REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITEMOULOUDMAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de fin d'études

En vue de l'obtention du diplôme de
Master en Informatique
Spécialité: Réseaux, Mobilités, et Systèmes Embarqués

Thème :

Implémentation d'une solution sécurisé dans une architecture d'un Cloud Computing

Encadré par:
M. Kibouh
A. Dib

Réalisé par :

Melle KHELIFI Mariem
&
Melle BELLIL Amina

REMERCIMENTS

Nous remercions le bon Dieu de nous avoir mis sur la voie du savoir.

Nous remercions vivement notre co-promoteur monsieur Mourad KIBOUH, et notre Promoteur monsieur Ahmed DIB d'avoir dirigé ce travail et ainsi pour leur conseils et leur soutien tout au long de notre travail.

Nos vifs remerciements vont également aux membres de Jury, devant qui nous avons l'honneur d'exposer notre travail.

On tient à remercier tous les enseignants qui ont assuré notre formation.

Enfin, on exprime notre reconnaissance envers toute notre famille, et tous ceux qui ont contribué de prés ou de loin pour réaliser ce travail.

Promotion : 2013/2014

Dédicaces

Je dédie ce modeste travail :

A la mémoire de mes chers grands parents paternels

A mes chers grands parents Maternels

A mes très chers parents que j'adore pour leur soutien tout au long de ma vie.

A mes chères sœurs Sarah et Aldjia.

A mon cher frère Moharezki

et à toute ma famille

A mes tantes et leurs époux

A mes oncles et leurs épouses

A mon binôme et toute ma promotion et tous mes amis

Amina.B

Dédicaces

Je dédie ce modeste travail :

A mes chers parents qui ont toujours étaient présents pour moi, et à qui je souhaite une bonne santé et une longue vie pleine de bonheur Nchallah.

A mes chers frères que j'aime énormément : Mohamed, Yacine et Alilou.

Et à mes adorables sœurs : Siham, Linda, son mari Fawzi et ses enfants Amine et Aya.

A mes amis : Imane, Fifi, Souhila, Mira, Razika, Ouiza, Houda, Amel, Mounir, Ghiles,Massi.

A mon binôme Amina.

A toute ma famille.

Je remercie tous ceux et celles qui m'ont aidé à réaliser ce travail.

Mariem.K

SOMMAIRE

CHAPITRE III : Datacenter et la sécurité physique

CHAPITRE IV : Réalisation de la solution Cloud Computing

ANNEXE « A »

ANNEXE « B »

ANNEXE « C »

Liste des Figures

Figures des Chapitres

Liste des Figures

Liste des Figures

Figures des Annexes

Introduction Générale

Au fur et à mesure que les systèmes informatiques évoluent, la demande en quantité d'espace de stockage, de convivialité et de simplicité dans le travail va grandissant. Il y a quelques années, les espaces de stockage réduits, les lignes de commandes et les systèmes complexes étaient le quotidien des employés d'entreprises. Les entreprises modernes traitent de grandes quantités d'informations aussi nombreuses que variées. Ainsi, elles ont besoin de grande capacité de stockage et d'une puissance de calcul élevé. Les ressources matérielles et logicielles nécessaires n'étant pas à la portée de toutes les entreprises.

Avec la généralisation d'Internet, le développement des réseaux haut débit, la location d'application et le paiement à l'usage résultat de l'apparition d'un nouveau concept : le « Cloud Compting ». Celui-ci consiste en une interconnexion et une coopération de ressources informatiques, situées dans diverses structures internes, externes ou mixte et dont le monde d'accès est basé sur les protocoles et standards Internet. Le Cloud Computing est devenu ainsi, le sujet le plus utilisé aujourd'hui dans le secteur des technologies de l'information. Il jouera un rôle de plus en plus important dans les opérations informatiques des entreprises au cours des années à venir.

Les services sur Internet sont en plein essor, le Cloud Computing permet de compléter le modèle traditionnel de stockage des données sur des PC et des serveurs. Il tend à améliorer l'expérience informatique en permettant aux utilisateurs d'accéder à des applications logicielles et à des données disponibles à la demande et hébergées dans des centres de données (Datacenter) ou dans les infrastructures internes d'une entreprise (Cloud privé). Les entreprises, dans ce cadre, n'auraient plus besoin de salles blanches ni de serveurs ni d'informaticiens. Toutes les applications sont louées et exécutées à travers un navigateur web.

L'objectif du Cloud Computing est de mettre à disposition des entreprises, des espaces de stockage en permettant dans un futur proche l'exploitation d'applications complexes, logiciels ou autre matériels. Cette technologie permettra une sécurité accrue pour les entreprises, qui seront bien moins exposés au risque lié à la perte de données. Avec le Cloud, pas d'investissement lourd dans le matériel, et la maintenance est externalisée, tout comme la gestion des sauvegardes.

Les solutions Cloud reposent sur des technologies de virtualisation et d'automatisation. Ce dernier est un concept beaucoup plus ancien qui consiste le socle du Cloud Computing. La virtualisation regroupe l'ensemble des techniques matérielles ou logicielles permettant de faire fonctionner, sur une seule machine physique, plusieurs configurations informatiques (systèmes d'exploitation, applications, mémoire vive, …) de manière à former plusieurs machines virtuelles qui reproduisent le comportement des machines physiques.

Notre mémoire est réparti en trois chapitres, dans le premier nous allons présenter l'étude de l'existant et ces critiques. Dans le deuxième chapitre nous expliquerons les différentes solutions proposées en citant la solution de Cloud Computing. Le troisième parle du Datacenter et ces différents équipements ainsi que la sécurité physique. Et en fin, nous terminerons notre mémoire par une conclusion générale ainsi que des perspectives ouvertes.

CHAPITRE I : Présentation du cadre d'étude

I.1. Introduction

L'expression « Cloud Computing », littéralement « nuage informatique », est apparue il y a deux ans et fait référence aux services et ressources informatiques pouvant être utilisés sur un réseau. L'idée de louer les technologies de l'information au lieu de les acheter n'est pas nouvelle.

Depuis 2008, un très grand nombre de contributions envahit le domaine de plus en plus populaire du « Cloud Computing ». Aujourd'hui, le « Cloud Computing » compte plus de 10,3 millions d'entrées dans Google. Sa portée est passée de simples services d'infrastructure tels que les ressources de stockage et de calcul à la mise à disposition d'applications. Cela signifie donc que les précurseurs tels que les prestataires de services d'application et les logiciels-services sont dorénavant inclus dans le « Cloud Computing ».

A la base de ces développements, se trouve l'éventuel passage des services informatiques des ordinateurs locaux vers l'Internet, ou, de manière plus générale, aux réseaux. Enfin, le « Cloud Computing » donne naissance à une idée déjà développée par Sun Microsystems, bien avant le succès du « nuage informatique » : le réseau est l'ordinateur.

C'est pourquoi le « Cloud Computing » possède de nombreux prédécesseurs et tout autant de tentatives de définitions. Le vaste monde des « nuages » compte de nombreux acteurs dont les fournisseurs de « Software as a Service » (le logiciel en tant que service), les prestataires de services d'externalisation et d'hébergement, les fournisseurs d'infrastructures réseaux et informatiques, et, plus particulièrement, les entreprises dont les noms sont étroitement liés au boom commercial de l'Internet.

Tous ces services regroupés donnent un aperçu de l'offre complète connue sous le nom de « Cloud Computing ». Tout ce qui s'est mis en place depuis un certain temps dans l'environnement grand-public de l'Internet intéresse clairement aujourd'hui les entreprises. Les développeurs, les jeunes entreprises mais également les grands comptes internationaux reconnaissent que le « Cloud Computing » constitue bien plus qu'un simple concept marketing. Derrière ce concept, il s'agit en effet d'offrir une solution qui permette aux utilisateurs d'accéder à des services à la demande, facturés sur l'usage. Les prestataires de services en réseaux y voient aussi des avantages puisque leurs ressources informatiques sont mieux utilisées, ce qui leur permet de réaliser des économies d'échelle supplémentaires.

De solides arguments soutiennent l'adoption du « Cloud Computing » : l'amélioration de la structure des coûts, une réaction plus rapide aux changements du marché et un potentiel d'augmentation de la productivité.

Le « Cloud Computing » offre la flexibilité tout en réduisant les coûts - avec pour avantage additionnel de s'inscrire dans une démarche de développement durable. Une grande partie du « Cloud Computing » n'est encore cependant qu'un projet. Il deviendra particulièrement intéressant si les grandes entreprises souhaitent profiter de ses possibilités. Enfin, des questions se posent quant à la sécurité et la qualité des services.

I.2. Problématique :

Le Cloud, c'est la promesse d'une informatique disponible tout le temps, accessible via le réseau, depuis n' importe où, sur et modulable en fonction de la demande.

Le Cloud Computing donne accès à des moyens de communication modernes et répond aux enjeux majeurs de l'entreprise :

- La réduction des coûts,
- La diminution des risques opérationnels,
- L'amélioration de la qualité de service,
- La facilitation de l'agilité d'un point de vue business.

Pour dresser un tableau exhaustif sur le Cloud Computing, il ne faut pas éluder certaines problématiques liées au modèle Cloud, qui demeurent des préoccupations majeures pour les entreprises :

- La sécurité et la confidentialité à problématique d'accessibilité continue du réseau
- La disparition de fonctionnalités
- L'intégration avec le système d'information existant
- La qualité de service et les engagements associés

De plus, les innovations en cours et les retours d'expériences largement positifs, qui abondent de nombreux clients, sont de nature à conduire les entreprises à envisager prochainement leur passage au Cloud Computing.

I.3. Etude de l'Existant :

I.3.1. Introduction :

L'étude de l'existant, point clé de notre démarche, est une étape essentielle qui vise à représenter l'architecture de notre travail, qui présente une architecture d'un site web d'un marchand de commerce électronique. Nous porterons une attention particulière sur le service où sera implémentée notre solution.

I.3.2. Objectif de l'Etude :

Le but de la thèse est de découvrir

- les avantages et les inconvénients dans des respects avec le coût, la sécurité des informations et la disponibilité de données.
- Comprendre le fonctionnement des réseaux de notre architecture.
- Présentation du réseau « LAN, WAN» de l'architecture.
- Déceler les anomalies, pouvant représenter un réel handicape pour le bon fonctionnement réseau du site.
- Proposer des solutions aux défaillances relevées.

I.3.3. L'architecture de l'entreprise :

- On va présenter l'architecture technique d'un site intranet puis l'architecture d'un site évolué d'un marchand de commerce électronique, puis on se conduit vers l'architecture Cloud Computing.

Le principe de base d'un site web :

Le mécanisme de base est très simple. Il est identique sur le réseau de l'entreprise (on parle d'intranet) et sur le réseau internet.

Figure I.1 : Le principe de base d'un site web.

Un utilisateur utilise un navigateur internet, il envoie une requête vers un site WEB. Le serveur de traitement reçoit la requête, il interroge la base de données, il construit une page HTML avec les données, puis il répond à l'utilisateur le résultat final. Ce principe de base est multiplié pour chaque utilisateur à l'infini, à chaque consultation d'une page internet.

Architecture d'un site web simple:

La construction d'un site WEB classique répond à des exigences simples.

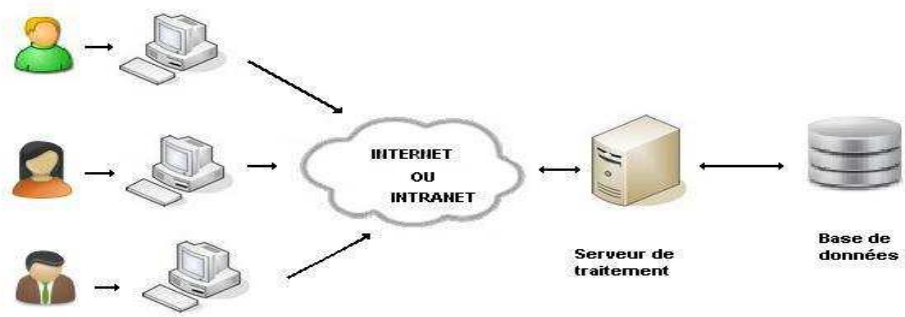


Figure I.2: Architecture d'un site web.

En simplifiant à l'extrême, nous avons besoin d'un serveur de traitement et d'une base de données. Cette architecture est très simple, elle est peu onéreuse. Elle répond à de faible sollicitation. Pour donner un ordre d'idée, nous envisageons 200 utilisateurs au maximum. La construction, la maintenance, la supervision des serveurs est simple.

Architecture d'un site web évolué :

Le site web gagne en popularité, le nombre d'utilisateurs croît fortement. Nous avons une population de 5 000 utilisateurs potentiels. Je prends le cas du site d'un marchand de commerce électronique, (par exemple une librairie en ligne). Le marchand est obligé d'avoir une infrastructure importante pour répondre aux besoins de ses clients actuels et futurs. Le nombre de client est aléatoire (les vacances, la nuit, les goûts). Malgré tout, son site internet doit tourner 24h sur 24h et être dimensionné pour accueillir le plus grand nombre.

L'architecture grossit pour répondre aux besoins.

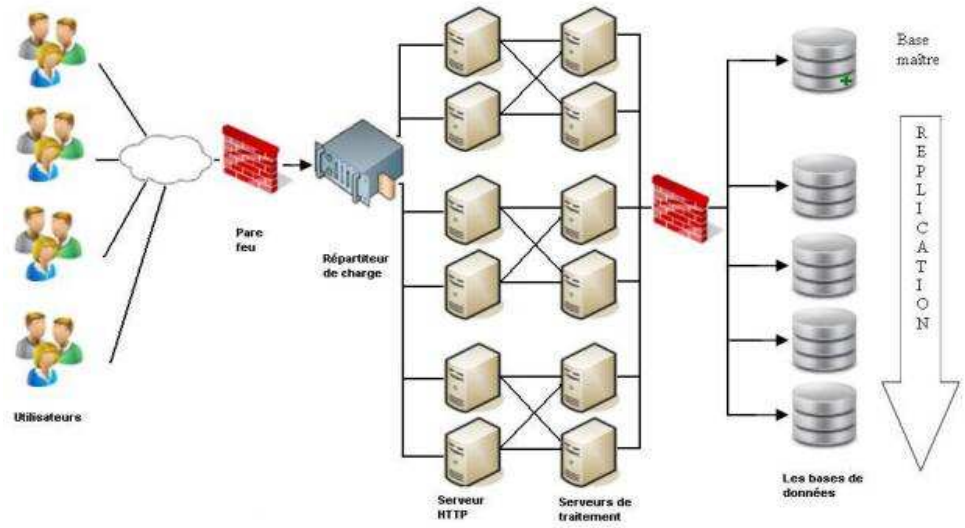


Figure I.3 : Architecture d'un site web évolué.

Tous les composants sont doublés (redondés) pour répondre aux problèmes de panne informatique. On ajoute de nombreux serveurs de traitement, on duplique les bases de données, on crée une base de données maitre, et des bases de données filles. On ajoute des serveurs de pages statiques (HTTP), pour soulager les serveurs de traitement. On ajoute des répartiteurs, pour répartir les charges sur les divers serveurs. Ainsi, de suite.

Les menaces sécurité sont plus importantes, on met en place des pares feux (firewall) pour contrôler et vérifier les risques d'intrusion.

Notre architecture évoluée répond aux sollicitations de plusieurs centaines d'utilisateurs.

La maintenance, la supervision des machines est une opération beaucoup plus complexe. La complexité grossit en fonction du nombre de machine, du nombre de composant, du nombre de programme informatique, de la répartition de la charge, des traitements en parallèles.

L'architecture doit être pensée, câblée, testée, validée, puis éprouvée. Elle nécessite un savoir faire important.

L'ajout d'une nouvelle machine, d'un nouveau serveur permet d'accroitre le nombre d'utilisateurs (clients) pouvant se connecter sur le site internet. Des nouvelles contraintes apparaissent, des goulots d'étranglement, qui nécessitent des nouveaux réglages. Ils sont levés soit par le matériel (hardware), soit par le logiciel, et par la manière de construire le logiciel

- **Le Cloud Computing** a été pensé à partir des retours d'expérience sur les architectures évoluées. L'architecture franchit un nouveau stade de complexité. Le principe de base du fonctionnement d'un site WEB reste le même. Dans le Cloud Computing, on ajoute la possibilité d'ajouter des nouvelles machines à la volée, en fonction des besoins. On cherche par tous les moyens à conserver des bonnes performances pour les utilisateurs et une solution exploitable techniquement pour les administrateurs. On regarde les entrées – sorties pour déterminer les besoins.

Le défi : Construire une architecture évoluée permettant de supporter 100 000 utilisateurs, voir plus, avec beaucoup de traitement, des grosses bases de données et de l'espace de stockage. Le Cloud doit répondre à un cahier des charges important, à des problématiques de temps d'accès. Le site internet doit être rapide, performant, agréable à utiliser.

Les entreprises se sont lancées dans la construction d'énorme Datacenter (centre de traitement informatique), pour centraliser les machines, pour faire des économies d'échelle (personnel, matériel, refroidissement) et pour fournir des débits énormes en sortie. Nous assistons à une concentration de puissance sans précédent. L'informatique de demain se joue dans le gigantisme des Datacenter et leur utilisation.

Prenons un exemple :

La société **Google** gère des millions d'index de mot, pour son moteur de recherche. Tous les jours, des automates scrutent des millions de page HTML, et créent des index. Les algorithmes de recherche sont connus, tout le monde peut créer son propre algorithme de recherche. La complexité de Google ne réside pas dans l'algorithme, elle réside dans le maintien, la supervision, l'administration de plusieurs milliers de machine, de serveur de part le monde. C'est l'infrastructure machine, l'architecture technique et les services d'exploitation, de supervision, d'administration mis en place qui font la différence. Les entreprises se sont lancées dans la course à l'industrialisation (à l'armement), pour conquérir le marché, une place au soleil dans la nouvelle économie.

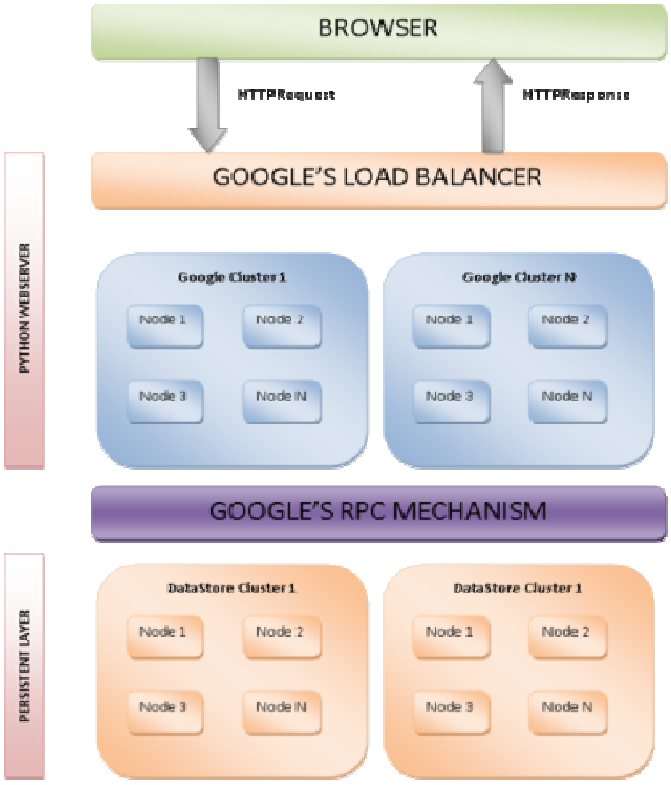


Figure I.4: Architecture Cloud Computing de Google.

Les architectures **Cloud Computing** sont particulières, et la course au part de marché est d'autant plus intéressante. Nous aborderons les détails des architectures Cloud par la suite.

Reprenant les grandes briques de la première partie, il complète l'architecture du site web de commerce électronique, et présente la notion de collaboration et de partenariat avec un acteur externe (via un tunnel VPN).

Nous allons aborder les échanges entrants et sortants nécessaires avec les partenaires, les fournisseurs, et les clients de l'entreprise.

La dernière partie sera consacrée à l'hébergement de l'infrastructure de notre site de commerce électronique chez un partenaire Cloud. Nous allons parler de l'hébergement d'infrastructure en tant que service (IAAS), des avantages, des inconvénients et des questions à se poser.

De nos jours les entreprises, les **systèmes d'information** (SI) sont de plus en plus interconnectés. Une entreprise communique avec de nombreux partenaires, fournisseurs et clients. Le SI est de plus en plus souvent ouvert sur le monde extérieur.

On va aborder la notion du raccordement des réseaux informatiques, cette notion est valable pour tous les types d'infrastructures informatiques (les sites web, la messagerie, la bureautique, etc.). Autour d'un site web, on parle de flux http, de web service, etc.

C'est quoi un tunnel VPN ?

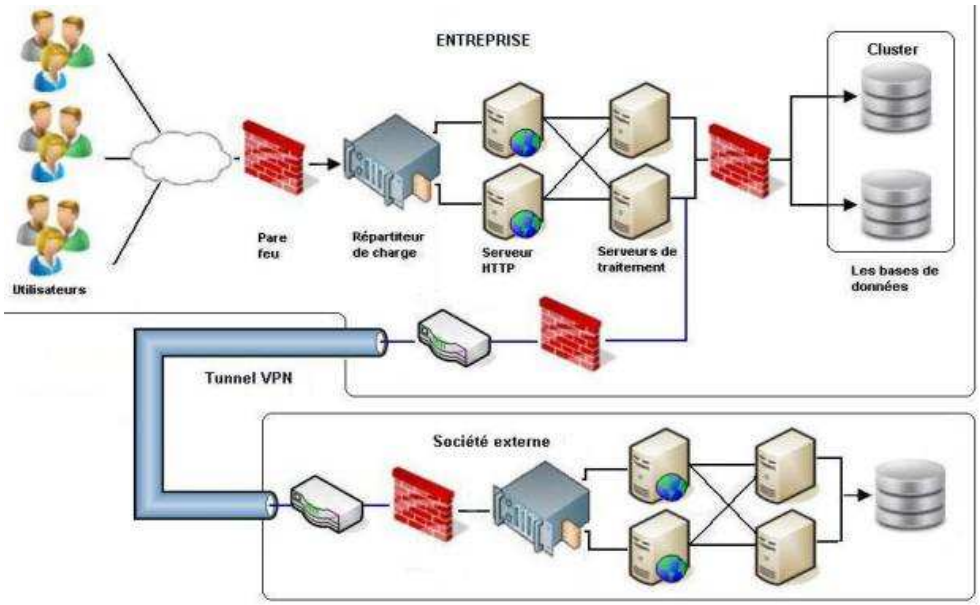


Figure I.5 : Réseau privé virtuel (VPN) entre l'entreprise et société externe.

.

Une société protège les accès vers son informatique, via diverses méthodes. Les plus simples font appel à des routeurs et des pares feu. L'entreprise va créer un réseau privé virtuel entre elle et l'entreprise distante, à l'abri des regards, avec la possibilité de sécurisé les données.

Le tunnel VPN (réseau Privé virtuel, *Virtual Private Network* en anglais) est un moyen de relier le réseau d'une entreprise avec une autre entreprise.

Le VPN garantit la sécurité et la confidentialité des échanges entre les deux entreprises, le pare feu garantit la sécurité des accès et des données au sein d'une infrastructure.

L'architecture de notre entreprise :

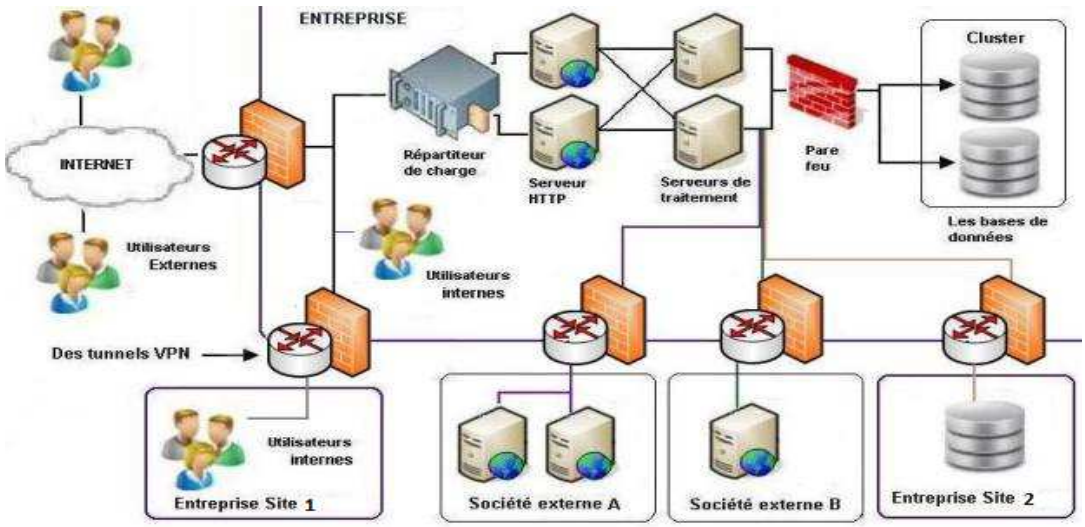


Figure I.6 : L'architecture de notre entreprise.

Une entreprise communique avec de nombreux partenaires, fournisseurs et clients. Elle utilise des traitements informatiques. Elle échange des informations avec des sociétés externes et des sites distants.

Le schéma ci-dessus présente des flux sortants. Afin de simplifier, le schéma, on a remplacé l'ensemble des tunnels VPN, pares feu, routeurs par des interconnexions. Chaque entreprise décide de la construction des interconnexions et gère des contrats de confidentialité, des politiques d'accès et de droit.

Dans l'exemple ci-dessus, l'entreprise de commerce électronique, elle dispose :

- **d'un site de rédaction sur site1**:

  1- **rédacteurs web :** est un des nouveaux métiers liés à l'internet. Ce métier consiste à produire des contenus rédactionnels adaptés au web

  2- **pigistes :** est un journaliste rémunéré à la tâche (par exemple au nombre de caractères ou de pages pour un rédacteur, à la durée dans l'audiovisuel

  3- **concepteurs graphiques :** Le concepteur graphique multimédia s'occupe de toute l'illustration graphique d'un produit ou service multimédia. Il peut intervenir à différents stades du projet

- d'un site de sauvegarde (base de données) sur site 2.

Elle passe des commandes à une société externe A, elle utilise les services bancaire d'une autre société (B) ou d'une Banque.

Le graphique ci-dessus, présente uniquement l'informatique lié au site de commerce électronique. Dans la réalité, le système d'information d'une entreprise est beaucoup plus vaste (l'informatique du service comptable, le service ressource humaine, etc.).

Une entreprise nomme un responsable de la sécurité de Système d'information (RSSI), qui devient le garant du bon fonctionnement et de la cohésion du réseau de l'entreprise.

Dans la première entreprise, l'entreprise est construite, bâtie autour du noyau, autour du site web (de commerce électronique) et de son informatique. Le site est beaucoup plus grand. L'informatique représente une large part de l'activité de l'entreprise. Nous avons des chefs de projets, des ingénieurs, des analystes, des experts, des techniciens réseaux, etc. Propres à l'entreprise.

I.3.4. Critiques de l'Existant:

I.3.4.1. L'antivirus et pare feu PIX:

A sa sortie le PIX, un des premiers sur le marché, était un excellent firewall mais le paysage depuis la sécurité à bien changé. Aujourd'hui, pour protéger un réseau un PIX n'est plus suffisant au vu du nombre de type d'attaques possibles comme les virus, les vers, ainsi que les applications non désirées (P2P, jeux, messageries instantanée). C'est pour cela que la gamme PIX a été suspendue en juillet 2008.

Figure I.7 : Pare feu PIX

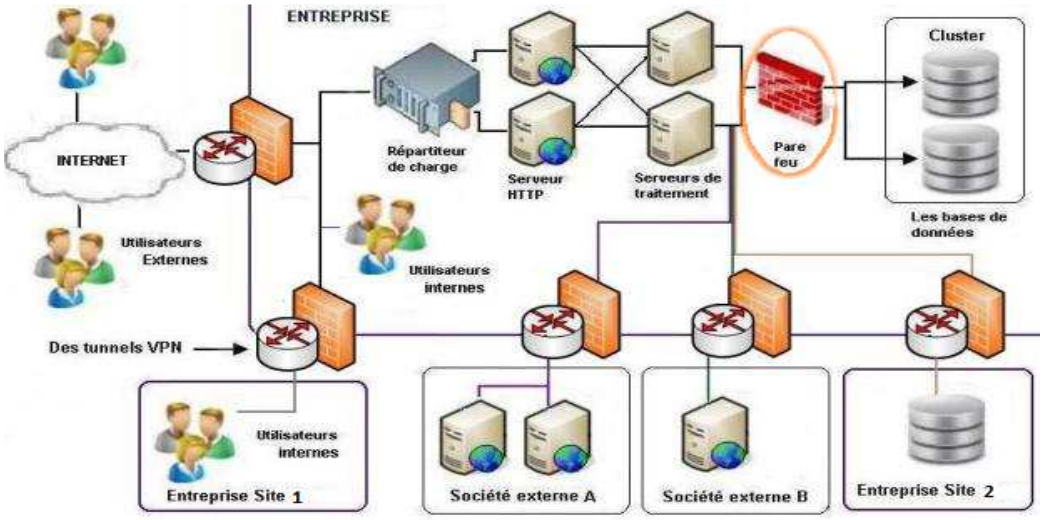


Figure I.8 : la base de données de l'entreprise protégée par un pare feu PIX

I.3.4.2. problème de sauvegardes :

Si la plupart des systèmes de stockage en ligne (Cloud) proposent des sauvegardes, les données situées sur votre poste de bureau sont souvent conservées sur un seul disque. Que se passe-t-il si ce disque dur ne répond plus, en cas d'incendie ou d'un simple vol de votre portable ?

- Il faut avoir une sauvegarde séparée du lieu de stockage de vos données. Les risques sont généralement liés à la conservation de toutes vos données dans un même lieu.
- Plusieurs niveaux de sauvegardes peuvent être utiles : Certaines vous permettent de revenir en arrière de manière instantanée, d'autres de revenir sur des périodes plus longues (24h, semaine, mois...). Cette sauvegarde peut être utilisée suite à une erreur humaine, un bug, etc...

I.3.4.3. Vulnérabilités De Configuration Et De Gestion De Pare-feux

a. ICMP et SNMP Permis:

ICMP et SNMP sont permis à travers toutes les pattes du pare-feu. Ceci permet d'identifier tout les systèmes qui se trouvent derrière les pattes du pare-feu, les chaines faibles de communauté SNMP (SNMP Community String), et les services qui sont démarrés sur les hôtes. Ces deux protocoles doivent être filtrés et l'utilisation doit être restreinte aux stations de gestion du réseau.

b. Dépendance sur le Fournisseur pour la Gestion et Configuration:

Cette entreprise dépend sur le fournisseur du pare-feu pour la gestion et la configuration de l'appareil. Les consultants ont remarqués qu'il existe un manque de compréhension vis-à-vis de la configuration du pare-feu et de ce qui est permis ou non. De même, la présence du fournisseur était toujours nécessaire pour répondre aux questions techniques des consultants.

Ce pare-feu est le composant le plus important de l'architecture de sécurité actuelle des réseaux des sites web. La dépendance excessive vis-à-vis du fournisseur pour la gestion et configuration du pare-feu a un effet négatif sur la réponse aux incidents du site comme le fournisseur doit nécessairement être contacté pour assurer une bonne configuration.

c. Trafique Sortant Non Restreint:

Les consultants ont trouvé que les règles du pare-feu ne n'interdit pas aux IP internes, ou celles de la DMZ, de se connecter au réseau externe. Ceci peut permettre a un intrus d'initier un « reverse tunnel » de l'intérieur du site, et ainsi lui permettent de dévier les règles « externes » du pare-feu.

d. Manque de Contrôle de Changement :

Les règles du pare-feu ont été modifiées instantanément durant la revue du pare-feu. Même, pendant la revue, il a été découvert que certains ports, qui normalement doivent être fermés, sont ouverts. La dépendance complète sur le fournisseur, l'existence d'un compte partagé, et le manque de documentation des changements effectués, constituent une vulnérabilité sérieuse du mécanisme de défense du site. Il se peut que des ports soient ouverts pour but de tester et que les administrateurs oublient de les fermer, et ainsi les biens protégés par le pare-feu seront exposés.

I.3.4.4. Mots de Passe Faibles :

Les consultants ont pu obtenir un accès administratif à deux routeurs car ils étaient protégés par des mots de passe faibles. Les intrus auront ainsi des diverses options qui leur permettront de causer des dommages et d'interrompre les activités métier. Par exemple, un intrus peut :

- Causer un déni de service à travers la falsification (Tampering) des tables de routage.
- Exécution d'attaques d' « homme au milieu » (man-in-the-middle) à travers la modification des tables de routages, qui peut causer une divulgation des informations confidentielles.
- Blocage de l'accès des administrateurs aux routeurs et interruptions de la productivité.

Cette vulnérabilité existe à cause du manque de lignes directrices de sécurité de mot de passe, et la mauvaise appréciation des conséquences de l'utilisation de mots de passe faibles.

I.3.4.5. Transfert Non Chiffré Des Données Confidentielles :

La réplication des données entre le site de production de site de Nantes et le site de Rouen est effectuée à travers un lien non chiffré fourni par l'entreprise. Ceci peut mener à la révélation d'informations confidentielles étant donné que rien n'assure que l'entreprise met en œuvre les mesures nécessaires pour sécuriser son environnement.

La communication avec les sièges du site web et les autres sites est également non chiffrée. Des mesures doivent être mises en place pour protéger cette connexion.

I.3.4.6. Récupération des données :

Lorsque les entreprises commencent à s'appuyer sur les services de Cloud Computing, elles n'ont plus besoin de programmes complexes de récupération des données. Les fournisseurs de Cloud Computing se chargent de la plupart de ces tâches et ils le font plus vite.

Une étude menée a montré que les entreprises qui utilisaient le Cloud parvenaient à résoudre leurs problèmes en 2,1 heures en moyenne, soit presque quatre fois plus rapidement que les entreprises qui n'y avaient pas recours (8 heures).

La même étude a également démontré que les petites et moyennes entreprises bénéficiaient du meilleur temps de récupération de données, mettant presque deux fois moins de temps que les grandes entreprises.

I.4. Conclusion

La complexité des attaques, la facilité de se renseigner sur les logiciels et les moyens d'intrusions via le net, font que n'importe qu'elle architecture aussi sécurisée soit-elle peut être confrontée à d'innombrables défaillances. C'est le cas de notre architecture, qui doit être protégée des attaques informatiques pouvant nuire à son bon fonctionnement. Mais comme nous l'avons vu, en nous basant uniquement sur les documents fournis sur l'infrastructure de l'entreprise, il existe diverses vulnérabilités que nous avons découvertes et expliquées dans ce chapitre. Nous tenons à souligner que cette liste de failles n'est pas exhaustive car nous nous sommes limitées aux données qui ont été mises à notre disposition.

Apres avoir examiné les différentes failles, nous avons proposé des solutions qui permettront de pallier ces différentes vulnérabilités qu'elles soient réseaux ou systèmes. Ce que nous pouvons affirmer après notre étude c'est qu'il faut mettre à jour l'infrastructure réseau (réseau et systèmes) avec des moyens récents et effectuer des tests en tenant compte des nouvelles techniques de piratages pour optimiser les chances de sécurités.

CHAPITRE II : Etudes et Conceptions

II.1. Introduction :

Virus, pourriels, chevaux de Troie, logiciels espions... Les types d'infections qui s'attaquent au réseau informatique sont extrêmement variés. Heureusement, différentes solutions de sécurité permettent aux entreprises de bien se protéger.

La sécurité doit être envisagée dès la conception du site et les dispositifs de protection mis à jour régulièrement. L'analyse et la mise en place de solutions sont incontournables car la cybercriminalité augmente.

L'infrastructure d'un site internet est complexe. Elle comprend plusieurs serveurs qui hébergent différentes bases de données. Chacune se compose de plusieurs tables (dédiée aux clients, au catalogue, etc.). Pour sécuriser l'ensemble, mieux vaut avoir cette complexité à l'esprit et intégrer la problématique dès la conception de l'infrastructure.

Les serveurs en mutualisé des hébergeurs devraient être relativement sécurisés et disposer d'outils qui lui permettent de bloquer certains comportements suspects. Il est donc préférable de prévenir ce type de piratage. En tant que client et utilisateur, nous devons éviter la suspension de notre compte si nous sommes la victime d'une attaque.

II.2. Les Solutions Proposées :

Les exigences de la sécurité de l'information au sein des organisations ont conduit à deux changements majeurs au cours des dernières décennies. Avant l'usage généralisé d'équipements informatiques, la sécurité de l'information était assurée par des moyens physiques (classeurs fermés par un cadenas) ou administratifs (examen systématique des candidats au cours de leur recrutement).

Avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour protéger fichiers et autres informations stockées est devenu évident. Ce besoin est accentué pour un système accessible via un téléphone public ou un réseau de données. On donne à cette collection d'outils conçus pour protéger des données et contrecarrer les pirates le nom de sécurité informatique.

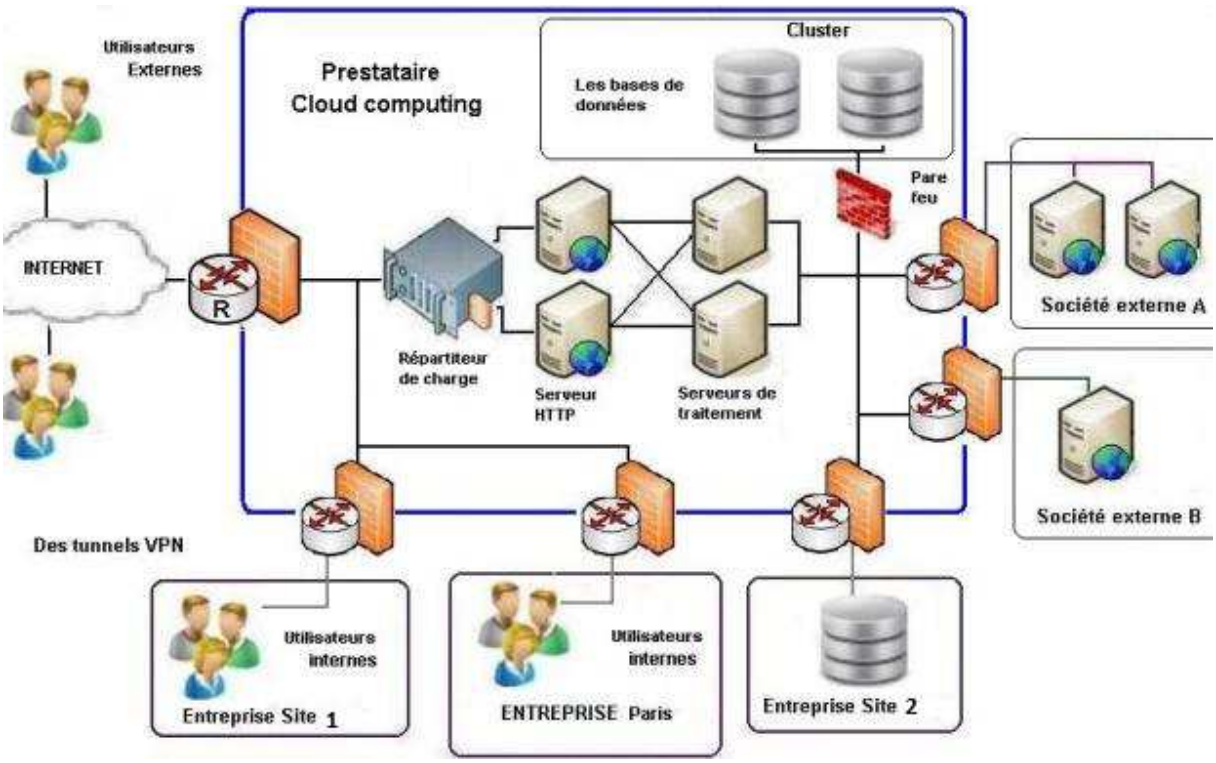


Figure II.1 : La nouvelle architecture avec le Cloud Computing.

Les objectifs d'une politique de sécurité sont de garantir la sécurité des informations et du réseau de l'entreprise. Ces impératifs peuvent être définis à plusieurs niveaux:

- ***Authentification du client :***

Le service d'authentification permet évidemment d'assurer l'authenticité d'une communication. Dans le cas d'un message élémentaire, tel un signal d'avertissement, d'alarme, ou un ordre de tir, la fonction du service d'authentification est d'assurer le destinataire que le message a bien pour origine la source dont il prétend être issu. Dans le cas d'une interaction suivie, telle une connexion d'un terminal à un serveur, deux aspects sont concernés. En premier lieu, lors de l'initialisation de la connexion, il assure que les deux entités sont authentiques (c'est-à-dire, que chaque entité est celle qu'elle dit être). Ensuite, le service dont assurer que la connexion n'est pas perturbée par une tierce partie qui pourrait se faire passer pour une des deux entités légitimes à des fins de transmissions ou de réceptions non autorisées.

- ***Confidentialité des échanges :***

La confidentialité est la protection contre les attaques passives des données transmises. Plusieurs niveaux de protection de la confidentialité sont envisageables. Le service le plus général protège toutes les données transmises entre deux utilisateurs pendant une période donnée. Des formes restreintes de ce service peuvent également être définies, incluant la protection d'un message élémentaire ou même de champs spécifiques à l'intérieur d'un message. Un autre aspect de la confidentialité est la protection du flot de trafic contre l'analyse. Cela requiert qu'un attaquant ne puisse observer les sources et destinations, les fréquences, longueurs ou autres caractéristiques du trafic existant sur un équipement de communication.

- ***Intégrité :***

À l'instar de la confidentialité, l'intégrité s'applique à un flux de messages, un seul message, ou à certains champs à l'intérieur d'un message. Là encore, la meilleure approche est une protection totale du flux. Un service d'intégrité orienté connexion, traitant un flot de messages, assure que les messages sont reçus aussitôt qu'envoyés, sans duplication, insertion, modification, réorganisation ou répétition. La destruction de données est également traitée par ce service. Ainsi, un service d'intégrité orienté connexion concerne à la fois la modification de flux de messages et le refus de service. D'un autre côté, un service d'intégrité non orienté connexion, traitant des messages individuels sans regard sur un contexte plus large, fournit généralement une protection contre la seule modification de message.

- ***Non Répudiation :***

La non-répudiation empêche tant l'expéditeur que le receveur de nier avoir transmis ou reçu un message. Ainsi, lorsqu'un message est envoyé, le receveur peut prouver que le message a bien été envoyé par l'expéditeur prétendu. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le message a bien été reçu par le receveur prétendu.

- ***Contrôle d'accès :***

Dans le contexte de la sécurité des réseaux, le contrôle d'accès est la faculté de limiter et de contrôler l'accès à des systèmes et des applications via des maillons de communications. Pour accomplir ce contrôle, chaque entité essayant d'obtenir un accès doit d'abord être authentifiée, ou s'authentifier, de telle sorte que les droits d'accès puissent être adaptés à son cas.

- ***Disponibilité :***

De nombreuses attaques peuvent résulter en une perte ou une réduction de la disponibilité d'un service ou d'un système. Certaines de ces attaques sont susceptibles d'être l'objet de contre-mesures automatiques, telle que l'authentification et le chiffrement, alors que d'autres exigent une action humaine pour prévenir ou se rétablir de la perte de disponibilité des éléments d'un système.

II.2.1. Quelques Solutions Proposées :

a) Remplacer le PIX par ASA :

Après que le firewall PIX été suspendu, une autre gamme dite ASA a vu le jour. Dans l'impossibilité d'effectuer une mise à jour du firewall PIX qui n'existe plus, il doit être remplacé par un autre Firewall. Nous proposons le Firewall ASA. Ce dernier regroupe trois éléments de la gamme Cisco en une seule plate-forme, le Cisco PIX firewall, le Cisco VPN, le Cisco IPS Sensor et le module qui le différencie vraiment du PIX, alors que le PIX n'était qu'un firewall avec quelques fonctions VPN et sonde IPS assez limitées.

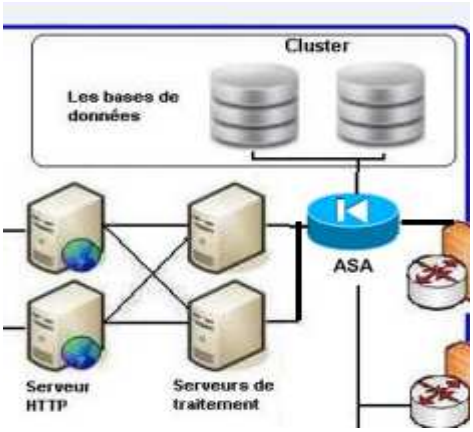


Figure II.2 : Le remplacement de PIX par ASA.

b) l'ajout de firewall TMG :

Forefront Threat Management Gateway est une passerelle de haute sécurité qui protège contre les menaces en provenance d'Internet, tout en offrant à nos utilisateurs un accès à distance rapide et sécurisé aux données et aux applications.

La solution Forefront Threat Management Gateway inclut deux composants :

- **Forefront Threat Management Gateway Server**, qui fournit un filtrage d'url, une protection anti malware, un pare feu agissant au niveau applicatif et au niveau du réseau, une protection des flux http et https, une passerelle VPN et un reverse proxy (publication Web sécurisée basique).
- **Forefront Threat Management Gateway Web Protection Service**, qui fournit des mises à jour continuelles pour le filtrage des malwares et l'accès aux données concernant le filtrage d'url (disponible uniquement avec la souscription à un abonnement Web Protection service).

Bénéfices du produit : Voici quelques-uns des avantages proposés par Forefront Threat Management Gateway 2010 :

protection complète	Sécurité intégrée	Gestion simplifiée
▪ Multiples sources de données concernant le filtrage d'url pour améliorer le blocage des sites malveillants. ▪ Moteurs antimalwares performants. ▪ Prévention des intrusions basée l'exploitation des vulnérabilités. ▪ Garde les technologies éprouvées de protection de réseau présentes dans ISA Server 2006.	▪ De multiples technologies de sécurité Web en une seule solution ▪ Authentification et mises à jour continuelles	▪ Interface dédiée pour gérer les politiques de sécurité web Rapports complets et détaillés

Threat Management Gateway (TMG) a plusieurs fonctionnalité pour sécuriser un réseaux qui sont :

*par feu
*VPN (site a site et accès a distance)
*proxy web
*protection anti-malware
*sécurité des courriels électroniques

c) La sécurisation des points d'entrées réseau :

Nous proposons des solutions pour sécuriser les points d'entrées selon la chronologie citée dans les vulnérabilités liées à ce titre.

La solution à apporter pour sécuriser le deuxième point d'entrée que constitue PIX, remplacé par TMG, est la création d'une DMZ.

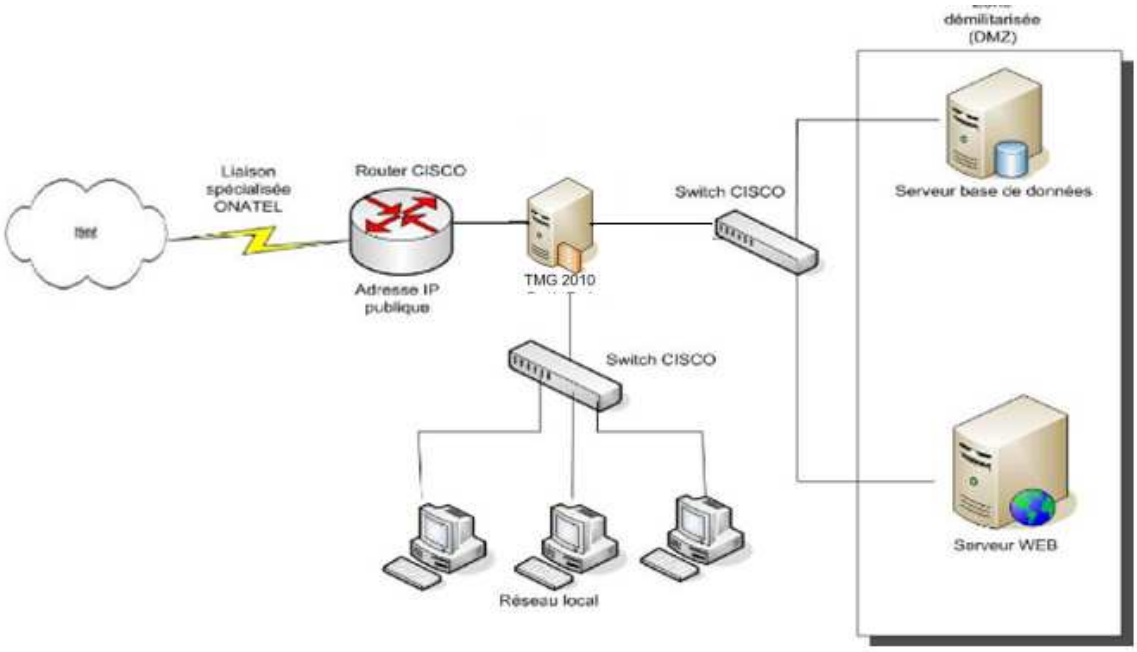


Figure II.3 : La création de la DMZ TMG.

Cette DMZ englobera, un serveur base de donnée et un serveur Web.

d) Solutions de configuration et de gestion du firewall :

1. La formation des équipes de travail :

Afin de remédier au problème de la dépendance du fournisseur pour la configuration et la gestion des firewalls, nous suggérons d'organiser périodiquement des formations pour améliorer les compétences des équipes de travail et les connaissances sur les technologies actuellement utilisées au niveau de l'infrastructure de l'entreprise.

2. La restriction du trafic sortant :

Les règles du firewall doivent être bien réfléchies pour bien exploiter ses fonctionnalités, comme exemple, la configuration des ACL, de sorte à limiter le trafic sortant du réseau interne vers le réseau externe.

3. L'utilisation d'un seul compte pour la gestion du firewall et la documentation de changement :

Pour ne pas permettre des accès non autorisés, des changements non contrôlés et l'impossibilité de surveiller des activités de l'administrateur, la solution proposée est de désigner un seul administrateur pour gérer le compte, et s'il a besoin de subordonnés ils doivent avoir chacun leurs comptes différents de l'administrateur pour exécuter les charges de gestion.

Pour pallier au manque de documentations sur les changements effectués, tous changement dans la configuration du firewall doit être documenté et archivé par l'administrateur. Les modifications doivent être autorisées si les conditions suivantes sont assurées :

- ✓ Le changement a été examiné méthodiquement et avec succès.
- ✓ Les impacts du changement sur le fonctionnement du système ont été testés.
- ✓ Les impacts du changement sur la sécurité du système ont été vérifiés.
- ✓ Toutes les entités affectées par le changement ont été informées.

e) Utilisation De Protocoles Sécurisés De Gestion :

Des protocoles sécurisés comme SSH et HTTPS devraient être utilisés pour gérer les dispositifs de réseau au lieu des protocoles non sécurisés actuellement utilisés comme HTTP et Telnet. Ces protocoles chiffrés rendront beaucoup plus difficile qu'une personne écoutant sur le réseau puisse deviner les mots de passe administratifs et toute autre information importante.

f) Désactivation Des Services Non Utilisé :

Les seuls services qui doivent être activés sur les dispositifs réseau sont les services qui sont nécessaire pour le fonctionnement exigé. Tous autres service, sécurisé ou non, devrait être désactivé.

g) Utilisation De Mots De Passe et Des Communautés SMNP Forts :

Les mots de passe sont le mécanisme le plus généralement utilisé pour le contrôle d'accès. Ils sont typiquement la dernière ligne de la défense qui protège un dispositif. Il est essentiel que des mots de passe complexes avec au moins 7 caractères alphanumériques soient utilisés pour sécuriser toutes les infrastructures de réseau.

h) Cryptage :

Les mesures recommandées pour le chiffrement des liens sont les suivants :

Il est conseilles que des appareils de protection unifiée UTM soient installés dans les sièges. Ces appareils contiennent plusieurs modules de sécurité. L'entreprise a besoin des modules suivant :

- Passerelle VPN
- Pare-feu

Le pare-feu sera utilisé pour protéger le réseau ……. Le module VPN sera utilisé pour créer un lien VPN et ainsi pour chiffrer les liens avec les sites 1et 2.

i) L'ajout des IDS et IPS :

Il est également plus possible de contenir les intrusions à quelques points du réseau. Prévention des intrusions est nécessaire tout au long de l'ensemble du réseau pour détecter et arrêter une attaque sur tous les points entrant et sortant.

Un réseau d'architecture changement de paradigme est nécessaire pour se défendre contre évolution rapide et l'évolution des menaces. Cela doit inclure la détection et de prévention des systèmes rentables, tels que les systèmes de détection d'intrusion (IDS) ou, les systèmes de prévention d'intrusion (IPS plus évolutives). L'architecture de réseau intègre ces solutions dans les points du réseau d'entrée et de sortie.

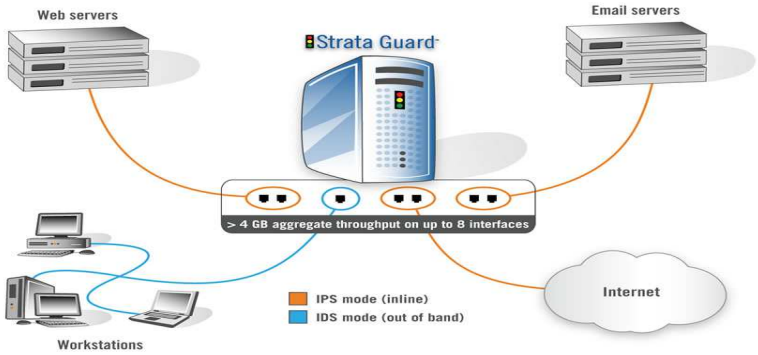


Figure II.4 : L'utilisation de l'IPS/IDS.

j) Serveur Radius :

RADIUS (Remote Authentication Dial-In User Service) est un protocole client/serveur destiné à permettre à des serveurs d'accès de communiquer avec une base de données centralisée regroupant en un point l'ensemble des utilisateurs distants. Ce serveur central (appelé serveur RADIUS) va authentifier ces utilisateurs, et leur autoriser l'accès à telle ou telle ressource. Une autre fonctionnalité importante d'un serveur RADIUS est la comptabilisation des informations concernant les utilisateurs distants.

Cependant, à l'exploitation, le protocole révèle non seulement des contraintes qui compliquent son déploiement, mais aussi des failles de sécurité inquiétantes. Ainsi, une étude récente réalisée par Infoguard, un cabinet d'experts américain, démontre que l'identifiant généré par le client, permettant au serveur Radius de reconnaître l'origine d'une requête, autant que le secret partagé, utilisé pour chiffrer et déchiffrer l'échange du mot de passe de l'utilisateur, sont vulnérables aux attaques de pirates chevronnés.

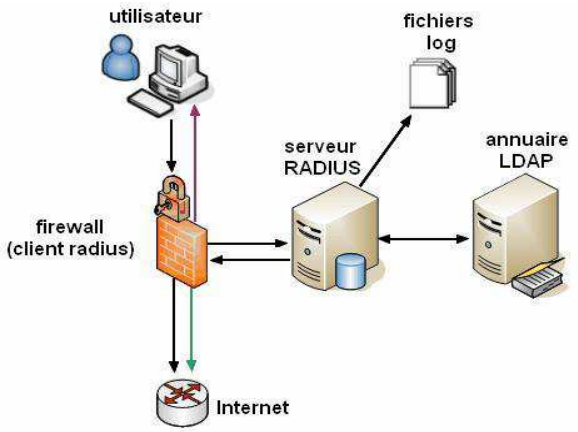


Figure II.5 : L'utilisation du serveur Radius.

k) Autorité de Certification :

Un *certificat* est un document électronique utilisé pour identifier un individu, un serveur, une entreprise ou toute autre entité et pour associer une clef publique à cette identité. Tout comme un permis de conduire, un passeport, ou tout autre moyen d'identification personnelle couramment utilisé, un certificat fournit généralement une preuve reconnue de l'identité de la personne. La cryptographie à clef publique utilise les certificats pour éviter les problèmes d'usurpation d'identité.

Les certificats hébergés sur un serveur peuvent également être installés sur les clients pour une sécurité théoriquement absolue.

En cryptographie, une **autorité de certification** ou **Certification Authority**(CA), est une entité qui émet des certificats numériques. Le certificat numérique atteste la propriété d'une clé publique par le sujet nommé du certificat. Cela permet d'autres (parties utilisatrices) de recourir à des signatures ou des affirmations faites par la clé privée qui correspond à la clé publique qui est certifié. Dans ce modèle de relations de confiance, un CA est un tiers de confiance qui est approuvé à la fois par le sujet (propriétaire) du certificat et la partie se fiant au certificat. CA sont caractéristiques de nombreuses infrastructures à clés publiques (ICP) des régimes.

Les certificats sécurisés sont généralement utilisés pour faire des connexions sécurisées sur un serveur sur Internet. Un certificat est requis pour éviter le cas où un tiers malveillant qui se trouve être sur le chemin vers le serveur cible prétend être la cible. Un tel scénario est communément appelé une attaque **man-in-the-middle** .Le client utilise le certificat de CA pour vérifier la signature CA sur le certificat de serveur, dans le cadre des contrôles avant d'établir une connexion sécurisée. Habituellement, un logiciel pour le client, par exemple, les navigateurs comprennent un ensemble de certificats de confiance. C'est logique dans la mesure où les utilisateurs ont besoin de faire confiance à leur logiciel client: Un client malveillant ou compromis peut sauter une vérification de sécurité et encore tromper les utilisateurs en leur faisant croire le contraire.

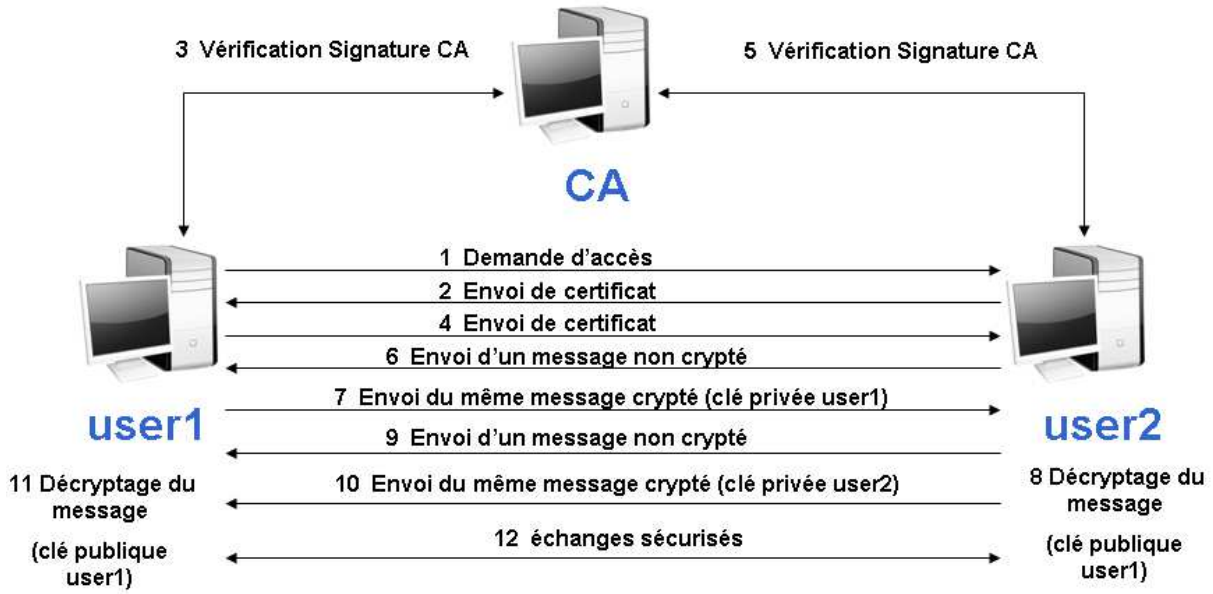


Figure II.6 : Authentification basée sur un Certificat.

k.1. Délivrance d'un certificat :

Une autorité de certification émet des certificats numériques qui contiennent une clé publique et l'identité du propriétaire. La clé privée correspondant n'est pas accessible au public, mais gardé secret par l'utilisateur final qui a généré la paire de clés. Le certificat est également une confirmation ou la validation par le CA que la clé publique contenue dans le certificat appartient à la personne, l'organisation, serveur ou autre entité mentionné dans le certificat. L'obligation d'un CA dans ces régimes est de vérifier les informations d'identification du demandeur, de sorte que les utilisateurs et les parties utilisatrices peuvent faire confiance aux informations dans les certificats de l'AC. CA utilisent une variété de standards et de tests à faire. En substance, l'autorité de certification est chargée de dire «oui, cette personne est bien ce qu'elle dit qu'elle est, et nous, le CA, certifie cela".

Si l'utilisateur fait confiance à la CA et peut vérifier la signature de l'autorité de certification, puis (s) il peut aussi supposer que d'une certaine clé publique appartient bien à celui qui est identifié dans le certificat.

l) Réseau de stockage SAN :

Un **réseau de zone de stockage** (**SAN**) est un réseau dédié qui permet d'accéder à, consolidé stockage de données au niveau bloc . SAN sont principalement utilisés pour améliorer les dispositifs de stockage tels que des baies de disques , les bibliothèques de bandes , et juke-box optiques , accessibles aux serveurs de sorte que les dispositifs apparaissent comme connectés localement dispositifs à la système d'exploitation . Un SAN a généralement son propre réseau de périphériques de stockage qui ne sont généralement pas accessibles via le réseau local (LAN) par d'autres appareils. Le coût et la complexité des réseaux SAN ont chuté au début des années 2000 à des niveaux permettant une plus large adoption dans les deux entreprises et les petites et les milieux d'affaires de taille moyenne.

Un SAN ne fournit pas de fichier abstraction, seules les opérations au niveau du bloc. Cependant, les systèmes de fichiers construits sur des SAN fournissent un accès au niveau du fichier, et sont connus comme *les systèmes de fichiers SAN* ou les systèmes de fichiers du disque partagé .

Partage stockage simplifie généralement l'administration du stockage et ajoute de la souplesse car les câbles et les périphériques de stockage ne doivent pas être déplacé physiquement à passer du stockage d'un serveur à un autre.

Les autres avantages comprennent la capacité de permettre aux serveurs de démarrer à partir du SAN lui-même. Cela permet un remplacement rapide et facile des serveurs défectueux depuis le SAN peut être reconfiguré afin qu'un serveur de remplacement peut utiliser le numéro d'unité logique du serveur défectueux. Bien que ce domaine de la technologie soit encore nouveau, beaucoup le considèrent comme étant l'avenir du centre de données de l'entreprise.

SAN ont aussi tendance à permettre à plus efficaces de reprise après sinistre processus. Un SAN pourrait s'étendre sur un emplacement distant contenant une matrice de stockage secondaire. Cela permet la réplication de stockage soit mis en œuvre par les contrôleurs de réseau de disques, par le logiciel de serveur, ou par des dispositifs spécialisés SAN. Depuis IP WAN sont souvent la méthode la moins coûteuse de transport longue distance, le Fibre Channel sur IP (FCIP de) et les protocoles iSCSI ont été développés pour permettre l'extension SAN sur des réseaux IP. La couche SCSI physique traditionnelle ne peut soutenir quelques mètres de distance - pas assez pour assurer la continuité des opérations en cas de catastrophe.

La consolidation économique des baies de disques a accéléré la promotion de plusieurs fonctionnalités, y compris E / S en cache, snapshots, et le clonage de volumes (Volumes de continuité de l'activité ou BCV)

m) Migration dans le Cloud Computing :

L'exemple ci dessous, représente l'entreprise, le site de commerce électronique migré dans le nuage (dans le Cloud Computing). Il focalise l'attention sur le prestataire "Cloud Computing". Nous avons conservé la même entreprise.

Pourquoi le Cloud ? C'est une bonne question.

Dans une entreprise, les flux des utilisateurs du site internet sont en évolution permanents. Les besoins et les usages fluctuent en permanence. Un responsable informatique est confronté au dilemme de l'achat d'une machine encore plus puissante pour accueillir encore plus de client. A partir d'un certain nombre d'utilisateur, il est obligé d'investir encore plus fortement sur d'autres machines et ainsi de suite. L'informatique n'évolue plus sur une seule grosse machine, mais sur un ensemble de machine. Les coûts explosent.

Le Cloud Computing est une solution plus flexible. Le site internet est hébergé sur une méga plateforme. Elle s'adapte à l'augmentation du nombre d'utilisateur, en fonction du besoin.

Le prestataire gère la sécurité des accès vers le site Cloud, il devient le garant du bon fonctionnement de l'infrastructure, des accès de l'entreprise vers le site depuis les divers sites, et des accès des prestataires. Il garantie la bonne exécution des traitements. Il s'engage à fournir des accès externes (internet) de qualité. La rémunération du prestataire est basée sur l'usage des ressources informatique.

Le Cloud, c'est la flexibilisation de la ressource informatique.

Il y a une autre tendance qui est importante, c'est l'industrialisation des traitements informatiques et la manipulation des données. De nos jours, on ne conçoit plus les programmes informatiques, les traitements comme il y a 10 ans. On parle de l'informatique disponible partout, depuis n' importe où, tout le temps. Petit à petit l'informatique est devient un centre de profit au lieu d'un centre de coût.

II.3. Le Cloud Computing :

II.3.1. Définition :

Le Cloud Computing est un modèle permettant de favoriser un accès ubiquitaire, commode et sur demande à un ensemble partagé de ressources informatiques configurables (par exemple, des réseaux, serveurs, ressources de stockage et logiciels) pouvant être déployées rapidement avec un minimum de gestion ou d'intervention de la part du prestataire de service.

Ce modèle, qui favorise l'accessibilité, comporte cinq caractéristiques essentielles, trois modèles de services et quatre modèles de déploiement.

Cloud ⟹ Convention graphique du domaine des TI consistant à représenter Internet sous forme de « nuage » dans les diagrammes de systèmes informatiques.

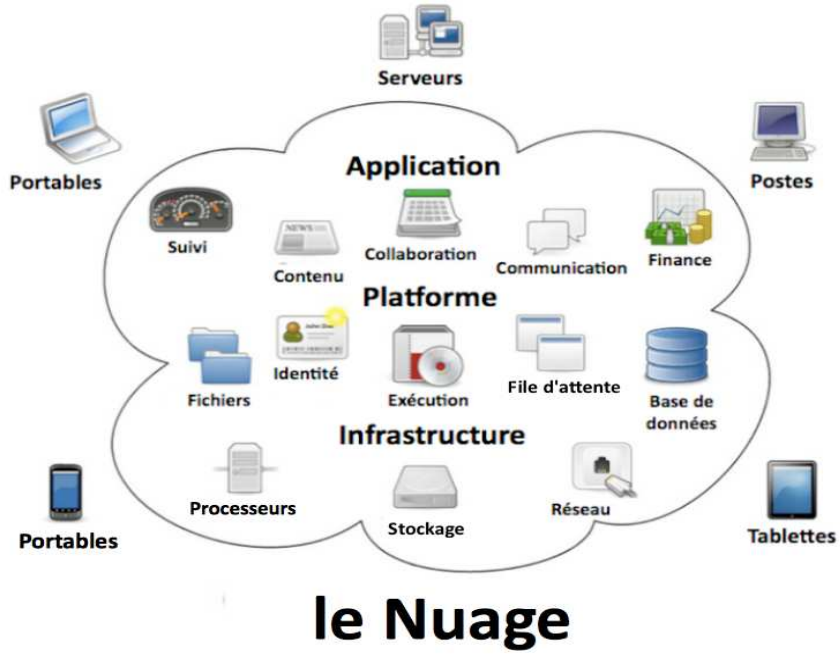


Figure II.7 : Le Cloud Computing.

II.3.2. Caractéristiques essentielles :

1. **Libre-service sur demande :** L'utilisateur peut accéder aux ressources informatiques - physiques et virtuelles - à tout moment et selon ses besoins et ce, sans intervention« humaine » de la part du prestataire du service Cloud Computing. Le stockage de données, le traitement informatique, la mémoire, la bande passante de réseau et les «appareils virtuels » sont des exemples de ces ressources.

2. **Accès ubiquitaire :** Les ressources informatiques sont accessibles en tout lieu, par Internet ou autre réseau de télécommunication, par l'intermédiaire de mécanisme d'accès usuels, même légers (fureteur, applications mobiles), et par l'entremise de multiples plateformes (ordinateurs portables, assistants numériques personnels ou téléphones cellulaires).

3. **Agrégation de ressources :** Les ressources informatiques sont mises à la disposition de plusieurs utilisateurs au moyen d'un modèle multi client (« colocalisation »). Ces ressources peuvent ainsi être affectées et réaffectées aux utilisateurs en fonction de la demande. L'utilisateur n'a habituellement ni connaissance ni contrôle du lieu exact des ressources qui lui sont fournies; il peut toutefois préciser le lieu à un plus haut niveau d'abstraction (par exemple, le lieu géographique ou le centre de données).

4. **Ajustements rapides :** Les ressources peuvent être ajustées rapidement – voire instantanément - tant à la hausse qu'à la baisse, selon les besoins de l'utilisateur. Aux yeux de l'utilisateur, les capacités disponibles paraissent souvent illimitées, et il peut en acquérir à tout moment, sans limite de volume.

5. **Services mesurables :** L'utilisation des ressources peut être contrôlée et mesurée par le prestataire, conditions essentielles pour la facturation, le contrôle d'accès, l'optimisation et la planification du déploiement des ressources informatiques et gage de transparence pour le prestataire et l'utilisateur du service.

II.3.3. Modèles de déploiement :

1. ***Services du Cloud Computing Publique :* « Public Cloud »**
   - Les services sont mis à la disposition du grand public par l'entremise d'Internet.
   - Les données des utilisateurs ne sont cependant pas, par essence, accessibles au public, les fournisseurs offrant normalement aux utilisateurs des mécanismes de contrôle d'accès à leurs données.
   - Les services peuvent être fournis à titre gratuit ou onéreux.
   - Le système appartient à une entreprise et est localisé à l'externe.

2. ***Systèmes du Cloud Computing Privé : « Private Cloud »***
   - Le système est exploité pour le compte d'une seule personne (individu, entreprise ou organisation).
   - Le système est géré soit par cette personne, soit par une tierce partie, et peut être localisé à l'interne ou à l'externe.
   - Ce système réduit les enjeux liés à la sécurité des données et à la conformité statutaire et règlementaire (localisation des données, vérification,…).
   - Les avantages du Cloud Computing peuvent être toutefois largement atténués par ce modèle sauf si le système est hybridé à un système public, ou s'il est sécurisé (système privé virtuel).

3. ***Système Cloud Computing communautaire : « Community Cloud »***

• L'infrastructure Cloud Computing est contrôlée et utilisée par des personnes partageant des préoccupations ou intérêts communs (mission, exigences de sécurité, politiques, exigences en matière de conformité).

• Ce système est géré soit par ces personnes, soit par une tierce partie, et peut être localisé à l'interne ou à l'externe.

4. ***Système Cloud Computing hybride : « Hybrid Cloud »***

• Ce système est composé d'au moins deux autres modèles de déploiement Cloud Computing, normalement « privé » et « public ».

• Ce modèle permet par exemple à une entreprise de conserver certaines données ou application sensibles sous la protection d'un système Cloud Computing privé en permettant le déploiement (permanent ou occasionnel) de ses autres données ou application vers un système public «*Cloud bursting* », par exemple pour répondre à une demande accrue en période de pointe.

II.3.4. Modèles de Services Cloud Computing :

1. **Modèle Logiciel en tant que service : « *Software as a Service* » ou « *SaaS* »**

• L'utilisateur a uniquement accès à une application logicielle aux fins l'utilisation de cette dernière.

• L'utilisateur peut contrôler la configuration de l'application logicielle en fonction de ses besoins.

• L'utilisateur n'a toutefois aucun contrôle sur l'infrastructure informatique sous-tendant l'application logicielle (système d'exploitation, équipements informatiques et réseau).

2. **Modèle Plateforme en tant que service : « *Platform as a Service* » ou « *PaaS* »**

• L'utilisateur a accès à un environnement de développement (langage et outils de programmation) et d'hébergement d'applications logicielles.

• L'utilisateur choisit et gère les applications exécutées dans l'environnement et peut avoir un certain contrôle de l'environnement d'hébergement mais ne contrôle pas l'infrastructure informatique sous-jacente (système d'exploitation, infrastructure matérielle, réseau).

3. **Modèle Infrastructure en tant que service : « *Infrastructure as a Service* » ou « *IaaS* »**

• L'utilisateur a accès à des ressources informatiques fondamentales : capacité de traitement, capacité de stockage de données, composantes réseau, intergiciels (*middleware*).

• L'utilisateur peut contrôler le système d'exploitation, le système de stockage, les applications logicielles et les composants réseaux (coupe-feux, répartiteur de charges) mais pas l'infrastructure Cloud Computing sous-jacente.

Autres (exemples)

• Données en tant que Services (DaaS).

• Base de données en tant que Services (DBaaS).

• Communications en tant que Services (CaaS).

• Réseau en tant que Service (NaaS).

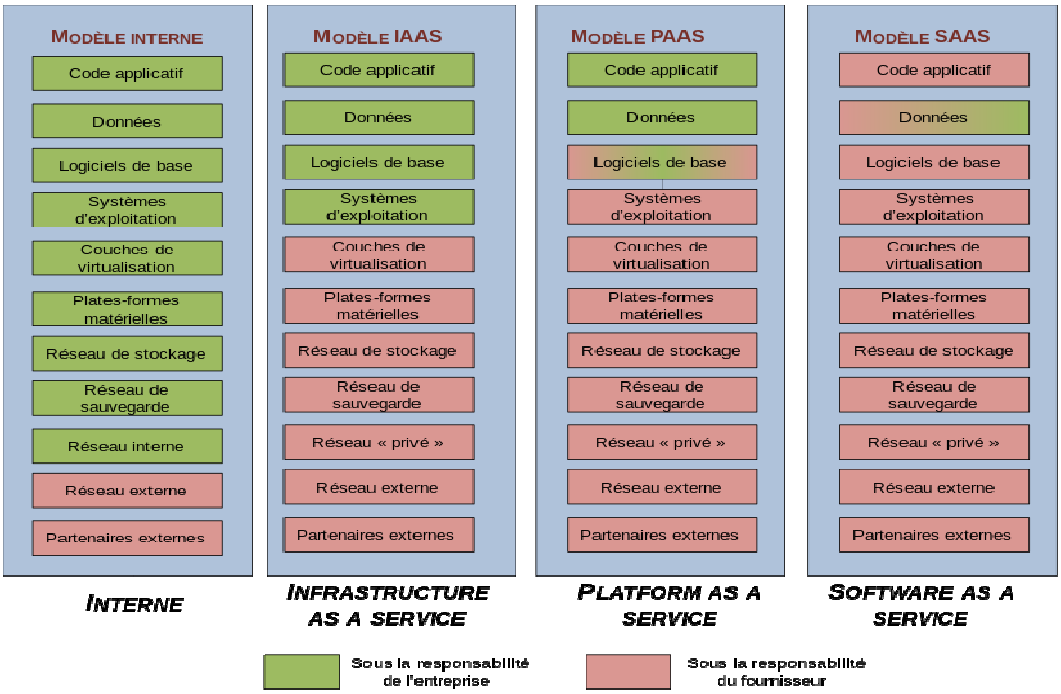


Figure II.8 : Les différents modèles de services.

II.3.5. Les avantages du Cloud Computing (CC) :

Le Cloud Computing est généralement associé à une multitude d'avantages qui créent l'unanimité parmi les professionnels de l'entreprise. Notez toutefois que ces avantages demeurent théoriques, étant donné la nature même du concept.

- La possibilité de déployer et de rendre disponibles des applications majeures et des environnements de travail de manière immédiate. La mise à jour des applications est systématique, et le fournisseur décharge son client de toute responsabilité de maintenance. Une simplicité imbattable donc, qui vous épargne en plus les développements coûteux
- Les données peuvent être partagées, puisque tout utilisateur du Cloud Computing peut aisément rendre disponibles ses données à un ou plusieurs autres utilisateurs du CC. Il est donc possible de créer une plateforme virtuelle collaborative en un temps record.
- Un calcul particulièrement puissant, ce qui constitue probablement l'argument de choc en faveur de ce type de solution. Il faut effectivement garder à l'esprit que les structures limitées à ce niveau (puissance de calcul) peuvent ici se permettre une délocalisation de leurs traitements, et bénéficier ainsi de toutes les ressources et performances mises à leur disposition par le serveur du Cloud Computing. Bien qu'il ne concerne qu'un nombre assez réduit d'entreprises, cet avantage demeure l'un des plus importants du CC.
- Un accès libre et ouvert au client, qui peut établir sa connexion de n'importe où et avoir accès à ses données immédiatement, sans passer par la mise en place d'un VPN (réseau privé virtuel) dans l'entreprise.

- Un suivi constant du développement de votre espace Cloud Computing. Vous êtes généralement informé, en temps réel, de l'évolution de votre plateforme de Cloud Computing, puisque l'installation d'un logiciel n'est pas nécessaire et que l'accès est effectué via un simple navigateur web
- Une liberté totale, puisque vous n'êtes lié à votre fournisseur par aucun engagement à long terme. Les services du Cloud Computing sont soit facturés à la demande ou par abonnement mensuel. Vous demeurez donc libre de mettre un terme à ce service à tout moment, si vous jugez n'en avoir plus besoin, ou si vous désirez simplement changer de fournisseur.
- Coût : du fait que le même service est proposé à de nombreux utilisateurs, son coût en est nettement amoindri.

II.3.6. Les inconvénients du Cloud Computing :

Plusieurs catégories d'inconvénients existent :

- L'utilisation des réseaux publics, dans le cas du *Cloud* public, entraîne des risques liés à la sécurité du *Cloud*. En effet, la connexion entre les postes et les serveurs applicatifs passe par le réseau internet, et expose à des risques supplémentaires de cyber attaques, et de violation de confidentialité. Le risque existe pour les particuliers, mais aussi pour les grandes et moyennes entreprises, qui ont depuis longtemps protégé leurs serveurs et leurs applications des attaques venues de l'extérieur grâce à des réseaux internes cloisonnés.

- Le client d'un service de *Cloud Computing* devient très dépendant de la qualité du réseau pour accéder à ce service. Aucun fournisseur de service Cloud ne peut garantir une disponibilité de 100 %. Par exemple, des défaillances sur les services *Cloud* sont référencées par l'International Working Group of Cloud Resiliency.

- Les entreprises perdent la maîtrise de l'implantation de leurs données. De ce fait, les interfaces inter-applicatives (qui peuvent être volumineuses) deviennent beaucoup plus complexes à mettre en œuvre que sur une architecture hébergée en interne.

- Les entreprises n'ont plus de garanties (autres que contractuelles) de l'utilisation qui est faite de leurs données, puisqu'elles les confient à des tiers.

- Les questions juridiques posées notamment par l'absence de localisation précise des données du *Cloud Computing*. Les lois en vigueur s'appliquent, mais pour quel serveur, quel *data center*, et surtout quel pays ?

- Tout comme les logiciels installés localement, les services de *Cloud Computing* sont utilisables pour lancer des attaques (craquage de mots de passe, déni de service…). En 2009, par exemple, un cheval de Troie a utilisé illégalement un service du *Cloud* public d'Amazon pour infecter des ordinateurs.

- Du fait que l'on ne peut pas toujours exporter les données d'un service Cloud, la réversibilité (ou les coûts de sortie associés) n'est pas toujours prise en compte dans le cadre du projet. Le client se trouve souvent « piégé » par son prestataire et c'est seulement lorsqu'il y a des problèmes (changement des termes du contrat ou des conditions générales d'utilisation, augmentation du prix du service, besoin d'accéder à ses données en local, etc.) qu'il se rend compte de l'enfermement propriétaire (Vendor Lock-In) dans lequel il se trouve.

II.3.7. Les besoins :

Une entreprise qui se lance dans l'aventure Cloud Computing doit :

- Faire appel a un **Expert Cloud**.
- Mettre en place un chantier progressif, avec un découpage.
- Réfléchir l'architecture Cloud en termes de service et de processus de création de valeur.
- Penser le système d'information en termes de service.
- Former les développeurs aux bonnes pratiques Cloud Computing.
- Mettre en place des processus de création logiciel Cloud .
- Sensibiliser les utilisateurs sur la sécurité et l'informatique transverse.
- Prévoir des environnements pour les tests, les recettes et la production.

Avant Propos du Solution et la Construction du Cloud Computing :

La gestion des environnements est un terme qu'on utilise pour simplifier la compréhension du sujet. En fonction de l'entreprise, on parle de plate-forme, de serveur, d'environnement, de VM (machine virtuelle). C'est un environnement d'hébergement, de travail et d'exécution d'un programme informatique. Il est constitué de une à plusieurs machines réelles ou virtuelles en production.

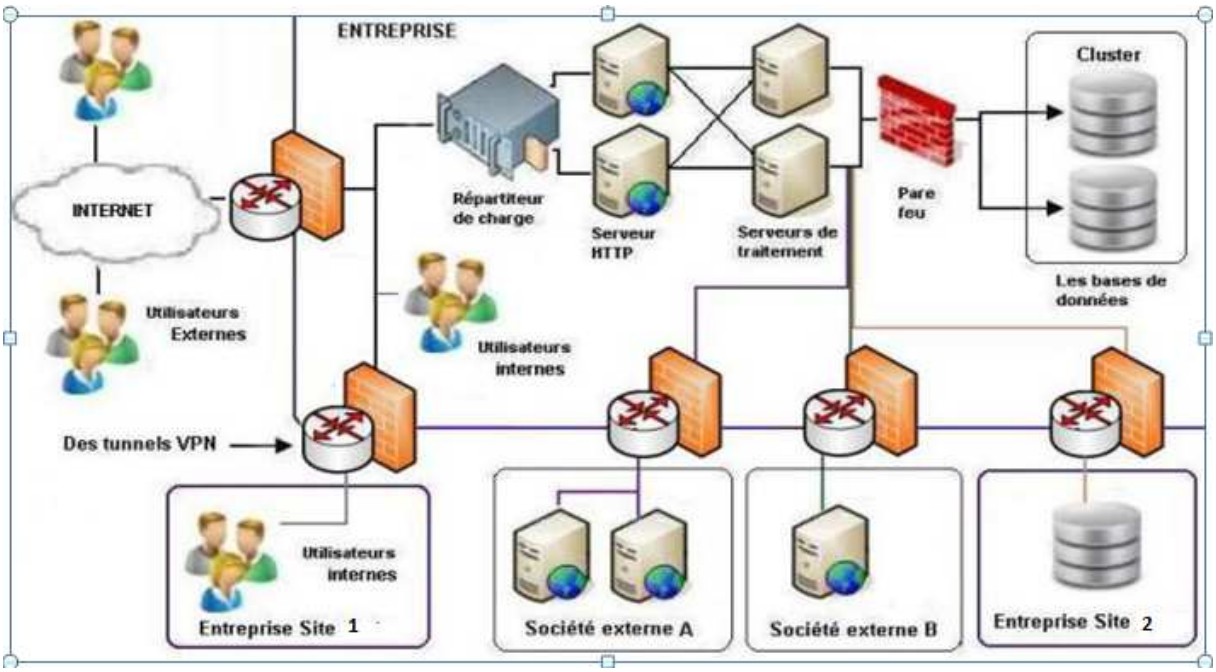
Cette partie aborde le Cloud à partir de cas concret et d'une réflexion basée sur de l'existant. Afin de présenter au mieux le sujet web classique, on est parti d'un site de commerce électronique, avec de nombreux utilisateurs (acheteurs et fournisseurs).

Les schémas qui vont être présentés, intègrent des notions de répartition de charge (load balancing), de serveur http, de serveur de traitement et de cluster de base de données. Ils proposent des flux entrants et sortants vers des fournisseurs, vers des entreprises externes.. Ils sont très utiles à la compréhension des impacts et des enjeux du Cloud Computing.

Comparatif de la structure d'une entreprise classique VS entreprise Cloud.

Nous avons vu dans le 1ére chapitre :

- L'architecture d'une entreprise classique



L'entreprise est répartie sur 3 sites (site 1, site 2, site principal), elle fait appel à 2 sociétés externes.

- La même architecture dans le Cloud Computing.

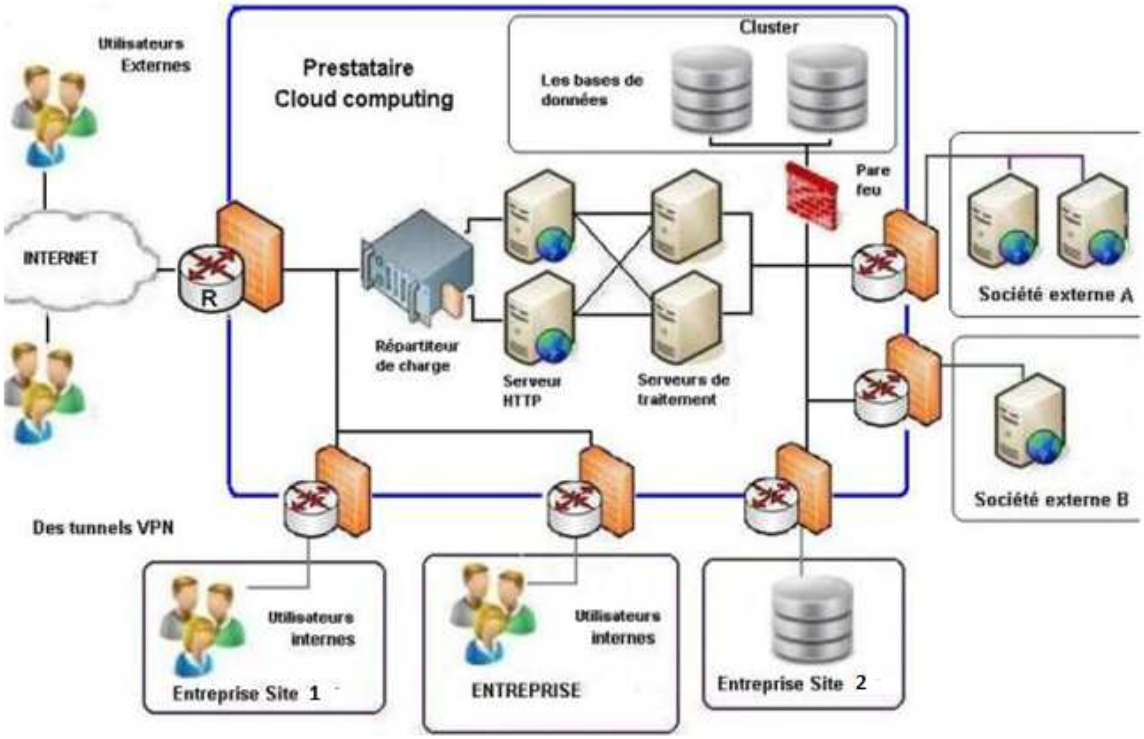


Figure II.9 : L'architecture dans le Cloud Computing.

Le schéma ci dessus, représente la même entreprise, le site de commerce électronique migré dans le nuage (dans le Cloud Computing), chez un prestataire Cloud Computing. Il représente l'entreprise d'un point de vue production.

Le premier constat

Dans la première entreprise, l'entreprise est construite, bâtie autour du noyau, autour du site web (de commerce électronique) et de son informatique. Le site de l'entreprise est beaucoup plus grand. L'informatique représente une large part de l'activité de l'entreprise. Nous avons des chefs de projets, des ingénieurs, des analystes, des experts, des techniciens réseaux, etc. propres à l'entreprise.

Dans l'entreprise qui utilise les services Cloud Computing d'un prestataire ou d'un hébergeur, l'informatique est plus diffuse. L'informatique, la technique, les machines ne sont plus le centre, le cœur ou le poumon de l'entreprise. L'activité est décentralisée par rapport au client. Les chefs de projets sont toujours là, par contre les techniciens réseaux, les experts sont chez le prestataire de Cloud Computing. La population informatique a été scindée en deux parties. La partie fonctionnelle se situe prés du cœur de métier de l'entreprise, la partie technique se retrouve prés et chez l'info gérant.

La perception de l'informatique et du rôle au sein de l'entreprise sont différents. Les équipes internes n'ont plus exactement le même rôle. Il y a une transformation de l'informatique. Dans le premier cas, elle est dans les locaux de l'entreprise (interne), dans le deuxième cas, elle est fortement externalisée.

On vous propose de rentrer un peu plus dans le cœur de la production informatique, de la conduite de projet, pour affiner, notre réflexion.

Les impacts sur la réalisation d'un projet Cloud ?

La méthode de conduite d'un projet :

Dans les entreprises, tous les projets suivent une méthode de conduite de projet (les diverses méthodes de conduite de projet). La plus connue est la Démarche de cycle en V. Il existe de nombreuses méthodes.

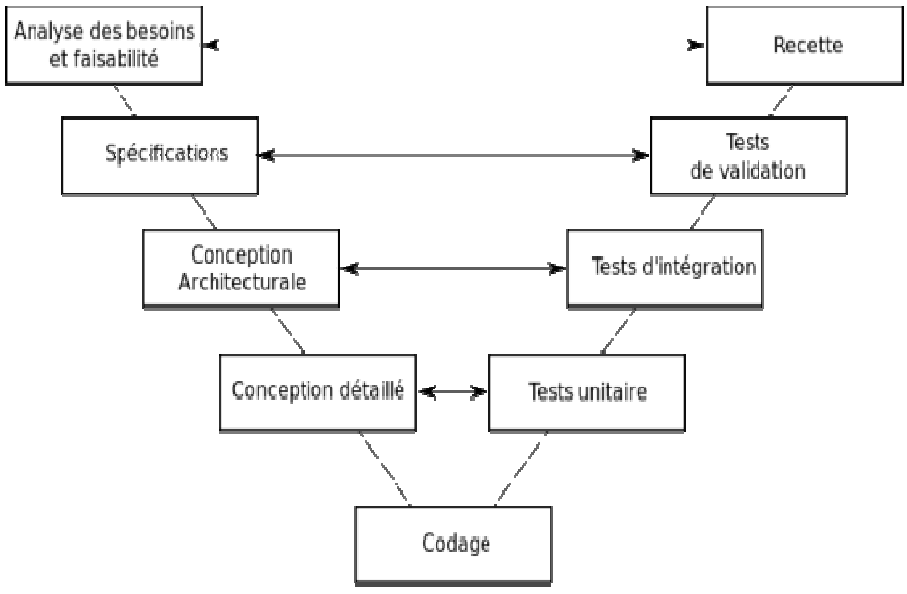


Figure II.10 : La méthode de projet de l'entreprise.

La méthode de projet sert à conduire le projet informatique à son terme en respectant les impératifs de qualité, coût et délai est le découpage du projet en phases. Chaque phase est accompagnée d'une fin d'étape destinée à formaliser la validation de la phase écoulée avant de passer à la phase suivante.

Tous les projets informatiques suivent une méthode de conduite de projet. Ils s'inscrivent dans les bonnes pratiques d'une entreprise. Un projet de logiciel informatique est décomposé en plusieurs phases.

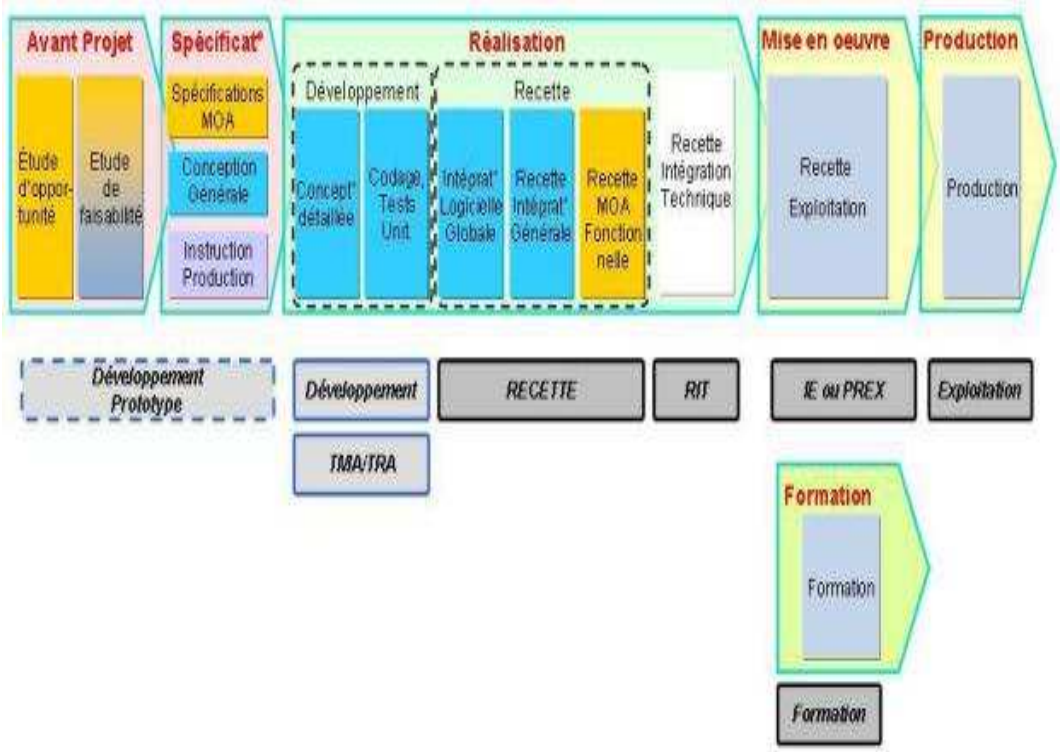


Figure II.11 : Les phases de la méthode de projet de l'entreprise.

Pour mener à bien, la réalisation d'un projet informatique d'une certaine taille, le chef de projet doit découper le projet en plusieurs phases, et prévoir un environnement de travail et d'exécution par phase. La construction d'un environnement demande l'achat de matériel, la préparation et l'installation des divers serveurs.

Les phases d'un projet :

A partir de la phase d'étude et de rédaction du cahier des charges, des spécifications générales et détaillées, le projet entame un parcours plus ou moins long. Nous avons des phases qui sont incontournables et d'autres pas.

- *La phase développement :*

Le poste développeur est l'un des postes les plus difficiles à représenter. Le développeur teste les nouvelles fonctionnalités au travers d'un navigateur internet. Les besoins du développeur sont simples, par contre ils sont conditionnés par les choix techniques et logiciels de la production.

Figure II.12 : La phase du développement.

- *La phase de recette :*

La recette d'un projet informatique est réalisée par une ou des personnes, et aussi des automates. L'utilisation des automates permet de reproduire les cas de tests plusieurs fois. La phase de recette permet de vérifier la conformité du développement avec le cahier des charges et le cahier des tests.

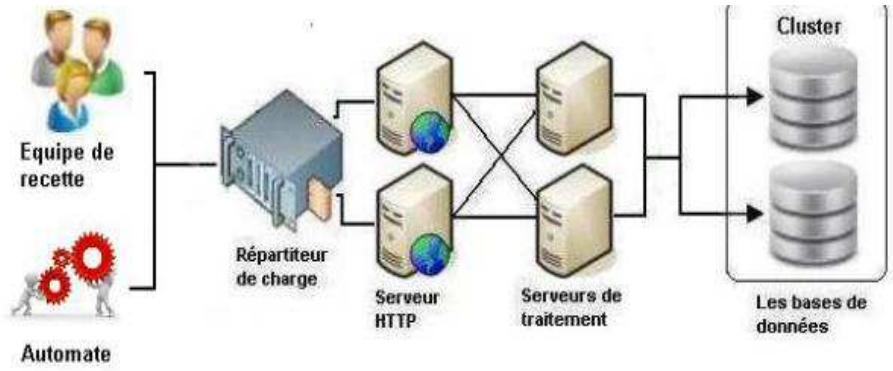


Figure II.13 : La phase de recette.

- *La phase de pré production :*

Elle permet de produire le livrable finale et la documentation d'installation avant la livraison finale. L'environnement de pré production ressemble fortement à la production, par contre, il n'y a pas d'utilisateurs finaux. Les équipes utilisent des bouchons pour simuler la présence d'un dispositif, d'une machine, d'un service interne ou externe à l'entreprise.

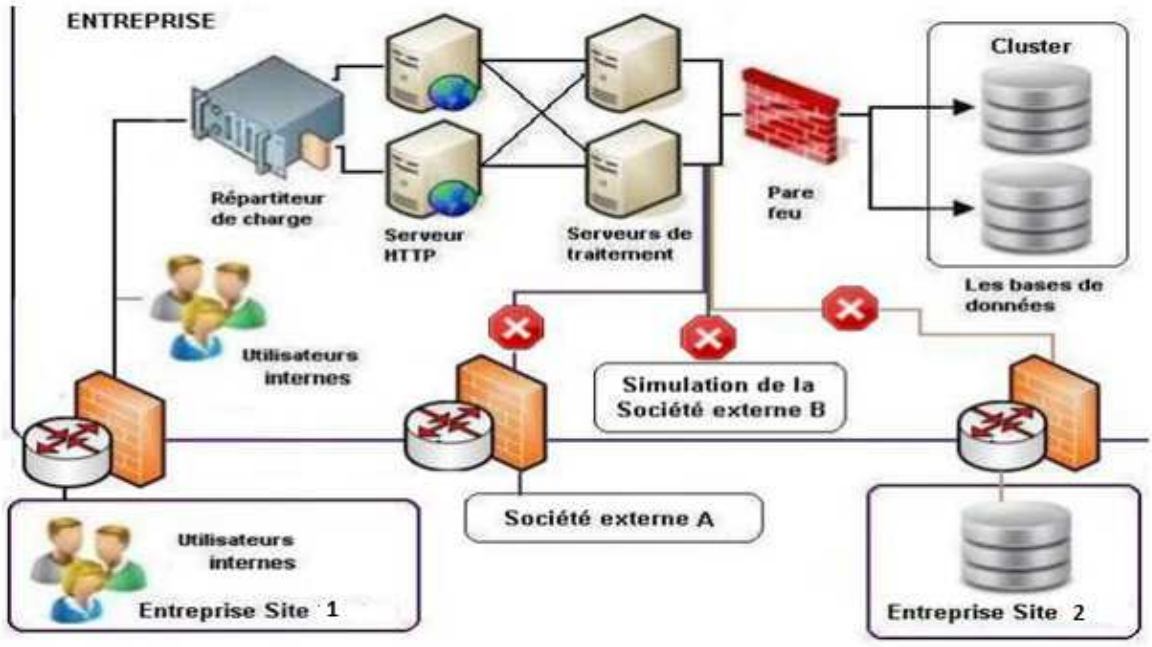


Figure II.14 : La phase de pré production.

- *La phase de mise en production :*

La mise en production est l'étape ultime d'un projet. C'est le passage délicat vers la production, l'instant de vérité sur les projets. Chaque phase a un rôle distinctif. Elle complète et valide des qualités du livrable finale, elle a une durée variable et se répète pour chaque version du logiciel. Il est important de retenir. Chaque phase dispose d'un environnement distinct, d'une équipe de personne. Les environnements sont dimensionnés en fonction des besoins de chaque phase, des plus simples aux plus compliqués. La réalisation d'un projet informatique important demande de nombreux environnements techniques et du temps de préparation (création, administration, initialisation).

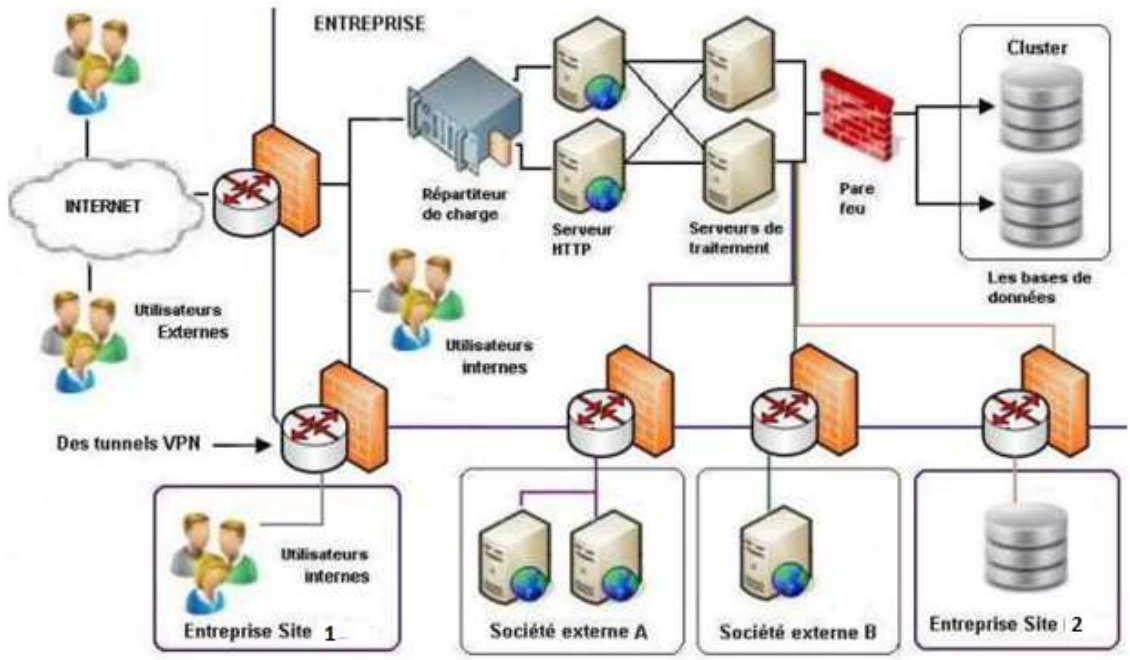


Figure II.15 : La phase de mise en production.

La construction des environnements :

La construction des environnements est un service transverse au sein d'une entreprise. Ce service est constitué de plusieurs dimensions, l'achat des ressources, la gestion de la capacité, la construction et maintenance des environnements, la cartographie et les référentiels des machines.

La construction des environnements intègre la notion de "socle". Un socle est un ensemble de briques logiciels et techniques pour répondre aux besoins d'un ou des projets. Le socle comprend l'achat des licences de logiciel, l'achat du matériel, le façonnage des environnements et la maintenance. Le socle est adapté et décliné sur tous les environnements d'un projet.

Tous les 5 ans environ, une entreprise doit changer et construire des nouveaux socles, pour suivre les progrès technique et mettre à jour les parties logicielles obsolètes, ou plus maintenues par les éditeurs logiciels.

On va citer 2 exemples de socles différents:

- Nous avons un socle autour de **Microsoft Windows 2012**. De nombreuses entreprises sont en train de migrer leurs sites web vers Microsoft **Windows 2012** en 64 bits. La solution est plus performante, elle est plus stable, etc..

- Dans le monde des serveurs d'application Java, c'est la même chose, nous avons la pile logicielle **IBM Webphere Application Serveur 5.1** (2001) vers la version 6.1 (juin 2006), vers la **version 7** (septembre 2008), vers la **version 8** (2011). Les diverses versions de WAS suivent et intègrent les évolutions du langage java et de la pile J2EE (Java Enterprise Edition).

Chaque nouvelle version apporte de nouveaux services, de nouvelles options, des améliorations, des évolutions, etc. On ne parle pas des correctifs, des fixes patchs qui s'ajoutent à cette liste. Un socle repose sur une à plusieurs briques techniques (machine, réseau) et des briques logiciels (un système d'exploitation (Unix, Windows, Mac OS/X, Linux, AIX), un serveur de traitement, des logiciels maison, etc.).

La mise au point d'un socle technique est un investissement souvent important, qui demande des ressources logicielles, techniques, humaines, et du temps. La construction d'un socle à un impact majeur sur la conduite et le maintien des projets informatique.

Le rapport avec le Cloud ?

Le processus de création logicielle Cloud suit les phases de réalisation d'un projet classique (développement, recette, production, etc.). Il faut prévoir le même nombre d'environnement sur le Cloud.

Qu'est ce qui change ? Nous commençons à nous rapprocher du mystère. Je dénombre quatre changements majeurs :

- la mise à disposition des infrastructures,
- la gestion de l'hébergement,
- la construction du socle,
- la création du logiciel.

La présentation du processus de création du logiciel permet d'entrevoir ces différences.

La mise à disposition des infrastructures Cloud :

La construction et la production d'environnement Cloud repose sur les infrastructures de l'info gérant. Le client doit faire une **demande d'environnement détaillé**, avec une typologie, le détail de chaque serveur (machine), les usages, les accès internes ou externes vers cet environnement. Le client doit procéder à la recette de l'environnement par rapport au cahier des charges et il doit s'assurer de la conformité des installations.

Le client doit s'approprier une vision de la structure informatique et l'infrastructure réseaux du partenaire "Cloud", établir et cartographier l'ensemble de ses besoins Il doit déterminer ce qu'il est possible de faire ou pas en terme de sécurité, en terme de flux, en terme de mutualisation. Il doit déterminer **tel projet travaille avec tel autre projet.**

La gestion de l'hébergement Cloud :

La disponibilité des ressources, l'optimisation des machines, le dimensionnement des machines sont régit par l'hébergeur. Il se doit de disposer de ressource sur étagère rapidement et sur demande. Il a un rôle d'anticipation par rapport aux besoins. Il échelonne les achats des machines en fonction des besoins des divers clients.

Le client bénéficie des économies d'échelle liées à l'achat groupé, à l'administration, à l'expertise groupée. Le client bénéficie des infrastructures de sauvegarde mutualisé. Il dispose d'un levier puissance et d'une facturation à l'usage. La facturation unique permet de connaître le cout d'un service, et de quantifier les efforts à faire. Le client peut à tout moment figer un environnement et reprendre plus tard les travaux.

La construction du socle technique Cloud :

La bataille du Cloud repose sur la maîtrise du socle.

Nous avons deux types de Cloud qui s'affrontent, le IAAS (Infrastructure as a service, le service c'est l'infrastructure), et le PAAS (Plateforme as a service, le service c'est la plateforme – l'environnement).

- Les fournisseurs d'infrastructure (de type IAAS) proposent des machines virtuelles avec du disque, de la mémoire, de la puissance CPU et un système d'exploitation. La **création du socle repose** sur les épaules du client.
- Les fournisseurs de plateforme (de type PAAS) proposent des solutions beaucoup plus complètes, ils intègrent des socles **Cloud** plus ou moins évolués. Le client **doit s'adapter** au fonctionnement des socles distribués (Cloud).

La frontière entre les deux types de Cloud à tendance à s'estomper. Les éditeurs de logiciel proposent de plus en plus des solutions Cloud. Il y a une convergence entre les socles classiques et les socles Cloud.

La création du logiciel Cloud :

La création du logiciel est fortement liée au socle et au type d'hébergement. L'informatique, les programmes sont morcelés en programmes beaucoup plus petit. Les entreprises écrivent et migrent des morceaux de programmes vers le Cloud. Elles transforment les programmes en **service**. Elles tissent des partenariats et gère la consommation des services à l'usage.

Les socles classiques reposent sur des systèmes d'exploitation (Windows), des serveurs d'application (websphere), et des bases de données (oracle). Ces composants sont très répandus dans les entreprises.

De l'autre côté, nous avons **les socles Cloud**. Je vais prendre le cas de Google Application Engine (GAE), il repose sur un serveur Jetty modifié (java), sur une base de données BigTable, et sur des infrastructures de plusieurs machines. On parle de base de données **NoSQL,** de nuage de données, de BigData**.**

Une base de données classique se retrouve sur une ou deux machines. Une base de données Cloud est répartie sur plusieurs machines. La structure de la base de données est totalement différente et le fonctionnement aussi.

La création de logiciel sur le Cloud répond à de nouvelles contraintes, la facturation à l'usage, les temps de latence réseau, la perte de localisation (stateless), l'emprunte mémoire, le nombre de connexion à la base de données, etc.

Les socles Cloud actuellement offrent de nombreux avantages, par contre ils sont limités par deux aspects (les accès vers les bases de données, et les temps de latences). De nombreux progrès ont été réalisés afin de réduire ces défauts.

Les socles Cloud s'adaptent de plus en plus aux besoins classiques et inversement.

Pour conclure

On est suis forcé a rester claire tout au long de cet article, sur un sujet compliqué. L'univers du Cloud, du bigdata est un univers passionnant, qui réserve de jolies surprises à venir.

Le Cloud est une tendance de fond, lié d'une part à la virtualisation, d'une autre part à la mutualisation des ressources dans des data-center de part le monde.

Nous sommes dans un monde fini, avec des connaissances limités. Une entreprise, un département dispose de compétence dans un domaine, une autre dans un autre domaine. Le Cloud permet de s'affranchir des limites et de créer du partenariat. Il permet de faire des économies autour de la conception des produits et du cycle de vie d'un projet.

Nous allons de plus en plus vers des projets hybrides (classique et Cloud), vers un informatique multi-acteur, vers une informatique de service (entreprises externes, recherche interne). Elle demande une bonne maitrise de l'existant, du fonctionnelle, une connaissance approfondie des environnements et des contraintes techniques et logicielles.

On va continuer l'exploration du monde "Cloud Computing", et de la création de site web. Pour illustrer, les problématiques dont on va parler. On va repartir du projet de site de commerce en ligne. On est une entreprise de taille moyenne, On dispose de 3 équipes dédiées à la création du site web. On dispose de 3 environnements, un environnement de développement, un environnement de recette et un environnement de production.

La gestion des sauvegardes :

La gestion des sauvegardes informatique est une notion simple liée à l'activité d'une entreprise. Elle consiste à mettre de côté une copie, à sauvegarder les données informatiques utiles et sensibles d'une entreprise à un instant donné.

*La sauvegarde (*backup *en anglais) est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique.*

Il existe divers types de sauvegarde, la sauvegarde complète, la sauvegarde incrémentale, la sauvegarde différentielle, l'archivage, etc.

Le corollaire de la sauvegarde, c'est la restauration. L'unique moyen de vérifier le bon fonctionnement d'une sauvegarde est de faire une restauration ! Nous avons souvent des surprises lors de la restauration.

La gestion des sauvegardes peut être liée à une activité de l'entreprise, à un besoin, à une réglementation administrative ou fiscale.

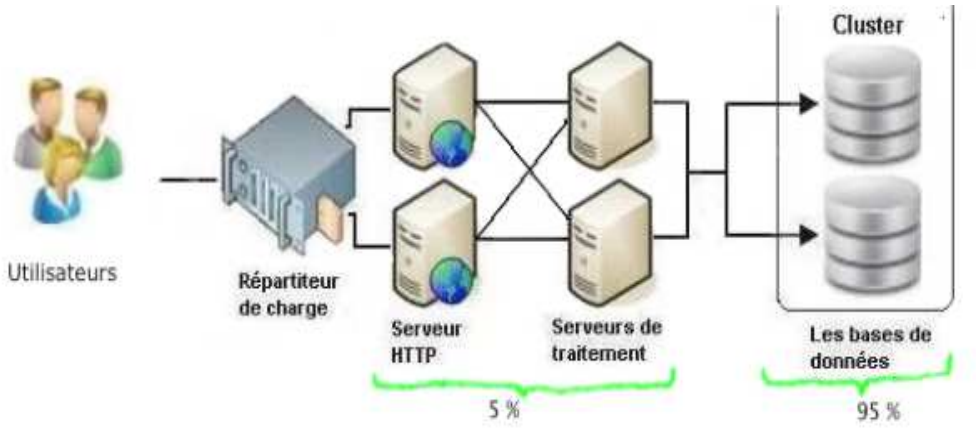


Figure II.16 : La gestion de la sauvegarde.

Qu'est ce qu'une entreprise sauvegarde autour d'un site web ?

C'est la bonne question à poser. Dans un site web, un bon 95% des données sont stockées actuellement dans les bases de données. Les 5 % restants sont liés au logiciel installé, et à des fichiers externes (des images, des ressources CSS, des fichiers PDF, etc.). La majorité des sauvegardes est réalisée autour de la base de données de production.

Les entreprises mettent en place des systèmes de sauvegarde pour les environnements de développement, de tests, de recettes. Elles créent des jeux de données, de tests, pour vérifier le bon fonctionnement des programmes. Elle accentue les sauvegardes sur les parties sensibles des diverses phases. Dans les environnements de développement, on sauvegarde de préférence les différentes versions de logiciel, et des jeux de données mineurs. Dans les environnements de recette, on focalise l'attention sur une version du logiciel et un jeu de données de test et ou un jeu de données quasi production (très souvent il s'agit d'une recopie de la production).

Comment on sauvegarde ?

Les entreprises déploient un logiciel (un démon) sur tous les serveurs à sauvegarder. Toutes les nuits, ou à intervalle régulier, le serveur de sauvegarde se connecte sur les machines, il appelle le satellite de sauvegarde (le démon) et lance la sauvegarde. La restauration des données effectue le même chemin. Les données sont stockées sur des baies de sauvegarde.

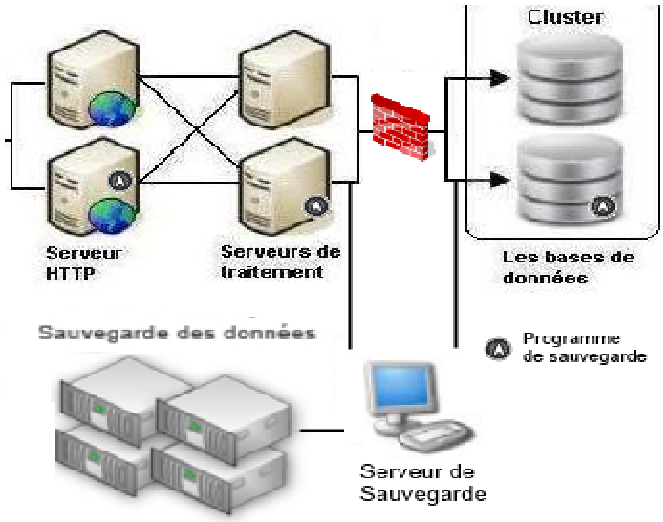


Figure II.17 : La sauvegarde de données.

La reprise d'activité :

Au delà de la gestion des sauvegardes, les entreprises doivent faire face à des risques d'incidents informatique graves, d'incendie, de dégâts des eaux, de corruption des données ou d'indisponibilité totale ou partielle de leur informatique. Pour une entreprise la perte d'activité informatique se chiffre en perte de capital, elle doit mettre en œuvre un plan de reprise d'activité (ou PRA). L'image d'une entreprise est de plus en plus sensible aux variations et incidents de leur système informatique.

Le plan de reprise d'activité est un plan de sécurisation de l'informatique d'une entreprise. Il se traduit le plus souvent par la mise en d'un ou de plusieurs site de secours. En cas d'indisponibilité d'un site web, les traitements, les données sont basculées vers le site de secours. Les banques, les assurances, les grandes entreprises sont contraintes de mettre en place des solutions de reprise d'activité.

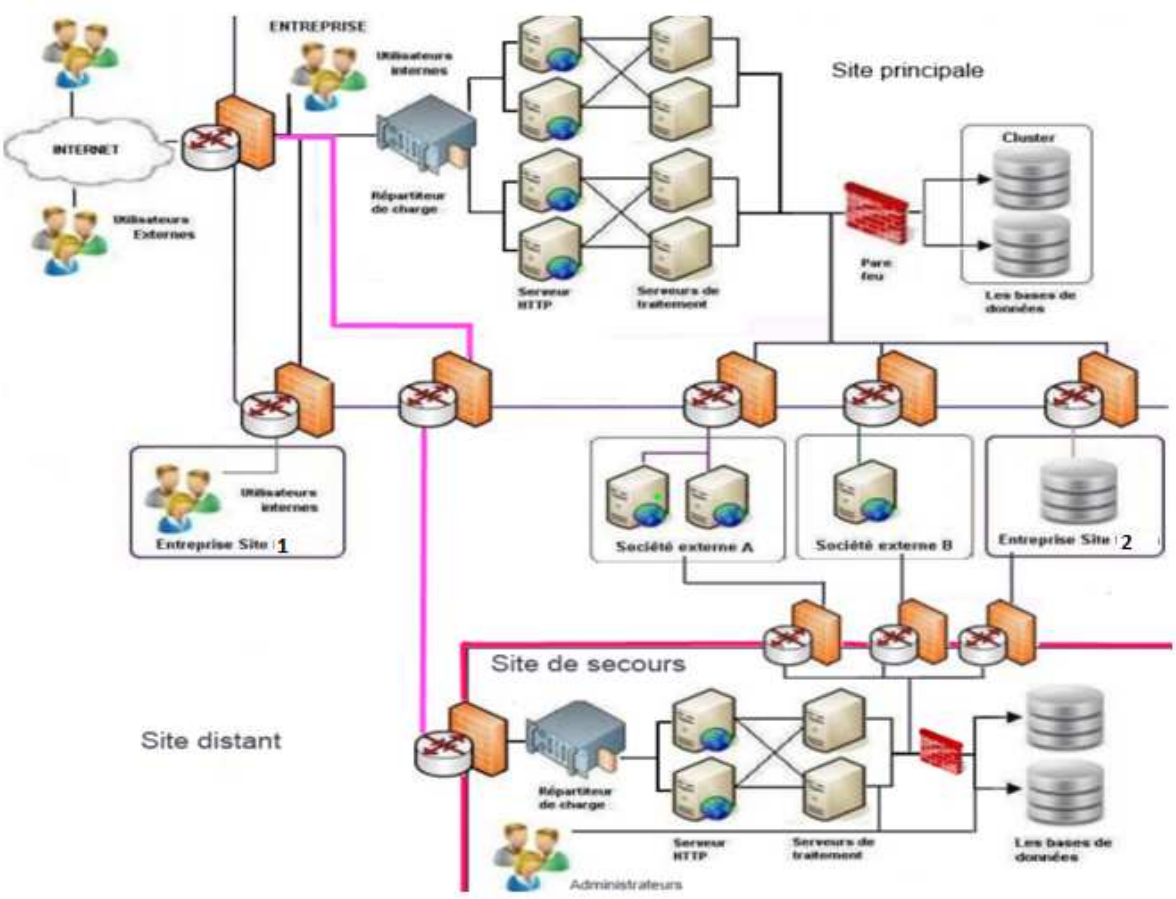


Figure II.18 : La reprise d'activité.

La mise en place d'un site de secours demande la mise en place de procédure de recopie et de backup des données, de synchronisation des données, d'ouverture de flux vers les divers acteurs internes et externes au site web. Le site de secours n'est pas à 100% l'équivalent du site de production principale, par contre il se doit de pouvoir tenir la charge, et être exhaustif.

Après un moment de silence autour du Cloud, on a eu envie d'écrire un ensemble d'articles autour des transformations actuelles sur la partie des données. Je vais aborder des notions autour de bigData, autour des bases de données NoSQL.

On va expliquer les enjeux autour de la maîtrise des données, les avantages, les inconvénients.

Au delà des aspects théoriques et techniques, on va vous parler d'infrastructure et d'architecture de données, de la modélisation des données dans les bases NoSQL, des graphes d'objets et de la création des bases hybrides, et aussi des impacts pour les concepteurs de logiciel.

C'est un vaste programme.

Les bases de données NoSql.

Il y a de nombreux articles autour des bases de données, autour du BigData, autour du NoSQL. Par ou commencer ? Je vous propose de regarder de plus près le puits de données.

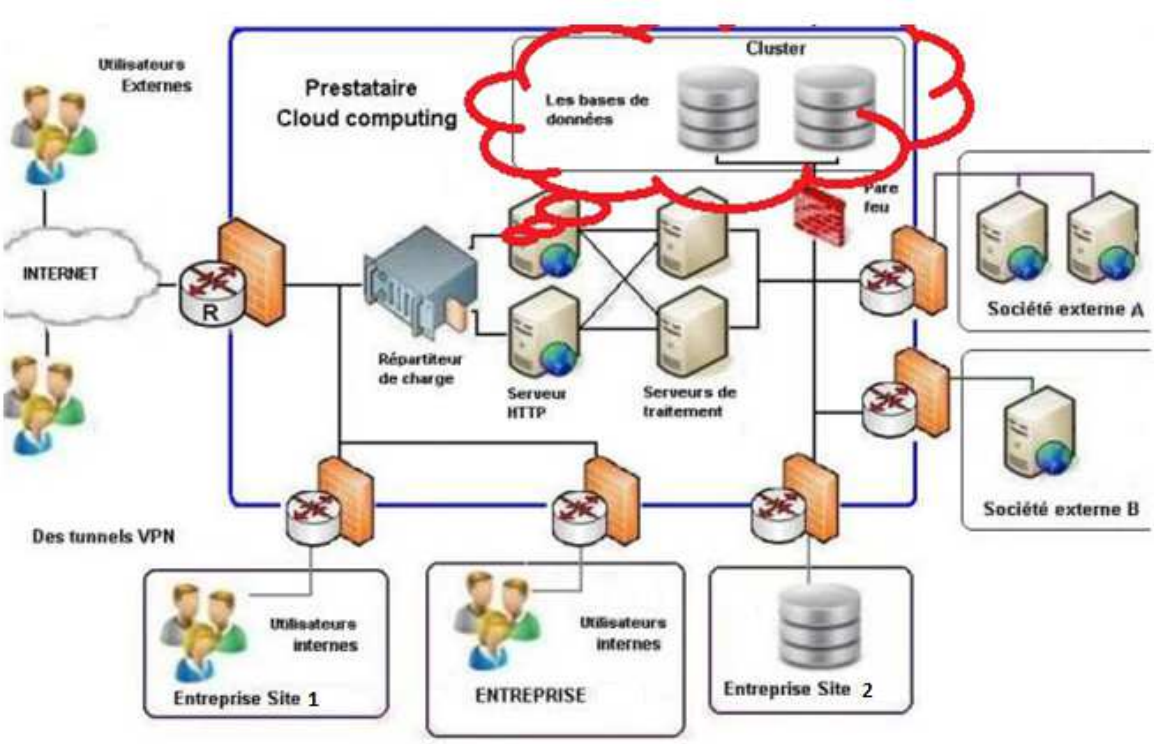


Figure II.19 : Les bases de données NoSql.

Le puits de données

Je vais faire un petit retour en arrière. Nous sommes **dans les années 80**, les entreprises utilisent de plus en plus l'informatique, sur les gros serveurs IBM, BULL et autres (sur les mainframes). Les entreprises stockent des données dans des puits de données, sur des bandes, sur des cassettes.

Figure II.20 : Ordinateur de la NASA en 1962

Figure II.21 : Un Dec PDP-10

Un ordinateur central, ou un mainframe, est un ordinateur de grande puissance de traitement.

Les bases de données n'avaient pas de structure (ou très peu), il n'y avait pas de langage de requête pas de SQL. Les serveurs étaient constitués de systèmes de fichiers. Les gros serveurs étaient utilisés pour stocker (sauvegarder de la données), effectuer de la recherche (requête) et modifier (manipuler) de la donnée. C'était fiable et robuste. Pour développer l'informatique, les entreprises ajoutaient une machine supplémentaire, du disque et de la mémoire. Les gros serveurs étaient utilisés par de nombreuses dactylos, pupitreuses, etc. Les programmes étaient réalisés en **COBOL**, **TELON** et d'autres langages exotiques.

Les années 90 ont marqué un tournant dans le monde des bases de données. De nombreux ingénieurs ont réfléchi sur la problématique des bases de données et sur un langage pour questionner les bases de données. L'informatique est aussi devenue moins lourde, avec l'arrivée de la micro informatique. Les gros serveurs continuent d'évoluer dans le monde bancaire, dans les assurances.

Le langage SQL ((Strutured Query Language) a créé en 1974, normalisé en 1986, il est reconnu par la grande majorité des systèmes de gestion de bases de données relationnelle (abrégé SGBDR) du marché. La normalisation du SQL à créer un engouement des entreprises vers une compréhension des données, vers une représentation (modélisation) des données et vers une idée de ce que doit être une base de données.

De nos jours.

L'informatique est un perpétuel recyclage d'idées qui fonctionnent. Nous avons un retour en force des puits de données des mainframes sur ordinateur. La puissance de traitement des ordinateurs a augmenté, et ils répondent très bien à des problématiques de volumétrie, de quantité de connexion simultanée et aussi de disponibilité.

Du non SQL au NoSQL, il n'y a qu'un pas.

En informatique, NoSQL désigne une catégorie de systèmes de gestion de base de données(SGBD) qui n'est plus fondée sur l'architecture classique des bases relationnelles. L'unité logique n'y est plus la table, et les données ne sont en général pas manipulées avec SQL.

À l'origine servant à manipuler des bases de données géantes pour des sites web de très grande audience tels que Google, Amazon.com, Facebook ou eBay, le NoSQL s'est aussi étendu par le bas après 2010. Il renonce aux fonctionnalités classiques des SGBD relationnels au profit de la simplicité. Les performances restent bonnes avec la montée en charge (scalabilité) en multipliant simplement le nombre de serveurs, solution raisonnable avec la baisse des coûts, en particulier si les revenus croissent en même temps que l'activité. Les systèmes géants sont les premiers concernés : énorme

II.4. Conclusion :

Le Cloud, c'est un nouveau challenge pour les entreprises qui commence. Des nouveaux métiers sont en train d'apparaitre. Ils vont bousculer l'existant. L'urbanisation des services, la mesure de la performance (réduction des factures), la construction de la valeur ajoutée, la formation Cloud, le pilotage d'un centre (de service) Cloud, etc.

Le Cloud est un sujet vaste, beaucoup, beaucoup plus vaste, c'est une transformation de la société en profondeur. L'informatique à la demande existe depuis un moment (ASP), le mouvement prend de l'ampleur.

C'est un domaine, un secteur en plein ébullition, difficile à comprendre pour un novice, qui demande des compétences techniques, logicielles, commerciales et des idées de création de valeurs pour l'entreprise.

Le marché du Cloud s'adresse à trois populations :

- Une entreprise qui souhaite développer (ouvrir) son informatique, ses usages sur l'extérieur, tester des concepts, des idées et être plus proche de ses clients (Co création de valeur). Elle va investir dans la recherche et le développement, dans l'innovation, dans un contexte de maitrise des coûts.
- Une entreprise consommatrice, qui souhaite faire appel à des services externes, pour réduire les coûts internes de son informatique. Cette entreprise va découper les fonctions transverses, et rechercher des économies de services.
- Une entreprise hybride, qui va consommer et produire des nouveaux usages et services.

Il faut sensibiliser et convaincre les DSI, et les décideurs des entreprises, de l'intérêt et des perspectives de l'informatique de demain. Il faut **simplifier**, et **banaliser** les usages pour tous. Par exemple, Apple propose désormais des services Cloud gratuits pour ses clients. L'informatique de l'utilisateur est partagé, et disponible depuis tous les médias de la pomme (ordinateurs, tablettes, Smartphone). Les utilisateurs adhèrent à la mobilité de leurs données.

Les enjeux pour les entreprises sont importants. Il faut créer de la valeur en adéquation avec les valeurs de l'entreprise et créer de la valeur **sociable et sociale** (référence à Facebook). Il faut concilier les deux. On parle d'esprit d'entreprise, de faire mieux avec moins de moyen, de développer la cohésion des groupes en interne, on parle beaucoup d'innovation, d'intuition, d'agilité, d'endroit ou il faut être (the place to be). Maintenant, il faut créer le lien.

CHAPITRE III : Datacenter et la sécurité physique

III.1. Introduction

Au centre du système d'information, le Datacenter concentre les données et les traitements informatiques. En effet, le lieu d'hébergement des données est généralement multiple, et réparti sur plusieurs Datacenter. Il est donc un espace aménagé et sécurisé pour abriter, traiter et protéger les données. Il peut éventuellement être un centre de backup (centre de sauvegarde), un centre de fall-back (centre de secours) ou un centre de documentation électronique.

III.2. Datacenter

Un **centre de traitement de données** (*data center* en anglais) est un site physique sur lequel se trouvent regroupés des équipements constituants du système d'information de l'entreprise (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien de prestataires. C'est un service généralement utilisé pour remplir une mission critique relative à l'informatique et à la télématique. Il comprend en général un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée.

Cette infrastructure peut être propre à une entreprise et utilisé par elle seule ou à des fins commerciales. Ainsi, des particuliers ou des entreprises peuvent venir y stocker leurs données suivant des modalités bien définies.

Un Datacenter est toujours constitué de trois composants élémentaires :

- **L'infrastructure**

C'est-à-dire l'espace et les équipements nécessaires au support des opérations du Datacenter. Cela comprend les transformateurs électriques, les alimentations, les générateurs, les armoires de climatisation, les systèmes de distribution électrique, etc.

- **Les équipements informatiques**

Comprenant les racks, les serveurs, le stockage, le câblage ainsi que les outils de gestion des systèmes et des équipements réseaux.

- **Les espaces d'exploitation**

C'est-à-dire le personnel d'exploitation qui pilote, entretient et répare les systèmes IT et non-IT lorsque cela est nécessaire.

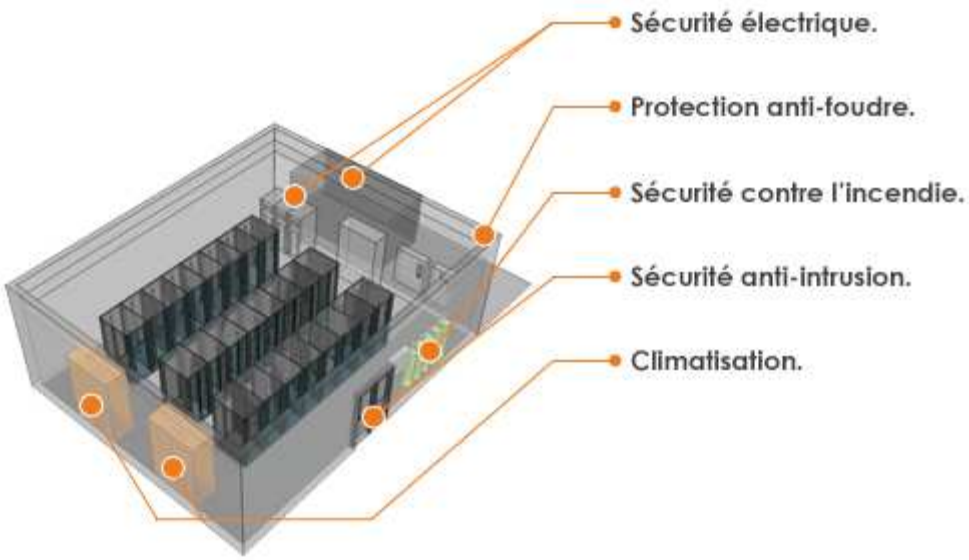


Figure III.1 : Une infrastructure maitrisée en interne

.

III.3. Les caractéristiques fondamentales du Datacenter

III.3.1. Disponibilité électriques

La fonction la plus évidente du Datacenter est sa capacité à fournir de l'énergie électrique conformément au besoin de puissance et avec la stabilité requise par les équipements informatiques. Cette fourniture électrique doit répondre à trois exigences incontournables :

- Fournir de l'électricité en qualité suffisante.
- Fournir de l'électricité de haute qualité.
- Fournir de l'électricité secourue.

III.3.2. Systèmes de refroidissement

Le dispositif de refroidissement doit répondre à trois exigences principale :

- Refroidissement des équpements.
- Refroidissement des baies.
- S'accommoder avec l'implantation des baies dans les salles.

III.3.3. Equipements informatiques

Pour traiter, stocker et router des informations, le Datacenter contient un grand nombre d'armoires qui accueillent différents composants informatiques : les serveurs d'applications, les serveurs de stockage et les éléments réseaux.

III.3.3.1. Rack

Le rack est une armoire sert à stocker plusieurs machines (serveurs physiques, routeurs, commutateurs…) sur une même surface en les empilant les unes sur les autres. Ce qui fait que l'on peut avoir jusqu'à 48 machines. Les racks assurent entre autre la sécurité des appereils.

Figure III.2 : Armoire Rack.

III.3.3.2. Serveurs

Un serveur est par définition, une machine sur laquelle les logiciels s'éxcutent. Les serveurs peuvent être classés suivant leur format et leur capacité de traitement. On distingue trois grandes catégories.

- **Les serveurs tradtionnels (stand-alone)**

Sont les plus couramment utilisés à l'heure actuelle. Ils hébergent une à deux applications par machine physique, dotée d'un seul système d'éxploitation. Leur capacité de traitement est faible, mais largement suffisante pour exécuter une application. Chaque serveur possède sa propre alimentation électrique, son propre système de refroidissement, d'accès au réseau et de périphériques (claviern souris, écran).

- **Le serveur lame (Blade)**

Un serveur lame appelé encore serveur blade ou carte serveur est un serveur conçu pour un très faible encombrement. Alors qu'un serveur en rack n'est qu'un serveur traditionnel de taille un peu réduite, le serveur lame est beaucoup plus compact, car plusieurs composants sont enlevés, étant mutualisés dans châssis capable d'accueillir plusieurs serveurs lames.

Le chêssis fournit ainsi l'alimentation électrique, le refroidissement, l'accès au réseau, la connectique pour écran, clavier et souris.

- **Châssis à lame**

Le châssis permet de regrouper des équipements, habituellement présents dans chaque ordinateur traditionnel, offrant une plus grande efficacité. Le châssis permet aussi d'utiliser des

disques durs qui ne sont pas toujours physiquement présents dans le serveur lame, par exemple dans un contrôleur externe ou dans un SAN.

Serveur lame IBM HS20

Châssis à 16 lames

Figure III.3 : Le serveur lame et Châssis à lames

III.3.3.3. Stockage

La consommation électrique liée au stockage des données représente environ 30% de celle du Datacenter. Lorsque la majorité des serveurs aura été virtualisée, le stockage sera le premier poste de consommation énergétique, repréentant la moitié de la facture électrique liée à l'informatique. Cette énergie est utilisée pour écrire et lire l'information mais aussi pour garder l'information inscrite et disponible sur l'emplacement qu'on lui a donné.

On parle souvent de deux techniques de stockage :

- **Stockage local**

L'information est stockée sur le serveur qui l'utilise, on parle alors du DAS.

DAS :

Système de disque en attachement direct, par opposition au NAS qui est en attachement réseau. Le système disque ainsi installé n'est accessible directemenr qu'aux ordinateurs auquel il est raccordé.

- **Stockage dédié**

Le modèle de San regroupe le stockage en un seul réseau, et chaque serveur du réseau principale utilise une connexion iSCSI ou fibre Channel avec le SAN et bénéficie donc d'un accès à grande vitesse au stockage des données dans son ensemble. Chacun d'eux traite son espace SAN alloué comme un disque directement connecté et le SAN utilise le même protocole de communication que le plupart des serveurs pour communiquer avec leurs disques connectées.

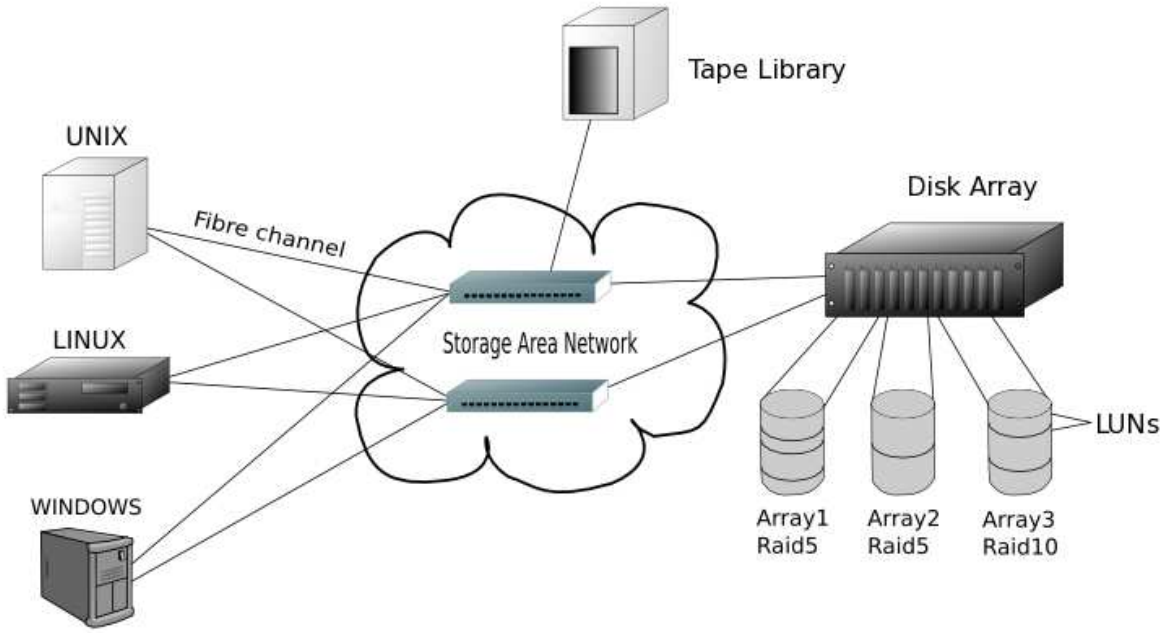


Figure III.4 : Représentation du SAN

Fibre Channel :

La solution la plus haute de gamme pour implémenter un réseau de stockage est l'utilisation d'une baie dédiée et du protocole Fibre Channel. Basé sur des fibres optiques, il assure une latence et un débit bien meilleurs qu'iSCSI, à un prix bien sûr élevé. Son principe d'utilisation est le même qu'un SAN iSCSI.

iSCSI :

L'iSCSI est un protocole d'accès disque fonctionnant sur un réseau Ethernet, il permet d'implémenter un réseau de stockage en profitant de la connectique et des équipements de commutation standards.

III.3.3.4. Réseau

Les éléments réseau servent à router les informations entre les utilisateurs et les serveurs. Ils sont principalement constitués de commutateurs (Switch), routeurs (router), coupes feux (firewalls) et répartiteurs de charge (load balancers). Physiquement, ils sont reliés à différents types de médias : fibre optique pour de longues distances, câble cuivre réseau, liaison radio, etc. Ces éléments supportent des fonctions de qualité de service qui leur permettent de gérer plusieurs réseaux dictincts en toute sécurité.

III.4. La Virtualisation

La virtualisation est une technique qui permet de partager et d'utiliser les ressources à partir d'un seul système informatique composé de plusieurs machines virtuelles. Chaque machine virtuelle fournit un système informatique complet très semblable à une machine physique. Ainsi, chaque machine virtuelle peut avoir avoir son propre système d'exploitation, applications et services réseau.

III.4.1. Intérêts

Les intérêts de la virtualisation sont nombreux, on peut citer principalement :

- Installation, déploiement et migration facile des machines virtuelles d'une machine physique à une autre, notamment dans le contexte d'une mise en production à partir d'un environnement de qualification ou de pré-production, livraison facilitée.
- Installation, tests, développements, cassage et possibilité de recommencer sans casser le système d'exploitation hôte.
- Sécurisation ou isolation d'un réseau (cassage des systèmes d'exploitation virtuels, mais pas des systèmes d'exploitation hôtes qui sont invisibles pour l'attaquent, tests d'architectures applicatives et réseau).
- Isolation des différents utilisateurs simultanés d'une même machine (utilisation de type site central).
- Allocation dynamique de la puissance de calcul en fonction des besoins de chaque application à un instant donné.
- Diminution des risques liés au dimensionnement des serveurs lors de la définition de l'architecture d'une application, l'ajout de puissance (nouveau serveur etc.) étant alors transparente.

III.4.2. Machine virtuelle

III.4.2.1. Principe

Une machine virtuelle est un ordinateur logiciel qui, à l'instant d'un ordinateur physique, exécute un système d'exploitation et des applications. La machine virtuelle se compose d'un ensemble de fichiers de spécification et de configuration, elle est secondée par les ressources physiques d'un hôte.

Chaque machine virtuelle a des périphériques virtuels qui fournissent la même fonction que le matériel physique et présentent un intérêt supplémentaire en termes de portabilité, maniabilité et sécurité.

Une machine virtuelle se compose de plusieurs types de fichiers qui peuvent être stocké sur un périphérique de stockage compatible. Les fichiers clés qui constituent une machine virtuelle sont les suivants : le fichier de configuration, le fichier de disque virtuel et le fichier de configuration NVRAM.

III.4.2.2. Composants de machine virtuelle

- Les machines virtuelles comportent un système d'exploitation ainsi que des ressources virtuelles et du matériel qui sont gérés de manière très semblable à un ordinateur physique.
- Un système d'exploitation client s'installe sur une machine virtuelle quasiment de la même manière que sur un ordinateur physique. On doit avoir un CD/DVD-ROM ou une image ISO contenant les fichiers d'installation d'un éditeur de système d'exploitation.
- Toutes les machines virtuelles ont une version matérielle. La version matérielle indique les fonctions de matériel virtuel prises en charge par la machine virtuelle, telles que le BIOS, le nombre de logements virtuels, le nombre maximum de CPU, la configuration de mémoire maximum ainsi que d'autre caractéristiques typiques du matériel.
- Les périphériques matériels indiqués dans l'éditeur de propriétés de la machine virtuelle complètent la machine virtuelle. Les périphériques ne sont pas tous configurables. Certains périphériques matériels font partie de la carte mère virtuelle et apparaissent dans la liste de périphériques étendus de l'éditeur de propriétés de la machine virtuelle.

III.4.3. Techniques de virtualisation

On distingue plusieurs techniques de virtualisation à savoir : l'isolation, la paravirtualisation et la virtualistualisation complète. Ces trois techniques sont détaillés dans ce qui suit :

Dans les systèmes de virtualisation, il faut noter les notions suivantes :

- SE hôte : le système d'exploitation installé sur la machine physique.
- SE invité : les systèmes d'exploitations des machines virtuelles.

III.4.3.1. Les isolateurs

L'isolation permet de diviser un système d'exploitation en plusieurs espaces mémoires ou encore contextes. Chaque contexte est géré par le SE hôte. Cette isolation permet de faire tourner plusieurs fois la même application prévue pour ne tourner qu'une seule fois par machine.

Les programmes de chaque contexte ne sont capables de communiquer qu'avec les processus et les ressources associées à leurs propre contexte. L'isolation est uniquement liée aux systèmes Linux.

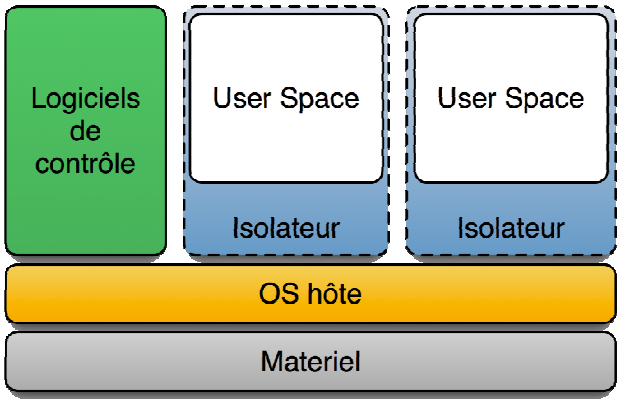


Figure III.5 : Isolateur.

III.4.3.2. La paravirtualisation (virtualisation type 1)

La paravirtualisation est une technique de virtualisation qui présente ç la machine invitée une interface mogicielle similaire mais non identique au matériel réel. Ainsi, elle permet aux systèmes d'exploitation invités d'intéragir directement avec le système d'exploitation hôte et donc ils seront conscients de la virtualisation.

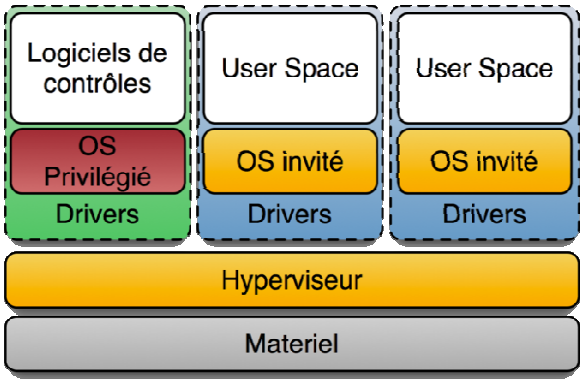


Figure III.6 : Paravirtualisation.

III.4.3.3. La virtualisation complète (virtualisation type 2)

la virtualisation complète est une technique de virtualisation qui permet de créer un environnement virtuel complet. En utilisant cette technique, le système d'exploitation invité n'interagit pas directement avec le système d'exploitation hôte et donc il croit s'exécuter sur une véritable machine physique.

Cette technique de virtualisation ne permet de virtualiser que des SE de même architecture matérielle que l'hôte.

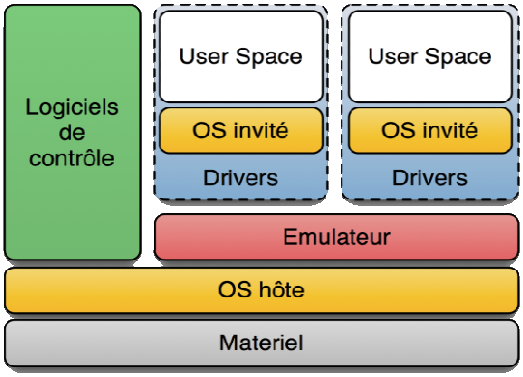


Figure III.7 : Virtualisation complète.

III.4.4. Virtualisation de Datacenter

La virtualisation du datacenter rend l'ensemble des ressources (serveurs, stockage, réseau) indépendantes de leur ssystème physique. Il devient ainsi possible de déplacer des machines virtuelles (par exemple serveurs virtuels) d'un Datacenter vers un autre, voire vers un hébergeur et bénéficier des avantages de la virtualisation indépendamment de la localisation.

Il existe différents types de virtualisation mais le plus connus est la virtualisation des serveurs.

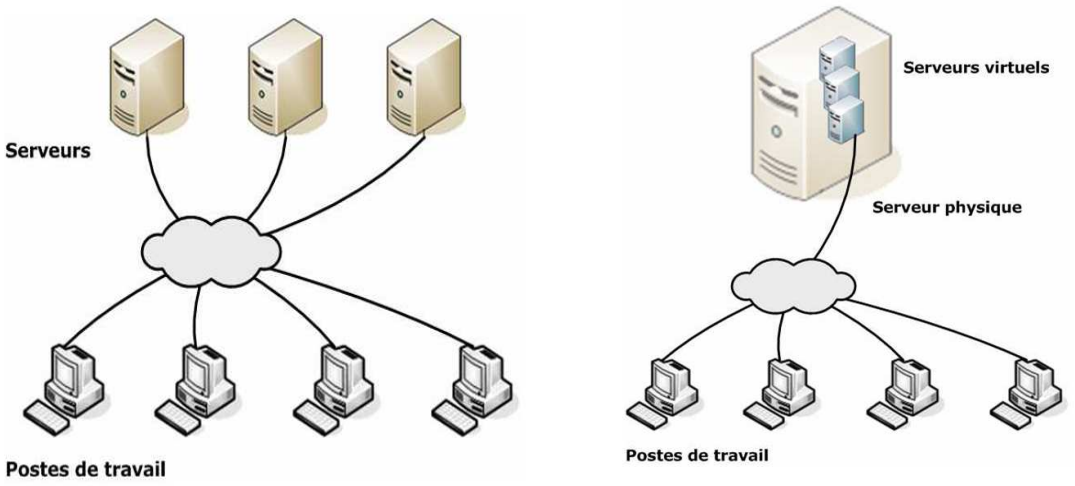
Ces différents types de virtualisation sont :

III.4.4.1. La virtualisation des serveurs

La virtualisation des serveurs sépare e matériel du système d'exploitation permettant de faire fonctionner plusieurs systèmes d'exploitation sur un même serveur physique. Elle utilise un logiciel pour sréer un système d'exploitation dépare qui est logiquement isolé du serveur hôte. En fournissant plusieurs systèmes virtuels à la fois, un Datacenter peut exécuter plusieurs systèmes d'exploitation en même temps sur un seul serveur physique.

✓ **Avantages**

- **Compatibilité :** les serveurs virtuels sont compatibles avec tous les standards X86 et autres.
- **Isolation :** les serveurs virtuels sont isolés des autres machines si elles étaient des machines physiques.
- **Encapsulation :** les serveurs virtuels encapsulent un environnement informatique complet. Indépendance matériel : les serveurs virtuels fonctionnent indépendamment du matériel inhérent.



Avant la virtualisation Après la virtualisation

Figure III.8 : Virtualisation des serveurs.

III.4.4. 2. La virtualisation des applications

La virtualisation des applications sépare du système d'exploitation la couche de configuration des applications. Elle permet aux applications d'être exécutées sur des clients (ordinateurs) sans y être installées, et d'être administrées à partir d'un emplacement central.

Dans un environnement sans virtualisation d'application, les applications sont directement installées sur le systèmé d'exploitation alors qu'avec la virtualisation des applications, chaque application fonctionne dans son propre environnement d'exécution protégé qui l'isole des autres applications et du système d'exploitation sous-jacent.

- ✓ **Avantages**

L'avantage de la virtualisation des applications est donc la résolution des problèmes de comptabilité entre plusieurs applications installées sur un même système d'exploitation.

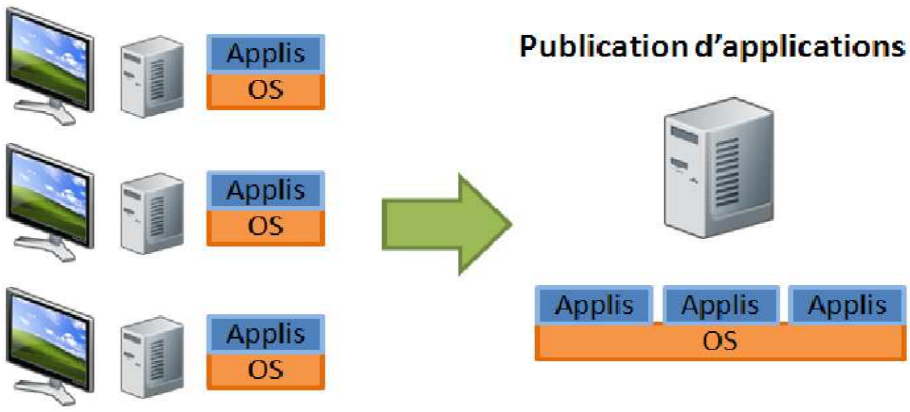


Figure III.9 : Virtualisation d'applications.

III.4.4.3. La virtualisation des postes de travail

La virtuamisation des postes de travail crée un environnement de système d'exploitation séparé sur le poste de travail, permettant aux applications non compatibles defonctionner sur un système d'exploitation plus moderne.

Dans un environnement sans virtualisation de poste de travail, chaque ordinateur physique exécute un seul système d'exploitation aui est étroitement lié à ce matériel alors qu'en utilisant la même approche que la virtualisation des serveurs, la virtualisation des postes de travail permet de créer des systèmes virtuels séparés sur un même poste de travail, chacun virtualisant le matériel d'un ordinateur physique complet.

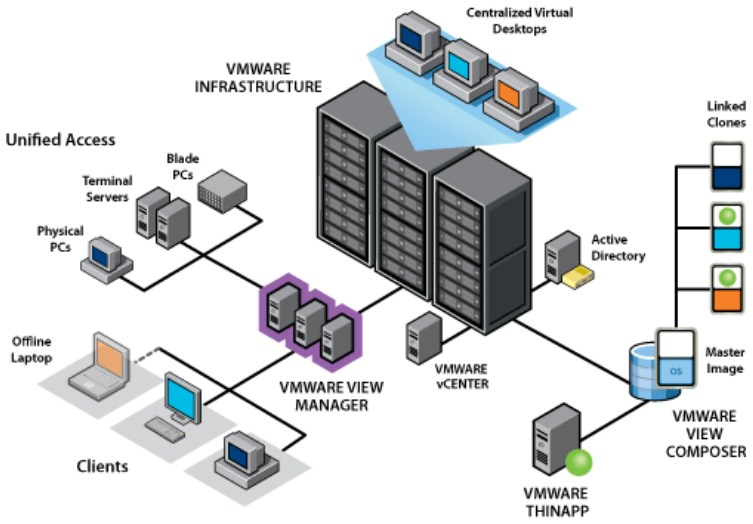


Figure III.10 : Virtualisation de postes de travail.

III.4.4.4. La virtualisation du stockage

La virtualisation du stockage permet à de nombreux utilisateurs ou applications d'accéder au stockage sans se soucier de son emplacement physique ni de la façon dont il est administré. Ainsi, le stockage physique d'un environnement peut être partagé entre plusieurs serveurs d'application. Par ailleurs, les équipements physiques derrière la couche de virtualisation peuvent être virtualisés et administrés comme s'ils formaient un seul groupe de stockage sans aucune limite physique.

✓ **Avantages**

- Possibilité de masquer ou de cacher des volumes à la vue des serveurs qui ne sont autorisés à y accéder, ce qui fournit un niveau de sécurité additionnel.
- Possibilité de modifier ou d'augmenter les volumes à la volée pour répondre aux besoins des différents serveurs.

III.4.4.5. La virtualisation des réseaux

Une illustration de la virtualisation des réseaux est le VPN. Les VPNs rendent abstraite la notion d'une connexion réseau, permettant à un utilisateur distant d'accéeder au réseau interne d'une entreprise comme s'il était physiquement rélié à ce dernier.

✓ **Avantages**

- L'avantage de la virtualisation des réseaux est qu'elle favorise la protection des environnements informatiques des menaces Internet tout en offrant aux utilisateurs un accès rapide et sécurisé aux applications et données.

III.4.5. Les avantages et les inconvénients de la virtualisation

✓ **Avantages**

- ***La sous exploitation des serveurs physiques :*** il est estimé que dans un Datacenter privé, le taux d'utilisation moyen est de 10%. Celui-ci passe à 35% sur une architecture virtuelle.
- ***La croissance du nombre de serveurs physique :*** les ressources physiques d'un serveur seront partagée entre différents serveurs virtuels ce qui permet de ne pas acheter plusieurs serveurs physiques.
- ***La sécurité et la fiabilité :*** isoler les services sur des serveurs différents.
- ***Gestion automatiques de la puissance serveur :*** L'hyperviseur qui gère les serveurs physiques peut d'une manière automatisque régler la puissance du serveur à chaud : augmenter la mémoire RAM, l'espace disque, la puissance des processeurs, etc.
- ***Isolation :*** les machines virtuelles sont considérées comme des ordinateurs physiques et donc possèdent chacune sa propre adresse IP.
- ***Disaster recovery :*** d'une manière automatique, un système de snapshot est mis en place toutes les heures. En cas de crash du serveur, nous pouvons démarrer les sauvegardes des serveurs. Celles-ci sont également sauvegardées d'une manière dissociée par rapport aux serveurs physiques.
- ***Migration à chaud :*** le transfert d'une machine virtuelle d'un serveur à un autre serveur peut se faire sans arrêter la machine virtuelle.
- ***Disponibilité :*** le Cloud Computing se base sur la virtualisation. En effet, l'ensemble des machines est virtualisé et tourne sur un ou plusieurs serveurs physiques. Il n'y a plus une machine physique qui fait tourner le serveur, mais bin plusieurs serveurs physiques. Si l'un d'eux tombe en panne, les autres sont présents afin d'assurer une haute disponibilité.

✓ **Inconvénients**

- ***Les performances :*** selon la technique de virtualisation utilisée, l'impact sur les performances en entrées/sorties peut être inportant rendant difficile la virtualisation de certaines applications.
- ***Configurations plus puissantes (mémoires, CPU,…).***

III.5. La sécurité physique dans le Cloud Computing

La sécurité physique dans le Cloud Computing permet de garantit :

- ✓ L'extensibilité des resssources,
- ✓ La disponibilité,
- ✓ La fiabilité,
- ✓ L'intégrité des données.

a) Extensibilité

L'éxtensibilité est principalement fournit par la virtualisation. Celle-ci permet de rajouter des ressources très rapidement et très efficacement. La virtualisation consiste à lancer un ou plusieurs systèmes d'exploitation sur un ou plusieurs ordinateurs à la place d'avoir un système d'exploitation par ordinateur. Les systèmes d'exploitation dans un environnement virtuel. Les principaux composants de cet environnement sont :

- **La machine virtuelle :** les ressources logicielles et matérielles (principalement la puissance de calcul) sont simulées. Le système d'exploitation peut alors s'executer comme s'il s'agissait d'une machine physique.
- **Le stockage virtuel :** seule une partie de la puissance de stockage de la machine physique n'est visible pour chaque machine virtuelle.
- **Le réseau virtuel :** seule une partie de la bande passante disponible et de l'espace d'adressage (adresse IP) n'est disponible pour chaque machine virtuelle. Cela permet de communiquer avec une machine virtuelle comme s'il s'agissait d'une machine physique connectée sur le réseau.

b) Disponibilité et fiabilité

Le Cloud Computing fournit également la disponibilité et la fiabilité. Ceci est réalisé par le biais de la répartition de charge. La répartition de charge est une technique permettant de distribuer le travail entre toutes les ressources disponibles. Cela est réalisé à l'aide d'un load balancer qui transmet à tour de rôle les requêtes à chaque ressource. Cette technique est largement utilisée pour minimiser le temps d'accès aux bases de données et aux sites web.

Grâce à l'aide d'un système de secours, le plan de continuité d'activité a pour but de garantir la disponibilité de services fournis par une entreprise en permettant de redémarrer raapidement l'activité en cas de crise majeure. Le Cloud Computing donne la possibilité de lancer des instances de serveurs (machines virtuelle) sur des serveurs éloignés physiquement. Si un sinistre majeur touce une partie des serveurs physiques.

c) Intégrité

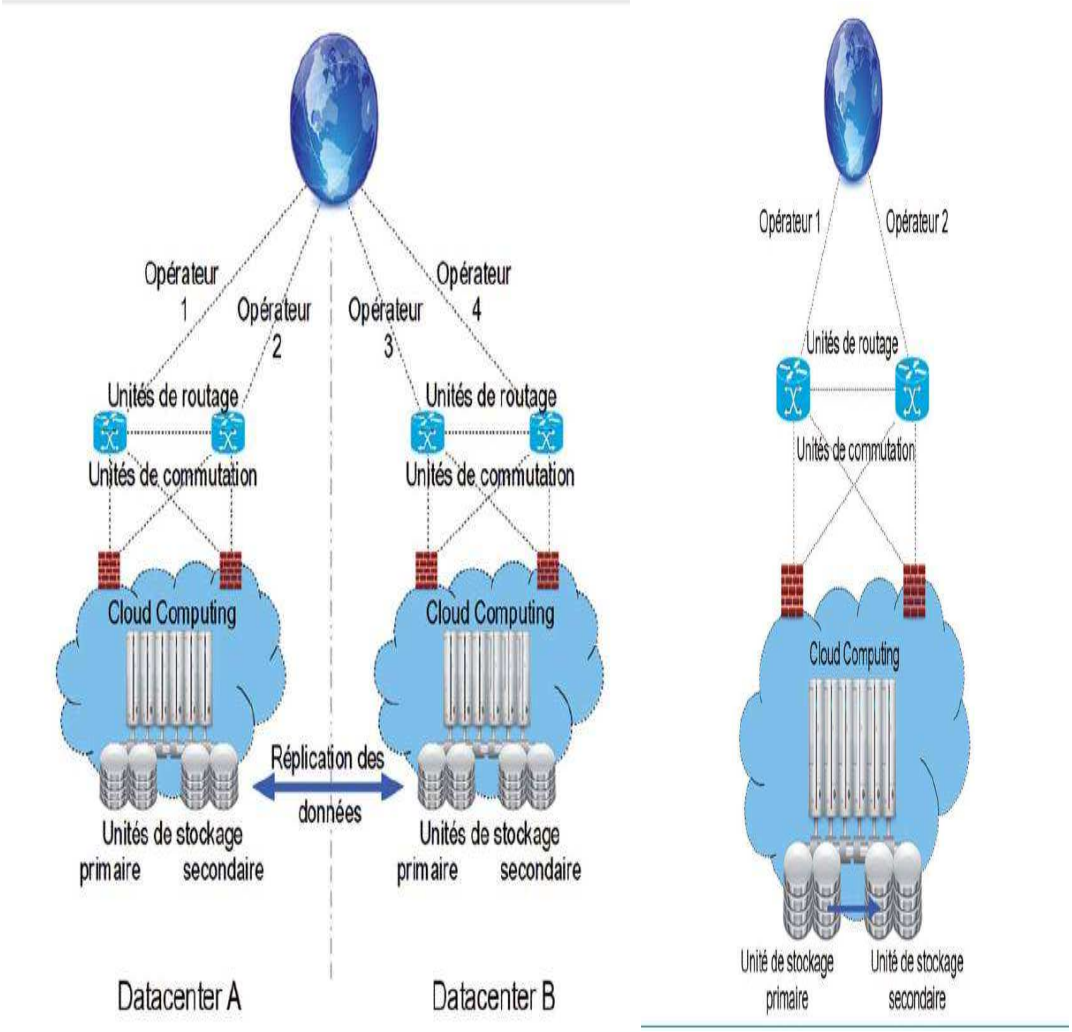
L'intégité des données est fournie grâce à des techniques de souvegarde entre des bases de données physiquement éloignées l'une de l'autre. Plusieurs copies des données sont automatiquement réalisées afin de faciliter la restauration des données. Les principales techniques employées sont l'utilisation de RAID ou de SAN.

III.5.1. Sécurité physique

III.5.1.1. Disaster recovery

Une catastrophe d'origine humaine ou naturelle peut avoir des impacts radicaux sur le fonctionnement du Cloud Computing et amplifier une panne totale ou partielle du service. La perte totale de l'infrastructure du Cloud Computing pourrait entrainer une nterruption de service d'une durée indéterminée et une perte de données irrémédiable sans possibilité de remise en service de l'infrastructure.

Une archirecture de secours doit exister, sur un site géographiquement éloigné, avec des équipements redondants et permettant de réaliser un PCA (plan de continuité d'activité) sans interruption de service.



Architecture multi-Datacenter Architecture mono-Datacenter

Figure III.11 : Architecture du Datacenter

III.5.1.2. Redondance matérielle

l'architecture Cloud Computing doit garantir un accès au service en très haute disponibilité avec des performances optimales. La seule défaillance d'un équipement matériel peut engendrer une dégradation ou une coupure du service voire une perte de données. Pour limiter les risques d'arrêt de service liés à la défaillance d'un aquipement, il est nécessaire de le redonder.

Une réplication des configurations entre les équipements peut faciliter la bonne prise en charge de la redondance et ainsi augmenter la haute disponibilité du service.

De plus, une redondance des moyens de connexion, par la multiplication des liaisons, des opérateurs, et des chemins d'accès permet une accessibilité accrue au service en augmentant la tolérance aux pannes.

III.5.1.2.1 La haute disponibilité

La haute disponibilité correspond au fait de maintenir l'accessibilité d'un service suivant un taux de disponibilité élevé. Pour cela il faut mettre en place une architecture matérielle dédiée et donc de la redondance matériels, la sécurisation des données afin de garantir leurs intégrités (RAID, Sauvegarde…), la répartition de charge pour faire face à des pics d'activités.

III.5.1.2.1.1 La répartition de charge (Load Balancing)

La répartition de charge consiste à mettre un système entre les clients (demandeures de ressources) et les ressources. Ce système se chargera de désigner le fournisseur le mois occupé au moment de la demande pour servir le client.

Les demandes seront amors réparties sur plusieurs fournisseurs de ressources au lieu d'un seul. Dans une architecture classique, c'est-à-dire une connexion directe entre les clients et le serveurs, lors de fortes activités, de serveur ne pourra pas servir tout le monde et l'accès aux ressources sera bloqué. C'est ce qu'on appelle déni de service. La partition de charge permet d'optimiser le trafic et de répartir les chargees sur un ensemble de seveurs. La capacité totale de traitement est alors plus importante.

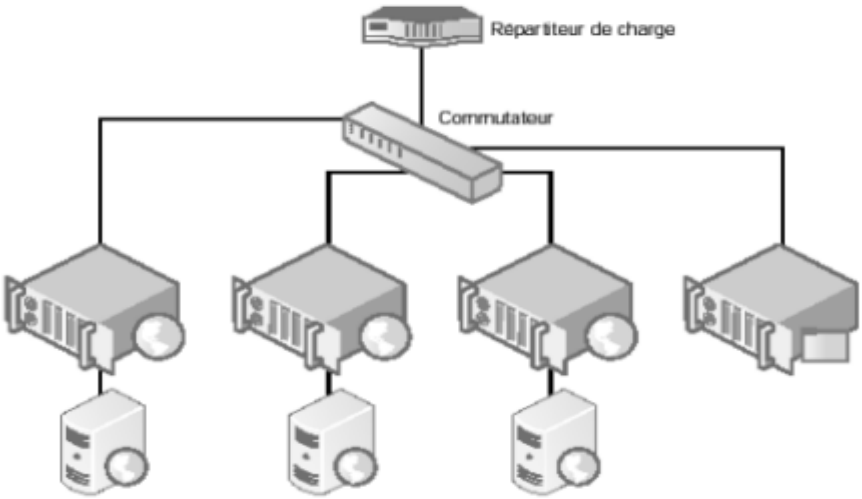


Figure III.12 : la répartition de charge

- ✓ Avantages

La répartition de charge est une forme d'optimisation. Les avantages sont nombreux.

- Augmentation de la qualité des services.
- Amélioration des temps de réponse des services.
- Capacité à palier la défaillance d'une ou de plusieurs machines.

III.5.1.2.1.2. Le DNS

- **Principe de fonctionnement**

La répartition de charge de niveau DNS intervient dans l'association d'une adresse IP à un nom de serveur.

Lorsque le navigateur doit accéder à un serveur dont il connait le nom, par exemple *www.google.fr*. Il commence par recherche l'adresse IP correspondante à ce serveur www sur le domaine google.fr. Il adresse une requête à son serveur DNS, qui lui-même, s'il ne dispose pas de formation, interrogera d'autre serveurs DNS, de manière récursive.

Une fois que le poste client a obtenu l'adresse IP, il a conserve en cache selon différentes règles, généralement d'une demi-heure.

C'est dans cette phase d'association entre un nom de serveur et une adresse IP, c'est-à-dire un serveur web, qu'intervient la répartition de charge de niveau DNS, simplement en fournissant différentes adresses IP pour un même nom de serveur.

III.5.1.2.2 Cluster

III.5.1.2.2.1. Définition

Un cluster (grappe) est un ensemble d'ordinateurs connectés les uns aux autres en réseau dans le but de partager des ressources. Ces ordinateurs sont appelés nodes (nœuds) et l'ensemble forme le cluster.

III.5.1.2.2.2. Réseau de répartition de charge (NLB)

NLB permet d'équilibrer le trafic IP entrant. Il réparti de manière transparente les demandes des clients entre les serveurs d'un cluster NLB en utilisant des adresses IP virtuelles. Du point de vue du client, le cluster NLB semble être un serveur unique. NLB est une solution entièrement distrbuée par le fait qu'il n'utilise pas un répartiteur centralisé.

A travers différents règles établies les connexions entrantes sont réparties entre les différents nœuds du cluster, il peut y avoir jusqu'à 32 nœuds pour équilibrer la charge IP en mode Network Load Balancing.

Le service d'équilibrage de charge de réseau augmente le disponibilité et la montée en charge des apllications serveur basées sur l'accès Internet, tels que des serveurs WEB, des serveurs médias streaming, serveur Windows Terminal serveur ou autres.

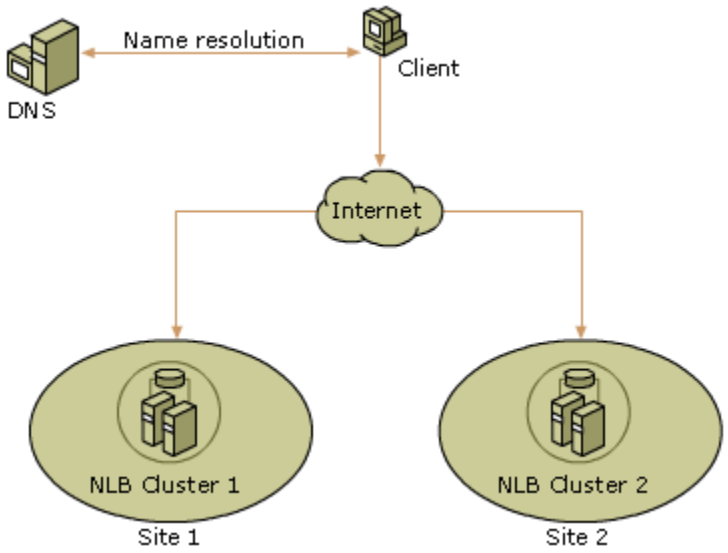


Figure III.13: Network Load Balancing

III.5.1.2.2.3. Cluster de basculement (Failover Clustering)

Un cluster de basculement est groupe de deux ou plusieurs ordinateurs utilisés pour éviter les temps d'arrêt des applications et services sélectionnées. Les serveurs en cluster (appelés nœuds) sont connectés par des câbles physiques les uns aux autres et au stockage de disque partagé. Si l'un des nœuds du cluster tombe en panne, un autre nœud commence à prendre plus de service pour le nœud perdu dans un processus appelé basculement. A la suite de basculement les utilisateurs se connectant au serveur expérience minimum de perturbations dans le service.

Les serveurs d'un cluster de basculement peuvent fonctionner dans une variété de rôles y compris les rôles de serveur de fichiers, serveurs d'impression, serveur de messagerie, ou un serveur de base de données, et ils peuvent fournir une haute disponibilité pour une variété d'autre services et applications.

Dans la plupart des cas, le cluster de basculement comprend une unité de stockage partagé qui est physiquement connecté à tous les serveurs de la grappe, bien que tout le volume donné dans le stockage soit accessible par un seul à la fois.

La figure illustre le processus de basculement dans un cluster de basculement à deux nœuds de base.

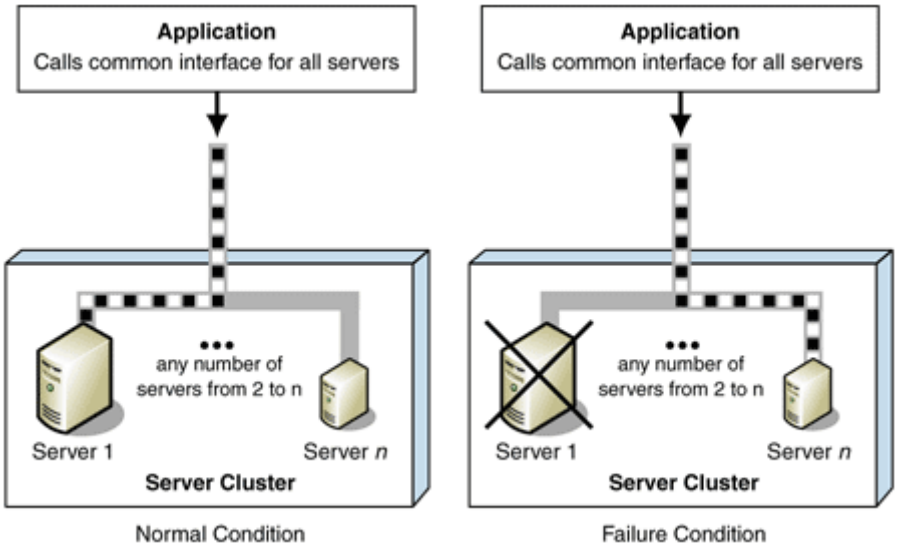


Figure III.14: Failover Cluster

Avantages et Inconvénients du Cluster

- ✓ ***Avantages***
  - Haute disponibilité.
  - Sécurité.
  - Redondance.
  - Rapidité.

- ✓ ***Inconvénients***
  - Coût important.
  - Nécessite de solides connaissances informatiques.
  - Technique gourmande en bande passante et en temps.

III.5.1.3. Sécurisation des données

La possibilité de réimplanter les données rapidement et sans corruption de celle-ci. On peut utiliser les technologies de RAID, le stockage des copies des données sur un serveur de sauvegarde.

- ➢ **Technologies de récupération de données**

La sécurité de l'information passe par la disponibilité de celle-ci, y compris lorsqu'il y a eut une attaque ou un problème matériel/logiciel.

Il existe plusieurs solutions pour parvenir à cet objectif indispensable au bon fonctionnement de l'entreprise.

Le RAID : est un ensemble de technique permettent de répartir les données sur plusieurs disques durs. Son but est l'amélioration de la tolérance aux pannes et les performances du système. Il existe différents niveaux de RAID dont les principaux sont :

III.5.1.3.1. Les niveaux Raid

RAID 0 : à entrelacement de disques : ce système permet de faire travailler plusieurs disques en parallèle, accélérant les traitements, mais ne permet pas de redondance et donc n'apporte aucune sécurité.

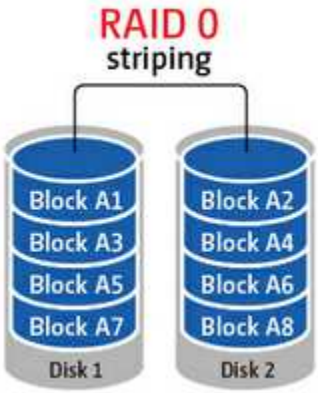


Figure III.15: RAID 0

RAID 1 : en miroir : Ce système permet une grande sécurité des données puisque qu'il y a redondance. Chaque information étant présente sur tous les disques de la grappe.

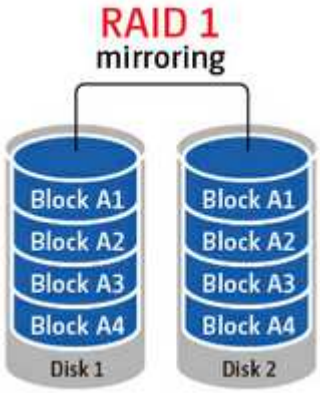


Figure III.16 : RAID 1

RAID 5 : La capacité de mémoire d'un disque est utilisée pour stocker les informations de parités. Celles-ci vérifient la cohérence des données. Cette solution permet une amélioration des performances tout en augmentant la tolérance aux pannes.

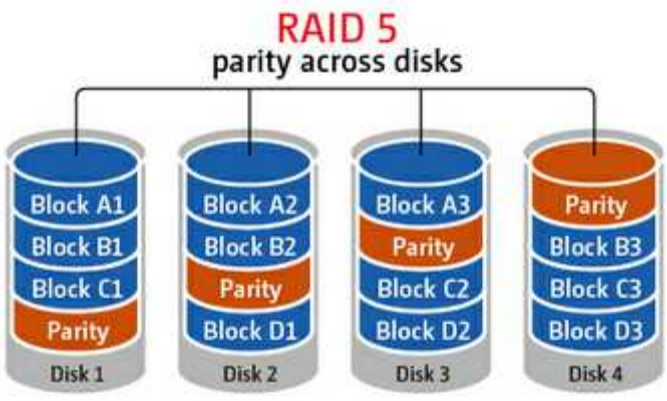


Figure III.17 : RAID 5

RAID 10 : c'est une combinaison entre l'agrégat et le miroir. Il est donc le plus sûr et le plus performent. Il est rapide car les données sont réparties sur plusieurs disques, il est sûr car le contrôle de parité est réparti sur tous les disques.

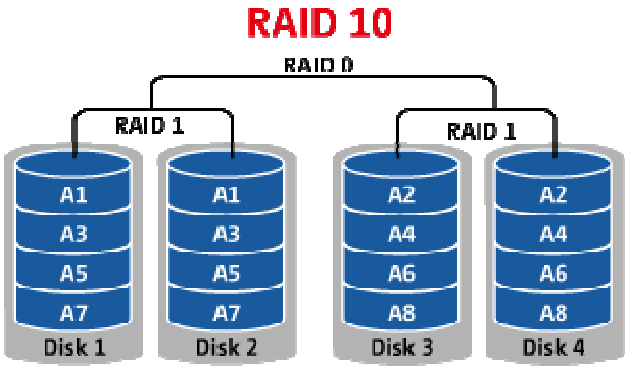


Figure III.18 : RAID 10

III.6. Conclusion

Les Datacenters assurent le premier niveau de sécurité (la sécurité physique) qui concerne tout l'environnement du système d'information (sécurité d'accès, Load Balancing, redondance matérielles, Failover cluster, protection contre les inondations, …) par les moyens bien étudiés et bien conçus. Dans les deux chapitres nous avons bien présenté le concept du Cloud Computing est ces différents éléments. Le prochain chapitre nous allons mettre en œuvre la solution du Cloud Computing.

CHAPITRE IV : Réalisation de la solution Cloud Computing

IV.1. Introduction

Quelle que soit la performance et l'efficacité des outils et techniques utilisés pour la mise en place d'une solution de sécurité, il reste difficile, voire impossible, d'assurer la sécurité à 100%.

L'évènement d'internet et des nouvelles technologies donnent une raison et une curiosité motivante aux pirates et aux malveillants de pénétrer de plus en plus dans les réseaux que ce soit par fun ou pour usurper des données et informations confidentielles.

Dans cette solution nous essaierons de minimiser au maximum les risques d'attaques et les points vulnérables de la banque en accordant aux différents administrateurs la responsabilité de sensibiliser les membres de l'entreprise au secret professionnel.

Dans ce chapitre, nous représenterons les différentes étapes suivies afin d'implémenter les solutions citées précédemment.

IV.2. Présentation des outils utilisés

IV.2.1. Le simulateur graphique de réseaux

Dans le but de se rapprocher le plus possible de la mise en place d'une architecture réseau réelle, nous avons opté pour l'utilisation de GNS3 (Graphical Network Simulateur). Un logiciel open source qui est à la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur de routeurs et firewalls CISCO et Juniper. Autant que simulateur il imite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel. (Dans l'annexe A, vous trouverez plus d'information sur le fonctionnement et l'installation de GNS3).

GNS3 0.8.3.1
Under GPL v2 license

Developers:
Jeremy Grossmann
Benjamin Marsili
Claire Goudjil
Alexey Eromenko "Technologov"

Former developers:
Xavier Alt
Romain Lamaison
Aurelien Levesque
David Ruiz

Visit our website
Make a donation
Contact us

IV.2.2. La VMware Workstation 9.0.0

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 9.0.0. Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique. Cette version exécute les applications les plus exigeantes, elle utilise le dernier

matériel pour répliquer l'environnement des serveurs postes de travail tout en étant accessible de n'importe quel périphérique grâce à son interface Web.

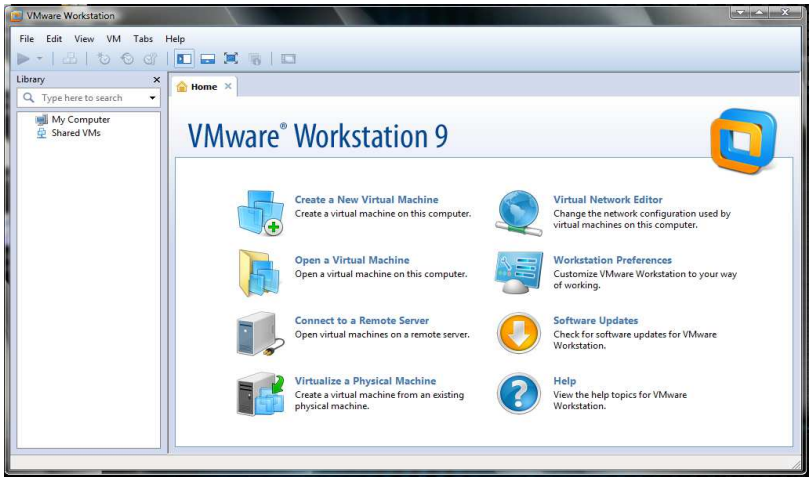


Figure IV.1: VMware Workstation 9.

IV.2.3. Microsoft Windows Server 2012

Microsoft Windows Server 2012, anciennement connu sous le nom de code Windows Server 8, est la dernière version du système d'exploitation réseau Windows Server .

Il s'agit de la version serveur de Windows 8 et du successeur de Windows Server 2008 R2. Windows Server 2012 est la première version de Windows Server à ne pas supporter les systèmes Itanium depuis Windows NT 4.0.

IV.2.4. Active Directory

Pour réaliser la gestion des objets sans liens avec la disposition réelle des protocoles réseaux employés, nous avons utilisé Active Directory qui est un annuaire des objets du réseau. Il permet aux utilisateurs de localiser, gérer et utiliser facilement les ressources, en organisant l'annuaire en sections, ce qui permet de suivre le développement d'une société allant de quelques objets à des millions d'objets. Combiné aux stratégies de groupes, Active directory permet une gestion des postes distants de façon complètement centralisée.

IV.2.5. Les caractéristiques du PC utilisé

Vu que notre application exige de grandes ressources matérielles, l'utilisation d'un PC professionnel était primordiale pour regrouper les solutions proposées, réseaux et systèmes. Les caractéristiques du PC portable professionnel utilisé sont :

- ✓ Processeur I7 x64 bits
- ✓ RAM 6G
- ✓ Disque dur 750 G
- ✓ Système Windows 7 professionnel x64 bits
- ✓ Prise en charge de la virtualisation.

IV.2.6. les images IOS:

1. Pour le router on a utilisé **ios cisco 7200**

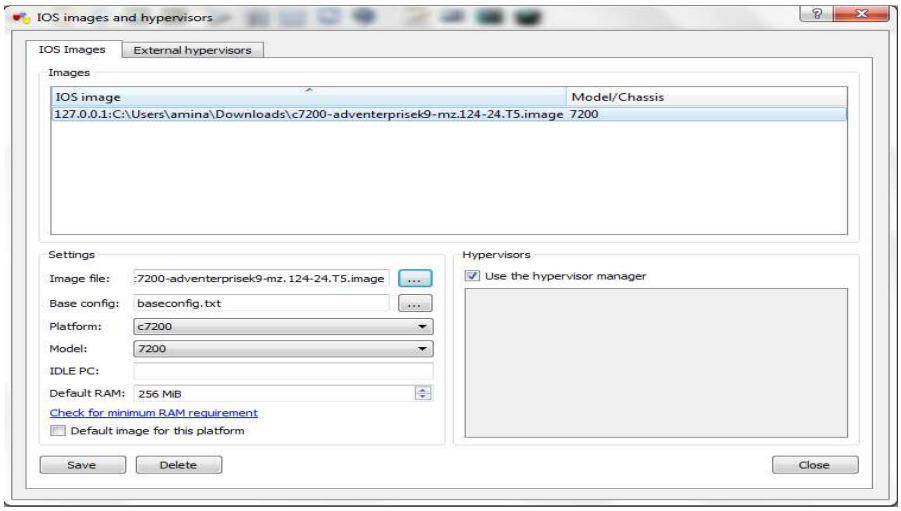


Figure IV.2: Charger l'image ISO du l'outil.

2. Pour **ASA** on a besoin de :
   - RAM de 256 MB ;
   - Champ **Initrd :** on doit chercher le fichier **initrd asa802-k8.initrd** ;
   - Champ **kernel :** on doit aussi chercher le fichier **kernel asa802-k8.kernel** ;
   - Aussi la commande cmd line : **console=ttyS0,9600n8 bigphysarea=16384 auto nousb ide1=noprobe hda=980,16,32**.

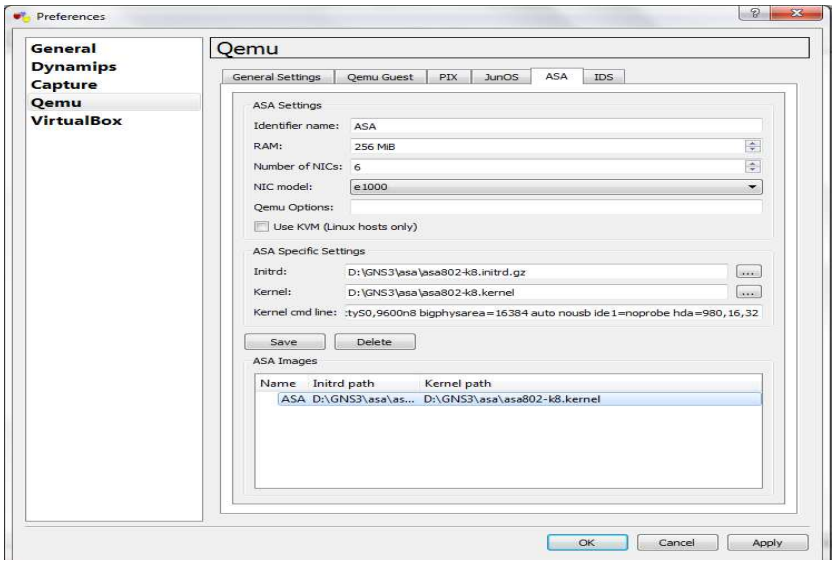


Figure IV.3: Remplir les champs du Qemu ASA.

IV.3. Les étapes suivies pour la mise en place de notre application

Vu qu'il est impossible d'implémenter toute l'infrastructure réseau de l'entreprise avec les solutions réseaux et systèmes proposées. Nous avons simplifié l'architecture de sorte à permettre la mise en place de notre politique de sécurité. La figure suivante montre l'architecture simplifiée.

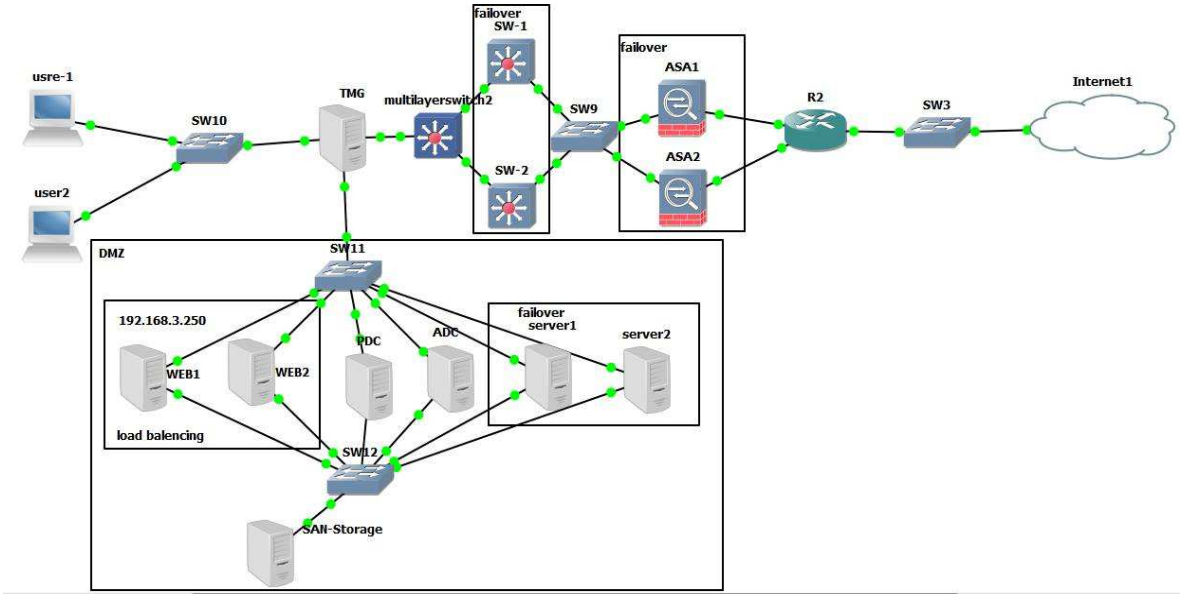


Figure IV.4: Notre architecture simplifiée.

- Dans ce qui suit, nous présentons les différentes étapes suivies pour la réalisation de notre application.

IV.3.1. la préparation des machines

Nous avons préparé les machines suivantes :

- ✓ Un contrôleur de domaine principal.
- ✓ Un contrôleur de domaine secondaire.
- ✓ Un serveur membre pour l'installation de la TMG.
- ✓ Un serveur SAN Storage.
- ✓ Deux machines membres pour l'implémentation de la solution Load Balancing.
- ✓ Deux machines membres pour l'implémentation de la solution Failover.
- ✓ Deux serveur membre pour l'installation de Microsoft Exchange Server 2010 et aussi implémenter de la solution Load Balancing et Failover.
- ✓ Deux serveurs membre pour l'installation de serveur Web implémenté de la solution Load Balancinget Failover.
- ✓ serveur Certification d'Autorité (CA).

1. L'installation du contrôleur de domaine principale et secondaire

Windows Server 2012: Active Directory Domain Services

Active Directory est la base d'un réseau Microsoft. Il permet la gestion des ressources : utilisateurs et périphériques, l'authentification et la sécurisation des accès. Mais c'est aussi la base de nombreux autres services comme DNS, WINS, DHCP, …..

Après préparation de deux machines virtuelles Windows Server 2012, nous avons installé sur la première machine un contrôleur de domaine principal (PDC), **RTGS.com.** Sur la deuxième machine nous avons effectué le déploiement du contrôleur de domaine pour avoir un contrôleur de domaine secondaire (ADC). Ce dernier sert à la réplication du PDC.

L'installation des deux contrôleurs est la même à la différence du choix de l'étape montrée ci-dessous. La première figure montre le choix de la création d'un nouveau domaine principal et la deuxième l'installation d'un contrôleur de domaine secondaire.

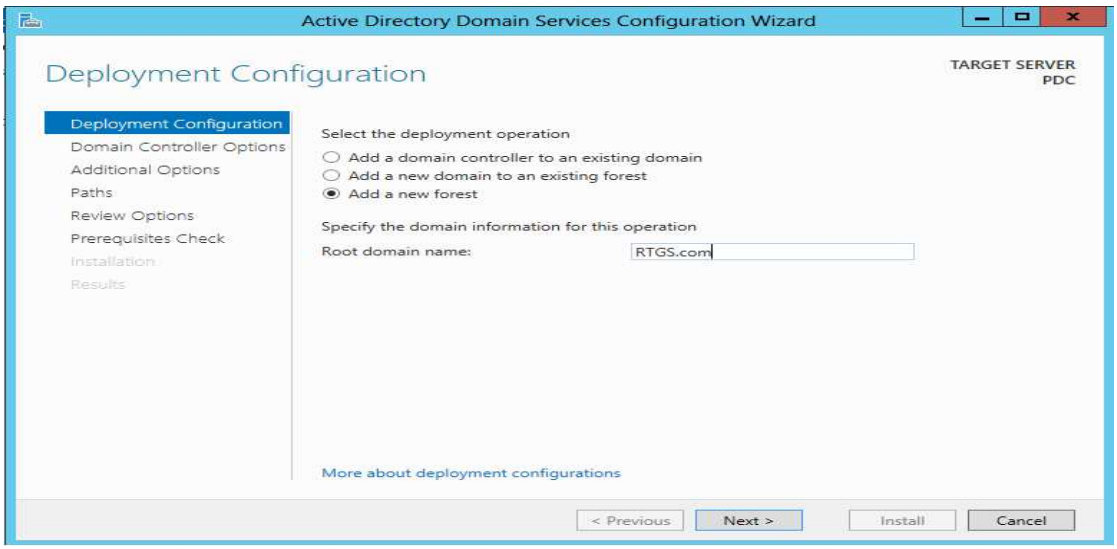


Figure IV.5: La création du domaine principal.

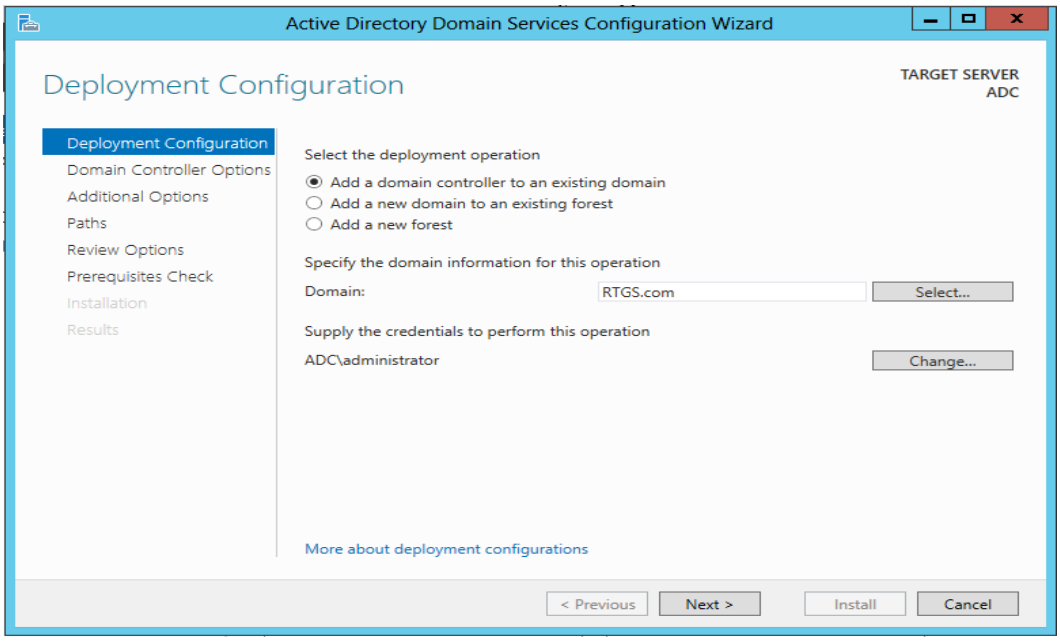


Figure IV.6: L'ajout du domaine secondaire.

Dans l'annexe A, vous trouverez l'installation et le fonctionnement de l'Active Directory sous le Windows serveur 2012.

2. L'ajout d'un serveur ou machine membre

Un serveur ou une machine membre ne sont pas des contrôleurs de domaine mais seulement des membres du domaine. Pour ajouter un membre, il faut accéder aux propriétés systèmes et modifier le domaine de l'ordinateur comme le montre la figure suivante :

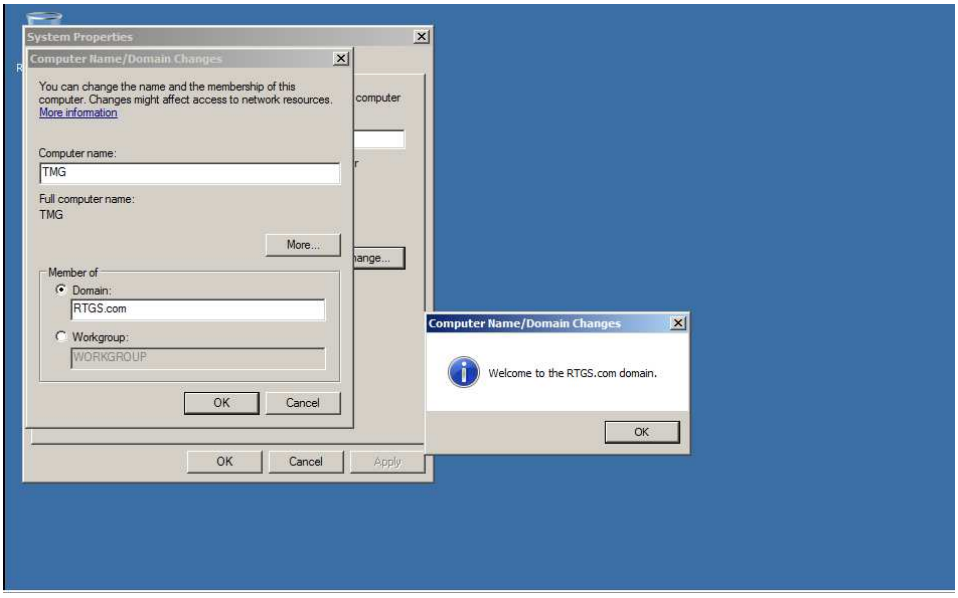


Figure IV.7: Ajout de la TMG au domaine RTGS.com.

IV.3.2. L'installation et configuration de la TMG

Pour éviter tout problème pendant l'installation de Forefront TMG 2010, avant de commencer, nous avons pris en compte les conditions suivantes :

1. Matériels exigés

- ✓ Un ordinateur avec un processeur 64 bits.
- ✓ Système d'exploitation Windows Server 2008 R2 64-bits.
- ✓ 2 Go ou plus de mémoire
- ✓ Une partition de disque dur local, formatée avec le système de fichiers NTFS.
- ✓ 2,5 Go d'espace disque disponible.

2. Configuration des cartes réseaux

L'installation préalable de la TMG exige l'ajout et la configuration de 3 cartes réseaux :

- ✓ Une interne avec l'adresse 172.16.0.0/16
- ✓ Une externe avec l'adresse 10.0.0.0/24
- ✓ Une pour la DMZ avec l'adresse 192.168.3.0/24

3. Lancement de l'installation de la TMG

Les différentes étapes d'installation de la TMG sont définies dans l'annexe A**.**

Figure IV.8: La console de gestion de la TMG.

4. La création des règles de la TMG

Il est indispensable de configurer les règles qu'il faut autoriser avant d'entreprendre n'importe quelle configuration au niveau interne, car la TMG interdit par défaut tout le trafic entrant et sortant sur tous les réseaux (internes, externes et locaux). Nous avons autorisé les règles, DNS, PING, HTTP /HTTPS en spécifiant, pour chacun d'eux le réseau entrant, sortant et les utilisateurs sur les quels elles seront appliquées. Comme exemple de création d'une règle TMG, nous prenons celle du DNS qui permet de spécifier un ordinateur sur le quel elle s'applique. Et afin de restreindre le trafic HTTP /HTTPS autorisé nous créons une règle pour empêcher l'accès à certains sites.

- **Exemple de la règle DNS**

Pour la création de la règle d'accès DNS, stratégie de pare-feu -> entrons le nom DNS.

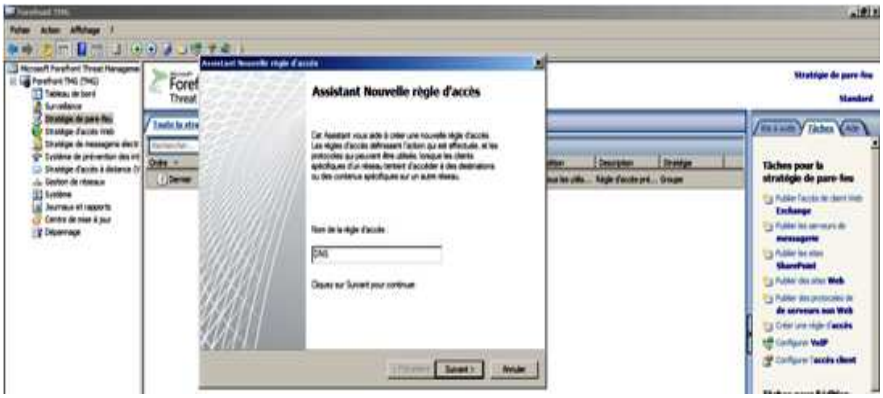
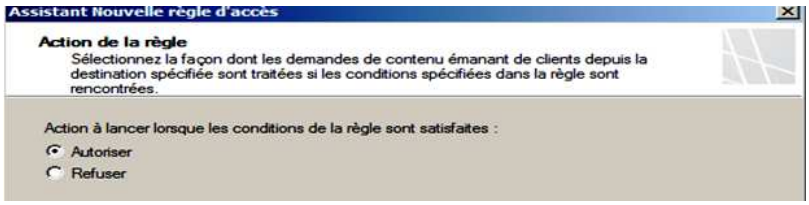


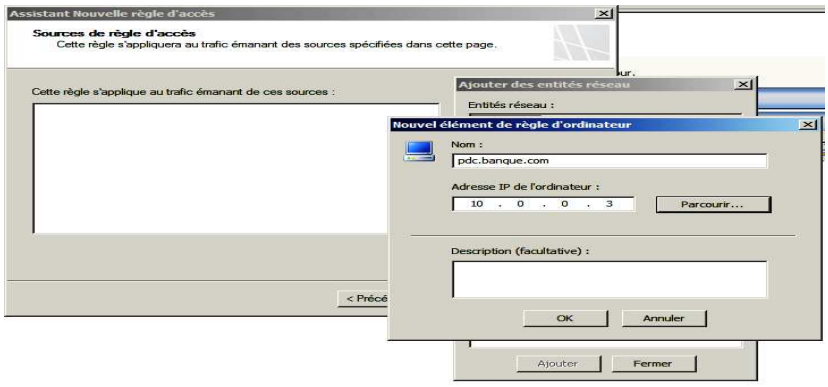
Figure IV.9: création de la règle d'accès DNS.

Notre objectif étant d'autoriser la règle DNS, sélectionnons autoriser.



Dans ajout de protocoles nous spécifions sur quels protocoles s'applique cette règle (DNS).

Cette règle s'appliquant sur le serveur DNS, **RTGS.dz**, dans l'ajout des entités réseau, nous sélectionnons ce serveur avec son adresse IP comme source de règle d'accès.

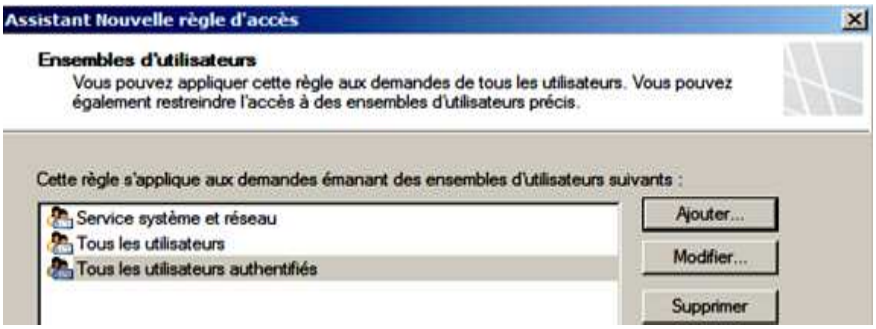


Le trafic destinataire étant le réseau local séléctionnons l'hote local.

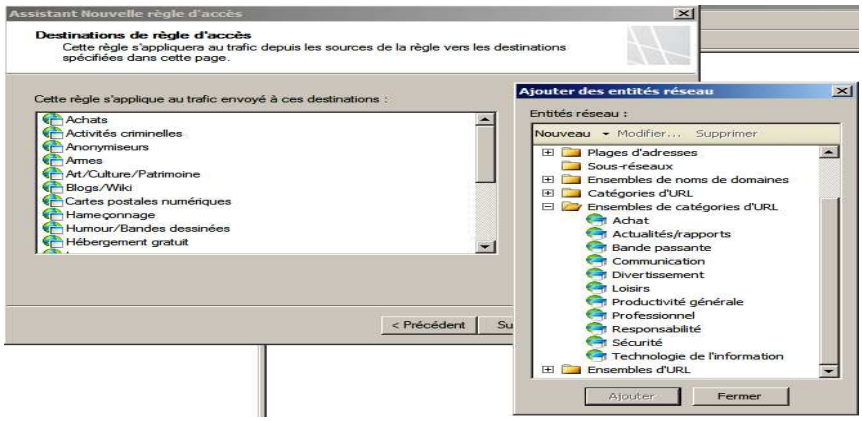
Spécifions sur quels utilisateurs s'applique cette règle, dans ce cas tous sont concernés par le DNS.

- **Exemple de la règle pour empêcher l'accès à certain sites**

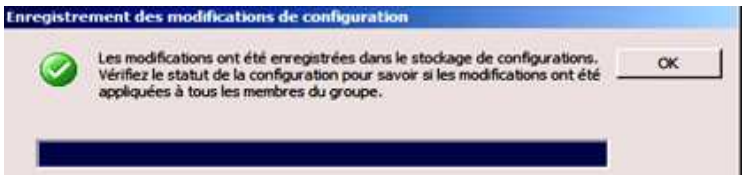
Définissons les utilisateurs sur lesquels s'applique cette règle.



Choisissons les sites à exclure, comme les réseaux sociaux, les sites d'achat e-commerce et autres.



Afin de valider et enregistrer toute modification apportée à la TMG, nous cliquons sur Appliquer.



Le récapitulatif des règles TMG configurées est montré sur la figure ci-dessous :

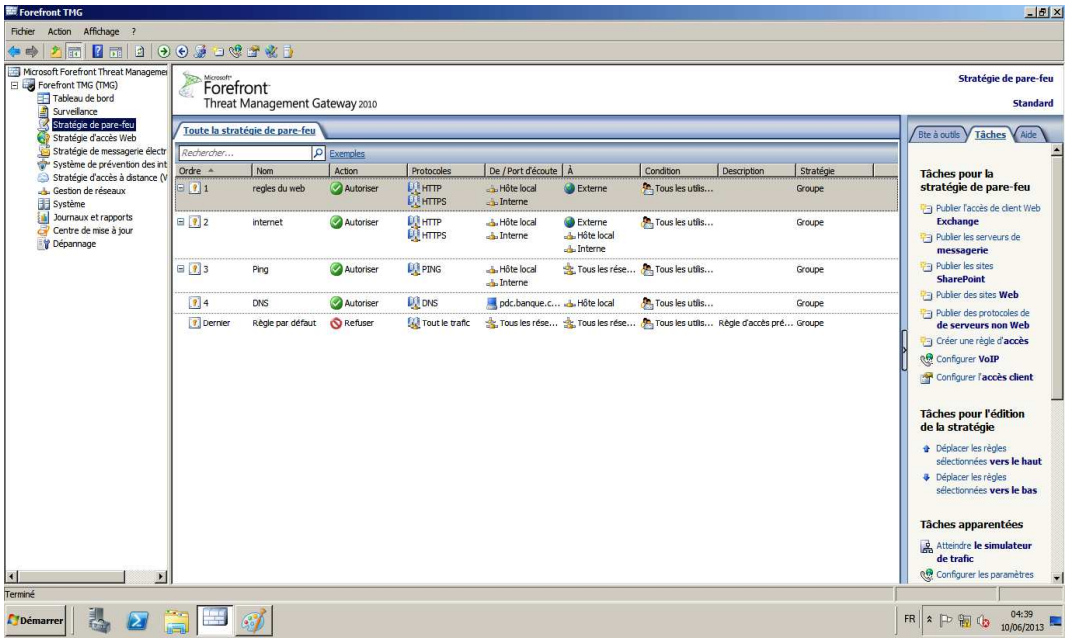


Figure IV.10: Récapitulatif des règles TMG.

IV.3.3. Configuration du stockage serveur et des clusters de serveurs

Dans ce titre nous configurons les deux types de cluster, **le cluster avec répartition** de la charge réseau (NLB pour Network Load Balancing) qui est un groupe de serveurs utilisés pour fournir un équilibrage de charge et augmenter l'extensibilité et **le cluster de basculement** qui permet d'accroitre la disponibilité d'une application ou d'un service dans le cas d'une défaillance du serveur.

IV.3.3.1. Cluster avec répartition de charge : on a besoin de 3 serveurs

- ✓ Deux serveurs web (web1 et web2) ;
- ✓ Serveur de domaine PDC.

1. Installation du serveur Web IIS

Le rôle du serveur Web l'IIS 8 de Windows Server 2012 est de partager des informations avec des utilisateurs sur internet, intranet ou extranet. IIS nous permet d'avoir une plateforme web unifiée, améliorée et permet de personnaliser les sites web. (Voir annexe B). Une fois IIS 8 installé une page par défaut s'ouvre sur le port 80

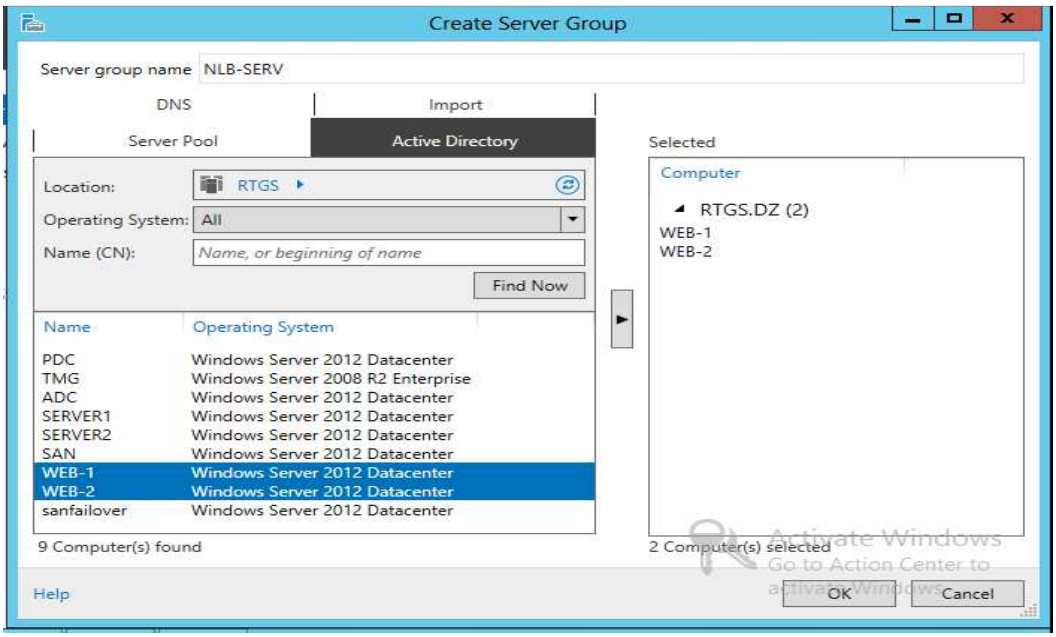
Figure IV.11 : Fenêtre IIS 8 par défaut.

2. Création d'un cluster NLB

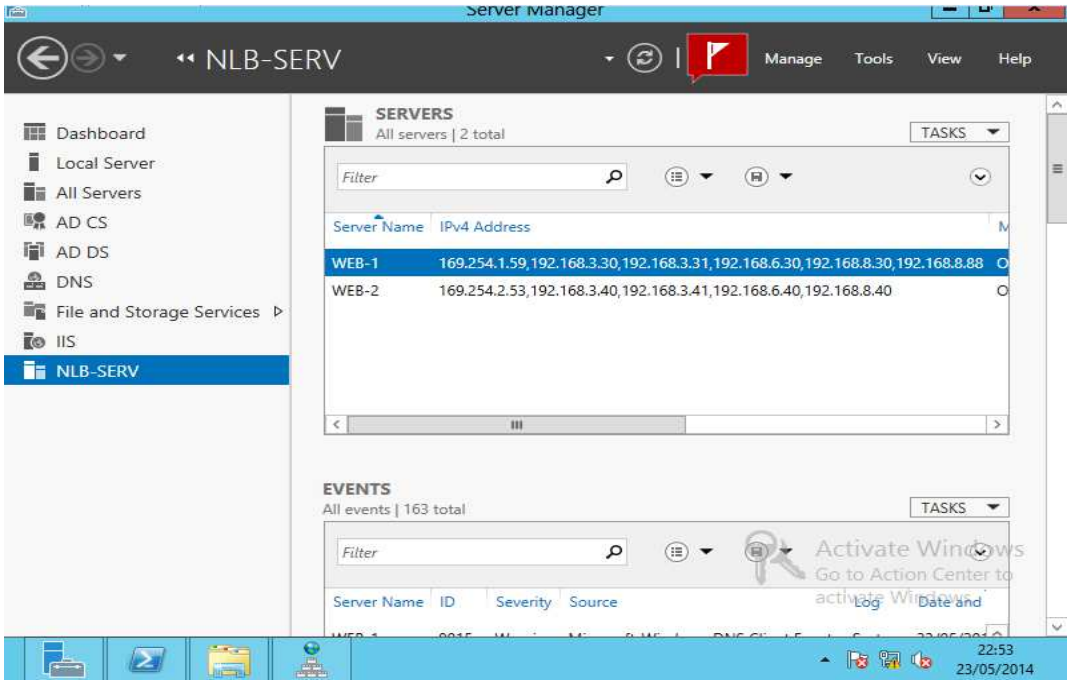
Afin de pouvoir créer un NLB, nous avons préparé deux nœuds machines Windows Server 2012 membres du domaine (WEB 1 et WEB 2) et configuré le service IIS à fournir aux clients en assurant une configuration identique pour les deux nœuds.

- ➢ Les deux serveurs WEB on doit les ajouté au domaine RTGS.dz
- ➢ Et la suite des noms d'hôte configuré sur le serveur DNS :
  - ✓ WEB 1 :192.168.3.30
  - ✓ WEB 2: 192.168.3.40
  - ✓ Et le serveur de domaine PDC : 192.168.3.3

La 1ére tache qu'on doit faire, on installe NLB sur les deux serveurs WEB-1 et WEB-2 puisque on utilise Windows server 2012 il dépose dans ses caractéristique l'installation des rôles a distance. Dans le serveur de domaine on doit crée un serveur de groupe qui appelé NLB-SERV.
Dans le serveur manager on clique sur **create a server groupe** et on ajoute les deux serveurs web 1 et web 2

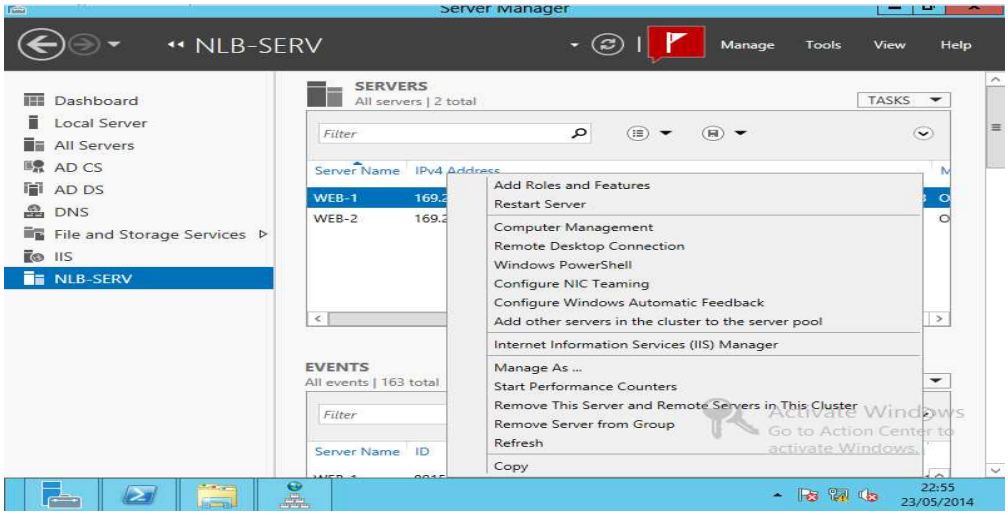


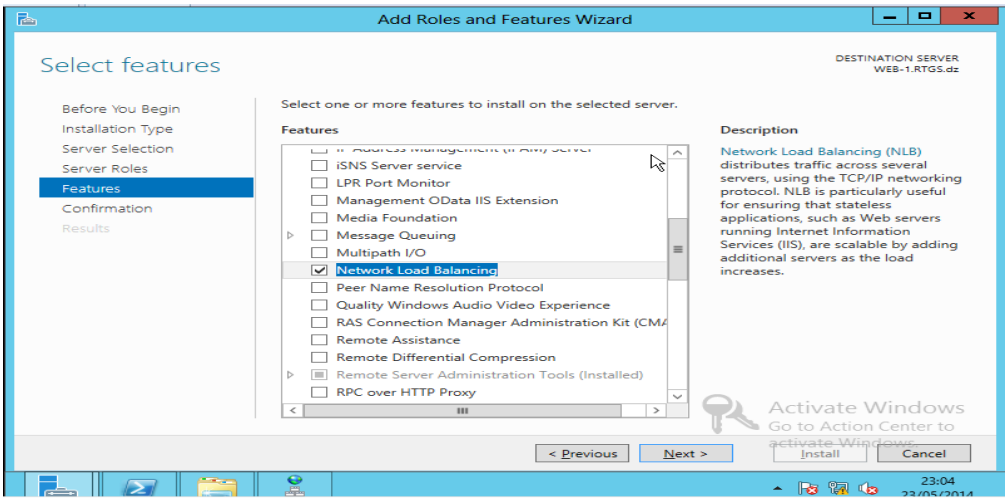
On clique sur ok le groupe NLB-SERV et ajouté dans le serveur de domaine :



3. L'ajout de rôle de cluster:

Dans le serveur de domaine on installe NLB a distance dans les deux serveurs on clique sur **add roles and features.**





4. Création du cluster :

Sur la page adresse IP du cluster, cliquons sur ajouter pour saisir l'adresse IP du cluster partagé par chaque hôte du cluster.

Après ajout des nœuds de cluster NLB, nous les trouvons listés dans le gestionnaire d'équilibrage de la charge réseau.

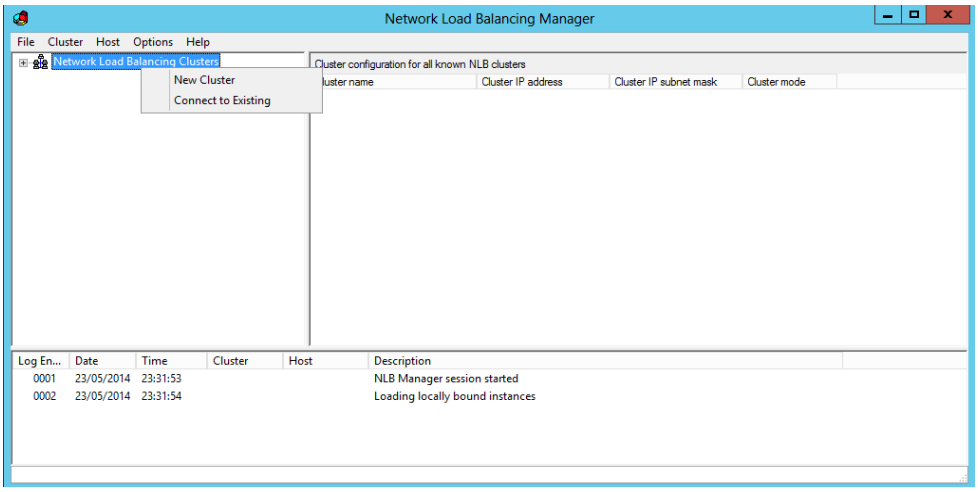
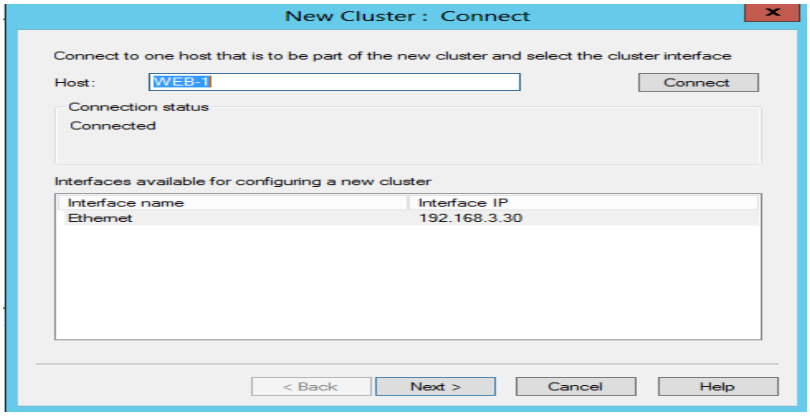
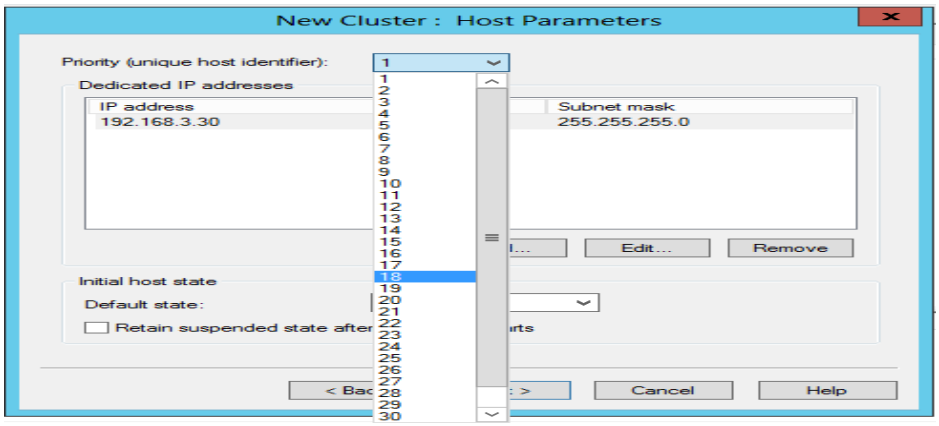


Figure IV.12 : gestionnaire d'équilibrage de charge**.**

Dans l'arborescence, choisissons nouveau cluster, dans l'hôte, tapons le nom de la machine qui doit faire partie du nouveau cluster et cliquons sur connexion.



Sur la fenêtre des paramètres de l'hôte, sélectionnons une valeur de priorité dans la liste déroulante. Ce paramètre spécifie un ID unique pour chaque hôte. L'hôte ayant la priorité la plus haute parmi les membres actuels du cluster pourra gérer tout le trafic réseau du cluster.



En suite, saisissons l'adresse IP virtuelle employés par le cluster pour répartir la charge.

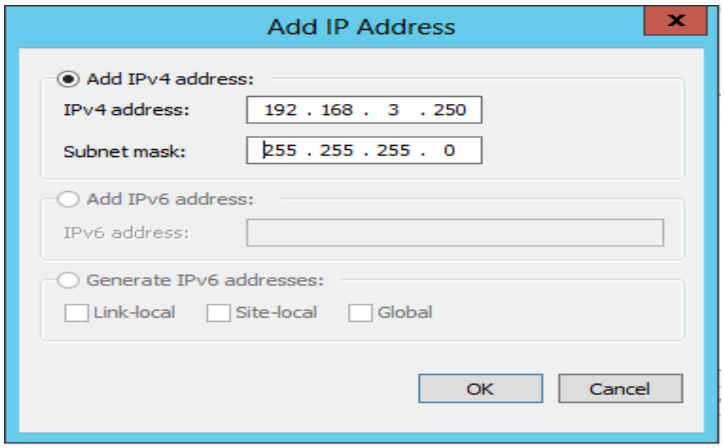
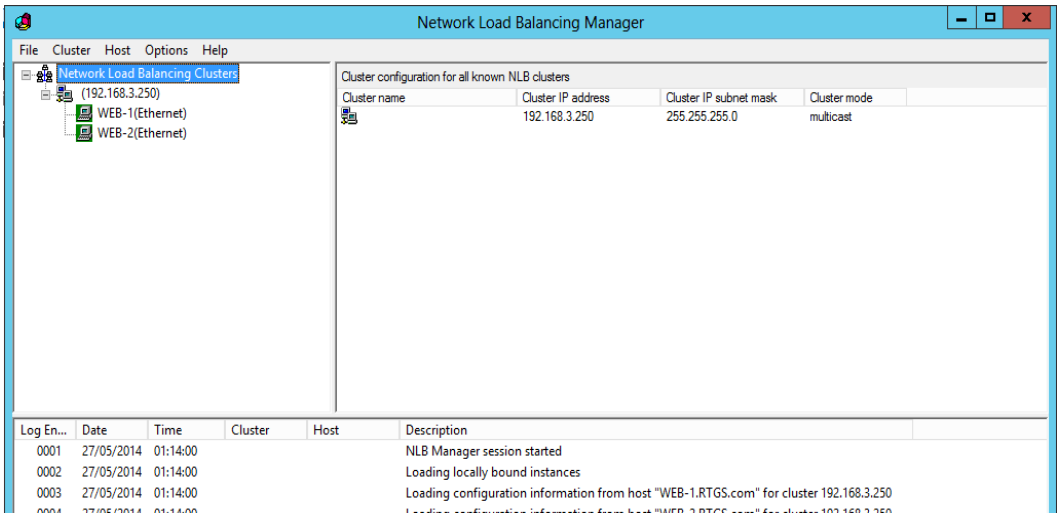


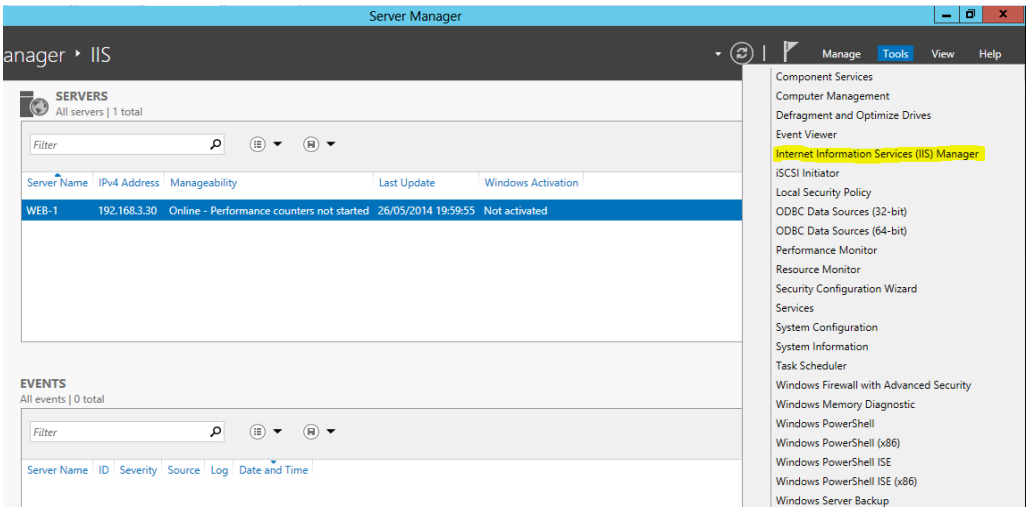
Figure IV.13 : L'adresse IP du cluster

Après ajout des nœuds de cluster NLB, nous les trouvons listés dans le gestionnaire d'équilibrage de la charge réseau. Les deux serveurs sont ajoutés dans le cluster **:**

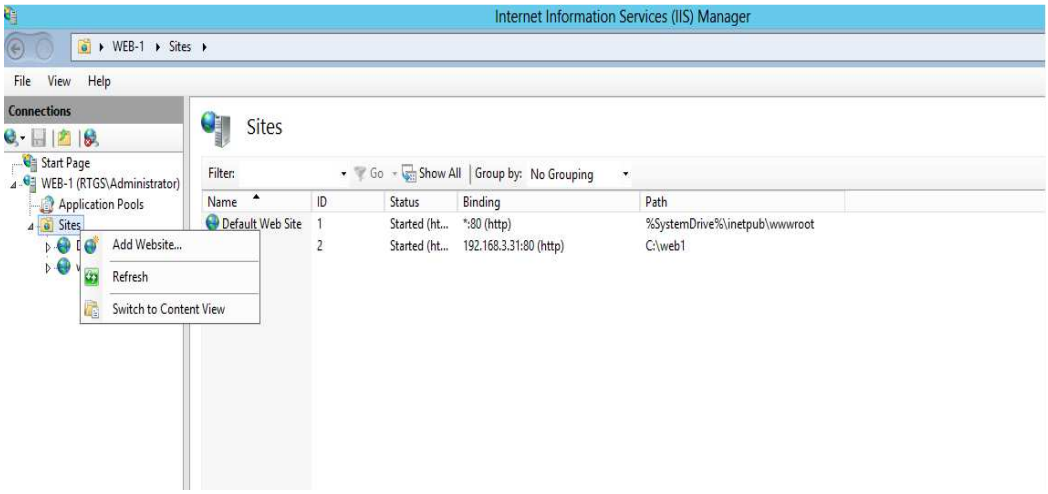


5. Création de site web:

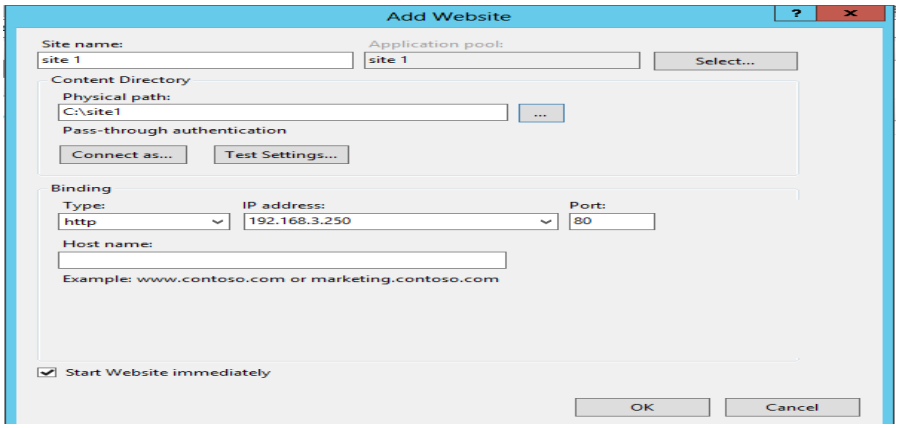
On va crée **site 1** sur le serveur **web 1** et **site 2** sur le serveur **web 2,** clique sur **tools** dans **server manager > internet information services IIS Manager :**



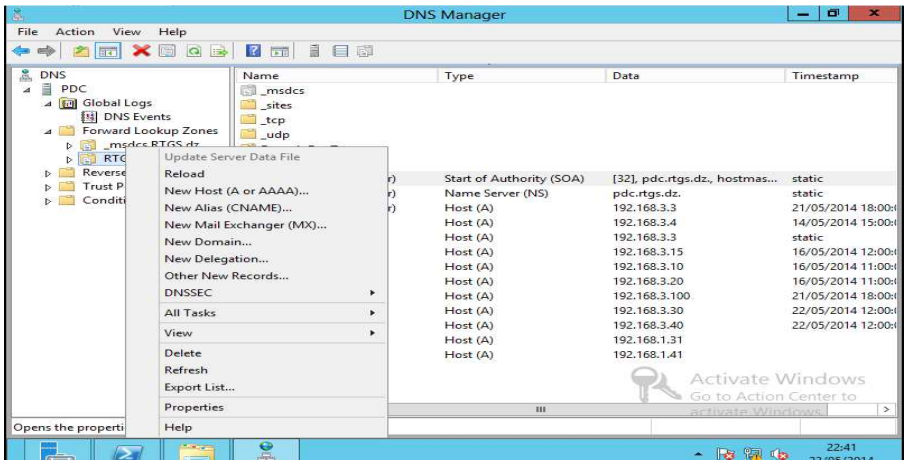
La fenêtre IIS s'ouvre on clique sur **Add Website**, on crée notre site web site 1 :



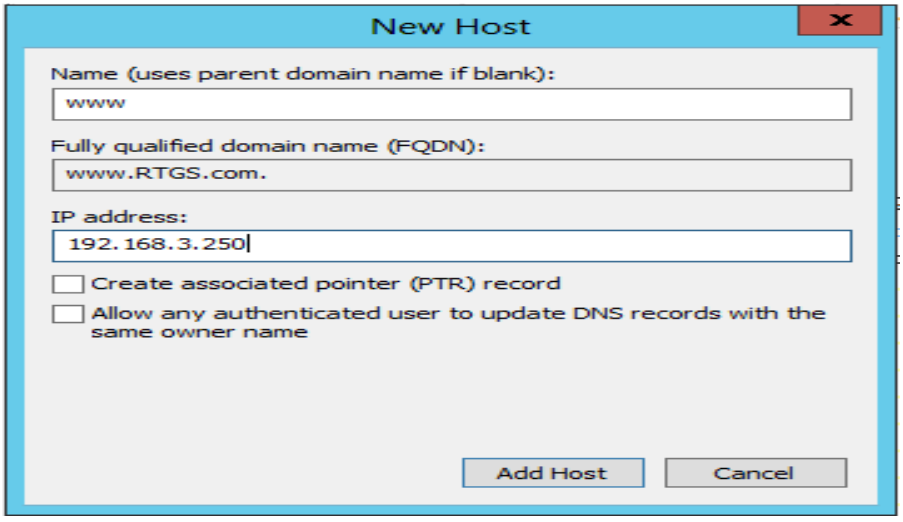
Ajoutons le nom de dossier de site et l'adresse IP du cluster avec le port 80.



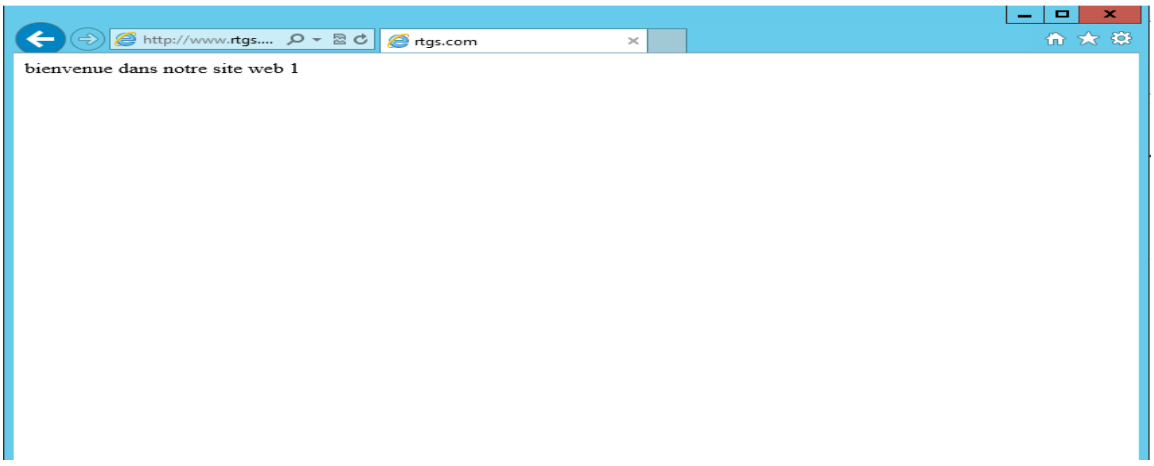
On ajoute de DNS dans le serveur PDC.



On ajoute l'adresse DNS du cluster



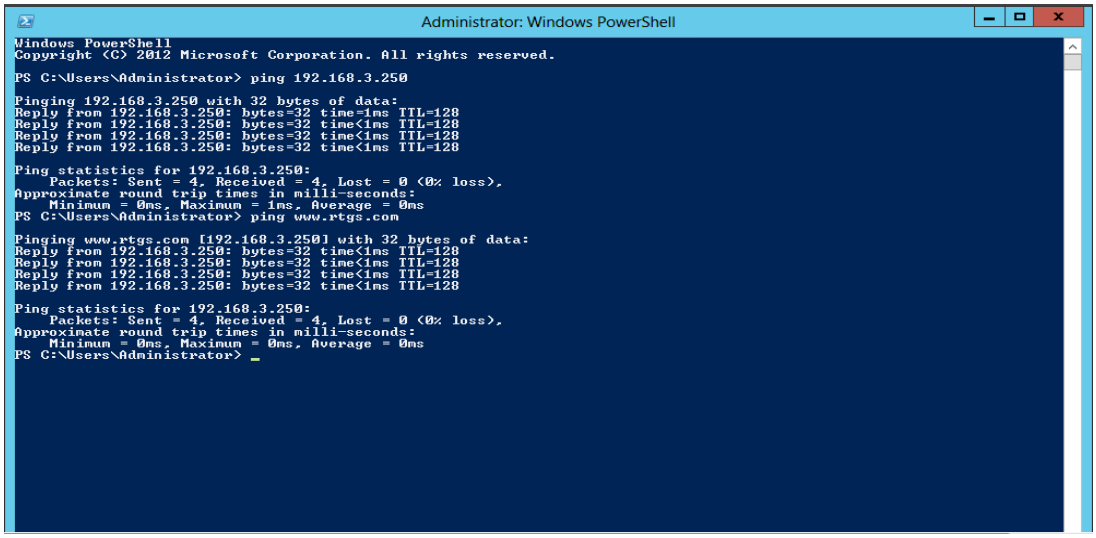
Après la création de site web et l'ajout de mappage de DNS l'adresse 192.168.3.30 et www.RTGS.com on tape l'adresse de site web une page web s'affiche :



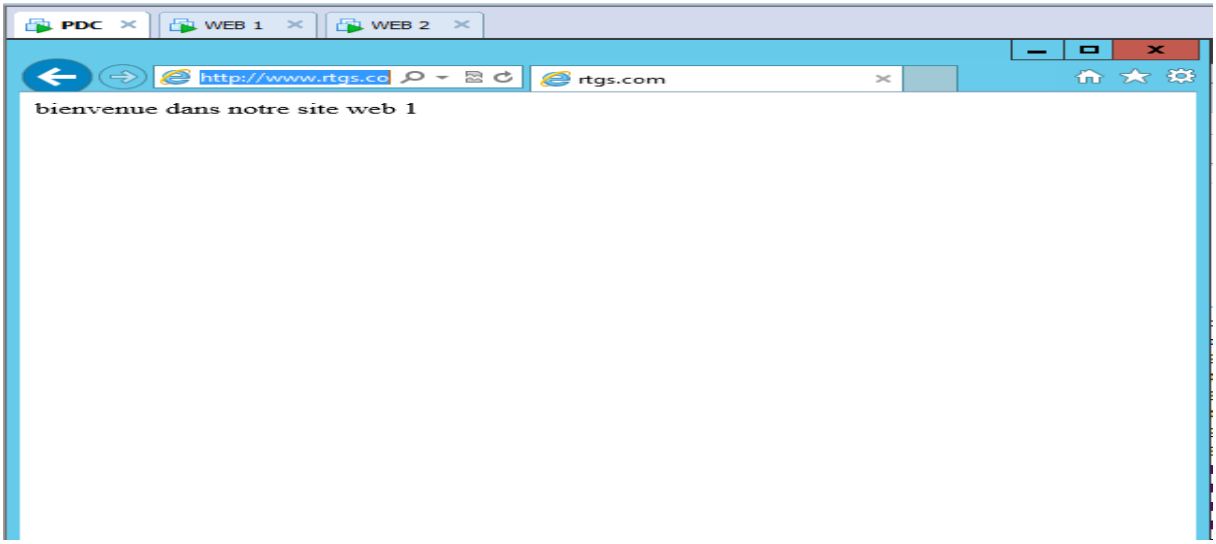
On applique sa au serveur web 2 aussi.

6 tester le NLB :

Après avoir exporté le site, on Ping avec le nom et l'adresse du cluster depuis le PDC, comme nous voyons c'est réussi.

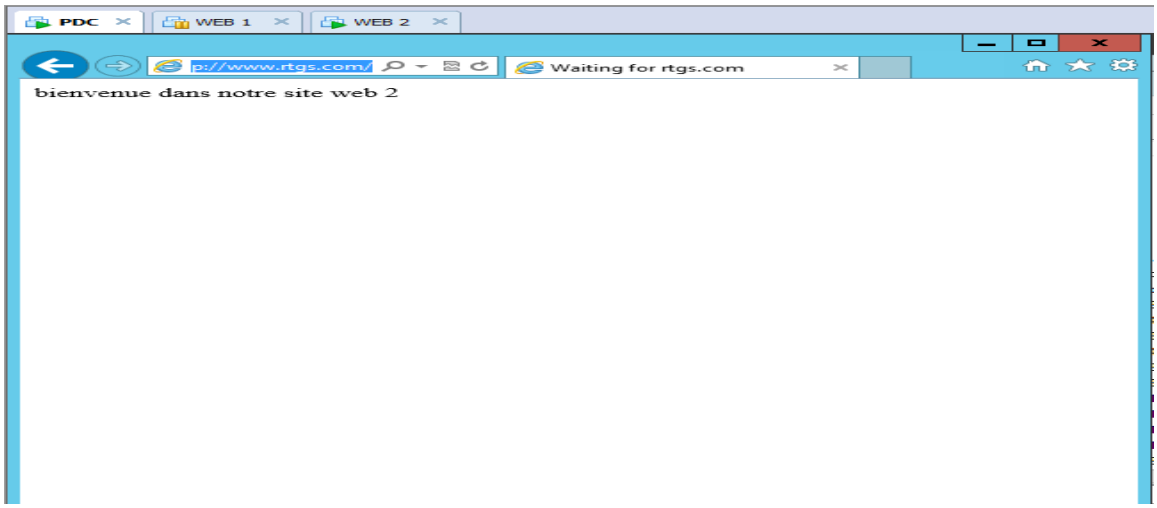


La deuxième étape de test consiste à naviguer avec le nom de cluster NLB via un navigateur.



La page de site 1 qui s'affiche, car on a donnée la priorité à web 1.

Si on arrête le la machine du web 1, on va voir que la page de site 2 qui s'affiche donc le Laod Balancing (l'équilibrage de charge) est réussi.



IV.3.3.2. Installation et configuration du stockage

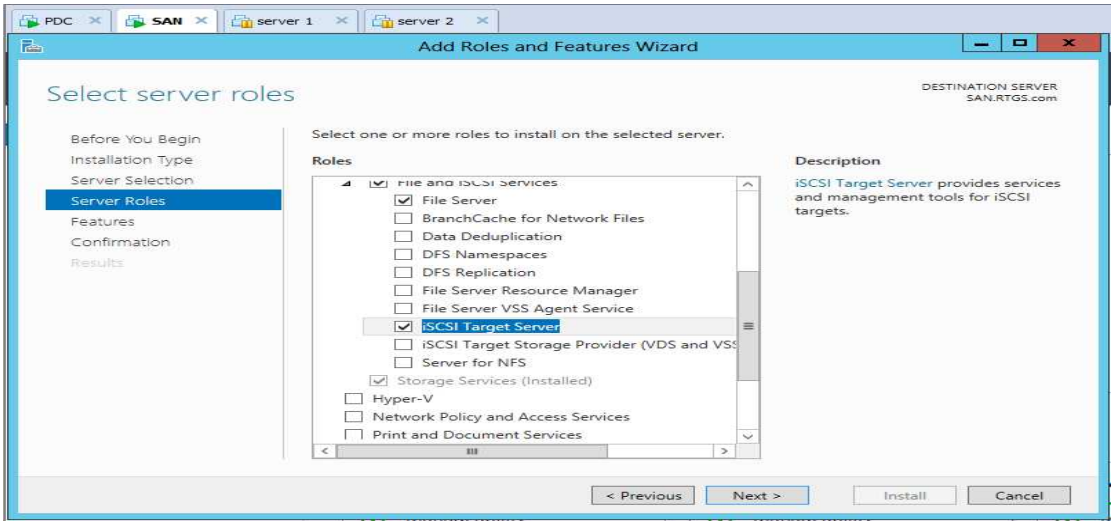
1. Installation de SAN

Dans une entreprise, l'indisponibilité des données est un point critique nécessitant une solution bien réfléchie. Après avoir étudié les différentes méthodes de stockage, nous avons choisi d'utiliser la méthode iSCSI SAN (Storage area network). Son principe de fonctionnement, installation et utilisation sont détaillés dans l'annexes B.

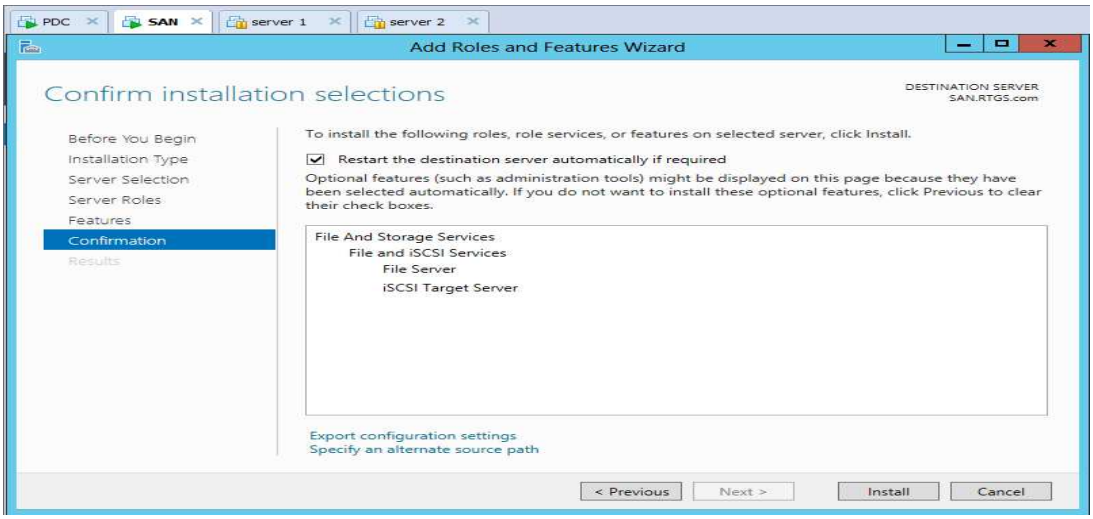
2. Les réseaux iSCSI SAN

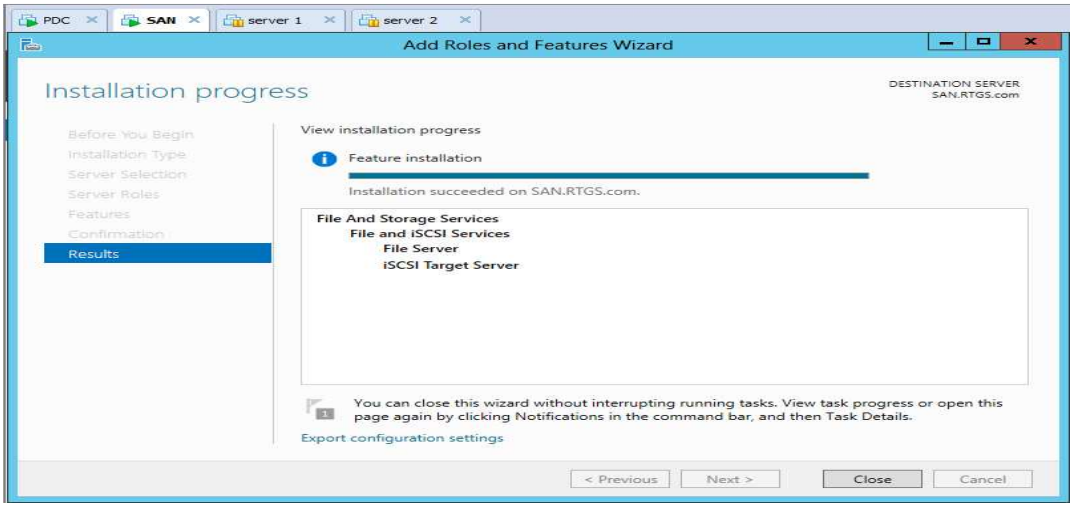
iSCSI (Internet SCSI) est un standard industriel développé pour permettre une transmission de commande via un réseau Ethernet en utilisant le protocole TCP/IP. Les serveurs communiquent avec les périphériques iSCSI grâce à un agent logiciel installé localement appelé initiateur iSCSI. Ce dernier exécute des demandes et reçoit des réponses d'une cible iSCSI, qui peut elle-même être le périphérique de stockage final ou un périphérique intermédiaire comme un commutateur.

Dans cette section nous présenterons les différentes étapes d'installation du service iSCSI SAN sur un serveur membre de **RTGS.com** que nous avons nommé **SAN**.



Clique sur **Install** pour installer le rôle iSCSI :





Une fois l'ajout de rôle de iSCSI, allez à Server Manager > Fichier et services de stockage > iSCSI. Cliquez sur Créer un disque virtuel iSCSI, démarrer l'Assistant disque virtuel iSCSI Nouvelle.

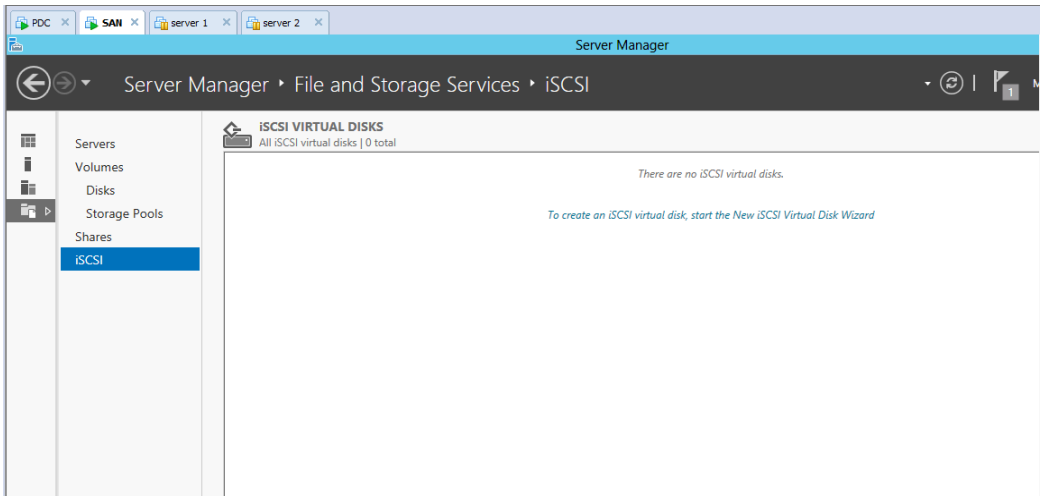
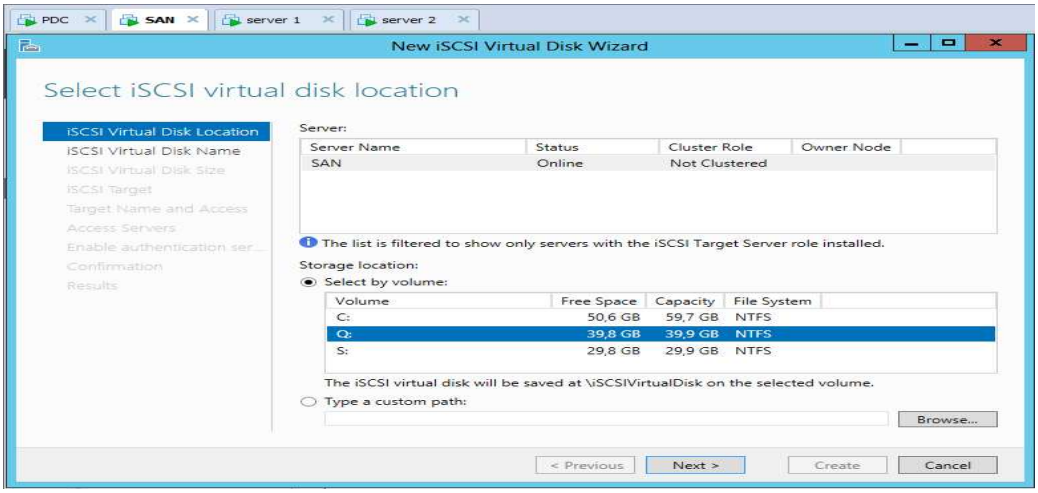
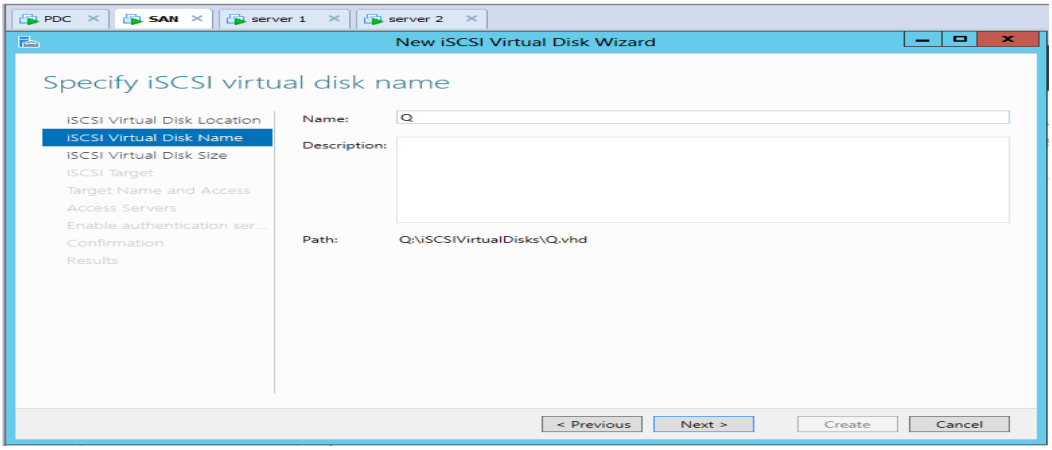


Figure IV.15 : Création d'un disque virtuel iSCSI.

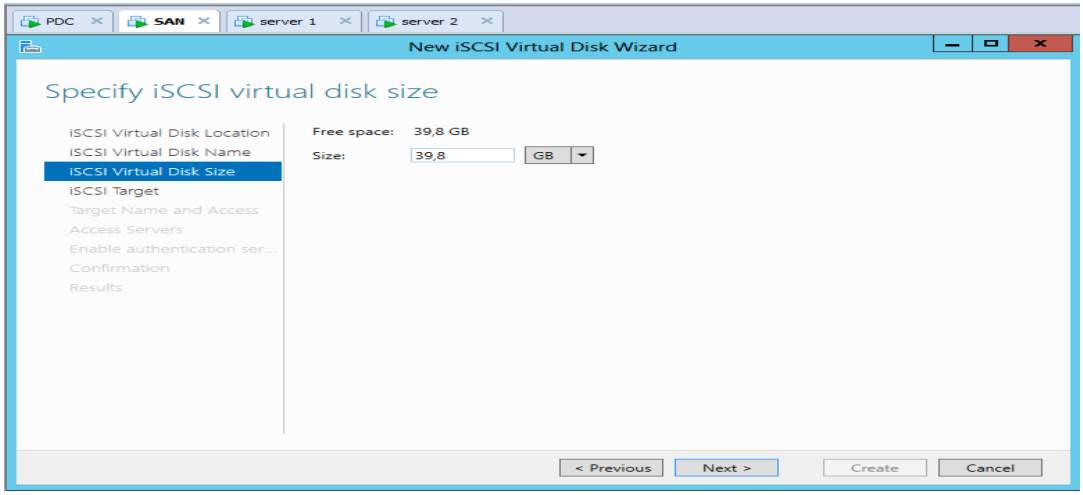
Choisissez où vous souhaitez créer le disque virtuel, puis cliquez sur Suivant. Pour nous, On a choisi de le placer dans le Q.



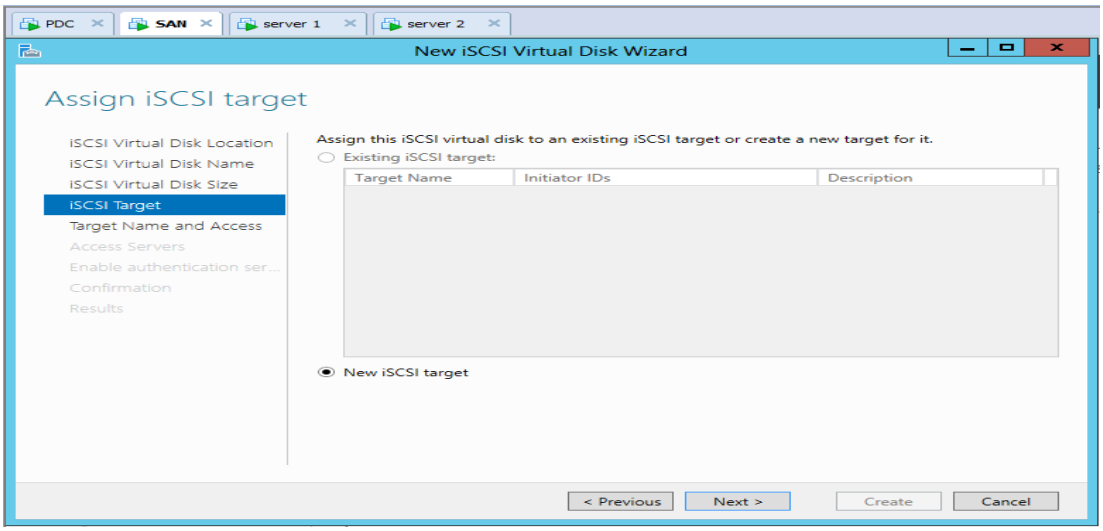
Donnez-lui un nom.



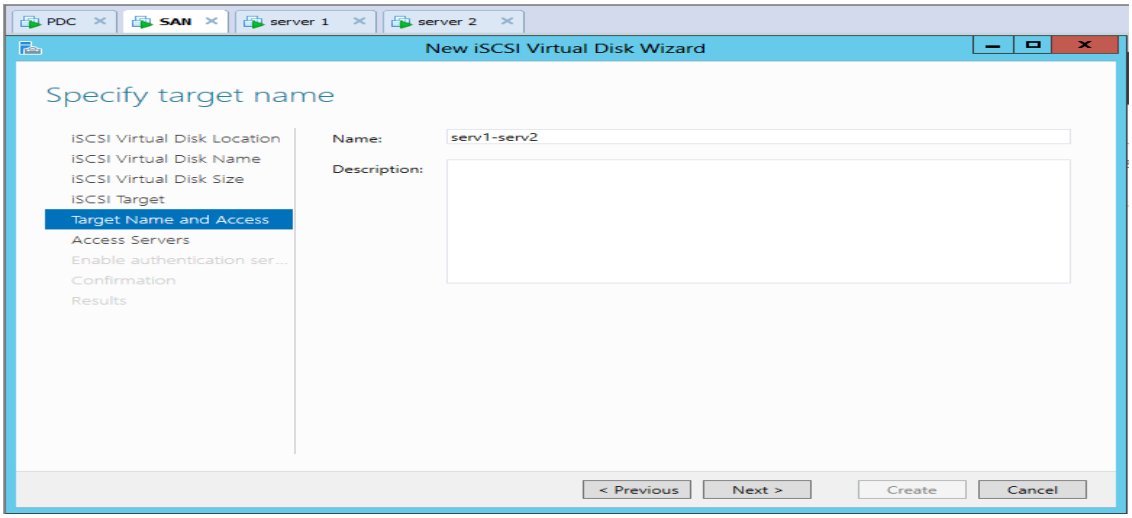
On a donné un 39.8 Go sur l'espace de disque :



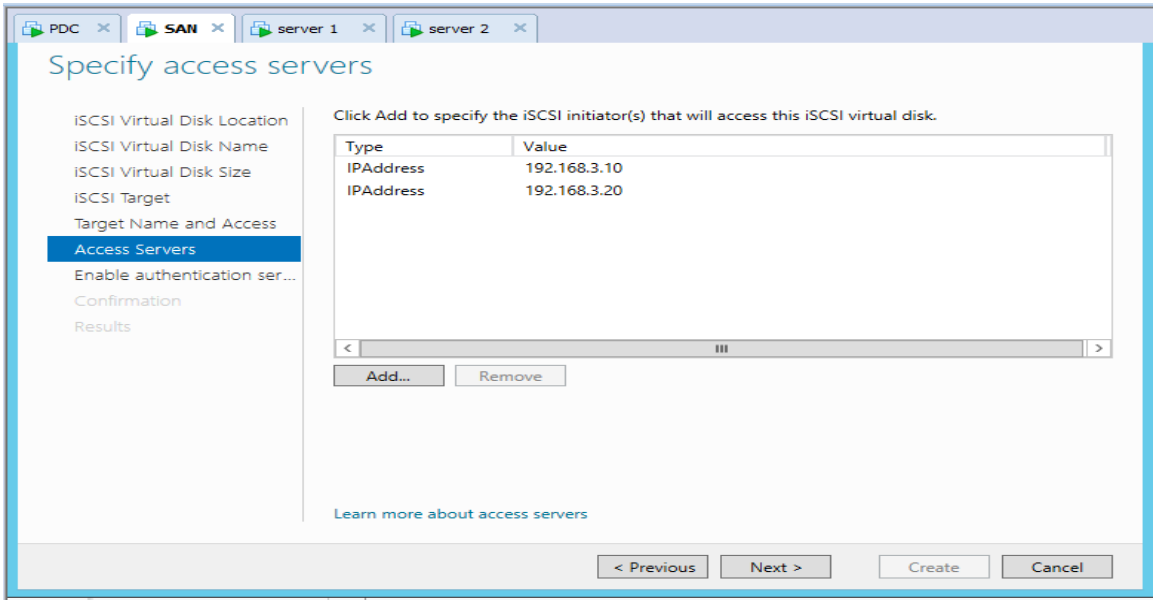
On crée une nouvelle cible iSCSI, cliquez sur Suivant.



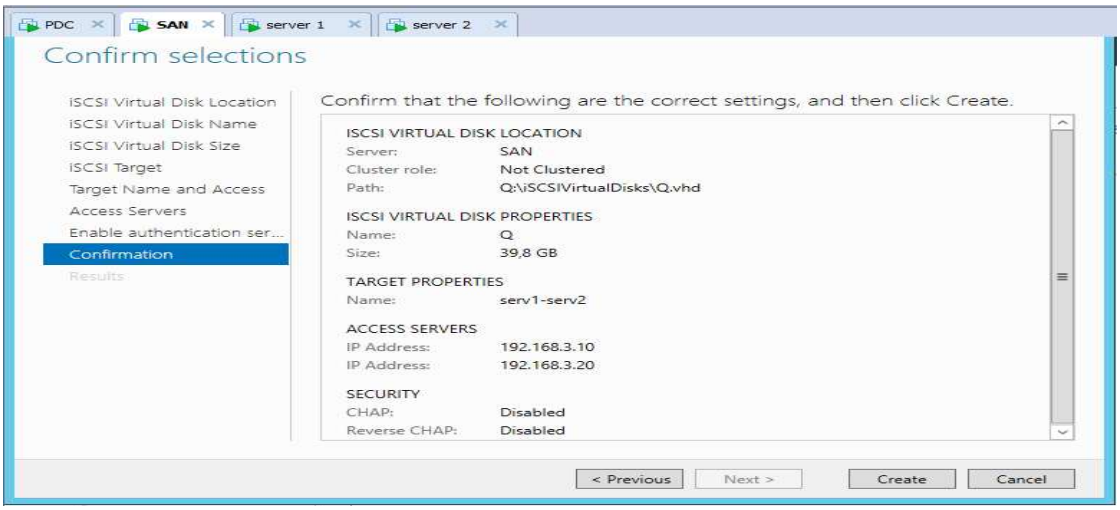
Donnez un nom à votre cible puis cliquez sur Suivant.

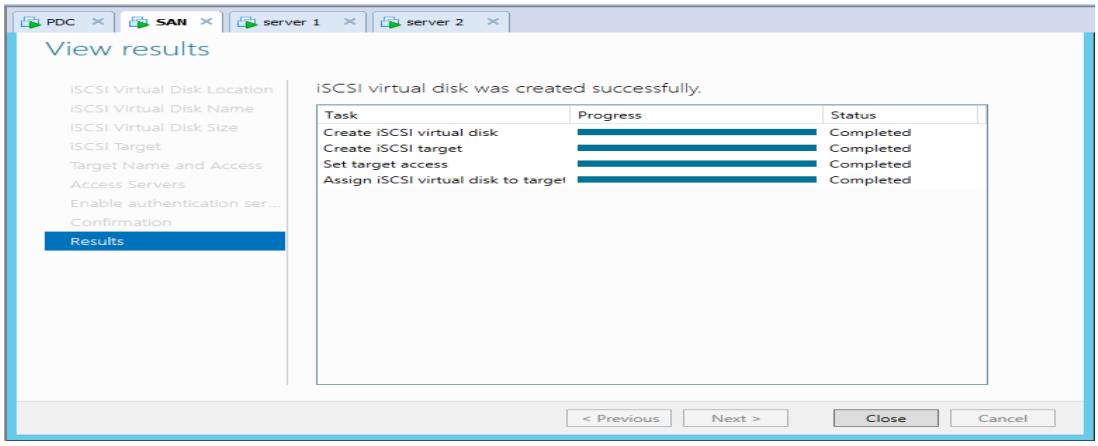


Cliquez sur Ajouter pour ajouter les serveurs qui se connecteront à votre SAN iSCSI.



Confirmation ... cliquez sur **Créer**.

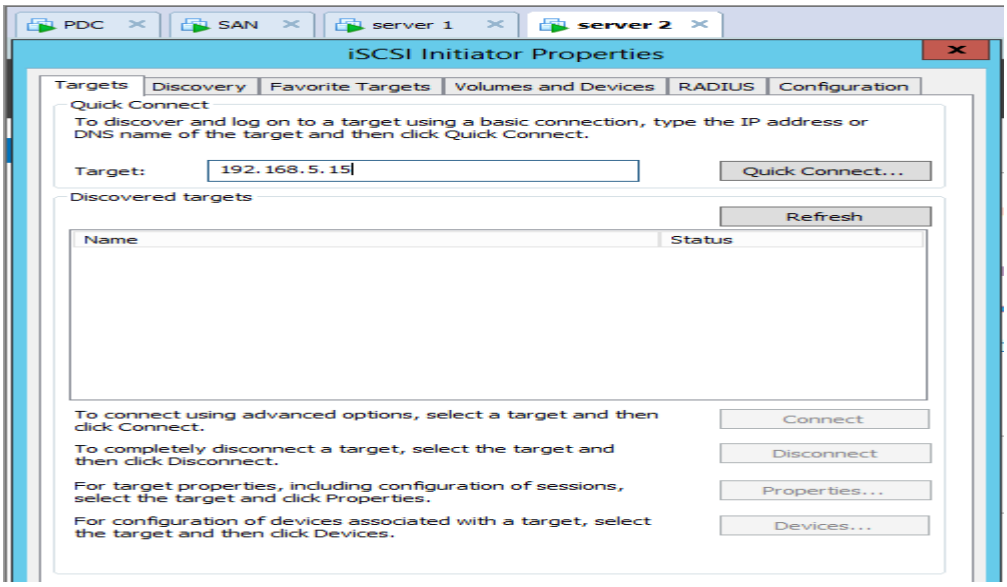




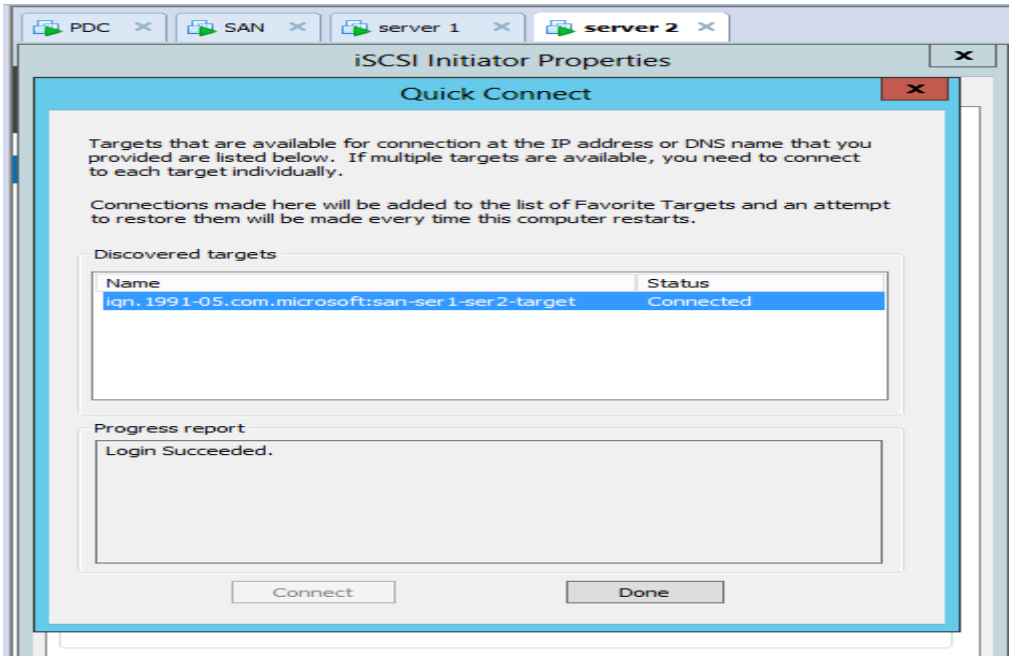
Et c'est fait!

Maintenant, c'est prêt pour le serveur 2 pour s'y connecter. Donc, sur les serveurs, sélectionnez **tools > initiateur iSCSI**.

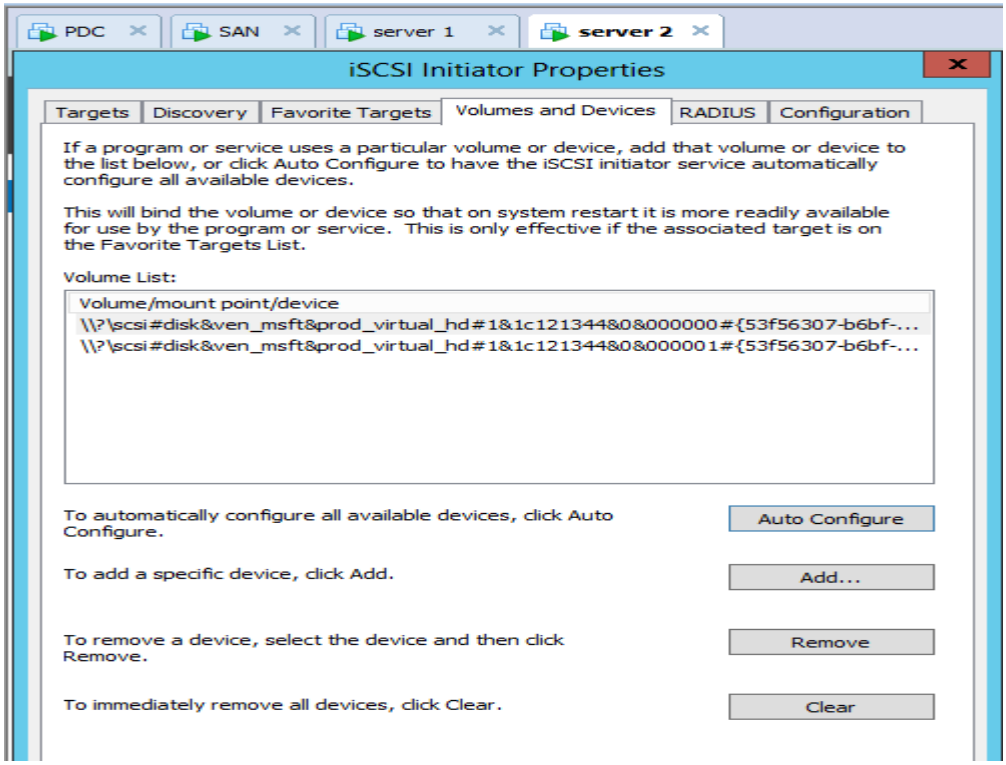
Entrez l'adresse IP de votre réseau SAN iSCSI que vous venez de configurer, puis cliquez sur Connexion rapide ...



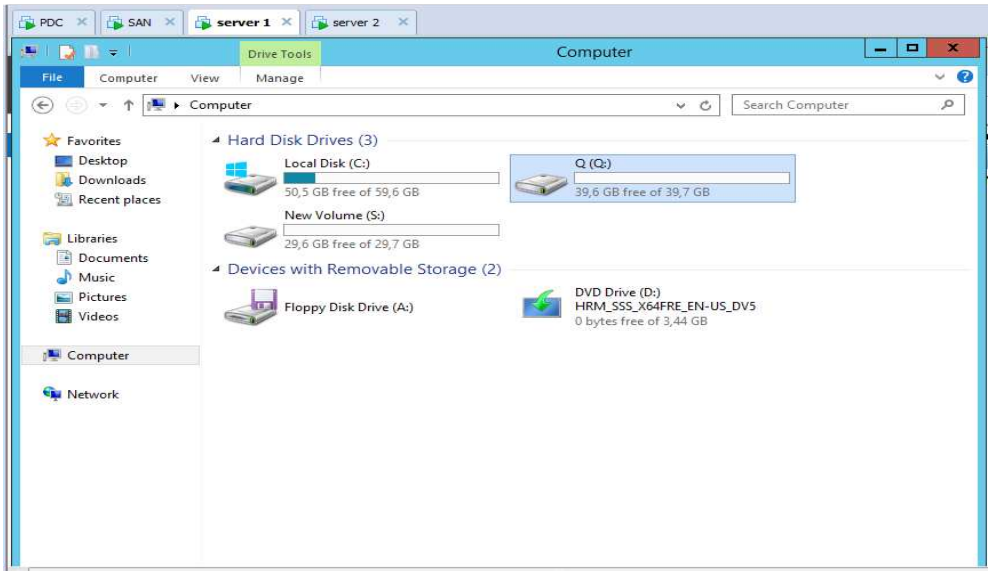
Là, Il indique qu'il est connecté.



Maintenant qu'on est connecté au SAN.



Nous allons à notre Espace disque qui montre en effet que nous avons maintenant un nouveau lecteur.



IV.3.3.3. Cluster du basculement (Failover cluster)

Afin d'implémenter cette solution, nous avons préparé deux nœuds (Windows Server 2012) membres du domaine **RTGS.com**, puis nous avons installé, sur les deux, la fonctionnalité cluster avec basculement via le gestionnaire de serveur.

1. Configuration des cartes réseaux

On a besoin de 3 cartes réseaux dans server 1 et server 2

Server 1 :

- ✓ Interne 192.168.3.10
- ✓ Passerelle 192.168.6.10
- ✓ SAN 192.168.5.10

Server 2 :

- ✓ Interne 192.168.3.20
- ✓ Passerelle 192.168.6.20
- ✓ SAN 192.168.5.20

Une cartes réseaux sure SAN

- ✓ SAN 192.168.5.15 et deux cartes réseaux PDC de domaine avc DNS
- ✓ Interne 192.168.3.3
- ✓ SAN 192.168.5.25

2. L'ajout de rôle de cluster du basculement

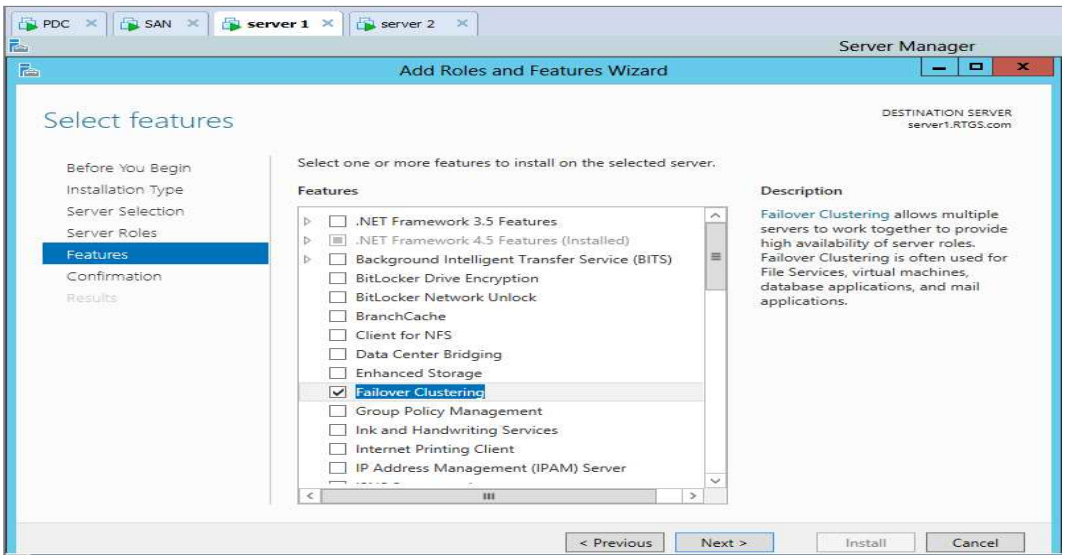
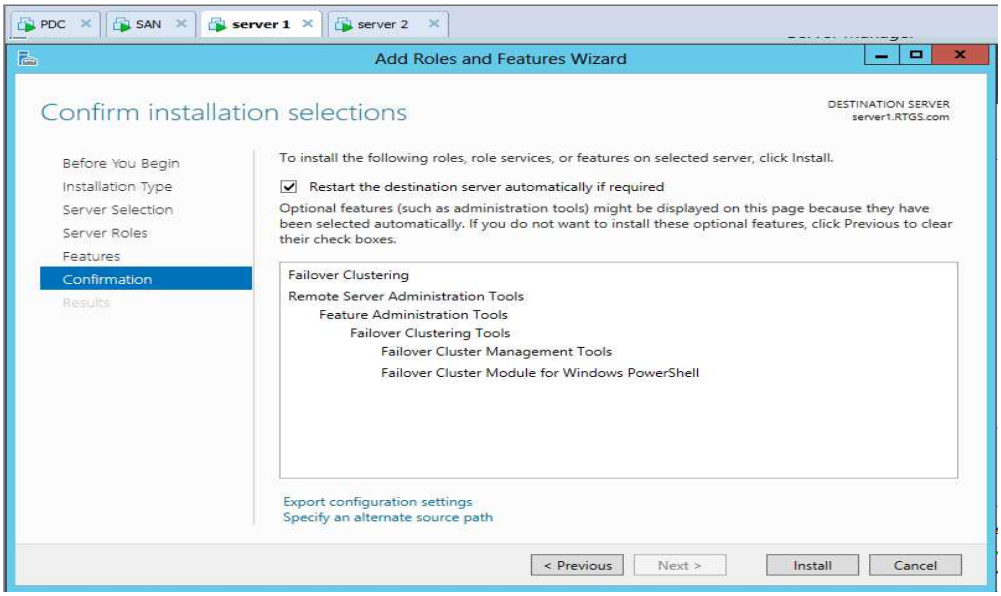
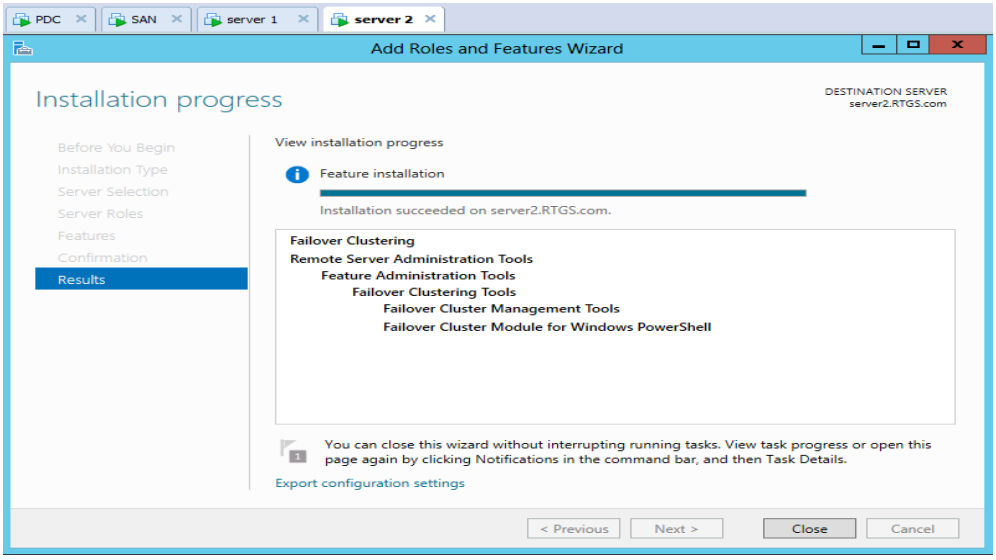


Figure IV.16 : Ajout de rôle de Cluster de Basculement.

Clique sur **Next** après sur **Install**

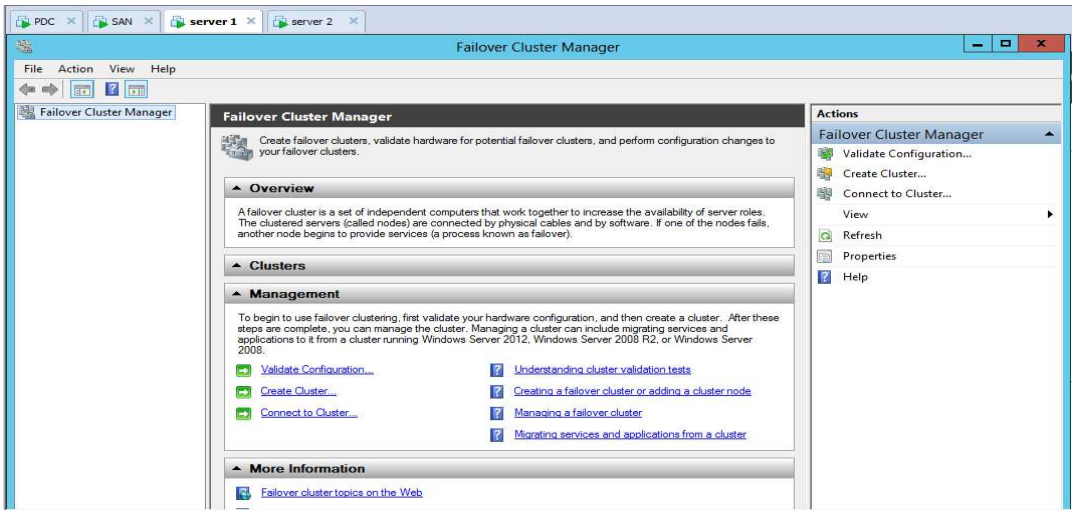




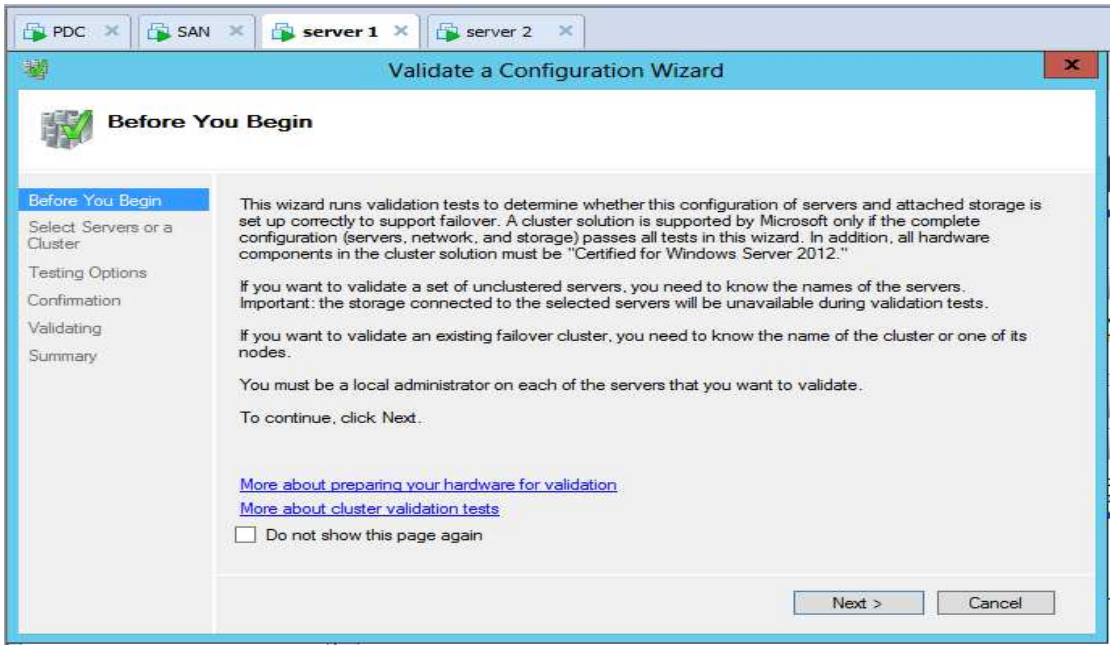
Le rôle failover cluster est installé.

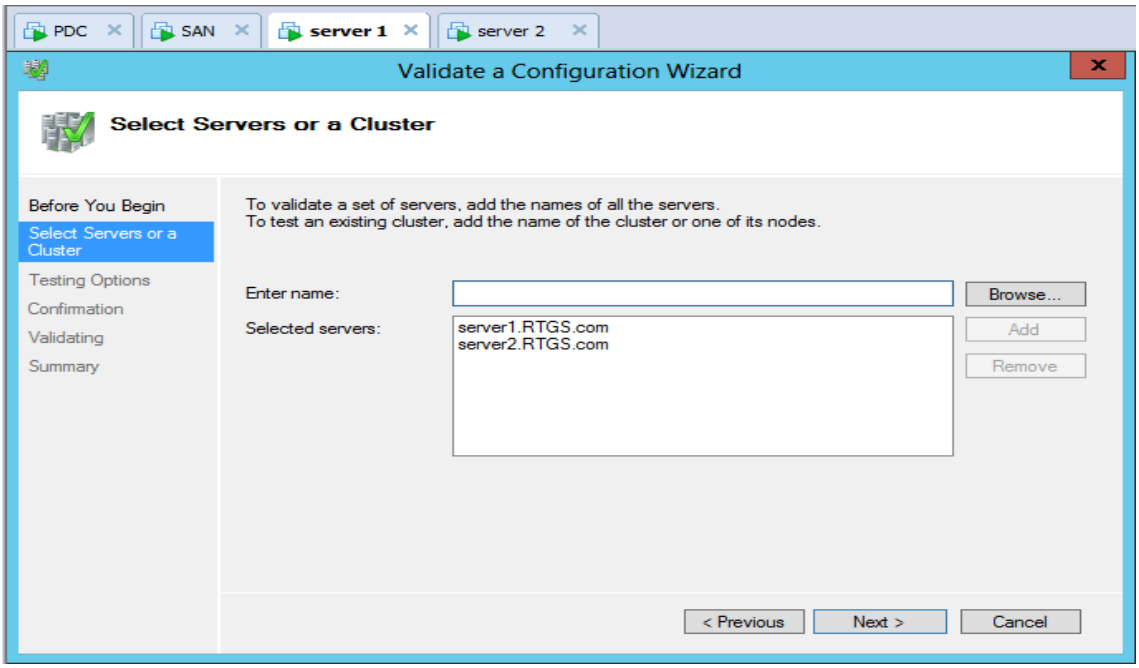
3. Validation de la configuration du cluster

Avant de créer un nouveau cluster, nous validons la configuration via la gestion de cluster en cliquant sur valider une configuration afin d'assurer que les nœuds respectent les pré-requis matériels et logiciels d'un cluster de basculement. Une fois la configuration validée, nous pouvons créer le cluster.

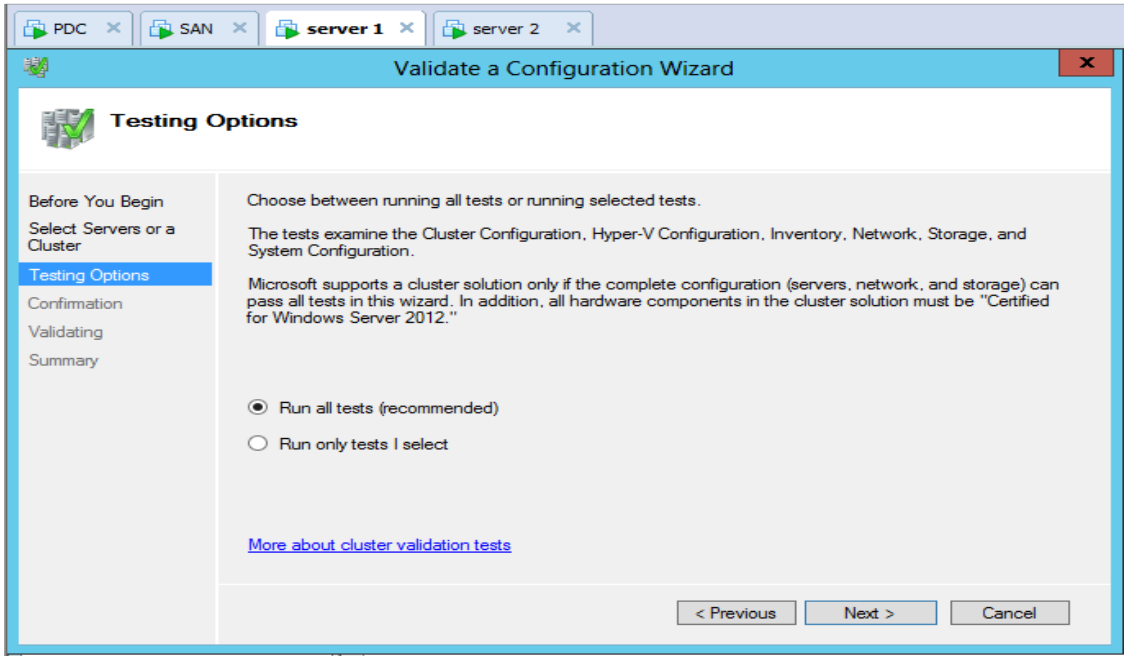


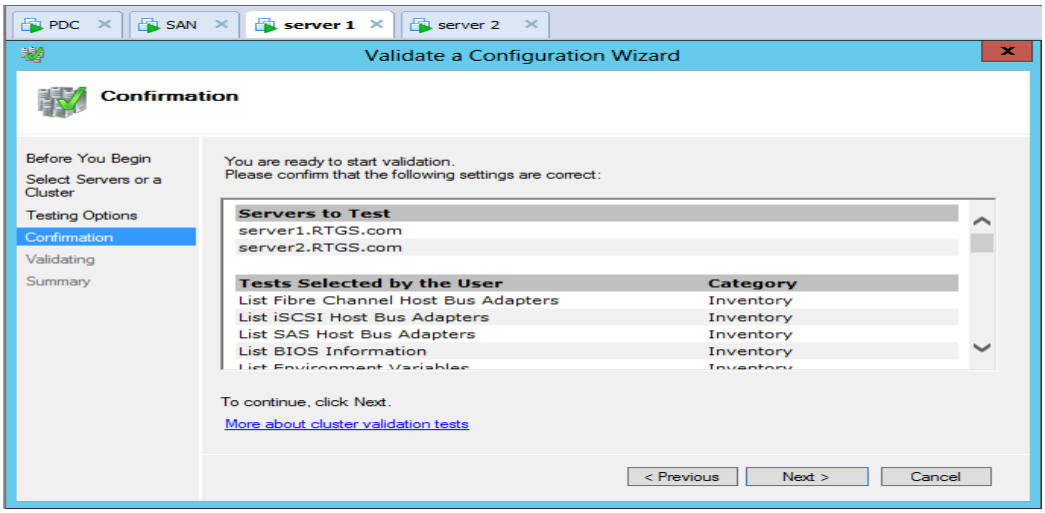
L'assistant affiche d'abord une page d'accueil. Cliquez sur Suivant pour aller à la page Sélectionner des serveurs ou une page de cluster. Sur cette page, entrez les noms des nœuds de cluster que vous souhaitez valider





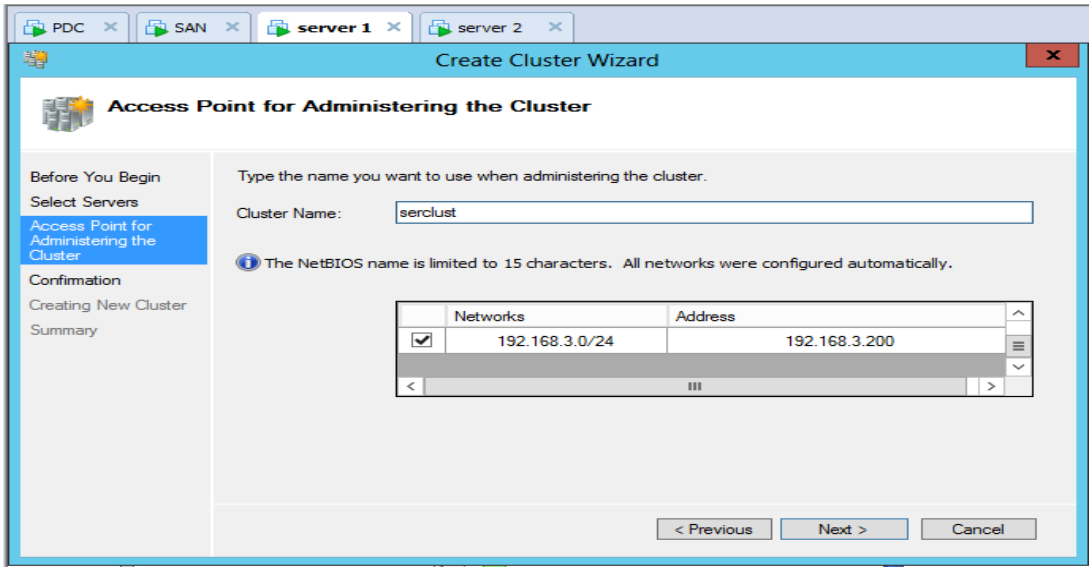
Cliquez sur Suivant pour accéder à la page de confirmation, qui porte sur les tests qui seront exécutés. Cliquez sur Suivant pour démarrer le processus de test de validation de cluster.





Une fois les tests de validation réussissent, nous pouvons créer le cluster.

Sur le point d'accès pour l'administration la page de cluster, vous devez spécifier le nom de votre groupe et l'adresse IP, à la fois de ce qui doit être unique dans le réseau.



4. Tester le cluster de basculement

Après avoir complété l'assistant, nous testons le failover dans l'outil de gestion du cluster de basculement. Dans l'arborescence de la console, sélectionnons le service que nous venons de créer DTC, cliquons avec le bouton droit sur le service en cluster, déplacer ce service vers un autre nœud et cliquons sur l'autre nœud .Nous observons les changements d'états dans le volet central du composant logiciel enfichable pendant le déplacement du service en cluster.

IV.3.4. PKI services de certificats Active Directory

PKI est fortement utilisé dans le Cloud Computing pour le cryptage des données et la sécurisation des transactions.

1. Installation d'autorité de certification

Un CA est un service bien conçu et très digne de confiance dans une entreprise qui fournit des utilisateurs et des ordinateurs avec des certificats. Vous pouvez installer un CA dans votre environnement en déployant le rôle AD CS sur Windows Server 2012. Lorsque vous installez le premier CA, il établit l'ICP dans le réseau, et il constitue le point le plus élevé dans l'ensemble de la structure. Vous pouvez avoir une ou plusieurs autorités de certification dans un réseau, mais un seul CA peut être au point sur la hiérarchie de CA plus élevé. Vous pouvez voir l'installation de CA dans l'annexe C.

Après l'installation et la configuration de CA dans le serveur CA et serveur de domaine PDC. Voyons comment demander pour créer un Certificat simple de l'autorité de certification interne. Maintenant, si votre gestionnaire IIS est ouvert, vous verrez "CertSrv" un répertoire virtuel créé,

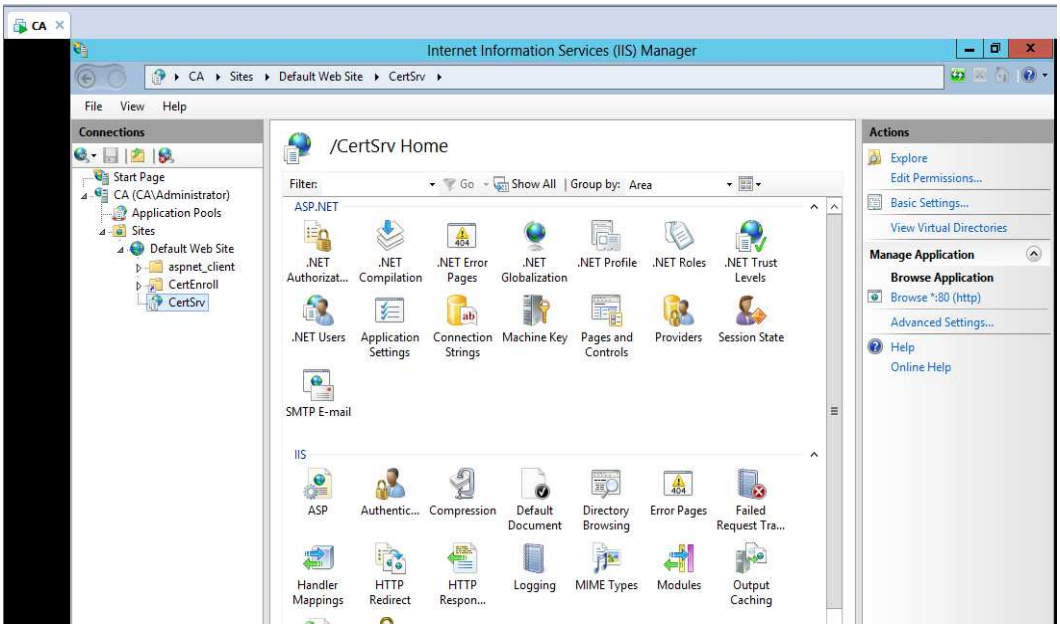
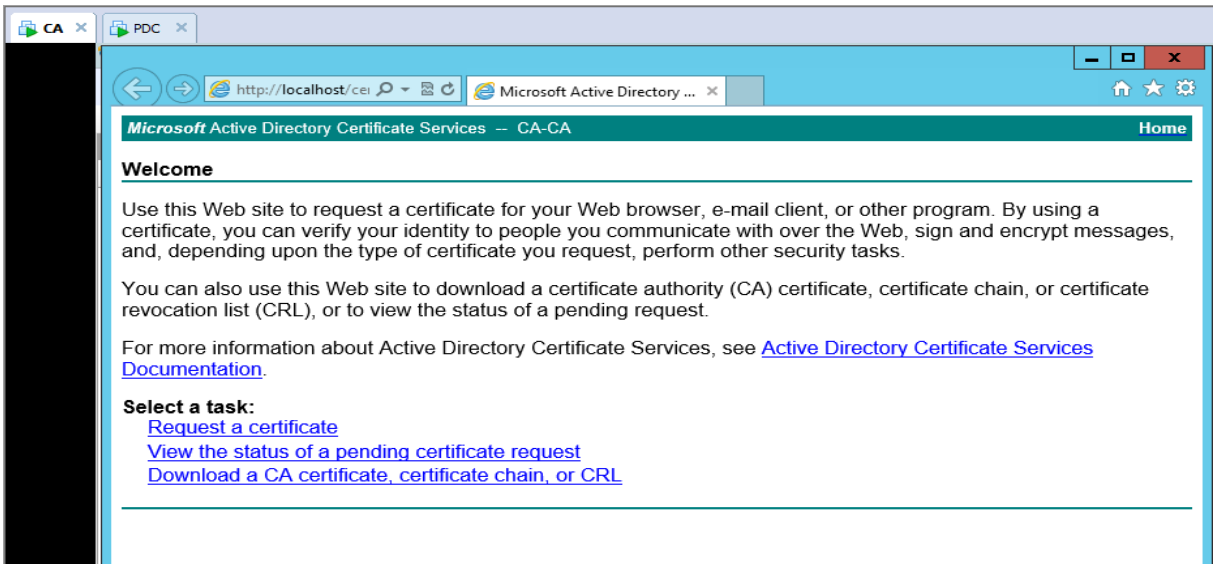


Figure IV.17 : Le répertoire CertSrv crée.

Utilisez la colonne de droite sur "Parcourir * .80 (http)

On doit avoir une page comme celle-là, choisissez Demander un certificat (Request a Certificate).



Cliquez sur Demande de certificat avancée (Advanced Certificate Request)

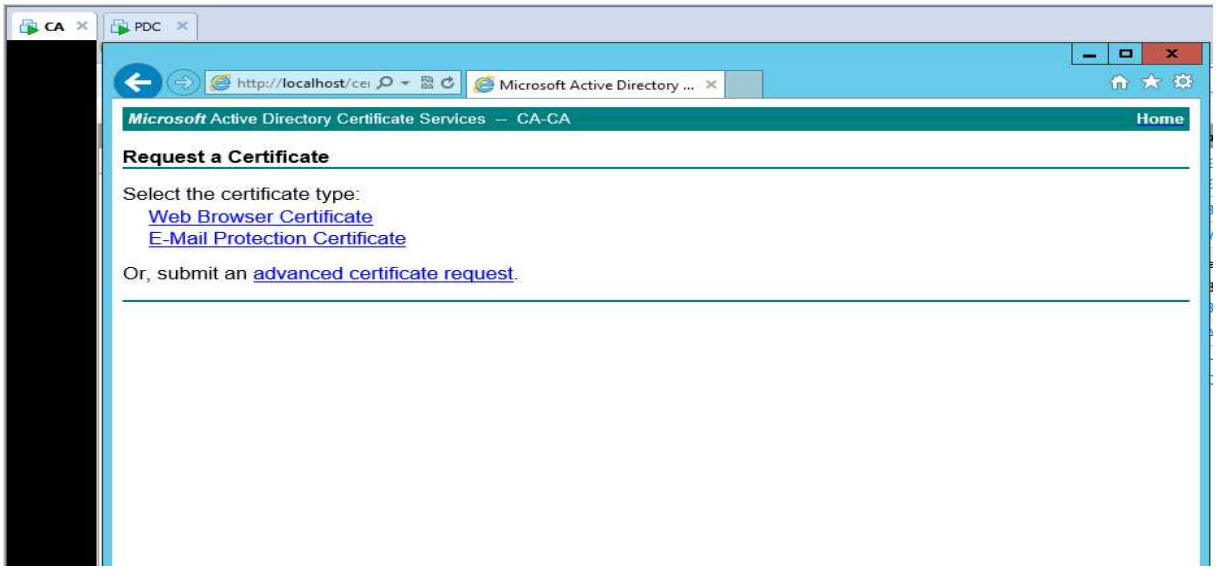
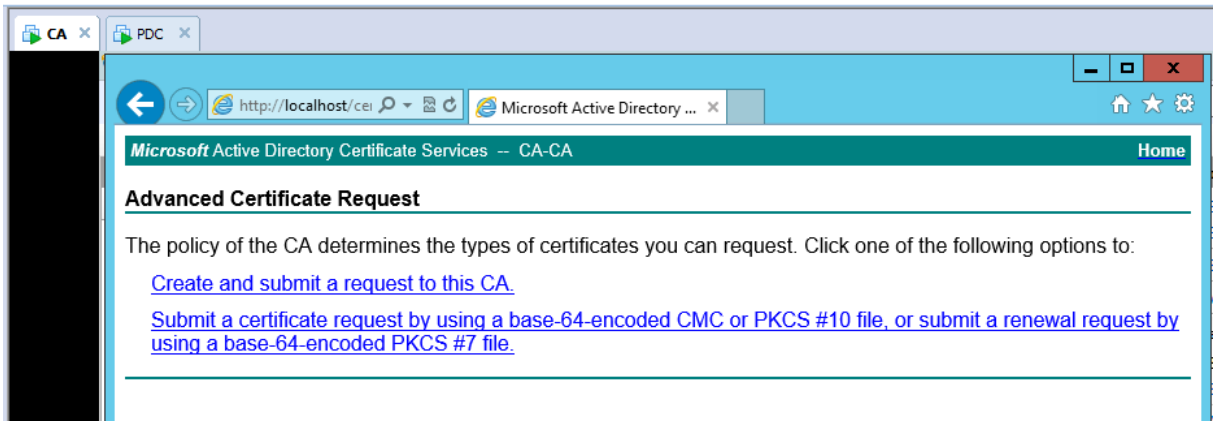
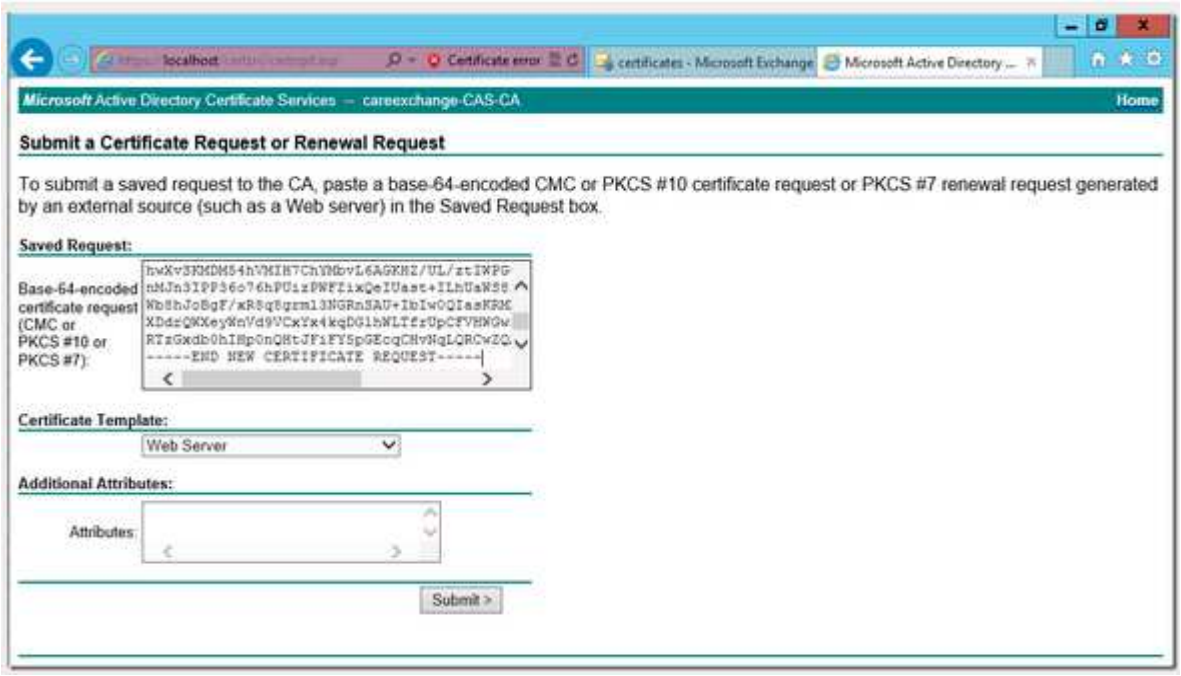


Figure IV.18 : La demande de certificat avancé.

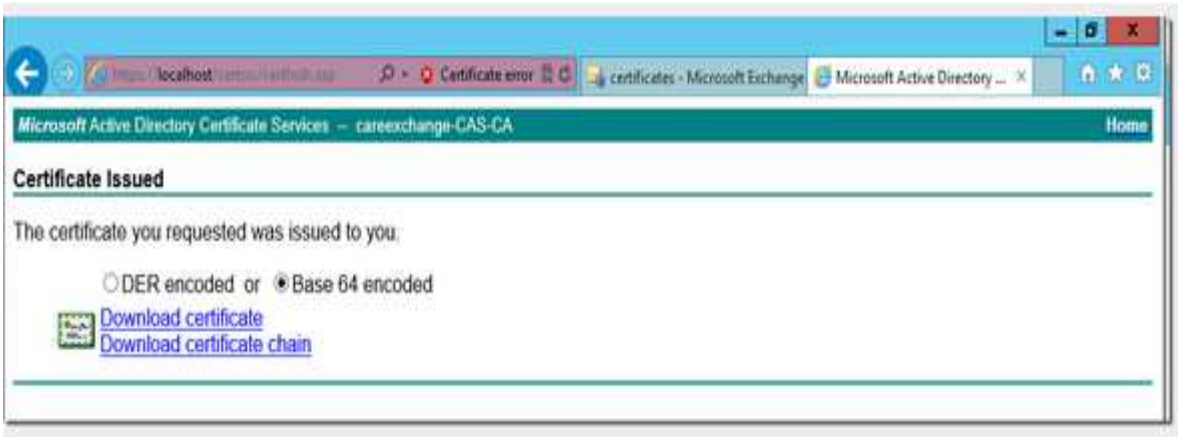
Choisissez le second. Soumettre une demande de certificat en utilisant un CMC base 64 codé



Maintenant Copiez le Bloc-notes - Choisir un modèle: WebServer



Choisissez "encodés en base 64"



Enregistrer le certificat

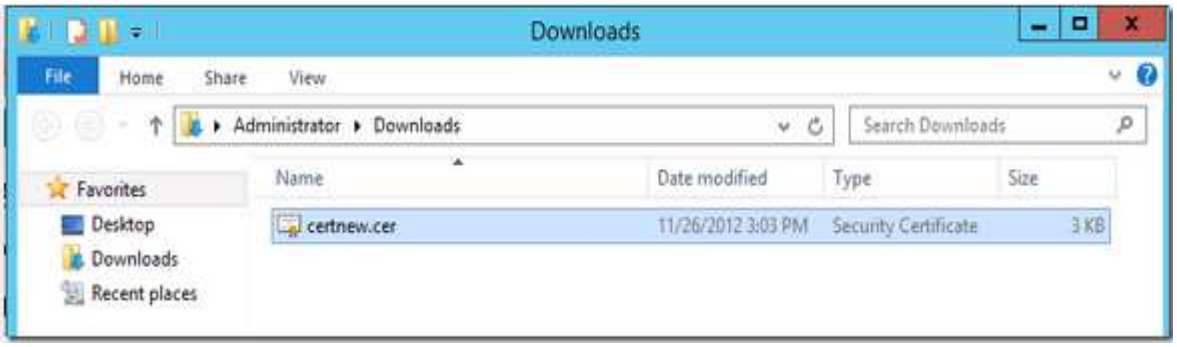


Figure IV.19 : L'enregistrement du certificat.

IV.3.5. Haute Disponibilité

IV.3.5.1. Configuration de basculement actif/veille sur le par feu ASA

Le basculement (en anglais, **Failover** qui se traduit par passer outre à la panne) est la capacité d'un équipement à basculer automatiquement vers un réseau alternatif ou en veille.

Caractéristiques :

Cette capacité existe pour tout type d'équipements réseau: du serveur au routeur en passant par les pare-feu et les commutateurs réseau (*switch*). Le basculement intervient généralement sans action humaine et même bien souvent sans aucun message d'alerte. Le basculement est conçu pour être totalement transparent.

Les concepteurs de systèmes prévoient généralement cette possibilité dans les serveurs ou les réseaux qui nécessitent une disponibilité permanente (HA=*High Availability*). Dans certains cas, le basculement automatique n'est pas souhaité et le basculement requiert une action humaine ; c'est ce que l'on appelle *automatisation avec approbation humaine*.

Il existe deux modes principaux de basculement :

- ✓ actif/actif qui s'apparente plus à de l'équilibrage de charge (*Load-Balancing*) ;
- ✓ et le mode classique couramment répandu, actif/passif où l'équipement secondaire (passif) est en mode veille tant que l'équipement primaire (actif) ne rencontre aucun problème.

Notons enfin, que le retour à la situation originelle après correction du problème (en anglais **Failback**) est une action manuelle dans la majorité des cas de basculement.

On a besoin de deux pare-feux ASA, ils ont le même matériel et logiciels (et une licence valide pour le basculement), il n'est pas difficile de configurer paires actif / passif.

Tout d'abord, on doit déclarer ce rôle. Chaque unité aura - primaire ou secondaire. Ceci est juste une étiquette et ne donne pas à la paire un avantage sur l'autre. Ce n'est certainement pas une priorité, il ne pense pas comme ça. C'est surtout de savoir quel pare-feu que vous utilisez depuis **configs** et les deux pare-feux seront les mêmes (y compris le nom d'hôte et IP).

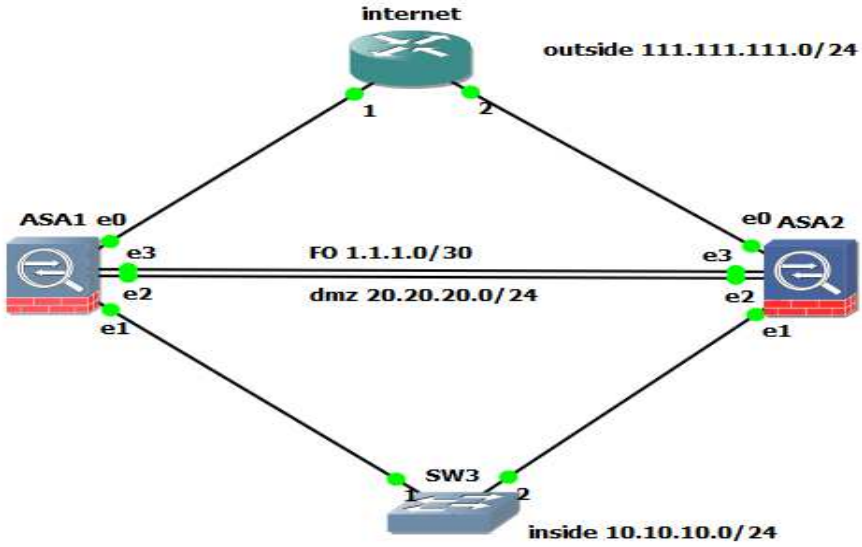
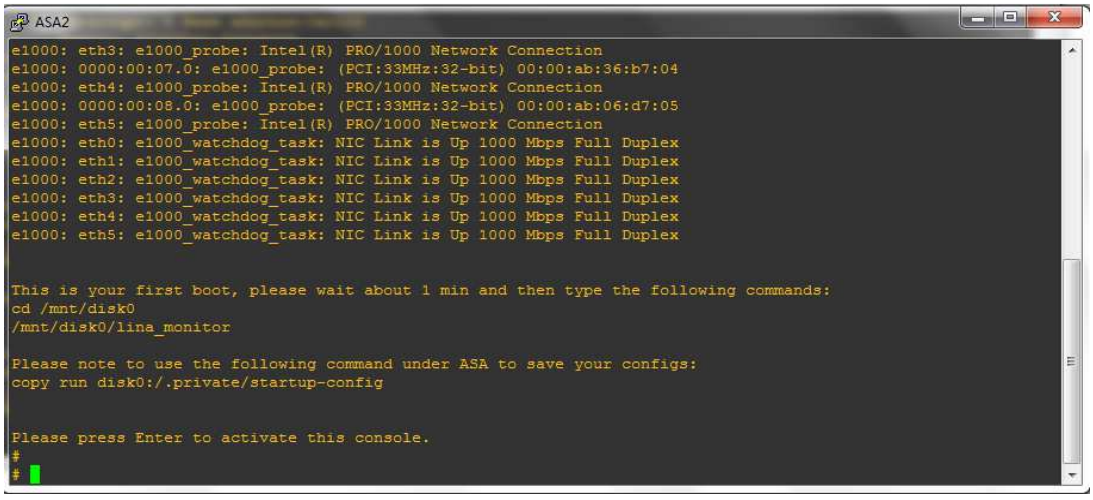


Figure IV.20 : Topologie des pare-feux ASA.

La configuration de basculement requiert deux Appliance de sécurités identiques connectées entre elles par un lien de basculement dédié et éventuellement un lien de basculement dynamique. La santé des interfaces et des unités actives est surveillée pour déterminer si les conditions spécifiques de basculement sont remplies. Si ces conditions sont remplies, le basculement se produit.

1.1. L'activation de la console

A l'ouverture de la console, un message d'activation de la console s'affiche, nous tapons les commandes suivantes comme la montre la figure ci-dessous pour activer la console.



1.2. La configuration des interfaces

L'attribution des adresses se fait comme tout autre équipement Cisco, néanmoins on doit préciser la nature de l'interface Inside ou Outside et DMZ et le niveau de sécurité de chaque interface ainsi le nom de pare-feu.

Configuration de l'interface Inside :

```
ciscoasa> en
Password:
ciscoasa# config t
ciscoasa(config)# hostname ASA-1
ASA-1(config)# interface e0/1
ASA-1(config-if)# ip address 10.10.10.1 255.255.255.0 stanby
10.10.10.2
                                                          ^
ERROR: % Invalid input detected at '^' marker.
ASA-1(config-if)# ip address 10.10.10.1 255.255.255.0 st
ASA-1(config-if)# ip address 10.10.10.1 255.255.255.0 standby
  10.10.10.2
ASA-1(config-if)# name
ASA-1(config-if)# namei
ASA-1(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA-1(config-if)# no shut
ASA-1(config-if)#
```

Configuration de l'interface DMZ.

```
ASA-1(config-if)# interface e0/2
ASA-1(config-if)# ip address 20.20.20.1 255.255.255.0 standby 20.20.
20.2
ASA-1(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA-1(config-if)# security-level 50
ASA-1(config-if)# no shut
ASA-1(config-if)#
```

Configuration de l'interface Outside.

```
ASA-1(config-if)# interface e0/0
ASA-1(config-if)# ip address 111.111.111.1 255.255.255.0 standby 111
.111.111.2
ASA-1(config-if)# no shut
ASA-1(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA-1(config-if)# int e0/3
ASA-1(config-if)# no shut
ASA-1(config-if)#
```

Désignez l'unité comme l'unité principale.

```
ASA-1(config)# failover lan unit primary
ASA-1(config)# failover replication http
ASA-1(config)#
```

Cette étape est la seule qui est différente entre les pare-feux primaires et secondaires. Le reste s'applique aux deux unités.

L'étape suivante consiste à configurer une interface appelée le lien de basculement qui est utilisé pour synchroniser la configuration. Le choix logique pour une config est l'interface Ethernet e0/3, mais la recommandation est que vous utilisez une interface qui a la même capacité que les interfaces de production. Pour configurer cette interface pour le basculement, vous devez lier une interface physique à un nom logique et puis donner ce nom une adresse IP. Bien sûr, n'oublions pas à l'administrateur de l'interface. Nous appelons notre interface **failover.**

```
ASA-1(config)# failover mac address e0/1  00ab.cd92.5201  00a
b.a72f.0101
ASA-1(config)# failover mac address e0/2 00ab.cd92.5202  00ab
.a72f.0102
ASA-1(config)# failover mac address e0/0 00ab.cd92.5200  00ab
.a72f.0100
ASA-1(config)#
```

Activez le basculement :

```
ASA-1(config)# failover interface ip failover 1.1.1.1 255.255.255.252 standby $
ASA-1(config)# failover
```

```
ASA-1(config)# $ver 1.1.1.1 255.255.255.252 standby 1.1.1.2
```

Pour le 2éme par feu ASA c'est le secondaire s'applique aussi sur unité.

On tape les mêmes configurations de premier pare-feu, voici les configurations.

```
ASA-2(config)# failover lan unit secondary
```

```
ASA-2(config)# failover lan interface failover e0/3
```

```
ASA-2(config)# failover interface ip failover 1.1.1.1 255.255.255.252 standby $
```

```
ASA-2(config)# $ver 1.1.1.1 255.255.255.252 standby 1.1.1.2
```

On tape **sh failover** pour vérifier notre configuration :

Voila le résultat de notre configuration des 2 pare-feux ASA, le premier pare-feu est en mode actif et le deuxième en mode veille.

```
ASA-1(config)# sh failover
Failover On
Failover unit Primary
Failover LAN Interface: failover Ethernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
failover replication http
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 00:00:10 UTC Nov 30 1999
        This host:  Primary - Active
                Active time: 256 (sec)
                slot 0: empty
                  Interface outside (111.111.111.1): Normal
                  Interface inside (10.10.10.1): Normal
                  Interface dmz (20.20.20.1): Link Down (Waiting)
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: empty
                  Interface outside (111.111.111.2): Normal
                  Interface inside (10.10.10.2): Normal
                  Interface dmz (20.20.20.2): Link Down (Waiting)
                slot 1: empty

Stateful Failover Logical Update Statistics
        Link : Unconfigured.

ASA-1(config)#
```

1.3. tester le basculement :

Pour désactiver le basculement, entrez la commande suivante

Si vous désactivez le basculement sur une paire actif/veille, l'état actif et en veille de chaque unité est conservé jusqu'à ce que vous redémarriez. Par exemple, l'unité en veille reste en mode de veille, et donc les deux unités ne commencent pas à acheminer le trafic. Pour activer l'unité en veille (même avec le basculement désactivé), référez-vous à la section Basculement forcé.

IV.3.5.2. Configuration de basculement actif/veille sur les Switch 3560

1. **Hot Standby Router Protocol** (HSRP) :

Est un protocole propriétaire de Cisco implémenté sur les routeurs et les commutateurs de niveau 3 permettant une continuité de service. HSRP est principalement utilisé pour assurer la disponibilité de la passerelle par défaut dans un sous-réseau en dépit d'une panne d'un routeur.

Le protocole HSRP est très répandu avec du matériel Cisco sur les LAN. Cela permet une souplesse de configuration sur tous les matériels Cisco.

2. **Configuration de HSRP** :

Nous allons prendre comme cas de figure, le schéma suivant :

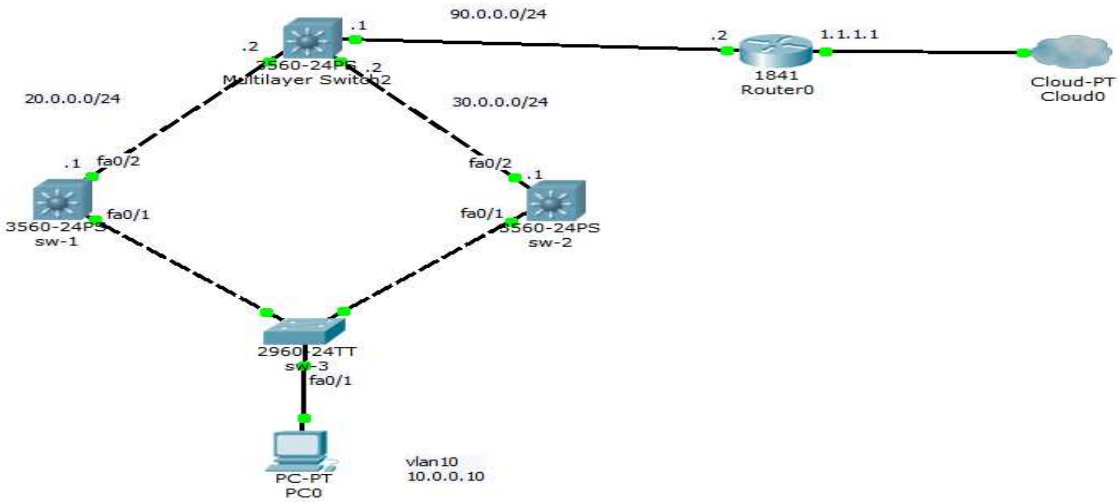
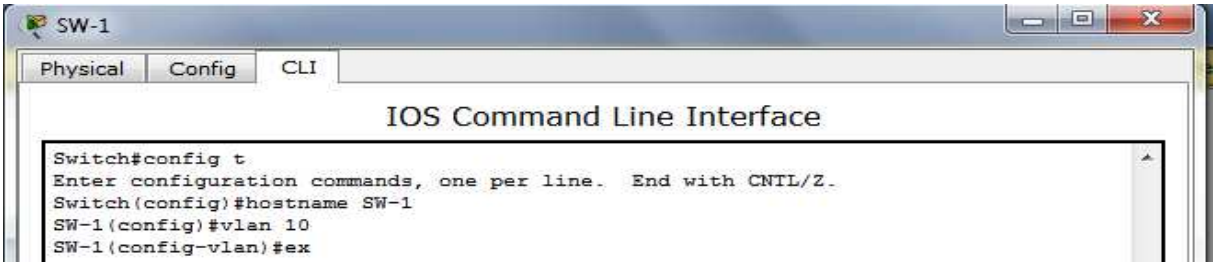


Figure IV.21 : Configuration HSRP typique.

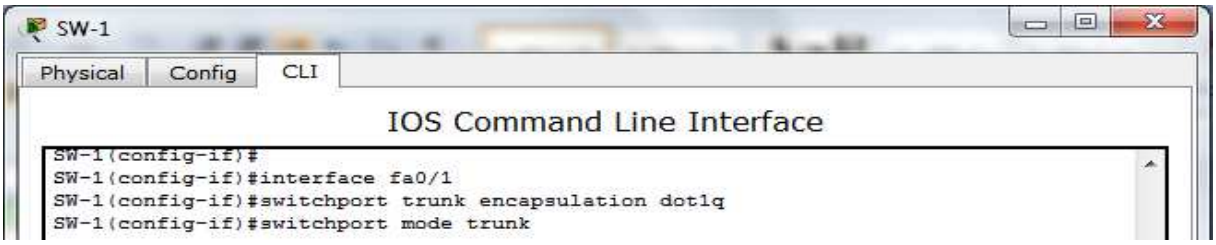
Les interfaces FastEthernet 0/2 des Switchs sont pour les liens vers Internet et les interfaces FastEthernet 0/1 pour les liens du LAN.

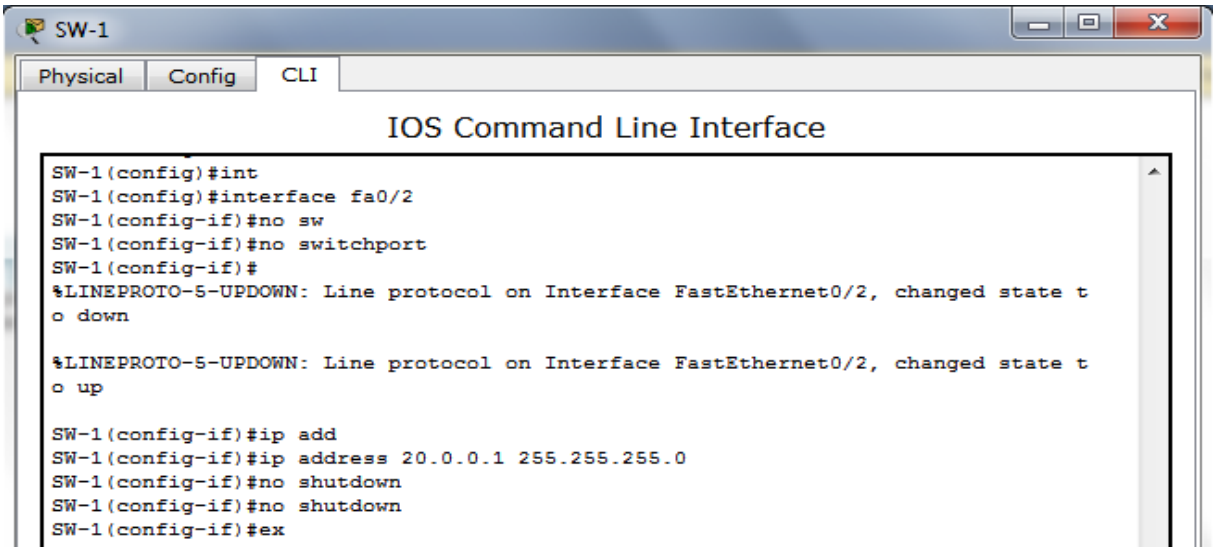
Nous choisirons le groupe HSRP Numéro 1 et SW-1 en tant que routeur primaire. Nous créant le vlan 10 dans le sw-1.

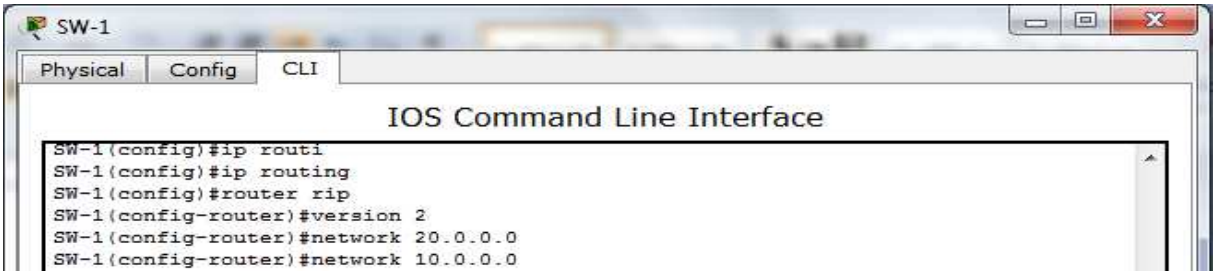


Il faut de toute façon affecter une adresse IP physique réelle à chacune des interfaces puis configurer le HSRP.

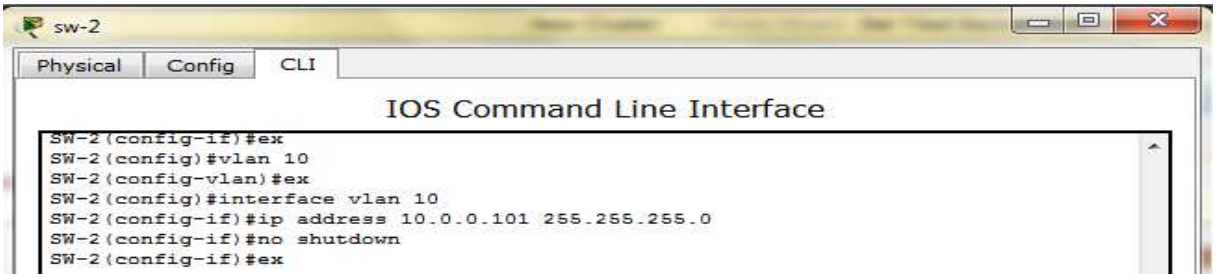
- Configurant l'interface fastethernet 0/1 en mode trunk,

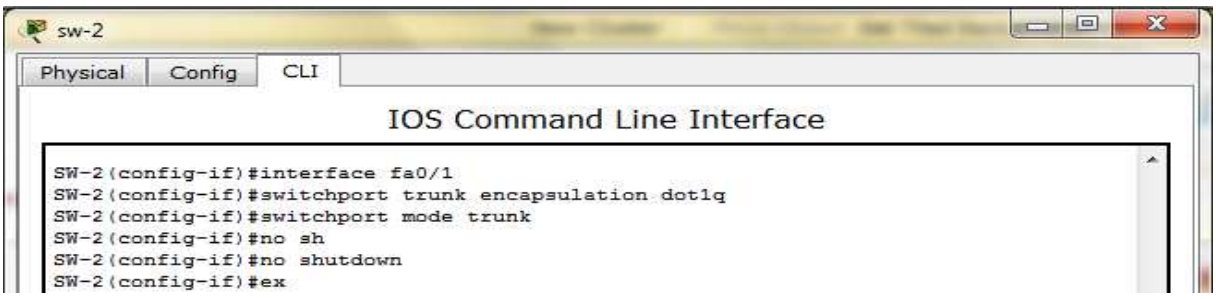


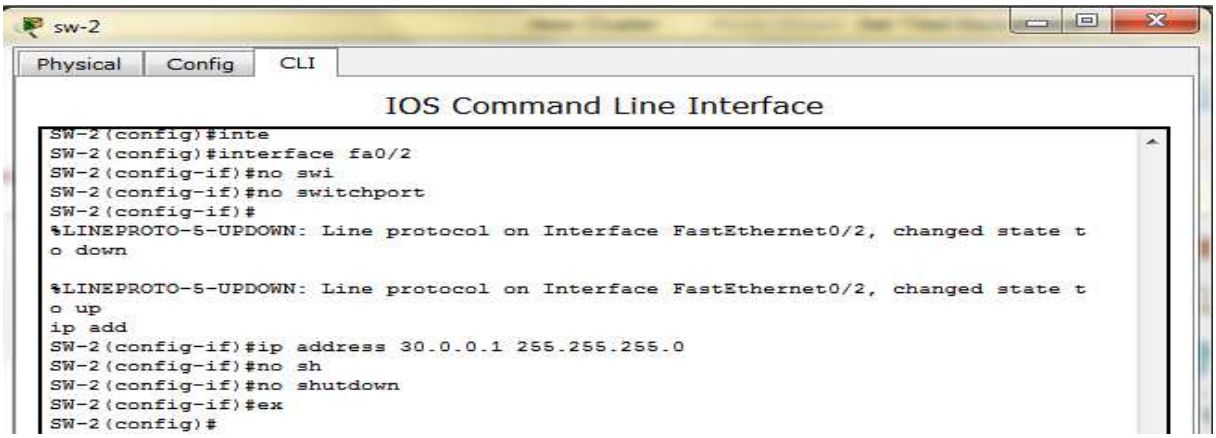


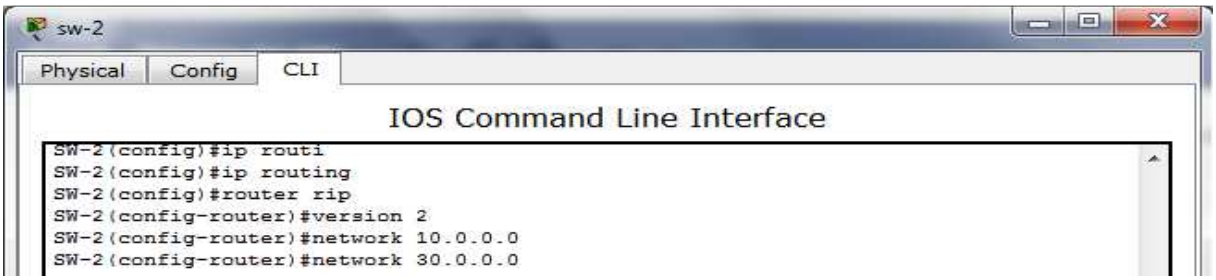


On refait les mêmes configurations avec les 2éme switch sw-2,

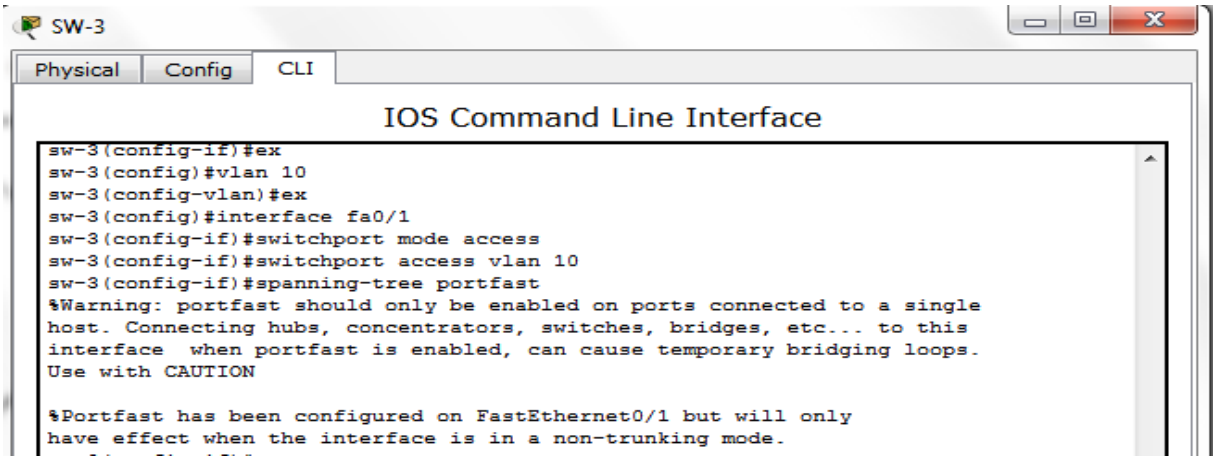








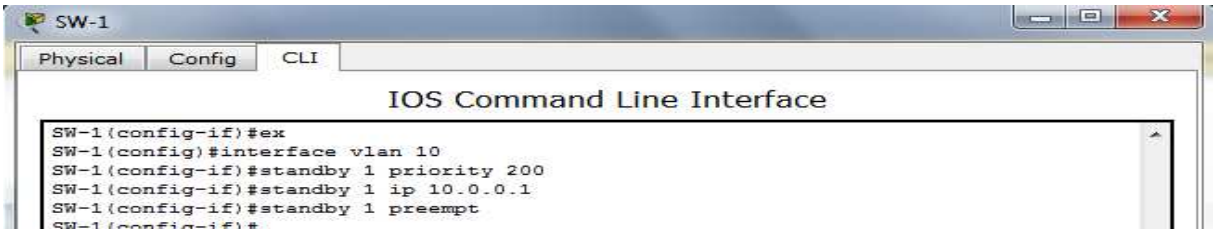
L'interface fastethernet 0/1 de switch 3 est configurer en mode **access** sur le vlan 10,

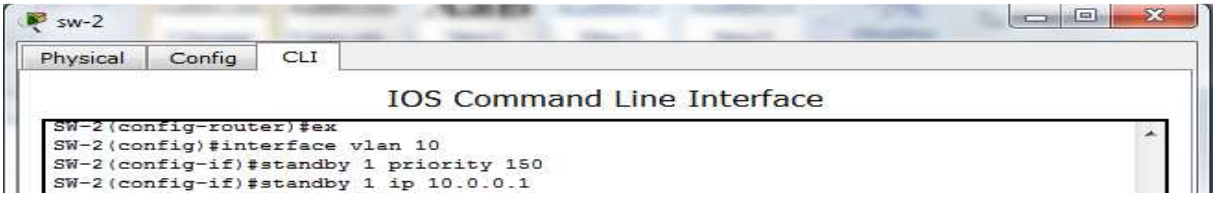


Dans chaque sous-réseau où HSRP est actif, on définit un *groupe* de Switch, c'est-à-dire un identifiant numérique. Le numéro du groupe varie de 0 à 255, il peut donc exister jusqu'à 256 groupes HSRP dans un même sous-réseau. Chaque groupe est associé à une adresse IP virtuelle distincte dans notre cas on a choisi groupe 1 et l'adresse virtuel 10.0.0.1**.**

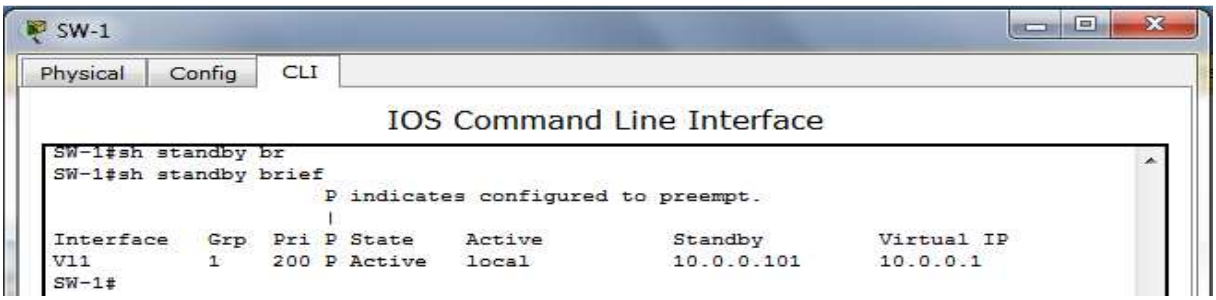
La priorité est définie ici, en effet par défaut elle est à 100. Donc sw-1 avec sa priorité 200 sera élu primaire (active) et sw-2 secondaire (Standby) 150.

Le denier paramètre "*preempt*" permet d'accélérer le processus d'élection. Le Switch avec la plus haute priorité sera élu, même si un nouveau Switch avec une priorité plus haute est ajouté.

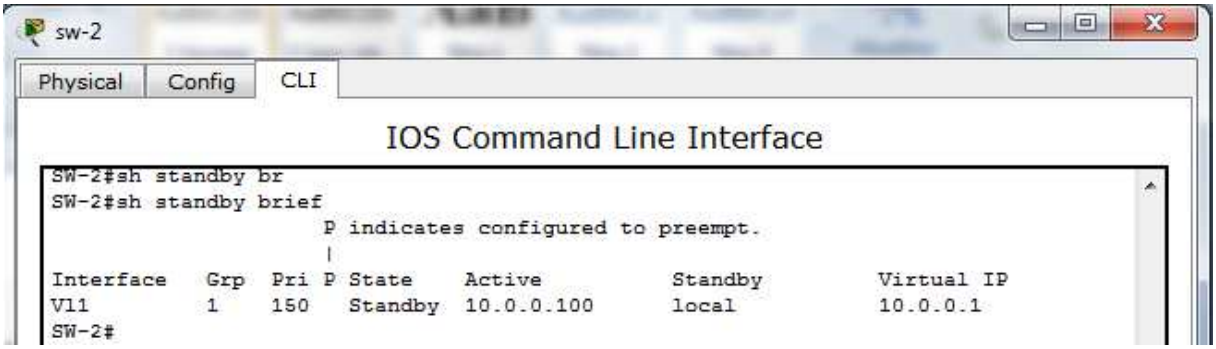




Avec la commande **sh standby brief** permet d'afficher le résultat de notre configuration le Switch sw-1 il est en mode actif et le sw-2 en mode veille.



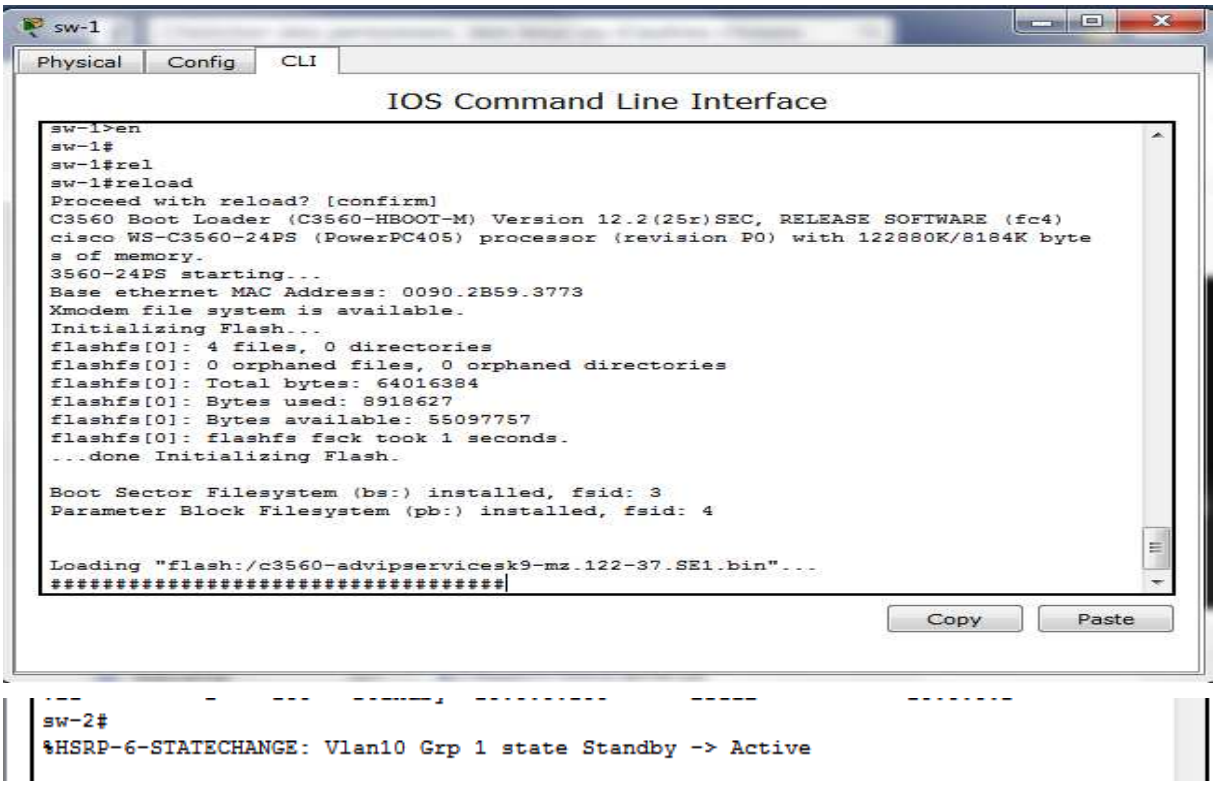
Et c'est la même chose pour sw-2,



a. Tester le basculement:

Dans le groupe 1, le sw-1 est *actif* sera élu : celui qui aura la priorité la plus élevée. L'autre Switch sw-2 est en *standby* et écoutent les messages émis par le Switch actif. Périodiquement, le Switch du groupe 1 échange des messages *Hello* pour s'assurer que le Switch du groupe 1 est encore joignable. Par défaut, les messages *Hello* sont envoyés toutes les 3 secondes, et un délai de 10 secondes sans message Hello de la part du Switch actif entraîne la promotion du Switch *Standby* en actif.

On redémarre le sw-1 et on voit le résultat sur le sw-2 il est on mode active donc le test est réussi.



IV.4. Conclusion

Les entreprises conservent leurs données dans les disques durs des ordinateurs, tout en installant des logiciels et des applications sur ces derniers. Ce type de stockage bien que pratique, expose cependant les entreprises à un risque de perte de leurs données en cas de détérioration ou de panne de leurs disques durs. Grâce à l'architecture Cloud, les entreprises peuvent bénéficier d'une haute disponibilité. Comme les ressources (données informatiques, stockage…) ne sont plus sur des machines physiques spécifiques, le Cloud peut répondre rapidement à toute panne en déplaçant les ressources vers les machines qui sont toujours actives.

Conclusion Générale

Le Cloud Computing est aujourd'hui une vraie révolution et une bonne opportunité pour les entreprises. Elles sont de plus en plus nombreuses à exploiter le Cloud Computing pour offrir de nouveaux services.

Dans notre mémoire nous nous sommes intéressés à la réalisation d'une infrastructure Cloud Computing, qui permettra une sécurité accrue pour les entreprises, qui seront bien moins exposés au risque lié à la perte des données.

Ce projet nous a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il nous a initiés au monde de la recherche sur l'évolution des technologies informatique. Il nous a également permis de découvrir le logiciel de simulation VMware Workstation, GNS3, Windows server 2008, Windows server 2008 R2, Windows server 2012 et services d'annuaire Active Directory.

Le Cloud Computing augmente le nombre de services web, permettant aux fournisseurs d'offrir plus de services plus rapidement et plus efficacement. Grâce à ces derniers, les entreprises obtiennent de meilleurs résultats.

L'inconvénient du Cloud Computing est que les données sont hébergées en dehors de l'entreprise. Ceci peut donc poser un risque potentiel fort pour l'entreprise de voir ses données mal utilisées ou volées.

Le modèle Cloud Computing va donc s'imposer largement et inspirer le modèle d'organisation de tous les centres informatiques dans les vingt prochaines années. Cependant, ce modèle est encore très jeune et en évolution rapide. Le développement de l'Internet mobile avec les centaines de millions de téléphones mobiles et de tablettes va largement amplifier le besoin d'avoir un accès universel aux données par tout type d'équipement. Le Cloud Computing deviendra l'acteur majeur de cette transformation.

Annexes

A.1. GNS3

Pour la rédaction de cette annexe nous nous sommes basés sur le site officiel de GNS3.

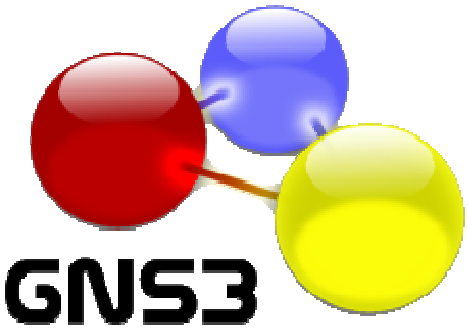
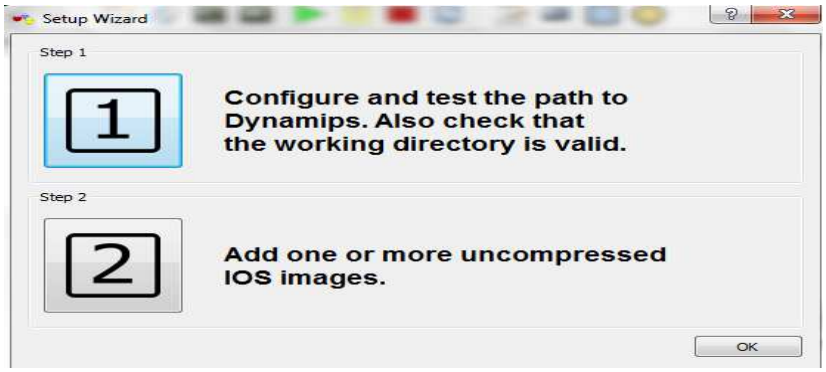


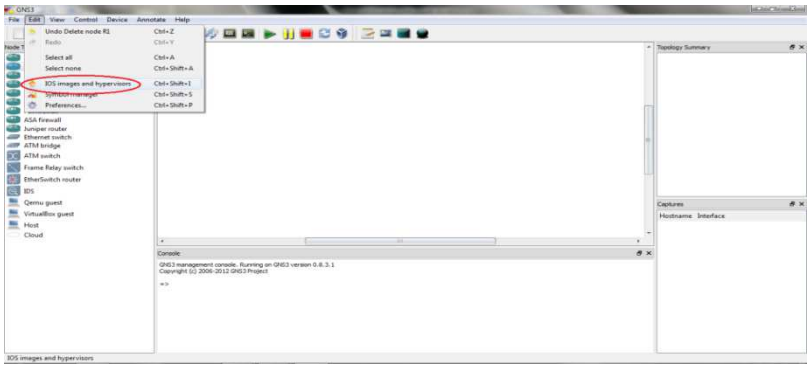
Figure A.1: GNS3.

A.1.1. Installation de GNS3

GNS3 est téléchargeable depuis le site officiel de GNS3. La version téléchargée est GNS3 v0.7.4 all-in-one. Son installation est une succession du terme suivant. Au lancement de GNS3, il existe deux possibilités de configuration qui sont :



A.1.2. L'ajout et configuration des IOS

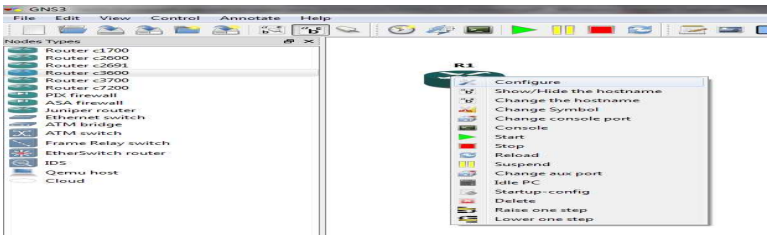


L'IOS étant le système d'exploitation des équipements Cisco, il les gère en se basant sur l'architecture matérielle. Avant de configurer les IOS, il faut les télécharger. Après le téléchargement, l'étape suivante consiste à lier l'IOS à son modèle d'équipement.
Pour ajouter l'IOS aux équipements adéquats:

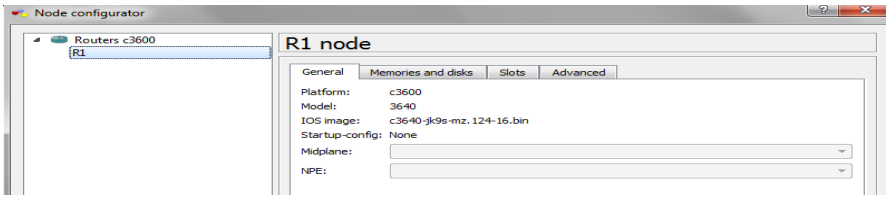
- ✓ Sélectionnons dans le menu Edit->IOS Images and Hypervisors.
- ✓ Cliquons sur image file et sélectionnons l'IOS depuis son emplacement, puis choisissons la plate forme et le modèle de l'équipement et enfin sauvegardons.

A.1.3. Création d'une topologie réseaux basique

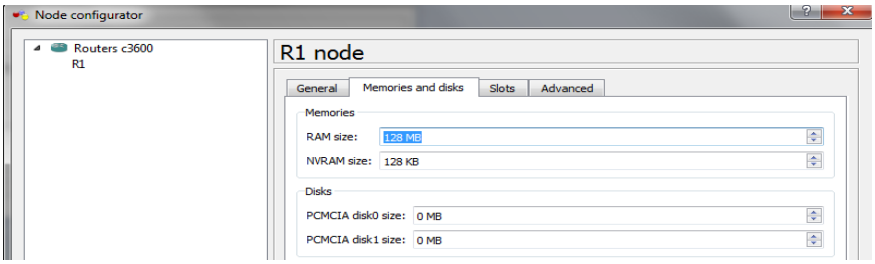
Après avoir configuré l'IOS d'un routeur 7200, faire un drag and drop sur la fenêtre principale, le routeur apparaîtra avec un nom par default R1. Pour le configurer, cliquons sur configurer.



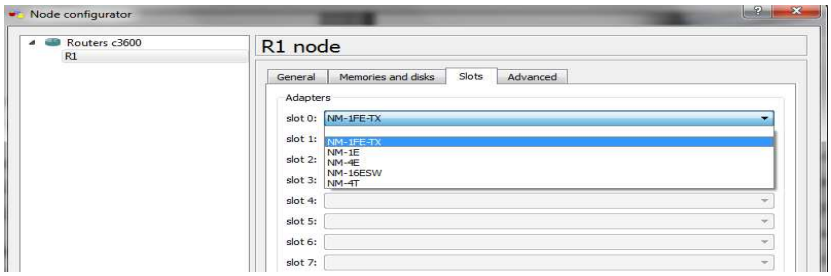
Ensuite apparaît la fenêtre indiquant les propriétés du routeur (appelé node configurator). L'onglet général indique la plateforme, le modèle du routeur ainsi que son IOS. Startup config est le fichier de configuration stocké dans la NVRAM.



Sur l'onglet **Memories and Disk**, la RAM et la NVRAM peuvent être configurées.



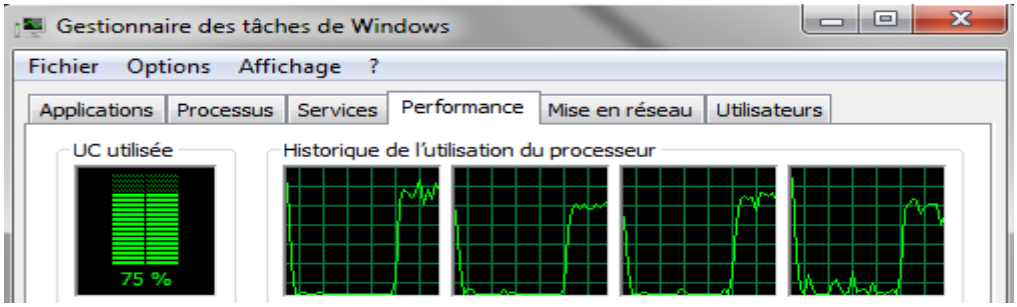
L'onglet slot (interfaces) permet de choisir les modules à ajouter au routeur.



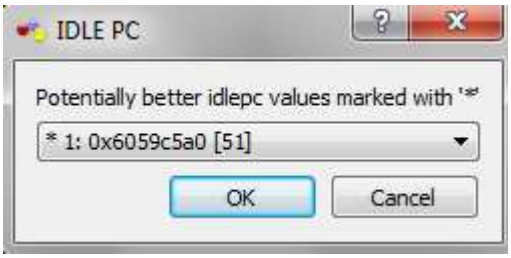
Apres avoir fait le choix du routeur, effectuant un clic droit sur le routeur et start, et pour avoir accès à la console, puis effectuons un clic droit et console. L'image de l'IOS apparaît décompressée et chargé en RAM.

A.1.4. Optimisation de l'utilisation des ressources CPU

GNS3 consommant les ressources matérielles, la CPU du PC utilisé peut atteindre des sommets comme ci-dessous.

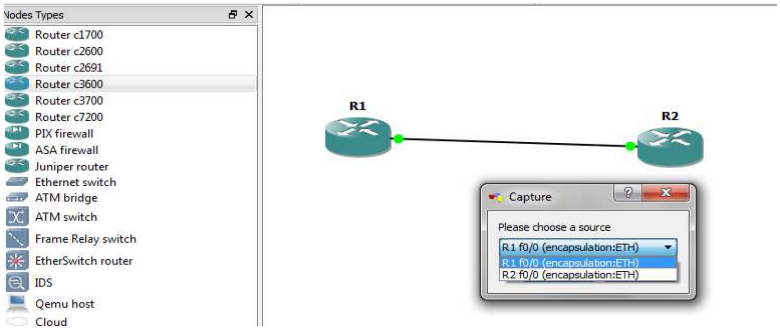


Pour éviter cela, effectuons un clic droit sur le routeur et sélectionnant idle PC. Une fenêtre temporaire apparaît le temps de calculer ce qui est appelé idle value, puis s'affiche un menu déroulant avec une ou plusieurs valeurs différentes de l'idle value. Il faut choisir la valeur avec un astérix. Un message de confirmation apparaitra pour indiquer que cela a été appliqué. L'utilisation de la CPU devrait revenir à un niveau raisonnable (quelques %)



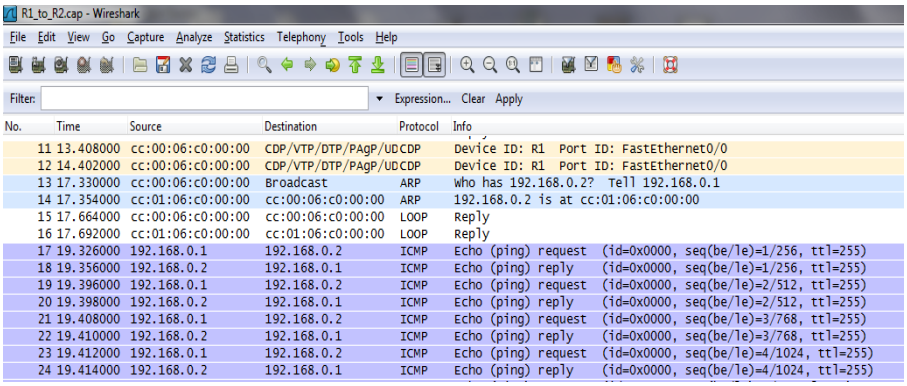
A.1.5. Capture de paquet

GNS3 permet de capturer le trafic sur un lien donné à l'aide de wireshark (qui est installé avec cette version de GNS3). Prenons un exemple de deux routeurs connectés en Fastethernet, il faut effectuer un clic droit sur le lien physique, et cliquer sur capture. Un menu déroulant apparait avec possibilité de choisir l'interface physique.



Après sélection, wireshark se charge (s'il n'a pas été installé dans le répertoire par default, il faut modifier cela dans le menu Edit-> Préférence ->Capture en sélectionnant le répertoire où il se trouve).

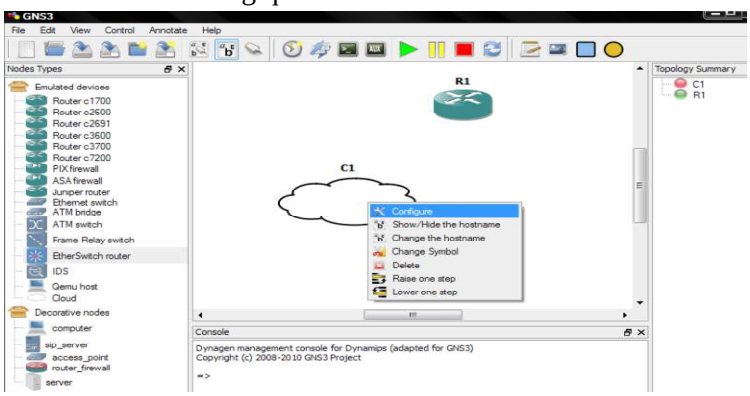
Il permet de visualiser le Ping qui sera effectué entre les deux routeurs.



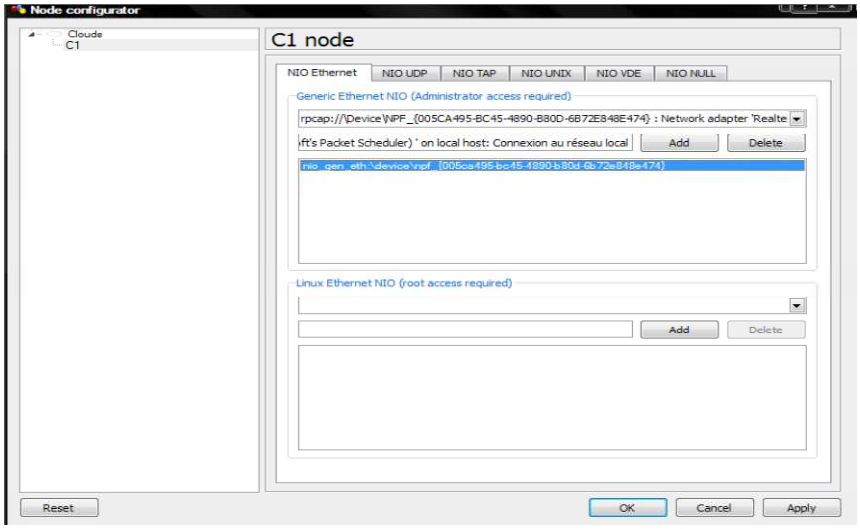
A.1.6. La connexion d'une interface routeur à la carte réseau d'une machine virtuelle

La procédure

Ajoutons un Cloud (nuage) dans l'espace de travail en choisissant « Change Symbol », il est possible de le transformer en un autre équipement (une machine) et le connecter par un câble avec une interface du routeur. Celle-ci connectée, elle représente la carte réseau qui peut être configurée avec les paramètres IP pour une connexion logique à l'interface du routeur.



Lors de la configuration de la machine la fenêtre Node configurator apparaît. Elle liste les différentes cartes réseau dont dispose la machine physique. Apres sélection de la carte réseau voulue, il suffit de l'ajouter.



A.2. Packet Tracer

Figure A.2 : Packet Tracer.

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc. . . .

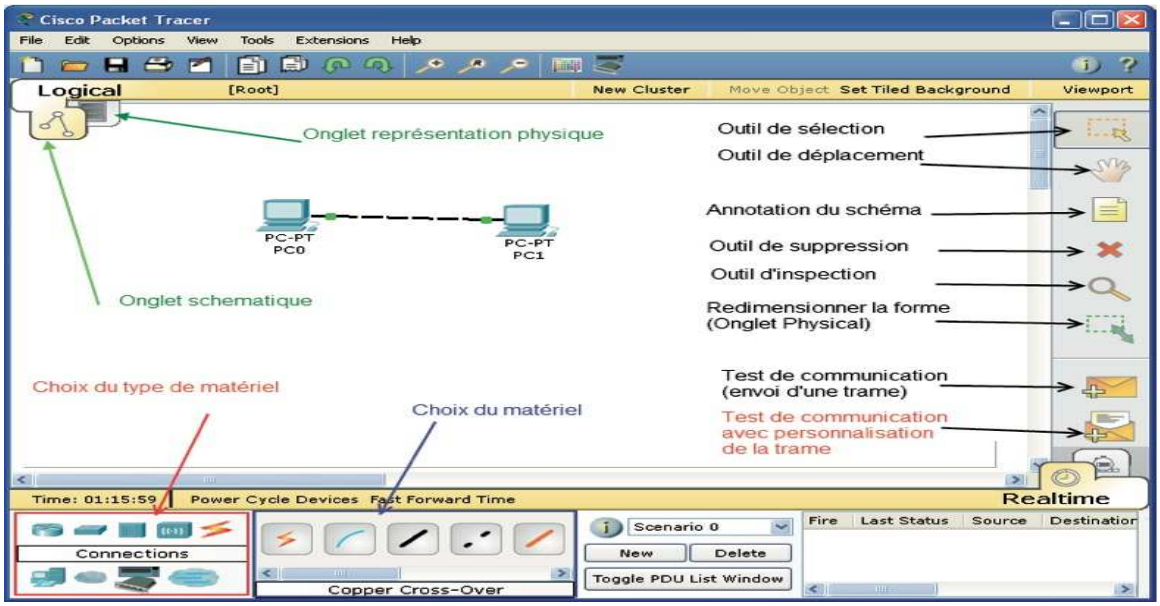
A.2.1. Présentation de l'écran principal :

- Une barre de menu classique.
- Une barre d'outils principale avec les fonctionnalités de base de gestion de fichier, d'impression, etc.….
- Une barre d'outils à droite avec les outils minimaux.
- Une barre en bas avec trois boites :
  - ✓ Choix du type de matériel (ordinateur, routeurs, etc.…).
  - ✓ Choix du matériel en fonction du type.
  - ✓ Résultats de l'échange de données.

Pour créer votre schéma :

On suppose qu'il n'y a pas de schéma au départ sinon cliquer sur File/New.

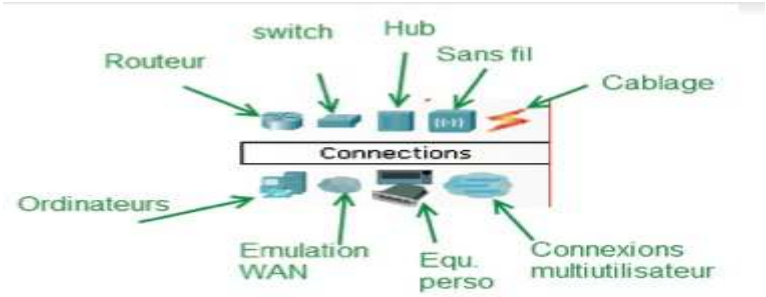
Se placer dans l'onglet LOGICAL sous la barre d'outils principale.



A.2.2. Placement du matériel

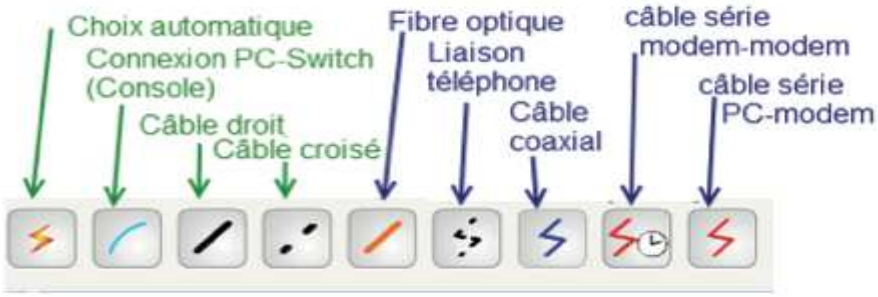
- Choisir le Type de matériel
- Selon le type, la liste du matériel change de manière dynamique. Cette liste est conséquente et basée sur des références Cisco.
- Cliquer sur le matériel souhaité pour le sélectionner et déplacer le dans l'espace de travail pour placer le matériel.

- Placer tout le matériel souhaité pour créer votre architecture.



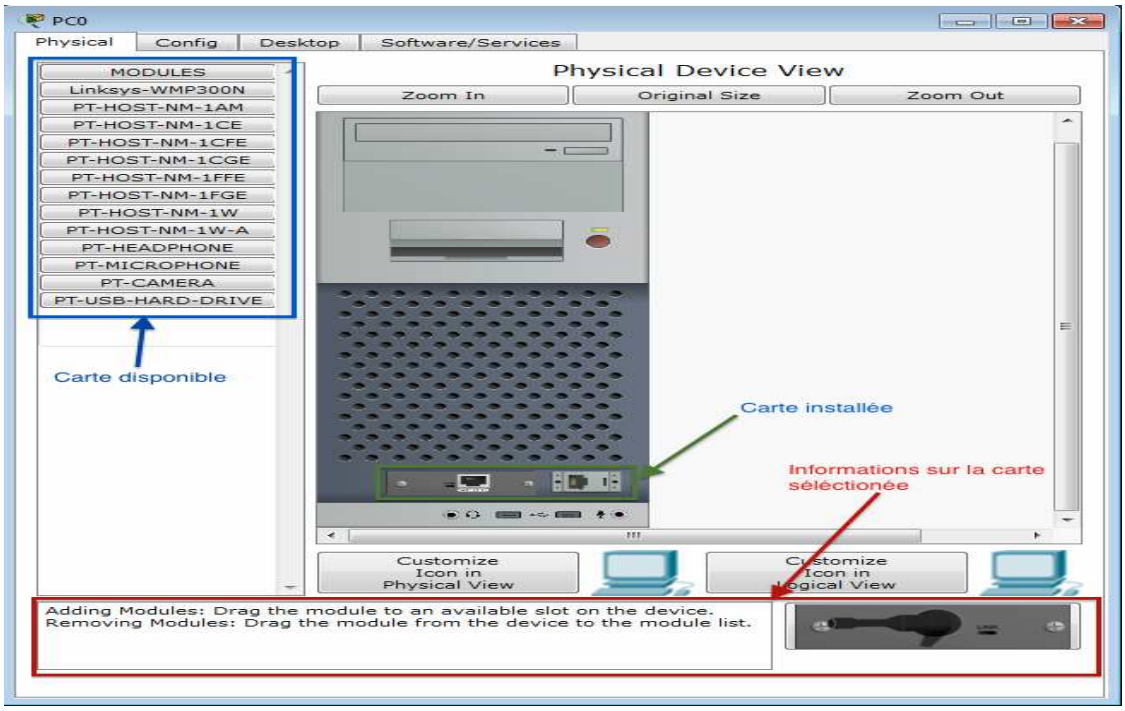
A.2.3. Interconnecter vos équipements

- Choisir l'outil câblage.
- Choisir le type de connexion.
- Cliquer sur le premier équipement.
- Choisir le connecteur désiré.
- Cliquer ensuite sur le deuxième équipement et choisir le connecteur désiré.
- La connexion doit être visible sur le schéma.
- Les points de couler aux extrémités de la connexion informe de l'état de la liaison. Ils peuvent être rouges, orange ou vert.
- Il est possible de modifier le nom des éléments en double cliquant sur leur nom.
- Il est souhaitable également d'annoter le schéma (adresse IP, adresse du réseau, etc.…) avec l'outil Note.



A.2.4. Paramétrage des appareils :

Pour accéder au paramétrage d'un appareil, il faut cliquer sur la représentation de l'appareil. Deux à quatre onglets sont accessibles avec cette fenêtre en fonction de type de l'équipement. Paramétrage physique (Physical). Le paramétrage physique consiste à placer les bonnes cartes dans l'appareil. Les cartes disponibles se trouvent à gauche de l'écran. Pour le placer, commencer par éteindre l'appareil avec le bouton Marche/Arrêt (M/A). Si besoin retirer la carte en place, par glisser déplacer de l'appareil vers la liste des cartes. Glisser la nouvelle carte sélectionnée de la liste des modules à l'emplacement vide. Appuyer à nouveau sur le bouton M/A.



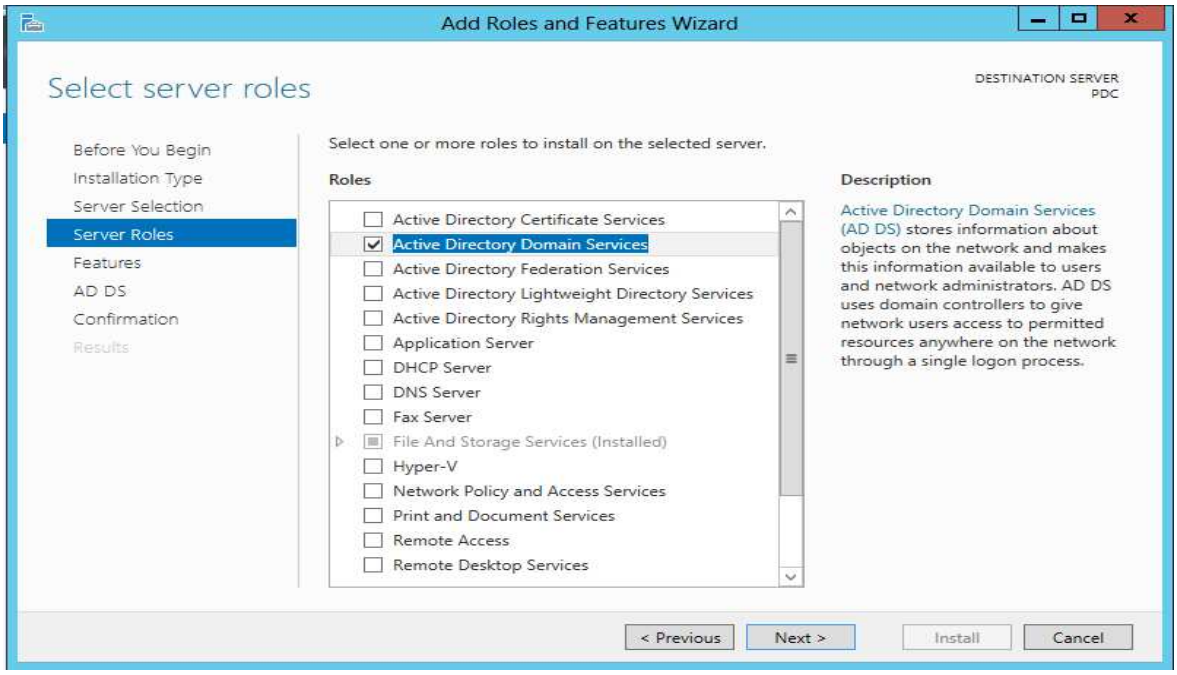
A.3. Windows Server 2012: Active Directory Domain Services

Figure A.3 : Windows Server 2012 et Active Directory.

Active Directory est la base d'un réseau Microsoft.

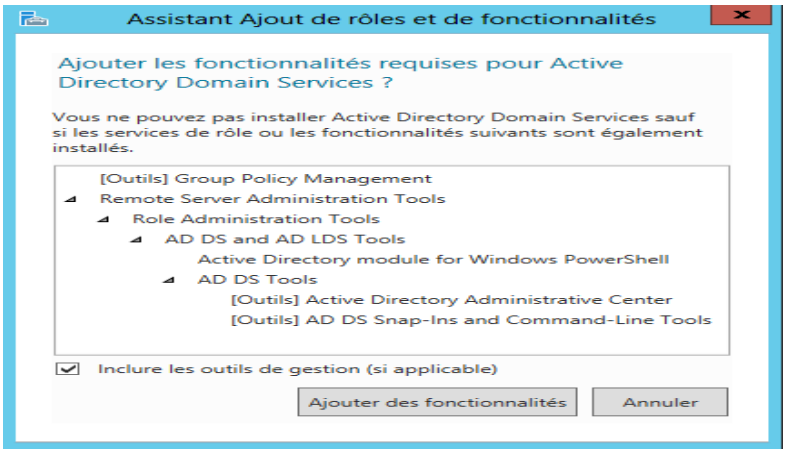
Il permet la gestion des ressources : utilisateurs et périphériques, l'authentification et la sécurisation des accès. Mais c'est aussi la base de nombreux autres services comme DNS, WINS, DHCP, …..

Pour ajouter Active Directory, vous devez passez par l'assistant de gestion des Rôles :



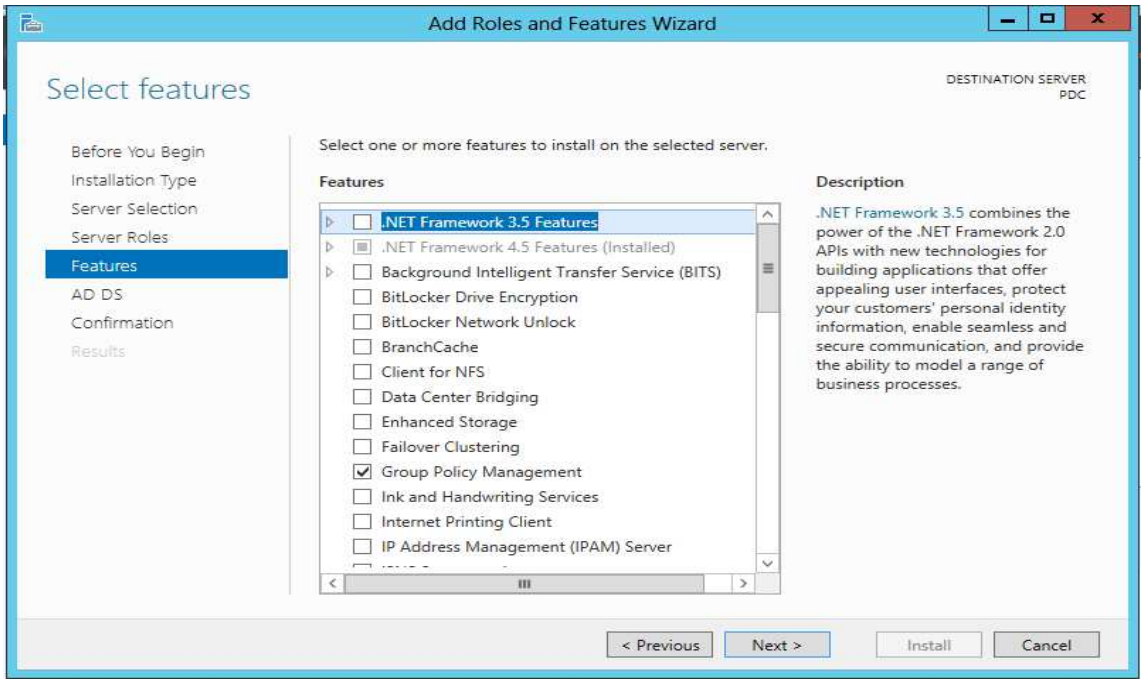
Auparavant, il était possible de lancer l'assistant Active Directory avec la commande **dcpromo**, mais celle ci a été supprimée.

Naturellement Active Directory Domain Services a besoin de fonctionnalités annexes :



On clique donc sur Ajouter des fonctionnalités, puis continuez l'assistant en cliquant sur Suivant.

Les fonctionnalités obligatoires ont été pré cochées, cliquez sur Suivant.

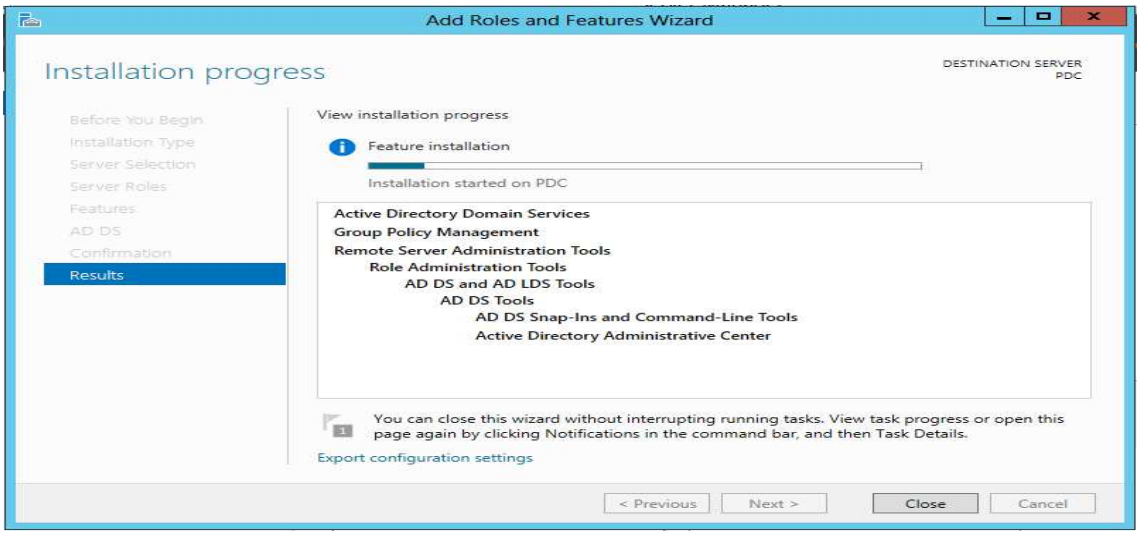


Un message d'avertissement est affiché, il rappelle les bases d'active Directory : redondance des contrôleurs de domaine, nécessité de DNS, …

Enfin un dernier récapitulatif est affiché :

Cliquez sur Installer

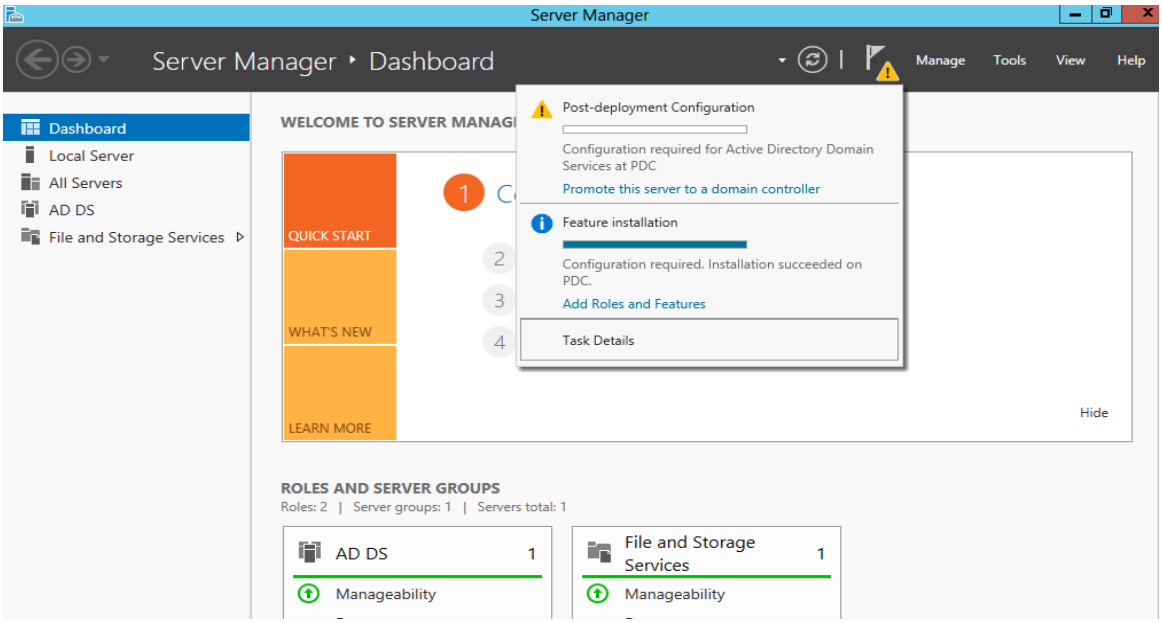
L'assistant installe maintenant Active Directory Domain Services.



Puis le message suivant est affiché :

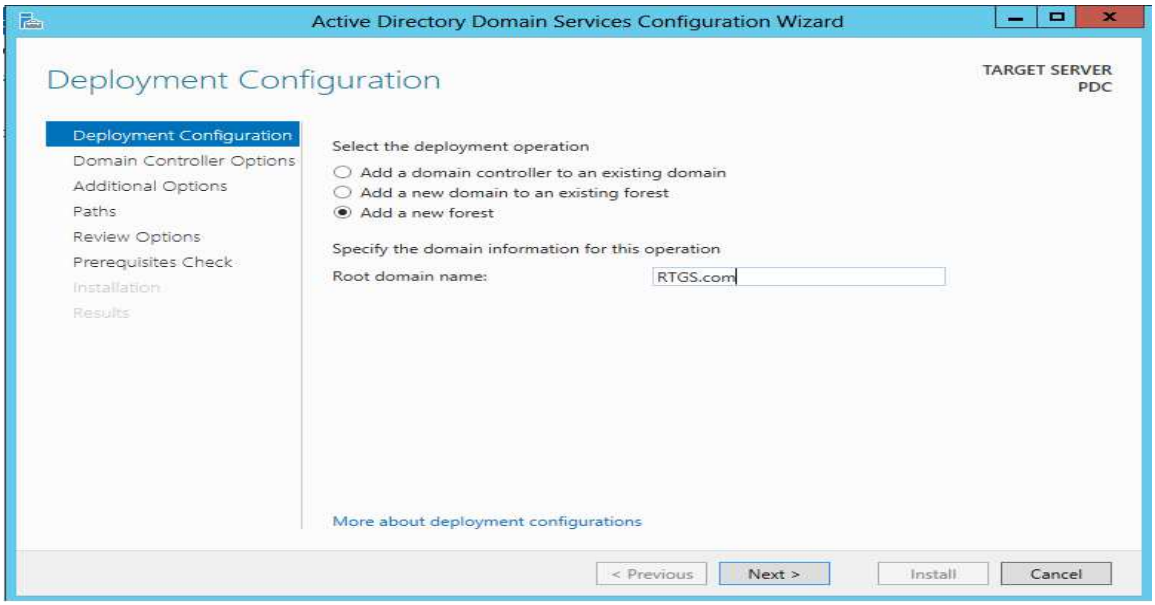
Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.

Cliquez donc sur Promouvoir ce serveur en contrôleur de domaine.

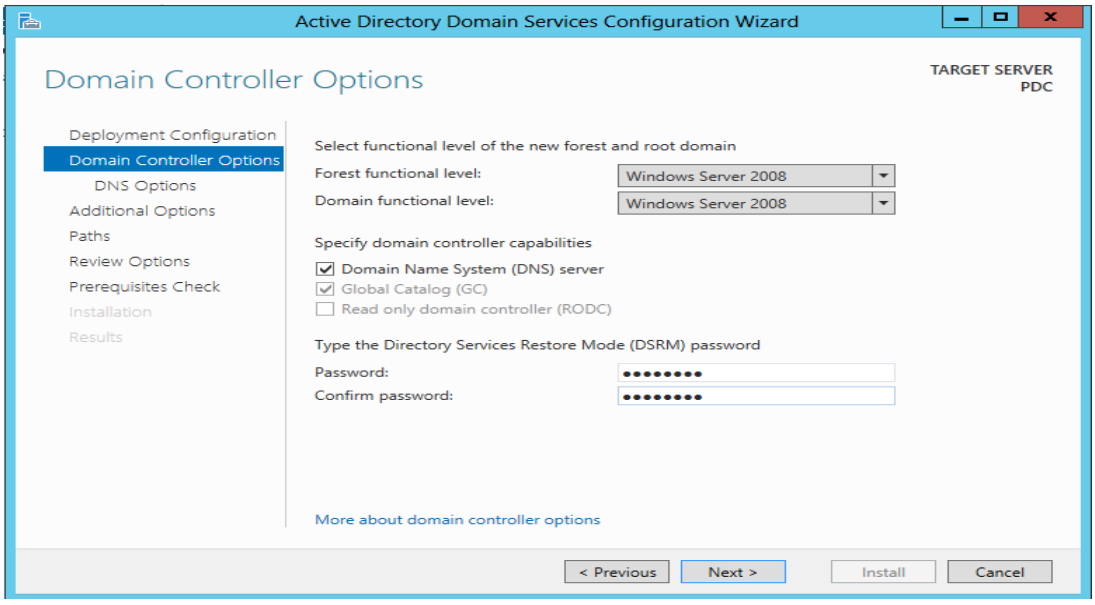


L'assistant de Configuration des services de domaine Active Directory se lance :

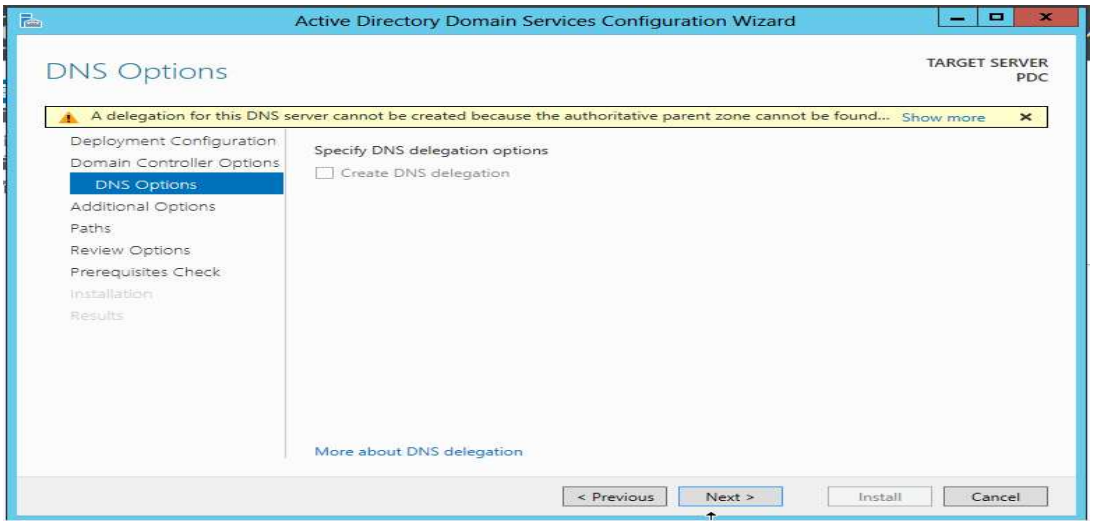
On doit créer une forêt :



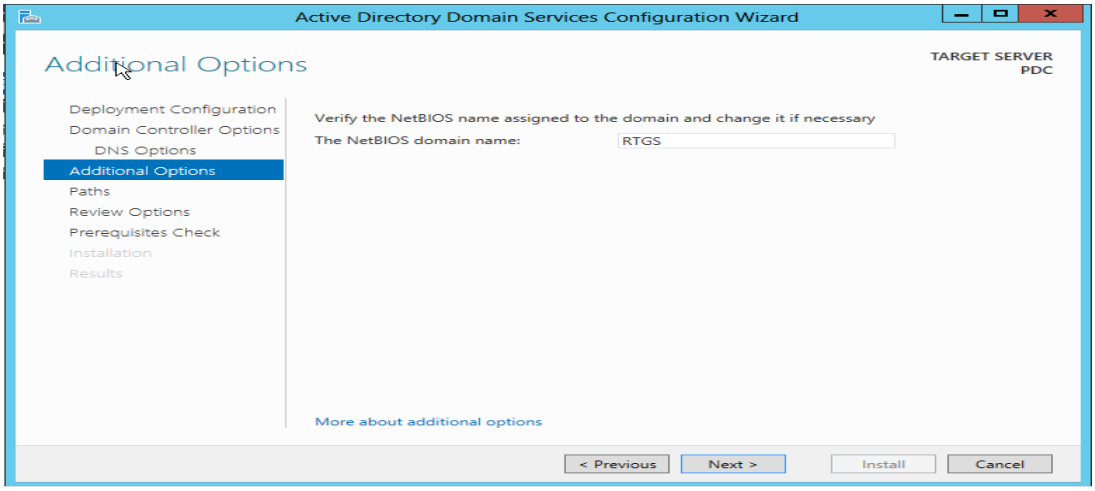
Puis vous définissez le niveau fonctionnel de la forêt et du domaine et définissez le mot de passe de restauration.



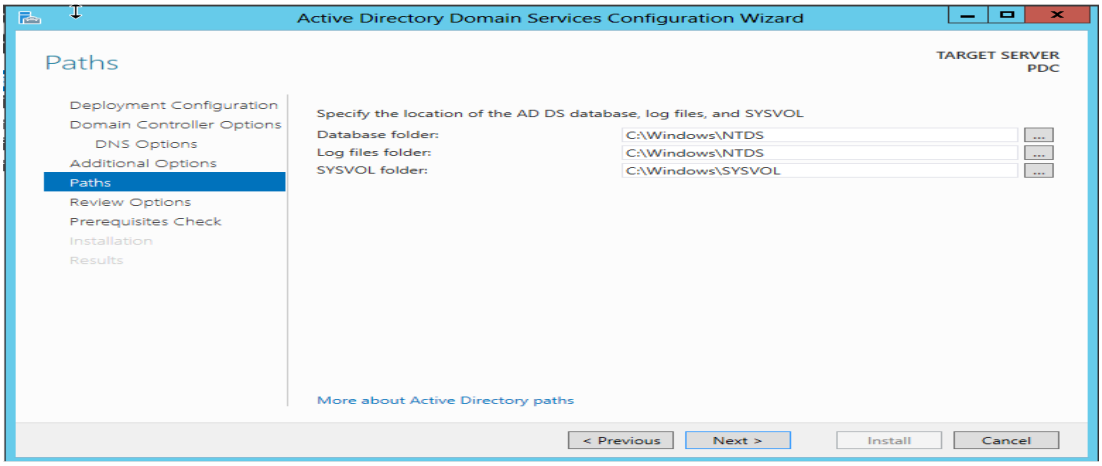
Si vous créez votre premier domaine dans une infrastructure n'ayant pas de DNS, le message d'erreur suivant est normal : la zone de nom de votre domaine sera créée automatiquement par la suite.



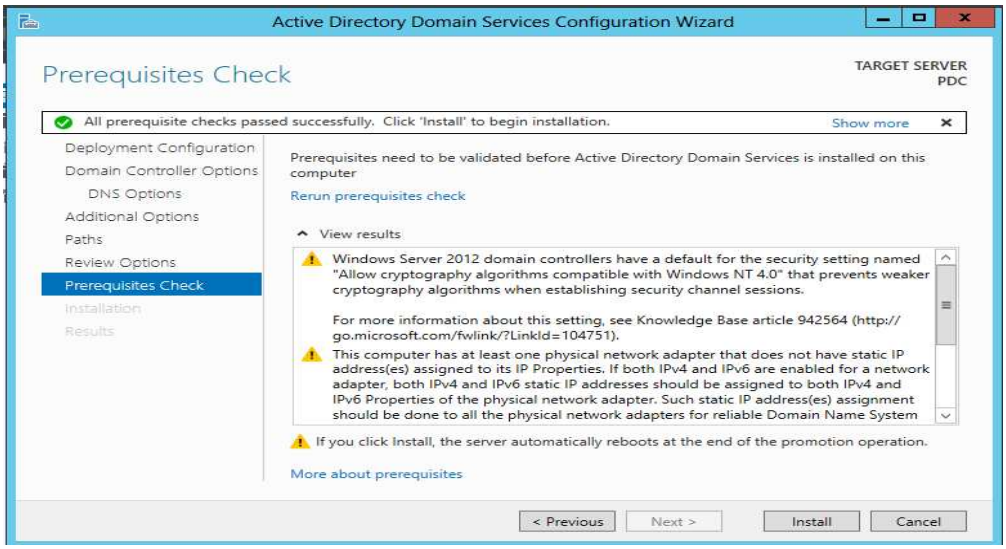
Le nom NetBIOS de votre domaine est ensuite déterminé, vous pouvez éventuellement le changer :



Vous devez ensuite préciser les chemins de stockage de l'AD :



On clique sur suivant après sur installer :



Après configuration le serveur redémarre automatiquement.

A.4. Installation de Forefront TMG 2010

Installation d'un serveur mono-carte (rôle proxy Web ou reverse proxy)

Etape 1 – Installation d'un Windows Server 2008 R2

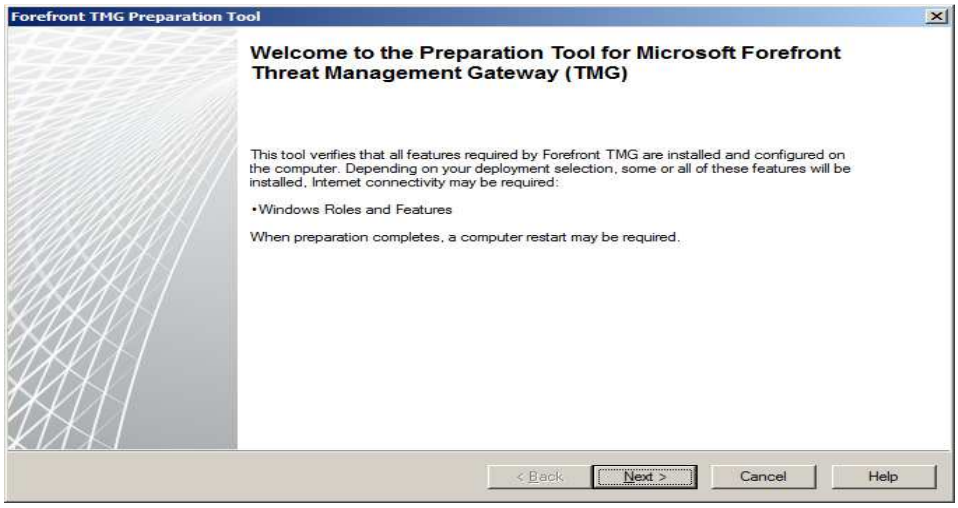
Forefront TMG 2010 ne s'installe que sur Windows Server 2008 édition 64 bit ou Windows Server 2008 R2 qui lui n'est disponible qu'en 64 bit.

Etape 2 – Mise à jour du système via Microsoft Update

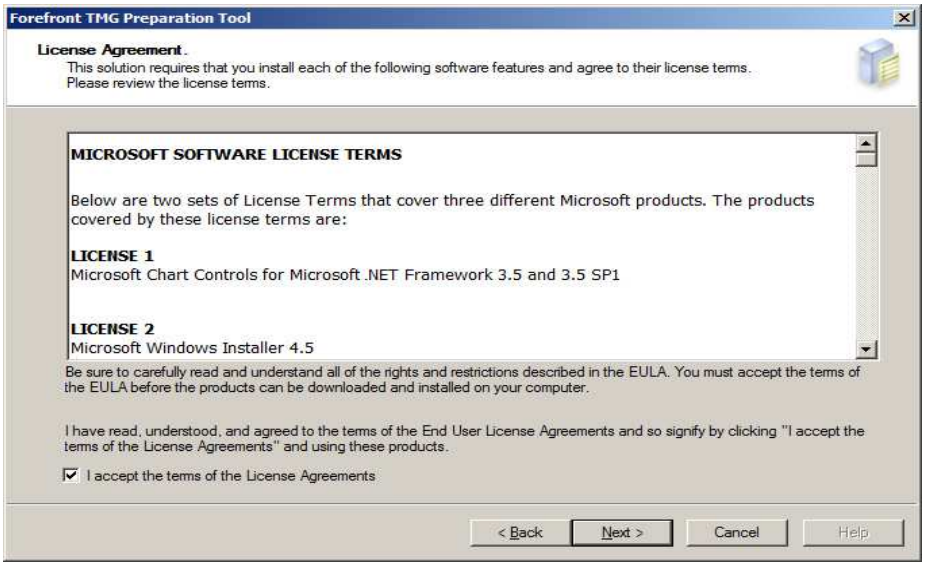
Etape 3 – Préparation à l'installation de Forefront TMG 2010

Figure A.4: Forefront, Threat Management Gateway.

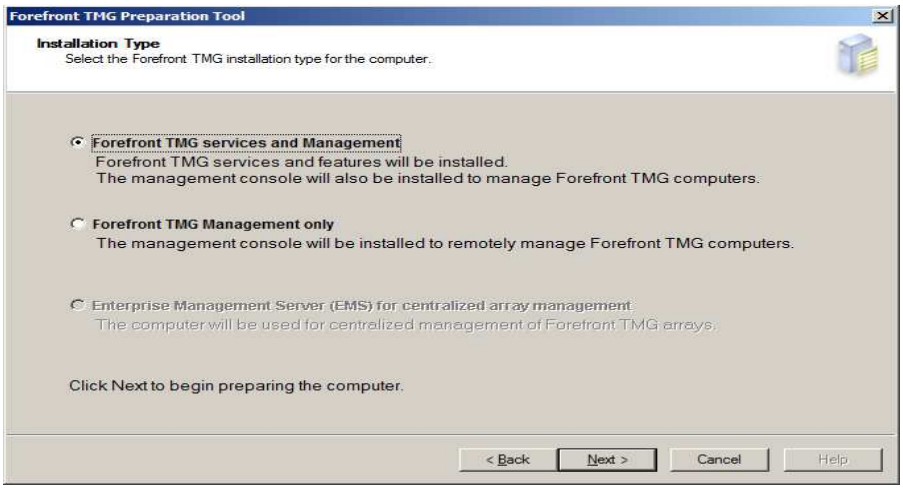
Sélectionner **Run Preparation Tool**



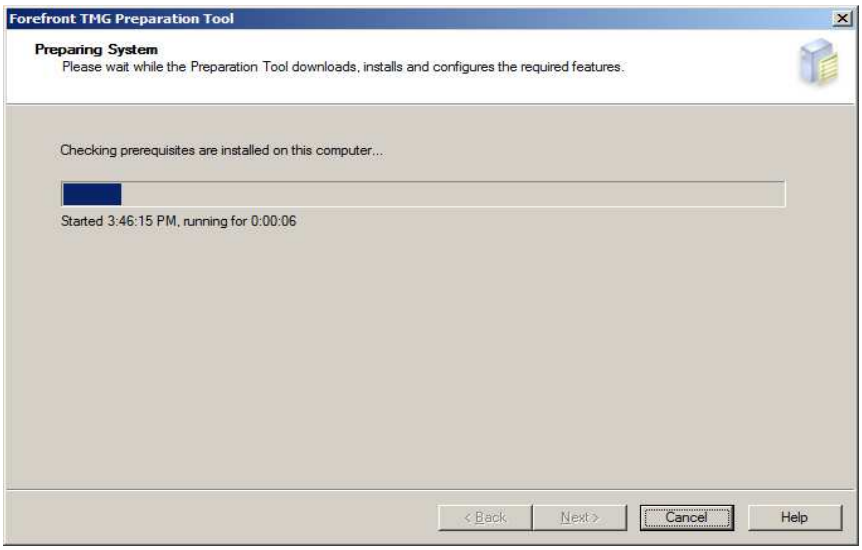
Cliquer sur **Next**

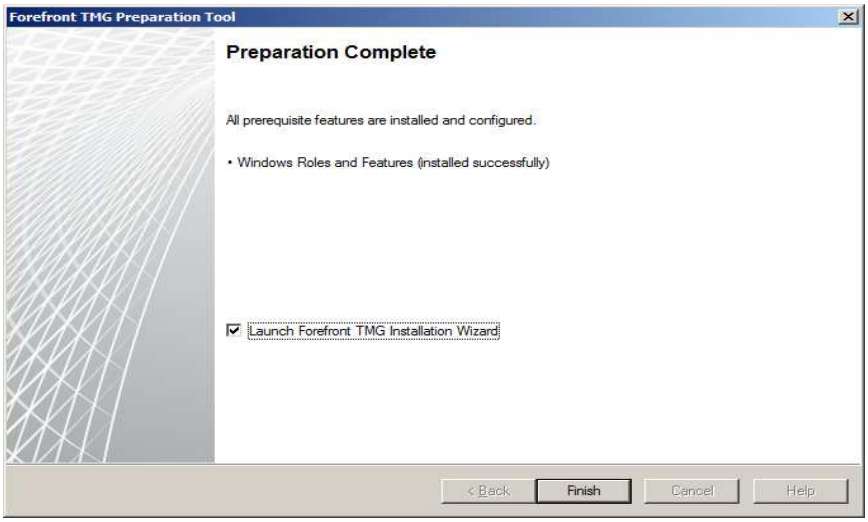


Accepter la licence et cliquer sur **Next**



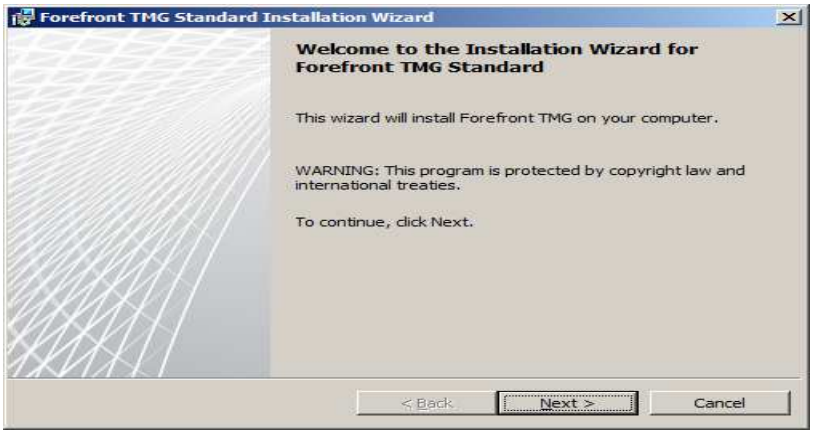
Ici la machine va être le serveur Forefront TMG donc on garde la sélection proposée (si c'était juste un poste d'administration, il faudrait sélectionner la seconde option). Cliquer sur **Next.**





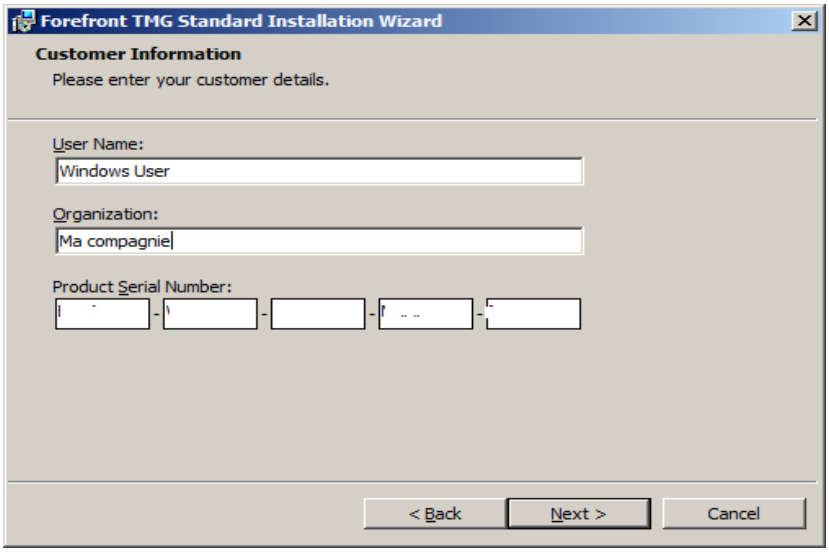
Fin de la préparation. Cliquer sur **Finish** pour démarrer l'installation de Forefront TMG 2010.

Etape 4– Installation de Forefront TMG 2010

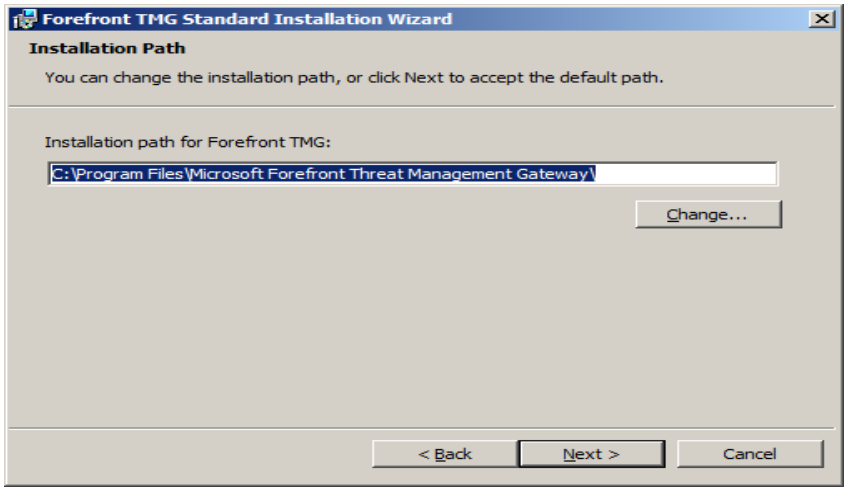


Cliquer sur **Next**

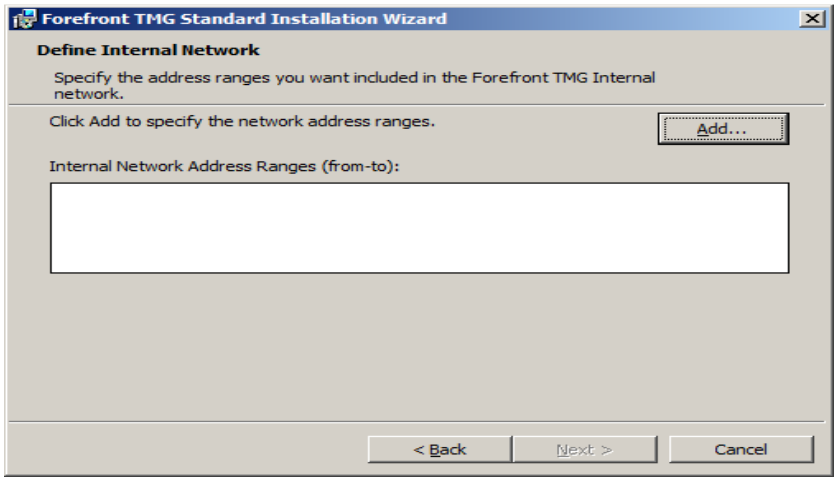
Accepter la licence et cliquer sur **Next**



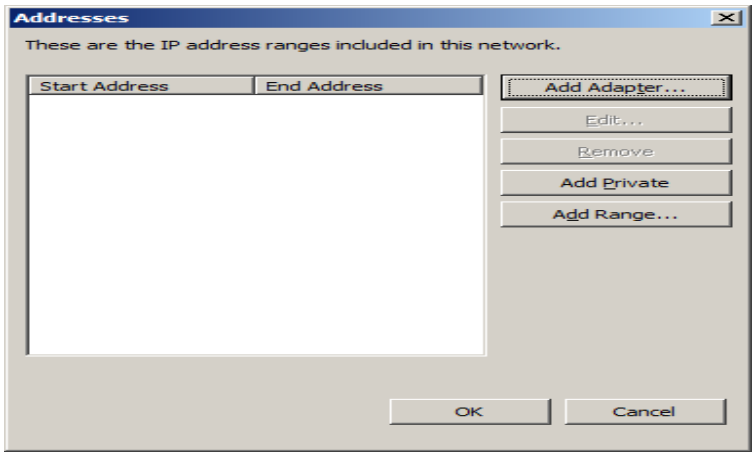
Saisir les informations de licence et cliquer sur **Next**



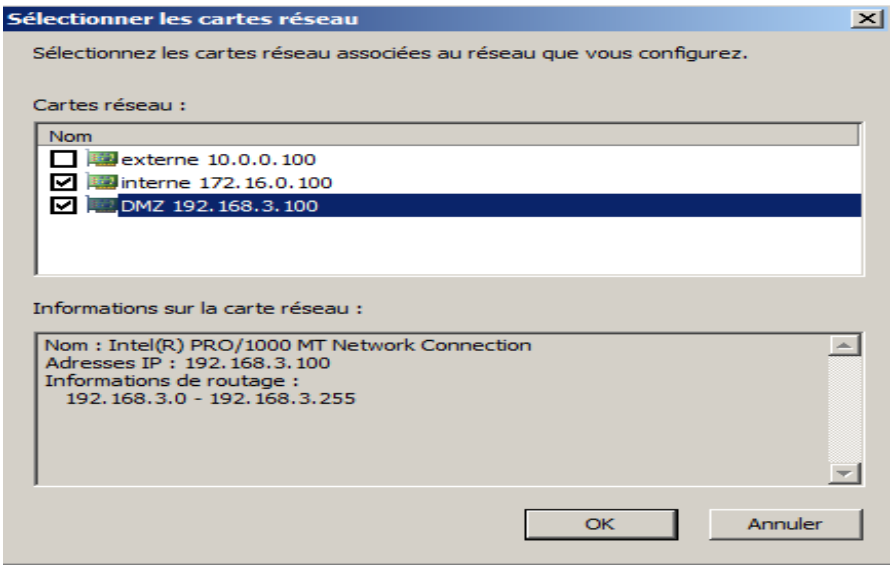
Choisir le chemin d'installation de Forefront TMG 2010. Cliquer sur **Next**

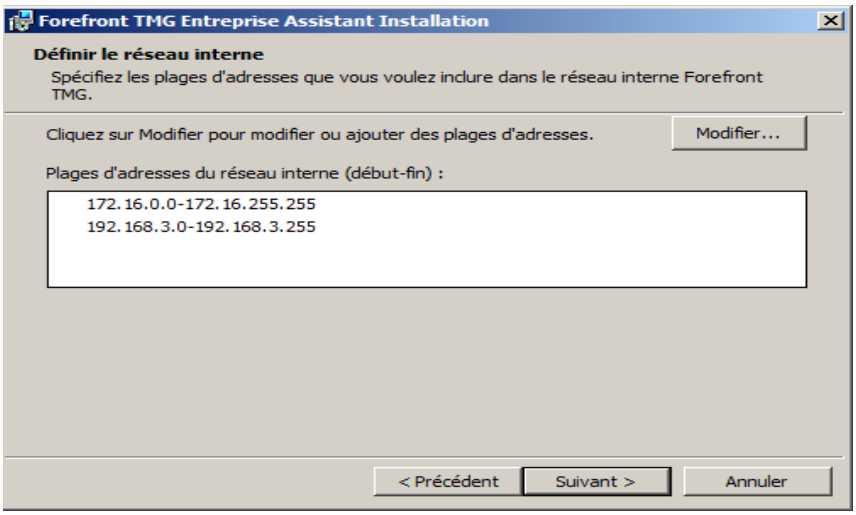


Dans cette étape sont déclarés les réseaux internes qui est inclut au domaine RTGS.dz externe et DMZ (ce qui dans le cas d'une configuration mono-carte est un peu particulier à la différence d'une configuration multi cartes réseau). Cliquer sur **Add.**

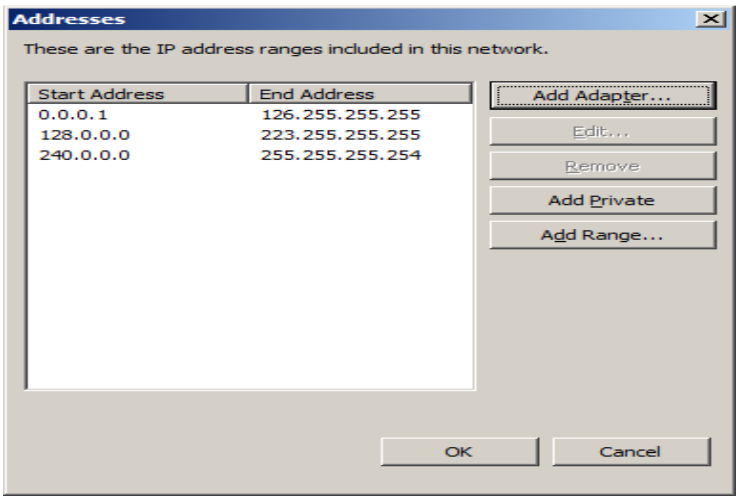


Cliquer sur **Add Adapter et on ajoute les 2 carte réseaux internal et DMZ.**

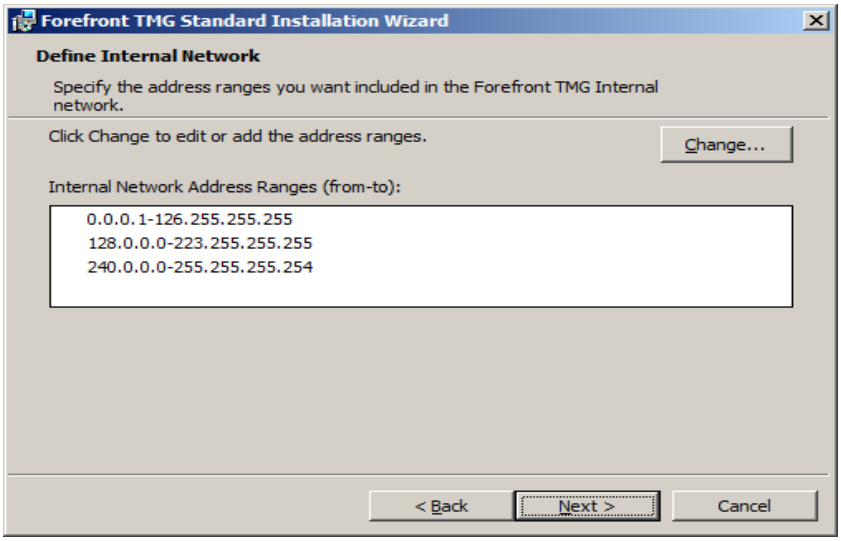




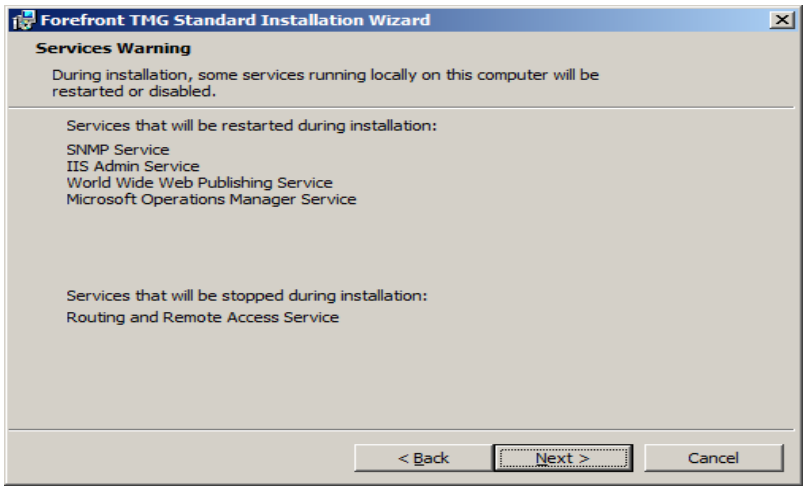
Cliquer sur **OK**



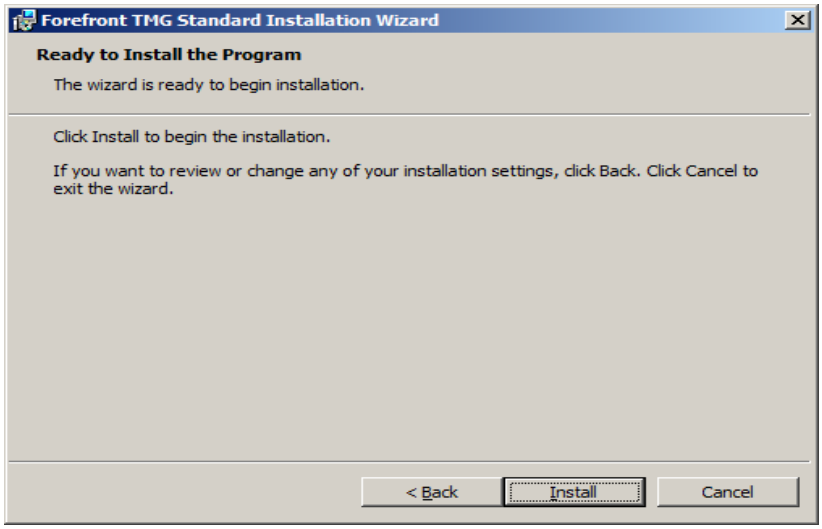
La table des adresses locales a été construite automatiquement. Cliquer sur **OK**.



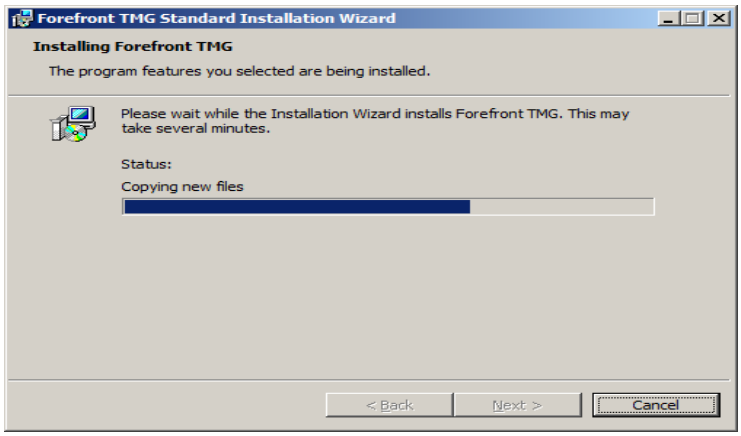
Cliquer sur **Next**

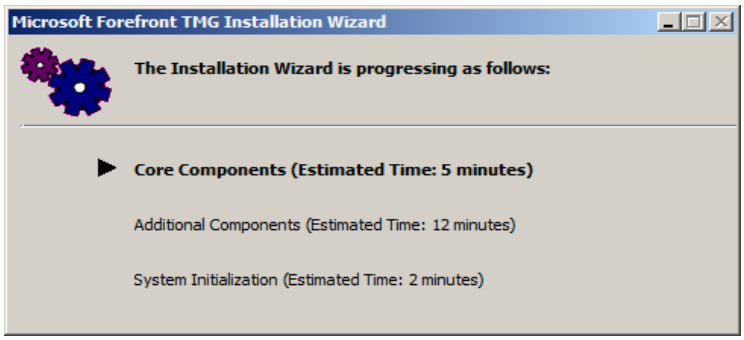


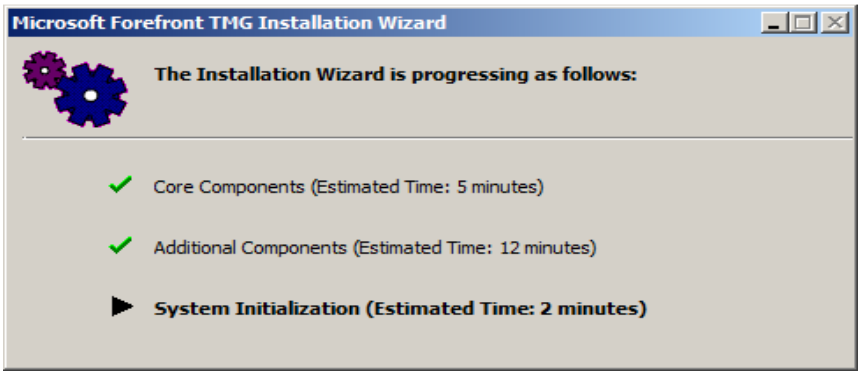
Cliquer sur **Next**



Cliquer sur **Install**. A partir de cet instant,



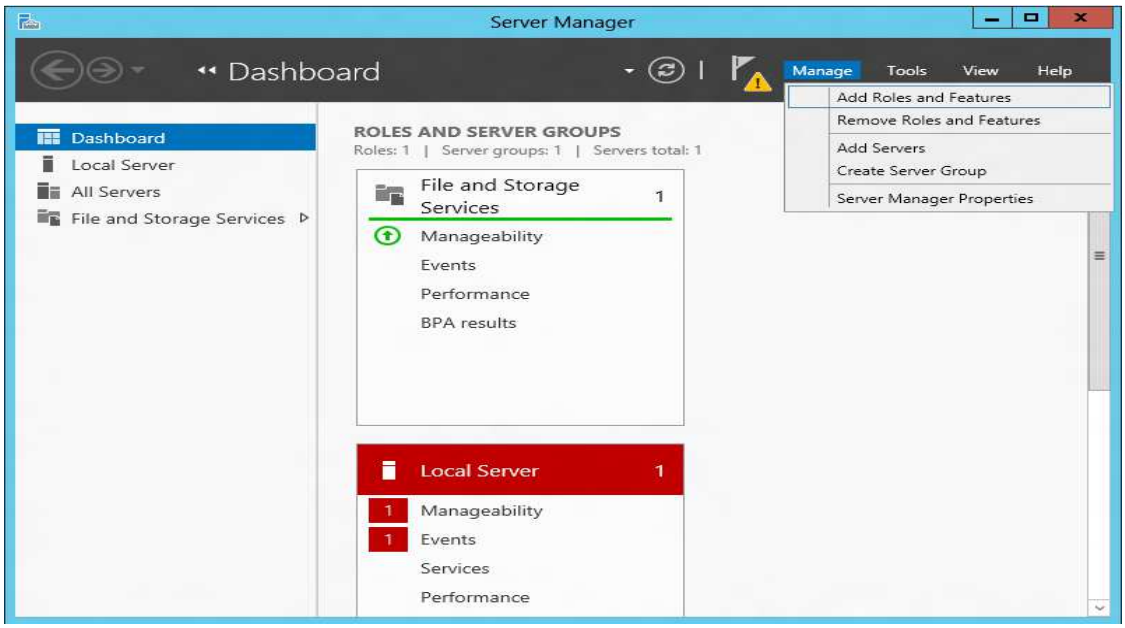

Microsoft Forefront TMG Installation Wizard
The Installation Wizard is progressing as follows:
Core Components (Estimated Time: 5 minutes)
Additional Components (Estimated Time: 12 minutes)
System Initialization (Estimated Time: 2 minutes)


Microsoft Forefront TMG Installation Wizard
The Installation Wizard is progressing as follows:
Core Components (Estimated Time: 5 minutes)
Additional Components (Estimated Time: 12 minutes)
System Initialization (Estimated Time: 2 minutes)

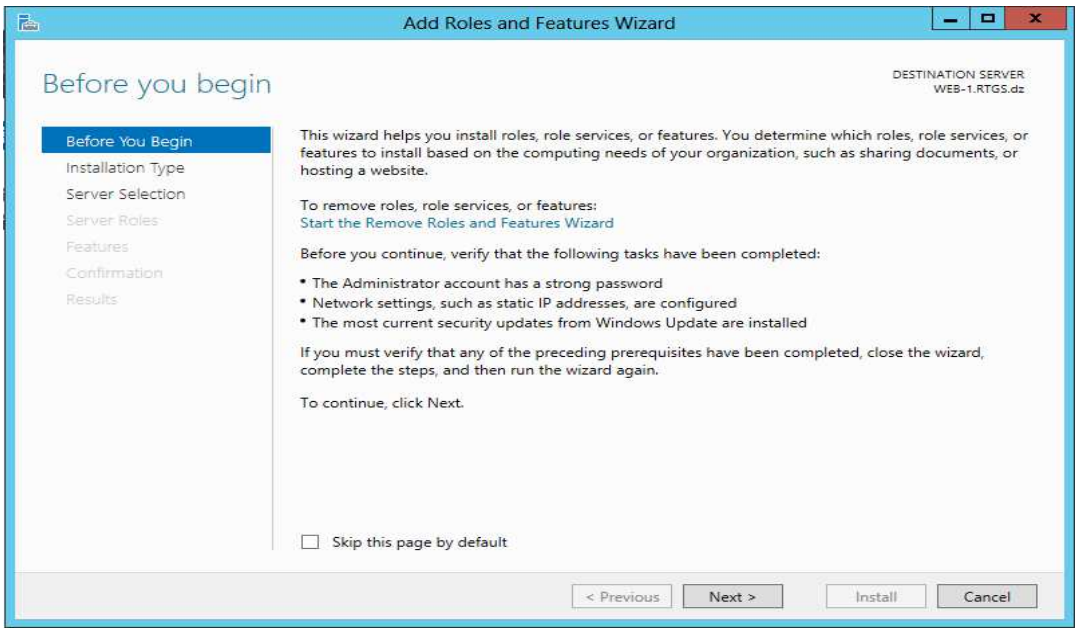

Microsoft Forefront TMG Installation Wizard
Installation Wizard Completed
The Installation Wizard completed successfully.
Launch Forefront TMG Management when the wizard closes
Click Finish to exit the wizard.
Finish

B.1.Installation de serveur Web IIS 8

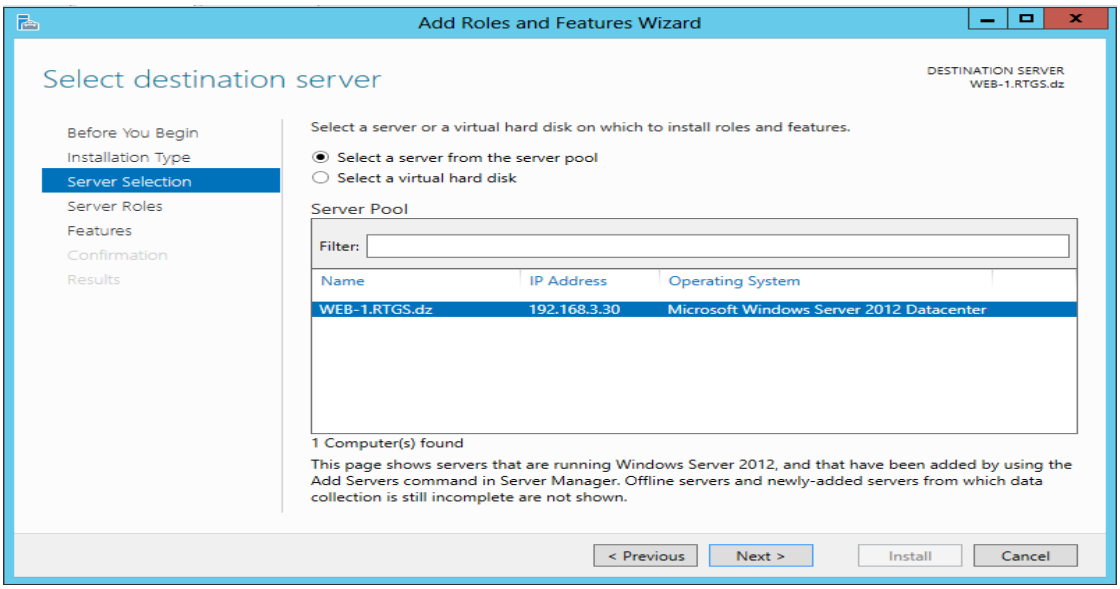
On ouvre **le Gestionnaire de serveur** sous gérer menu, cliquant sur ajoutez des rôles et fonctionnalité



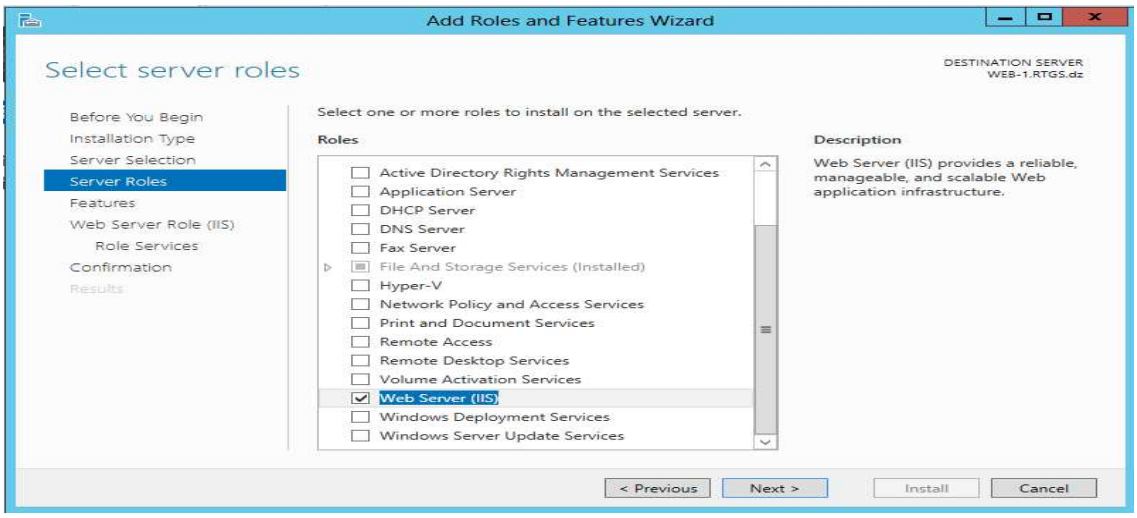
Sélectionnez **basée sur les rôles ou d'installation basée en fonctionnalités** :



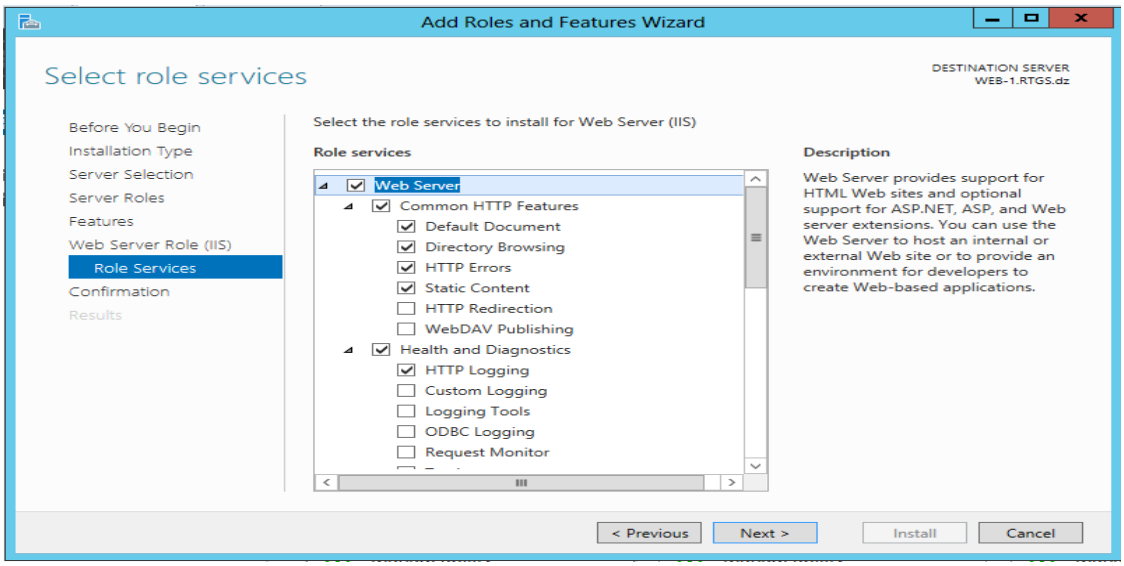
Sélectionnez le serveur approprié (local est sélectionné par défaut), comme indiqué ci-dessous:



Sélectionnez **Serveur Web (IIS):**



Cliquez sur **Suivant** :



Cliquez sur **Installer** et l'installation se lance :

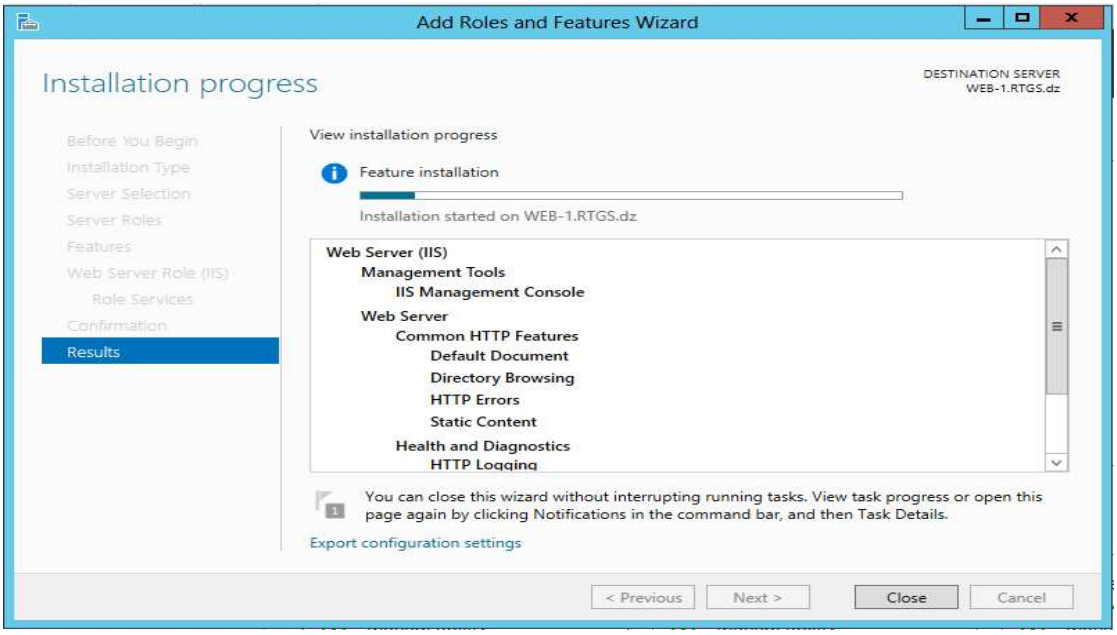
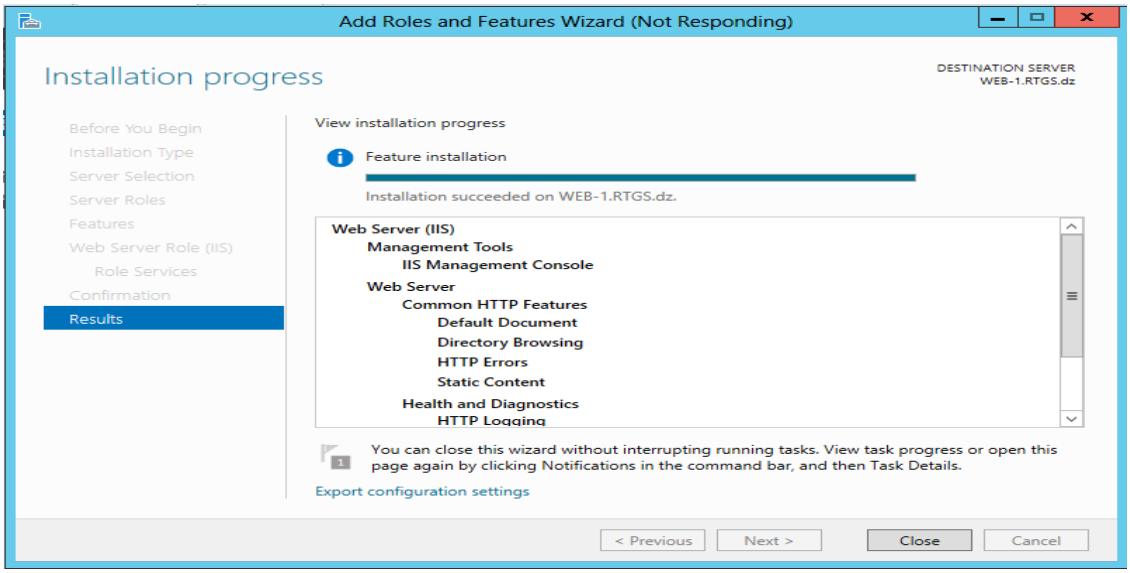


Figure B.1: Installation IIS.

Lorsque l'installation IIS complète, l'assistant reflète l'état de l'installation:



Cliquez sur **Fermer** pour quitter l'assistant.

B.2. Installation et configuration du stockage SAN

B.2.1vérifier la présence des disques dans le gestionnaire de disques

Normalement le gestionnaire de disque doit proposer d'initialiser les nouveaux disques présents dans la machine.

Là aussi, les 3 disques apparaissent dans la branche **physical Disks**

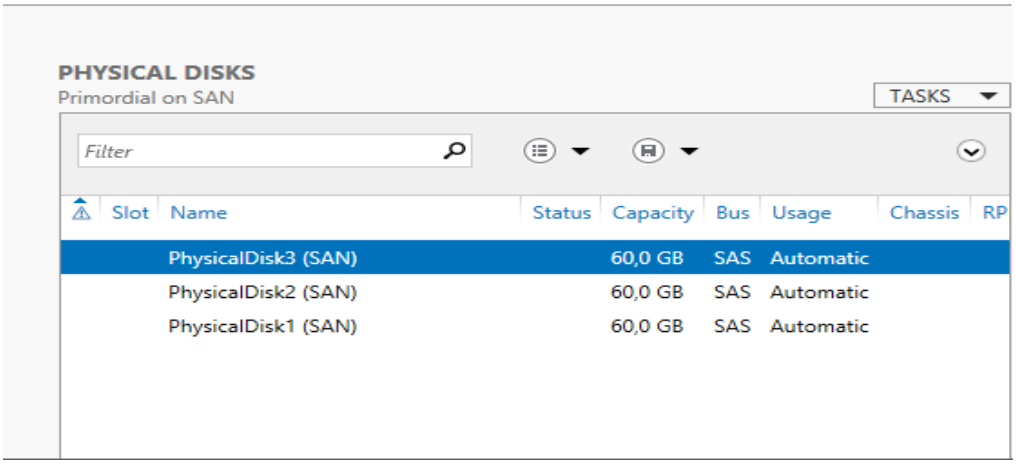
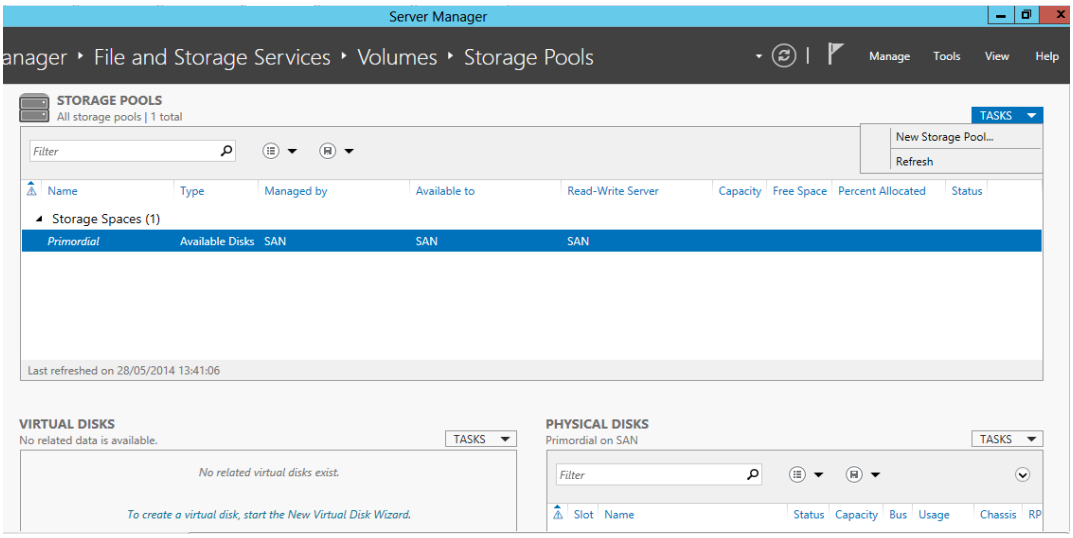


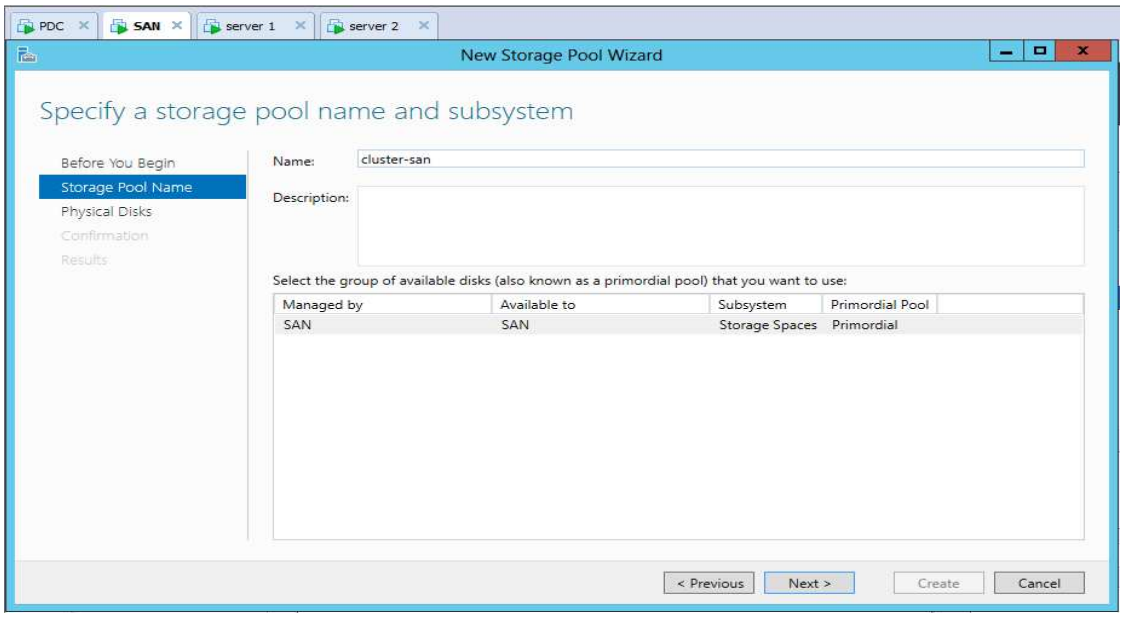
Figure B.2: Disques Physiques.

B.2.2 Création du Storage Pool et d'un disque virtuel

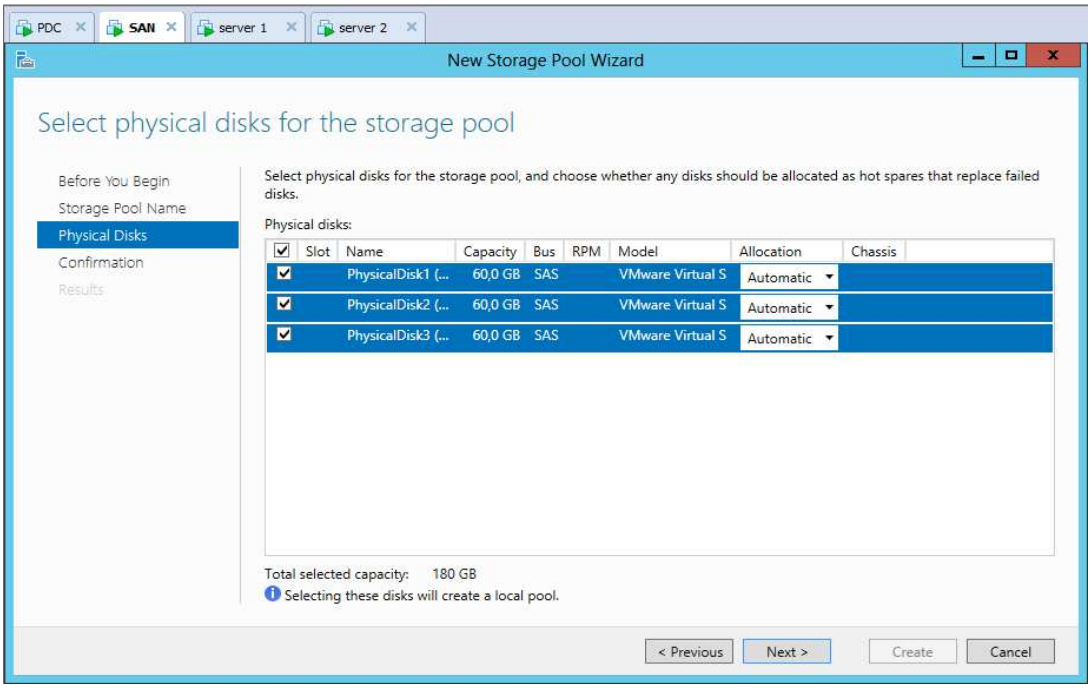
Dans le gestionnaire de serveurs, sélectionner la partie spécifique aux services de fichiers et de stockage.



Nommer le Storage Pool



Sélectionner les disques durs physiques à inclure dans le Storage Pool à créer.



Valider la création du Storage Pool

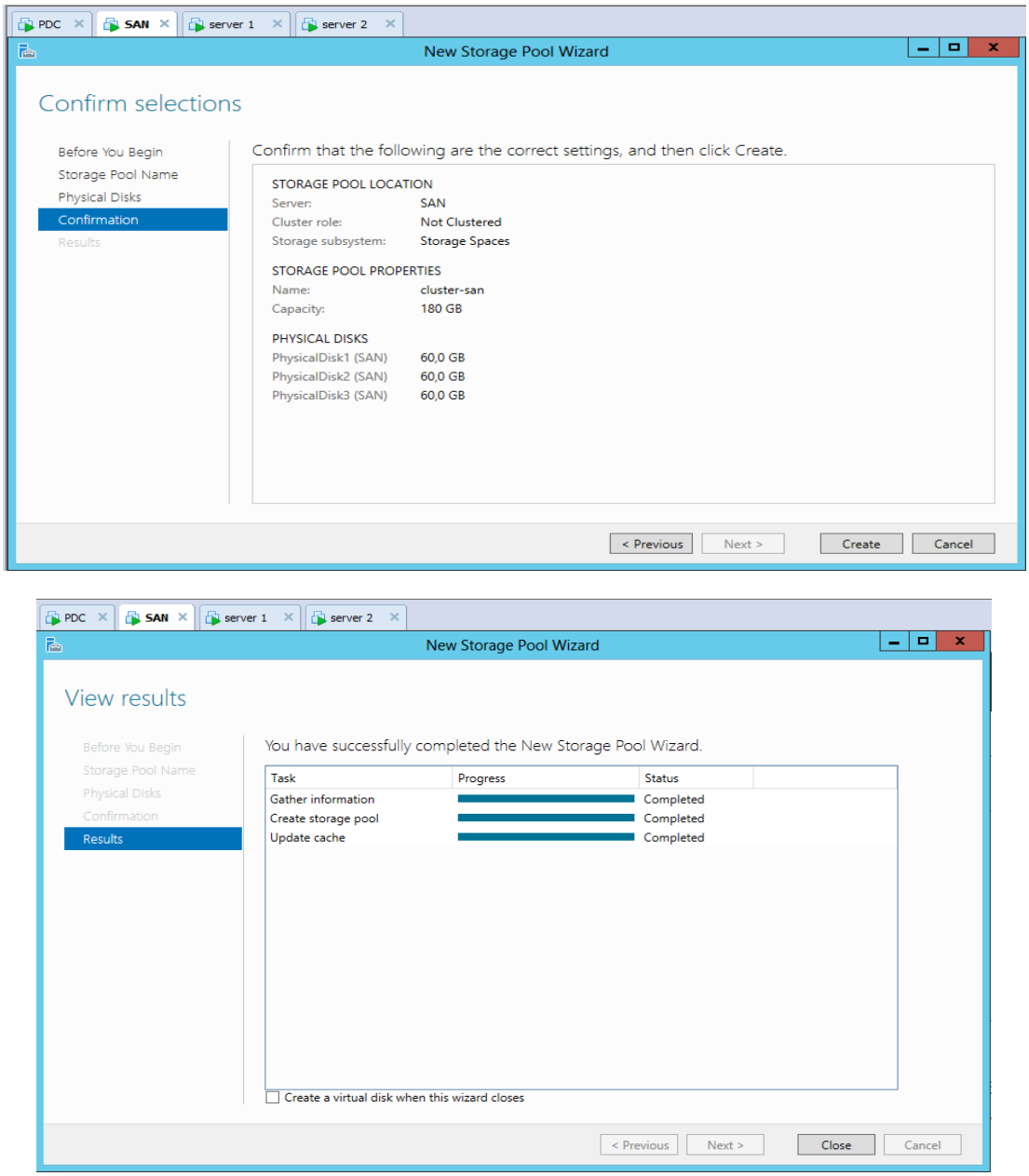
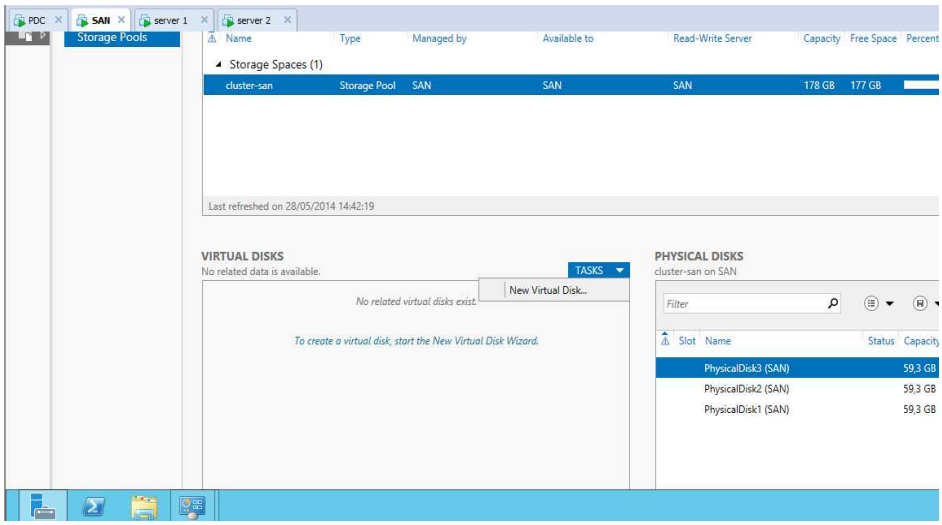
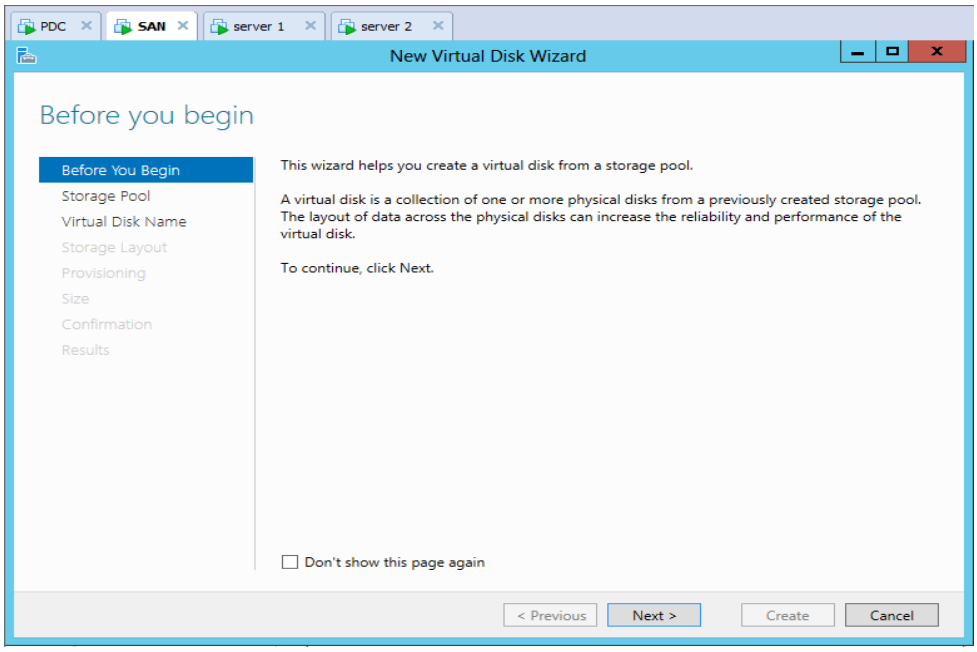


Figure B.3 : Création du Storage Pool.

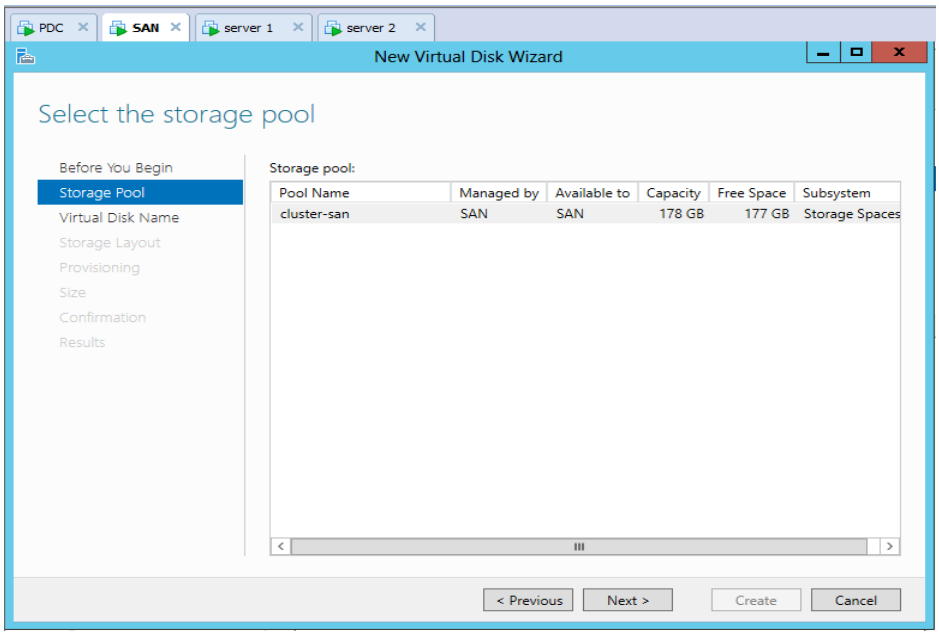
Le Storage Pool est créé et regroupe donc un ensemble de disques physiques. Cet ensemble sera extensible par la suite via ajout de disques physiques.

Sur ce Storage pool, il va falloir ensuite créer un ou plusieurs disques virtuels. Dans notre cas on a crée 2 disques suffira. Ces disques virtuels sont donc un mécanisme d'abstraction des supports physiques lors de la création de partitions/volumes.

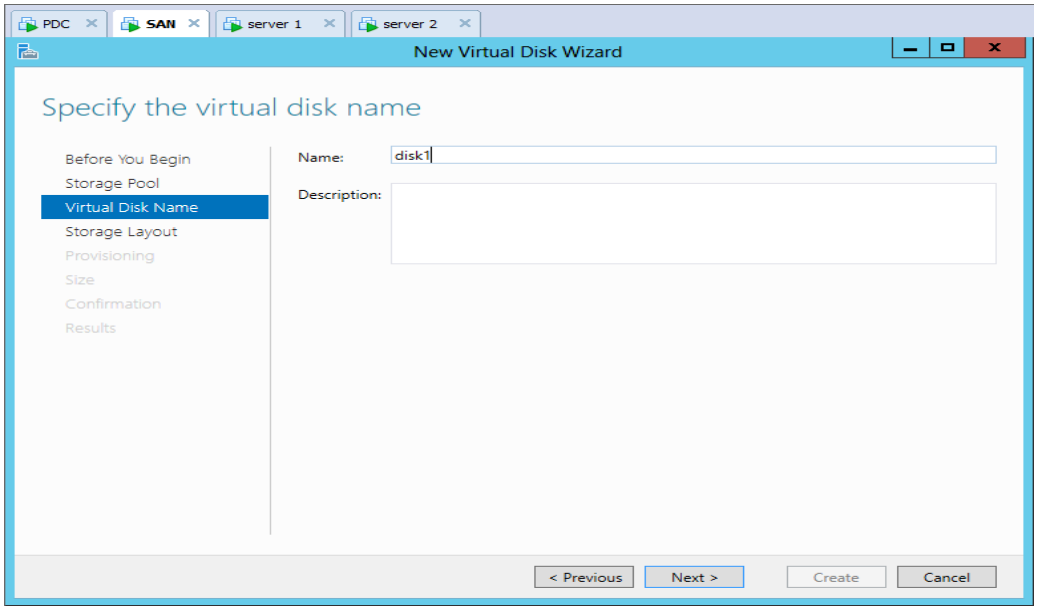




Sélectionner le Storage Pool sur lequel créer le disque virtuel.



Nommer le disque virtuel.

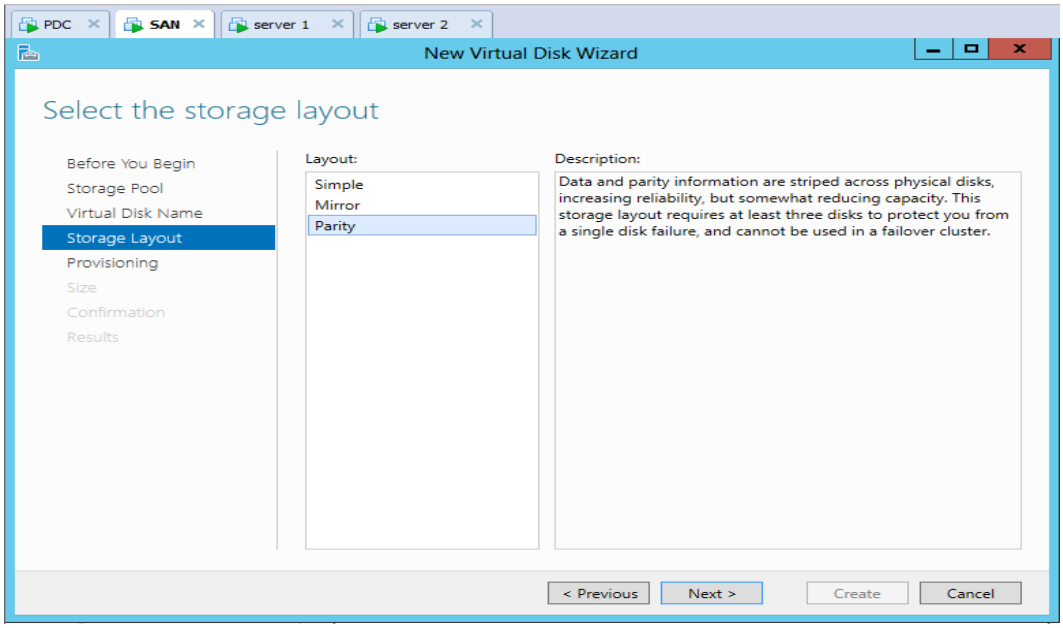


Choisir ensuite la structure de stockage (permettant plus de performances ou plus de sécurité).

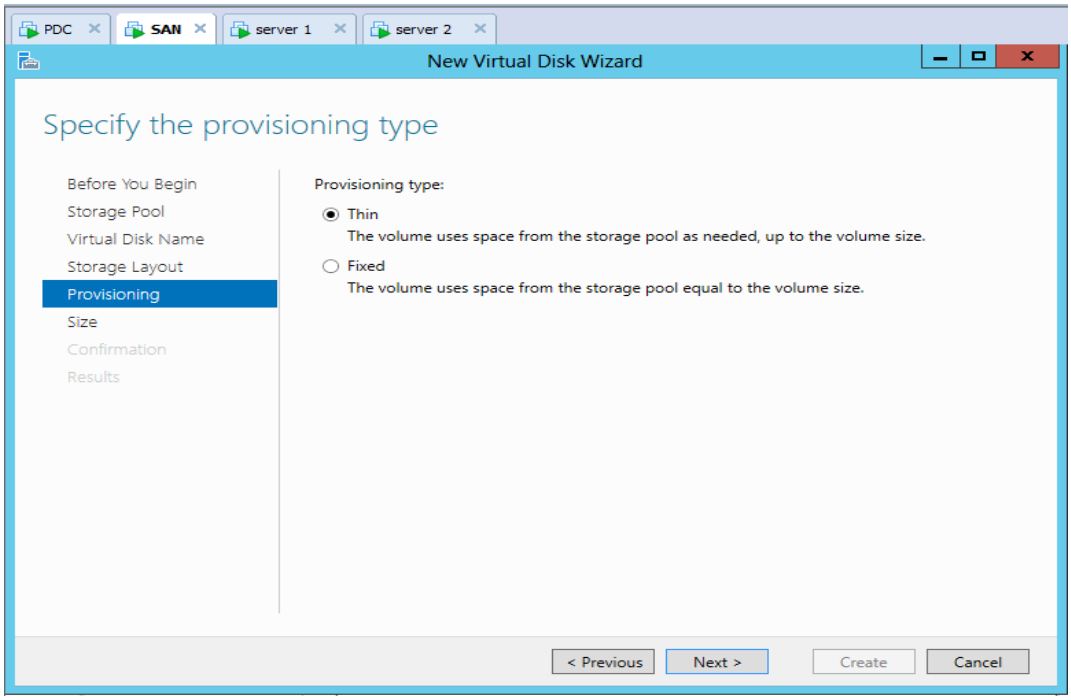
3 modes sont possibles :

- **Simple** : agrégat de disques sans aucun mécanisme de redondance donc très performant mais zéro sécurité
- **Mirror** : avec 3 disques, chaque donnée est répliquée 2 fois sur les autres. Avec 3 disques, garanti la sécurité des données en cas de perte d'un disque. Avec 5 disques garanti la sécurité des données en cas de perte de 2 disques. Nécessite 2 disques mini.
- **Parity** : agrégat avec bande de parité. garanti la sécurité des données en cas de perte d'un disque. Nécessite 3 disques mini.

Dans notre cas, on a pris l'option parité (ce qui correspond à du RAID5)

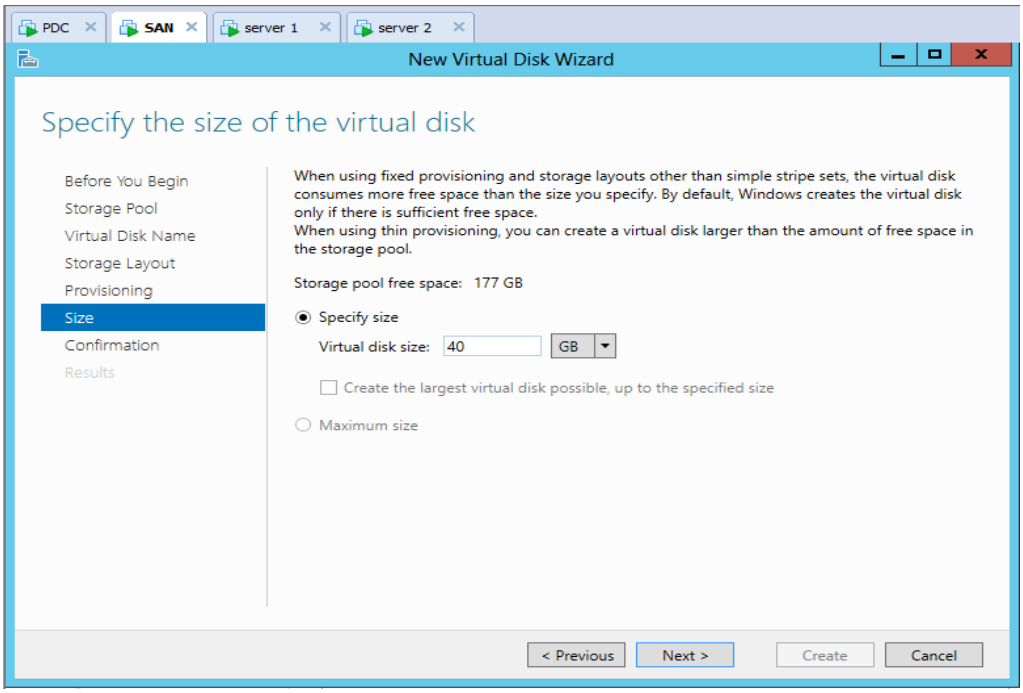


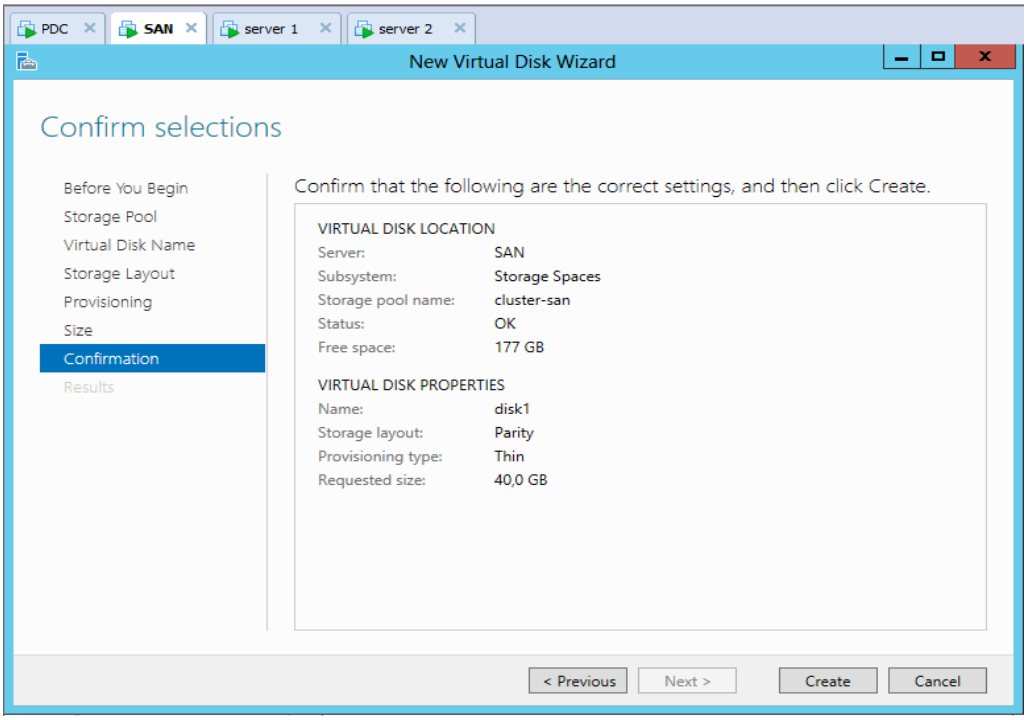
Choisir le type de Provisioning : fin ou de taille fixe.



Ici

Choisir ensuite la taille du disque virtuel. Ici, on a pris l'ensemble de l'espace disponible sur le Storage Pool.


PDC
SAN
server 1
server 2
New Virtual Disk Wizard
Specify the size of the virtual disk
Before You Begin
Storage Pool
Virtual Disk Name
Storage Layout
Provisioning
Size
Confirmation
Results
When using fixed provisioning and storage layouts other than simple stripe sets, the virtual disk consumes more free space than the size you specify. By default, Windows creates the virtual disk only if there is sufficient free space.
When using thin provisioning, you can create a virtual disk larger than the amount of free space in the storage pool.
Storage pool free space: 177 GB
Specify size
Virtual disk size: 40 GB
Create the largest virtual disk possible, up to the specified size
Maximum size
< Previous
Next >
Create
Cancel


PDC
SAN
server 1
server 2
New Virtual Disk Wizard
Confirm selections
Before You Begin
Storage Pool
Virtual Disk Name
Storage Layout
Provisioning
Size
Confirmation
Results
Confirm that the following are the correct settings, and then click Create.
VIRTUAL DISK LOCATION
Server: SAN
Subsystem: Storage Spaces
Storage pool name: cluster-san
Status: OK
Free space: 177 GB
VIRTUAL DISK PROPERTIES
Name: disk1
Storage layout: Parity
Provisioning type: Thin
Requested size: 40,0 GB
< Previous
Next >
Create
Cancel

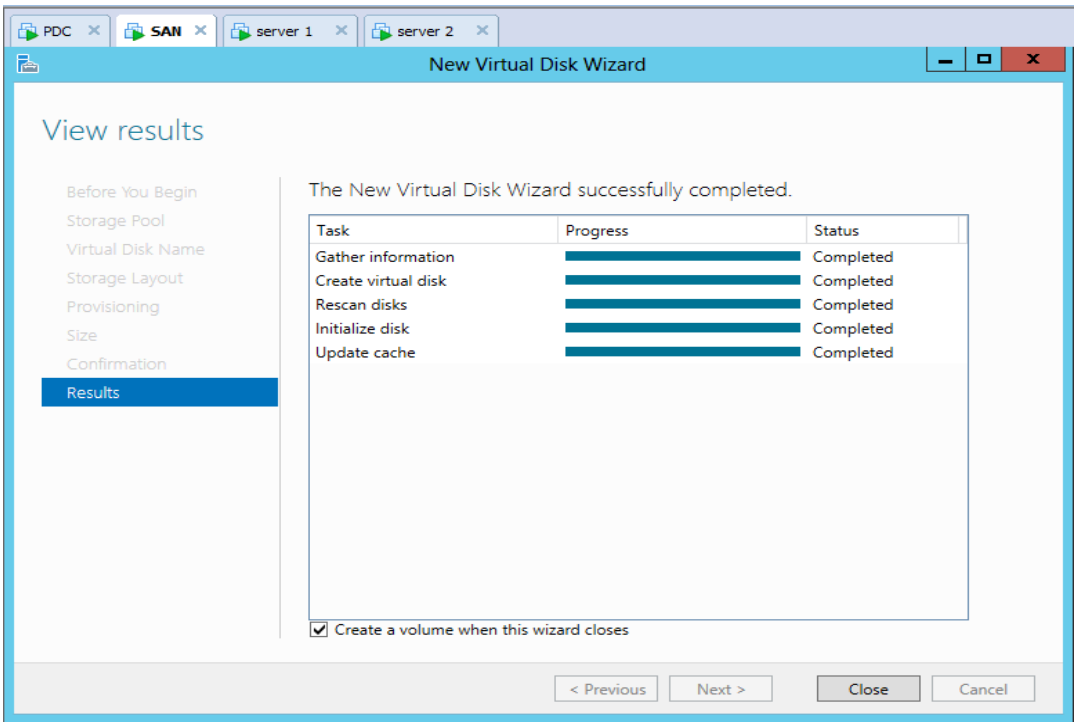
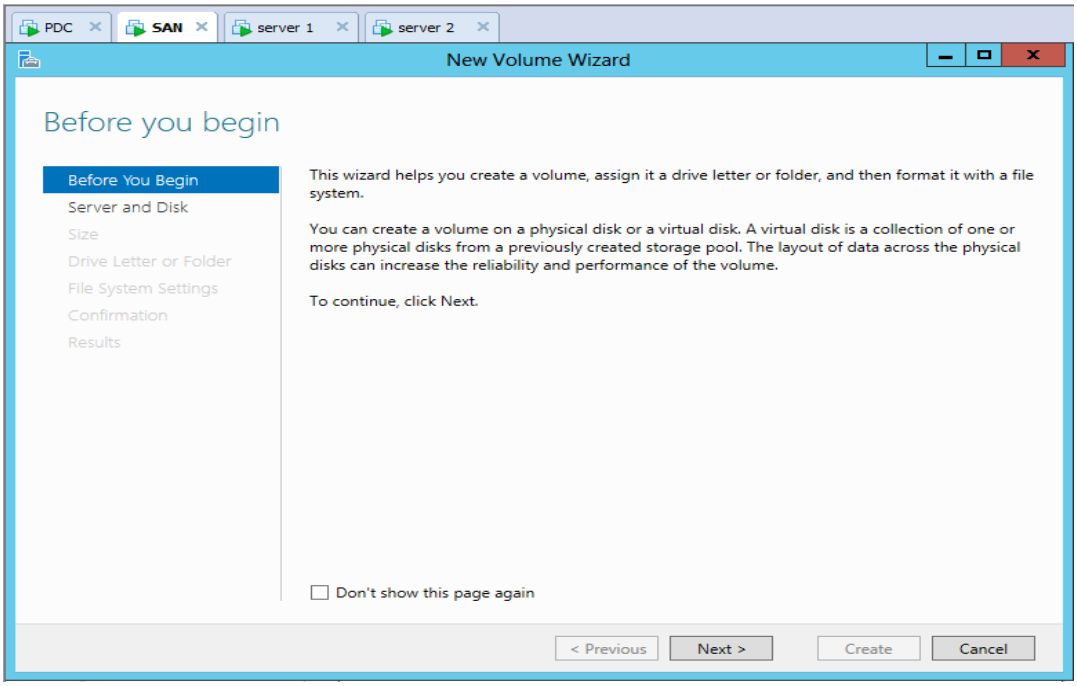


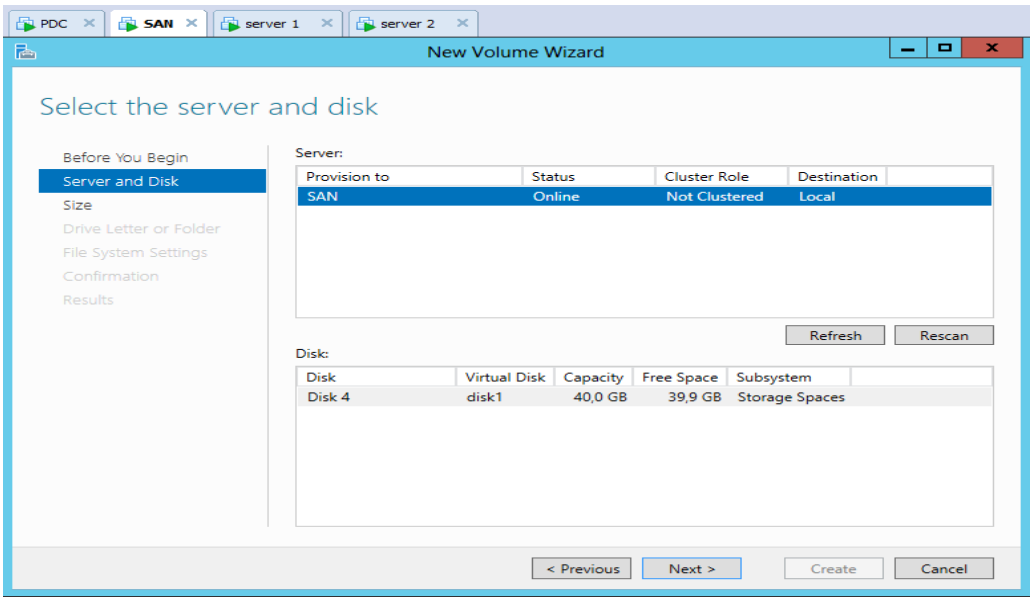
Figure B.4: Création du Nouvel Disque Virtuel.

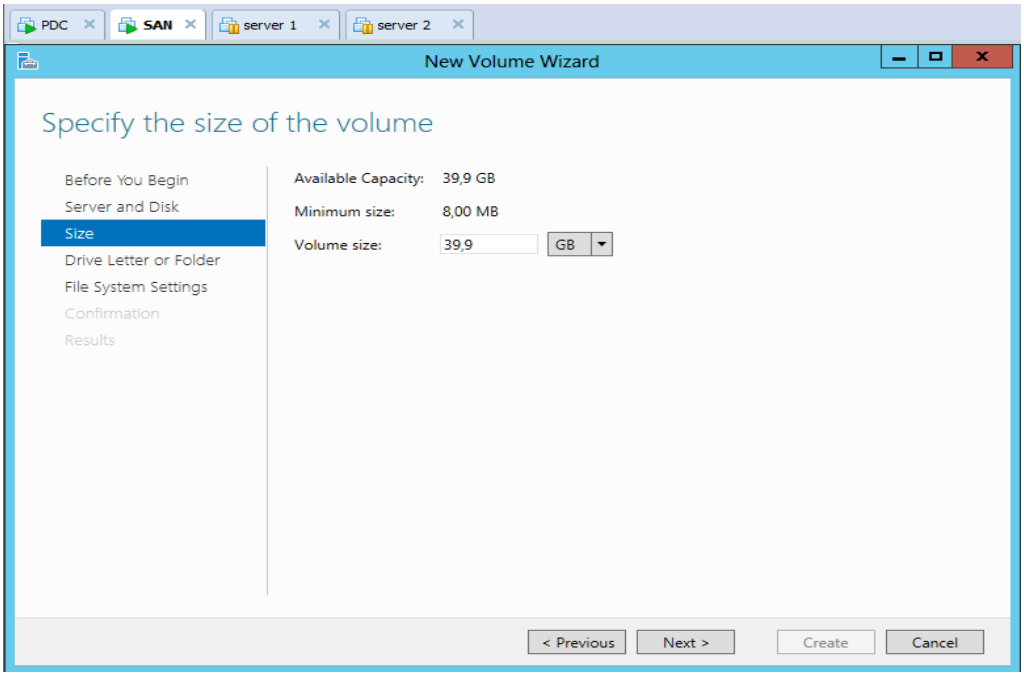
Le disque virtuel est créé. Il ne reste plus qu'à créer des partitions sur ce disque.

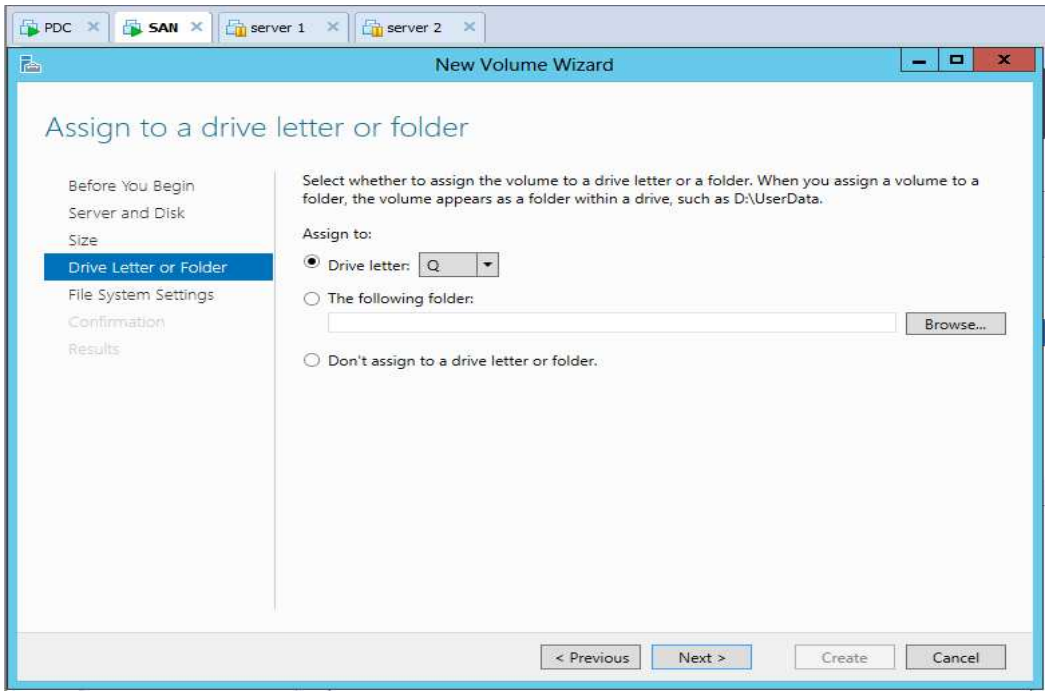
B.2.3. Installation de la fonctionnalité de déduplication de données

On crée des nouveaux volumes, dans notre cas on a crée deux disque Q et S,

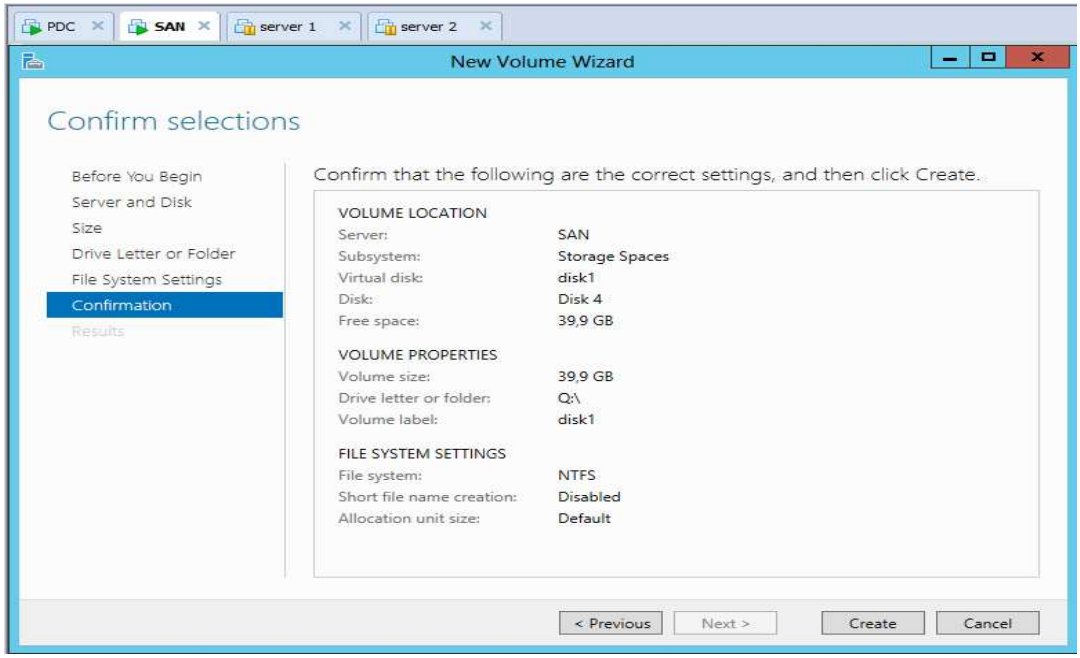



PDC
SAN
server 1
server 2
New Volume Wizard
Select the server and disk
Before You Begin
Server and Disk
Size
Drive Letter or Folder
File System Settings
Confirmation
Results
Server:
Provision to
Status
Cluster Role
Destination
SAN
Online
Not Clustered
Local
Refresh
Rescan
Disk:
Disk
Virtual Disk
Capacity
Free Space
Subsystem
Disk 4
disk1
40,0 GB
39,9 GB
Storage Spaces
< Previous
Next >
Create
Cancel


PDC
SAN
server 1
server 2
New Volume Wizard
Specify the size of the volume
Before You Begin
Server and Disk
Size
Drive Letter or Folder
File System Settings
Confirmation
Results
Available Capacity:
39,9 GB
Minimum size:
8,00 MB
Volume size:
39,9
GB
< Previous
Next >
Create
Cancel



Valider la création de volume



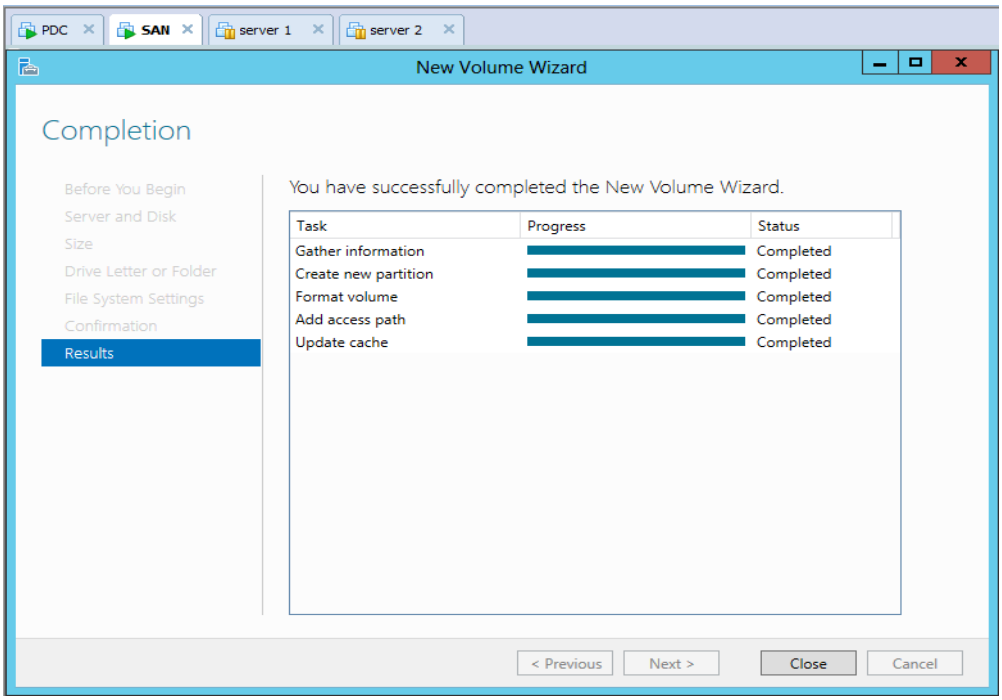


Figure B.5: Création des nouveaux volumes.

Installation de l'autorité de certification sur Windows Server 2012

C.1. Construire une autorité de certification racine autonome

C'est la première AD CS rôle pour être installé dans une PKI d'entreprise. Il s'agit d'une ancre de confiance et établit la racine d'une hiérarchie de confiance. Pour sécuriser la racine CA, une pratique courante est de le garder hors de minimiser l'exposition. Et mettre en ligne que lors de la délivrance d'un certificat d'autorité de certification secondaire. Le processus consiste simplement à ajouter et configurer AD CS rôle de l'autorité de certification (CA) sur un serveur non-joint au domaine.

Sur le serveur CA, cliquez sur Ajouter des rôles et des fonctions ... puis sur Suivant. Et Choisissez: Certification Authority.

Choisissez: autorité de certification d'inscription Web

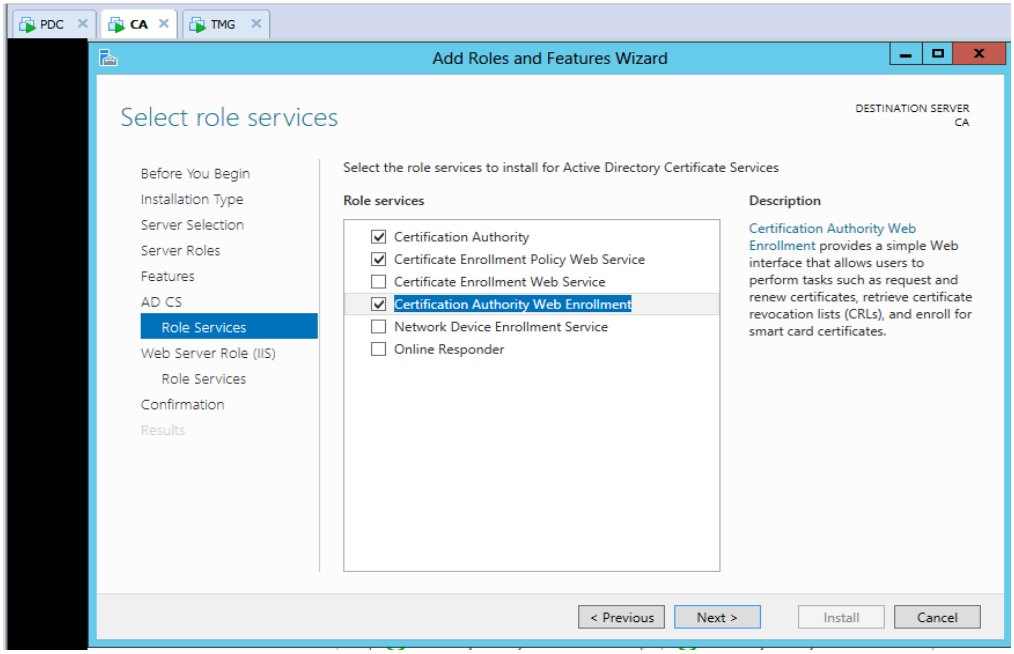
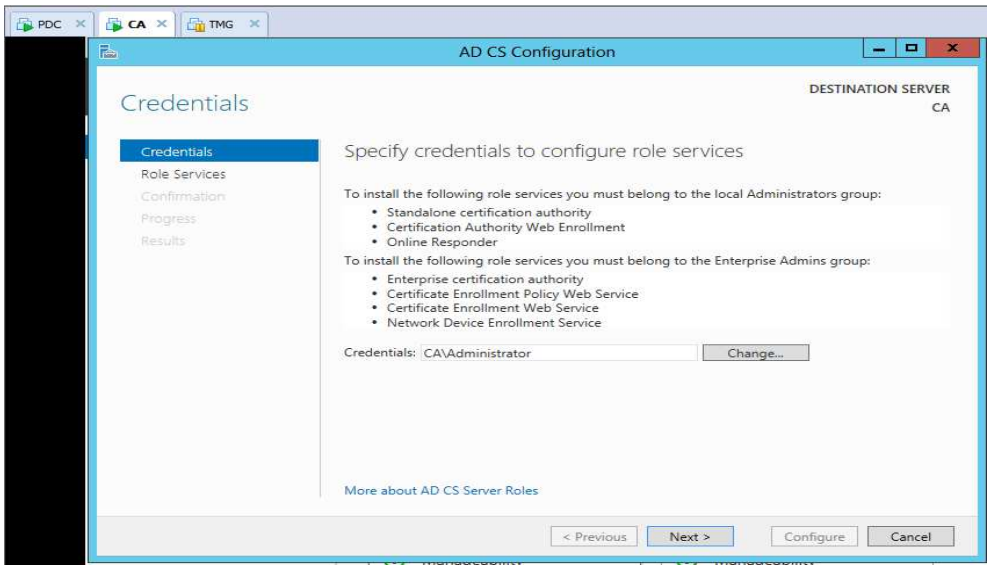
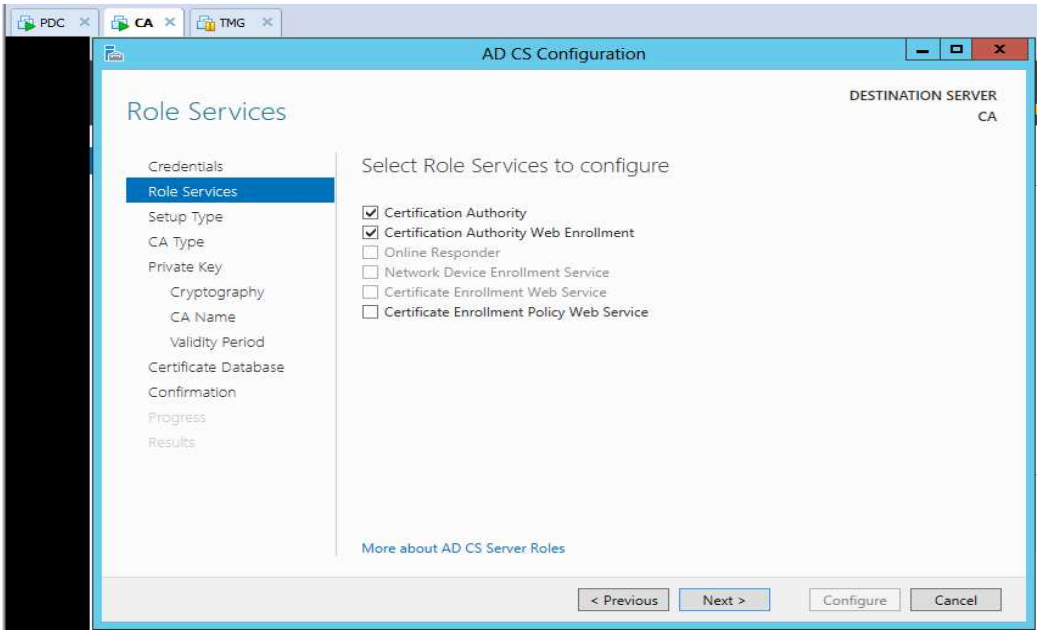


Figure C.1: Installation d'autorité de certification sur Windows 2012.

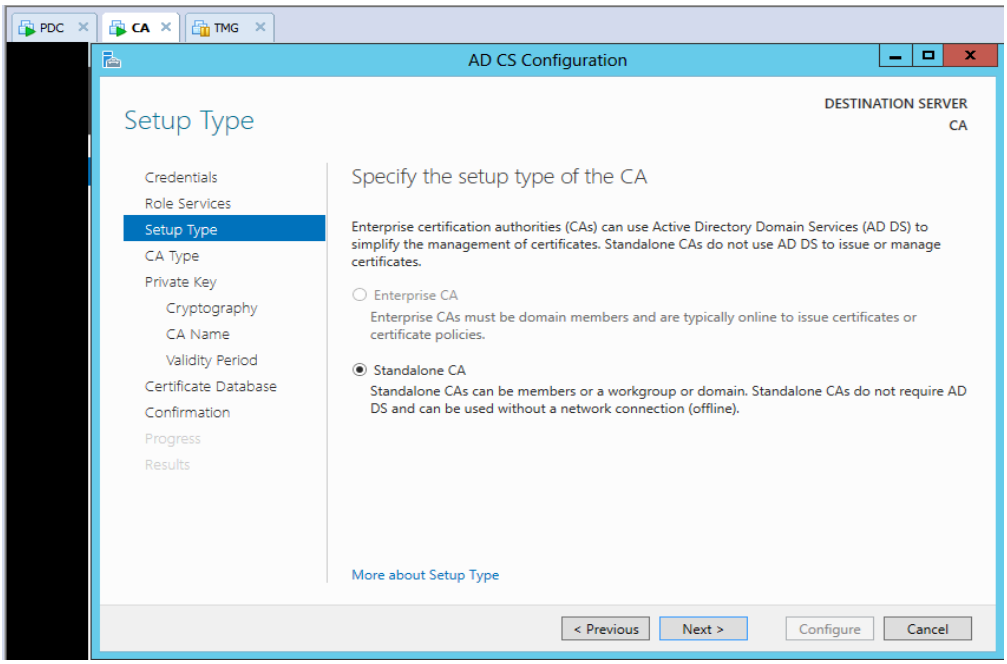
Cliquez sur Suivant



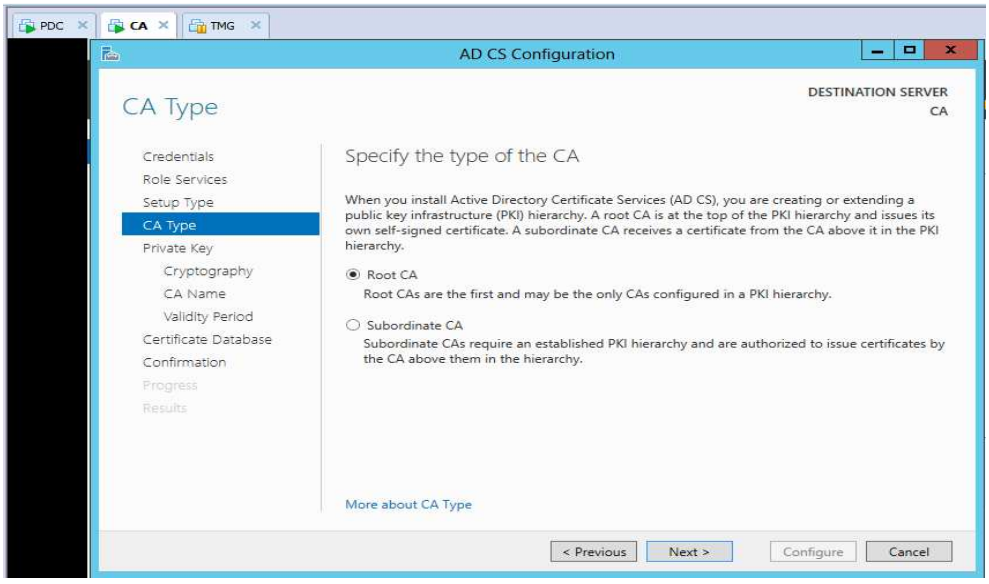
Choisir Autorité de certification & Autorité de certification d'inscription Web



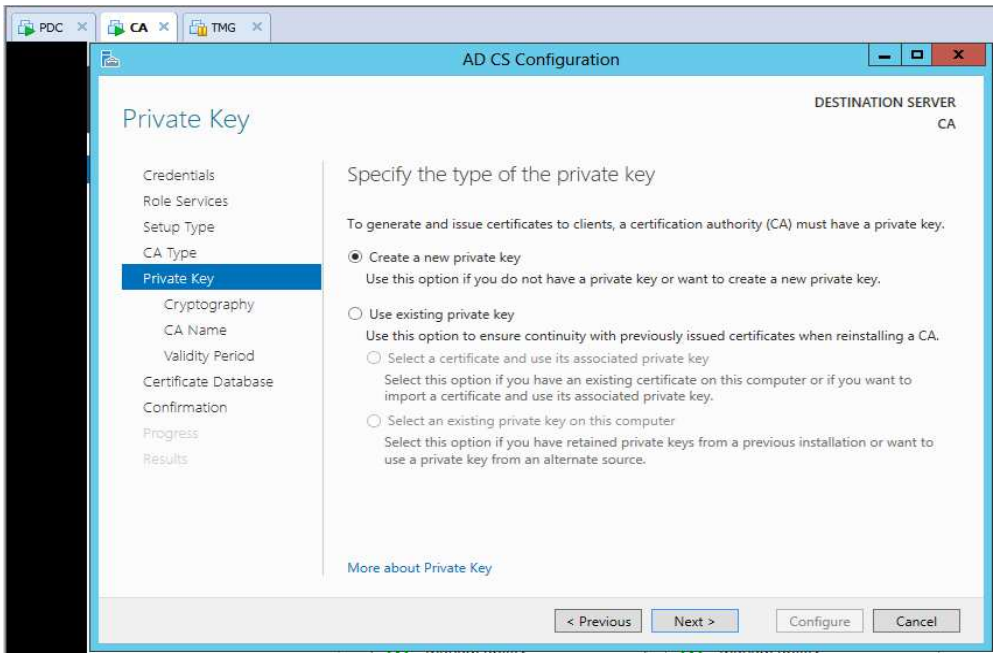
Choisissez standalone CA



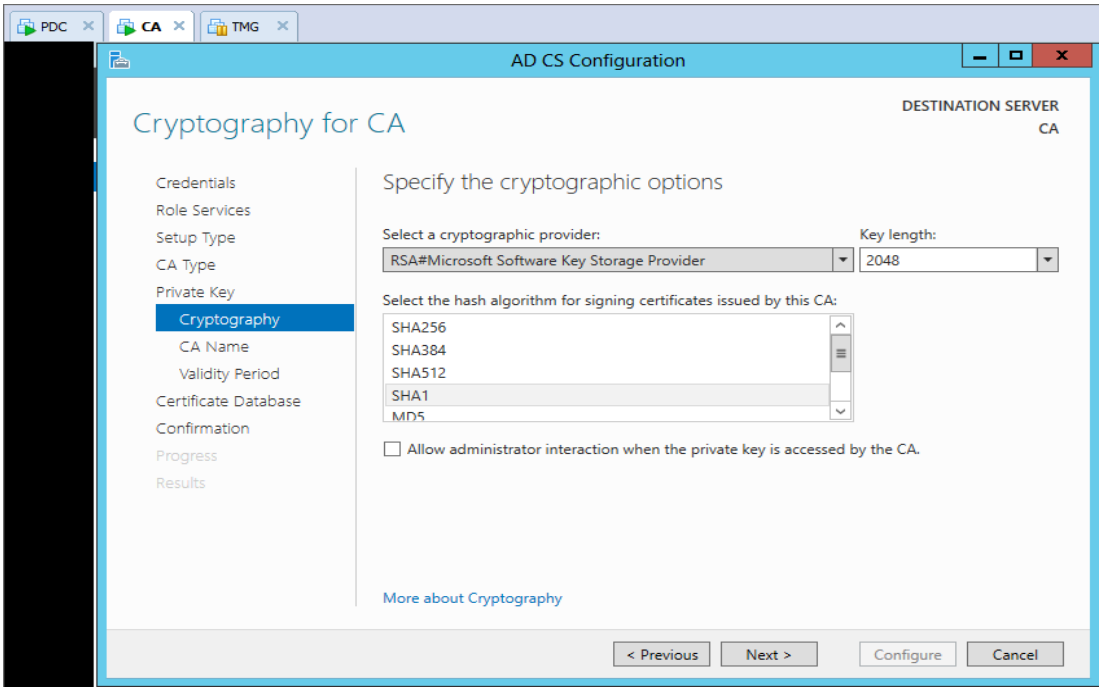
Choisissez Root CA



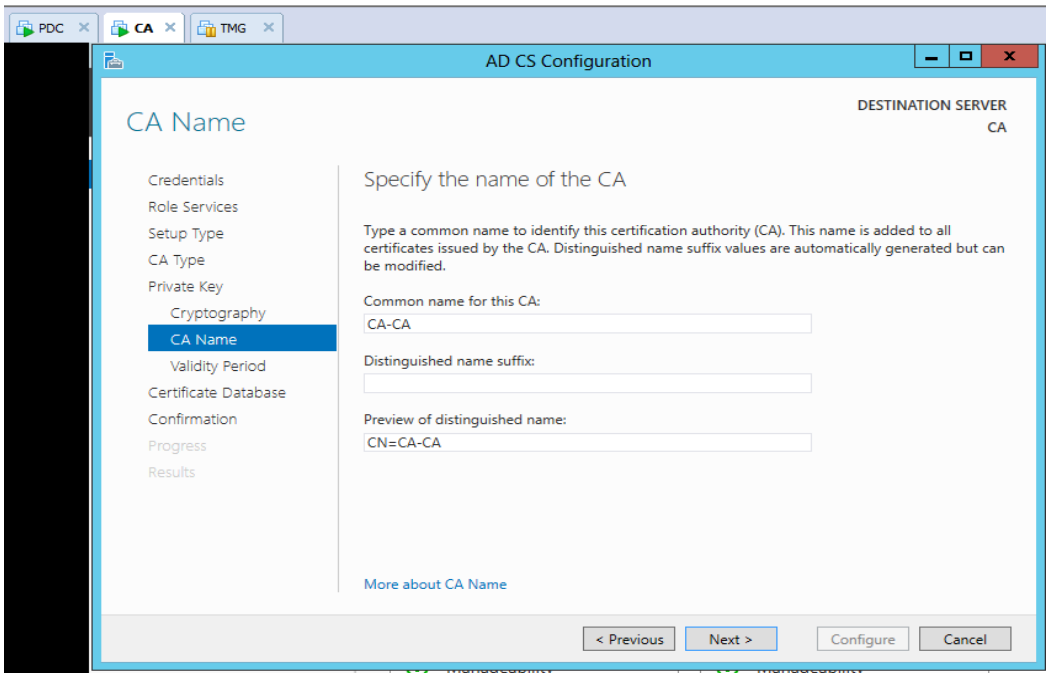
Créez une nouvelle clé privée



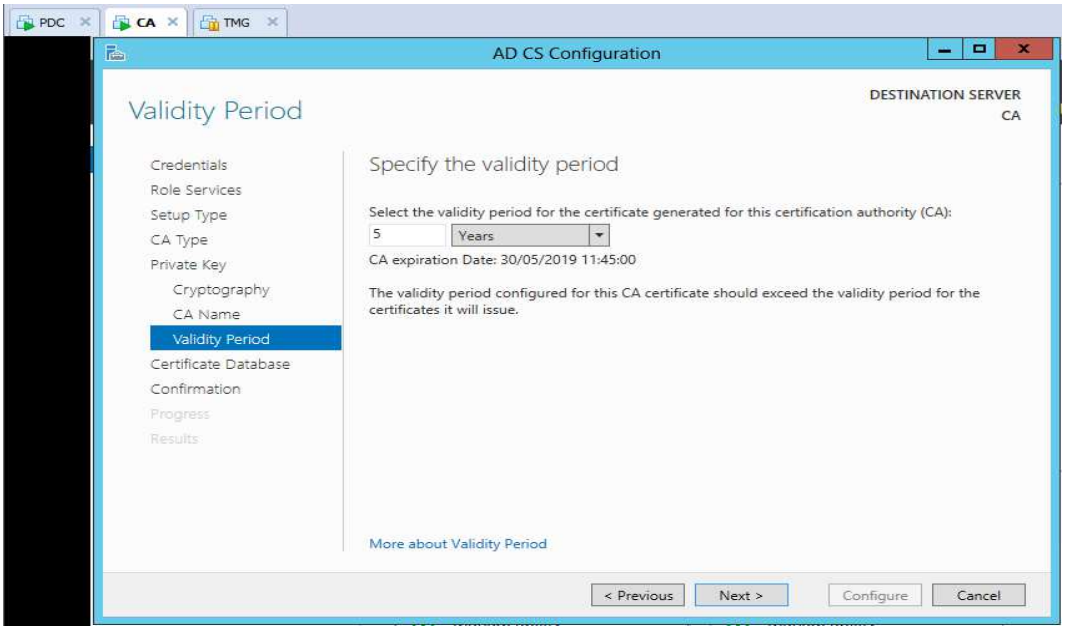
Vous avez ce défaut 2048 touche Nombre de caractères

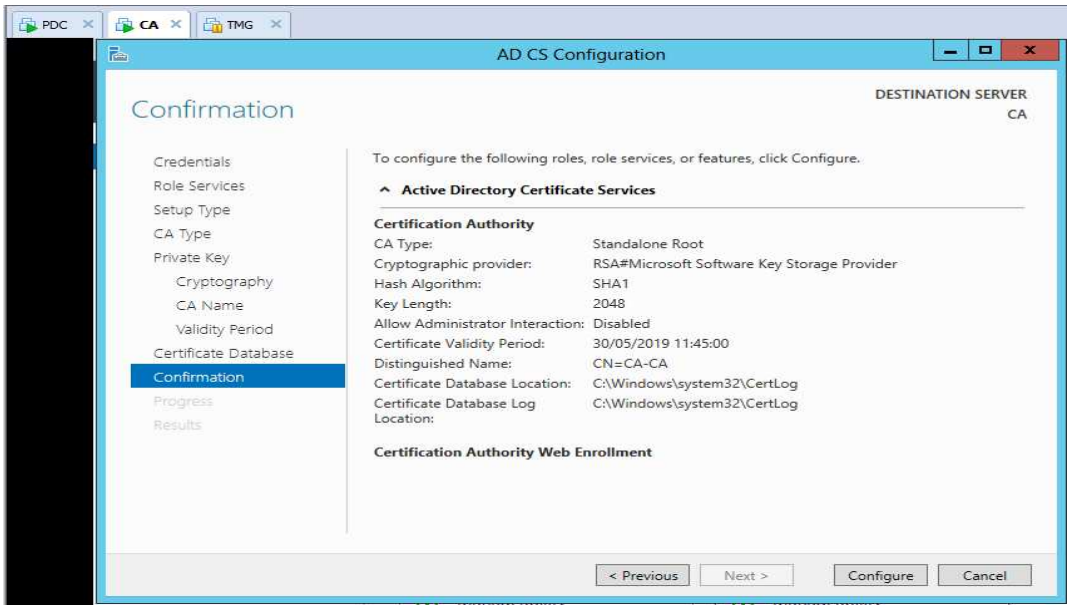


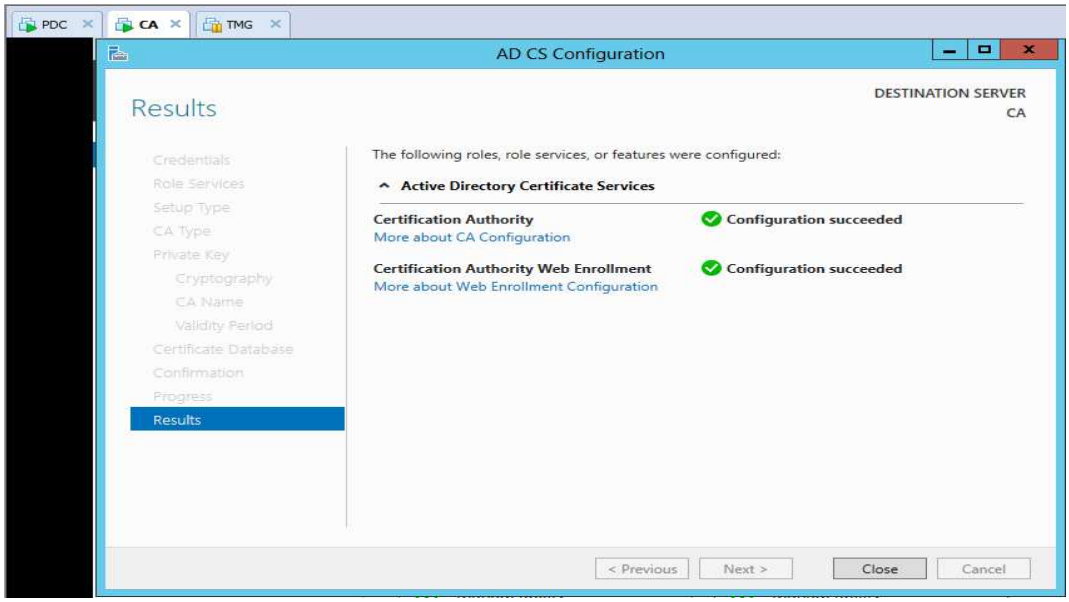
Cliquez sur Suivant



Par défaut certificat est valable pendant 5 ans, Ne pas apporter de modifications à ce sujet, cliquez sur Suivant







Pour configurer les services de certificats Active Directory

Choisissez active directory certificat service

Cliquez sur Suivant

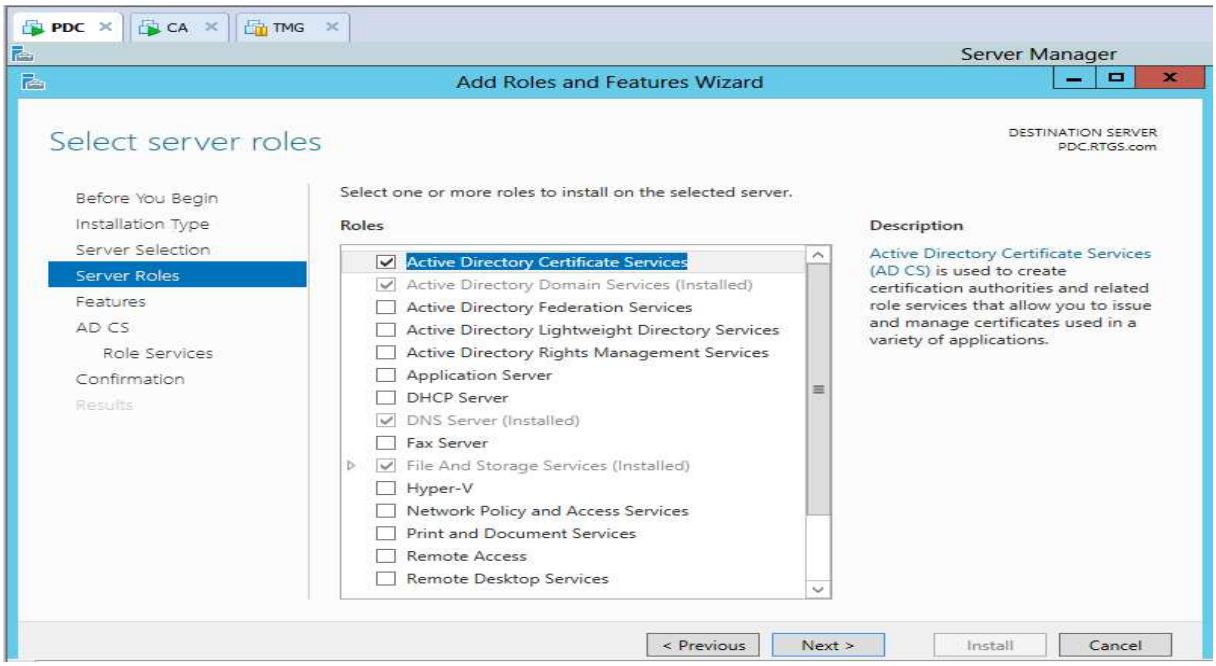
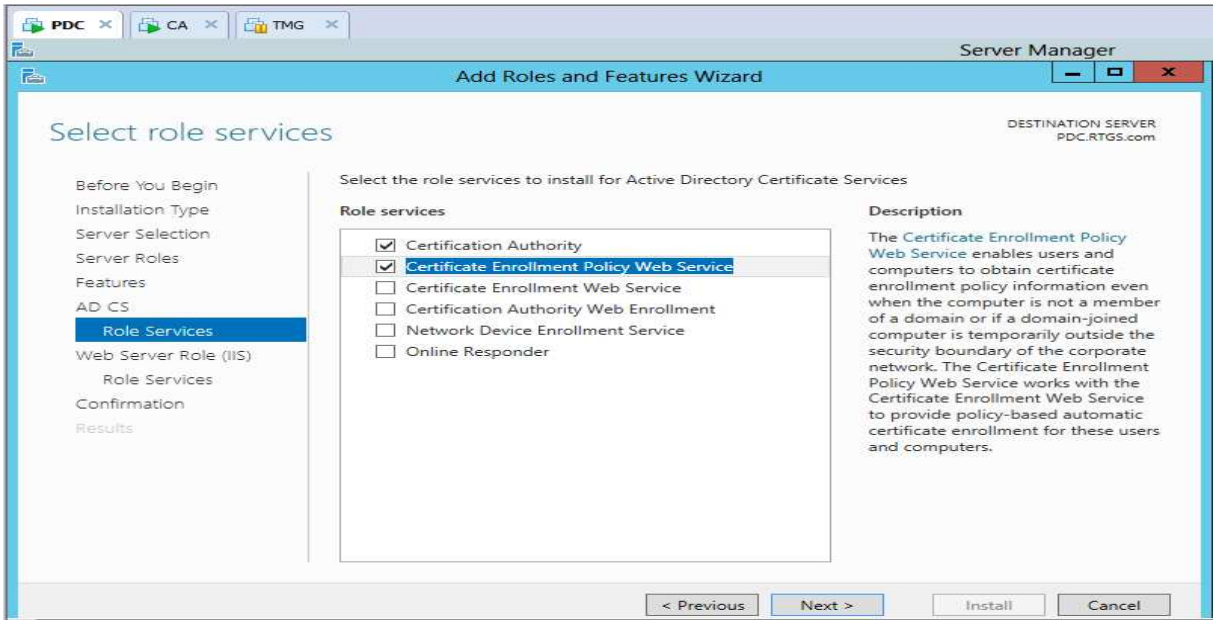
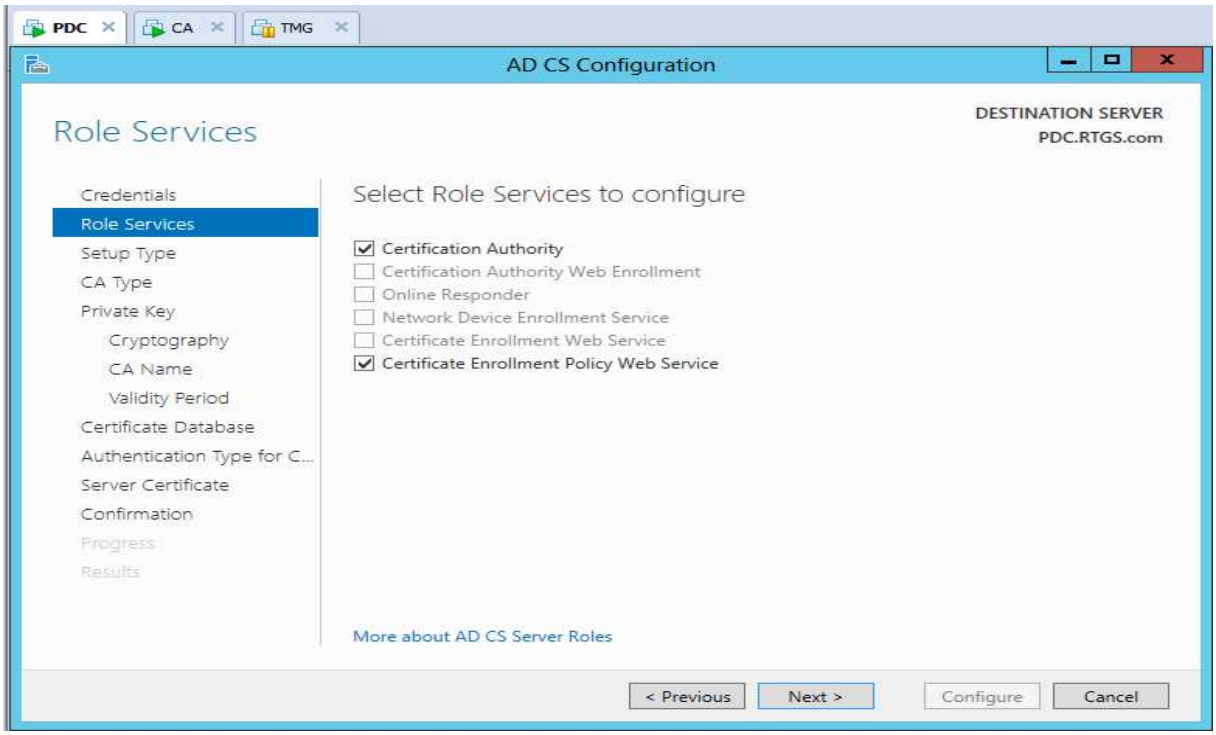


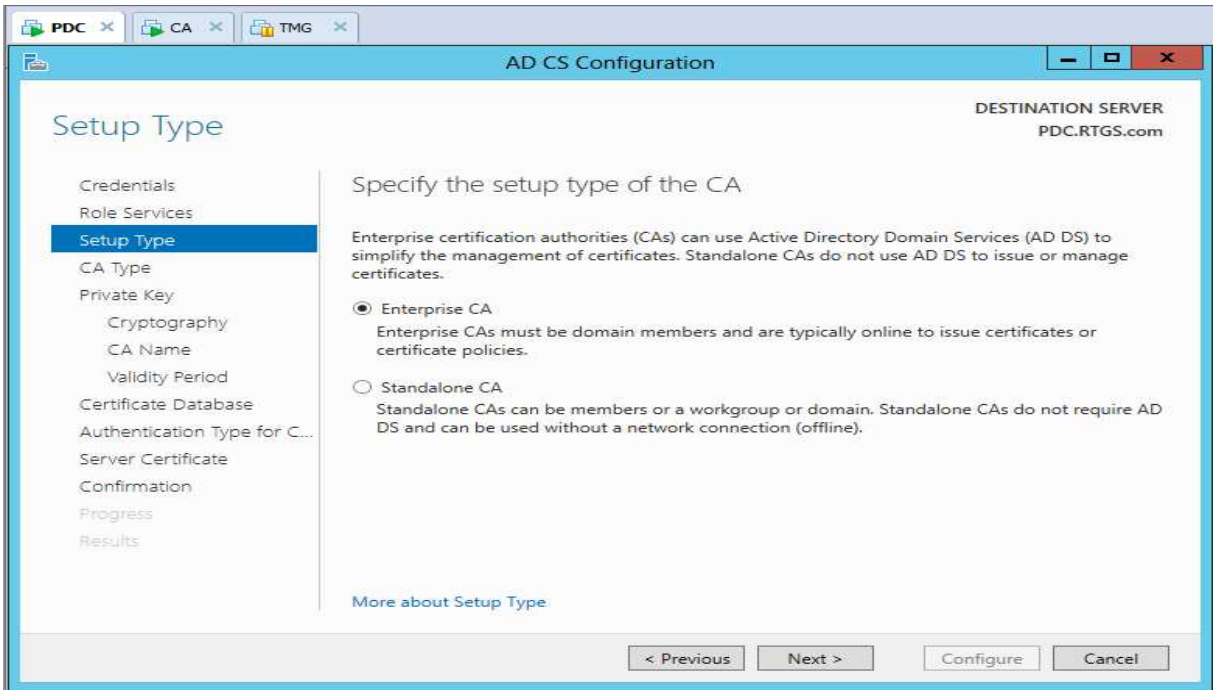
Figure C.2: Configuration les services d'Active Directory.

Choisir Autorité de certification & Autorité de certification d'inscription Web

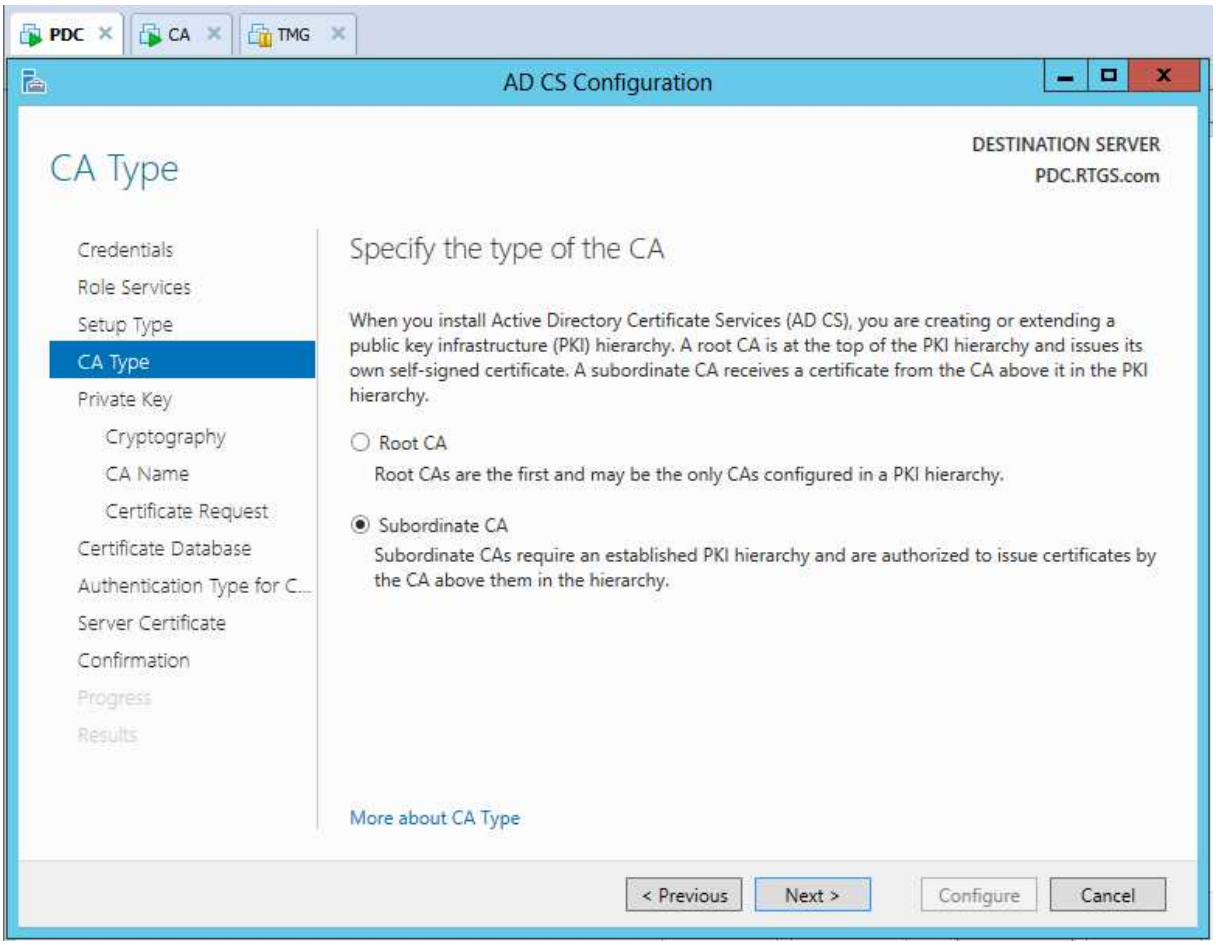




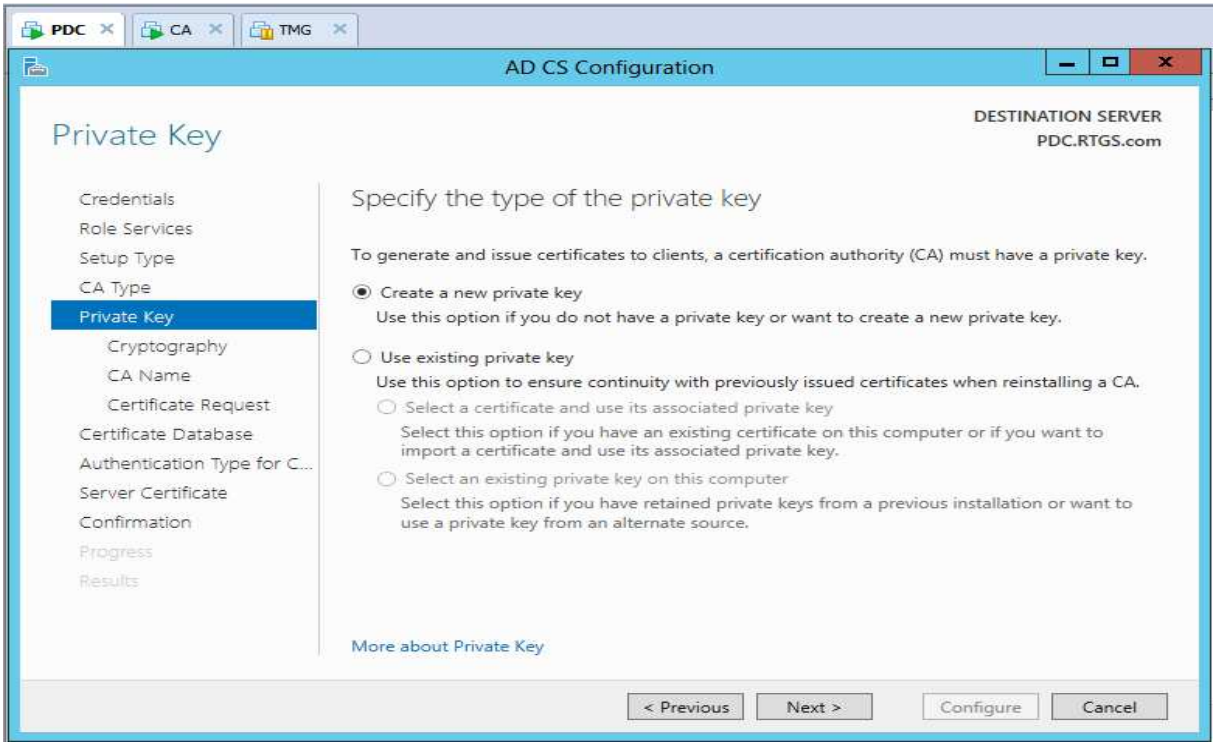
Choisissez Enterprise

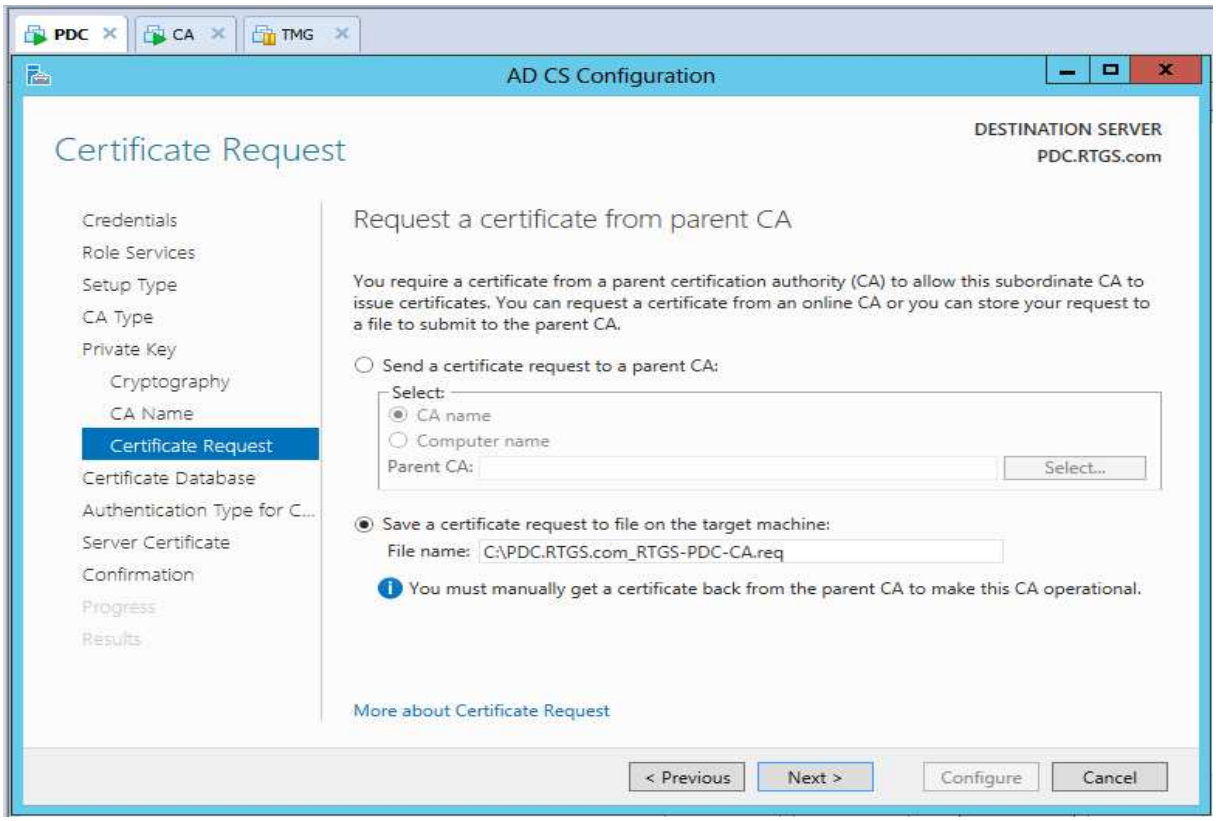


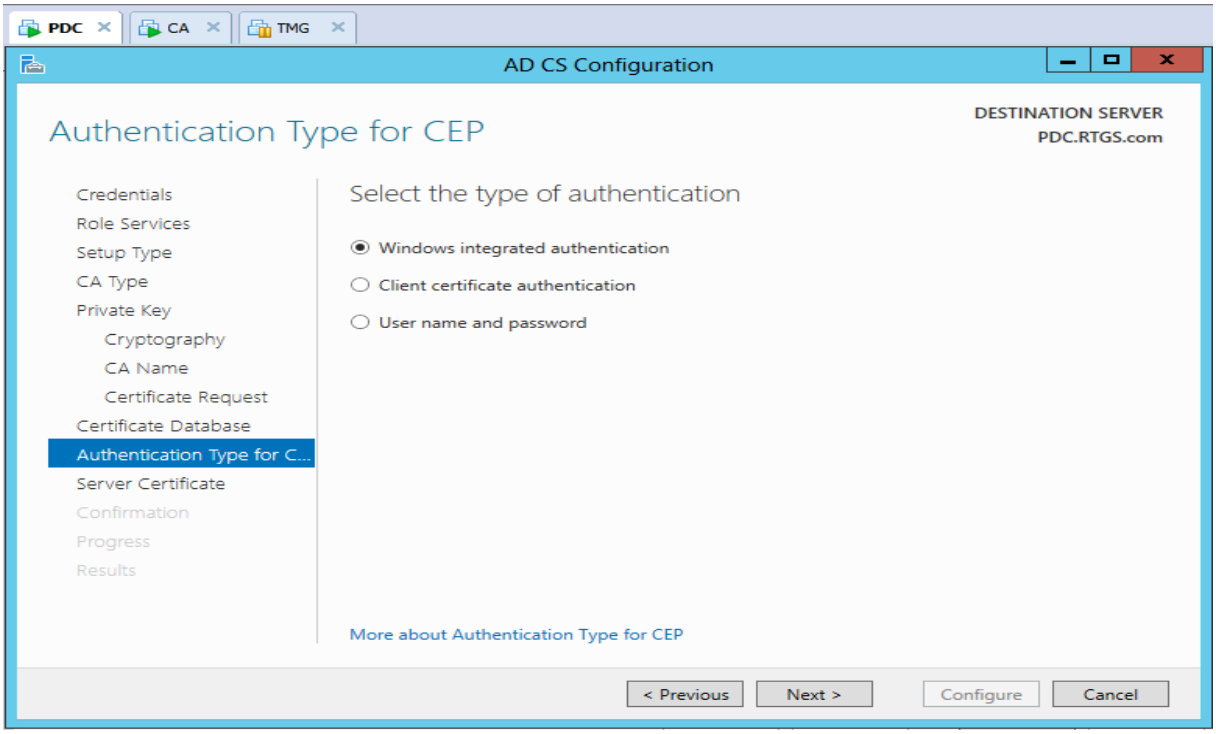
Choisissez subordinate CA

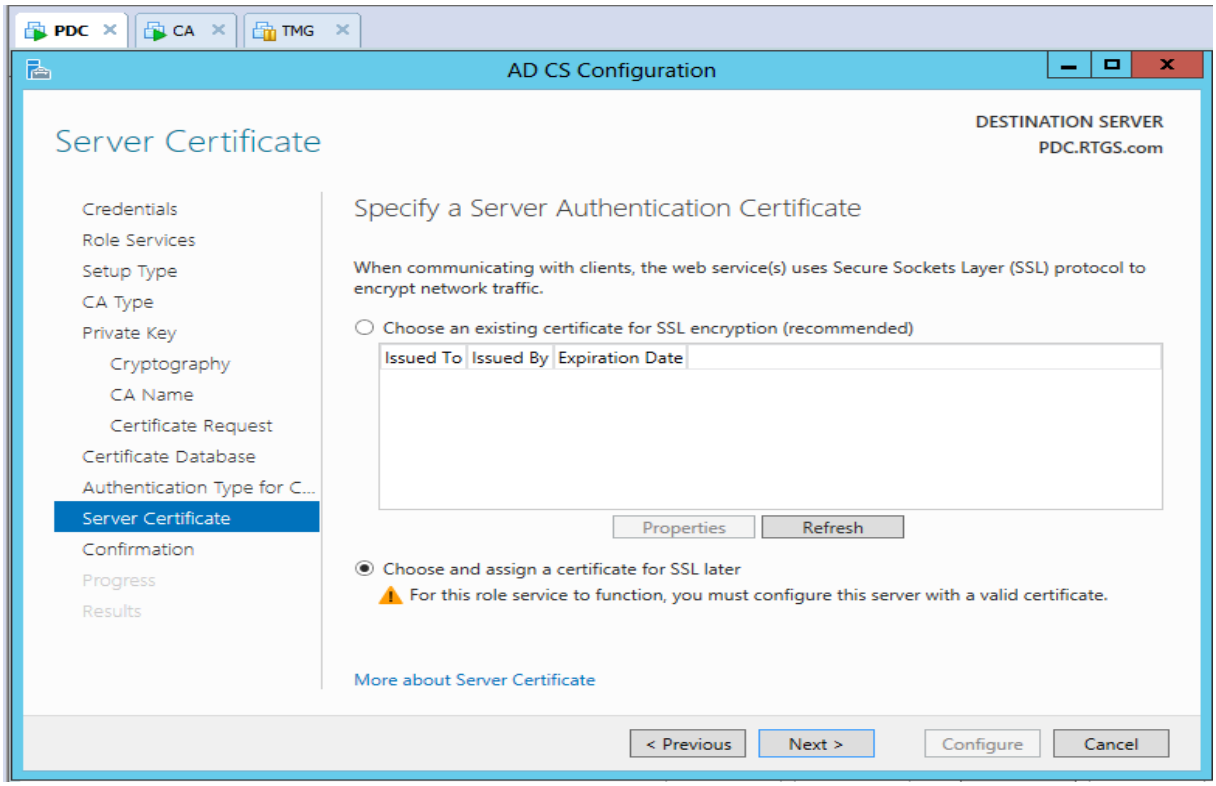


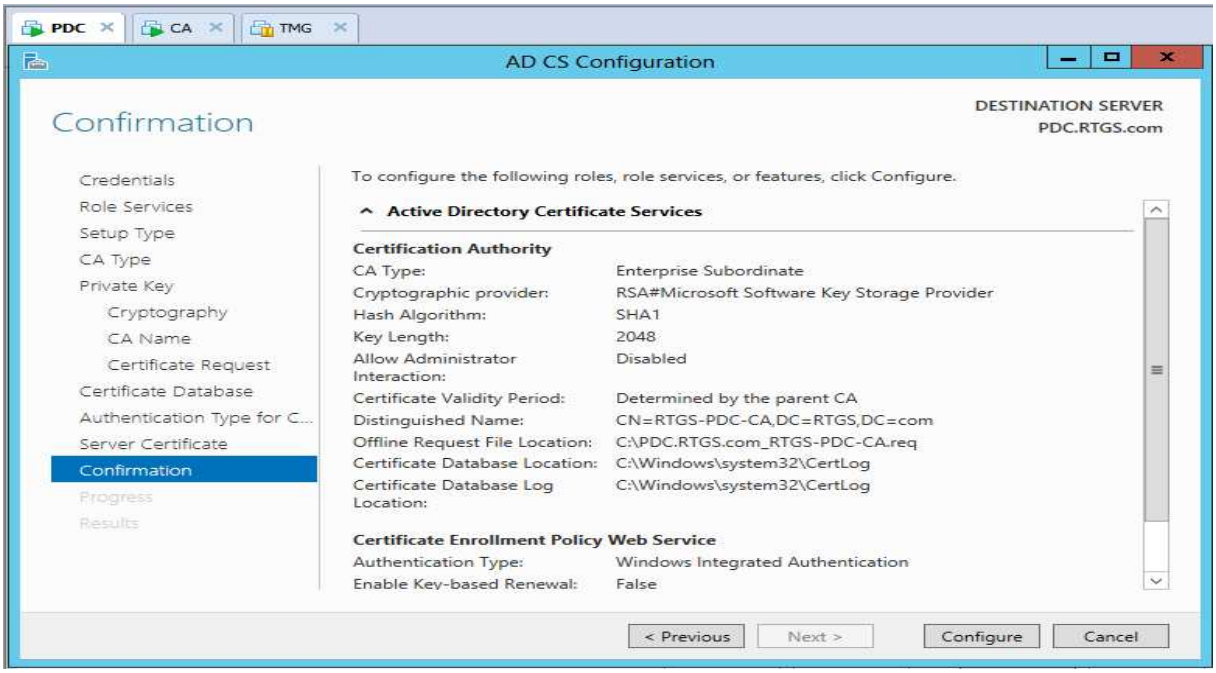
Créez une nouvelle clé privée

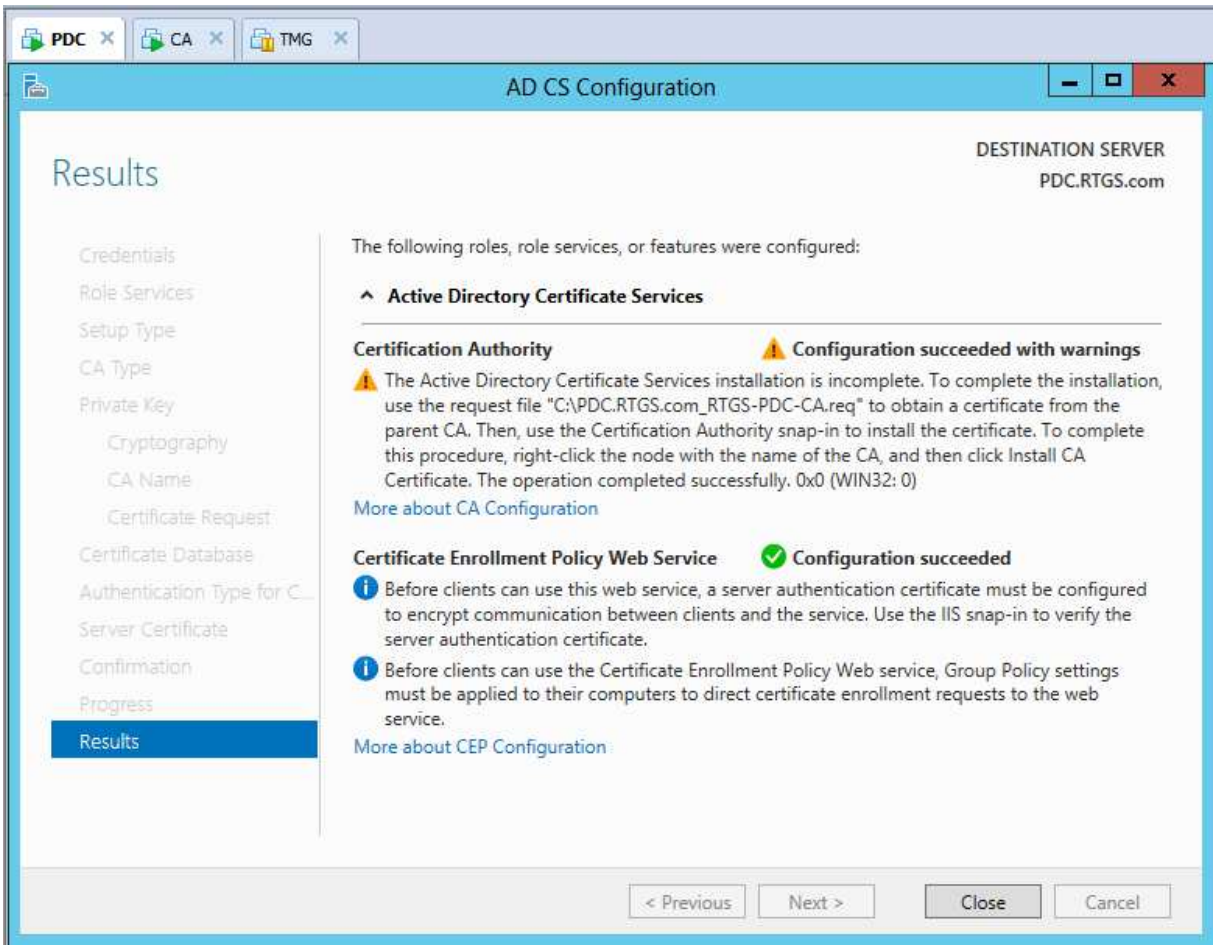



PDC
CA
TMG
AD CS Configuration
Certificate Request
DESTINATION SERVER
PDC.RTGS.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Request a certificate from parent CA
You require a certificate from a parent certification authority (CA) to allow this subordinate CA to issue certificates. You can request a certificate from an online CA or you can store your request to a file to submit to the parent CA.
Send a certificate request to a parent CA:
Select:
CA name
Computer name
Parent CA:
Select...
Save a certificate request to file on the target machine:
File name: C:\PDC.RTGS.com_RTGS-PDC-CA.req
You must manually get a certificate back from the parent CA to make this CA operational.
More about Certificate Request
< Previous
Next >
Configure
Cancel


PDC
CA
TMG
AD CS Configuration
Authentication Type for CEP
DESTINATION SERVER
PDC.RTGS.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Select the type of authentication
Windows integrated authentication
Client certificate authentication
User name and password
More about Authentication Type for CEP
< Previous
Next >
Configure
Cancel


PDC
CA
TMG
AD CS Configuration
Server Certificate
DESTINATION SERVER
PDC.RTGS.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Specify a Server Authentication Certificate
When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.
Choose an existing certificate for SSL encryption (recommended)
Issued To
Issued By
Expiration Date
Properties
Refresh
Choose and assign a certificate for SSL later
For this role service to function, you must configure this server with a valid certificate.
More about Server Certificate
< Previous
Next >
Configure
Cancel


PDC
CA
TMG
AD CS Configuration
Confirmation
DESTINATION SERVER
PDC.RTGS.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Certification Authority
CA Type: Enterprise Subordinate
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA1
Key Length: 2048
Allow Administrator Interaction: Disabled
Certificate Validity Period: Determined by the parent CA
Distinguished Name: CN=RTGS-PDC-CA,DC=RTGS,DC=com
Offline Request File Location: C:\PDC.RTGS.com_RTGS-PDC-CA.req
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog
Certificate Enrollment Policy Web Service
Authentication Type: Windows Integrated Authentication
Enable Key-based Renewal: False
< Previous
Next >
Configure
Cancel



Installation et configuration est OK.

Bibliographie

Bibliographie

[1] David GELIBERRT Sécurité et virtualisation, Livre Blanc, Mai 2012.

[2] Philippe Hedde Sécurité Sécurité du Cloud Computing, Livre Blanc, Avril 2010.

[3] Eric Besson Datacenters et Développement durable, Livre Vert, Juin 2011.

[4] http://www.howtogeek.com/99323/installing-active-directory-on-server-2008-r2/

[5] http://www.xerunetworks.com/2012/03/asa-84-asdm-on-gns3-step-by-step-guide/

[6] http://www.xerunetworks.com/2012/02/cisco-asa-84-on-gns3/

[7] http://www.loria.fr/~lnussbau/files/ptasrall2011-cloud-rapport.pdf

[8] http://www.passionmicro.fr/Docs/Livre-Blanc-Cloud.pdf

[9] http://www.ge.ch/ppdt/doc/privatim_Cloud_Computing_2013_f.pdf

[10] https://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-Cloud-2010-Datacenter.pdf

[11] http://www.prepressure.com/library/technology/raid

[12] http://www-igm.univ-mlv.fr/~dr/XPOSE2008/virtualisation/

[13] http://www.finyear.com/SAP-et-la-Virtualisation-un-mariage-technique-reussi_a18767.html

[14] http://network-blog.shost.ca/2014/03/26/presentation-cisco-packet-tracer/

[15] http://regardsurlecloud.wordpress.com/2012/06/03/du-web-classique-vers-le-cloud-computing/

Glossaire

Glossaire

CC	Cloud Computing
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
ROM	Read Only Memory
BIOS	Basic Input Output System
VPN	Virtual Private Network
RAM	Random Access Machine
IP	Internet Protocol
CPU	Central Processing Unit
IT	Information Technology
SAN	Storage Area Network
DAS	Direct Attached System
iSCSI	Internet Small Computer System Interface
RAID	Redundant Array of Independent Disks
DOS	Deny Of Service
DNS	Domain Name System
LB	Load Balancing
NLB	Network Load Balancing
UDP	User Datagram Protocol
NAS	Network Attached Storage
ICMP	Internet Control Message Protocol

Glossaire

SNMP	Simple Network Management Protocol
ASA	Adaptive Security Appliance
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
TMG	Threat Management Gateway
ISA	Internet Security and Acceleration
DMZ	Demiltarized zone
ACL	Access Control List
SSH	Secure Socket Shell
RADIUS	Remote Authentication Dial-In User Service
CA	Certificate Authority
NVRAM	Non-Volatile Random Access Memory
ADC	Advanced Domain Controller
PDC	Primary Domain Controller
IIS	Internet Information Services
HSRP	Hot Standby Router Protocol