FMS ACADEMY BY FMS

FACYLITIES MULTI SERVICES

Une entreprise ordinaire à l'agilité extraordinaire

FORMATION PYTHON AWS

GESTION D'UNE INFRASTRUCTURE AVEC AWS

martial.bret@fms-ea.com

06 49 71 51 16

Version : 1.0

DMAJ : 29/11/23

FMS-EA 2023 © M. Bret – Tous droits réservés

Module : DEV-AWS-001
AWS

01 – Avoir un panorama détaillé du Cloud Computing
02 – Connaitre les fondamentaux des services AWS
03 – Prendre en main la console Web et AWS CLI
04 – Mettre en place avec CloudFormation une infrastructure de blog (WordPress)
05 – Manipuler avec le service IAM les utilisateurs, groupes d'utilisateurs et politiques d'autorisation
06 – Créer et se connecter à une instance EC2
07 – Créer et utiliser une instance RDS
08 – Déployer une infrastructure avec Terraform

FMS-EA 2023 © M. Bret – Tous droits réservés

Sommaire

FMS-EA 2023 © M. Bret – Tous droits réservés

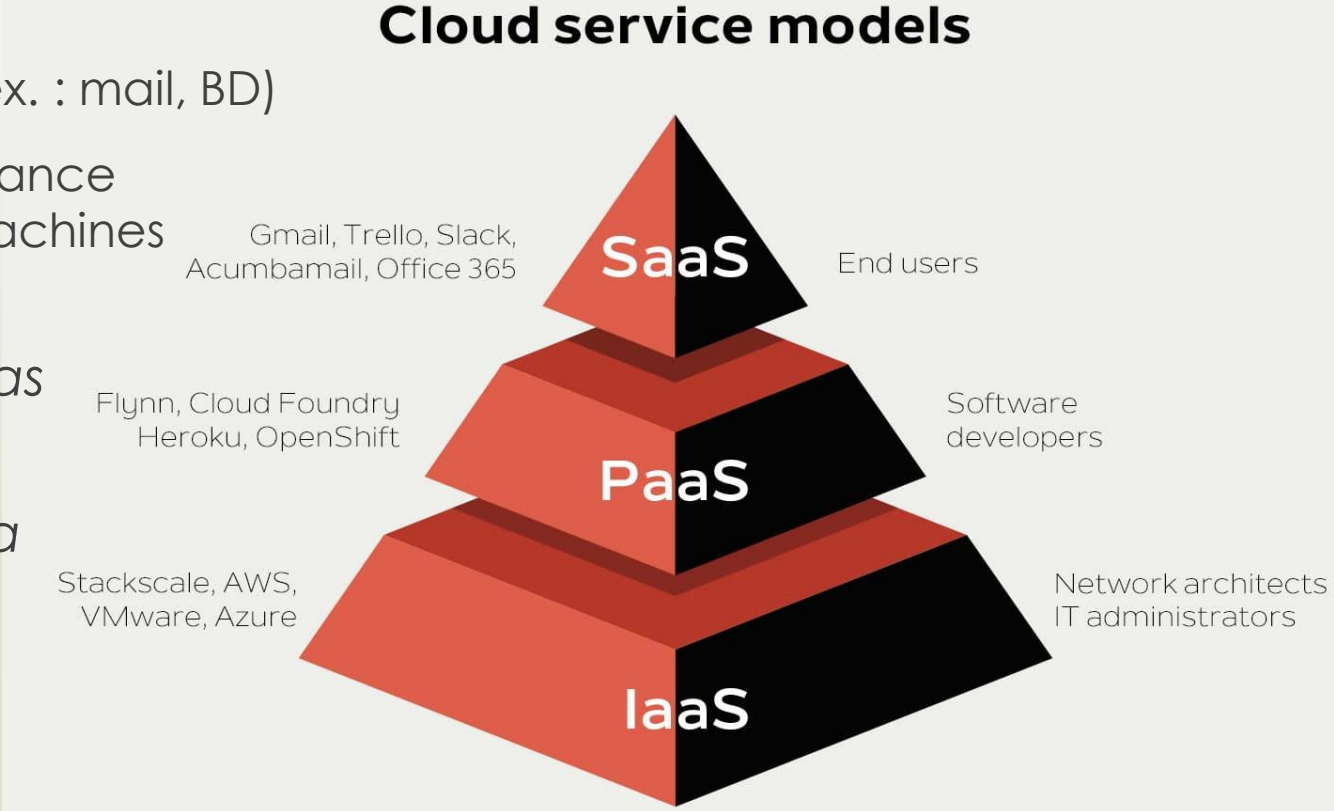
Cloud Computing > historique

- 2002 : Amazon > site de vente en ligne à succès
  - construction grosse infrastructure technique : *datacenters* > serveurs
  - demande croissante → infrastructure croissante et surdimensionnée pour faire face aux pics de charge (ex. : Noël)
  - → idée de louer les serveurs inutilisés hors de ces périodes
    - location à la demande d'un morceau de la puissance d'un serveur
      - ≠ achat ou location machine physique, dite *on-premise*
      - maintenu (disque, mémoire…) par Amazon
    - accessible par réseau, provisionnement rapide, élasticité
    - coût réduit : investissement initial + consommation ressources
    - → client n'a plus besoin d'acheter des serveurs / pics de charge
  - *Cloud* > responsabilité partagée, ex. (IAAS) :
    - AWS : système d'exploitation hôte (dont stockage & réseau), couche de virtualisation, sécurité physique des installations
    - client : système d'exploitation invité (cf. mises à jour), logiciels applicatifs, configuration pare-feu AWS, chiffrage…

FMS-EA 2023 © M. Bret – Tous droits réservés

Cloud Computing > typologie

- IaaS (*Infrastructure as a Service*) > héberger
  - location de la puissance (infrastructure) d'un serveur
- STaas (*Storage as a service*)
- PaaS (*Platform as a Service*) > déployer
  - services offerts (ex. : mail, BD)
  - adaptation puissance et nombre de machines / trafic
- DBaas (*Database as a service*)
- FaaS (*Function as a service*)
- SaaS (*Software as a Service*) > utiliser
  - logiciel en ligne

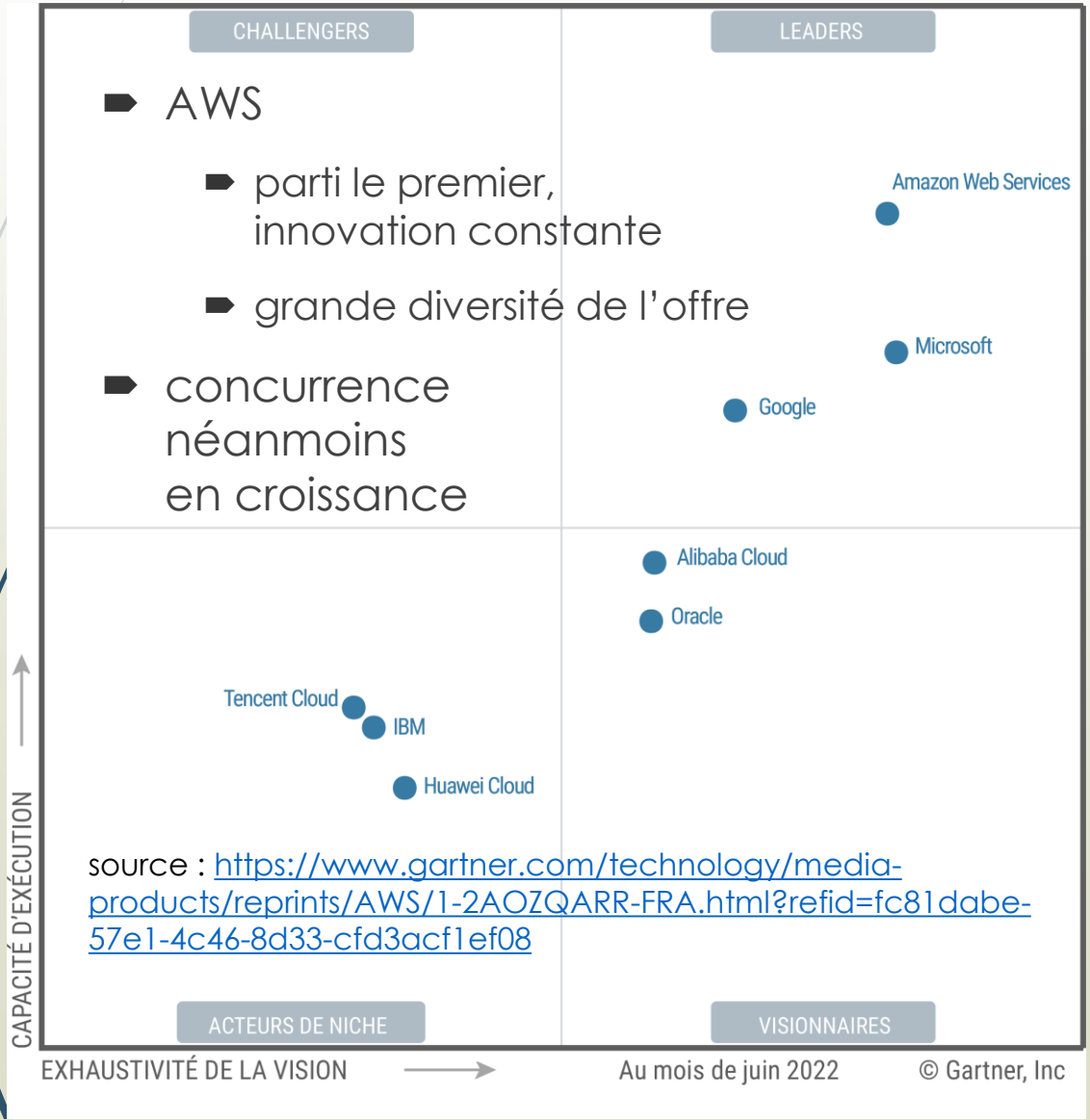


source : https://www.stackscale.com/blog/cloud-service-models/

FMS-EA 2023 © M. Bret – Tous droits réservés

Cloud Computing > panorama

- Principaux fournisseurs PaaS + IaaS
  (part de marché fin 2021, sur ~ $180 milliards)



source : https://www.gartner.com/technology/media-products/reprints/AWS/1-2AOZQARR-FRA.html?refid=fc81dabe-57e1-4c46-8d33-cfd3acf1ef08

AWS	33 %
Azure	21 %
Google Cloud	10 %
Alibaba Cloud	6 %
IBM Cloud	4 %
Salesforce	3 %
Tencent Cloud	3 %
Oracle Cloud	2 %

- Modèles de déploiement
  - public
  - privé
  - hybride
  - multicloud

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > géographie

- Cloud public
  - (très) grande variété de services, tarification à la demande
  - possibilité d'utiliser ses propres OS, BD, architecture de dév.
  - répartition géographique
    - 32 régions (isolées / autres, fonctionnement autonome) > ex. « Europe »
      - 102 AZ (*Availability Zones*), interconnectées au sein d'une même région
        > ex. « EU (Paris) », code **eu-west-3**
        > composée de *datacenters*

source : https://aws.amazon.com/fr/about-aws/global-infrastructure/

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > services 1/2

- de Fondation : piliers principaux d'une infrastructure AWS
  - serveurs
    - EC2 (*Elastic Compute Cloud*) :
      serveur virtuel (*Xen*) configurable > processeurs, OS, mémoire, stockage…
    - ECS (*EC2 Container Service*) : solution Docker
    - VPC (*Virtual Private Cloud*) :
      cloud virtuel privé doté d'une sécurité plus forte que EC2
  - stockage
    - S3 (*Simple Storage Service*) :
      infrastructure de stockage redondante à haute fiabilité
    - EBS (*Elastic Block Storage*) :
      périphérique virtuel de type bloc, branchable sur instance EC2
    - Glacier : ~ S3 > stockage à long terme (ex. : sauvegarde)
    - EFS (*Elastic File System*) : NFS *scalable* à haute performance
  - bases de données
    - RDS (*Relational Database Service*) :
      MySQL, SQL Server, PostgreSQL, Oracle
    - DynamoDB : BD NoSQL
    - Redshift : *data warehouse* (ex. : analyses en temps réel, *data mining*)

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > services 2/2

- de Fondation : piliers principaux d'une infrastructure AWS
  - réseaux
    - ELB (*Elastic Load Balancer*) : service de distribution de la montée en charge
    - Route 53 : service DNS à haute disponibilité
    - CloudFront : service CDN (*Content Delivery Network*)
- Applicatifs : plus spécifiques, utilisables avec services de fondation
  - workflow et messaging
    - *Simple Notification Service* : SMS vers mobile ou service AWS
    - *Simple Email Service* : envoi de courriels en masse
  - … > recherche, diffusion, traitement distribué, multimédia
- Administratifs : gestion de l'environnement AWS
  - identité et accès
    - IAM (*Identity and Access Management*) : gestion des utilisateurs, rôles et permissions, directement ou par fédération (ex. : LDAP, *Active Directory*)
  - monitoring
    - cloud watch (ex. : instance EC2, DB RDS, répartiteur de charge ELB)
  - déploiement et automatisation

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > démarrage 1/2

- Création compte « racine » : https://aws.amazon.com/fr/
  - nécessite la fourniture des informations de paiement d'une carte de crédit
  - 12 mois d'essais gratuits, avec usages limités :
    - EC2 : 750 h / mois d'utilisation d'instance *micro* (Linux ou Windows)
    - S3 : 5 Go de stockage, 20 000 requêtes GET, 2 000 requêtes PUT
    - RDS :
      - 750 h / mois d'utilisation d'instance *micro*
      - 20 Go de stockage et 20 Go de sauvegarde
    - …
  - d'autres services sont avec essai gratuit ou toujours gratuits
  - offres payantes (/ mois) offrant support supérieur
  - *Facturation* >
    - *Préférences de facturation* : ajouter alerte / l'offre gratuite
    - *Budgets* : configurer un budget (ex. *Budget de dépense nul*)
  - Utiliser ce compte uniquement pour de l'administratif

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > démarrage 2/2

- Connexion compte « racine » > Console Web
  - Création compte utilisateur IAM : *Services > Sécurité, identité et conformité > IAM > Utilisateurs > Créer un utilisateur >*
    - [x] *Fournir aux utilisateurs l'accès à la console de gestion AWS*
    - (o) *Je souhaite créer un utilisateur IAM*
    - Options d'autorisations >
      - *Ajouter un utilisateur à un groupe | Copier les autorisations |*
      - *Attacher directement des politiques* > ex. > filtrer > *Gérées par AWS – fonction professionnelle* > [x] *AdministratorAccess* (seulement)
  - Connexion compte utilisateur IAM
    - ID du compte racine à spécifier
    - accès à la console Web
    - menu compte > *Informations d'identification de sécurité > Informations d'identification d'AWS IAM > Créer une clé d'accès > Cas d'utilisation > CLI*
      > récupérer clé d'accès et clé d'accès secrète

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > CLI

- AWS CLI (*Command Line Interface*) >
  - `aws --version`
  - `aws configure`
    - de l'utilisateur utilisant AWS CLI
    - entrer clé d'accès, clé d'accès secrète et région *eu-west-3* (Paris)
- IAC (*Infrastructure as Code*)
  - AWS > CloudFormation
  - `aws cloudformation describe-stacks`
- Terraform : langage de script (HCL) multicloud
  - positionner variables d'environnement `AWS_ACCESS_KEY` et `AWS_SECRET_ACCESS_KEY`

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > sécurité

- Cloud → complexité et coût de sécurisation des équipements matériels déléguées au fournisseur
- AWS > niveaux de sécurité
  - *datacenter* :
    - équipements matériels, réseaux câbles, volumes de stockage, processeurs… > conformité / meilleures pratiques de sécurité
    - bâtiments banalisés, localisation secrète, accès strictement contrôlé
  - OS (natif ou virtuel) : audits de sécurité, correctifs de sécurité…
  - Conformité règlementaire : certification infrastructure AWS / sécurité et protection des données / normes SOC 1, SOC2, SOC 3, FISMA, DIACAP, FedRAMP, ISO 27001 et HIPAA
- Modèle de la responsabilité partagée
  - AWS : infrastructure de sécurité, des services et éléments constitutifs nécessaires
  - utilisateur final : sécurité des données, applications et systèmes d'exploitation >
    - outils fournis : IAM (*Identity Access Management*), MFA (*Multi Factor Authentication*), AWSCloudTrail…

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > IAM > présentation

- IAM (*Identity Access Management*) > permet
  - accès partagé à un seul compte
  - authentification de type multifactorielle
    - nom d'utilisateur et mot de passe +
    - code stocké sur un périphérique spécial
      - smart card, token, application Google Authenticator…
    - clé secrète
  - intégration avec d'autres produits AWS
    - fournit accès granulaire à de nombreux services
  - fédération des identités
    - annuaire LDAP, ActiveDirectory… > utilisateurs, groupes et rôles
  - disponibilité globale > toute région
  - pluralité des mécanismes d'accès
    - console Web, AWS CLI, Terraform, SDK (Java, .NET, Python…), API REST

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > IAM > gestion de l'accès

- Entité
  - types :
    - utilisateur, groupes d'utilisateurs
    - rôle :
      - identité qui peut être endossée par des utilisateurs pendant une courte durée (session)
      - permet de déléguer un accès à des utilisateurs, applications ou services qui n'en sont pas pourvus
    - ressource : ex. : instance EC2, compartiment S3
  - possède un ensemble de politiques d'autorisations, éventuellement assortie d'une limite d'autorisations
- Politique (ensemble) versionnée d'autorisations
  - autorisation (format *JSON*) :
    - effet : *Allow* | *Deny*
    - liste d'actions, portant sur :
    - ressource : spécifiée ou *
    - éventuellement assortie de conditions (ex. : MFA, IP)

FMS-EA 2023 © M. Bret – Tous droits réservés

IaC (Infrastructure as Code)

- Mécanismes pour gérer par du code une infrastructure (informatique) virtuelle complète
  - machine virtuelle, volumes, réseau, DNS, *load balancing*, sous-réseaux, groupes de sécurité…
  - → automatisation du déploiement (cf. DevOps)
    - réduction du coût, du risque
    - rapidité et reproductibilité d'exécution
    - collaboration sur l'infrastructure facilitée
- AWS, Microsoft Azure, Heroku, OpenStack…
- → besoin d'un langage pivot
  - outils Terraform, Pulumi, OpenTofu
    - fichiers descripteurs (variables possibles)
    - interprété via l'API du fournisseur de cloud
    - interaction possible avec outils de gestion, suivi (ex. : monitoring)

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > images et instances 1/4

- service EC2 (*Elastic Compute Cloud*) >
  - capacité de traitement sur demande
  - serveurs virtuels (« instances »)
  - facturation à l'usage
  - cas d'utilisation typiques :
    - hébergement
    - environnement de développement et de test
    - sauvegarde et secours
    - marketing et campagnes publicitaires
    - traitement de haute performance

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > images et instances 2/4

- Image > AMI (*Amazon Machine Images*)
  - modèle préconfiguré servant de base pour la création d'instances
  - OS + applications et services optionnels
  - statique, mais instances (basées sur) modifiables
  - peut être soumise à règles de sécurité
    - ex. : utilisation d'un compte spécifique, privée, payante…
  - AWS Marketplace > achat et vente d'AMI
  - catégories d'AMI (persistance / vie de l'instance) :
    - persistante : ex. : à base d'EBS (*Elastic Block Store*) : volume de stockage, type NAS, transférable entre zone/région
    - volatile : stockage des données via service AWS S3 (*Simple Storage Service*), non transférable entre zone/région
  - AMI Amazon Linux : basé sur RHEL (*Red Hat Entreprise Linux*), facilite intégration avec services AWS

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > images et instances 3/4

- Instance >
  - machine virtuelle créée à partir d'une AMI
  - ensemble de ressources (CPU, mémoire, stockage, réseau) différenciées selon type d'instance > https://aws.amazon.com/fr/ec2/ :
    - usage général : type moyen à utilisation quotidienne
    - calcul optimisé : utilisation intensive de CPU
    - mémoire optimisée :
      - application nécessitant consommation mémoire importante
    - calcul accéléré : accélération matérielle (coprocesseur)
      - calculs des nombres à virgule flottante, traitement graphique, encodage vidéo, machine learning, modélisation 3D
    - stockage optimisé : performances E/S très élevées (SSD)
    - optimisée pour HPC (*High Performance Computing*)
      - simulations complexes de grande envergure
      - deep learning

FMS-EA 2023 © M. Bret – Tous droits réservés

AWS > images et instances 4/4

- Instance > option tarifaire EC2 :
  - instance à la demande >
    - créée dynamiquement
      (possible dans 99 % des cas, selon capacité *data center*)
    - facturée à l'heure
    - 20 instances max. pour compte standard
    - ex. : *t2.micro* >
      - $0,0132 / heure sur région UE Paris = $0.312 / jour
  - instance réservée >
    - déploiement garanti, avec disponibilité 7 j / 7, 24 h / 24
    - économie ~ 30 % / à la demande
    - 3 options de règlement (avec économie croissante) :
      sans avance, avance partielle, à l'avance
  - instance spot :
    - fonctionnement sur la base d'un système d'enchères
    - / problèmes de dépassement de capacité dans AWS
    - prix horaire fluctuant, allocation si (et tant que) enchère > prix

FMS-EA 2023 © M. Bret – Tous droits réservés

Ressources

- Typologie de Cloud et modèles de déploiement :
  - https://www.stackscale.com/blog/types-of-cloud/#What_are_the_costs_of_a_Hybrid_Cloud_environment
  - https://www.vmware.com/fr/topics/glossary/content/private-cloud-vs-public-cloud.html
- AWS
  - https://aws.amazon.com/fr/compliance/shared-responsibility-model/
  - https://docs.aws.amazon.com/fr_fr/cloudformation/
  - https://aws.amazon.com/fr/security/
  - https://docs.aws.amazon.com/iam/
- Sécurité et conformité
  - https://geekflare.com/fr/understanding-compliance/
  - https://aws.amazon.com/fr/compliance/
- Terraform
  - https://blog.stephane-robert.info/docs/infra-as-code/provisionnement/terraform/introduction/
  - https://www.terraform.io/, https://developer.hashicorp.com/terraform/tutorials/aws-get-started

FMS-EA 2023 © M. Bret – Tous droits réservés

Pour aller plus loin

- Cours OpenClassrooms
  - Découvrez le cloud avec Amazon Web Services
  - Déployez vos systèmes et réseaux dans le cloud avec AWS
  - Devenez un architecte de solutions AWS
- Terraform
  - Terraform Language Documentation
- OpenTofu
  - La Linux Foundation lance OpenTofu, une nouvelle alternative Open Source à Terraform
- AWS
  - AWS CloudShell, AWS CodeCommit
  - AWS Cloud9 (IDE Cloud)
  - AWS Educate, AWS Skill Builder
  - AWS Lambda
- LocalStack

FMS-EA 2023 © M. Bret – Tous droits réservés