Fiche de révision Amazon S3

Généralités

- **Introduction à Amazon S3**
- **Stockage d'Objets** : Amazon S3 stocke des objets (fichiers) dans des "buckets".
- **Utilisations Principales** :
  - Sauvegarde et restauration
  - Archivage à long terme
  - Stockage en nuage hybride
  - Hébergement d'applications et de médias
  - Data Lake pour analyses Big Data
  - Hébergement de sites web statiques
- **Concepts Clés**
  - **Buckets S3**
    - Conteneurs de base pour les objets S3.
    - Un nom de bucket est unique globalement.
    - Doit être créé dans une région AWS spécifique.
  - **Objets S3**
    - Fichiers stockés dans des buckets.
    - Chaque objet a une clé (chemin complet du fichier dans le bucket).
    - Maximum de 5 téraoctets par objet.
    - Pour les objets volumineux (>5 Go), utiliser le téléchargement en plusieurs parties.
  - **Métadonnées et Balises**
    - **Métadonnées** : Paires clé-valeur décrivant l'objet.
    - **Balises** : Étiquettes pour organiser et gérer les objets.
    - **Versioning** : Optionnel pour gérer les versions des objets.
- **Caractéristiques Importantes**
  - **Universellement Unique** : Les noms de bucket doivent être uniques à travers AWS.
  - **Conservation des Données** : Répliques des données dans différentes zones de disponibilité pour haute disponibilité.
  - **Sécurité** : Contrôle d'accès granulaire avec des politiques IAM.
  - **Gestion de Cycle de Vie** : Automatisation de la transition et de l'expiration des données.
- **Interface S3**

- **Clés d'Objet** : Chemin complet du fichier dans le bucket.
- **Pas de Véritables “Répertoires"** : Tout est géré par des clés.
- **Téléchargement en Plusieurs Parties** : Pour les fichiers volumineux (>5 Go).

Sécurité Amazon S3

- **Contrôle d'Accès Basé sur les Ressources :**
  - IAM Policies : Pour les utilisateurs IAM, gèrent les autorisations API.
  - Bucket Policies : Directement attachées aux buckets S3, permettent l'accès croisé et les autorisations publiques.
- **Liste de Contrôle d'Accès aux Objets (ACL) :**
  - Permet des permissions fines au niveau des objets.
  - Moins couramment utilisée aujourd'hui.
- **Chiffrement des Objets :**
  - Assure la sécurité des données stockées via des clés de chiffrement.
- **Politiques de Bucket S3**
- **Format JSON** : Document structuré définissant les permissions.

  Exemple :

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": "*",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::examplebucket/*"
      }
    ]
}
```

- **Principaux Éléments** :
  - Resource : Référence aux buckets et objets concernés.
  - Effect : Autorisation ou refus (Allow/Deny).
  - Action : Actions API autorisées (ex: `GetObject`).

- Principal : Entité à qui s'applique la politique (ex: * pour tous).

- **Scénarios d'Utilisation**
  - Accès Public :
    - Autoriser l'accès public aux objets via une politique de bucket.
  - Accès par Utilisateur IAM :
    - Attribution d'autorisations via une politique IAM pour accéder aux buckets S3.
  - Accès depuis des Instances EC2 :
    - Utilisation de rôles IAM attachés aux instances EC2 pour accéder aux buckets S3.
  - Accès Inter-Comptes AWS :
    - Création de politiques de bucket S3 pour autoriser l'accès d'utilisateurs IAM d'autres comptes AWS.
- **Paramètres de Sécurité Additionnels**
  - Bloquer l'Accès Public :
    - Paramètres Bucket pour empêcher l'accès public même si une politique le permet.
  - Sécurité Contre les Fuites de Données :
    - Mécanismes pour garantir que les données restent privées même en cas de mauvaise configuration de politique.

Classe de Stockage	Durabilité	Disponibilité	Durée Minimale de Stockage	Cas d'Utilisation
S3 Standard	99.999999999 %	99.99%	Aucune	Données fréquemment consultées
S3 Standard-IA	99.999999999 %	99.9%	30 jours	Sauvegardes, récupération après sinistre
S3 One Zone-IA	99.999999999 %	99.5%	30 jours	Copie secondaire de sauvegardes
S3 Glacier Instant Retrieval	99.999999999 %	Variable	90 jours	Archivage de données consultées rarement
S3 Glacier Flexible Retrieval	99.999999999 %	Variable	90 jours	Archivage à long terme
S3 Glacier Deep Archive	99.999999999 %	Variable	180 jours	Archivage à très long terme
S3 Intelligent-Tiering	99.999999999 %	Variable	Variable	Données à accès imprévisible

Types de Chiffrement dans Amazon S3

- **Chiffrement côté serveur (Server-Side Encryption - SSE)**
  - Description :
    - Les données sont chiffrées par Amazon S3 lorsque vous les téléchargez dans un bucket.
    - Amazon S3 gère les clés de chiffrement.
  - Méthodes de SSE :
    - SSE-S3 : Chiffrement géré par S3 (Amazon S3-Managed Keys)
      - Amazon S3 utilise ses propres clés de chiffrement.
      - Chiffrement et déchiffrement automatiques des données.
    - SSE-KMS : Chiffrement géré par AWS Key Management Service (AWS KMS-Managed Keys)
      - Utilise AWS KMS pour gérer les clés de chiffrement.
      - Offre un contrôle supplémentaire sur la gestion des clés et les audits.
    - SSE-C : Chiffrement géré par le client (Customer-Provided Keys)
      - Vous fournissez vos propres clés de chiffrement.
      - Amazon S3 utilise ces clés pour chiffrer et déchiffrer les données.
- **Chiffrement côté client (Client-Side Encryption - CSE)**
  - Description :
    - Les données sont chiffrées par le client avant d'être téléchargées dans un bucket S3.
    - Le client gère les clés de chiffrement et le processus de chiffrement.
  - Méthodes de CSE :
    - CSE avec KMS : Utilise AWS KMS pour gérer les clés de chiffrement côté client.
    - CSE avec des clés gérées par le client (CSE-C): Utilisation de clés fournies et gérées par le client.
- **Comparaison des Méthodes de Chiffrement**

Méthode de Chiffrement	Gestion des Clés	Chiffrement/Déchiffrement Automatique	Contrôle sur les Clés	Cas d'Utilisation
SSE-S3	Amazon S3	Oui	Faible	Chiffrement par défaut pour la plupart des cas d'utilisation.
SSE-KMS	AWS KMS	Oui	Élevé	Conformité réglementaire, audit et contrôle fin des clés.
SSE-C	Client	Oui	Très élevé	Contrôle complet des clés par le client.
CSE-KMS	AWS KMS	Non	Élevé	Sécurisation avant transfert, utilisation avec AWS SDK.
CSE-C	Client	Non	Très élevé	Sécurisation avant transfert, utilisation avec des clés personnalisées.

- **Configuration et Gestion du Chiffrement**
  - Activer le Chiffrement SSE-S3 :
    - Peut être configuré par défaut pour un bucket.
    - Les données sont automatiquement chiffrées lors de l'upload.
  - Utiliser SSE-KMS :
    - Configurez une clé AWS KMS pour votre bucket.
    - Offre des options de contrôle supplémentaires comme la rotation des clés et les audits.

    - Configurer SSE-C :
        - Fournir vos propres clés de chiffrement à Amazon S3 pour chaque opération d'upload.
        - Vous êtes responsable de la gestion et de la sécurité des clés.
    - Mettre en œuvre CSE :
        - Utiliser AWS SDK pour chiffrer les données côté client avant l'upload.
        - Gérer les clés de chiffrement localement ou via AWS KMS.
- Bonnes Pratiques
    - Utiliser SSE par défaut : Pour garantir un chiffrement automatique et simplifié des données.
    - Choisir SSE-KMS pour plus de contrôle : Si vous avez besoin de fonctionnalités avancées comme la gestion des clés et les audits.
    - Implémenter CSE pour une sécurité renforcée : Lorsque vous voulez contrôler totalement le processus de chiffrement.
    - Protéger les clés de chiffrement : Toujours sécuriser et gérer les clés de chiffrement de manière appropriée, surtout pour SSE-C et CSE.

Modèle de responsabilité partagée avec Amazon S3

- **Le modèle de responsabilité partagée** est un concept fondamental pour comprendre les responsabilités en matière de sécurité et de conformité dans le cloud AWS. Ce modèle divise les responsabilités entre AWS et le client, permettant ainsi une gestion efficace et sécurisée des services cloud, notamment Amazon S3.
- **Responsabilités d'AWS**
    - Infrastructure et Réseau
        - Gestion de l'infrastructure physique hébergeant Amazon S3, y compris les centres de données.
        - Maintenance de l'infrastructure matérielle et logicielle.
        - Garantir la capacité et la disponibilité des services S3.
        - Assurer la redondance des installations pour résister aux pannes électriques.
    - Sécurité Physique et Environnementale
        - Surveillance des centres de données pour prévenir les accès non autorisés.

        - Protéger les installations contre les catastrophes naturelles, les pannes électriques et autres menaces physiques.
    - Configuration et Conformité Interne
        - Effectuer des analyses de vulnérabilité et des tests de pénétration sur l'infrastructure.
        - Valider la conformité aux standards et aux réglementations internes.
        - Maintenir les certifications de sécurité et de conformité (par exemple, ISO 27001, SOC 1/2/3).
- **Responsabilités du Client**
    - Configuration des Buckets S3
        - Configurer correctement les buckets S3 pour répondre aux besoins spécifiques en termes de sécurité et de gestion.
        - Mettre en place des politiques de contrôle d'accès (Bucket Policies, IAM Policies).
        - Activer et gérer la versioning pour protéger les objets contre les suppressions accidentelles.
    - Chiffrement des Données
        - Activer le chiffrement côté serveur (SSE) ou côté client (CSE) pour sécuriser les données au repos.
        - Gérer les clés de chiffrement si vous utilisez SSE-C ou CSE.
    - Journalisation et Surveillance
        - Activer les logs d'accès pour surveiller les accès aux buckets S3 (Server Access Logging, AWS CloudTrail).
        - Mettre en place des alarmes et des notifications (Amazon CloudWatch) pour surveiller l'activité des buckets.
    - Gestion des Coûts et de la Performance
        - Utiliser les classes de stockage S3 appropriées (Standard, Intelligent-Tiering, Glacier) pour optimiser les coûts.
        - Configurer les règles de cycle de vie (Lifecycle Rules) pour automatiser le transfert des objets entre les différentes classes de stockage.
    - Conformité et Sécurité
        - Effectuer des audits réguliers de la configuration des buckets S3.
        - Mettre en place des contrôles de conformité pour répondre aux exigences réglementaires spécifiques à votre secteur.

Suivez-nous

- **Site web** : https://lecloudfacile.com
- **Youtube** : https://www.youtube.com/@lecloudfacile
- **Linkedin** : https://www.linkedin.com/company/lecloudfacile/
- **Udemy** : https://www.udemy.com/course/nouveau-aws-cloud-practitioner-clf-c02/?referralCode=8CE99E6C2100F1998BDF
- **Communauté WhatsApp** : https://chat.whatsapp.com/HIeIlLVOJ9xCJKX8VhbLSr