***Résumé :***

L’objectif principal de la phase d’analyse d'une solution de sécurité dans le cloud est de capturer les exigences de l'utilisateur, c'est-à-dire de définir le périmètre des mesures de sécurité à mettre en place. Dans ce dossier, nous commencerons par une étude préliminaire de la sécurité dans le contexte de l'infrastructure cloud AWS, en présentant les parties prenantes et les rôles critiques. Ensuite, nous réaliserons une analyse des besoins en matière de sécurité, en fournissant une vue d'ensemble ainsi qu'une analyse détaillée des mesures de sécurité nécessaires pour protéger les données et les ressources dans le cloud.

***Aperçu :***

**Introduction**

1. **PRESENTATION DU THEME**
2. **ETUDE DE L’EXISTANT**
3. **CRITIQUE DE L’EXISTANT**
4. **PROBLEMATIQUE**
5. **PROPOSITION DE SOLUTION**

**Conclusion**

## PRESENTATION DU THEME DE STAGE

Dans le cadre de l'obtention du diplôme de technicien supérieur, notre projet de stage de trois mois porte sur l'étude et l'implémentation de la sécurité dans le cloud, avec un focus particulier sur les services AWS (Amazon Web Services). L'objectif principal est d'analyser les aspects de sécurité spécifiques à AWS et de mettre en œuvre des solutions efficaces pour protéger les ressources cloud de l'entreprise.

La sécurité dans le cloud est cruciale pour garantir la confidentialité, l'intégrité et la disponibilité des données et des services. Avec l'adoption croissante du cloud computing, il est essentiel de comprendre et de gérer les risques associés, notamment en matière de gestion des identités, de chiffrement des données, de surveillance et d'audit, ainsi que de réponse aux menaces.

## ETUDE DE L’EXISTANT

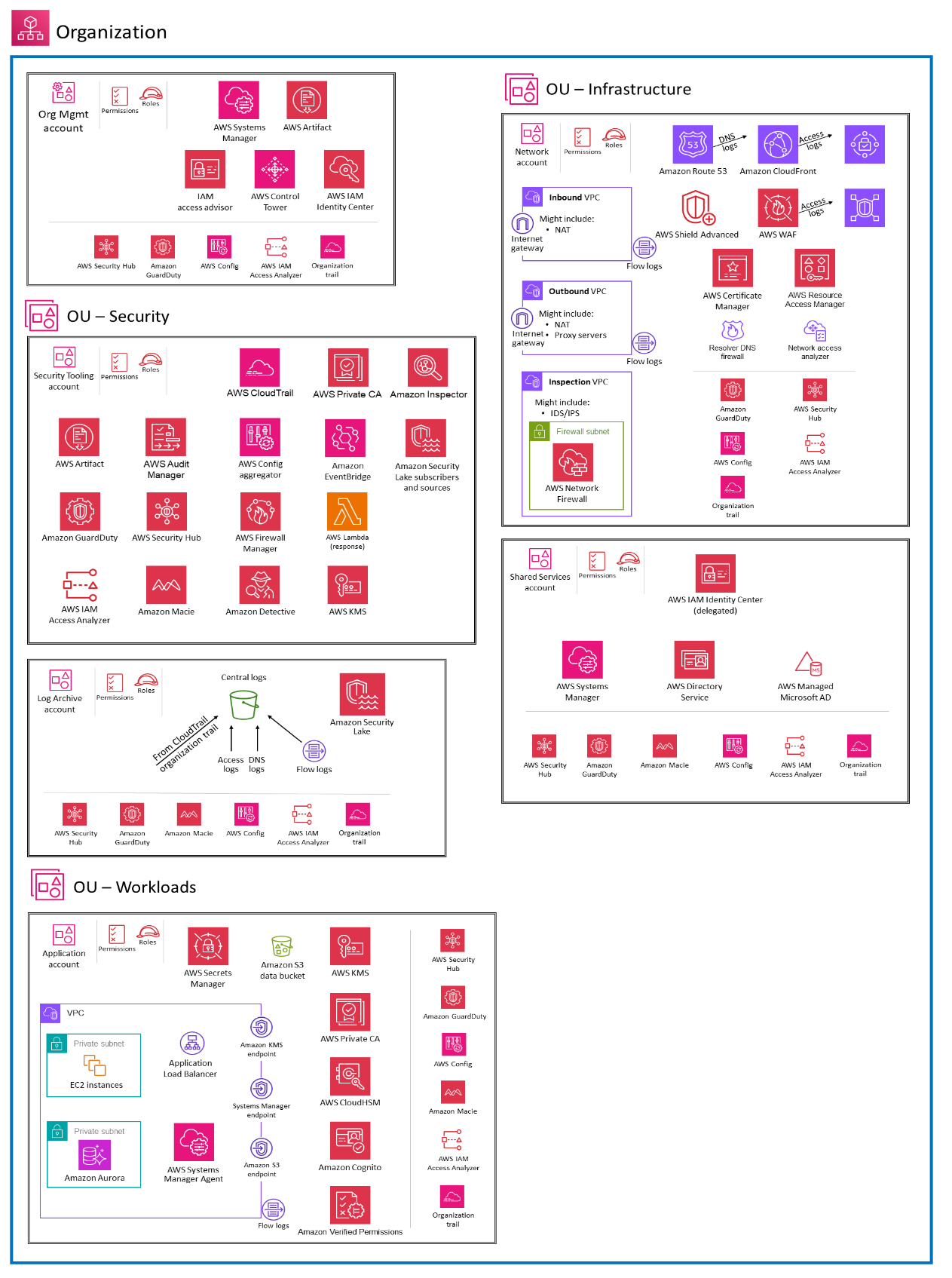


Figure 1:architecture de référence de sécurité aws

La sécurité dans le cloud est essentielle pour garantir la protection des données, des applications, et des infrastructures contre les menaces internes et externes. Les entreprises doivent veiller à ce que leurs ressources cloud soient sécurisées pour prévenir les violations de données, les pertes de confidentialité, et les interruptions de service. Mais il y’a un problème qui subsiste, c’est celui concernant la responsabilité partagée qui pourrait causer des problèmes inattendus et de depenser plus d’argent pour les résoudre.

Cependant l’on peut observer que son architecture globale est constituée des services suivant :

*  **AWS Identity and Access Management (IAM) :** Permet de gérer les permissions et l'accès aux ressources AWS. IAM facilite la gestion des utilisateurs, des groupes, des rôles et des politiques d'accès.

Figure : aws IAM

* **AWS Key Management Service (KMS) :** Fournit une gestion sécurisée des clés de chiffrement pour protéger les données en transit et au repos.

Figure :aws kms

* **AWS Route 53 :**fournit plusieurs fonctionnalités clés pour la gestion et l’optimisation des noms de domaines , ainsi que pour la distribution du trafic.



Figure :aws Route 53

*  **Amazon Secret Manager :** Outil pour la surveillance et la gestion des secrets dans le aws.

Figure : aws secret manager

* **AWS WAF (web application firewall) :** Protégez les applications web contre les attaques courantes, telles que les injections SQL et les scripts intersites (XSS).



Figure : aws waf

Tous ces services sont managés à travers une interface utilisateur appelé console.

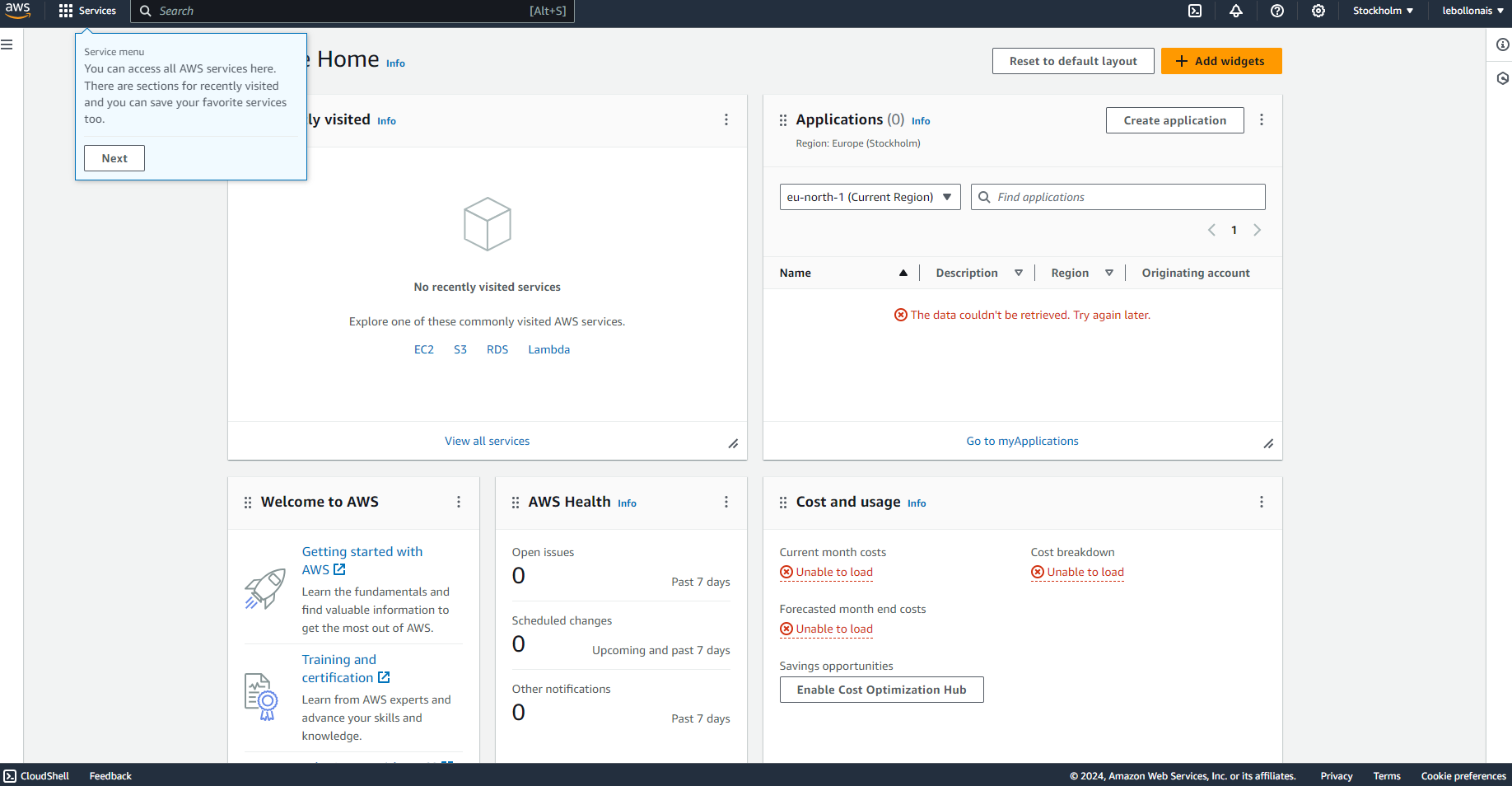


Figure 7:console AWS

Toutes ces ressources sont pris en charge par l’utilisateur du compte aws.

## CRITIQUE DE L’EXISTANT

AWS offre un ensemble complet de service et d’outils complet pour garantir la sécurité des ressources cloud. Ces services incluent AWS IAM, AWS KMS, AWS ACM, AWS WAF et bien d’autre encore. Ce qui rend leurs systèmes de sécurité presque indéfectible.

Mais au milieu de tous ces atouts que possèdent AWS, il y’a des améliorations à apporter sur des points impactant afin de le rendre meilleur. Tout d’abord on a le problème de la complexité de configuration qui subsiste. Dans des réseaux de grandes tailles il peut devenir complexe de gérer les politiques avec de nombreux utilisateurs et services, ces erreurs de configuration pouvant conduire à des failles de sécurités. On a aussi le problème de responsabilité partagée qui est en gros porté sur les erreurs de configuration ou la mauvaise gestion des permissions et qui plus peut causer des malentendus sur les responsabilités de sécurité avec des conséquences potentielles en cas de mauvaise configuration ou de gestion des données et au-dessus on peut rajouter la complexité des configurations.

## PROBLEMATIQUE

Les éléments cités plus haut dans l’étude de l’existant nous ont permis d’avoir une vue globale sur l’architecture de AWS dans le cadre de la gestion de ses différents services de sécurités et cela nous a permis de déceler dans la critique de l’existant plusieurs manque et faiblesses. Les problèmes centraux sont :

* **Les erreurs de configuration ;**
* **La mauvaise gestion des permissions ;**
* **La complexité de configuration.**

Ainsi donc, nous avons ressorti plusieurs problématiques partant de ces différents problèmes :

**« Comment optimiser la gestion de la sécurité dans un environnement cloud AWS en surmontant les défis liés à la complexité des configurations, à la gestion des permissions, et à la couverture des menaces, tout en garantissant une protection efficace des données et des applications ? »**

## PROPOSITION DE SOLUTION

Notre évaluation approfondie de notre environnement AWS a mis en évidence la nécessité d'adopter une approche de sécurité proactive et globale. Pour y parvenir, nous proposons de mettre en œuvre une stratégie d'implémentation de la sécurité cloud robuste et adaptée à nos besoins spécifiques. Cette solution se base sur le thème : « **Etude et implémentation de la sécurité dans le cloud : cas de aws** ». Cette solution nous permettra non seulement d’automatiser et d’optimiser les différentes tâches liées à la sécurité mais également de réduire les dépenses et les risques en cas de problèmes car cela va permettre une garantie de niveau de service maximal, ce qui signifie moins de faille de sécurités, une gestion centralisées et minutieuse des ressources.

## CONCLUSION

Pour clore ce chapitre, la question était ici de faire une analyse profonde et rigoureuse de notre entreprise d’accueil, de connaître ces problèmes, de faire un critique, d’en ressortir la problématique et enfin faire une proposition de solution qui permettre de résoudre cette problématique. C’est le chapitre fondamental du projet et l’étude qui y est faite nous a permis ici de définir un canevas pour la suite du projet.