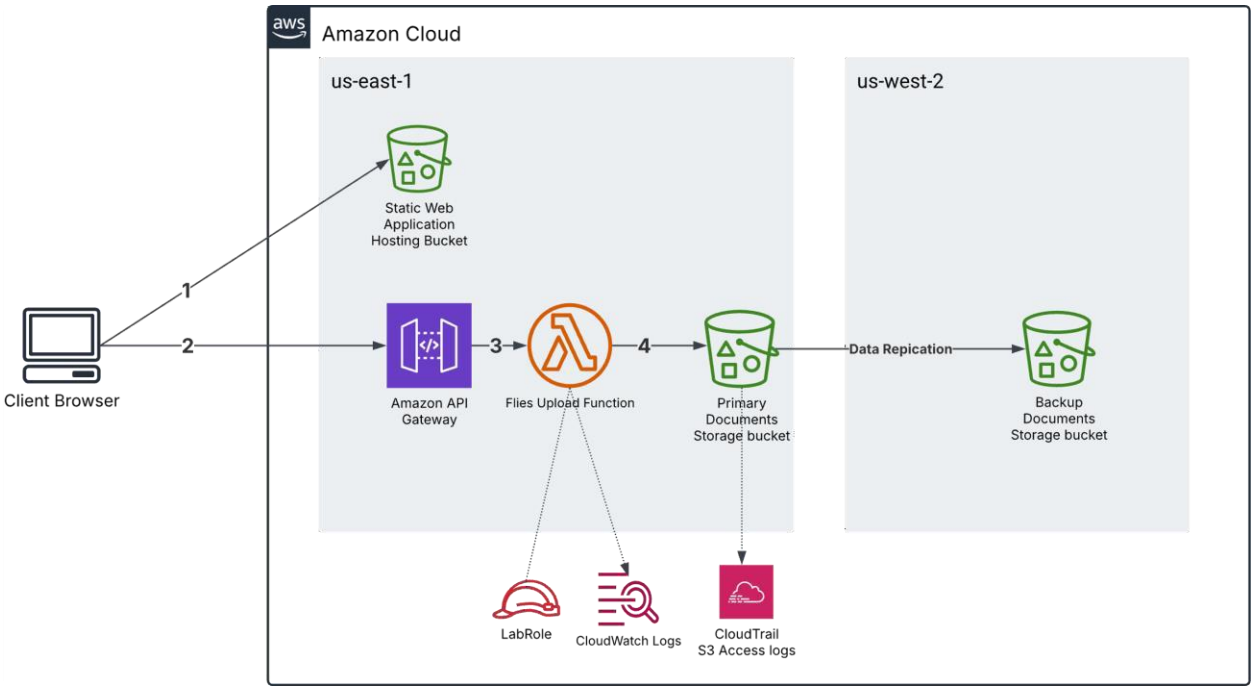
Compétences Ontario : exemple du concours Services infonuagiques



Amazon Cloud – Infrastructure infonuagique Amazon
us-east-1 – us-east-1
us-west-2 – us-west-2
Client browser – Navigateur client
Static Web Application Hosting Bucket – Compartiment d'hébergement d'une application Web statique
Amazon API Gateway –API Gateway d'Amazon
Files Upload function – Fonction de téléversement de fichiers
Primary Document Storage Bucket – Compartiment principal de stockage de documents
LabRole – LabRole
CloudWatch Logs – Journalisation CloudWatch
CloudTrial S3 Access Logs – Journalisation d'accès S3 Cloudtrial
Data Replication – Réplication de données
Backup Documents Storage Bucket – Compartiment de stockage des documents de sauvegarde

Tâches et durée

● La tâche comprend trois (3) modules. Chaque module peut être déployé soit à l'aide de l'AWS Management Console, soit au moyen d'une approche de type infrastructure en tant que code (IaC) (p. ex. Terraform ou CloudFormation) afin d'obtenir des points supplémentaires.

Restrictions et limites

● Limites régionales : toutes les opérations principales doivent être exécutées dans la région *us-east-1*, tandis que la réplication pour la reprise après sinistre doit être effectué dans *us-west-2*.
● Contraintes budgétaires : les solutions doivent être conçues et déployées en respectant un budget maximal de 10 $ pour l'ensemble de la tâche, afin d'éviter de dépasser le budget AWS alloué.

Module 1 : Système sécurisé de stockage de documents (Gateway DataSecure Inc.)

Scénario

Gateway DataSecure Inc., une entreprise spécialisée en cybersécurité, doit mettre en place un système sécurisé de stockage de documents évolutif pour des données clients sensibles. La solution doit être conforme aux principales normes de protection des données (p. ex., HIPAA, RGPD) et prendre en charge le chiffrement, la gestion du cycle de vie, le versionnage, ainsi que la reprise après sinistre. Vous devrez déployer cette solution à l'aide d'Amazon S3 (AWS S3) et la provisionner en utilisant une approche IaC.

Objectif

Créer et provisionner une solution de stockage des documents sécurisée à l'aide d'AWS S3 qui répond aux exigences suivantes:

- Activer le chiffrement au repos (p. ex. chiffrement côté serveur-service de gestion des clés (SSE-KMS)) et le chiffrement des données en transit (HTTPS)
- Mettre en œuvre des règles de gestion du cycle de vie pour optimiser les coûts de stockage
- Activer le versionnage et la réplication inter-régions (CRR)
- Configurer la surveillance et l'audit au moyen d'AWS CloudTrail
- Automatiser le déploiement en utilisant Terraform ou CloudFormation

Tâches

Tâche 1: Compartiment S3 sécurisé

- Créer un compartiment nommé *gateway-datasecure-inc-docs-XXXX* dans la région *us-east-1*
- Autoriser le chiffrement SSE-KMS à l'aide de la clé KMS (avec rotation des clés)

Tâche 2 : Stratégie de compartiment

- Autoriser l'accès *HTTPS-only* au moyen d'une stratégie de compartiment
- Accorder l'accès *LabRole* préalablement fourni

Tâche 3 : Gestion du cycle de vie

- Ajouter des règles pour :
    - Transférer les données vers S3 Standard-IA après 30 jours
    - Transférer les données vers S3 Glacier après 90 jours

Tâche 4 : Reprise après sinistre

- Activer le versionnage
- Créer un compartiment de réplication nommé *gateway-datasecure-inc-crr-XXXX* dans la région *us-west-2*
- Configurer la CRR en utilisant *ReplicationRole*

Tâche 5 : Surveillance et vérification

- Activer la journalisation AWS CloudTrail pour toutes les opérations S3 effectuées dans le compartiment principal

Mise en œuvre d'une approche IaC (extension du module)

Vous devez mettre en œuvre toutes les tâches ci-dessus en utilisant une approche IaC :

- Utiliser Terraform ou CloudFormation
- Fournir un code modulaire, organisé logiquement selon les objectifs fonctionnels
- Référencr les noms de ressources Amazon (ARN) des rôles de gestion des identités et des accès (IAM) fournis (la création de nouveaux rôles IAM est interdite)
- Respecter l'ensemble des conventions d'appellation ainsi que les contraintes régionales

Liste de vérification de la soumission

Veuillez fournir les éléments suivants :

1. Approche IaC :
    a. Terraform : fichiers tels que *main.tf, variables.tf*, etc.

    b. OU CloudFormation : modèles YAML ou JSON
2. `README.md` ou `document` PDF incluant :
    a. Choix de l'outil et justification
    b. Instruction de déploiement
    c. Hypothèses (p. ex., étapes manuelles, IAM ARN)
3. Captures d'écran ou sortie de l'interface de ligne de commande (CLI) confirmant :
    a. Création du compartiment
    b. Configuration de la clé KMS
    c. Règles de gestion du cycle de vie
    d. Configuration de la CRR
    e. Activation de la journalisation CloudTrail

Validation

Avant la soumission, veuillez vous assurer que :

- le chiffrement SSE-KMS est activé
- l'accès HTTPS-only est correctement appliqué
- les règles de gestion du cycle de vie sont mises en œuvre et fonctionnelles
- la CRR est configurée et opérationnelle
- CloudTrail journalise l'ensemble des interfaces de programmation d'applications (API) liés à S3
- aucun rôles IAM supplémentaire n'a été créé
- les conventions d'appellation, la région requise, et les contraintes budgétaires sont respectées

Module 2: Interface de téléversement de fichiers pour le portail Gateway DataSecure Inc., développée au moyen d'une application Web simple

Contexte

À la suite de la mise en œuvre réussie du système sécurisé de stockage dans le Module 1, Gateway DataSecure Inc. souhaite renforcer ses capacités numériques en ajoutant une interface Web simple et conviviale pour ses clients. Cette interface permettra le téléversement sécurisé de différents types de documents (p. ex., .doc, .txt, .pdf, .ppt) directement dans un compartiment AWS S3, tout en assurant une expérience intuitive et sécurisée. L'objectif est de simplifier le processus par lequel les clients soumettent des documents de nature sensible, souvent associés à des dossiers critiques, tout en respectant des exigences strictes en matière de confidentialité et de rapidité de traitement.

Objectif

Concevoir et déployer une interface Web sécurisée permettant aux clients de téléverser des documents, accompagnés de métadonnées, vers une structure de répertoire S3 définie. Vous déploierez cette interface en tant que site Web statique, configurerez des téléversements sécurisés, et mettrez en œuvre une infrastructure en utilisant une approche IaC.

Exigences détaillées

1. Création et configuration du compartiment S3 pour l'hébergement de l'application Web statique

Créez un nouveau compartiment S3 intitulé : *skills-ontario-2025-[votrenom]-web-v1*. Remplacez [votrenom] par votre nom réel (p. ex., johnsmith).

2. Déploiement de l'application Web

Le dossier *upload_to_s3* contient une application Web statique.
Téléversez l'ensemble des fichiers du dossier *upload_to_s3* dans votre compartiment *S3 skills-ontario-2025-[votrenom]-web-v1*.
Ensuite, validez que l'application se charge correctement dans un navigateur en utilisant le point d'extrémité de terminal du site Web statique.

3. Modification de l'application pour téléverser des fichiers dans S3

Configurez l'application pour téléverser les fichiers sélectionnés par l'utilisateur dans le compartiment *skills-ontario-2025-[votrenom]-web-v1*. L'application doit :

- accepter les fichiers téléversés par l'utilisateur
- recueillir le numéro d'identification du client, le numéro d'identification du cas, et le type de document
- téléverser chaque fichier dans une clé structurée, suivant ce format : *uploads/{clientId}/{caseId}/{documentType}/{filename}*

4. Mise en œuvre selon une approche IaC

Utilisez Terraform ou CloudFormation pour :

- créer le compartiment S3, incluant la configuration nécessaire à l'hébergement d'un site Web statique
- configurer tous les paramètres du compartiment
- déployer les fichiers du site Web statique vers S3 en appliquant une approche IaC (*Terraform aws_s3_bucket_object*, ou *CloudFormation AWS::S3::Bucket* + custom resources).

5. Exigences relatives à la soumission

Veuillez inclure les éléments suivants dans votre rapport :

- capture d'écran de l'application Web affichée dans votre navigateur montant le message de réussite
- capture d'écran du contenu de votre compartiment S3, indiquant clairement le(s) fichier(s) téléversé(s).
- capture d'écran du déploiement réussi en utilisant une approche IaC

Créez un tableau qui décrit toutes les modifications que vous avez apportées à :

- l'application HTML/JS
- l'infrastructure AWS (politique S3, CORS, etc.)

Exemple (à des fins de démonstration seulement, il ne s'agit pas de véritables changements) :

Élément	Changement apporté	Motif
index_to_s3.html	Mise à jour du fichier *script.js* avec le nom du compartiment	Assurer la bonne destination de téléversement dans S3
script_to_s3.js	Ajout du chiffrement de l'objet en transit	Garantir que les objets sont téléversés par des voies sécurisées

Rédigez un court paragraphe portant sur les éléments suivants :

- Risques pour la sécurité associés à la solution actuelle (p. ex., authentifiants codés en dur, compartiment public)?
- Bonnes pratiques qui devraient être adoptées
- Amélioration à mettre en œuvre parmi celles proposées, telles que : passer à des URL pré-signées, restreindre l'accès, déplacer les authentifiants dans des variables environnementales.
- Améliorations possibles :
    - Remplacer les authentifiants codés en dur par des authentifiants temporaires obtenus au moyen d'AWS STS.
    - Mettre en œuvre une validation des fichiers côté frontal (limitation des types et des tailles).
    - Utiliser des URL pré-signées pour contrôler l'accès en écriture au compartiment.
    - Restreindre l'accès au compartiment S3 à l'aide d'une politique incluant des référents autorisés.

Soumission

Veuillez fournir les éléments suivants :

- Rapport en Markdown (README.md) ou en format .pdf contenant :
- Captures d’écran
- Tableaux des changements
- Discussion sur la sécurité et les améliorations
- Site Web déployé et pleinement fonctionnel (incluant un lien vers le point d’extrémité de terminal de votre site Web statique S3)

Module 3 : Portail de téléversement de fichiers avec passerelle API propre à l'environnement et stockage de métadonnées dans DynamoDB

Scénario

Gateway DataSecure Inc. étend son système de transfert de fichiers afin de prendre en charge plusieurs environnements (développement et production) tout en permettant le téléversement de documents de manière sécurisée et vérifiable. Les clients transmettront des documents sensibles au moyen d'un simple portail Web. Les fichiers téléversés seront stockés dans S3, tandis que leurs métadonnées seront traitées et enregistrées dans DynamoDB afin de permettre la vérification, l'extraction d'informations et le soutien aux divers flux de travail liés à la conformité.

Objectif

Créer et déployer un système sécurité de téléversement de documents, adapté à l'environnement, en utilisant le dossier *`upload_via_gateway/`*. Votre solution doit inclure :

- Application frontale hébergée dans S3
- Application dorsale mise en œuvre à l'aide d'**API Gateway** et de **Lambda** pour les environnements de **développement** et de **production**
- Métadonnées stockées dans DynamoDB pour chaque fichier téléversé
- Permissions IAM appropriées, traitement des erreurs, et journalisation dans l'ensemble de la pile

Exigences

1. Code et environnements fournis

- Utilisation du code dans le dossier *`upload_via_gateway/:`*
  - `application frontale/`: portail Web pour le téléversement des fichiers
  - `application dorsale/`: modèle de la fonction lambda pour le traitement des téléversements
- Configuration de deux environnements :
  - `Développement` : utilisé pour les essais
  - `Production` : simule un déploiement en environnement réel

2. Hébergement de l'application frontale

- Hébergement de l'application frontale dans un compartiment S3 avec l'option

d’hébergement de sites Web statiques activée

- Portail doit :
  - valider les types de fichiers acceptés : `.doc`, `.txt`, `.pdf`, `.ppt`
  - limiter la taille des fichiers à un maximum de 2Mo
  - exiger des champs de saisie pour les métadonnées : numéro d’identification du `client`, numéro d’identification du cas, type de document
  - afficher le résultat du téléversement (qu’il s’agisse d’une réussite ou d’une erreur)

3. Configuration d’une API Gateway

- Création d’une **API Gateway** comprenant :
  - deux étapes : `développement et production`
  - des intégrations Lambda distinctes pour chaque étape (en utilisant des variables d’environnement ou des alias)
  - CORS activé
  - HTTPS appliqué
  - Journalisation activée pour chaque étape

4. Traitement Lambda (par environnement)

Chaque environnement doit disposer de sa propre fonction Lambda, laquelle doit :

- valider la taille et le type de fichier
- téléverser le fichier dans S3 sous :
uploads/{ClientID}/{CaseID}/{DocumentType}/{filename}

- extraire et stocker les métadonnées dans DynamoDB :
  - `Numéro d’identification du client` (clé de partitionnement)
  - `Numéro d’identification du cas` (clé de tri)

    - `Type de document`
    - `Nom de fichier`
    - `Taille de fichier` (en octets)
    - `Temps alloué pour le téléversement` (format ISO)
    - `Emplacement du téléversement` (chemin S3 ou URL)
- mettre en œuvre le traitement des erreurs :
    - rejeter les données manquantes ou invalides
    - journaliser les étapes de traitement ainsi que les erreurs de traitements dans CloudWatch
    - renvoyer les codes de réponse HTTP appropriés

5. Tableau de métadonnées DynamoDB

- Créer un tableau DynamoDB intitulé *`DocumentMétadonnées`*
- Clés :
    - **Clé de partitionnement** : Numéro d'identification du `client`
    - **Clé de tri** : Numéro d'identification du cas
- Stocker un enregistrement pour chaque fichier téléversé, incluant l'ensemble des attributs de métadonnées
- Assurer une interrogation efficace basée sur le numéro d'identification du `client et le numéro d'identification du cas`

6. Sécurité et IAM

- Utiliser HTTPS pour toutes les communications entre l'application frontale et l'application dorsale
- Ne pas coder les authentifiants en dur
- Utiliser le *`LabRole`* fourni pour toutes les permissions requises par les fonctions Lambda
- Accorder uniquement l'accès requis à S3 et DynamoDB (principe de moindre privilège)

Tâches

Tâche 1 : Hébergement Web statique

- Téléverser l'application frontale dans un compartiment S3
- Configurer l'hébergement du site Web statique
- S'assurer que le portail achemine les fichiers téléversés vers le bon point d'extrémité de terminal API Gateway (développement ou production)

Tâche 2 : API Gateway et étapes

- Créer une API REST avec l'itinéraire *`POST/upLoad`*

- Déployer deux étapes : `développement et production`
- Associer chaque étape à la fonction Lambda qui lui correspond

Tâche 3: Fonctions Lambda propres à l'environnement

- Déployer une fonction Lambda pour chaque environnement
- Utiliser des variables d'environnement pour la configuration (p. ex., nom du tableau, nom du compartiment)
- S'assurer que la fonction puisse effectuer :
    - la validation du fichier
    - le téléversement vers S3
    - l'insertion des métadonnées dans DynamoDB
    - la journalisation

Tâche 4 : Configuration du tableau DynamoDB

- Créer un tableau avec :
    - Clé de partitionnement : numéro d'identification du `client`
    - Clé de tri : numéro d'identification du cas
- Enregistrer les métadonnées à chaque téléversement
- Utiliser *Temps alloué pour le téléversement* et *Nom de ficher* comme attributs supplémentaires

Tâche 5 : Essais et documentation

- Effectuer des essais avec les flux de travail des environnements de développement et de production
- Présenter tous les produits livrables requis

4. Mise en œuvre selon une approche IaC

Utiliser Terraform ou CloudFormation pour :

- créer le compartiment S3 avec l'hébergement de site Web statique activé
- créer une API Gateway comprenant des environnements de développement et de production
- créer et déployer la fonction Lambda

Exigences relatives à la soumission

- URL :
    - Application frontale hébergée dans S3
    - Points d'extrémité de terminal API Gateway (`développement et production`)
- Captures d'écran :
    - Téléversement réussi par l'entremise de l'interface utilisateur

    - Structure des fichiers dans S3
    - Entrée correspondante dans DynamoDB
- Code source :
    - Fonctions Lambda (`développement et production`)
    - Application frontale modifiée (le cas échéant)
    - Mise en œuvre d'une approche IaC
- `README.md` ou format .pdf :
    - Étapes de configuration
    - Différences entre les environnements de `développement et de production`
    - Présentation du schéma de métadonnées
    - Exemple de requête et de réponse API
    - Résumé de la mise en œuvre de la sécurité et de la journalisation