Rapport de Mise en Œuvre d'une Infrastructure Cloud Sécurisée sur AWS

Conformité à ISO 27001 et Gestion des Risques avec Modèles STRIDE et DREAD

Projet de Sécurisation et Mise en Place d'une Infrastructure Cloud

Date de soumission : [Insérer la date]
Présenté par : [Ton nom]
Encadrant : [Nom de l'encadrant]
Entreprise/Organisation : [Nom de l'entreprise]

Résumé

Ce rapport présente la mise en œuvre d'une infrastructure Cloud sécurisée sur Amazon Web Services (AWS), en utilisant des services tels que EC2, RDS, S3 et ELK, pour héberger un site web et une solution de gestion des logs de sécurité. Le projet suit les meilleures pratiques de sécurité et se conforme aux normes ISO 27001 pour garantir la protection des données sensibles et la résilience de l'infrastructure. En outre, une gestion rigoureuse des risques a été mise en place en appliquant les méthodologies de **modélisation des menaces STRIDE** et **évaluation des risques DREAD**.

Table des matières

1. **Introduction**
    - Contexte du projet
    - Objectifs du rapport
    - Méthodologie
    - Importance de la sécurité et de la conformité
    - Structure du rapport
2. **Partie 1 : PLAN**
    - 2.1. Objectifs du projet
    - 2.2. Définition de l'infrastructure Cloud sur AWS
        - Services AWS utilisés (EC2, RDS, S3, ELK)
        - Architecture Cloud et schéma de réseau
    - 2.3. Identification des risques
        - Méthodologie de gestion des risques
        - Modèle STRIDE et analyse des menaces
    - 2.4. Conformité aux normes ISO 27001
        - Politique de sécurité et gestion des actifs
        - Inventaire des actifs
        - Gestion des accès et des données sensibles
    - 2.5. Plan de traitement des risques
        - Evaluation des risques (DREAD)
3. **Partie 2 : DO**
    - 3.1. Mise en œuvre de l'infrastructure Cloud
        - Création et configuration des instances EC2
        - Déploiement de RDS pour la gestion des bases de données
        - Mise en place des buckets S3 pour le stockage des logs
        - Déploiement du SIEM ELK pour la gestion des logs de sécurité
    - 3.2. Configuration de la sécurité sur AWS
        - Politiques IAM (Identity and Access Management)
        - Contrôles de sécurité réseau (VPC, NACL, Security Groups)
        - Cryptage des données (en transit et au repos)
    - 3.3. Utilisation de Terraform et CloudGoat pour la gestion de l'infrastructure et les tests de sécurité
    - 3.4. Mise en place de la surveillance et des alertes
4. **Partie 3 : CHECK**
    - 4.1. Tests de sécurité et vérification de la conformité
        - Tests de pénétration (Pentests)
        - Vérification des configurations AWS (Best Practices)
    - 4.2. Analyse des résultats de DREAD et STRIDE
    - 4.3. Audits de conformité ISO 27001
        - Evaluation des contrôles de sécurité
        - Évaluation de la gestion des risques
    - 4.4. Validation des performances et de la résilience de l'infrastructure
    - 4.5. Révision des logs et rapports de SIEM
5. **Partie 4 : ACT**
    - 5.1. Résultats des évaluations et ajustements nécessaires

- 5.2. Améliorations de la sécurité et de la gestion des risques
- 5.3. Mise à jour des politiques de sécurité et des contrôles
- 5.4. Plan d'amélioration continue et recommandations
- 5.5. Processus d’audit de certification et actions à mener

6. **Conclusion**
   - Récapitulatif des principales actions réalisées
   - Bilan de la conformité et de la sécurité de l’infrastructure Cloud
   - Perspectives d’amélioration et de maintenance continue
7. **Annexes**
   - A.1. Diagrammes d'architecture réseau
   - A.2. Liste des services AWS et configurations
   - A.3. Résultats des tests de pénétration et audits de sécurité
   - A.4. Exemples de configurations Terraform
8. **Références**
   - Bibliographie et sources utilisées

Introduction

Dans un environnement numérique en constante évolution, la sécurité et la conformité des infrastructures Cloud sont devenues des priorités cruciales pour les entreprises cherchant à protéger leurs données sensibles et assurer la continuité de leurs opérations. Le projet décrit dans ce rapport vise à concevoir, déployer et sécuriser une infrastructure Cloud sur Amazon Web Services (AWS), tout en assurant la conformité aux exigences de sécurité ISO 27001.

Contexte du projet

L'objectif principal de ce projet est de mettre en place un environnement Cloud pour héberger un site web et une solution de gestion des logs de sécurité, en utilisant des services d'AWS tels qu'EC2, RDS, S3 et un système SIEM basé sur ELK (Elasticsearch, Logstash, Kibana). Ce projet doit garantir non seulement la performance et la disponibilité de l'infrastructure, mais aussi la sécurité des données et la conformité aux standards de gestion des risques.

Objectifs du rapport

Ce rapport présente la planification, la mise en œuvre, et la gestion des risques associés à l'infrastructure Cloud sur AWS. Il est structuré selon le modèle **PDCA** (Plan-Do-Check-Act), qui permet d'assurer une approche continue d'amélioration de la sécurité et de la conformité. Le rapport décrit également les processus de gestion des risques appliqués à l'infrastructure, en se basant sur des méthodologies telles que le **modèle STRIDE** pour l'identification des menaces et **DREAD** pour l'évaluation des risques.

Méthodologie

La méthodologie employée repose sur plusieurs étapes essentielles :

1. **PLAN** : Définition des objectifs, des services nécessaires et des risques associés à l'infrastructure.
2. **DO** : Mise en œuvre de l'infrastructure Cloud sur AWS, configuration des services et sécurité.
3. **CHECK** : Évaluation de l'infrastructure via des tests de sécurité, analyses des logs et vérification de la conformité aux normes ISO 27001.
4. **ACT** : Réajustement des politiques de sécurité et des contrôles en fonction des résultats des évaluations, amélioration continue de l’infrastructure.

Importance de la sécurité et de la conformité

Le respect des normes de sécurité et de conformité est essentiel pour protéger les données sensibles de l'entreprise et éviter les risques de violations de sécurité. En suivant les principes de la norme ISO 27001, ce projet s'assure que des contrôles de sécurité adéquats sont en place pour répondre aux exigences légales et réglementaires, tout en garantissant la résilience et la sécurité de l'infrastructure Cloud.

Structure du rapport

Ce rapport est structuré comme suit :

1. **Plan** : Description des objectifs, des ressources nécessaires et de l’évaluation des risques.
2. **Do** : Mise en œuvre de l'infrastructure Cloud avec les services AWS.
3. **Check** : Évaluation des résultats des tests de sécurité, audit de la conformité.
4. **Act** : Ajustements des politiques de sécurité et des contrôles basés sur les résultats de l’évaluation.

2. PLAN (Planification des actions)

La phase PLAN consiste à définir la stratégie, les objectifs et les actions nécessaires pour déployer une infrastructure Cloud sécurisée et conforme sur AWS. Cela inclut l'identification des services nécessaires, l'analyse des risques, la définition des politiques de sécurité, la planification de la gestion des risques, et l'établissement des ressources et des processus pour maintenir la conformité ISO 27001.

2.1. Objectifs du projet

L'objectif principal du projet est de déployer une infrastructure Cloud sur AWS pour héberger un site Web sécurisé. Cette infrastructure doit utiliser Amazon RDS pour le stockage des bases de données, Amazon S3 pour le stockage des logs, et un SIEM (ELK) pour assurer le monitoring et l'analyse des événements de sécurité. L'ensemble doit garantir une haute disponibilité, une sécurité des données optimale, ainsi qu'une gestion et une surveillance efficaces des logs et des incidents de sécurité.

Objectifs spécifiques :

- Fournir un environnement sécurisé pour l'hébergement du site Web.
- Implémenter un SIEM pour la collecte, l'analyse et le stockage des logs de sécurité.
- Mettre en place des mécanismes de sauvegarde et de récupération des données via RDS et S3.
- Assurer la conformité avec les exigences de sécurité définies par ISO 27001.
- Réaliser une évaluation des risques et appliquer des contrôles appropriés.

2.2. Définition du périmètre du projet (Scope)

Le périmètre de ce projet inclut la mise en place des services suivants sur AWS :

- EC2 pour l'hébergement du site Web et de l'application.
- RDS pour la gestion de la base de données.
- S3 pour le stockage des logs et des sauvegardes.
- SIEM (ELK) pour la collecte, l'analyse et la gestion des logs de sécurité.
- VPC pour isoler et sécuriser les ressources internes.
- IAM (Identity and Access Management) pour gérer les accès et la sécurité des utilisateurs.

Le projet exclut la gestion des utilisateurs finaux du site Web, ainsi que la configuration des services AWS non liés à la sécurité et au stockage des logs.

2.3. Analyse des risques et gestion des risques

2.3.1. Identification des risques

Les risques suivants ont été identifiés pour l'infrastructure Cloud :

- **Accès non autorisé aux ressources** : Risque lié à une mauvaise gestion des accès aux ressources AWS.

- **Violation de données** : Risque de fuite de données sensibles hébergées sur l'infrastructure.
- **Perte de disponibilité** : Risque d'indisponibilité du site Web ou du SIEM en raison de défaillances matérielles ou d'attaques.
- **Mauvaise configuration des services** : Risque lié à des configurations incorrectes des services AWS, telles que les groupes de sécurité ou les buckets S3.

2.3.2. Méthodologie de gestion des risques

La gestion des risques suivra une approche combinée utilisant **STRIDE** pour identifier les risques et **DREAD** pour les évaluer et les classer.

- **STRIDE (Identification des risques)** :
  - **S (Spoofing)** : Risque de falsification d'identité.
  - **T (Tampering)** : Risque de modification non autorisée des données.
  - **R (Repudiation)** : Risque d'absence de traçabilité des actions effectuées.
  - **I (Information Disclosure)** : Risque de divulgation non autorisée d'informations sensibles.
  - **D (Denial of Service)** : Risque de déni de service empêchant l'accès aux ressources.
  - **E (Elevation of Privilege)** : Risque d'élévation des privilèges permettant un accès non autorisé.
- **DREAD (Classification des risques)** :
  Chaque risque identifié sera évalué et classé en fonction des critères suivants :
  - **D (Damage potential)** : L'impact potentiel du risque sur les systèmes et les données.
  - **R (Reproducibility)** : La facilité avec laquelle le risque peut être reproduit.
  - **A (Exploitability)** : La facilité avec laquelle le risque peut être exploité.
  - **D (Discoverability)** : La facilité avec laquelle la vulnérabilité peut être découverte.
  - **E (Affected users)** : Le nombre d'utilisateurs ou de systèmes affectés par le risque.

Les risques seront ensuite classés par ordre de priorité en fonction de leur score DREAD, et des plans de traitement adaptés seront élaborés pour chaque risque, en mettant l'accent sur ceux qui représentent une menace la plus élevée.

2.3.3. Traitement des risques

Les risques identifiés seront traités par :

- **Mitigation** : Mise en place de mesures pour réduire la probabilité ou l'impact du risque.
- **Transfert** : Externalisation des risques à un prestataire de services (par exemple, assurances).
- **Acception** : Pour les risques faibles qui ne justifient pas de mesures supplémentaires.
- **Évitement** : Modification de l'architecture pour éliminer les risques identifiés.

2.4. Sécurisation de l’infrastructure selon ISO 27001

Dans le cadre de la norme ISO 27001, plusieurs contrôles de sécurité devront être appliqués pour garantir la confidentialité, l'intégrité et la disponibilité des systèmes et données.

2.4.1. Politique de sécurité

Une politique de sécurité sera définie pour gouverner l’utilisation des services Cloud et la gestion des données sensibles. Cette politique inclura des directives sur :

- La gestion des identités et des accès via IAM.
- La gestion des configurations sécurisées des services AWS.
- Le chiffrement des données sensibles en transit et au repos (utilisation du chiffrement sur S3, RDS, et dans les communications réseau).

2.4.2. Contrôles d'accès et gestion des identités

La gestion des accès sera contrôlée via des rôles IAM qui appliqueront le principe du moindre privilège. Seuls les utilisateurs autorisés auront accès aux services et ressources nécessaires. Les pratiques suivantes seront mises en œuvre :

- Authentification multifacteur (MFA) pour tous les utilisateurs AWS.
- Contrôle d'accès basé sur des politiques strictes, suivant les besoins métier.

2.4.3. Surveillance et gestion des logs

Les logs de sécurité seront collectés via le SIEM ELK, qui sera configuré pour analyser en temps réel tous les événements de sécurité et générer des alertes en cas d’anomalies. Les logs de tous les services AWS (CloudTrail, CloudWatch, EC2, etc.) seront envoyés vers le SIEM pour centralisation et analyse.

2.5. Planification de la conformité et des audits

- **Conformité ISO 27001** : Un audit interne sera effectué pour vérifier que toutes les mesures de sécurité et les contrôles définis dans le cadre de la norme ISO 27001 sont bien appliqués et respectés.
- **Plan de gestion des incidents** : Un plan de réponse aux incidents sera mis en place pour garantir une réponse rapide et efficace en cas de violation de la sécurité.

2.6. Ressources et chronogramme

2.6.1. Ressources nécessaires

- **Personnel** : Les équipes techniques (développeurs, administrateurs système, ingénieurs sécurité) et les auditeurs internes seront impliqués.
- **Outils** : Terraform pour la gestion de l’infrastructure, CloudGoat pour les tests de sécurité, outils d'analyse des logs comme ELK et CloudWatch.

2.6.2. Chronogramme

Le projet sera déployé en 4 étapes majeures :

- **Phase 1 (15 jours)** : Planification et évaluation des risques.
- **Phase 2 (1 mois)** : Mise en place de l'infrastructure et des services AWS.

- **Phase 3 (15 jours)** : Tests, validations de sécurité, et mise en conformité.
- **Phase 4 (Ongoing)** : Surveillance continue, maintenance et améliorations.

2.7. Conclusion de la phase PLAN

La phase PLAN a permis de définir clairement le périmètre du projet, d'identifier les risques et de planifier la mise en œuvre des services AWS nécessaires pour déployer une infrastructure Cloud sécurisée et conforme à la norme ISO 27001. Le plan a pris en compte les meilleures pratiques de sécurité et de gestion des risques, tout en s'assurant que les objectifs de sécurité et de performance sont atteints.

3. DO (Mise en œuvre des actions)

Dans cette phase, les actions définies dans la phase PLAN ont été mises en œuvre pour déployer l'infrastructure Cloud sur AWS, tout en respectant les exigences de sécurité, la conformité ISO 27001 et en utilisant des pratiques de gestion des risques. Le but est de concrétiser le projet, en intégrant les services nécessaires, en sécurisant l'infrastructure, et en veillant à la bonne configuration des composants.

3.1. Mise en œuvre de l'Infrastructure Cloud AWS

La première étape a été la mise en place des ressources AWS nécessaires pour le déploiement de l'infrastructure Cloud, incluant EC2, RDS, S3, et un SIEM (ELK).

3.1.1. Création de l'Instance EC2 pour le Serveur Web

- **Choix du type d'instance** : Une instance EC2 de type t2.micro a été sélectionnée pour héberger le serveur Web. Ce choix permet d'optimiser les ressources tout en répondant aux besoins de performance du site Web.
- **Sécurisation de l'instance** : L'accès SSH a été restreint aux adresses IP spécifiques à l'équipe technique, et un groupe de sécurité a été configuré pour limiter l'accès uniquement sur le port 80 (HTTP) et 443 (HTTPS).
- **Déploiement de l'application Web :** L'application Web a été déployée dans un conteneur Docker sur une instance EC2, avec une architecture microservices. Un WAF basé sur les règles OWASP protège l'application, et les communications se font en HTTPS. L'authentification est gérée via JWT pour sécuriser les sessions utilisateurs. Conformément au RGPD, les données personnelles sont protégées et les utilisateurs peuvent exercer leurs droits sur leurs données, comme la suppression ou l'anonymisation.

3.1.2. Mise en œuvre du SIEM ELK pour la Surveillance

- **Création d'une instance EC2 dédiée pour ELK** : Une autre instance EC2 a été provisionnée pour héberger le stack ELK (Elasticsearch, Logstash, Kibana).

- **Installation d'ELK sur EC2** : La dernière version du stack ELK a été installée sur cette instance afin de collecter, stocker, et analyser les logs de sécurité.
    - **Elasticsearch** : Utilisé pour indexer et rechercher les logs collectés.
    - **Logstash** : Configuré pour collecter, transformer, et transférer les logs depuis différents services, y compris les logs d'EC2 et d'autres services AWS.
    - **Kibana** : Déployé pour fournir une interface graphique permettant d'analyser et de visualiser les données collectées par Elasticsearch.
- **Configuration de l'intégration avec les logs :** Les logs du serveur web et de CloudTrail ont été envoyés à Logstash pour analyse et visualisation dans le SIEM, avec un stockage supplémentaire dans S3 pour archivage.

3.1.3. Mise en œuvre de S3 pour le Stockage des Logs

- **Création du bucket S3** : Un bucket S3 a été créé pour stocker les logs collectés par ELK. Ce bucket est configuré pour être accessible uniquement par des rôles IAM spécifiés.
- **Chiffrement des logs** : Le chiffrement AES-256 // SSE-S3 (Server-Side Encryption with Amazon S3-Managed Keys) ou SSE-KMS (Server-Side Encryption with AWS KMS) a été activé sur le bucket S3 pour sécuriser les logs stockés.
- **Gestion des versions** : La gestion des versions a été activée afin de garder un historique des logs et permettre la récupération des versions précédentes en cas de besoin.

3.1.4. Mise en œuvre de RDS pour la Base de Données

- **Création d'une instance RDS** : Une base de données Postgresql a été provisionnée sur RDS pour héberger les données du site Web. Ce choix permet une gestion simplifiée et une haute disponibilité des données.
- **Sécurisation de la base de données** : L'instance RDS a été configurée pour ne permettre l'accès qu'aux instances EC2 internes, assurant ainsi qu'aucune connexion externe non autorisée ne puisse accéder à la base de données.
- **Backup et récupération** : La fonctionnalité de sauvegarde automatique de RDS a été activée, avec des snapshots réguliers pour garantir la résilience de la base de données.

3.1.5. Configuration de la Sécurité de l'Infrastructure

- **Mise en place de IAM (Identity and Access Management)** : Des rôles IAM ont été créés pour restreindre les accès aux services AWS en fonction des besoins spécifiques des utilisateurs. Le principe du moindre privilège a été appliqué à chaque rôle.
- **Activation de CloudTrail** : AWS CloudTrail a été activé pour auditer toutes les actions effectuées sur l'infrastructure, permettant ainsi une traçabilité complète des activités liées à la sécurité.
- **Mise en place de CloudWatch** : Des alarmes et métriques CloudWatch ont été configurées pour surveiller les ressources AWS et détecter toute activité anormale.
- **Mise en place de VPC (Virtual Private Cloud)** : Un VPC a été créé pour isoler les ressources internes (comme l'instance RDS, S3 et le SIEM ELK) du réseau public.

Des subnets publics et privés ont été configurés pour garantir une séparation claire entre les ressources accessibles depuis Internet et celles qui doivent être protégées.

3.2. Tests et Validation de la Mise en œuvre

Avant de considérer l'infrastructure comme prête à être mise en production, plusieurs tests ont été effectués pour valider le bon fonctionnement de l'ensemble de l'architecture :

- **Tests de performance** : L'instance EC2 a été testée pour s'assurer qu'elle supporte la charge prévue. Des tests de montée en charge ont permis de vérifier que les performances restaient optimales sous des charges accrues.
- **Tests de sécurité** : Un pentest cloud a été effectué en utilisant CloudGoat et d'autres outils de sécurité pour tester la résistance de l'infrastructure face aux attaques courantes, telles que l'injection SQL, les attaques XSS, et les vulnérabilités liées à AWS.
- **Tests d'intégration** : L'intégration entre les services ELK, S3 et RDS a été testée pour s'assurer que les logs sont bien collectés, stockés et analysés dans l'outil SIEM.

3.3. Documentation et Procédures de Sécurité

Une fois l'infrastructure mise en place, la documentation des processus de sécurité et des configurations a été rédigée. Celle-ci inclut :

- **Documentation des configurations IAM** : Les rôles, politiques et utilisateurs IAM sont documentés pour garantir que toutes les actions effectuées dans l'infrastructure sont traçables et justifiables.
- **Procédures de réponse aux incidents** : Des procédures détaillées ont été rédigées pour répondre rapidement à toute alerte de sécurité détectée par ELK ou CloudWatch.
- **Documentation de la gestion des logs** : Un plan de gestion des logs a été élaboré pour assurer une collecte, une analyse et une conservation des logs dans le respect des exigences de sécurité et de conformité.

3.4. Formation et Sensibilisation

Afin de garantir que l'équipe respecte les meilleures pratiques en matière de sécurité, des sessions de formation ont été organisées. Les principales thématiques abordées incluent :

- **Formation à la sécurité dans le Cloud** : Les équipes ont été formées aux meilleures pratiques de sécurité sur AWS, notamment l'utilisation d'IAM, la gestion des ressources, et l'analyse des logs.
- **Sensibilisation à la conformité ISO 27001** : Les équipes ont été sensibilisées aux exigences de la norme ISO 27001, et aux contrôles nécessaires pour maintenir la sécurité et la conformité de l'infrastructure.

3.5. Conclusion de la phase DO

La phase DO a permis de mettre en place une infrastructure Cloud sur AWS, sécurisée, performante et conforme aux exigences de sécurité et de conformité. Les services AWS tels

qu'EC2, RDS, S3, et ELK ont été déployés et intégrés efficacement pour fournir une solution complète et sécurisée pour héberger le site Web, collecter les logs de sécurité, et garantir la performance et la résilience des services.

4. CHECK (Évaluation et Contrôle)

4.1. Évaluation des Performances et Conformité

Tests de Sécurité et Pentests

Après la mise en place de l'infrastructure AWS, nous avons effectué des tests de sécurité pour évaluer la robustesse de l'environnement et détecter d'éventuelles vulnérabilités. Ces tests incluent des **Pentests Cloud** réalisés à l'aide de **CloudGoat**, un outil conçu pour simuler des attaques sur des environnements Cloud et mettre en évidence les failles de sécurité.

Les résultats des tests ont révélé les vulnérabilités suivantes :

- **Instance EC2 non sécurisée** : Une instance EC2 déployée dans un sous-réseau public était exposée à Internet sans protection adéquate. Les tests ont montré que cette instance pouvait être compromise via des attaques par force brute sur des services exposés.
- **Permissions excessives sur IAM** : Certaines rôles IAM étaient trop permissifs, donnant accès à des actions sensibles comme la gestion des instances EC2 et des buckets S3.
- **Données sensibles non chiffrées sur S3** : Des données sensibles stockées dans un bucket S3 étaient en texte clair, ce qui exposait des informations confidentielles.

Actions Correctives Entreprises

Suite aux résultats des tests de sécurité, plusieurs actions correctives ont été mises en place :

1. **Restriction des accès EC2** : Des groupes de sécurité ont été configurés pour limiter l'accès aux instances EC2 à des IPs spécifiques, et des règles strictes ont été appliquées pour désactiver l'accès SSH non autorisé.
2. **Revue des rôles IAM** : Les rôles IAM ont été révisés pour limiter les permissions, assurant ainsi que seuls les utilisateurs autorisés aient accès aux actions sensibles.
3. **Chiffrement des données S3** : Le chiffrement des données au repos a été activé sur tous les buckets S3 pour garantir que toutes les données sensibles soient protégées.

4.2. Modélisation des Menaces avec STRIDE

Lors de la phase de **modélisation des menaces**, nous avons utilisé la méthodologie **STRIDE** pour identifier les menaces potentielles et définir des stratégies de mitigation.

Résultats de l'analyse STRIDE :

1. **Spoofing (Usurpation d'identité)** :
    - **Menace Identifiée** : Usurpation d'identité via l'exploitation de vulnérabilités dans le processus de gestion des identifiants IAM.
    - **Mesure Mitigée** : Mise en place de l'authentification multifactorielle (MFA) sur tous les comptes IAM, et application de politiques de mot de passe strictes.
2. **Tampering (Altération de données)** :
    - **Menace Identifiée** : Modification non autorisée des données sensibles dans les buckets S3.
    - **Mesure Mitigée** : Activation du chiffrement des données et des logs de modification d'objets S3 pour détecter toute altération.
3. **Repudiation (Repudiation des actions)** :
    - **Menace Identifiée** : Les utilisateurs pourraient refuser des actions qu’ils ont effectuées, rendant l’audit difficile.
    - **Mesure Mitigée** : Activation des logs CloudTrail pour tracer toutes les actions effectuées sur les services AWS.
4. **Information Disclosure (Divulgation d'informations)** :
    - **Menace Identifiée** : Exposition accidentelle de données sensibles en raison d'une mauvaise configuration des permissions sur S3.
    - **Mesure Mitigée** : Révision des permissions d'accès S3 et mise en place de contrôles d'accès basés sur des politiques de sécurité.
5. **Denial of Service (Refus de service)** :
    - **Menace Identifiée** : Potentielle attaque par déni de service contre l'infrastructure EC2.
    - **Mesure Mitigée** : Mise en place d'une architecture scalable utilisant **Auto Scaling** et **Elastic Load Balancer (ELB)** pour répartir la charge.
6. **Elevation of Privilege (Élévation de privilèges)** :
    - **Menace Identifiée** : Utilisation des privilèges d'un utilisateur pour obtenir un accès non autorisé à des services AWS sensibles.
    - **Mesure Mitigée** : Restriction des privilèges IAM et mise en place de contrôles de sécurité renforcés avec des audits réguliers des rôles IAM.

4.3. Évaluation des Risques avec DREAD

La méthode **DREAD** a été utilisée pour évaluer les risques liés aux menaces identifiées dans le modèle de menace. Chaque risque a été évalué selon les critères suivants :

- **D (Damage potential)** : Impact potentiel du risque.
- **R (Reproducibility)** : Facilité de reproduction du risque.
- **E (Exploitability)** : Facilité d'exploitation du risque.
- **A (Affected users)** : Nombre d'utilisateurs affectés par le risque.
- **D (Discoverability)** : Facilité de découverte du risque.

Voici un tableau récapitulatif des risques et de leurs scores **DREAD** :

Risque	D (Damage)	R (Reproducibility)	E (Exploitability)	A (Users)	D (Discoverability)	Score Total
Attaque DoS sur serveur EC2	4	3	4	5	4	20
Exposition de données sur S3	5	3	3	4	4	19
Elevation de privilèges IAM	4	2	3	3	3	15

Les scores DREAD ont permis de prioriser les risques et de concentrer les efforts de mitigation sur les risques les plus critiques. Par exemple, l'attaque **DoS** sur les serveurs EC2 a été jugée comme ayant un impact élevé et a conduit à la mise en place de mécanismes de **scalabilité automatique** et de **répartition de charge** pour atténuer ce risque.

4.4. Résultats des Tests de Performance et Audits de Conformité

Dans cette section, les tests de performance ont montré que le système était capable de gérer une charge accrue, en particulier après la mise en place d'**Auto Scaling** et d'**Elastic Load Balancer (ELB)**. Toutefois, certains ajustements ont été nécessaires pour optimiser la configuration des **groupes de sécurité** et des **permissions IAM**, afin d'assurer un accès sécurisé tout en maintenant les performances.

Audit de Conformité ISO 27001

Un audit interne a été réalisé pour s'assurer que l'infrastructure respecte les exigences de la norme **ISO 27001**. Les éléments suivants ont été évalués :

- **Gestion des accès (Contrôles d'accès IAM)** : Les politiques de sécurité sont conformes aux bonnes pratiques ISO 27001.
- **Chiffrement des données** : Le chiffrement des données au repos sur **S3** et en transit (via **SSL/TLS**) respecte les recommandations de sécurité.
- **Journalisation des événements** : L'utilisation de **CloudTrail** et de **CloudWatch Logs** garantit la conformité aux exigences de surveillance et d'audit.

Les résultats de cet audit interne ont montré que l'infrastructure est conforme à la norme ISO 27001, mais quelques améliorations mineures ont été suggérées pour renforcer la gestion des incidents et la documentation des contrôles de sécurité.

Conclusion de la section CHECK

Dans cette phase, nous avons effectué une évaluation approfondie des risques, des menaces et de la performance de l'infrastructure mise en place. Les tests de sécurité, les évaluations des menaces (STRIDE) et l'évaluation des risques (DREAD) ont permis de prioriser les mesures de sécurité et de prendre des actions correctives pour atténuer les vulnérabilités découvertes. L'infrastructure est désormais prête à passer à la phase **ACT** (Amélioration continue), avec un focus particulier sur la surveillance continue et l'audit des performances de sécurité.

5. ACT (Amélioration Continue et Actions Correctives)

5.1. Améliorations Basées sur les Résultats des Tests

Dans cette phase, toutes les actions correctives et améliorations nécessaires sont mises en œuvre à la suite des résultats de la phase **CHECK**. Les tests de sécurité, les évaluations des risques et les audits de conformité ont permis d'identifier les domaines nécessitant des ajustements. Nous avons pris les mesures suivantes pour renforcer la sécurité et améliorer l'infrastructure dans le respect des bonnes pratiques de sécurité et de la norme ISO 27001.

5.1.1. Sécurisation des Instances EC2

Bien que l'accès SSH non sécurisé ait été limité et les groupes de sécurité correctement configurés, nous avons décidé de renforcer la sécurité de l'instance EC2 en appliquant les actions suivantes :

- **Implémentation d'Elastic Load Balancer (ELB)** pour rediriger le trafic et ajouter une couche de sécurité supplémentaire en distribuant la charge.
- **Renforcement de la gestion des clés SSH** : L'utilisation de **clé SSH** a été renforcée avec des **clépair RSA 4096 bits** pour augmenter la sécurité des connexions.
- **Mise en place de l'authentification multifactorielle (MFA)** pour les utilisateurs ayant des accès privilégiés aux instances EC2.

5.1.2. Révision et Renforcement des Permissions IAM

Suite à la découverte de permissions excessives dans les rôles IAM, plusieurs actions ont été prises pour minimiser les risques d'accès non autorisés et assurer un contrôle granulaire des accès :

- **Application du principe du moindre privilège** : Les rôles IAM ont été révisés et ajustés pour accorder uniquement les permissions strictement nécessaires à chaque utilisateur ou service.
- **Automatisation des contrôles IAM** : Mise en place de **politiques IAM automatisées** avec des outils comme **AWS IAM Access Analyzer** pour analyser les permissions en continu et détecter toute permission excessive.

5.1.3. Amélioration du Chiffrement des Données

Le chiffrement des données sensibles stockées sur S3 a été activé. Cependant, des mesures supplémentaires ont été prises pour renforcer le contrôle sur le stockage des données :

- **Chiffrement obligatoire de tous les objets S3** via des politiques IAM imposant le chiffrement des objets dès leur dépôt sur S3 (en utilisant **AES-256** pour les données au repos).
- **Utilisation de **AWS Key Management Service (KMS)** pour une gestion centralisée des clés de chiffrement, avec des politiques de gestion des clés définies pour renforcer la sécurité.

5.1.4. Renforcement de la Surveillance avec CloudWatch et CloudTrail

Bien que **CloudTrail** et **CloudWatch Logs** aient été activés pour la surveillance, nous avons pris des mesures supplémentaires pour assurer une surveillance continue et proactive de l'infrastructure :

- **Activation des alertes CloudWatch** pour détecter les comportements anormaux ou toute activité suspecte (comme des tentatives de connexion échouées ou des changements dans les configurations IAM).
- **Analyse continue des logs CloudTrail** : Mise en place d'un processus d'analyse continue des logs pour détecter toute activité anormale et agir rapidement en cas de besoin.
- **Création de dashboards personnalisés sur CloudWatch** pour obtenir une visibilité claire sur la sécurité, les performances et la conformité de l'infrastructure.

5.2. Révision et Mise à Jour des Politiques de Sécurité

Dans le cadre de l’amélioration continue, des révisions périodiques des politiques de sécurité sont effectuées pour s'assurer que l'infrastructure reste conforme aux normes de sécurité et qu'elle évolue en fonction des nouvelles menaces.

5.2.1. Revue des Politiques de Gestion des Incidents

Afin de répondre rapidement et efficacement à toute menace ou incident de sécurité, une revue des politiques de gestion des incidents a été réalisée. Les éléments suivants ont été mis à jour :

- **Procédures de réponse aux incidents** : Les procédures ont été améliorées pour inclure des étapes claires et automatisées de détection, de réponse et de récupération après un incident de sécurité.
- **Formation continue des équipes** : Des sessions de formation régulières sont organisées pour les équipes responsables de la gestion des incidents, afin de maintenir un niveau élevé de réactivité et de préparation.

5.2.2. Mise à jour des Règles de Sécurité

Les règles de sécurité, notamment pour les services S3, EC2 et RDS, ont été mises à jour pour tenir compte des nouvelles menaces et des vulnérabilités découvertes. Des actions spécifiques incluent :

- **Révision des contrôles d'accès** : Les **politiques de contrôle d'accès basées sur des rôles** (RBAC) ont été mises en place pour renforcer la gestion des permissions.
- **Renforcement des configurations S3** : Mise en place de règles pour garantir que les buckets S3 ne sont pas accidentellement rendus publics.

5.3. Plan de Continuité et de Récupération

Afin de garantir la continuité des services et la protection des données en cas de défaillance ou de cyberattaque, un plan de continuité des activités et de récupération après sinistre (DRP) a été mis en place. Ce plan inclut les éléments suivants :

- **Sauvegardes régulières des données** : Mise en place de sauvegardes automatisées des bases de données RDS et des données S3 sur une période définie, avec des tests périodiques de la récupération des données.
- **Test de récupération après sinistre** : Un test annuel de la procédure de récupération après sinistre sera effectué pour valider l'efficacité du plan.

5.4. Suivi des Améliorations et Réévaluations Périodiques

Afin d'assurer l'efficacité continue des mesures de sécurité mises en place, un suivi et des réévaluations périodiques de l'infrastructure Cloud sont nécessaires. Les étapes suivantes seront prises :

- **Audits internes réguliers** : Des audits internes seront réalisés tous les six mois pour vérifier la conformité aux normes ISO 27001 et pour identifier toute zone nécessitant des améliorations.
- **Réévaluations des risques** : Les risques seront réévalués en continu à l'aide des méthodologies STRIDE et DREAD afin de rester vigilant face aux menaces émergentes.

5.5. Conclusion de la phase ACT

Dans cette phase, nous avons pris des mesures concrètes pour corriger et améliorer l'infrastructure en fonction des résultats de la phase **CHECK**. La sécurité a été renforcée grâce à des ajustements dans les configurations des services AWS, la mise à jour des politiques de sécurité, et l'activation de mécanismes de surveillance avancés. Le suivi régulier et les audits périodiques garantiront que l'infrastructure reste conforme aux meilleures pratiques de sécurité et aux exigences réglementaires. L'amélioration continue sera essentielle pour maintenir une posture de sécurité robuste dans le temps.

Conclusion

En conclusion, ce projet a permis la mise en place d'une infrastructure cloud sécurisée sur AWS, avec une attention particulière portée à la conformité avec la norme ISO 27001, ainsi qu'à la gestion des risques à travers les modèles STRIDE et DREAD. L'intégration de services tels que EC2, S3, RDS, et l'utilisation de SIEM pour la collecte et l'analyse des logs ont permis de garantir un environnement cloud robuste et sécurisé, adapté aux besoins de l'entreprise.

Les différentes phases de planification, mise en œuvre et évaluation ont été réalisées avec succès, permettant d'assurer la sécurité des données des utilisateurs tout en maintenant une performance optimale du système. Grâce à l'application rigoureuse de l'ISMS (Système de gestion de la sécurité de l'information), le projet a non seulement atteint ses objectifs de sécurité, mais a aussi posé les bases solides pour la gestion continue des risques et l'amélioration de l'infrastructure.

Les tests effectués ont permis d'identifier des vulnérabilités potentielles, et des actions correctives ont été mises en place pour atténuer ces risques, assurant ainsi une couverture de sécurité complète. En suivant les recommandations issues des évaluations DREAD et STRIDE, l'infrastructure est maintenant mieux protégée contre les menaces potentielles.

Prochaines étapes :

1. **Surveillance continue** : Mettre en place un système de surveillance en temps réel pour détecter toute activité anormale ou tentative d'intrusion.
2. **Amélioration continue** : Effectuer des audits réguliers pour garantir la conformité continue avec les normes de sécurité et les meilleures pratiques.
3. **Formation et sensibilisation** : Sensibiliser les équipes internes sur les meilleures pratiques en matière de sécurité cloud et de gestion des données sensibles.
4. **Optimisation des coûts** : Continuer à optimiser les coûts d'infrastructure cloud tout en maintenant un niveau de sécurité élevé.

Ce projet marque une étape significative dans la transformation digitale de l'entreprise, assurant à la fois la sécurité des données et la conformité avec les exigences réglementaires. Grâce à une gestion proactive des risques et une approche de sécurité renforcée, l'entreprise est désormais mieux préparée pour faire face aux défis futurs du cloud computing.