REPUBLIQUE TOGOLAISE

Travail – Liberté - Patrie

MINISTERE DE LA
PLANIFICATION
DU DEVELOPPEMENT

Institut Africain d'Informatique-
Représentation du TOGO (IAI-TOGO)
Tel : 22 20 47 00
E-mail : iaitogo@iai-togo.tg
Site web: www.iai-togo.tg
07 BP 12456 Lomé 07, TOGO

Conseil Etude Réalisation et Gestion Informatique
Tel : (+228) 22 50 02 40
E-mail : cergi@cergibs.com
Site web: www.cergibs.com
08 BP: 80171 Lomé-TOGO

MEMOIRE DE FIN DE FORMATION POUR L'OBTENTION DU DIPLOME D'INGENIEUR DES TRAVAUX INFORMATIQUES

Option : Administration Réseaux et Systèmes

Thème :

OPTIMISATION DE L'ARCHITECTURE CLOUD COMPUTING DE CERGI SA

Période : Du 6 juillet au 30 septembre 2020

Rédigé et soutenu par : KPALOU Afeidé Augustin
Etudiant en troisième année

Année universitaire : 2019 – 2020

SUPERVISEUR

M.TETE K. Senan

Enseignant à IAI-TOGO

MAITRE DE STAGE

M. NONDOH-ADABI Essobyô

Chef Administrateur Systèmes Réseaux à CERGI SA

DEDICACE

REMERCIEMENTS

AVANT-PROPOS

Résumé

Abstract

SOMMAIRE

INTRODUCTION

Au cours de la première décennie du 21e siècle, les Datacenter ont acquis une place d'actif majeur de l'entreprise, en raison de leur rôle vital dans la gestion des activités et le service à la clientèle. Tout au long de cette période, les Datacenter ont subi une évolution avec la croissance rapide des capacités de calcul et de stockage.

Le cloud computing est un modèle de Datacenter qui permet un accès omniprésent, pratique et à la demande à un réseau partagé et à un ensemble de ressources informatiques configurables (comme par exemple : des réseaux, des serveurs, du stockage, des applications et des services) qui peuvent être provisionnées et libérées avec un minimum d'administration. Les principaux services proposés en cloud computing sont le Saas (Software as a Service), le PaaS (Platform as a Service) et le IaaS (Infrastructure as a Service) ou le MBaaS (Mobile Backend as a Service) généralement sur trois niveaux, le cloud public accessible par Internet, le cloud d'entreprise ou privé accessible uniquement sur un réseau privé, le cloud intermédiaire ou hybride qui est un mix entre le cloud public et le cloud privé. Les utilisateurs ne sont plus propriétaires de leurs serveurs informatiques mais peuvent ainsi accéder à de nombreux services en ligne sans avoir à gérer l'infrastructure sous-jacente, souvent complexe. Les applications et les données ne se trouvent plus sur l'ordinateur local, mais métaphoriquement parlant dans un nuage (Cloud) composé d'un certain nombre d'équipements informatique interconnectés au moyen d'une excellente bande passante indispensable à la fluidité du système.

Les Datacenter ont toujours été construits de manière à pouvoir accueillir des charges supplémentaires mais, au cours des dix dernières années, la demande en termes de ressources de stockage et de traitement de l'information à augmenter si vite que les capacités informatiques des Datacenters se retrouvent dépasser. Cette augmentation exige donc une Amélioration de l'architecture des Datacenters visant à répondre aux besoins actuels et futurs. Dans cette vision, CERGI SA, une entreprise de prestation de solutions bancaire, se donne comme objectif d'optimiser son infrastructure cloud Computing,

dans le but d'offrir à ses clients une expérience utilisateurs meilleurs possible, Améliorer l'excellence opérationnelle, et fournir de façon évolutive des services innovants.

Le présent mémoire rend compte de tout ce qui est réaliser durant notre stage de fin de formation en cycle ingénieur des travaux informatiques, option Administration Réseaux et Systèmes (ASR) à CERGI SA. Il sera structuré comme suit : en premier lieu nous présenterons IAI-TOGO notre institut de formation ainsi que CERGI SA notre cadre de stage ; en deuxième lieu nous ferons l'étude et la critique de l'existant, nous poserons la problématique et les approches de solutions ; nous étudierons les différentes solutions à déployer en troisième lieu et finirons en mettant en œuvre la solution retenue.

LISTE DES PARTICIPANTS

Nom et Prénom(s)	*Fonctions*	*Rôles*
TETE K. Senan	*Enseignant à IAI-TOGO*	*Superviseur*
Essobyô NONDOH-ADABI	*Chef Administrateur Réseaux et système*	*Maitre de Stage*
Augustin Afeidé KPALOU	*Etudiant en 3eme Année ASR à IAI TOGO*	*Réalisateur*

Tableau 1: Liste des participants au projet

LISTES DES TABLEAUX

LISTE DES FIGURES

GLOSSAIRE

PARTIE I : PRESENTATIONS

A. PRESENTATION DE l'IAI-TOGO

a) Historique

Après les indépendances, la formation des cadres technique de haut niveau, adaptés aux besoins socio-économiques des pays apparaissait comme l'une des priorités pour soutenir les actions d'un plan de développement national harmonieux. C'est ainsi que les chefs d'Etat de l'ancienne Organisation Commune Africaine, Malgache et

Mauritanienne (OCAM) considérant le développement continu et accéléré de l'informatique dans le monde et la nécessité de disposer d'un personnel qualifié pour faire face au développement de l'informatique, ont convenu dans le cadre de leur politique de renforcement de la solidarité africaine de créer une école dénommée

Institut Africain d'Informatique (IAI). Cette structure a pour mission de former de personnel qualifié en informatique dont les différents Etats ont besoin pour répondre aux exigences du développement. La convention portant la création de l'institut et les statuts y affèrent ont été signés en janvier 1971 à Fort Lamy (actuel N'Djamena) en

République du TCHAD. Le siège a été fixé à Libreville au Gabon et l'accord entre l'IAI et le Gabon a été signé en Janvier 1975. L'Institut Africain d'Informatique (IAI) fut ainsi créé le 29 janvier 1971 et compose de 11 pays que sont :

Le BENIN, le BURKINA-FASO, le CAMEROUN ; le CONGO, la CÔTE-D'IVOIRE, le GABON, le NIGER, la REPUBLIQUE CENTRAFRICAINE, le SENEGAL, le TCHAD et le TOGO.

Le TOGO est un membre du Conseil d'Administration de l'IAI. Le 24 octobre 2002, Le

Centre Nationale d'Etudes et de Traitements Informatiques (CE.N.E.T. I) héberge la représentation de l'IAI au Togo. Celle-ci a ouvert ses portes le 24 octobre 2002 sous l'appellation d'IAI-TOGO il forme en trois (03) ans, des Ingénieurs des Travaux

Informatiques. Cette formation constitue le cycle préparatoire des cycles d'ingénieurs concepteurs en Informatique et de celui des titulaires de Maîtrise en Informatique

Appliquée à la Gestion (MIAGE) à Libreville.

b) Objectif de l'IAI-TOGO

Dans le domaine de l'informatique et des Nouvelles Technologies de l'Information et de la Communication, l'IAI-TOGO concourt :

- A la formation (initiale et continue) ;
- Au perfectionnement ;
- A la recherche ;
- Au conseil ;
- A l''information ;
- A la documentation et la communication ;
- A la certification à l'académie CISCO.

c) Les formations de l'IAI-TOGO

L'IAI-TOGO forme essentiellement des Ingénieurs des Travaux Informatique pour une durée de trois (03) ans dans trois (03) filières : Génie Logiciel (GL), Systèmes et Réseaux (SR) et Multimédia et Technologie Web et Infographie (M-TWI) en collaboration avec l'Université Technologique de Belfort-Montbéliard (UTBM) en France.

d) Formation modulaire (CISCO)

L'IAI-TOGO, toujours dans le souci de former des cadres de qualité et très compétitifs sur le marché, a ouvert le lundi 14 Mai 2012 une nouvelle branche de formation dénommée formation Cisco. Les cours Cisco sont découpés en quatre (4) modules CCNA1, CCNA2, CCNA3 et CCNA4, tous accessibles via Internet. Cette formation est destinée aux techniciens réseaux, revendeurs de produits Cisco et à toute personne désirant embrasser la carrière d'informaticien réseau.

e) Condition d'admission

Les conditions d'admission à l'IAI-TOGO sont les suivantes :

- Première année : l'étudiant doit être titulaire d'un baccalauréat scientifique (C, D, E, F2 ou équivalent) et être admis au concours ;
- Deuxième année : l'entrée sur titre pour les titulaires d'un DUT en Informatique ou équivalent obtenu en deux (ans) d'études ;
- Troisième année : l'étudiant doit être titulaire d'un DUT en informatique délivré par le Centre d'Informatique et de Calcul (C.I.C).

f) Organigramme

L'organigramme de l'IAI-TOGO se présente comme suit :

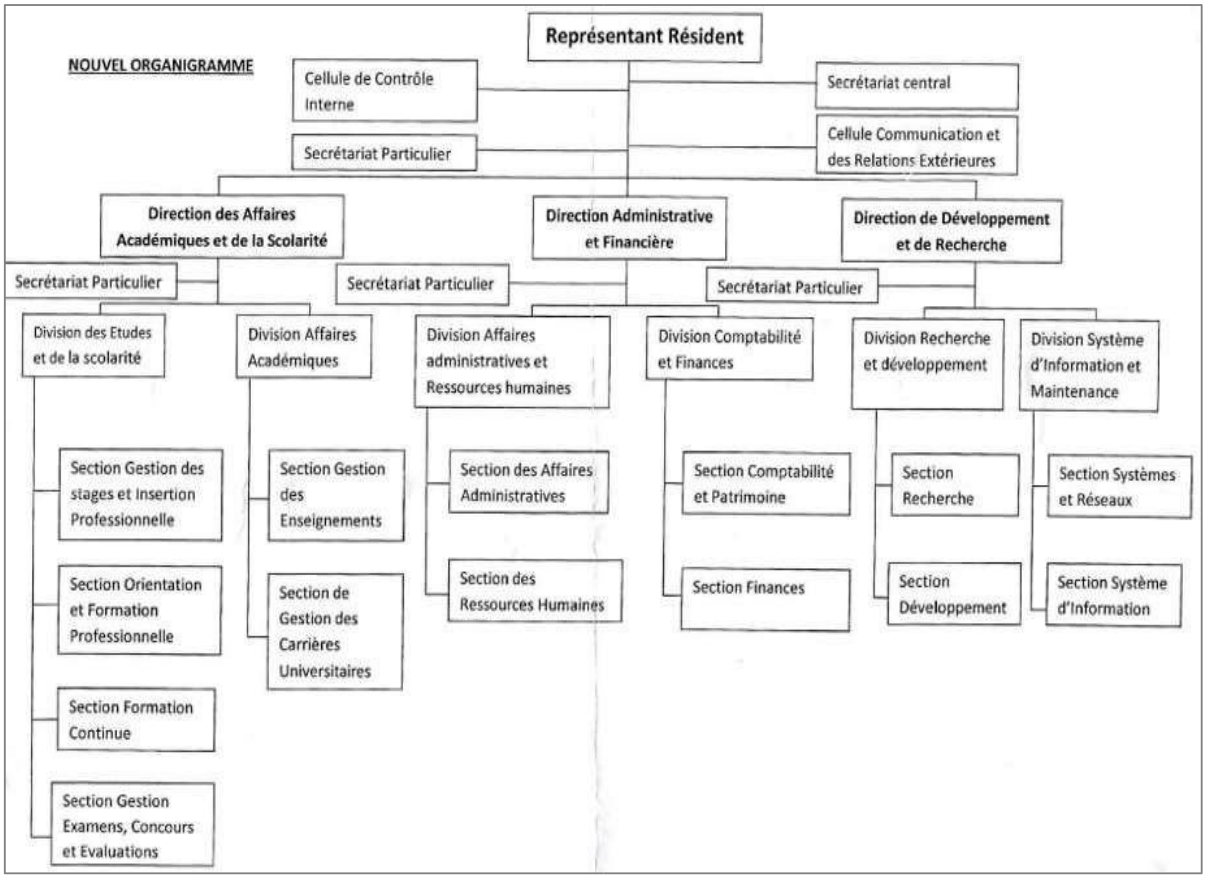


Figure i: Organigramme de IAI-TOGO

g) Situation géographique

L'IAI-TOGO se trouve à Lomé, dans les locaux du CE.N.E.T.I. Il est situé dans le quartier administratif (Nyékonakpoè) à côté de la Communauté Electrique du

Bénin (C.E.B), derrière l'Union Togolaise des Banques (U.T.B) et AIR FRANCE, sur la rue de la Kozah.

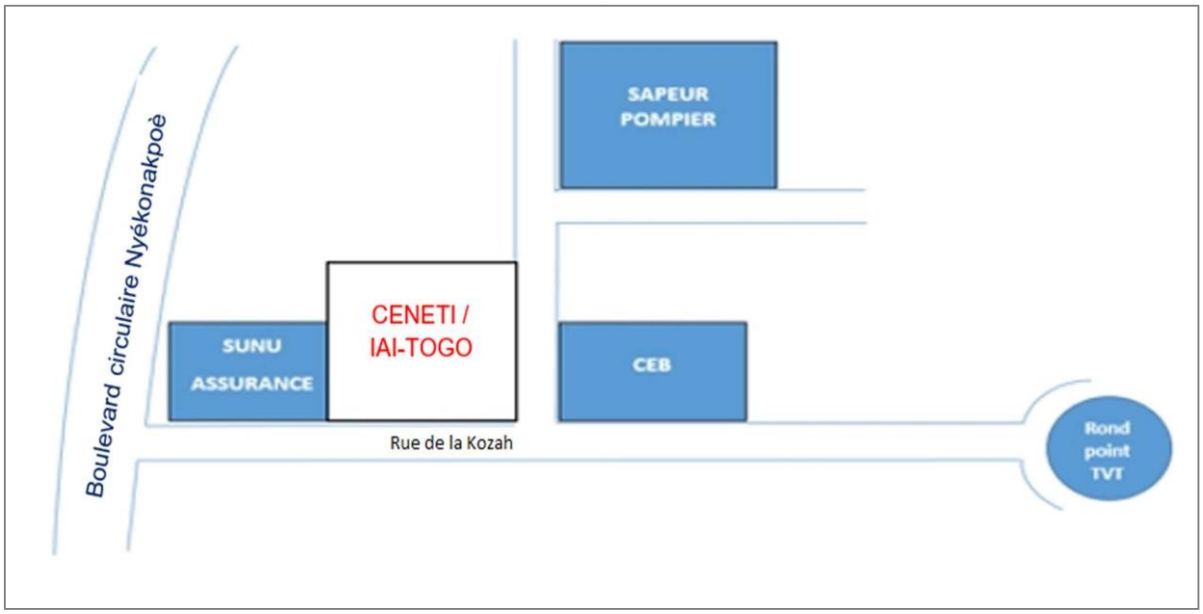


Figure ii: Localisation Géographique de IAI-TOGO

B. PRESENTATION DE CERGI SA

Défini comme Conseil Etude Réalisation et Gestion Informatique, CERGI SA est une société anonyme de développement de services informatiques bancaires. Grâce à son réseau d'ingénieurs, d'experts et de partenaires, les solutions logicielles développées par CERGI sont exploitées par des institutions financières réparties dans les espaces UEMOA (Union Economique et Monétaire des Etats de l'Afrique de l'Ouest) et CEMAC (Communauté Economique et Monétaire des Etats de l'Afrique Centrale). Le cabinet CERGI a pour objectif d'apporter un appui stratégique et couvrir la totalité des fonctionnalités métiers et supports des banques et établissements financiers dans le strict respect des instructions des autorités de régulation (BCEAO, BEAC) et des législations internationales. Il nourrit ainsi la vision d'offrir des solutions logicielles de gestion les plus adaptées aux activités et à l'évolution du secteur bancaire et financier africain.

- **Statut**

L'entreprise prend la dénomination de : Conseil Etude Réalisation et Gestion Informatique par abréviation CERGI. Créée à Abidjan (Côte d'Ivoire) en 1991 à l'initiative de M. Yao Dodzi DOGBO, CERGI Afrique Sarl est née du rachat du fonds de commerce de la filiale africaine du Groupe français, Société Générale de services et de Gestion (SG2-Afrique). Devenue en 2003 CERGI Banking Services SA, elle a poursuivi sa structuration en 2015 avec la création de CERGI SA à Lomé en vue d'une configuration de Groupe. CERGI SA étant reconnu légalement comme Société Anonyme siégeant à Lomé (TOGO), quartier Avenou, 5330 Immeuble Eros 2ème étage, Boulevard du 30 Août.

- **Mission**

CERGI SA a pour mission de fournir aux banques et établissements financiers (Fonds de Garantie, Crédit-Bail et Leasing, Systèmes Financiers Décentralisés) un progiciel de gestion bancaire. Ce progiciel dénommé IBIS (Integrated Banking Information System) se veut intégrer, complet, fortement paramétrable, performant et économique, le tout conçu strictement selon les instructions des autorités de régulation.

- **Organigramme**

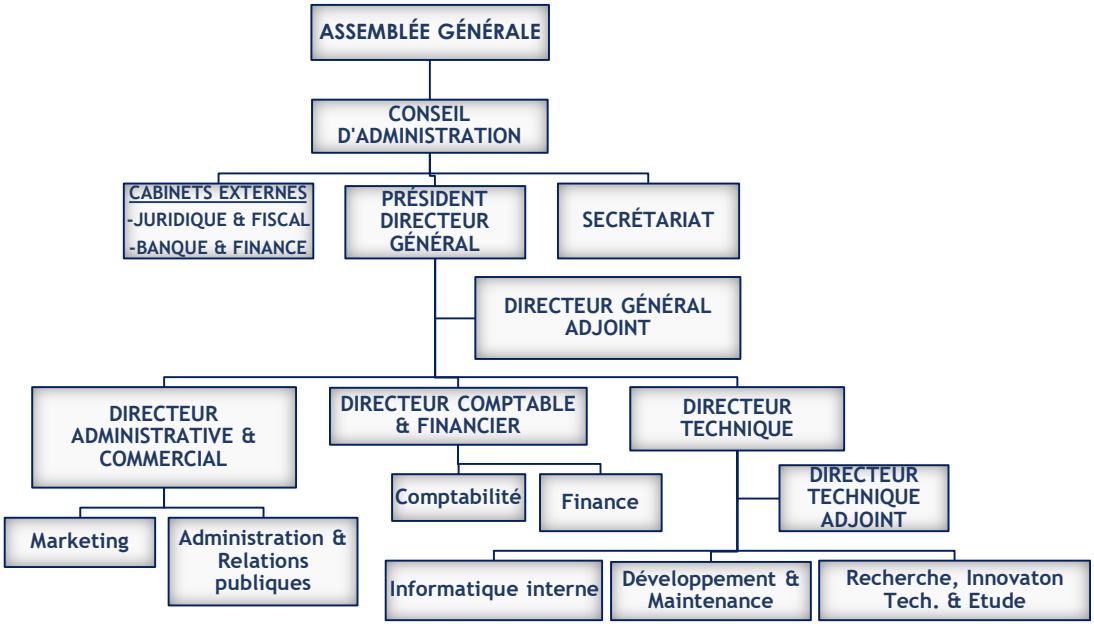


Figure iii: Organigramme de CERGI-SA

- **Activités**

Les activités de la société sont multiples. Elles consistent entre autres à :

Développer des modules évolutifs de services bancaires ;

Déployer, configurer et assurer le suivi des solutions IBIS auprès des banques et institutions financières clientes ;

Offrir aux utilisateurs une formation de qualité en vue d'un transfert de compétences efficient pour l'exploitation optimale du Core Banking ;

Assurer des services de maintenance de proximité pour apporter dans les meilleurs délais, une assistance de qualité à la clientèle ;

Garantir une téléassistance à travers des infrastructures de télémaintenance, help desk, hotline, FAQ.

- **Quelques réalisations**

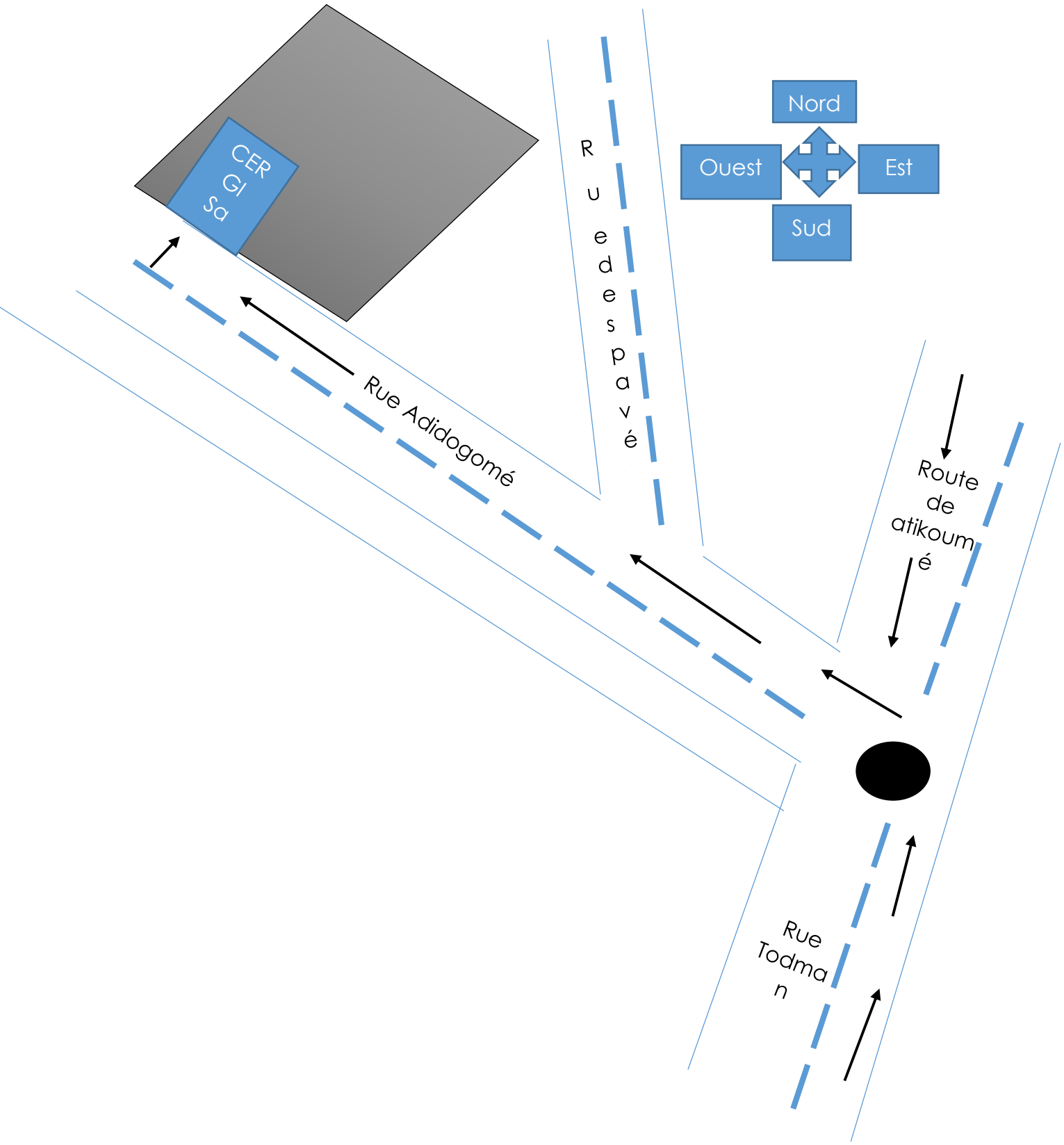
Au chapitre des réalisations de CERGI, on compte les 64 modules du progiciel IBIS autour des 14 centres d'intérêt que sont :

- Noyau comptable ;
- Sécurité ;
- Gestion commerciale ;
- Opérations d'agence ;
- Gestion des engagements ;
- Crédit-Bail ;
- Fonds de Garantie ;
- Trésorerie ;
- Déclarations réglementaires ;
- Mobile Banking ;
- E-Banking ;
- Business Intelligence ;
- Moyens Généraux ;
- Interfaces.

Par ailleurs, le cabinet possède à son actif, une plateforme de notation de contreparties dénommée Scoring Center.

- **Plan de localisation**

La société CERGI SA est située à Lomé, quartier Avenou, au 2ème étage de l'immeuble Eros 5330 au bord du boulevard du 30 août comme l'illustre la figure suivante :


CER
GI
Sa
Nord
Ouest
Est
Sud
R u e d e s p a v é
Rue Adidogomé
Route de atikoumé
Rue Todman

PARTIE II : ETUDE PREALABLE DU SUJET

A. Etude de l'existant

a) Architecture du Cloud computing de CERGI SA

Pour la prestation de ses différents services, la société CERGI SA dispose d'une architecture de cloud computing hybride. En effet, un cloud hybride est la combinaison d'un prestataire de cloud public et d'une plate-forme de cloud privé, destinée à être utilisée par une seule entreprise. CERGI SA associe donc un cloud privé et des services cloud public reparti sur trois sites :

- **L'infrastructure privé d'Abidjan**

Basé à Abidjan en côte d'ivoire, c'est une infrastructure composée principalement de trois serveurs :

- **Contrôleur de domaine** : c'est un serveur qui répond aux demandes d'authentification et contrôle les utilisateurs du réseau. La mission première du contrôleur de domaine est d'authentifier un utilisateur et de valider son accès au réseau. Il vérifie donc les identifications des objets, traiter les demandes d'authentification et veiller à l'application des stratégies de groupe. Il contient l'Active Directory (AD), le DHCP, le DNS et tourne sur une machine de marque HP Intel® pentium® CPU G630@ 2 ,70GHz, RAM 4GB, SDD 1.5TB avec un système d'exploitation Windows server entreprise 2008.
- **Serveur de base de données** : C'est un serveur dédié au stockage des bases de données des clients. Il extrait et gère la mise à jour des données dans des bases de données. Et fournit aux clients la possibilité de manipuler leurs données à travers une application Web, tout en assurant l'intégrité des données. Ce serveur de base de donnée fonctionne sur le langage d'interrogation et de manipulation de donnée SQL(SQL server 2014) et tourne sur une machine DELL Intel® Xeon® Silver 4108 CPU @ 2.70GHz RAM 320GB SSD 10TB, avec comme système d'exploitation Windows server Datacenter 2012 R2.
- **Serveur de stockage** : C'est une architecture de stockage en mode fichier. Il permet la sauvegarde des bases de données du serveur de

base de données. Il fonctionne sur une machine Lenovo Intel® Xeon® CPU E5-2420 V2 @ 2.20Ghz RAM 128GB, SSD 1.5TB avec Windows server entreprise 2012 R2 comme système d'exploitation.

- **L'infrastructure de Lomé :**

Elle est composée principalement d'un serveur de stockage, et permet de répliquer les bases de données stocker sur le NAS d'Abidjan. C'est une machine Windows server entreprise 2008 R2 de marque Lenovo, Intel® Xeon CPU E5-2420 V2 @2.20GHZ RAM 80 GB SSD 1.5TB

- **Le réseau d'entreprise de CERGI Sa**

Le réseau d'entreprise de CERGI SA est d'un topologie étoile :

Deux routeurs desservent chacun la connexion internet des CANAL BOX et FAI TOGOCOM. Sur le premier routeur se trouve deux serveurs directement connecté au moyen d'un Switch :

Le serveur de domaine : il gère l'ensemble des ordinateurs de tout le pack informatique soit environ 60 hôtes. Il permet d'authentifier chaque machines et validé les accès aux ressources du serveur de travail. C'est un serveur de Marque DELL Xeon Silver RAM 4GB, HHD 1TB, X64 Windows Server 2012 R Edition Standard

Le serveur de travail : il est à la fois un serveur de ficher et de base de données. Il permet de stocker de différents les données de travail (ficher, applications, bases de données …) de l'ensemble du corps professionnel. De Marque LENOVO RAM 32 BG HHD 5TB, il tourne sous Windows server 2012 Datacenter x64.

Les hôtes du réseau sous interconnectés par deux point accès(AP) qui étendent toujours le premier routeur.

Le second routeur permet d'interconnecté les autres périphériques finaux.

Le réseau interne est assuré au moyen de 3 points d'accès lié à un routeur central par le biais d'un switch.

- **Le cloud public de CERGI Sa :**

C'est une infrastructure de serveur dédié virtuel héberger chez l'hébergeur français www.godaddy.com. Ce VPS de 32 GO de Ram et de 400 Go de stockage SSD tourne sur Windows server 2016, sert de serveur WEB. Il héberge les applications développer par la société. Ainsi il intègre les fonctionnalités suivantes :

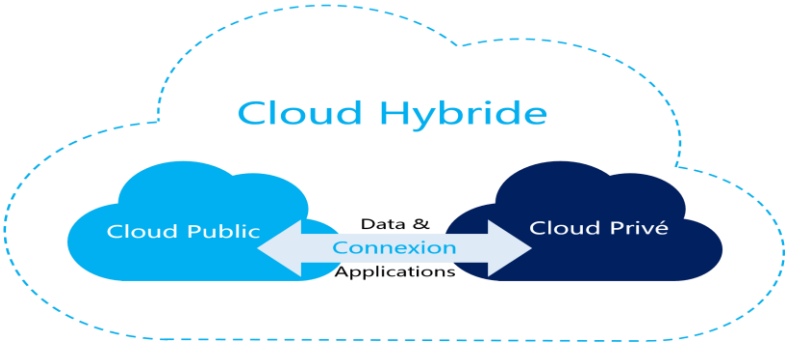
Internet Information Services **(IIS)** : il joue le rôle de serveur web et permet d'héberger en toute fiabilité des sites, services et application Web.

Microsoft SQL Server : c'est un système de gestion de base de données (SGBD) en langage SQL .il est responsable de l'exécution des tâches et des travaux planifiés (création ,mise à jour ,Backup ...)

Un espace de stockage : il contient les ficher indispensable au bon fonctionnement des applications.

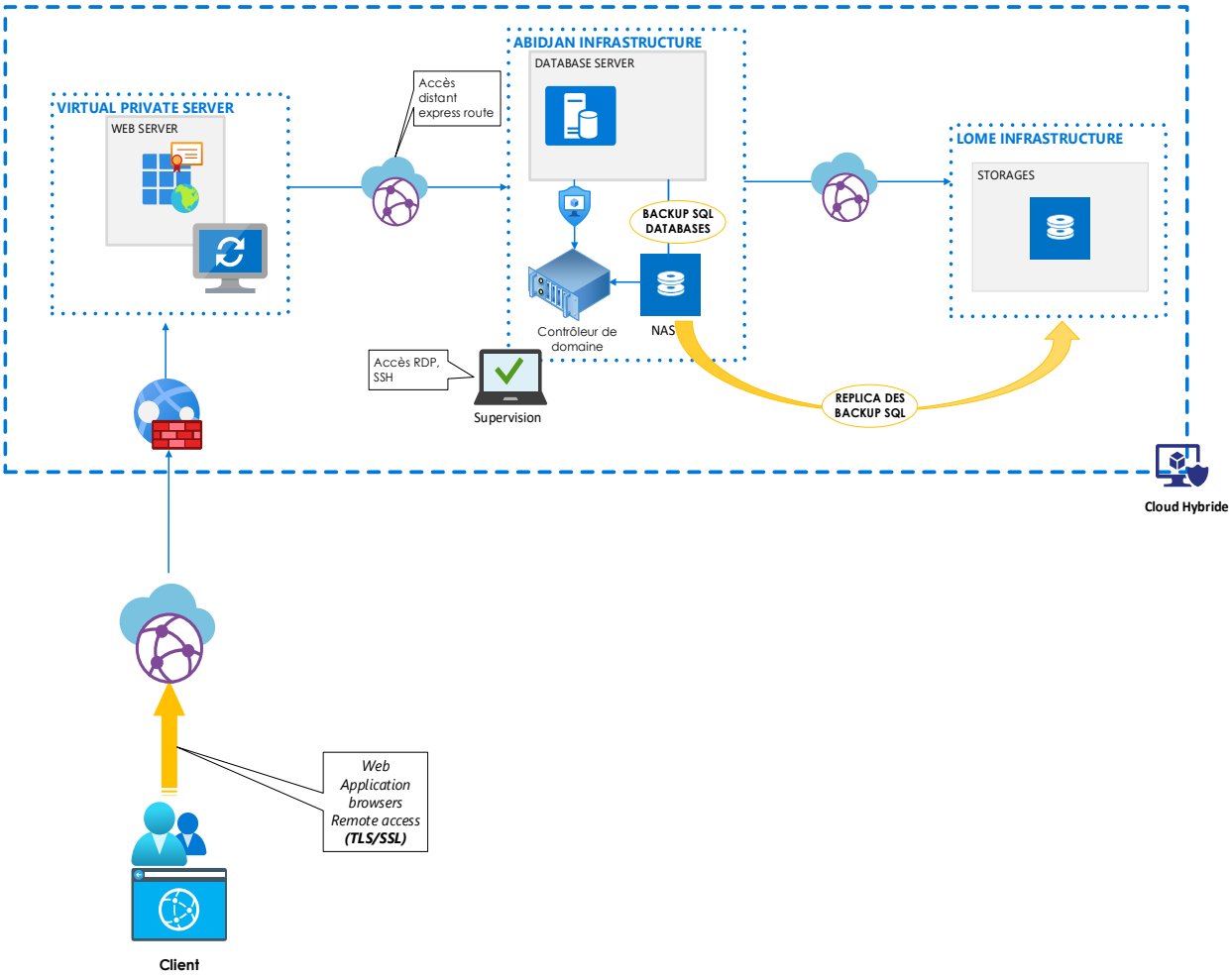
Le serveur est protégé par un WAF (Web application firewall) des certificats SSL et TLS, permettant une communication sécurisée HTTPS entre le client depuis son navigateur et le serveur WEB.

Les trois infrastructures entretiennent une communication sécurisée et cryptés, gérer par Express Route une fonctionnalité de Microsoft pour créer des connexions privées entres les infrastructures publiques et les centres de données locaux ou tout simplement entre deux environnements locaux distantes.



b) Architecture Cloud

L'architecture Cloud Hybride de CERGI SA s'illustre comme le présente la figure suivante :



B. Critique de l'existant

Le cloud computing de CERGI SA est une solution de cloud Hybride puisque les données transitent entre ses clients, son infrastructure privée et son Infrastructure louée dans le cloud public.

- Le VPS public par exemple regorge un serveur web, dont un pare-feu web applicatif (WAF) en assure la sécurité des services fournis, malgré la présence des Certificats SSL et TLS qui activent une communication sécurisée entre serveur web et le client. Le serveur web formule les requêtes des clients en langages SQL pour interroger le serveur de base de données dans l'infrastructure privé d'Abidjan.
- Au niveau du serveur de base données est implémenter des mécanismes de backup dont le but est d'assurer par un une sauvegardes récurrente la restauration facile et spontanée des bases du serveur principal en cas de sinistre.
- Les bases de données sont déversées sur le serveur de fichiers et conduit en toutes sécurité (SFTP) vers un autre serveur de stockage à Lomé.
- Bref Tout semble être bien organisée ; une haute importance est donnée à la sauvegarde des bases de données, en vue de permettre une reprise d'activité rapide après sinistre. Les applications sont hébergées chez un grand prestataire des services cloud pour bénéficier d'une large bande passante et assurer des temps de réponses court.

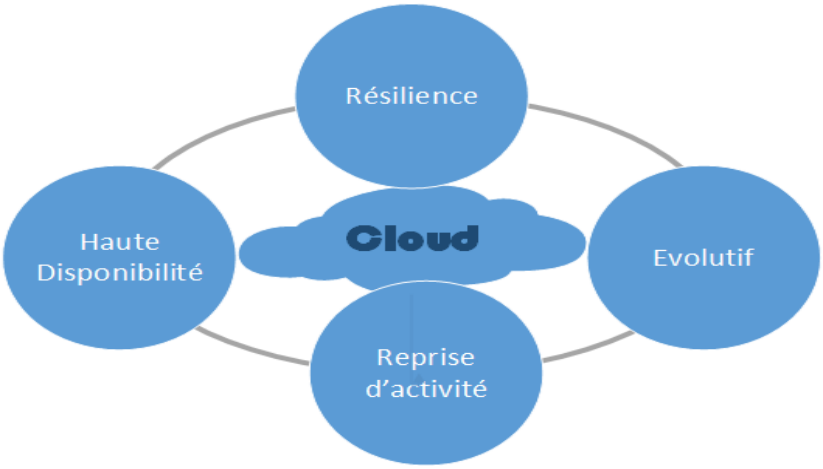
Mais néanmoins, nous rencontrons des problèmes de performances :

- Le serveur de bases donnée doit supporter à lui seul trop de charge, et malheureusement sa vitalité se détériore à avec le temps. Surtout que le temps ne fait qu'accroitre l'activité de CERGI Sa en conséquence de l'augmentation de ses clients.
- La disponibilité et l'intégrité des données sont menacés parce que les traitements des requêtes mettre trop de temps à aboutir dû à leurs lourdeurs.

- ❖ Nous risquons d'être étouffé dans les années avenir du fait principalement de la lenteur des instances de base de données qui sont très importante dans le fonctionnement des applications.
- ❖ En plus le serveur web loin aussi doit supporter un grand nombre de requêtes HTTPS ralentissant considérablement sa vitesse de transmission.

Aux vues de toutes ces difficultés, nous devons prendre des mesures pour bannir à jamais ou tout au moins pour une longue période l'ensemble des causes de l'indisponibilité régulière des services et des applications. Nous devons répondre en temps réels au besoin de ces banques qui ont fait confiance à la puissance de traitement de notre Cloud, pour achever les défis liés à leurs secteurs d'activités. Nous devons maintenir cette confiance en honorant les promesses qu'a fait le Cloud à ceux qui décident en être client. Le cloud promet :

- La haute disponibilité des services (généralement de 99,99%)
- La résilience (c'est-à-dire se réadapté à une situations pannes ou de crise du moins le temps d'apporté une solution optimale)
- Assurer des temps de réponses relativement court
- Une reprise d'activité effective
- Et une évolution avec le temps



C. Problématique

Comme nous avons su les ressortir dans la partie précédente, les enjeux sont grands d'autant plus que les affaires financières se basent sur la rapidité des échanges, et les banques n'en demandent pas moins

- Le nombre de clients augmentent
- Mais les ressources des serveurs de données s'épuisent
- Les requêtes SQL mettre du temps à retourner une réponse
- Le temps de latence des applications devient par conséquent élevé

Pour cela Notre centre d'intérêt au cours de l'acheminement de ce présent mémoire sera « **L'optimisation de l'architecture Cloud computing de CERGI SA** ». Nous devrions réussir à répondre aux grandes questions suivantes :

- Comment satisfaire les clients en garantissant la disponibilité des ressources de traitements
- Comment parvenir à un système d'information Cloud hautement disponible et réduire le temps de réponses ?
- De quelle manière assurer la tolérance aux fautes tout en assurant la sécurité de son architecture ?
- Quel mécanisme mettre en place pour permettre la scalabilité et l'évolutivité de son architecture ?

D. Intérêt du sujet

a. Objectif

Nous poursuivons des objectifs bien circonscrit, dans un marché constamment en évolution et dont l'acteur client, se fiche de savoir les causes (de quelles natures qu'elles puissent être) de la lenteur des applications, mais recherche ou dirions-nous mieux espère une grande vitesse dans ses traitements. Mais cela est tout à fait juste car il appartient au fournisseur cloud d'assurer la disponibilité et la continuité de ses services. Les institutions financières ne n'occupent en aucun moment de l'infrastructure

sous-jacente. C'est pour cela les objectifs dans le processus d'amélioration de son infrastructure cloud sont formulés de la manière qui suit :

- Assurer l'évolution des fonctionnalités des serveurs par la migration des systèmes vers leurs plus récentes versions
- Optimiser la qualité des services par une meilleure configuration de ses bases de données. (Il convient certainement de réfléchir aux solutions qui vont assurer l'intégrité des données et par-dessus tout raccourcir la durée de réponse des applications). Il faut donc veiller à :
    - La bonne gestion des ressources allouées aux instances SQL en fonction des demandes
    - L'analyse et L'amélioration des composants SSIS (SQL Server intégration Services) pour la sauvegarde et la maintenance des bases de données.
    - La réplication des bases de données, les distribués à différents emplacements et les rendre disponible en cas de défaillance ou de saturation d'une instance des bases de données
- Pour finir, Mettre en place une meilleure configuration de son architecture cloud ainsi des meilleures mesures de sécurité informatique pour protéger les données.

b. Résultats attendus

Face aux défis et aux problématiques auxquels fait face CERGI SA, les finalités dans le processus d'amélioration de son Cloud computing sont les suivantes :

Offrir une expérience utilisateur inégalée à ses clients : cela passe par l'amélioration du temps de réponse des applications.

- Procurer à son cloud une bonne flexibilité : Il convient pour se faire de migrer les serveurs vers des versions de système d'exploitation offrant plus de fonctionnalités et même en dupliquer d'autres.
- Offrir des services hautement disponibles évolutifs, et rapide, essentiellement par la configuration des mécanismes de basculement en cas de pannes, ou lenteur d'un serveur.

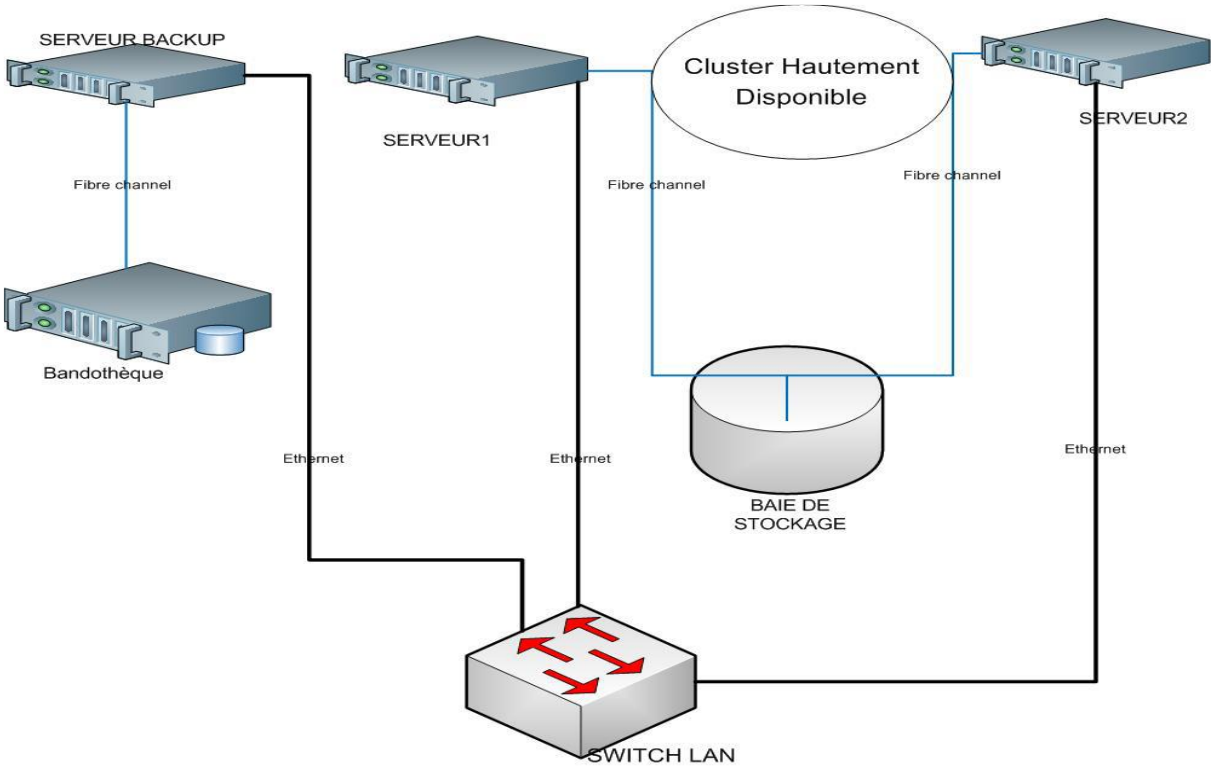
- Assurer la sécurité des données qui transitent au niveau de toute les couches réseau
- Baisser les dépenses liées au maintien de son cloud computing : en adoptant des solutions performantes et économique dans le temps.

E. Propositions de solutions

L'adoption d'une architecture de cloud hybride provoque d'énorme répercussions sur la qualité des offres de services de la société CERGI SA. Or cette dernière à la responsabilité de satisfaire un nombre sans cesse croissant de client. Il convient pour cela de proposée une solution qui pourra éradiquer ces problèmes de délai de réponse trop long, de disponibilité, de résilience, de reprise d'activité après sinistre et d'évolutivité. Pour cela avons 2 solutions en vue :

a) Première Solution : Mettre en place d'un cloud « On Premise »

Cette solution demande la prestation d'une société spécialisé dans ce domaine. Dans notre cas, nous avons sollicité la prestation de IBMC. IBMC est une entreprise spécialisée dans les Matériels informatique, les Réseaux et Télécommunication, la Sécurité incendie, Internet et Informatique/la consultation informatiques/. Cette solution consiste à mettre un place centre de donnée hautement performante et sécurisé sur un seul site suivant l'architecture logique suivante.



Le schéma ci-dessus explique l'architecture qui sera mis en place en phase de production. Il comprend entre autres :

- Deux serveurs physiques qui seront configurés dans un cluster comprenant des fonctionnalités telles que : la haute disponibilité et équilibrage de charges (avec la virtualisation) ;

- Un système de stockage pour le partage de ressources data et quorum entre les serveurs configurés dans le cluster ;

- Serveur physique destiné aux sauvegardes et archivages des données de l'environnement système ;

- Une bandothèque qui servira de support de sauvegarde physique sur bande des données.

❖ **Quelques Caractéristique**

Serveurs de production

Désignation	Spécification technique
Marque	LENOVO
Modèle	ThinkSystem SR630
Processeur	1xIntel Xeon Silver 4215 8C 2.5GHz 85W
Mémoire ram	4x32GB 2Rx8 (128 GO),
Disque dur interne	8 x ThinkSystem 2.5" 300GB 10K SAS 12Gb Hot Swap 512n HDD
Raid	RAID 930-8i 2GB Flash PCIe 12Gb Adapter
Alimentation	2x750W, XCC Enterprise
Network	ThinkSystem 1Gb 4-port RJ45 LOM
SAN	Emulex 16Gb Gen6 FC Dual-port HBA
OS	Windows Svr 2016 Standard ROK (16 core) - MultiLang

- **Routeurs**

Désignation	Spécification technique
Marque	Cisco ISR 1111X
Environnement	Enterprise branch, managed service provider (MSP), small business (SMB)
Ports	WAN 10/100/1000 Ethernet ports 8 LAN 10/100/1000 Ethernet ports 4 Ports POE 1 GE/SFP combo 1 port USB 3.0 console
Memory	DRAM : 8 GB fixed ; Flash memory : 4GB USB type A 3.0 ports
VPN	IPsec Performance: 200 Mbps for ISR 1100-8P with 150 connections Advanced Security: Zone-based firewall, IPsec VPN, Dynamic Multipoint VPN (DMVPN), FlexVPN, GETVPN.

❖ **Evaluation Financière**

Désignation	Quantité	Prix unitaire (XOF)	TOTAL (XOF)
SERVEURS DE PRODUCTION	02	5 099 815	10 199 629
SERVEUR DE SAUVEGARDE	01	5 373 261	5 373 261
BANDOTHEQUE	01	12 570 782	12 570 782
BAIE DE DISQUE	01	24 611 099	24 611 099
SWITCH SAN	02	3 362 515	6 725 030
SWITCH	01	1 072 526	1 072 526
ONDULEUR	01	2 993 412	2 993 412
RACK ET ACCESSOIRES	01	3 892 981	3 892 981
LOGICEL DE SAUVEGARDE - 5 TO	01	5 402 740	5 402 740
APPLIANCE DE SAUVEGARDE (NET BACKUP) 20 TO	01	43 560 649	43 560 649
Cisco RV345P Dual WAN Gigabit VPN Router	01	1 103 386	1 103 386
FortiWeb-400D Hardware plus 1 Year 8x5 FortiCare and FortiGuard Stand	01	10 587 962	10 587 962
Mise en oeuvre serveurs	10 jours	360 000	3 600 000
Mise en oeuvre routeur et par feu	5 jours	360 000	1 800 000
Mise en oeuvre appliance (NETBACKUP)	01 jours	5 400 000	5 400 000
Mise en oeuvre Veritas Backup Exec	05 jours	360 000	1 800 000
TOTAL HT			91 732 809
TVA			16 511 906
TOTAL TTC			**108 244 714**

b) Deuxième Solution : Amélioration de l'architecture actuelle

Cette optique peut être répartis en trois phase :

✓ Une optimisation de l'architecture matérielle

Nous appelons optimisation matérielle l'ensemble des équipements à acquérir afin d'améliorer les ressources et la sécurité des services. Nous citerons et expliquerons ultérieurement les niveaux ou chacun ces équipements entreront en applications :

- Deux (2) pare-feu

- Un (1) serveur

✓ Une optimisation de l'architecture système

D'une parte, Nonobstant la migration des serveurs existant vers une version Windows server 2016, l'un des serveurs à acquérir servira de cluster de basculement avec le serveur de base de données de l'infrastructure d'Abidjan. En effet nous mettrons en place une réplication avec Failover dans un cluster de deux serveur Actif-passif. Ainsi non seulement l'intégrité des bases de données sera assurée, les ressources allouées aux instances SQL seront équilibré offrant par conséquent une haute disponibilité et un délai moins longue dans le traitement des requêtes.

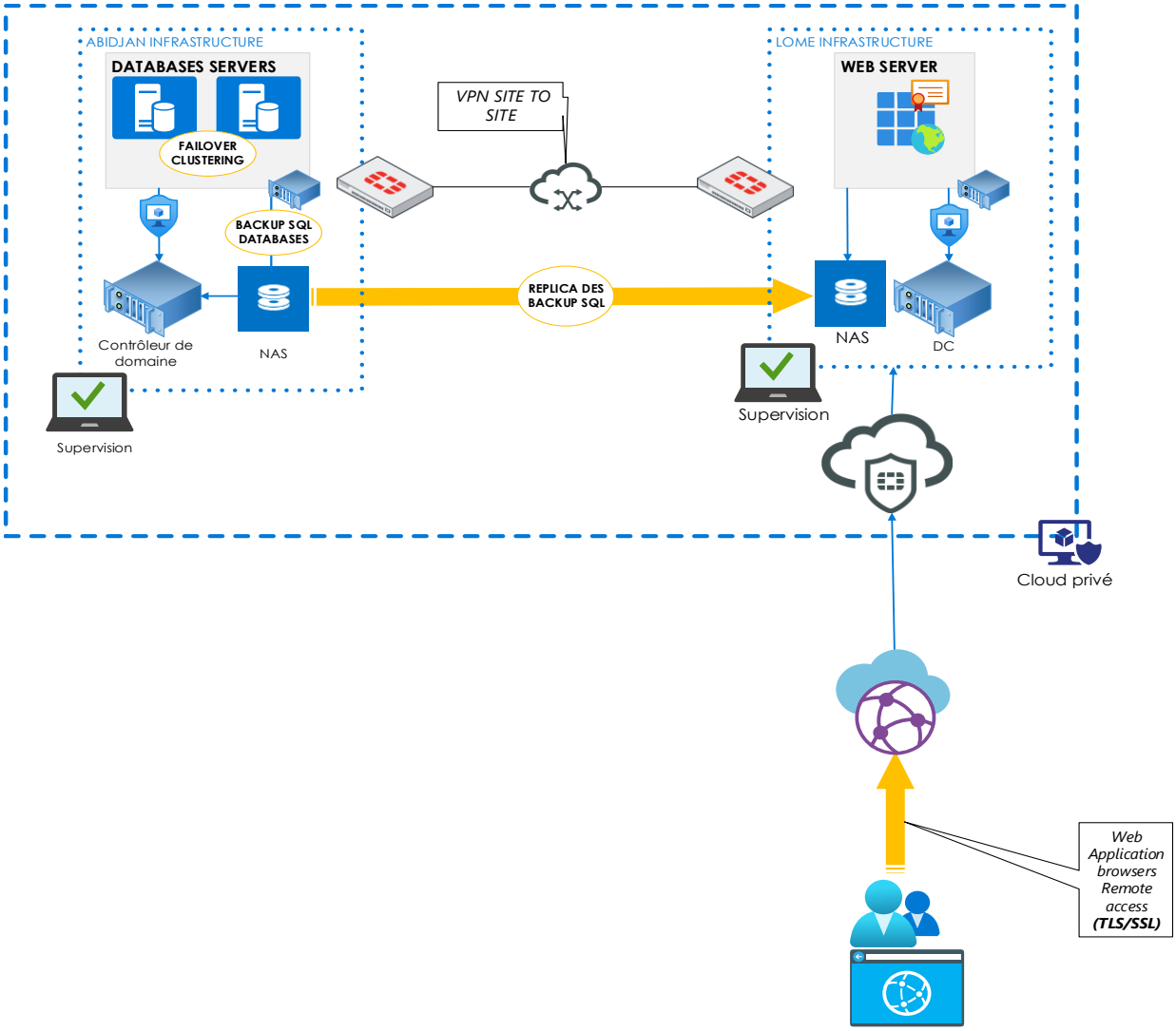
D'une autre parte, nous critiquons l'architecture hybride du cloud computing de CERGI SA, en déclarant inutile la location d'un VPS pour l'hébergement de nos applications web. La base de données est l'élément le plus important pour le fonctionnement d'une application. Et pourtant le Serveur de base de données se trouve dans l'infrastructure privé. En se réappropriant le serveur Web dans notre infrastructure privée, Nous éliminons les dépenses liées au payement de l'hébergement chez Goddady, et gagnerons en vitesse de transmission car la distance entre le serveur de base donnée et le serveur web sera moins longue donc permettra un aboutissement rapide des requetés. Nous passerons ainsi à une infrastructure de cloud exclusivement privé en transplantant le serveur web dans l'infrastructure de Lomé.

✓ L'optimisation de la sécurité

La sécurité est un l'élément d'importance majeur dans tout système d'information. Optimiser la sécurité veut dire crypté la communication entre les deux sites privés, notamment par la Configuration d'un VPN site to site et client to site. Ainsi l'échange entre les deux infrastructures sera fait de façon sécurisée sans crainte des différentes attaque cybercriminel. C'est dans scénarios s'inscrit le besoin d'acquissions de deux (2) pare-feu de nouvelle génération (NGFW) pour la configuration du site to site VPN, et la sécurisation

du trafic HTTPS entre le serveur Web et les clients par la configuration d'un Web application firewall (WAF).

- **Nouvelle Architecture cloud :** Nous parvenons à une architecture de cloud privé qui s'illustre de comme suit



- **Caractéristique de quelques équipements choisi dans cette solution**
  - **Firewall FORTIGATE 60E**

L'Appliance de sécurité pare-feu VPN Fortinet FortiGate 60E à 10 ports offre une sécurité réseau qui fonctionne sur une plate-forme unique. Il fournit une protection réseau complète qui fonctionne avec une gestion unifiée des politiques, et il fait tout à partir d'une seule vitre. Les attaques ciblées et les menaces de sécurité avancées ne sont plus un problème avec cette

appliance. L'outil est construit sur FortiASIC, un style d'architecture propriétaire qui offre un excellent débit et de faibles niveaux de latence.

FortiGate 60E

- **Serveur DELL PowerEdge T420**

Le Dell PowerEdge T420 est un puissant et serveur tour fiable à 2 sockets qui offre performances et capacité intégrée. Le T420 s'intégrer très bien dans les environnements de bureau et les centres de données. Ce serveur est un excellent choix pour un usage général pour toute charges tels que base de données, partage de fichiers, vente au détail et e-mail. Le gestionnaire des systèmes Dell OpenManage ™ comprend un Contrôleur d'accès à distance Dell intégré (iDRAC) avec Lifecycle Controller. Cette fonctionnalité intégrée aide les administrateurs informatiques à gérer les serveurs Dell de manière physique, virtuelle, locale à distance.

❖ **Evaluation financière**

Désignations	Caractéristiques	Quantité	Prix unitaire en XOF	Prix total En XOF
Serveur	DELL Xeon Silver	01	2.762.720	2.762.720
RAM	DDR4 PC4 2300 32GB	10	335.000	3.350.000
Disk Dur	SSD mu sata classic 2TB	02	230.000	460.000
Routeur	CISCO small business RV340	02	324.500	649.000
Firewall	FORTINET FORTIGATE 60E	02	772.310	1.544.620
TOTAL				8.766.340

c) Etude Comparée des solutions

Solutions	Avantages	Inconvénients
Première solution	-Elle tient compte l'ensemble du problème -Elle offre de très haute performance quittant de la haute disponibilité, en passant par la vitesse, la reprise d'activité et l'évolutivité	-Le principal inconvénient est le cout qui est très élevé
Deuxième solution	- Cette solution résout le problème de latence des applications - Elle intègre des mesures de haute disponibilité et de reprise rapide en cas de pannes - Elle améliore la confidentialité des échanges entre la région de Lomé et celle d'Abidjan - Elle permet au système d'être plus fluide à l'utilisation - Elle change l'architecture cloud la société en la fessant quitté une architecture hybride vers une architecture privé favorable à l'évolutivité - Les couts sont négligeable comparer au résultat	- Cette solution résout le problème pour un temps donné mais pas permanemment. - Des couts supplémentaires pour l'entreprise car elle demande l'acquisition de nouveau équipements informatiques,

d) Choix de solution

Nous devons faire le choix entre 2 solution toute deux performante, et résolvant considérablement notre défi. Mais la contrainte de prix se pose car l'un de nos objectifs stipule que nous devons réussir à réduire les dépenses liées aux maintien de notre infrastructure cloud. AU vue de toute ces contrainte notre choix s'est porté sur la Deuxième solutions.

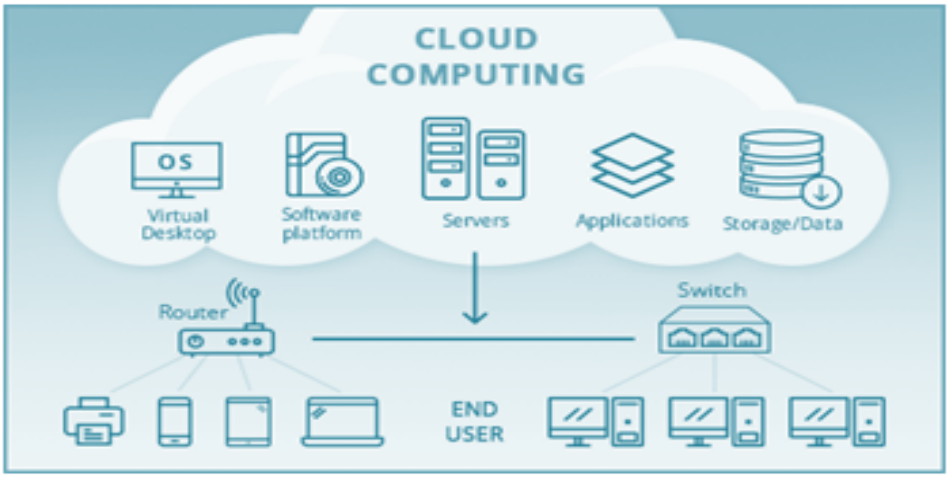
PARTIE III : GENERALITES

A. Le cloud computing : « L'informatique dans le nuage »

a) Description du cloud computing

Durant la dernière décennie, il y eut plusieurs tentatives de définitions pour le Cloud Computing. Nous donnons dans ce qui suit quelques-unes de ces définitions. Le « cloud computing » est un néologisme utilisé pour décrire l'association d'Internet (« cloud », le nuage) et l'utilisation de l'informatique (« computing »). C'est une manière d'utiliser l'informatique dans laquelle tout est dynamiquement couplé et évolutif et dans laquelle les ressources sont fournies sous la forme de services au travers d'Internet. Les utilisateurs n'ont ainsi besoin d'aucune connaissance ni expérience en rapport avec la technologie derrière les services proposés. Cette nouvelle technologie permet la mise à disposition dynamique des technologies d'information sur Internet et les présente comme services selon le modèle « pay-as-you-go ».

Wikipédia définit le Cloud comme un ensemble de services mis en réseau, offrant sur demande des plates-formes informatiques extensibles et peu chères, garantissant une certaine qualité de service, généralement personnalisée. Ces plates-formes doivent être accessibles de façon simple et continue. Dans une autre définition, les auteurs présentent le cloud computing comme un type de système parallèle et distribué, constitué d'une collection d'ordinateurs interconnectés et virtualisées et ils sont dynamiquement fournis et présentés comme une seule ou plusieurs ressources de calcul basés sur le contrat de service à niveau établi par la négociation entre le fournisseur de services et les consommateurs. Selon l'Institut national des normes et de la technologie français, Cloud computing est un modèle pour permettre un accès pratique à la demande du réseau à un ensemble partagé de ressources informatiques configurables (par exemple, les réseaux, les serveurs, le stockage, les applications et les services) qui peuvent être provisionnés rapidement et libérés avec un effort de gestion minimale ou par l'interaction de fournisseur de services.



b) Historique

Les fondations de cloud computing peuvent être retracées jusqu'aux années soixante où John McCarthy, pionnier de l'intelligence artificielle, a pour la première fois formulé l'idée d'un informatique utilitaire, en anglais utility computing. L'idée consiste à pouvoir fournir à l'utilisateur de la puissance de calcul, des capacités de stockage et des capacités de communication, de la même façon que l'on lui fournit l'´électricité ou l'eau dans les réseaux publics. Bien avant la naissance du terme de Cloud computing, les informaticiens utilisaient déjà des services de Cloud computing comme le webmail2, le stockage de données en ligne (photos, vidéos...) ou encore le partage d'informations sur les réseaux sociaux. Dans les années 90, un autre concept avait déjà préparé le terrain au Cloud computing. Il s'agit de L'ASP (Application Service Provider) qui permettait au client de louer l'accès à un logiciel installé sur les serveurs distants d'un prestataire, sans installer le logiciel sur ses propres machines. Le Cloud computing ajoute `à cette offre la notion d´élasticité avec la possibilité d'ajouter de nouveaux utilisateurs et de nouveaux services d'un simple clic de souris. Il est communément admis que le concept de Cloud Computing a été initié par le géant Amazon en 2002. Le cybermarchand avait alors investi dans un parc informatique afin de pallier les surcharges des serveurs dédiés au commerce en ligne constatées durant les fêtes de fin d'année. A ce moment-là, Internet comptait moins de 600

millions d'utilisateurs mais la fréquentation de la toile et les achats en ligne étaient en pleine augmentation. En dépit de cette augmentation, les ressources informatiques d'Amazon restaient peu utilisées une fois que les fêtes de fin d'année étaient passées. Ce dernier a alors eu l'idée de louer ses capacités informatiques le reste de l'année à des clients pour qu'ils stockent les données et qu'ils utilisent les serveurs. Ces services étaient accessibles via Internet et avec une adaptation en temps réel de la capacité de traitement, le tout facturé à la consommation. Cependant, ce n'est qu'en 2006 qu'Amazon comprit qu'un nouveau mode de consommation de l'informatique et d'internet faisait son apparition. Réalisant ce qu'ils pourraient faire de toute cette puissance, de nombreuses compagnies ont ensuite commencé à montrer un certain intérêt à échanger leurs anciennes infrastructures et applications internes contre ce que l'on appelle les "pay per-use service" (services payés à l'utilisation). Actuellement, que ce soit pour les petites, moyennes ou grandes entreprises, le Cloud Computing est devenu la solution de prédilection pour le déploiement de leurs services informatiques. Ainsi, on estime qu'actuellement 70% du trafic réseau global est imputable au Cloud, et que celui-ci va doubler et atteindre un taux de 86% en 2025.

c) Caractéristiques

Le Cloud computing se distingue des solutions traditionnelles par les caractéristiques suivantes :

- Large accessibilité via le réseau : Les services sont accessibles en ligne et sur tout type de support (ordinateur de bureau, portable, smartphone, tablette). Tout se passe dans le navigateur Internet.
- Mesurabilité du service : L'utilisation du service par le client est supervisée et mesurée afin de pouvoir suivre le niveau de performance et facturer le client en fonction de sa consommation réelle.
- Solution multi-client : Une même instance d'un logiciel est partagée par l'ensemble des clients de façon transparente et indépendante. Tous les clients utilisent la même version du logiciel et bénéficient

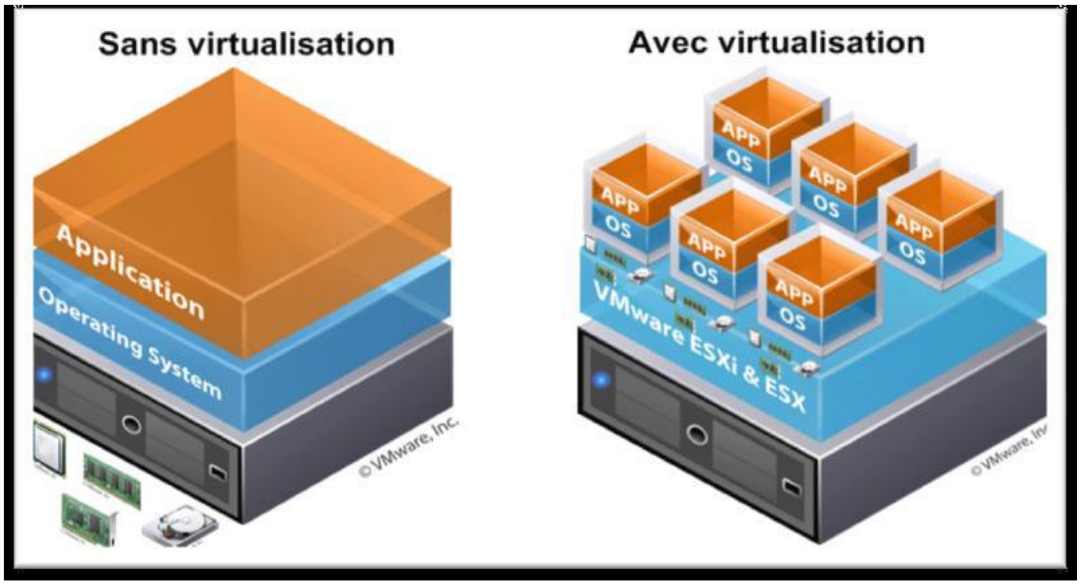
instantanément des dernières mises à jour. Chaque client dispose d'un paramétrage utilisateur qui lui est propre.

- Disponibilité à la demande : Le service peut être souscrit rapidement et rendu opérationnel automatiquement avec un minimum d'interaction avec le fournisseur.
- Elasticité immédiate des ressources : Des ressources supplémentaires peuvent être allouées au service pour assurer la continuité du service en cas de pic de charge, ou bien être réallouées `a un autre service dans le cas inverse.
- Mutualisation des ressources : Des ressources utilisées pour exécuter le service sont mutualisées pour servir à de multiples clients. Les multiples serveurs sollicités, totalement interconnectés, ne forment plus qu'une seule ressource virtuelle puissante et performante.

d) Virtualisation

C'est ensemble des techniques matérielles et/ou logiciels qui permettent de faire fonctionner simultanément sur une seule machine plusieurs systèmes d'exploitation (appelés VM). A titre d'exemple nous avons VMware, KVM, HyperV.

Plus formellement, la virtualisation fait référence à l'abstraction physique des ressources informatiques. En d'autres termes, les ressources physiques allouées à une machine virtuelle sont abstraites à partir de leurs équivalents physiques. Les disques virtuels, interfaces réseau virtuelles, réseaux locaux virtuels, commutateurs virtuels, processeurs virtuels et la mémoire virtuelle correspondent tous à des ressources physiques sur des systèmes informatiques physiques, la figure I.2 est une représentation avec et sans virtualisation



❖ **Comparaison avant et après l'apparition du Cloud Computing**

L'apparition du Cloud Computing a bouleversé le monde informatique. Cela crée un grand écart entre l'utilisation ou non de ce concept, ci-dessous un schéma illustrant les étapes de passage de l'évolution en informatique. Le tableau ci-dessus démontre une petite comparaison avant et après l'apparition du Cloud Computing

Avant l'apparition du Cloud Computing	**Apres l'apparition du Cloud Computing**
Les clients accèdent aux ressources : serveurs, applications, espaces de stockage et services via le réseau LAN ou intranet et internet. Un groupe d'ingénieurs spécialisés est nécessaire pour garantir l'installation, la configuration, la sécurité et la mise à jour du hardware et software.	Les clients accèdent à des infrastructures informatiques mises à disposition par un prestataire de Cloud via Internet. Le client ne gère aucun matériel, ni logiciels c'est le prestataire de Cloud qui sans charge. Il peut donc se concentrer avant tout sur son travail et son savoir-faire.

L'accès au serveur ou à l'application sensible se fait depuis l'intranet en passant par l'authentification et selon des droits d'accès bien défini ou depuis Internet en utilisant les VPN « Virtual Private Network ». Si le serveur ou l'application tombe en panne et s'il n'existe pas de mécanisme de reprise après panne ou de sauvegarde toutes les données seront perdues Pour faire la sauvegarde ou les backups de plusieurs serveurs cela nécessite une grande capacité de stockage Si le serveur ou l'application n'est pas bien sécurisé, il est facile a attaqué. Quand le nombre d'utilisateurs augmente dans les entreprises et les organisations…, celle-ci doit investir pour acheter plus d'équipements matériels qui peuvent être couteux. Le client paie le support même s'il ne l'utilise pas à 100%. On ne garantit pas l'accès de n'importe où car ceci représente une faille de sécurité et l'entreprise doit	L'accès au serveur ou à l'application se fait de n'importe où et avec n'importe quel périphérique avec un accès prédéfini à travers le Web. On ne se soucie pas des sauvegardes car la panne est transparente aux clients On dispose d'une capacité de stockage illimité et qui peut augmenter selon les besoins, si le client oublie de sauvegarder ses données ou de faire les backups de ces serveurs, le prestataire de Cloud s'engage à prendre en main cette tache lourde afin de ne pas tomber en panne. Le Cloud Computing garantit la sécurité à travers les mécanismes de réplication des données, plan de reprise d'activité, … Le Cloud Computing permet d'accéder plus rapidement à des ressources via un portail web et donc cela nous permet de réduire le cout d'investissement, on a plus à investir dans des équipements matériels très coûteuse en interne.

investir et acheter un grand matériel afin de garantir la haute disponibilité. La connexion internet est indispensable pour les clients qui utilisent les VPN,	Le client paie uniquement ce qu'il consomme ou par abonnement mensuel. Le Cloud Computing permet de garantir les accès et la haute disponibilité des services, se facteurs est très important pour les clients nomades.

e) Les différents services du Cloud Computing

Le Cloud Computing fournit une infrastructure, plate-forme et application comme des services, qui sont rendus disponibles comme des services payants dans un modèle " pay-as-you-go "aux consommateurs. Ces services dans l'industrie sont respectivement référencés comme Infrastructure as a Service (IaaS), Plat forme as a Service (PaaS) et le Software as a Service (Saas).

- ✓ **Le logiciel en tant que service (SaaS) :**

Est comme son nom l'indique, un modèle de fourniture de logiciels héberges à distance. L'utilisateur ne gère ni l 'infrastructure du cloud ni la plate-forme où l'application s'exécute. Plus besoin d'installer l'application sur ses propres ordinateurs, le client y accède via sa connexion Internet et n'a donc pas à mettre à jour ou à gérer le fonctionnement et la sécurité du logiciel, toutes ces taches sont effectuées par l'´éditeur (le fournisseur). Ce qui simplifie la maintenance et le support. Ces applications sont accessibles à partir de différents périphériques clients par le biais d'une interface client l´légère, comme un navigateur Web (par exemple : le courrier électronique base sur le Web), ou une interface spéciale. Parmi les exemples les plus connus, on retrouve : Google Apps, Microsoft Office, CERGI compliance.

- ✓ **Plateforme en tant que service (PaaS) :**

Les PaaS sont des services Cloud destinées aux développeurs d'applications qui leur facilitent le déploiement de leurs applications dans le cloud à l'aide d'outils (langages de programmation, bibliothèques, ...) pris en charge généralement par le fournisseur. Les développeurs n'ont donc pas accès à l'infrastructure, mais ont le contrôle sur les paramètres de configuration de leur environnement d'hébergement (serveur, base de données, ...), leur permettant ainsi de se concentrer uniquement sur le développement de leurs applications et de ne pas perdre de temps sur leur déploiement. Exemples de PaaS : Google App engine ou AppFog.

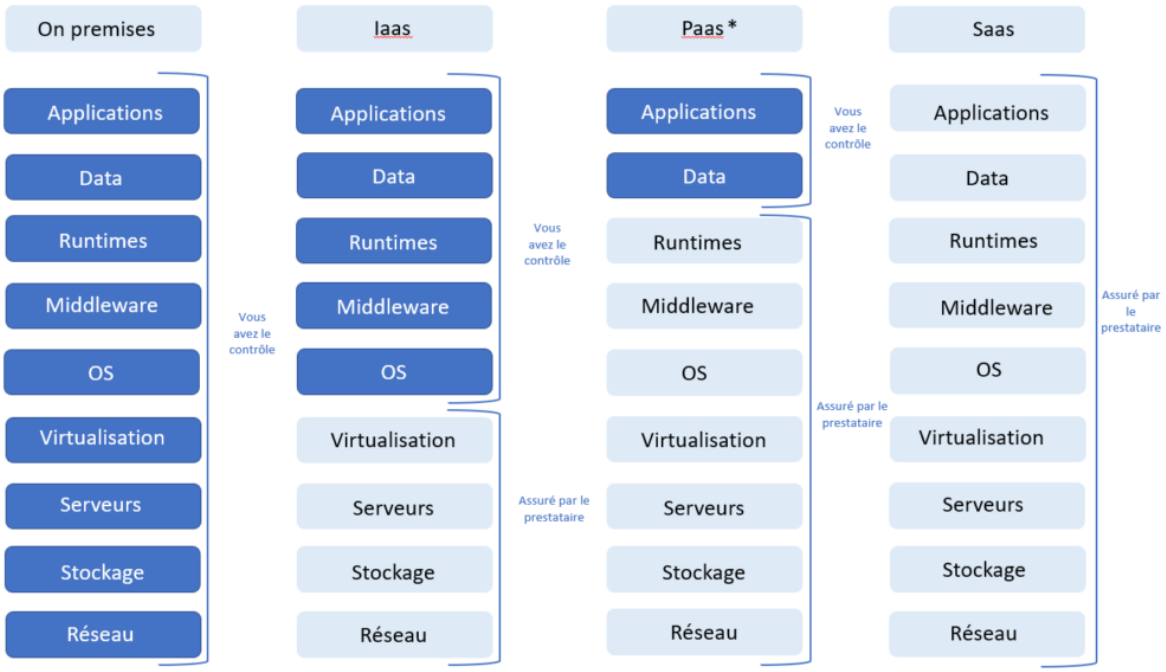
- ✓ **Infrastructure en tant que service (IaaS)**

C'est la couche la plus basse des niveaux de services Cloud. Sur une IaaS l'utilisateur gère librement son infrastructure et peut définir et contrôler précisément les serveurs qu'il utilise, le système d'exploitation, le stockage, etc. Par rapport à d'autres modèles de service, ce modèle offre un niveau de contrôle et une flexibilité élevée aux clients, mais exige un effort d'administration important. De ce fait, c'est un modèle qui est plus destiné aux architectes informatiques. Dans ce modèle de service, les fournisseurs mettent à disposition du client une ou plusieurs machines physiques ou, plus généralement, virtuelles (c.-à-d. des VMs) avec différentes capacités en calcul, en mémoire, en stockage ou en transfert réseau. Le client peut alors librement choisir les systèmes d'exploitation et les applications qu'il souhaite installer sur ces machines, et il s'occupe de leur administration Exemple d'IaaS : Amazon et son EC2 :

- ✓ **Avantages et Inconvénients des services**

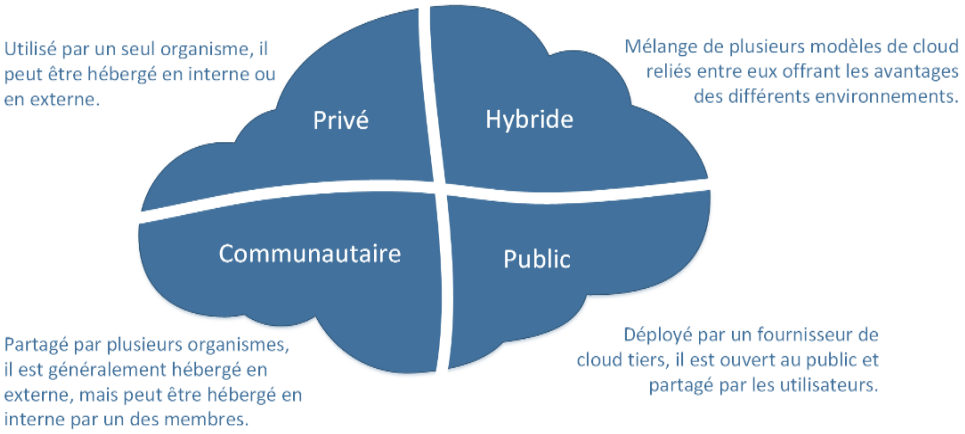
Services	Avantages	Inconvénients
SaaS	- Cela n'implique aucun matériel et aucun coût d'installation. -Le fournisseur s'occupe de tous les problèmes liés aux logiciels et à l'infrastructure.	-L'utilisateur n'a aucun contrôle sur le matériel qui s'occupe des données. -Afin de bénéficier des services SaaS pour votre

	- Facilement accessible depuis l'emplacement de votre choix où les services Internet sont disponibles. -plus de licence	entreprise, vous devez disposer d'une connectivité Internet suffisante.
PaaS	-Le processus de développement est accéléré et simplifié -Réduction des dépenses de création, de test et de lancement -les ressources peuvent être facilement augmentées ou diminuées en fonction des besoins de l'entreprise	- Dépendance à la vitesse, à la fiabilité et au support du fournisseur -Le modèle de cloud PaaS nécessite des compétences de base en codage et des connaissances en programmation pour le déployer avec succès dans le système
IaaS	- plus de flexibilité et de dynamisme - Rentable grâce à la tarification à l'utilisation -IaaS est livré avec une capacité de personnalisation élevée qui permet à l'utilisateur d'installer facilement des services cloud qu'il peut associer au centre de données de l'organisation	- Problèmes de sécurité des données dus à l'architecture mutualisée - Les pannes des fournisseurs empêchent les clients d'accéder à leurs données pendant un certain temps



f) Types de Cloud Computing

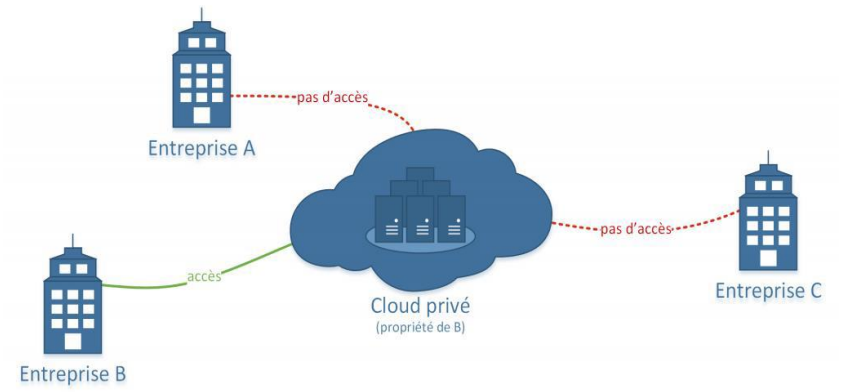
Le concept de Cloud Computing est encore en évolution. On peut, toutefois, dénombrer quatre types de Cloud Computing :



✓ Cloud privé

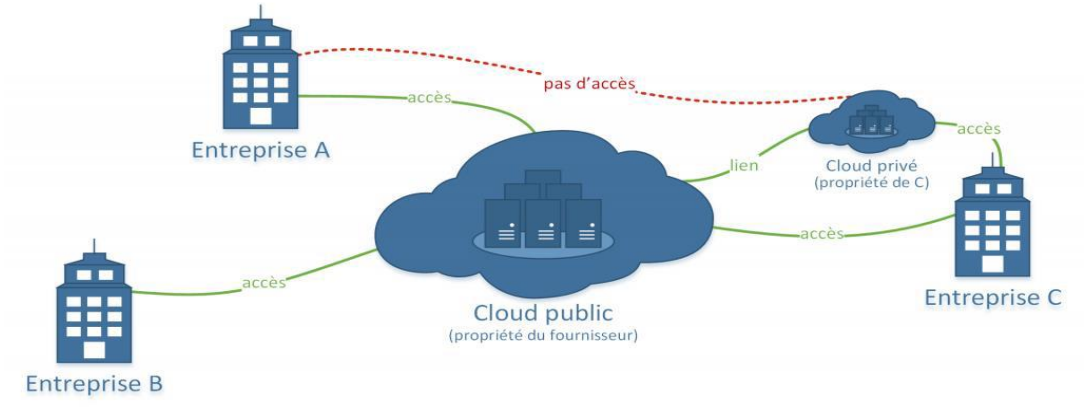
Cloud privé (également appelé Cloud interne) est un terme marketing pour une architecture informatique propriétaire qui fournit des services hébergés à un nombre limité de personnes derrière un pare-feu. Typiquement, les Clouds privés sont mis en application au centre de traitement des données de

l'entreprise et contrôlés par les ressources internes. Un Cloud privé maintient les données de corporation dans les ressources sous la commande du tutelle légale et contractuelle de l'organisation.



✓ Cloud public

Cloud public (ou Cloud externe) est un modèle standard du Cloud Computing, dans lequel un prestataire de services met des ressources, telles que les applications et le stockage, à la disposition du grand public sur Internet. Les services de ce Cloud peuvent être gratuits ou offerts sur un modèle de payer-par-utilisation. L'un des principaux avantages de ce type de Cloud est que la mise en place est facile et peu couteuse parce que le matériel, l'application et les coûts de bande passante sont couverts par le fournisseur. Les Clouds externes sont connus aussi pour leur évolutivité pour répondre aux besoins.



Quelque fournisseur de cloud public

Amazon Web Services

AWS (Amazon Web Services) est une plateforme de cloud computing complète et évolutive, lancé en lancé en 2006 à partir de l'infrastructure interne créée par Amazon.com pour gérer ses opérations de vente au détail en ligne. AWS a été l'une des premières entreprises à introduire un modèle de cloud computing payant à l'utilisation qui évolue pour fournir aux utilisateurs le calcul, le stockage ou le débit selon leurs besoins. Amazon Web Services fournit des services à partir de dizaines de centres de données répartis dans les zones de disponibilité (AZ) des régions du monde entier.

Microsoft Azure

Concurrent direct d'AWS, Microsoft a créé son Cloud public Azure11 par-dessus Windows Server et Hyper-V. Cette proximité logicielle facilite la migration des VMs entre les Data Centers locaux et Azure. Il est possible également de connecter ce dernier à votre réseau d'entreprise via un VPN point à point.

Sur le marché de l'IaaS, l'approche de Microsoft est complète, surtout après le lancement d'Azure Stack, sa plateforme de déploiement de Cloud hybride.

Microsoft a défini 17 régions pour Azure, situées un peu partout aux États-Unis, en Europe, en Asie, en Amérique du Sud et en Australie.

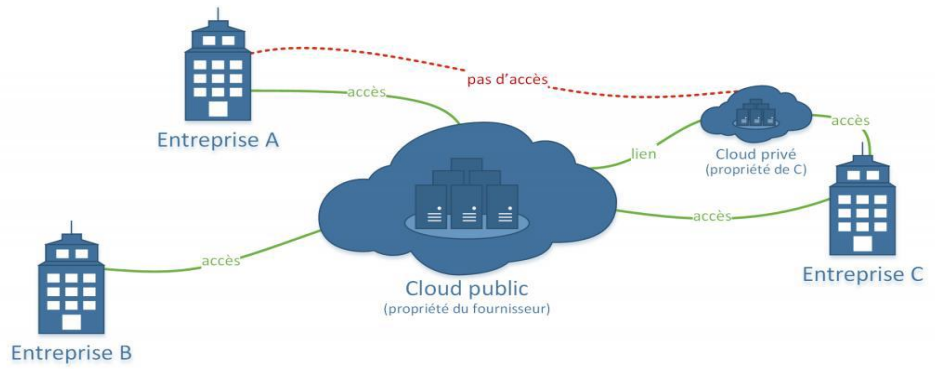
Google

Google Compute Engine offre toutes les fonctionnalités de base de la connectivité réseau d'un Cloud, directement ou via un VPN. Mais il ne prend pas en charge les migrations des VM dans le Cloud Google Compute Engine. Il est nécessaire de passer par des fournisseurs tiers.

Google permet de choisir les régions d'hébergement des VM. Le géant a des Datacenters en Europe (Belgique, Royaume-Uni, Allemagne, Pays-Bas et Finlande).

- ✓ **Cloud hybride**

Pour rencontrer les avantages des deux approches, de nouveaux modèles d'exécution ont été d'enveloppées pour combiner les Clouds publics et privés dans une solution unifiée, c'est les Clouds hybrides. Les entreprises peuvent par exemple effectuer des tâches très importantes ou des applications sensibles sur le Cloud privé, et utiliser le Cloud public pour les tâches nécessitant une scalabilité des ressources. L'objectif du Cloud hybride est de créer un environnement unifié, automatisé et scalable tirant avantage des infrastructures de Cloud public tout en maintenant un contrôle total sur les données

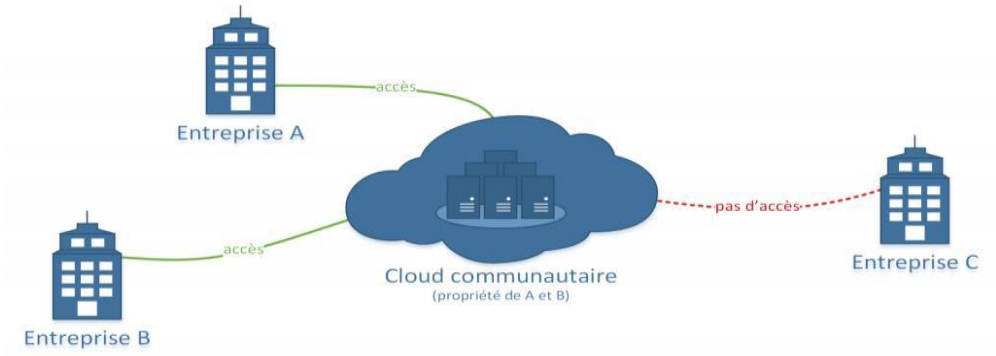


- ✓ **Cloud communautaire**

C'est un nouveau type du Cloud plus récent, qui est multi-tenant[16] partagé entre plusieurs entreprises, il est régi, géré et sécurisé par un groupe de participants ou par un fournisseur de service. Le Cloud communautaire est sous

forme hybride de plusieurs Clouds privés interconnectés sans ouverture vers l'extérieur. [12]

Exemple : des hôpitaux partageant des dossiers de patients, un logiciel de gestion mutualisé … etc.



B. Les grands défis relatifs à l'adoption du Cloud Computing

Le Cloud Computing a connu un succès rapide notamment du fait qu'il permette aux clients de réaliser une économie d'échelle importante en payant uniquement pour les ressources utilisées tout en déléguant la gestion de l'infrastructure au fournisseur. Cependant, il existe encore un nombre important de défis inhérents à l'adoption du Cloud Computing

a) Tolérance aux fautes et disponibilité

Le fournisseur Cloud est censé fournir à ses clients un environnement tolérant aux fautes où le client ne risque ni de perdre ses données, ni de voir l'exécution de ses applications perturbées. De même, une certaine disponibilité doit être garantie pour les services Cloud. Ainsi, l'exécution des applications déployées dans le Cloud doit être continuelle, et le client doit avoir à tout moment avoir ses applications accessibles pour l'utilisation.la mise en œuvre de la tolérance aux fautes se fait par une politique de backup(sauvegarde) ou de réplication de données, et la disponibilité implique la mise en place des mécanismes de répartition de charge des serveurs.

❖ **La sauvegarde**

Le dicton « il faut toujours avoir un plan de secours » est plus vrai que jamais quand on parle de service cloud computing. Le sauvegarde de données informatiques devrait être une routine enracinée chez un fournisseur cloud pour éviter une perte de produit de travail précieux et d'argent. Les fournisseurs de système de sauvegarde gèrent leur sauvegarde chacun à leur manière car il existe en fait, plus de 10 types de sauvegardes différents. Mais les 4 principaux sont les suivantes :

- La sauvegarde complète

Elle copie l'ensemble des données à chaque fois qu'une sauvegarde est lancée. Elles offrent donc le plus haut niveau de protection. Cependant, la plupart des entreprises ne peuvent pas se permettre d'effectuer des sauvegardes complètes fréquemment, car elles risqueraient de mobiliser le réseau trop longtemps et consommeraient une trop grande capacité de stockage.

- La sauvegarde incrémentale

Elle n'enregistre que les données qui ont été modifiées ou mises à jour depuis la précédente sauvegarde. Cette méthode permet d'économiser du temps et de l'espace de stockage, mais peut compliquer la réalisation d'une restauration complète. La sauvegarde incrémentale est une forme courante de sauvegarde en cloud, car elle tend à utiliser moins de ressources.

- La sauvegarde différentielle

Elle est similaire à la sauvegarde incrémentale, car elle ne contient que les données qui ont été modifiées. Cependant, les sauvegardes différentielles enregistrent les données qui ont été modifiées depuis la dernière sauvegarde complète, plutôt que la dernière sauvegarde en général. Cette méthode simplifie les restaurations.

- La sauvegarde Miroir (Mirroring)

Une sauvegarde miroir, est une réplique exacte sur un autre disque dur de tout ce qui se trouve sur le disque dur de notre serveur, le système d'exploitation, les informations de démarrage, les applications et des fichiers cachés à nos préférences et paramètres les bases de données, tout ce dont nous avons besoin pour redémarrer notre système telle qu'il était.

Avantages :

Les données étant copiées sur plusieurs disques, il existe une redondance complète des informations. En cas de perte d'un disque, on peut retrouver les données intégralement à partir d'un autre disque.

Les données étant dupliquées sur plusieurs disques, il sera possible d'accéder simultanément aux 2 unités d'où une amélioration des performances en lecture.

La mise en place d'une telle méthode est très flexible.

Inconvénients :

Les accès en écriture sont ralentis, chaque donnée étant inscrite sur chaque disque.

Perte de l'espace disque, au moins 50% étant réservé à la duplication.

b) L'équilibrage de charge

L'équilibrage de charge est un élément important lors de la mise en place de services amenés à croître. Il faut s'assurer que la capacité à monter en charge soit la plus optimale possible afin d'éviter toute dégradation que ce soit en termes de performances ou de fiabilité lors d'affluences importantes.

Le principe de base de l'équilibrage de charge (**Load Balancing**) consiste à effectuer une distribution des tâches à des machines de façon intelligente.

Les objectifs de l'équilibrage de charge sont les suivantes :

- Amélioration des temps de réponse des services.

- Capacité à pallier la défaillance d'une ou de plusieurs machines,
- Ajout de nouveaux serveurs sans interruption de service

Problème de l'équilibrage de charge

Le problème de l'équilibrage étant un problème relativement ancien, beaucoup d'approches ont été proposées pour le résoudre. ***Casavant*** *et* ***Kuh****l* ont défini une taxonomie largement adoptée par la communauté scientifique dont les principales classes sont :

- ***Approche Statique Vs. Approche Dynamique***

Dans une approche statique, les tâches sont assignées aux machines avant l'exécution de l'application qui les contient. Les informations concernant le temps d'exécution des tâches et les caractéristiques dynamiques des machines sont supposées connues a priori. Cette approche est efficace et simple à mettre en œuvre lorsque la charge de travail est au préalable suffisamment bien caractérisée.

Dans une approche dynamique, l'assignation des tâches aux machines se décide durant la phase d'exécution, en fonction des informations qui sont collectées sur l'état de charge du système. Ceci permet d'améliorer les performances d'exécution des tâches mais au prix d'une complexité dans la mise en œuvre de cette stratégie, notamment en ce qui concerne la définition de l'état de charge du système, qui doit se faire de manière continue.

- **Approche Centralisée Vs. Approche Distribuée**

Dans une approche centralisée, un site du système est choisi comme coordinateur. Il reçoit les informations de charge de tous les autres sites qu'il assemble pour obtenir l'état de charge global du système.

Dans le cas d'une approche distribuée, chaque site du système est responsable de collecter les informations de charge sur les autres sites et de les rassembler pour obtenir l'état global du système. Les décisions de placement de tâches sont prises localement, étant donné que tous les sites ont la même perception de la charge globale du système.

- **Approche Source-Initiative Vs. Receveur-Initiative**

L'approche source- initiative est appliquée lorsqu'un site, appelé source, détecte qu'il a une surcharge de travail et qu'il cherche à transférer le surplus vers un site faiblement chargé. L'approche receveur initiative s'applique lorsqu'un site faiblement chargé, appelé receveur, demande à recevoir tout ou partie du surplus des sites surchargés.

Algorithmes d'équilibrage de charge

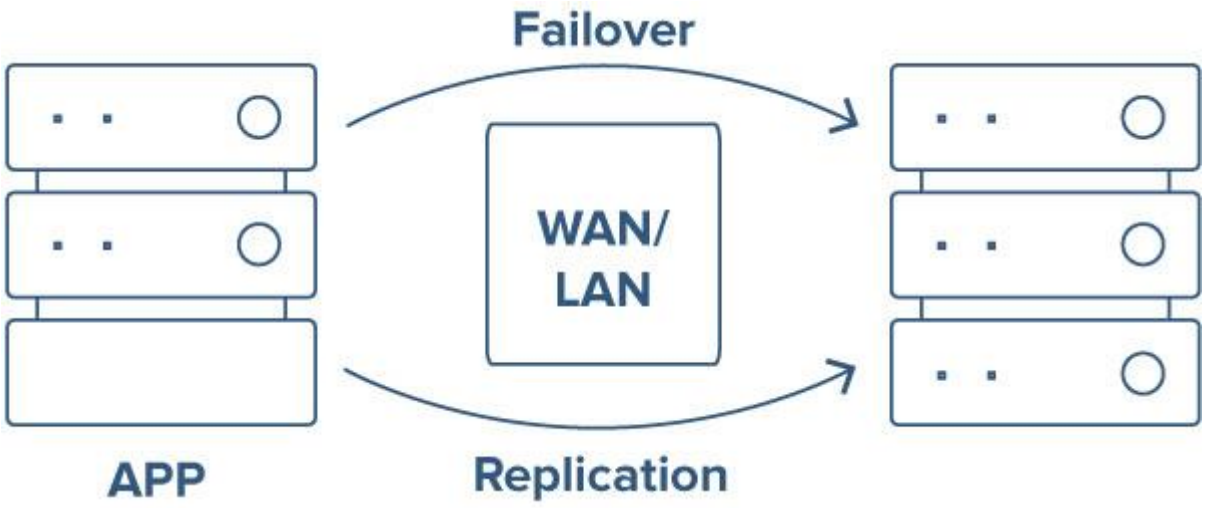
Divers algorithmes d'équilibrage de charge offrent divers avantages, le choix de la méthode d'équilibrage de charge dépend de chaque exigence:

- **Round Robin :** Il s'agit de la méthode la plus simple pour équilibrer la charge des serveurs ou pour fournir une tolérance aux pannes simple. Plusieurs serveurs identiques sont configurés pour fournir précisément les mêmes services ou applications. Tous sont configurés pour utiliser le même nom de domaine Internet, mais chacun possède une adresse IP unique. L'équilibreur de charge a une liste de toutes les adresses IP uniques associées au nom de domaine Internet. Lorsque des demandes de sessions sur les serveurs associés au nom de domaine Internet sont reçues, elles sont allouées de manière aléatoire ou séquentielle rotative. Par exemple, la première demande obtient l'adresse IP du serveur 1, la deuxième demande l'adresse IP du serveur 2, et ainsi de suite, les demandes recommençant au serveur 1 lorsque tous les serveurs ont reçu une demande d'accès pendant un cycle.
- **Least Connections :** c'est un algorithme d'équilibrage de charge dynamique dans lequel les demandes des clients sont distribuées au serveur d'applications avec le moins de connexions actives au moment de la réception de la demande du client.
- **IP Hash :** L'adresse IP du client est utilisée pour décider de quel serveur reçoit la demande.

c) Le Clustering de basculement (Failover clustering)

Un Failover Clustering est un ensemble de serveurs informatiques qui fonctionnent ensemble pour fournir une haute disponibilité (HA) ou une disponibilité continue (CA). Si l'un des serveurs tombe en panne, un autre nœud du cluster peut assumer sa charge de travail avec un temps d'arrêt minimal ou nul via un processus appelé basculement. Certains clusters de basculement utilisent uniquement des serveurs physiques, tandis que d'autres impliquent des machines virtuelles (VM)

L'objectif principal d'un cluster de basculement est de fournir une autorité de certification ou une haute disponibilité pour les applications et les services. Également appelés clusters à tolérance de panne, les clusters CA permettent aux utilisateurs finaux de continuer à utiliser des applications et des services sans rencontrer de délais d'attente en cas de défaillance d'un serveur. Avec les clusters HA, d'un autre côté, un utilisateur peut subir une brève interruption de service, mais le système se rétablira automatiquement sans perte de données et sans temps d'arrêt minimum



Fonctionnement des clusters de basculement

Alors que les clusters de basculement CA sont conçus pour une disponibilité de 100%, les clusters HA tentent une disponibilité de 99,999%, également

connue sous le nom de « heartbeat », pour des temps d'arrêt ne dépassant pas 5,26 minutes par an. Cependant, en contrepartie de leur plus grande disponibilité, les clusters CA sont plus coûteux à implémenter, en raison des exigences matérielles accrues.

Dans un cluster de basculement, des groupes de serveurs indépendants sont faiblement couplés pour partager des ressources et des données dans tout le système. Tous les nœuds d'un cluster de basculement ont accès au stockage partagé. Les clusters à haute disponibilité incluent également une connexion de surveillance que les serveurs utilisent pour vérifier le « battement de cœur » ou la santé les uns des autres. Au moins l'un des nœuds d'un cluster est actif, tandis qu'au moins un est passif.

Dans une configuration simple à deux nœuds, par exemple, si le nœud 1 échoue, le nœud 2 utilise la connexion Heartbeat pour reconnaître l'échec, puis se configure comme nœud actif. Le logiciel de clustering installé sur chaque nœud du cluster garantit que les clients se connectent à un nœud actif.

Certains logiciels de gestion de cluster fournissent une haute disponibilité aux machines virtuelles (VM) en les regroupant ainsi que les serveurs physiques sur lesquels elles résident dans un cluster. En cas de panne, les machines virtuelles de l'hôte défaillant sont redémarrées sur d'autres hôtes.

Le stockage partagé présente un risque en tant que point de défaillance unique potentiel. Cependant, l'utilisation de RAID 6 avec RAID 10 peut aider à garantir que le service continuera même en cas de panne de deux disques durs.

- **Reprise après sinistre**

La reprise après sinistre est une autre application pratique des clusters de basculement. Bien entendu, il est fortement recommandé que les serveurs de basculement soient hébergés sur des sites distants pour prévenir le cas où un sinistre tel qu'un incendie ou une inondation prendrait tout le matériel et les logiciels physiques du centre de données principal. Dans Windows Server 2016 et 2019, par exemple, Microsoft fournit la réplication de stockage, une

technologie permettant la réplication des données entre serveurs pour la reprise après sinistre. La technologie comprend une fonction de « basculement étendu » pour les clusters de basculement couvrant deux sites géographiques.

- **Réplication de base de données**

La réplication des bases de donnée est une technologie permettant de copier et de distribuer des données et des objets de base de données d'une base de données à une autre, puis de se synchroniser entre les bases de données pour maintenir la cohérence et l'intégrité des données. La réplication SQL Server est utilisée pour copier et synchroniser les données en continu ou elle peut également être planifiée pour s'exécuter à des intervalles prédéterminés. Il existe plusieurs techniques de réplication différentes qui prennent en charge diverses approches de synchronisation des données ; une manière ; un-à-plusieurs ; plusieurs à un ; et bidirectionnel, et maintenez plusieurs ensembles de données synchronisés les uns avec les autres.

La Réplication Transactionnelle SQL Server

L'architecture de la réplication SQL Server repose sur les différentes techniques qui permettent de copier et de distribuer les données des différents objets d'une base de données vers une autre. SQL Server propose trois types de réplication :

- La réplication transactionnelle (Transactional Replication).
- La réplication de capture instantanée (Snapshot Replication).
- La réplication par fusion (Merge Replication).

La réplication transactionnelle est généralement utilisée dans un environnement serveur à serveur pour répondre aux besoins suivants :

- Redondance des données sur un ou plusieurs serveurs qui se trouvent sur le même site ou sur des sites différents.
- Utilisation du serveur abonné comme un serveur de reporting et de lecture seule.
- Consolidation des données sur un serveur central en provenance de plusieurs sites distants.

- Besoin d'avoir un serveur abonné mis à jour en quasi temps réel avec le serveur de publication.
- La volumétrie et l'activité de la base est très importante, dans ce cas la réplication par capture instantanée peut prendre longtemps et verrouille à chaque fois l'accès aux données sur la base de publication.
- Réplication vers un serveur non-SQL Server, comme Oracle ou Sybase.

Principe de fonctionnement :

La réplication transactionnelle commence en général par une capture instantanée des objets et des données de la base à publier. Une fois la première capture effectuée, toutes les modifications effectuées sur les schémas et les données de la base de publication sont transmis au fur et à mesure (presque en temps réel) aux différents abonnés. Les changements et les transactions produites sur le serveur de publication sont appliqués dans le même ordre sur les abonnés, donc la cohérence des données est garantie par le mécanisme de la réplication. La réplication transactionnelle est effectuée par différents agents :

- Agent de capture instantanée (Snapshot)
- Agent de lecture du journal de transaction
- Agent de distribution.

Types de cluster de basculement

- **Clusters de basculement VMware**

Parmi les produits de virtualisation disponibles, VMware propose plusieurs outils de virtualisation pour les clusters de VM .vSphere 6 Fault Tolerance fournit une architecture CA qui réplique exactement une machine virtuelle VMware sur un hôte physique alternatif en cas de panne du serveur hôte principal.

Un deuxième produit, VMware HA, suit l'approche consistant à fournir une haute disponibilité pour les machines virtuelles en les regroupant ainsi que leurs hôtes dans un cluster pour un basculement automatique. L'utilisation de

VMware HA en conjonction avec le Distributed Resource Scheduler (DRS) de VMWare ajoute un équilibrage de charge, pour un rééquilibrage plus rapide des machines virtuelles après que VMware HA a déplacé les machines virtuelles vers d'autres hôtes.

- **Cluster de basculement Windows Server (WSFC)**

Nous pouvons créer des serveurs de basculement Hyper-V à l'aide de WFSC, une fonctionnalité de Windows 2016 et 2019 qui surveille les serveurs physiques en cluster, fournissant un basculement si nécessaire. WFSC surveille également les rôles en cluster, anciennement appelés applications et services en cluster. Si un rôle en cluster ne fonctionne pas correctement, il est redémarré ou déplacé vers un autre nœud.

WFSC inclut la technologie CSV (Cluster Shared Volume) précédente de Microsoft pour fournir un espace de noms cohérent et distribué pour accéder au stockage partagé à partir de tous les nœuds. En outre, WSFC prend en charge le stockage de partage de fichiers CA pour les machines virtuelles de cluster SQL Server et Microsoft Hyper-V. Il prend également en charge les rôles HA s'exécutant sur des serveurs physiques et des machines virtuelles de cluster Hyper-V. Voici un diagramme de cluster Hyper-V.

- **Clusters de basculement SQL Server**

Dans SQL Server 2017, Microsoft a présenté Always On, une solution haute disponibilité qui utilise WSFC comme technologie de plate-forme, enregistrant les composants SQL Server en tant que ressources de cluster WSFC. Selon Microsoft, les ressources associées sont combinées dans un rôle qui dépend d'autres ressources WSFC. WSFC peut ensuite identifier et communiquer la nécessité de redémarrer une instance SQL Server ou de la basculer automatiquement vers un nœud différent.

- **Clusters de basculement RedHat Linux**

Les fabricants de systèmes d'exploitation autres que Microsoft fournissent également leurs propres technologies de cluster de basculement. Par exemple, les utilisateurs de Red Hat Enterprise Linux (RHEL) peuvent créer des

clusters de basculement HA avec le module complémentaire High Availability et le système de fichiers global Red Hat (GFS / GFS2). Une assistance est fournie pour les clusters extensibles à cluster unique couvrant plusieurs sites ainsi que pour les clusters multi-sites « tolérants aux catastrophes ». Les clusters multi-sites utilisent généralement la réplication de stockage de données compatible SAN (Storage Area Network).

d) La sécurité

- **Les New Generation Firewall (NGFW)**

Qu'est-ce qu'un pare-feu de nouvelle génération (NGFW) ?

Un pare-feu de nouvelle génération (NGFW) est plus puissant qu'un pare-feu traditionnel. Les NGFW ont les capacités des pares-feux traditionnels, mais ils ont également une multitude de fonctionnalités supplémentaires pour répondre à une plus grande variété de besoins organisationnels et bloquer plus de menaces potentielles. Ils sont appelés « nouvelle génération » pour les différencier des anciens pares-feux qui n'ont pas ces capacités.

Que fait un pare-feu ?

Un pare-feu est un produit de sécurité qui surveille et contrôle le trafic réseau en fonction d'un ensemble de règles de sécurité. Les pares-feux peuvent être des applications logicielles installées sur un serveur ou un ordinateur, ou des appareils matériels physiques qui se connectent à un réseau interne. Les pares-feux se situent généralement entre un réseau de confiance et un réseau non de confiance. Souvent, le réseau de confiance est le réseau interne d'une entreprise, et le réseau non de confiance est Internet.

Les capacités typiques d'un pare-feu traditionnel comprennent le filtrage de paquets, l'inspection dynamique, le proxying, le blocage IP, le blocage des noms de domaine et le blocage des ports.

Le filtrage de paquets fait référence à la possibilité de filtrer le trafic réseau potentiellement dangereux. Toutes les données qui transitent sur un réseau (comme Internet) sont divisées en plus petits fragments appelés paquets. Un

pare-feu peut examiner chaque paquet individuel et, s'il correspond à certaines règles prédéterminées, l'empêcher d'entrer ou de sortir d'un réseau interne.

L'inspection avec état place le filtrage des paquets à un niveau plus profond. Grâce à l'inspection avec état, les pares-feux peuvent examiner les paquets de données dans le contexte d'autres paquets qui ont traversé le pare-feu. Un paquet de données peut sembler inoffensif en soi, mais s'il se dirige vers une destination inhabituelle au sein du réseau, il peut être malveillant. (Par exemple, une requête SQL n'est pas malveillante en soi, mais si elle est envoyée via un formulaire web, elle peut faire partie d'une attaque par injection SQL.)

Un proxy dans un réseau fait référence à une machine qui envoie ou reçoit du trafic réseau au nom d'une autre machine. Un pare-feu peut agir en tant que proxy en effectuant des demandes et en recevant des réponses du réseau au nom des appareils utilisateur sur son réseau interne, filtrant les données malveillantes avant qu'elles n'aient la possibilité d'atteindre ces appareils.

Le blocage des noms de domaines et des adresses IP signifie que le pare-feu peut empêcher complètement aux utilisateurs d'accéder à certains sites web ou applications.

Le blocage des ports permet aux pares-feux de filtrer certains types de trafic réseau. Dans les réseaux, un port est un endroit où une connexion entre une machine et une autre machine se termine. Les ports sont virtuels ou basés sur des logiciels et ne correspondent pas aux composants physiques de la machine. Certains ports sont réservés à certains types de connexions réseau : les connexions HTTPS, par exemple, ont lieu sur le port 443.

Quelles fonctionnalités différencient un pare-feu de nouvelle génération d'un pare-feu traditionnel ?

Les NGFW ont toutes les fonctionnalités ci-dessus. Mais au-delà, ils incluent des technologies qui n'étaient pas disponibles dans les produits de pare-feu antérieurs :

- Système de prévention des intrusions (IPS) : un système de prévention des intrusions détecte et bloque activement les cyberattaques. La différence est la même qu'entre un gardien de sécurité qui patrouille activement dans un bâtiment, et un gardien statique qui se trouve à côté de l'entrée principale.

- Inspection approfondie des paquets (DPI) : les anciens pares-feux inspectent généralement uniquement les en-têtes* des paquets de données qui transitent. Les NGFW inspectent à la fois les en-têtes de paquets de données et la charge utile des paquets, afin de mieux détecter les logiciels malveillants et autres types de trafic malveillant. Cela ressemble un peu à un point de contrôle de sécurité où les agents de sécurité inspectent réellement le contenu des bagages d'une personne, au lieu de lui demander simplement de déclarer aux agents les articles que ses bagages contiennent
- Contrôle des applications : en plus d'analyser le trafic réseau, les NGFW peuvent identifier les applications d'où provient le trafic. Sur cette base, les NGFW peuvent contrôler les ressources auxquelles différentes applications peuvent accéder ou bloquer complètement certaines applications.
- Intégration d'annuaires : les annuaires d'utilisateurs permettent aux équipes internes d'une organisation de suivre les privilèges et autorisations dont dispose chaque utilisateur. Certains NGFW peuvent filtrer le trafic réseau ou les applications en fonction de ces répertoires d'utilisateurs internes. Si un utilisateur n'est pas autorisé à accéder à une certaine application, cette application est bloquée pour cet utilisateur par le pare-feu, même si l'application n'est pas identifiée comme malveillante.
- Inspection du trafic chiffré : certains NGFW peuvent déchiffrer et analyser le trafic chiffré avec SL/TLS. Un pare-feu est capable de le faire en agissant en tant que proxy pour le processus TLS. Tout le trafic vers et

depuis le site web est déchiffré par le pare-feu, analysé et chiffré à nouveau. Du point de vue de l'utilisateur, cette fonction proxy est pratiquement transparente et l'utilisateur peut interagir avec des sites web HTTPS sécurisés comme d'habitude.

Quelques exemples de pares-feux de nouvelle génération

- ✓ **Fortinet FortiGate**

Les pares-feux NGFW milieu de gamme FortiGate offrent des performances optimales, une sécurité multicouche et une visibilité plus précise, autant d'atouts pour se protéger plus simplement des cyber-attaques. Les pares-feux FortiGate, conçus avec des processeurs de sécurité dédiés, visent l'excellence en matière de protection contre les menaces et de sécurité du trafic http, SSL… En apportant une visibilité granulaire sur les applications, les utilisateurs et les objets connectés, ses Appliance nous aident à identifier les incidents de manière rapide et intuitive

- ✓ **Juniper Networks SRX Firewall**

Les pares-feux de nouvelle génération de Juniper Networks SRX utilisent les informations du service cloud Juniper Sky Advanced Threat Protection et des flux GeoIP tiers pour bloquer les activités malveillantes lorsqu'elles entrent ou traversent le réseau. Il offre également une visibilité et un contrôle des applications, des politiques IPS et des applications basées sur l'utilisateur, ainsi

qu'une gestion unifiée des menaces (UTM) pour protéger et contrôler nos actifs d'entreprise.

- ✓ **Palo Alto Networks**

Les pares-feux de nouvelle génération de Palo Alto Networks sont tous basés sur une architecture à passage unique cohérente. Gartner a reconnu Palo Alto Networks en tant que leader pour la septième fois dans son Magic Quadrant 2018 pour les pares-feux de réseau d'entreprise, le mieux placé en termes de capacité d'exécution et le plus complet de vision pour les pares-feux de réseau d'entreprise.L'intégration de Palo Alto avec le service de sécurité mobile GlobalProtect étend la sécurité basée sur des politiques aux appareils mobiles (qu'ils soient sur site ou à distance). L'intégration avec les services de renseignement sur les menaces permet de mettre à jour les informations du pare-feu (par exemple, les catégories d'URL, les signatures de menaces). Les pares-feux de nouvelle génération de la série PA de Palo Alto réduisent les temps de réponse grâce à des actions automatisées basées sur des politiques, et vous pouvez automatiser les flux de travail via l'intégration avec des outils administratifs, tels que les services de billetterie, ou tout système avec une API RESTful.

:

PARTIE IV : MISE EN ŒUVRE

A. Les différentes installations et configurations

a) Windows server 2016

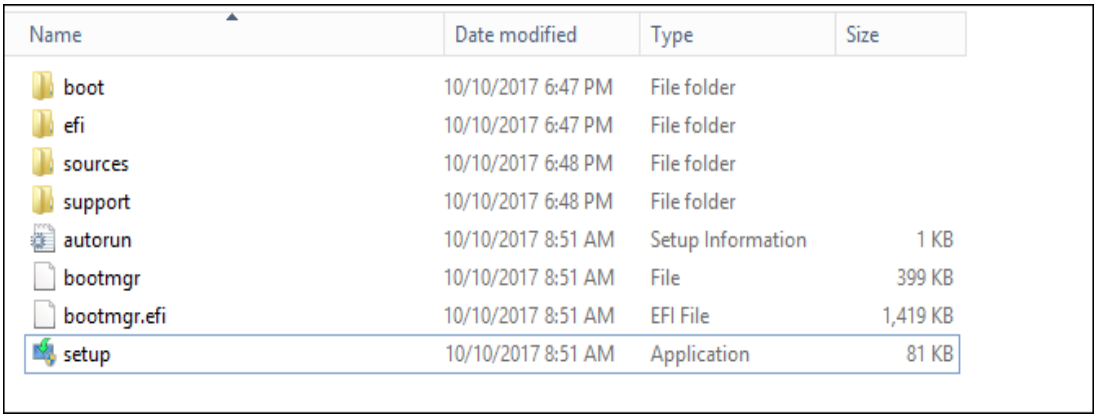
La version Datacenter du système d'exploitation Windows server 2016 x64 Langue : English fut installé en guise de migration des serveurs suivants : base données , contrôleur de domaine , stockage .Le fichez ISO est disponible sur le site officiel de Microsoft : https://www.microsoft.com/.

Prérequis

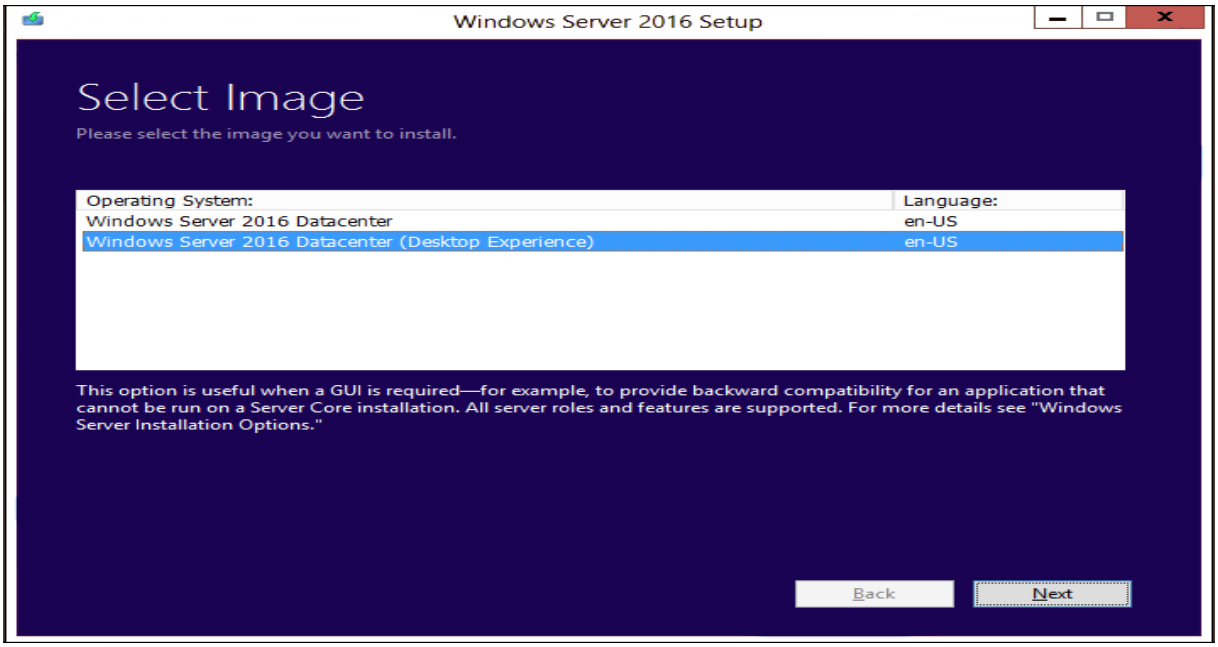
- Ouvrons une invite de commandes, accédons à c:\Windows\system32, puis tapons systeminfo.exe.
- Copions, collons et stockons les informations système résultantes quelque part hors de notre appareil.
- Tapons **ipconfig / all** dans l'invite de commande, puis copions et collons les informations de configuration résultantes dans le même emplacement que ci-dessus.
- Ouvrons l'Éditeur du Registre, accédons à la ruche **HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ WindowsNT \ CurrentVersion**, puis copions et collons Windows Server BuildLabEx (version) et EditionID (édition) dans le même emplacement que ci-dessus.
- Sauvegardons notre système d'exploitation, vos applications et vos machines virtuelles.

Effectuer la mise à niveau

- Assurons-nous que la valeur **BuildLabEx** indique que nous exécutons Windows Server 2012.
- Recherchons le support d'installation de Windows Server 2016, puis sélectionnons **setup.exe**

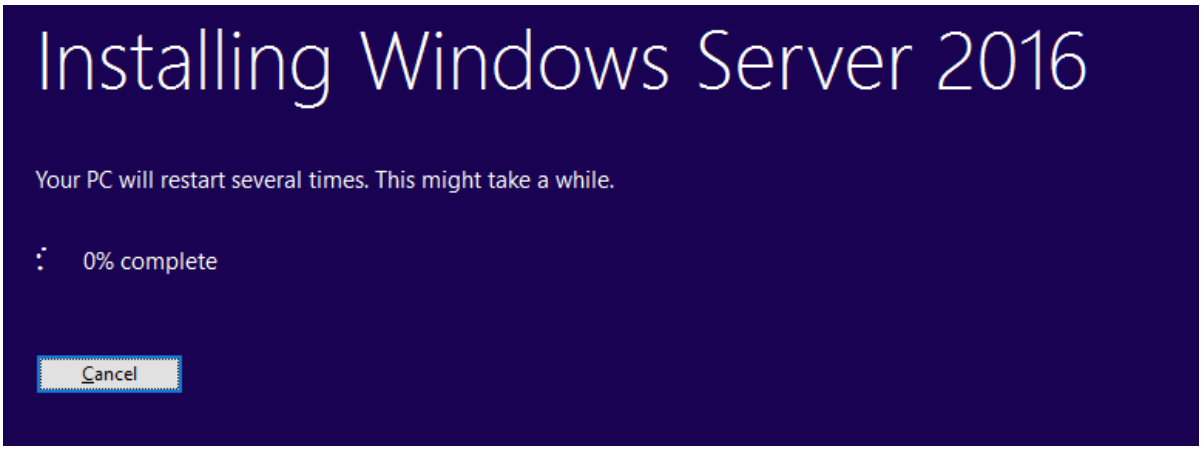


- Sélectionnons **Yes** pour démarrer le processus de configuration
- Sur l'écran Windows Server 2016, sélectionnez **Install now**
- Sélectionnons **Download and install updates (recommended)**
- Le programme d'installation vérifie la configuration de votre appareil, vous devez attendre qu'elle se termine, puis sélectionnez **Next**
- Entrons la licence du serveur
- Sélectionnons l'édition de Windows Server 2016 que nous souhaitons installer, dans notre cas **Windows Server 2016 Datacenter (Desktop Experience)** puis sélectionnez **Next**



- Sélectionnons **Accept** pour accepter les termes de notre contrat de licence
- Sélectionnons **Keep personal files and apps** pour choisir d'effectuer une mise à niveau sur place, puis sélectionnons **Next**.
- Une fois que le programme d'installation analyse votre appareil, il nous invite à poursuivre notre mise à niveau en sélectionnant **Install**

La mise à niveau sur place démarre, nous montrant l'écran de mise à niveau de Windows avec sa progression. Une fois la mise à niveau terminée, notre serveur redémarrera.



Une fois la mise à niveau terminée, nous pouvons nous assurer que la mise à niveau vers Windows Server 2016 a réussi :

- Ouvrons l'Éditeur du Registre, accédons à la ruche **HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ WindowsNT \ CurrentVersion** et affichons le **ProductName.** Nous devrions bien voir notre édition de **Windows Server 2016 Datacenter.**

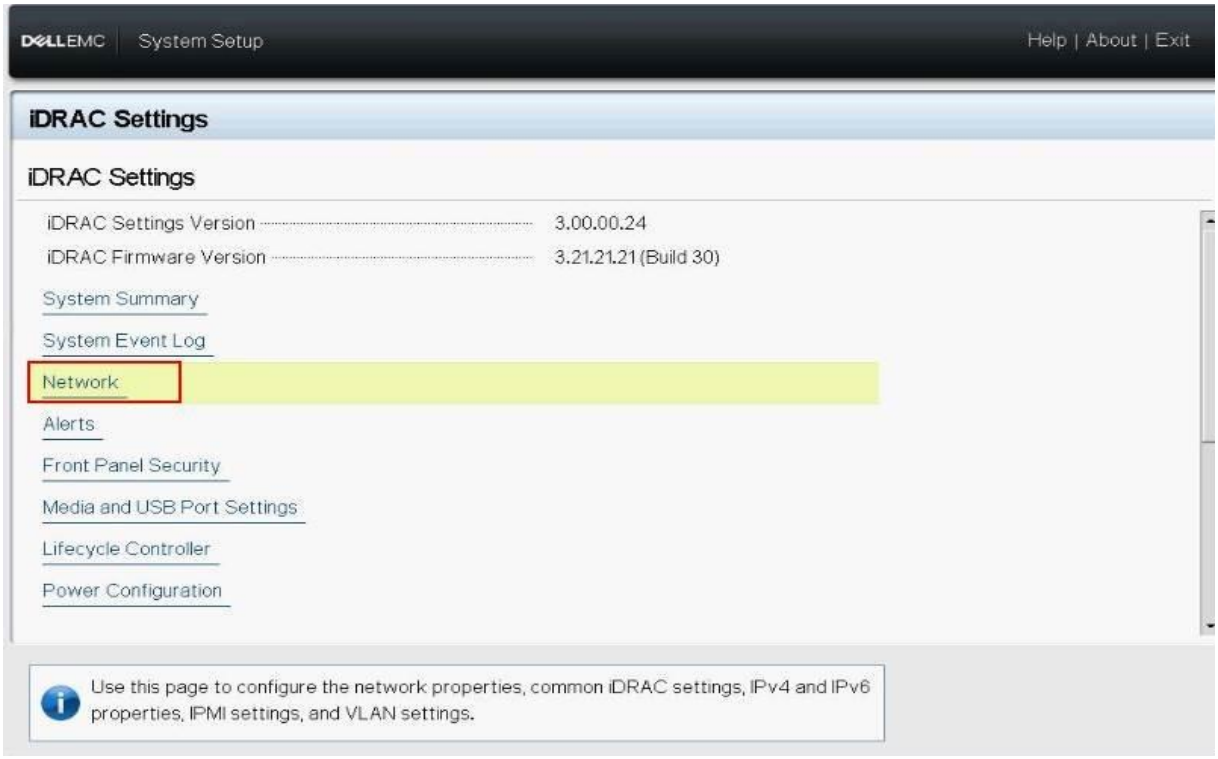
b) Installation et configuration du serveur

Configuration réseau de IDRAC

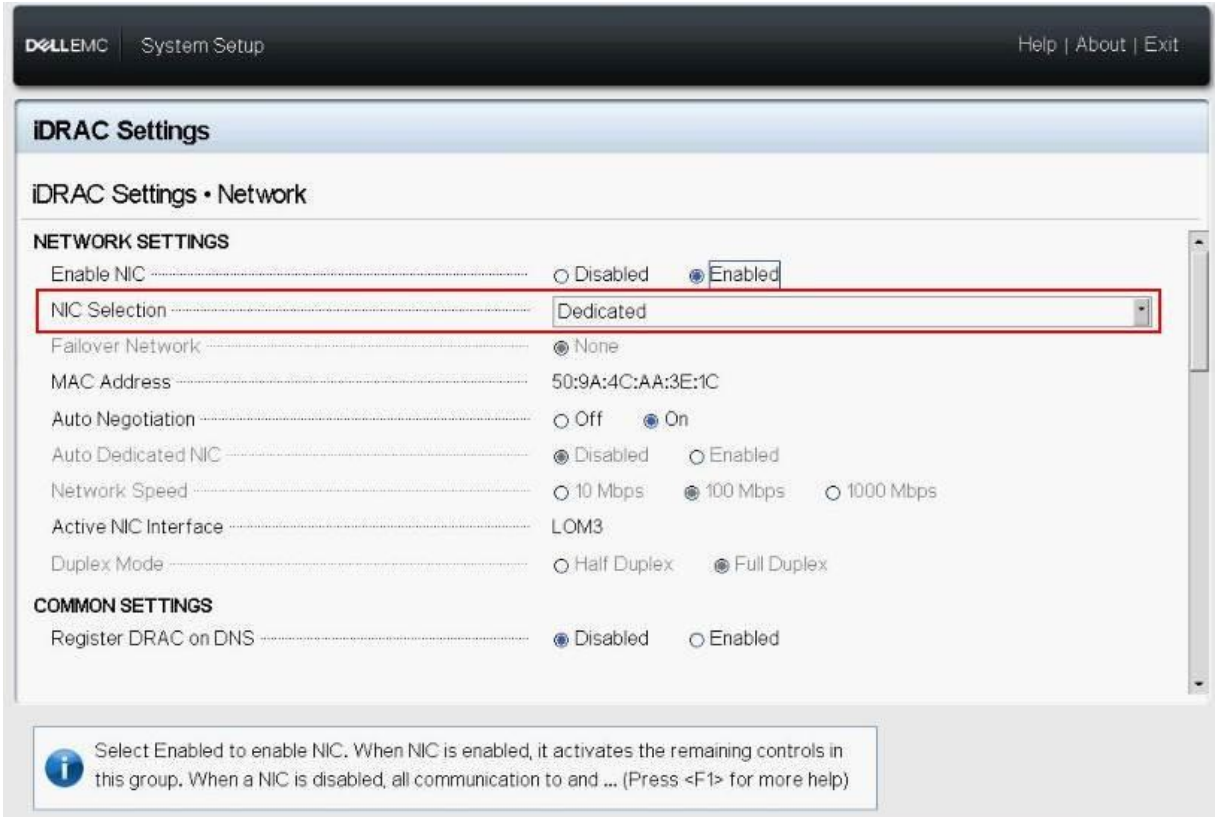
Le Contrôleur d'Accès à Distance intégré Dell (iDRAC) est conçu pour plus productivité et pour améliorer la disponibilité globale des systèmes Dell à travers une interface web. L'iDRAC aide à gérer le système à distance et réduit le besoin d'accès physique au système. Pour ce faire nous allons configurer un adresse réseau au serveur :

- Au démarrage du serveur Appuyons sur F2 pendant l'autotest :

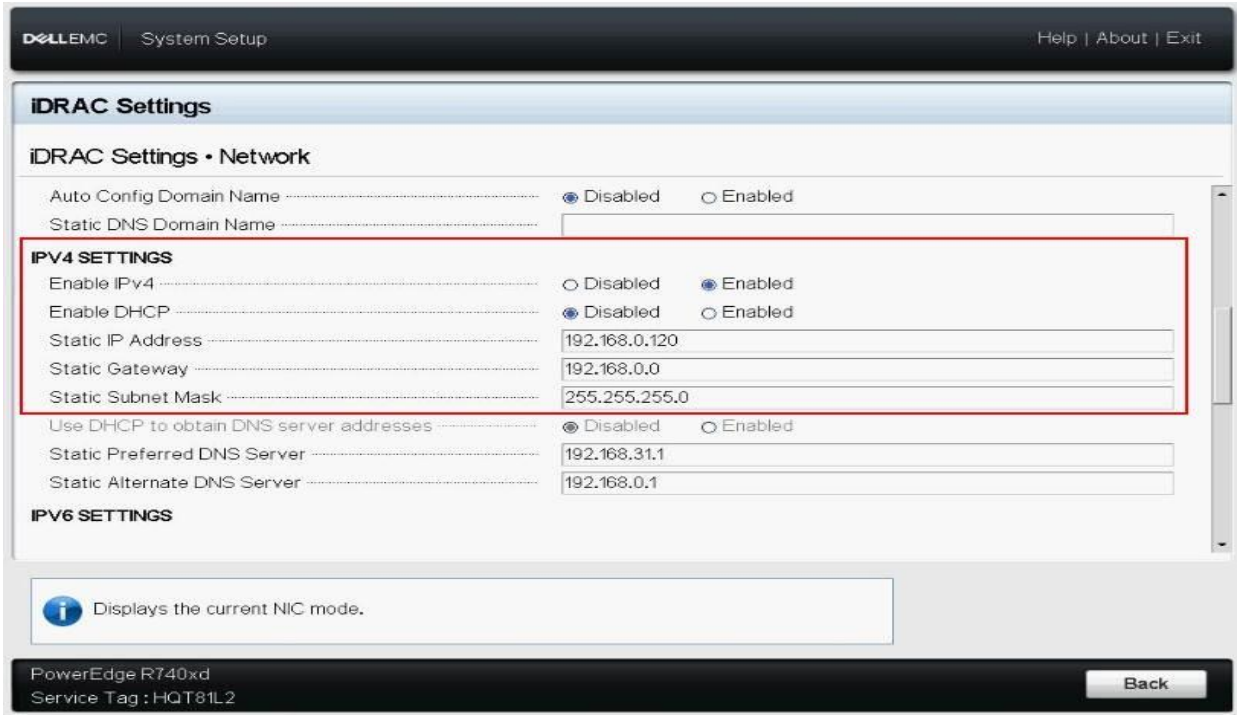
- Dans **System Setup Main Menu page**, cliquons sur **iDRAC Settings**. La page Paramètres iDRAC s'affiche.
- Appuyons sur **Network**. La page réseau s'affiche



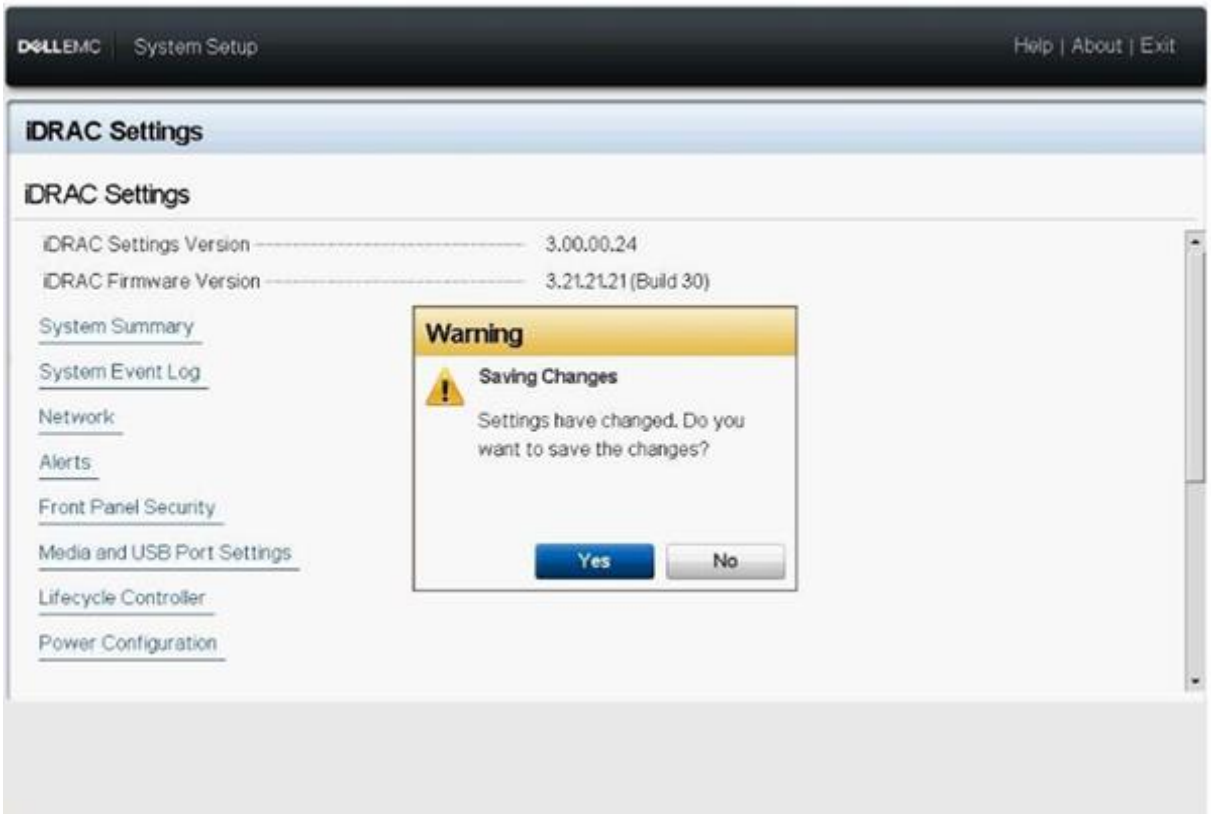
- Spécifions les paramètres réseau ; sous **Enable NIC**



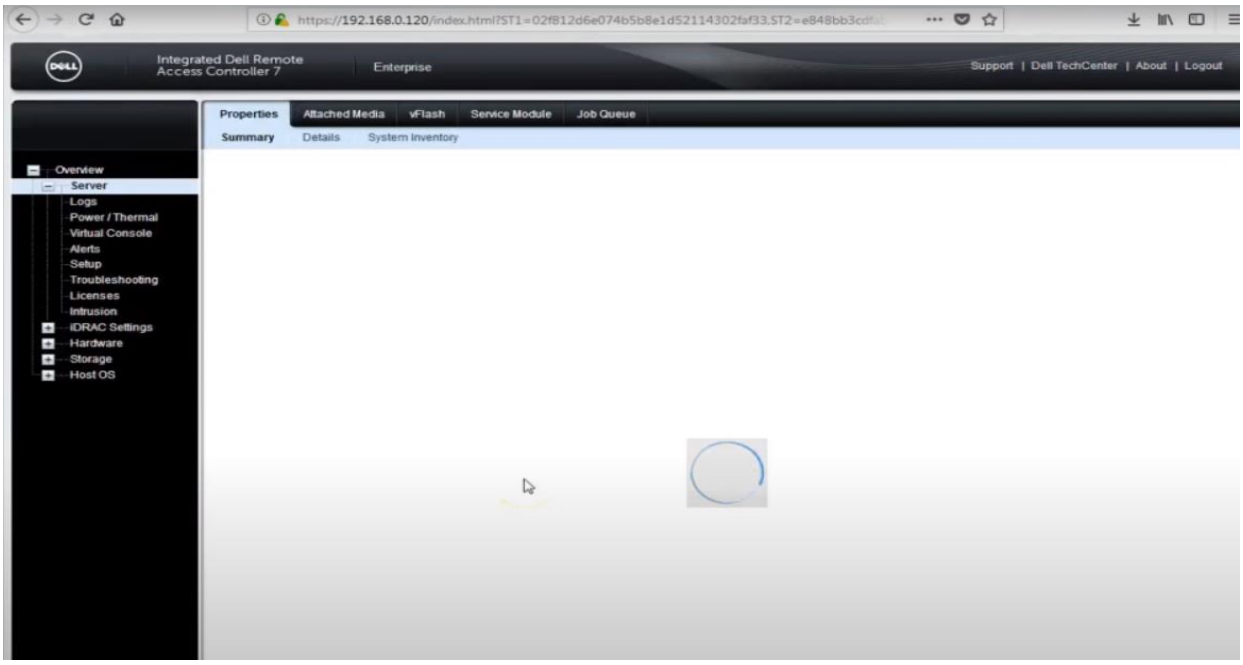
- Définissons maintenant les paramètres réseau IPv4 ou IPv6, en fonction de notre configuration locale



- Cliquons sur **Back**, sur **Finish**, puis sur **Yes**. Les informations réseau sont enregistrées et le système redémarre.



La configuration iDRAC est maintenant terminée. L'interface utilisateur Web iDRAC est désormais accessible avec n'importe quel navigateur pris en charge (IE, Firefox, Chrome, Safari). Dans notre cas, L'iDRAC répond sur l'IP « 192.168.0.120»

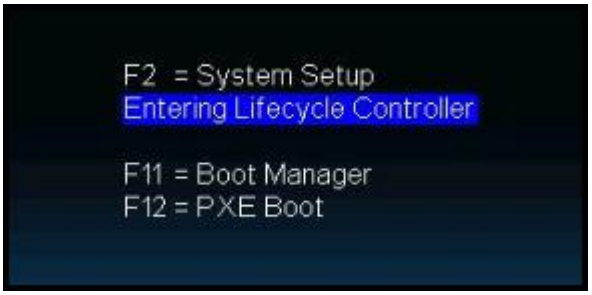


Déploiement de Windows server 2016 en utilisant Lifecycle Controller

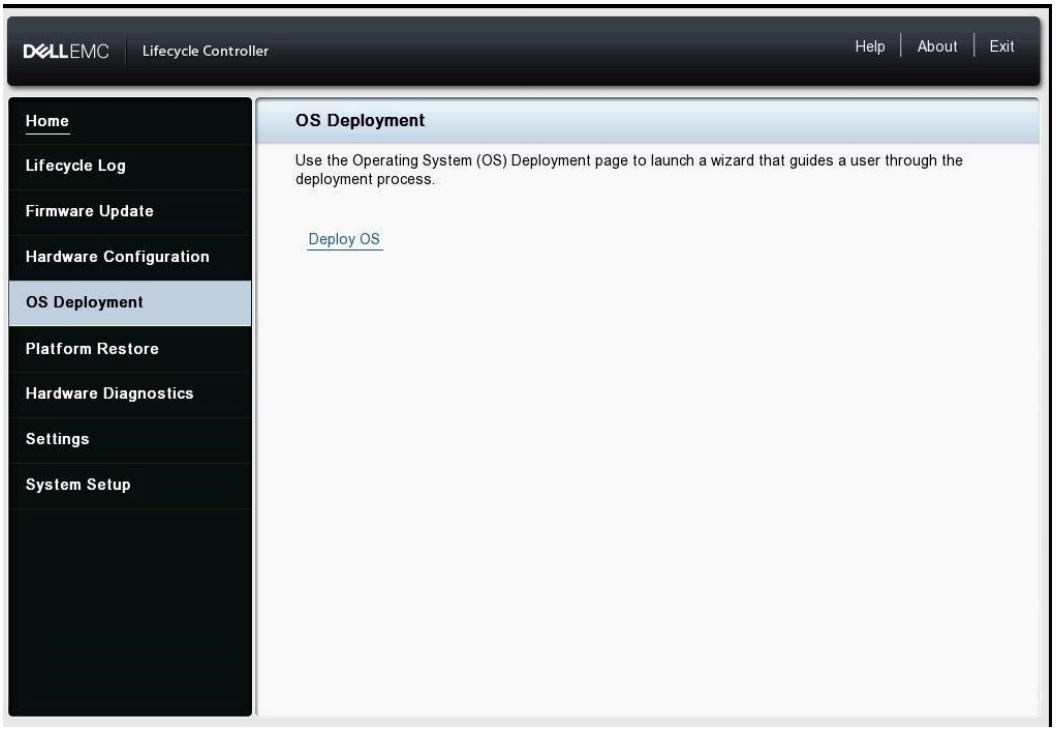
Pour installer Microsoft Windows Server 2016 pour l'édition Datacenter à l'aide de Lifecycle Controller il a fallu :

- Mettre le serveur sous tension

- Appuyer sur **F10**(Entering Lifecycle Controller) pendant l'autotest :

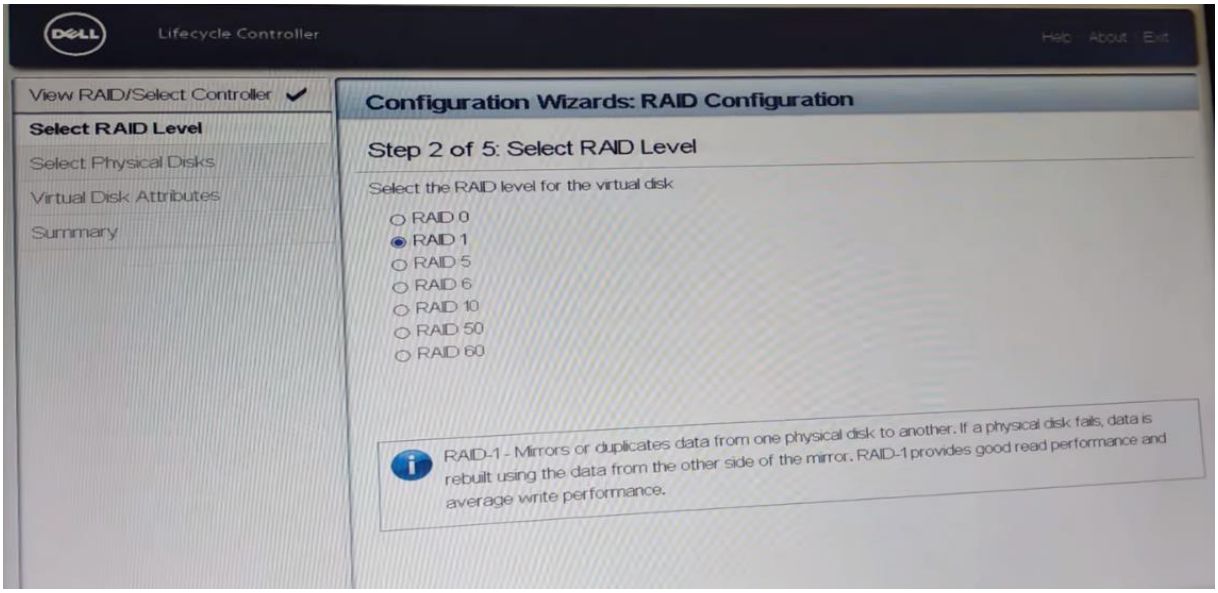


-Sur la page **Lifecycle Controller**, cliquer sur **OS Deployment**, puis sur **Deploy OS**

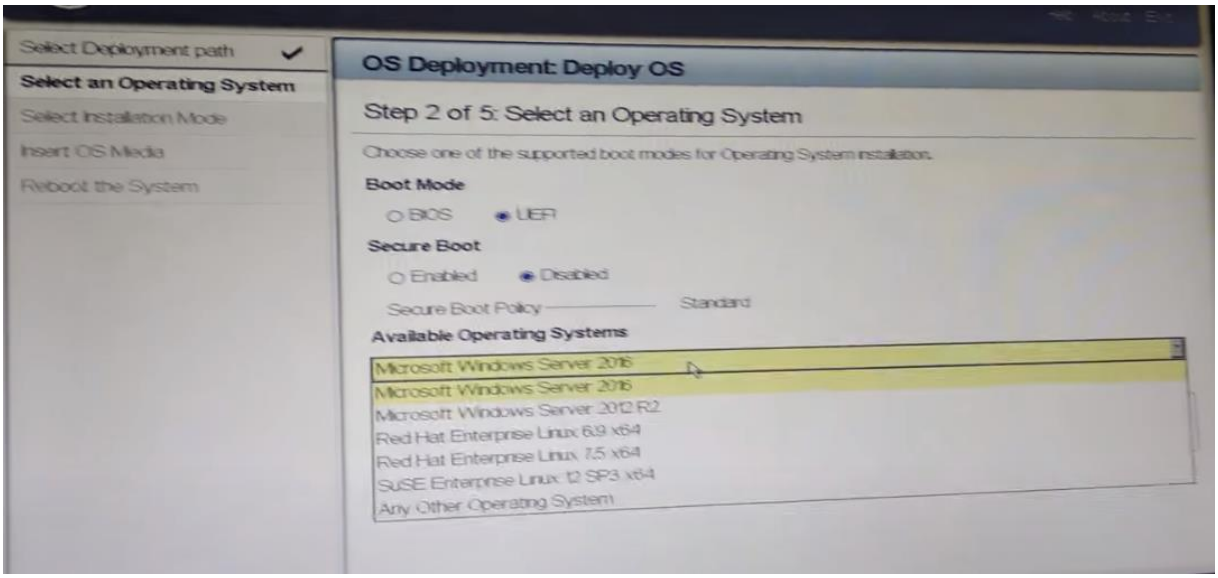


- La fenêtre pour ignorer ou configurer du raid s'affiche, cliquer sur **Configure RAID First**

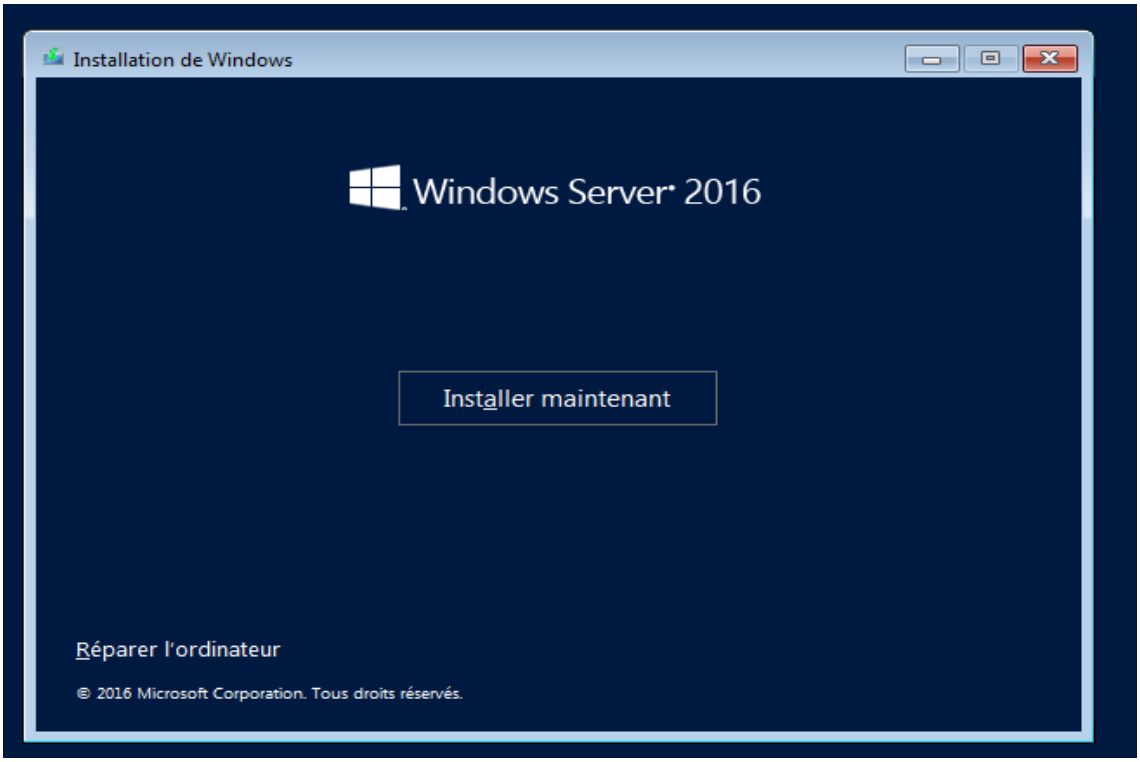
- Nous choisissons **RAID 1** pour mettre nos deux disque dur ssd dans une configuration Mirror pour plus de performance et une tolérance aux pannes.



- En cliquant sur Cliquez sur **Next,** La page **Select an Operating** s'affiche avec une liste des systèmes d'exploitation compatibles. Choisir alors le Microsoft Windows server 2016 et validé.



- Nous s'y sommes, le système charge les pilotes nécessaires à l'installation de OS. Ensuite il faudrait spécifier le disque d'installation contenant le système d'exploitation. Et c'est terminer le processus d'installation de Windows Server 2016 démarre. Nous pouvons consulté le site https://www.tactig.com/install-windows-server-step-by-step/ pour connaitre les étapes d'installation d'un serveur sous Windows .



c) Installation et configuration de SQL SERVER 2014 en Failover Cluster

L'installation de SQL Server 2014 est une procédure assez longue, pour ce cela dans cette partie, nous montrons juste comment mettre notre le serveur dans Cluster de basculement. Pour plus de détaille sur le processus nous conseillons de consulter le site web officiel https://docs.microsoft.com/en-us/sql/sql-server/failover-clusters/install/ .

❖ **Prérequis**

- Sur le contrôleur de domaine, développer notre nœud « sqlcergi», en ajoutant une nouvelle unité organisationnelle protégée contre la suppression accidentelle. Puis ajouté deux utilisateurs à cette unité.

C:\Users\Administrateur> New-ADOrganizationalUnit -Name "SQLCERGI " -Path "DC=FABRIKAM,DC=SQLCERGI.COM" -OtherAttributes @{seeAlso="CN=HumanResourceManagers,OU=Groups,OU=Managed,DC=S

QLCERGI,DC=.com";managedBy="CN=Administrator,DC=SQLCERGI,DC=.COM"}"

C:\Users\Administrateur>NET USER SQLAccount password /ADD

C:\Users\Administrateur> NET USER SQLAgentAccount password /ADD

C:\Users\Administrateur> NET GROUP SQLCERGI SQLAgentAccount /ADD /sqlcergi.com

C:\Users\Administrateur> NET GROUP SQLCERGI SQLAccount /ADD /sqlcergi.com

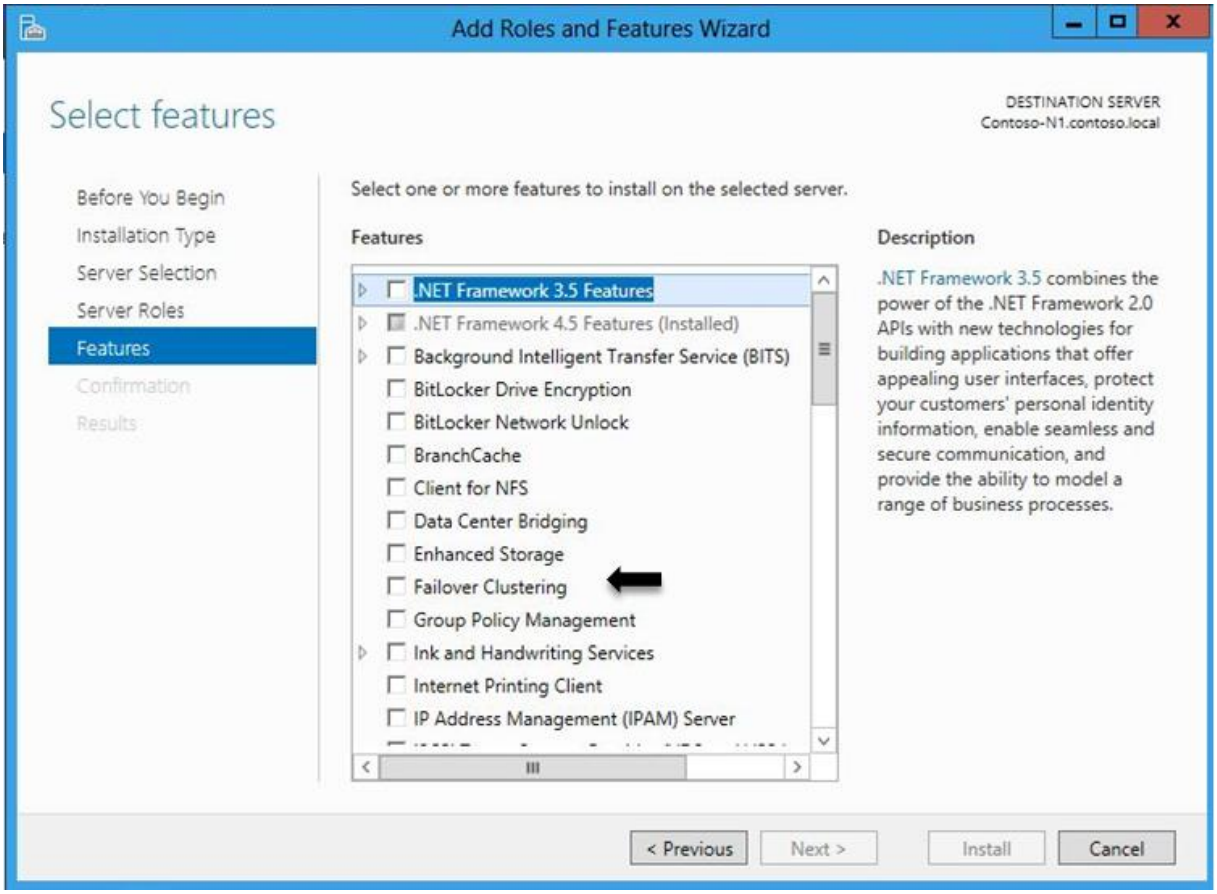
- Créer 2 disque virtuelle iSCIS sur notre contrôleur pour chaque nœud de notre cluster de basculement.

C:\Users\Administrateur> New-IscsiVirtualDisk -UseFixed -Path "E:\temp\iSCSI-Virtual-disk-1.vhdx" -Size 100 GB

C:\Users\Administrateur> New-IscsiVirtualDisk -UseFixed -Path "E:\temp\iSCSI-Virtual-disk-2.vhdx" -Size 100 GB

- **Installation de la fonctionnalité cluster de basculement sur les deux DB server**

Dans le Gestionnaire de serveur, l'Assistant Ajout de rôles et de fonctionnalités est utilisé pour ajouter des rôles et/ou des fonctionnalités. L'Assistant Ajouter des rôles et des fonctionnalités est accessible dans la barre de menus du Gestionnaire de serveur en choisissant **Ajouter des rôles et des fonctionnalités** dans la liste. Assurez-nous que le serveur approprié est sélectionné dans l'écran de **sélection** du **serveur.** Dans l'écran Fonctionnalités, sélectionnons **Failover Clustering**


Add Roles and Features Wizard
Select features
DESTINATION SERVER
Contoso-N1.contoso.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.5 Features (Installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Data Center Bridging
Enhanced Storage
Failover Clustering
Group Policy Management
Ink and Handwriting Services
Internet Printing Client
IP Address Management (IPAM) Server
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel