**Présentation**

Définis comme Conseil Etude Réalisation et Gestion informatique, CREGI est un société Anonyme de développement de services informatique Bancaire fondé en 1991 à l’initiative de Mr Yao DOGBO PDG actuelle de ladite société. CERGI offre des solutions de gestion à plus d’une trentaine de Banque et institution financière dans la sous-région UEMOA et CEMAC, il offre Notamment CERGI Compliance qui est une plateforme web de prestation de service.

L’activité de CERGI tourne autour du développement évolutif des modules de ses services bancaires, du déploiement et la configuration des solutions IBIS aux près des Banques et institutions financière cliente, ainsi que la formation des utilisateurs en vue du transfert de compétences efficient pour l’exploitation optimale de son Core Banking.

Pour Assurer la qualité et la disponibilité de ses services, CERGI dispose d’une architecture de cloud Hybride. Le cloud computing est modèle permettant de fournir des services et des ressources informatiques facturer à la demande. Les différents modèles de cloud sont : le cloud public qui correspond à une dématérialisation, une externalisation de ses ressources informatiques, et le cloud privé qui correspond à une matérialisation, une internalisation de ses ressources. Le cloud Hybride est donc simplement une combinaison d’un cloud public à un cloud privé dans le but d’offrir un service optimal. Les différents services offert dans un environnement cloud sont les suivantes : IAAS pour infrastructure as a services en français service d’infrastructure, le PAAS pour service de plateforme en anglais Platform as a services .et enfin le SAAS pour Software as a services en français service de logiciel.

L’activité de CERGI s’articule justement autour ce dernier service, en tirant parti de son cloud hybride reparti sur deux sites :

* D’abord Un cloud public qui est un VPS héberger cher les prestataires Goddady offrant exclusivement des services Web sécurisé par un Web Application firewall (WAF)et des Certificats SSL et TLS permettant une communication crypté HTTPS entre le client demandant un domaine et le serveur web.
* Et ensuite un cloud privé basé à Abidjan communicant à travers un tunnel (VPN) express route avec le cloud public qui lui fait fie pour le contrôle de domaine, le stockage, et la manipulation des bases de données. Nous avons deux serveurs de base de donnée en Mirroring c’est-à-dire en réplication de données
* Les données stocké dans le cloud privé sont migrées par le protocoles SFTP sur l’environnement de travail de CERGI SA bien entendu ici à Lomé. L’administration des différents serveurs se font en Remote desktop (RDP) ou en SSH

Comme vous le voyez Tout est es configurer afin d’assurer la disponibilité des services CERGI, mais face à la demande sans cesse croissante dû à l’augmentation de ses clients, un besoins d’optimisation de son Architecture cloud computing se pose. Il est question d’améliorer les performances son cloud afin d’assurer sa haute disponibilité, sa reprise d’activité, sa résilience, sa sécurité et son évolutivité.

Pour se faire, mise hors la recommandation de passer à une solution dématérialiser chez les prestataire cloud comme Microsoft azure, Amazon cloud ou Google cloud, qui peut impliquer des couts énormes pour l’entreprise, Notre étude s’est porté sur deux niveaux d’optimisation :

* L’optimisation de la disponibilité
* L’optimisation de la sécurité
* Pour améliorer la disponibilité nous avons pensé en premier lieu au Loadbalancing des services web,

Mettre en place un nouveau serveur web et repartir les charges de travail comme la résolution DNS, les réponses HTTPS, les requêtes SQL sur les deux serveurs

En deuxième lieu Nous avons pensé au FAILOVER Clustering, au niveau des serveurs de base de données en plus de la réplication des données techniquement le Mirroring nous allons implémenter un cluster de basculement permettant de gérer les pannes ou indisponibilité de l’un ou de l’autre.

* Pour améliorer la sécurité dans un premier temps nous avons prôné la migration des systèmes d’exploitations des serveurs, les mettre à jour vers les dernières fonctionnalités système.

En deuxièmement lieu, nous avons préconiser un firewall de nouvelle génération comme Fortigate dans le but de filtrer et sécuriser la communication et le transfert de ficher entre le cloud privé et notre environnement de travail.