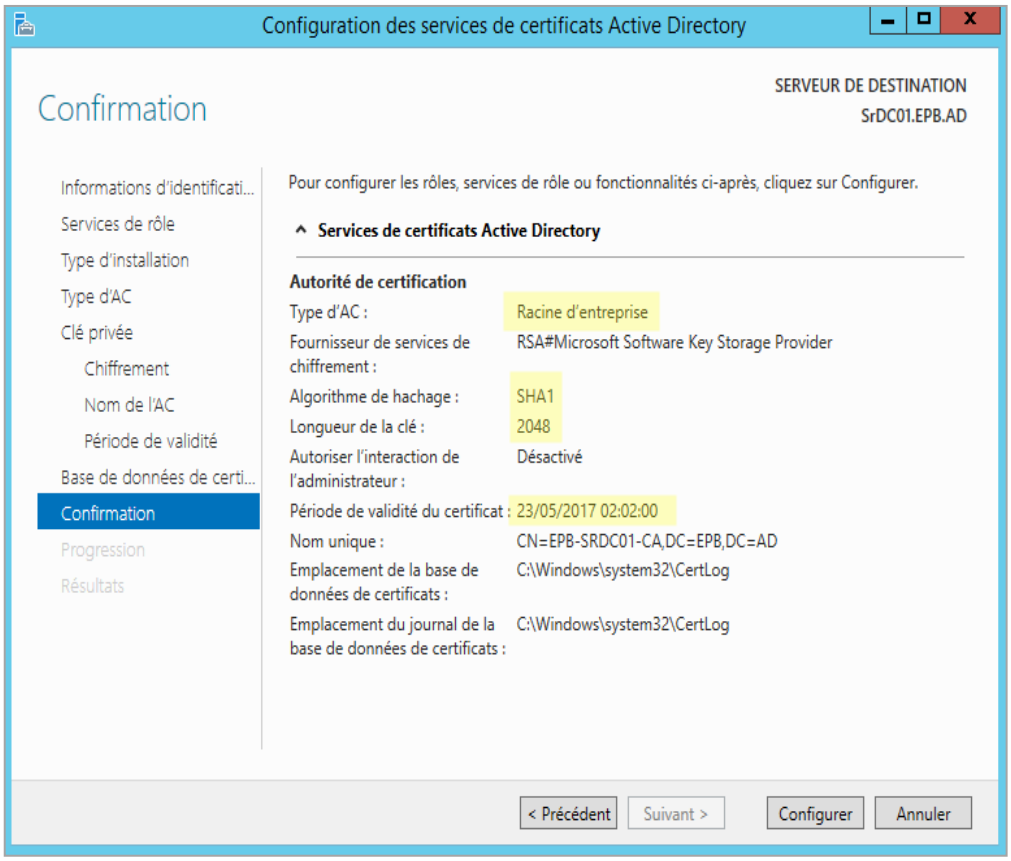


Figure III-36 : Configuration d'une PKI.

Etape 2 : Exportation du certificat de l'autorité racine

Pour pouvoir distribuer notre certificat racine aux clients de l'Active Directory, nous ouvrons la console « mmc » où nous pouvons voir que notre certificat est déjà présent dans cette liste, sous le nom d'**EPB-SERVEURDC01-CA** et nous n'avons plus qu'à l'exporter.

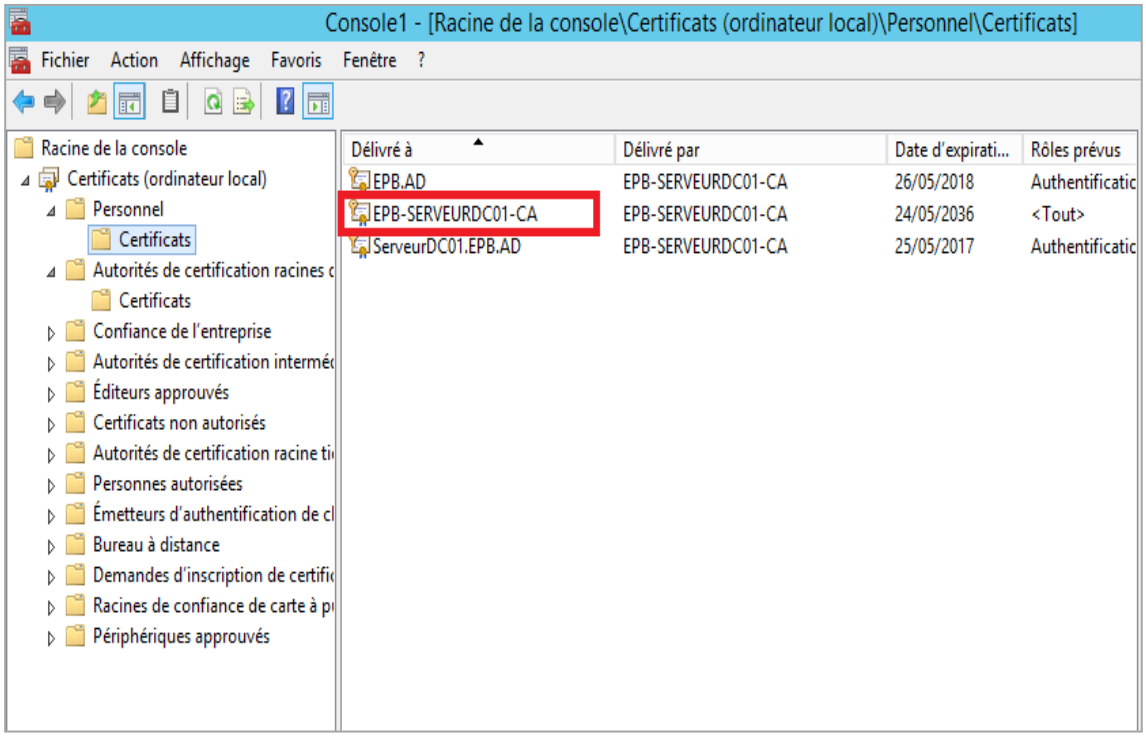


Figure III- 37 : Le certificat de l'autorité racine à exporter.

Afin d'exporter ce certificat d'autorité racine sous format « .pfx » (avec la clé privée), sur le dossier « Certificats » qui se trouve dans le dossier « Personnel », effectuer un clic droit et choisir l'option exporter et ce depuis le certificat de notre autorité de certification EPB-SERVEURDC01-CA.

Etape 3 : Création d'un nouveau modèle de certification

Pour gérer les modèles de certificats, ouvrir l'interface « Autorité de certification », dans « modèles de certificats » clique droit « gérer » ensuite dupliquer le modèle « Serveur web », l'étape qui suit consiste à renommer le nouveau modèle de certificat et modifier la période de validité, dans notre cas cette dernière est fixée à 10 ans.

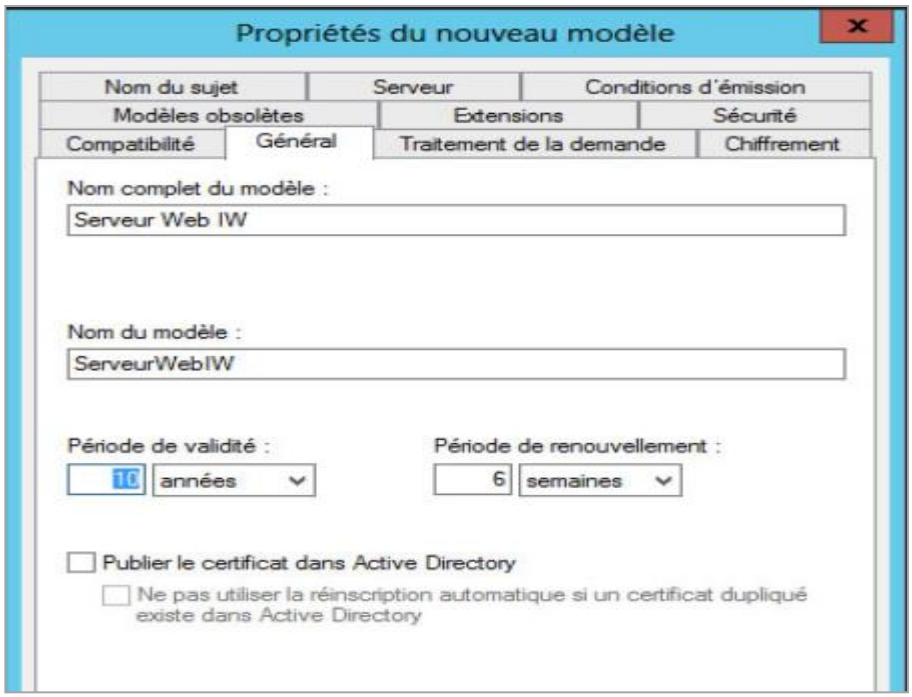


Figure III-38 : Propriétés du nouveau modèle de certification.

Ensuite, aller dans l'onglet « Sécurité » modifier les autorisations des « utilisateurs authentifiés » pour qu'ils puissent demander des certificats. Cocher les cases « Inscrire » et « Inscription automatique ».

Etape 4 : Demande d'un certificat

Pour demander un certificat qui sera signé par notre autorité de certification, sur la console aller à « Personnel » puis « Certificats ». Ensuite sur le menu qui apparait sélectionner « Toutes les tâches » puis « demander un nouveau certificat ».

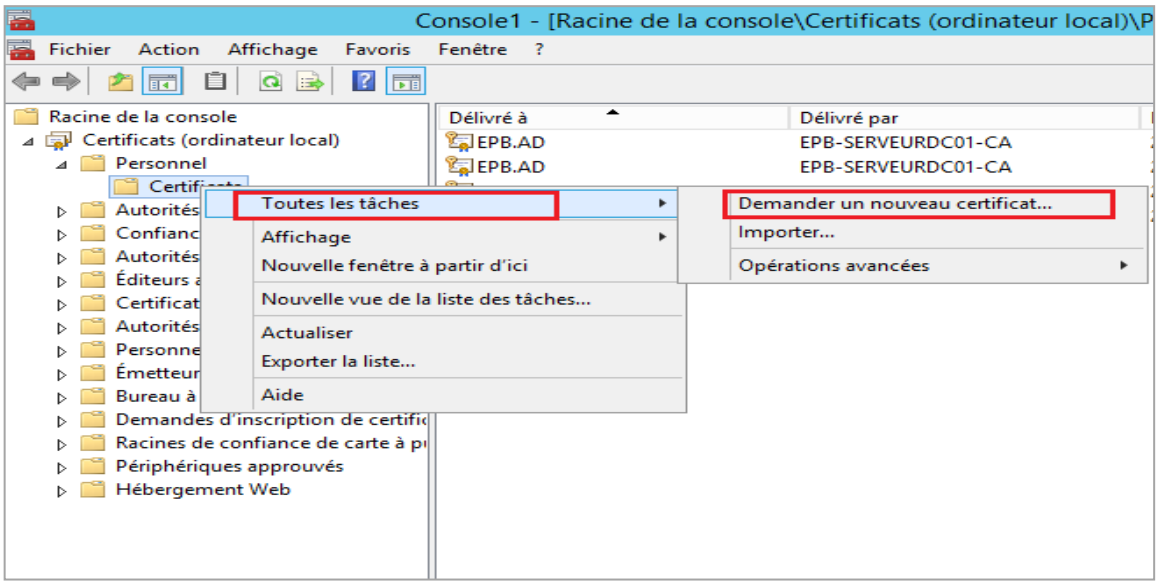


Figure III-39 : Demande d'un nouveau certificat.

Suite à ça, nous choisissons notre nouveau modèle de certificat crée auparavant qui est « serveur Web IW ».

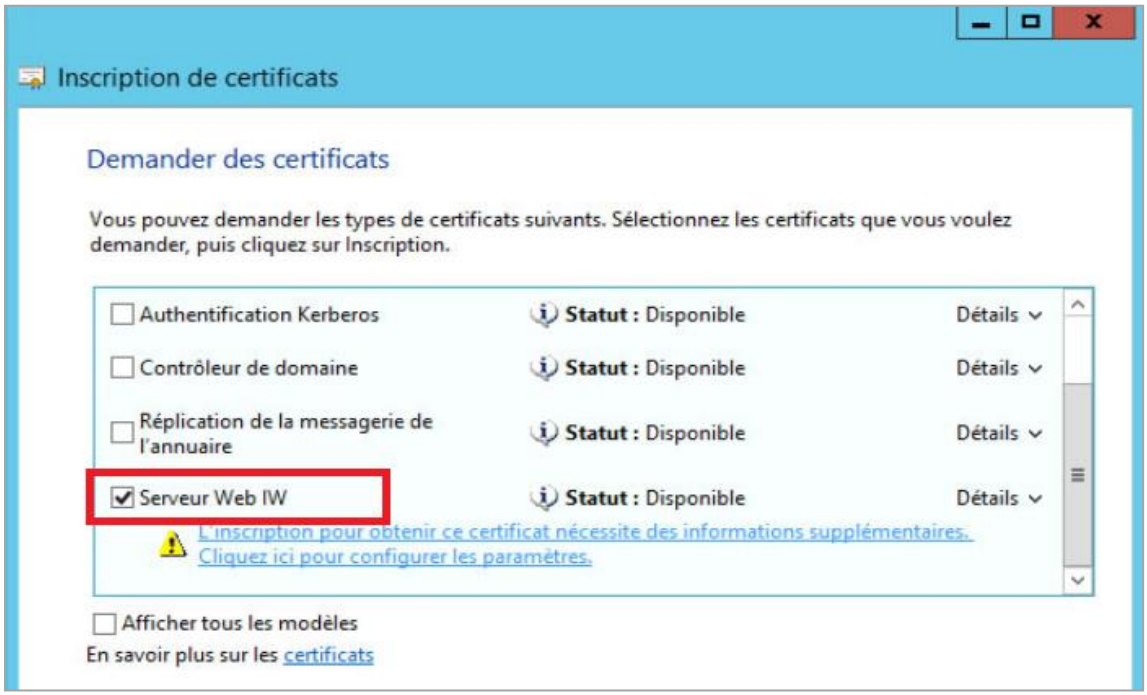


Figure III-40 : Le choix d'un type de certificat.

Etant donné que ce certificat sert à vérifier l'adresse d'un site internet, et que son inscription nécessite des informations supplémentaires, on doit alors indiquer le nom de domaine de l'ordinateur qui est « EPB.AD » comme « nom commun ».

Etape 5 : Protéger le serveur web IIS avec le certificat généré

Maintenant que nous avons notre certificat, nous allons sécuriser notre serveur web IIS grâce à ce certificat. Nous installons d'abord le serveur web sur notre machine virtuelle, pour cela il suffit d'installer le rôle « Serveur Web (IIS) » et de laisser le reste par défaut.

En suite dans l'interface « gestionnaire de serveur », on peut sélectionner le site qu'on souhaite sécuriser, dans notre cas, ce sera celui par défaut.

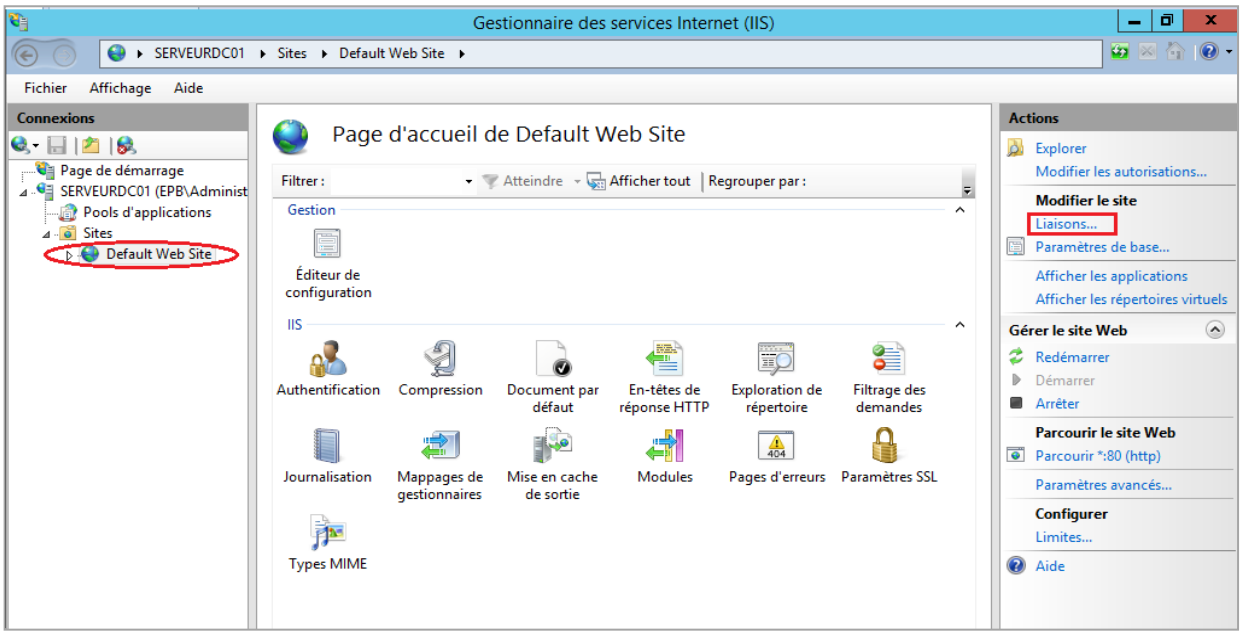


Figure III-41 : Sécuriser le serveur web avec un certificat.

Puis dans la colonne de droite sélectionner « Liaisons » et ajouter un nouveau port en sélectionnant « http » (port 443 par défaut) sans oublier notre certificat « EPB.AD » dans la liste « Certificat SSL ».

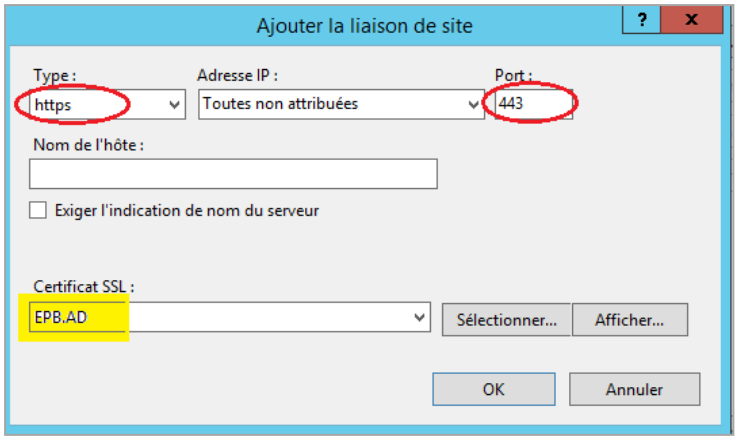


Figure III-42 : Ajout d'une liaison de site.

Désormais, en saisissant notre nom de domaine dans le navigateur web « Internet Explorer » du serveur et en cliquant sur le petit cadenas qui s'affiche dans la barre d'adresse, on peut voir que notre navigateur n'a pas affiché d'avertissement concernant notre certificat car celui-ci est signé par notre autorité de certification. Etant donné que le certificat de notre autorité de certification se trouve dans la liste des autorités de confiance de notre serveur, le certificat est considéré comme valide.

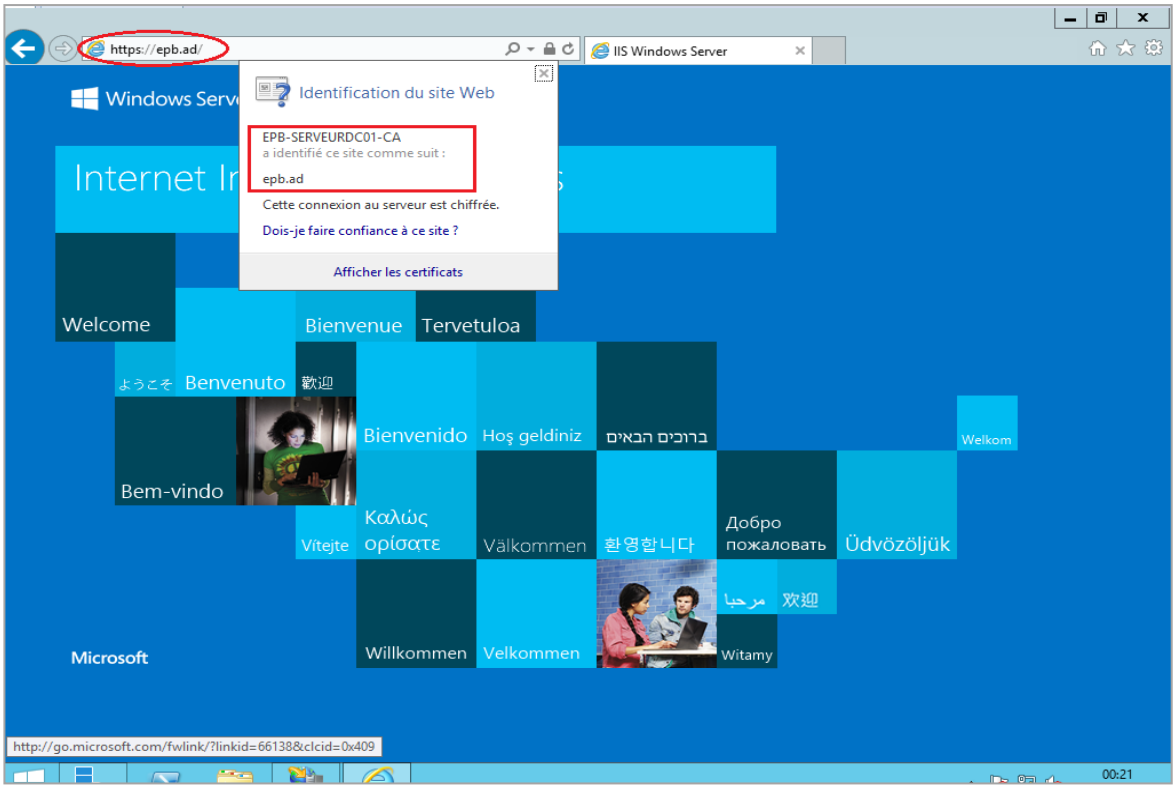


Figure III-43 : Accès à l'interface web de l'AC.

Etape 6 : Distribution du certificat aux clients de l'Active Directory

Etant donné que nous avons créé un Active Directory sur notre serveur, nous pouvons modifier les stratégies de groupe pour que nos clients reçoivent le certificat de notre autorité de certification. Ainsi, nos clients pourront accéder à notre intranet (site web accessible uniquement sur un réseau interne) de façon sécurisée et sans avoir d'avertissement concernant le certificat.

Dans la fenêtre « Gestion de stratégie de groupe », aller à Autorité de certification racines de confiance, effectuer un clic droit et choisir « importer ».

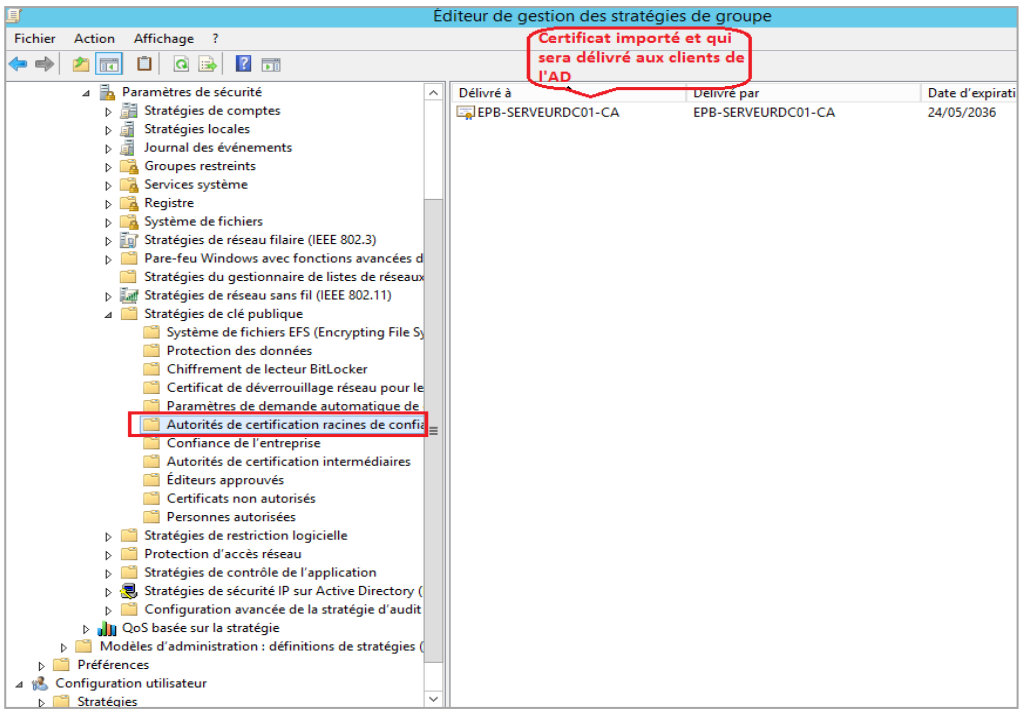


Figure III-44 : Distribution du certificat de l'autorité aux utilisateurs de l'Active Directory.

Maintenant que le certificat de notre autorité de certification est importé dans la liste des autorités de confiance de notre domaine, tous les clients de l'Active Directory recevront ce certificat par défaut.

Etant donné que l'on utilisera des certificats signés par cette autorité de certification, nos certificats seront toujours valides (jusqu'à leurs dates d'expiration).

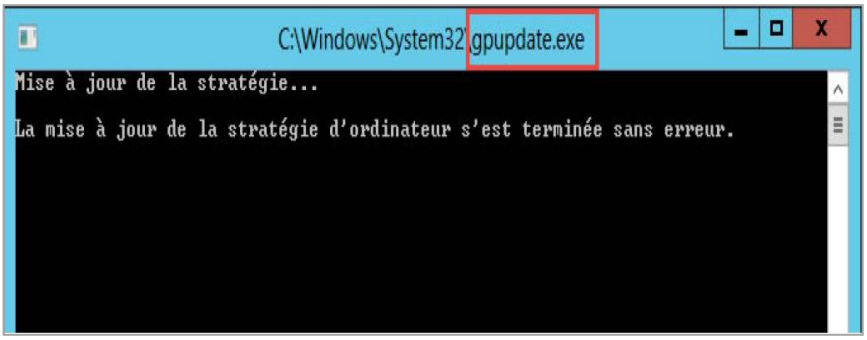


Figure III-45 : Mise à jour de la stratégie d'ordinateur.

Lancer le programme "gpupdate" pour mettre à jour la stratégie de l'ordinateur et celle du domaine.

Etape 7 : Révocation du certificat

Maintenant que notre autorité fonctionne correctement, nous allons configurer le système de révocation de certificats. Ce système nous permet de rendre un certificat invalide, pour une raison ou pour une autre.

Pour le moment, notre autorité de certification publie les listes de révocations, mais uniquement via le protocole LDAP.

Le problème, c'est qu'il n'y a que le serveur qui a accès à l'Active Directory (le LDAP). Pour résoudre ce problème, il suffit de publier ces listes de révocations pour le protocole http (le web).

Pour pouvoir publier les listes de révocations pour le protocole http, nous allons installer la fonctionnalité « Inscription de l'autorité de certification via le Web » du rôle « Services de certificats Active Directory ». Une fois le rôle installé, on accède à l'interface web en saisissant cette adresse https://epb.ad /CertSrv , tel que CertSrv désigne l'interface web de l'autorité de certification.

Figure III-46 : Interface de gestion d'autorité de certification.

Sur le « Gestionnaire de l'autorité de certification », au niveau « Certificats délivrés » nous choisissons de révoquer le certificat « Serveur Web IW », clic droit sur ce certificat et choisir « Révoquer un certificat », suite à ça une fenêtre apparait et nous demande de sélectionner la raison de la révocation.

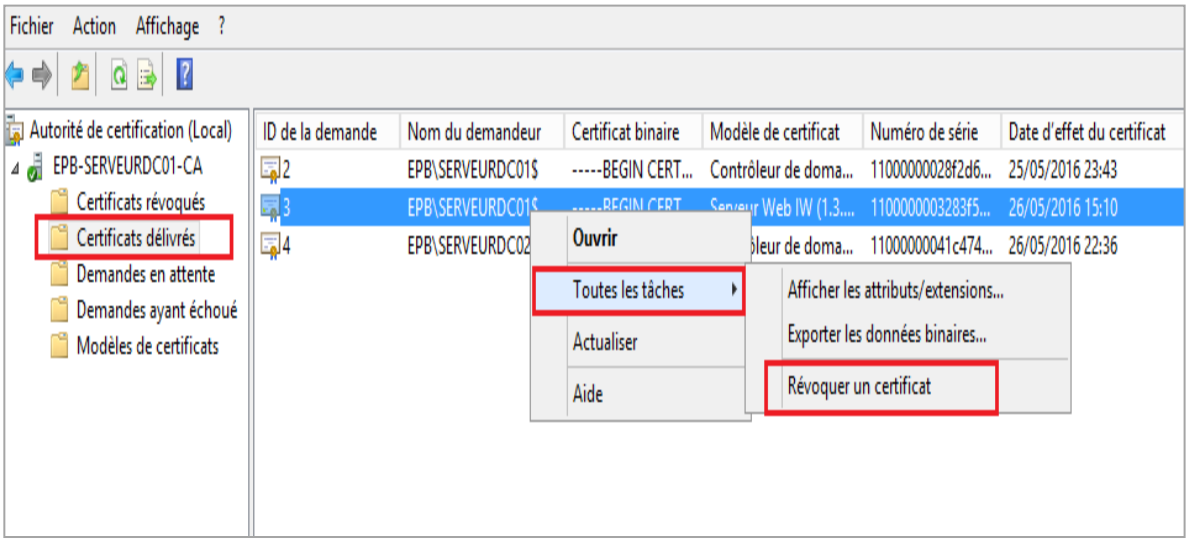


Figure III-47 : Révocation du certificat.

Maintenant, ce certificat est affiché dans les certificats révoqués. Pour que les clients sachent que ce certificat est révoqué, nous devons publier la liste des certificats révoqués.

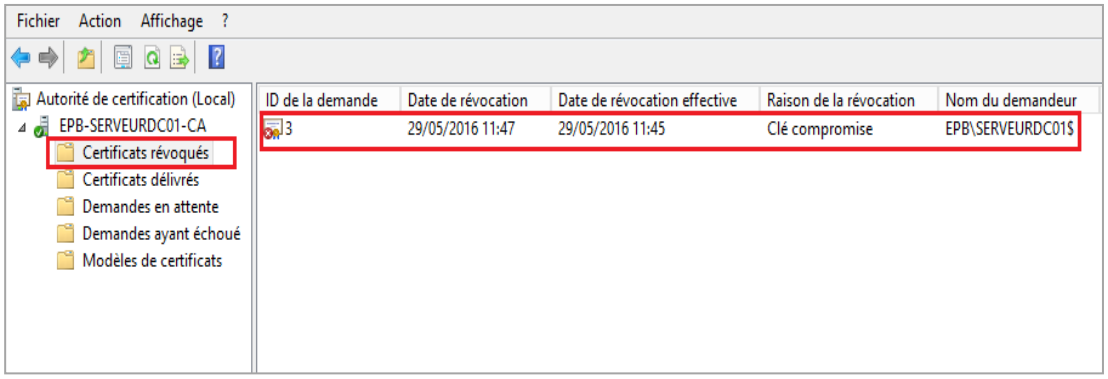


Figure III-48 : Certificat révoqué.

III.4.4 Mise en œuvre des services de fichiers avancés

III.4.4.1 Configuration de BranchCache

La fonctionnalité « branche cache » permet la mise en cache des éléments partagés. Prenons un exemple, une entreprise ayant un site principal et un site annexe, sur le site principal se trouve un serveur de fichiers qui partage les données à l'intégralité des collaborateurs. A chaque fois qu'un client du site annexe accède à un fichier celui-ci doit être téléchargé par la liaison WAN inter-sites, potentiellement une liaison lente (comparée à la vitesse d'une liaison LAN).

Sur le long terme, notamment si les fichiers sont conséquents et si nombreux sont les collaborateurs sur le site annexe, une telle pratique peut devenir problématique. C'est là qu'intervient le BranchCache ; lors de la récupération d'un document, ce dernier ne passe qu'une seule fois par la liaison lente. Une fois le fichier arrivé sur le site distant, il sera mis en cache pour tous les autres clients de ce site, quand ils voudront accéder à ce même document, ils récupéreront le document depuis l'endroit où il est stocké en cache. Avec BranchCache, l'économie est réalisée sur la bande passante de la liaison, mais aussi sur les temps d'accès aux documents.

L'installation du serveur BranchCache doit être effectuée sur tous les serveurs qui hébergent des données, la fonctionnalité peut être installé avec une commande PowerShell : *Install-WindowsFeature -Name BranchCache, FS-BranchCache* ou en suivant la procédure habituelle en interface graphique. Elle se trouvera alors sous « Services de fichiers et de stockage ».

La configuration s'effectue par l'intermédiaire des stratégies de groupe, son objectif est d'activer sur le serveur la publication de hachage concernant les données partagées.

Ces résultats de hachage seront utilisés par la suite dans le processus BranchCache, dans le but d'identifier de façon unique un document.

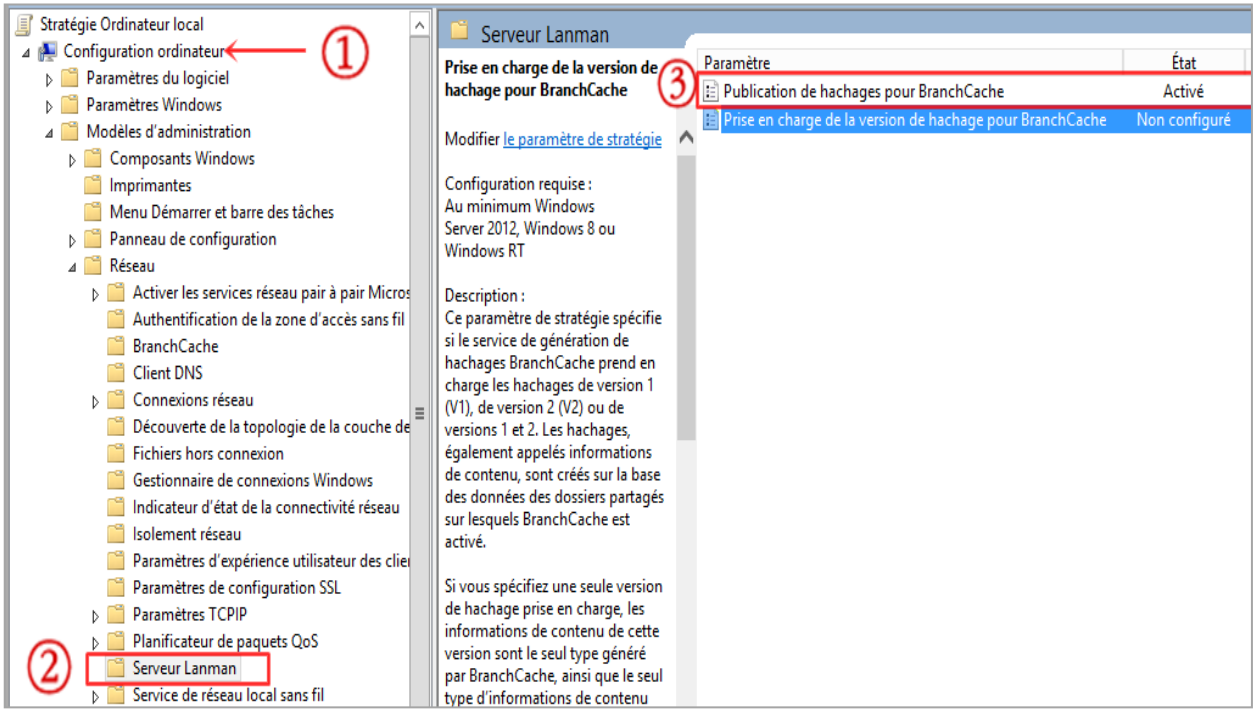


Figure III-49 : Activer la publication de hachage pour BranchCache.

Il suffit de valider la configuration du paramètre. Ensuite, actualiser la stratégie de groupe sur le serveur en forçant son activation avec la commande *GPUpdate / Force* sur PowerShell.

Nous avons autorisé la publication de hachages pour les dossiers partagés où BranchCache est actif. Il est donc nécessaire d'activer BranchCache sur le partage concerné. En effectuant un clic droit sur le dossier partagé concerné puis Propriétés, Cliquer sur le bouton *mise en cache* ➔ *Paramètres hors connexion* et cocher *Seuls les fichiers et les programmes spécifiés par les utilisateurs sont disponibles hors connexion* et cocher la case enfant *Activer BranchCache.*

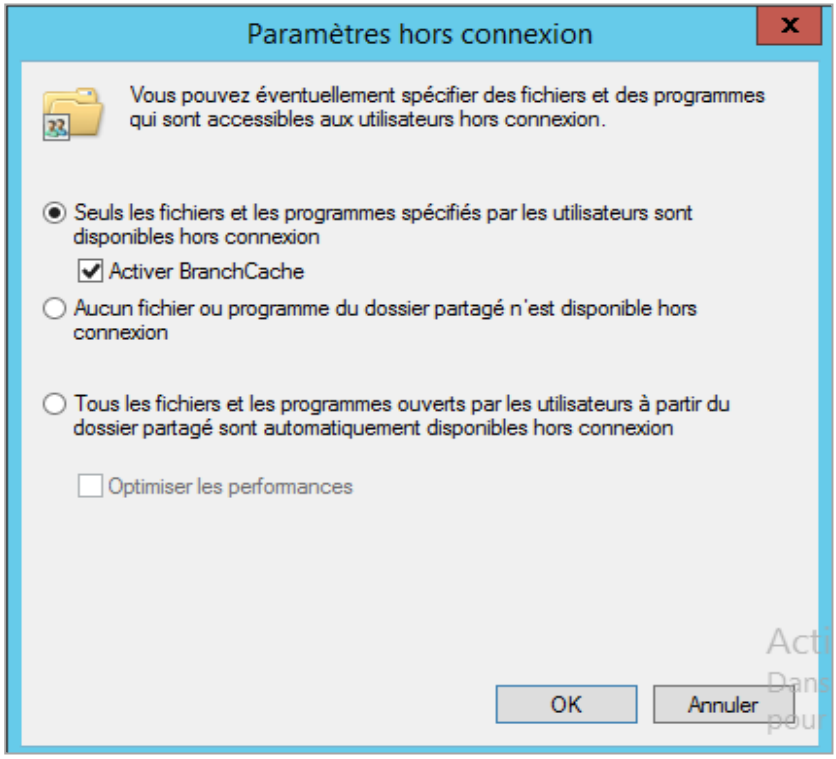


Figure III-50 : Activer BranchCache sur un partage.

Enfin, il est nécessaire de configurer les postes clients pour qu'ils puissent tirer parti de BranchCache. Pour cela, nous allons configurer les postes clients grâce aux GPO : Tout d'abord, nous ouvrons la *Console de gestion des stratégies de groupe*. On crée une nouvelle stratégie nommée ici *Windows BranchCache* qu'on va lier avec les utilisateurs ou serveurs distant et On déroule Configuration ordinateur > Stratégies > Modèles d'administration >Réseau, puis nous sélectionnons le paramètre BranchCache.

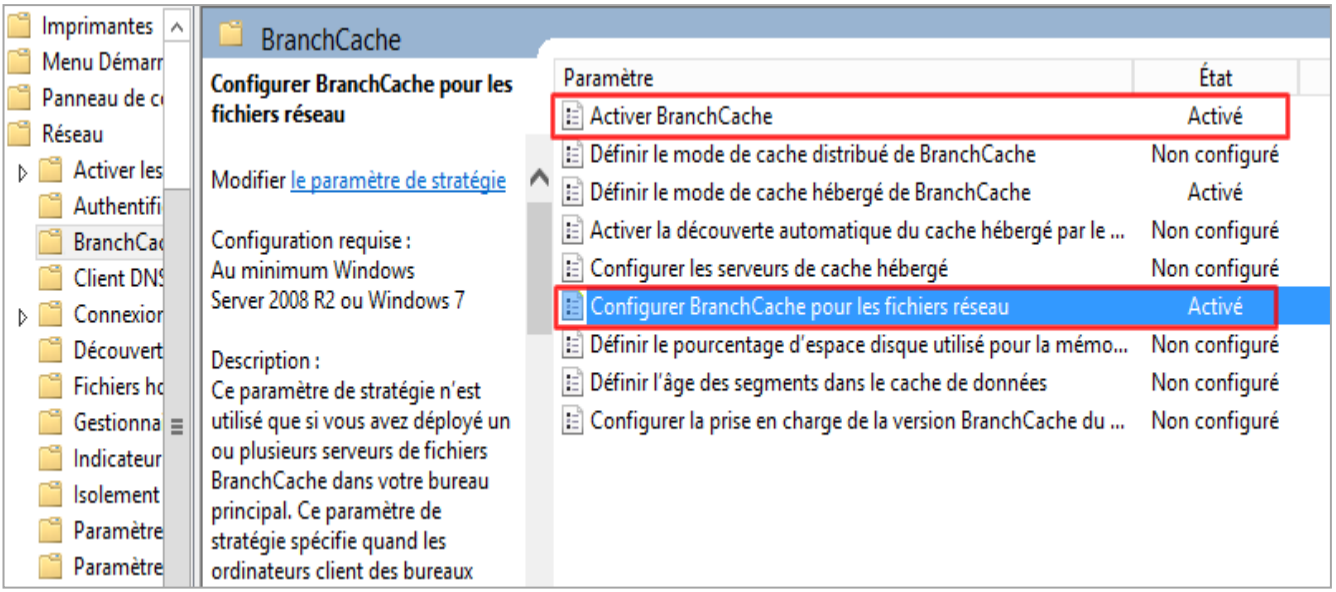


Figure III-51 : Configuration du client BranchCache.

Nous ouvrons le paramètre Activer BranchCache puis l'on sélectionne « *Activer* ». Enfin, pour que le client soit capable d'utiliser BranchCache afin de récupérer des fichiers provenant le serveur de fichier, nous sélectionnons le paramètre *Configurer BranchCache pour les fichiers réseau*, que l'on active.

III.4.4.2 Gestion et contrôle du partage

Dans un environnement d'entreprise il est essentiel de pouvoir s'échanger des fichiers sans pour autant avoir besoin d'utiliser quelques supports amovibles. L'une des techniques de collaboration les plus courantes est de ranger les fichiers dans des dossiers partagés. Il existe plusieurs types de partage de fichier sur Windows, mais nous avons choisi le SMB car c'est un partage qui fonctionne avec tous les autres systèmes d'exploitation MAC OS X et Linux.

Sur le gestionnaire de serveur, se positionner dans l'arborescence « Service de fichiers et de partages », sélectionner « tâches » puis « Nouveau partage », sur la fenêtre qui apparait choisir « SMB applications » ensuite saisir l'emplacement du fichier à partager, pour finir cliquer sur « créer » et le partage est opérationnel.

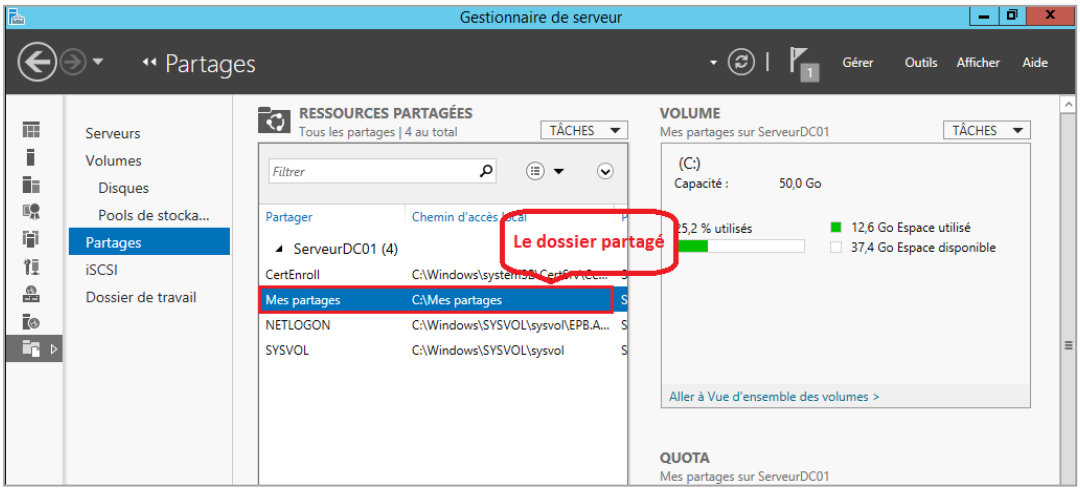


Figure III.52 : Dossier partagé.

III.4.4.3 Mise en œuvre du Cliché instantané

Ce système permet de disposer de plusieurs versions consistantes d'un fichier sur un volume donné et les rendre accessibles aux utilisateurs par le biais de répertoires partagés. Un utilisateur aura donc la possibilité de manipuler simplement et de façon autonome différentes versions d'un fichier ou d'un dossier pour le comparer, le copier ou le restaurer celons les cas.

On décide d'appliquer un cliché instantané sur le volume « disque local C », pour cela sur la fenêtre « propriétés de Disque local C », choisir l'anglet « Cliché instantané » puis « Activer ».

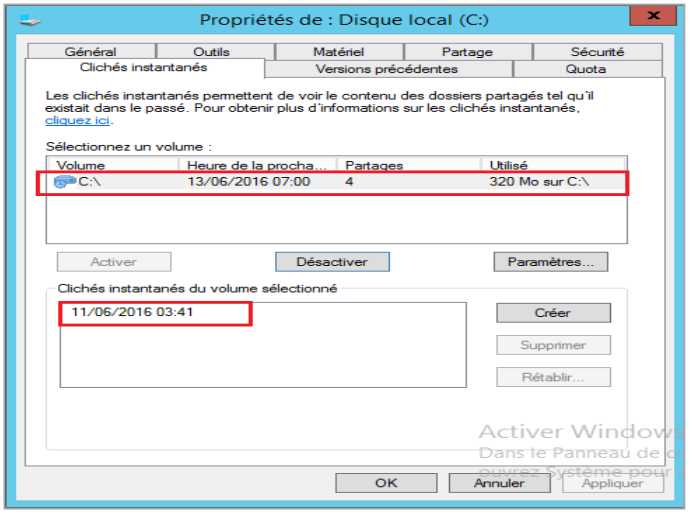


Figure III.53 : Cliché instantané activé.

III.4.5 Mise en œuvre d'une solution de sauvegarde « Backup »

La sauvegarde des données préserve l'activité de l'entreprise, notamment en cas de défaillance du système informatique.

L'entreprise peut faire face à plusieurs types de risques qui mettent en danger ses données : risques humains, Risques liés à l'environnement ou des risques liés aux dysfonctionnements matériels.

En cas de pertes de données, l'impact financier peut être notable pour l'entreprise en raison de la disparition de fichiers ou d'applications sensibles (base de données clients, rapports financiers, etc.), ou de la perte de temps engendrée par la remise en ligne de ces données. Pour cela nous avons mis au point une solution de sauvegarde des données de nos serveurs, appelées aussi Backup.

Pour installer le service de sauvegarde il faut passer par le gestionnaire de serveur et choisir l'option « Sauvegarde de Windows Server » dans la rubrique fonctionnalités. Une fois installée, nous allons démarrer la mmc « Sauvegarde de Windows Server » depuis « outils d'administration » puis désigner « Planification de sauvegarde ».

L'assistant de planification démarre et propose de sauvegarder l'intégralité du serveur ou le choix des volumes à sauvegarder. Nous allons opter pour une sauvegarde intégrale. Nous allons ensuite sélectionner la fréquence de sauvegardes.

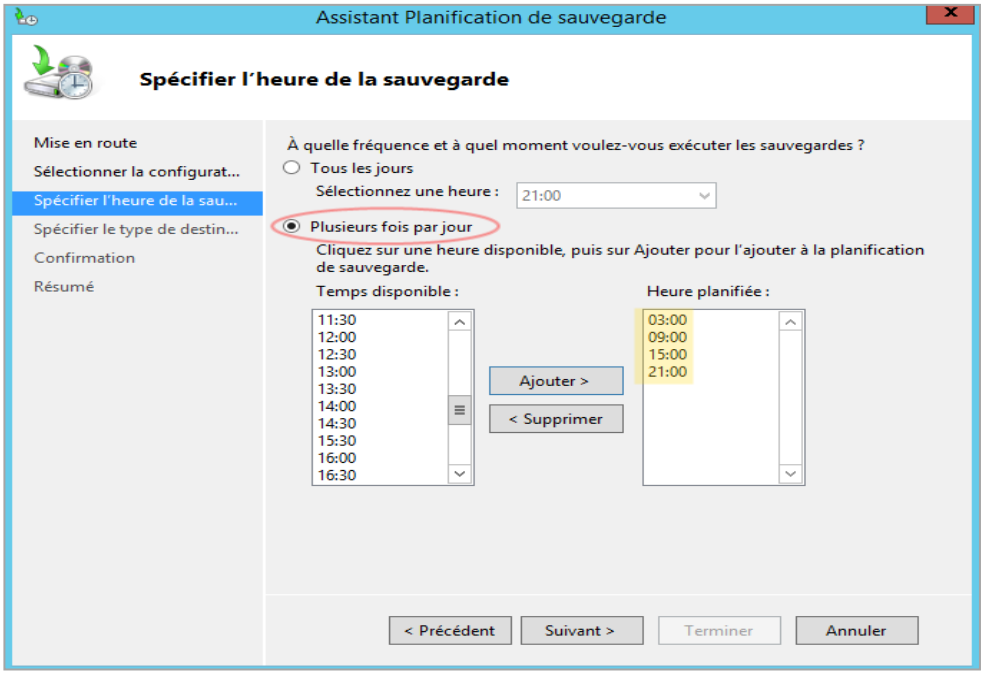


Figure III-54 : Spécifier l'heure de la sauvegarde.

Nous devons spécifier le type de support à disposition. Nous choisissons de sauvegarder les données du serveur principal sur un dossier partagé (qui se nomme Backup) se trouvant sur le serveur SrDC02.

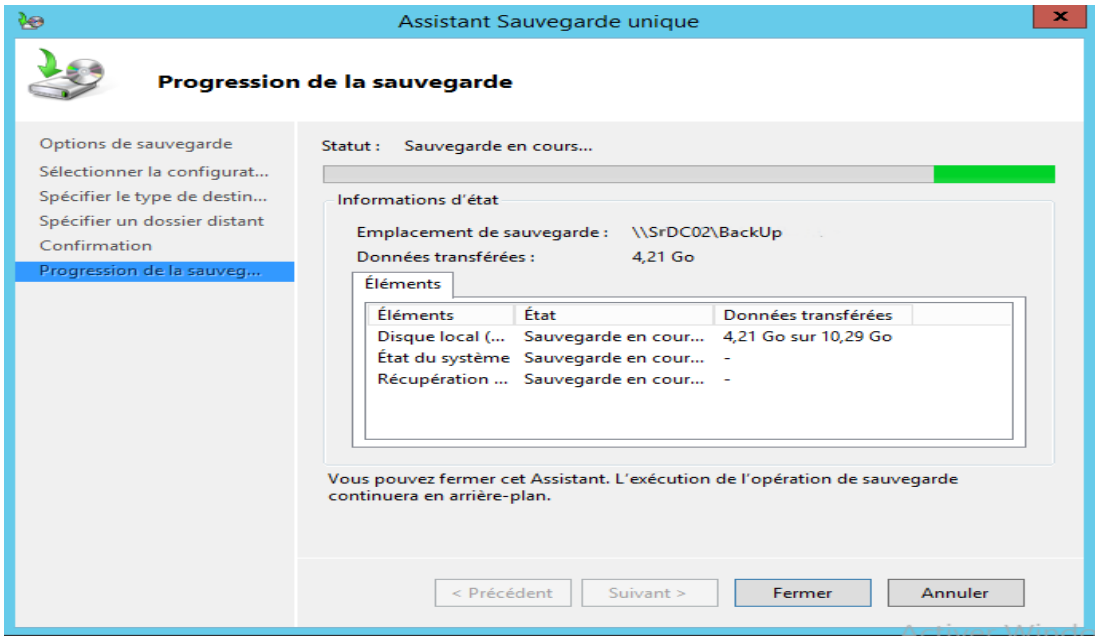


Figure III-55 : Sauvegarde sur le serveur secondaire.

Nous remarquons qu'une fois la tache terminée le serveur lance une première sauvegarde qui a été réussite, nous pouvons récupérer nos données sur le serveur secondaire.

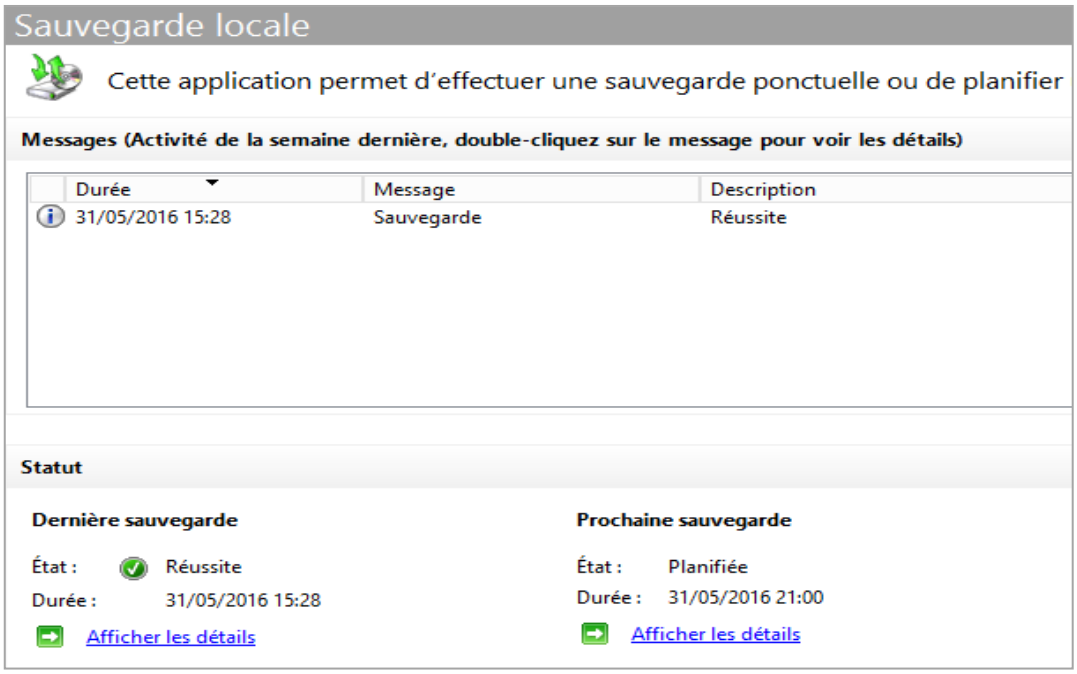


Figure III-56 : Résultat de la sauvegarde.

Conclusion

La réalisation de ce chapitre nous a permis de découvrir l'environnement de Windows Server 2012 R2 et de se familiariser avec ses différents composants et services. Ceci nous a permis également de voir la puissance de cet environnement. Premièrement, en termes de fonctionnalités à savoir l'organisation des ressources de l'entreprise que ce soit humaines ou matérielles en utilisant l'AD. Deuxièmement, en termes de sécurité, que ce soit par la définition des stratégies de groupe ou par l'infrastructure PKI qui offre aux utilisateurs du domaine la possibilité de chiffrement et de signature à l'aide des certificats. Troisièmement, en termes de gestion d'adressage dynamique qui se fait grâce au serveur DHCP.

Conclusion générale

Ce travail nous permis d'enrichir nos connaissances dans le monde des réseaux sur le plan administration, gestion et sécurité des réseaux informatiques de type LAN.

Dans le cadre de ce mémoire qui a pour objectifs la mise en œuvre d'une infrastructure réseau sous Windows server 2012 R2, nous avons étudié et mis en place :

- Le déploiement d'un contrôleur de domaine AD DS qui permet de gérer les utilisateurs et les ressources.
- Le renfoncement de la sécurité en mettant en œuvre une infrastructure à clés publiques PKI.
- Les services de fichiers avancés à savoir le BranchCache et le contrôle du partage.

Une attention particulière cependant a été portée aux mécanismes de tolérance aux pannes.

Nous avons implémenté, d'abord au niveau de la réplication du contrôleur de domaine puis le DHCP failover qui permet d'assurer la disponibilité du service DHCP. Nous avons proposé également, la solution de sauvegarde de reprise après sinistre (BackUp).

Perspectives :

- Implémentation d'un accès à distance, en mettant en œuvre des réseaux privés virtuels VPN.

- Mise en place d'un cluster NLB afin d'équilibrer les charges entre les serveurs de l'entreprise.

Références bibliographiques

Webographie

[2]: BUDAN N., TEDESCHI B., VAUBOURG S., « Nouvelles Technologies Réseau Les réseaux peer to peer », 19 janvier 2003 IN http://www-igm.univ-mlv.fr/~duris/NTREZO/20022003/Peer-to-peer.pdf

[3]: CALECA C, « Les réseaux », Réalisé à du site Laurent BAYSSE le du 6 mars 2005 IN http://csricted.univ-setif.dz/files/cours%20informatique/Les%20Reseaux.pdf

[4]: HAUTRIVE P., « La théorie des réseaux locaux et étendus » ,7 octobre 2006 IN http://hautrive.developpez.com/reseaux/?page=page_5

[9]: Microsoft IN https://www.microsoft.com/fr-fr/

[10]: LAMAISON F., "Migration Active Directory de Windows Server 2003 à 2012 », 05 Oct 2015 IN http://www.it-connect.fr/migration-active-directory-de-windows-server-2003-a-2012/

[11]: HAUTRIVE P. ; « Les systèmes d'exploitation réseaux » IN http://hautrive.free.fr/reseaux/architectures/systemes-exploitation-reseaux.html

Bibliographie

[1]: DOUKOE D., « Mise en place d'un réseau local avec connexion internet », BTS télécommunication, Centre d'enseignement supérieur des technologies internationales d'Abidjan, 2007

[5]: VAIRA T., « Cours Réseaux - Adressage IP », Frères des écoles chrétienne, Avignon, 2012

[6]: William R. Stanek, « guide de l'administrateur Windows server 2012 », edition Dunod, 2013.

[7]: BEUCHOT G., « Administration et sécurité des réseaux et des systèmes », institut national des sciences appliquées de Lyon, 2001

[8]: DJEBALI H., KENOUZE I., « Outil d'administration du Système de Gestion de Base de données Oracle », mémoire master en Informatique, université Kasdi Merbah, Ouargla, 2014.

[12] : Présentation de l'entreprise portuaire de Bejaia, document interne de l'EPB.

[13]: DESMOND B., « Designing, deploying and running Active Directory», 5 eme dition O'reilly, 2013.

[14] : DEPAGNE R., « les meilleures pratiques en design, sécurité et administration », microsoft tech-day, 7 février 2012.

Résumé

De nos jours et avec l'usage des réseaux locaux et d'internet, les entreprises ont toutes adopté un mode de présence sur la toile.

Le meilleur moyen d'être présent ne serait pas d'avoir uniquement une communication interne sur le réseau ou de disposer d'une connexion internet, mais d'avoir une bonne infrastructure informatique répondant aux nouveaux besoins.

Ce projet concerne l'étude du réseau informatique de l'entreprise EPBejaia où nous avons pu concevoir et mettre en place une infrastructure Active Directory pour l'administration et la sécurisation de son réseau local, aussi l'installation des différents services relatifs au bon fonctionnement de l'infrastructure EPB à savoir DNS, DHCP, PKI, les services de fichiers et les reprises après sinistre.

Mots clés : Windows Serveur 2012 R2, domaine, Active Directory, annuaire, service de fichier, infrastructure PKI, partage, sauvegarde.

Abstract

Nowadays and with the use of local networks and the Internet, companies have all adopted a mode of presence on the web.

The best way to be present would not only have an internal communication over the network or have an internet connection, but to have a good IT infrastructure responding to new needs.

This project concerns the study of computer network EPBejaia company where we were able to design and implement an Active Directory infrastructure for administration and securing its local network, as the installation of various services related to the proper functioning EPB infrastructure namely DNS, DHCP, PKI, file services and disaster recovery.

Keywords: Windows Server 2012 R2 Domain, Active Directory, directory, file services, PKI, sharing, backup.