

Module : Sécurité dans les Cloud

Projet : Scénario PME sur AWS (Learner Lab)

Objectif général

Mettre en œuvre, dans un environnement **AWS Learner Lab**, une **architecture cloud sécurisée adaptée à une PME**, intégrant des **mécanismes de sécurité, de surveillance et de conformité**, en tenant compte des **limitations de l'environnement**.

Chaque groupe conçoit un **scénario réaliste** de PME (secteur au choix) et développe une **preuve de concept (PoC)** démontrant les **principes fondamentaux de la sécurité dans le Cloud AWS**.

Contexte

Votre équipe agit comme **consultants en sécurité Cloud** mandatés par une **PME** souhaitant migrer une partie de son système d'information vers AWS. L'entreprise recherche une solution :

- simple à déployer,
- sécurisée par conception,
- observable (surveillance et alertes),
- et conforme aux bonnes pratiques AWS.

Organisation du travail

- Travail en **groupe de 2 à 3 étudiants maximum**.
- **Durée totale du projet : 5 semaines**.
- **Présentation finale : fin novembre** (Date exacte c'est la date de la séance du cours de cette semaine).
- **Durée de la présentation : 15 minutes par groupe**, suivies de 5 minutes de questions.

Étapes du projet

Étape 1 – Définition du scénario et des besoins

- Choisir une **PME fictive** : (ex. : e-commerce, cabinet médical, startup SaaS, agence de voyage, école, etc.)
- Décrire :
 - L'activité principale de la PME.
 - Les services à migrer sur le cloud.
 - Les risques de sécurité liés à son domaine.

Livrable : fiche de conception présentant le contexte, les besoins et les menaces principales.

Étape 2 – Conception et déploiement sur AWS

Créer une architecture réaliste mais compatible avec les restrictions du **Learner Lab**, en utilisant les services suivants :

Services autorisés / recommandés :

- **Amazon S3** → stockage sécurisé ou hébergement statique.
- **Amazon EC2** → hébergement applicatif ou API.
- **Amazon CloudFront** → distribution sécurisée avec HTTPS.
- **AWS WAF** → filtrage des attaques web (règles gérées AWS).
- **Amazon CloudWatch** → supervision et alertes.
- **AWS CloudTrail** → audit des actions effectuées dans le compte.

Précision pédagogique :

Les configurations IAM avancées (rôles, utilisateurs, politiques personnalisées) ne sont pas demandées, car restreintes dans l'environnement Learner Lab. L'objectif est de se concentrer sur la sécurisation des services AWS disponibles et sur la visibilité des activités (logs, alertes).

Exemples de mini-architectures :

- Site e-commerce statique sur S3 + CloudFront + WAF.
- API sur EC2 avec pare-feu (Security Groups) et journalisation.
- Portail web sur EC2 + stockage d'images sur S3 avec HTTPS.

Livrable : schéma d'architecture et justification des choix techniques.

Étape 3 – Sécurisation et surveillance

Appliquer les **bonnes pratiques de sécurité accessibles** :

- Restreindre l'accès public aux buckets S3.
- Configurer les **Security Groups** de manière restrictive (ports, IP).
- Déployer un **WAF** avec règles gérées.
- Forcer le **HTTPS** via CloudFront.
- Activer **CloudTrail** et **CloudWatch Logs**.
- Créer un tableau de bord ou une alerte CloudWatch.

Livrable :

- Captures d'écran des configurations :
- Exemple de log ou d'alerte ;
- Analyse démontrant la détection ou la prévention d'un risque.

Option bonus (pour les groupes motivés) :

Un bonus pourra être accordé aux groupes intégrant un petit test de sécurité. Par exemple, une simulation d'attaque ou de scan réseau, accompagnée d'une détection via CloudWatch Logs ou CloudTrail.

Livrables finaux

1. Rapport technique (5–7 pages) :

- Contexte et besoins de la PME.
- Schéma et description de l'architecture AWS.
- Mesures de sécurité mises en œuvre.
- Captures d'écran et logs illustratifs.
- Évaluation des risques restants et recommandations.

2. Présentation orale (15 min par groupe) :

- Démonstration du PoC et des protections déployées.
- Synthèse claire et structurée.

Bon courage