

Architecture et Conception d'un systèmes hybride sécurisée

pour la prise en charge de Canvas LMS au sein de **KADEA**
Campus

IT Expert

Eddy Disonua

1. Introduction.

Dans le but d'améliorer les conditions d'enseignement ainsi que l'accessibilité de contenus de la formation, l'institution **KADEA Academy** (Kinshasa) envisage de mettre en place un système hybride sécuriser avec une bonne accessibilité des contenus numérique dans le campus et hors campus. Le système prendra en charge l'utilisation du logiciels **CANVAS LMS**. Avec pour objectifs principal, de faciliter les consultations de cours, dépôt de devoirs ainsi qu'une excellente gestion des notes.

Pour atteindre cet objectif, au préalable, nous allons faire un état des lieux de l'actuel système utilisé dans le campus. Ensuite, nous examinerons la possibilité de trouver une solution pour répondre à nos préoccupations avant de conclure.

2. Développement (Choix des briques techniques)

CANVAS LMS est une application web, qui nécessite une connexion internet stables et permanentes pour être accessible. Actuellement, l'accessibilité à Internet au sein du campus KADEA Kinshasa est confrontée à plusieurs difficultés, notamment la disponibilité et la stabilité.

Afin de trouver une solution à ces problèmes, il a été suggéré d'améliorer l'accessibilité de la plateforme numérique CANVAS LMS, en offrant une **solution hybride**. Constituer d'un hébergement local au sein du campus pour une accessibilité directe et rapide, ainsi que sur le cloud, accessible via une connexion internet un peu plus stable tels que 3G, 4G, 5G ou fibre optique en dehors du campus.

Systeme Hybride

Le système hybride sera formé de deux environnements, le local et le Cloud, connectés entre eux et capables de synchroniser les données en cas de rétablissement ou de coupures d'internet.

Local

Pour implémenter le système d'hébergement local, le campus **Kadea** Kinshasa doit mettre à niveau son Data Center et le moyen d'accessibilités de données. Dans le tableau 1 ci-dessus nous trouverons la liste et la description des matériels requis pour la mise en œuvre du data center.

Table 1: Data center Locale liste d'équipement

Matériels	Description
Serveur	
Machine serveur 1	8 cœurs de processeur, 16 Go de RAM et un stockage SSD rapide.
Machine serveur 2	4 cœurs de processeur, 8 de RAM et un stockage SSD rapide.
Connectivité et sécurité	
Pare feu	FortiGate 100F/101F : Conçu pour 100 à 200 utilisateurs, offrant un débit de pare-feu de 20 Gbps et d'excellentes performances globales.
Routeur	Cisco Meraki MX75 : Ce dispositif est spécialement conçu pour un maximum de 200 utilisateurs et offre un débit de pare-feu de 1 Gbps, ainsi qu'une suite complète de fonctionnalités de sécurité dans un format simple et géré dans le cloud.
Commutateur	Couche d'accès : les commutateurs Cisco Catalyst série 9300 offrent des ports d'accès de 1 Gbps avec des capacités d'empilage et de couche 3.
Fibre optique	SCPT
4G Internet connections	VODACOM,ORANGE
Infrastructures énergétiques et de refroidissement	
Alimentations sans interruption (ASI)	Alimentation de secours par batterie pour une alimentation immédiate.
Groupe électrogène de secours	Pour les pannes de courant prolongées.
Systèmes de refroidissement :	Unités CRAC/CRAH
Logiciels et gestion	
Système d'exploitation	Linux Rocky
Plateforme de virtualisation	VMware
Base de données	Mysql
Plateforme de gestion de l'apprentissage (LMS) :	Canvas
Logiciel de supervision et de gestion de l'infrastructure.	Net box
Encryptions	Certificats

Cloud

Une autre version de l'application sera héberger dans un service cloud tels Amazone EC2 pour permettre une connections 24/7 a distance, avec une capacités recommandée de la machine virtuel qui varie d'un serveur de 4 vCPU et 8 Go de RAM pour une charge de travail raisonnable à un serveur de 8 vCPU 16 Go de RAM pour les pics de charge comme les examens en ligne ou une utilisation multimédia intensive. Dans l'environnement cloud deux machine virtuel seront utilise l'une pour le code de l'application et l'autre pour la base de données.

Architecture et conception

Les instances Cloud et Campus seront techniquement unifiée a l'aide du modèle de cloud hybride, pour intégrer ces deux environnements pour qu'ils fonctionnent comme une infrastructure unique.

Pour avoir accès a l'application les étudiants aurons besoin d'un navigateur a l'exemple de Google chrome, Firefox ou Microsoft Edge.

Nous utiliserons Linux Rocky pour sa stabilité et sa compatibilité binaire avancée qu'il offre, ainsi que Docker pour la gestion des environnements de notre application, services et micro-services.

Dans notre contexte, nous utiliserons la méthode de synchronisation bidirectionnelle, qui consiste à s'assurer d'avoir les mêmes données localement et sur le cloud, en assurant le mécanisme de résolution de conflits.

Avec l'API et les web services, la synchronisation sera personnalisée, à l'exemple de restfull, pour assurer la modification des données spécifiques.

Au cas où il y aurait interruption de la connexion internet, nous utiliserons un cache et nous synchroniserons une fois la connexion rétablie. Garantir l'intégrité et la cohérence des données dans tout le système, et éviter toute perte de mise à jour pendant le transfert. Nous allons opter pour la connexion sécurisée HTTPS et une méthode d'authentification à deux facteurs, en local et sur le cloud.

Briques technique

- Utilisateur (Navigateur)
- Web serveur (NGINX)
- Application
- serveur base de données (Mysql)

3. Sécurité & Réseau

Il y aura deux zones dans notre réseau, à savoir DMZ et LAN. Le DMZ et le LAN sont séparés par un pare-feu. Le port 443 (qui sera changé ultérieurement) sera utilisé avec la ligne sécurisée HTTPS, ce qui augmentera le niveau de sécurité.

I. DMZ

- LMS Web frontend
- Authentification

II. Réseaux interne

- Base de données
- Authentification

La politique de sauvegarde et de restauration sera basée sur l'ID des utilisateurs, leurs sessions et sur l'alpha numérique des caractères liés à chaque activité, par exemple la création de contenus. À chaque connexion, il y aura synchronisation, c'est-à-dire mise à jour de la base de données en local et sur le cloud, pour continuer à assurer la cohérence.

Pour assurer la continuité de service, la protection des données et une expérience utilisateur optimale, une surveillance multicouche est utilisée pour superviser un LMS (Learning Management System) en mode Cloud et Local.

La supervision est structurée en quatre domaines principaux :

- En local et sur le Cloud Contrôle de la consommation des ressources telles que l'utilisation du processeur (CPU), de la mémoire RAM, de l'espace de stockage et du trafic réseau.
- Contrôle de la disponibilité de la plateforme, du temps de chargement des pages, du temps de réponse des requêtes SQL et de la vitesse de téléchargement des contenus pédagogiques.
- En analysant les journaux (logs) d'accès, nous pouvons identifier les tentatives d'intrusion, les attaques par déni de service (DDoS) ou les anomalies de connexion.
- Niveau d'expérience et d'activité des utilisateurs.

Avec objectif principal celui de repérer et résoudre de manière proactive les pannes ou les ralentissements avant qu'ils n'affectent les sessions de formation en direct. Optimiser l'expérience utilisateur et maîtriser le changement de coûts.

