Comprendre les bases d’AWS



Comprendre les services essentiels du cloud

Amazon Web Services, plus connu sous le nom d’AWS, est aujourd’hui l’une des principales plateformes de cloud computing. Pourtant, lorsqu’on découvre son catalogue, les nombreux acronymes et services – EC2, S3, RDS, VPC, IAM ou Lambda – peuvent rapidement donner l’impression d’entrer dans un univers très complexe.

La bonne nouvelle? Il n’est pas nécessaire de connaître tous les services AWS pour comprendre son fonctionnement.

AWS repose avant tout sur quelques principes simples : louer des ressources informatiques selon ses besoins, les déployer rapidement et les adapter à l’évolution de son activité. Voyons comment ces éléments s’articulent.

Qu’est-ce qu’AWS?

AWS est une plateforme de services cloud proposée par Amazon.

Au lieu d’acheter, d’installer et d’entretenir ses propres serveurs, une organisation peut utiliser l’infrastructure d’AWS pour héberger ses

applications, stocker ses données, exécuter des logiciels ou mettre en place des systèmes de sauvegarde.

Les ressources sont accessibles à distance et peuvent généralement être activées ou ajustées à la demande.

Une entreprise peut ainsi utiliser AWS pour :

- héberger un site Web ou une application;
- stocker des fichiers et des sauvegardes;
- exploiter des bases de données;
- analyser de grandes quantités de données;
- automatiser ses déploiements;
- créer des solutions d'intelligence artificielle;
- mettre en place un plan de reprise après sinistre.

L'objectif n'est donc pas simplement de déplacer des serveurs vers Internet. Le cloud permet surtout de concevoir une infrastructure plus flexible, évolutive et disponible.



On distingue généralement trois grandes catégories de services cloud :

- **IaaS – Infrastructure as a Service :** accès à des serveurs, des réseaux et des espaces de stockage virtuels;
- **PaaS – Platform as a Service :** environnement géré permettant de développer et de déployer des applications;
- **SaaS – Software as a Service :** logiciel directement accessible en ligne.

AWS propose principalement des services IaaS et PaaS, tout en offrant

également plusieurs solutions applicatives spécialisées.

Régions et zones de disponibilité : où se trouvent les ressources AWS?

L'infrastructure mondiale d'AWS est divisée en régions.

Une région correspond à une zone géographique dans laquelle AWS exploite plusieurs infrastructures indépendantes appelées **zones de disponibilité**, ou Availability Zones.

Le choix d'une région peut dépendre de plusieurs facteurs :

- la proximité avec les utilisateurs;
- la vitesse d'accès recherchée;
- les exigences réglementaires;
- la localisation des données;
- la disponibilité des services;
- le coût des ressources.

Les zones de disponibilité permettent quant à elles de répartir une application entre plusieurs emplacements isolés.

Par exemple, une entreprise peut déployer son application dans plusieurs zones de disponibilité. Si l'une d'elles rencontre un problème, les autres peuvent continuer à traiter les demandes.

Cette approche contribue à améliorer la disponibilité et la résilience de l'application. Elle doit cependant être prévue dans l'architecture : le simple fait d'utiliser AWS ne rend pas automatiquement un système hautement disponible.

Les services AWS essentiels à connaître



AWS propose plusieurs centaines de services, mais quelques-uns suffisent pour comprendre les fondations de la plateforme.

Amazon EC2 : les serveurs virtuels

Amazon Elastic Compute Cloud, ou **Amazon EC2**, permet de créer des machines virtuelles dans le cloud.

Une instance EC2 peut être utilisée comme un serveur traditionnel pour :

- héberger une application;
- exécuter un logiciel;
- traiter des données;
- faire fonctionner un serveur Web;
- créer un environnement de développement ou de test.

Il est possible de choisir la puissance, la mémoire, le système d'exploitation et la capacité de stockage de chaque instance.

EC2 représente donc la composante « calcul » d'une architecture AWS.

Amazon S3 : le stockage de fichiers

Amazon Simple Storage Service, ou **Amazon S3**, est un service de stockage d'objets.

Il peut notamment servir à conserver :

- des images et des vidéos;
- des documents;
- des fichiers d'application;
- des journaux techniques;
- des sauvegardes;
- des archives.

Contrairement à un disque dur directement attaché à un serveur, les fichiers sont stockés sous forme d'objets dans des compartiments appelés *buckets*.

S3 offre différentes classes de stockage. Une organisation peut ainsi choisir une option adaptée à la fréquence d'accès et à la durée de conservation de ses données.

Amazon RDS : les bases de données relationnelles

Amazon Relational Database Service, ou **Amazon RDS**, permet d'exploiter une base de données relationnelle sans devoir administrer soi-même toute l'infrastructure sous-jacente.

AWS prend en charge plusieurs tâches techniques, comme certaines opérations de maintenance et de sauvegarde, selon la configuration choisie.

RDS prend en charge des moteurs de base de données courants, notamment MySQL, PostgreSQL, MariaDB, Oracle Database et Microsoft SQL Server.

Il s'agit d'un exemple de service géré : l'utilisateur conserve la maîtrise de ses données et de sa configuration, tandis qu'AWS automatise une partie de l'administration technique.

Amazon VPC : le réseau privé

Amazon Virtual Private Cloud, ou **Amazon VPC**, permet de créer un réseau

virtuel isolé dans AWS.

Dans ce réseau, l'organisation peut définir :

- les plages d'adresses IP;
- les sous-réseaux publics et privés;
- les routes réseau;
- les règles de sécurité;
- les connexions avec Internet ou un réseau d'entreprise.

Le VPC permet, par exemple, de rendre un serveur Web accessible au public tout en maintenant la base de données dans un sous-réseau privé.

AWS IAM : les utilisateurs et les permissions

AWS Identity and Access Management, ou **IAM**, permet de contrôler l'accès aux ressources AWS.

IAM répond à une question fondamentale : **qui peut faire quoi sur quelles ressources?**

Une organisation peut créer des utilisateurs, des rôles et des politiques d'autorisation. Elle peut ensuite limiter chaque personne ou application aux ressources dont elle a réellement besoin.

Cette approche correspond au principe du moindre privilège : ne fournir que les permissions nécessaires à l'accomplissement d'une tâche.

AWS Lambda : exécuter du code sans gérer de serveur

AWS Lambda permet d'exécuter du code en réponse à un événement sans devoir gérer directement un serveur.

Une fonction Lambda peut, par exemple, se déclencher automatiquement lorsqu'un fichier est ajouté dans Amazon S3 ou lorsqu'un utilisateur envoie une demande depuis une application.

Cette approche est souvent appelée **informatique sans serveur**, ou *serverless*. Les serveurs existent toujours, mais leur gestion est prise en charge par AWS.

Comment ces services fonctionnent-ils ensemble?

Prenons l'exemple d'une application Web.

Les fichiers statiques, comme les images, peuvent être conservés dans Amazon S3. L'application peut être exécutée sur des instances Amazon EC2 ou avec AWS Lambda. Les informations des utilisateurs peuvent être enregistrées dans une base de données Amazon RDS.

Ces ressources sont organisées dans un Amazon VPC, tandis qu'AWS IAM contrôle les permissions nécessaires à leur utilisation.

Pour rendre l’application plus résiliente, l’entreprise peut également :

- distribuer le trafic avec un équilibreur de charge;
- déployer ses ressources dans plusieurs zones de disponibilité;
- ajuster automatiquement le nombre d’instances selon la demande;
- surveiller les performances et les erreurs avec Amazon CloudWatch.

Chaque service remplit donc une fonction précise, mais leur véritable valeur apparaît lorsqu’ils sont combinés dans une architecture cohérente.

AWS est-il automatiquement sécurisé?



AWS applique un modèle de responsabilité partagée.

AWS est responsable de la sécurité de l’infrastructure physique et des technologies qui font fonctionner ses services. Le client reste toutefois responsable de plusieurs éléments liés à son utilisation du cloud.

Selon les services employés, l’organisation doit notamment protéger :

- ses comptes et ses identifiants;
- les permissions IAM;
- ses systèmes d’exploitation;
- les paramètres réseau;
- ses applications;
- ses données;
- ses sauvegardes.

Une configuration inadéquate peut donc exposer des données même si l’infrastructure AWS elle-même est sécurisée.

Quelques pratiques fondamentales permettent de réduire les risques :

- activer l’authentification multifacteur;
- appliquer le principe du moindre privilège;
- éviter de partager les comptes;
- chiffrer les données sensibles;
- surveiller les activités;
- installer les mises à jour nécessaires;
- tester les sauvegardes et les plans de reprise.

Comprendre ce partage des responsabilités est indispensable avant de déployer une infrastructure en production.

Comment fonctionne la tarification AWS?

AWS utilise principalement un modèle de paiement à l'utilisation.

Une organisation paie selon les services et les ressources qu'elle consomme : durée d'exécution, capacité de stockage, volume de données transférées ou nombre de requêtes, par exemple.

Ce modèle peut être avantageux, mais il ne garantit pas automatiquement une réduction des dépenses.

Les coûts peuvent augmenter en raison de :

- ressources surdimensionnées;
- instances laissées en fonctionnement inutilement;
- volumes ou sauvegardes oubliés;
- architecture mal adaptée;
- transferts de données importants;
- absence de suivi budgétaire.

La maîtrise des coûts doit donc être intégrée à la conception de l'architecture. AWS fournit des outils de suivi, de budgétisation et d'analyse, mais encore faut-il savoir les configurer et interpréter leurs données.

AWS est-il réservé aux développeurs?

Non. De nombreux profils professionnels peuvent être amenés à utiliser ou à comprendre AWS.

Les développeurs s'en servent pour créer et déployer des applications. Les administrateurs système gèrent les infrastructures, les accès et la surveillance. Les spécialistes DevOps automatisent les déploiements. Les architectes cloud conçoivent des solutions sécurisées et résilientes.

Les gestionnaires et responsables de projets technologiques doivent également comprendre les principes du cloud afin d'évaluer les coûts, les risques et les possibilités d'un projet.

Le niveau de connaissances nécessaire varie selon le rôle, mais une compréhension des services fondamentaux facilite la collaboration entre les équipes.

Pourquoi suivre une formation AWS?



Il est possible d’ouvrir un compte AWS et de créer quelques ressources en suivant des tutoriels. Toutefois, cliquer dans la console ne suffit pas pour concevoir une architecture professionnelle.

Une formation structurée permet de comprendre :

- comment sélectionner les services appropriés;
- comment organiser une infrastructure cloud;
- comment protéger les accès et les données;
- comment améliorer la disponibilité;
- comment surveiller les ressources;
- comment éviter les dépenses inutiles;
- comment préparer une certification reconnue.

La pratique accompagnée aide également à éviter les erreurs de configuration et à relier les différents services à des situations professionnelles concrètes.

Développez vos compétences AWS avec Doussou Formation

La formation AWS Solutions Architect Associate (SAA-C03) de Doussou Formation vous apprend à concevoir, déployer et sécuriser des architectures modernes sur Amazon Web Services.

Le programme couvre notamment les fondations du cloud, Amazon EC2, Amazon S3, Amazon RDS, Amazon VPC, AWS IAM, les architectures serverless, la haute disponibilité, la surveillance et l’optimisation des coûts.

Des ateliers pratiques, des études de cas et des exercices de préparation vous permettent de transformer les notions théoriques en compétences directement applicables.

La formation est offerte en classe virtuelle en direct, ainsi qu’en présentiel à Montréal et à Québec. Elle prépare également les participants à la certification AWS Certified Solutions Architect – Associate SAA-C03.

Découvrez la formation AWS Solutions Architect Associate et commencez à bâtir des architectures cloud sécurisées, évolutives et résilientes.