Conception et Déploiement d'un Environnement Cloud Sécurisé Sur AWS avec SLA, RPO et RTO

Contexte et Justification

Les organisations modernes s'attendent à une infrastructure cloud fiable et performante, avec des engagements clairs en termes de disponibilité (**SLA : Service-Level Agreement**), ainsi que des délais de récupération des données (**RPO : Recovery Point Objective**) et des systèmes (**RTO : Recovery Time Objective**) en cas d'incident. Ce projet vise à construire un environnement AWS sécurisé et hautement disponible, garantissant un SLA de **99.98 %**, tout en atteignant des objectifs RPO et RTO adaptés aux besoins métiers.

Objectifs du Projet

Objectif principal

Mettre en place un environnement AWS intégrant les meilleures pratiques en matière de sécurité, de disponibilité et de gestion des risques. L'application débutera avec une base de **1 000 utilisateurs**, avec la capacité d'évoluer pour prendre en charge **jusqu'à 100 000 utilisateurs simultanés.**

Objectifs spécifiques

1. **SLA :** Assurer une disponibilité globale d'au moins **99.98 %** pour les services essentiels.
2. **RPO :** Limiter la perte maximale de données à **5 minutes**.
3. **RTO :** Réduire le temps maximal pour restaurer les services critiques à **30 minutes**.
4. **Architecture sécurisée**
   - Concevoir une infrastructure basée sur les principes de sécurité AWS (**Well-Architected Framework**, modèle de responsabilité partagée).
   - Configurer des mécanismes robustes de contrôle d'accès (**IAM**, **MFA**).
   - Mettre en place un réseau sécurisé (VPC, groupes de sécurité, ACL).
5. **Protection des données**
   - Mettre en œuvre des mécanismes de surveillance et de gestion des incidents via **AWS CloudWatch**, **CloudTrail** et **AWS Config**.
   - Garantir la protection des données avec des outils de chiffrement (**KMS**, **SSE**).
   - Déployer des solutions de sauvegarde et de reprise après sinistre (**RDS Backup**, **AWS Backup**).
6. **Le budget maximal du projet (en dehors du** Free Tier**) est fixé à 1** euros**.**
   Si le cahier des charges exige un budget supérieur, il faudra expliquer l'architecture et les outils nécessaires de manière théorique, sans inclure la mise en place.

Livrables

1. **Document de Conception Technique :**
   - Politique de SLA de **99.98 %**, y compris les services couverts et les exclusions.
   - Tableau détaillant les objectifs SLA, RPO et RTO pour chaque composant.
   - Diagramme d'architecture (ex. : réseau VPC, configuration des zones de disponibilité).
   - Politique de sécurité pour les ressources AWS.
2. **Environnement Cloud AWS Fonctionnel**
   - Configuration sécurisée des principaux services AWS : **EC2**, **S3**, **RDS**, **Lambda**.
   - Gestion des identités et des accès (**IAM**).
   - Infrastructure réseau : **VPC**, sous-réseaux, passerelle NAT, VPN.
3. **Rapport d'Évaluation de la Sécurité**
   - Résultats des tests de vulnérabilité (ex. : **AWS Inspector**).
   - Plan d'amélioration continue pour la sécurité.
4. **Documentation Utilisateur**
   - Guide d'administration de l'environnement AWS.
   - Guide pour la gestion des incidents et la reprise après sinistre.

Plan de Travail Proposé

Phase 1 : Étude Préliminaire

- Analyse des besoins organisationnels.
- Exploration des normes de sécurité applicables (ex. : RGPD, ISO 27001, SOC 2).
- Présentation des services AWS pertinents pour la sécurité.

Phase 2 : Conception

- Élaboration d'une architecture réseau sécurisée (**VPC**, sous-réseaux publiques et privés).
- Définition des rôles et politiques d'accès (**IAM**).
- Choix des mécanismes de chiffrement (**KMS**, **SSL/TLS**).

Phase 3 : Mise en Œuvre

- Déploiement des ressources cloud : **EC2**, **S3**, **RDS**, etc.
- Configuration des services de monitoring (**CloudWatch**, **CloudTrail**).
- Tests des politiques de sécurité et des mécanismes d'accès.

Phase 4 : Validation et Tests

- Réalisation de tests de pénétration.
- Simulation d'incidents pour valider les mécanismes de réponse (basculement, sauvegarde/restauration).

Phase 5 : Documentation et Présentation

- Rédaction du rapport final et des guides.
- Présentation des résultats et démonstration pratique de l'environnement AWS.

Outils et Technologies

1. Services AWS

- **Réseau :** VPC, sous-réseaux, **Route 53**, **VPN**
- **Gestion des identités :** IAM, AWS SSO.
- **Stockage :** S3, Glacier.
- **Sécurité :** AWS WAF, Shield, GuardDuty, Inspector.
- **Monitoring :** CloudTrail, CloudWatch.

2. Outils tiers

- **Terraform** ou **AWS CloudFormation** pour l'infrastructure as code (IaC).
- Outils de tests de sécurité : **OWASP ZAP**, **Nessus**.

Critères d'Évaluation

1. **Respect des bonnes pratiques AWS**
   - Conformité au **AWS Well-Architected Framework**.
2. **Niveau de sécurisation**
   - Respect des objectifs SLA, RPO et RTO dans les simulations.
3. **Documentation**
   - Documentation claire et complète pour l'administration et la gestion des incidents.
4. **Performance et Résilience**
   - Fonctionnalité et robustesse de l'environnement face aux tests.
5. **Présentation et Tests Techniques**
   - Démonstration de l'architecture et des configurations mises en place.
   - Simulation en temps réel d'un scénario de reprise après sinistre pour valider les objectifs SLA, RPO et RTO.
   - Réponses aux questions techniques et justification des choix d'architecture.