E-learning

LeCloudFacile.com

AWS Certified

Cloud Practitioner

(en français)





Bienvenue

DE LA PART DE L'ÉQUIPE LECLOUDFACILE.COM



"Ensemble, rendons l'apprentissage du Cloud facile pour tous"

Amadou MERICO | Architecte AWS

LeCloudFacile.com

Les certifications AWS



La certification AWS Cloud Practitioner

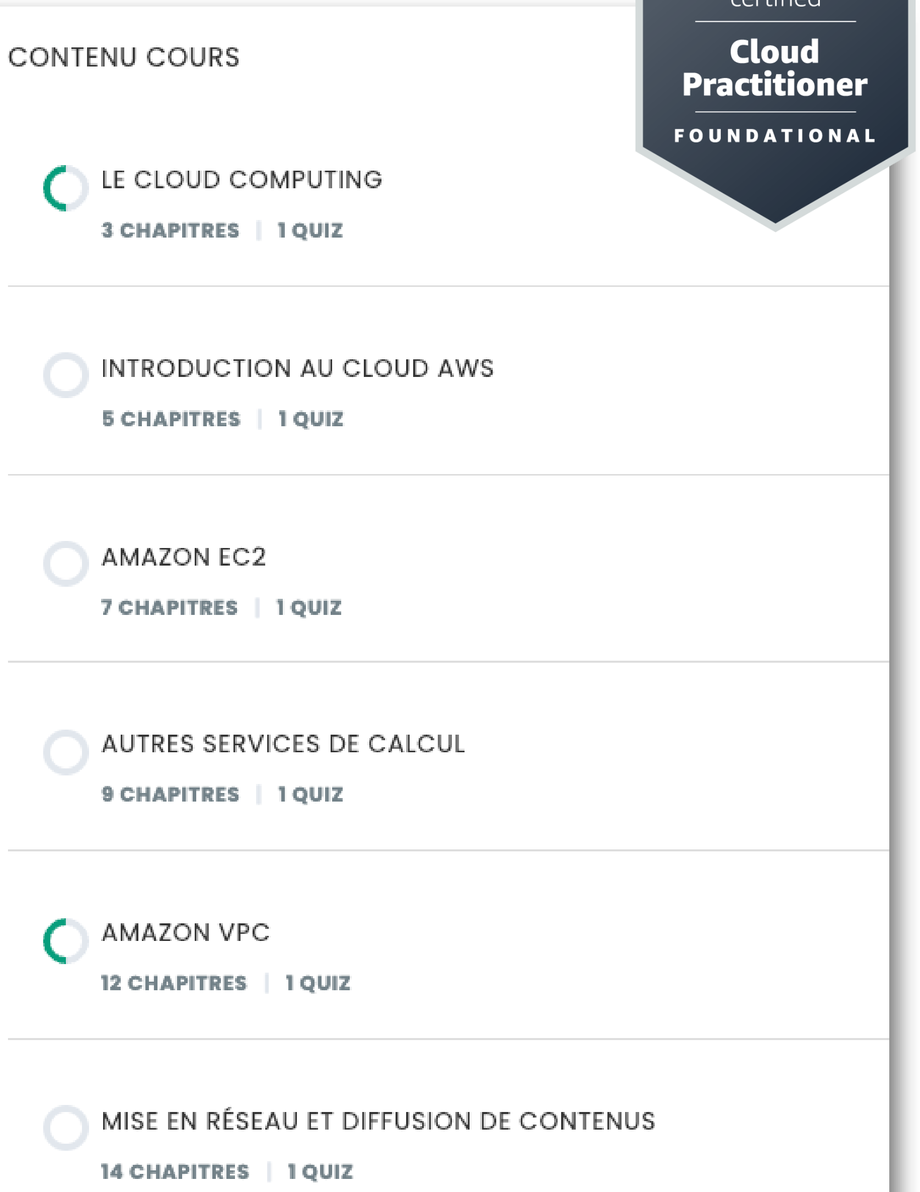
Le certificat **AWS Certified Cloud Practitioner** valide une compréhension fondamentale et de haut niveau des services et terminologie du Cloud AWS. Il s'agit d'un bon point de départ dans le parcours AWS Certification pour les personnes n'ayant aucune expérience préalable en informatique ou en cloud qui se lancent dans une carrière dans ce domaine, ou pour les employés de l'entreprise qui cherchent à acquérir des connaissances de base sur le cloud.



- Compréhension fondamentale et haut niveau du Cloud AWS
- Durée de l’examen : 90 minutes
- Format : QCM 65 questions
- Lieu : centre d’examen ou en ligne
- Langues : Anglais, français,…

Aperçu du cours

- ✓ + 50 heures de vidéo
- ✓ Démos pratiques
- ✓ Quiz de révision
- ✓ Examens Pratiques





Réussir l'examen



Régularité dans l'apprentissage

- Apprenez-en un peu tous les jours
- Planifiez des créneaux
- Prenez des notes

Apprendre par la pratique

- Compte AWS recommandé
- Pratiquez pour comprendre et retenir

Être curieux(se) du cloud

- Explorez la documentation AWS
- Livres blancs
- Blogs, Newsletter, groupe de discussion

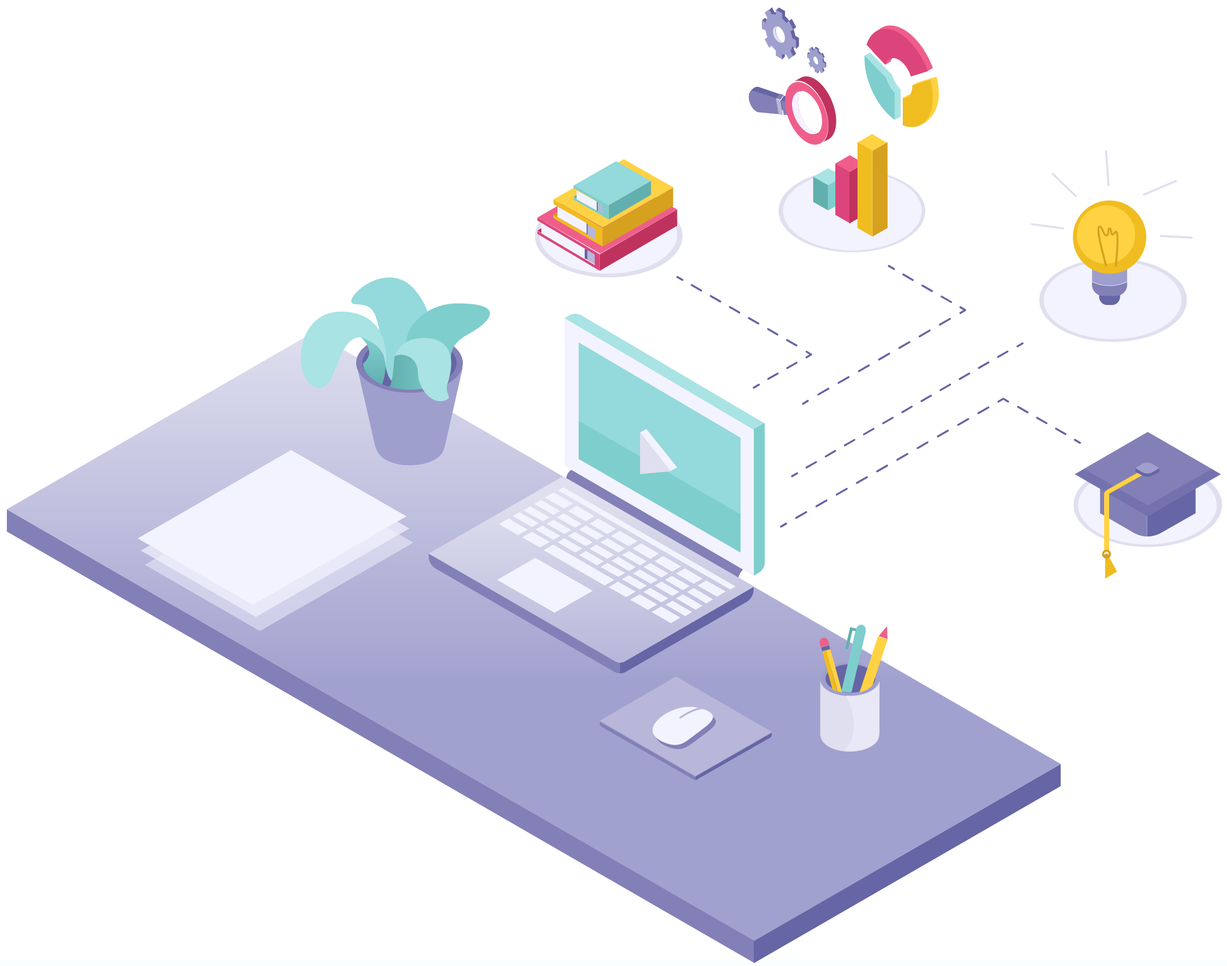




C’est parti !

Module 1 : Le Cloud Computing

Le Cloud vous donne accès à un large éventail de technologies pour innover plus rapidement.



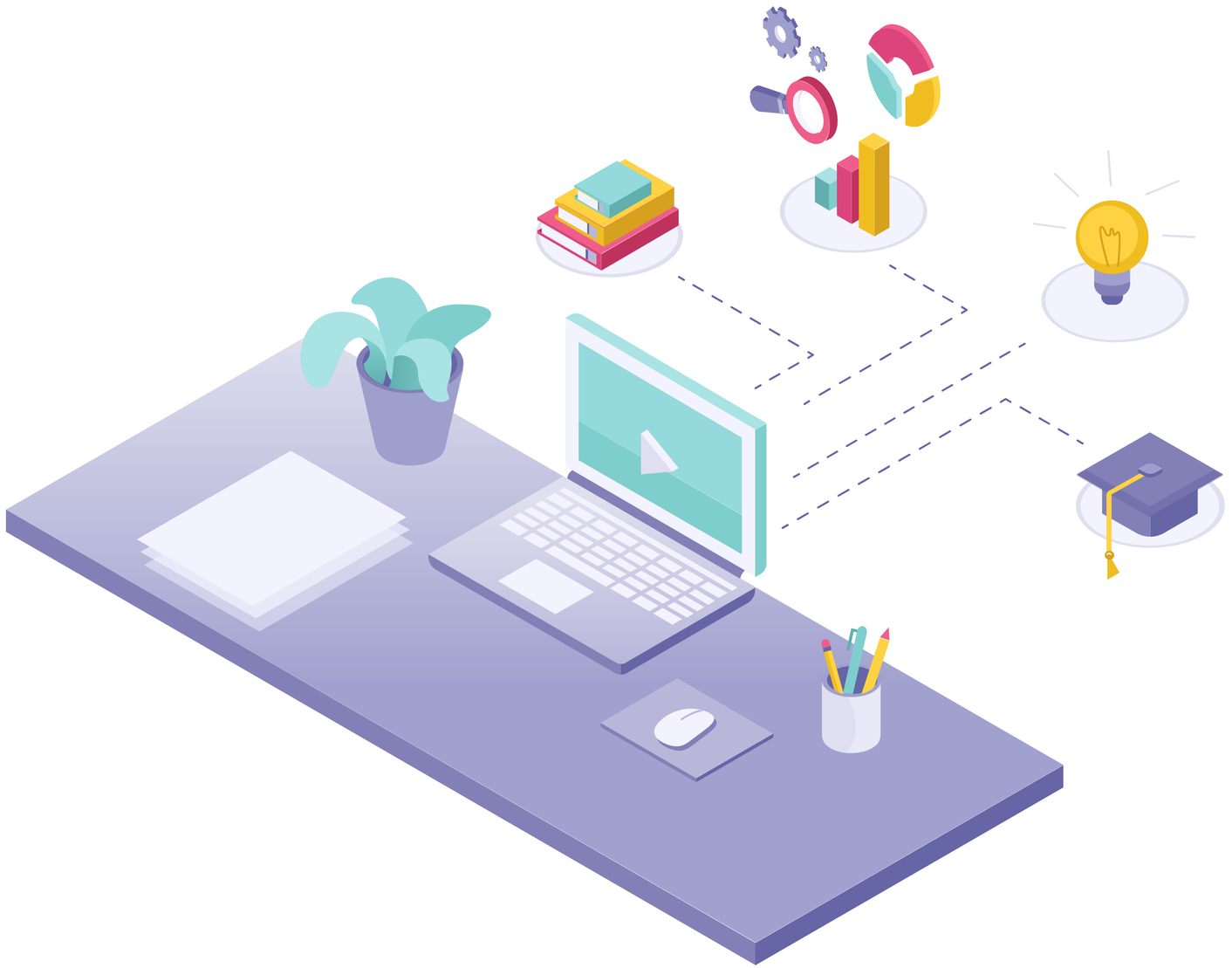
Qu’est-ce que le Cloud ?

Quels sont les types de Cloud ?

Quels sont les avantages du Cloud?



Le Cloud Computing



LeCloudFacile.com

Le Cloud Computing



LeCloudFacile.com

Le Cloud Computing



Le Cloud Computing



Mise à disposition de ressources informatiques à la demande via Internet

Microsoft

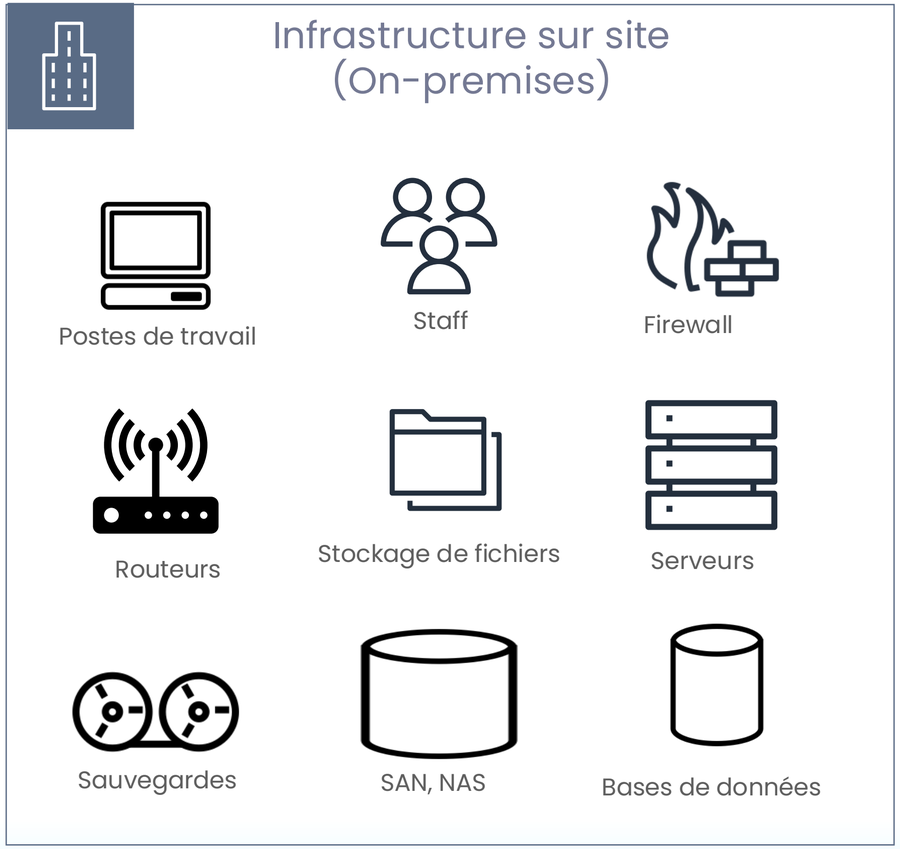
salesforce

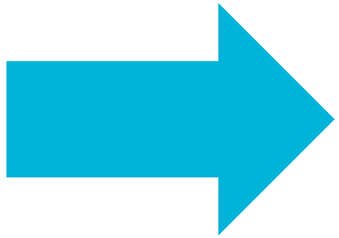
aws

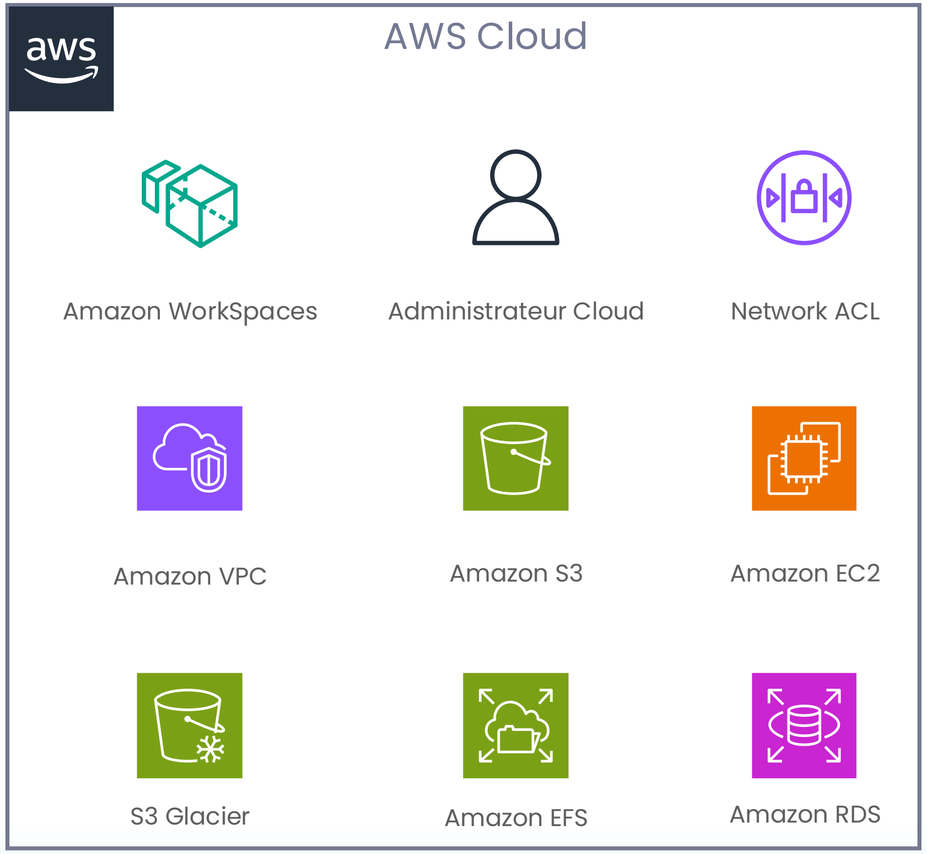
Azure

Google Cloud

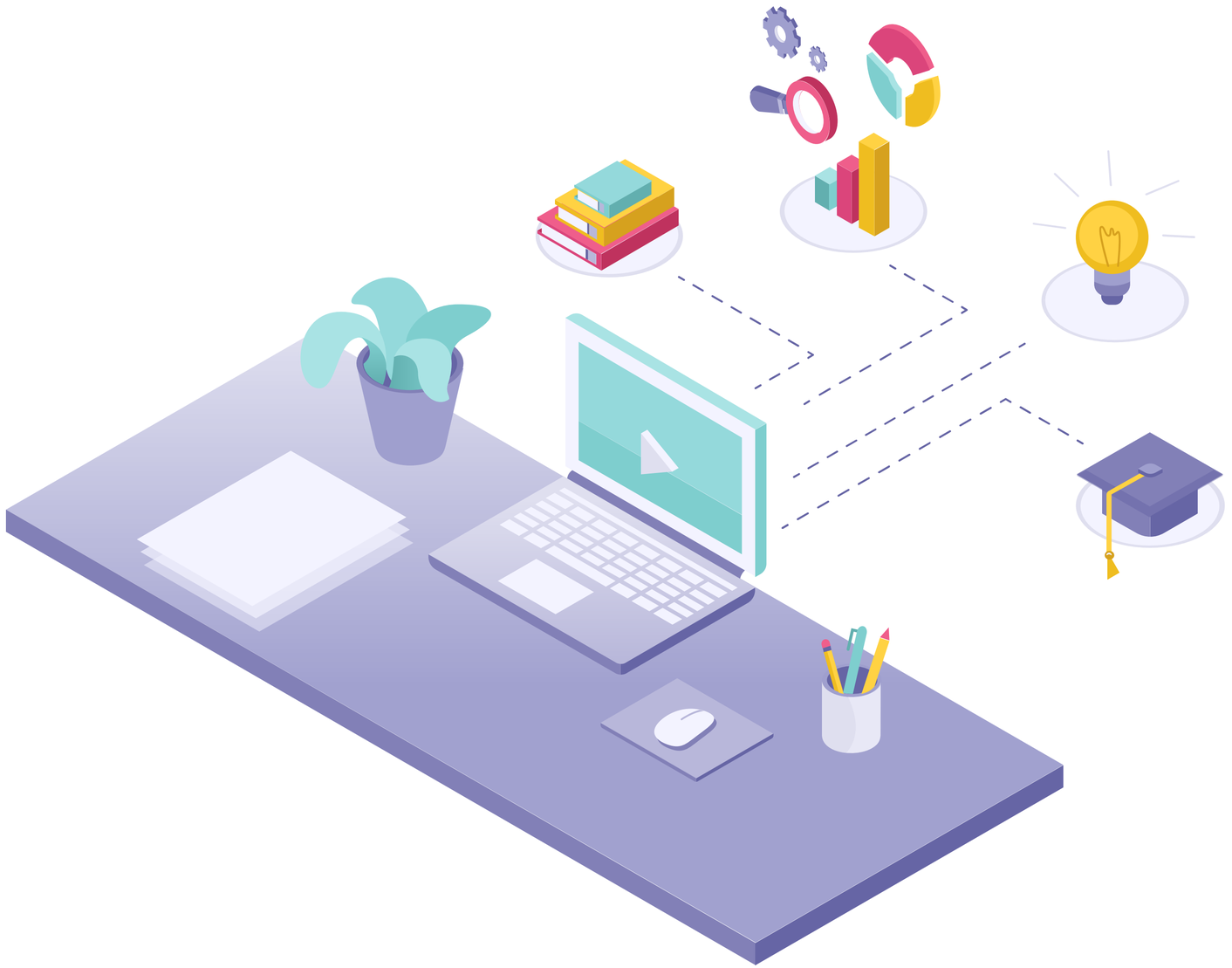
Le Cloud Computing







Modèles et types de Cloud



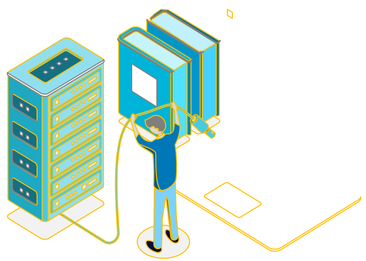
Les modèles de cloud

1. **IaaS**
   Infrastructure as a Service

2. **PaaS**
   Platform as a Service

3. **SaaS**
   Software as a Service

Les modèles de cloud



On-Premises	Iaas	Paas	Saas
Application	Application	Application	Application
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualisation	Virtualisation	Virtualisation	Virtualisation
Serveurs	Serveurs	Serveurs	Serveurs
Stockage	Stockage	Stockage	Stockage
Réseaux	Réseaux	Réseaux	Réseaux

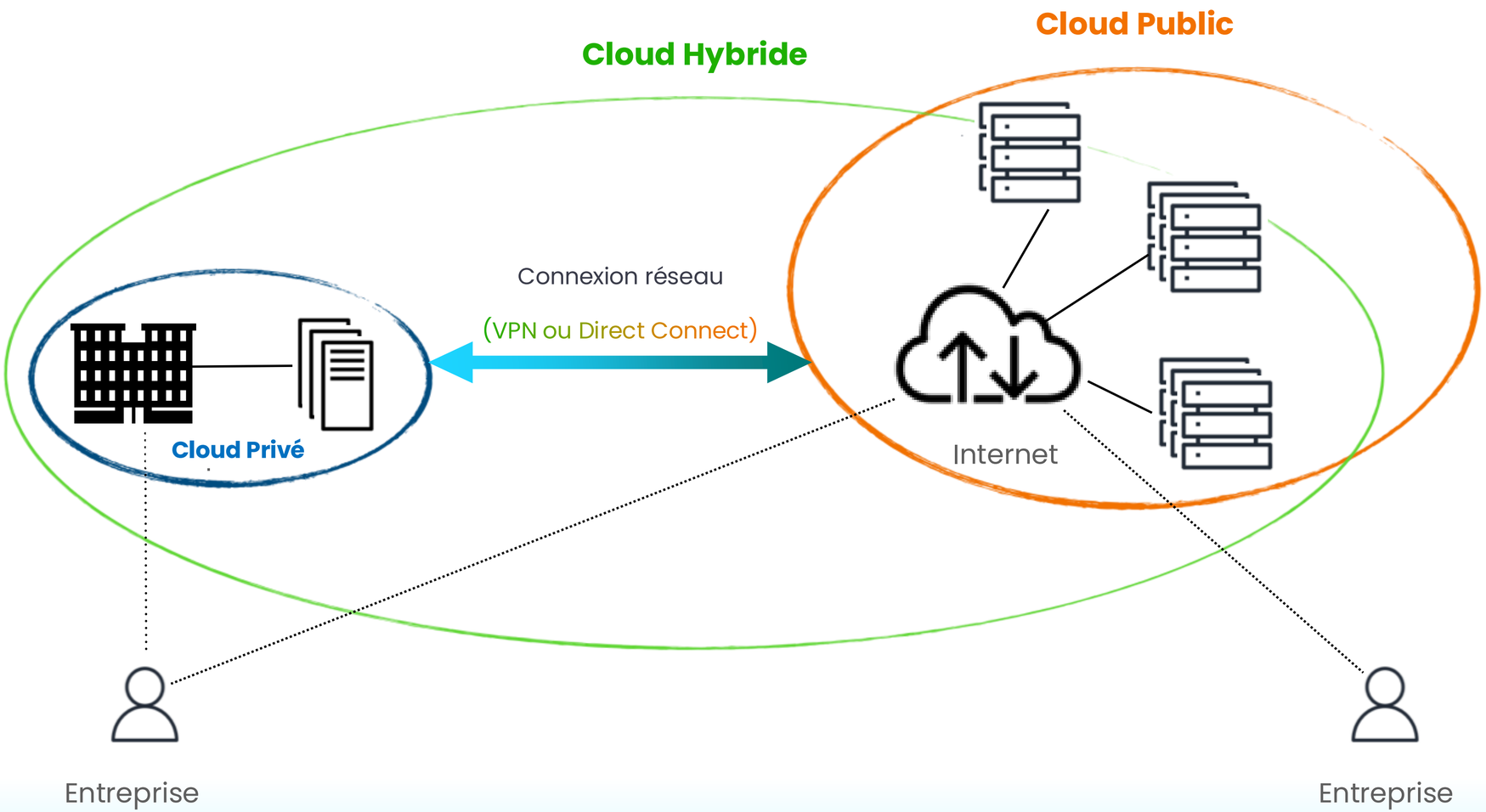
Géré par vous

Géré par le fournisseur

Efforts

Innovation

Les modèles de déploiement



Les modèles de déploiement

Cloud privé

Environnement Cloud dédié à une seule organization

Technos : OpenStack, Openshift, VMWare



Cloud public

Ressources informatiques à la demande accessibles à tous via Internet

Principaux fournisseurs : AWS, Microsoft Azure, Google Cloud Platform







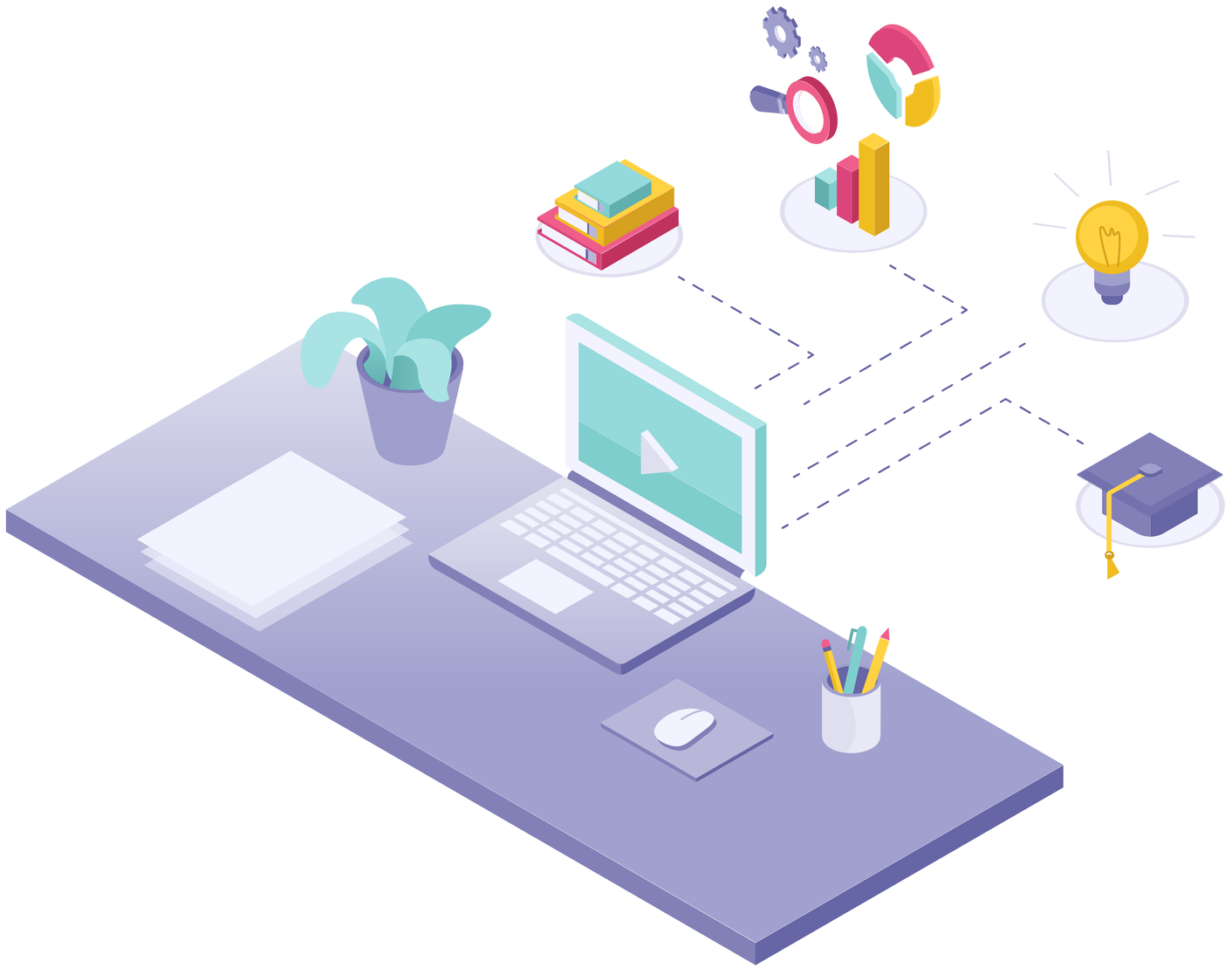
Cloud hybride

Utilisation combinée du cloud public et privé

Connectivité reseau : VPN, AWS Direct Connect



Les avantages du Cloud



LeCloudFacile.com

Les 6 avantages du Cloud

1. Opex vs Capex

Vous ne payez que les ressources informatiques que vous consommez, quand vous les consommez

2. Economies d'échelle

L'utilisation faite par des milliers de clients est cumulée dans le cloud, et se traduit pas des prix inférieurs

3. Capacité adaptée

Vous disposez de la capacité dont vous avez besoin, et vous pouvez l'agrandir ou la réduire en quelques minutes

4. + de Vitesse et d'agilité

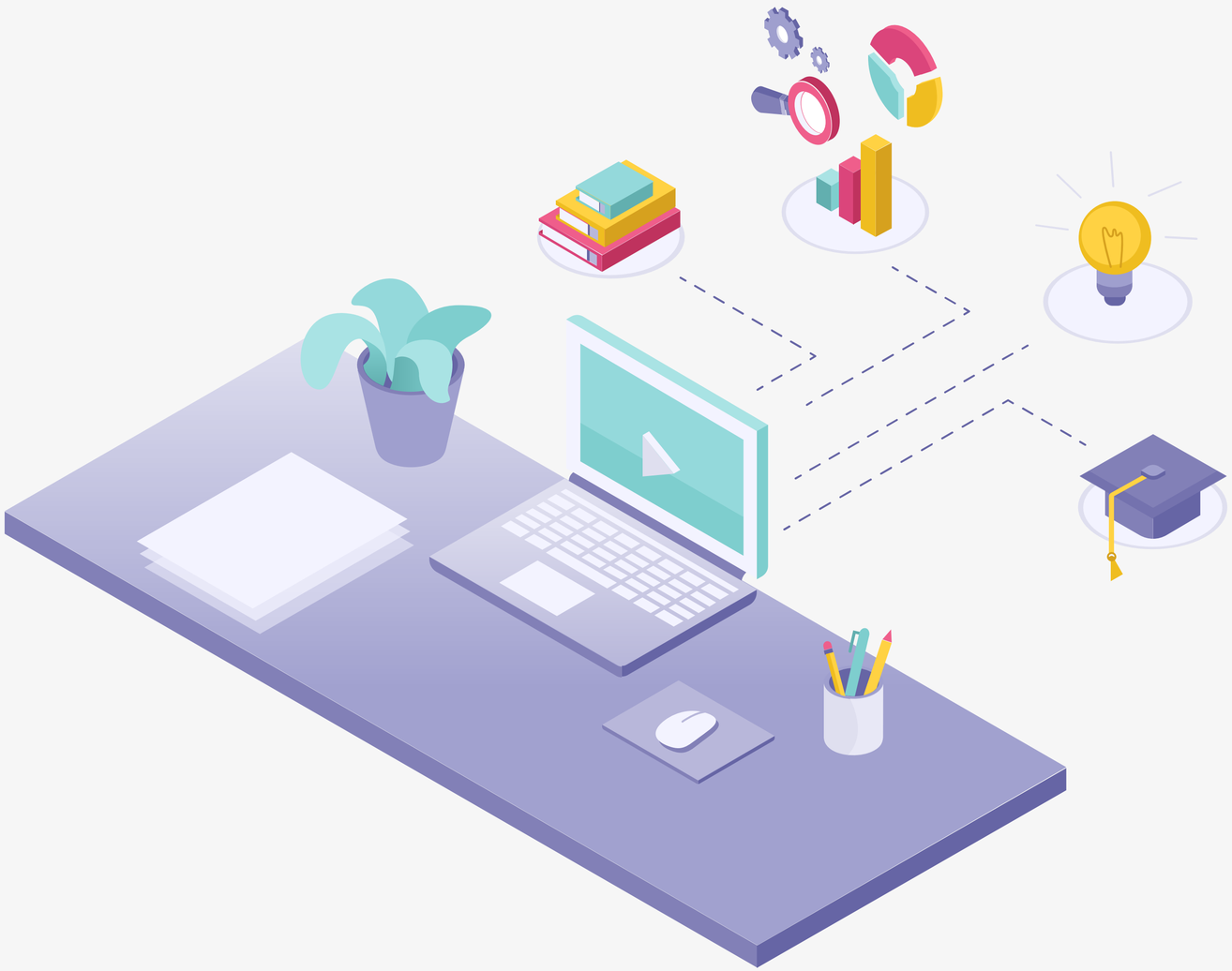
Des Nouvelles ressources informatiques à portée de clic, en quelques minutes au lieu de semaines

5. + d'Innovation

Concentrez vous sur vos projets et clients plutôt que sur la gestion d'infrastructure

6. Déploiement mondial

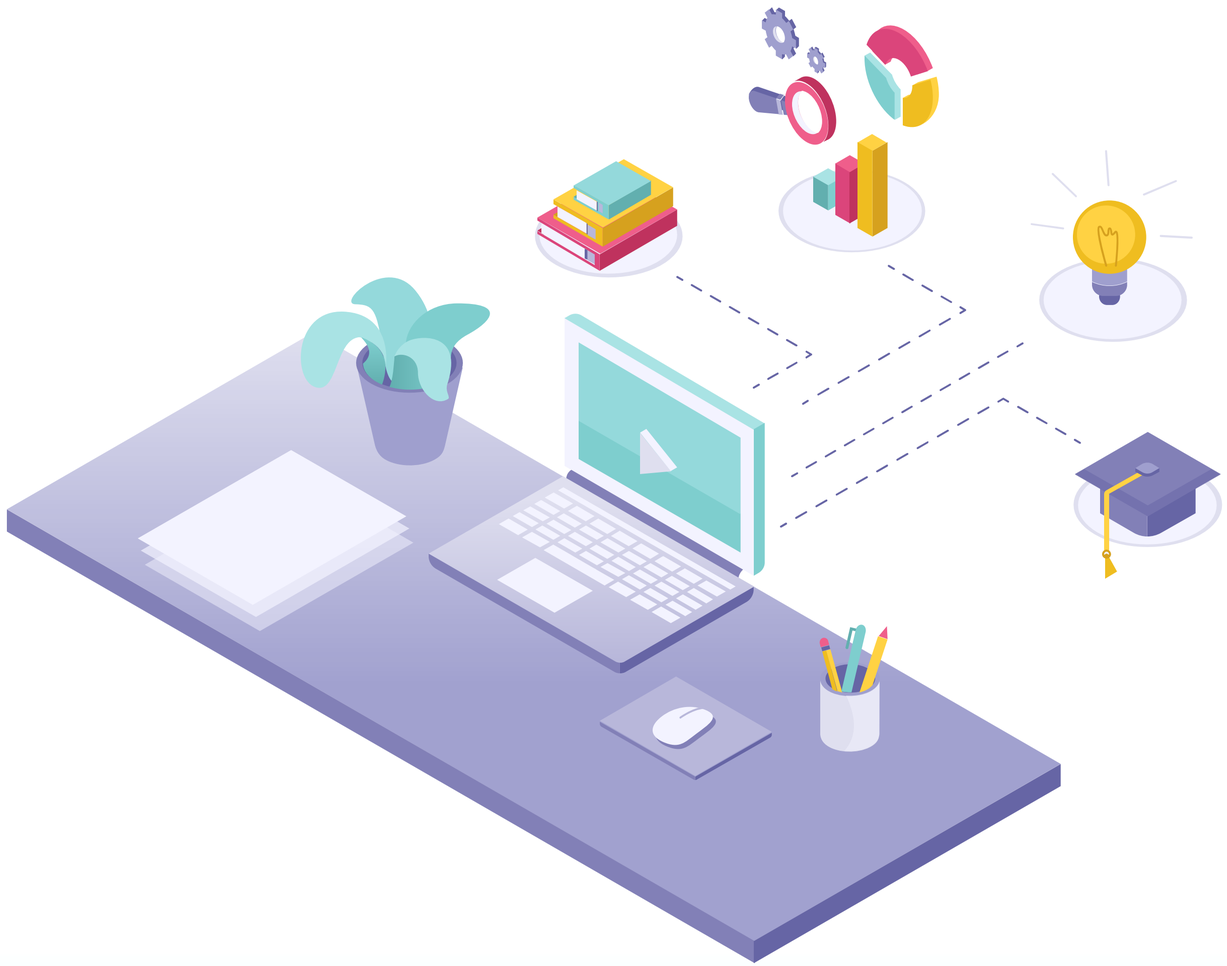
Déployez en quelques minutes dans plusieurs regions du monde



FIN DU MODULE

Module 2 : INTRODUCTION AU CLOUD AWS

Amazon Web Services (AWS) est la plateforme cloud la plus complète et la plus largement adoptée au monde.



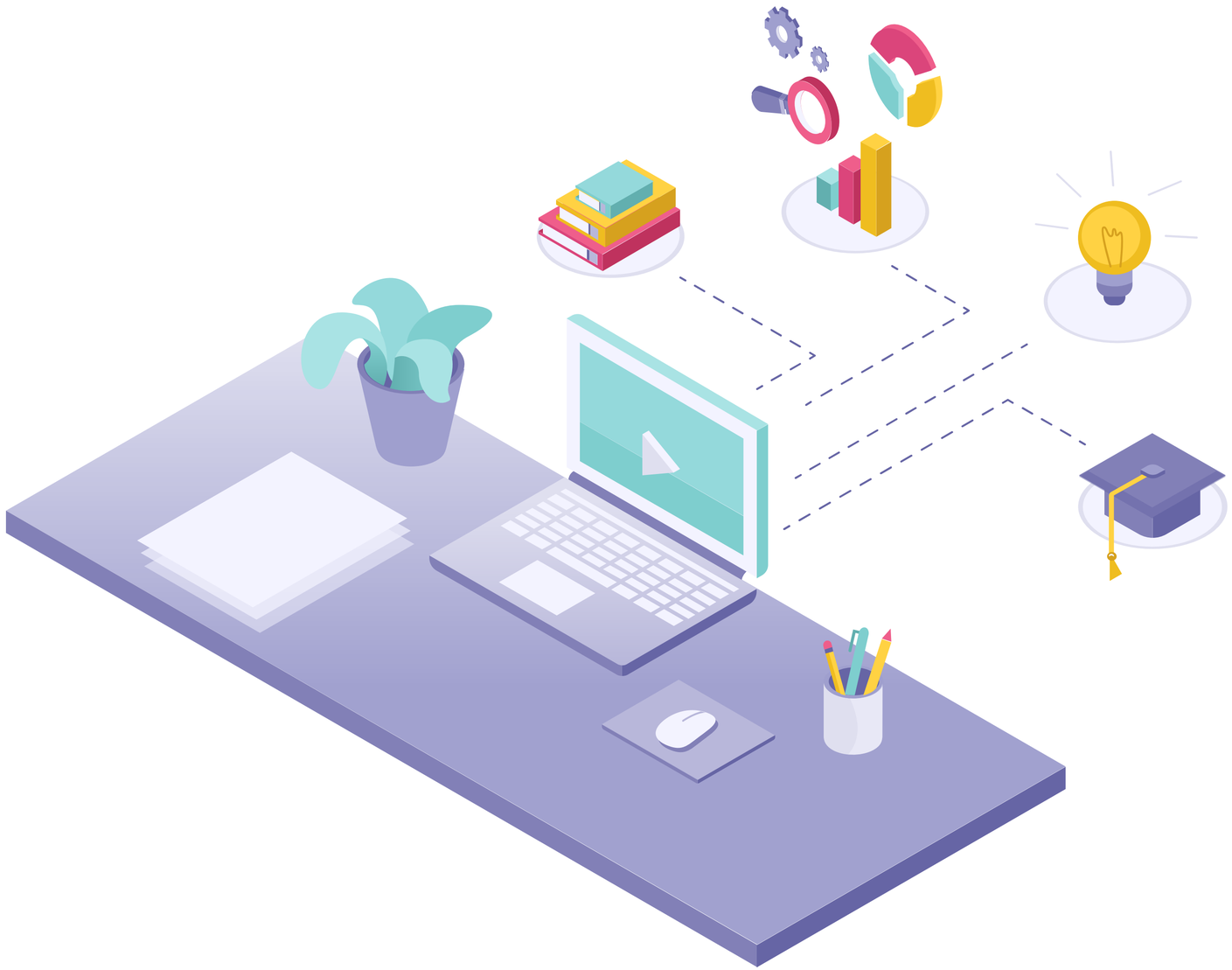
Qu’est-ce qu’AWS ?

Où sont les data centers ?

Comment utiliser le Cloud AWS ?



Présentation d'AWS



Amazon Web Services



Leader du marché du Cloud

Division Cloud du groupe Amazon

Créé en Mars 2006

Fournit +200 services web accessibles par Internet

Des milliers d'entreprises utilisent AWS

airbnb

Au début, l'attrait d'AWS résidait dans la facilité de gestion et de personnalisation de la pile. Pouvoir mettre à l'échelle plus de serveurs sans avoir à contacter quiconque et sans engagements d'utilisation minimale était un excellent atout. Notre entreprise continuait de se développer en même temps que notre confiance au Cloud AWS. Nous avons désormais adopté presque toutes les fonctionnalités offertes par AWS. AWS propose une réponse simple aux entreprises Web qui souhaitent se développer.

– Nathan Blecharczyk, cofondateur et directeur technologique, Airbnb, Inc.

ENGIE

ENGIE Builds the Common Data Hub on AWS, Accelerates Zero-Carbon Transition

ENGIE, a global utility company, built its Common Data Hub data lake on AWS, enabling the company's business units to collect and analyze data to support a data-driven strategy and to lead the zero-carbon transition.

NETFLIX

Netflix on AWS

Netflix is the world's leading internet television network, with more than 200 million members in more than 190 countries enjoying 125 million hours of TV shows and movies each day. Netflix uses AWS for nearly all its computing and storage needs, including databases, analytics, recommendation engines, video transcoding, and more—hundreds of functions that in total use more than 100,000 server instances on AWS.

Customer Stories | Architecture | Additional Resources

Pourquoi Veolia est en train de devenir une entreprise sans datacenter ?

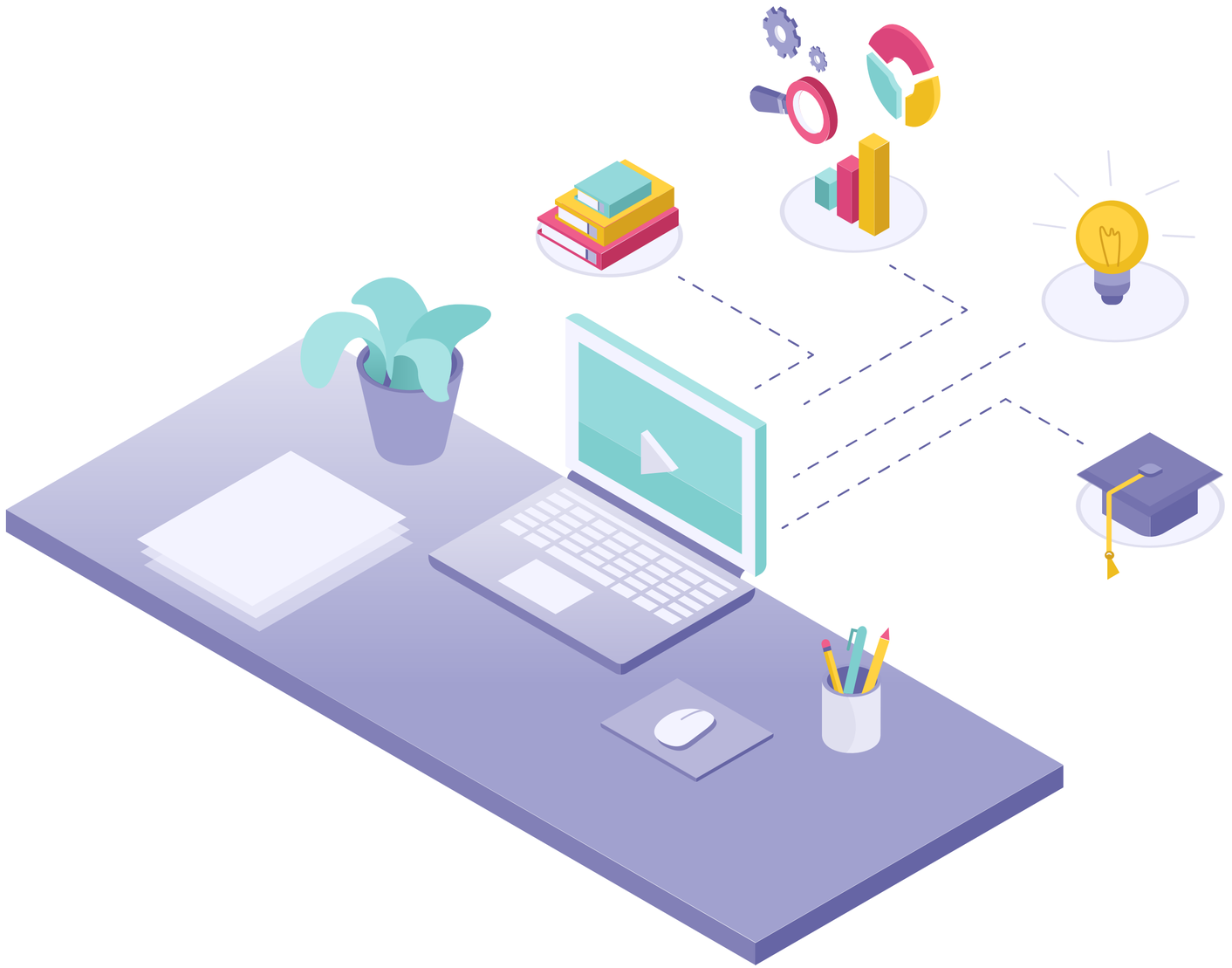
VEOLIA

A propos de Veolia Water

Veolia Eau France, spécialiste du traitement d'eau, offre à ses 8 millions de clients (B2B2C) une gamme complète de technologies et de services en conception-construction, exploitation, maintenance, modernisation et gestion des systèmes et des installations de traitement d'eau et d'assainissement.

Sur AWS, Veolia Eau France migre son application "Gestion Nouvelle", qui gère les relations avec ses 8 millions de clients, lui permettant de diviser par 10 ses coûts d'utilisation et d'ouvrir des possibilités d'innovation sur une plateforme auparavant figée.

L’infrastructure globale



L’infrastructure globale

Régions

Zones de disponibilité

Emplacement périphériques (Edge locations)

Zones locales

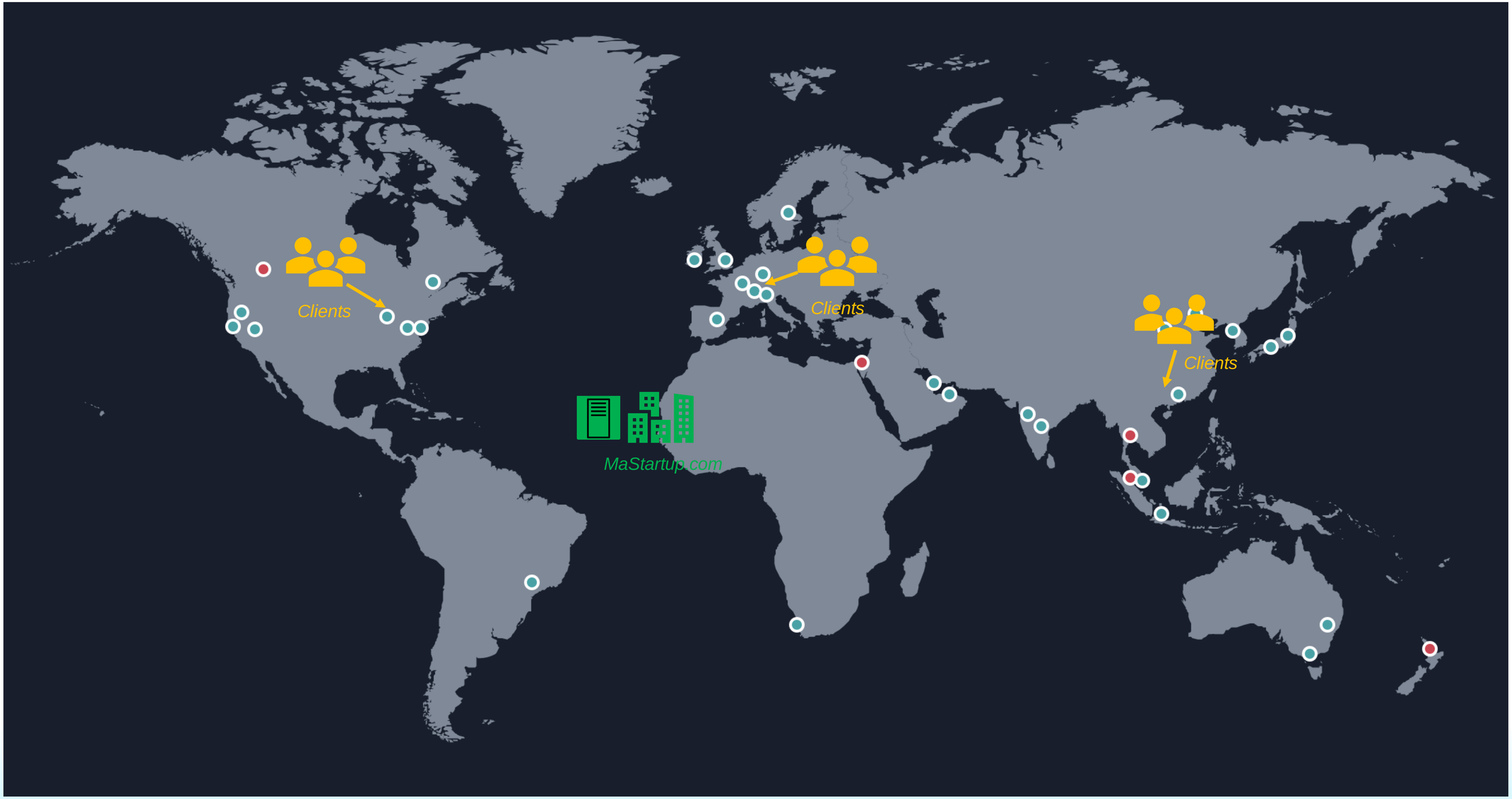
Les régions

33 régions

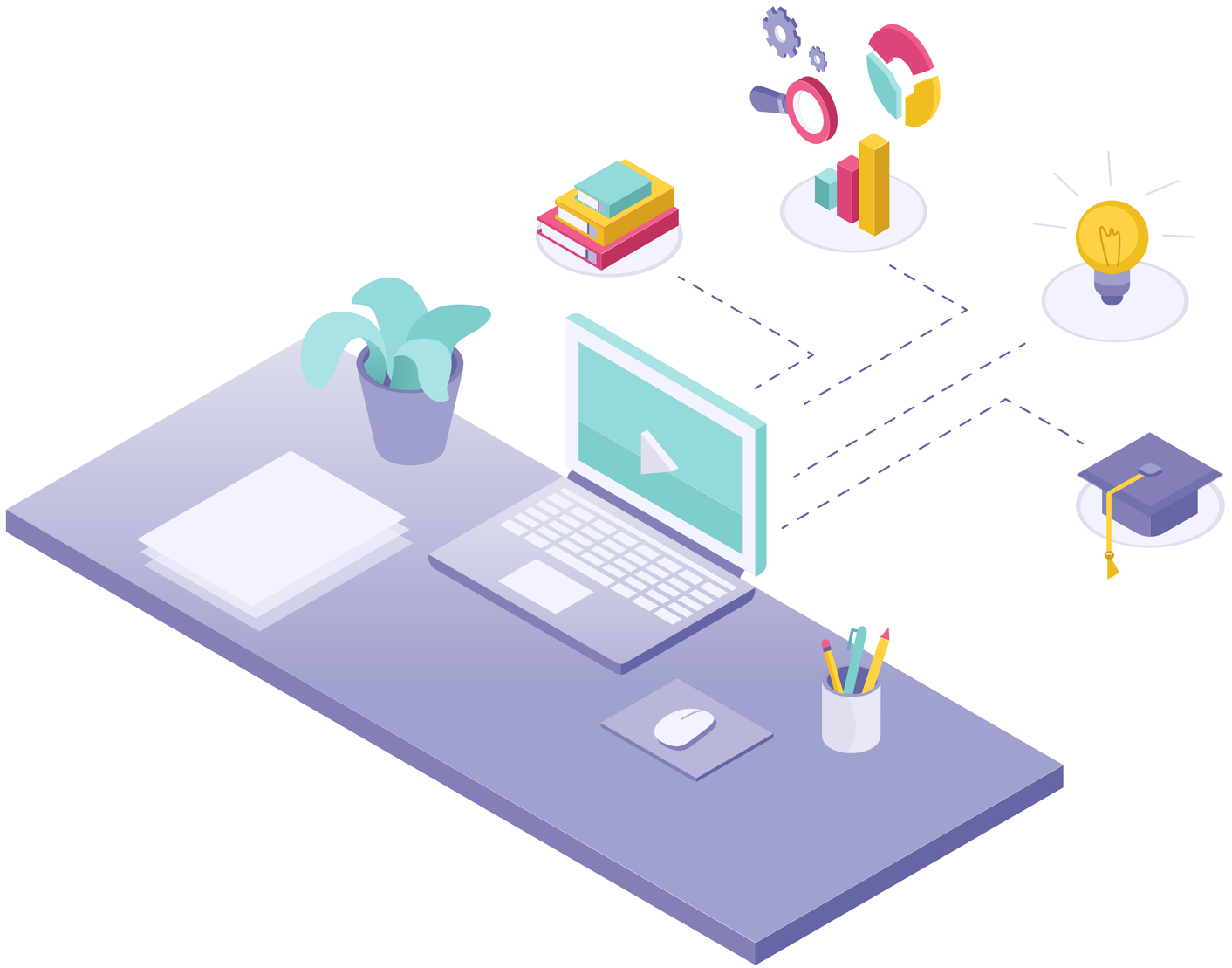
105 AZ



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


Clients
Clients
Clients
MaStartup.com

Anatomie d’une région



Anatomie d'une région



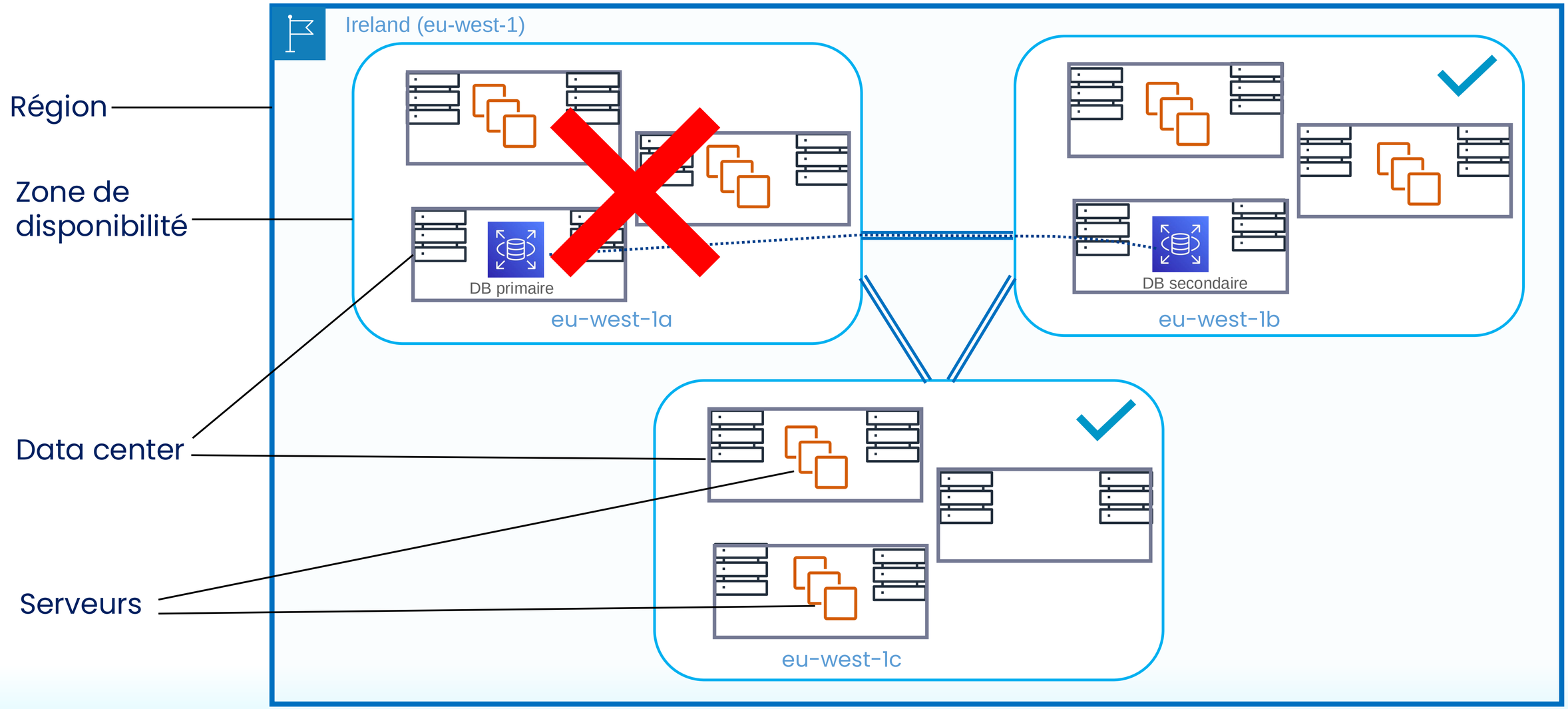
Une région contient plusieurs zones de disponibilités (AZ)

Une zone de disponibilité contient 1 ou plusieurs data centers

Un data center contient des centaines de milliers de serveurs

AWS ne dévoile pas la localisation de ses data centers

Anatomie d'une région



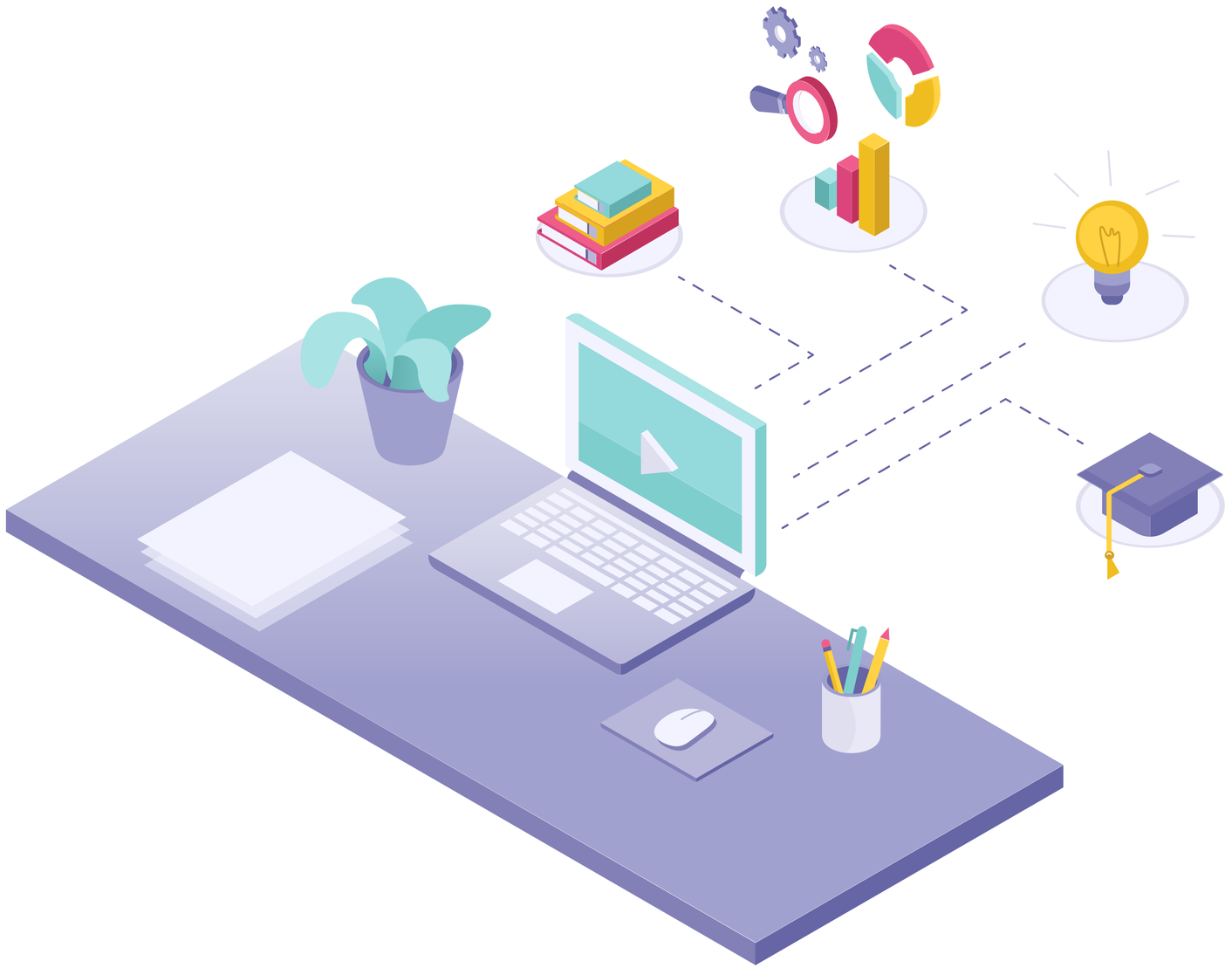
Anatomie d'une région

Une région AWS a un nom et un code

- Cape Town -> af-south-1
- Paris -> eu-west-3
- Irlande -> eu-west-1

Vous choisissez la région où vous hébergez vos données.

Choisir sa région



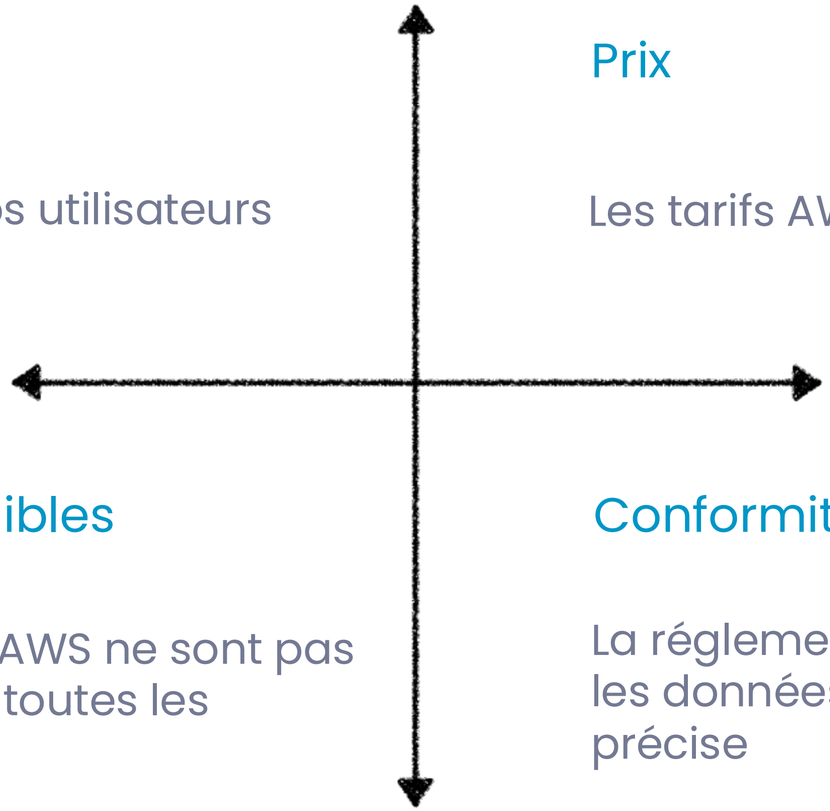
Choisir sa region : les critères

Latence

Proximité avec vos utilisateurs finaux

Prix

Les tarifs AWS varient d'une région à une autre



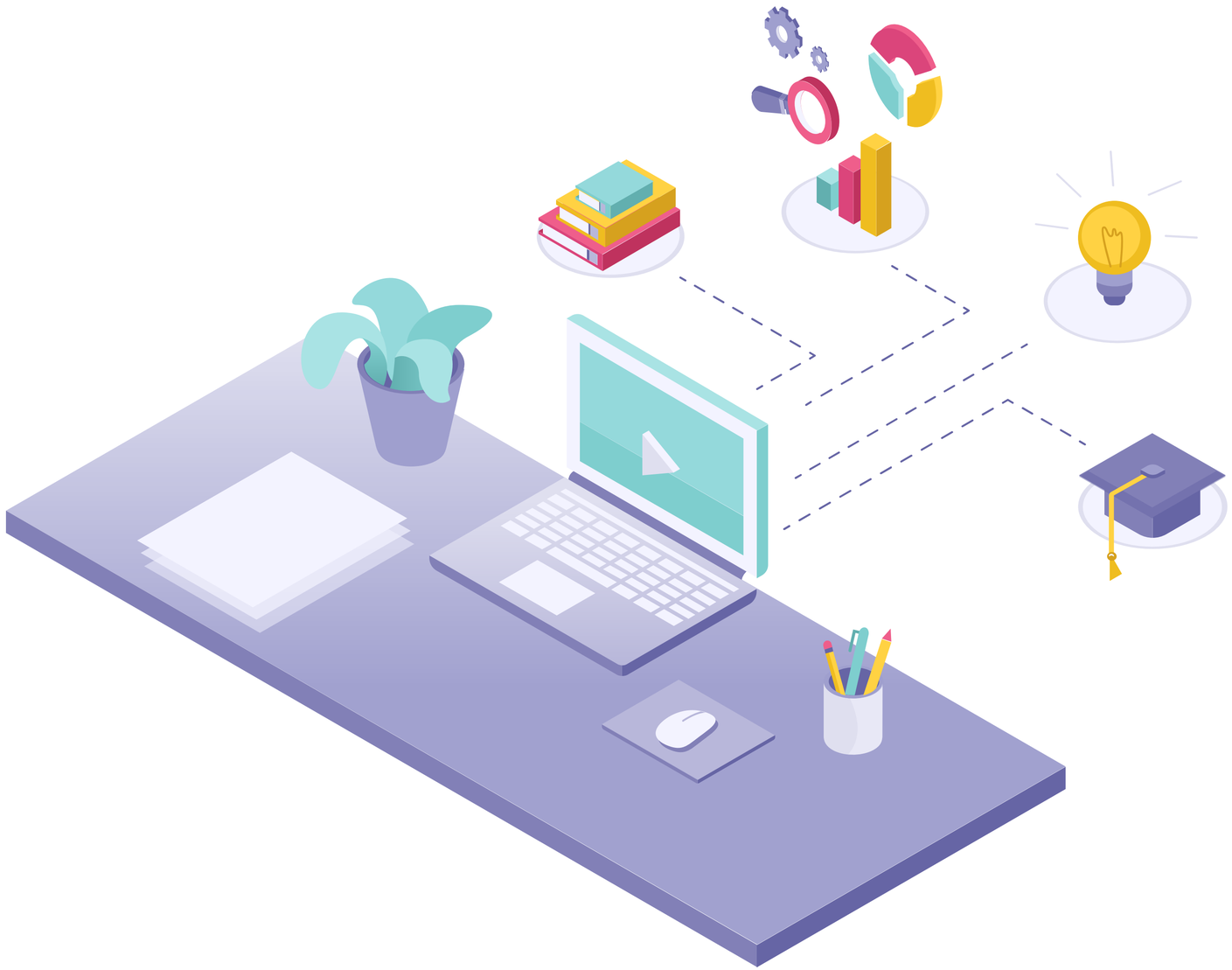
Services disponibles

Tous les services AWS ne sont pas disponibles dans toutes les régions

Conformité

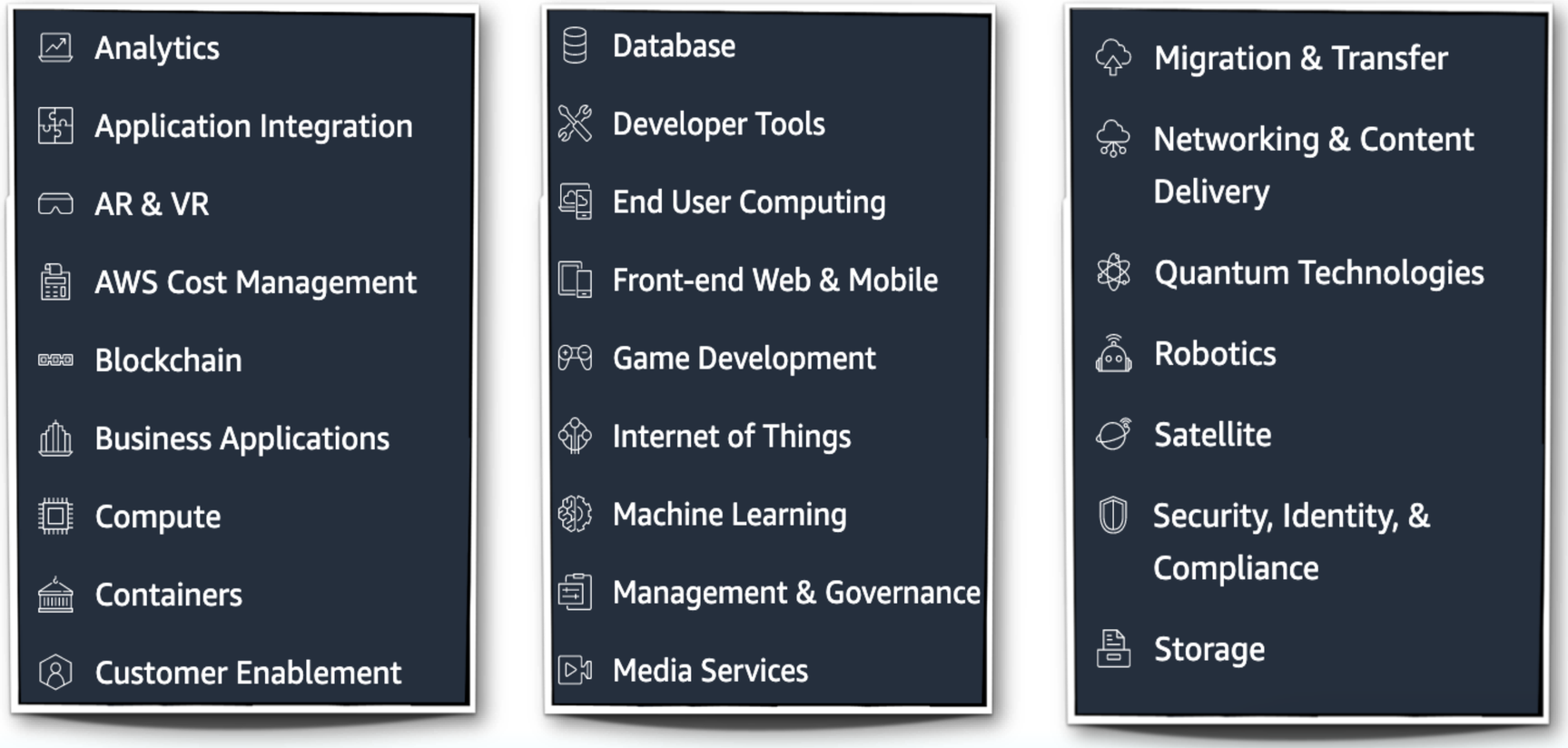
La réglementation vous oblige à localiser les données dans une zone géographique précise

Le catalogue de services



Le catalogue de services

AWS propose +200 services couvrant des dizaines de catégories



Le catalogue de services : exemples de services

Hébergement web


Amazon LightSail


AWS Elastic Beanstalk

Intelligence artificielle


Amazon Rekognition


Amazon SageMaker

Hébergement d'applications


Amazon EC2


EC2 Auto Scaling

Analyse de données


Amazon EMR


Amazon QuickSight

Stockage & Archivage


Amazon S3


AWS Backup

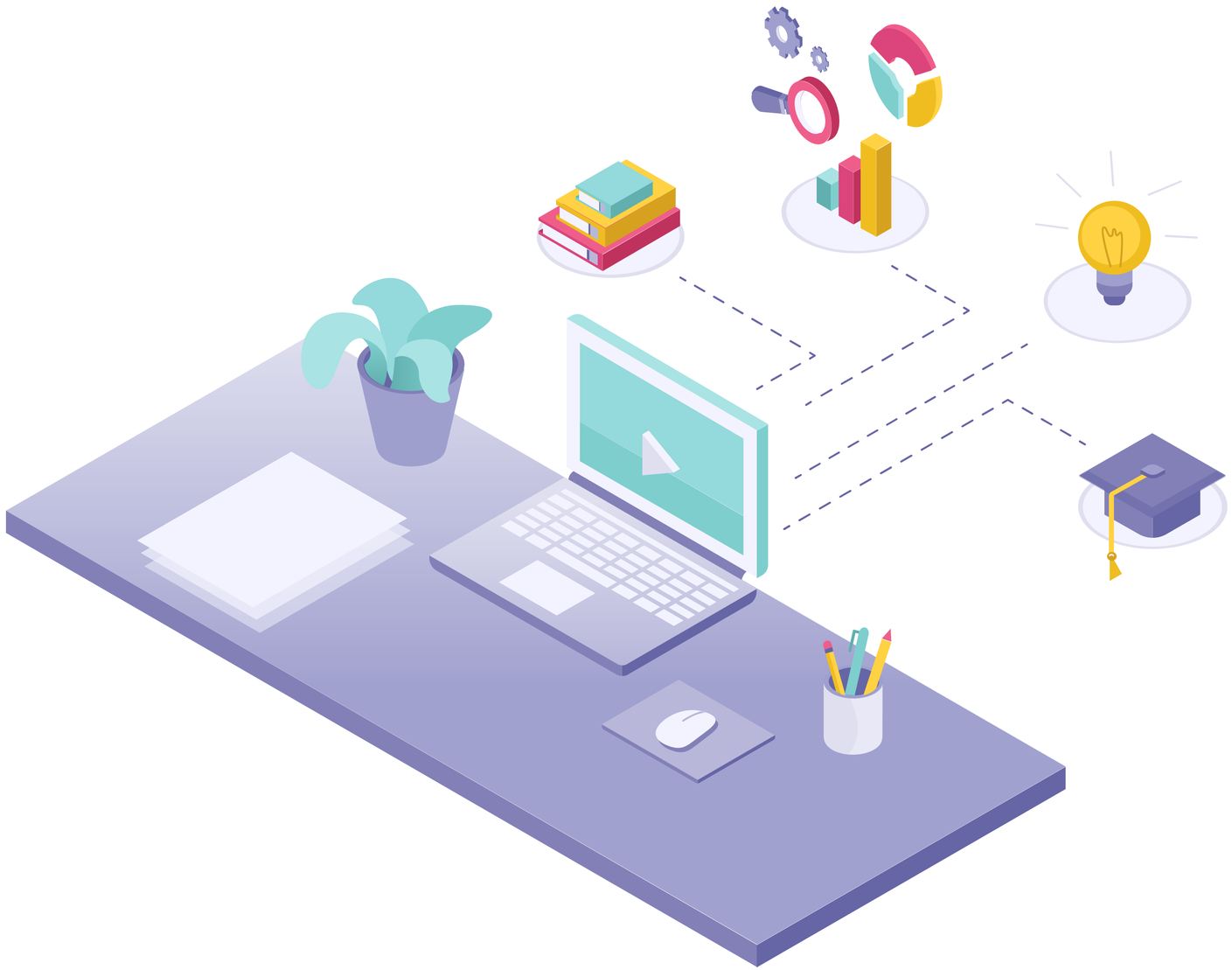
Diffusion de contenu


Amazon CloudFront

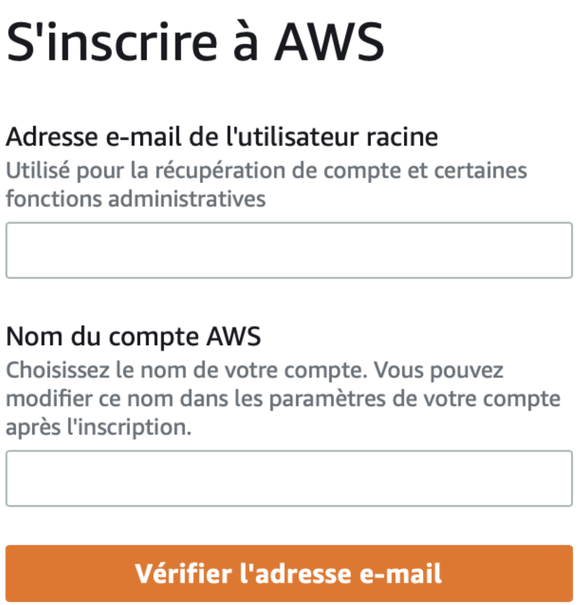


Amazon Route 53

Démarrer sur AWS



Créer son compte



Informations pour créer un compte AWS

- Une adresse e-mail (utilisateur racine)
- Une carte bancaire
- Un numéro de téléphone

Accéder aux services AWS



AWS Management console

Interface web simple

AWS CLI

ligne de commande

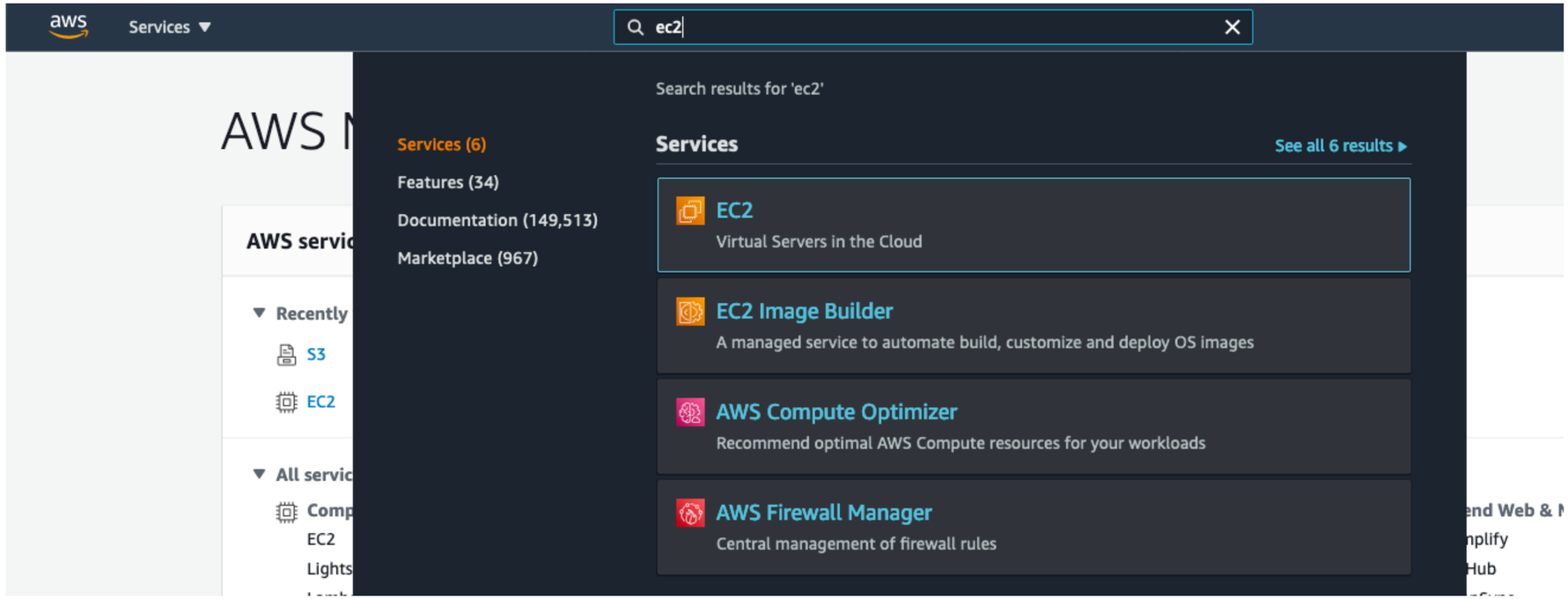
AWS SDK

Kit de développement logiciel

AWS Management console

Interface Web simple (chrome, firefox, safari…)

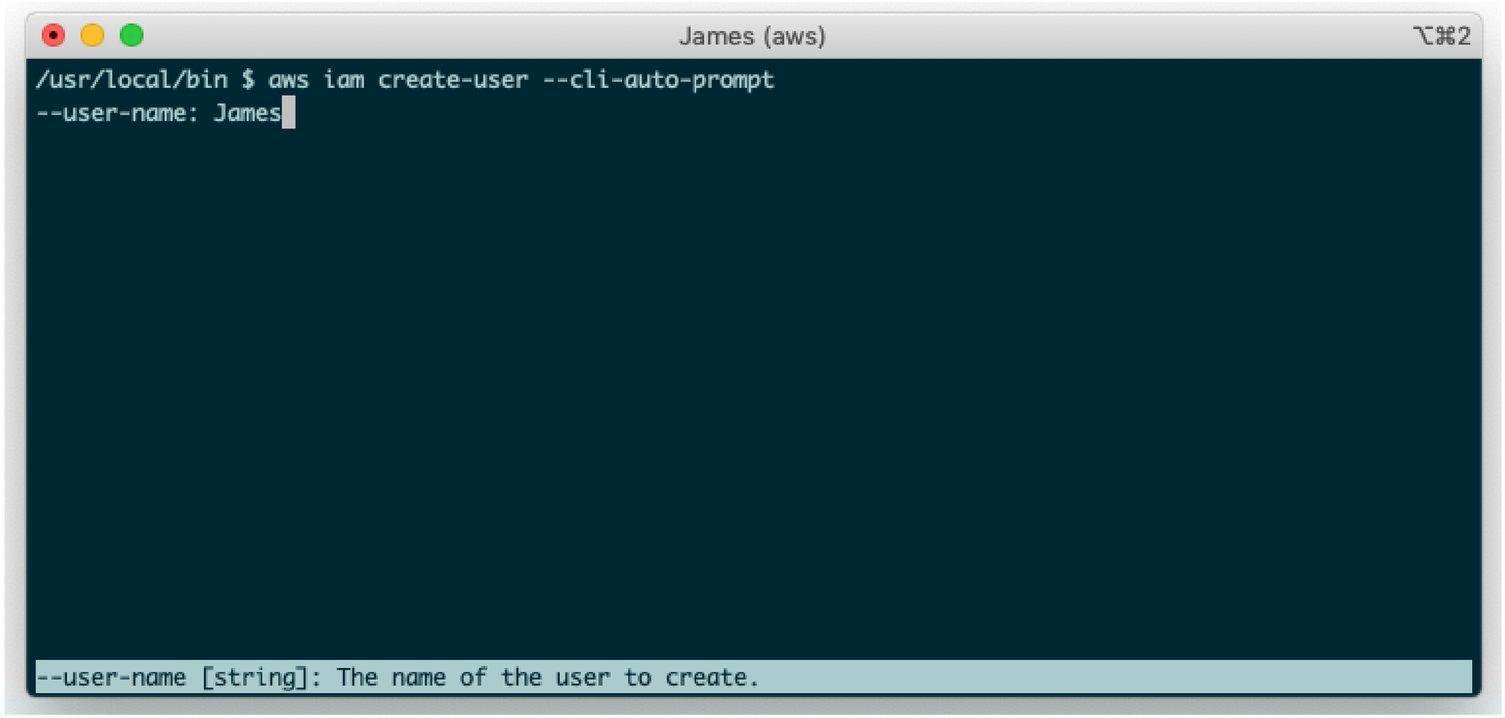
Idéal pour débuter avec AWS



AWS CLI

Outil de ligne de commande (Windows, MacOs, Linux)

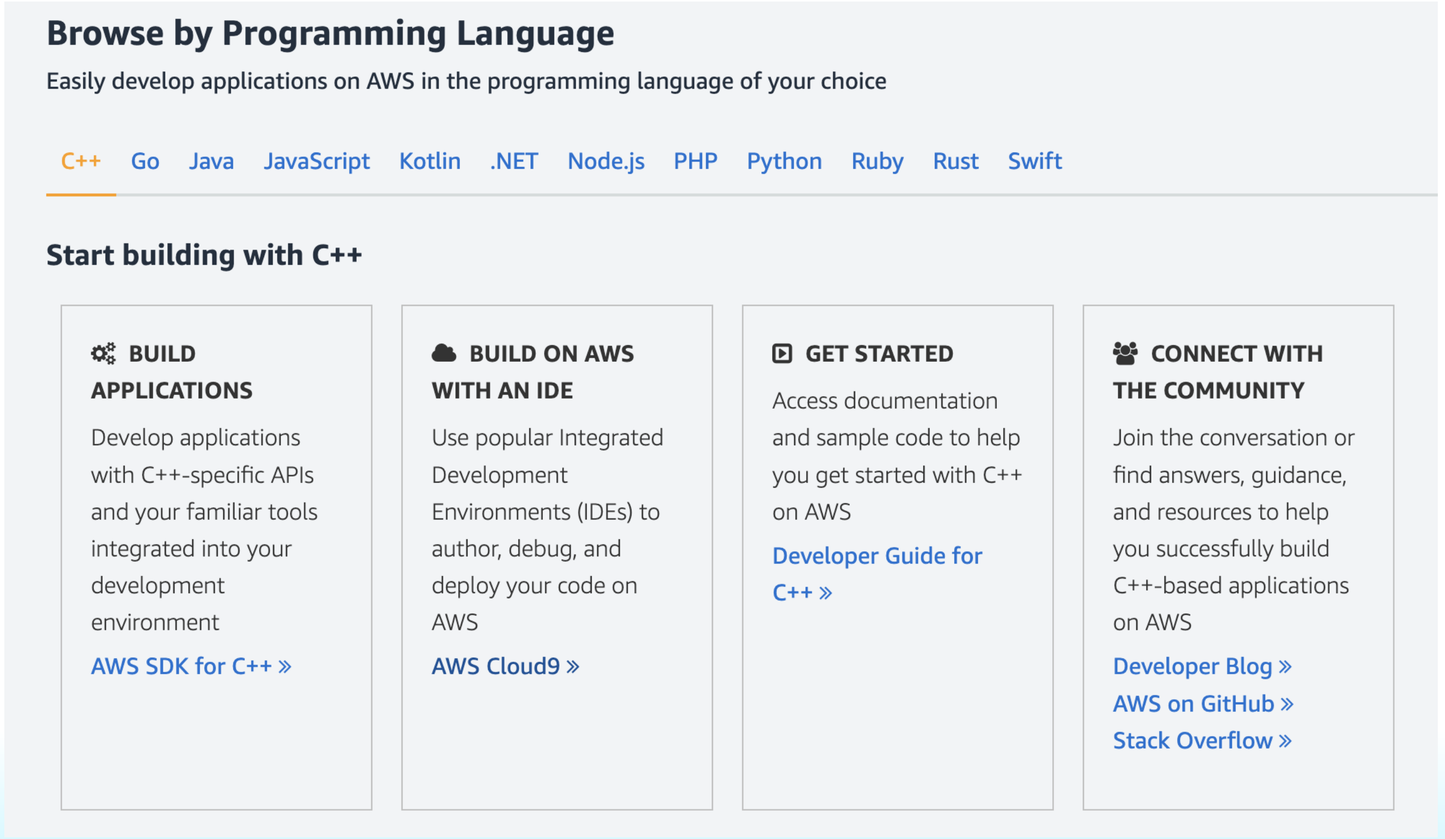
Idéal pour l'automatisation avec des scripts



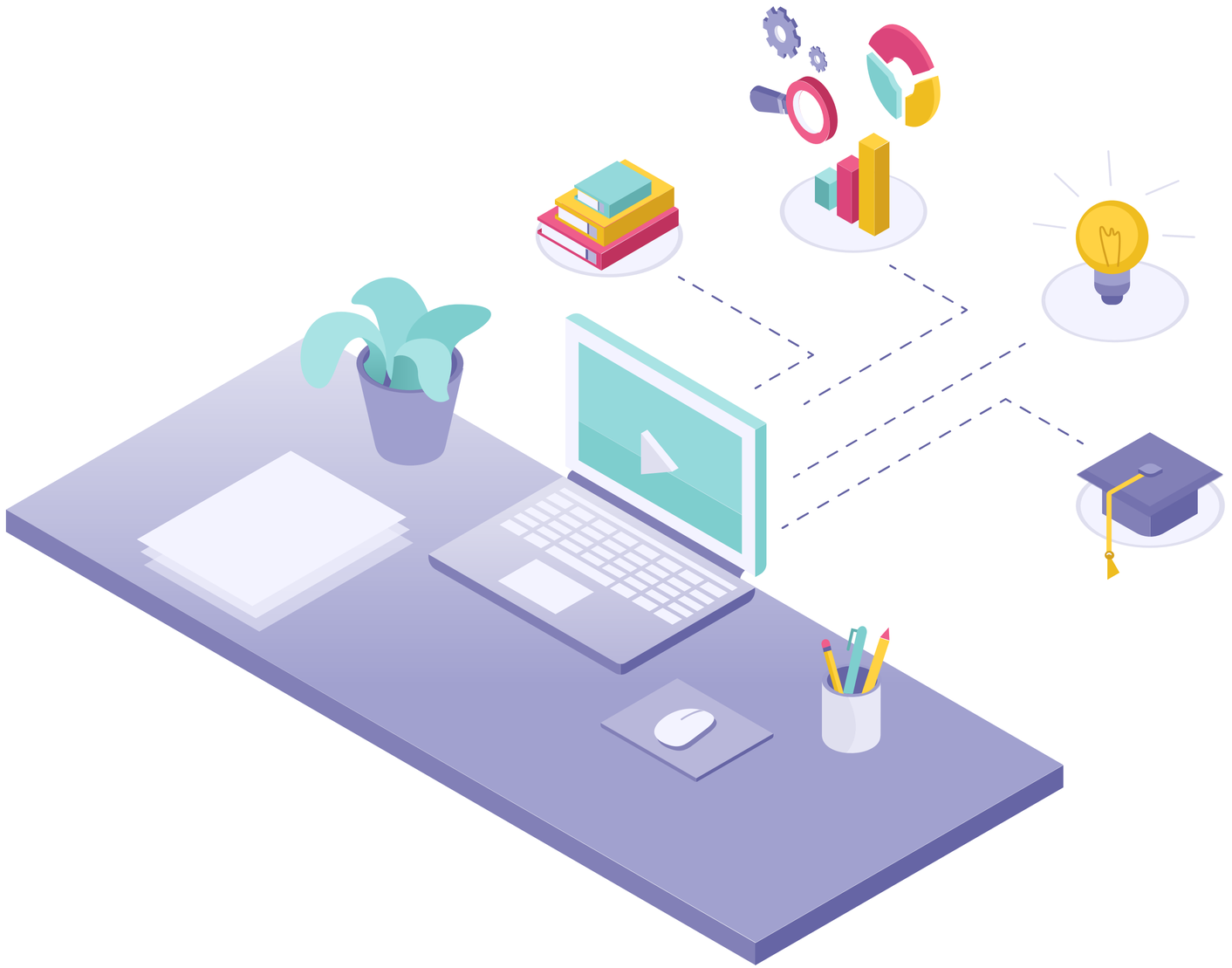
AWS SDK

Permet de développer des applications qui utilisent AWS

Supporte plusieurs langages de programmation: C++, Java, .Net, Python ...



AWS Free Tiers



AWS Free Tiers (Offre gratuite d'AWS)



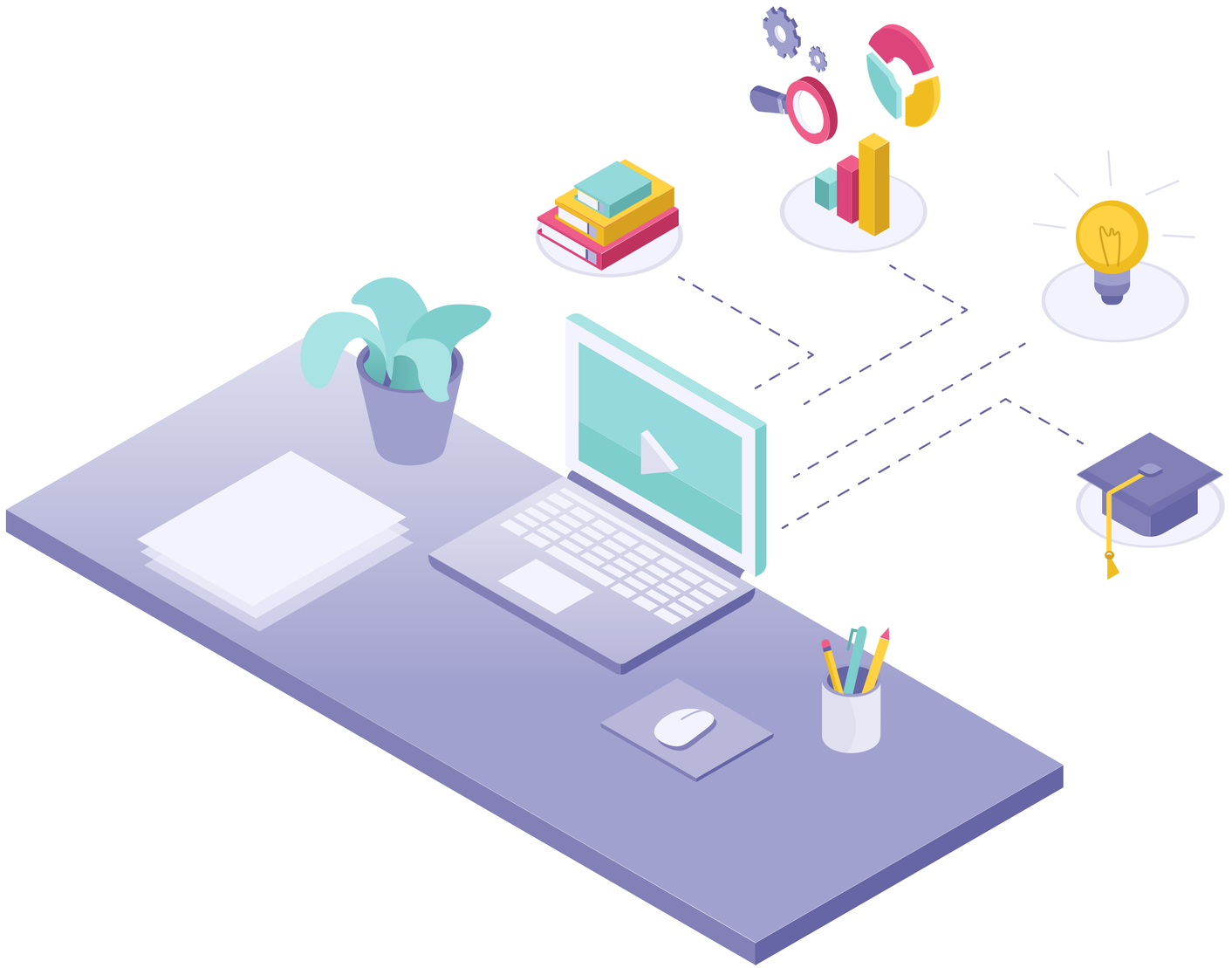
Permet d'essayer gratuitement les services AWS

3 types d'offres

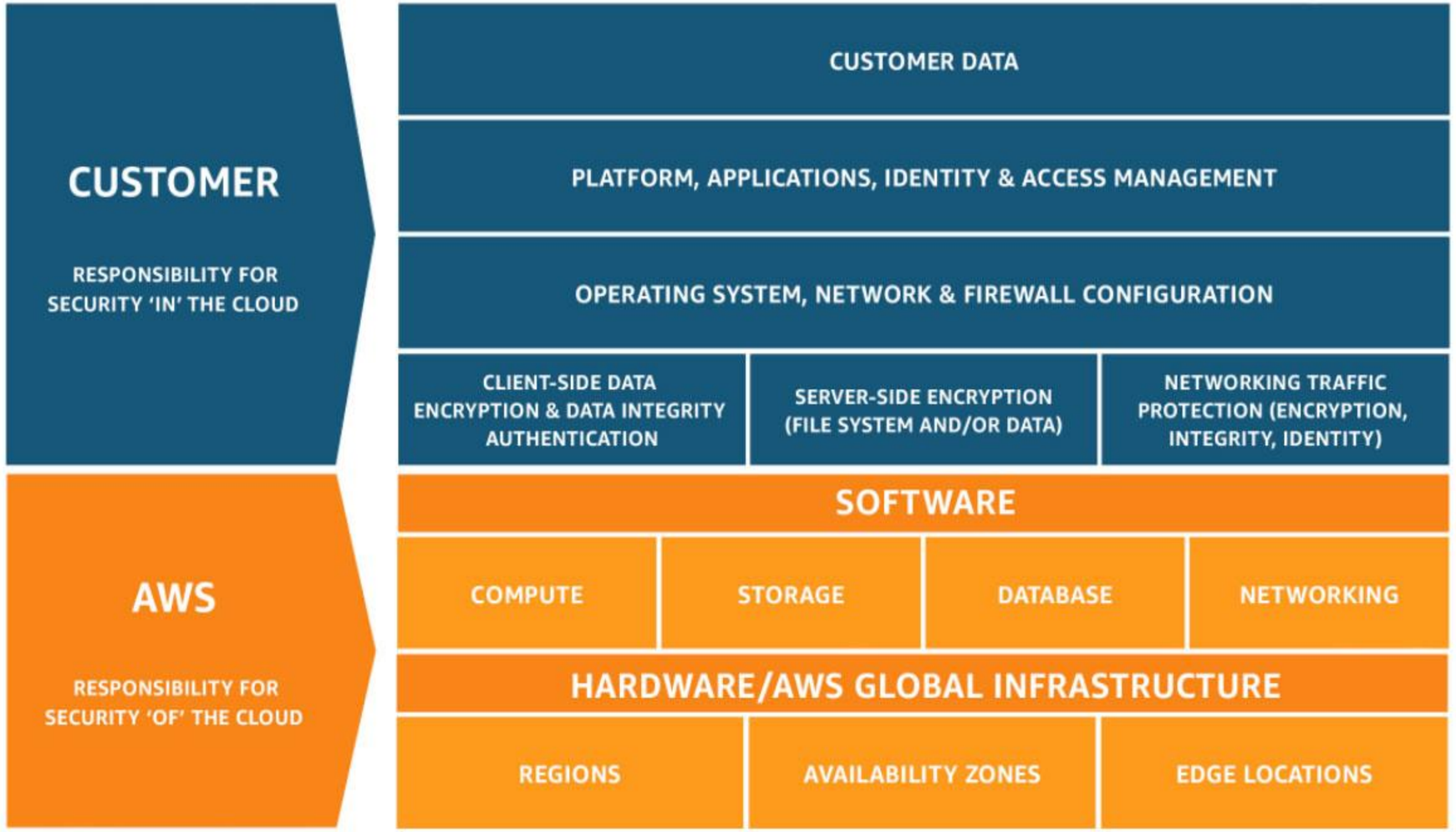
12 mois gratuits	Essais Gratuits	Toujours gratuit
Amazon EC2 750 heures	Sagemaker -> 2 mois	Amazon DynamoDB -> 25 Go
Amazon S3 5 GB	Redshift -> 2 mois	AWS Lambda -> 1 million requêtes
Amazon RDS 750 heures	Amazon Lightsail -> 750 heures	Amazon SNS –> 1 million publications
….	…	…

https://aws.amazon.com/fr/free

Responsabilité du client



Modèle de responsabilité partagée





EC2



RDS

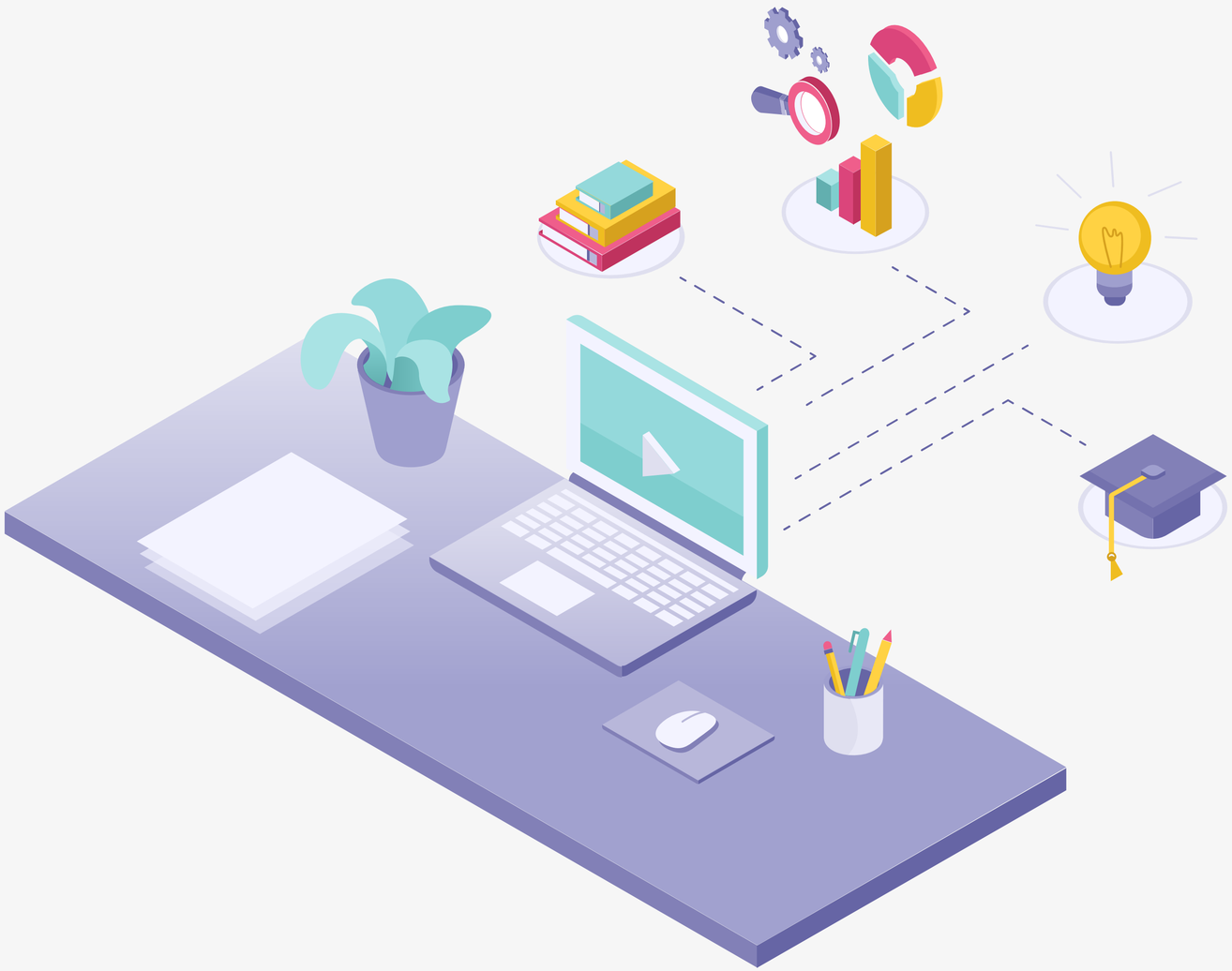


AWS Acceptable Use Policy

Politique d'AWS en matière d'utilisation acceptable

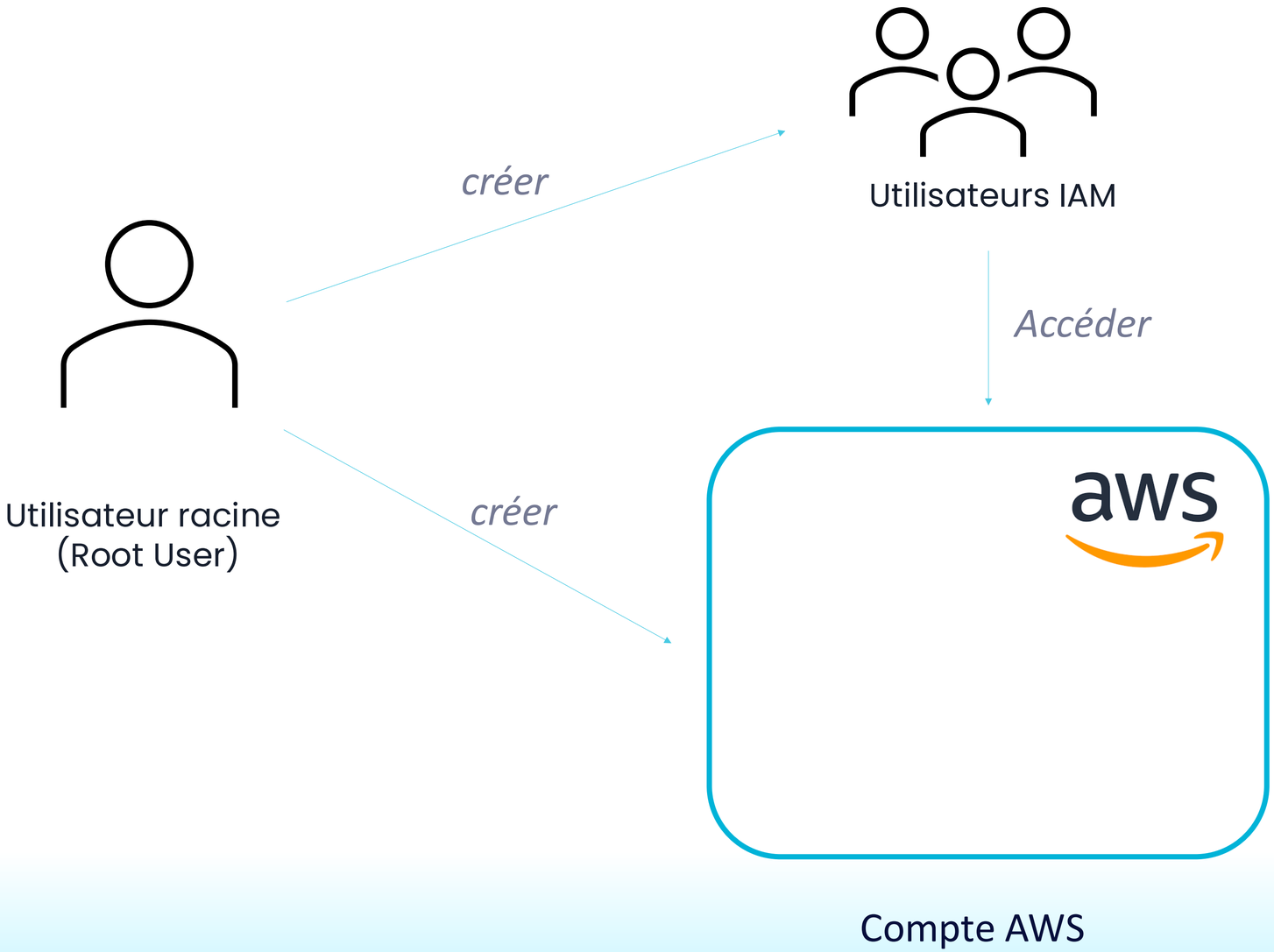
Il vous est interdit d'utiliser les Services ou le Site AWS, d'en faciliter l'usage ou de permettre à des tiers de les utiliser :

- à des fins illégales ou frauduleuses ;
- à des fins de violation des droits d'autrui ;
- à des fins de menace, d'incitation, de promotion ou d'encouragement actif en lien avec la violence, le terrorisme ou d'autres actes répréhensibles ;
- pour poster un contenu ou une activité quelconque faisant l'apologie de l'exploitation ou de la maltraitance sexuelle des enfants ;
- pour porter atteinte à la sécurité, l'intégrité ou la disponibilité d'un utilisateur, d'un réseau, d'un système informatique ou de communication, d'une application logicielle ou d'un périphérique réseau ou informatique ;
- à des fins de diffusion, publication ou envoi en masse de courriels non sollicités ou autres messages, promotions, publicités ou sollicitations (ce que l'on nomme « spam »), ou pour en faciliter l'envoi.

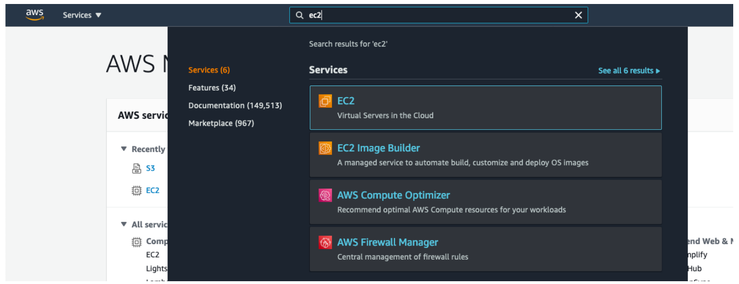


FIN DU MODULE

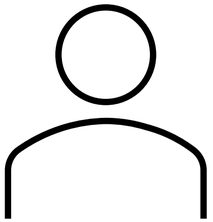
Lab : créer 1er utilisateur IAM



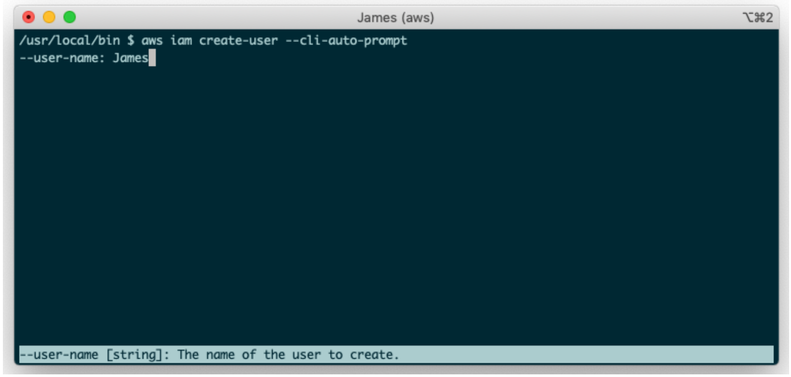
Lab : AWS CLI



AWS Console



Admin
(Utilisateur IAM)



AWS CLI

Accéder

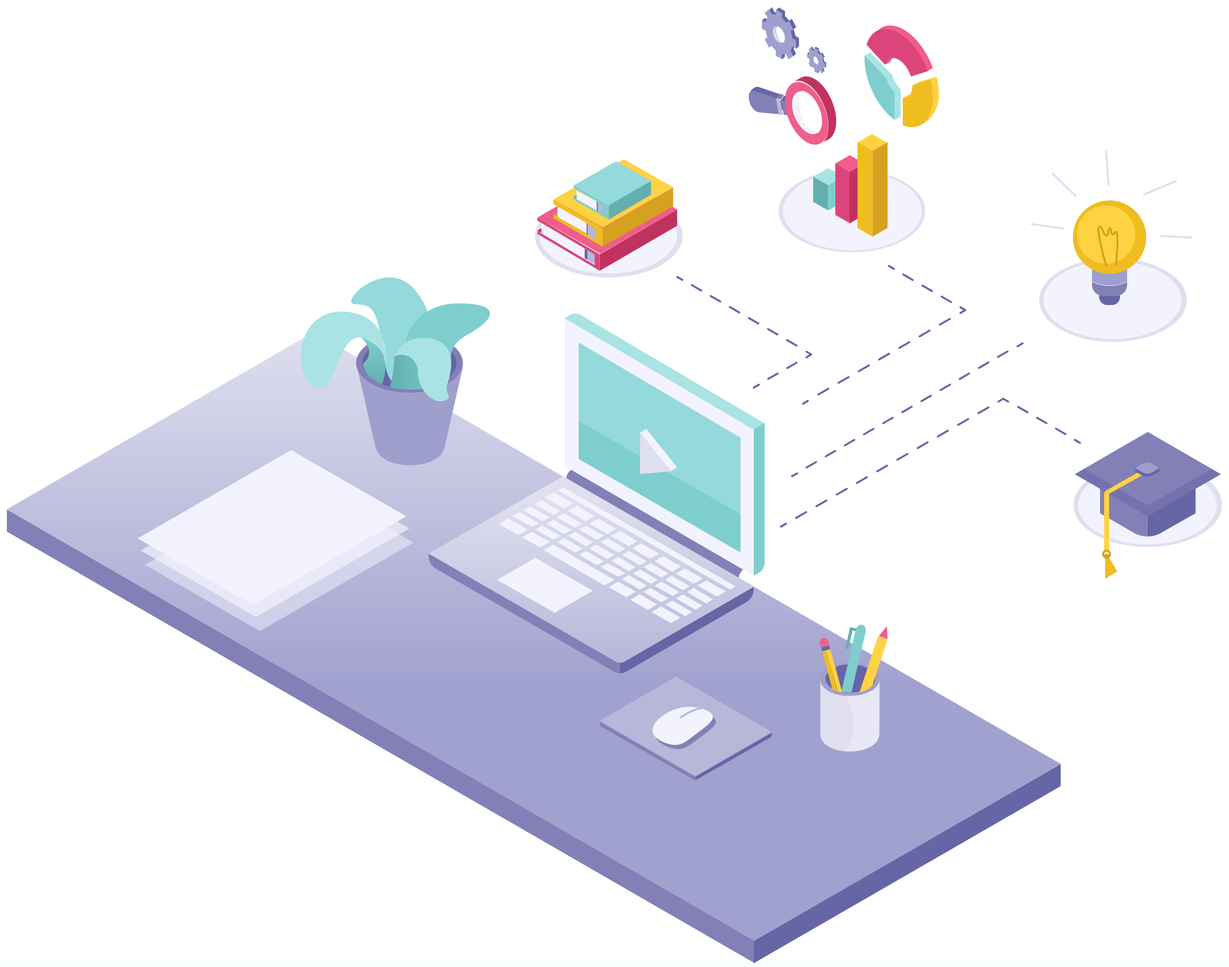


Compte AWS

1. Créer un utilisateur IAM Admin
2. Télécharger et installer AWS CLI
3. Configurer l'authentification (Access Key Id / Secret Access Key)
4. Utiliser le service Amazon S3. *Par exp: « aws s3 ls » pour lister les buckets*

Module 3 : Amazon EC2

Calcul pour n'importe quelle charge de travail : instances, conteneurs et serverless



LeCloudFacile.com

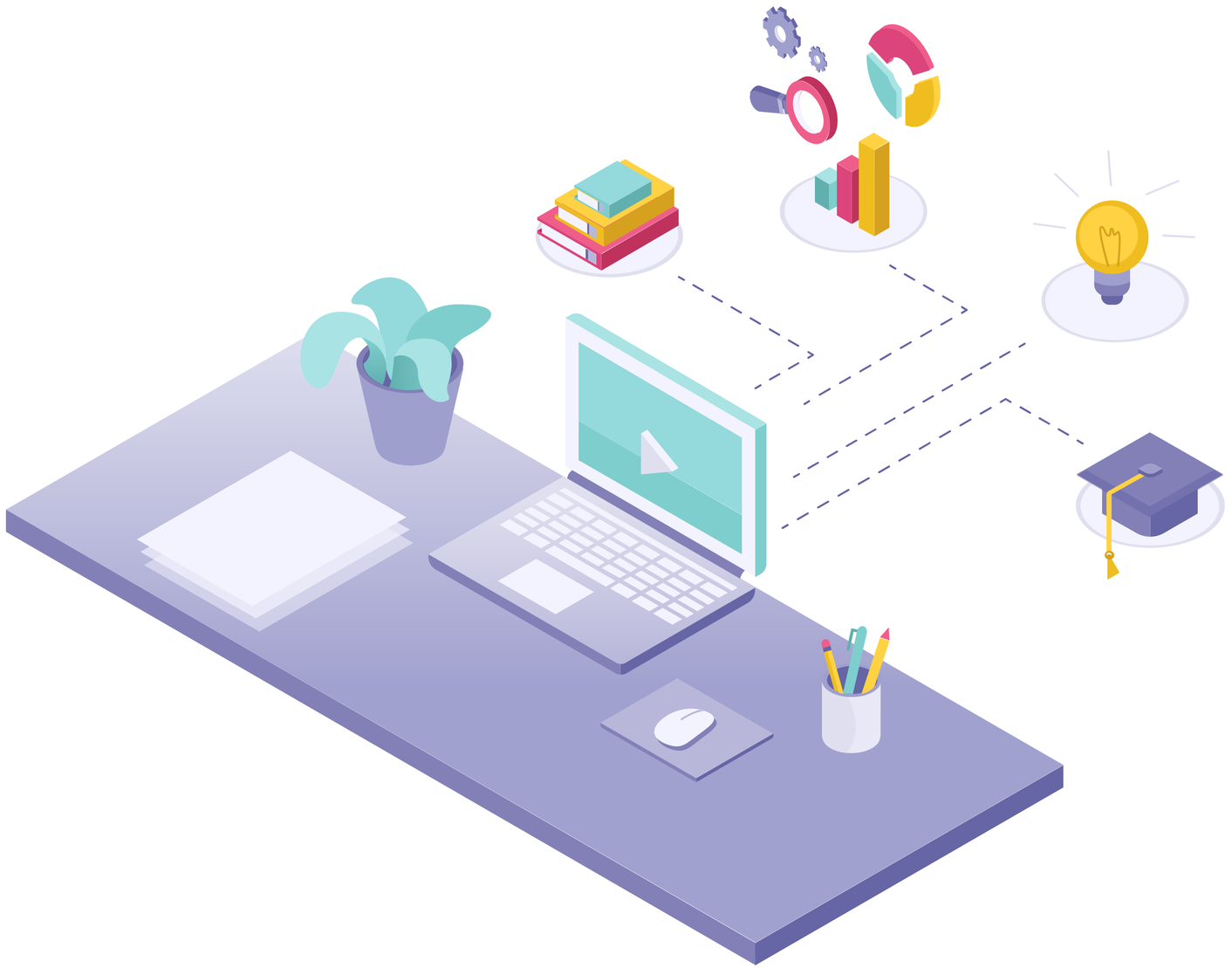
Comment utiliser les serveurs de calcul sur AWS ?

Quelle sont les options de configuration des serveurs ?

Quels sont les avantages à utiliser des serveurs dans le Cloud ?



Amazon Elastic Compute Cloud (EC2)



Amazon EC2



Fournit des serveurs de calcul appelés « **Instances** »

Systèmes d’exploitation : **Linux**, **Windows** ou **MacOS**

Processeurs : **Intel**, **AMD** ou **Graviton** (Arm)

Facturation à la **seconde ou à l’heure** par défaut

Offre gratuite : 750 heures par mois pour les nouveaux clients

Comment ça marche



Cas d'usage



Hébergement de **sites web**

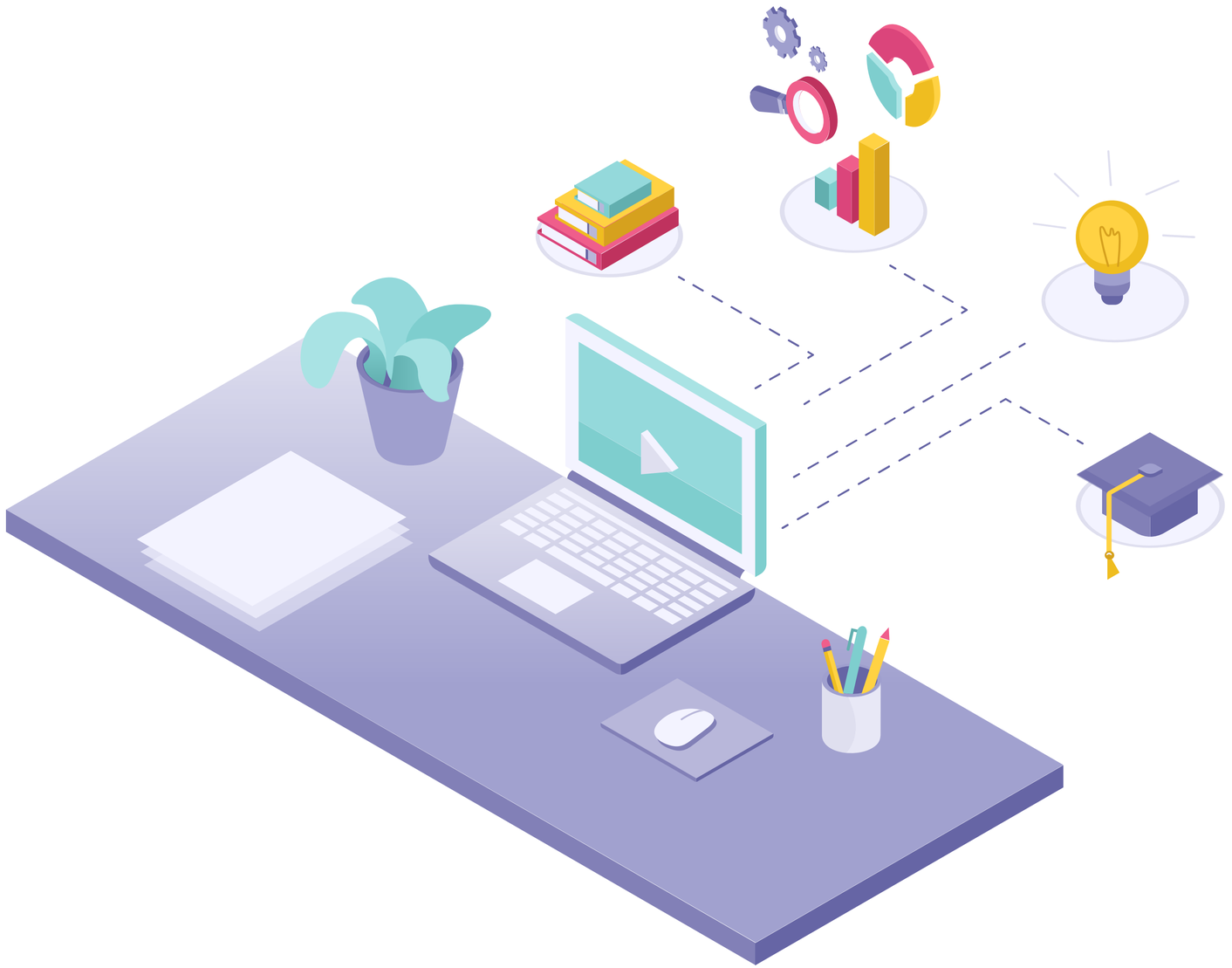
Hébergement d'**applications** : CRM, ERP, Bases de données

Environnements de **développements**

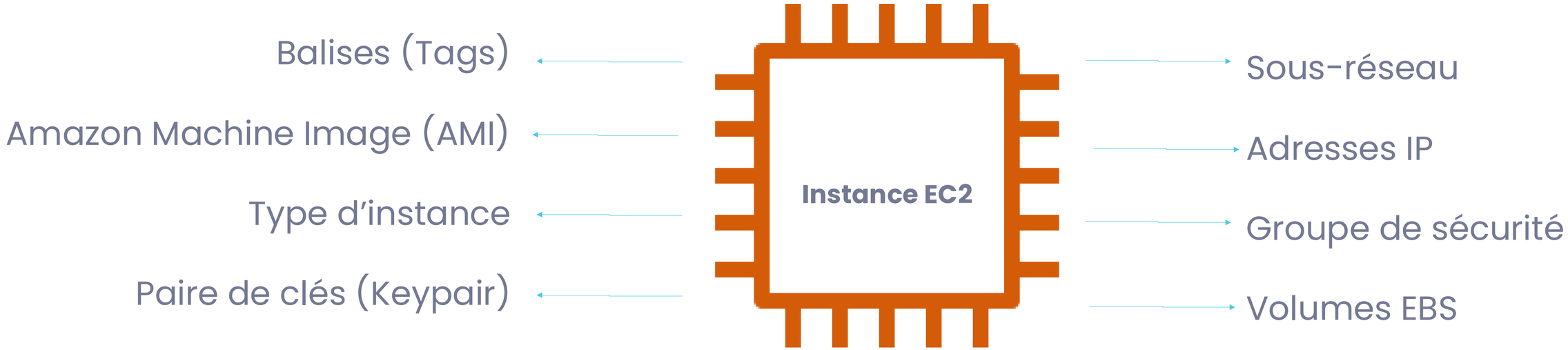
Environnements de **productions**

Stockage et traitements de **données**

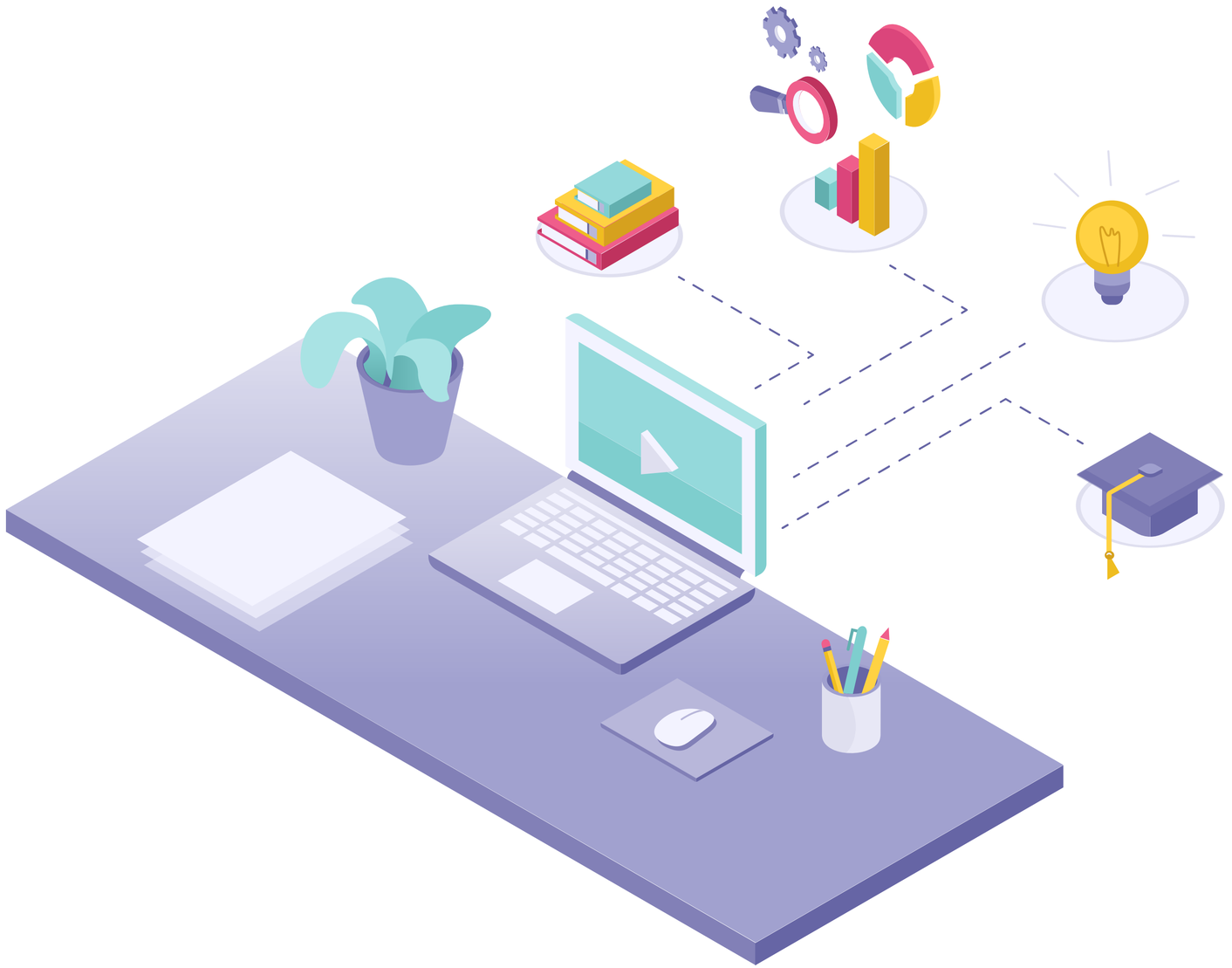
Caractéristiques d’une instance EC2



Les caractéristiques d'une instance EC2



Tags

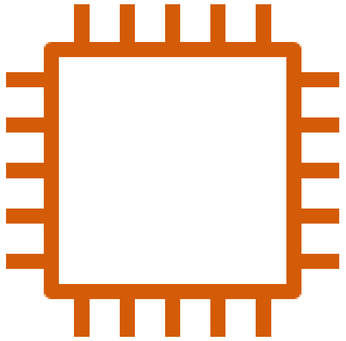


Balises (Tags)

Ce sont des métadonnées

Permettent de classer et d'identifier vos instances EC2

Paire clé/valeur. Exp : « *Nom = Serveur Web* »



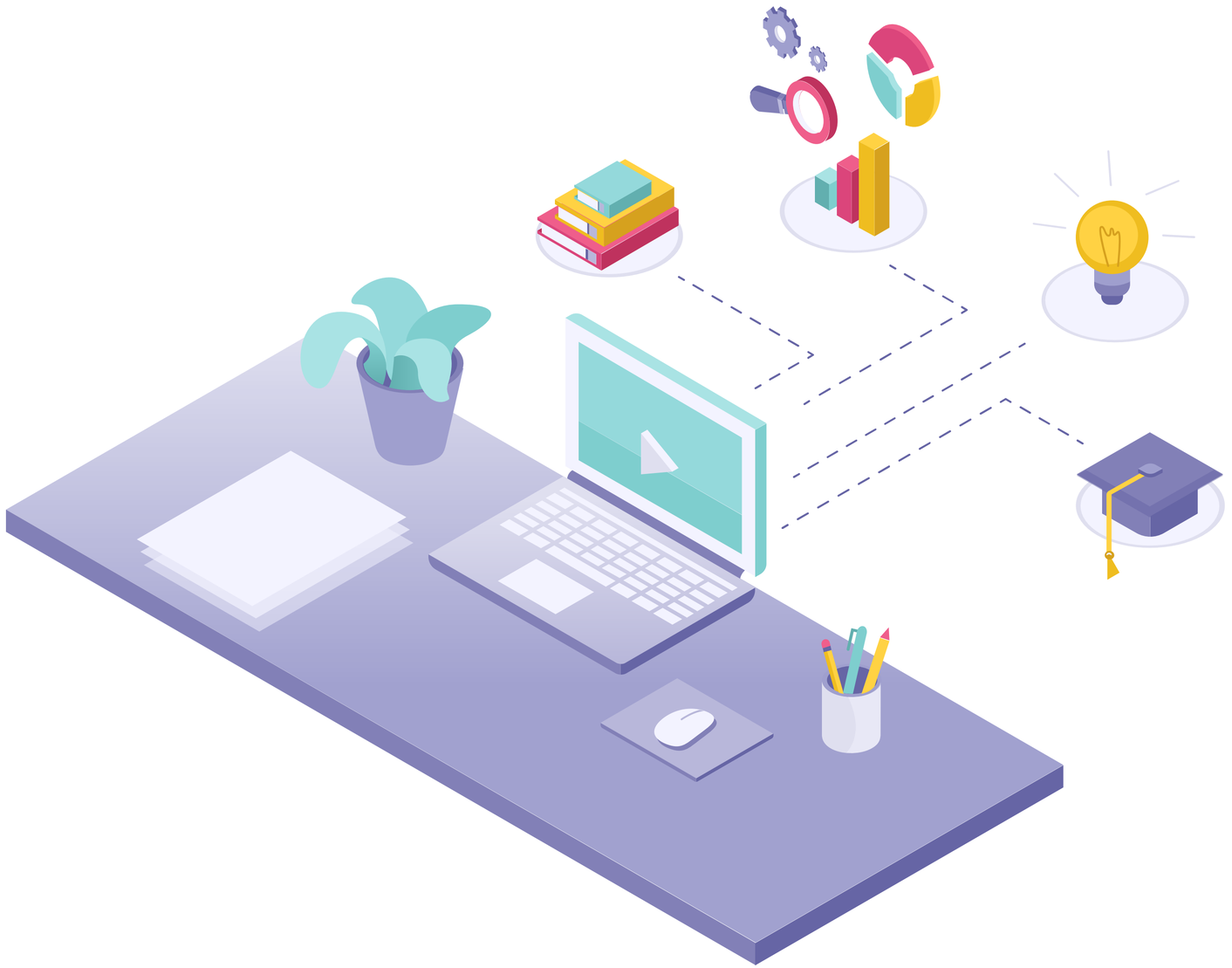
Instance EC2

Nom = MySQL_DB

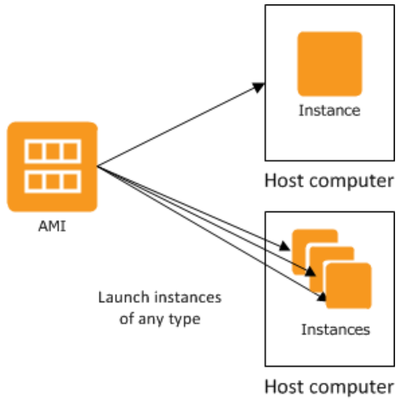
Departement = Marketing

Env = Dev

Amazon Machine Image (AMI)



Amazon Machine Image (AMI)



Template à partir duquel est lancé une instance EC2

Contient le système d'exploitation et des données

Fournis par AWS, par la communauté ou vendus sur la Marketplace

AWS (éditeurs de logiciels)

Quelques caractéristiques d'une AMI



AMI

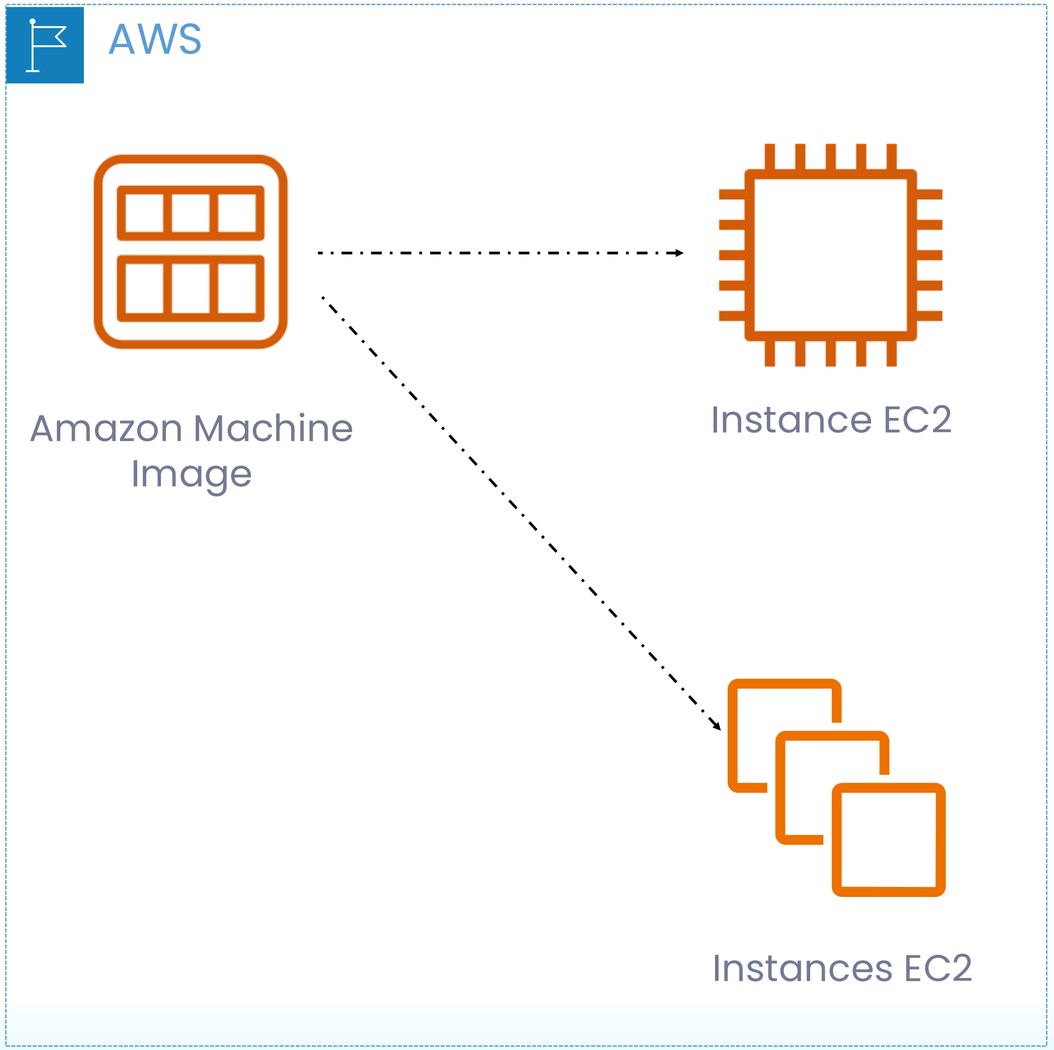
- Région
- Système d'exploitation (Windows, Linux, Ubuntu, Redhat,...)
- Architecture (32 bits ou 64 bits)
- Privée ou Publique

Amazon Machine Image (AMI)

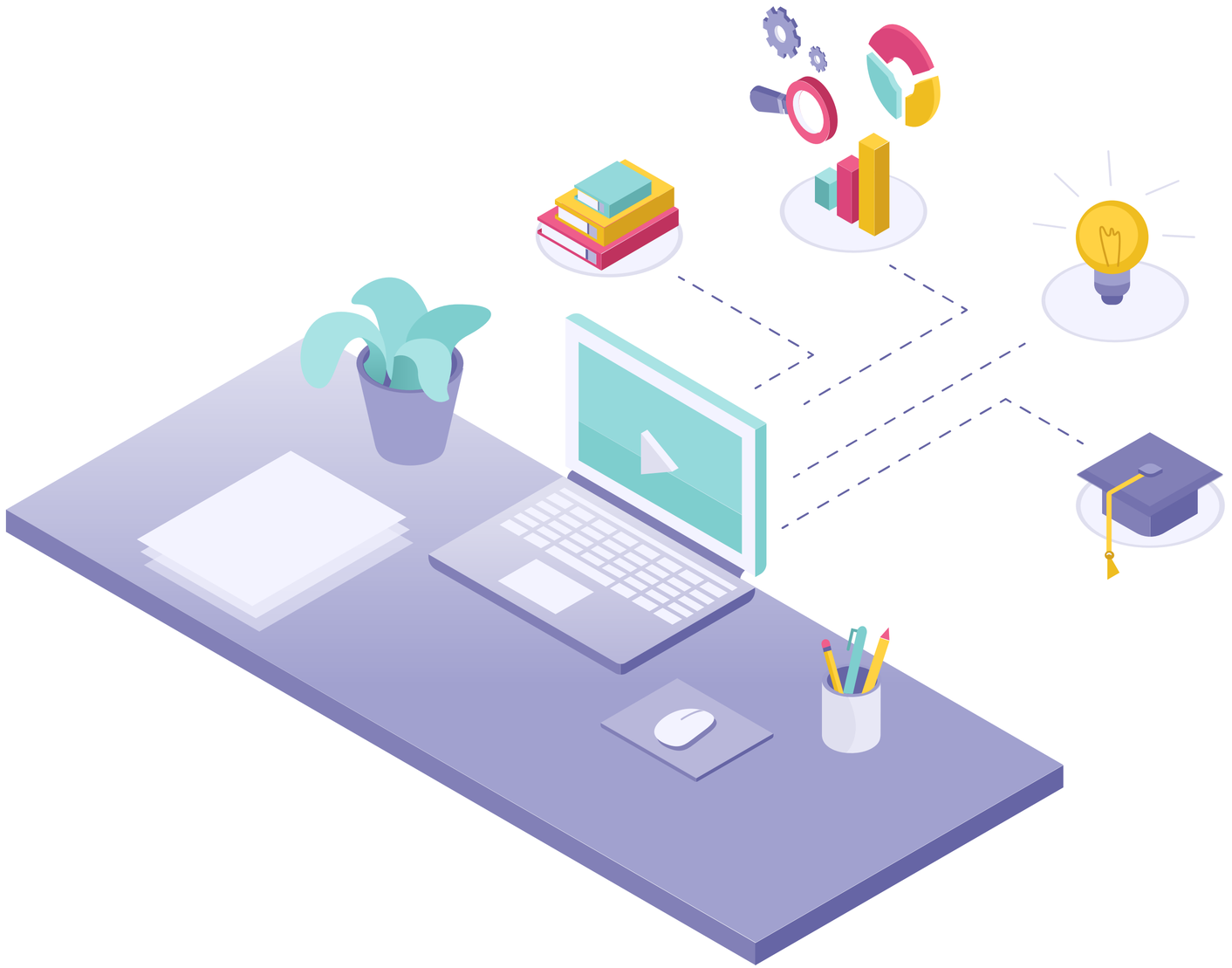
On peut lancer plusieurs instances EC2 à partir de la même AMI

➔ Les instances EC2 seront identiques

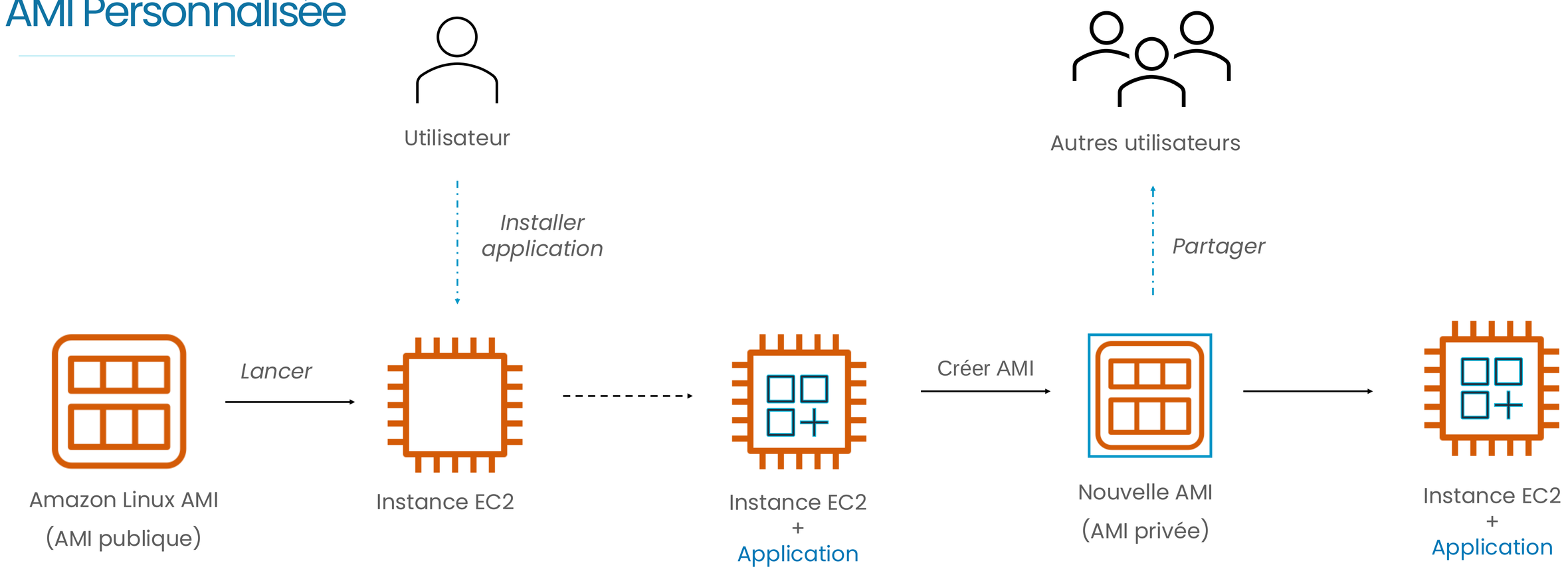
➔ Les instances EC2 seront indépendantes les unes des autres



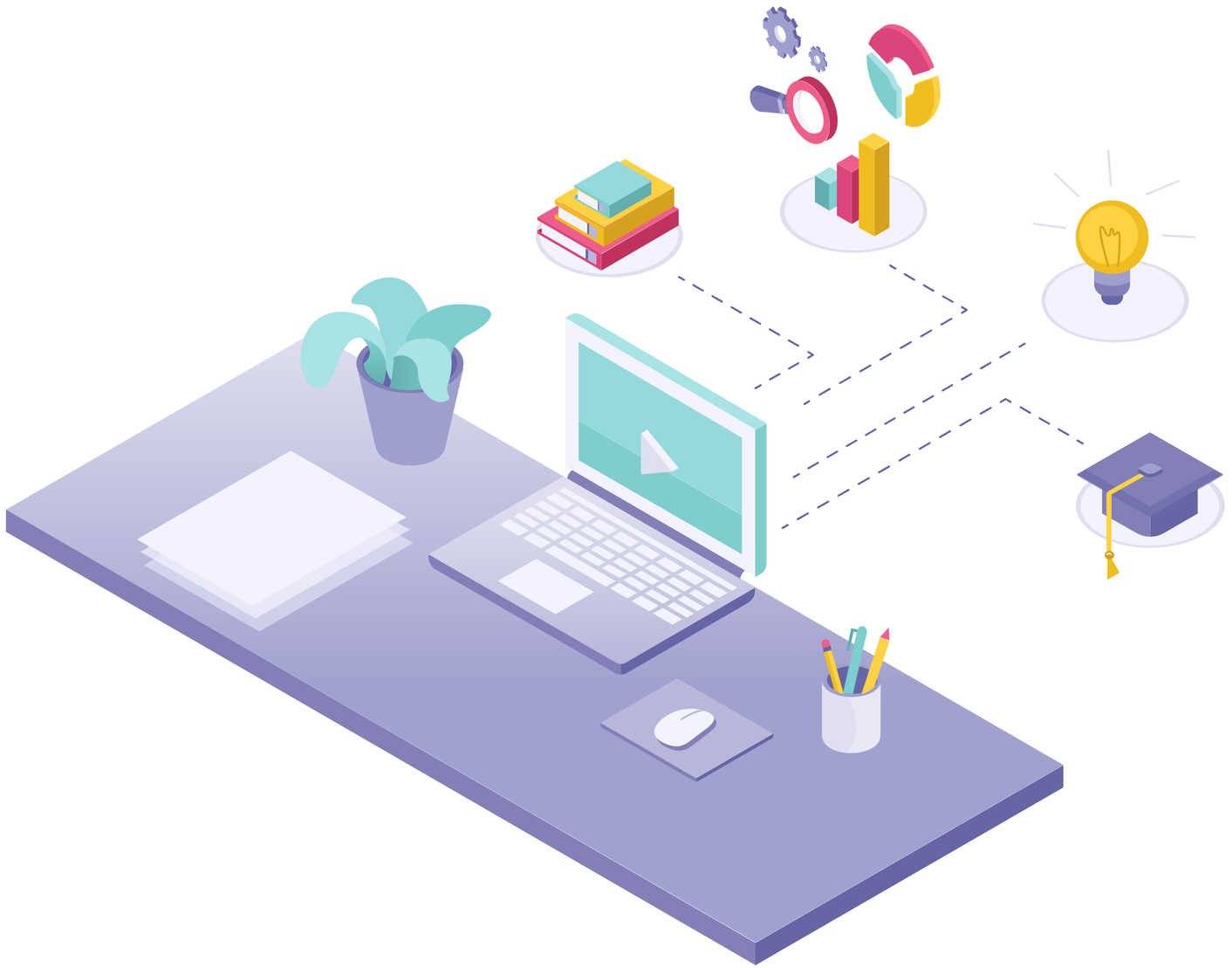
AMI Personnalisée



AMI Personnalisée



Types d’instances



Types d’instances



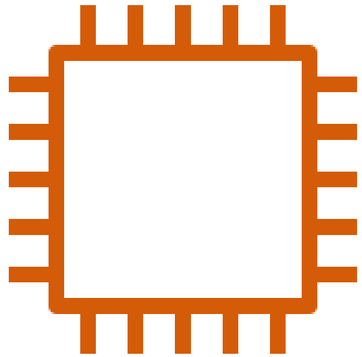
Définit les caractéristiques de l’instance EC2: capacité CPU, taille mémoire, performance réseau, type de stockage…

Choix au lancement de l’instance EC2

Il existe **+500** types d’instances

Choix **selon les exigences de votre application**

Nomenclature Types d'instances 1/2



t2.micro

- 1 vCPU
- 1 Gio mémoire
- Processeur Intel Xeon

Prix : $0.0116 / heure (Paris)

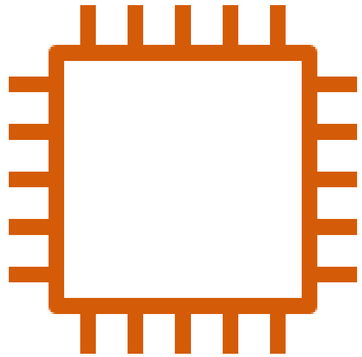
Eligible au AWS Free Tiers

Famille d'instance

Génération

Taille

Nomenclature Types d'instances 2/2



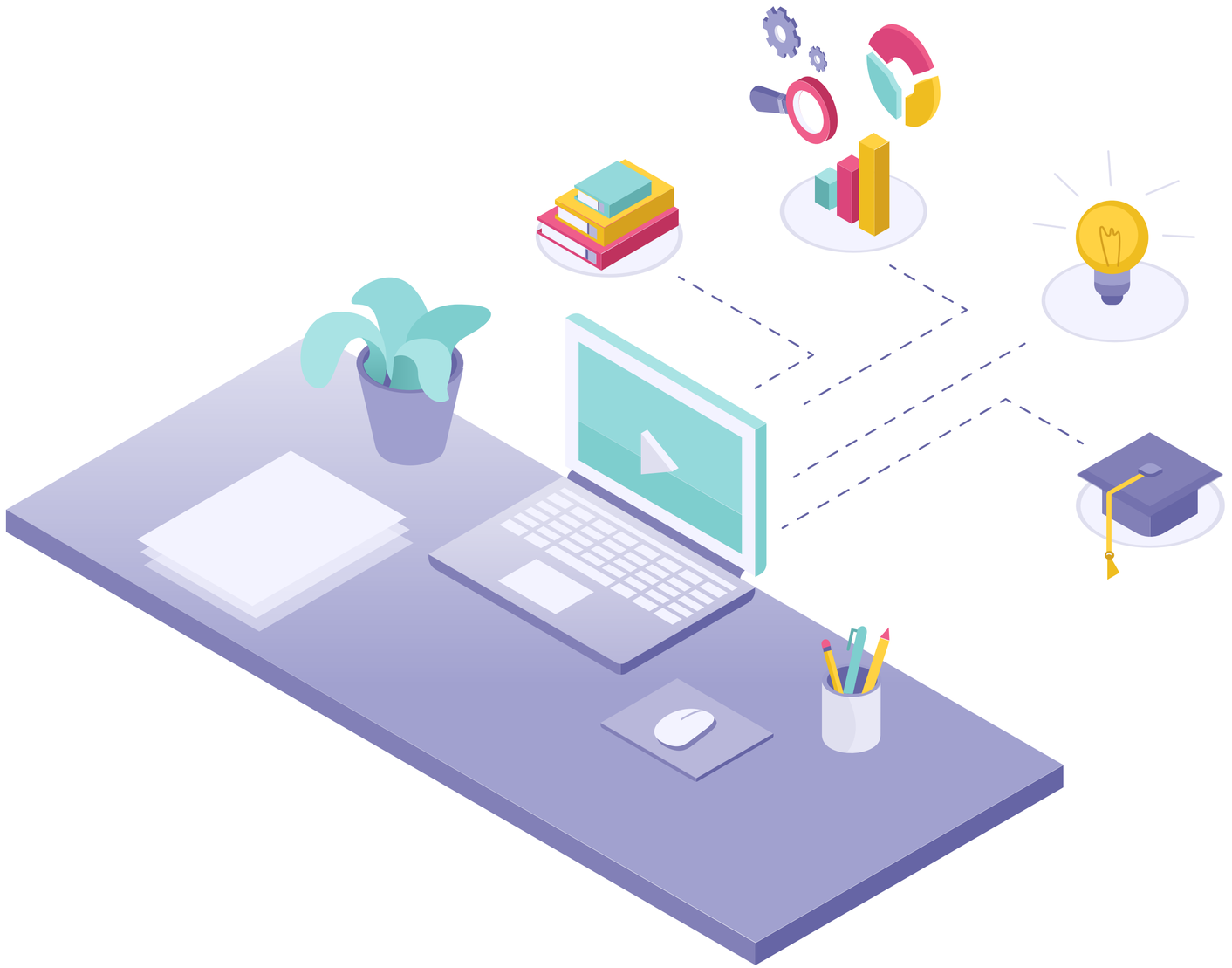
m6g.12xlarge

- 48 vCPU
- 192 Gio mémoire
- Processeur Graviton2

Prix : $2.16 / heure (Paris)

- Famille d'instance
- Génération
- Famille de processeurs
- Taille

Familles de types d’instances



Familles de types d'instances

+ 500 types d'instances

Regroupés par « famille » d'instances

Pour tous les cas d'usage

- Usage général
- Optimisé pour le calcul
- Mémoire optimisée
- Calcul accéléré
- Stockage optimisé
- Optimisée pour HPC

Famille d'instance

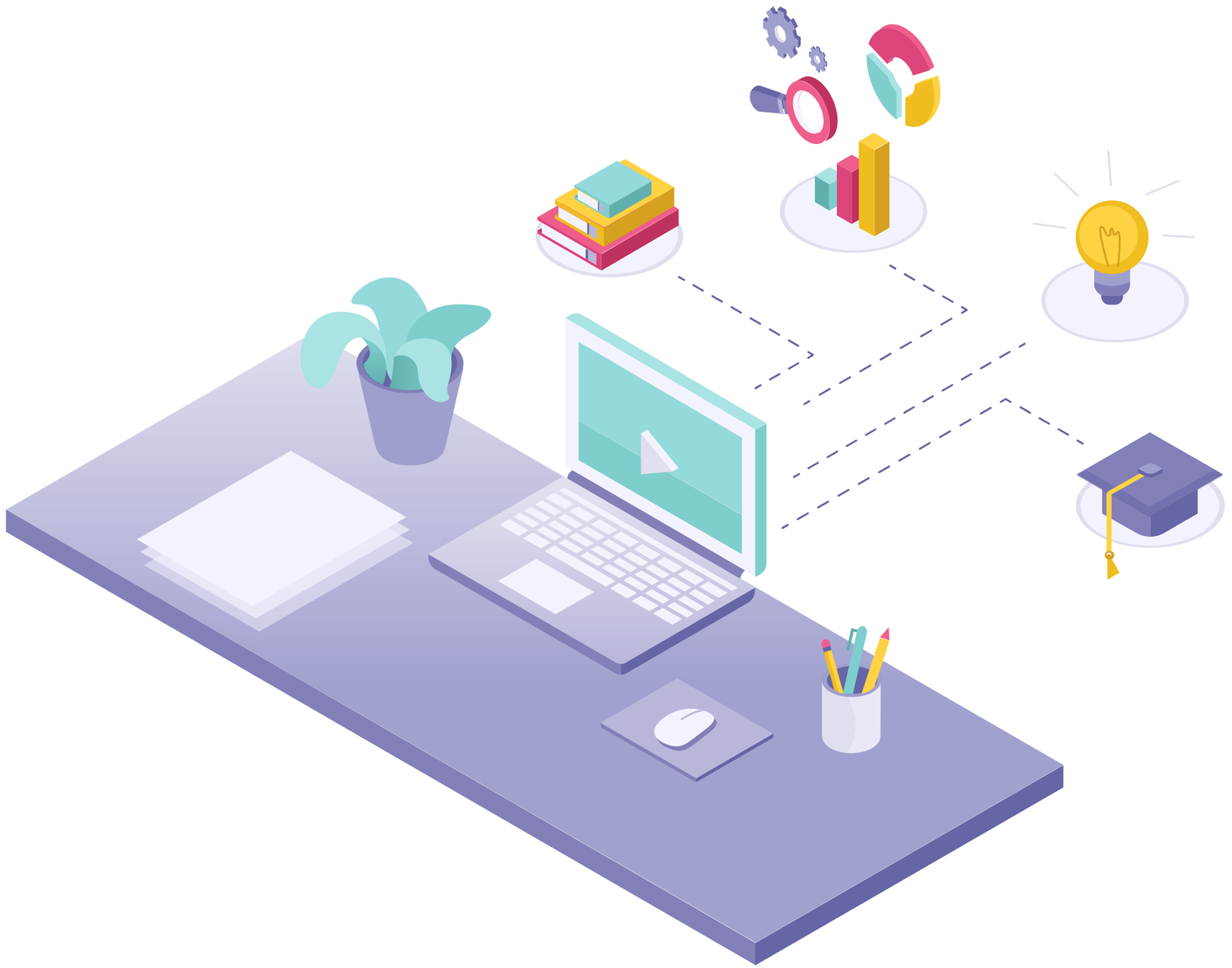
LeCloudFacile.com

Familles de types d'instances

Famille	Description	Cas d'usage	Type d'instance
Usage général	Instances EC2 avec un équilibre entre les ressources informatiques, la mémoire et les ressources réseau.	• Serveurs web • Serveurs d'applications • Microservices • Petites bases de données	• Instances T : T2, T3, T3a • Instances M : M4, M5, M6, M7 • ...
Calcul optimisé	Instances EC2 optimisées pour le calcul idéales pour les applications qui utilisent des processeurs haute performance.	• Traitements par lots (Batchs) • Serveurs web performants • Calcul haute performance (HPC) • Calcul intensif	• Instances C : C7g, C6g, C6i, C6a, C5, C5n, C5a, C4,...
Mémoire optimisée	Instances à mémoire optimisée conçues pour les charges de travail gourmandes en mémoire	• Bases de données open-source • Caches en mémoire • Big Data temps réel	• Instances R : R7, R6, R5, R4 • Instances X : X2, X1 • Instances Z : Z1
Calcul accéléré	Instances avec GPUs ou utilisant des accélérateurs matériels (coprocesseurs)	• Recherche en génomique • Analytique financière • Traitement vidéo temps réel	• Instances P : P5, P4, P3, P2 • Instances G : G5, G4, G3 • Instances F1, VT1, Inf2, Inf1, DL1 ...
Stockage optimisé	Instances optimisées pour le stockage. Idéales pour les besoins d'accès séquentiel élevé en lecture et en écriture à de gros volumes de données sur du stockage local	• Bases de données • Indexation de données (Opensearch) • Big Data temps réel (Spark	• Instances i : I4, I3, Is4gen, I4i • Instances D : D2, D3 • Instances H : H1
Optimisée pour HPC	Instances spécialement conçues pour les charges de travail HPC à grande échelle sur AWS.	• Calcul HPC • Prévisions météo • Dynamique moléculaire	• Instances Hpc : Hpc7g, Hpc6id, Hpc6a

https://aws.amazon.com/fr/ec2/instance-types/

Changer le type d’instance



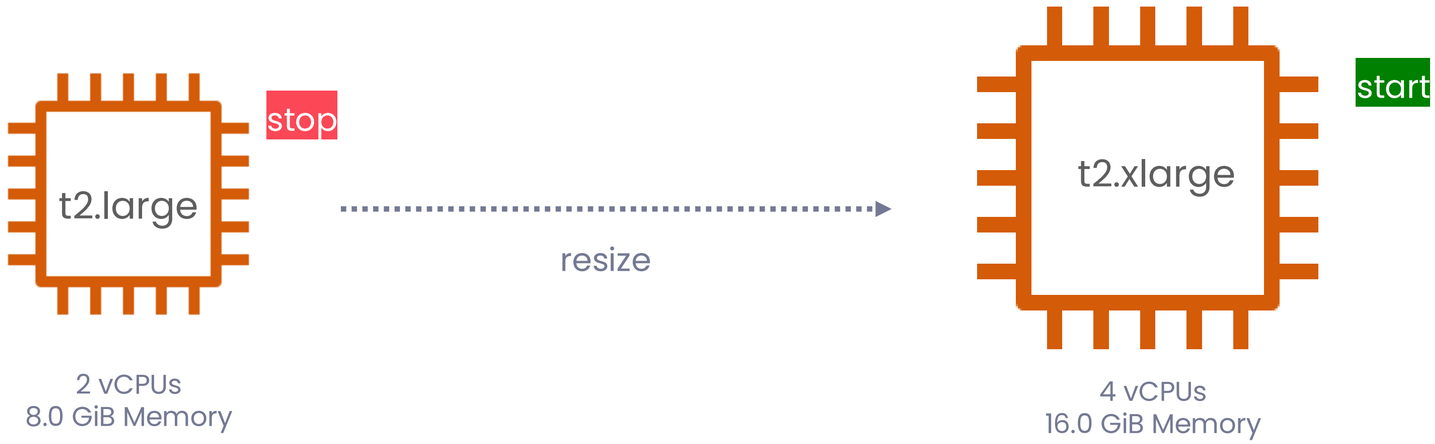
Changer le type d'instance

Permet d'augmenter ou de diminuer la taille d'une instance

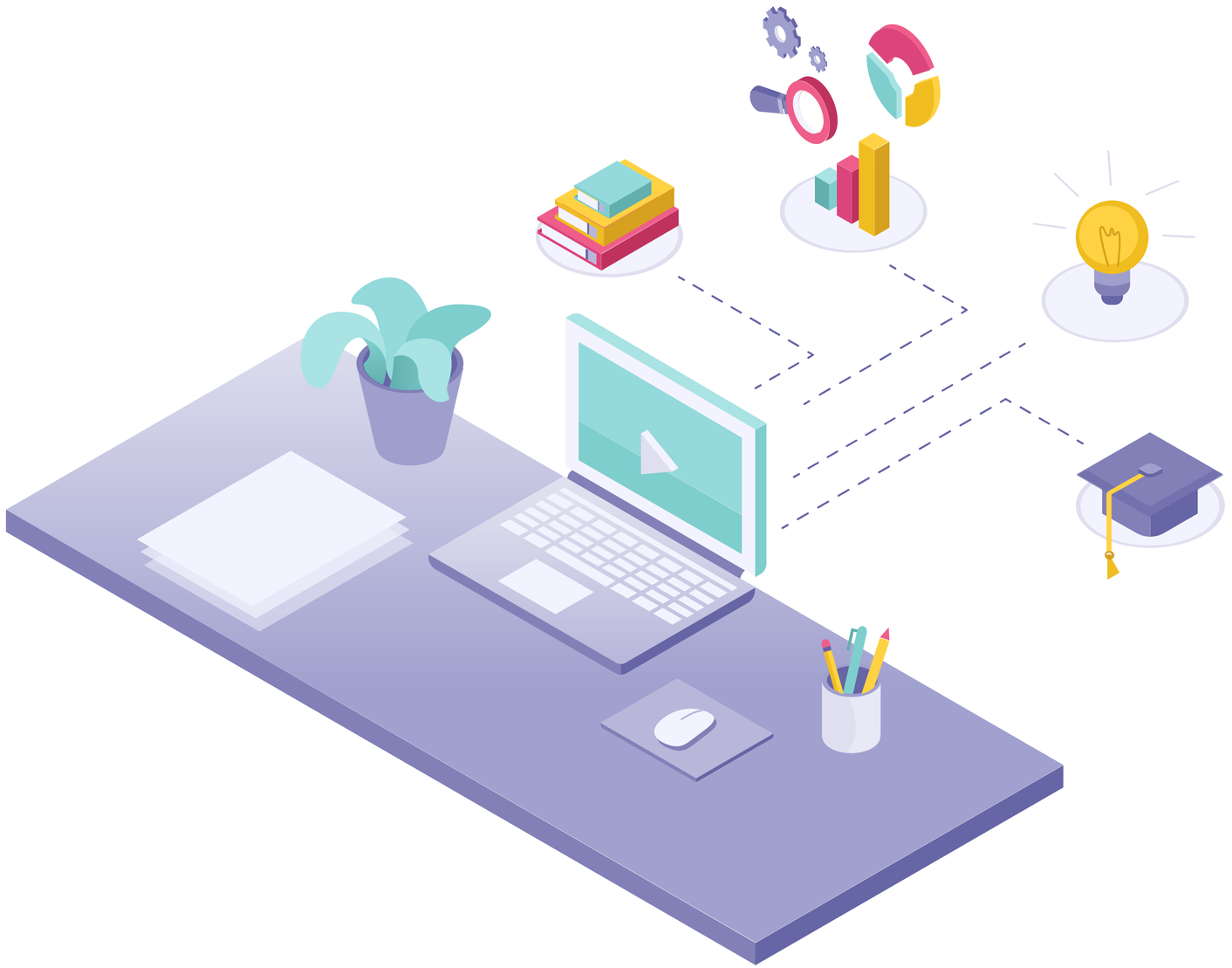
En anglais: « ***Resize*** »

Possible à tout moment -> Passe par un stop/start de l'instance EC2

Utile pour le Right-sizing : on adapte la taille de l'instance au besoin de l'application



Paire de clés (Keypair)



Paire de clés (keypair)



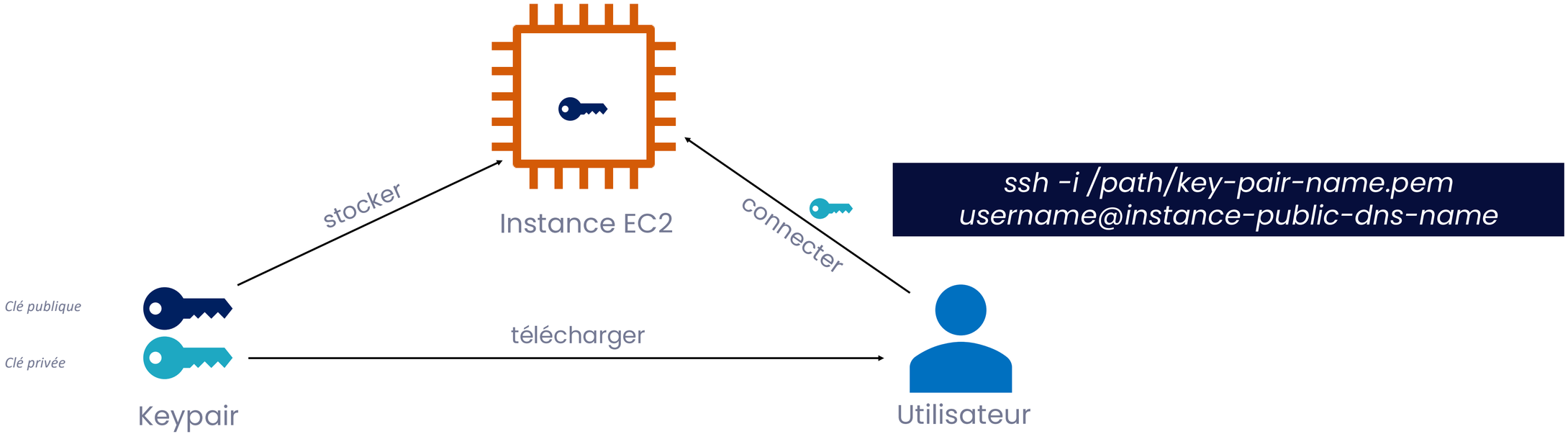
Permet de se connecter (ssh ou rdp) aux instances EC2

Composée d'une *clé privée* et d'une *clé publique*.

Possible de lancer une instance EC2 sans KeyPair.

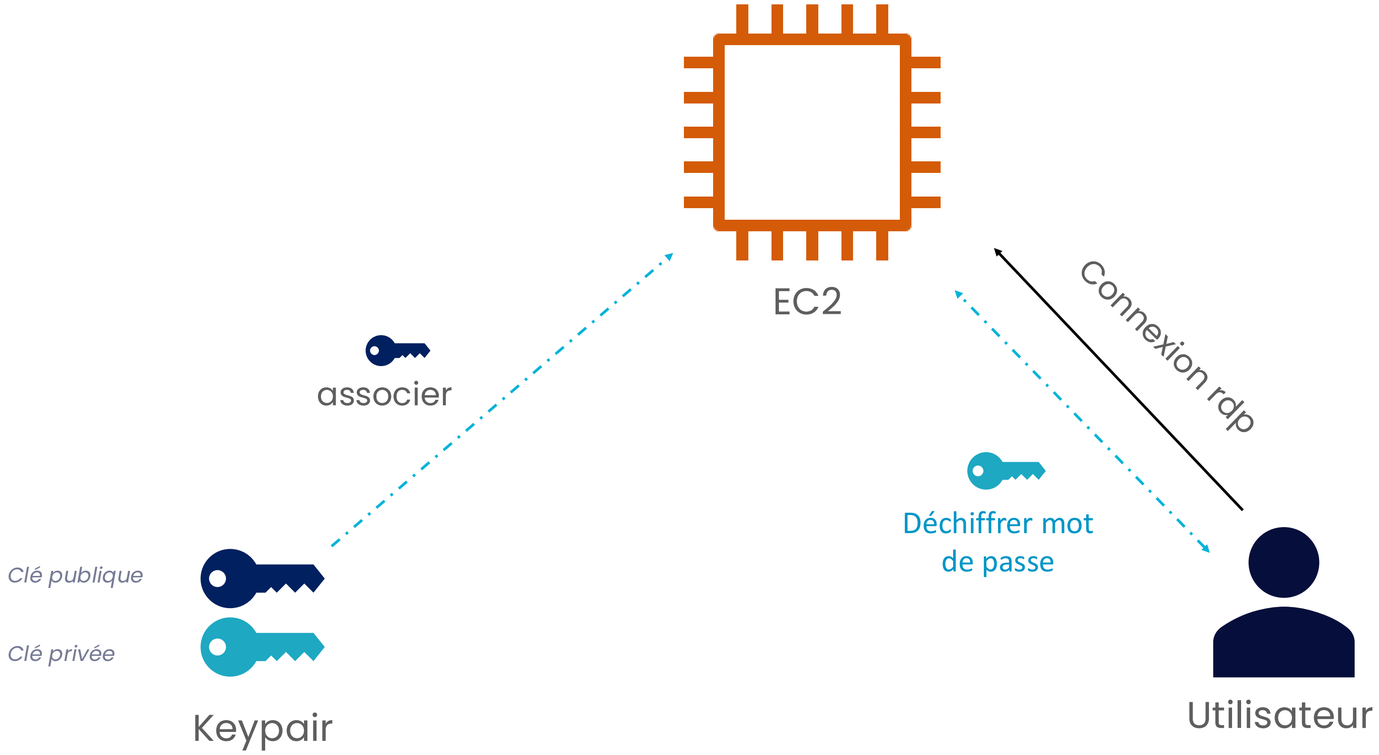
Paire de clés (keypair)

EC2 Linux

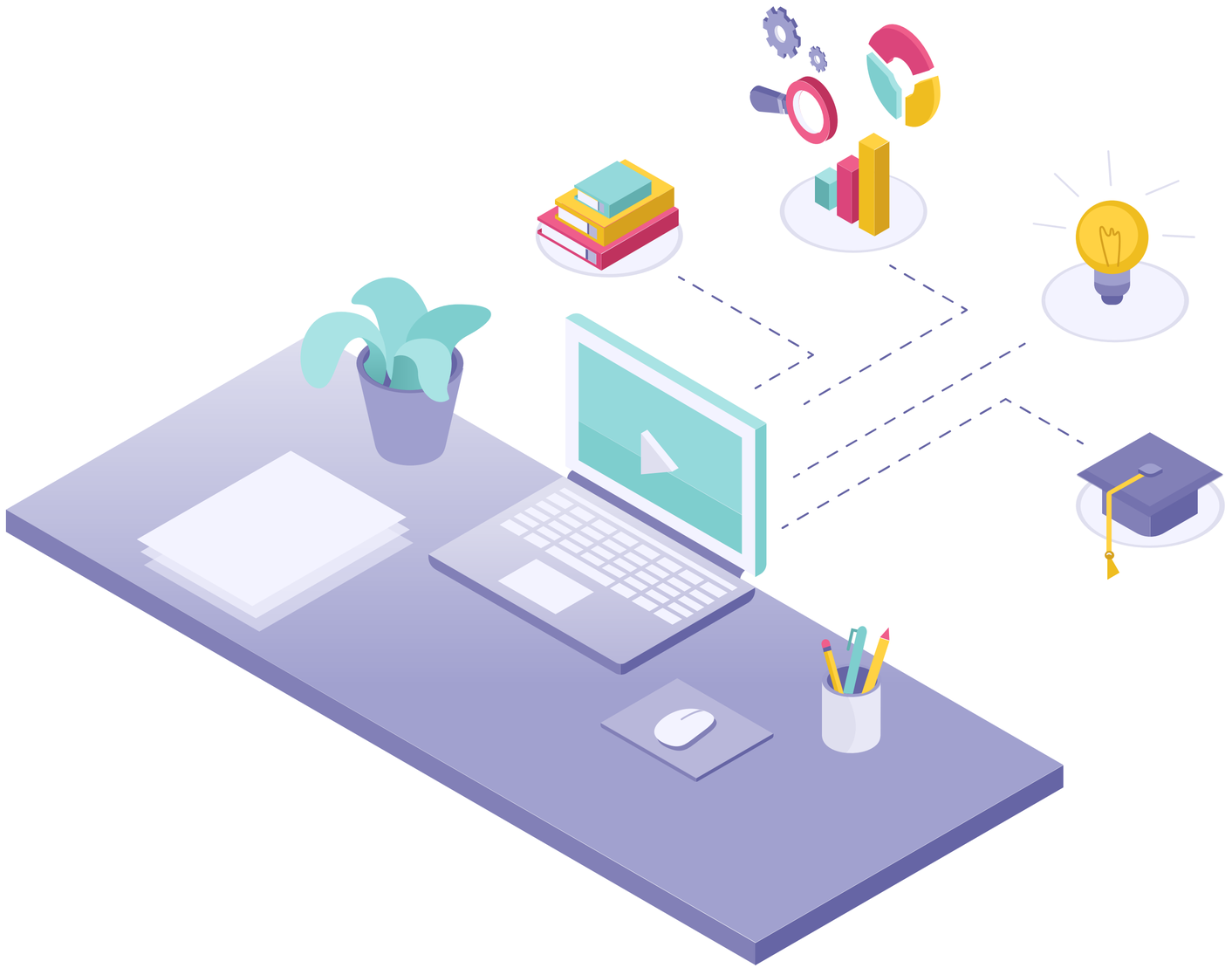


Paire de clés (keypair)

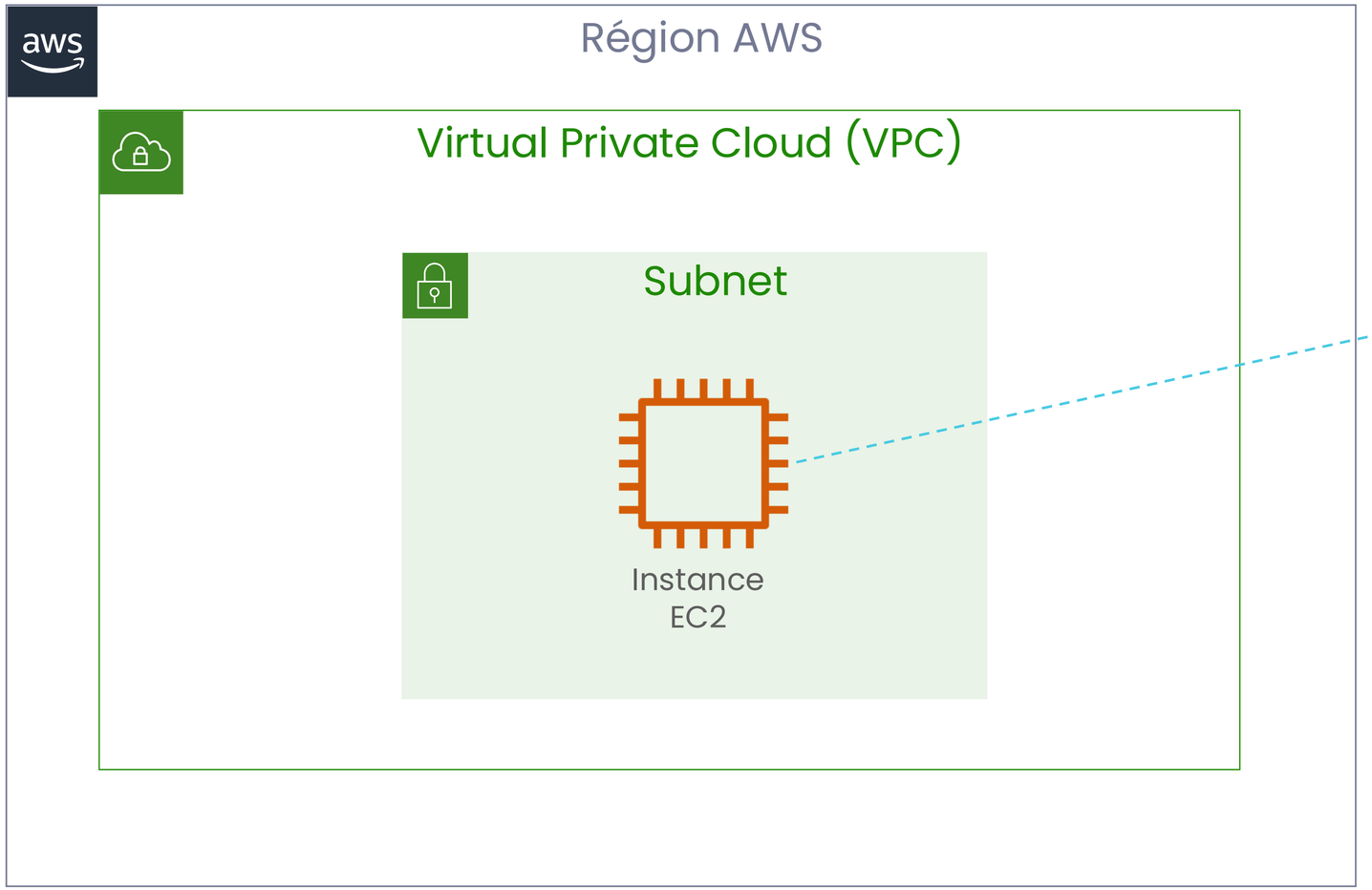
EC2 Windows



Adressage IP



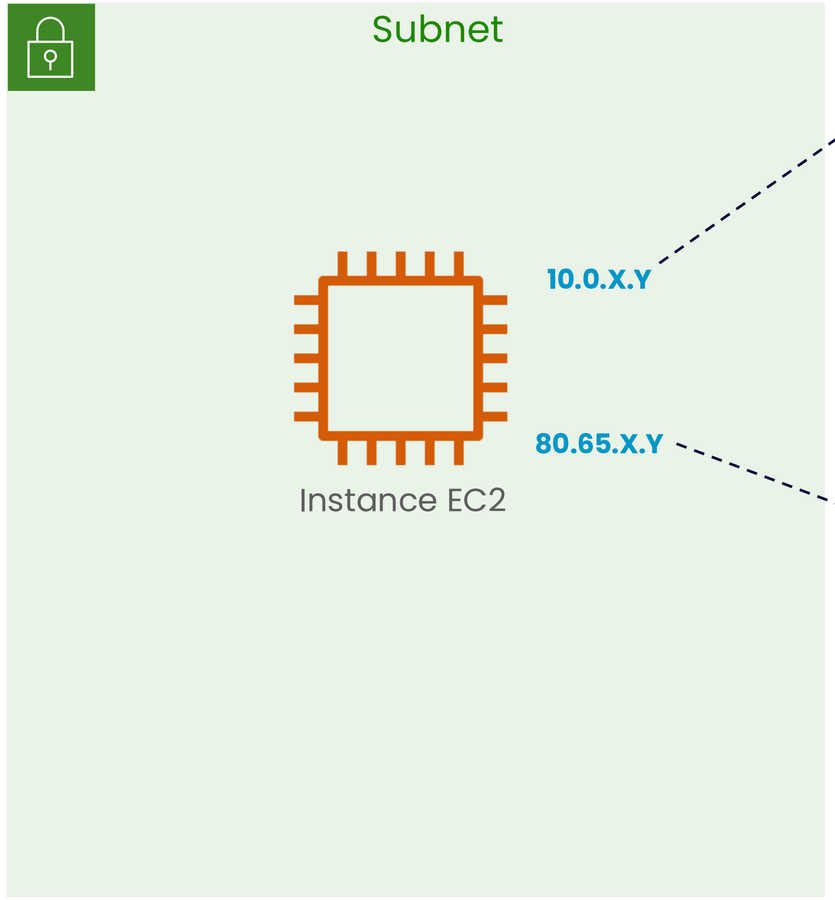
Sous-réseau (subnet)



1 instance EC2 s'exécute dans un sous-réseau choisi au lancement

Possible d'avoir plusieurs instances EC2 dans le même sous-réseau

Adresses IP



IP Privée (*Private IP*)

Assignée automatiquement par AWS

Permet uniquement une communication interne

Reste attachée à l'instance EC2 qu'elle soit stoppée ou démarrée

IP Publique (*Public IP*)

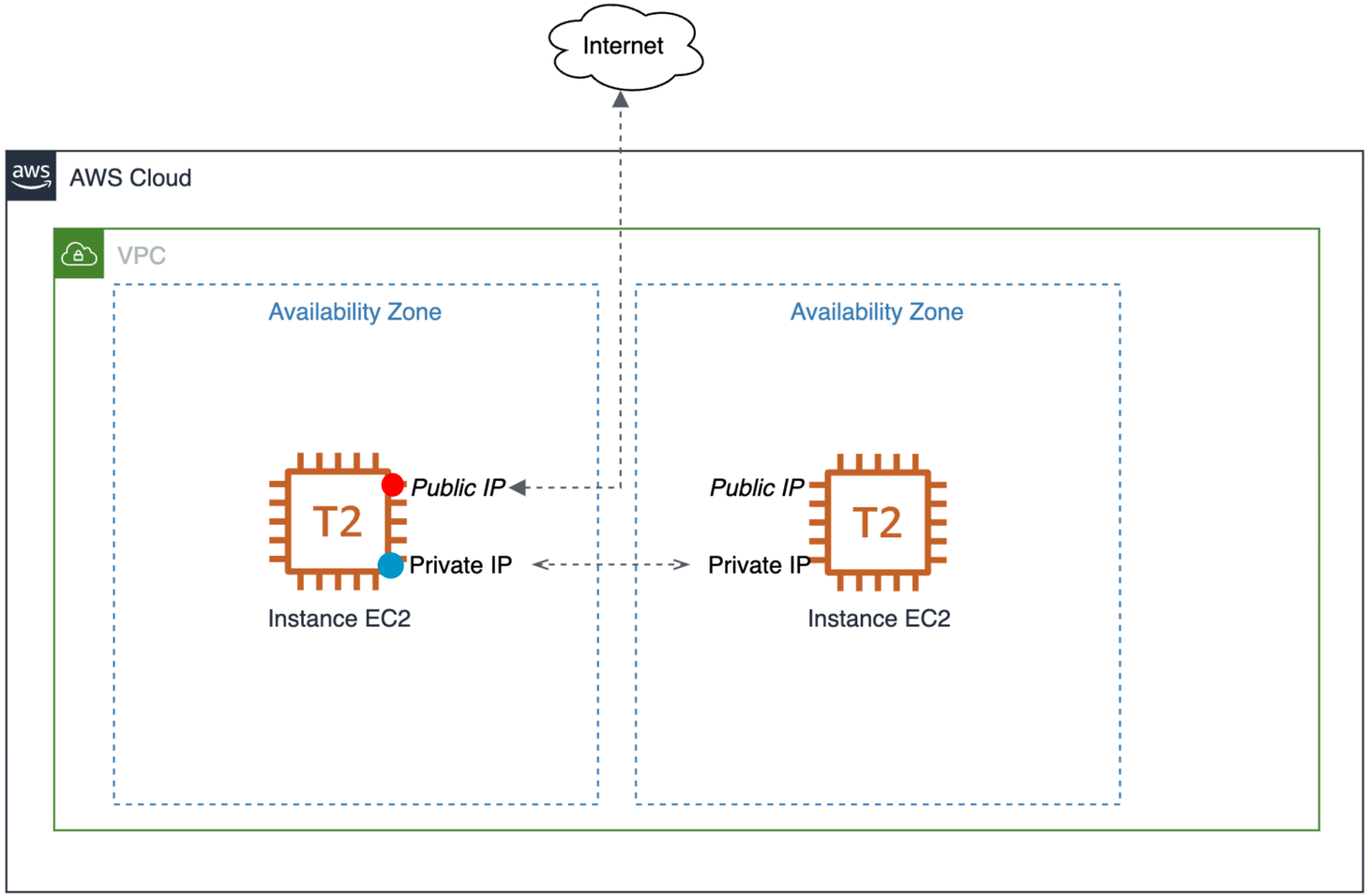
Permet à l'instance EC2 de se connecter à Internet

Permet à l'instance EC2 d'être joignable depuis Internet

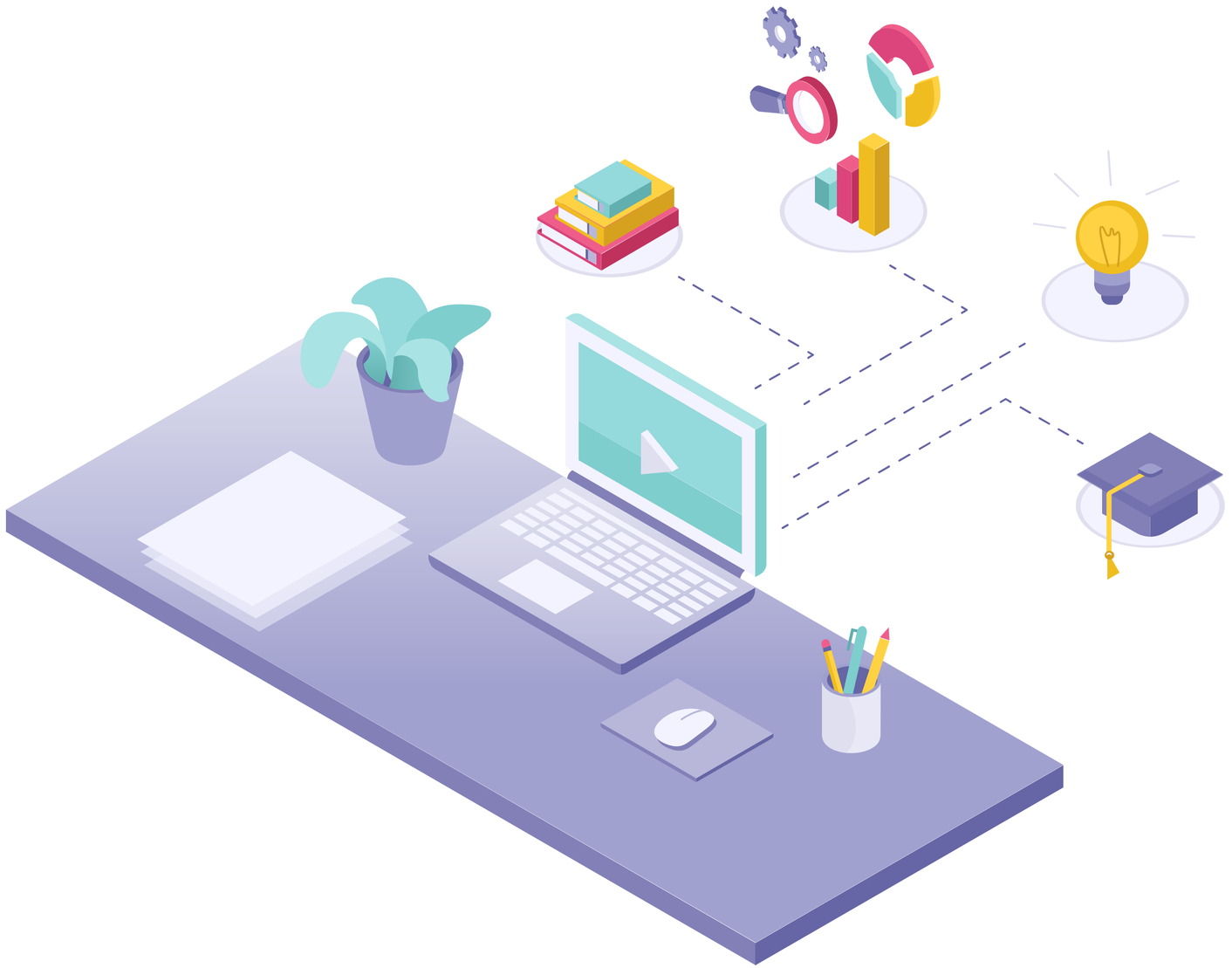
Change après un Stop -> Start de l'instance EC2.

Utilisez une *Elastic IP* pour avoir une IP fixe

Adresses IP


Internet
AWS Cloud
VPC
Availability Zone
Availability Zone
T2
Public IP
Private IP
Instance EC2
Public IP
Private IP
T2
Instance EC2

Groupe de sécurité



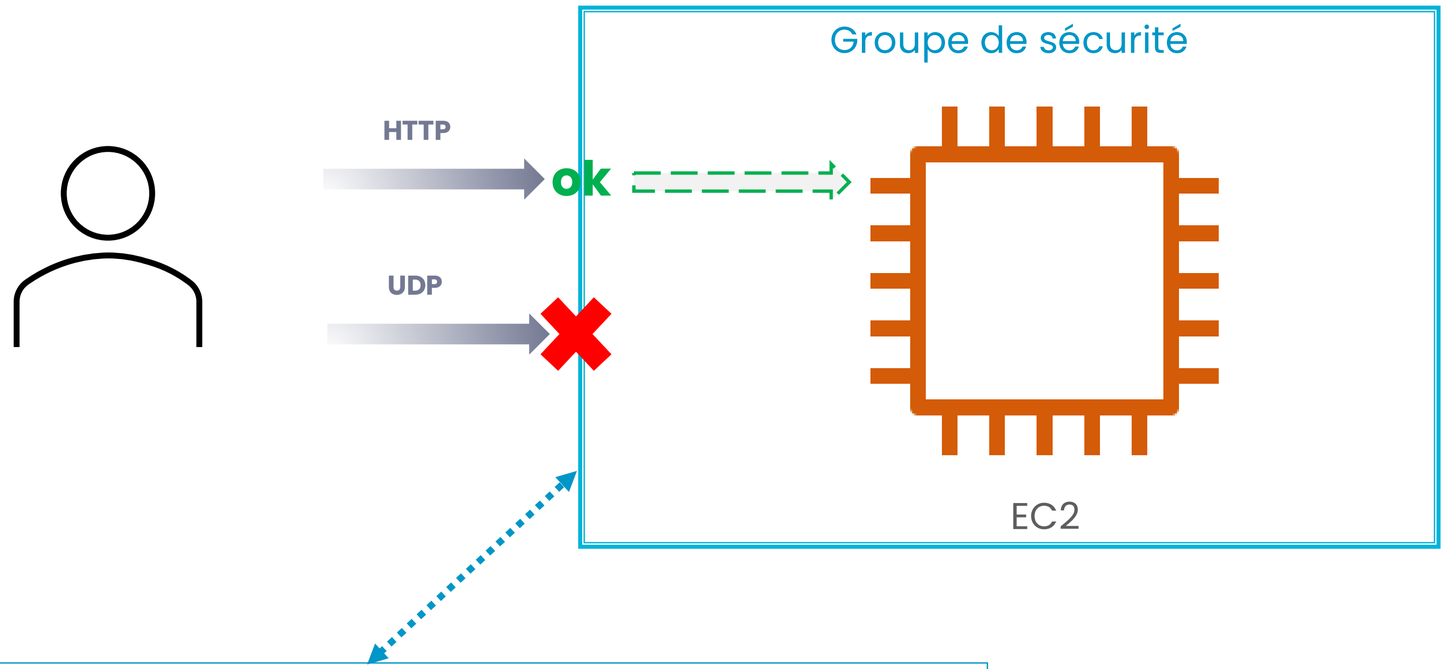
Groupe de sécurité

Parefeu virtuel qui protège votre instance EC2

Le même groupe de sécurité peut être associé à 1 ou plusieurs EC2

Permet de contrôler le trafic entrant (**inbound**) et sortant (**outbound**)

Illustration d'un groupe de sécurité



Security group rules:

Inbound | Outbound

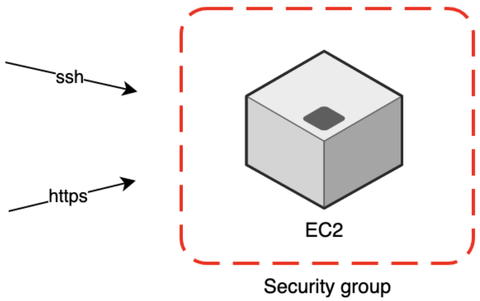
Type	Protocol	Port Range	Source	
SSH	TCP	22	Anywhere	0.0.0.0/0, ::/0
HTTP	TCP	80	Anywhere	0.0.0.0/0, ::/0
HTTPS	TCP	443	Custom	0.0.0.0/0, ::/0

Les règles

Contrôlent le trafic entrant et sortant en fonction du protocole et du port

Configuration via des règles **ALLOW** uniquement

Le DENY est **implicite** : tout trafic non autorisé est refusé



Security group name Web Server Security Group

Description Security for production web server.

VPC vpc-e68d9c81 | DefaultVPC (default)

Security group rules:

Inbound | Outbound

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Anywhere	0.0.0.0/0, ::/0	Admin access.
HTTP	TCP	80	Anywhere	0.0.0.0/0, ::/0	Web traffic.
HTTPS	TCP	443	Custom	0.0.0.0/0, ::/0	Secure web traffic.

Add Rule

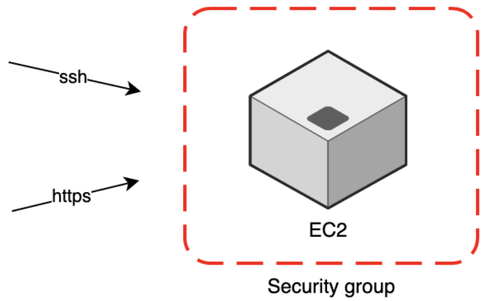
A retenir sur les groupes de sécurité

Groupe de sécurité : obligatoire pour une instance EC2

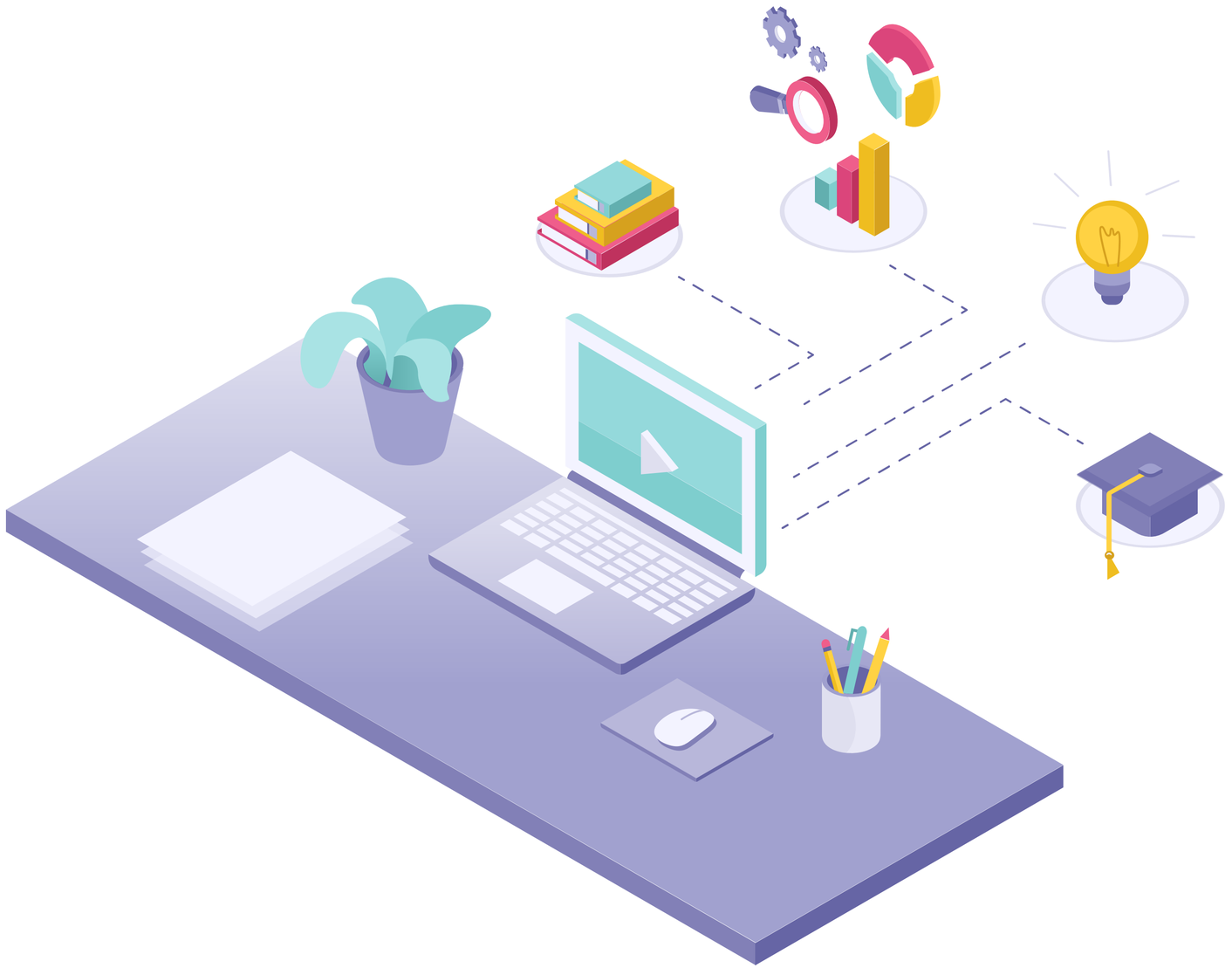
Règles **ALLOW** uniquement (Le DENY est **implicite**)

Filtrent le trafic en fonction des protocoles, numéros de port et plages d'IP

Vous pouvez ajouter et supprimer des règles à tout moment (Prise en compte dynamique)

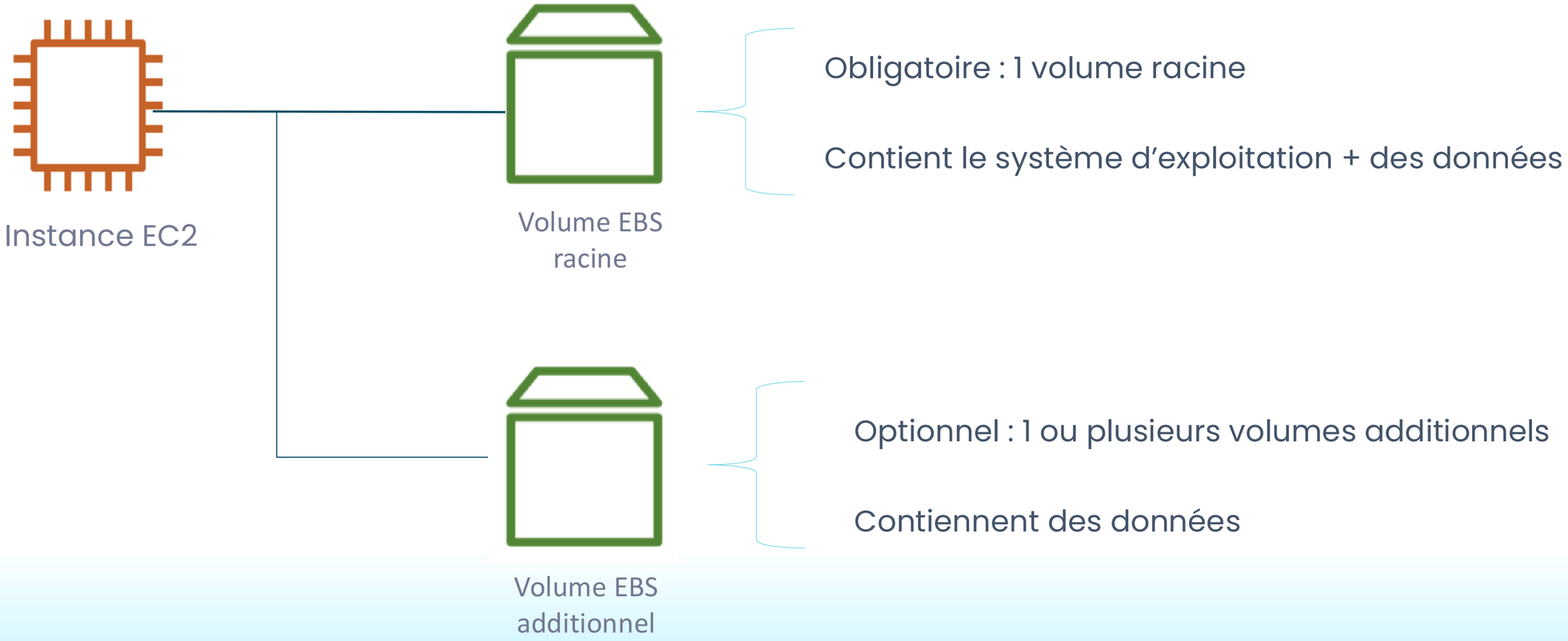


Volumes EBS

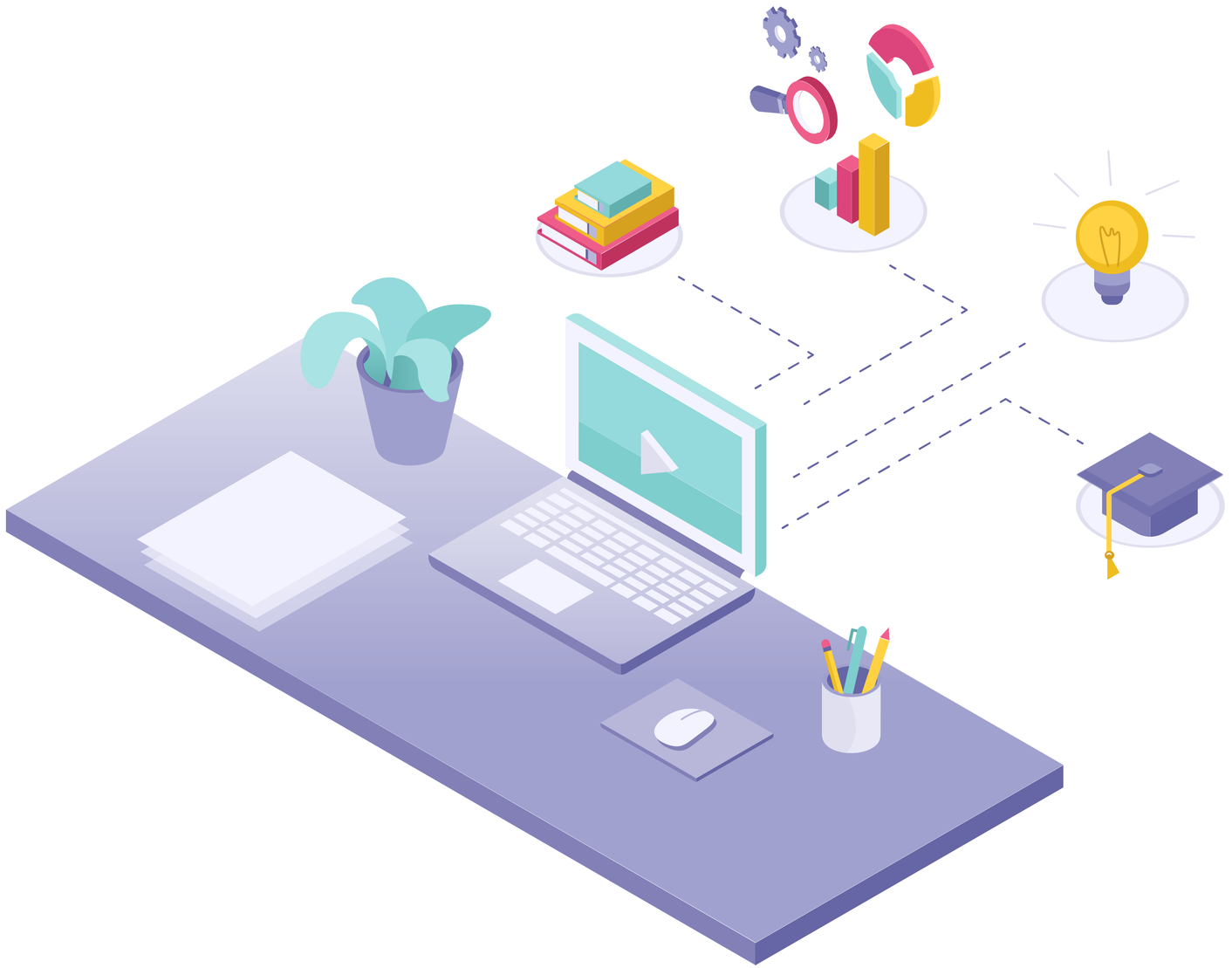


Volumes EBS

Disques de stockage des EC2, attachés via le réseau



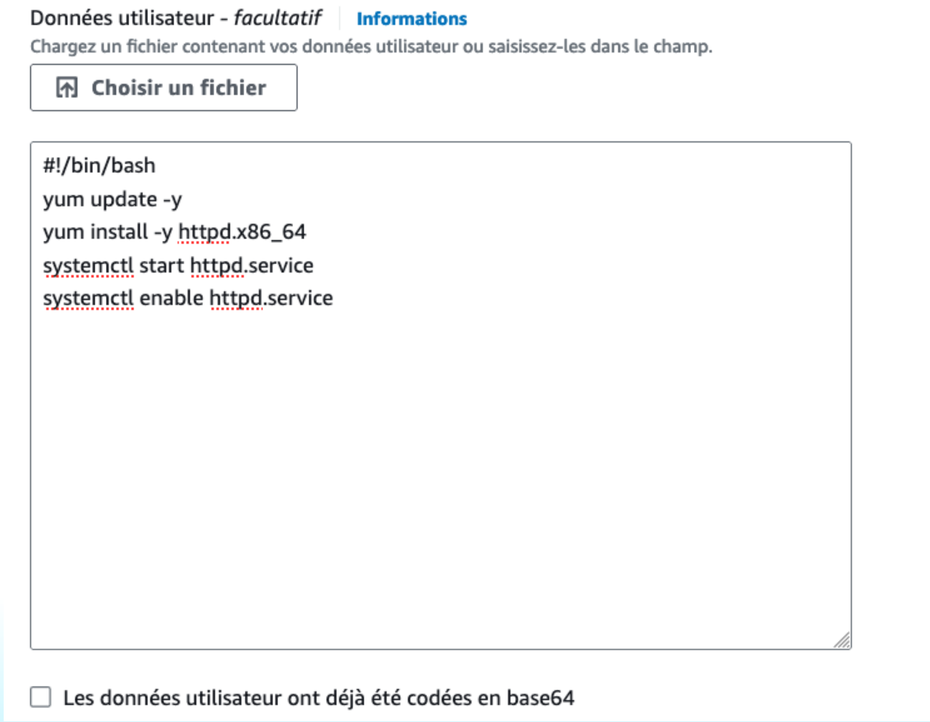
EC2 User Data



EC2 User Data (Données utilisateur)

Permet de passer des **scripts qui sont exécutés automatiquement au lancement** de l'instance

Configuration « ***Détails avancés*** » au moment de lancer l'instance



Exemples de cas d'usage :

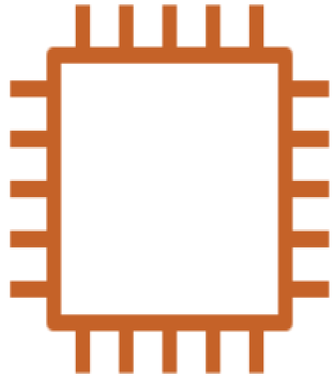
- Installer un serveur web ou un service (httpd,...)
- Installer et configurer un logiciel
- Installer des mises à jour

Exemple EC2 User Data

```
#!/bin/bash
yum update -y
yum install -y httpd.x86_64
systemctl start httpd.service
systemctl enable httpd.service
```

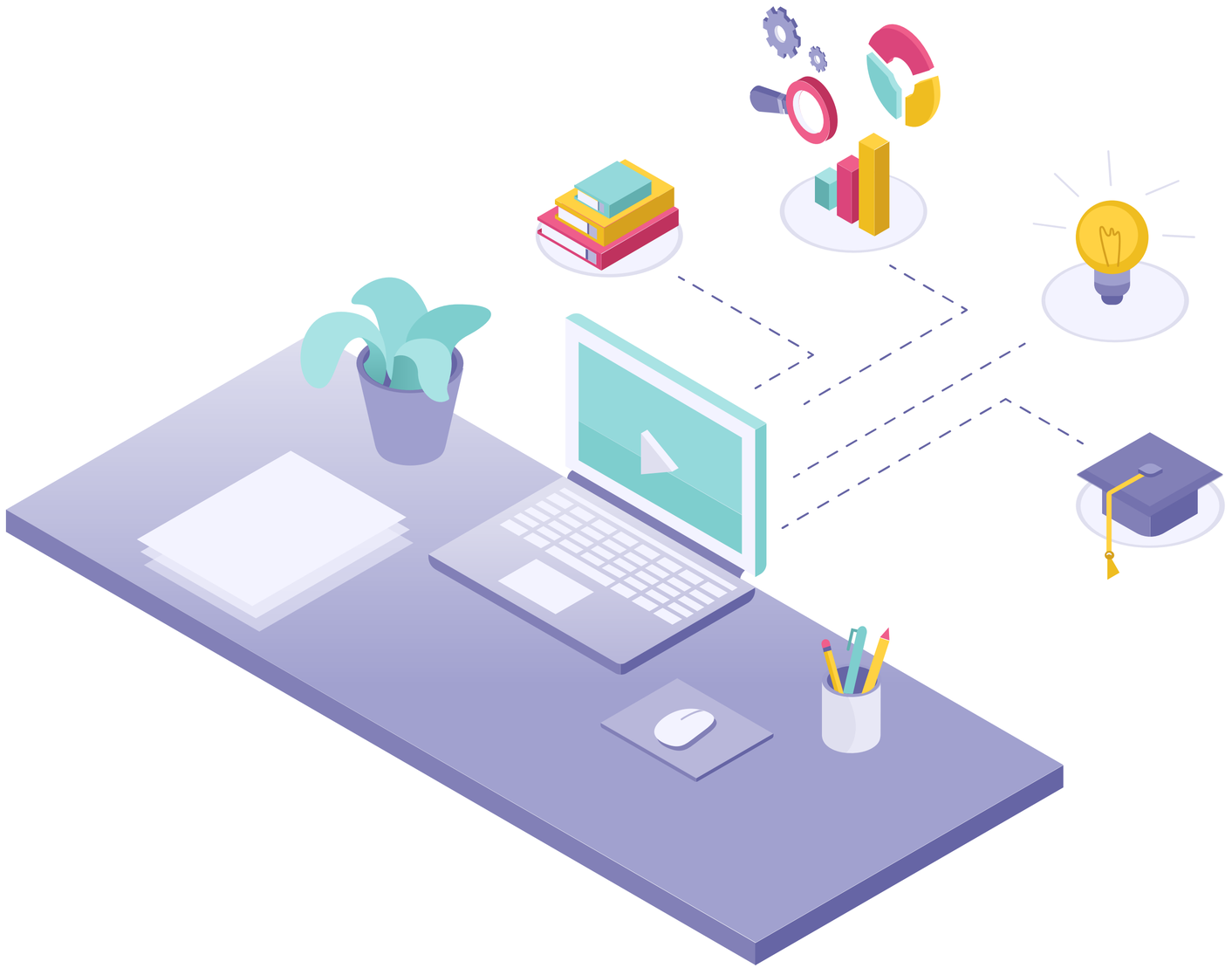
Exemple de script EC2 User Data

Au démarrage

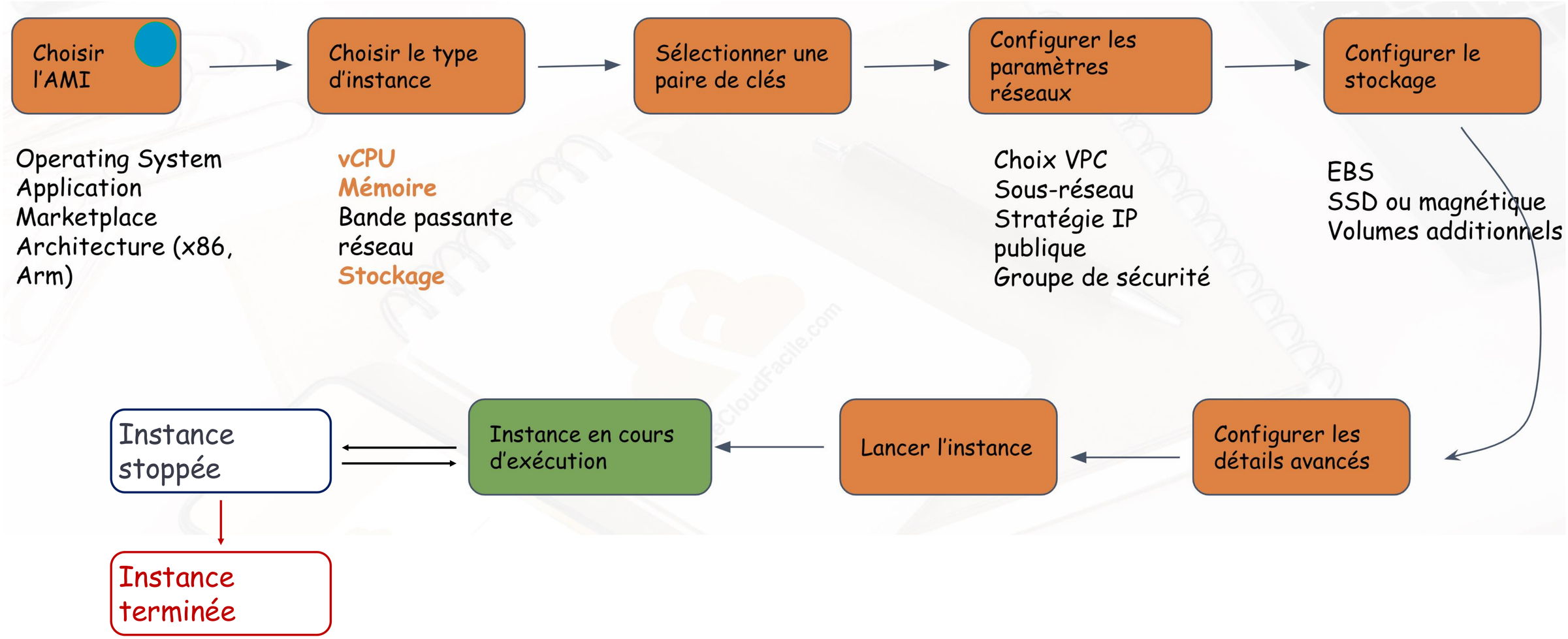


Instance EC2 Linux

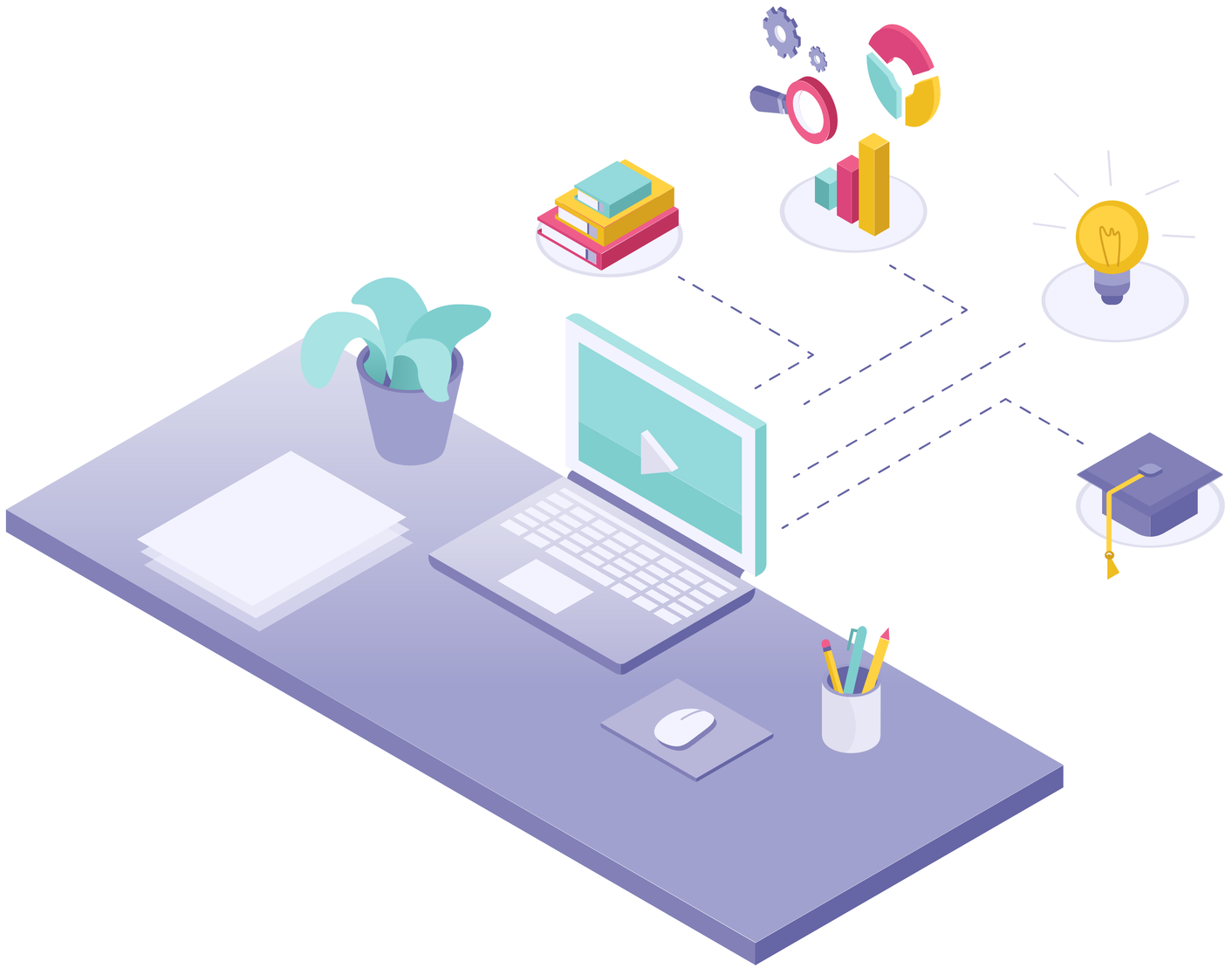
Cycle de vie d’une instance



Lancer une instance EC2

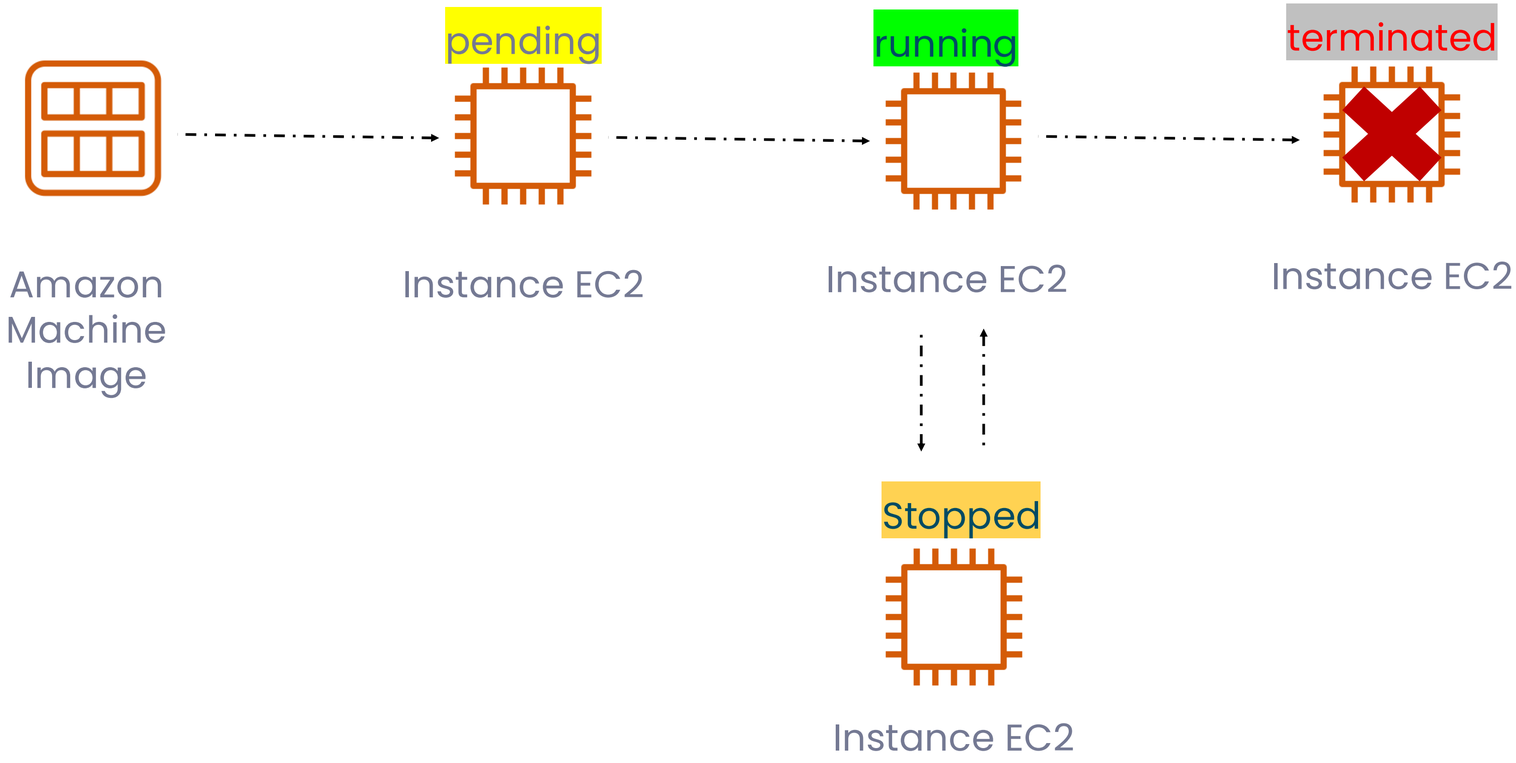


Lancer une instance EC2

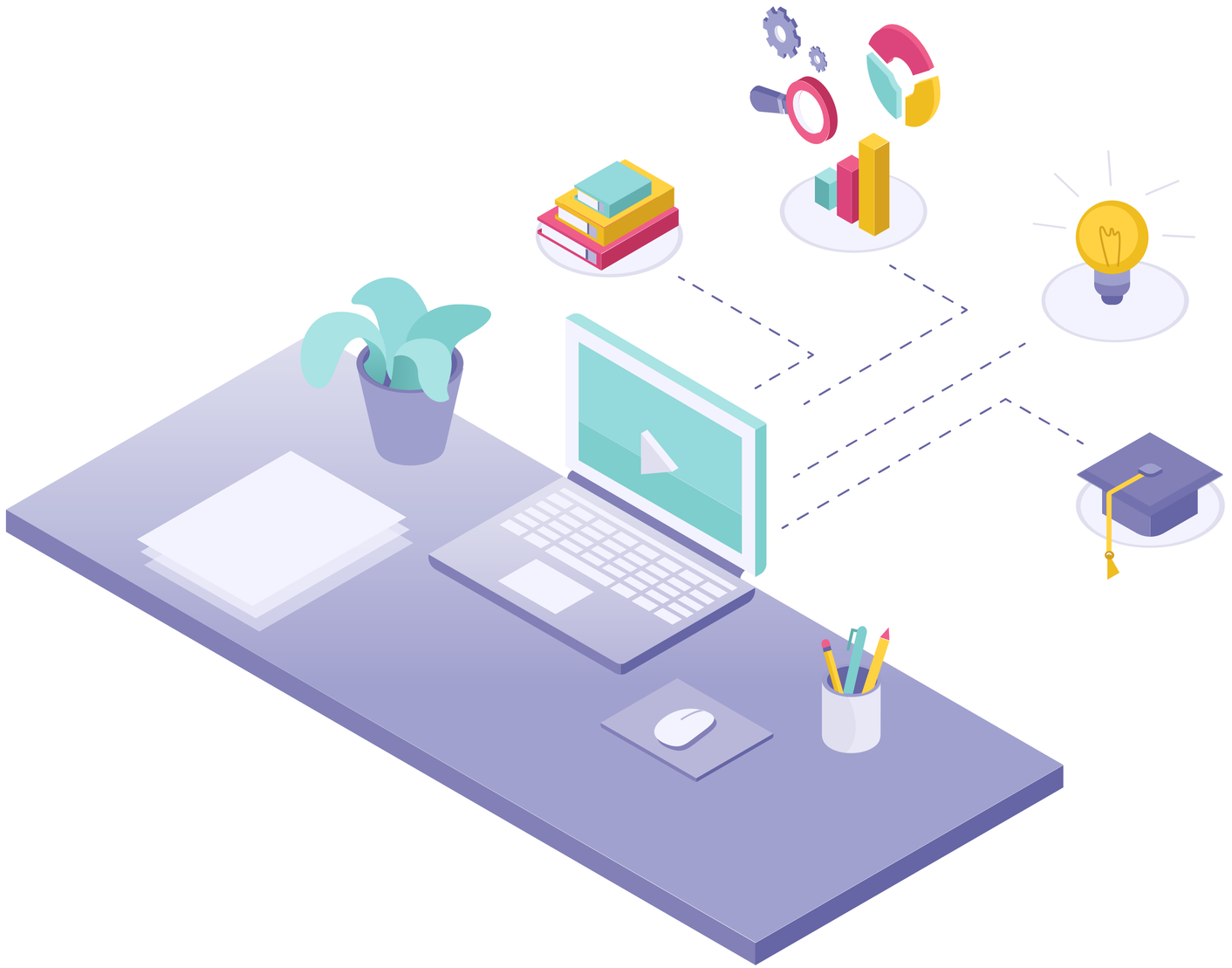


Cycle de vie d'une instance EC2

RAJOUTER TOUS LES ETATS + TRAD. EN Français + INFOS FACTURATION (QUELS SONT LES ETATS FACTURES PAR AWS)



Modèles de tarification EC2



LeCloudFacile.com

Modèles de tarification EC2



Instance EC2

Offre gratuite

Permet de tester gratuitement Amazon EC2 pendant 1 an

On-Demand

Paiement de la capacité utilisée à la seconde ou à l'heure, sans engagement

Savings Plans

Engagement sur 1 ou 3 ans avec une reduction jusqu'à -72%

Reserved Instances

Engagement sur 1 ou 3 ans avec une reduction jusqu'à -72%

Instances Spot

Utilisation d'instances EC2 aux enchères avec une reduction jusqu'à -90%

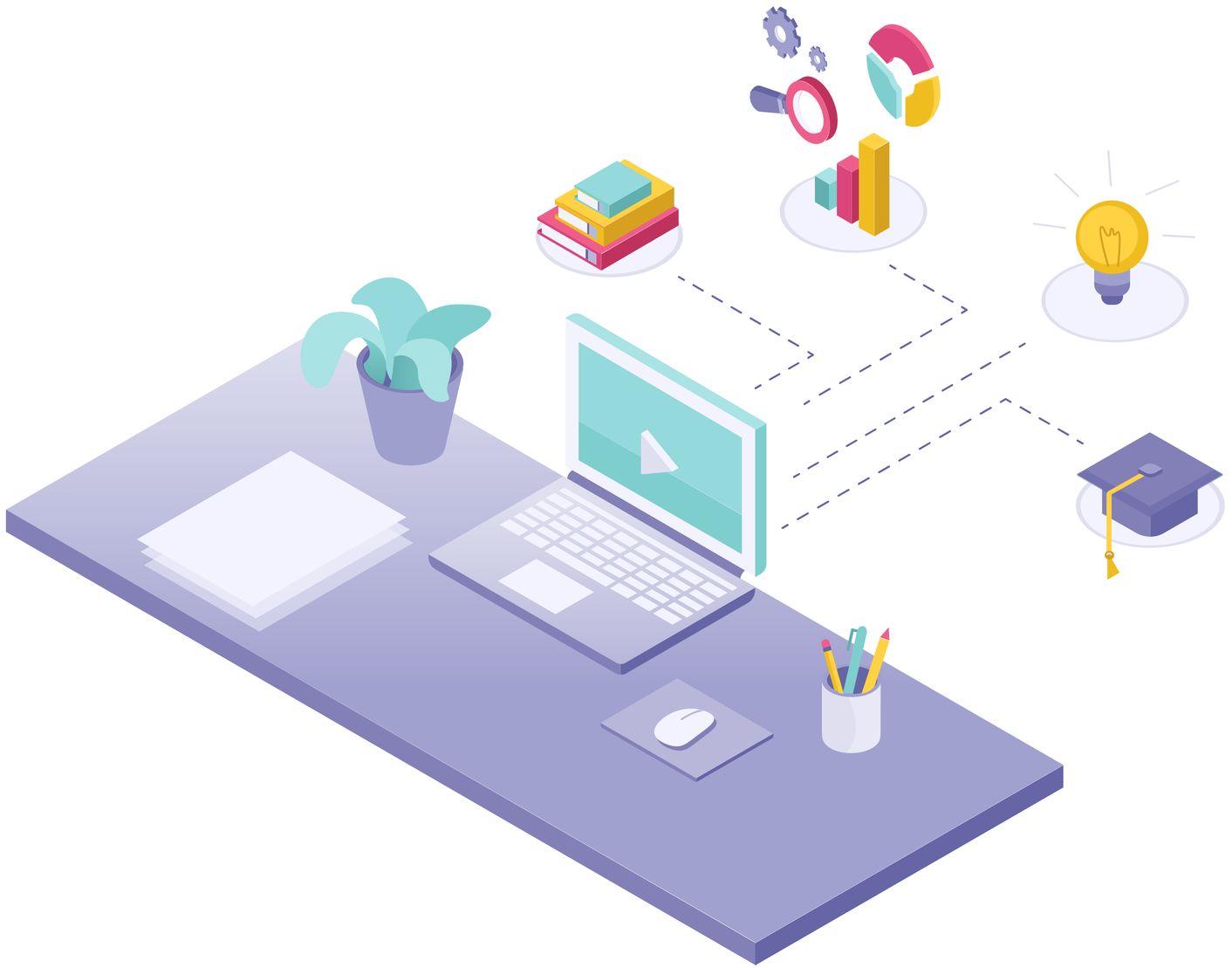
Dedicated Hosts

Serveur physique entièrement dédié.

Dedicated Instances

Instances qui s'exécutent sur du matériel physique dédié

Offre gratuite 12 mois



Offre gratuite 12 mois

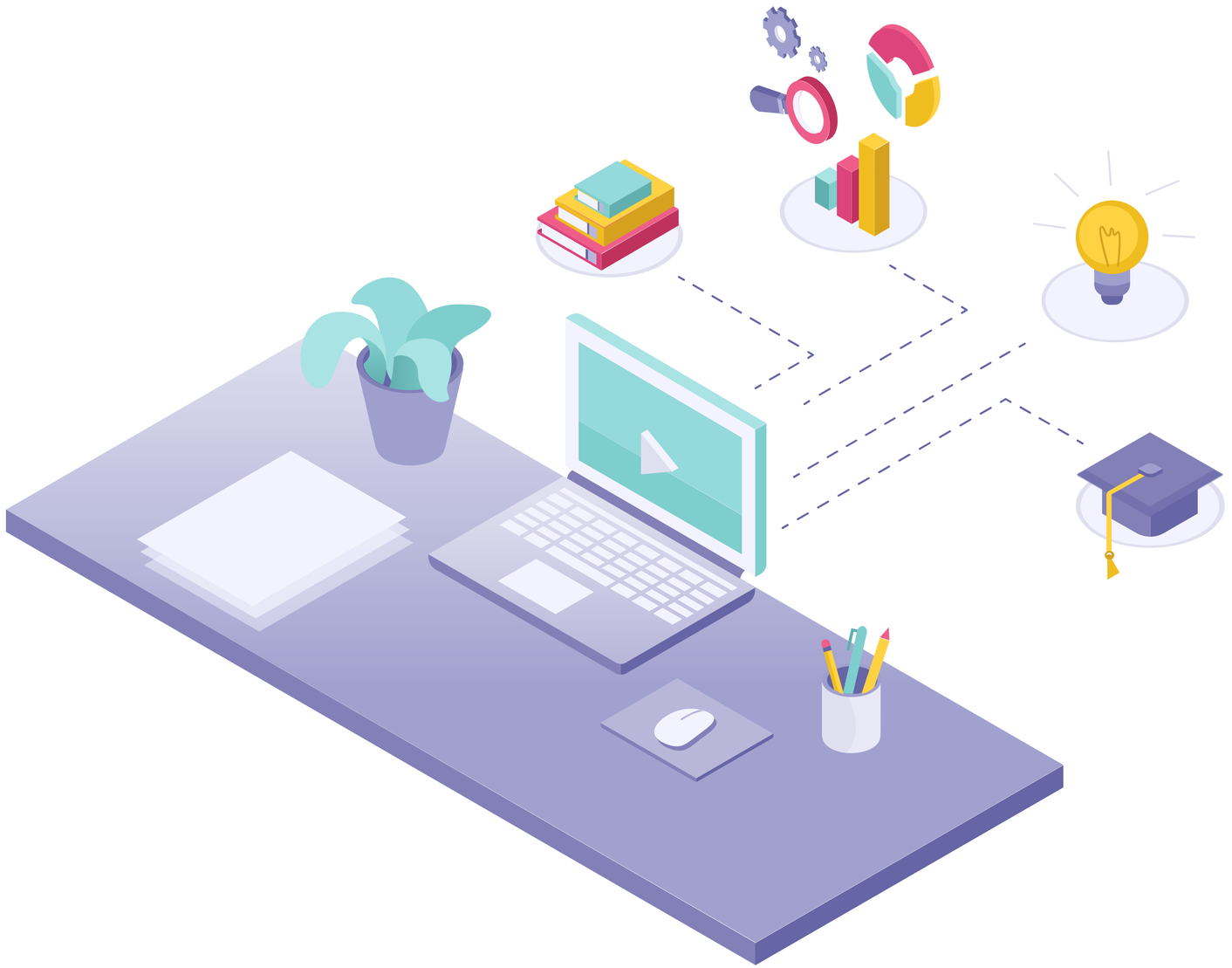
Pour les nouveaux clients (<= 12 mois)

Permet de tester EC2 gratuitement

750 heures par mois d'utilisation des instances Linux et Windows

Type d'instance: t2.micro (ou t3.micro selon les régions)

On-Demand



On-Demand

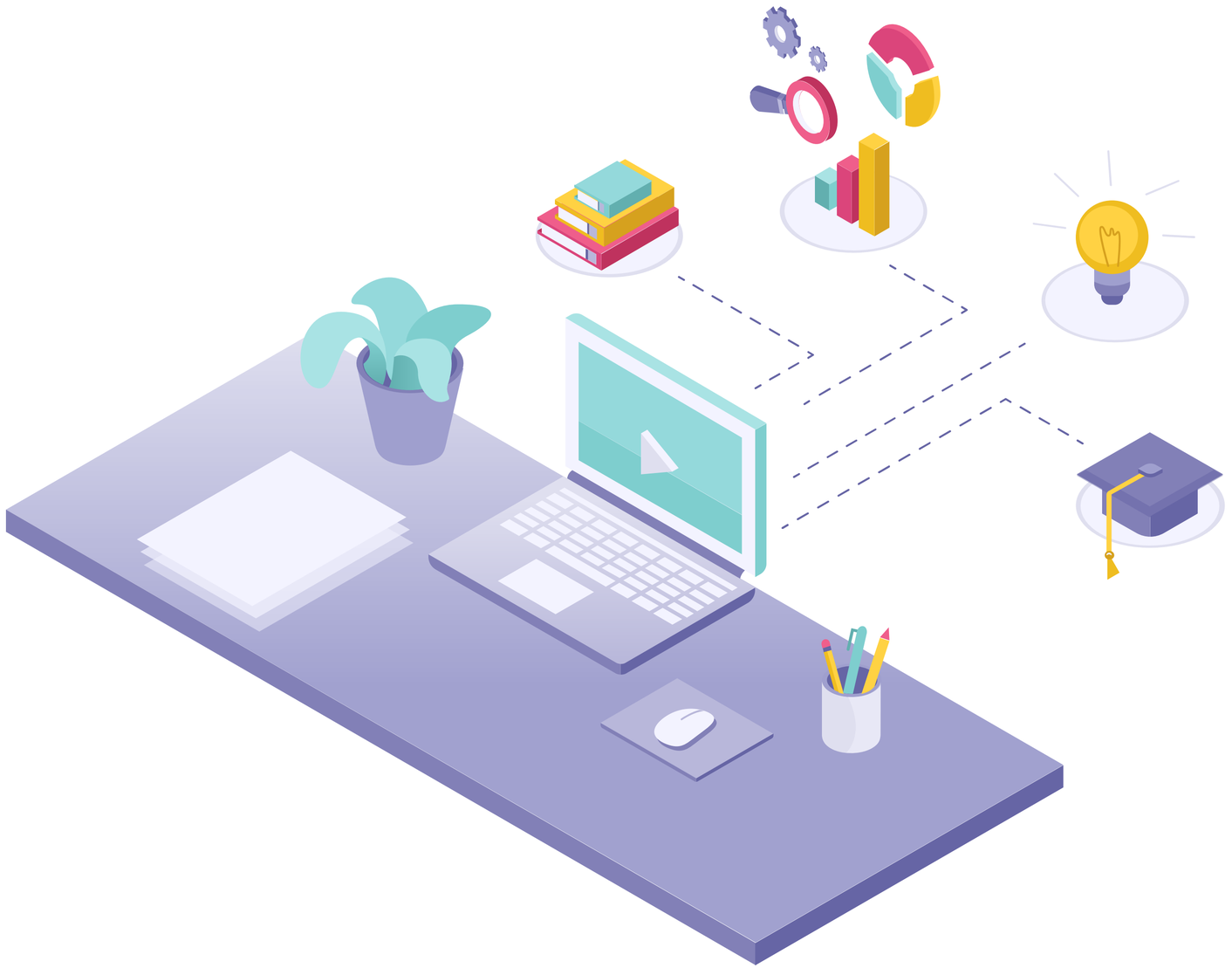
Sans engagement -> « *Pay as you go* »

Paiement à la seconde ou à l'heure d'utilisation des EC2

Recommandé pour :

- les utilisateurs ne souhaitant pas s'engager avec AWS
- les charges de travail à **court terme ou imprévisibles**
- les applications développées ou testées **pour la 1ère fois**

Savings Plans



Savings Plans

Modèle avec engagement sur 1 ou 3 ans

Discount jusqu'à -72% par rapport au *On-Demand*

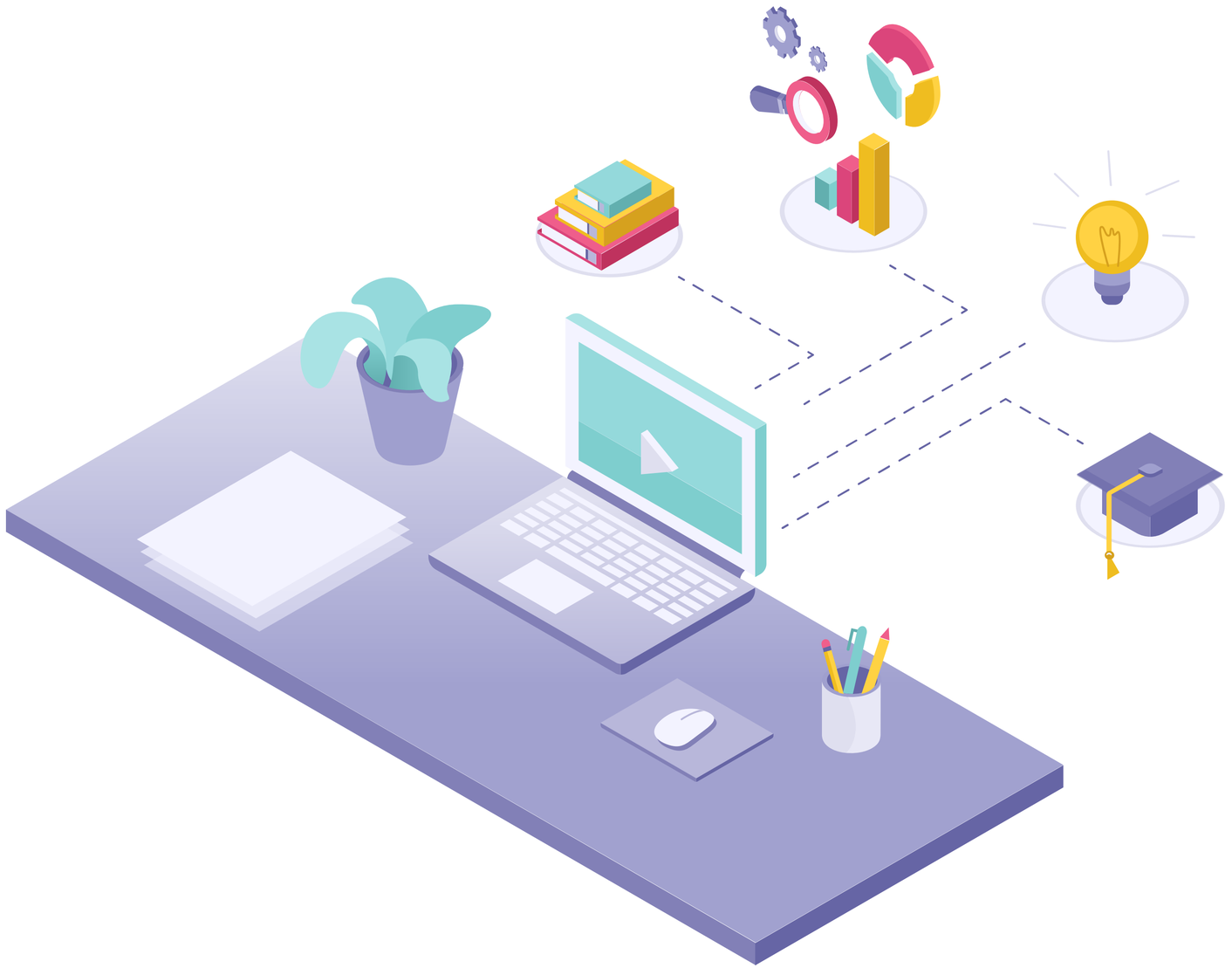
Engagement mesuré en $/heure

Options de paiement : *No Upfront, Partial Upfront, All Upfront*

Recommandé pour :

- Applications en production, avec une utilisation stable
- Bases de données avec un usage constant

Reserved Instances



Reserved Instances (RI)

Modèle avec engagement sur 1 ou 3 ans

Discount jusqu'à -72% par rapport au *On-Demand*

Engagement à utiliser une capacité EC2 (Type d'instance, région, OS)

Options de paiement : *No Upfront, Partial Upfront, All Upfront*

Réservation de capacité -> Il faut spécifier la zone (AZ) au moment d'acheter les RIs

Recommandé pour :

- Applications en production, avec une utilisation stable
- Bases de données avec un usage constant

Savings Plans vs Reserved Instances

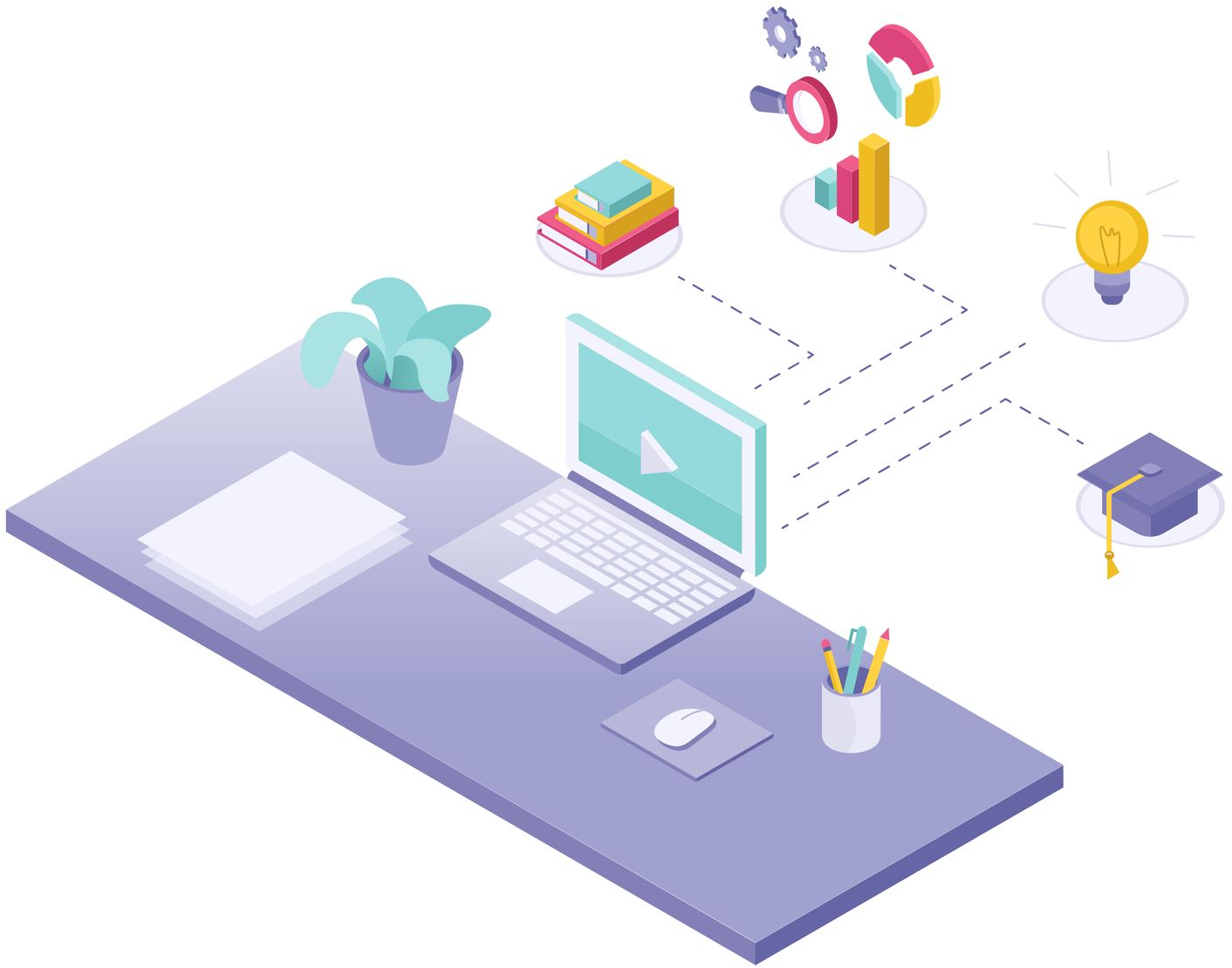
Savings Plans **Recommandé par AWS**

- Engagement sur 1 ou 3 ans
- Discount jusqu'à 72% par rapport à On-Demand
- Engagement sur une consommation : $ / heure
- Pas de réservation de capacité

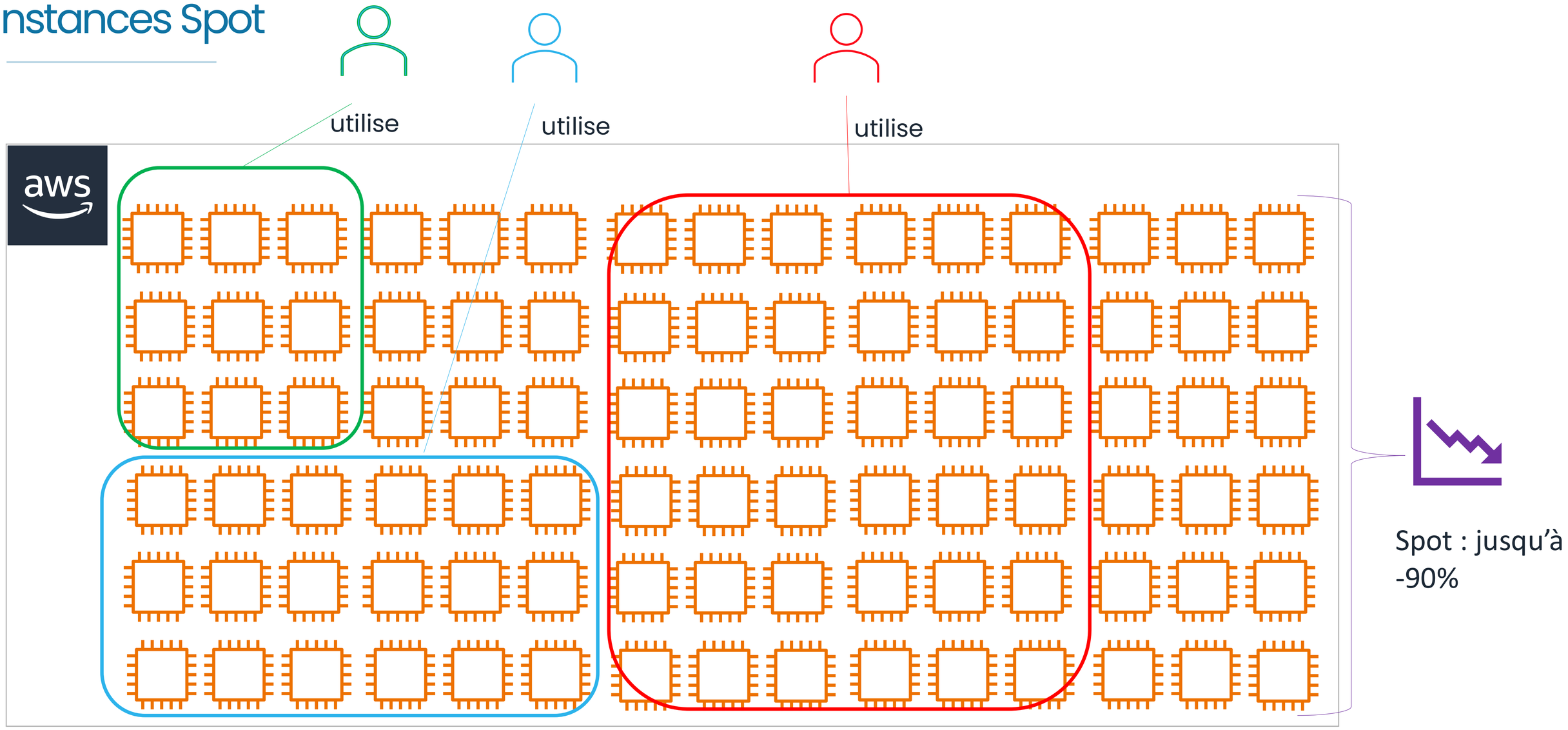
Reserved Instances

- Engagement sur 1 ou 3 ans
- Discount jusqu'à 72% par rapport à On-Demand
- Engagement à utiliser une capacité EC2 (*Type d'instance, plateforme, AZ,..*)
- Réservation de capacité (si AZ est spécifié)

Instances Spot



Instances Spot



Instance EC2

Instances Spot

Permettent de profiter d'instances EC2 non utilisées

Réduction allant jusqu'à 90% du prix On-Demand

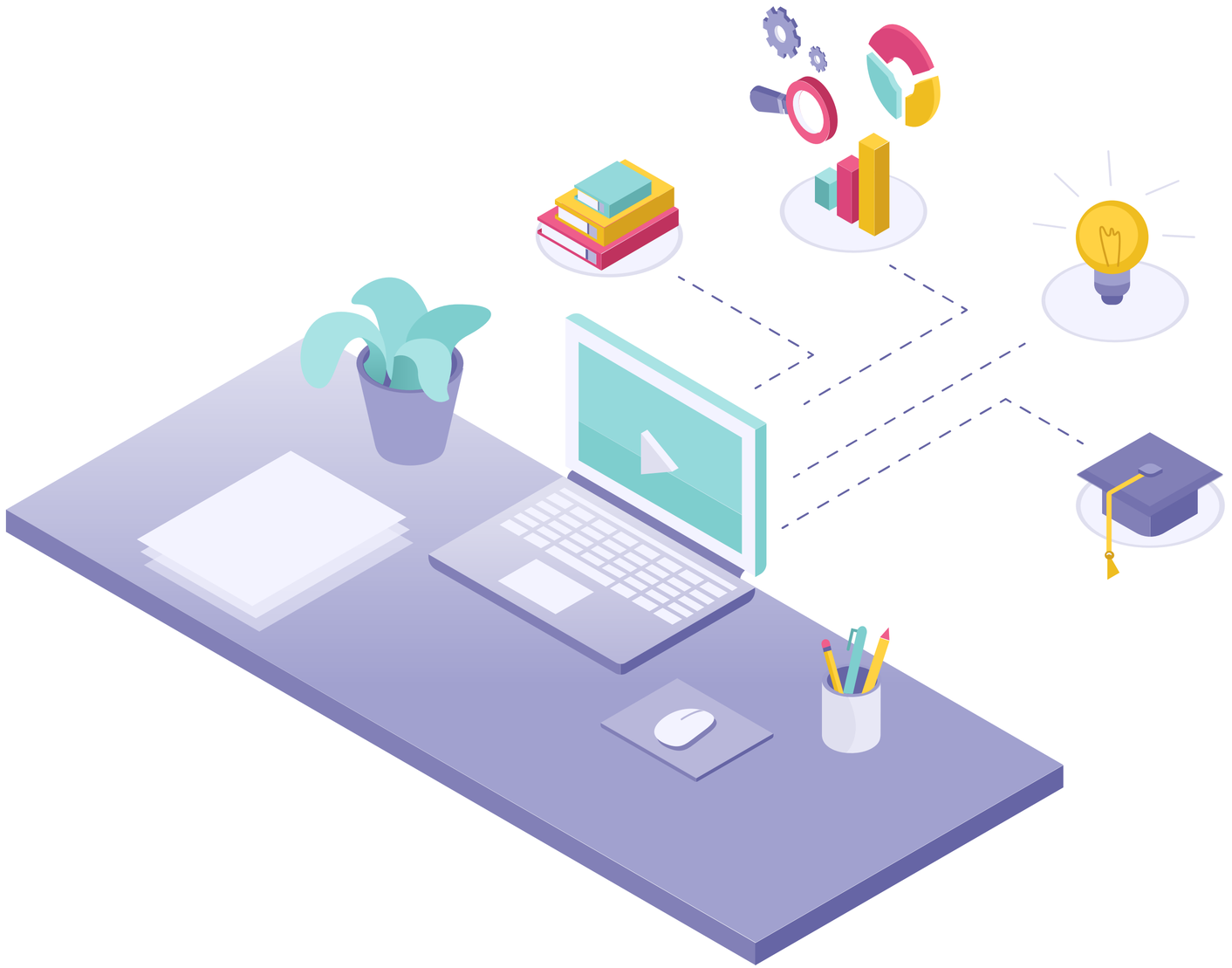
A tout moment, AWS peut reprendre les EC2 (2 minutes de notification)

Recommandé pour :

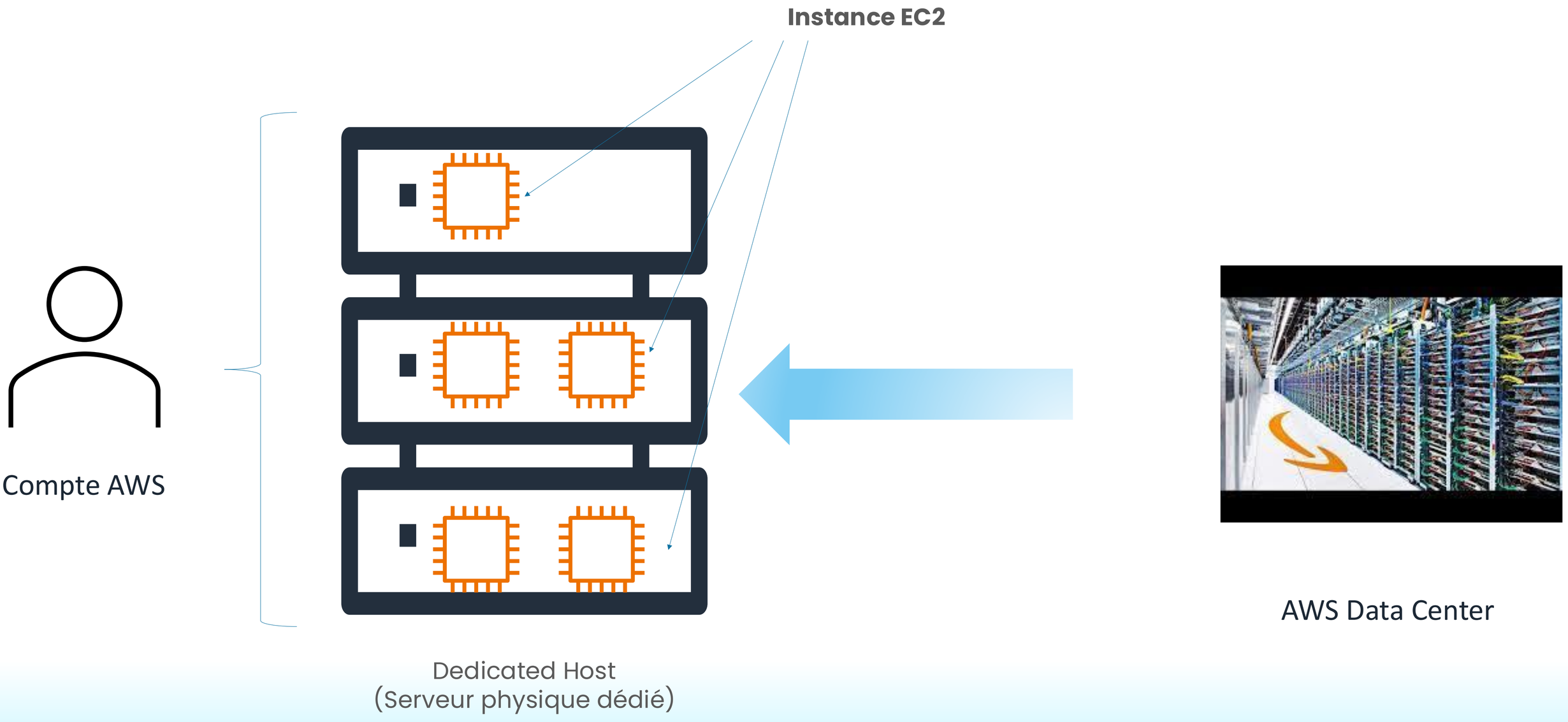
- les applications tolérantes aux interruptions / pannes
- Applications non critiques : Big Data, CI/CD, environnements de test…

Non recommandé pour les applications critiques

Dedicated Host



Dedicated Host



Dedicated Host

Serveur physique entièrement dédié à votre compte AWS

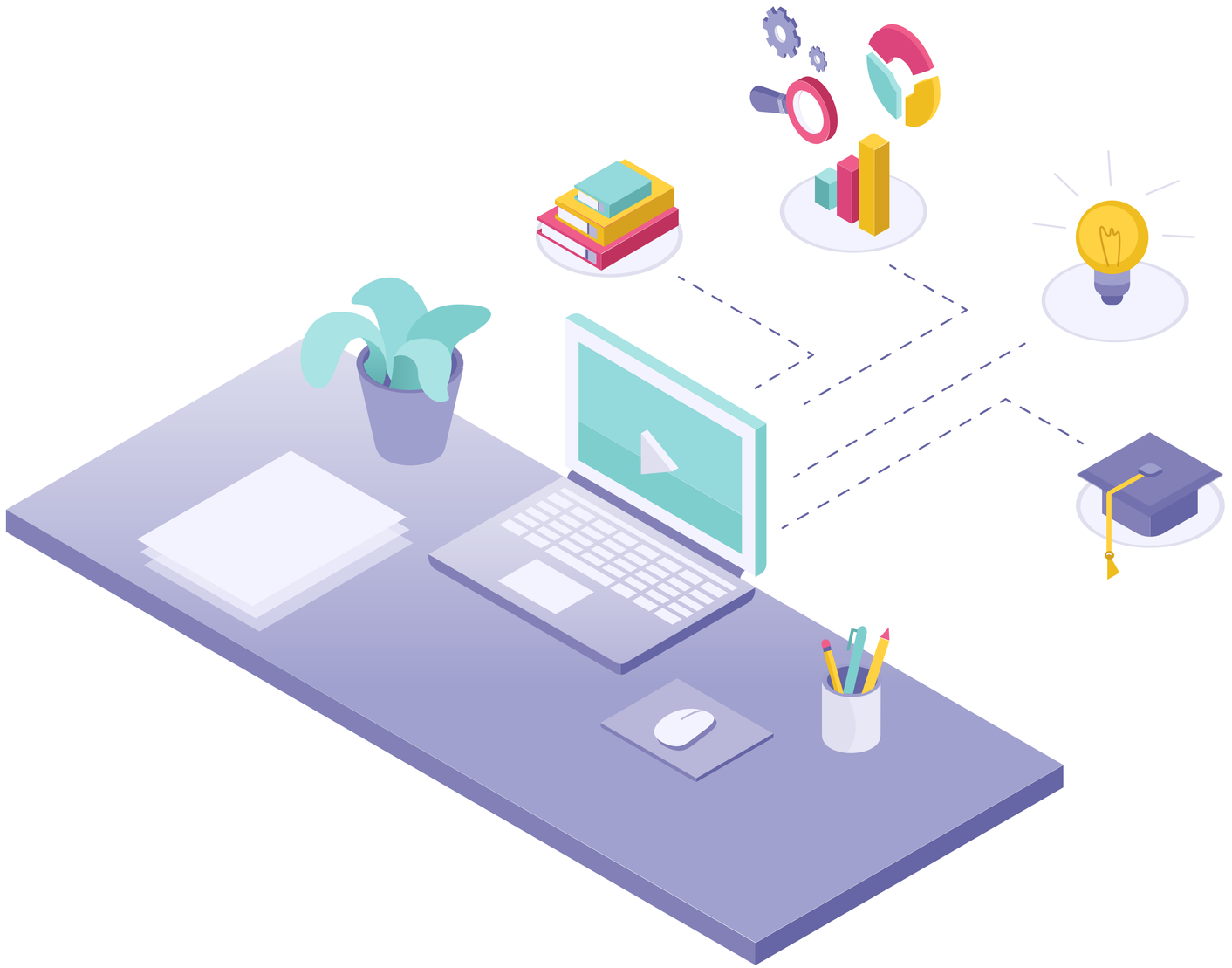
Contrôle total sur le placement des instances EC2 sur le serveur

Visibilité sur le nombre de sockets et de cœurs physiques

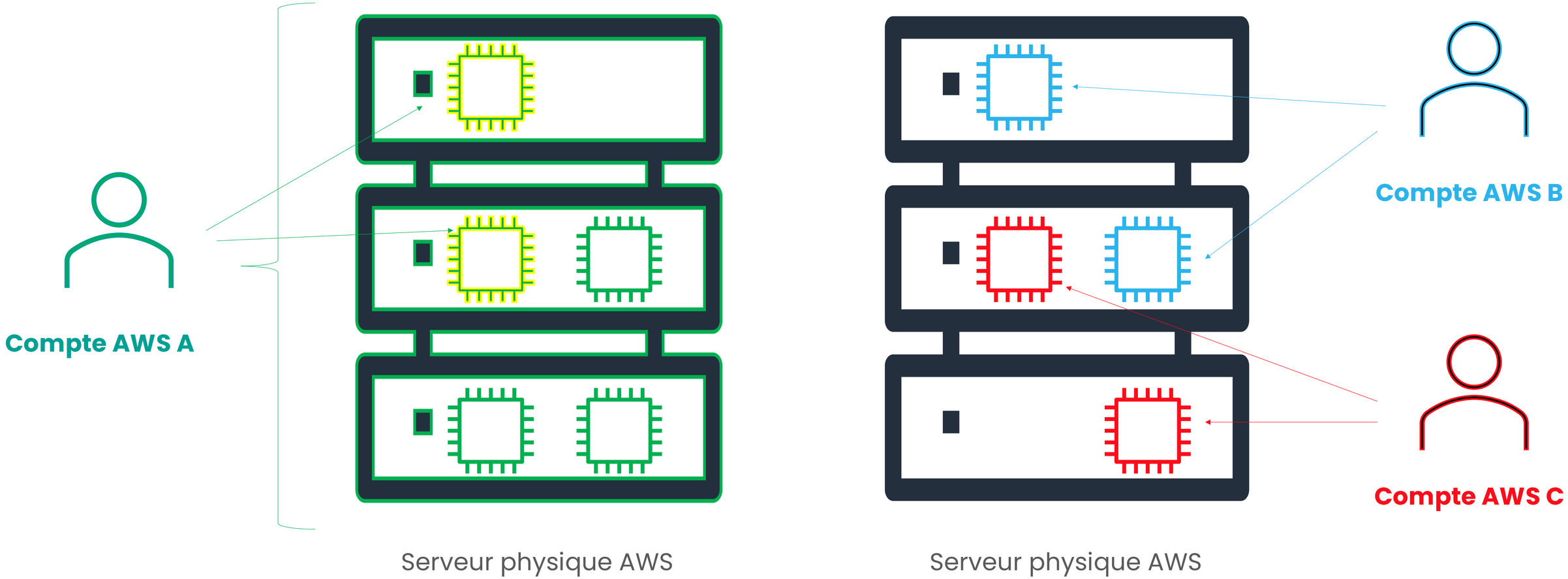
Recommandé pour :

- Utilisation de licences logicielles existantes par socket, core… (Windows Server, SQL Server, RHEL, …)
- (*Conformité*) Charges de travail qui requièrent des serveurs physiques dédiés

Dedicated Instances



Dedicated Instances



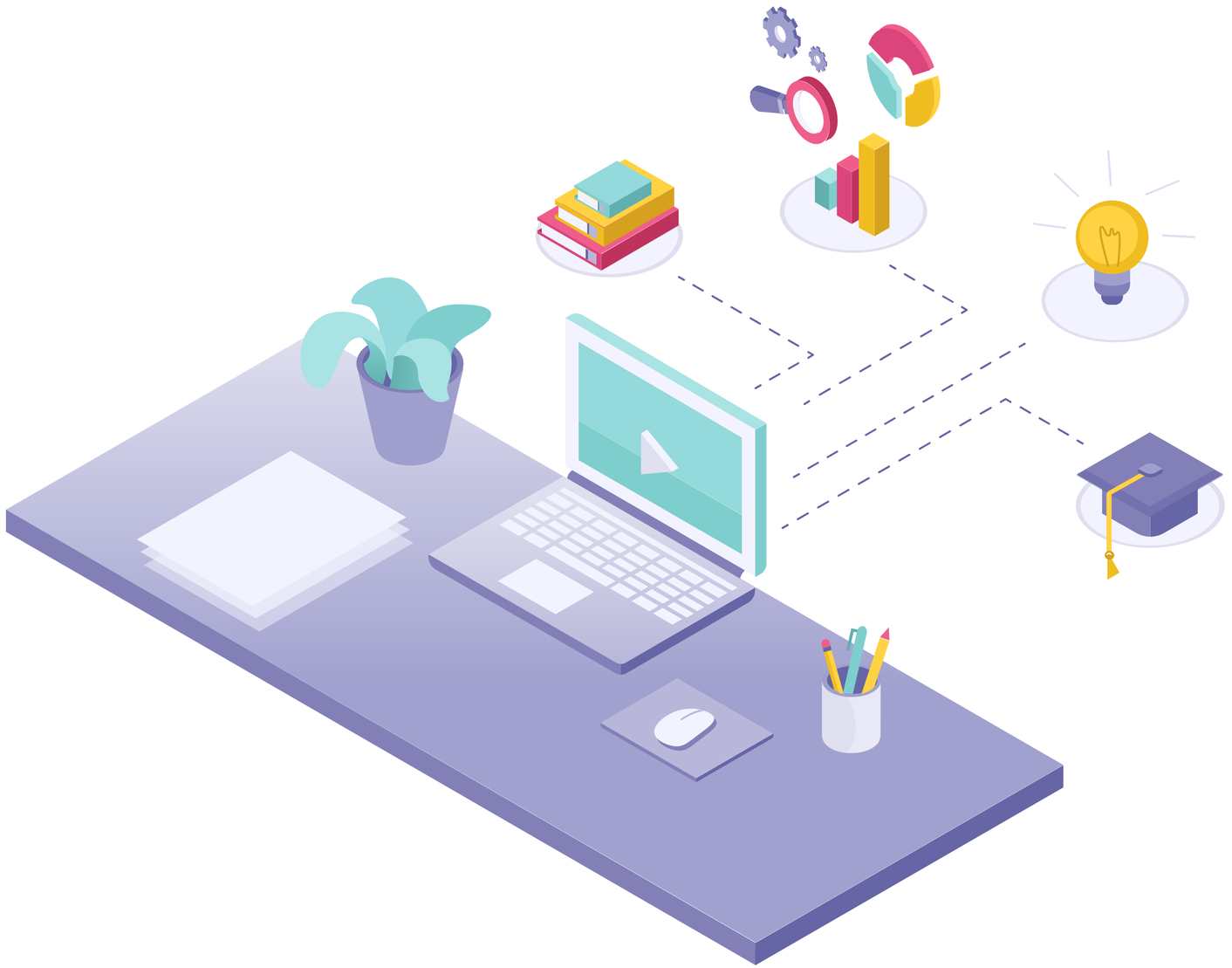
Dedicated Instances (Instances dédiées)

Les instances non dédiées s'exécutent sur du matériel physique partagé avec d'autres comptes AWS et d'autres clients.

Les instances dédiées s'exécutent sur du matériel physique dédié à **un seul compte AWS**.

	Dedicated Host	Dedicated Instance	Instance par défaut
Serveur physique dédié	Contrôle + visibilité totale sur tout le serveur physique	Le serveur physique est dédié à votre compte.	Le serveur physique est partagé avec d'autres comptes / clients.
Facturation	Facturation par hôte	Facturation par instance	Facturation par instance

Mise à l’échelle



Mise à l'échelle

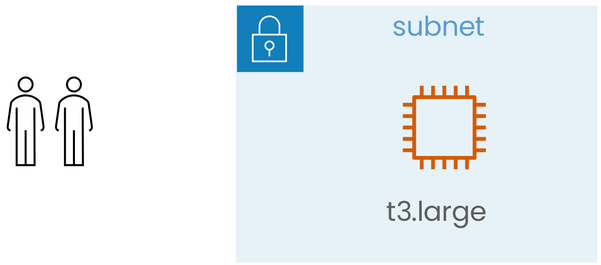
En anglais : « *Scaling* »

Définition -> *« Capacité d'un système informatique à gérer une augmentation de la charge de travail»*

2 types :

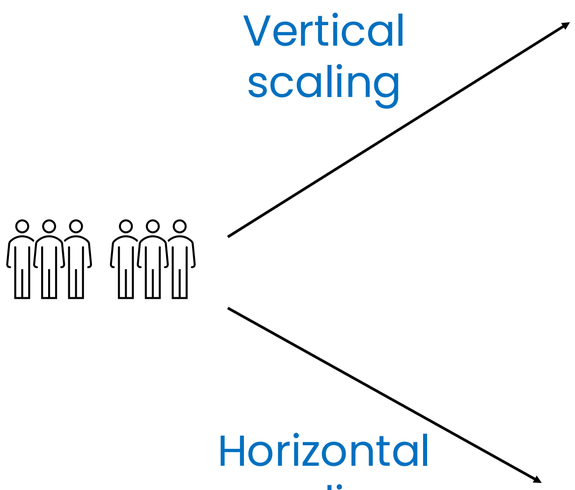
- -> Mise à l'échelle **verticale** -> augmentation de ses ressources
- -> Mise à l'échelle **horizontale ->** ajout de ressources supplémentaires

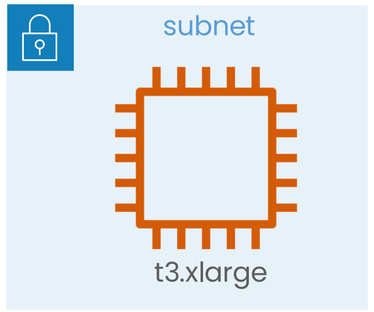
Exemples de mise à l'échelle



2 vCPU

8 GiB mémoire

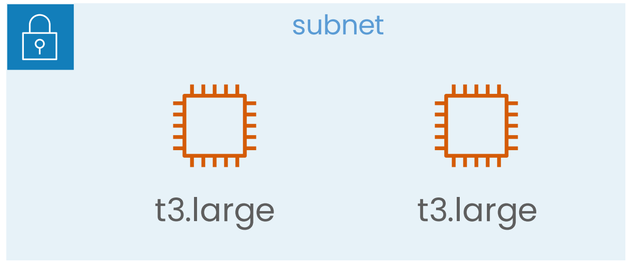




SPOF (Single Point of Failure)

4 vCPU

16 GiB mémoire



2 vCPU

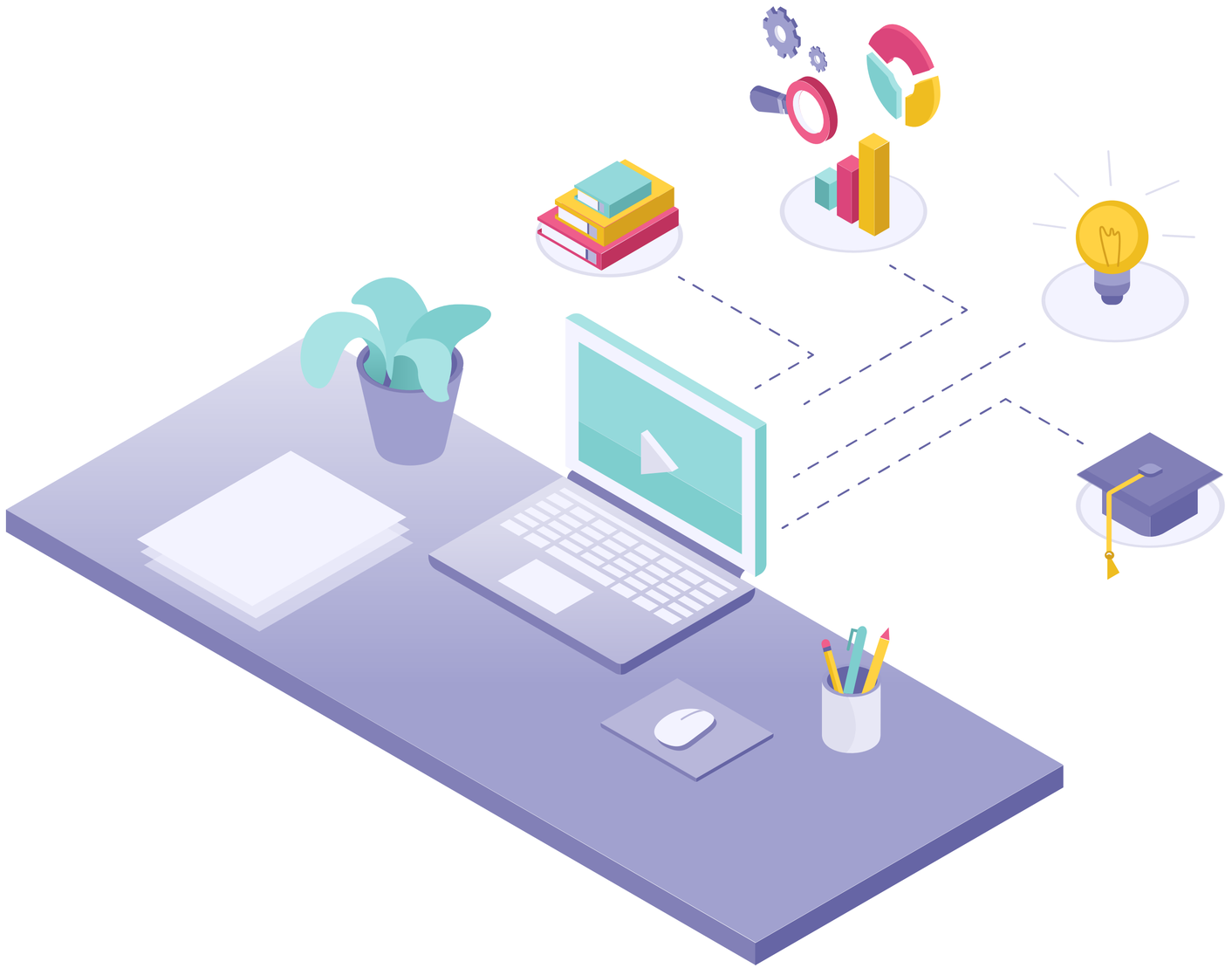
8 GiB mémoire

+

2 vCPU

8 GiB mémoire

EC2 Auto Scaling



EC2 Auto Scaling



Permet la mise à l'échelle **horizontale** (Elasticité) des instances EC2

Ajoute/supprime automatiquement des instances EC2 en fonction de la charge

Cas d'usage : Pic de trafic, Baisse de l'activité (soirées, week-ends,...)

Souvent couplé à un Load Balancer pour la répartition du trafic

Cas d'usage EC2 Auto Scaling

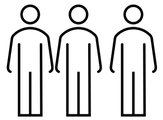
Ajuster automatiquement à la hausse ou à la baisse votre capacité Amazon EC2



Maintenir un **nombre fixe** d'instances EC2

Détecter et **remplacer** les instances EC2 en mauvais état

Gestion de la capacité

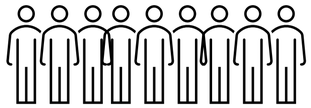


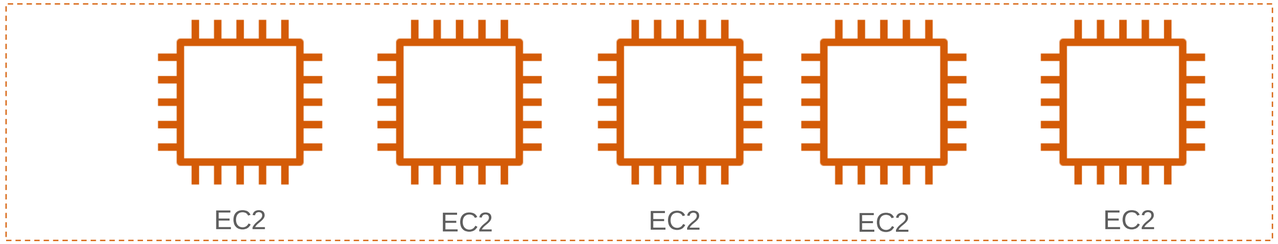


Auto Scaling group

Capacité souhaitée

Capacité initiale du groupe à sa création



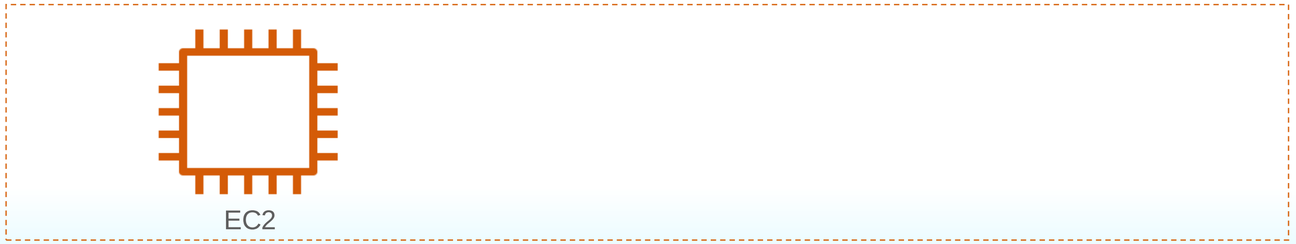


Auto Scaling group

Capacité maximale

Le nombre max d'instances EC2



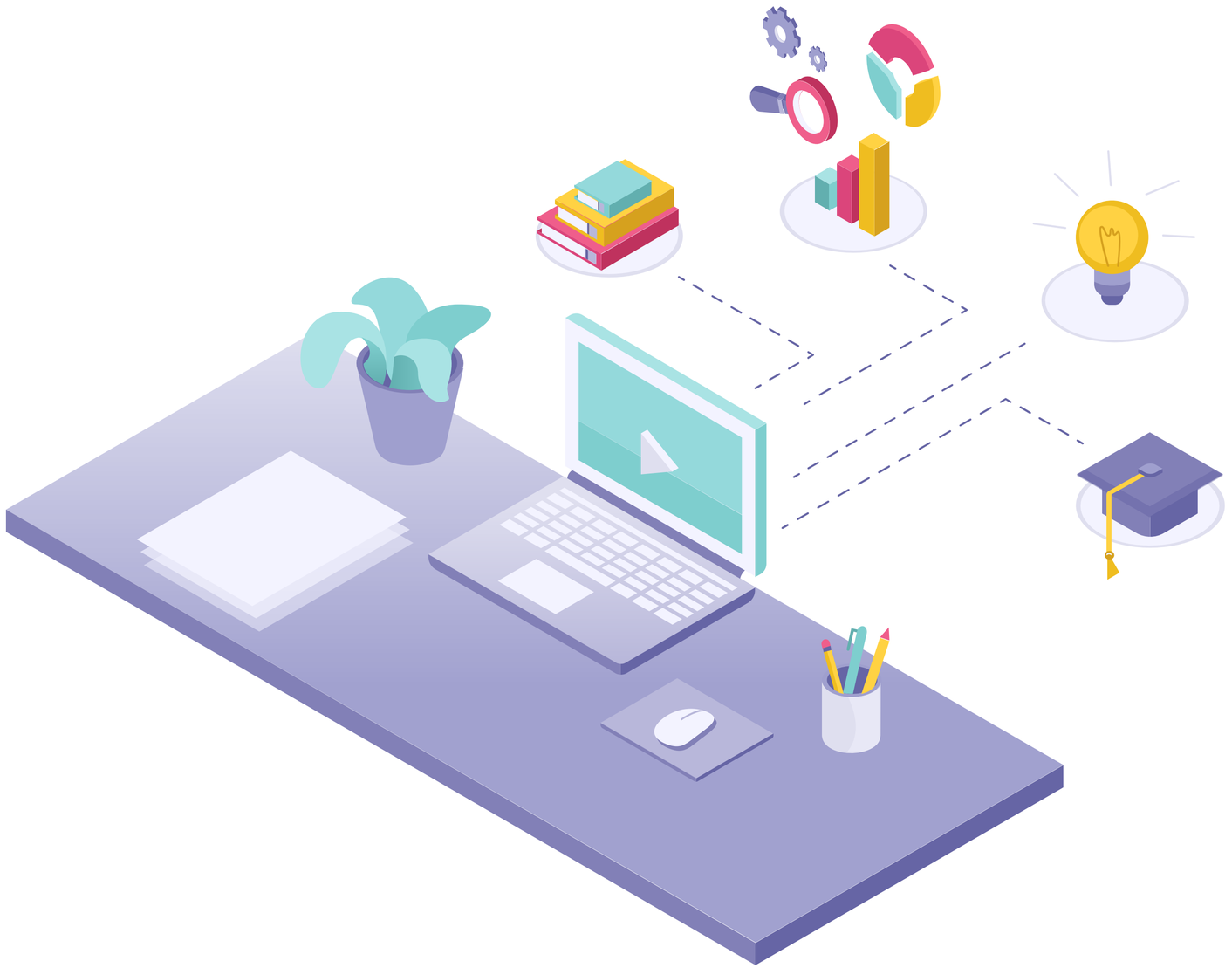


Auto Scaling group

Capacité minimale

Le nombre minimum d'instances EC2

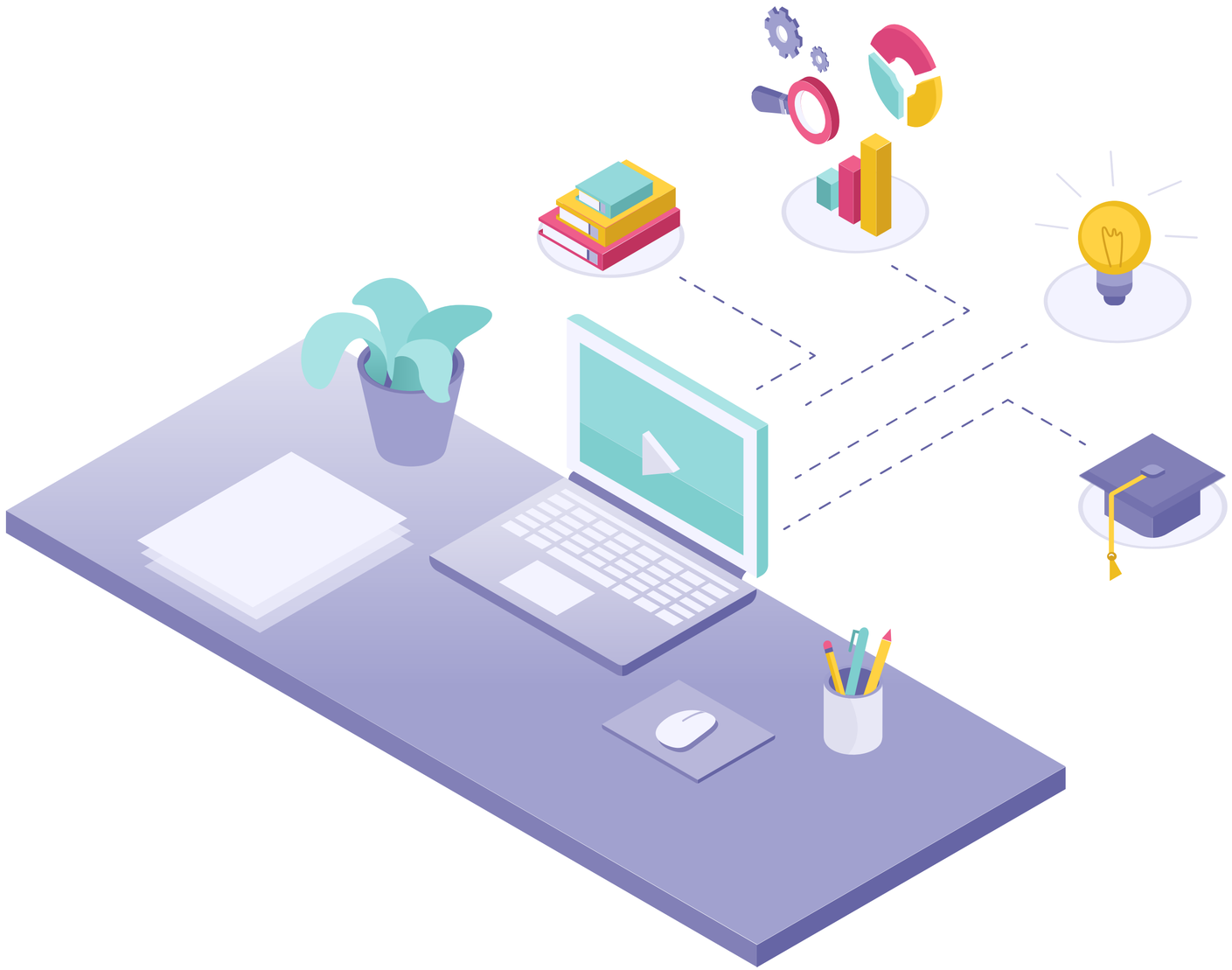
Les stratégies EC2 Auto Scaling



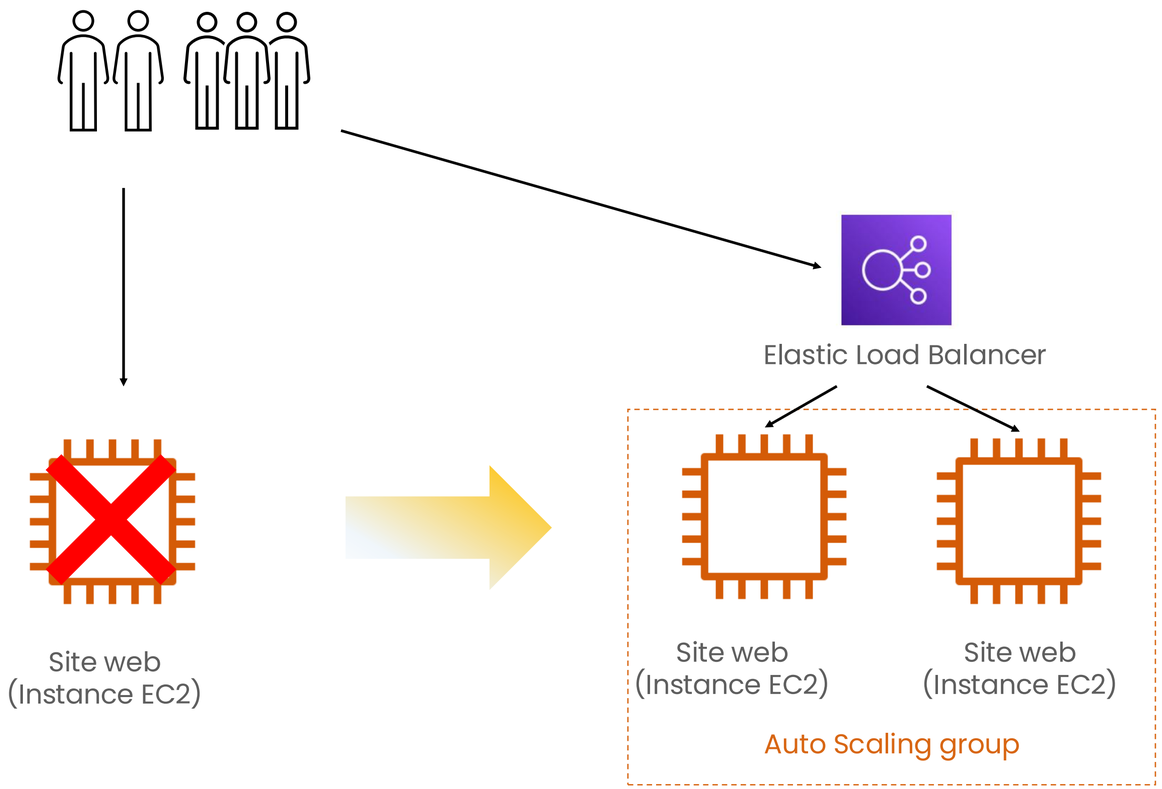
Les stratégies EC2 Auto Scaling

- **Dynamique**
  - Basé sur des règles que vous définissez
  - Exemple
    - *Rajouter 2 instances EC2 si le CPU > 70%*
    - *Terminer 1 instance EC2 si le trafic réseau < 20% pendant 10 mns*
- **Prédictif**
  - Gestion de la capacité basée sur du Machine learning
  - Exemple
    - *Auto Scaling démarre des EC2 en prévision de la période des soldes*

Elastic Load Balancer



Elastic Load Balancer



Problèmes

- SPOF
- Mise à l'échelle (*scalability*)

Elastic Load Balancer



Fournit des ***Load Balancers*** (équilibreurs de charge) entièrement gérés

Répartit automatiquement le trafic entrant (requêtes) sur plusieurs cibles (généralement des EC2)

Solutions similaires : HAProxy, serveur Apache (mod_proxy), F5 BIG-IP

Elastic Load Balancer : les différents types

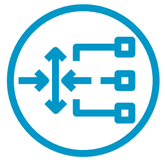
Application Load Balancer	Network Load Balancer	Gateway Load Balancer	Classic Load Balancer
HTTP / HTTPs (couche 7)	TCP / UDP (Couche 4)	Flux IP (Couche 3)	HTTP / HTTPS / TCP
Idéal pour les sites web	Idéal pour la très haute performance	Permet de router le trafic vers des appliances	Déprécié PAR AWS



ALB



NLB

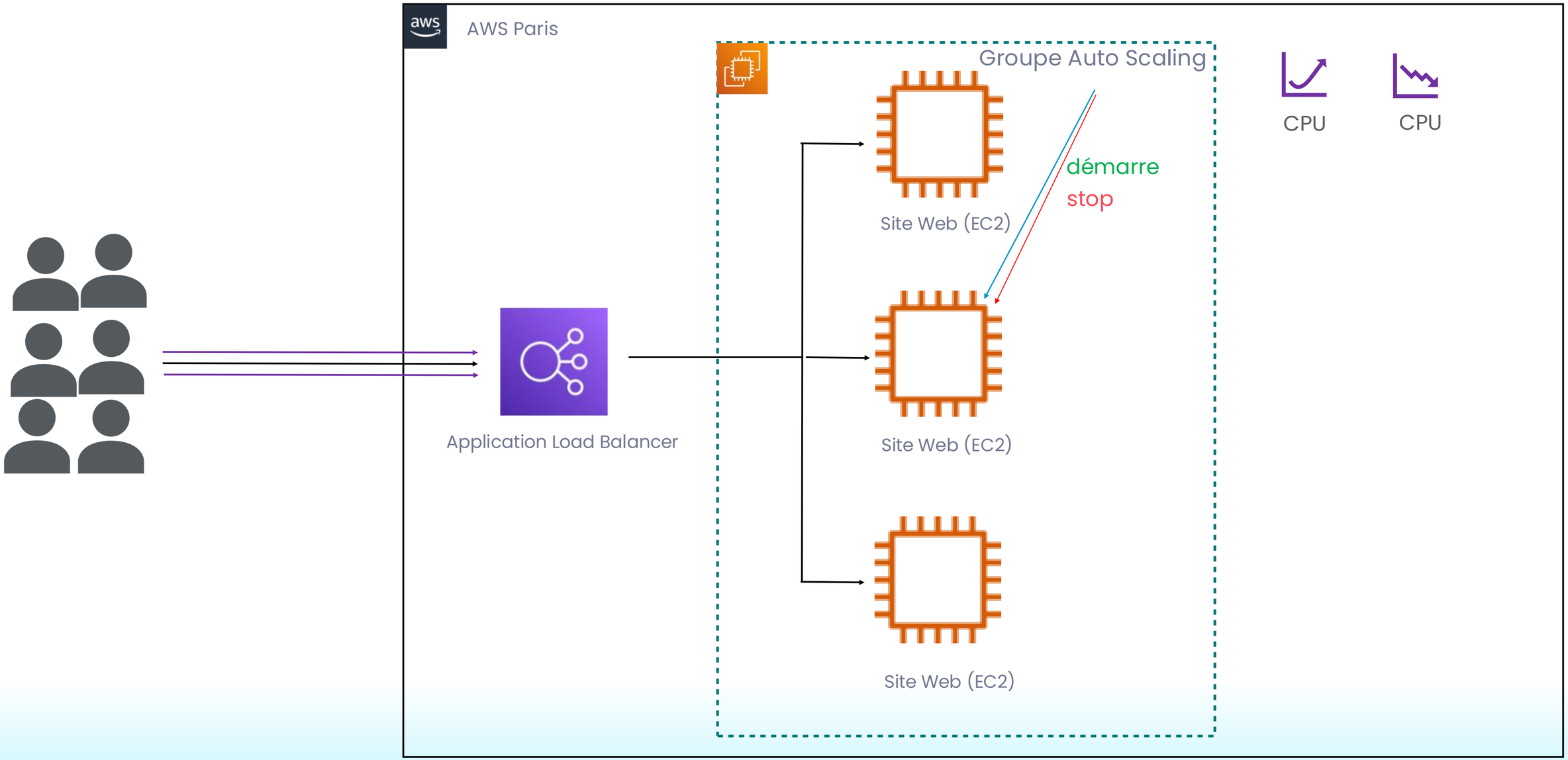


GLB

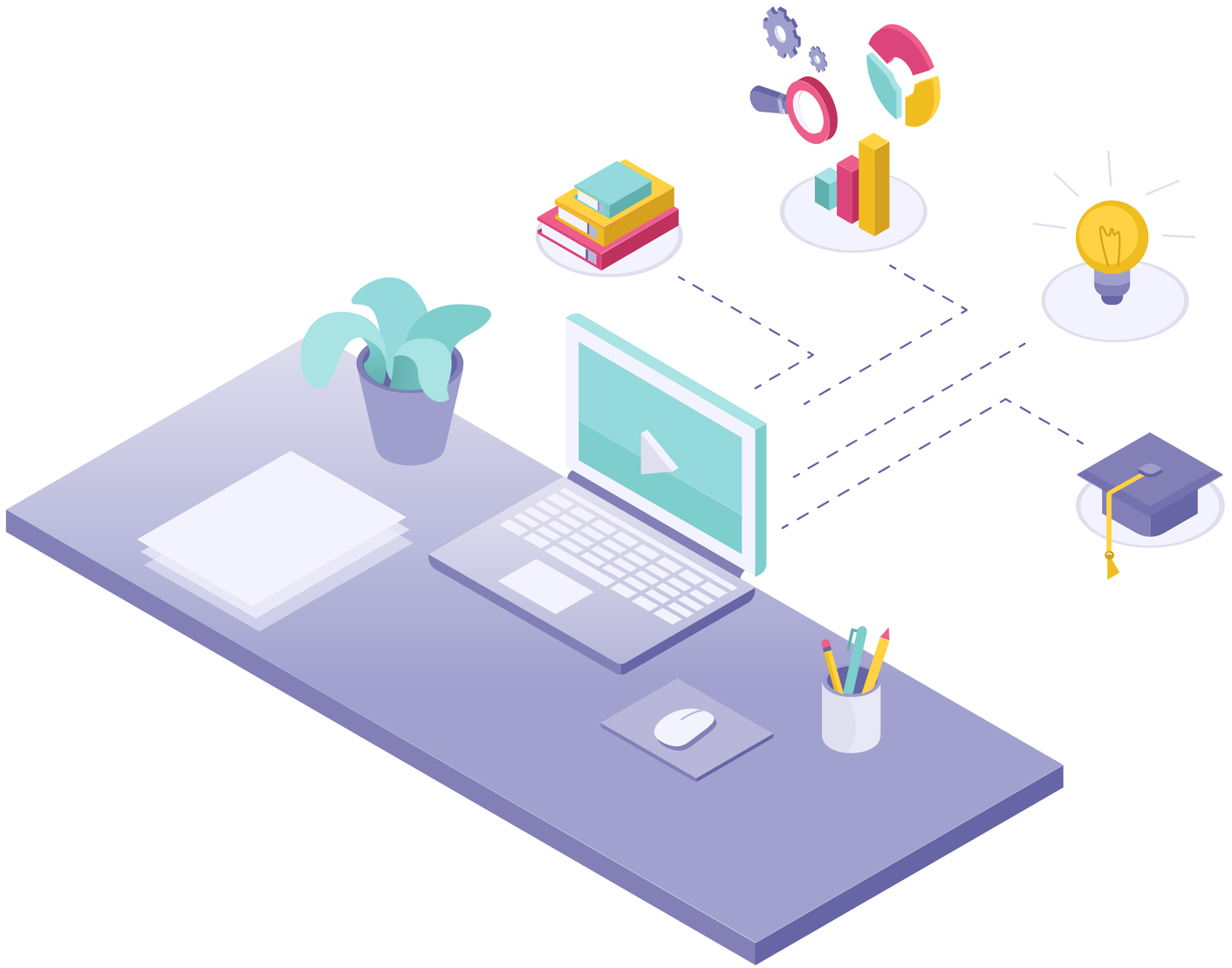


CLB

Exemple avec ALB & ASG



Architecture Multi-AZ



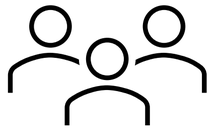
Architecture Multi-AZ

Multi-AZ → Haute Disponibilité

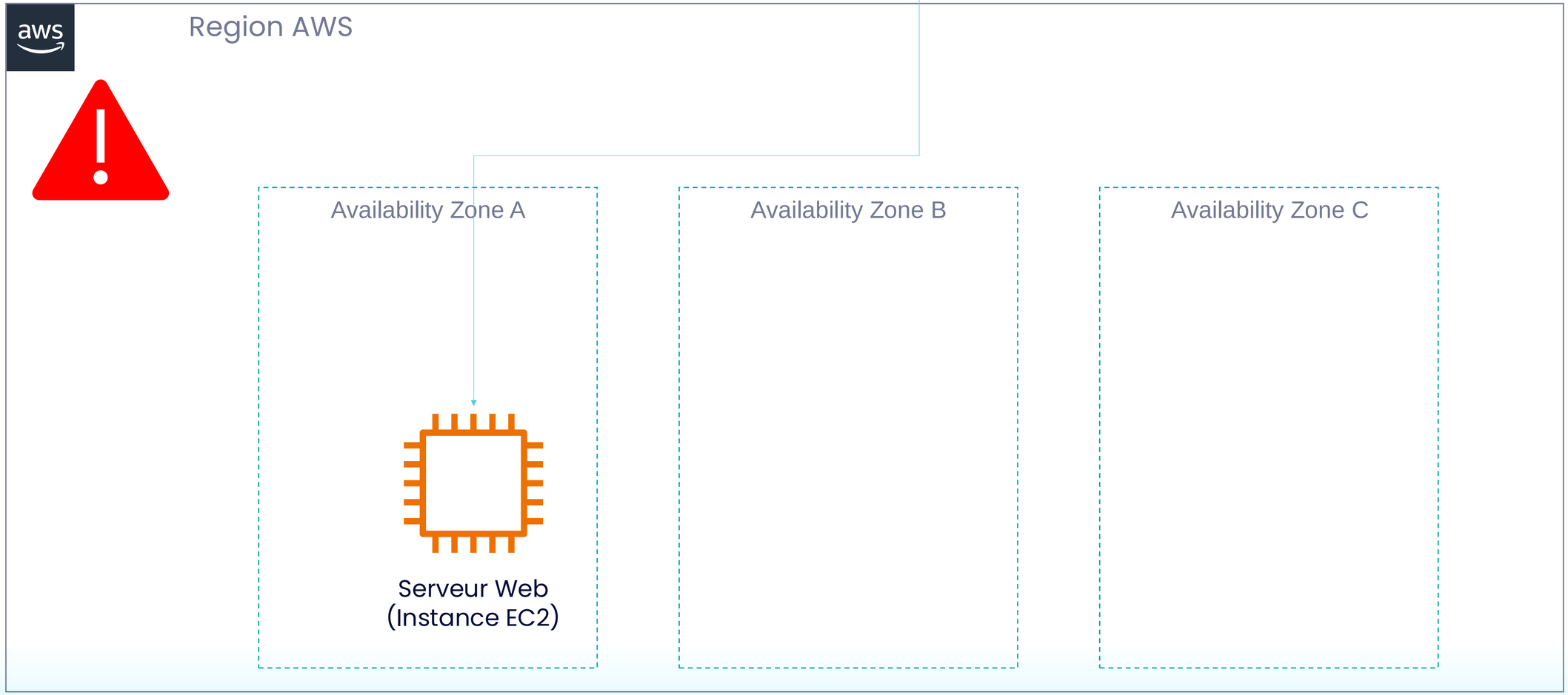
Redondance

« La haute disponibilité est la capacité pour un système informatique à être accessible et fiable presque 100 % du temps, afin de réduire, voire éliminer, les temps d'arrêt »

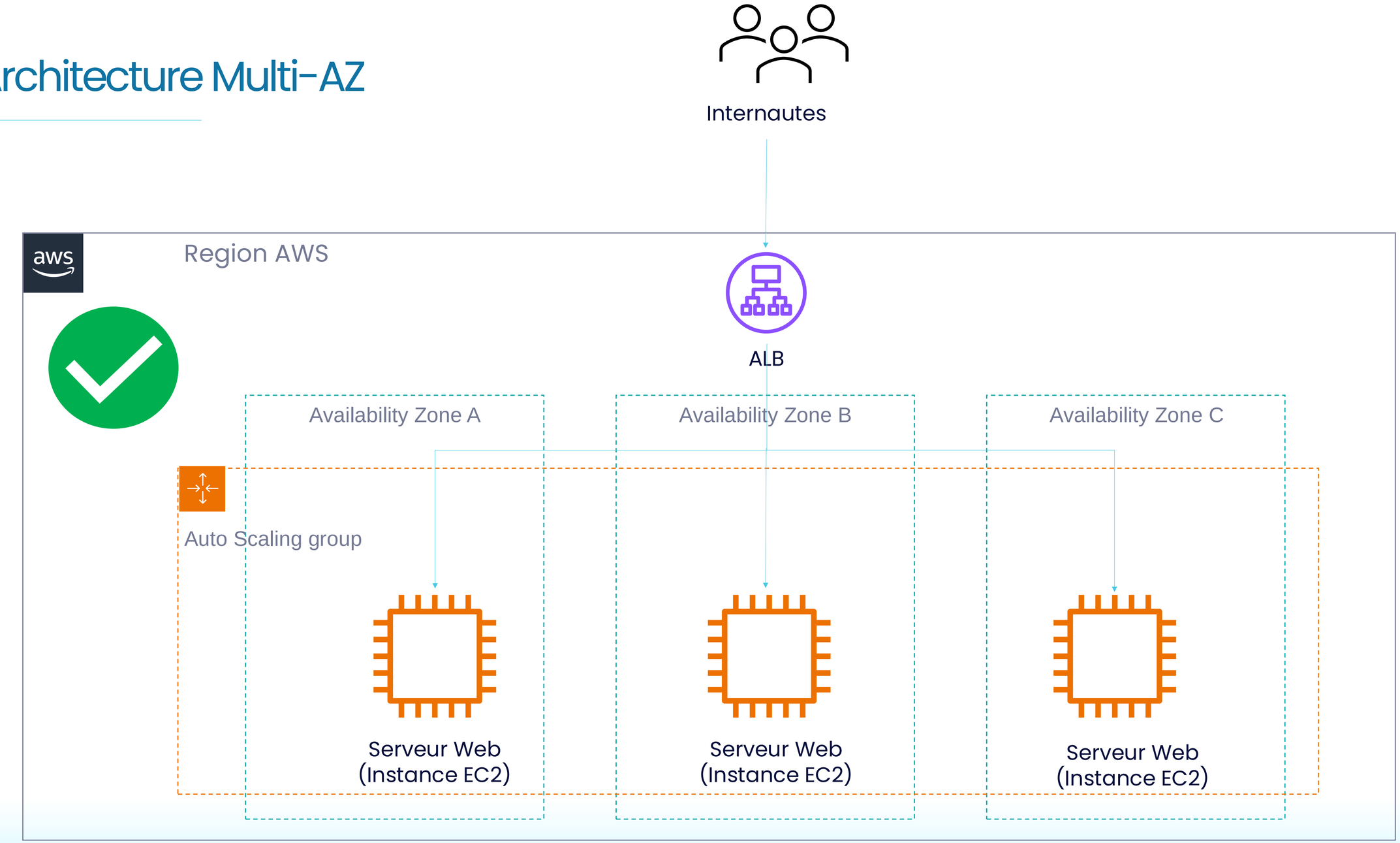
Architecture Multi-AZ

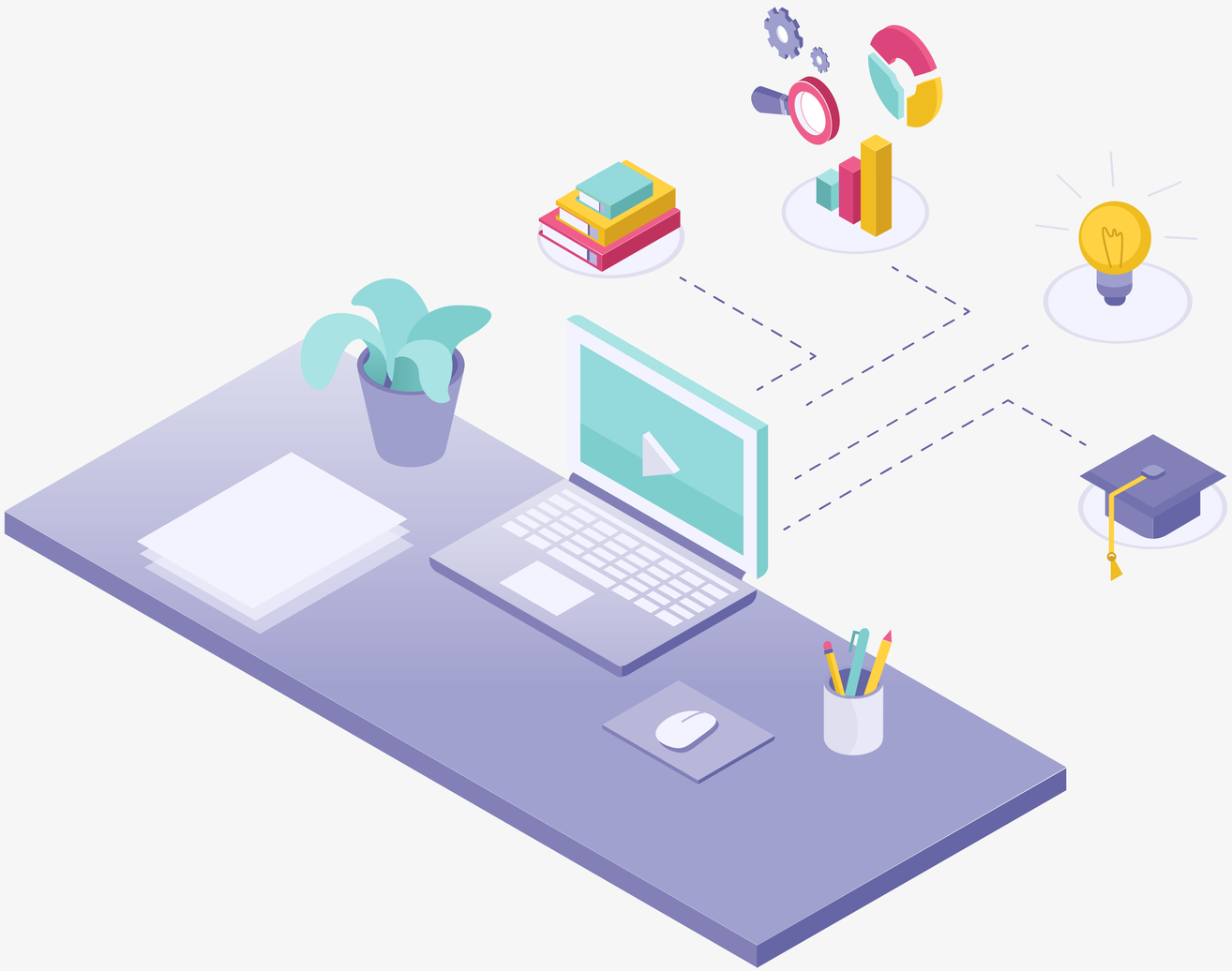


Internautes



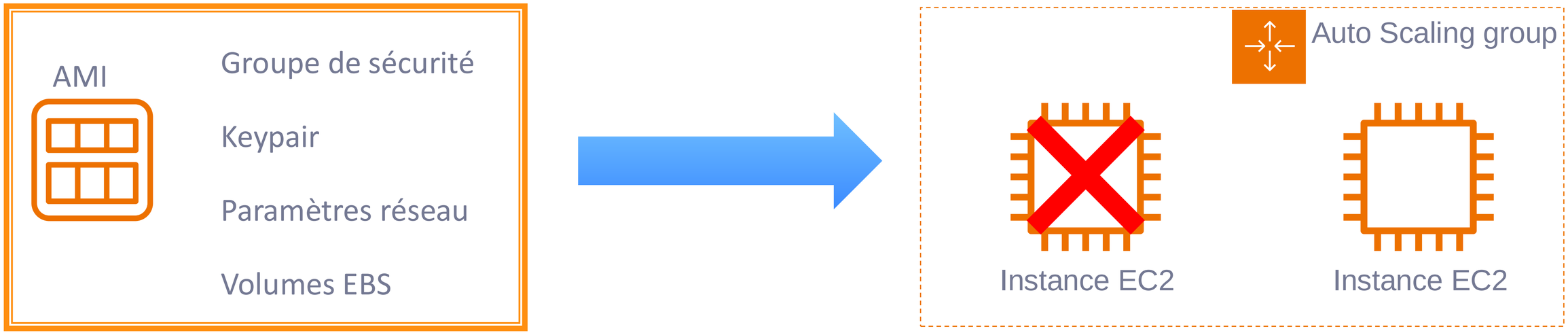
Architecture Multi-AZ





FIN DU MODULE

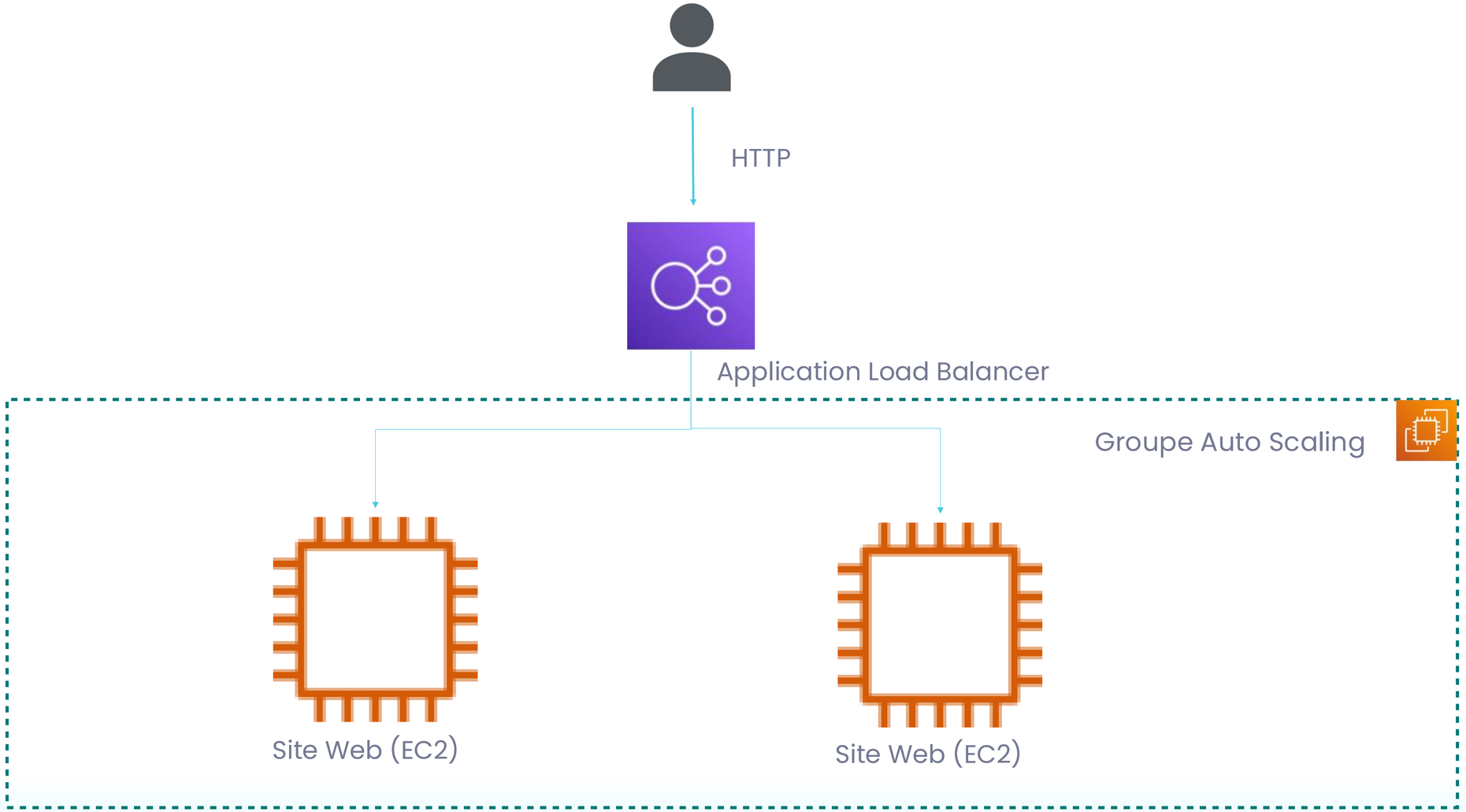
Lab Créer votre 1er EC2 Auto Scaling Groupe



1 - Launch Template

2 – Auto Scaling Group

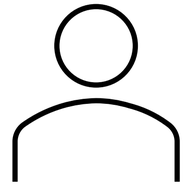
Lab Auto Scaling Group & Application Load Balancer



Lab Auto Scaling Group & Application Load Balancer

1. Créer un Launch Template
2. Créer un Auto Scaling Group + ALB
3. Tester la répartition de charge

Lab EC2 User Data



Internaute

http

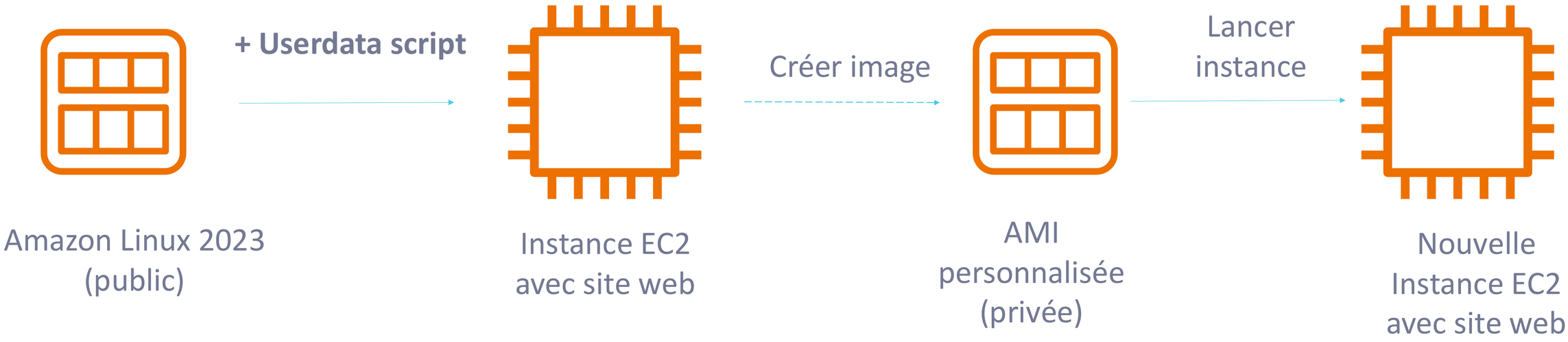
```
#!/bin/bash
yum update -y
yum install -y httpd.x86_64
systemctl start httpd.service
systemctl enable httpd.service
echo '<html><head><title>Success!</title></head><body><iframe width="560" height="315"
src="https://www.youtube.com/embed/7T-ungr_t80?si=gskPmA7AMHdRgyUf"
frameborder="0" allowfullscreen></iframe></body></html>' > /var/www/html/index.html
```

Au démarrage

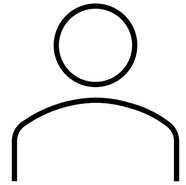


Instance EC2 Linux

Lab AMI Personnalisée

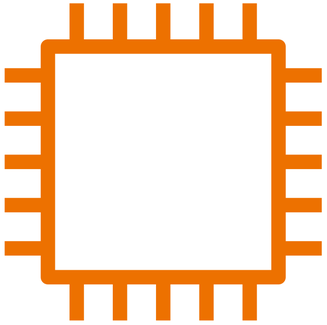


Lab Groupe de sécurité



http

Groupe de sécurité



Instance EC2
avec site web

Lab Changer type d'instance

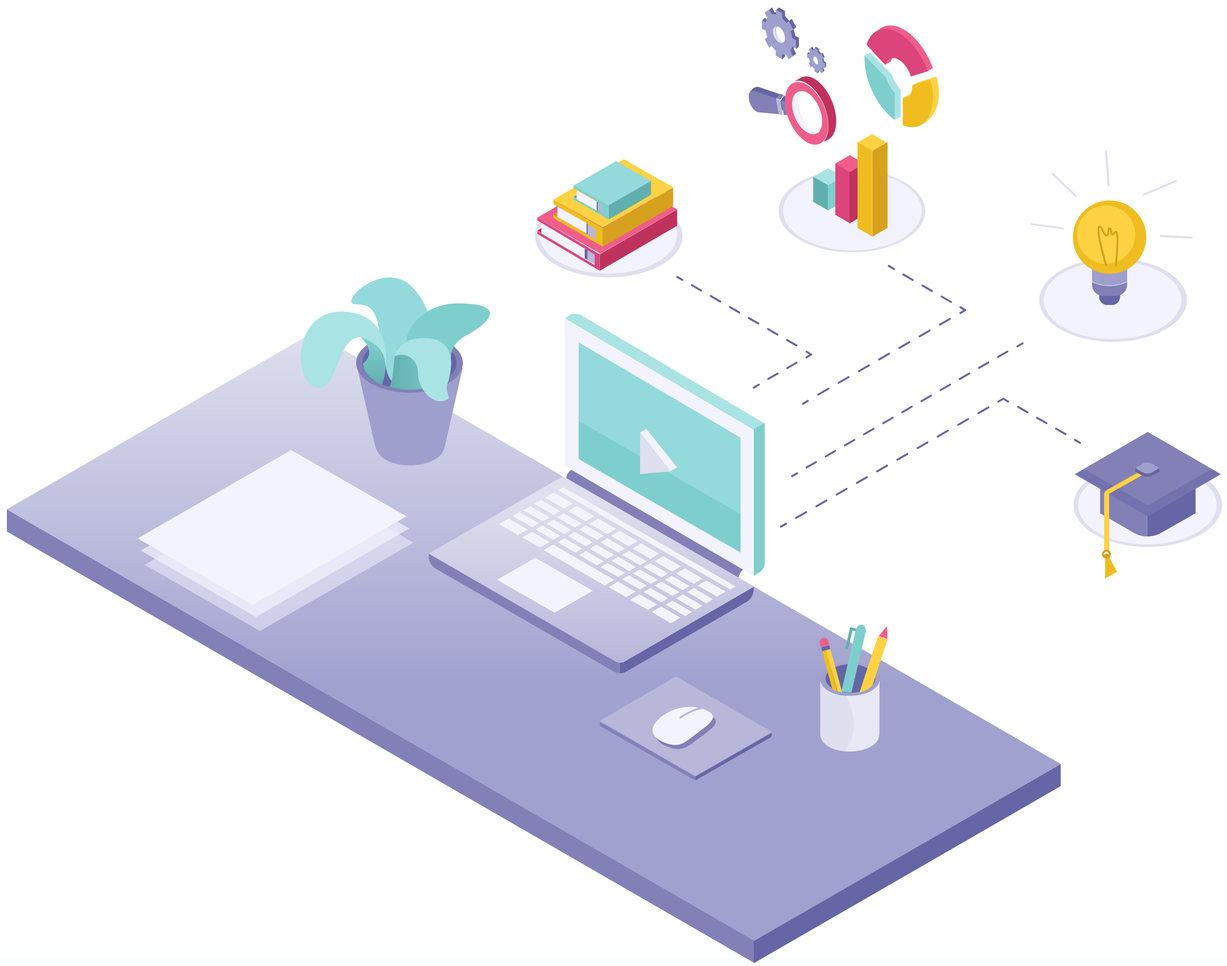


Lab Démarrer EC2 avec AWS CLI

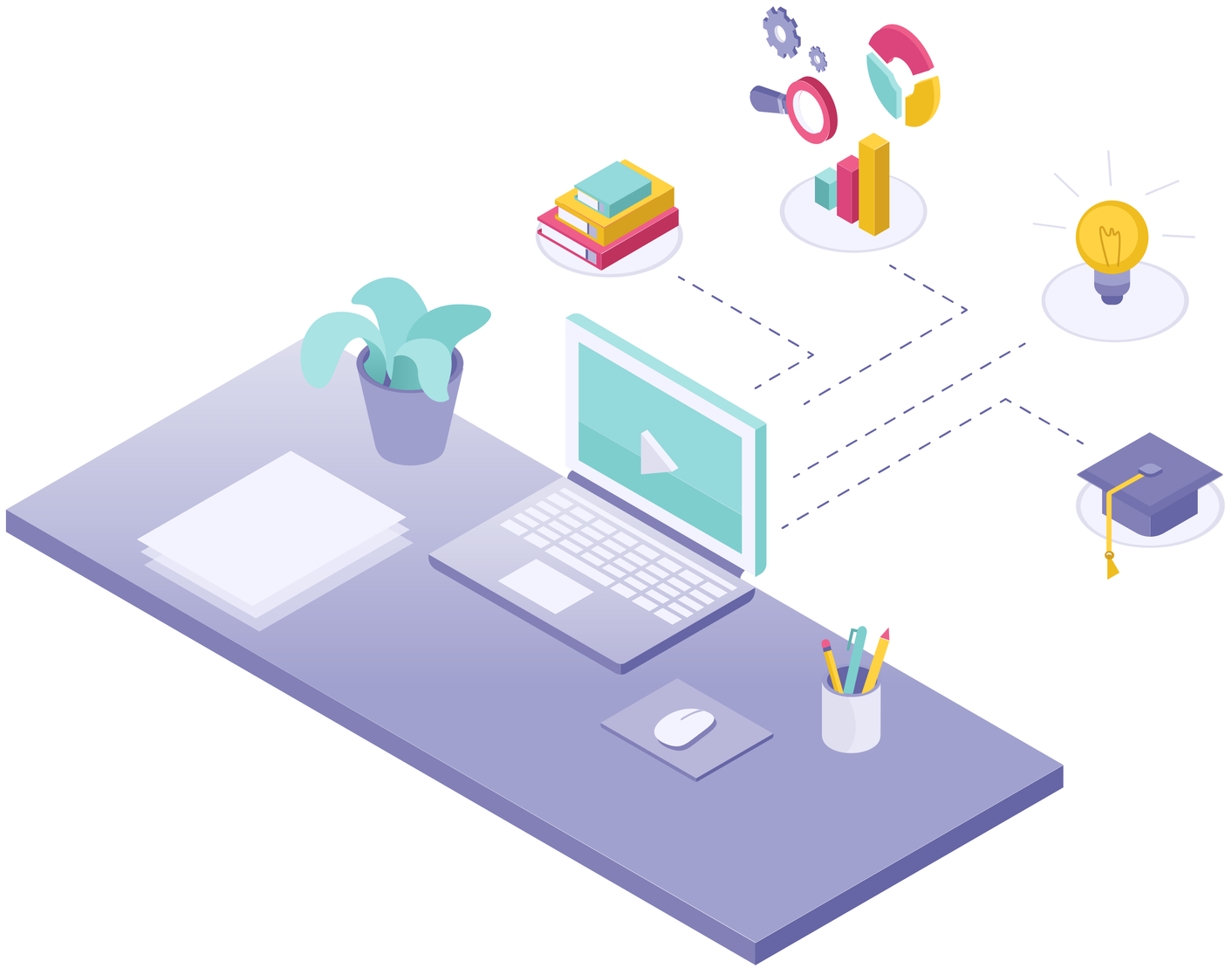
aws help	Pour afficher la documentation
aws ec2 run-instances	Pour démarrer une instance EC2
aws ec2 describe-instances	Pour lister les instances EC2
aws ec2 terminate-instances	Pour résilier une instance EC2

Module 4 : Autres services de calcul

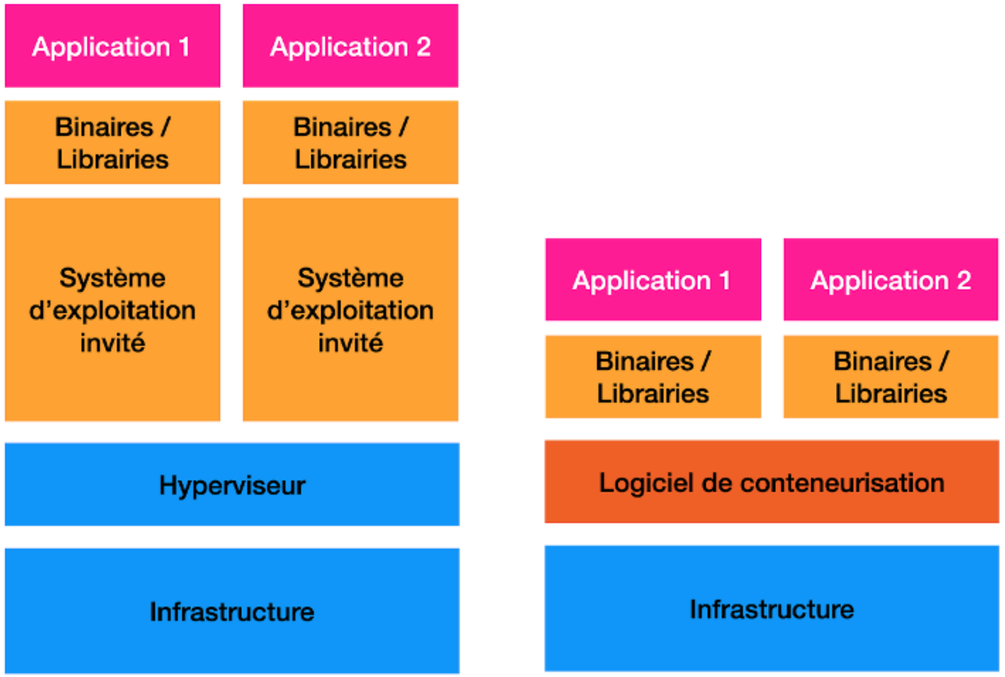
Calcul pour n'importe quelle charge de travail : instances, conteneurs et serverless

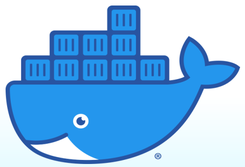


Conteneurs 101



Conteneurs 101





Docker

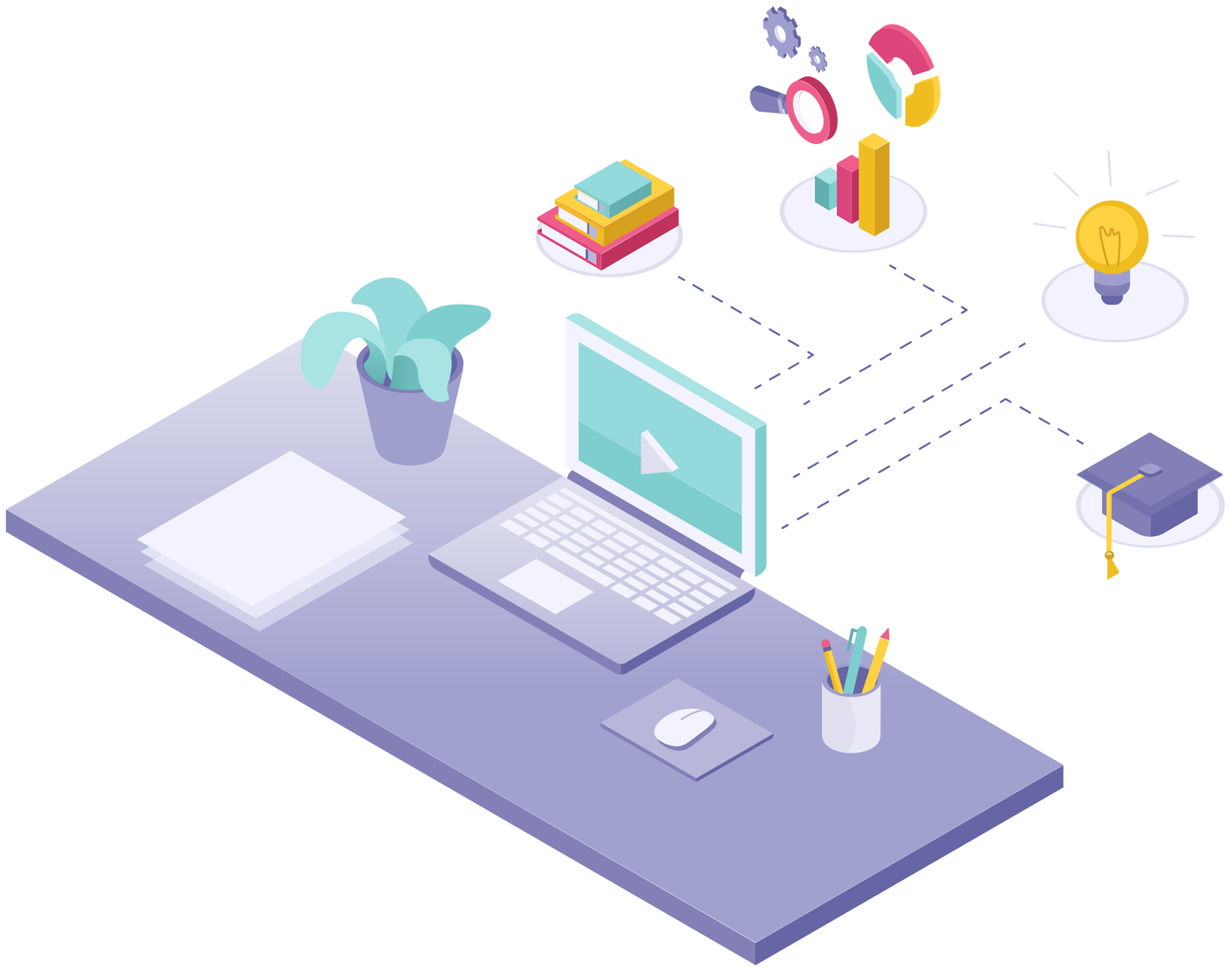
Les conteneurs

- *Packagent* les applications avec leurs dépendances
- Sont beaucoup **plus rapides, plus légers, plus simples à utiliser**

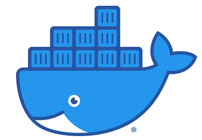
Avantages

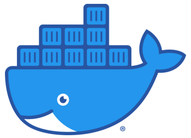
- Mise à l'échelle
- Portabilité des applications
- Faciliter les processus de développements agiles
- Améliorez l'efficacité informatique

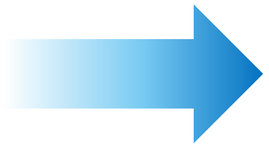
Conteneurs sur AWS

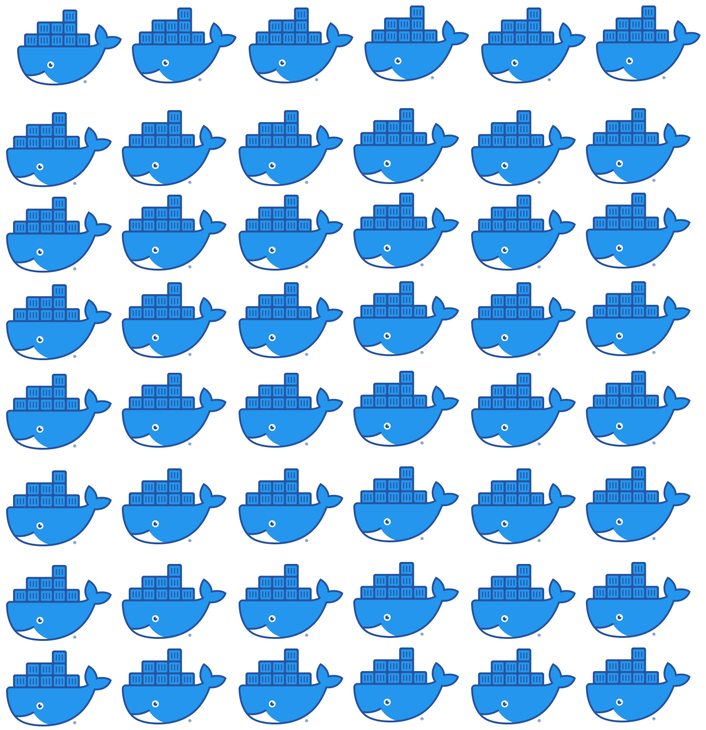


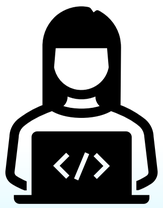
Conteneurs sur AWS











Ingénieure



Amazon ECS



Amazon EKS

Services d’orchestration de conteneurs

Conteneurs sur AWS



Amazon ECS



Amazon EKS

Services d’orchestration de conteneurs



AWS Fargate

Gestion de l’infrastructure



Amazon ECR

Registre de conteneurs

Amazon Elastic Container Service (ECS)



Service d’orchestration de conteneurs Docker entièrement géré

Permet de **lancer des conteneurs à grande échelle** sur le cloud AWS

S’intègre parfaitement aux autres services AWS (ELB, Fargate, Auto Scaling, AWS IAM…)

ECS peut s’appuyer sur **EC2** ou **Fargate** pour l’**infrastructure**

Amazon Elastic Kubernetes Service (EKS)

Service géré d'orchestration de conteneurs



Permet de déployer facilement des **clusters Kubernetes** sur le cloud AWS



Kubernetes = Projet Open Source + Forte communauté

AWS Fargate



Serverless pour les conteneurs sur AWS

Fargate permet d'exécuter des conteneurs **sans gérer de serveurs** (EC2)

Fargate est compatible avec **EKS et ECS**

Vous définissez la capacité souhaitée (CPU / RAM) et ***Fargate*** *s'occupe de l'infrastructure pour vos conteneurs*

Amazon Elastic Container Registry (ECR)



Registre de conteneurs entièrement géré sur le cloud AWS

Permet de stocker et partager des **images de conteneurs**

Alternative à Docker Hub

Intégration native avec Amazon ECS et Amazon EKS

Conteneurs sur AWS : En résumé

Registre de conteneurs

Amazon ECR

Orchestration de conteneurs

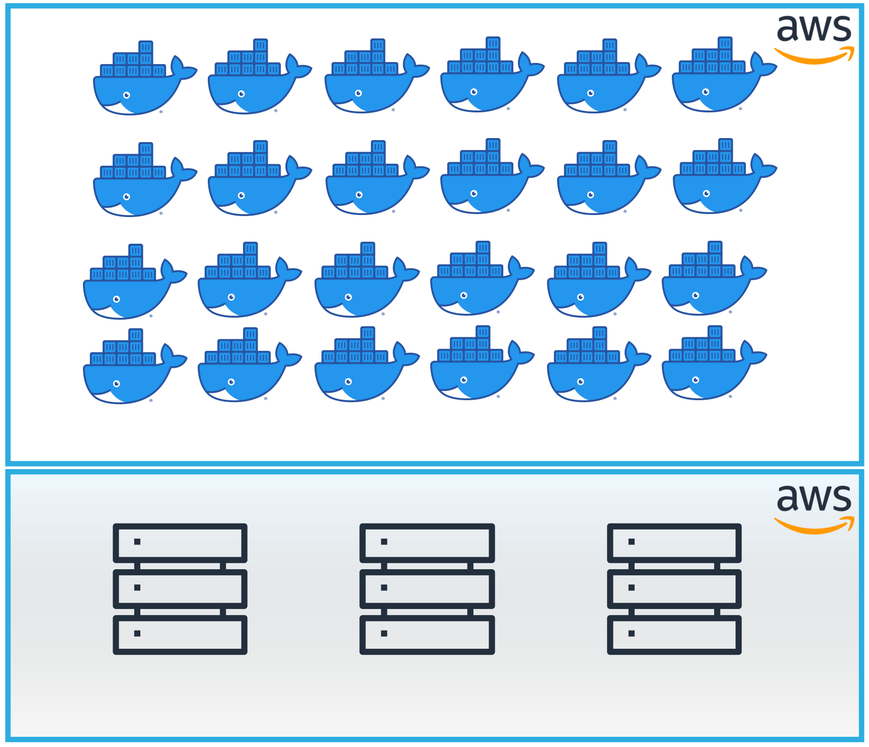
Amazon ECS

Amazon EKS

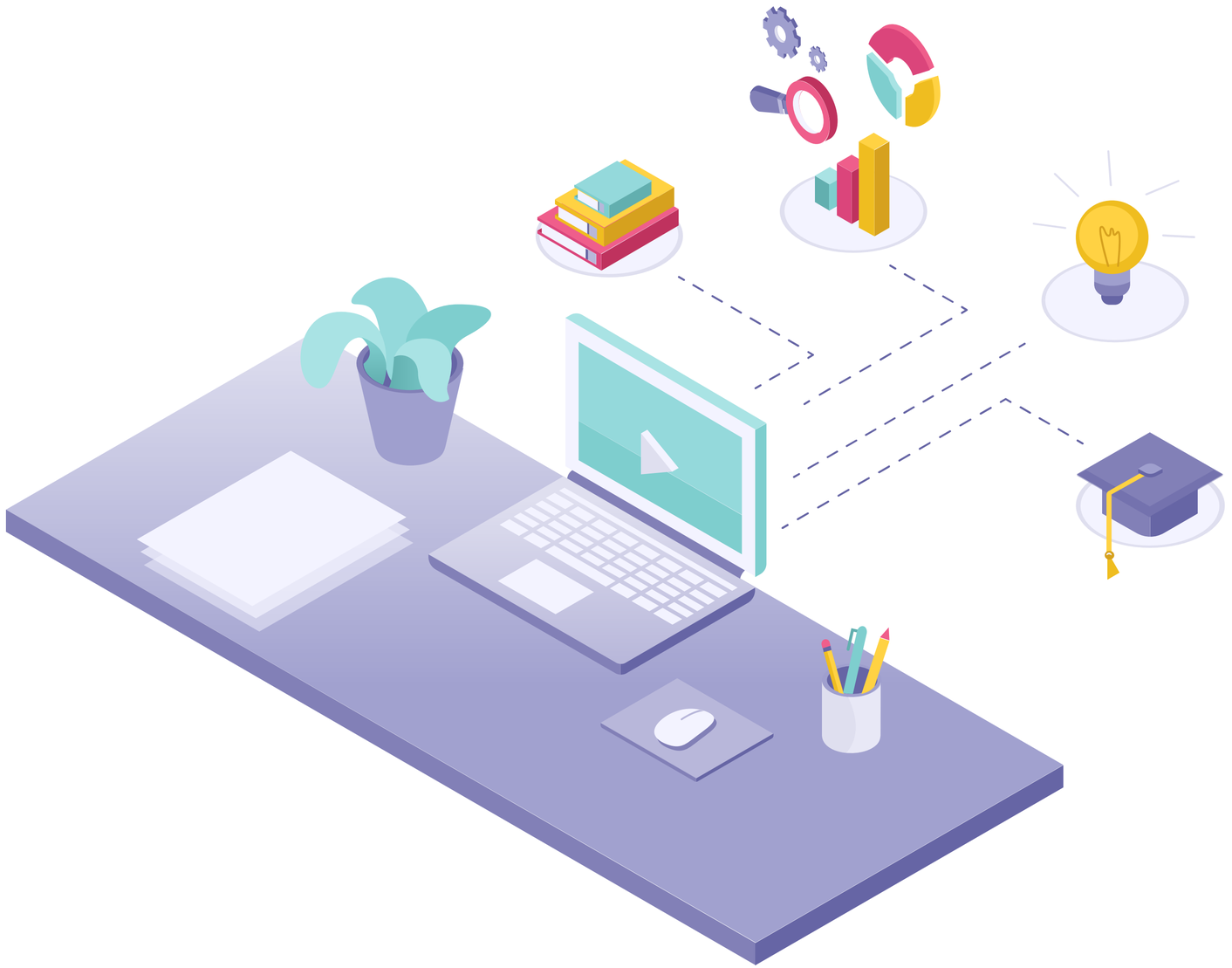
Gestion de l'infrastructure sous-jacente

Amazon EC2

AWS Fargate



Serverless



Serverless

Technologies pour exécuter du code ou déployer des applications, **sans avoir à gérer l'infrastructure**.



Avantages : Mise à l'échelle, Optimisation des coûts, Zéro gestion de serveurs

Serverless


AWS Fargate


AWS Lambda


Amazon SQS


Amazon S3

Non Serverless


Amazon EC2


Amazon RDS

AWS Lambda



Service de calcul **serverless**

Permet d'exécuter des fonctions **en réponses à des évènements**

Supporte **plusieurs langages** : Node.js, Python, Java, C, Ruby, Go ...

Supporte les « *Custom Runtime* » pour exécuter n'importe quel langage

Facturation : *Nombre d'exécutions* ***X*** *Durée d'exécution (ms)*

Offre gratuite : 1 million de requêtes par mois

Exemples d'invocation de fonctions Lambda

Requête HTTP

Amazon S3

Amazon SQS

Application tierce

IOT

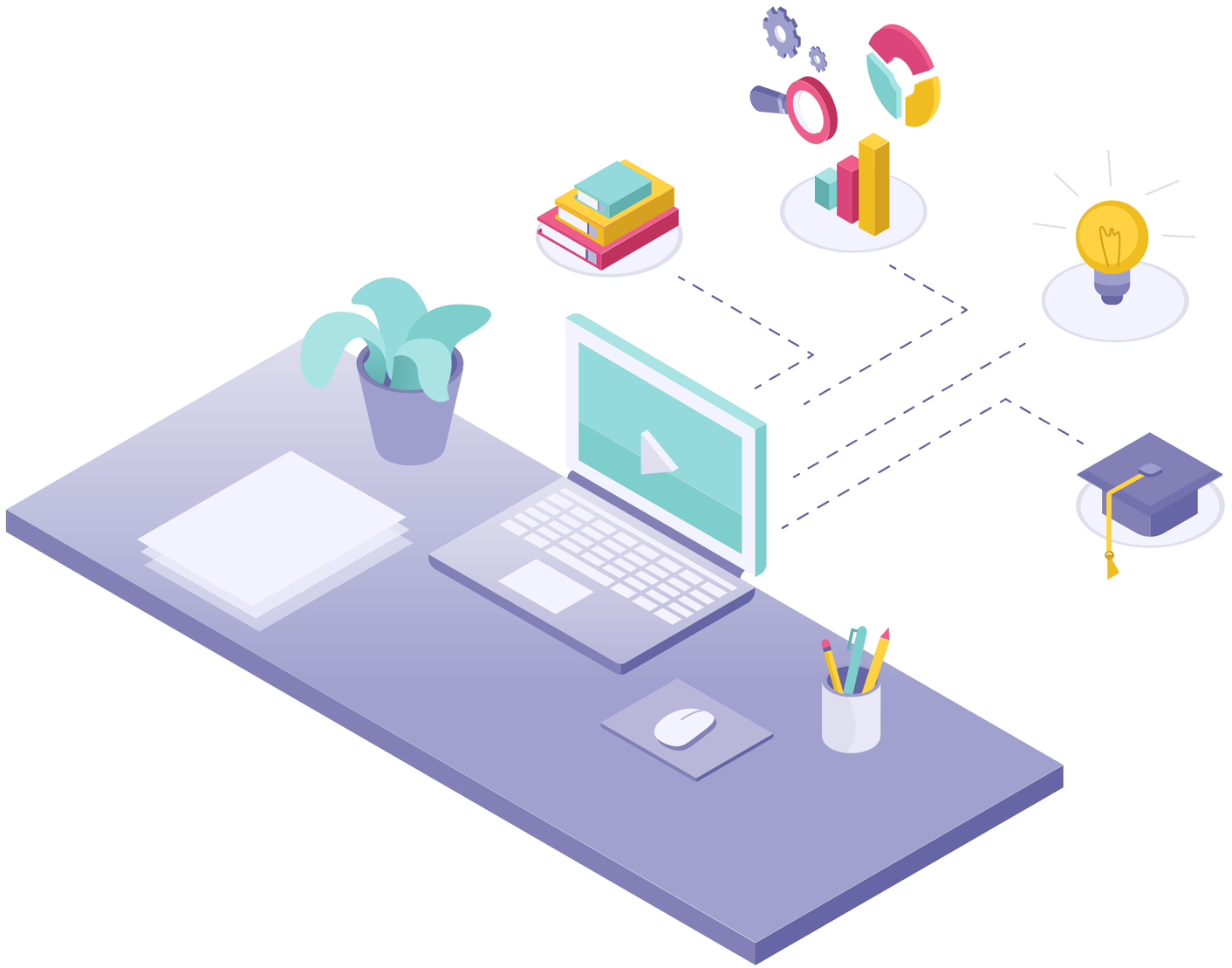


Fonction Lambda

Function code

```
1  console.log('Loading event');
2  var result;
3  exports.handler = function(event, context) {
4                    var AWS = require('aws-sdk');
5                    var s3 = new AWS.S3();
6                    var s3params = {
7                        Bucket: 'Bucket26', /* required */
8                        Key: 'myData' /* required */
9                        };
10                   s3.getObject(s3params, function(err, data) {
11                    if (err) console.log(err, err.stack); // an error occu
12                   else   {
13                       result = data.Body.toString();
14                       console.log("Data is", result);
15                        var sns = new AWS.SNS({endpoint:"https://sns.us-ea
16                   var params = {
17                   Message: result, /* required */
18                   TargetArn: 'arn:aws:sns:us-east-1:610719677073:endpoint
19                   };
20                   sns.publish(params, function(err, data) {
```

Amazon Lightsail



Amazon Lightsail



Service d'hébergement web **simplifié -> VPS** (Virtual Private Server)

Permet de déployer **en quelques clics**

- Des **applications** : *Wordpress, Drupal, Joomla, Magento, Prestashop…*
- Des **ressources** : *serveurs Linux/Windows, Bases de données, Conteneurs, Stockage, Stack LAMP (Linux/Apache/MySQL/PHP), serveurs Nginx…*

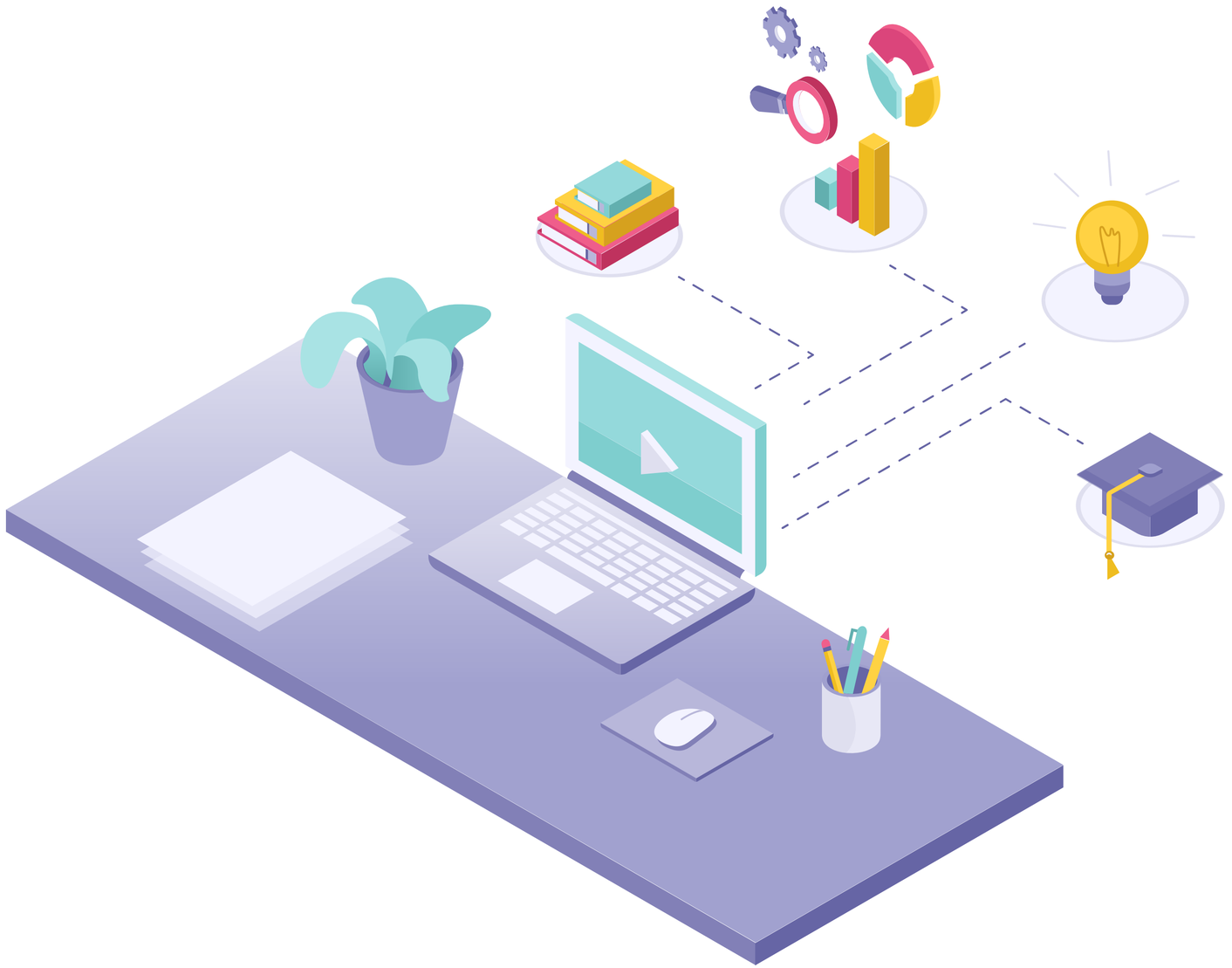
Destiné à des **utilisateurs**

- **Qui ne sont pas techniques ou qui débutent sur AWS**
- Qui veulent déployer des applications en **quelques clics**
- Qui ne veulent pas gérer l'**infrastructure**
- **Aux petites entreprises**

Tarification horaire **simplifiée et abordable** selon des forfaits

Exp : 1 instance Linux + Wordpress + 1 vCPU + 1 Go mémoire + Disque SSD à 40 Go + 2To Data Transfer = ***~5 USD***

AWS Elastic Beanstalk



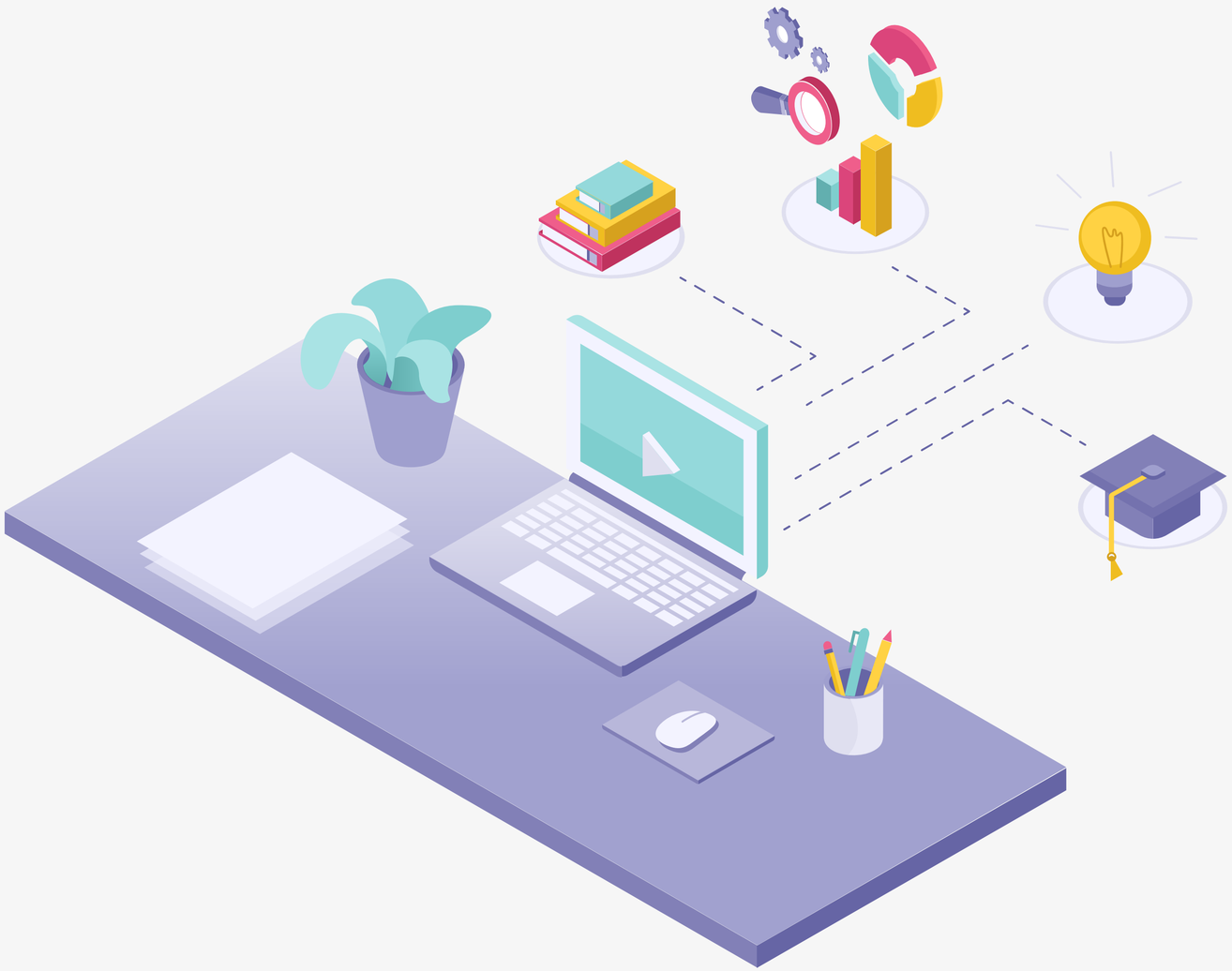
AWS Elastic Beanstalk



Permet de déployer rapidement des applications Web ou backends d’APIs

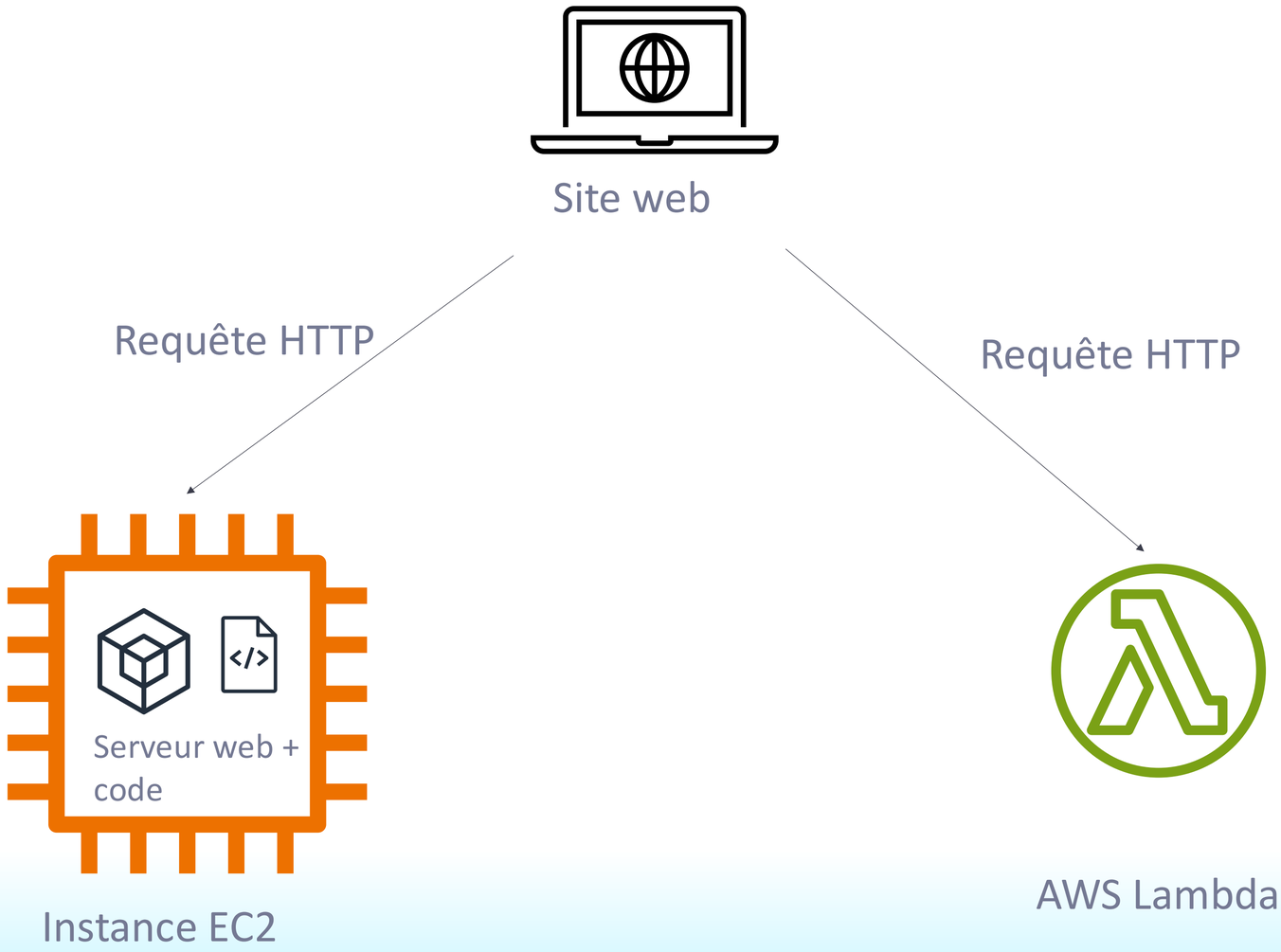
Service PaaS : vous passez votre application et Beanstalk l’exécute pour vous

Prend en charge les applications web Java, .NET, PHP, Node.js, Python, Ruby, Go et Docker.



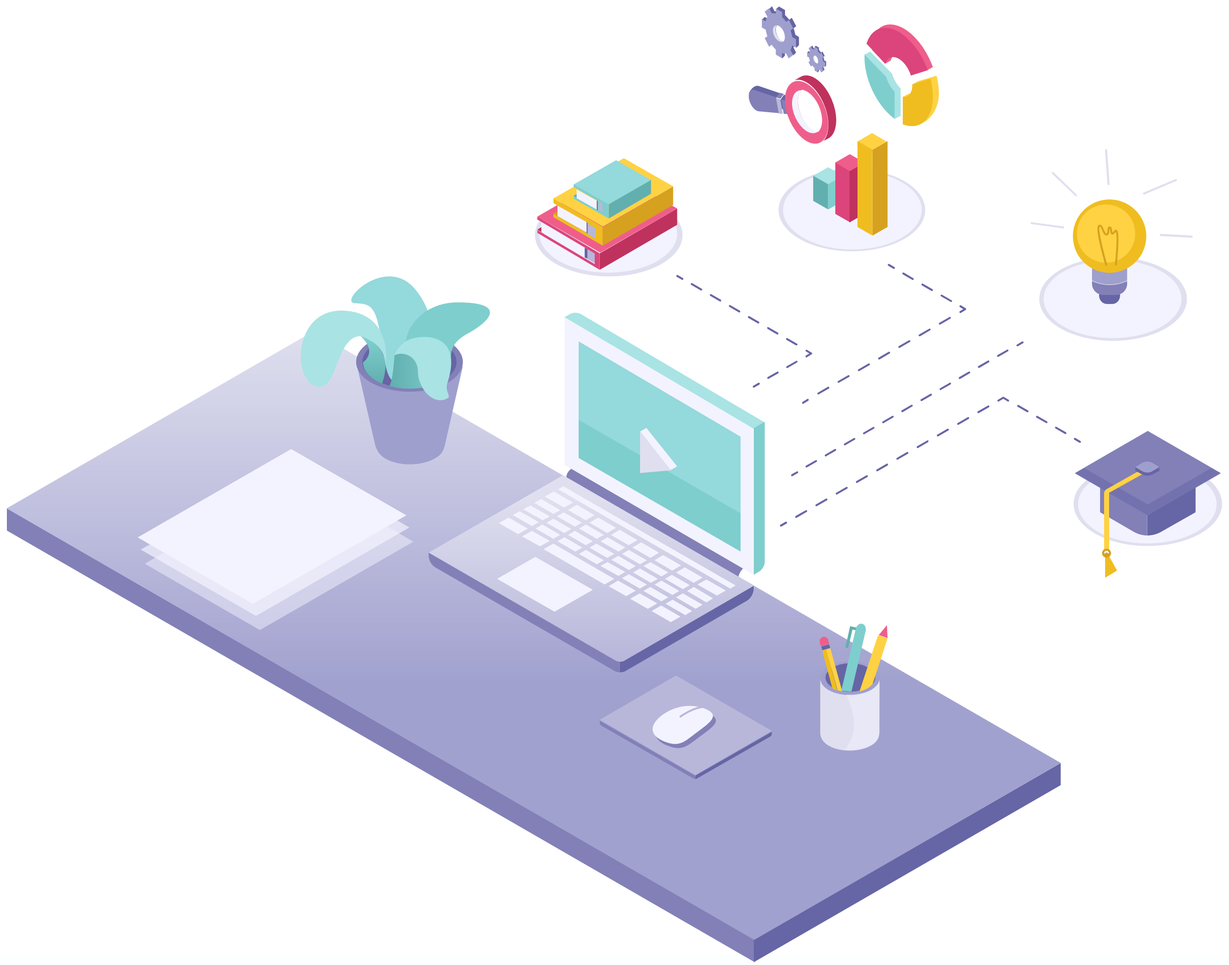
FIN DU MODULE

Lab Créer votre 1ère function AWS Lambda



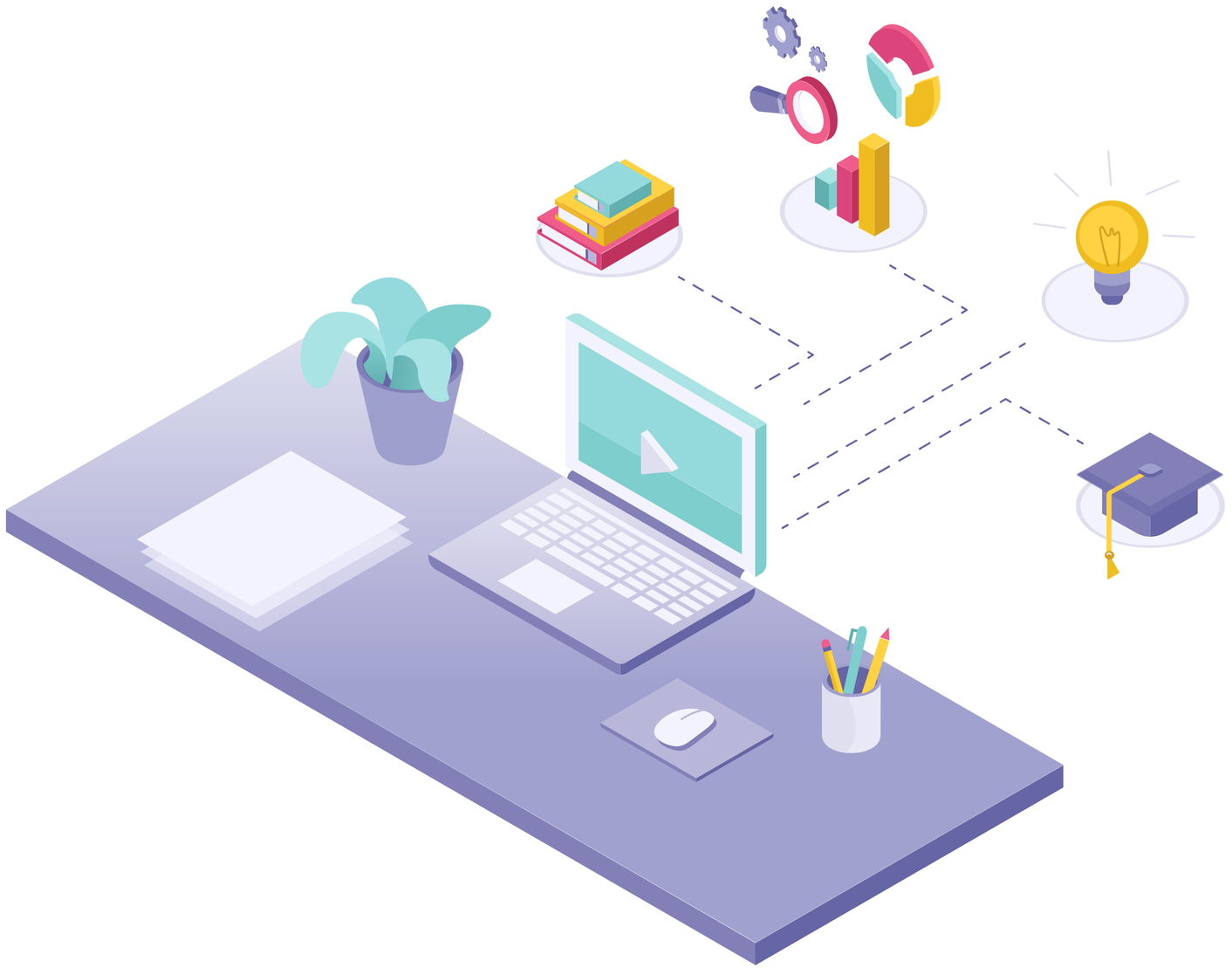
Module 5 : Amazon VPC

Exécutez chaque application sur un réseau mondial sécurisé et fiable



LeCloudFacile.com

Notation CIDR



Classless Inter Domain Routing (CIDR)

172.31.0.0/16

En français : « ***routage inter-domaines sans classe*** »

Permet d'identifier un bloc d'adresses IP

Utilisé lors de la création du VPC (spécifie la taille du VPC)

Classless Inter Domain Routing (CIDR)

Exemple de bloc d'adresses CIDR

172.31.0.0/16

1010 1100 0001 1111 0000 0000 0000 0000

65536 IPs

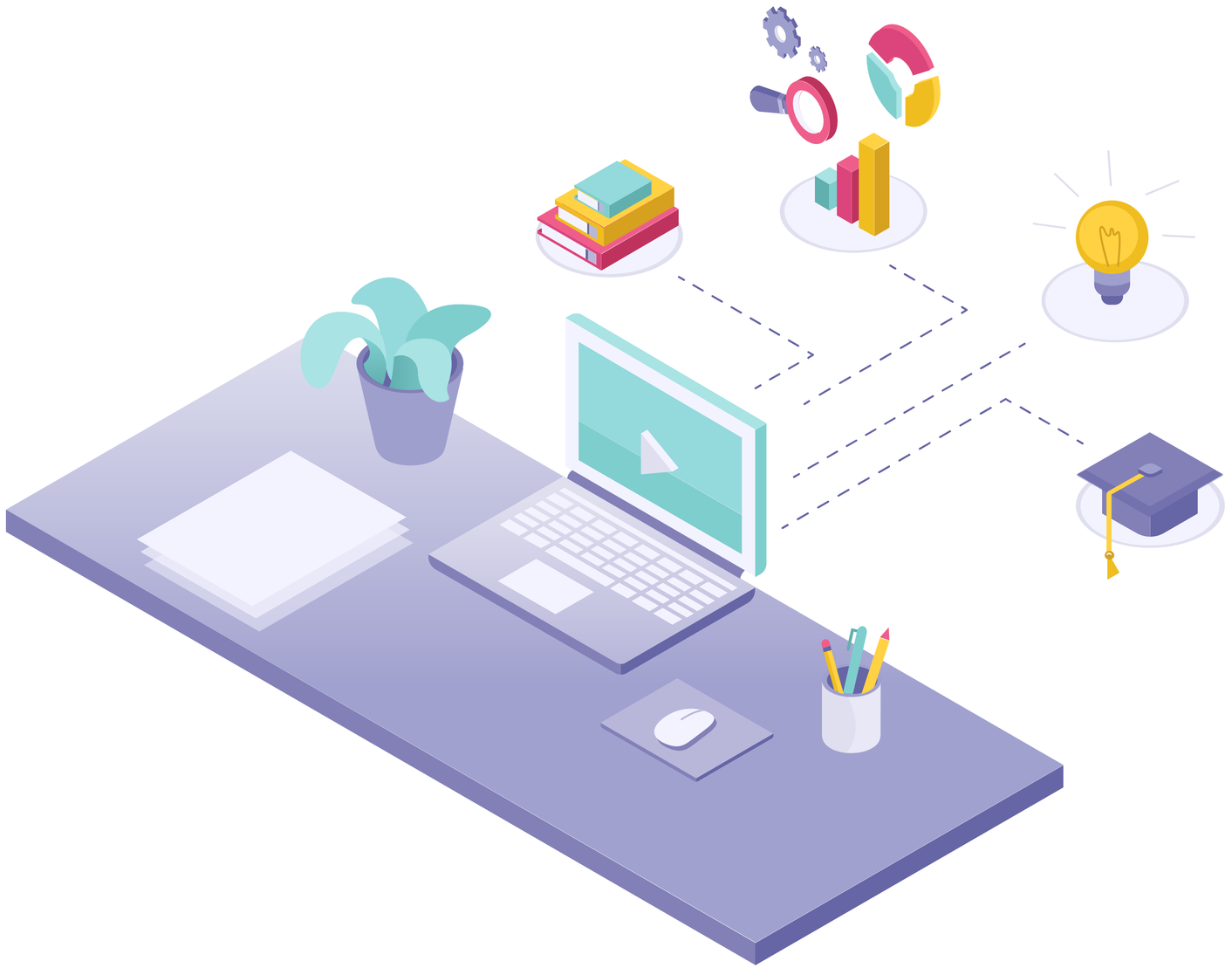
10.0.1.0/24

0000 1010 0000 0000 0000 0001 0000 0000

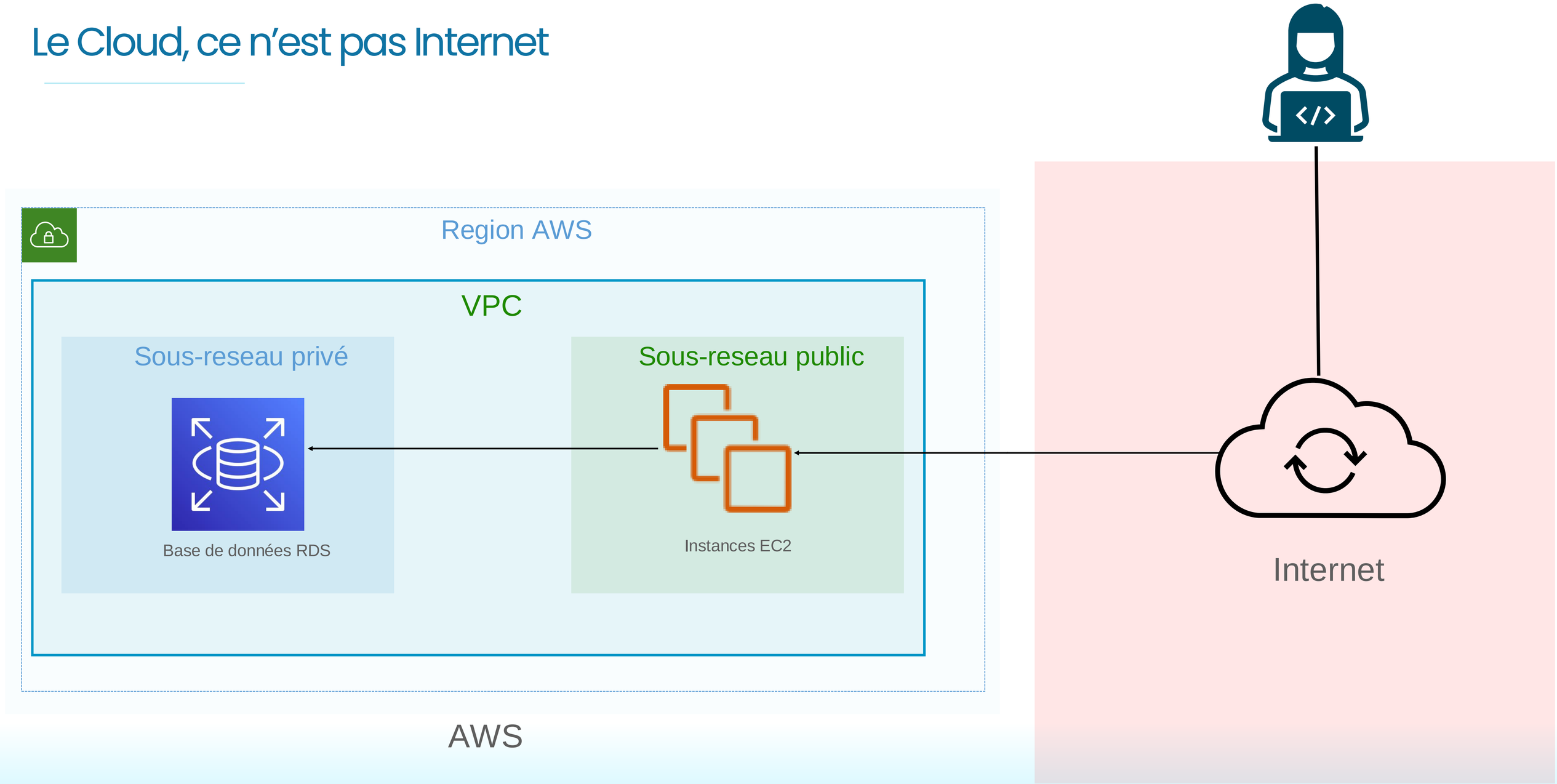
256 IPs

https://cidr.xyz/

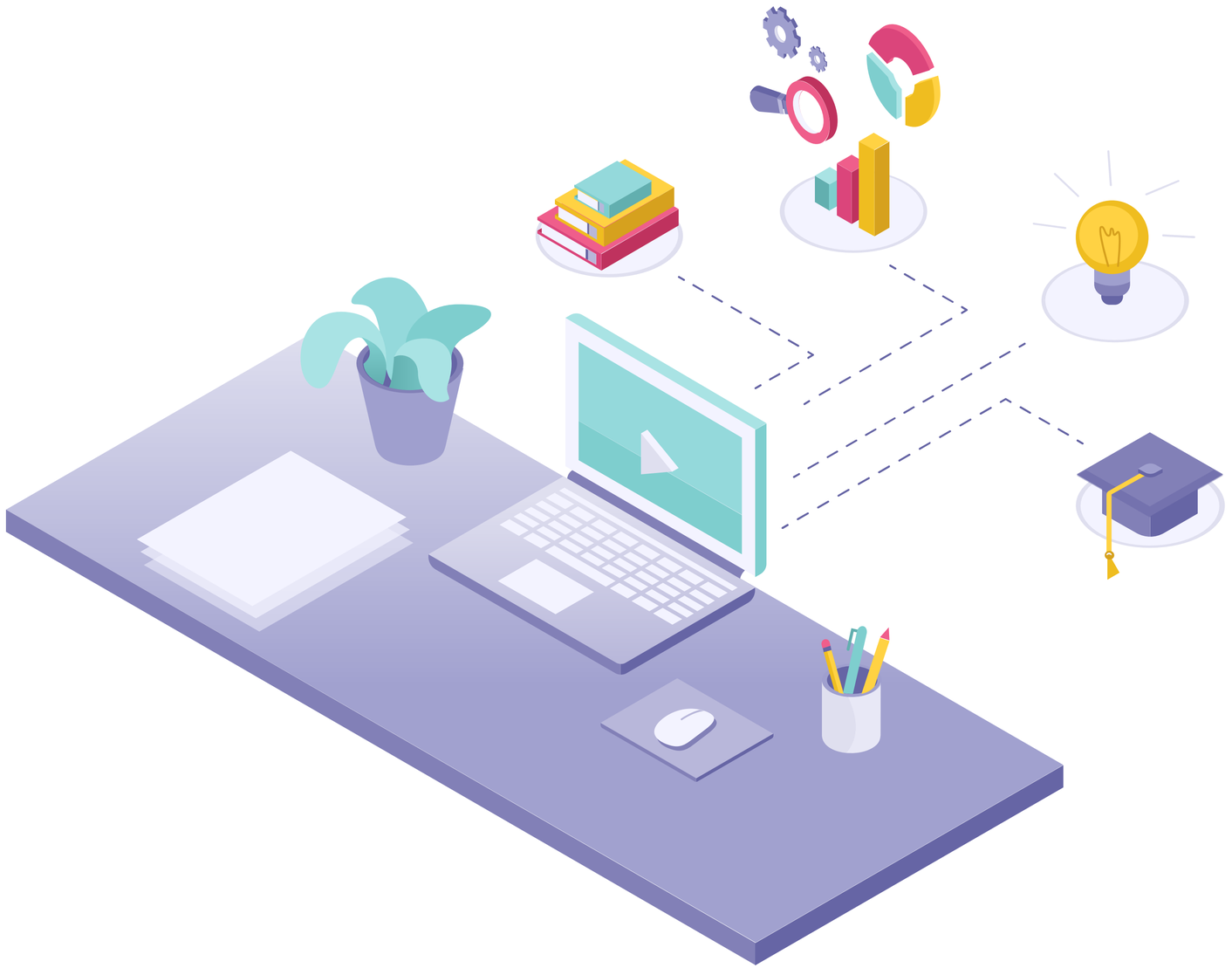
Le Cloud, ce n’est pas Internet



Le Cloud, ce n'est pas Internet



Amazon Virtual Private Cloud (VPC)



Amazon Virtual Private Cloud (VPC)

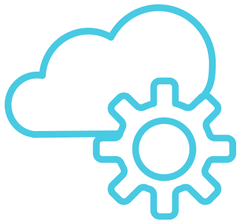
Cloud AWS



Votre VPC

Votre espace réseau privé dans le cloud AWS

Amazon Virtual Private Cloud (VPC)



C’est votre **espace réseau** dans le cloud AWS

Contient les ressources que vous créez : EC2, EBS, RDS…

Divisé en **sous-réseaux** (*subnets*) publics ou privés

Vous pouvez avoir plusieurs VPCs par région AWS

Supporte IPv4 et IPv6

Bloc CIDR

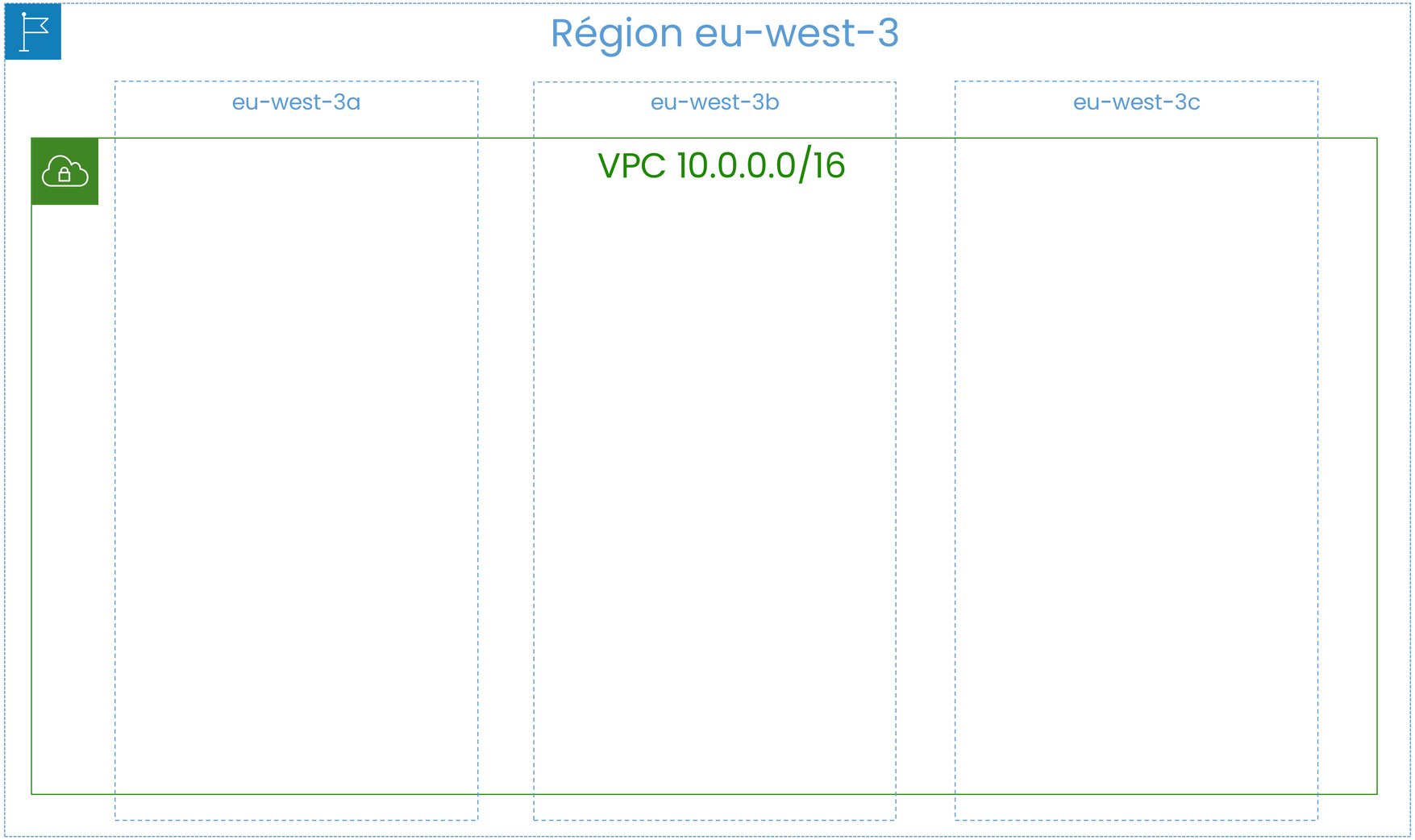
Lorsque vous créez un VPC, vous devez lui attribuer un **bloc d'adresses CIDR IPv4**

RFC 1918 range	Example CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	192.168.0.0/20

Masque réseau VPC **entre /16 (65.536 IPs) et /28 (16 IPs)**

Choisissez la taille de votre VPC en fonction de vos **besoins actuels et futurs**

Exemple de VPC



Exemple de VPC dans la région eu-west-3 (Paris)

A savoir sur les VPC

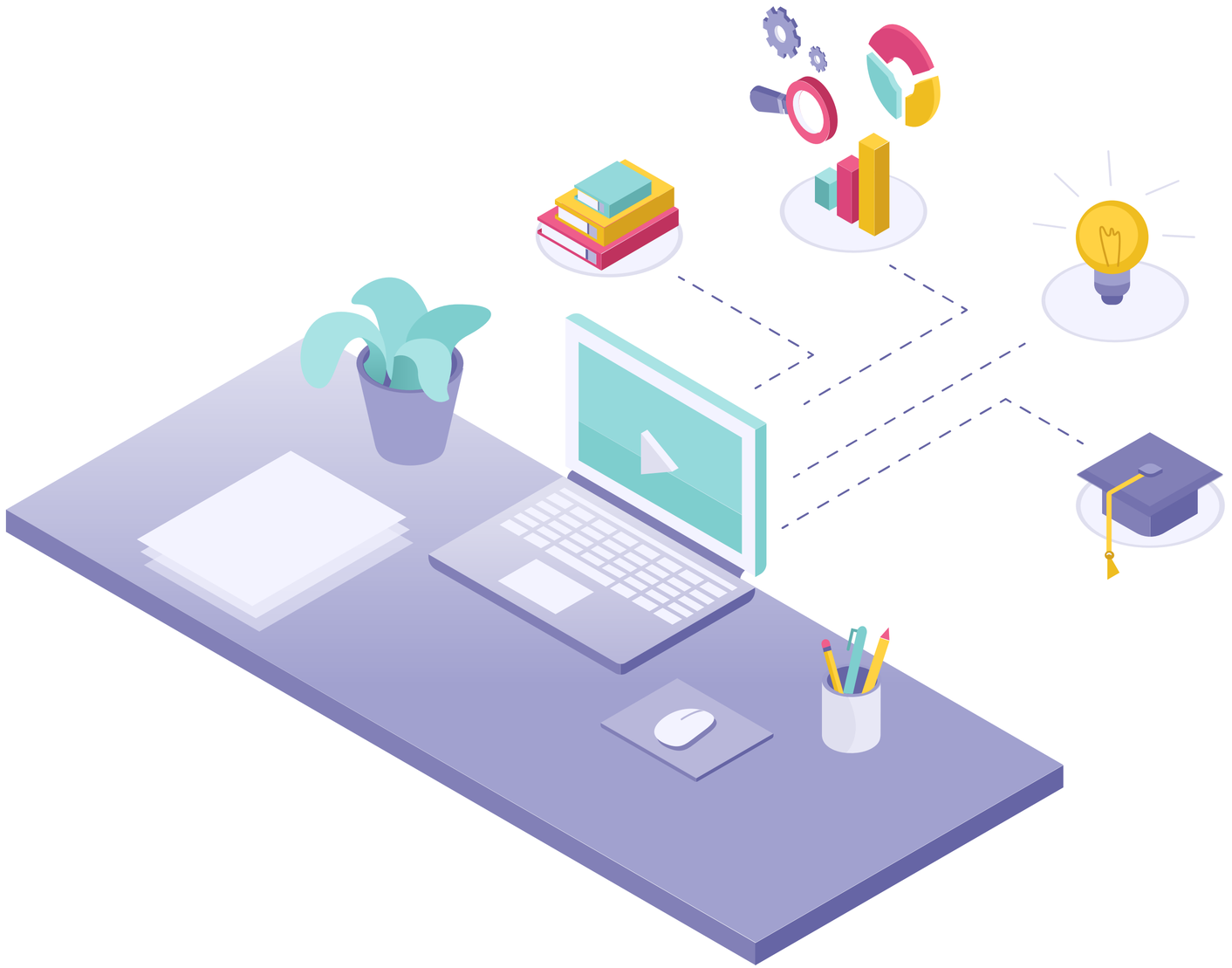
AWS crée automatiquement **un VPC par défaut** dans chaque région ->

172.31.0.0/16

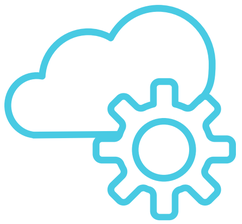
Par défaut, les VPC dans votre compte AWS sont **isolés les uns des autres**

Eviter d'utiliser le même bloc CIDR (**Overlap**) pour plusieurs VPC

Sous-réseaux



Sous-réseaux (subnets)



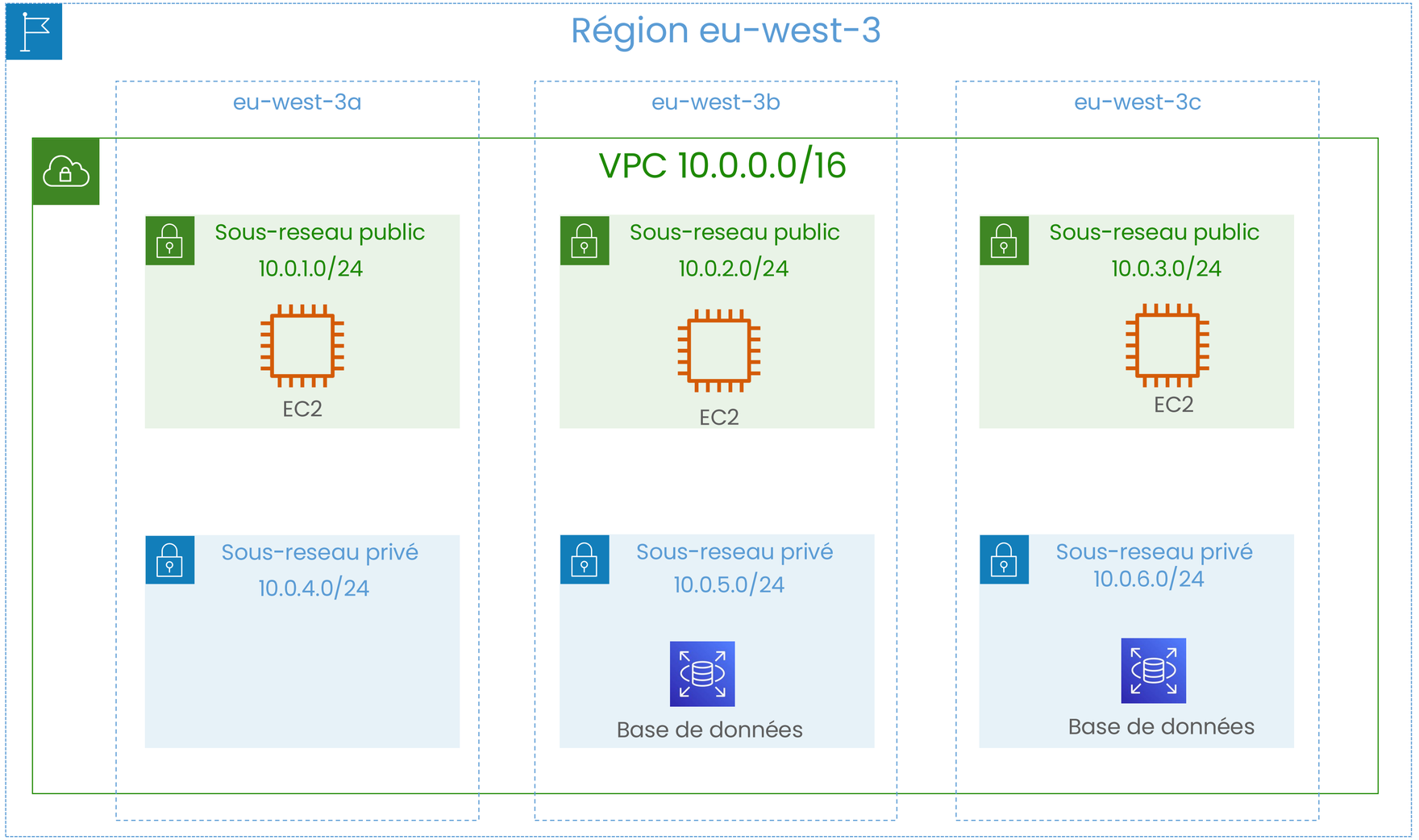
Sous-ensembles du VPC auquel ils appartiennent

Définis par un bloc CIDR. Exemple : 10.0.0.0/24

Contiennent les ressources que vous déployez : EC2, Bases de données,...

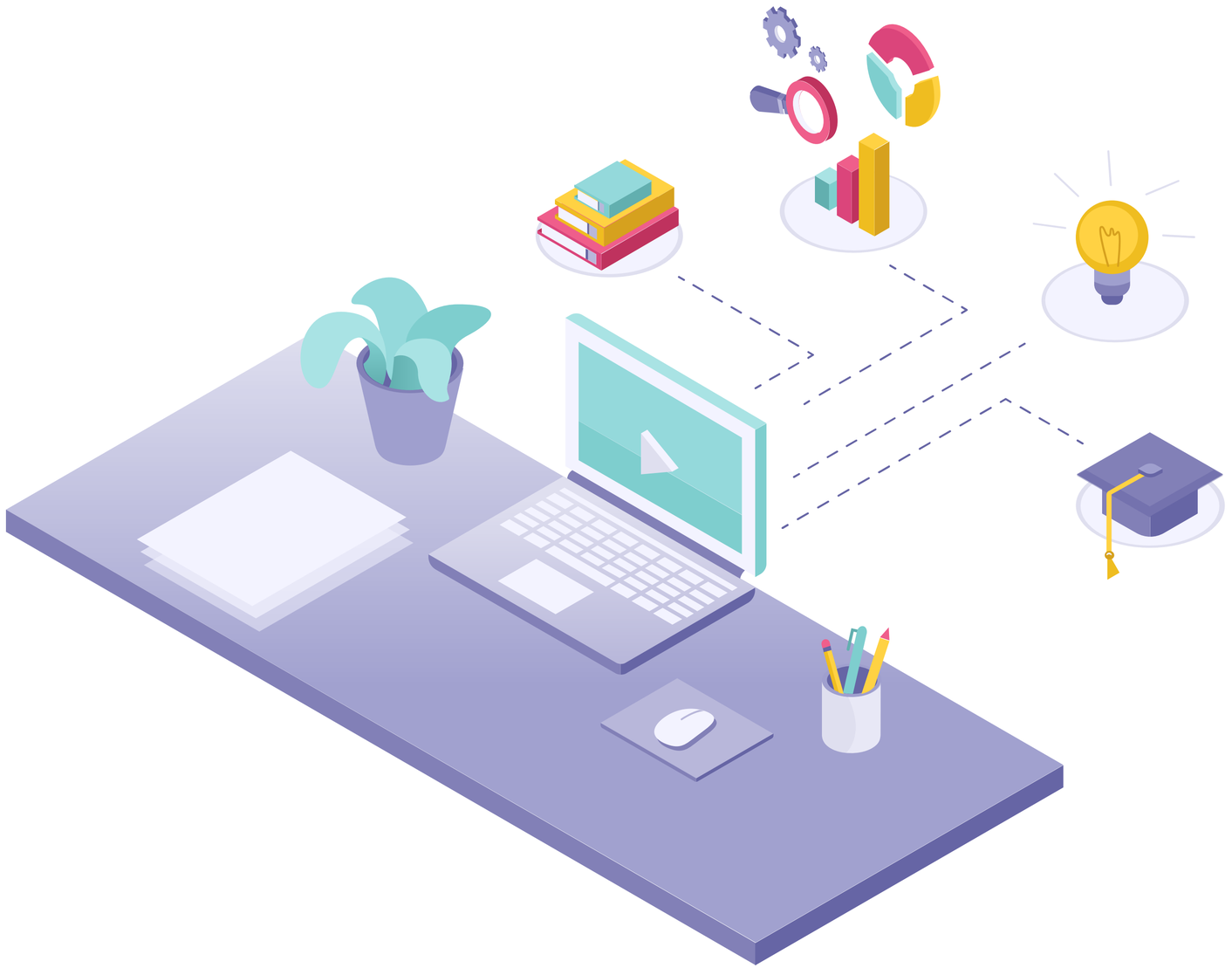
Appartiennent à 1 zone de disponibilité spécifique

Exemple de sous-réseaux

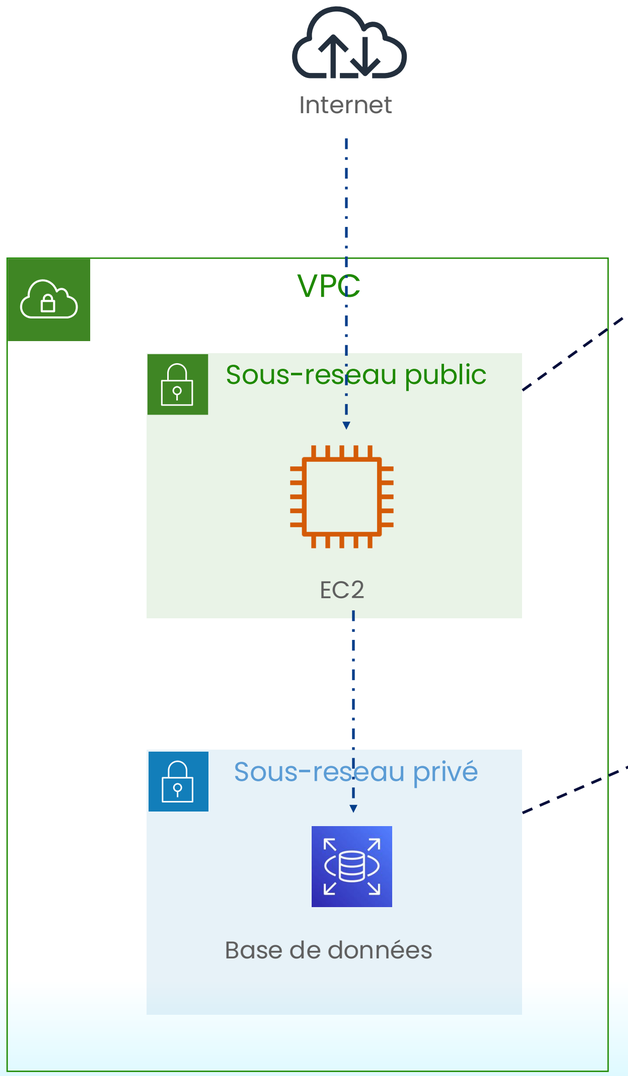


Exemple de VPC avec 6 sous-réseaux (3 publics et 3 privés)

Sous-réseau public vs privé



Sous-réseau public vs privé



Sous-réseau public

Les ressources sont accessibles et peuvent accéder directement à **Internet**

Le trafic vers Internet passe par une **Internet Gateway**

On y déploie : les proxys, load balancers ...

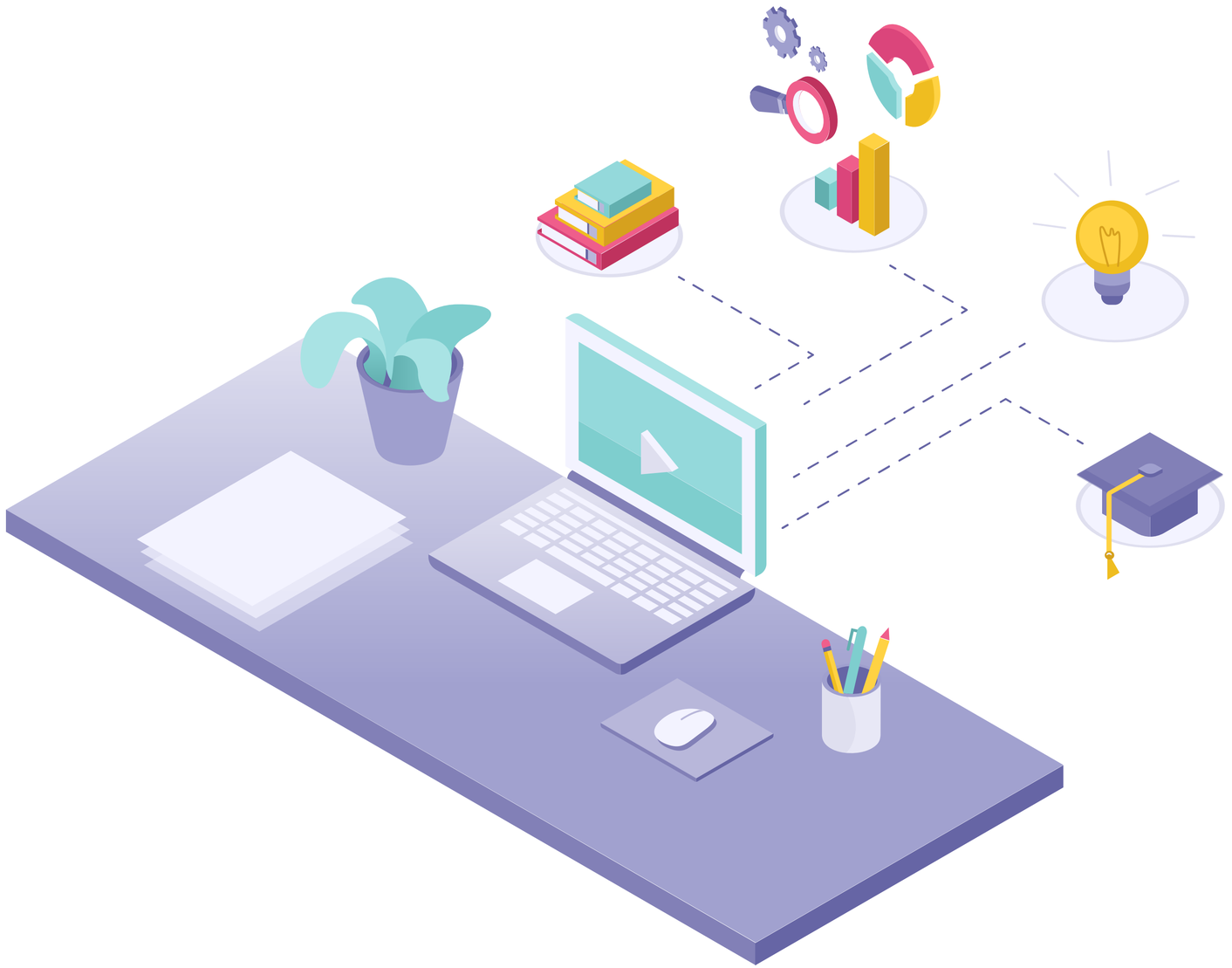
Sous-réseau privé

Ne sont pas accessibles et Ne peuvent pas accéder à **Internet**

Sauf si vous déployez une **NAT Gateway** pour router le trafic vers Internet

On y déploie : les applications sensibles, bases de données ...

Composants du VPC

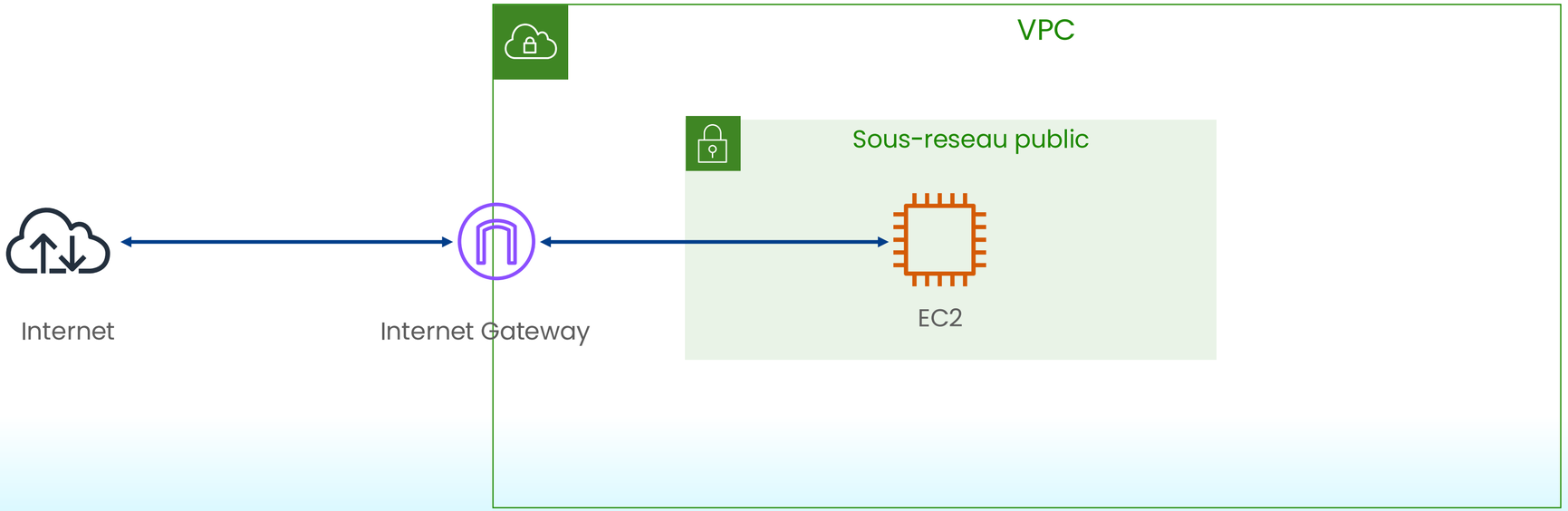


Internet Gateway

Composant réseau du VPC

Permet aux instances dans les sous-réseaux publics de se **connecter à Internet**

Redondant, hautement disponible et entièrement géré par AWS

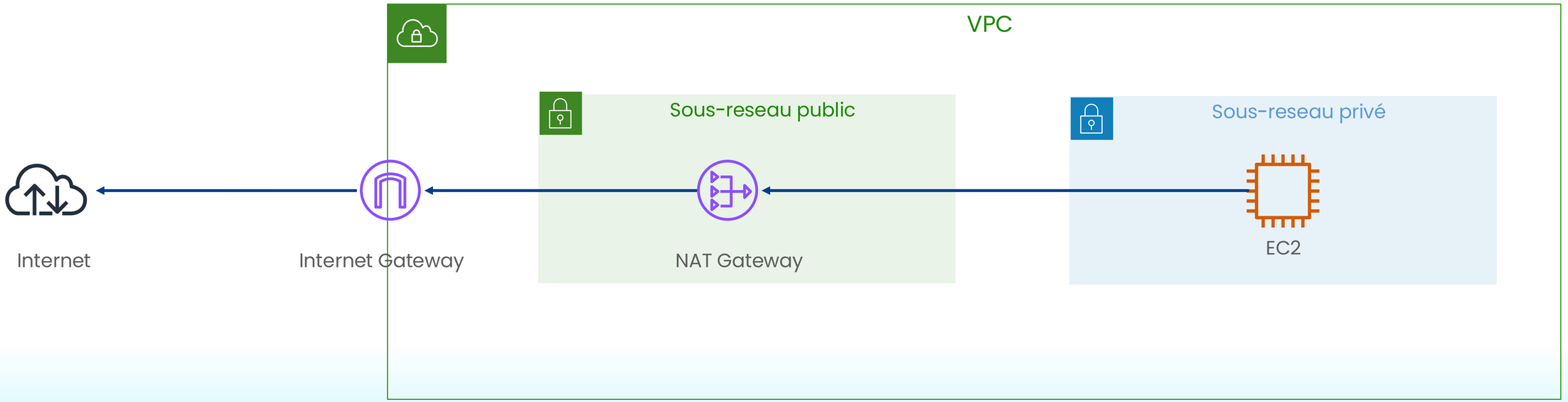


NAT Gateway

Composant réseau du VPC

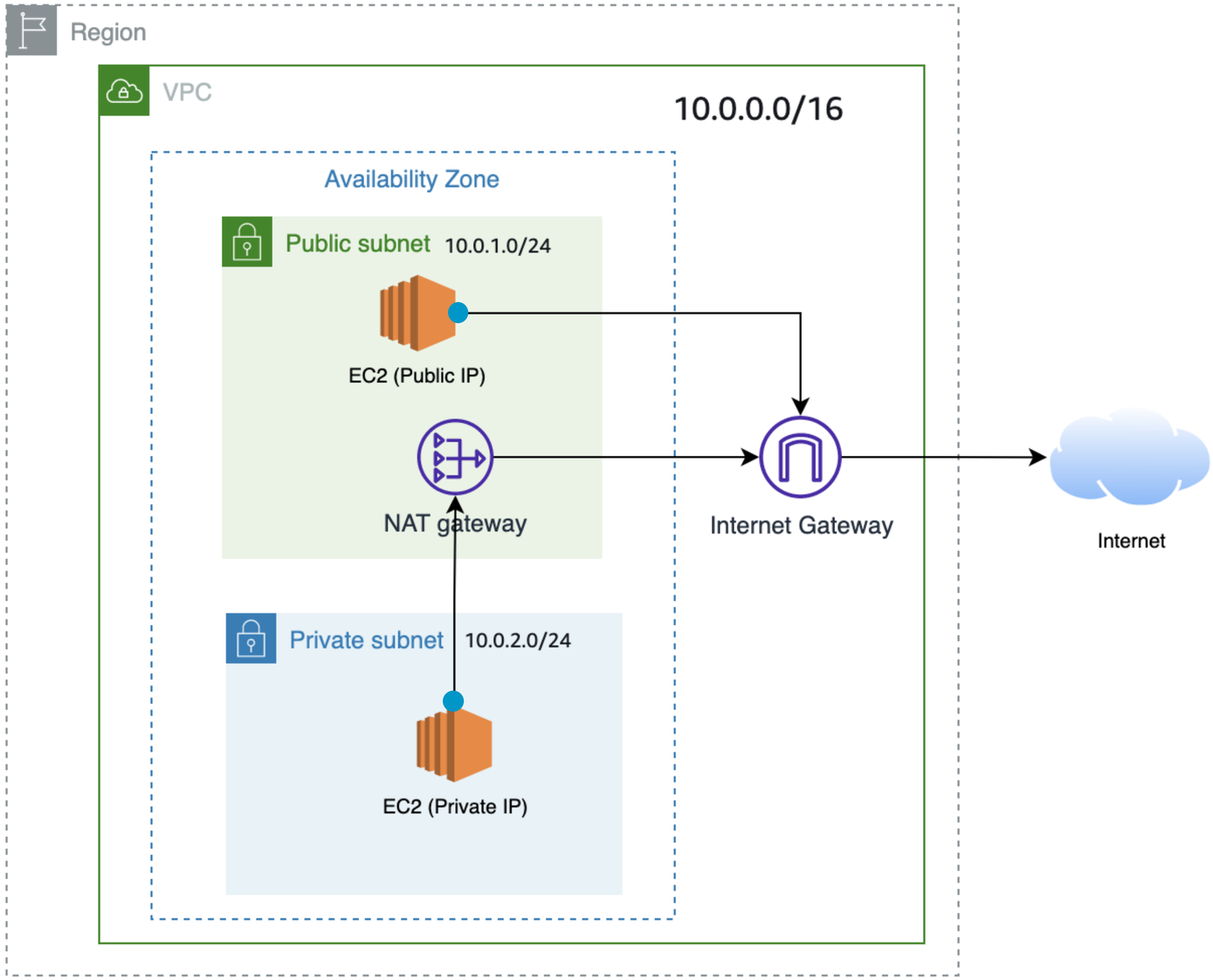
Permet aux instances dans les sous-réseaux **privés** de se connecter à **Internet**.

Ne permet pas à Internet de se connecter aux instances des sous-réseaux privés

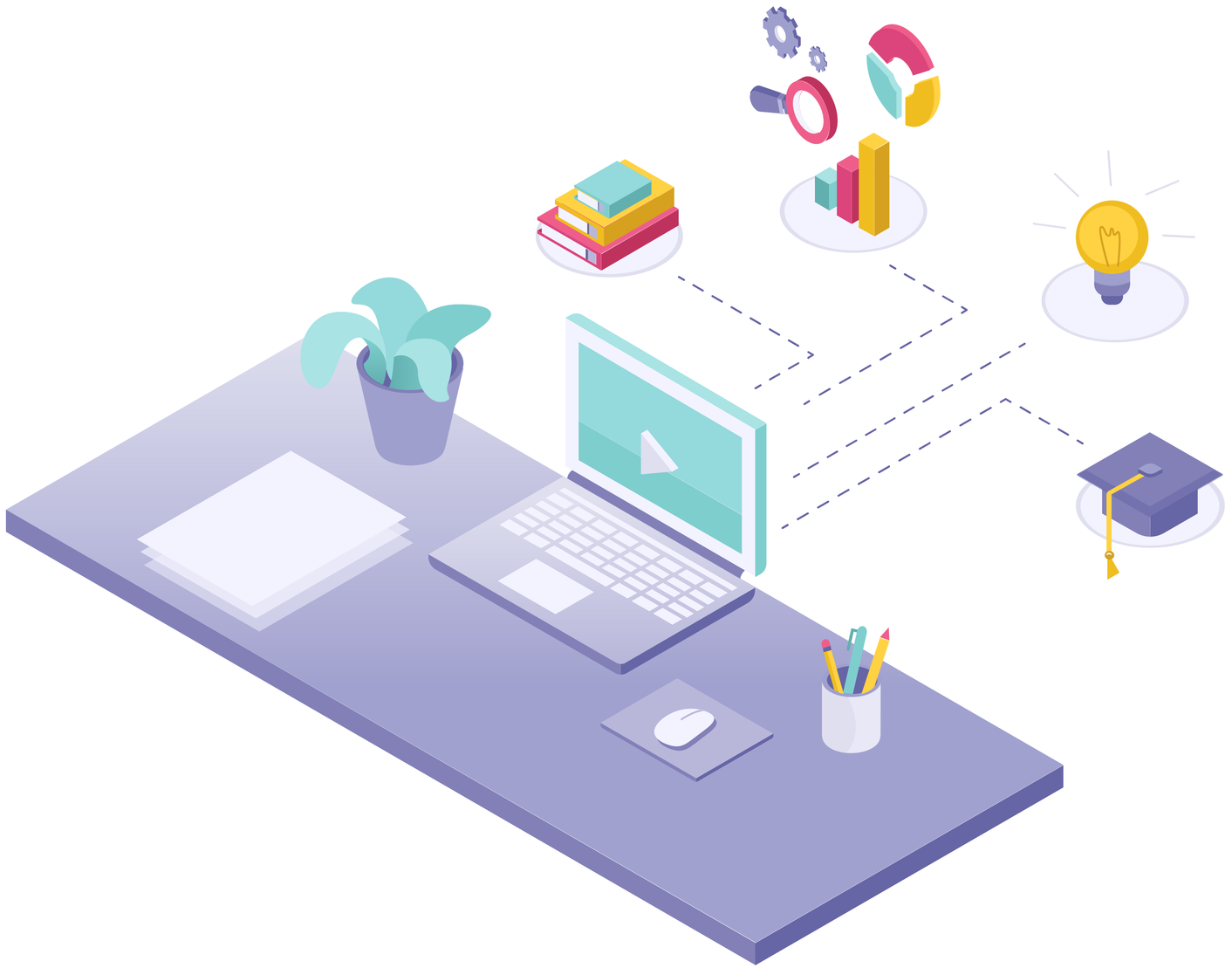


** NAT : Network Adress Translation*

Mise en oeuvre dans le VPC



Groupe de sécurité et NACL

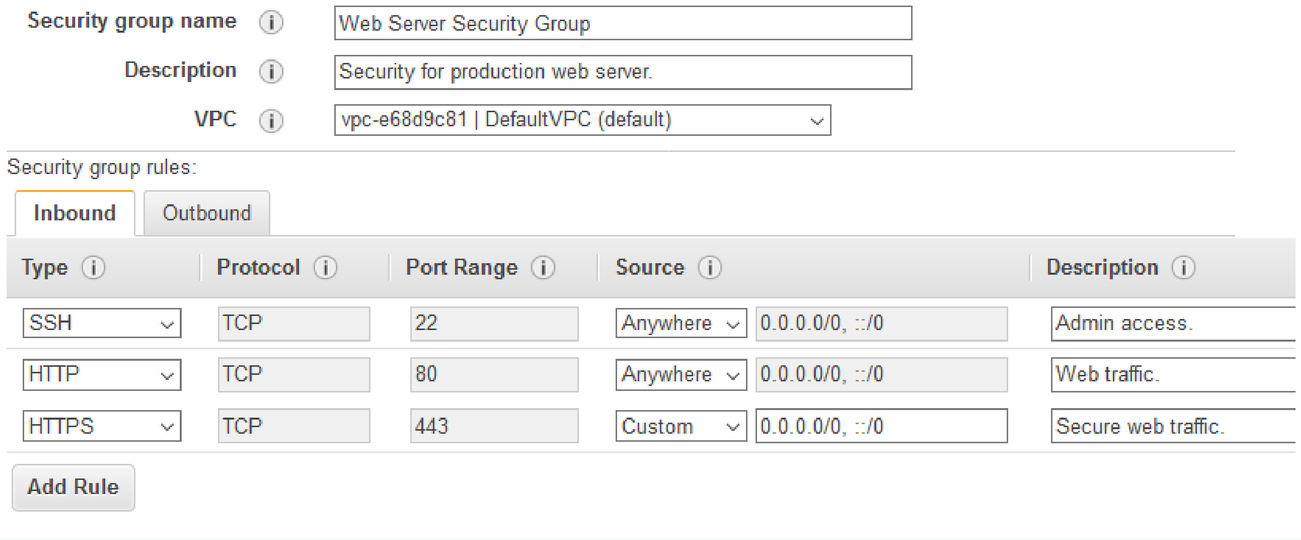


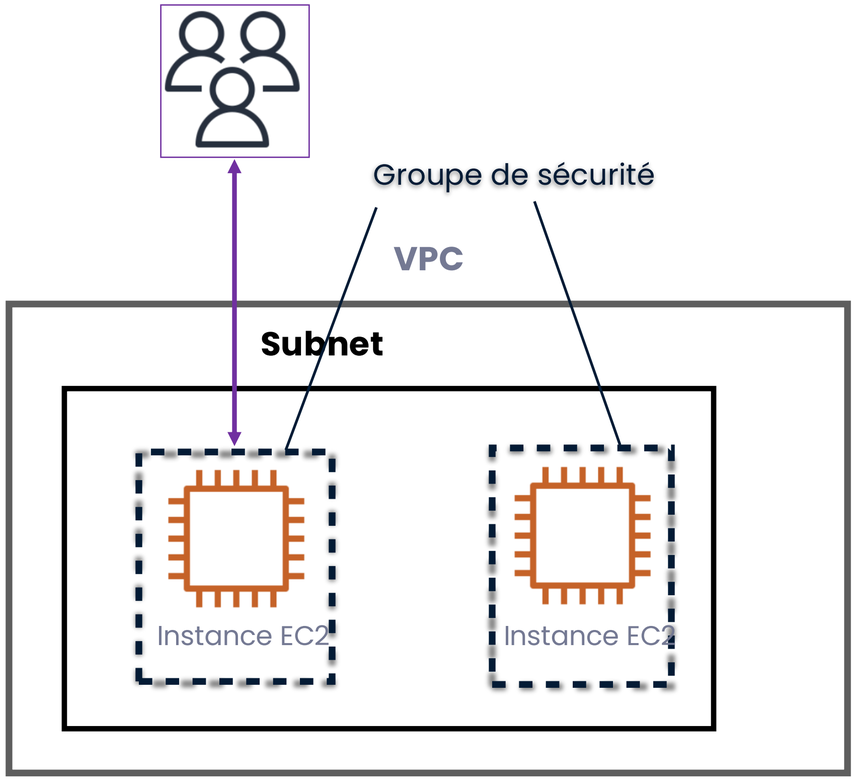
Groupe de sécurité (Rappel)

Pare-feu virtuel qui contrôle le trafic réseau des instances EC2

Configuration via des règles ALLOW pour autoriser les flux

DENY implicite : tout ce qui n'est pas autorisé (ALLOW) est refusé



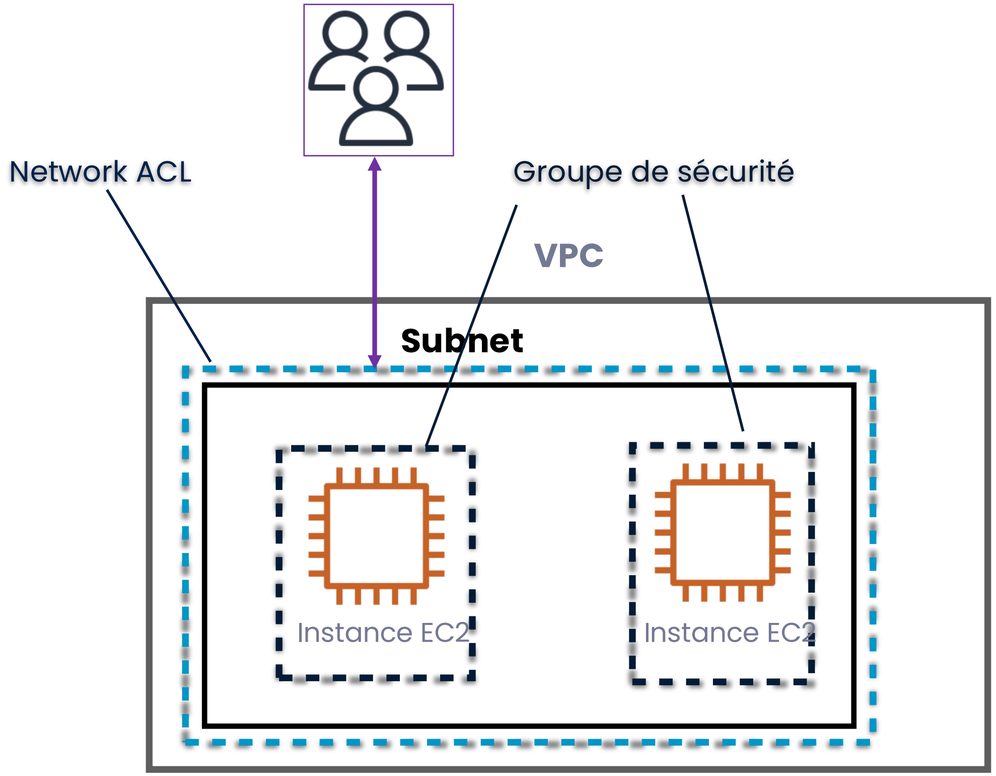


Network ACL

Pare-feu virtuel qui contrôle le trafic **de l'ensemble du sous-réseau**

Configuration via des règles ALLOW et DENY

Les DENY explicites sont utiles pour bloquer des flux ou des IP malicieuses



Inbound

Rule #	Type	Protocol	Port range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

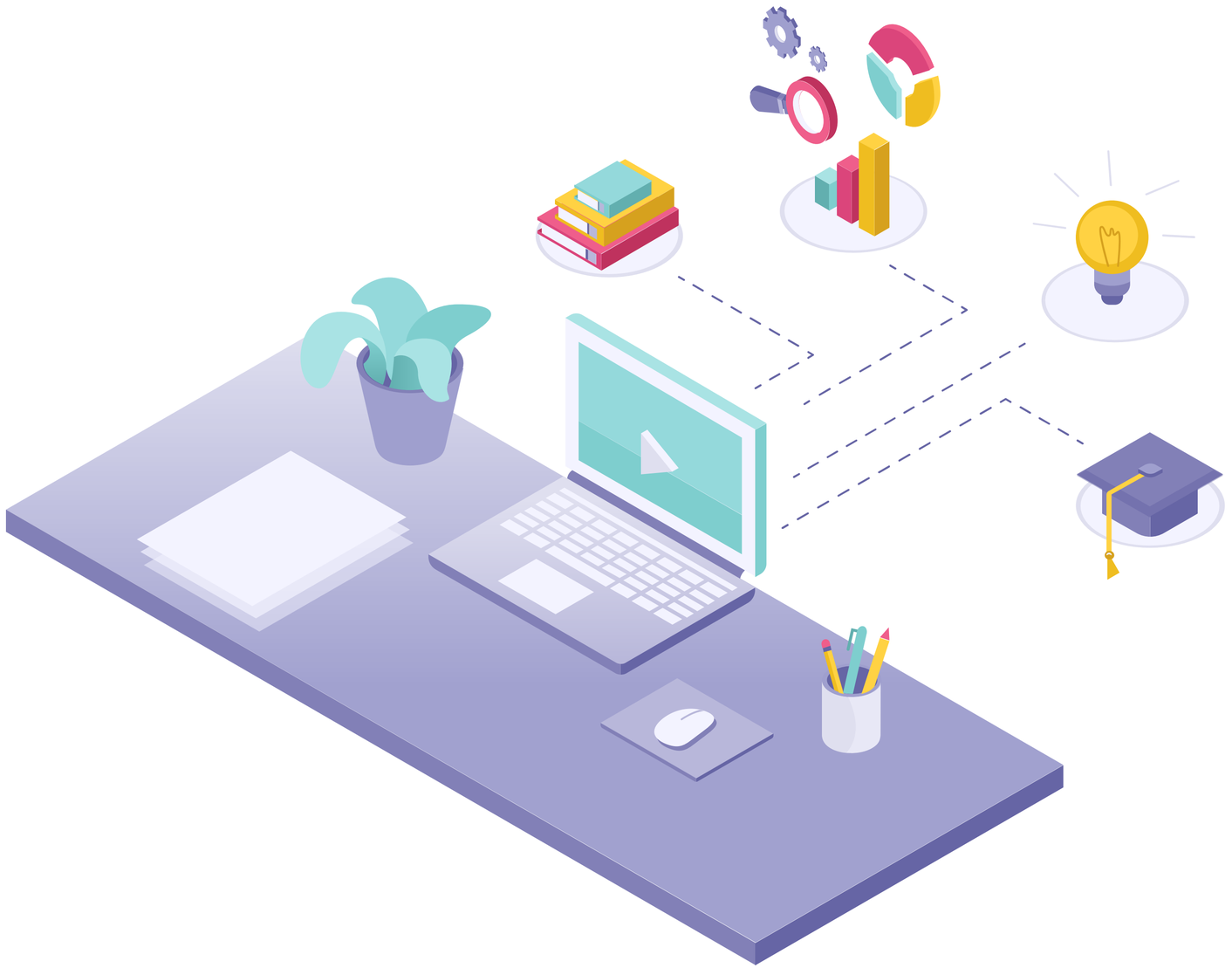
Outbound

Rule #	Type	Protocol	Port range	Destination	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

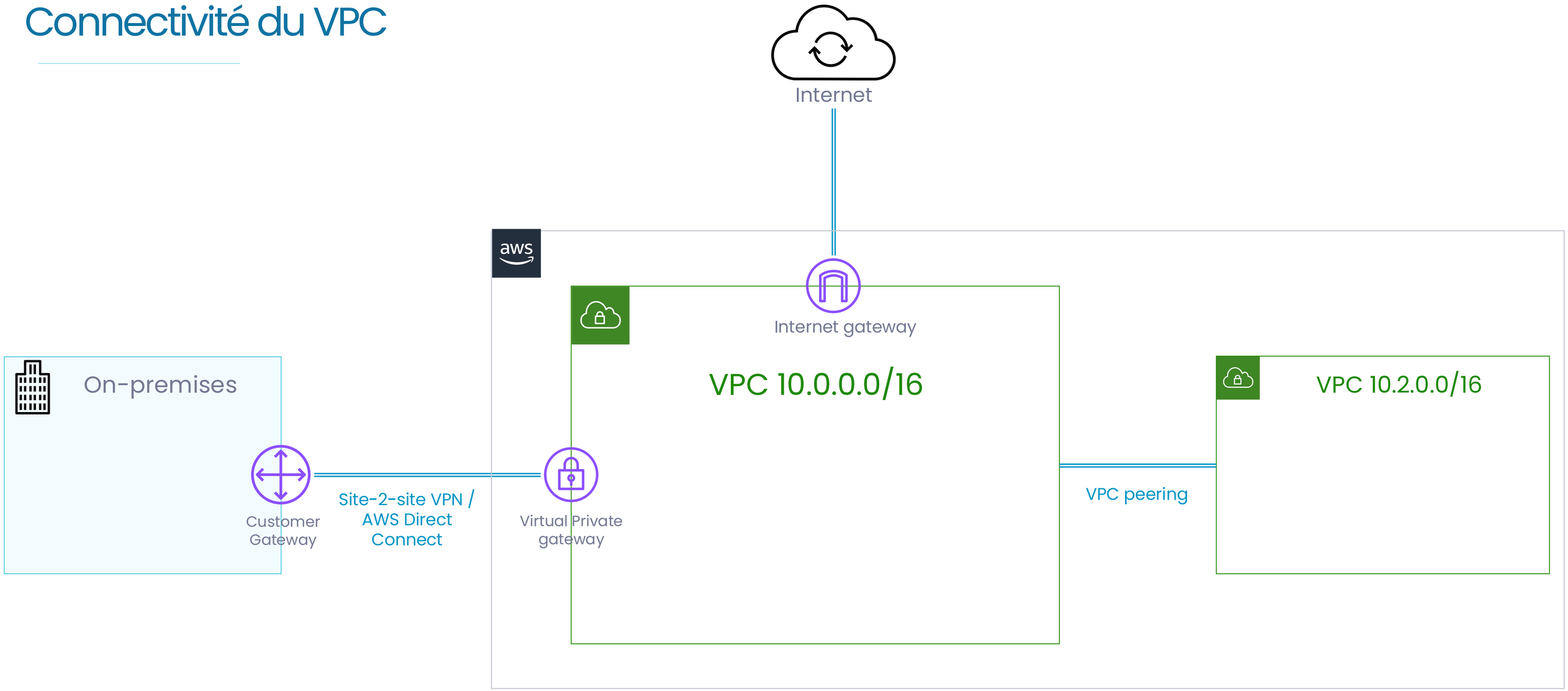
Network ACL vs Groupe de sécurité

Network ACL	Groupe de sécurité
Contrôle le trafic réseau de l'ensemble du sous-réseau	Contrôle le trafic entrant/sortant de l'instance EC2 associée
Les règles ACL sont sans état -> *Stateless*	Les règles sont avec état -> *Stateful*
Supporte les règles ALLOW et DENY	Supporte les règles ALLOW uniquement

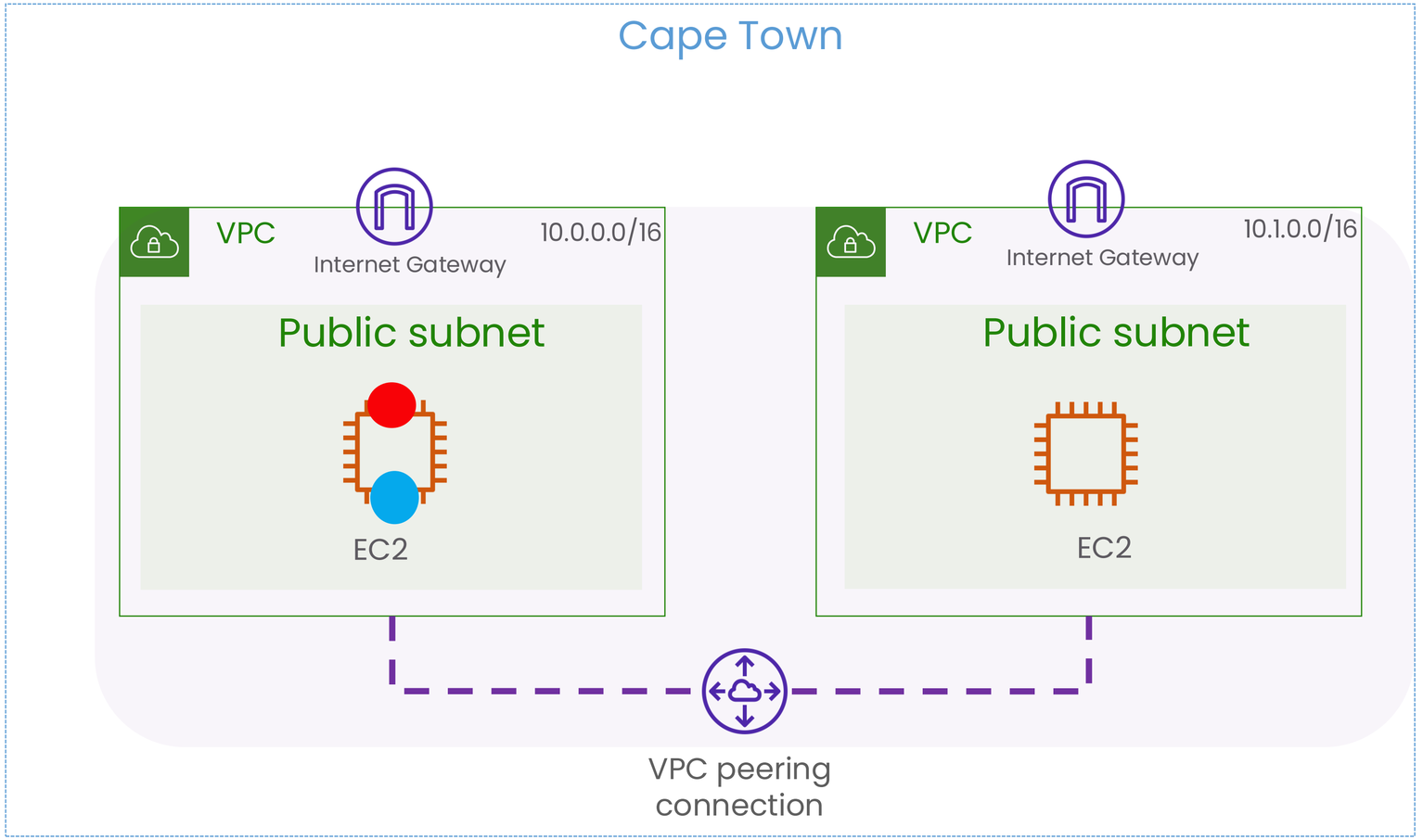
Connectivité du VPC



Connectivité du VPC

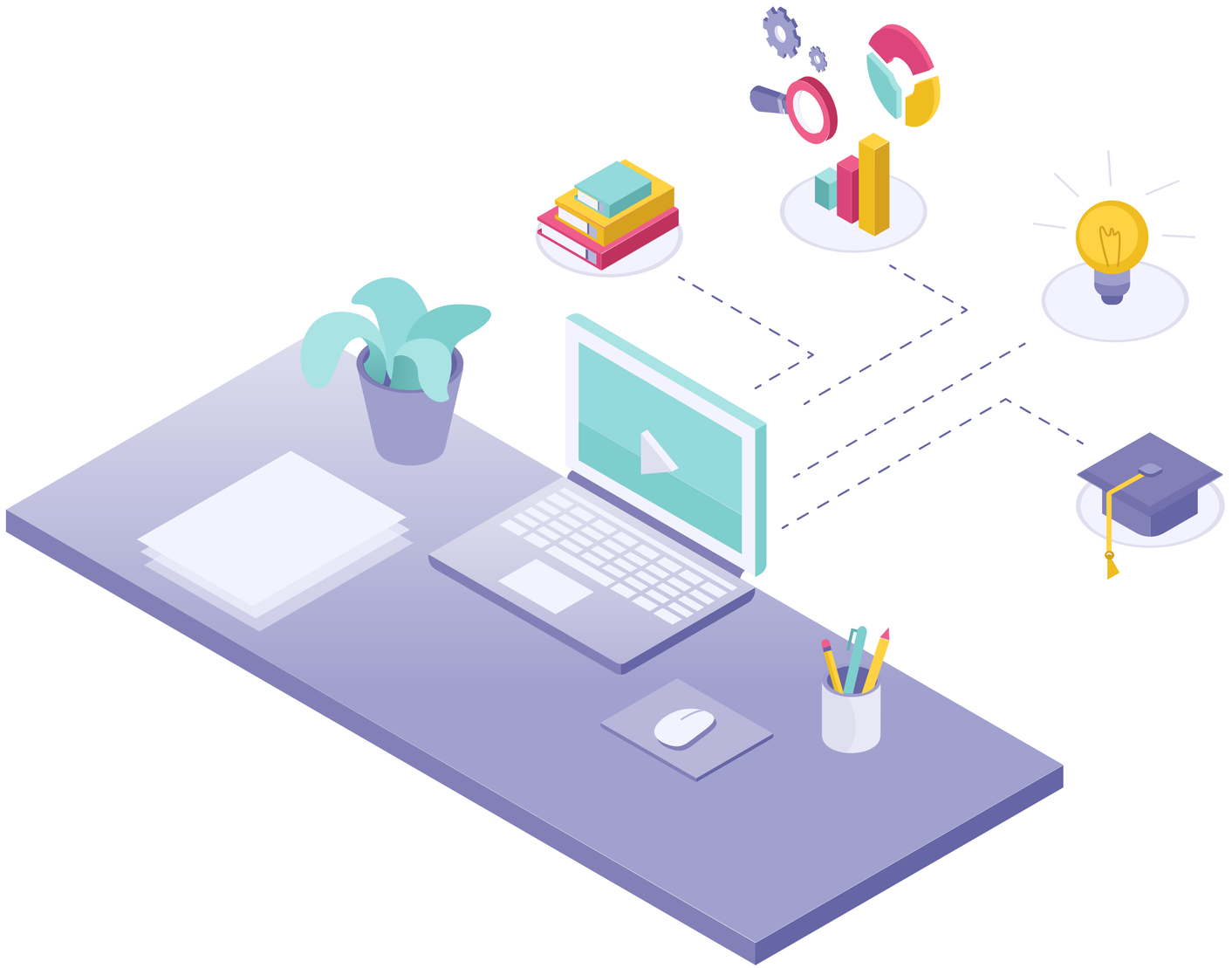


VPC Peering

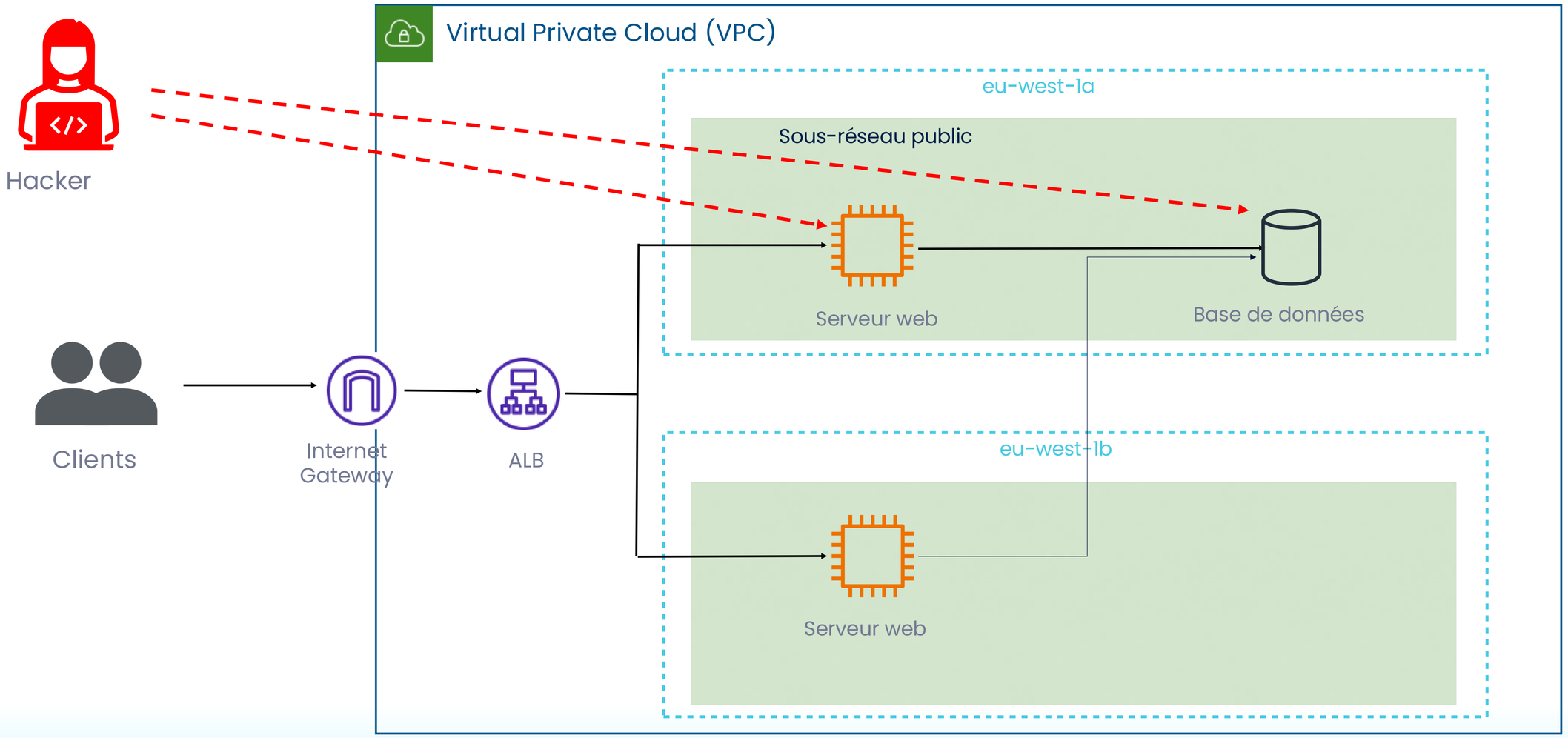


!!! Eviter les chevauchements de bloc CIDR entre VPC

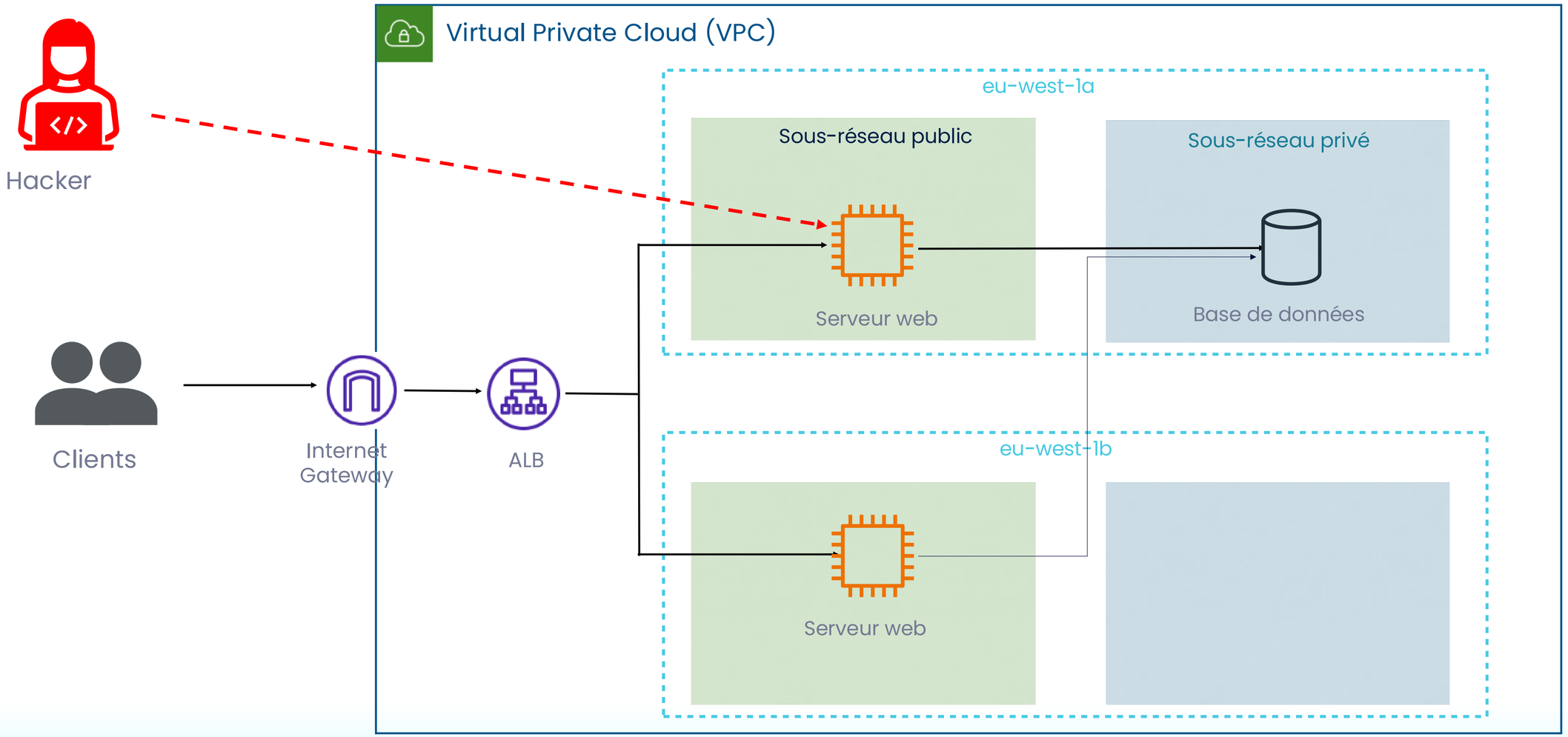
VPC Architecture



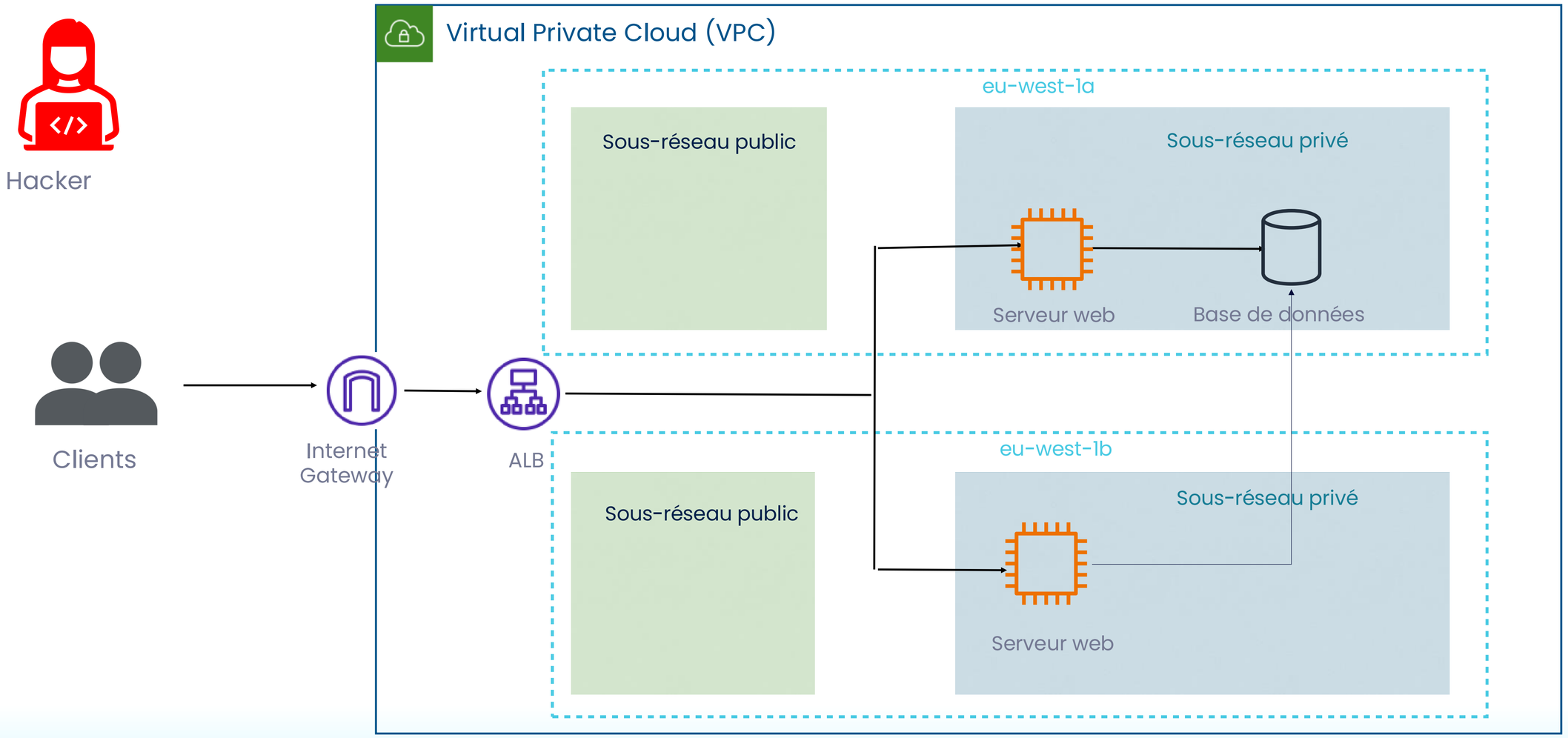
Exemple 1 : déploiement site web : Sous-reseaux publics



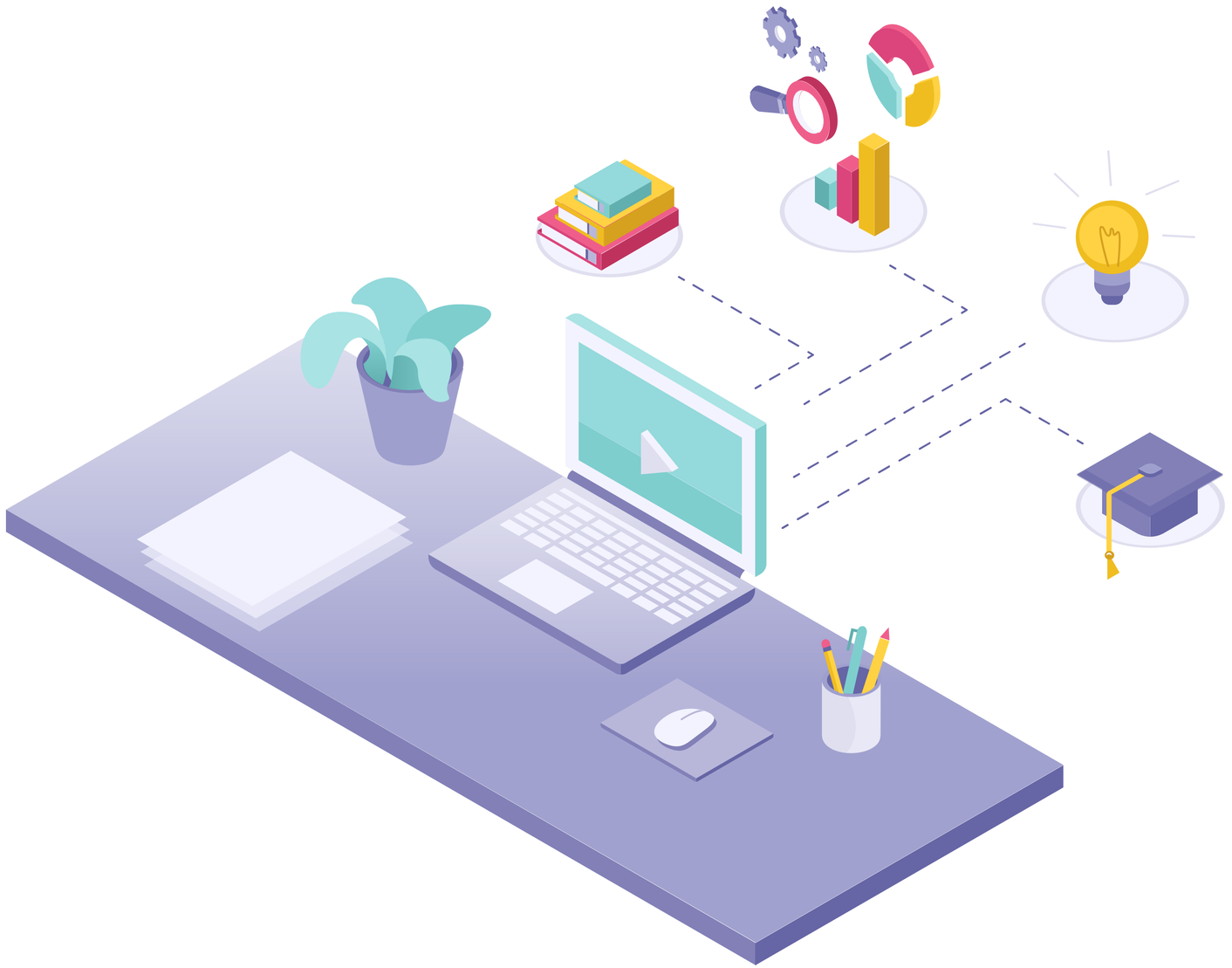
Exemple 2 : déploiement site web : Sous-reseaux publics & privés



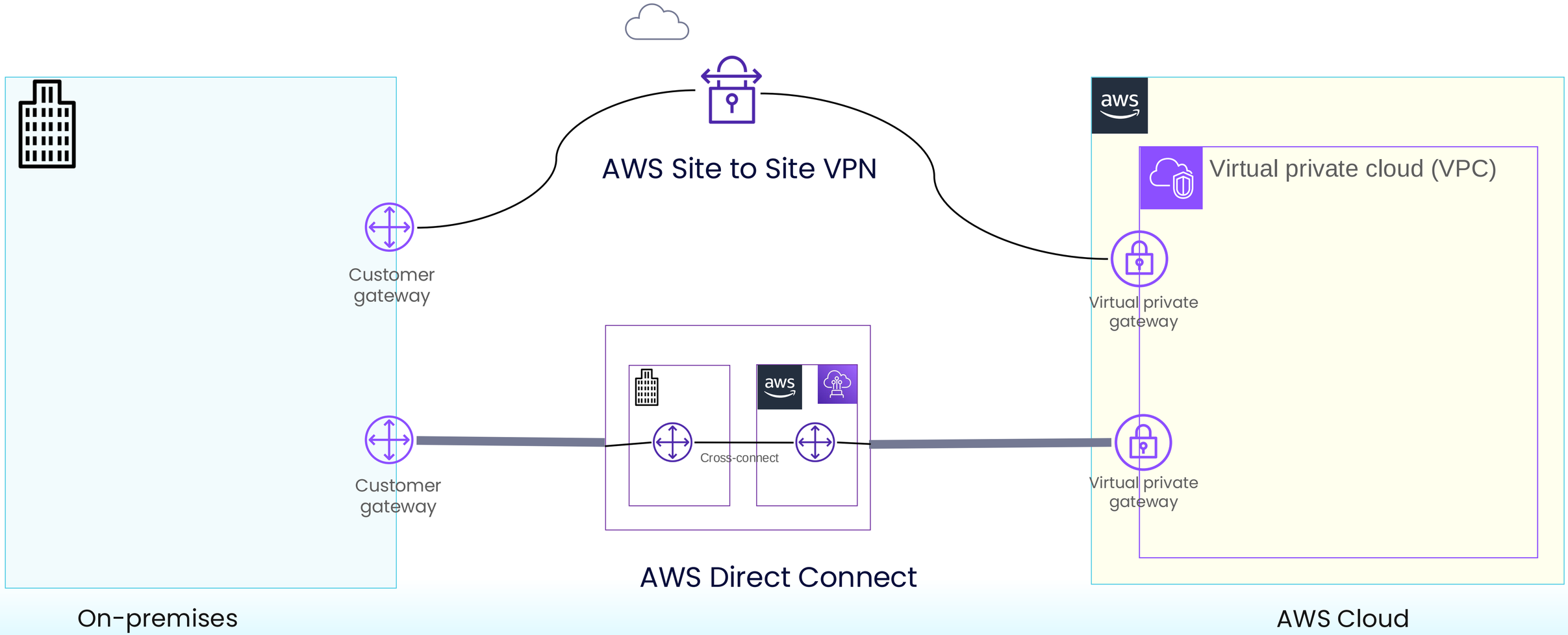
Exemple 3 : déploiement site web : Sous-reseaux privés



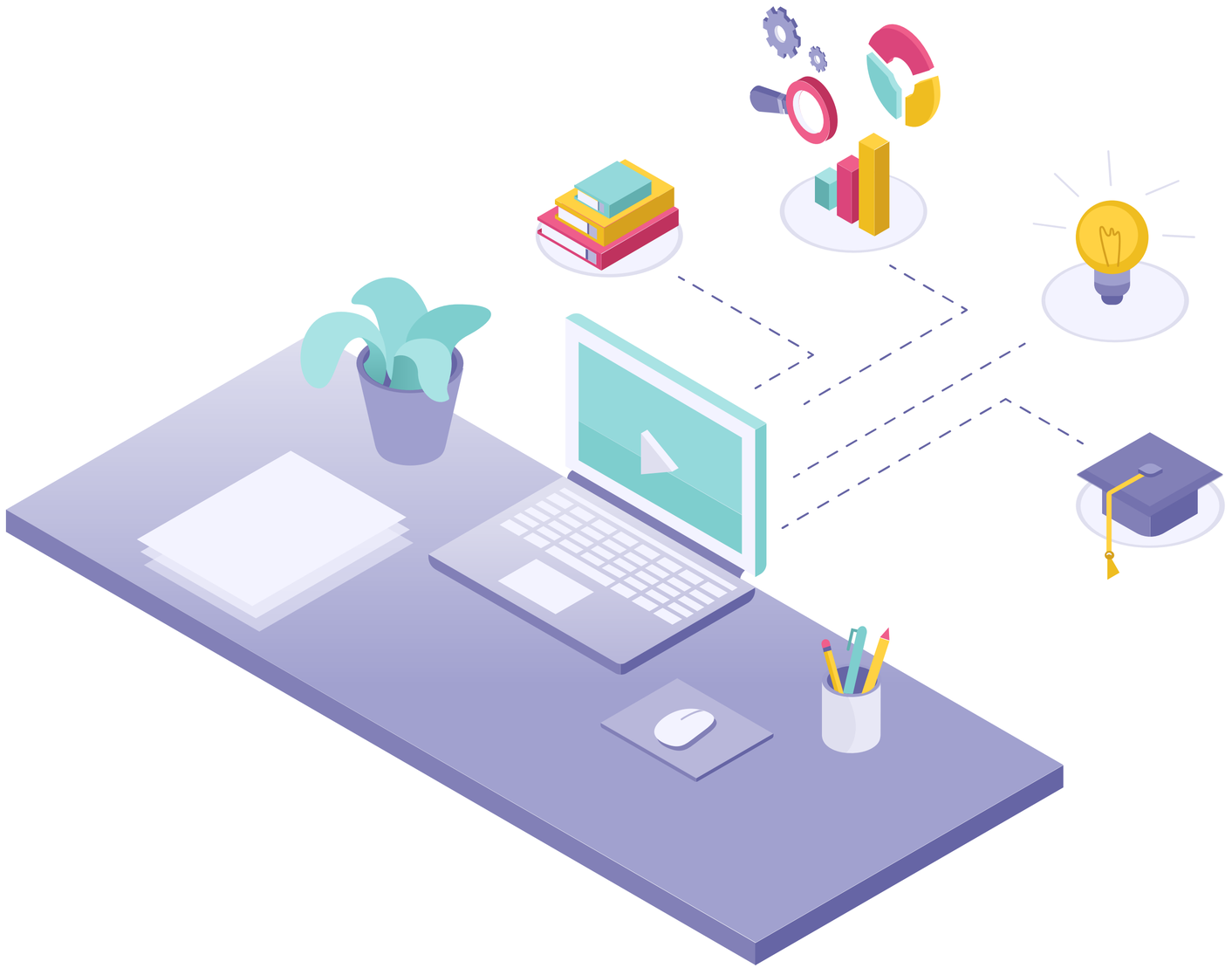
Connectivité hybride



Connectivité hybride – les différentes options



AWS Site-to-site VPN



AWS Site-to-Site VPN



Permet de créer des tunnels VPN IPSec entre

- **votre VPC** -> Composant Virtual Private Gateway
- et votre **infrastructure sur site** -> Composant Customer Gateway

Communication **chiffrée** qui passe par **Internet**

Temps de mise en place court -> **quelques heures**

Virtual Private Gateway

Point de terminaison VPN du côté Amazon

Permet d'établir une **connexion VPN** entre votre VPC et vos centres de données

Entièrement **managé par AWS**

Customer Gateway

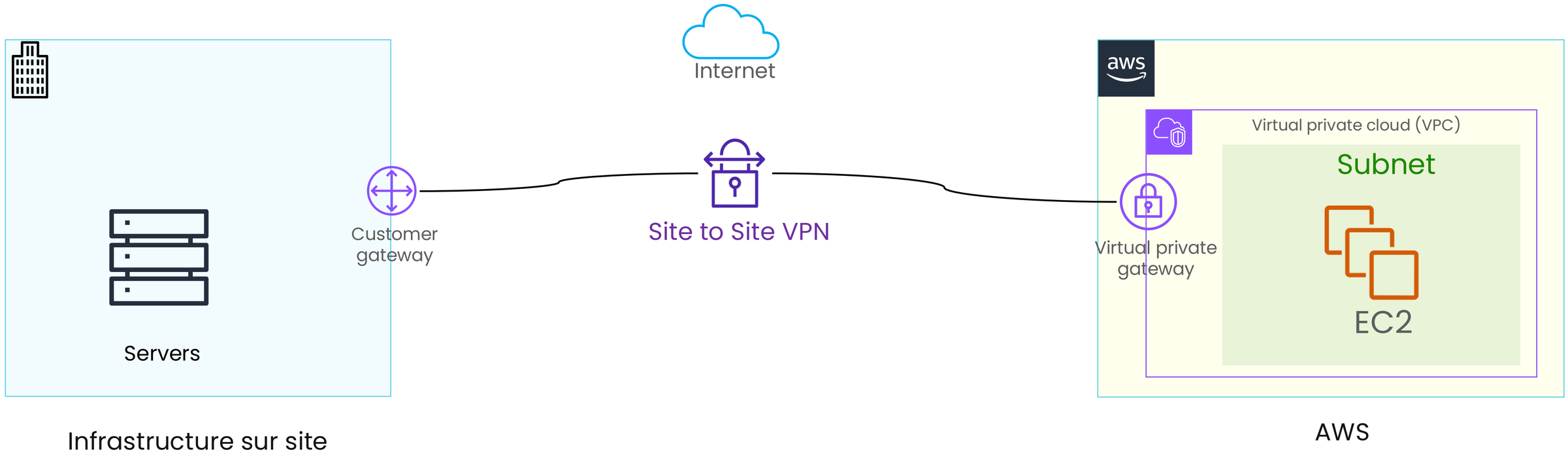
Point de terminaison VPN du côté **client**

Permet d'établir **une connexion VPN** entre votre VPC et vos centres de données

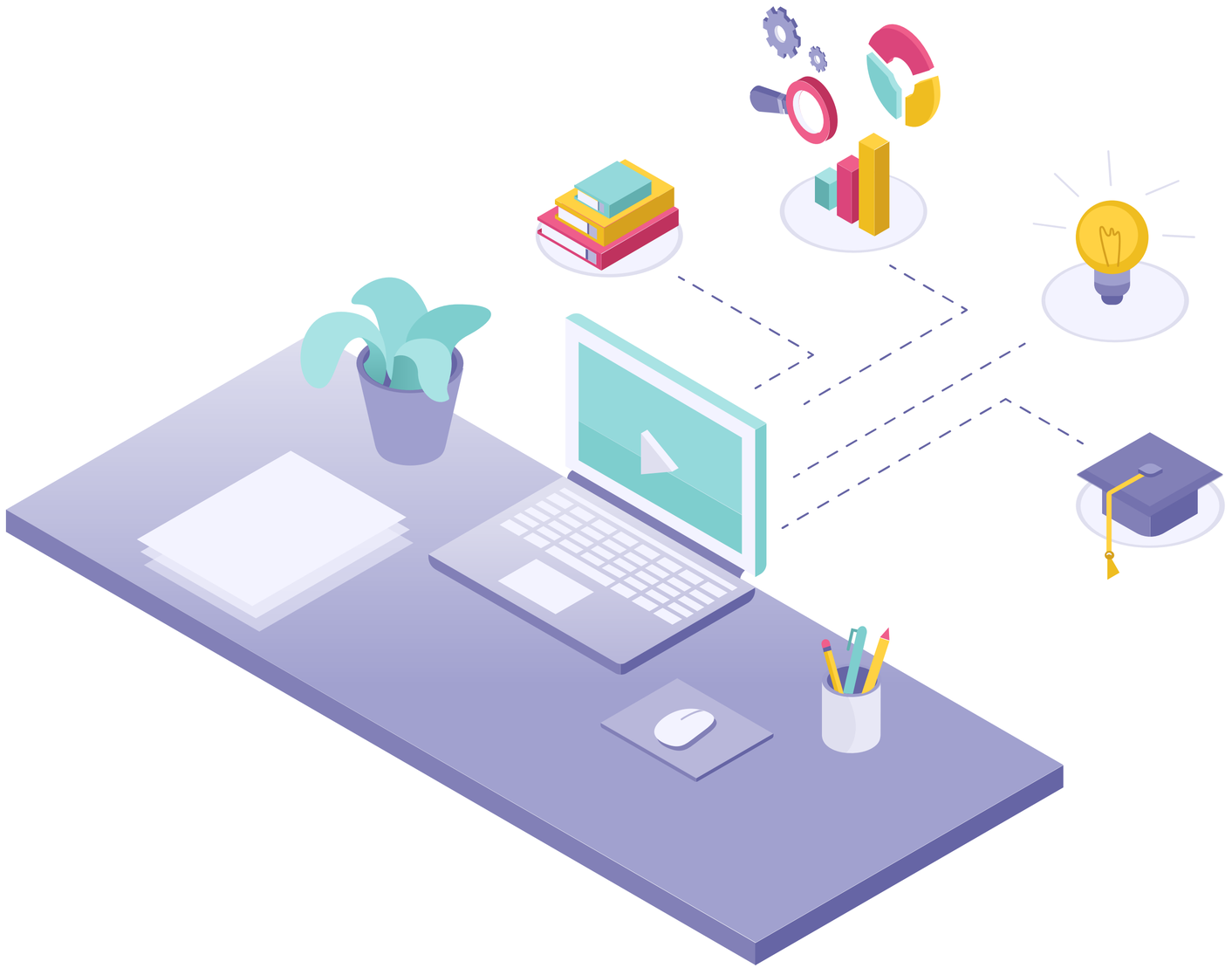
Exemple : *Routeur (Cisco, Fortinet, Juniper,...) installé sur votre site*

Entièrement sous la **responsabilité du client**

AWS Site-to-Site VPN



AWS Direct Connect



AWS Direct Connect



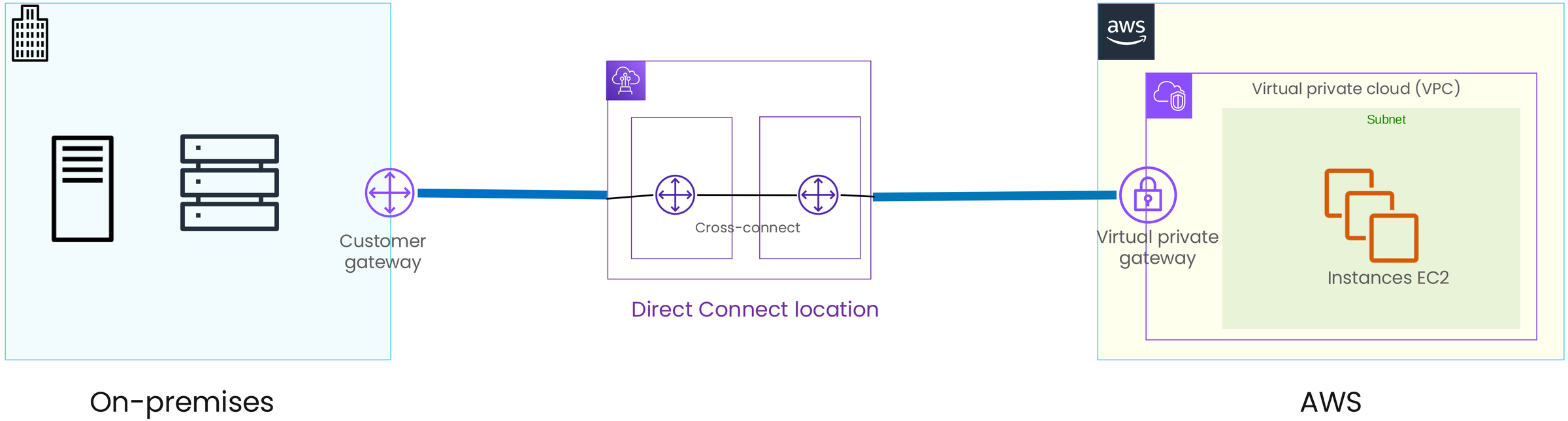
Connexion réseau privée et dédiée entre AWS et vos data centers

Lien physique qui **ne passe pas par Internet**

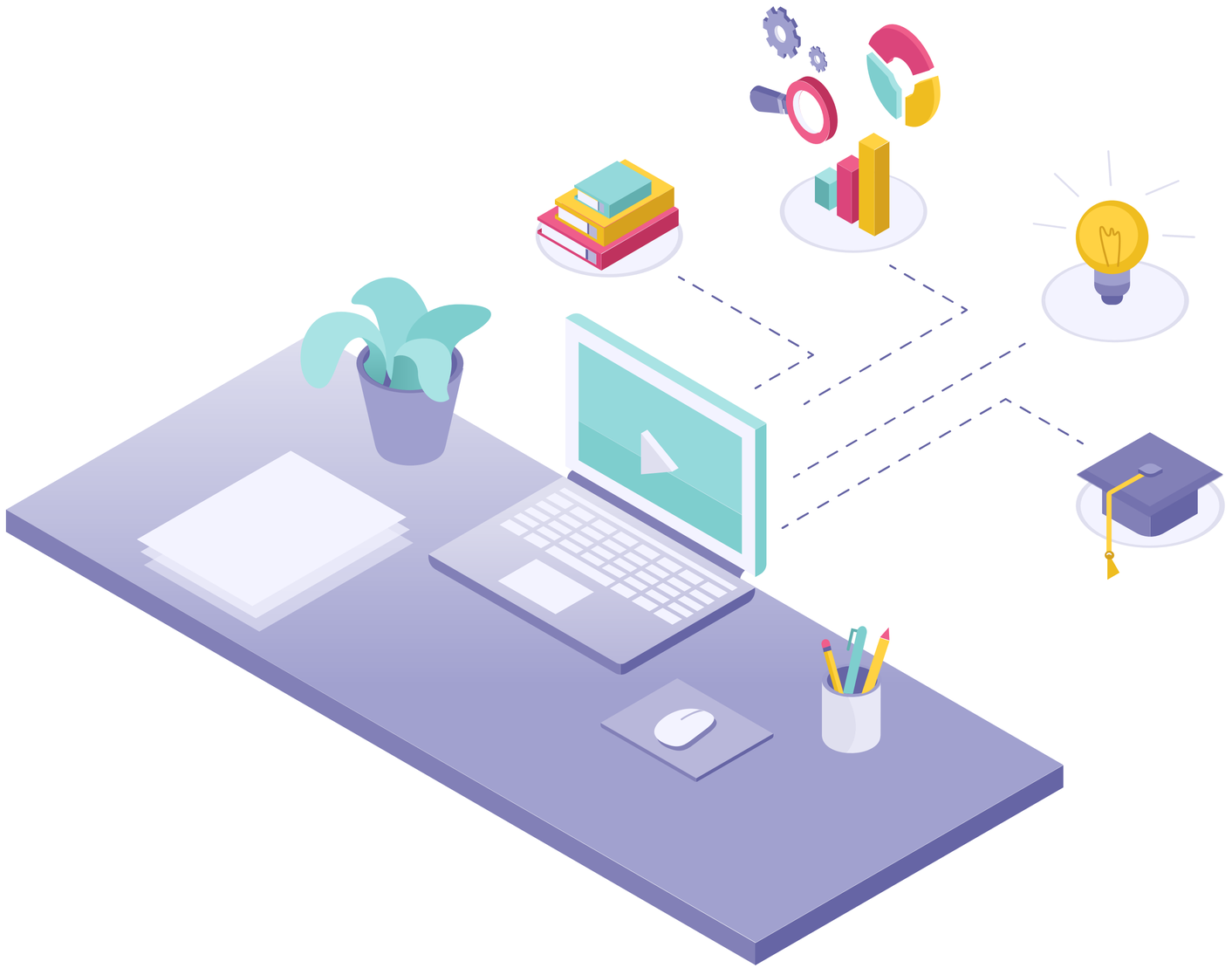
Connexion dédiée : 1 Gbit/s, 10 Gbit/s ou 100 Gbit/s

Temps de mise en place long -> **plusieurs semaines/mois**

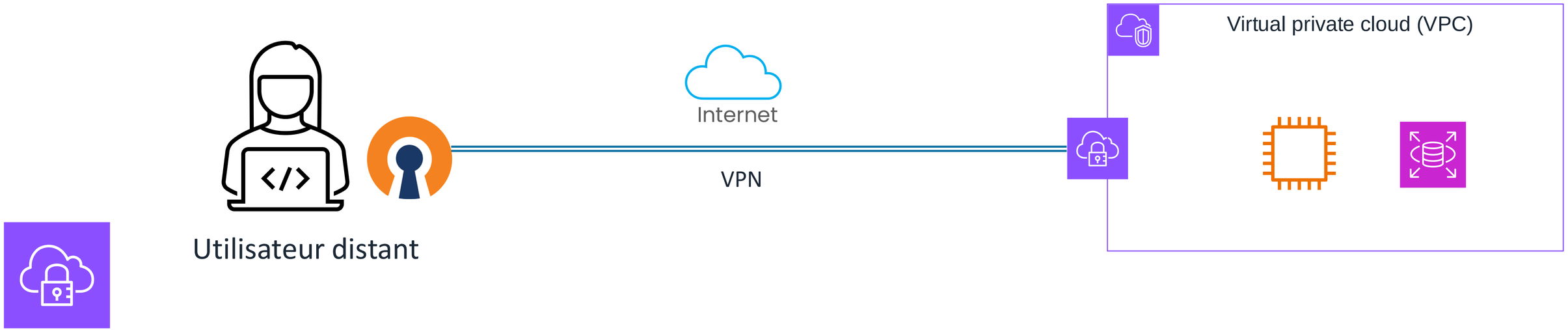
AWS Direct Connect



AWS Client VPN



AWS Client VPN

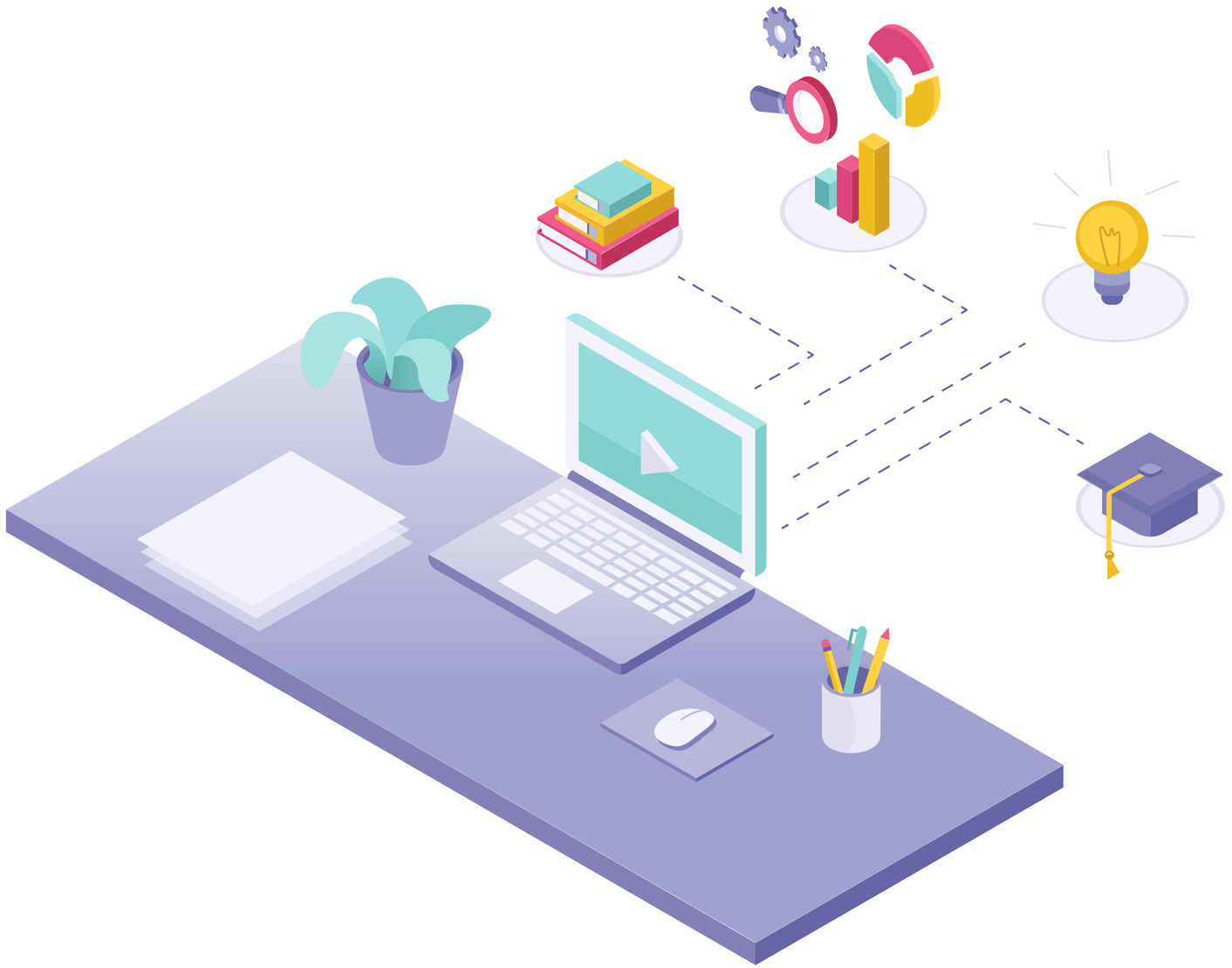


Permet aux utilisateurs de se connecter à leur VPC sur AWS via un VPN

L'utilisateur final doit télécharger un client **OpenVPN** sur son appareil

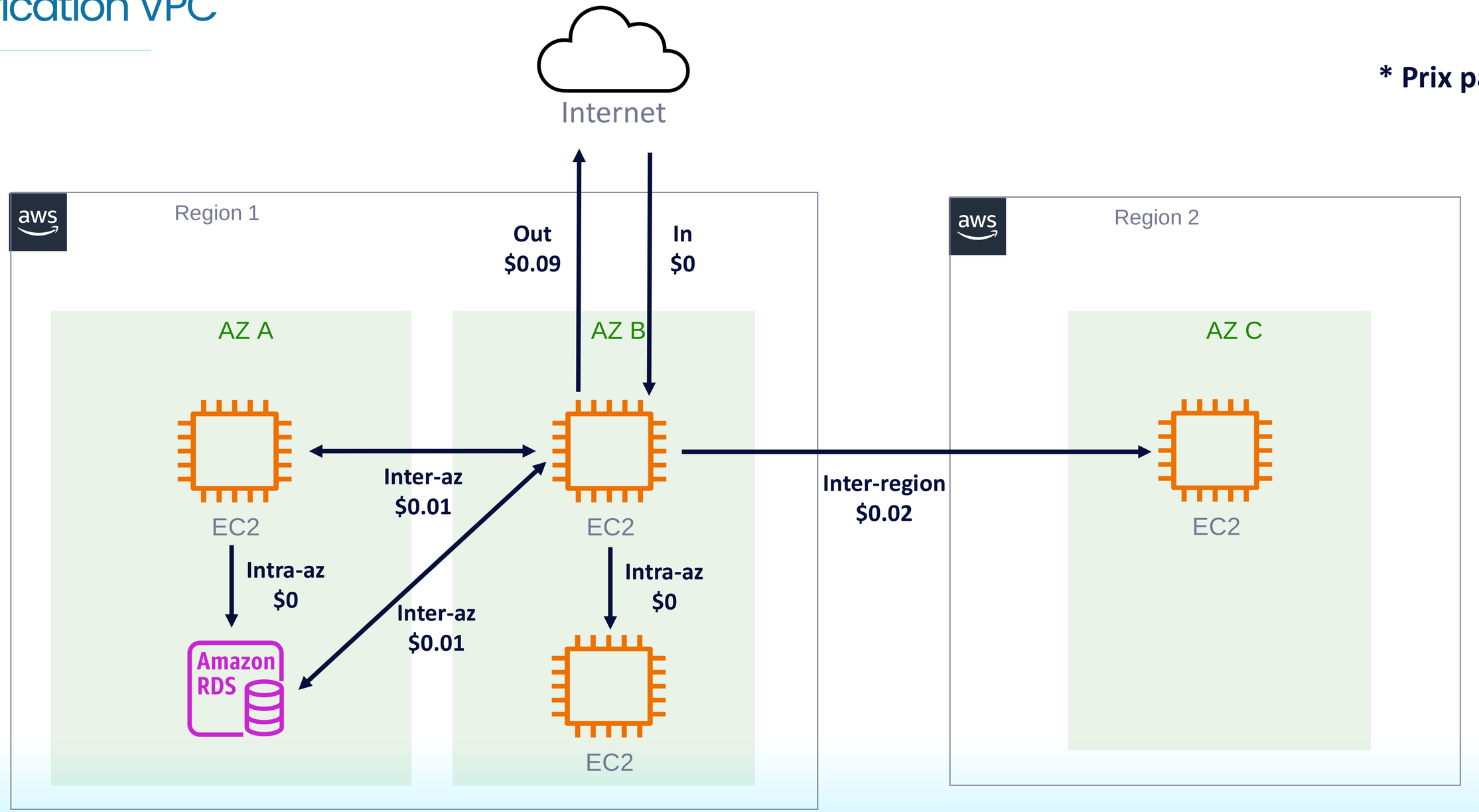
Communication **chiffrée et sécurisée** qui passe par Internet

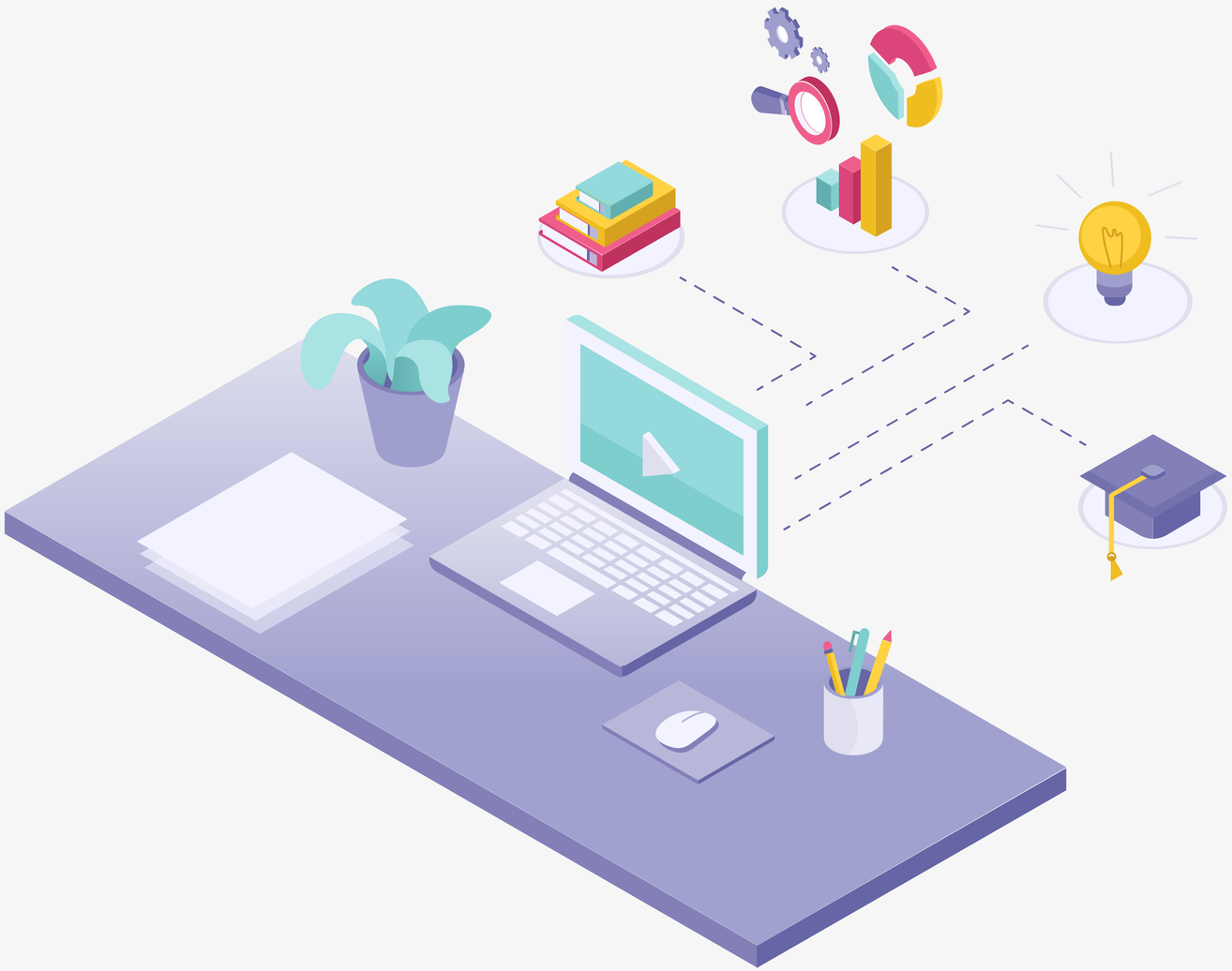
Tarification VPC



Tarification VPC

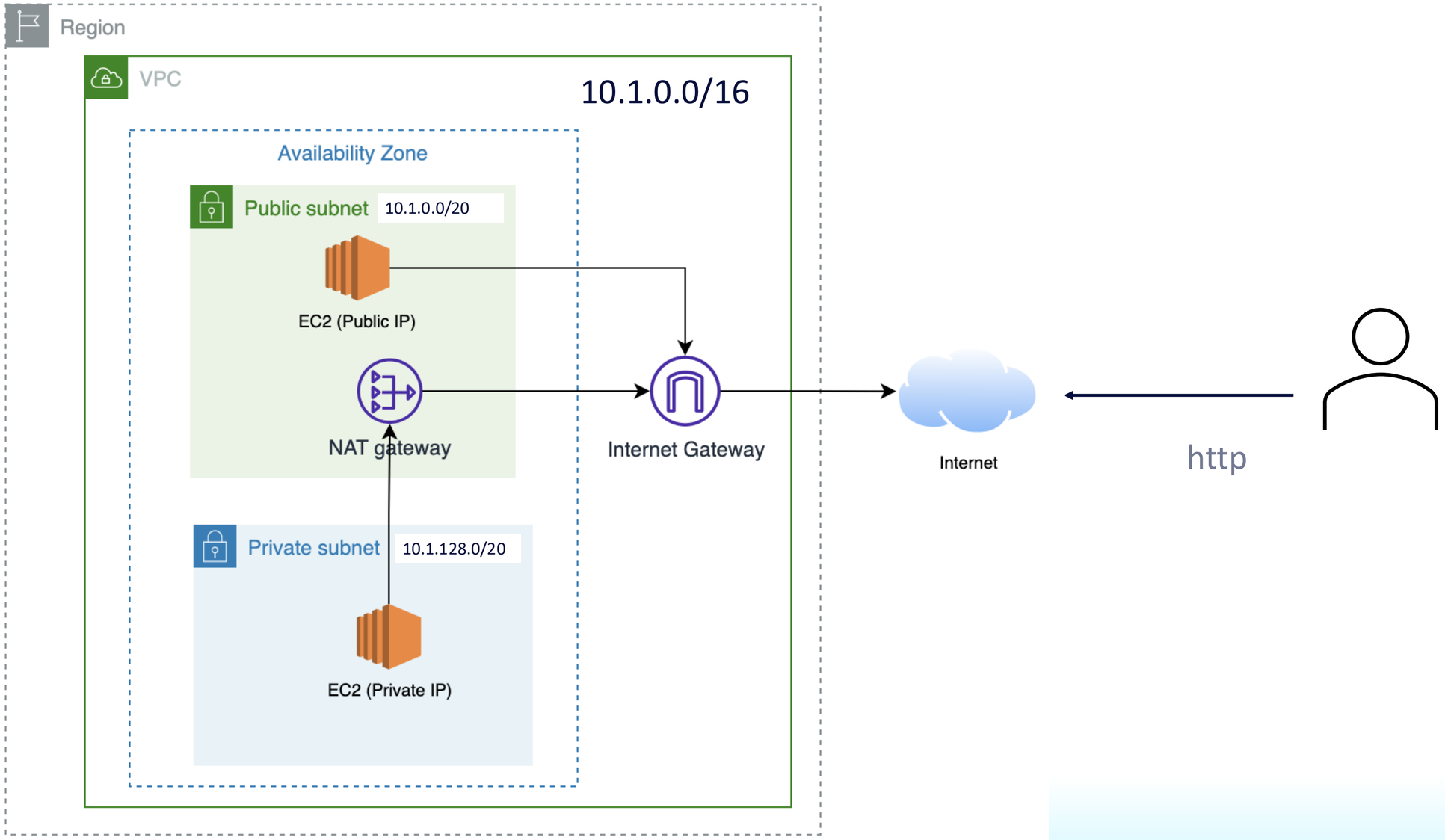
*** Prix par Go**



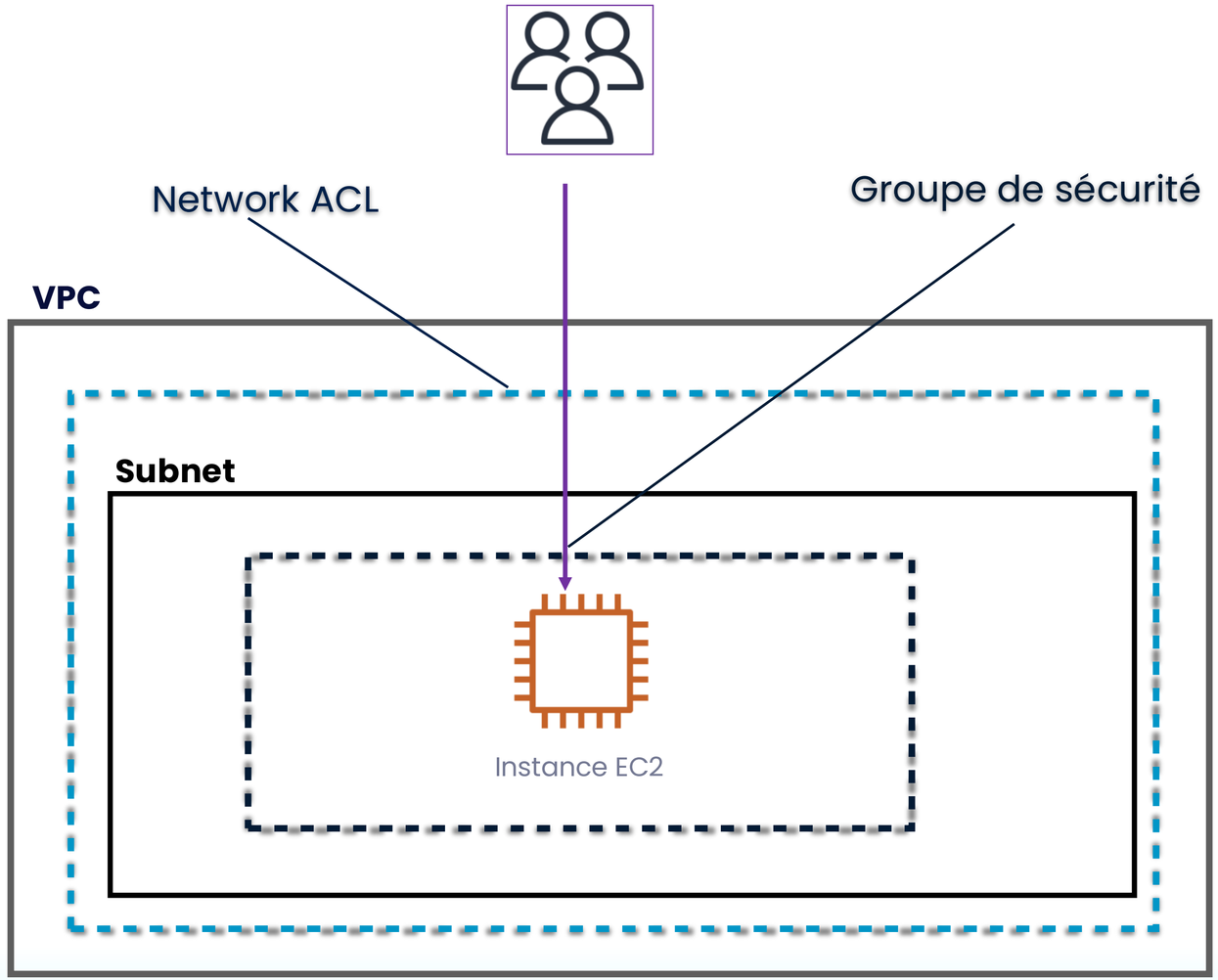


FIN DU MODULE

Lab Sous reseau public vs privé



Lab NACL vs Groupe de sécurité



Lab NACL vs Groupe de sécurité

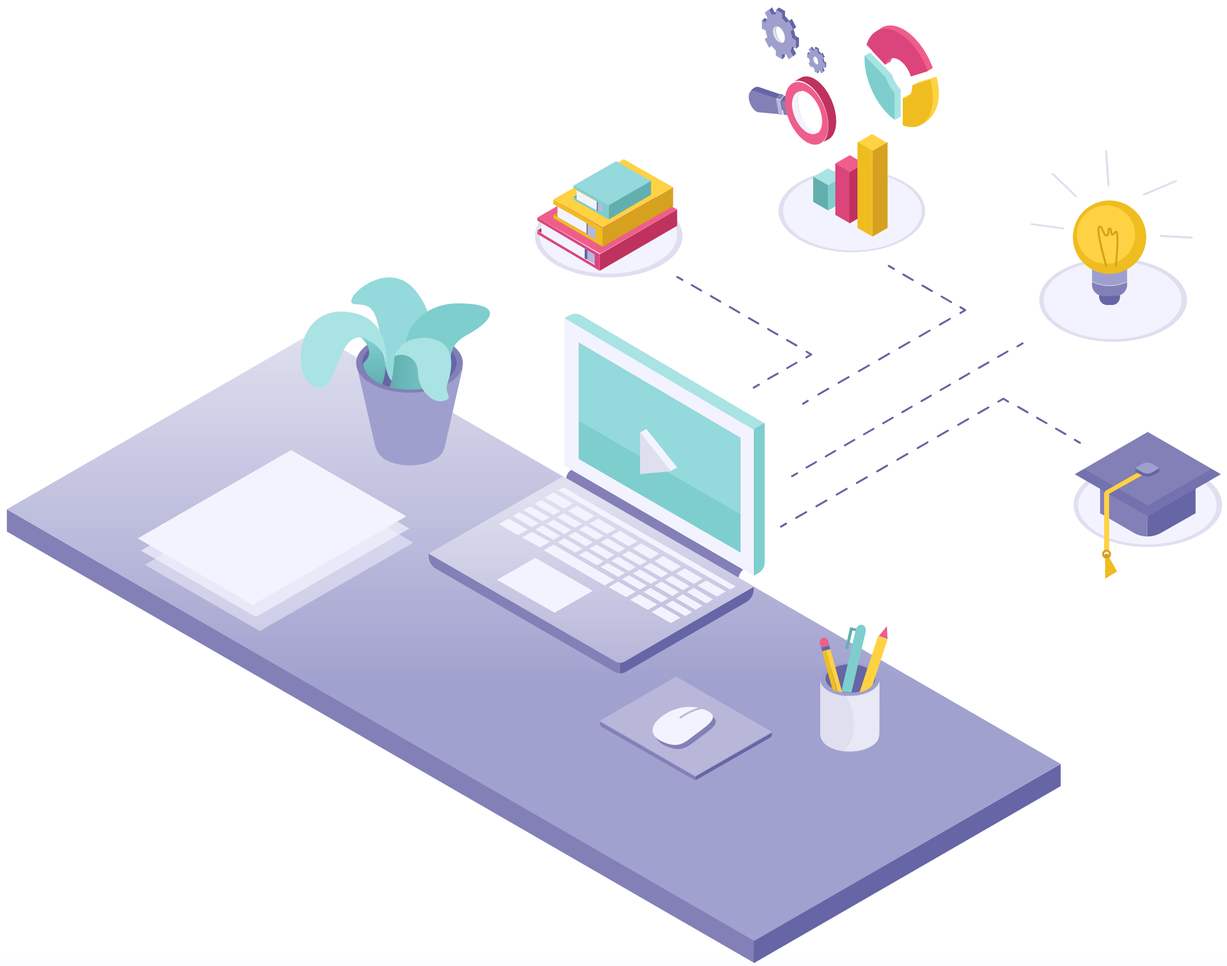
1. Explorer le NACL d’un subnet du VPC par défaut
2. Lancer 1 instance EC2 avec 1 site web dans le VPC par défaut
3. Modifier le NACL pour bloquer le trafic HTTP
4. Tester l’accès au site web

Lab Sous reseau public vs privé

1. Créer un VPC avec des subnets public et privés
2. Lancer un site web sur 1 instance EC2 dans un subnet **public**
3. Lancer un site web sur 1 instance EC2 dans un subnet **privé**
4. Tester les accès aux sites web (***public*** *vs* ***privé***)

Module 6 : Mise en reseau & Diffusion de contenus

Exécutez chaque application sur un réseau mondial sécurisé et fiable



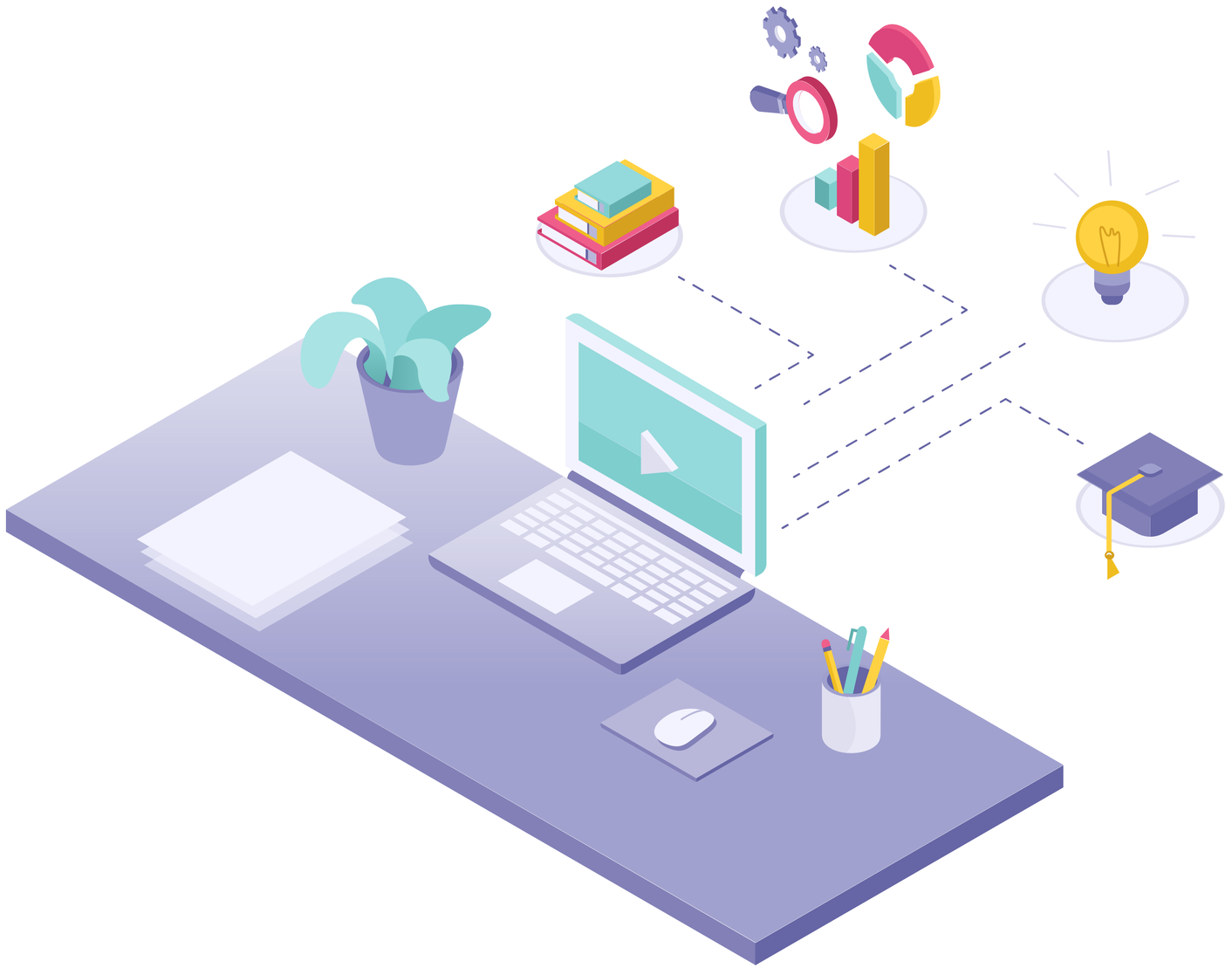
Comment gérer le DNS avec le Cloud AWS ?

Quels sont les services de diffusion de contenu ?

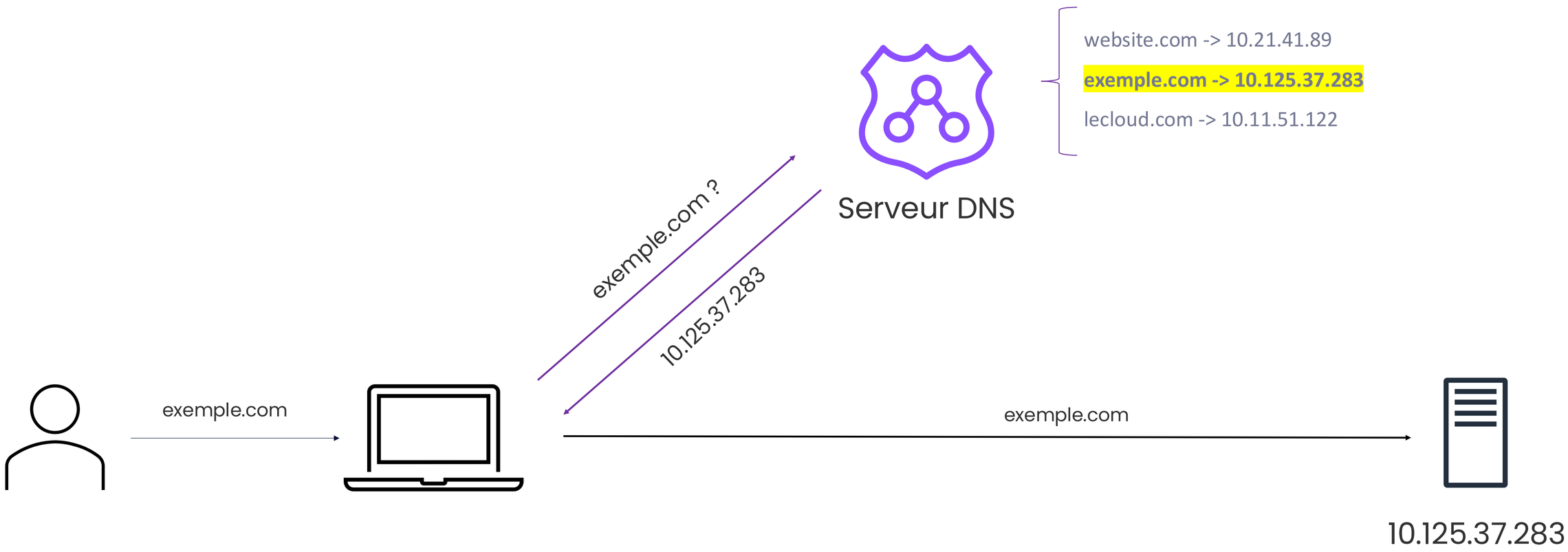
Quelles sont les options de déploiement à la périphérie des utilisateurs ?



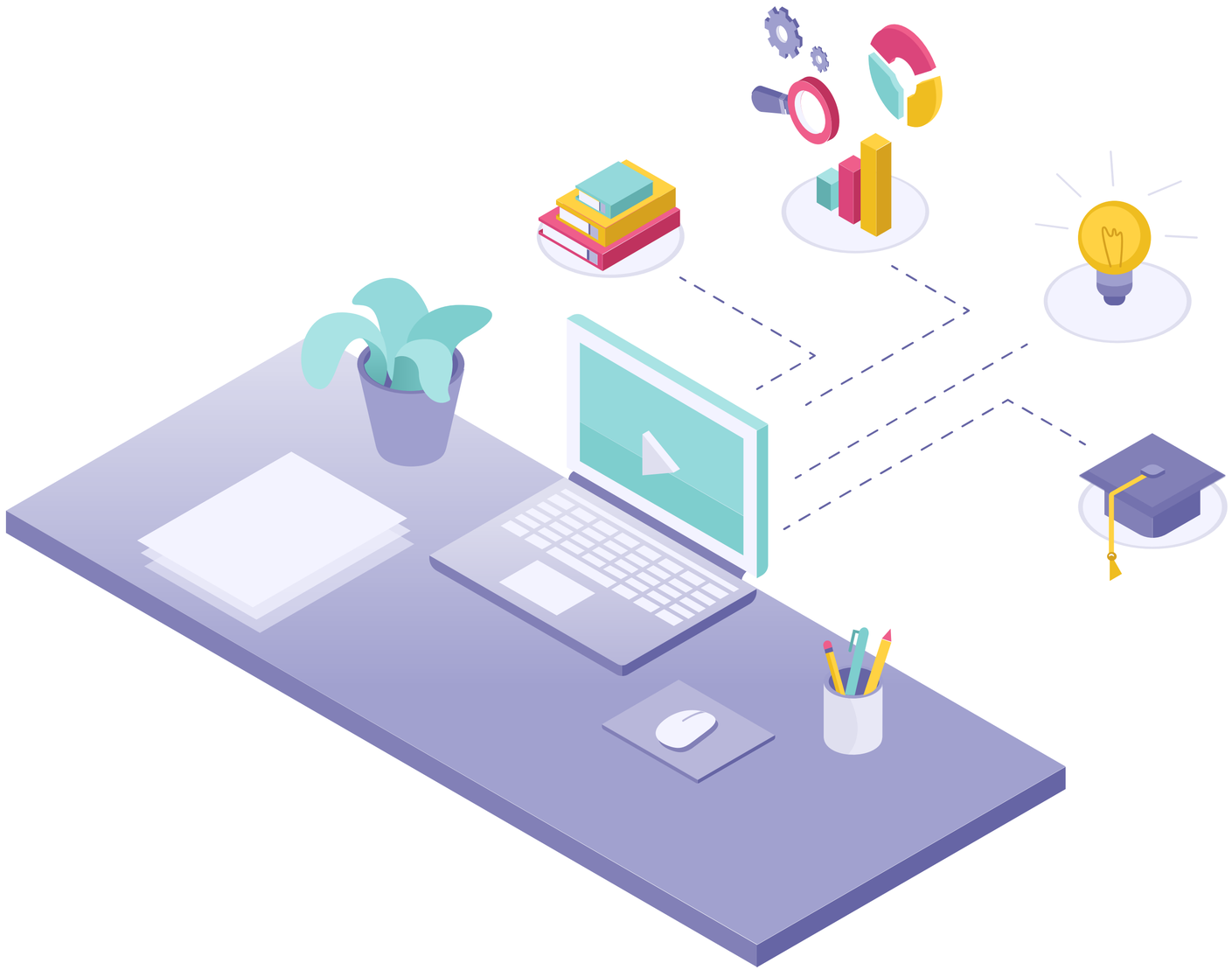
DNS 101
(Domain Name System)



DNS 101


website.com -> 10.21.41.89
exemple.com -> 10.125.37.283
lecloud.com -> 10.11.51.122
Serveur DNS
exemple.com ?
10.125.37.283
exemple.com
exemple.com
10.125.37.283

Amazon Route 53



Amazon Route 53



Service de gestion de *noms de domaines* (**DNS**)

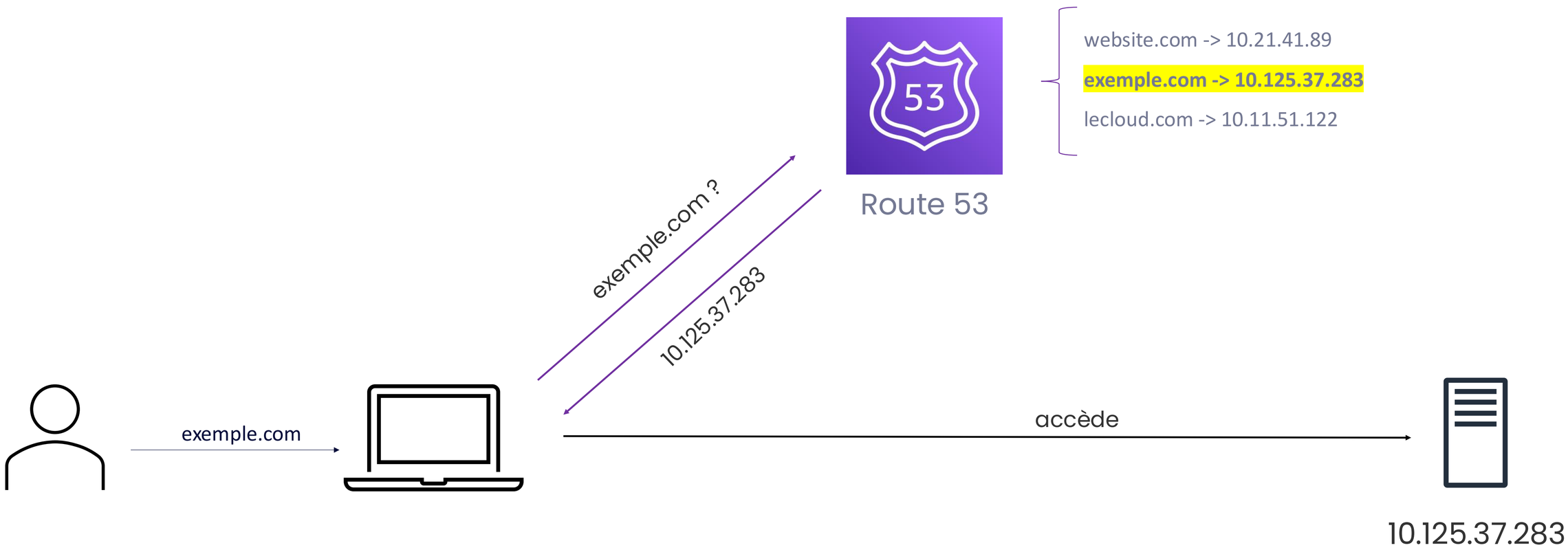
DNS publics (Internet) et privés (VPC)

Tarification à l'usage (zones hébergées + requêtes)

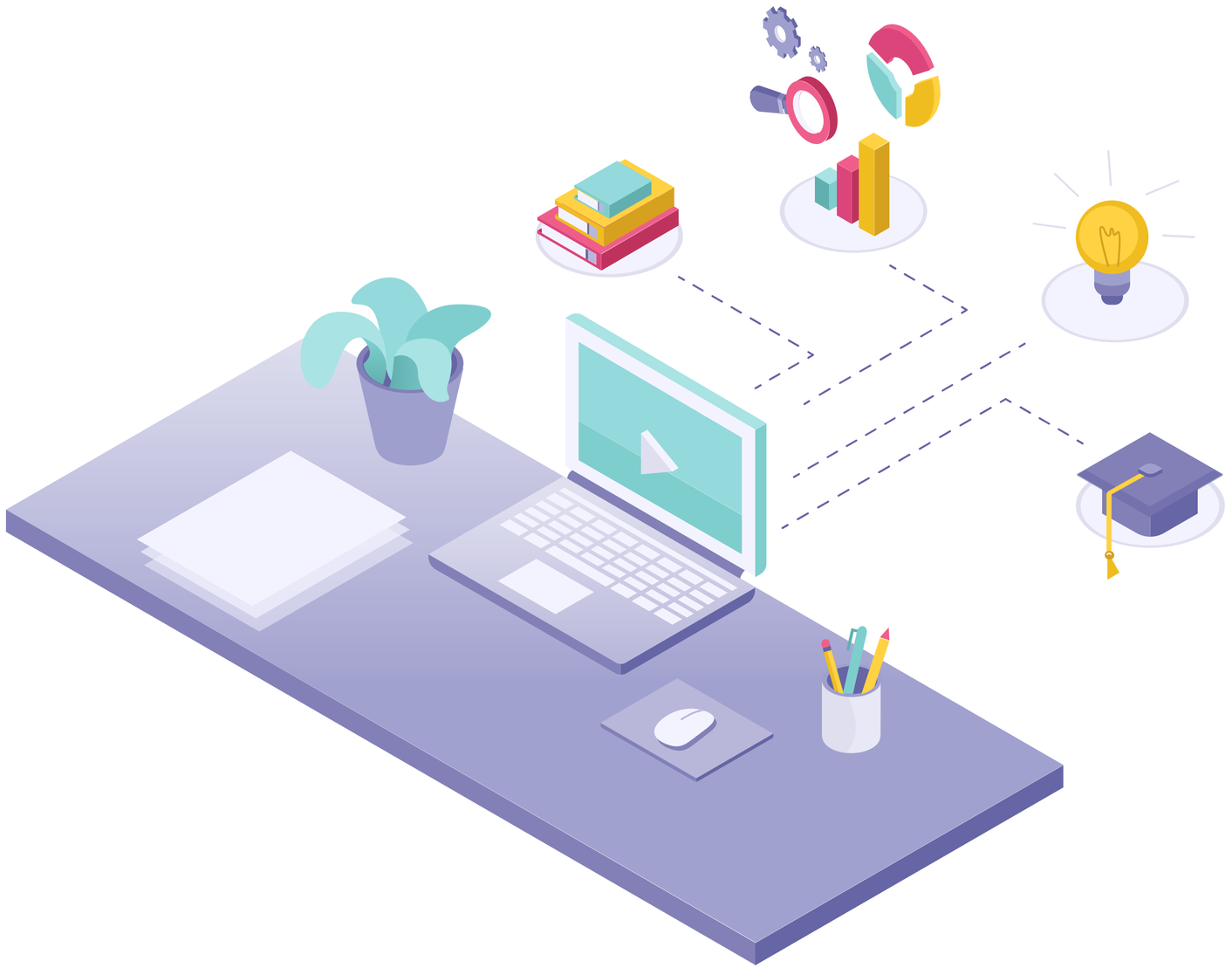
Fonctionnalités

- **Enregistrement ou transfert** de noms de domaine
- **Routage** DNS (politiques, *records*,..)
- **Health check et surveillance** de vos applications

Exemple avec Amazon Route 53



Fonctionnalités Amazon Route 53



Enregistrer un nom de domaine

1

Rechercher un domaine

Vérifier la disponibilité d'un domaine

exemple-2567.com

Rechercher

2

Résultat de la recherche

Domaine	Prix/année	
exemple-2567.com Correspondance exacte	13.00 USD	Sélectionner

3

Domaines sélectionnés (1/5)

Frais d'enregistrement de domaine

exemple-2567.com
13.00 USD

Retirer

Sous-total : **13.00 USD**

Les frais d'enregistrement du domaine affichés sont pour un an. Vous pouvez modifier la durée sur la page suivante.

Passer au paiement

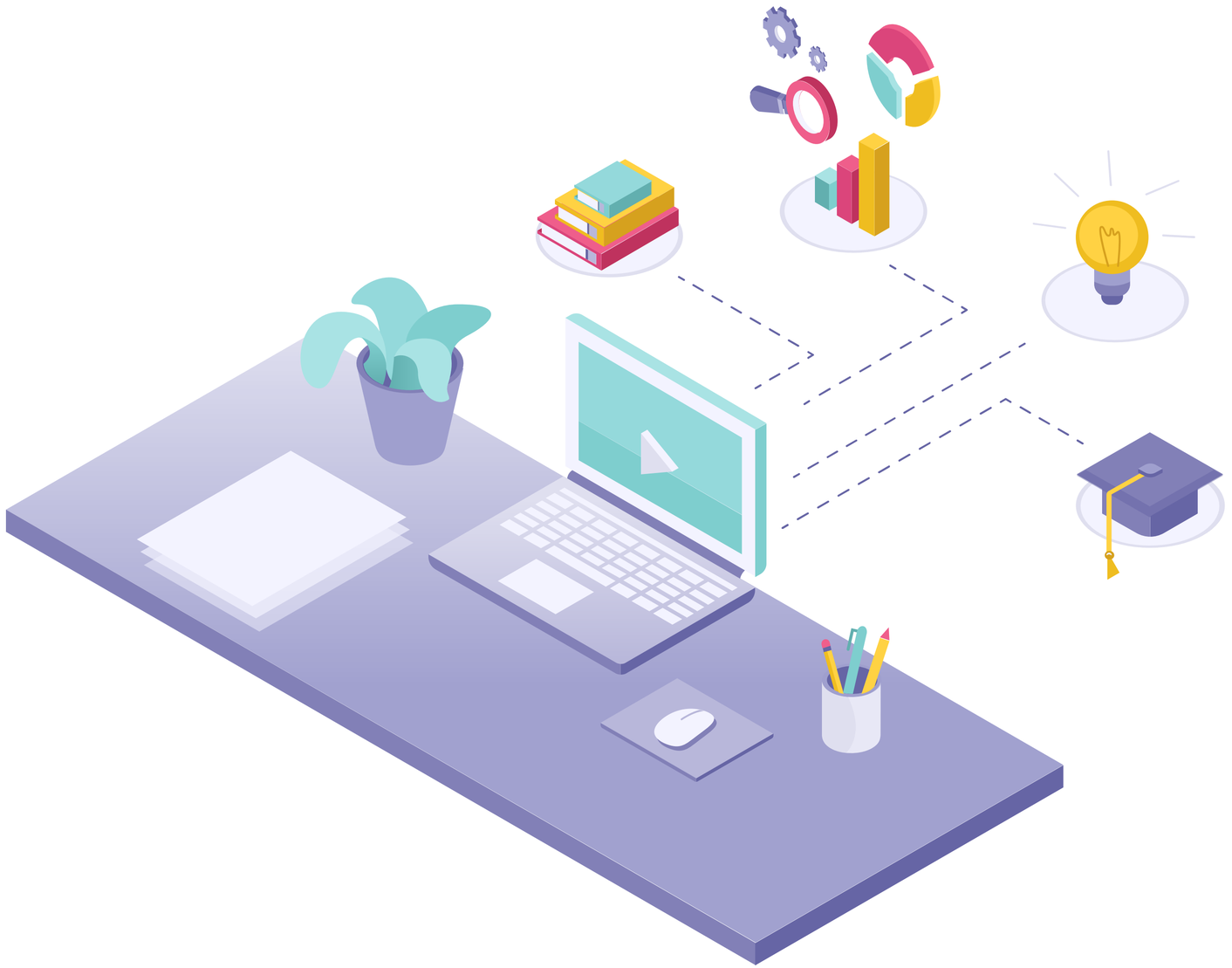
Vérifications d'état



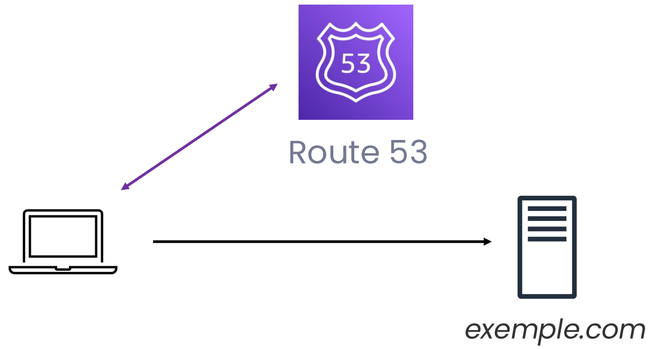
Surveille une ressource : application web, load balancer, Alarme CloudWatch

En cas de panne : Notification ou Failover vers une autre ressource

Stratégie de routage Route 53



Stratégie de routage



En anglais : ***Routing Policy***

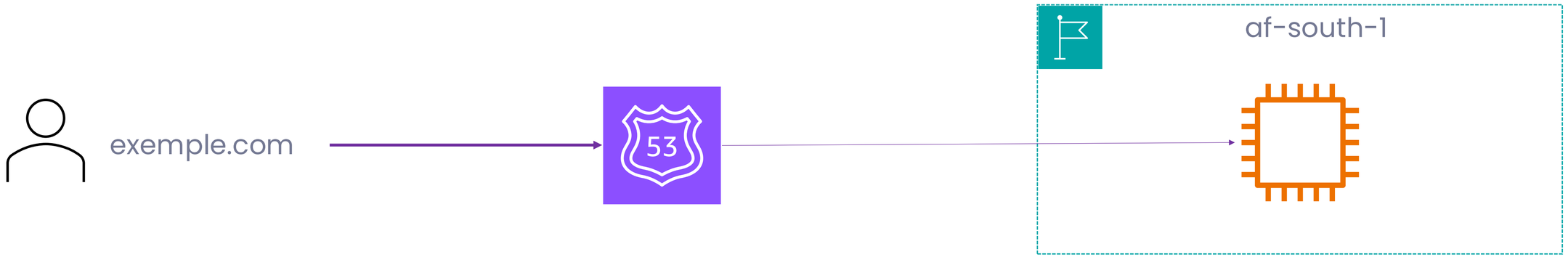
Détermine la **façon** dont Route 53 répond aux requêtes DNS

Plusieurs stratégies sont supportées :

- Simple routing
- Failover routing
- Latency routing
- Weighted routing
- Geolocation routing

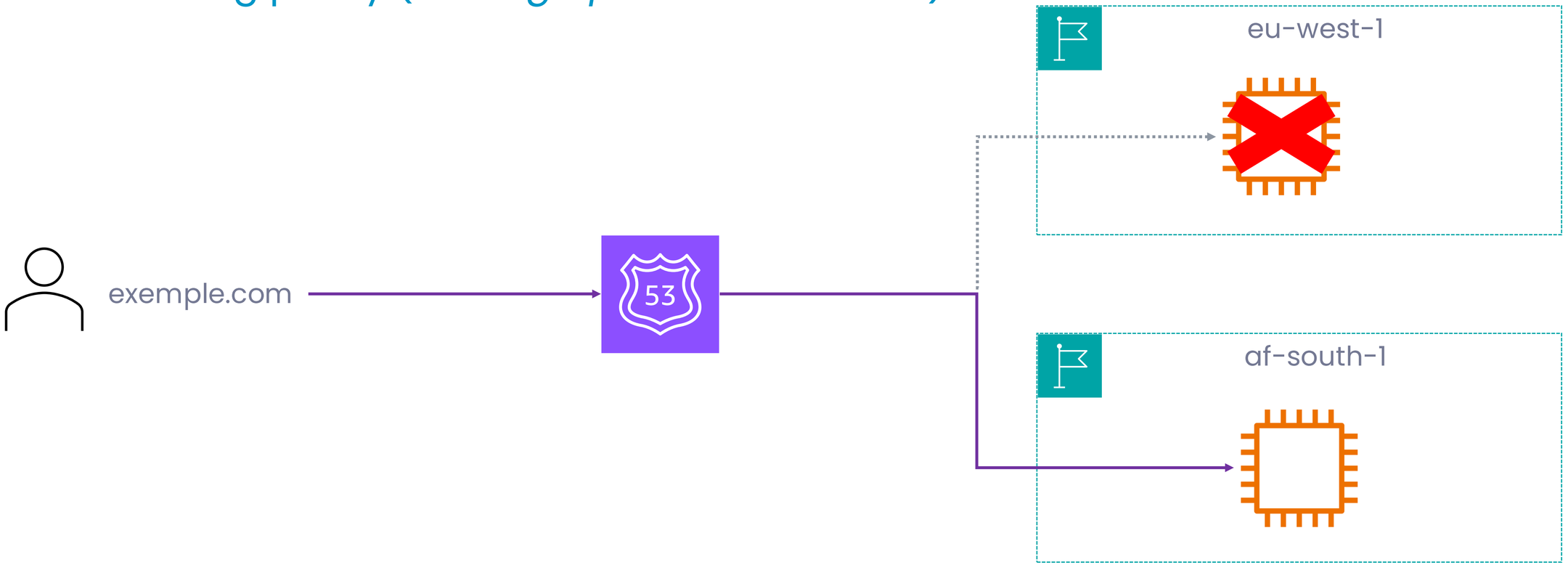
Amazon Route 53 : Stratégies de routage

Simple routing policy (*Routage simple*)



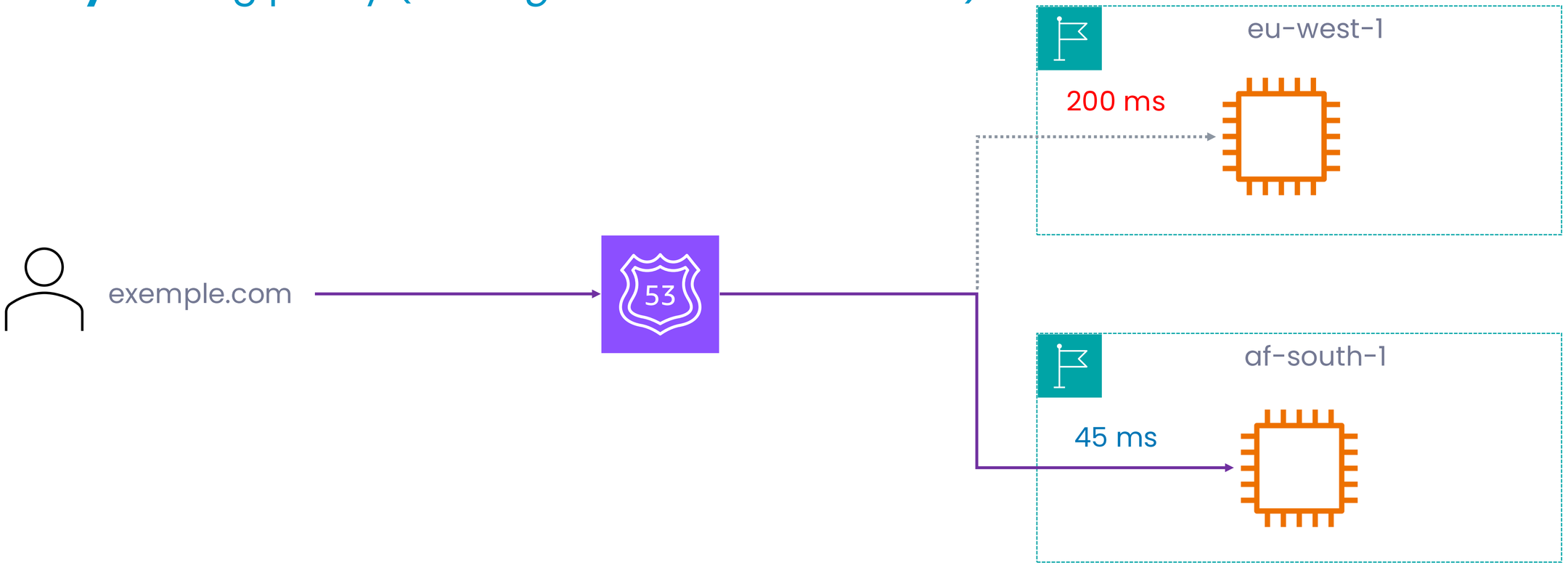
Amazon Route 53 : Stratégies de routage

Failover routing policy (*Routage par basculement*)



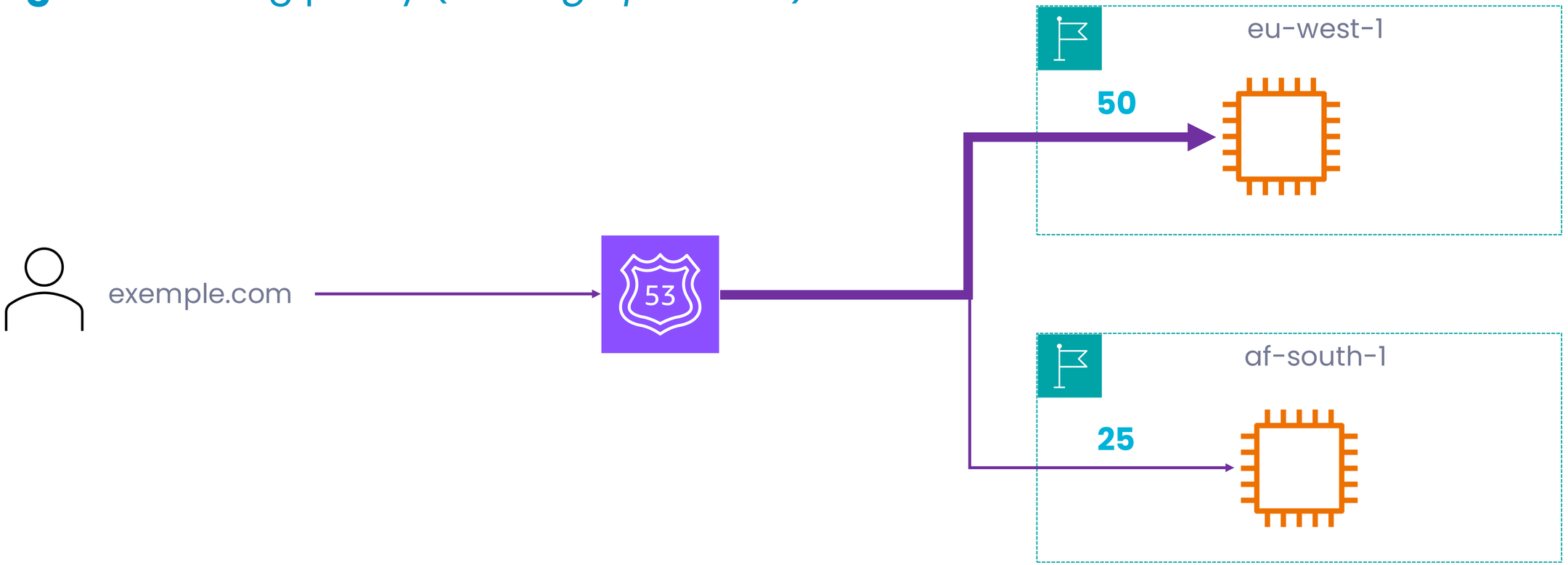
Amazon Route 53 : Stratégies de routage

Latency routing policy (*Routage basé sur la latence*)



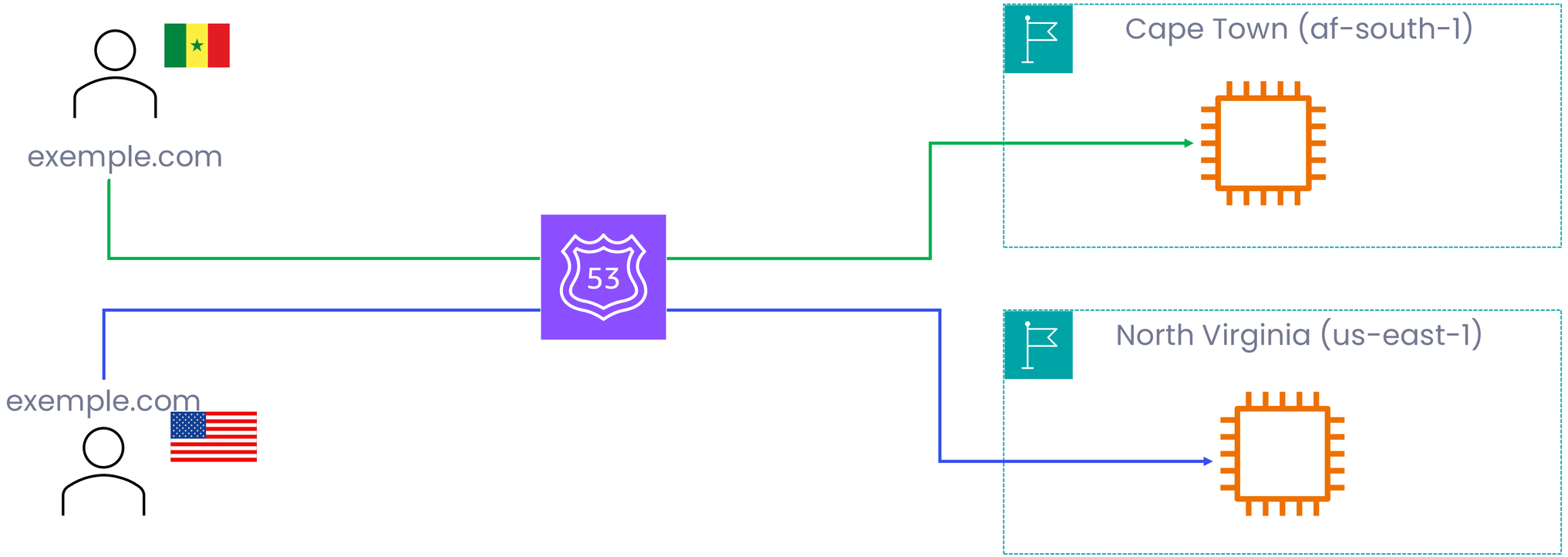
Amazon Route 53 : Stratégies de routage

Weighted routing policy (*Routage pondéré*)

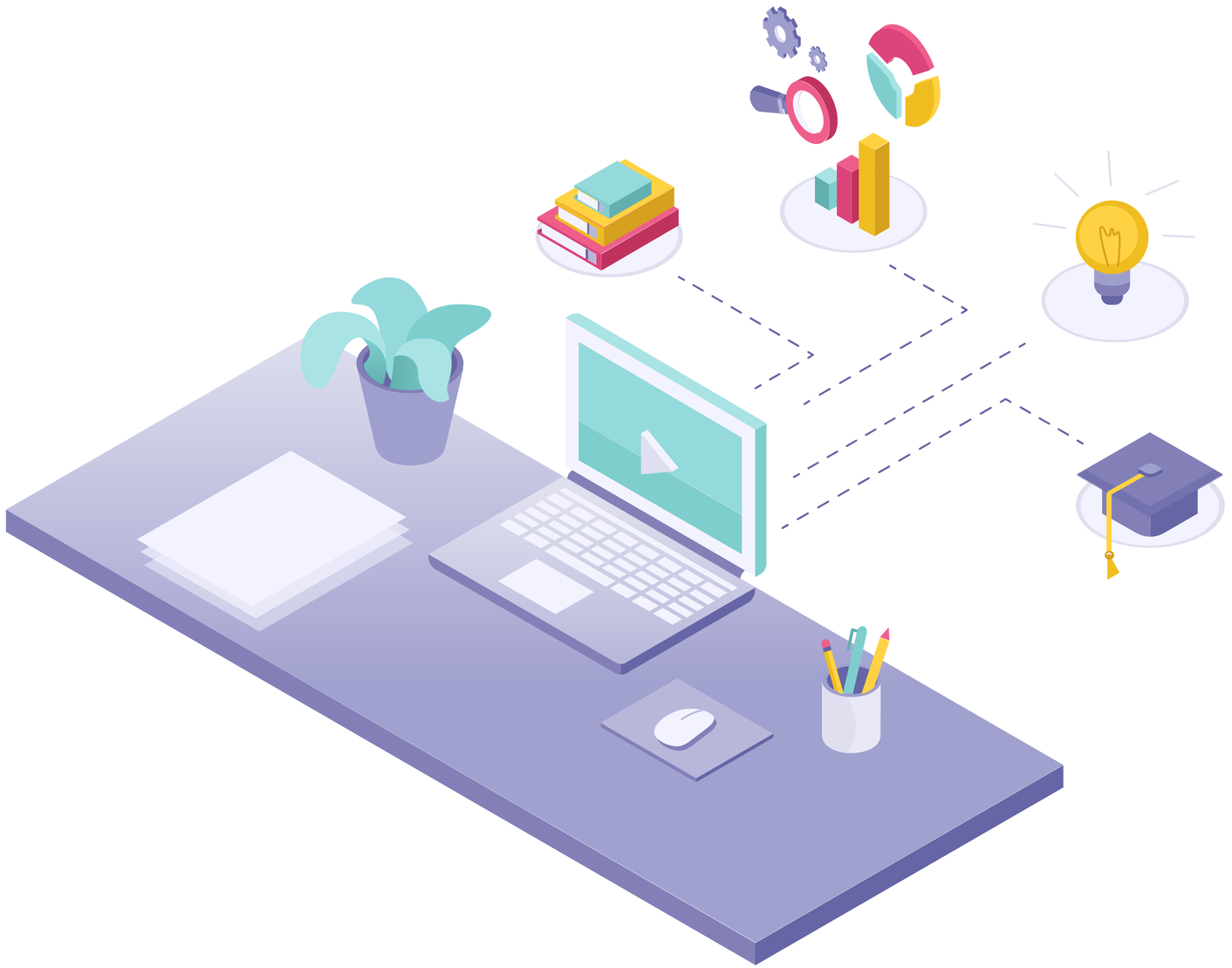


Amazon Route 53 : Stratégies de routage

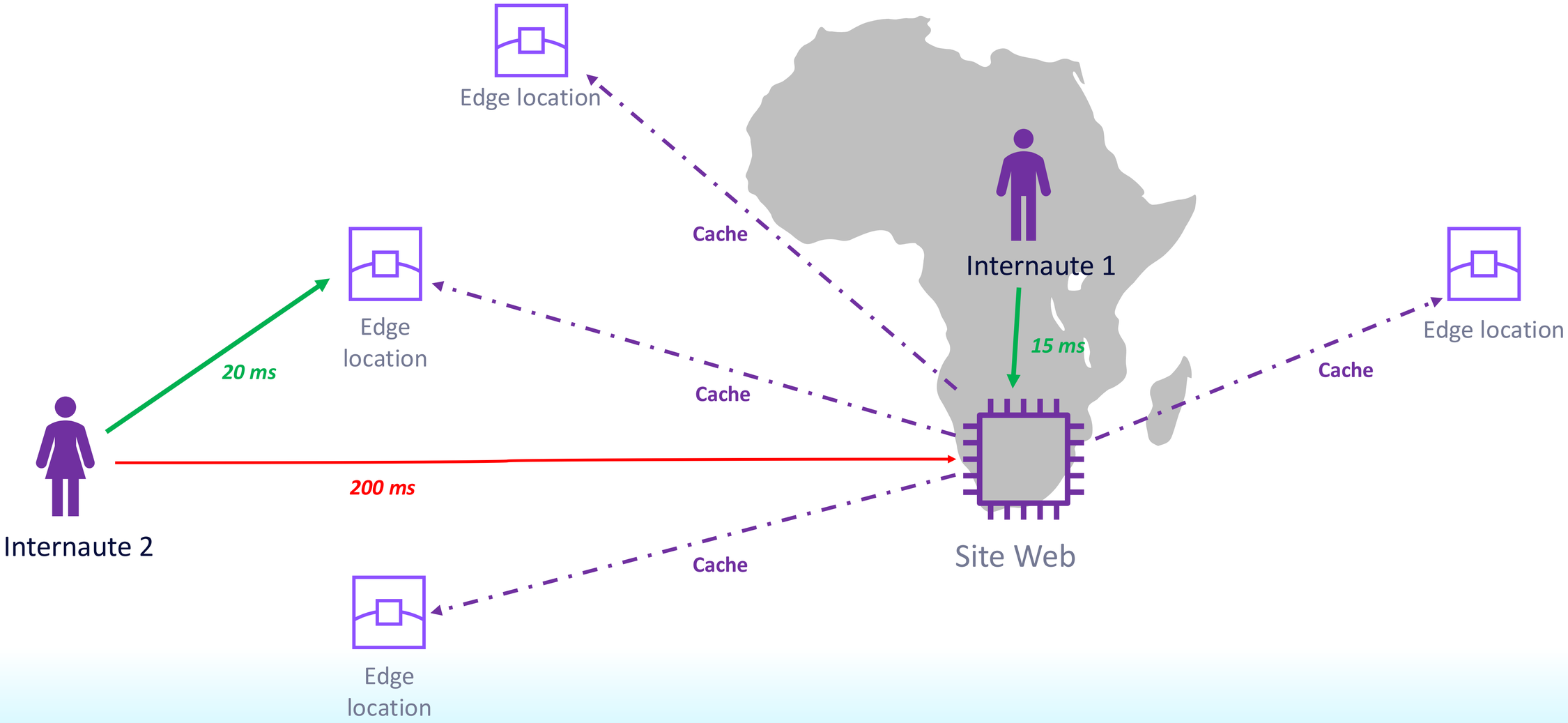
Geolocation routing policy (*Routage par géolocalisation*)



Amazon CloudFront



Content Delivery Network (CDN) : Illustration



Amazon Cloudfront



Service de **CDN** sur le cloud AWS (HTTP / HTTPS / Websockets)

Permet d'accélérer la diffusion de **contenu** **statique** et **dynamique**

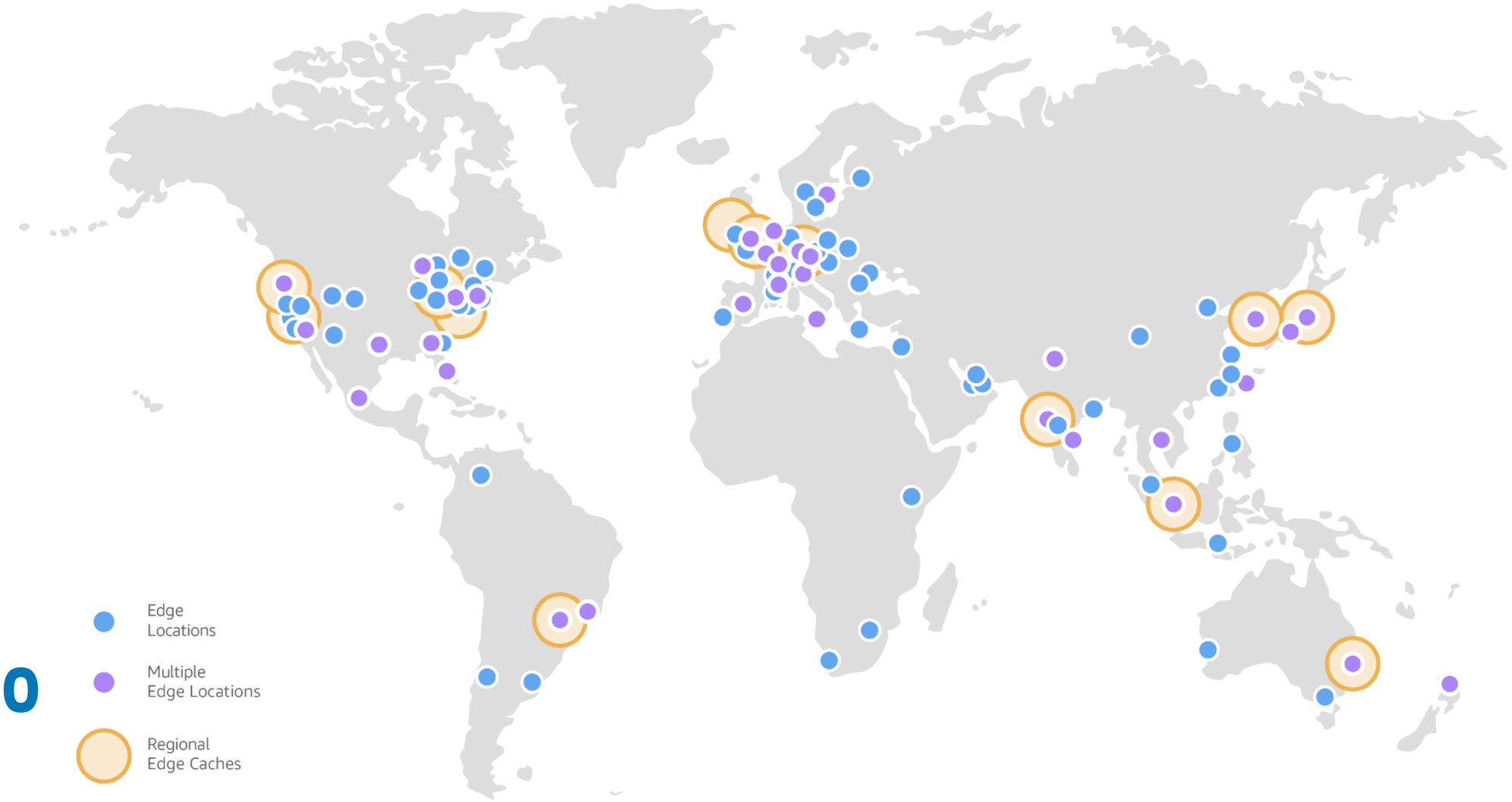
S'appuie sur un réseau de **+550** ***Edge locations***

Edge locations ≠ *Régions AWS*

Cas d'usage : site web, vidéo en streaming à la demande ou en direct, médias (photos, vidéos),...

LeCloudFacile.com

Edge locations (Emplacement périphériques)



+550

Autres bénéfices d'Amazon Cloudfront



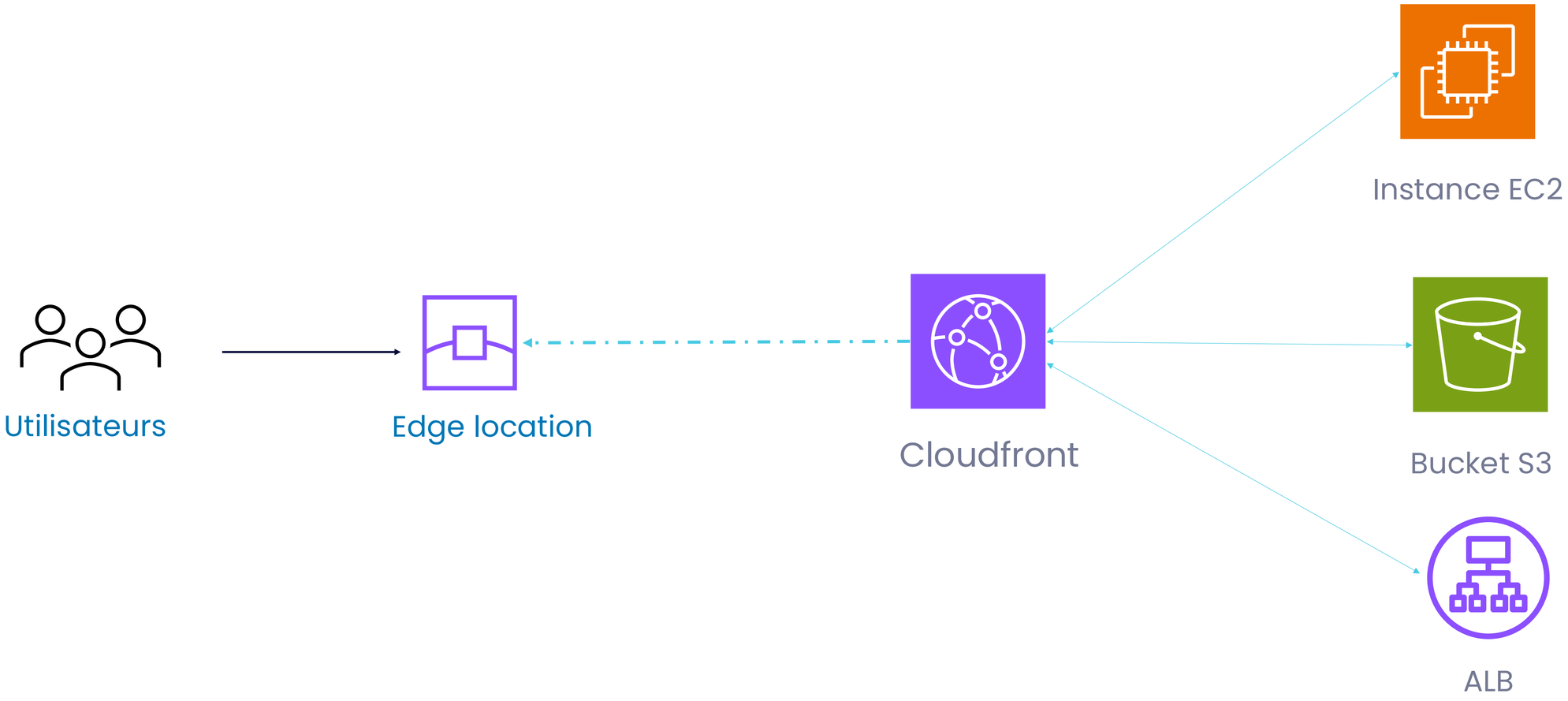
Accélére la diffusion de contenu **dynamique** (pas que statique)

Protège contre les attaques **DDoS**

Réduit la charge sur les applications d'origine

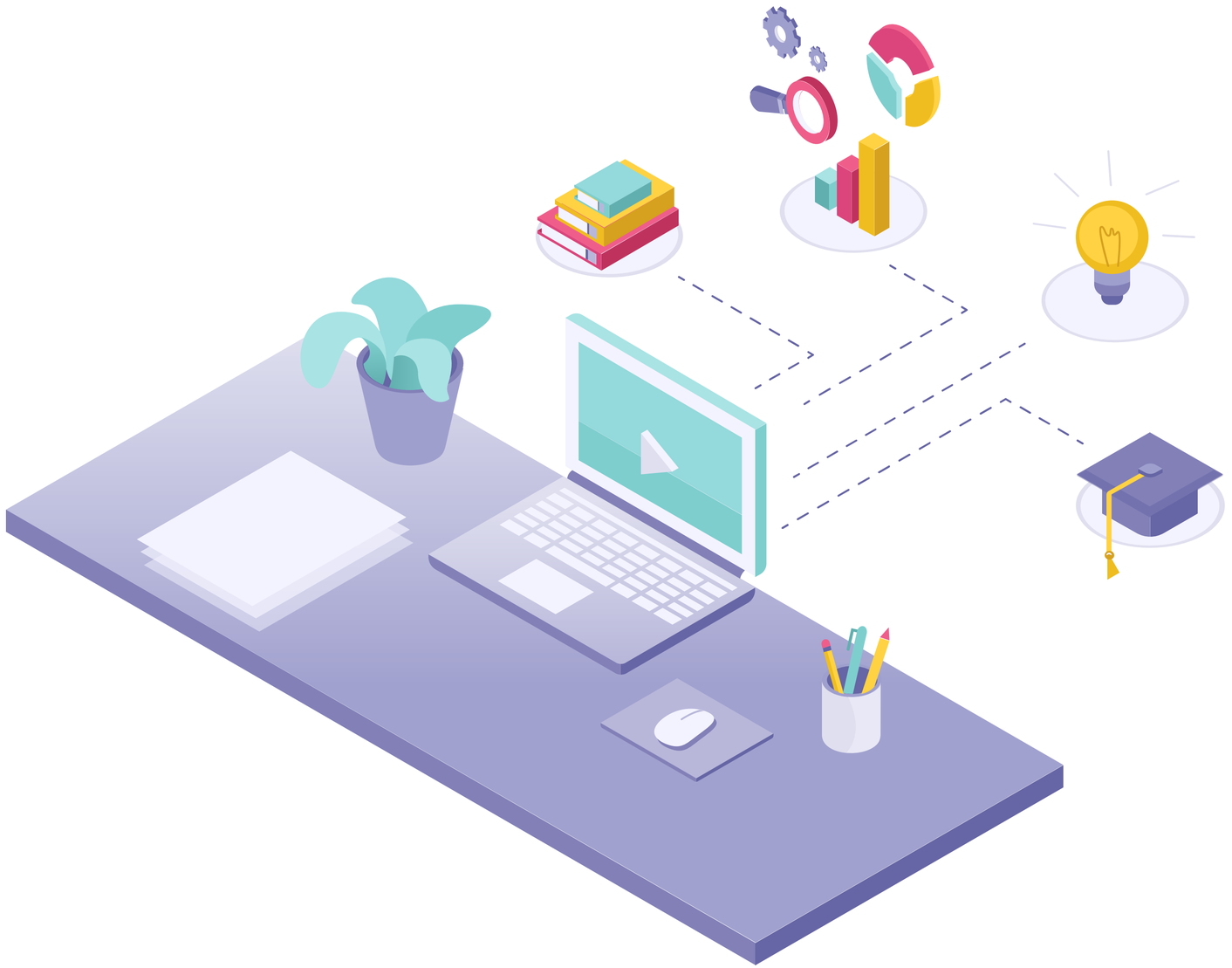
Permet de faire de la **restriction géographique.** Exemple : « *bloquer l'accès à votre contenu pour un pays XYZ* »

Origines Cloudfront



Origines

AWS Local Zone



AWS Local Zone

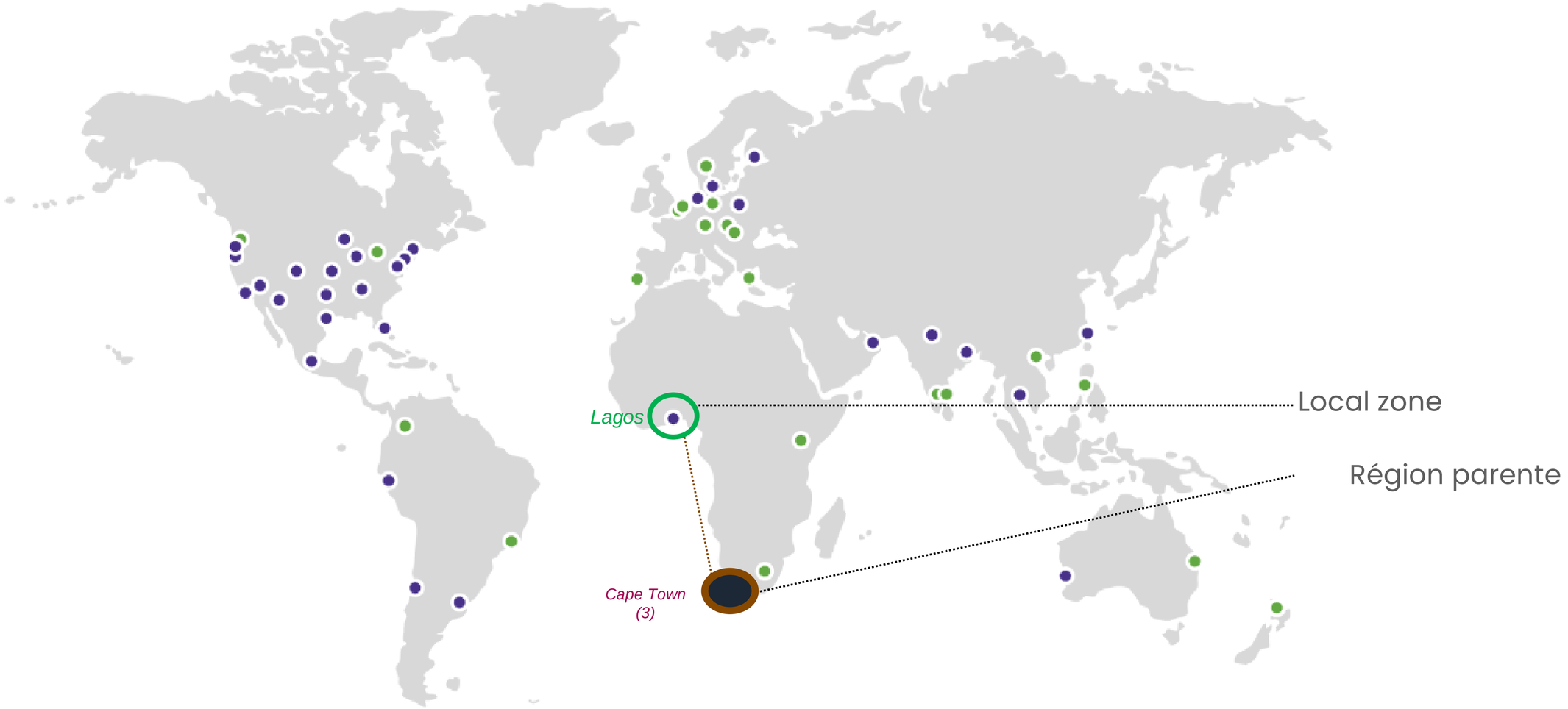
Déploiement d'infrastructure (EC2, EBS, VPC,...) à proximité **des grandes métropoles**

Cas d'usage : applications à faible latence, jeux en temps réel, streaming live, AR/VR, Résidence de données

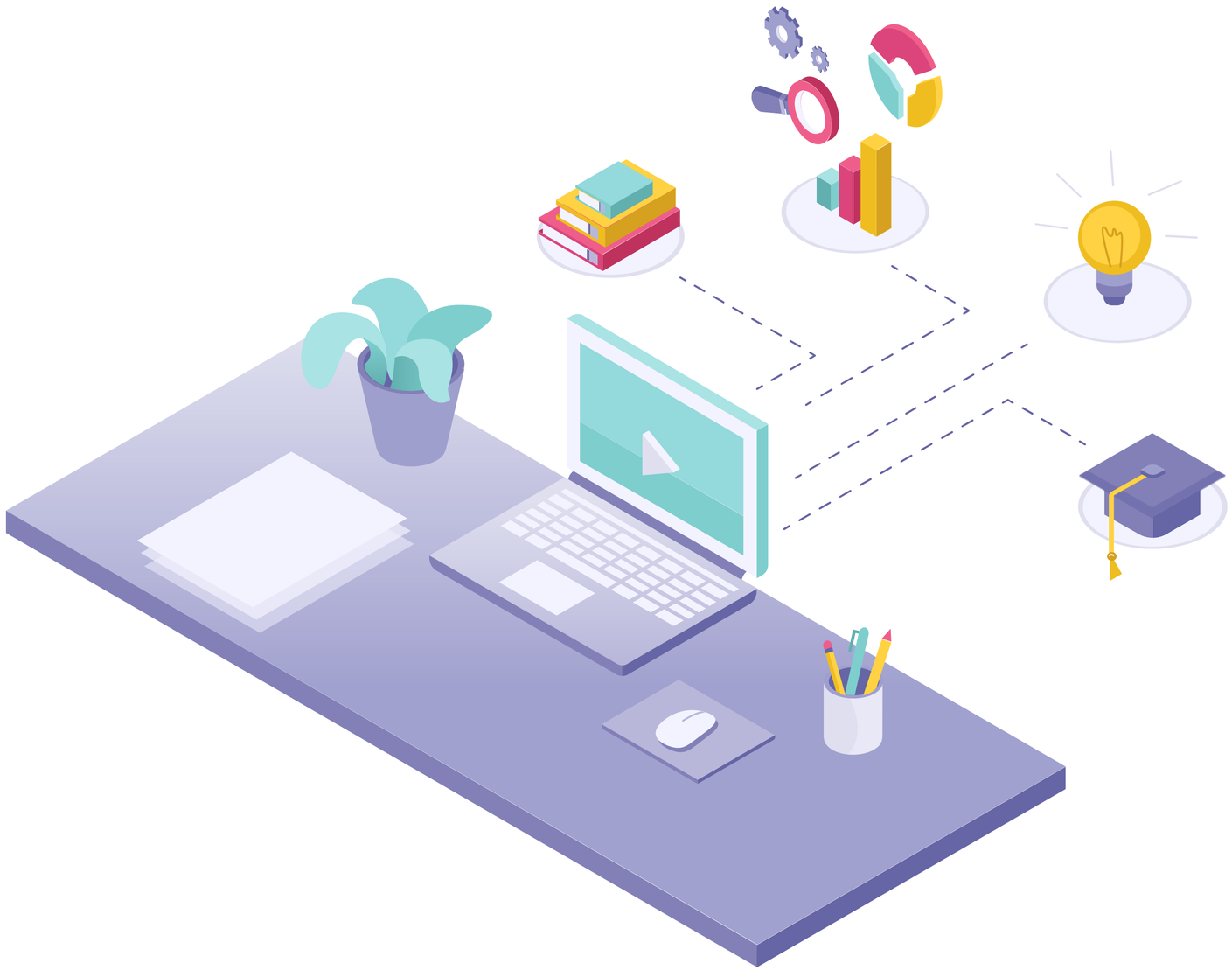
Connectées à une **région parente**. Exp : Lagos -> Cape Town, Los Angeles -> Oregon

Similaires à une zone de disponibilité, mais tous les services AWS **ne sont pas disponibles.**

Exemple de Local Zone : Lagos



AWS Outposts



AWS Outposts

Ressources de calcul et de stockage **AWS déployées dans les data centers** d'un **client**

Cas d'utilisation : traitement local, faible latence, résidence des données, …

Permet d'exécuter dans **vos propres data centers** les services AWS (EC2, ECS, EBS, RDS…)

Rack (42U standard) ou **serveurs** (1U, 2U)





AWS Outposts

Corporate Data Center

Instances EC2

Base de données RDS



AWS Outposts rack



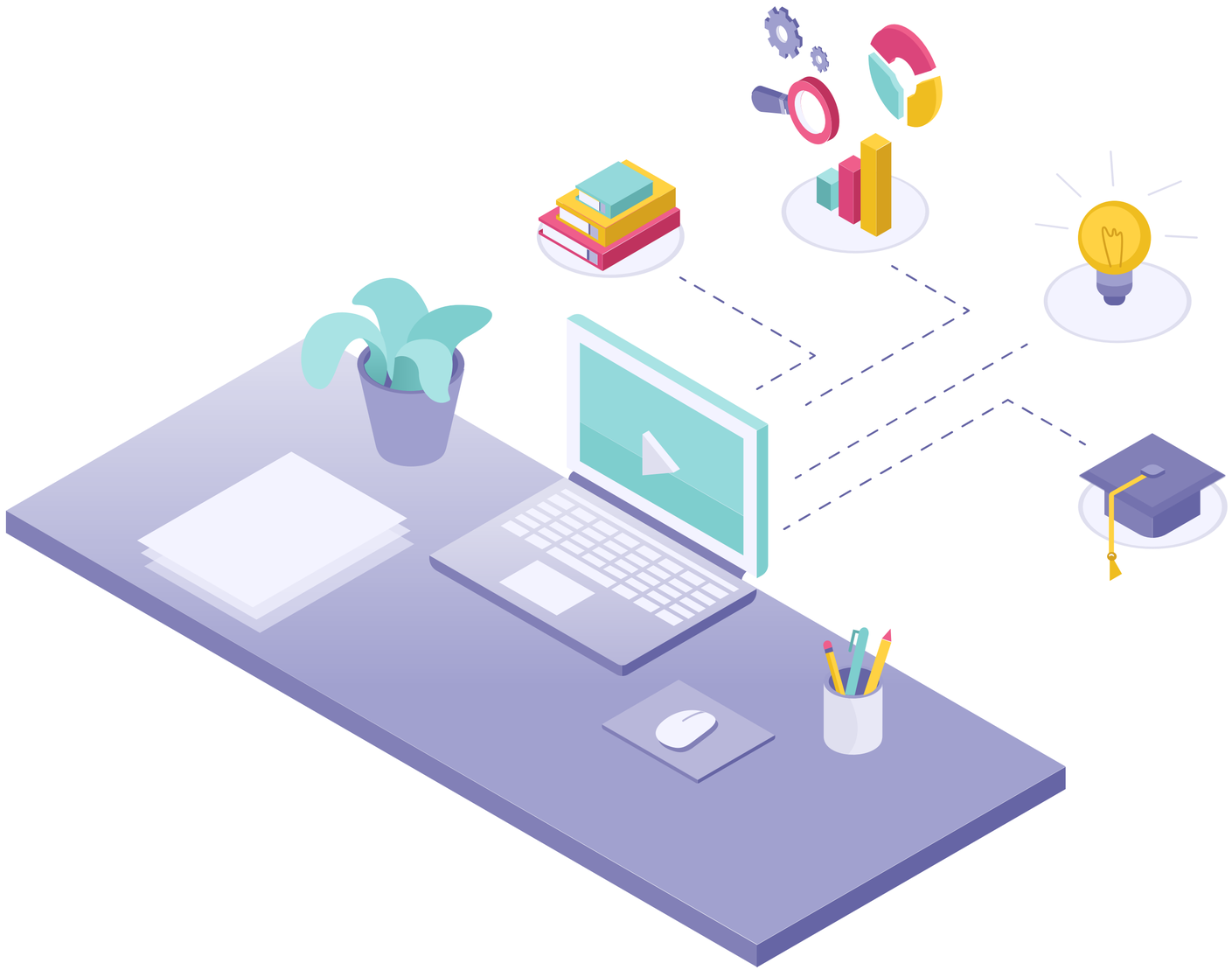
AWS Outposts Servers

AWS Cloud

Instances EC2

Base de données RDS

AWS WaveLength



AWS Wavelength



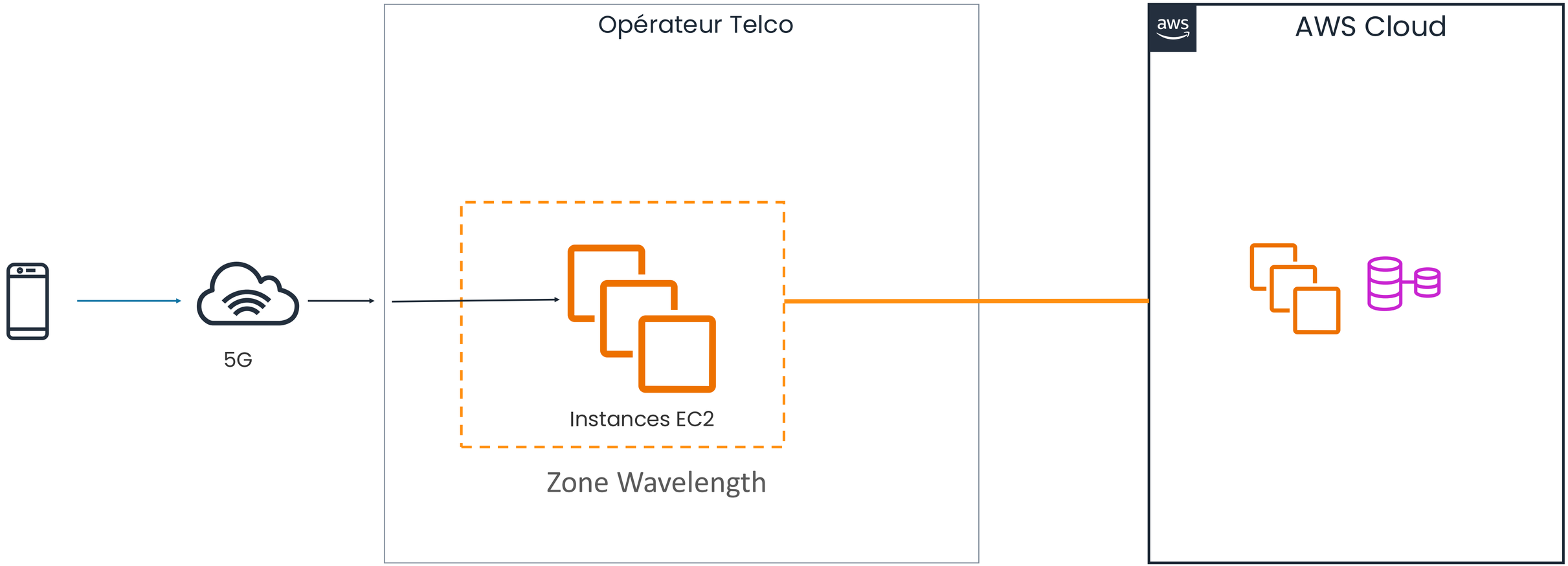
Zones Wavelength = Déploiement d'infrastructure AWS (calcul, stockage…) à la périphérie des **réseaux 5G**

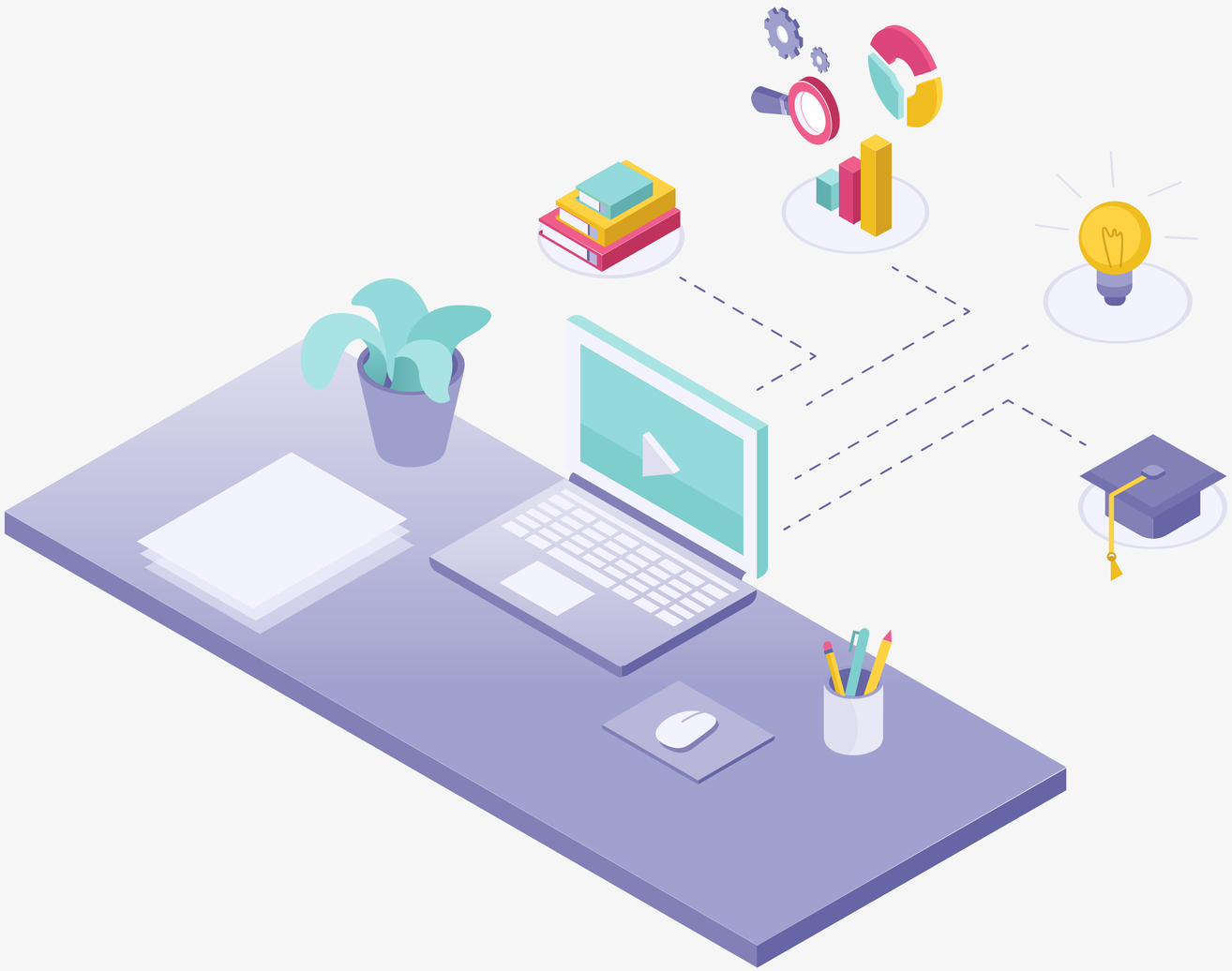
Déploiement **au sein des datacenters** des fournisseurs **Telco**

Exemples de cas d'usage :

- IoT (Internet of Thing)
- *Streaming de jeux*
- *Applications de média et divertissement*
- *Véhicules autonomes & Smart Cities*

AWS Wavelength





FIN DU MODULE

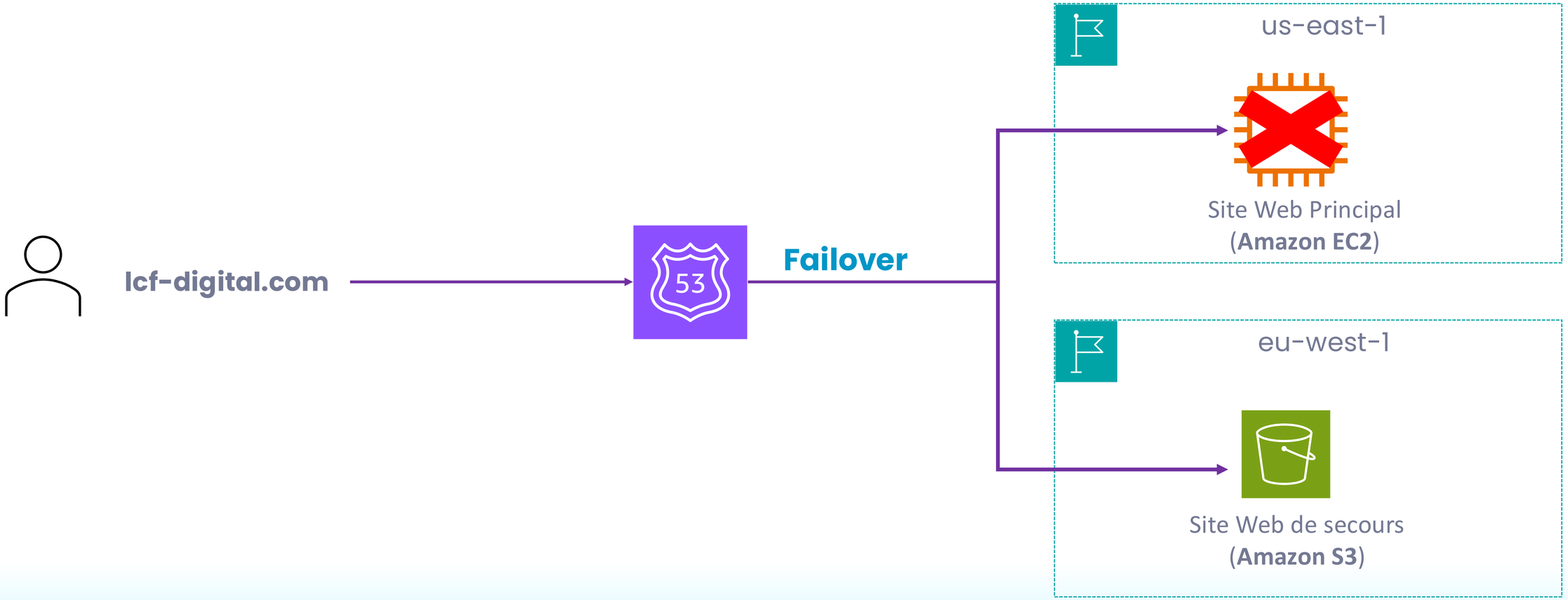
Lab : Démarrer Amazon Route 53

1. Enregistrer un nouveau nom de domaine

2. Explorer la zone hébergée

3. Associer le nom de domaine à un site web statique Amazon S3

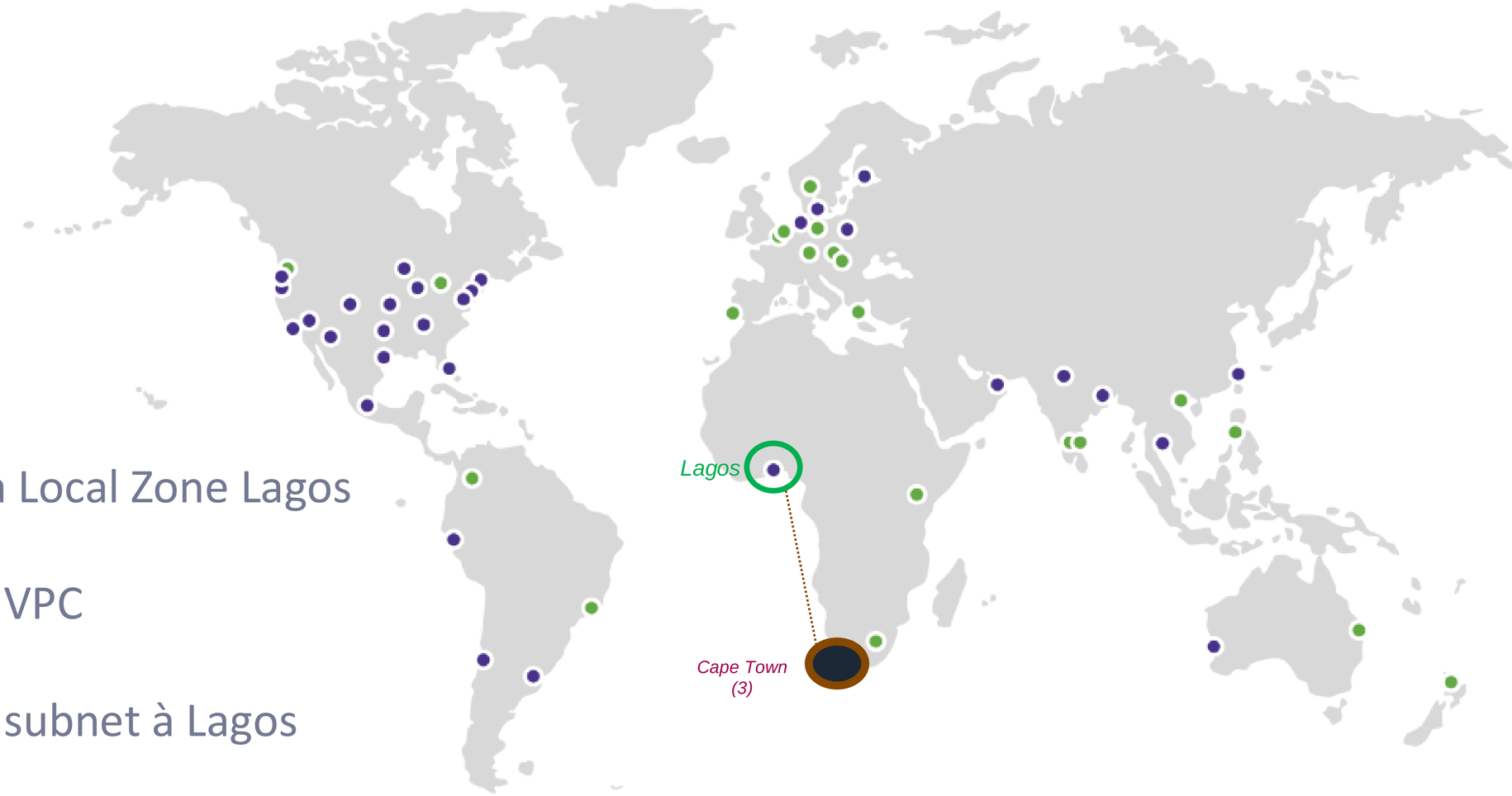
Lab Routing Policy



Lab Stratégie de routage

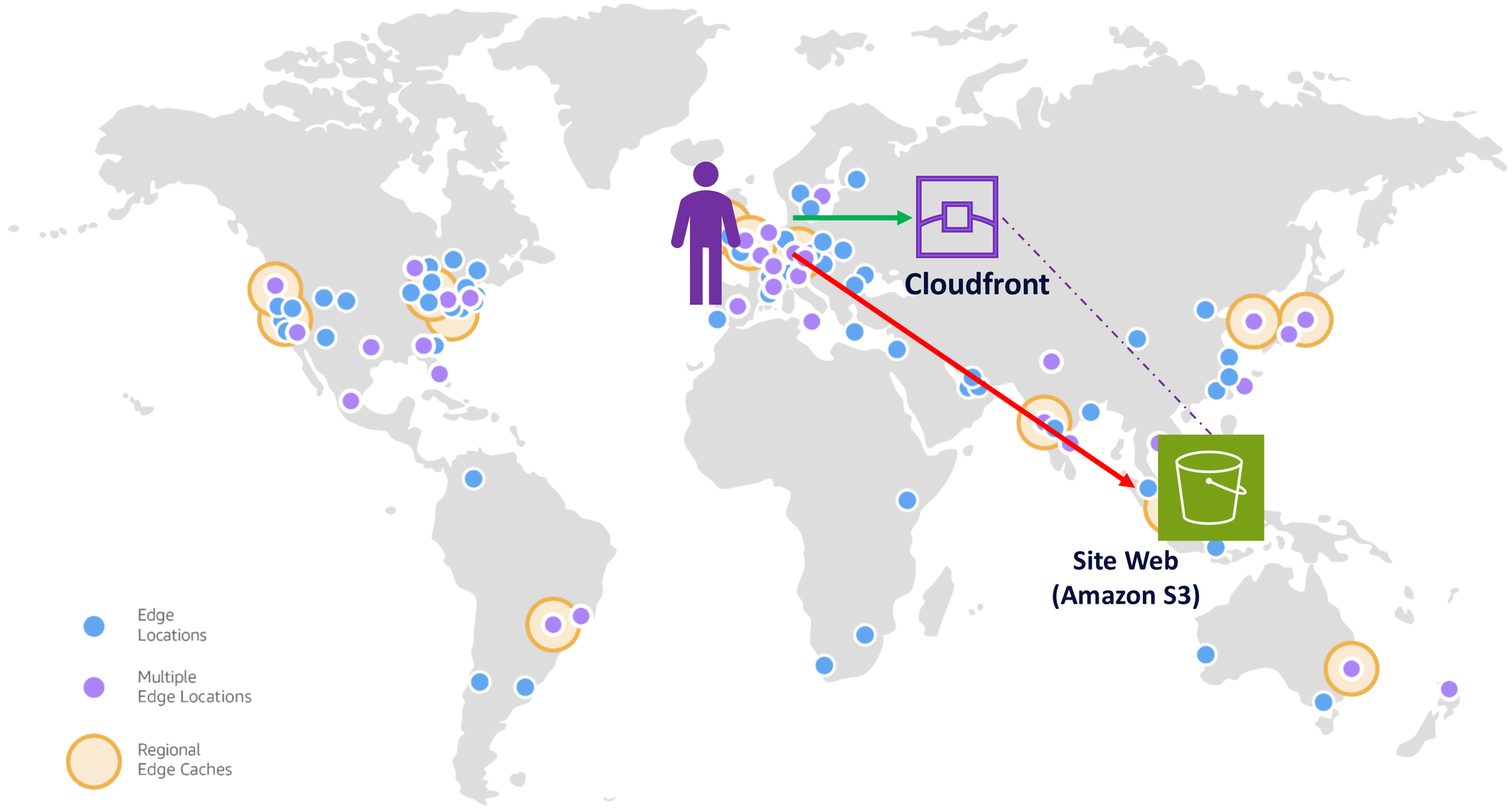
1. Déployer le site web principal sur 1 EC2 et associer une Elastic IP
2. Explorer le site web de secours sur Amazon S3
3. Configurer un health check pour surveiller le site principal
4. Configurer le routage Amazon Route 53 avec la stratégie Failover
5. Tester le basculement en simulant la panne du site web principal

Lab : Démarrer avec AWS Local Zone



1. Activer la Local Zone Lagos
2. Créer un VPC
3. Créer un subnet à Lagos
4. Lancer une EC2 à Lagos

Lab Amazon CloudFront

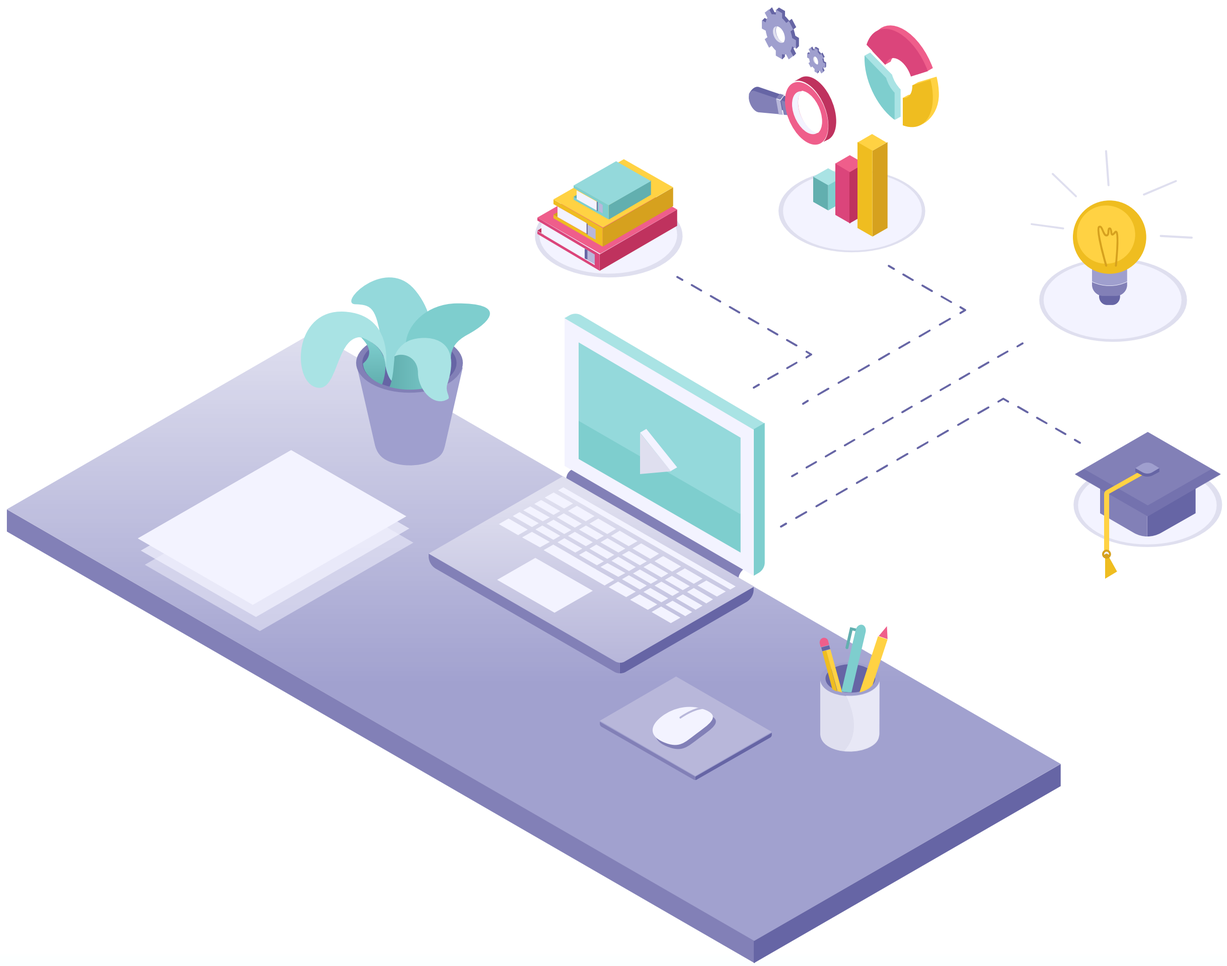


Lab Amazon CloudFront

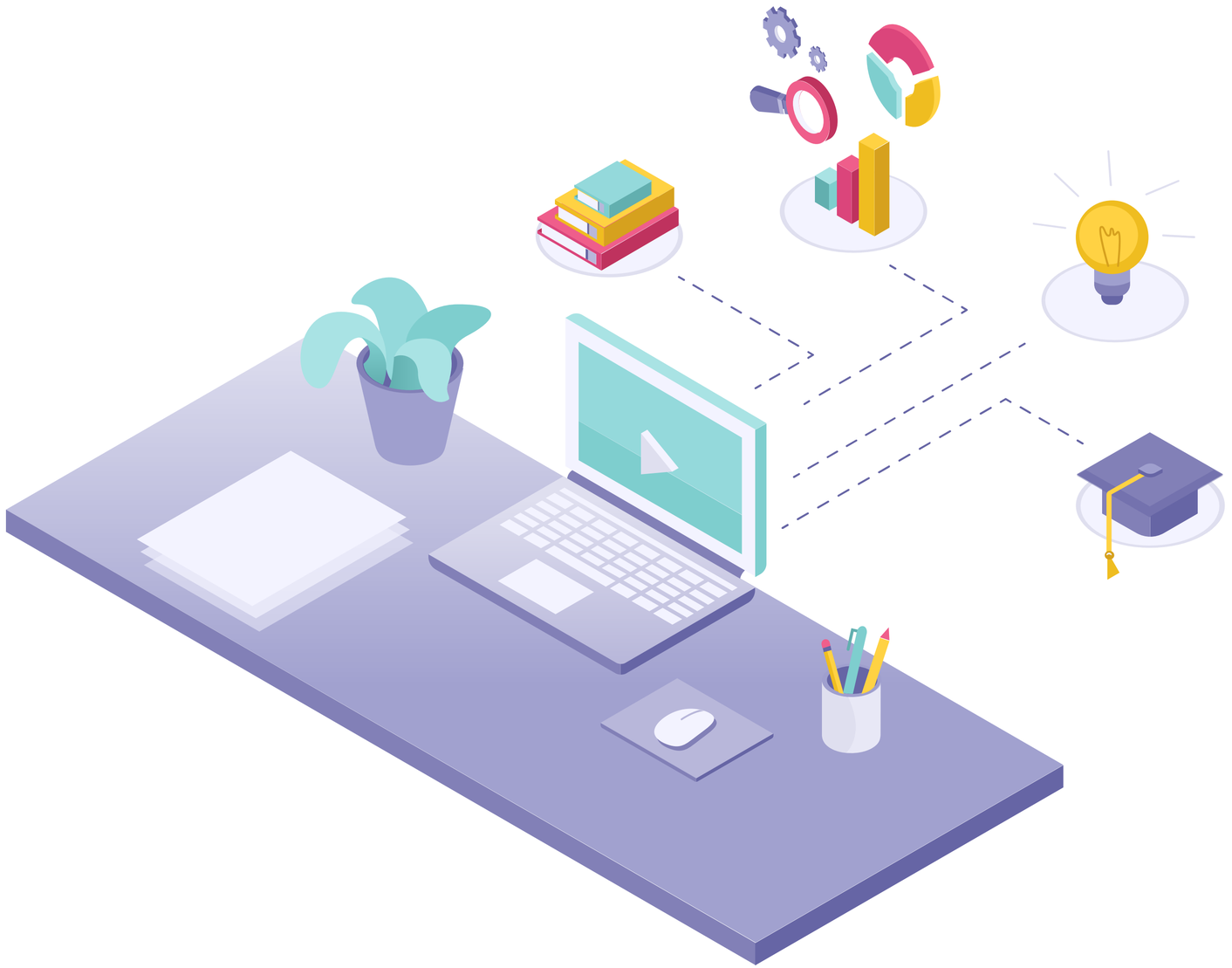
1. Déployer un site web statique S3 dans une région AWS distante
2. Déployer une distribution CloudFront pour accélérer le site
3. Faire un test comparatif entre le site S3 et CloudFront

Module 7 : Stockage sur AWS

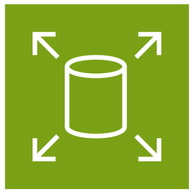
Stockage fiable, évolutif et sécurisé pour vos données



Amazon Elastic Block Store (EBS)



Amazon EBS



Fournit des volumes de stockage **orienté bloc**

Volumes **persistents**

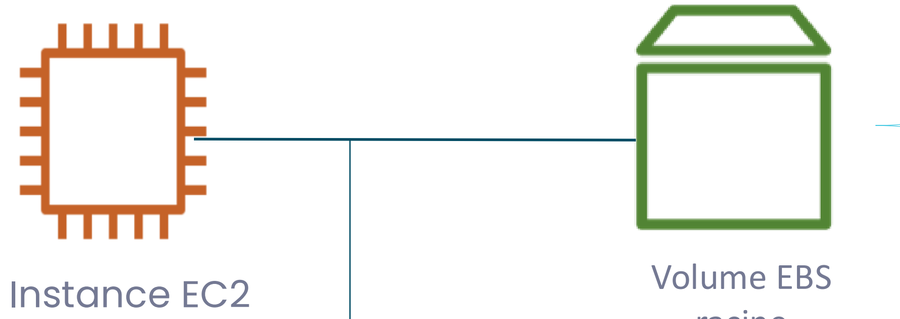
Utilisés uniquement par les **instances EC2**

SSD (gp2, gp3, io1, io2) ou HDD

Taille : de 1GB à 64 TiB

Service **zonal**

Amazon EBS



Obligatoire : 1 volume racine

Contient le **système d'exploitation + des données**

Ne peut pas être détaché

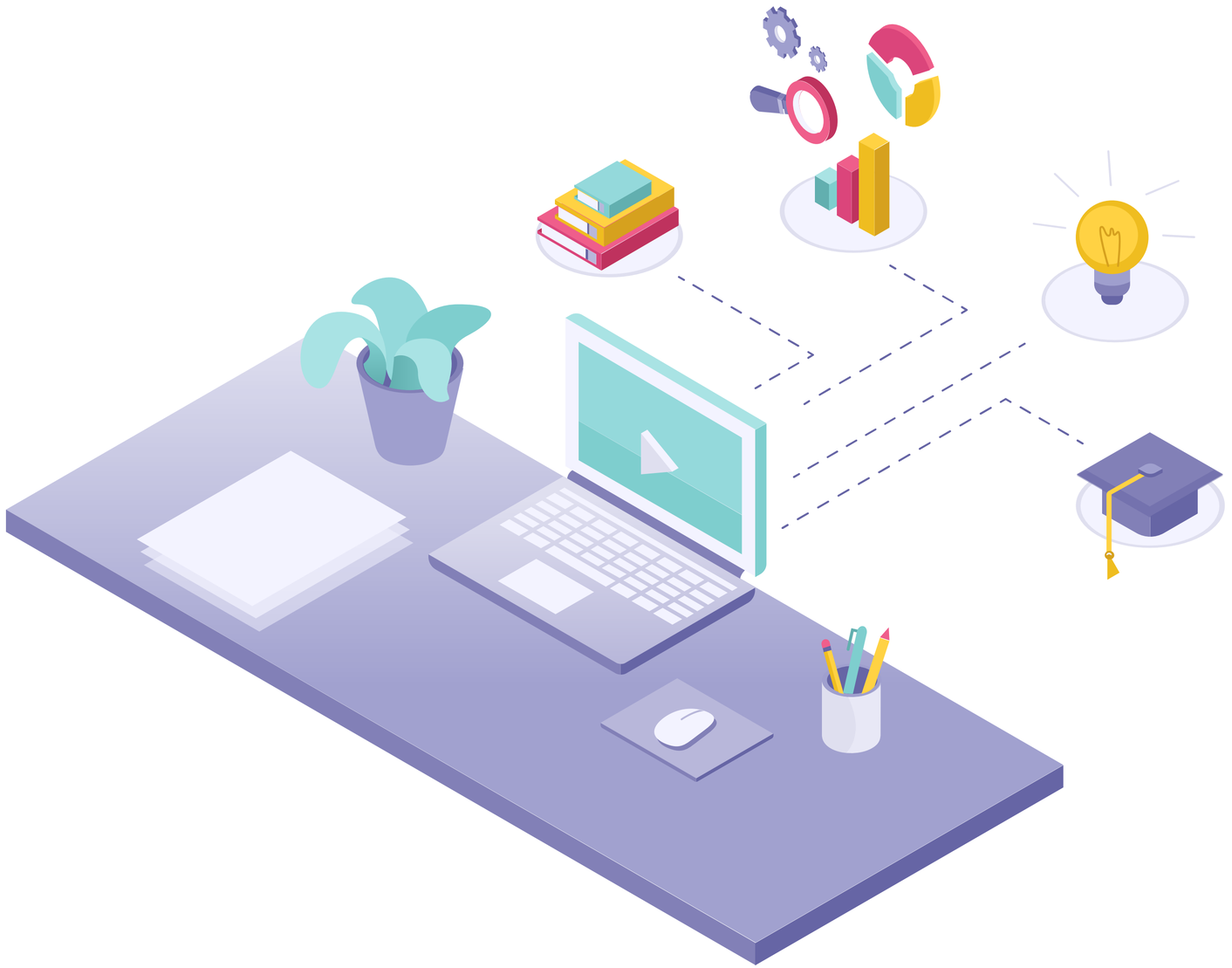
Optionnel : 1 ou plusieurs volumes additionnels

Contiennent **des données ou applications**

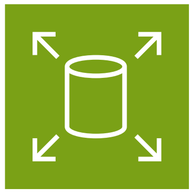
Peuvent être détachés à tout moment

Par défaut, le volume racine est supprimé lorsque l'instance EC2 est terminée

EBS Snapshots



EBS Snapshots (Instantanés)



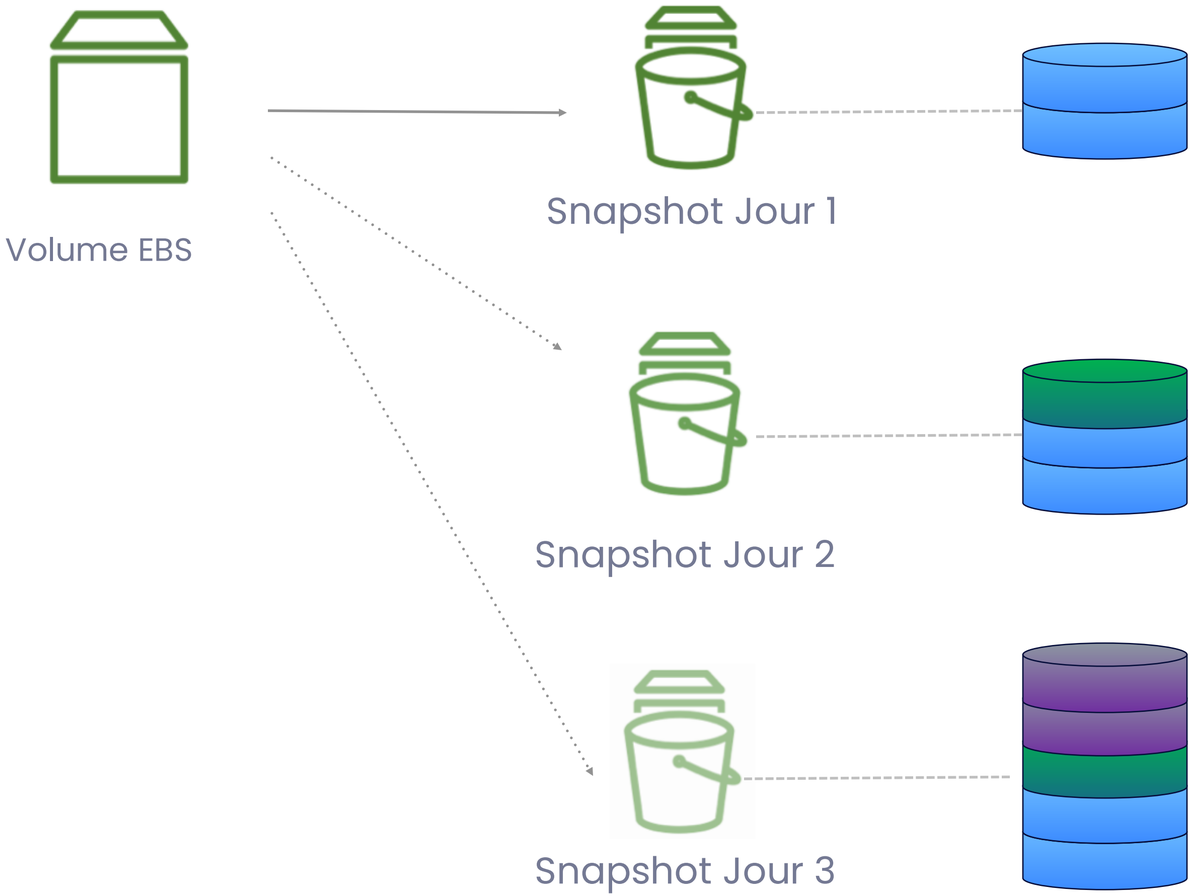
Sauvegardes (Backups) des volumes EBS

Stockés dans Amazon S3 (géré par AWS)

Durabilité = 99,999999999 %

Utilisables à tout moment pour restaurer des données

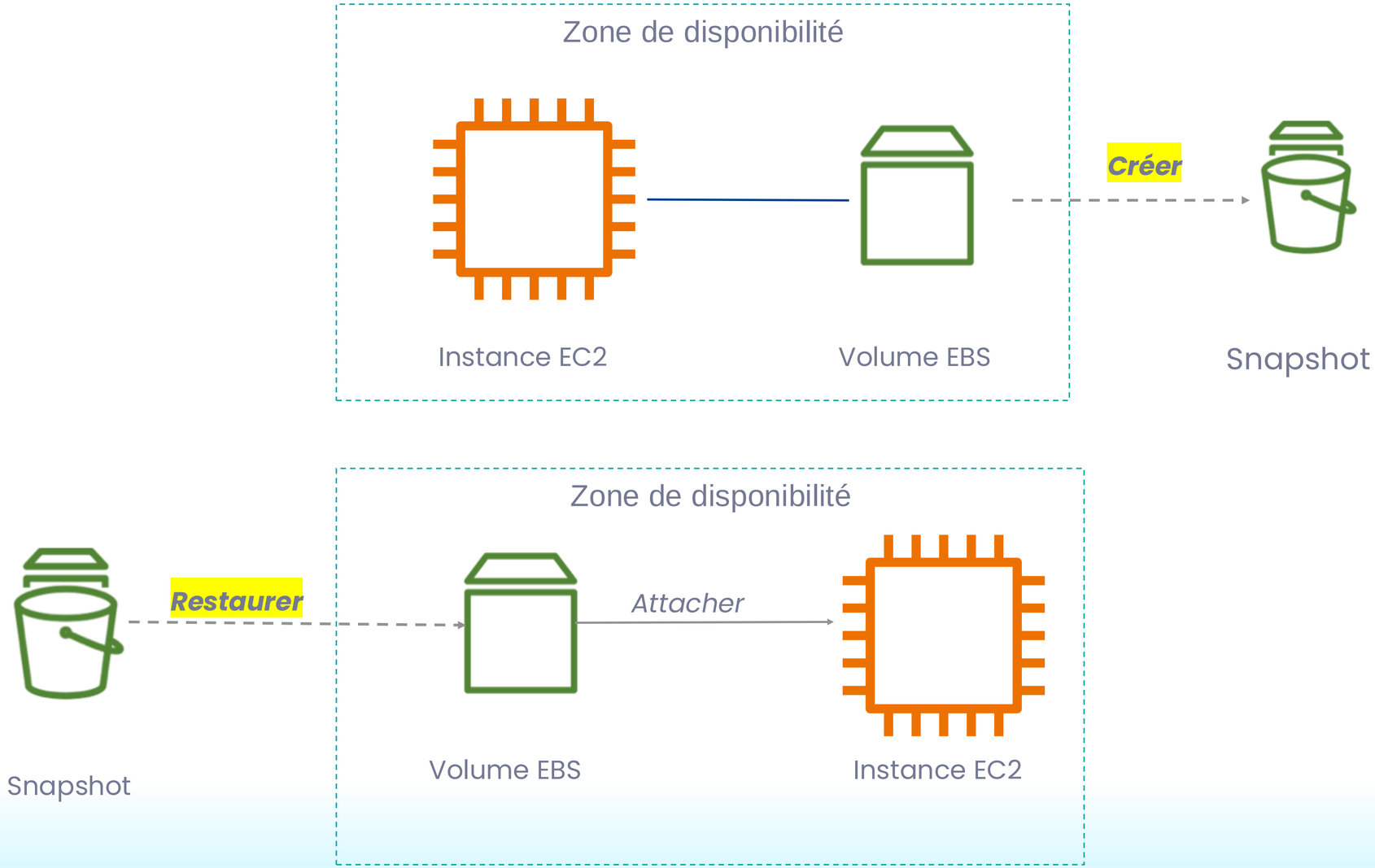
Sauvegardes incrémentielles



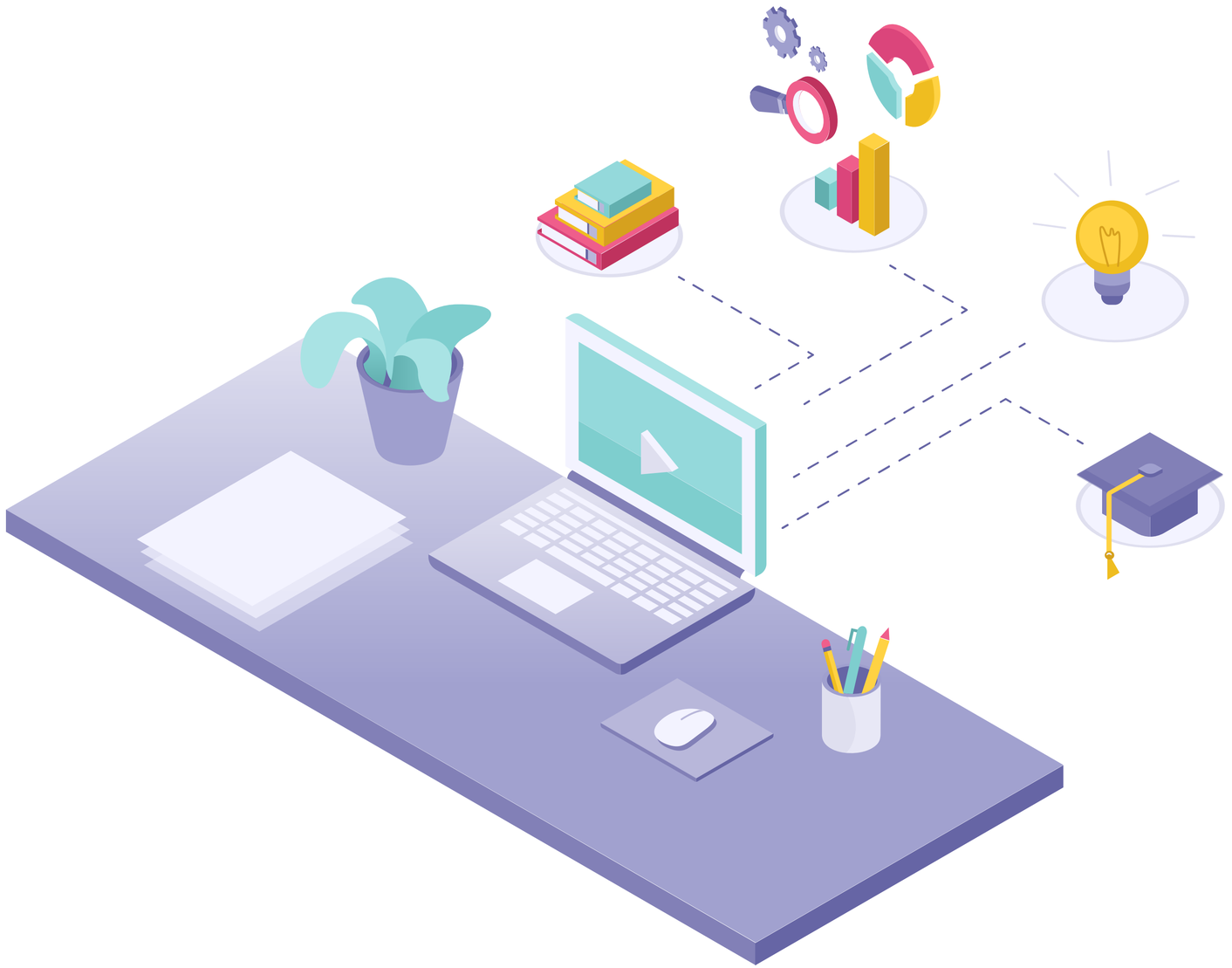
Les instantanés sont des sauvegardes ***incrémentielles***

Seuls les blocs **qui ont changé** depuis l'instantané le plus récent sont enregistrés

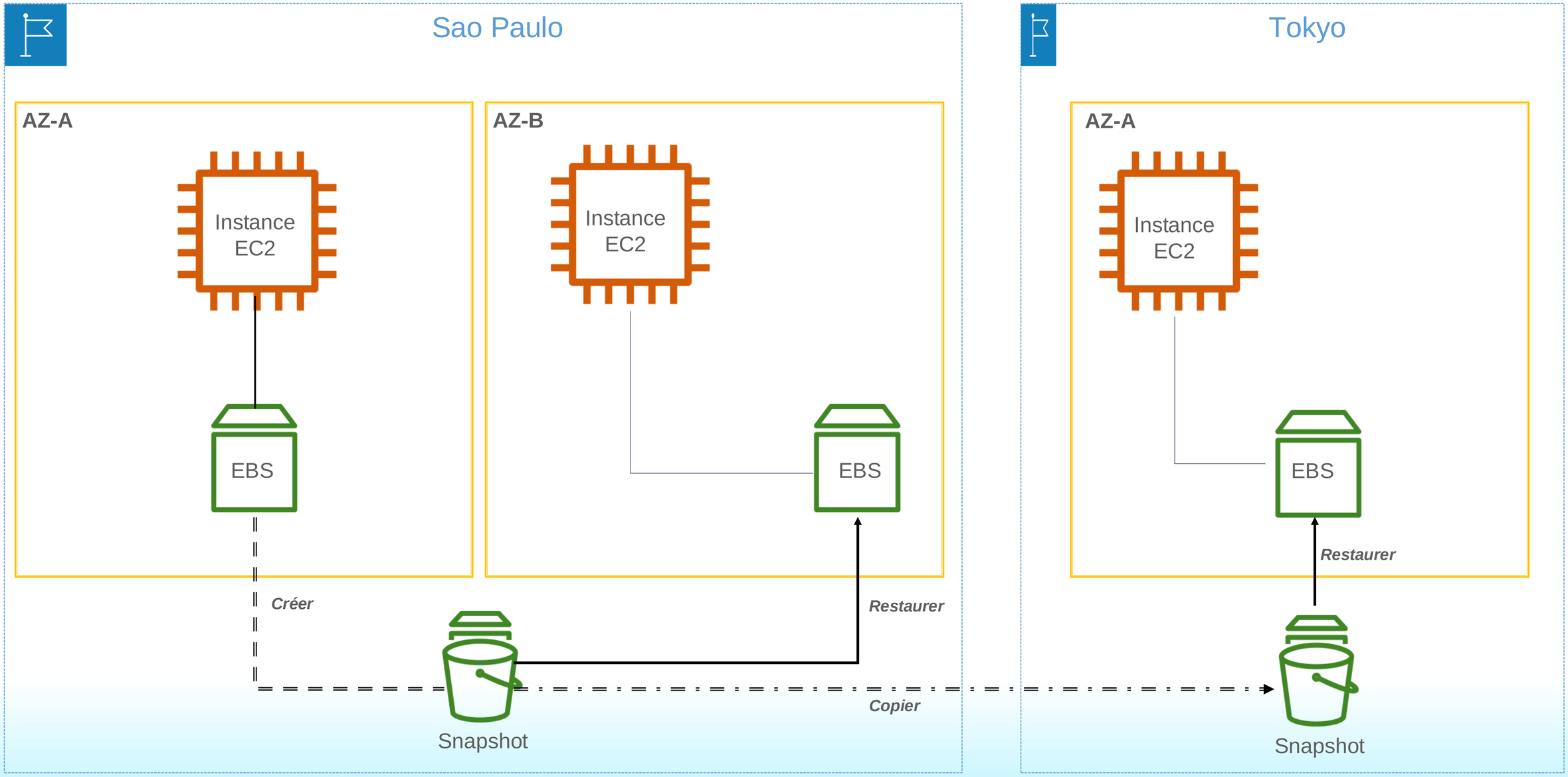
Créer / Restaurer un snapshot



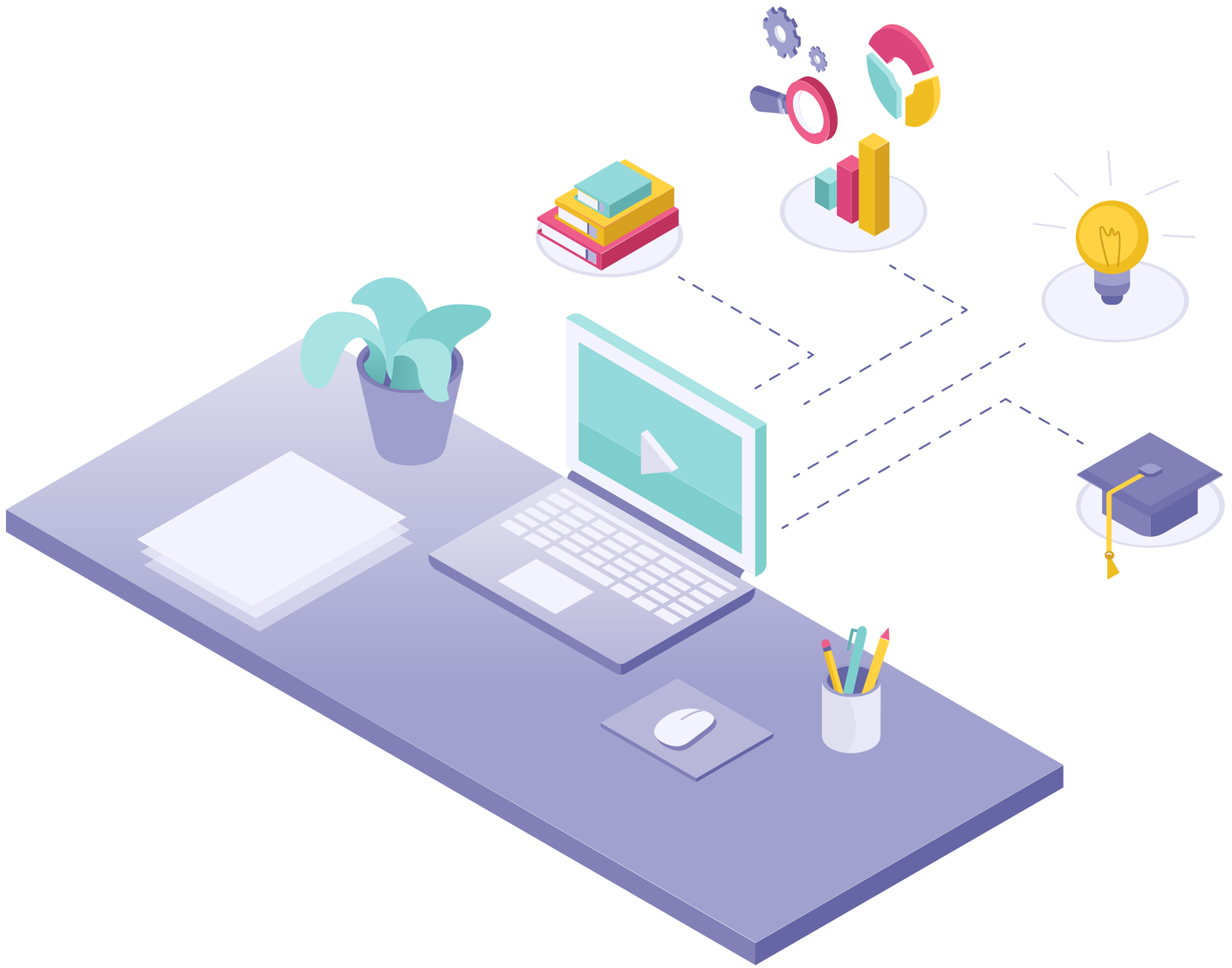
EBS Architecture



EBS Architecture



EC2 Instance Store



EC2 Instance Store



Stockage **temporaire** de niveau bloc pour votre instance EC2

Disques physiquement attachés à l'ordinateur hôte

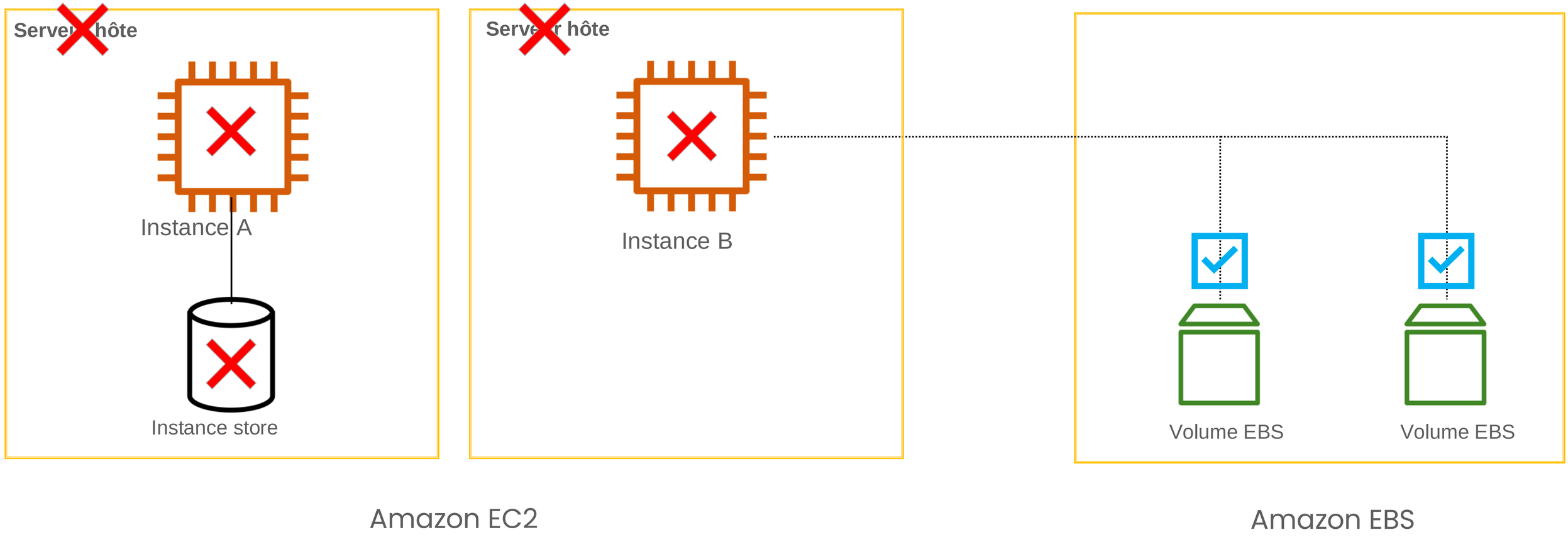
Ne sont pas disponibles sur tous les types d'instances EC2

Données perdues suite à stop/start de l'instance EC2

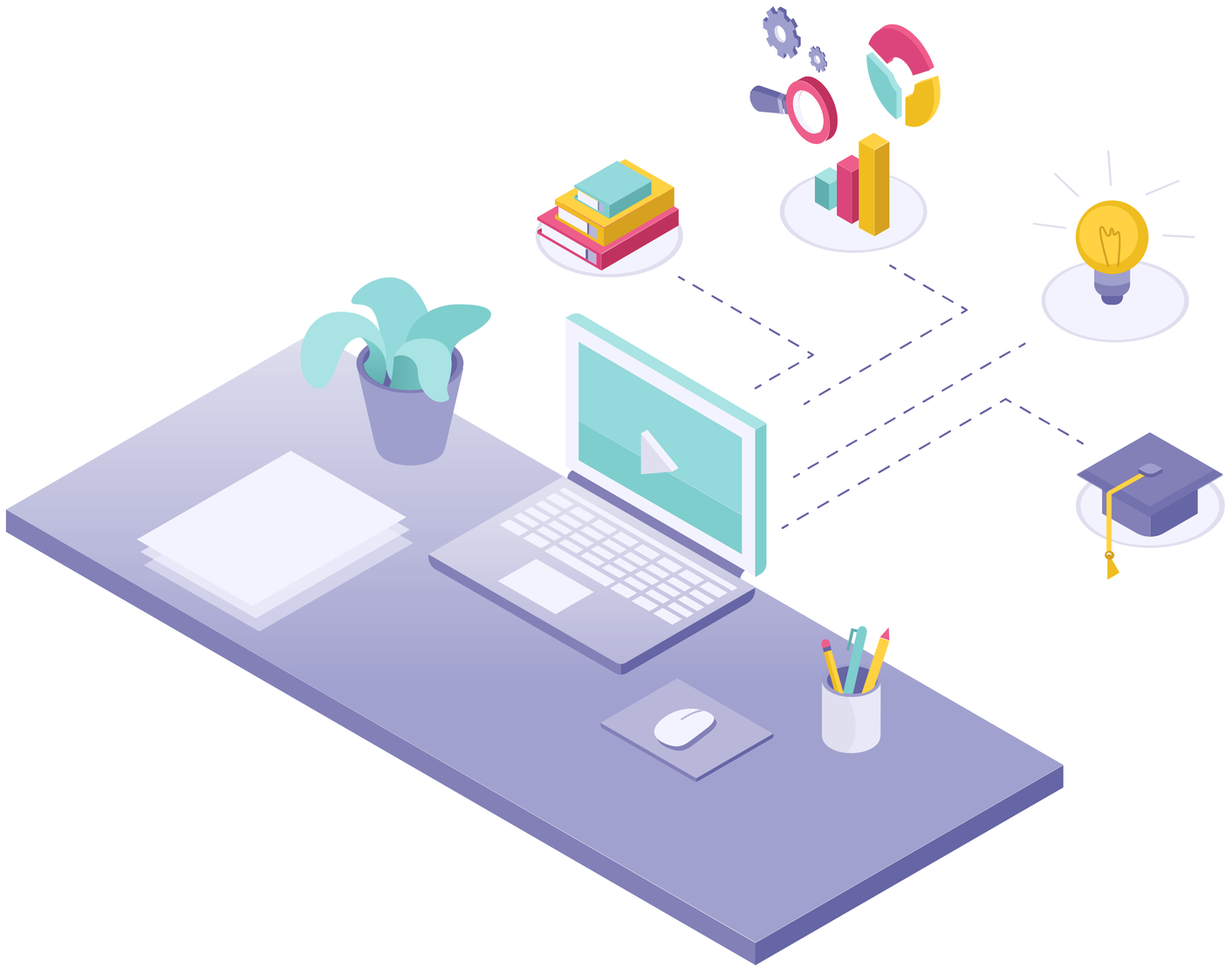
Cas d'usage

- stockage d'informations temporaires : Données tampons, caches, …
- **Ne convient pas** à des données critiques -> Utiliser EBS

EC2 Instance Store



Amazon Simple Storage Service (S3)



Amazon Simple Storage Service (S3)



Service de stockage en ligne de type ***objet***

Stockage virtuellement infini

Orienté « *WORM : Write Once Read Many* »

Durabilité : 99,999999999 %

Données chiffrées par défaut (***SSE-S3***)

Stockage plus économique qu'EBS par exemple -> $0.023/GB

Cas d'usage



Données statiques

Photos, vidéos,...

Big Data & Data Lake

Backup & Archivage

Hébergement de site web statiques

!!! N'est pas fait pour héberger un système d'exploitation

Les buckets (compartiments)



Stockent les **objets** (*fichiers*) dans S3

Représentés sous forme de “**dossiers**” dans la console AWS

Doivent avoir des noms uniques (comme les DNS)

Service **Régional** -> choix de la région à la création du bucket

Les objets



Ce sont les **fichiers** que vous stockez dans les **buckets**

Peu importe le **format** : *txt, xml, json, photos, vidéos, archives,...*

Taille max. d'un objet : **5 TB +**

Aucune limite sur le nombre d'objets dans un bucket

Les objets



Objet S3

Données : *tout type de contenu (Xml, json, txt, csv, binaire,…)*

Métadonnées : *Date, Content-length, Content-Type,…*

Clé : *Identifiant unique -> c'est le chemin absolu de l'objet.*

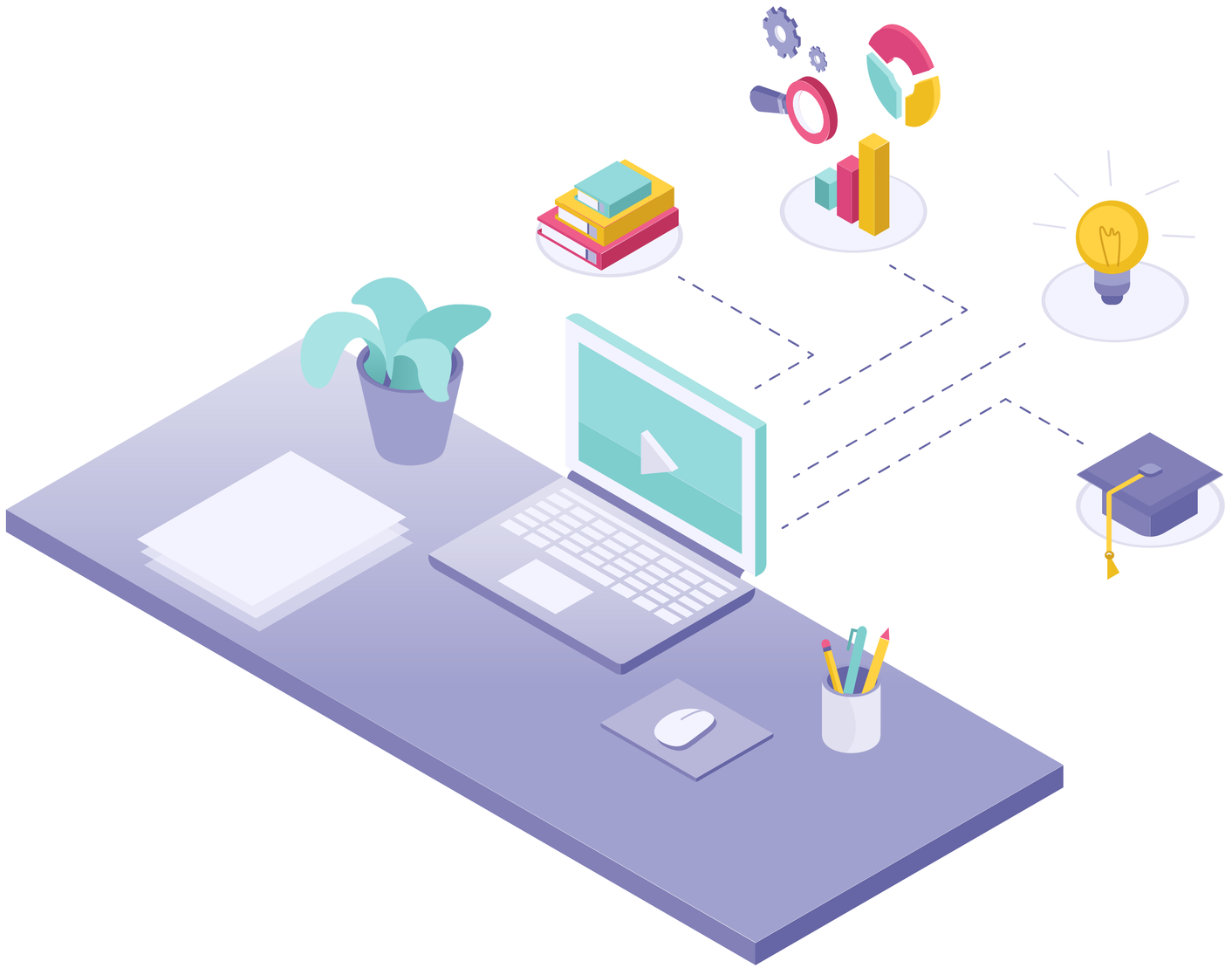
s3://my-bucket/formation/photo.jpg

Bucket

Nom

Clé

Classes de stockage Amazon S3



Classes de stockage

Similaires à des **zones de stockage** dans S3

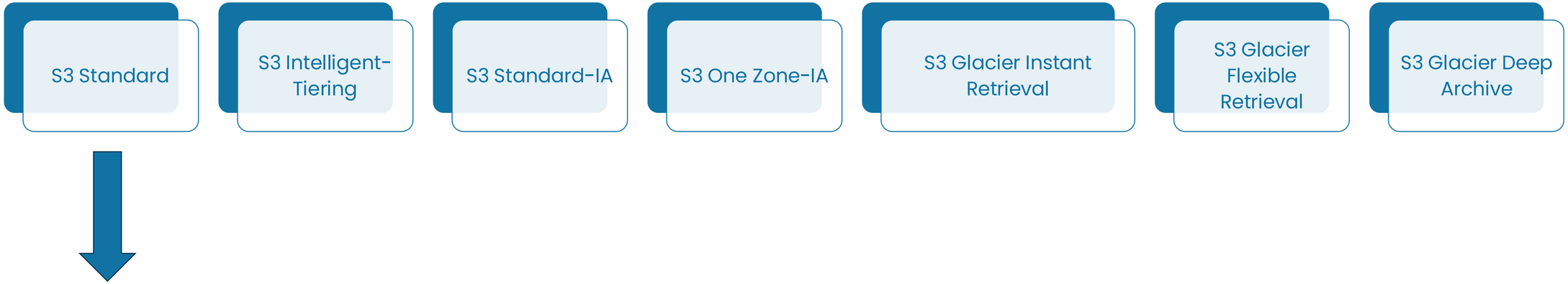
Fournissent **le stockage le plus économique** pour différents types d'accès

Classe par défaut : **standard**

Choix de la classe en fonction des exigences :

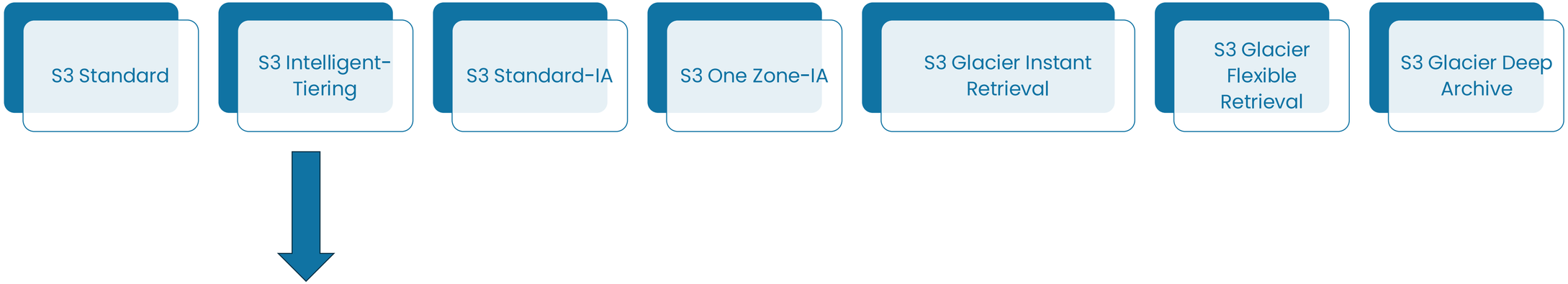
- *fréquence d'accès aux données, exigences de durabilité, coût, archivage..*

Classes de stockage



- Durabilité : 99.999999999 %
- Disponibilité : 99.99 %
- Données consultées fréquemment
- Accès rapide (millisecondes)

Classes de stockage



- Durabilité : 99.999999999 %
- Disponibilité : 99.9 %
- Déplace automatiquement les objets vers la classe la plus rentable
- Accès rapide (millisecondes)

Classes de stockage

S3 Standard

S3 Intelligent-Tiering

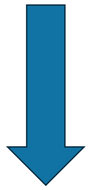
S3 Standard-IA

S3 One Zone-IA

S3 Glacier Instant Retrieval

S3 Glacier Flexible Retrieval

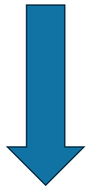
S3 Glacier Deep Archive



- Durabilité : 99.999999999 %
- Disponibilité : 99.9 %
- Données consultées peu fréquemment
- Accès rapide (millisecondes)

Classes de stockage

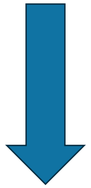
S3 Standard | S3 Intelligent-Tiering | S3 Standard-IA | S3 One Zone-IA | S3 Glacier Instant Retrieval | S3 Glacier Flexible Retrieval | S3 Glacier Deep Archive



- Durabilité : 99.999999999 % **dans 1 AZ**
- Disponibilité : 99.5 %
- Données consultées peu fréquemment
- Accès rapide (millisecondes)

Classes de stockage

- S3 Standard
- S3 Intelligent-Tiering
- S3 Standard-IA
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive



- Durabilité : 99.999999999 %
- Disponibilité : 99.9 %
- Stockage d’archives
- Accès rapide (millisecondes)

Classes de stockage

S3 Standard

S3 Intelligent-Tiering

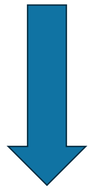
S3 Standard-IA

S3 One Zone-IA

S3 Glacier Instant Retrieval

S3 Glacier Flexible Retrieval

S3 Glacier Deep Archive



- Durabilité : 99.999999999 %
- Disponibilité : 99.99 %
- Stockage d’archives
- Accès long (minutes ou heures)

Classes de stockage

S3 Standard

S3 Intelligent-Tiering

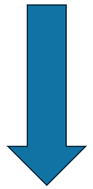
S3 Standard-IA

S3 One Zone-IA

S3 Glacier Instant Retrieval

S3 Glacier Flexible Retrieval

S3 Glacier Deep Archive



- Durabilité : 99.999999999 %
- Disponibilité : 99.9 %
- Stockage d’archives
- Accès long (heures)

Classes de stockage

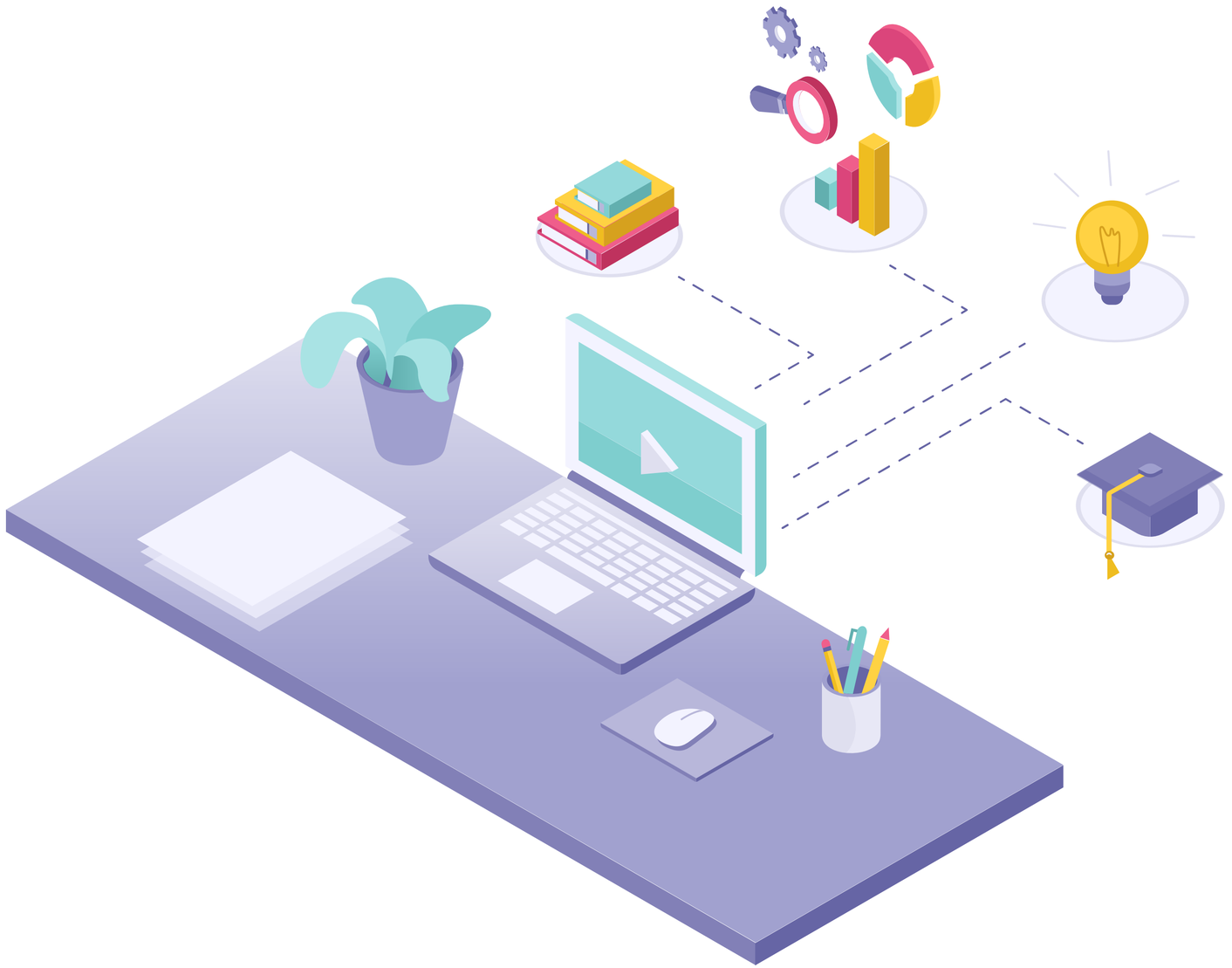
- S3 Standard
- S3 Intelligent-Tiering
- S3 Standard-IA
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive



Données chaudes

Données froides

Contrôle des accès Amazon S3



Contrôles d'accès

Vos données dans S3 sont **privées par défaut**, uniquement accessibles par vous.



Vous pouvez les partager avec d'autres entités (*via des Bucket policy ou IAM Policy*)

Vous pouvez les **rendre publiques sur Internet** (*via des Bucket policy ou ACL)*

Bucket policy



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Principal": {},
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::mybucket"
            ]
        }
    ]
}
```

Stratégie de compartiment

Document JSON

Permet d'accorder ou de refuser des autorisations d'accès

aux données dans S3

Bucket policy



Compte ou utilisateur concerné par l'autorisation

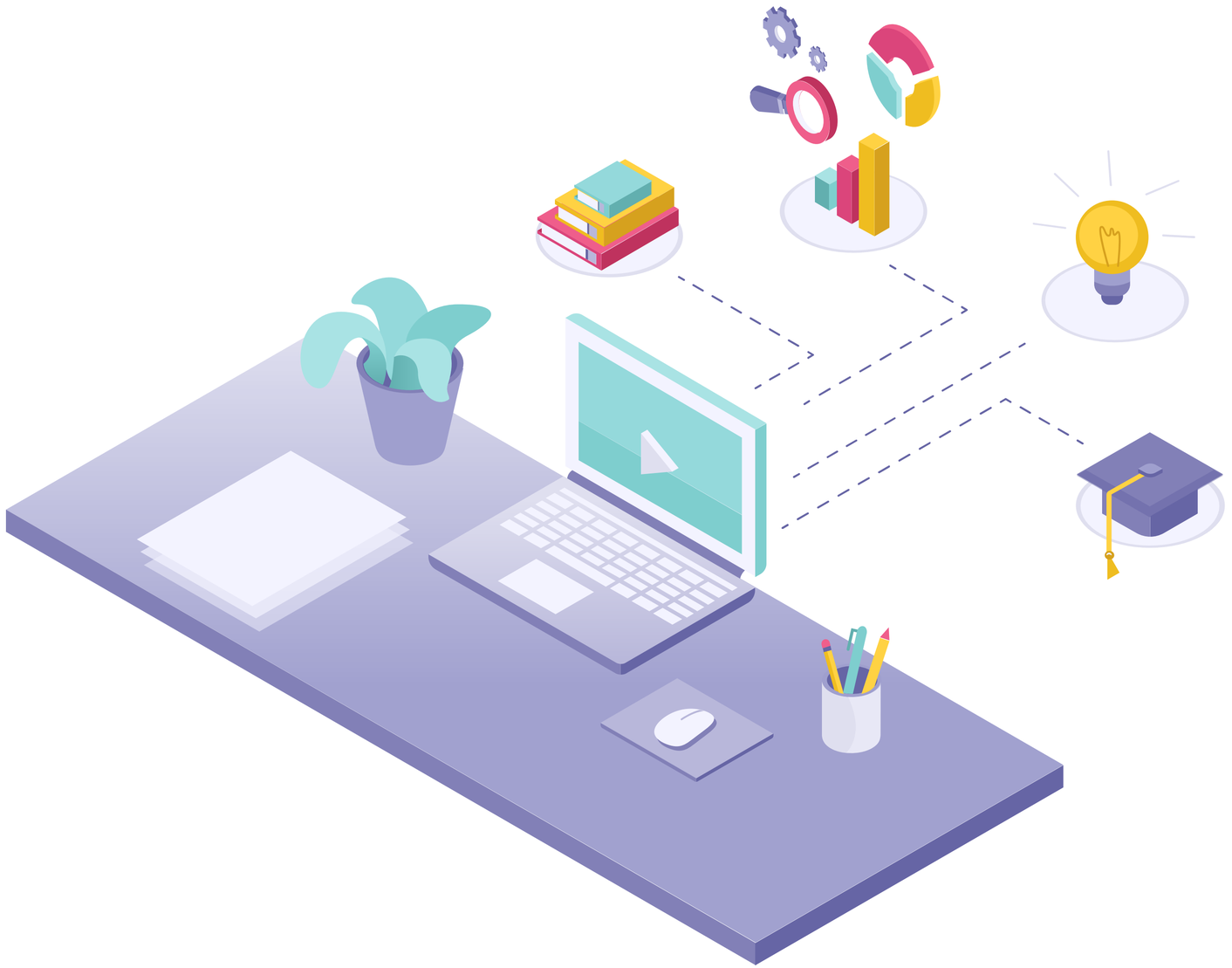
Effet produit : ALLOW (autorisation) ou DENY (refus)

Liste des actions autorisées ou refusées

Bucket et/ou objets ciblés par la politique

On peut également spécifier des conditions.
Exemple : *IP source, chiffrement…*

Amazon Elastic File System (EFS)



Amazon Elastic File System (EFS)



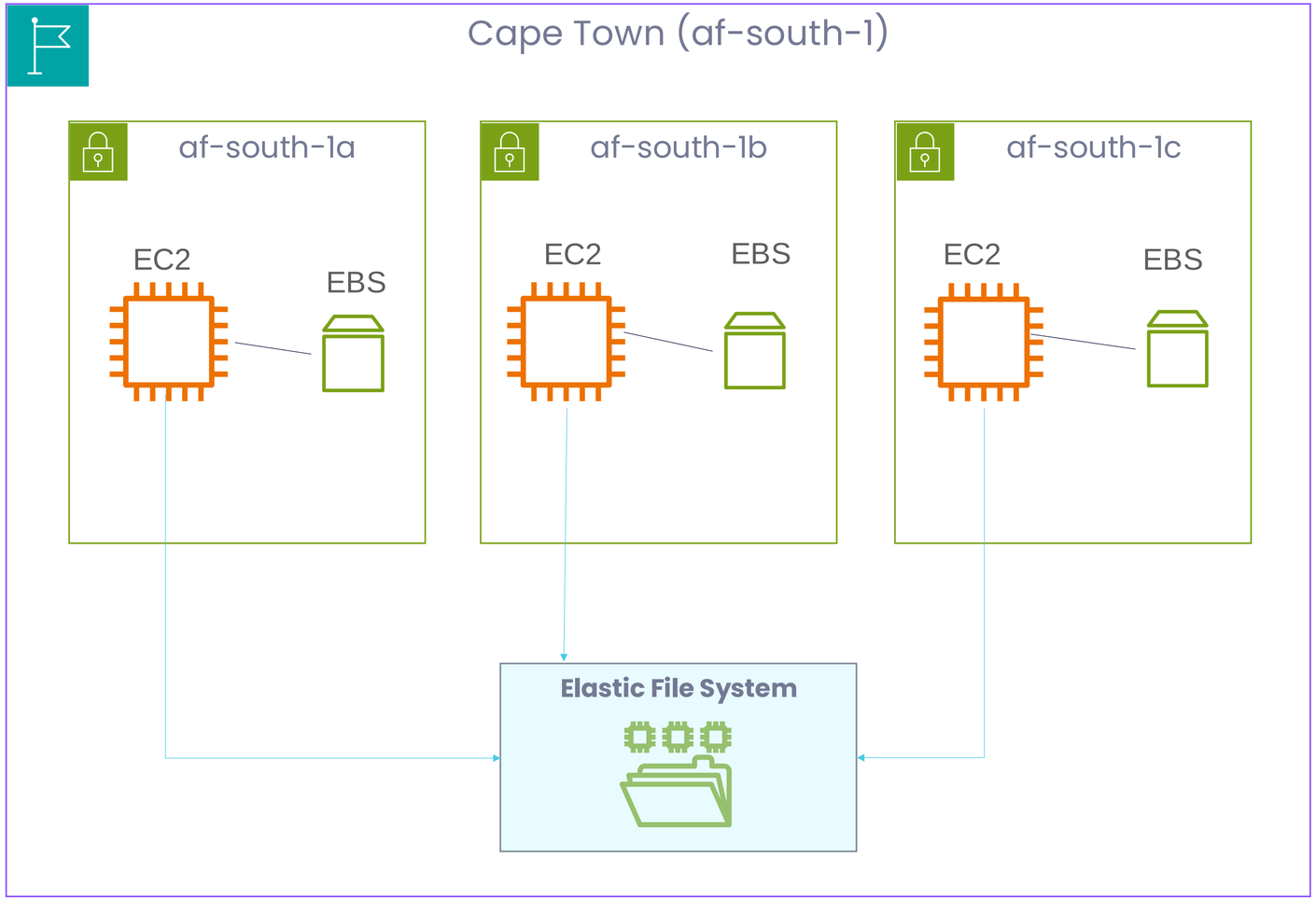
Stockage orienté « **fichier** »

Fournit des **systèmes de fichiers** partagés pour les serveurs **Linux**

Stockage **serverless**, entièrement **élastique**

Utilise le protocole **NFS v4**

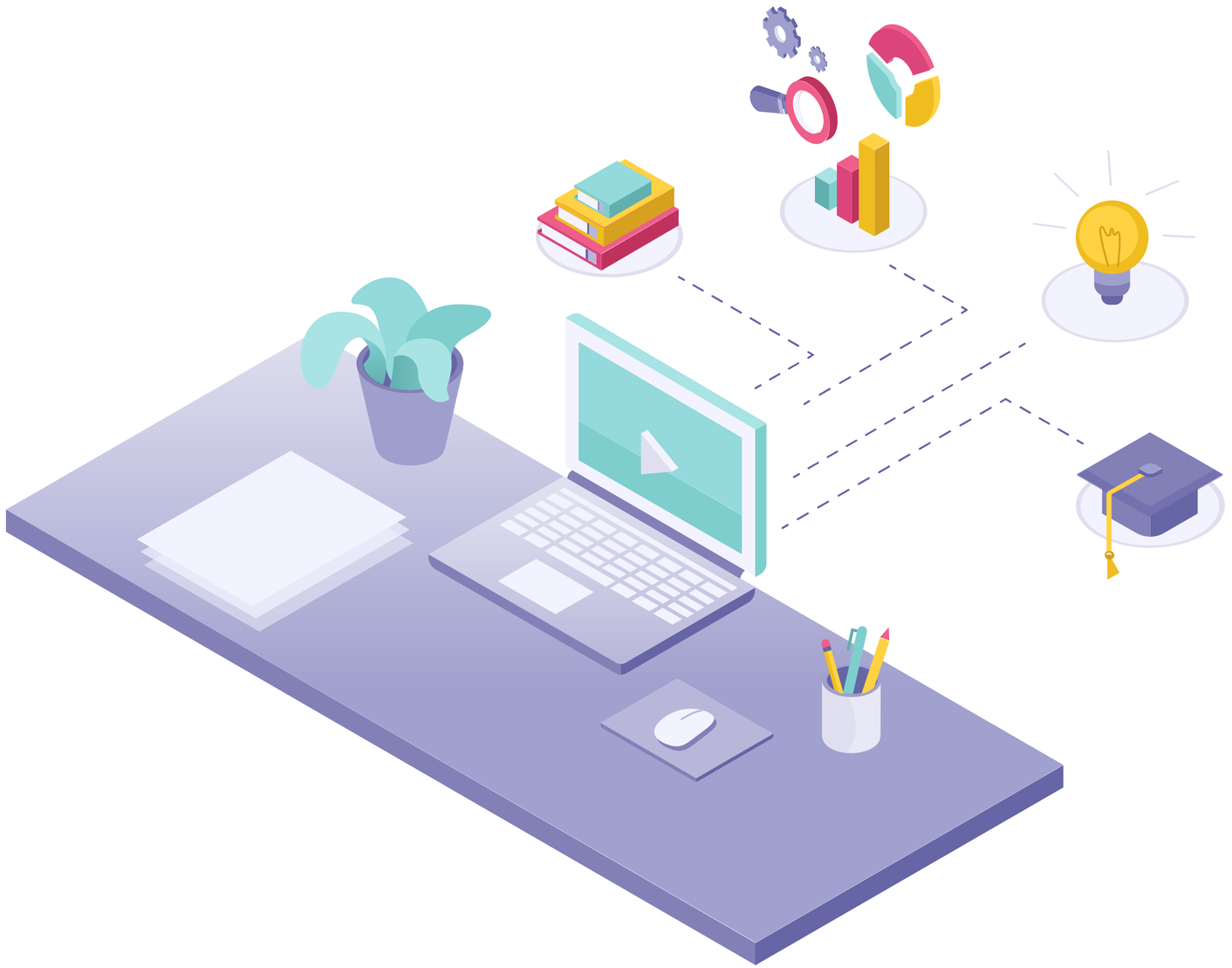
Amazon Elastic File System (EFS)



Multi-AZ

Permet le partage de fichiers (en lecture / écriture) entre **plusieurs instances Linux**

Amazon FSx



Amazon FSx

Fournit des **systèmes de fichiers hautement performants**

Supporte **4 systèmes de fichiers**



Amazon FSx for Windows File Server



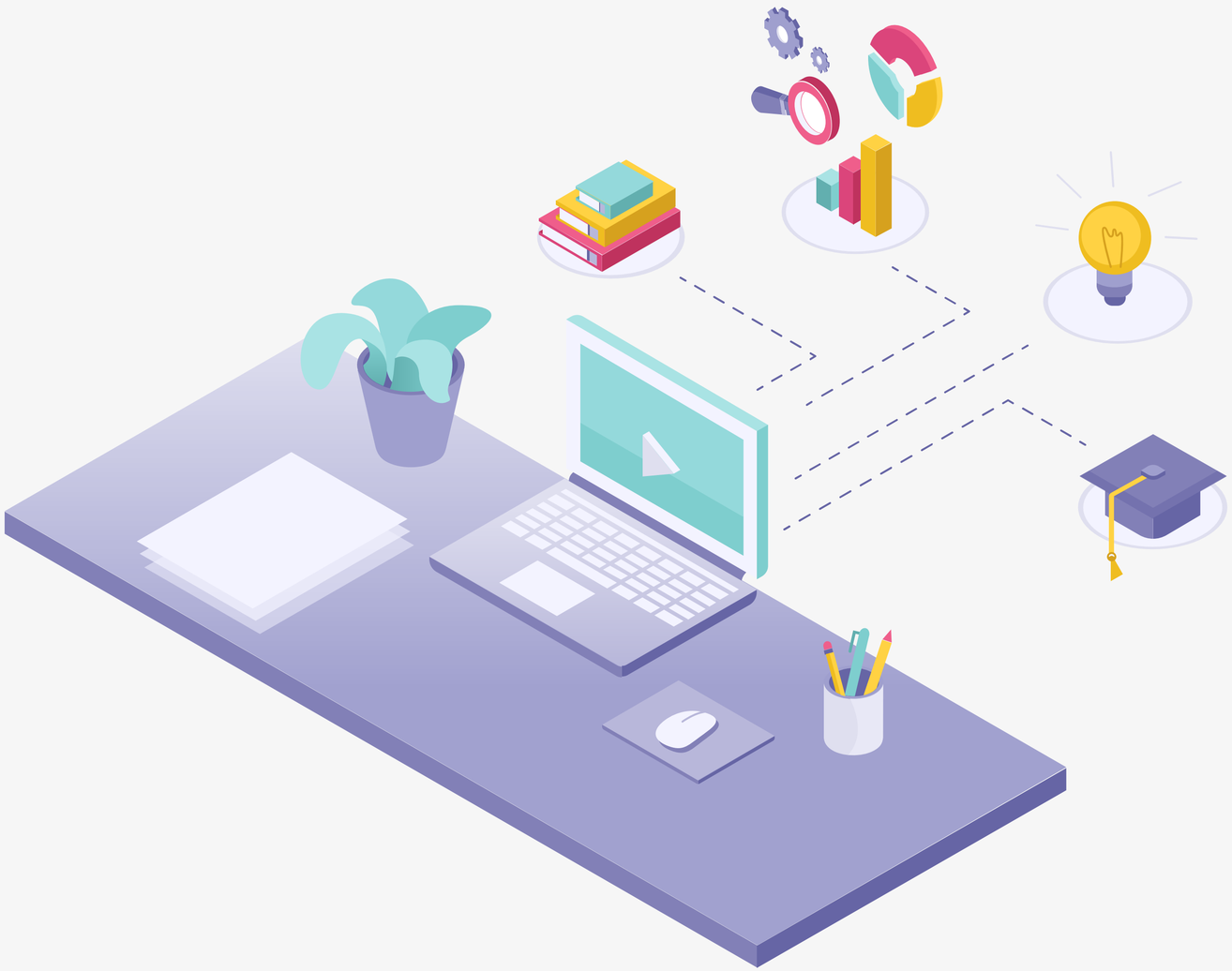
Amazon FSx for Lustre



Amazon FSx for OpenZFS

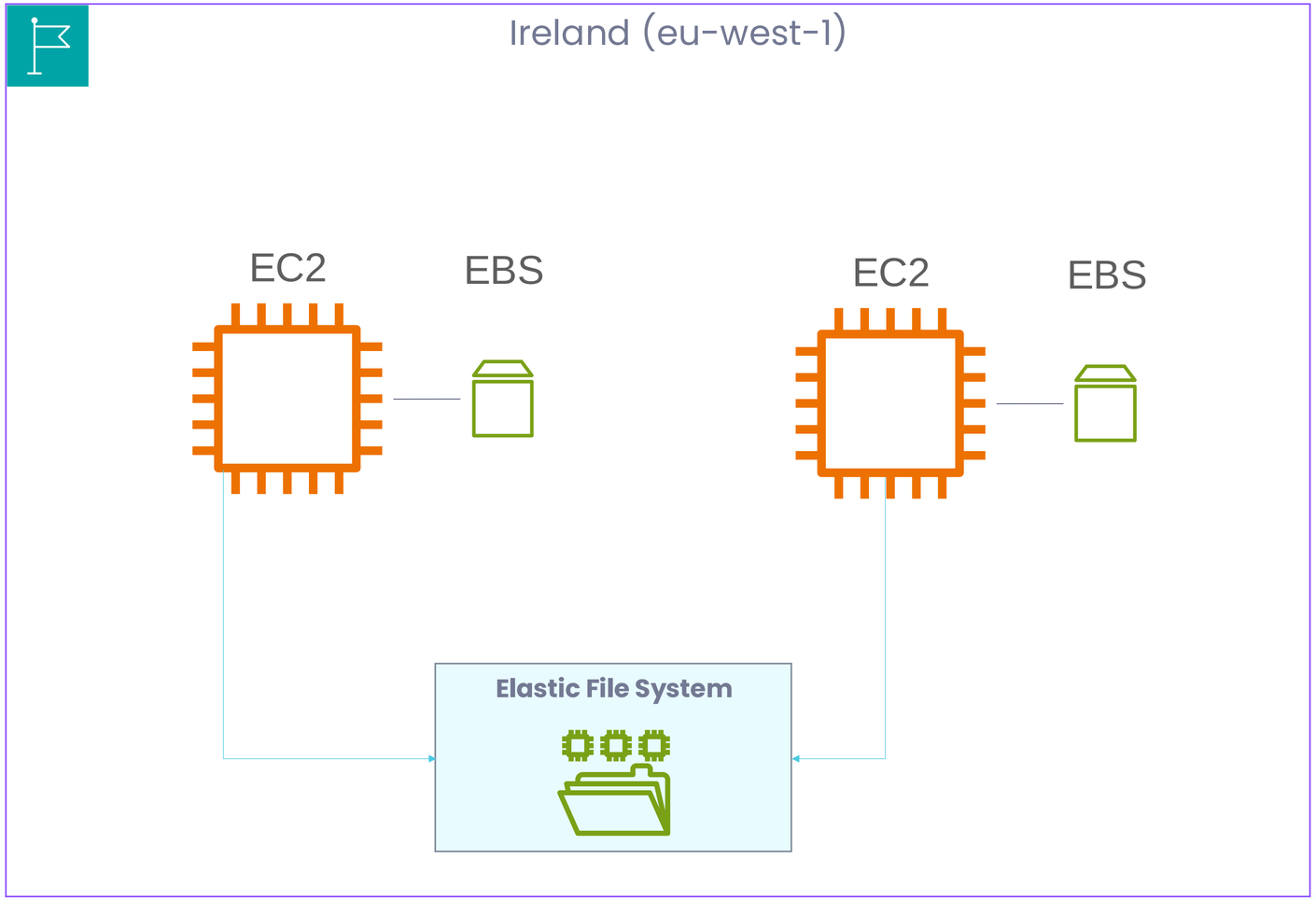


Amazon FSx for NetApp ONTAP

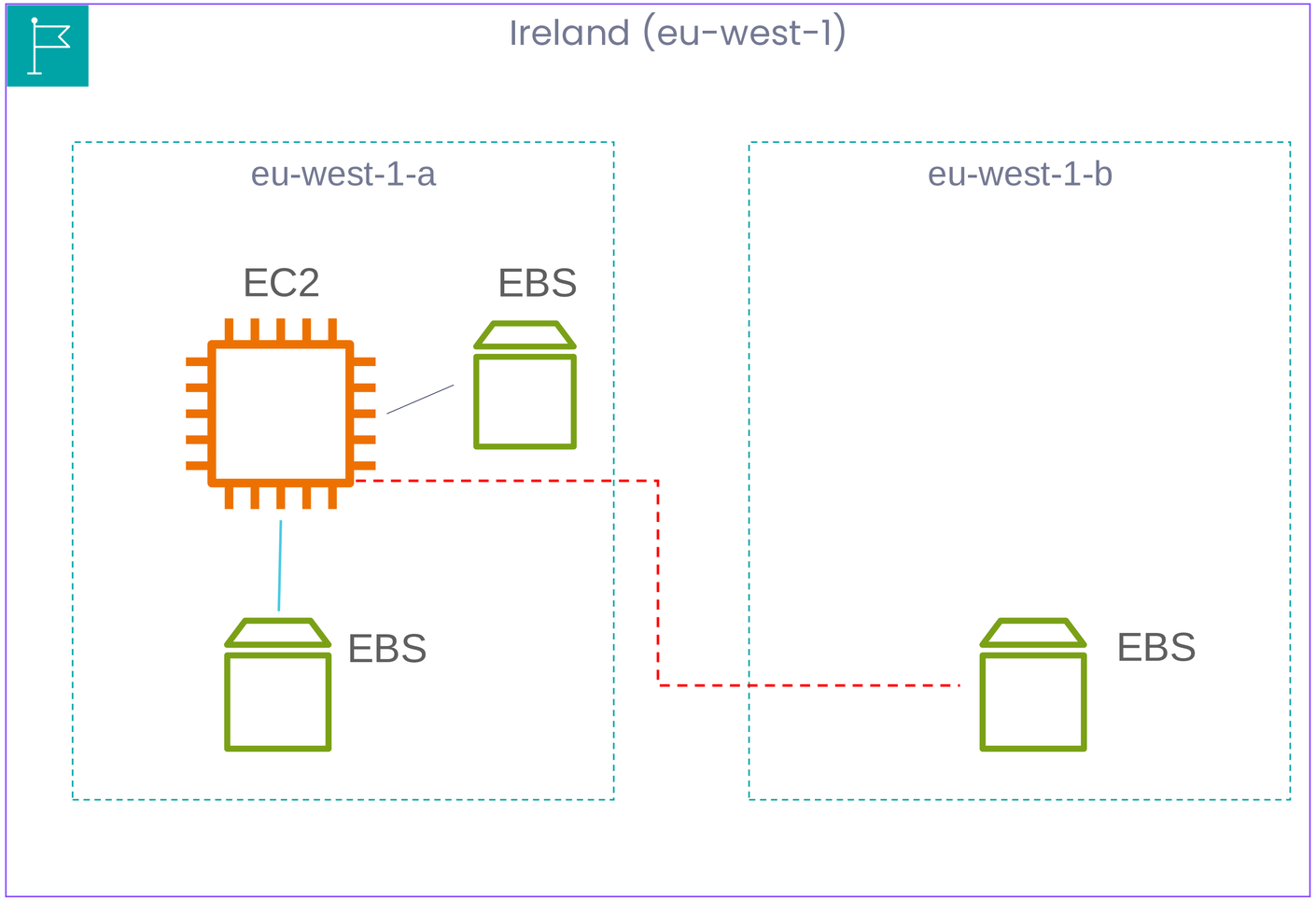


FIN DU MODULE

Lab Amazon Elastic File System (EFS)



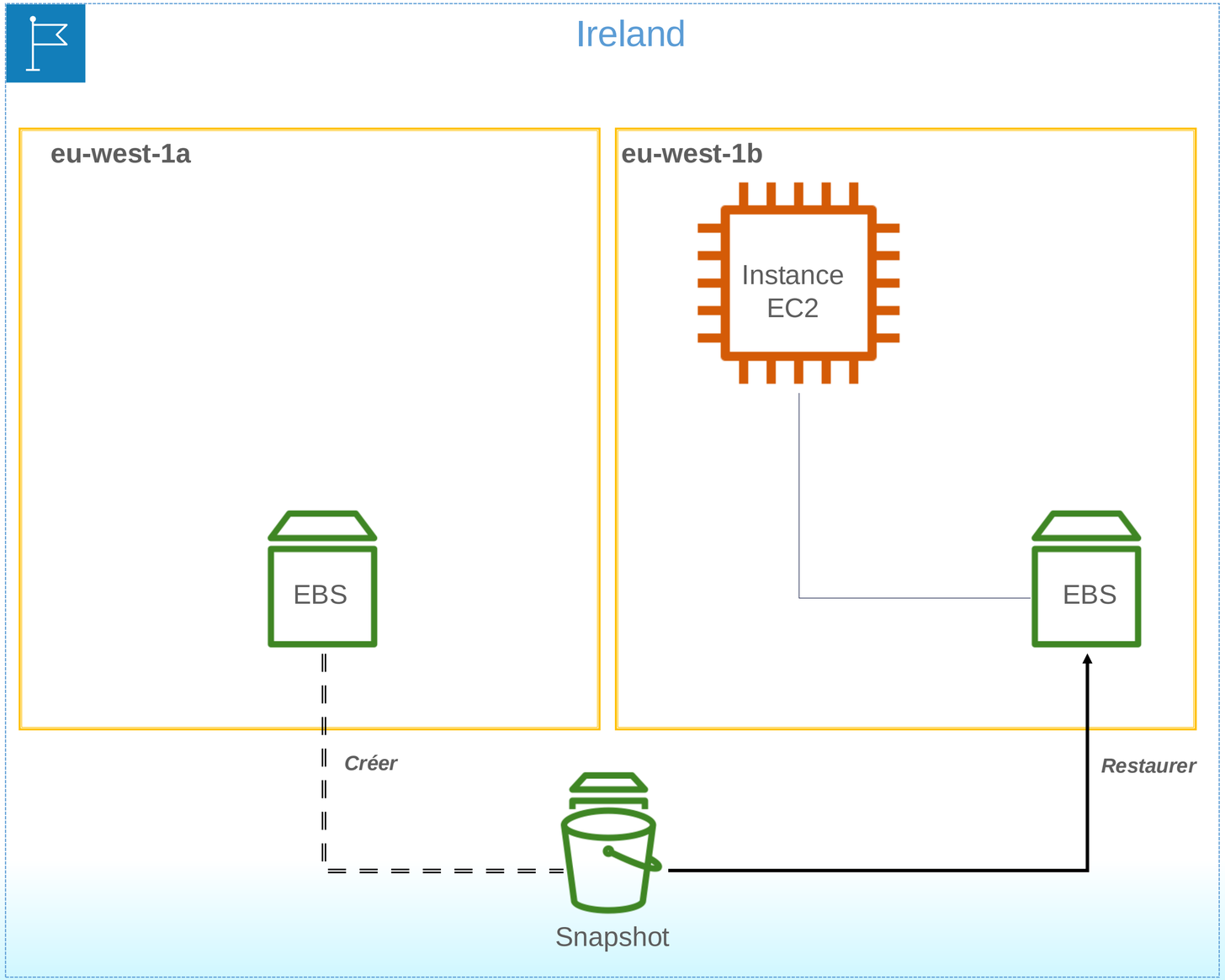
Lab Démarrer avec Amazon EBS



Lab Démarrer avec Amazon EBS

1. Lancer une instance EC2 dans eu-west-1a avec 1 volume EBS de 8 GB
2. Créer 2 volumes EBS dans eu-west-1a et eu-west-1b
3. Attacher les volumes EBS à l'instance EC2
4. Supprimer l'instance EC2 et les volumes EBS

Lab Déplacer un volume EBS à l'aide d'un snapshot EBS

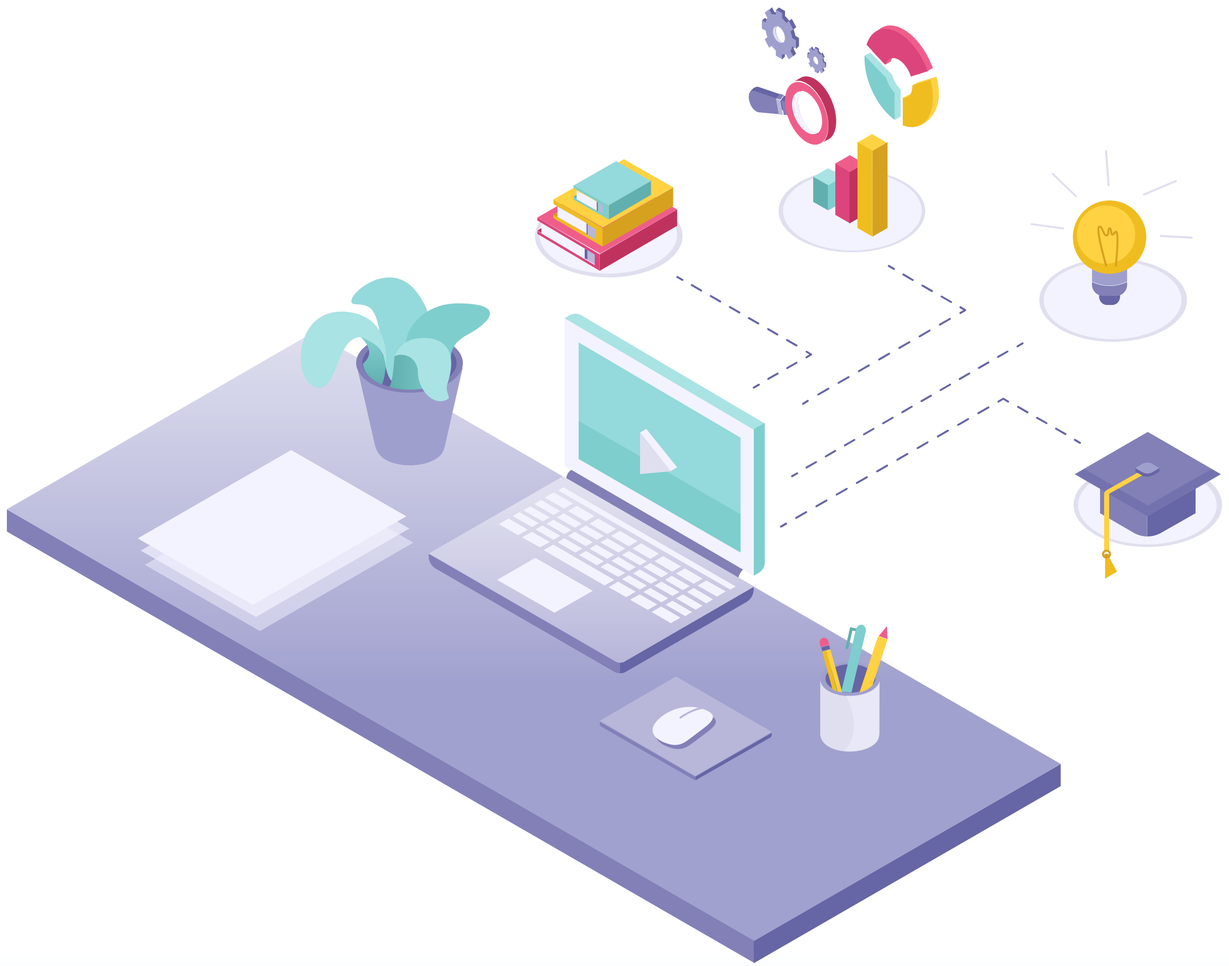


Lab Déplacer un volume EBS à l'aide d'un snapshot EBS

1. Lancer une instance EC2 dans **eu-west-1b**
2. Créer 1 volume EBS dans **eu-west-1a**
3. Créer 1 **snapshot** du volume EBS
4. Restaurer le snapshot vers 1 volume EBS dans **eu-west-1b**
5. **Attacher** le volume à l'instance EC2

Module 8 : BASES DE DONNEES

Une large sélection de bases de données sur mesure pour toutes les entreprises



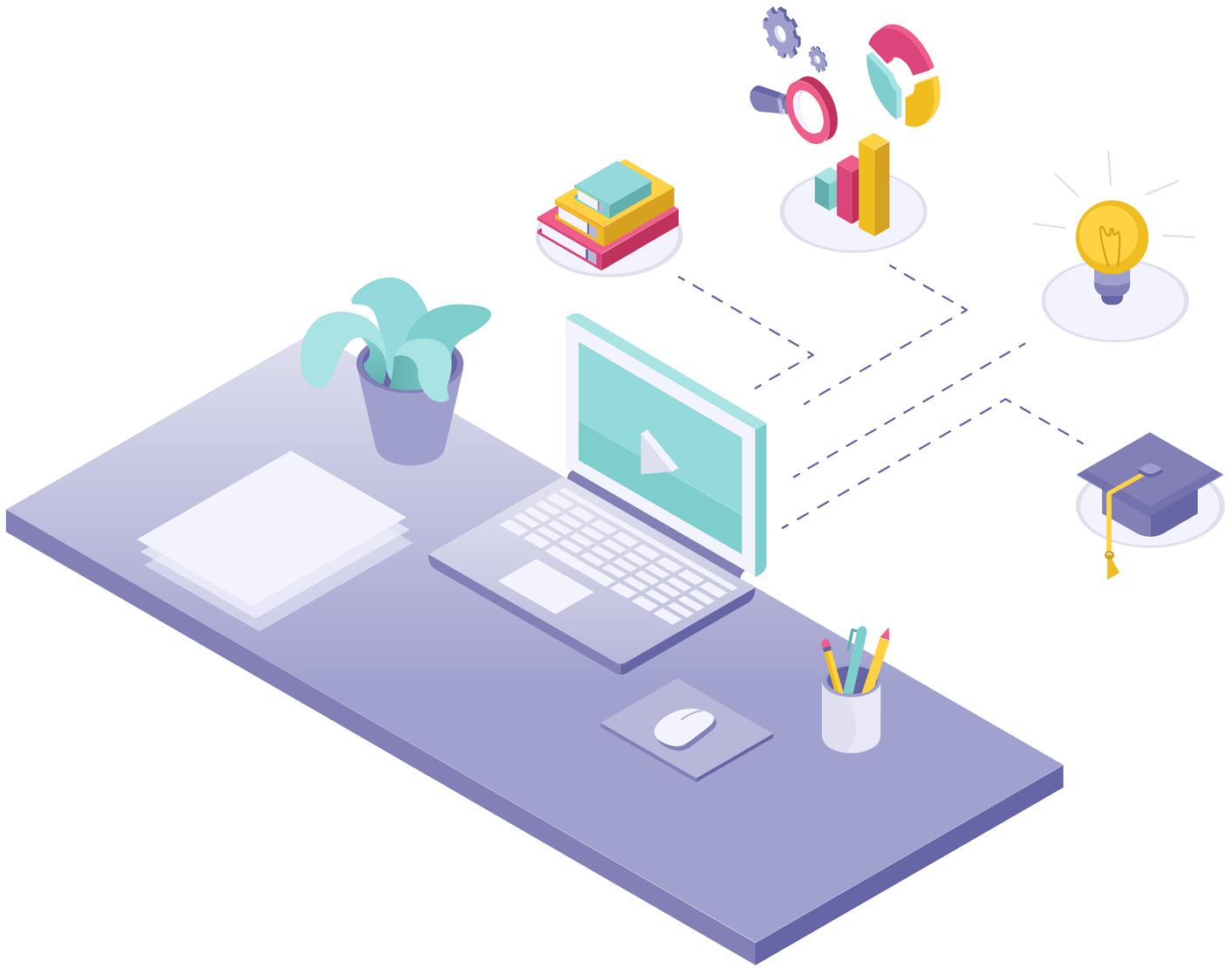
Quelles sont les bases de données supportées ?

Quels sont les services de bases de données ?

Quels sont les avantages de deployer une base de données sur AWS ?



Concepts IT



LeCloudFacile.com

SQL 101

	SQL	NoSQL
Data Storage	Rows and Columns	Key-Value
Schemas	Fixed	Dynamic
Querying	Using SQL	Focused on collection of documents
Scalability	Vertical	Horizontal

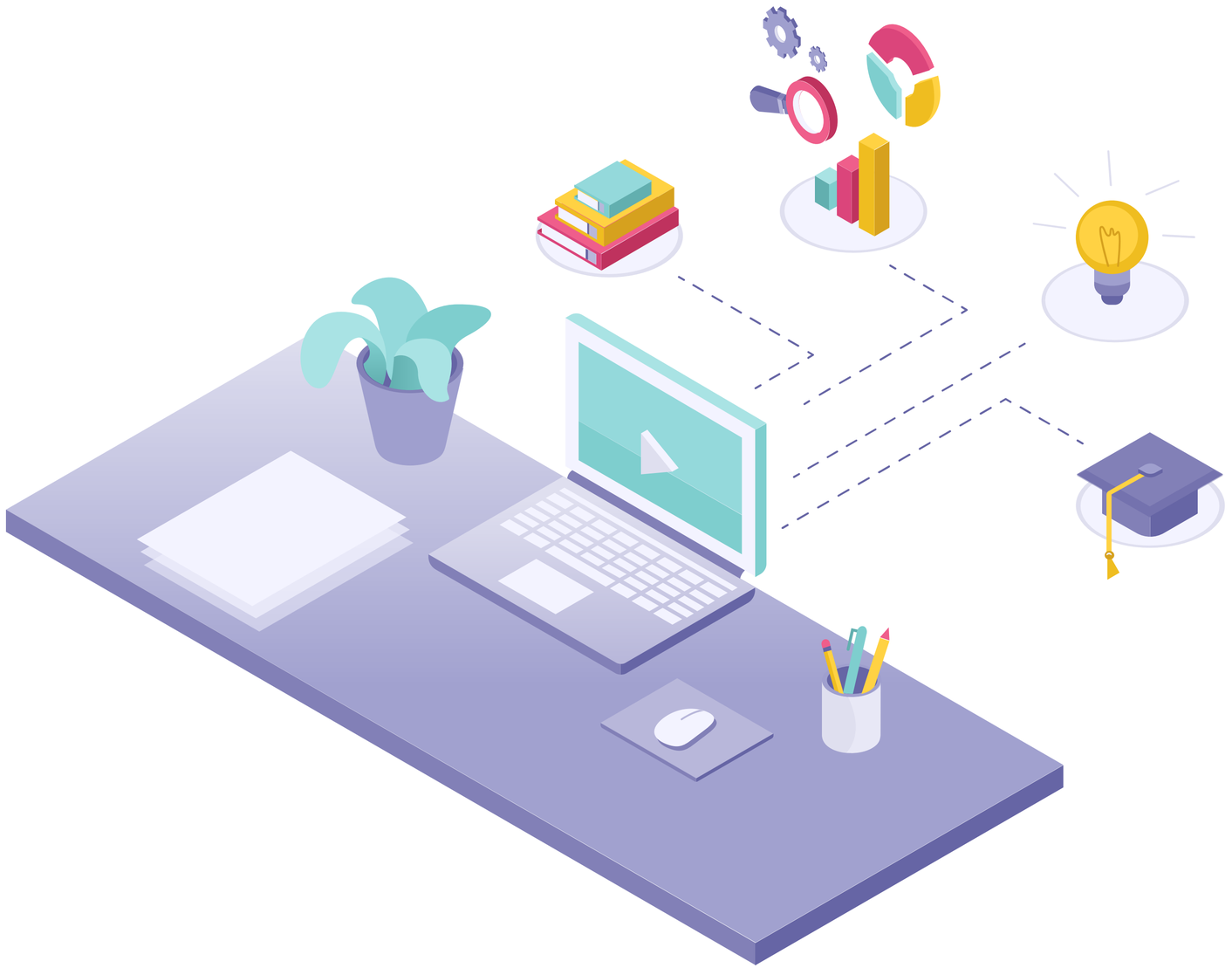
SQL

ISBN	Title	Author	Format
2837272777391	Cloud Computing	Doe, Joe	Paperback
2932536475869	The Database	Gomez, Anna	eBook

NoSQL

```
{
        ISBN: 2837272777391,
        Title: “Cloud Computing”,
        Author: “Doe, Jack”,
        Format: “Paperback”
}
```

Amazon Relational Database Service (RDS)



Amazon Relational Database Service (RDS)

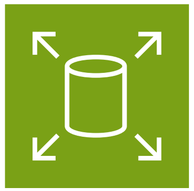
Permet de créer des **bases de données relationnelles entièrement gérées** par AWS



Moteurs supportés

- MySQL
- MariaDB
- PostgreSQL
- Microsoft SQL Server
- Oracle
- Aurora (MySQL/PostgreSQL)

Fonctionnalités d'Amazon RDS



Provisioning automatique

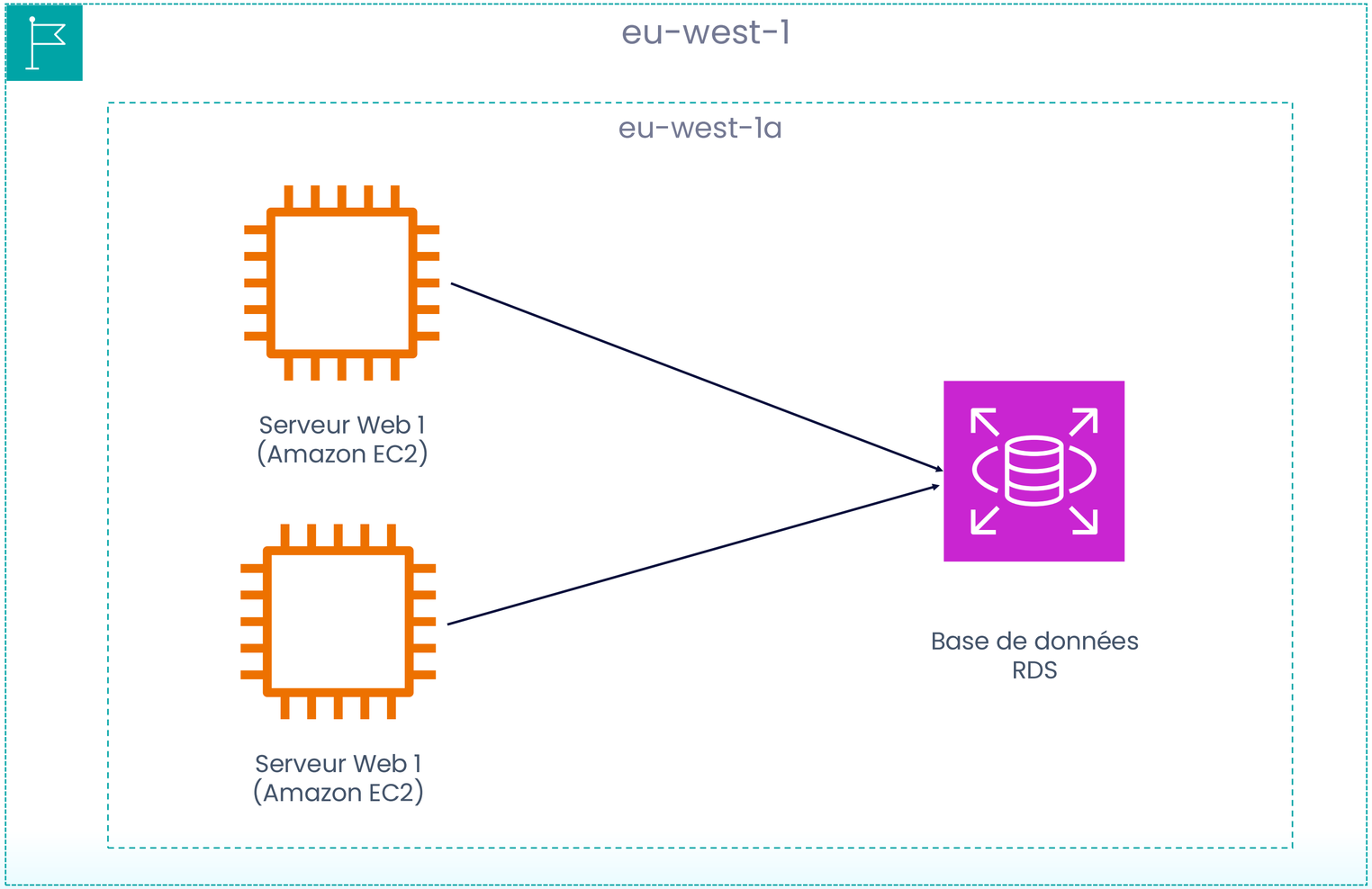
Application automatique des **correctifs logiciels**

Sauvegardes automatiques

Haute disponibilité (**Multi-AZ**)

Replicas de lecture (**Read Replica**)

Architecture Amazon RDS



Gestion de la base de données



Amazon Aurora



Base de données **conçue dans le Cloud**

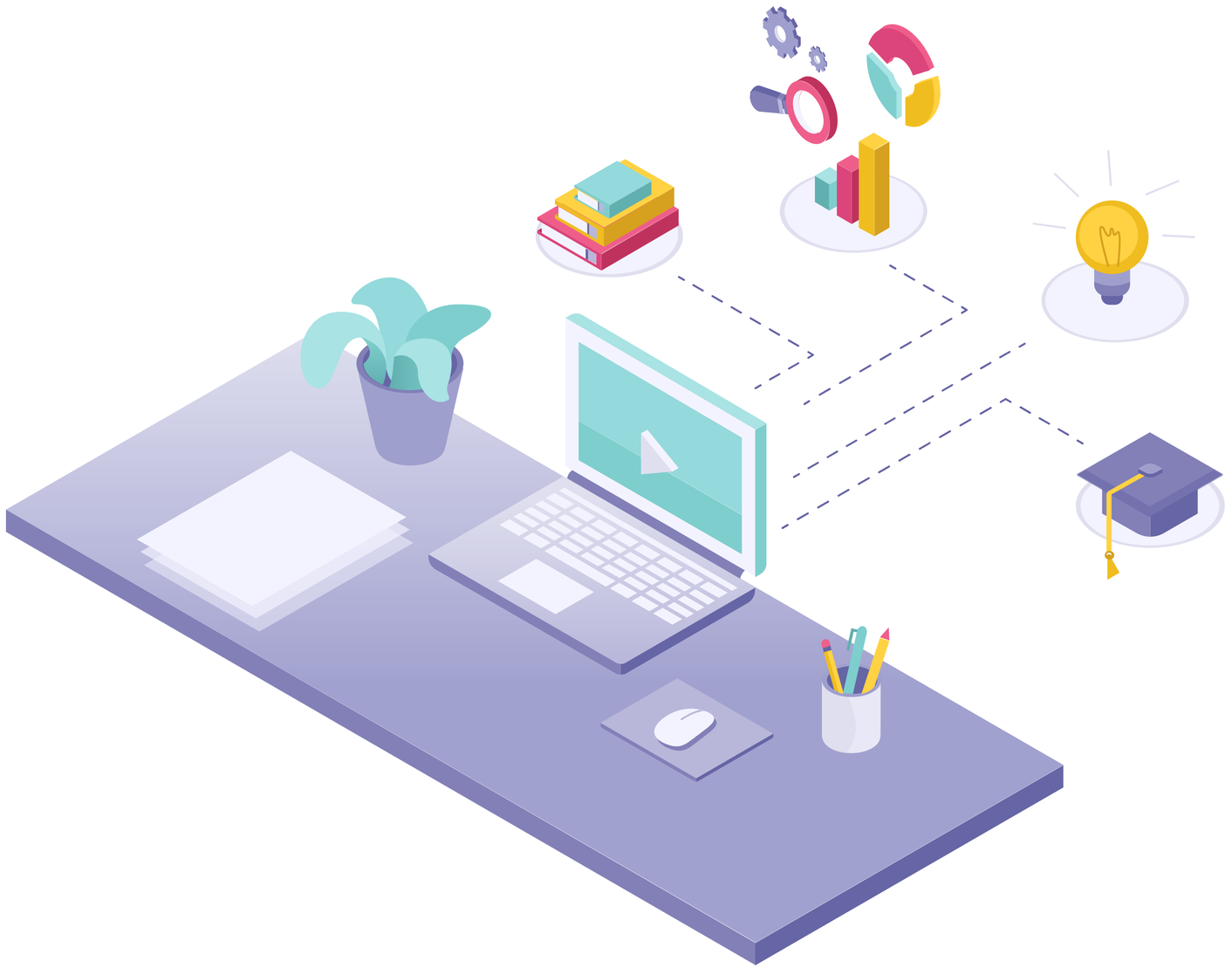
Compatible **MySQL** et **PostgreSQL**

5x plus rapide que MySQL, **3x** plus rapide que PostgreSQL

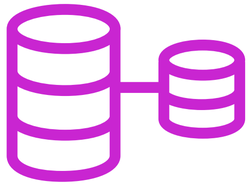
Recommandé pour les besoins de **très haute performance**

Alternative aux **bases de données commerciales** (Oracle,...)

RDS Multi-AZ



RDS Multi-AZ

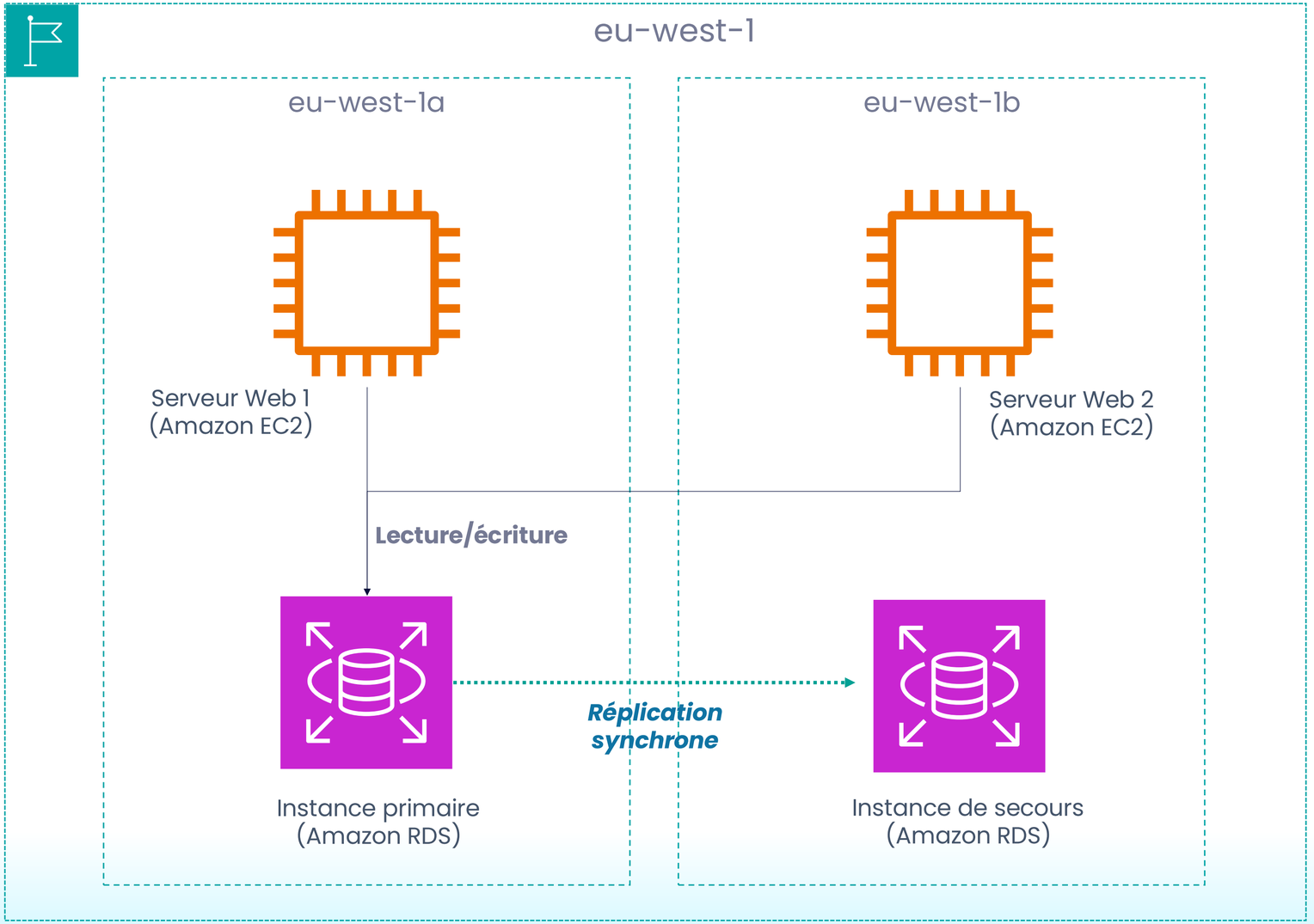


Option de configuration pour la **Haute Disponibilité**

Redondance : réplication de l'instance **primaire** vers une instance(s) de **secours** dans une autre **AZ**.

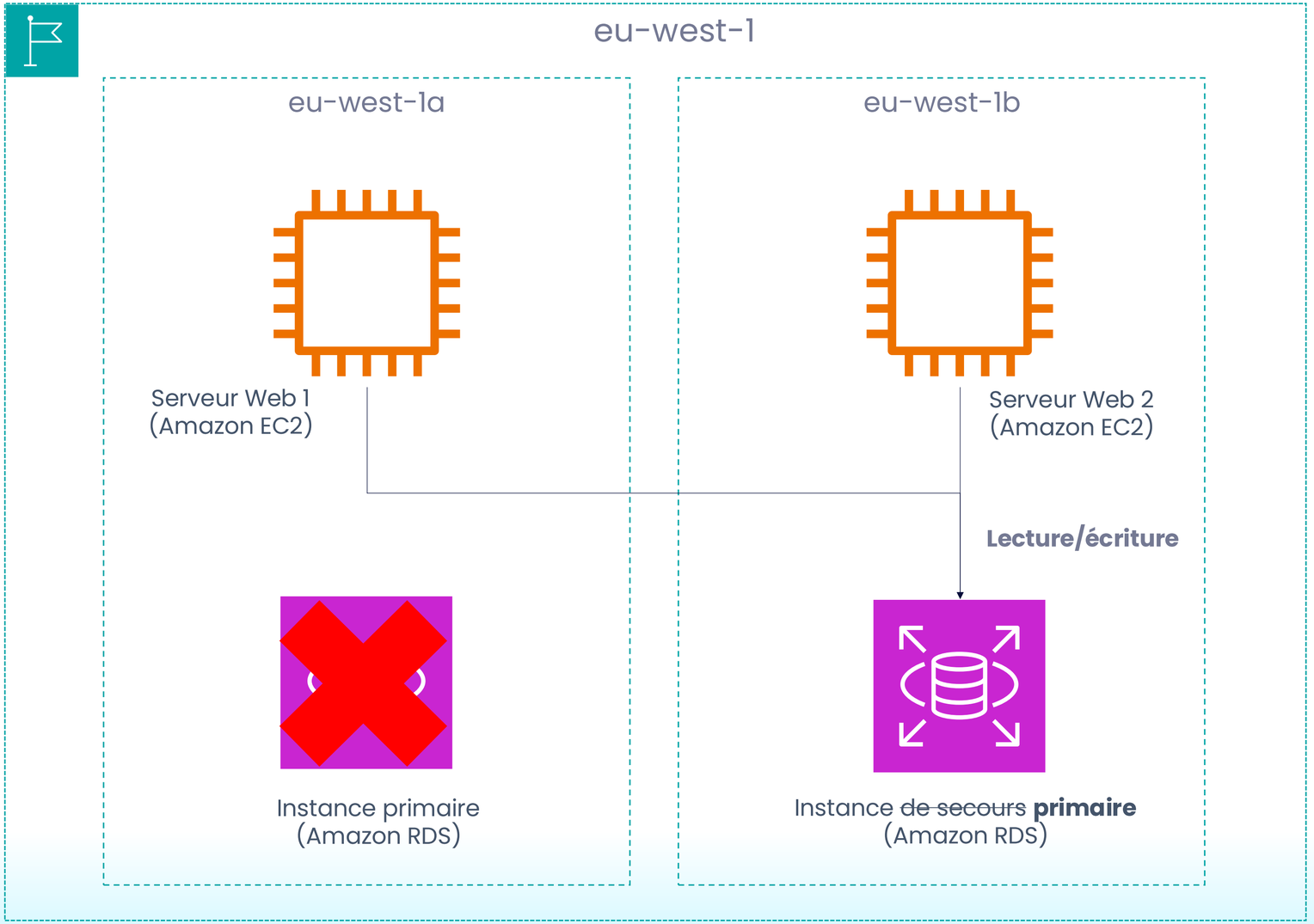
Réplication **synchrone** et gérée par AWS

RDS Multi-AZ

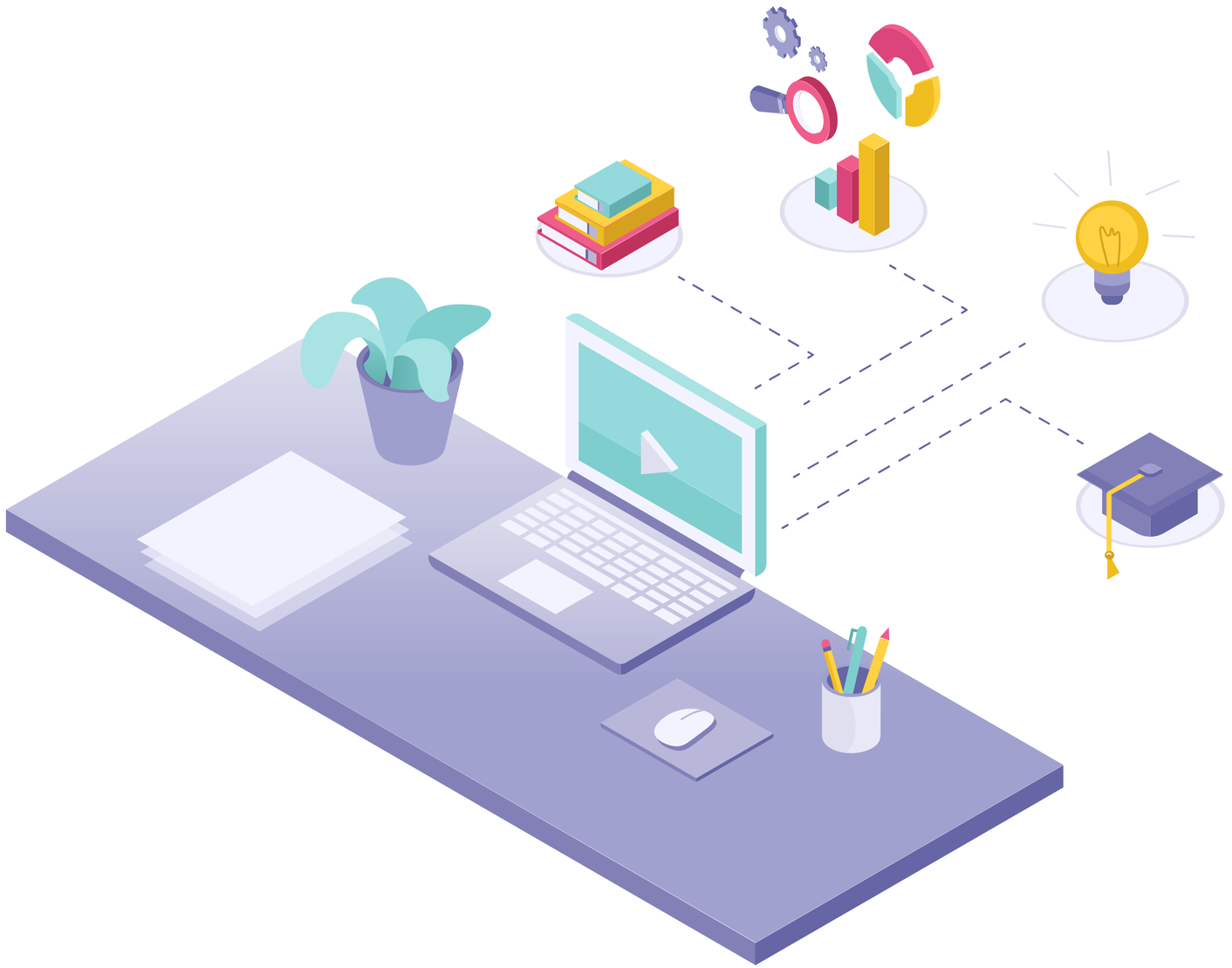

eu-west-1
eu-west-1a
eu-west-1b
Serveur Web 1
(Amazon EC2)
Serveur Web 2
(Amazon EC2)
Lecture/écriture
Réplication
synchrone
Instance primaire
(Amazon RDS)
Instance de secours
(Amazon RDS)

RDS Multi-AZ

PANNE DE l'INSTANCE PRIMAIRE



RDS Read Replica



RDS Read Replica

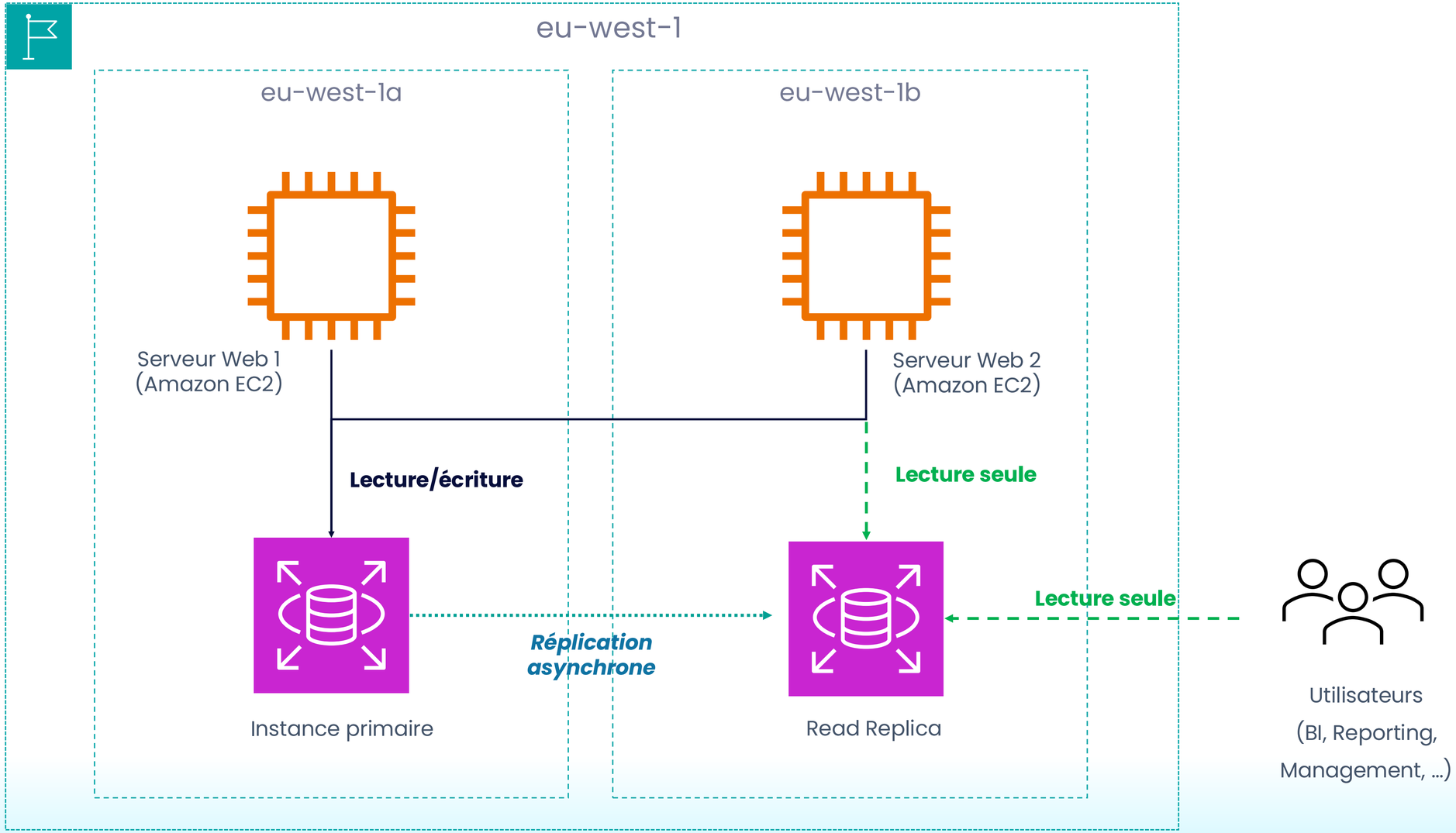


Option de configuration RDS qui permet d'**augmenter la performance de lecture**

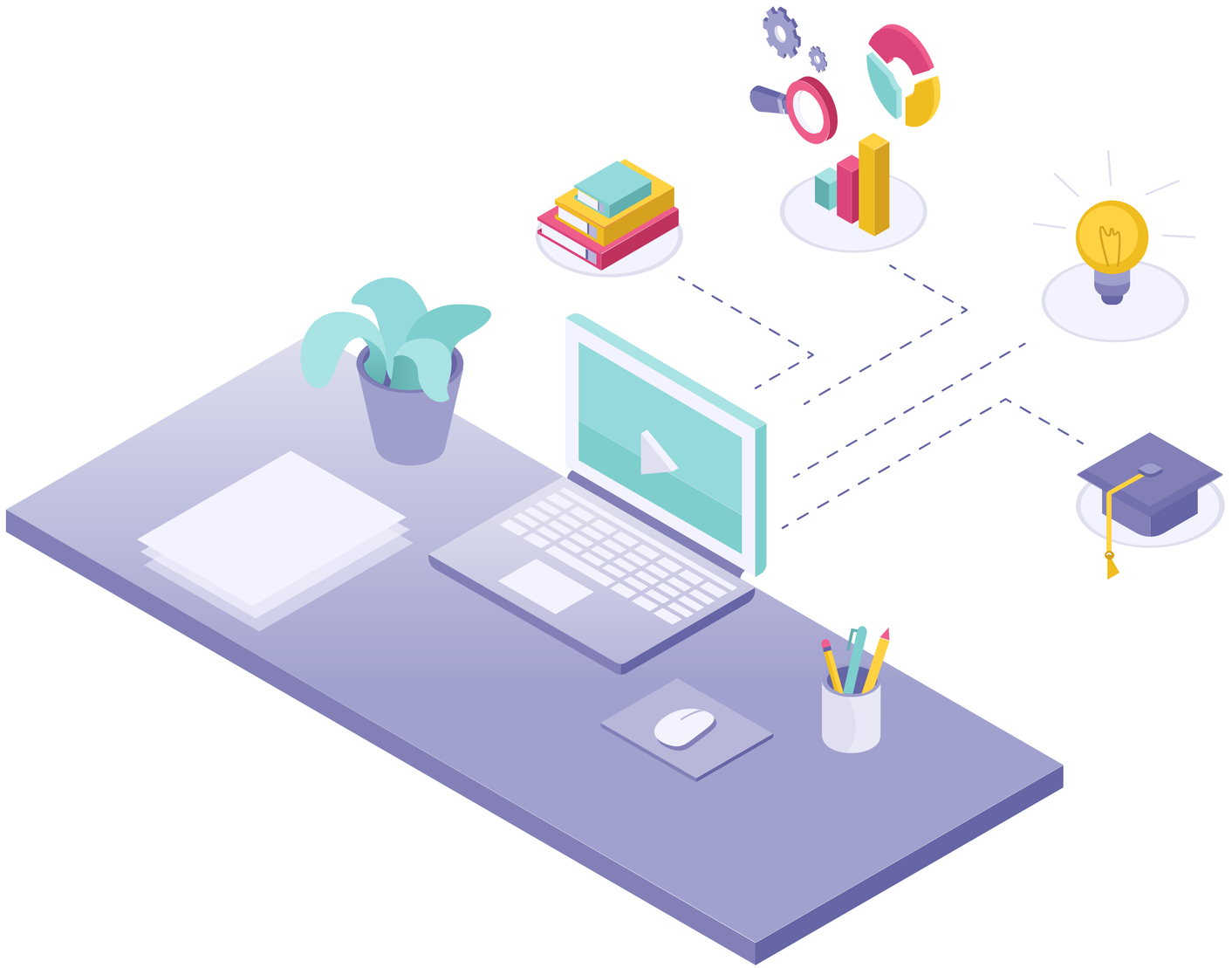
Read replicas dans la même région ou une autre région (**cross region**)

Réplication asynchrone entre l'instance primaire et le(s) Read Replica (s)

RDS Replica


eu-west-1
eu-west-1a
eu-west-1b
Serveur Web 1
(Amazon EC2)
Serveur Web 2
(Amazon EC2)
Lecture/écriture
Lecture seule
Réplication
asynchrone
Lecture seule
Instance primaire
Read Replica
Utilisateurs
(BI, Reporting,
Management, ...)

Les sauvegardes Amazon RDS



Les sauvegardes Amazon RDS

Automated Backups

Sauvegardes automatiques et quotidiennes de votre base de données

Snapshots manuels

Sauvegardes manuelles lancées par l'utilisateur



Automated Backups (sauvegardes automatiques)

Automated Backups

AWS sauvegarde automatiquement votre base de données tous les jours.

Vous choisissez la **fenêtre de sauvegarde**

Période de rétention : entre 1 et 35 jours max

Snapshots manuels (Instantanés)

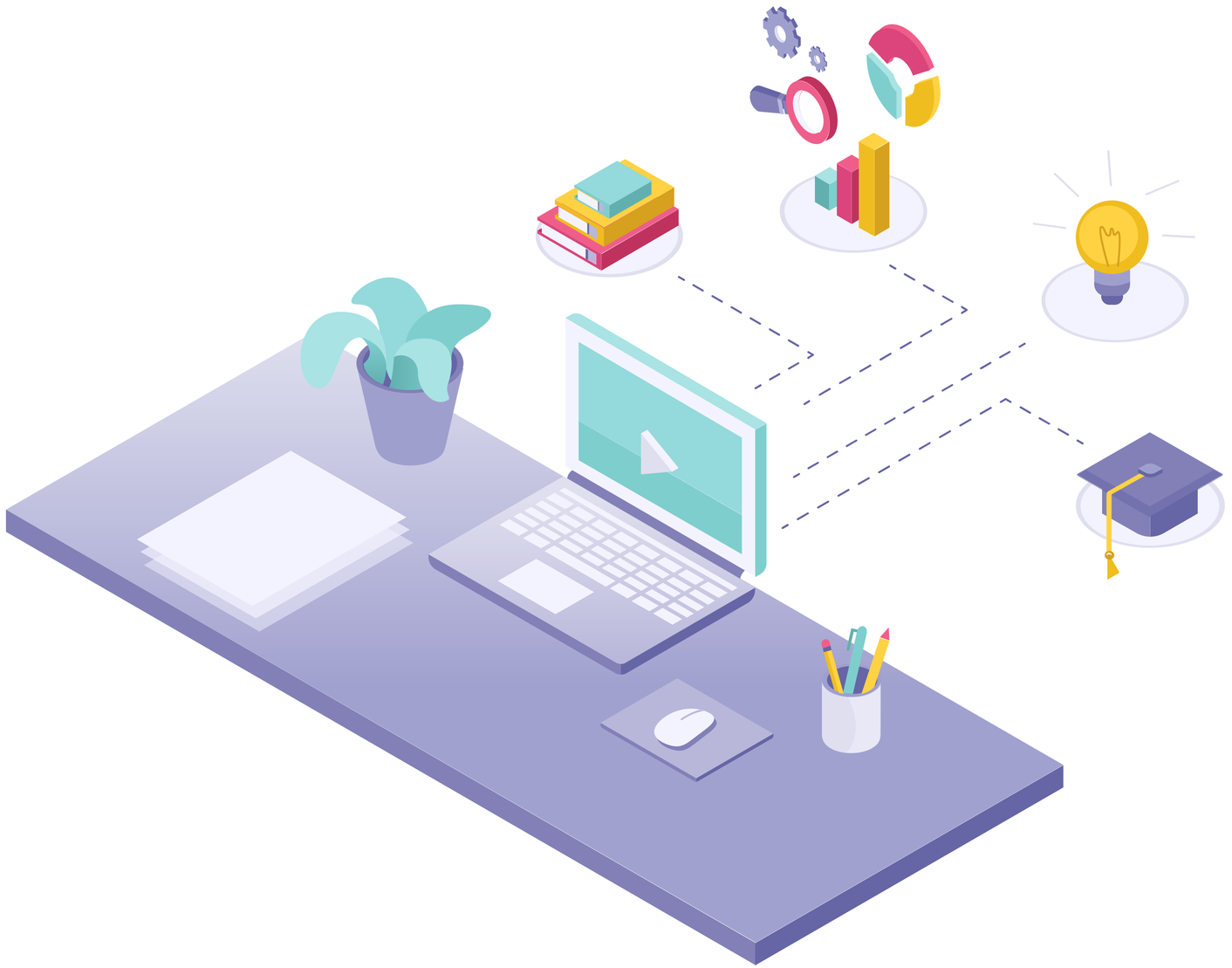
Snapshots manuels

Vous créez vos sauvegardes (via console, SDK ou API)

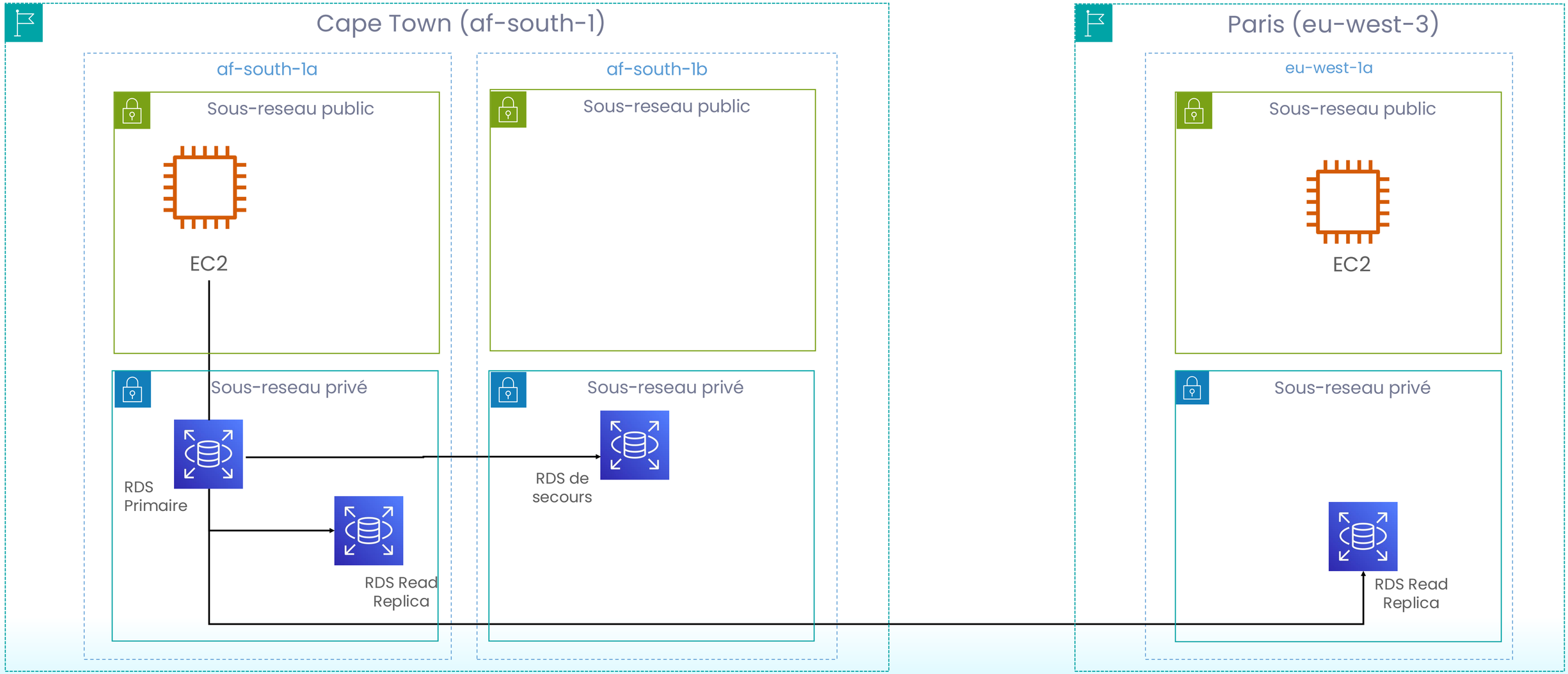
Backup à un instant T de la base de données

Rétention : indéfinie jusqu'à suppression **par l'utilisateur**

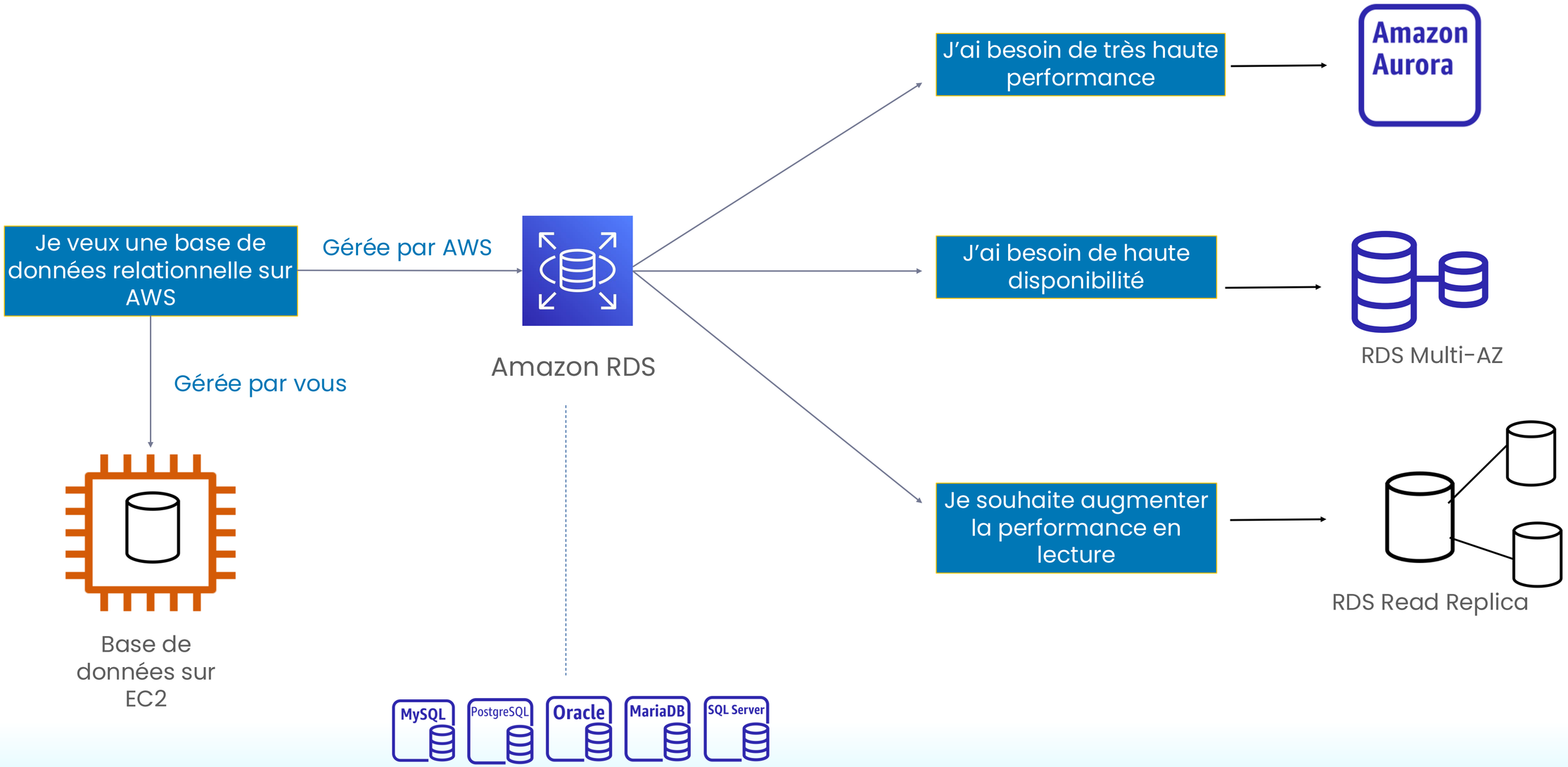
RDS Architecture



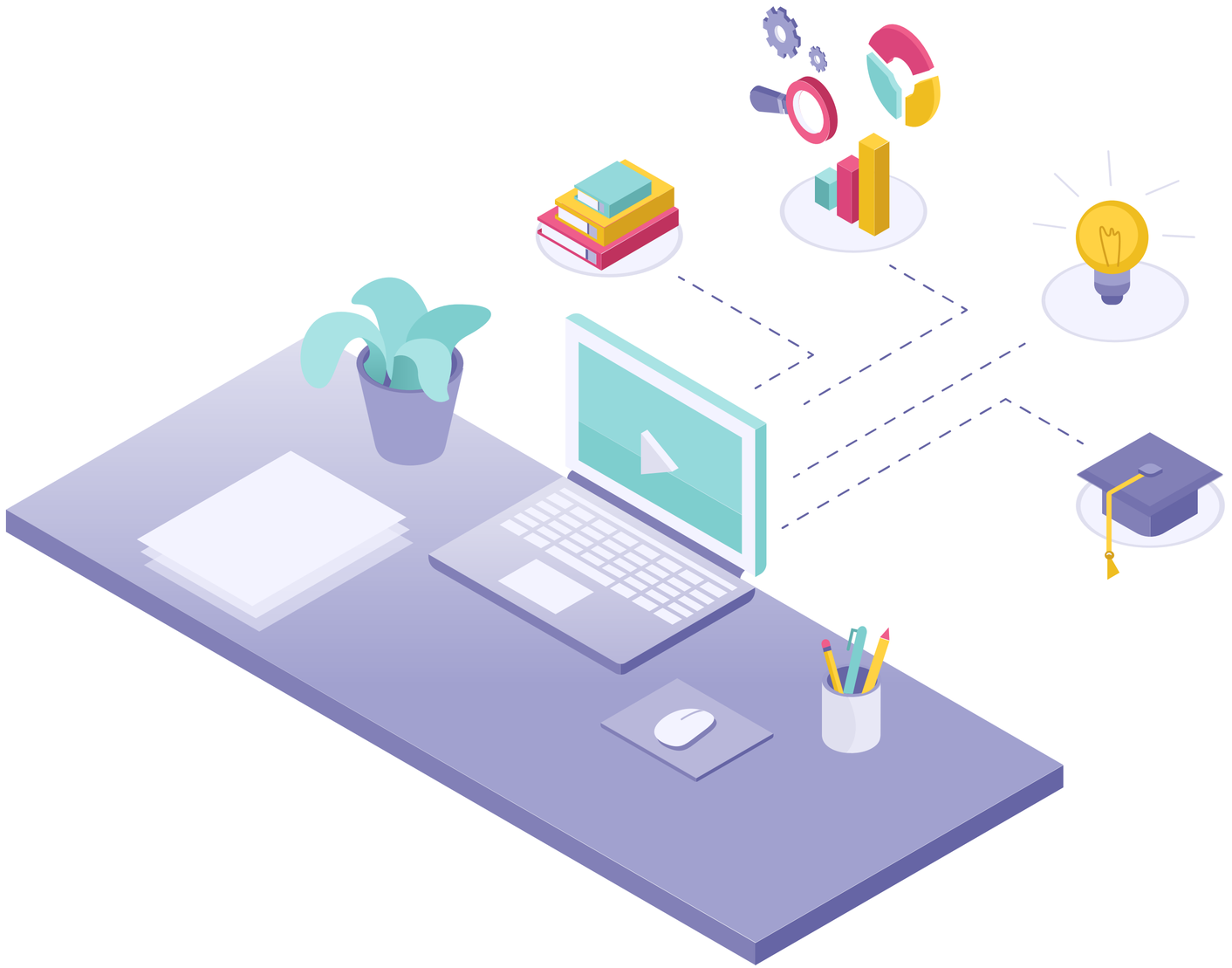
Architecture : RDS Multi-AZ et Read replica



Choisir sa base de données sur AWS



AWS Database Migration Service (DMS)



Migration homogène avec AWS DMS



Permet de **migrer vos bases de données** sur site vers AWS

Permet également de **changer de type** de base de données

Migration homogène (PostgreSQL -> PostgreSQL) ou hétérogène

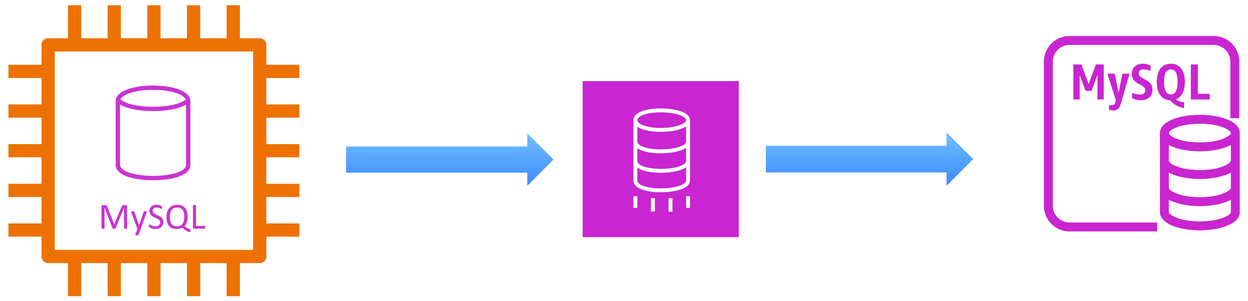
(Oracle -> MySQL)

Supporte les migrations **sans interruption de service**

LeCloudFacile.com

Types de migration

Homogène



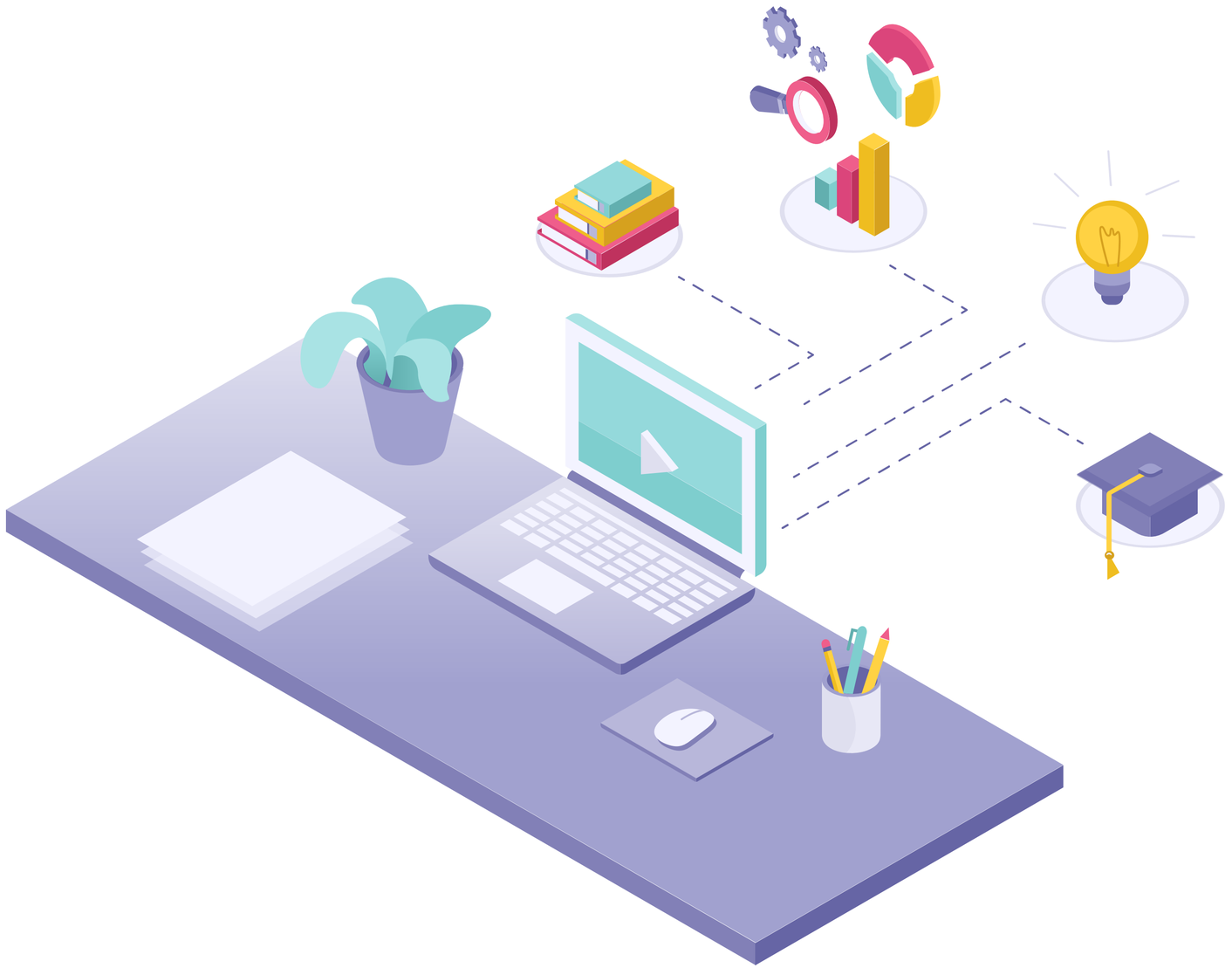
Instance EC2 — AWS DMS — RDS MySQL

Hétérogène



Oracle — AWS DMS — PostgreSQL

Bases de données NoSQL sur AWS



Les bases de données NoSQL



NoSQL = Not Only SQL -> « *Non relationnel* »

Schémas ***flexibles,*** Haute Performance & mise à l'échelle facile

Support de nouveaux cas d'usage : Big Data, IOT, E-commerce, Réseaux sociaux,...

Types : clé/valeur, document, graphe, colonne,...

Exemples : MongoDB, Cassandra, Hbase, Neo4J, Redis,...

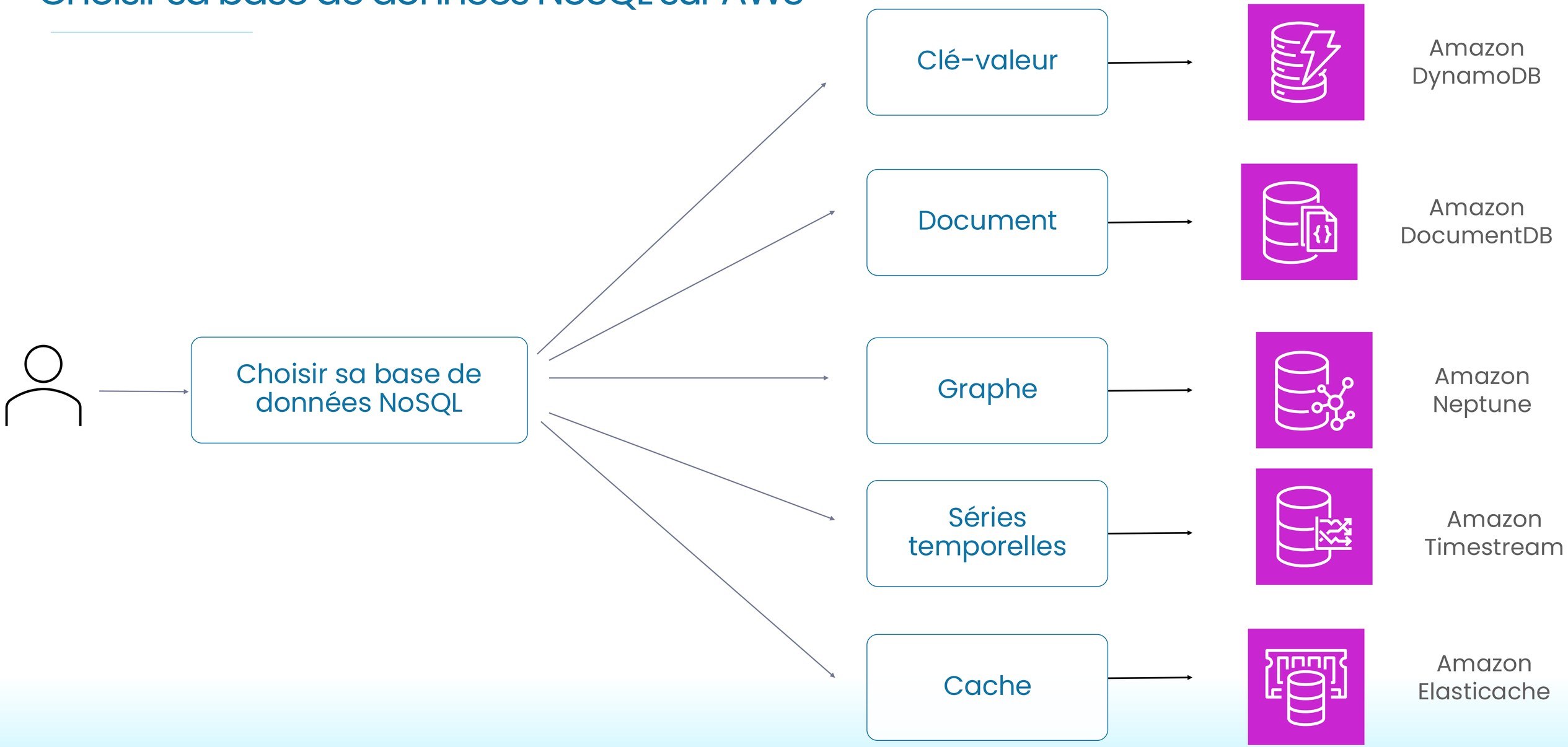
Les types de bases de données NoSQL

Chaque type répond à des besoins spécifiques / cas d'usage

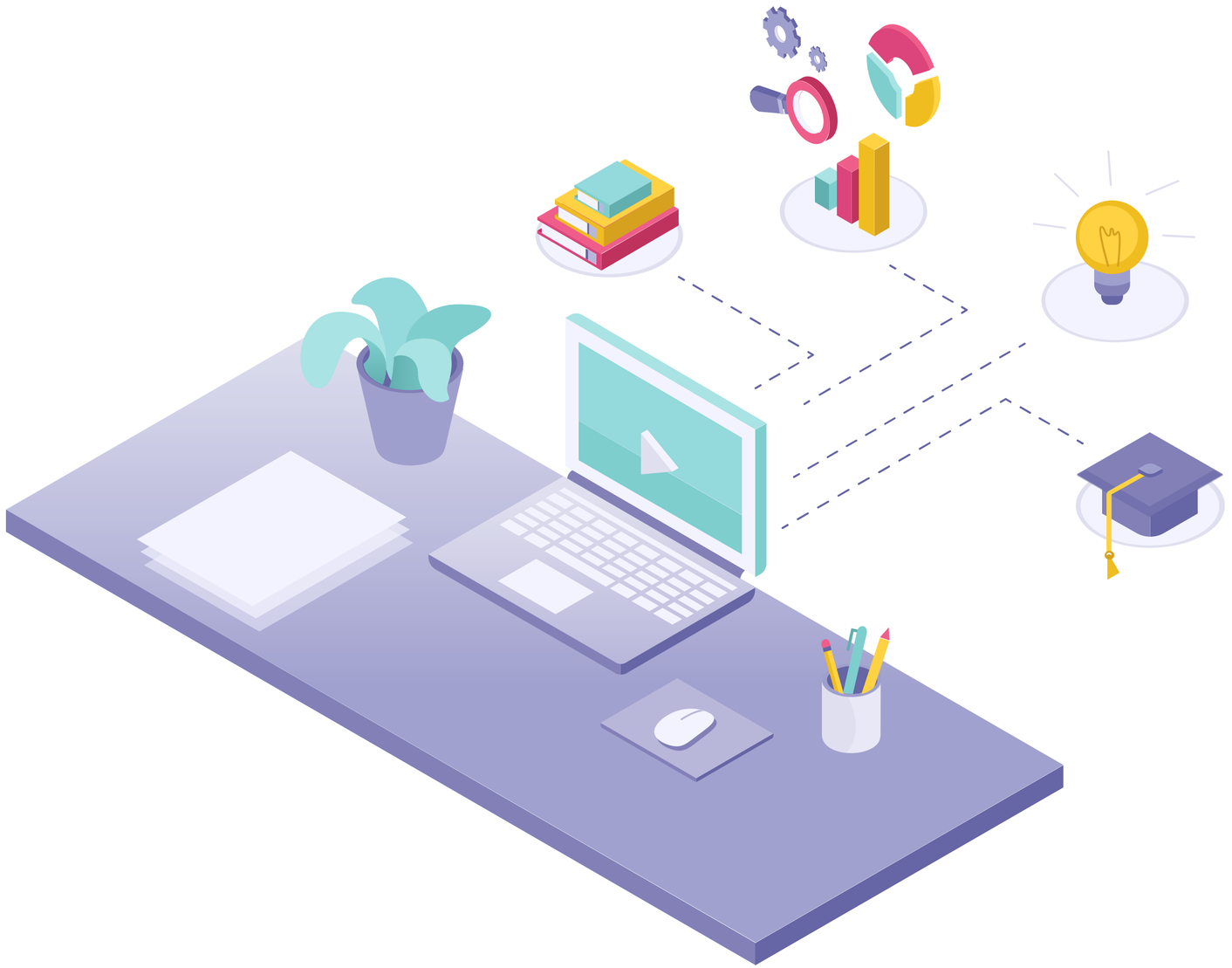
Clé-valeur	Document	Colonne	Graphe	Séries temporelles	Cache
• Redis	• MongoDB	• Apache Cassandra	• Neo4j	• InfluxDB	• Redis
• DynamoDB	• CouchDB	• HBase	• Amazon Neptune	• TimescaleDB	• Memcached
• …	• …	• …	• …	• …	• …

LeCloudFacile.com

Choisir sa base de données NoSQL sur AWS



Amazon DynamoDB



Amazon DynamoDB



Base de données **NoSQL**, et orientée **Clé-valeur**

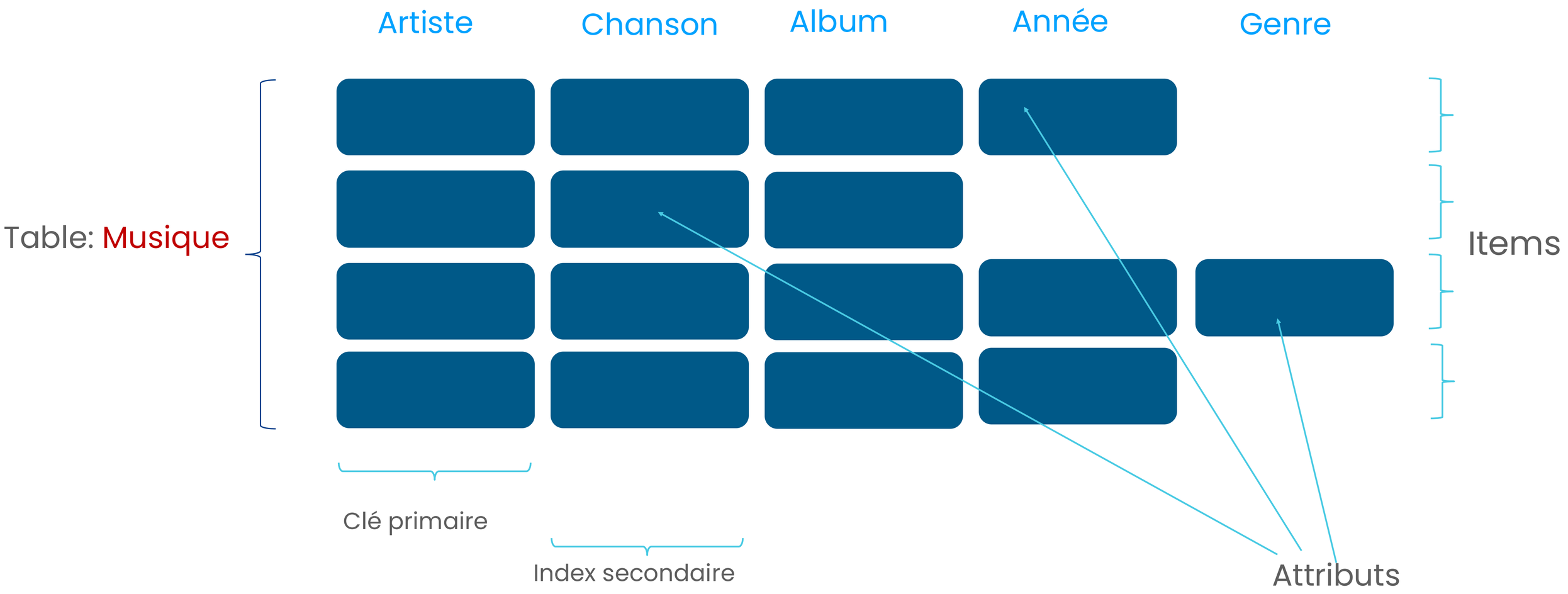
Entièrement Serverless & hautement disponible (jusqu'à 99,999%)

Haute performance (single-digit millisecond) et durabilité élevée

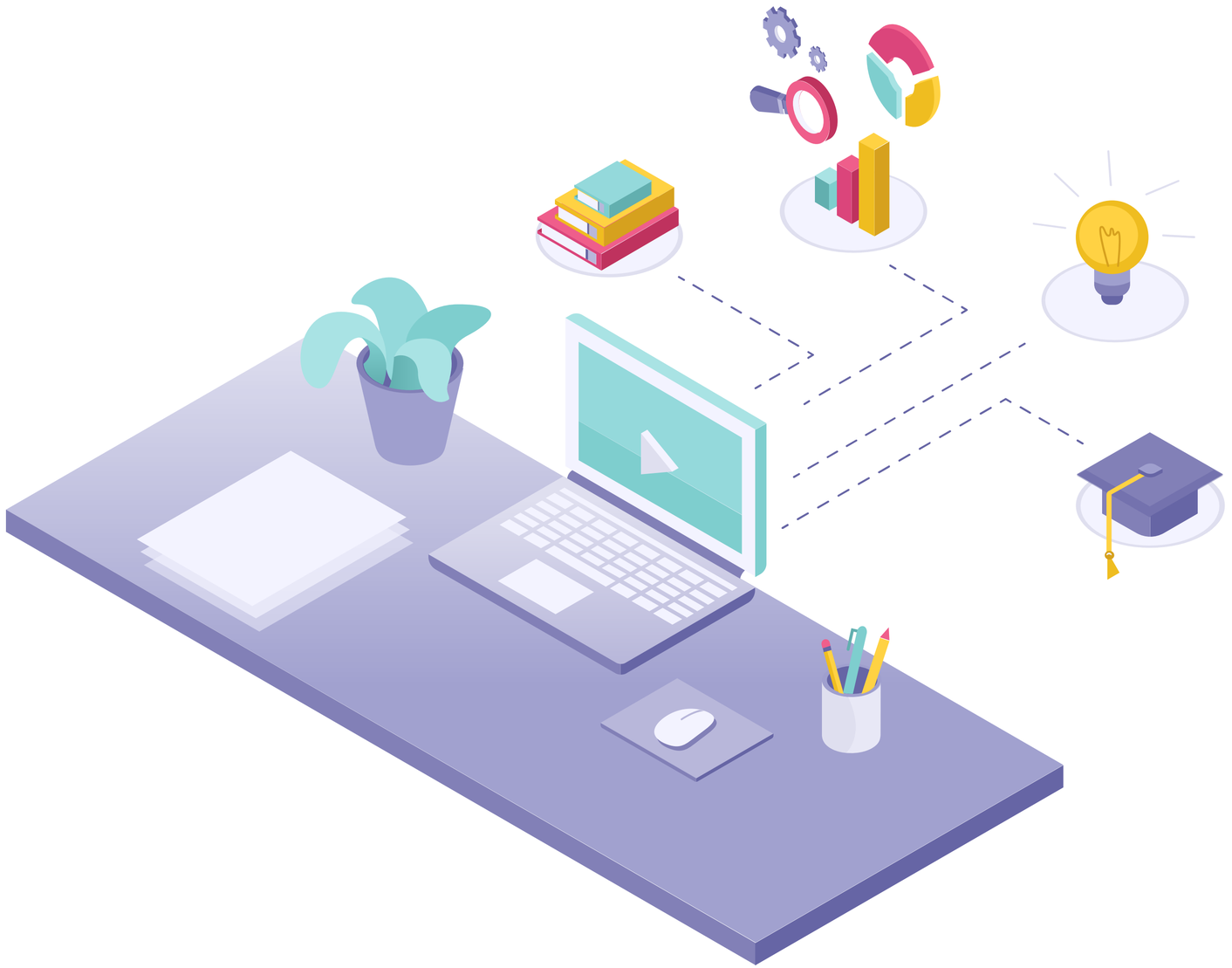
Cas d'usage : Haute performance, faible latence, applications mobiles, IOT, paniers d'achat E-commerce, architectures Serverless,..

Amazon DAX -> Cache mémoire pour encore plus de performance

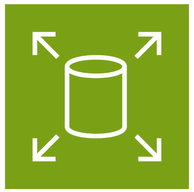
Amazon DynamoDB



Amazon DocumentDB



Amazon DocumentDB



Base de données NoSQL orientée Document (JSON)

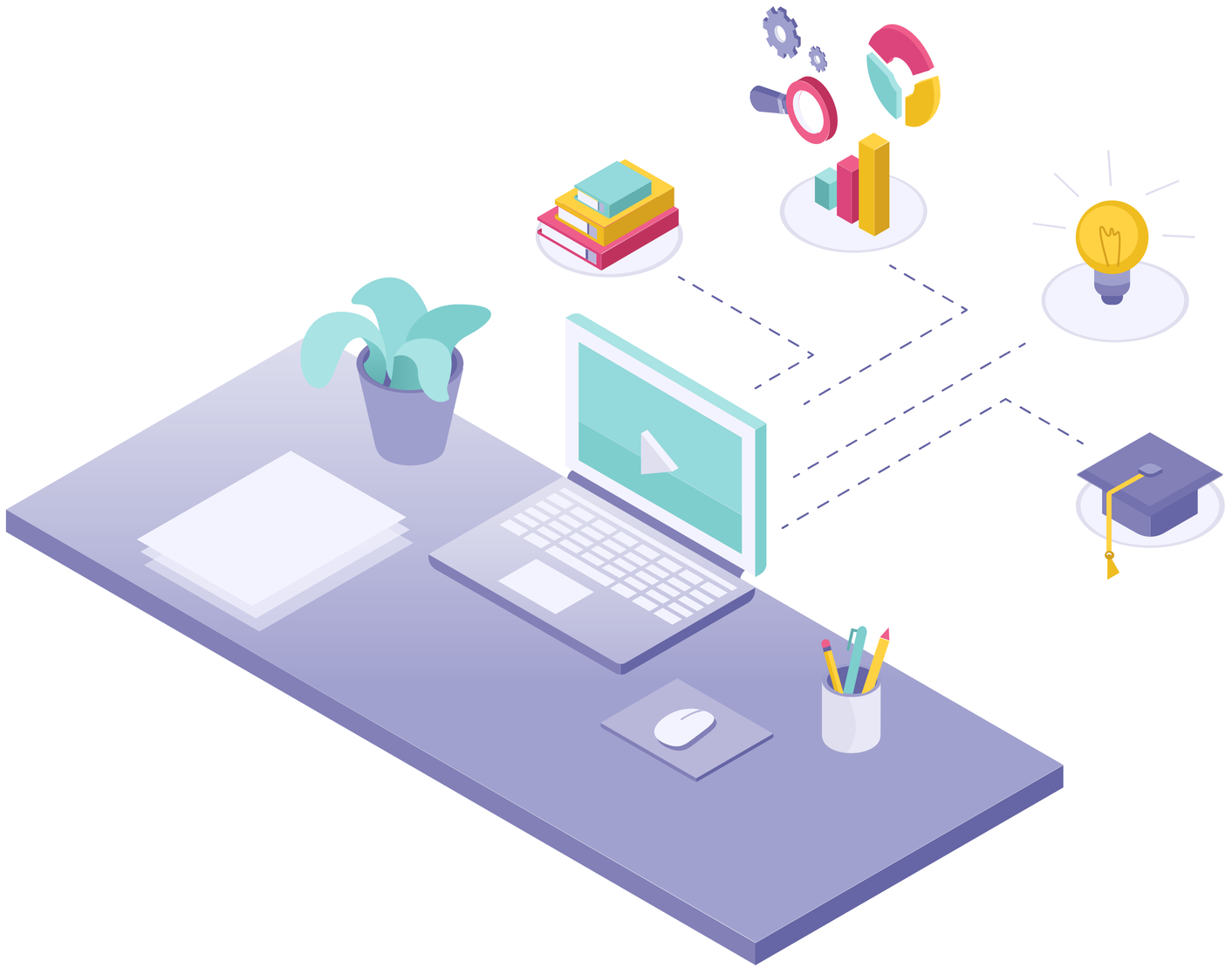
Compatible avec **MongoDB**

Entièrement **gérée** par AWS

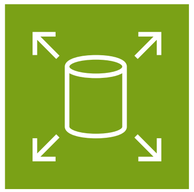
Quelques cas d'usage

- Migration d'une application existante (MongoDB)
- Données de gestion de contenu (CMS)
- Données de profils ou préférences utilisateurs
- Applications mobiles et web

Amazon Neptune



Amazon Neptune



Base de données NoSQL orientée **graphe**

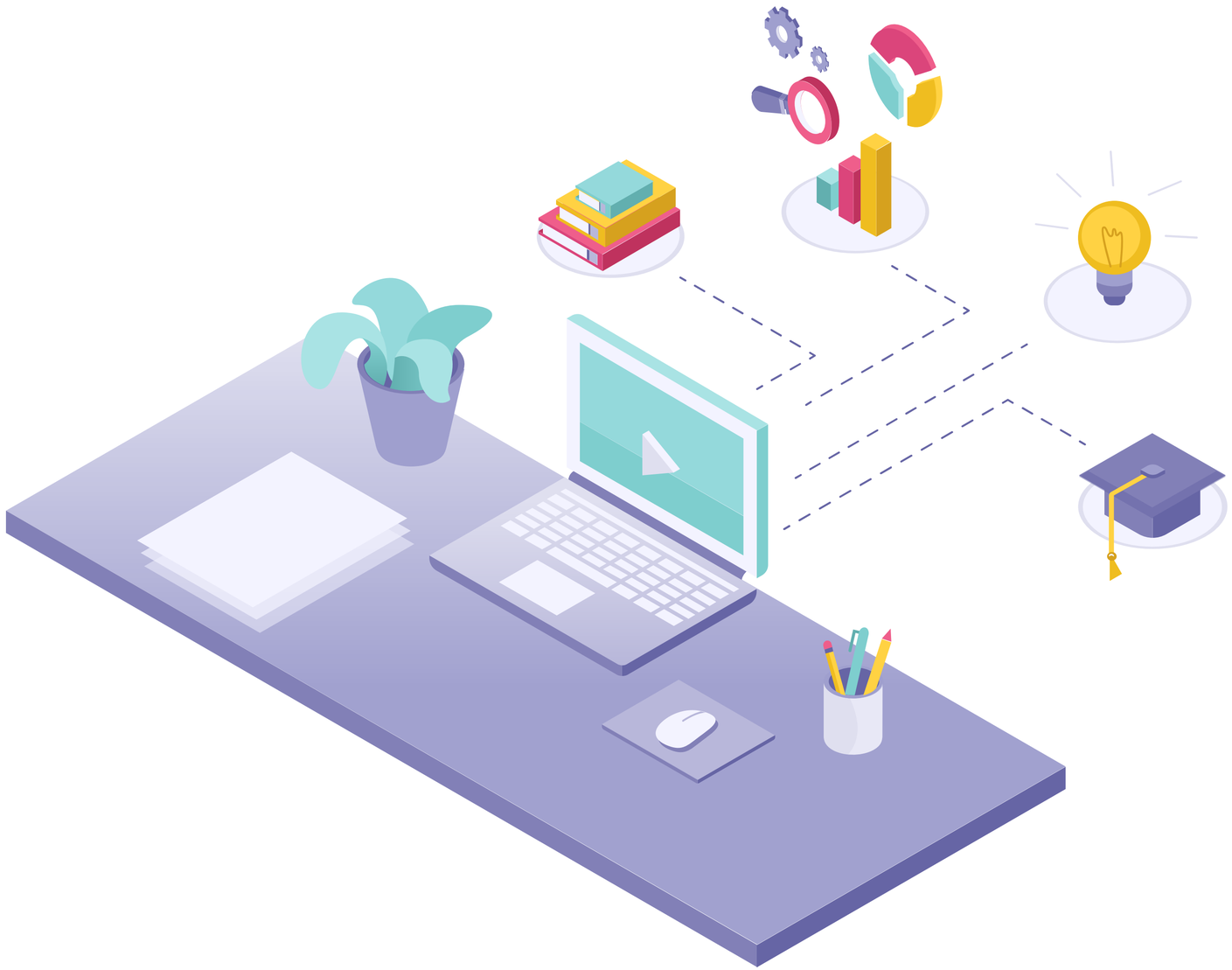
Entièrement **géré par AWS** ou **Serverless**

Supporte les **langages de requête de graphe populaires** Apache TinkerPop Gremlin, W3C SPARQL et openCypher

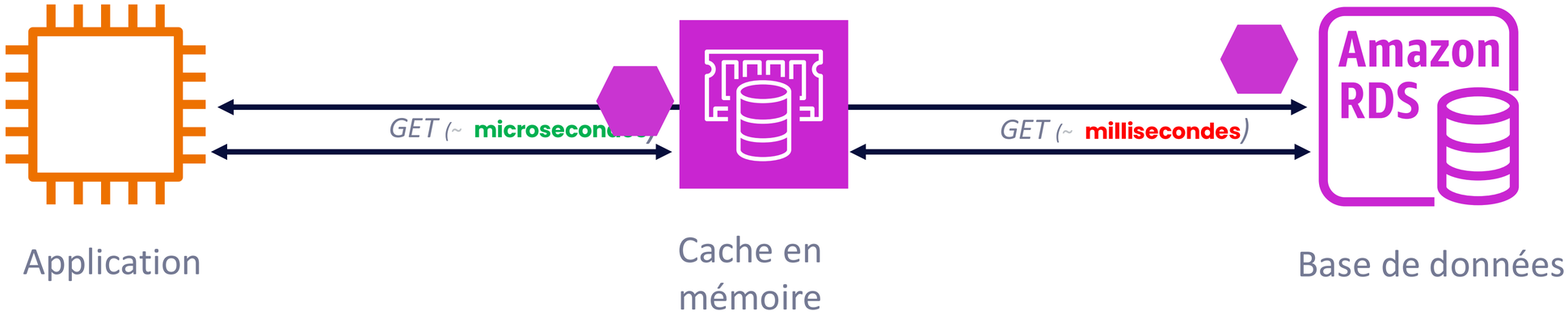
Cas d'usage

- Modéliser les liens entre données
- Détection des schémas de fraudes
- Données de réseaux sociaux

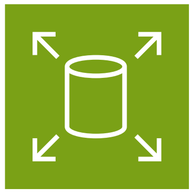
Amazon ElastiCache



Le cache, à quoi ça sert ?



Amazon ElastiCache

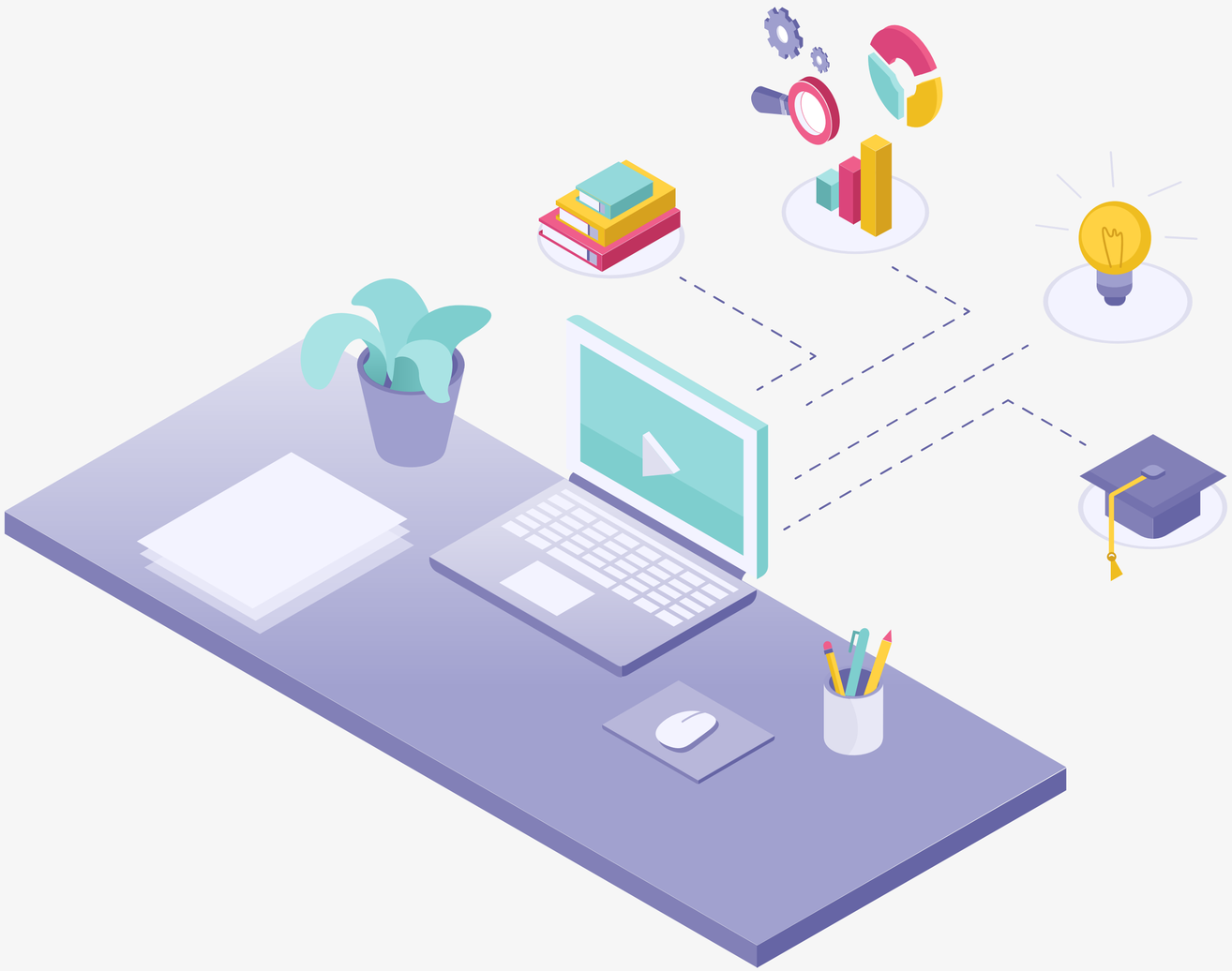


Permet de la **mise en cache** de vos données

Stocke en mémoire les données fréquemment utilisées pour améliorer les performances

Compatible Redis ou MemCached

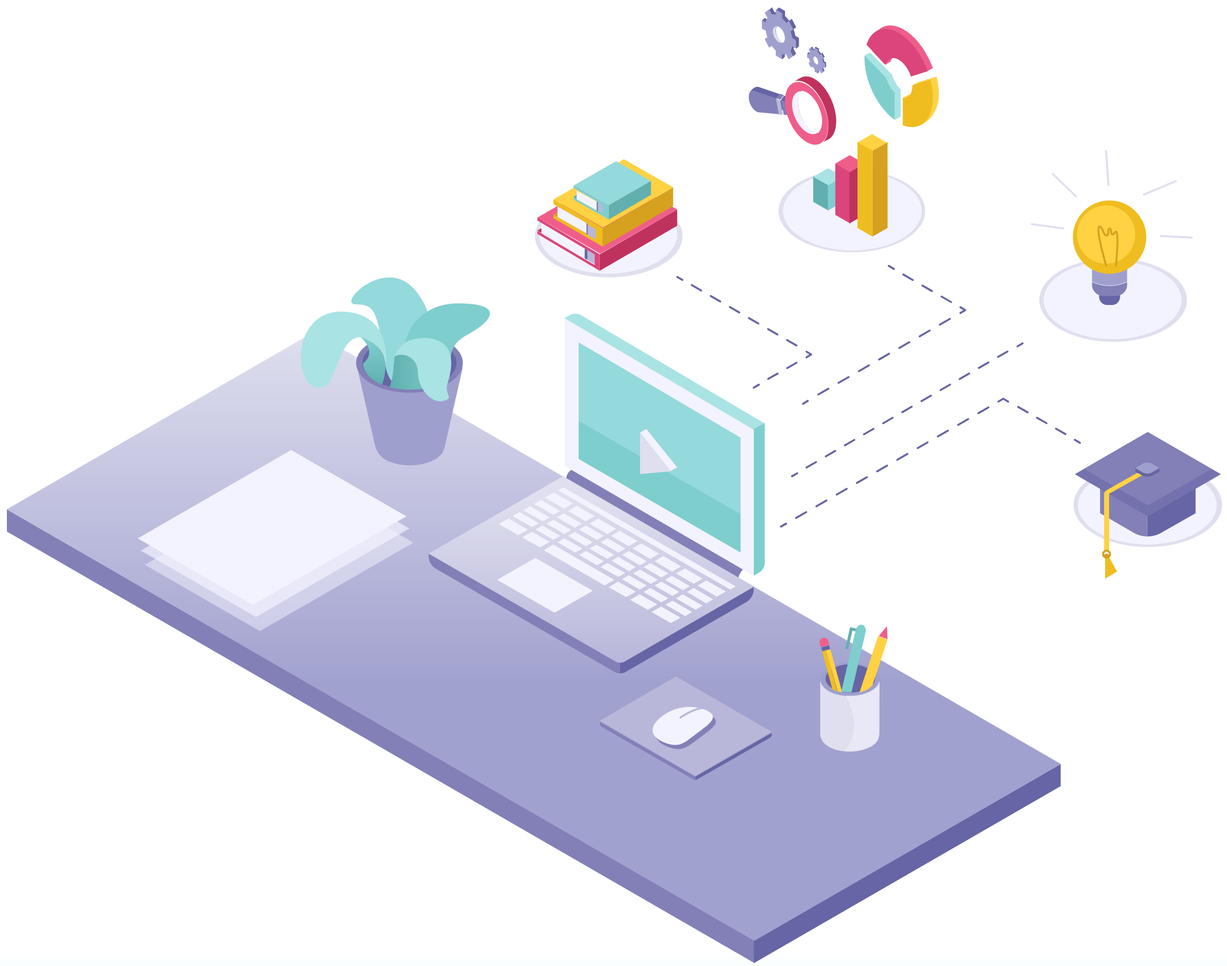
Cas d'usage : Améliorer la performance en lecture, Soulager la base de données, *Leaderboard* de jeux (avec Redis)…



FIN DU MODULE

Module 9 : Analytique & AI/ML

Le moyen le plus rapide d'obtenir des réponses à partir de toutes vos données et de les transmettre à tous vos utilisateurs



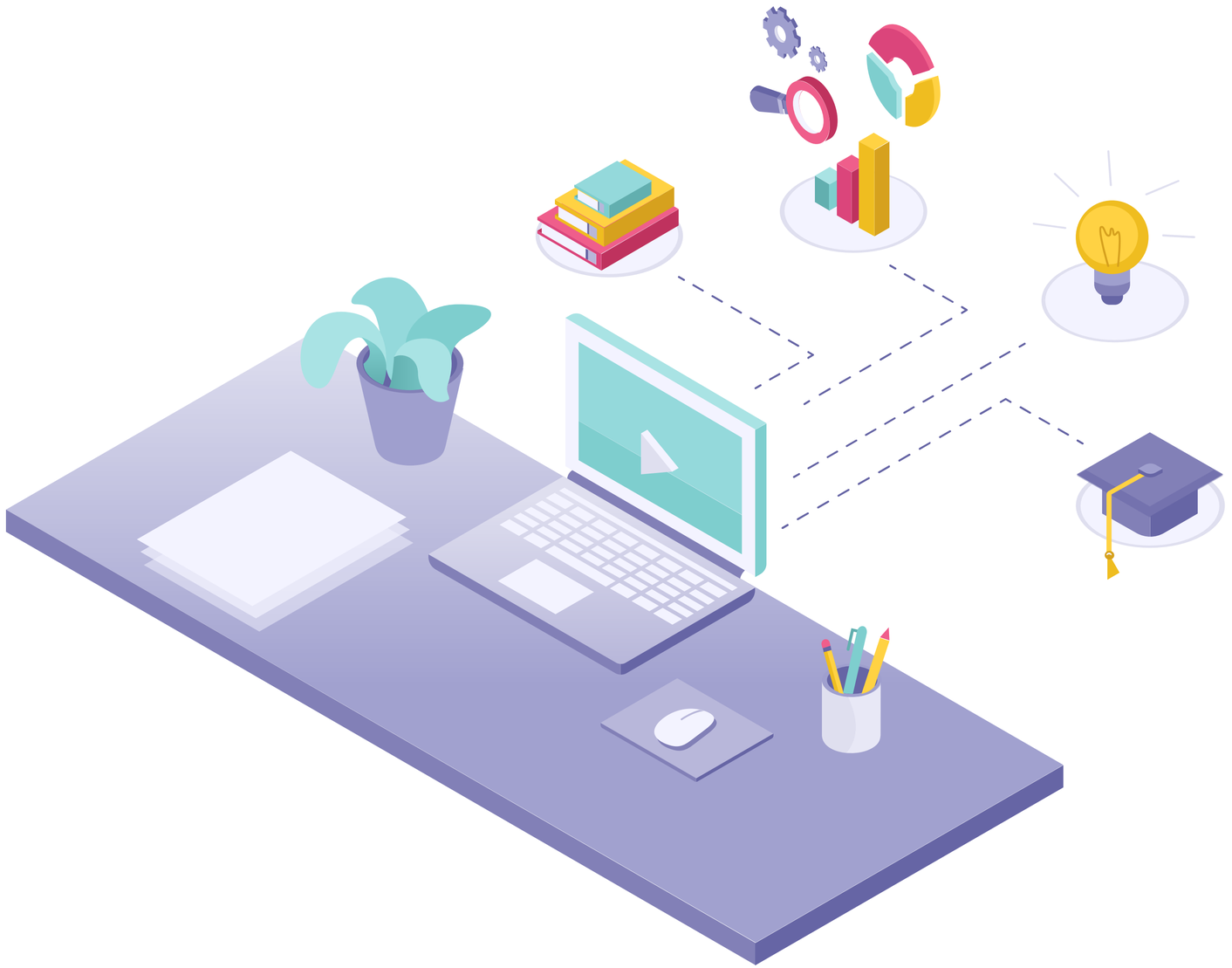
Quels sont les services Big Data et BI ?

Quels sont les services d'AI/ML ?

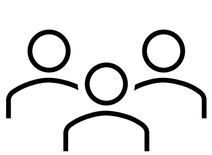
Quels sont les cas d'usage et patterns d'architecture ?



Concepts IT



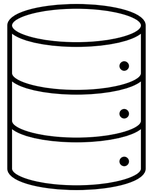
Exemple de reporting



Utilisateurs

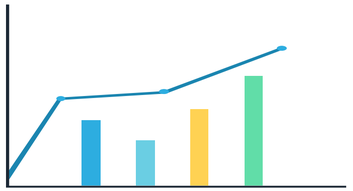


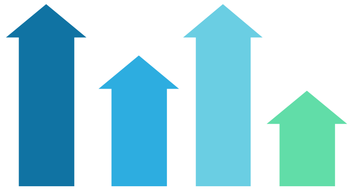
Site
e-commerce



Base de
données

Reporting





Evolution des ventes ?

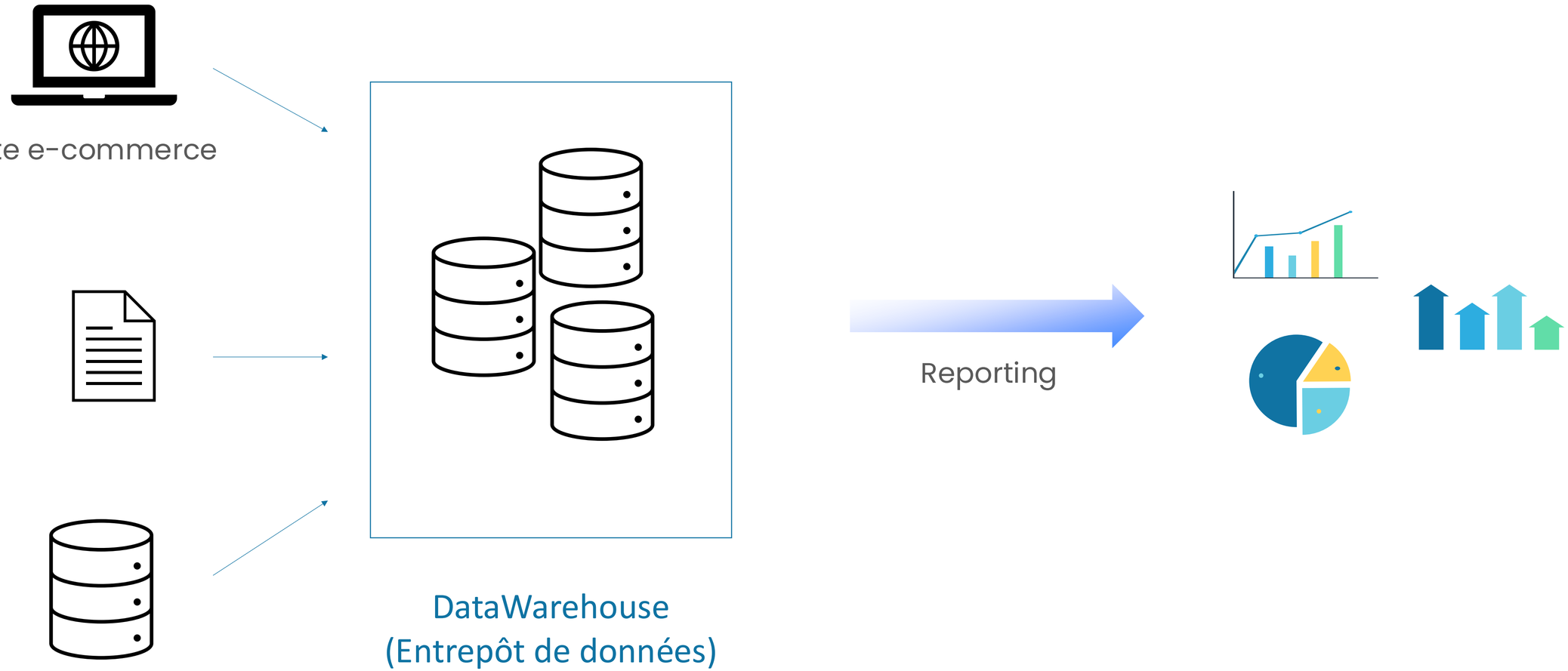
Evolution du stock ?

Evolution du trafic sur le site ?

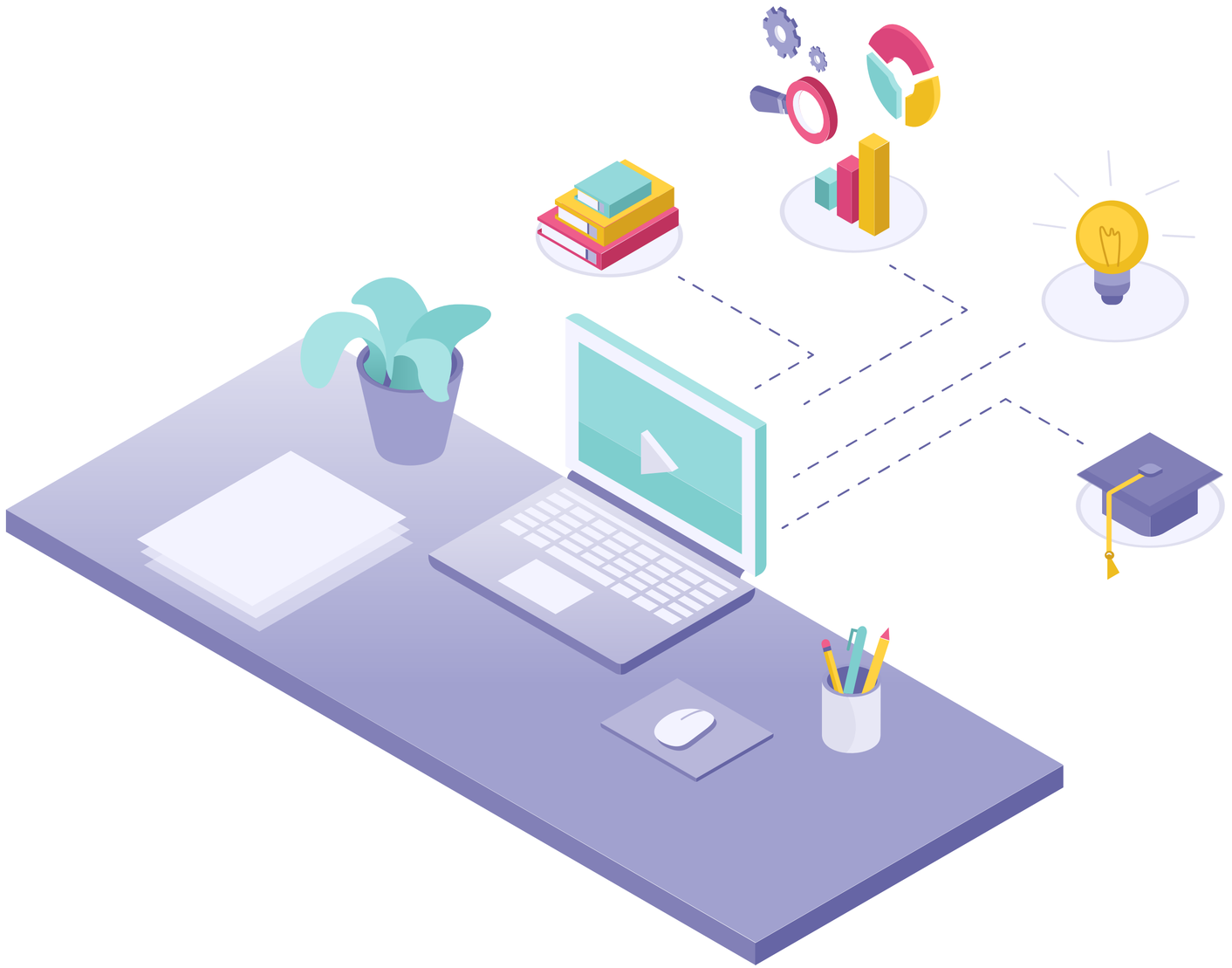
....

LeCloudFacile.com

Reporting : Architecture simplifiée



Amazon Athena



Amazon Athena



Permet d’analyser des données stockées dans **Amazon S3***

Langages supportés : **SQL** (Presto et Trino) ou **Python** (Apache Spark)

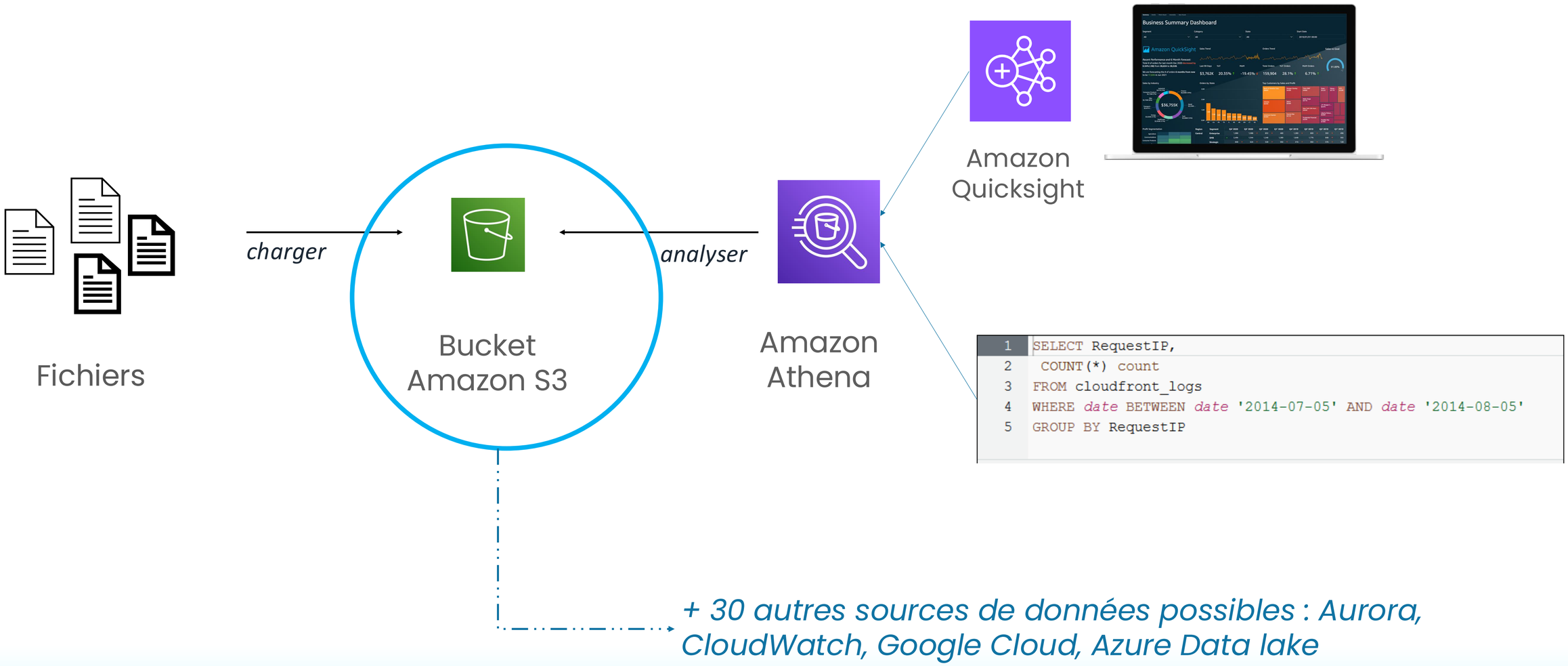
Formats de fichiers : texte, CSV, XML, Json, Parquet, Avro,...

Supporte les fichiers **compressés** (GZIP, ZLIB, Snappy,...)

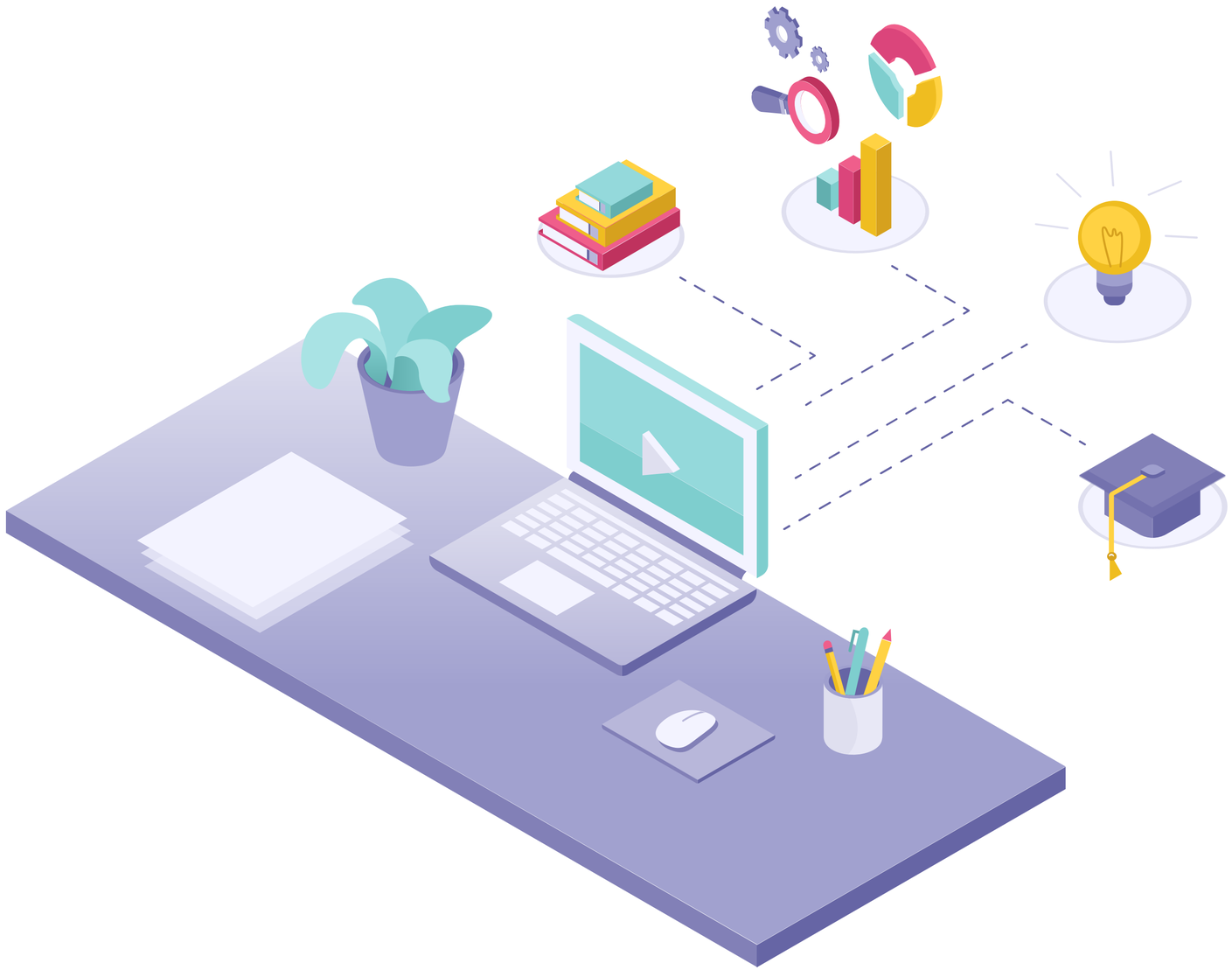
Entièrement **Serverless** et facturation au **volume de données analysées**

Cas d’utilisation : Business Intelligence (BI), Big Data, Analyse de logs,..

Démarrer avec Amazon Athena



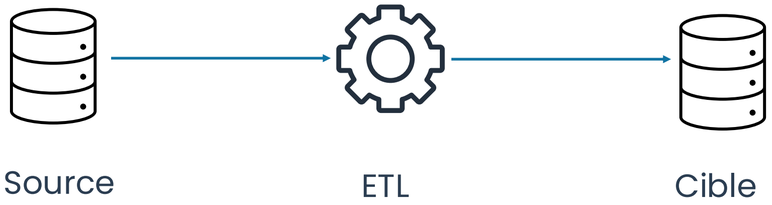
AWS Glue



AWS Glue

Permet de créer des *jobs* **ETL** de traitement de données (batchs)

ETL = *Extract, Transform, Load*

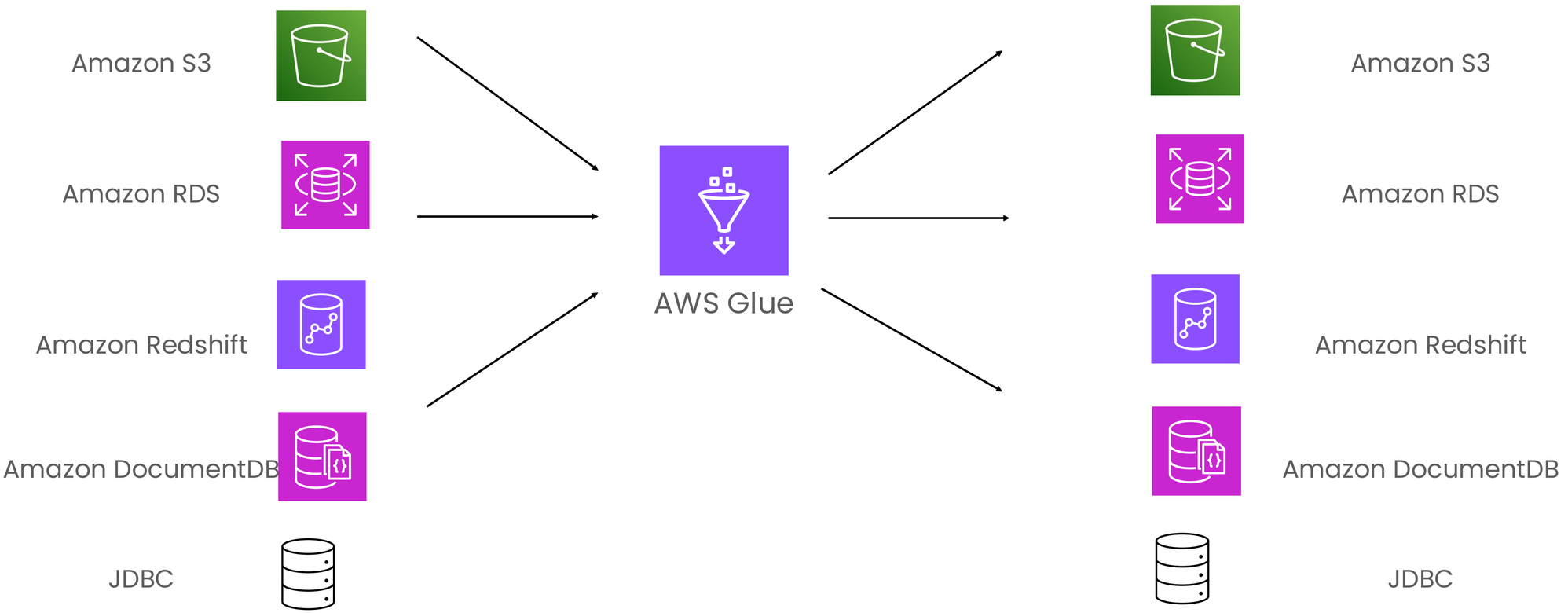


Basé sur le framework **Apache park**

Jobs = Batch ou *Streaming*. ***Langages*** = *Python ou Scala*

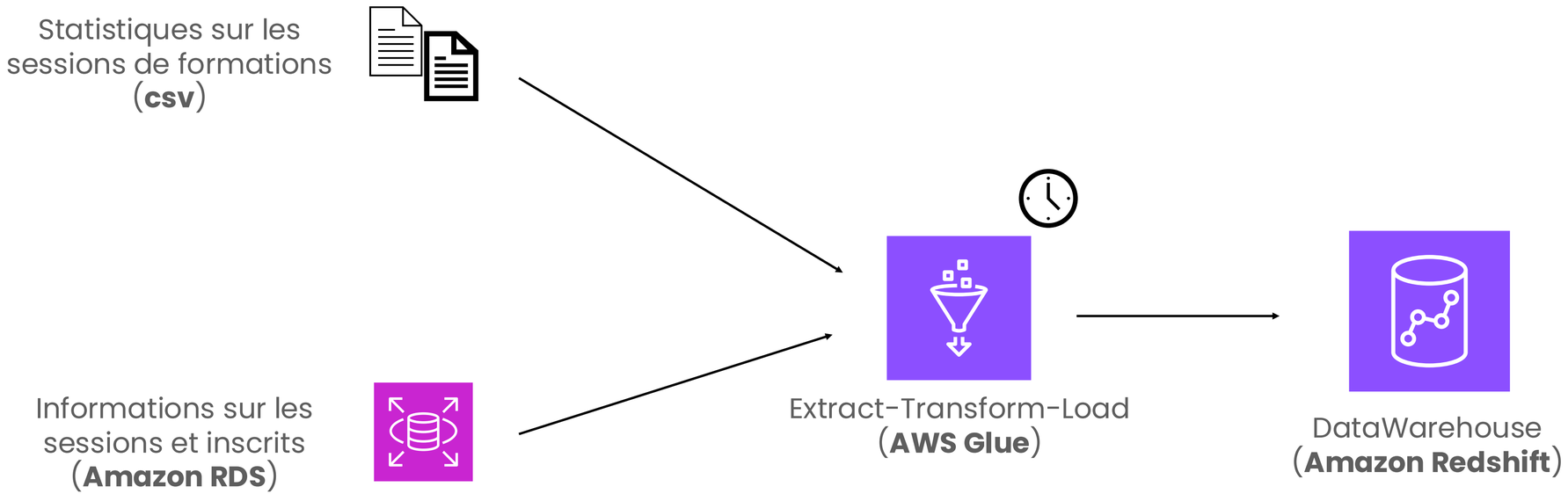
Cas d'utilisation : traitements batchs, projets BI / Big Data, …

AWS Glue

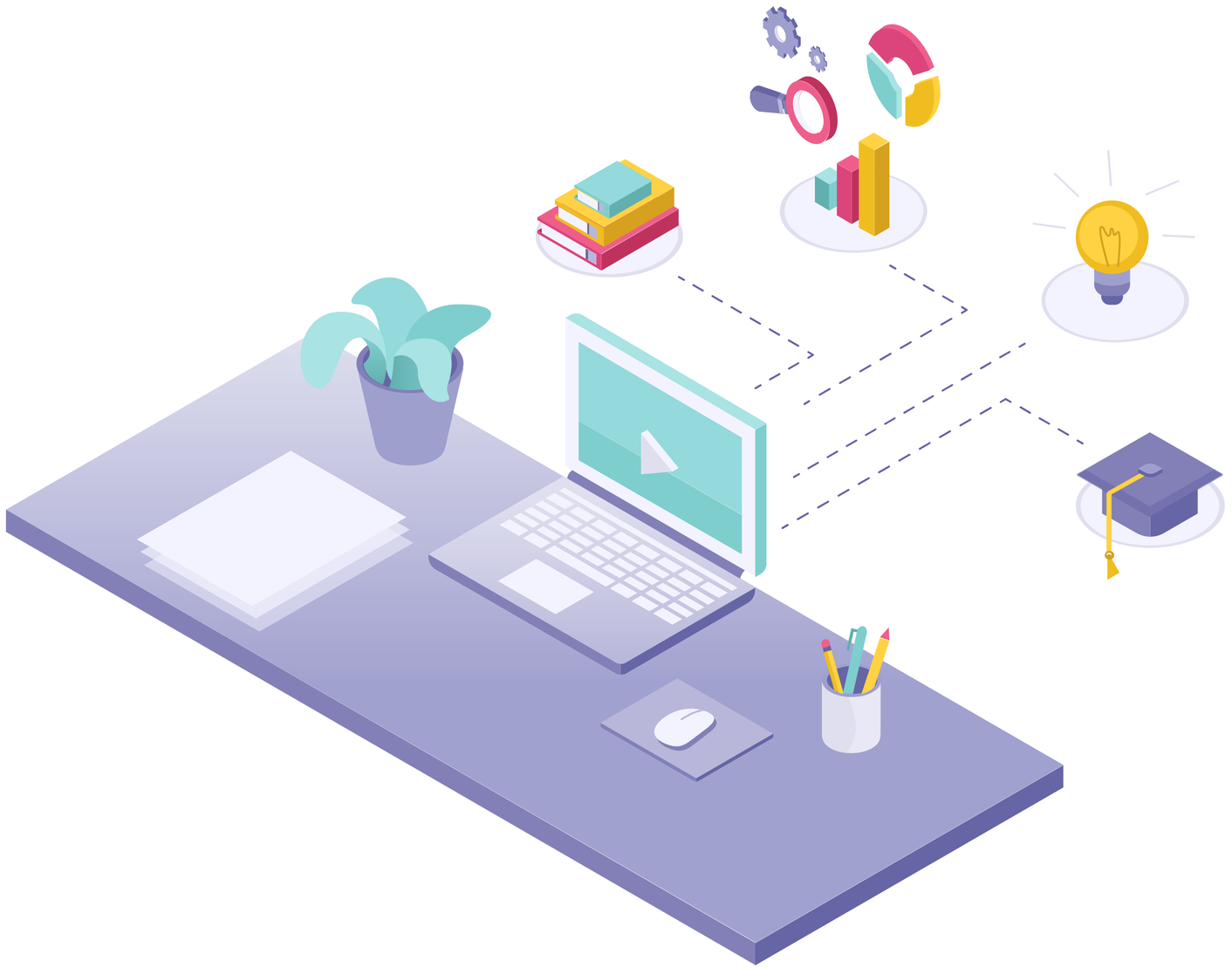


Extract | Transform | Load

Exemple


Statistiques sur les sessions de formations (**csv**)
Informations sur les sessions et inscrits (**Amazon RDS**)
Extract-Transform-Load (**AWS Glue**)
DataWarehouse (**Amazon Redshift**)

Amazon Elastic Map Reduce (EMR)



Amazon EMR



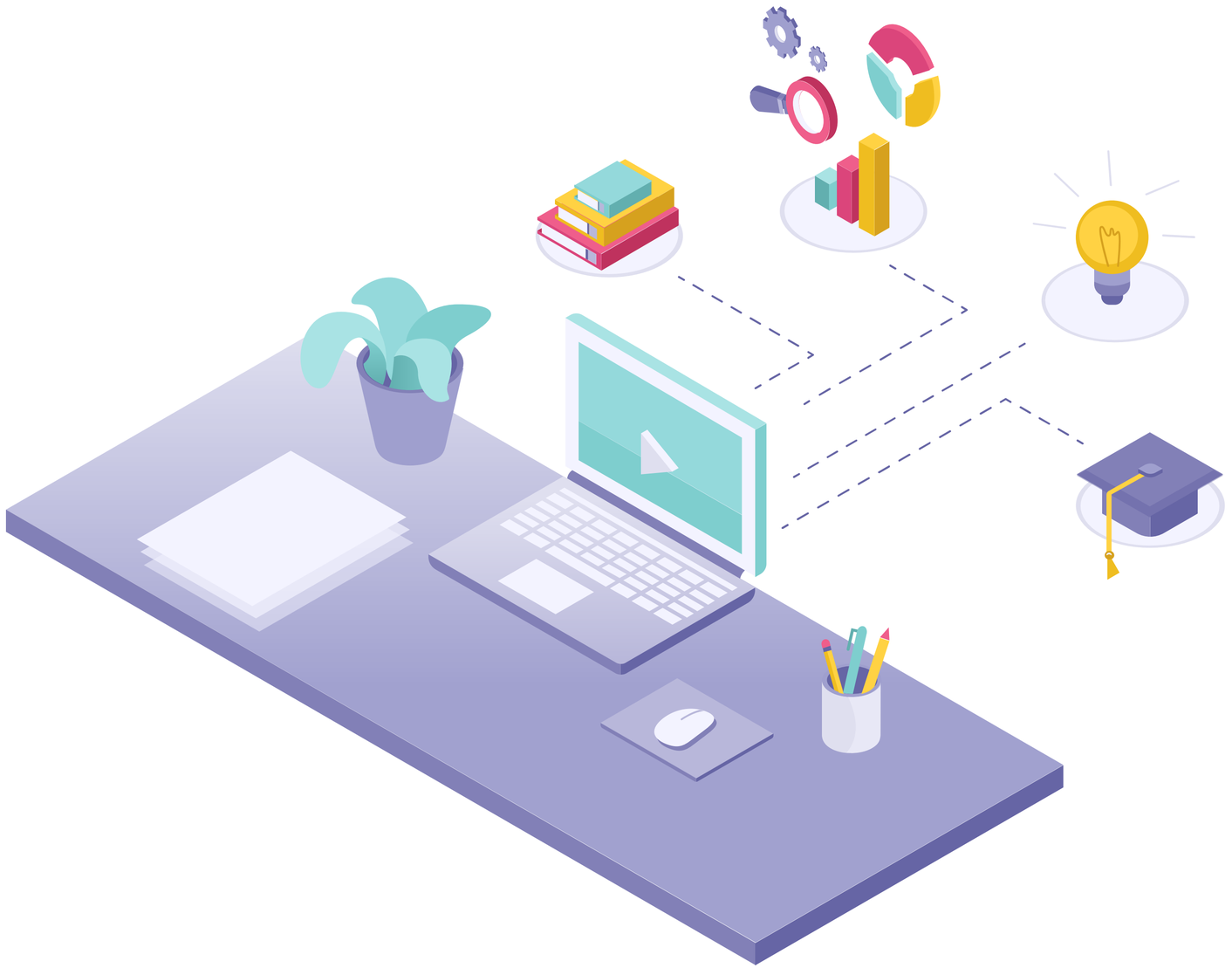
Permet de créer des **clusters Hadoop** gérés par AWS

Hadoop = framework open source pour le traitement Big Data

EMR = *Elastic Map Reduce (mais supporte les autres frameworks)*

Supporte les frameworks : Hadoop, Apache Spark, Hive, Pig, Presto ...

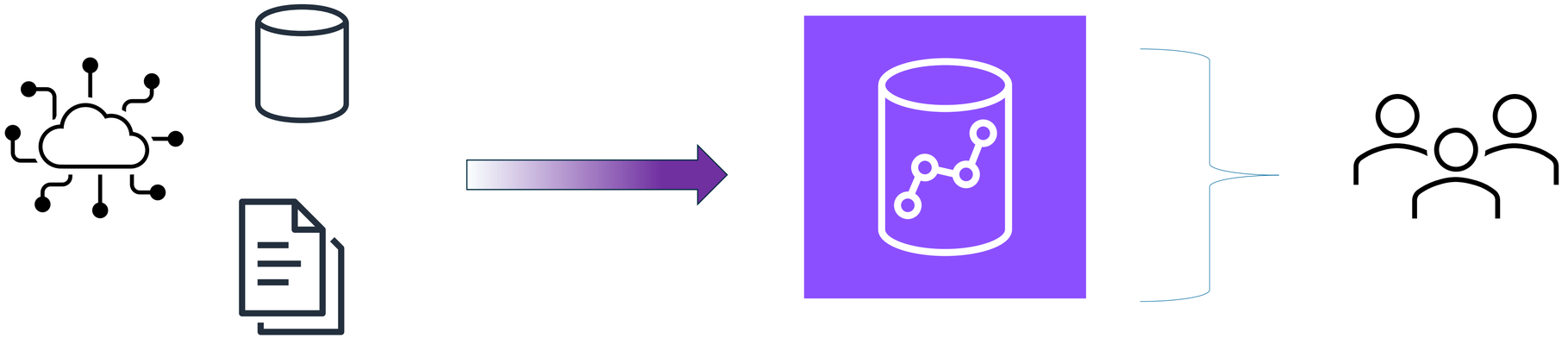
Amazon Redshift



Amazon Redshift

Permet de créer des **entrepôts de données** (Data Warehouse) gérés par AWS

Conçu pour le **stockage et l'analyse** de pétaoctets d'historique de données



Données d'entreprise

Amazon Redshift

Equipe
Business Intelligence

Amazon Redshift

Cas d'usage : principalement pour la Business Intelligence



OLAP = Online Analytical Processing

S'intègre avec les outils **Business Intelligence** tels que Amazon Quicksight, Tableau, PowerBI ...

Amazon Redshift : un peu de details techniques

Basé sur PostgreSQL, stockage orienté **colonne**



Cluster de serveurs appelés « nœuds » -> stockage des données et exécutent les requêtes SQL

Redshift **Serverless ->** version Serverless de Redshift

Redshift **Spectrum** -> pour requêter les données dans Amazon S3

LeCloudFacile.com

Exemple

Amazon RDS



Fichiers



Amazon S3

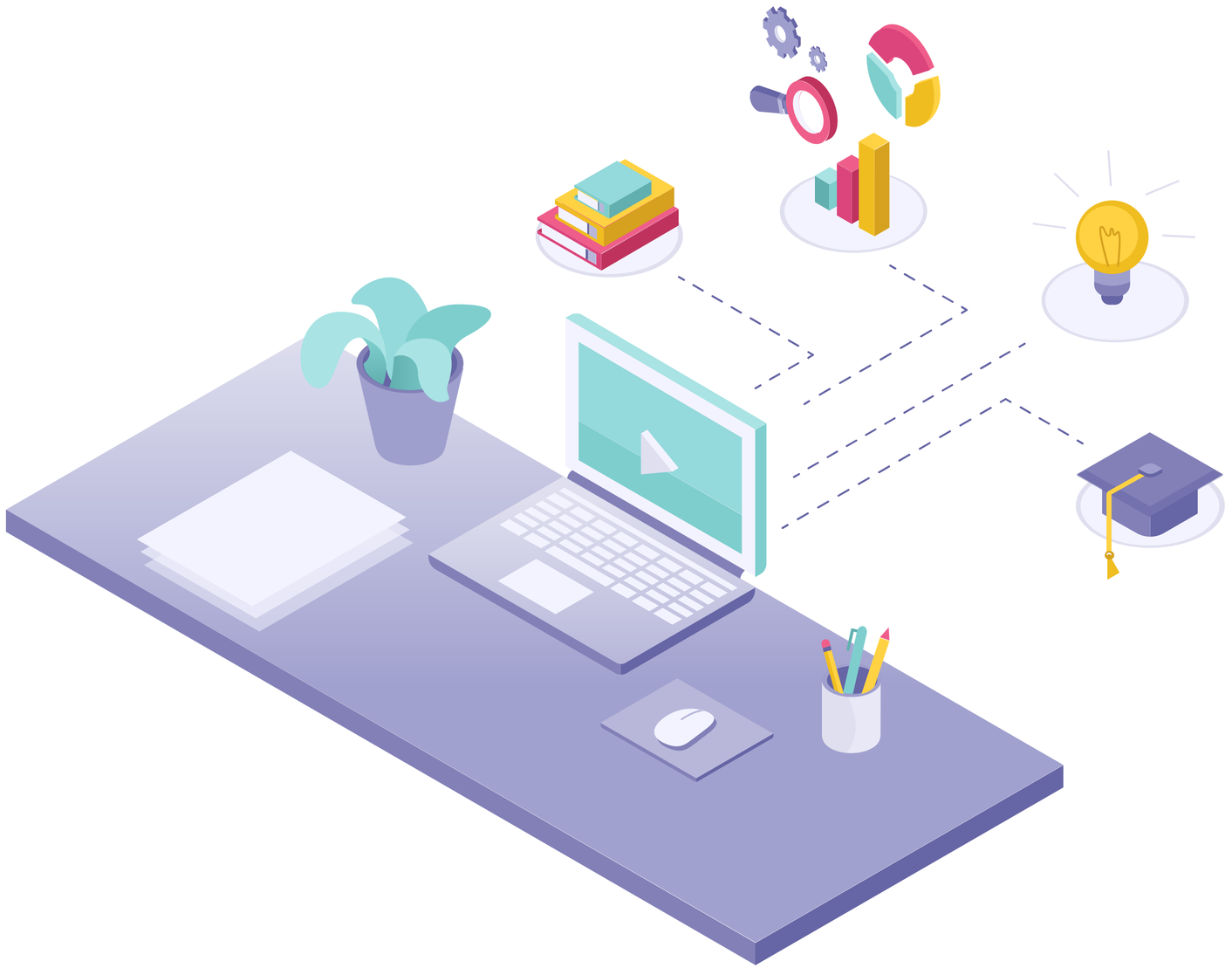


Chargement ETL

Amazon Redshift



Amazon QuickSight



Amazon QuickSight



Data Warehouse
(Amazon Redshift)





Amazon QuickSight



Service de **visualisation** et reporting de vos données

Fournit des **tableaux de bord et visualisations interactives**

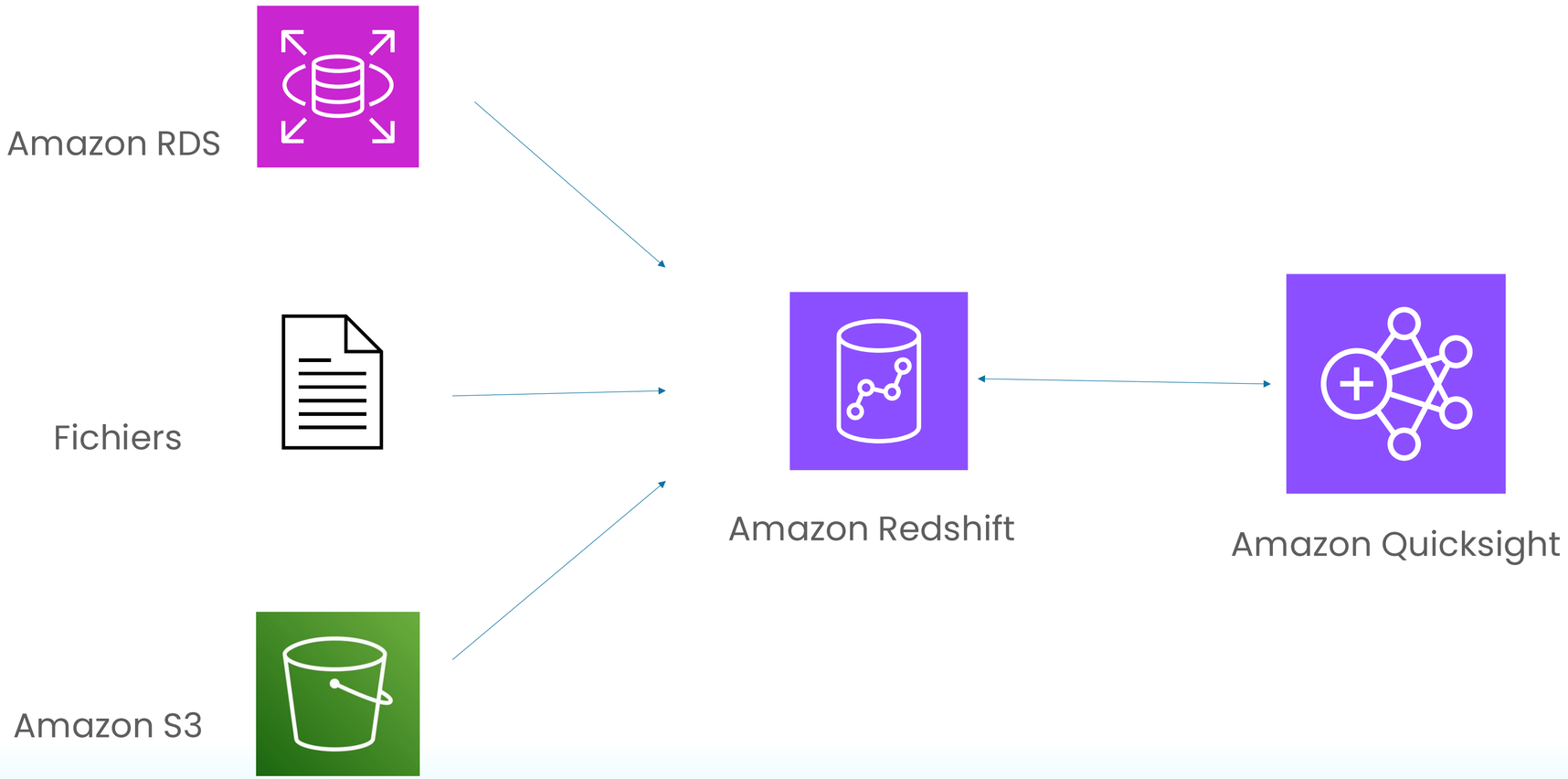
Principalement destinée aux équipes **Business Intelligence**

Sources de données : Amazon Redshift, fichiers, Bases de données, Services AWS (Athena, S3, RDS, Aurora,...), Logiciels SaaS,...

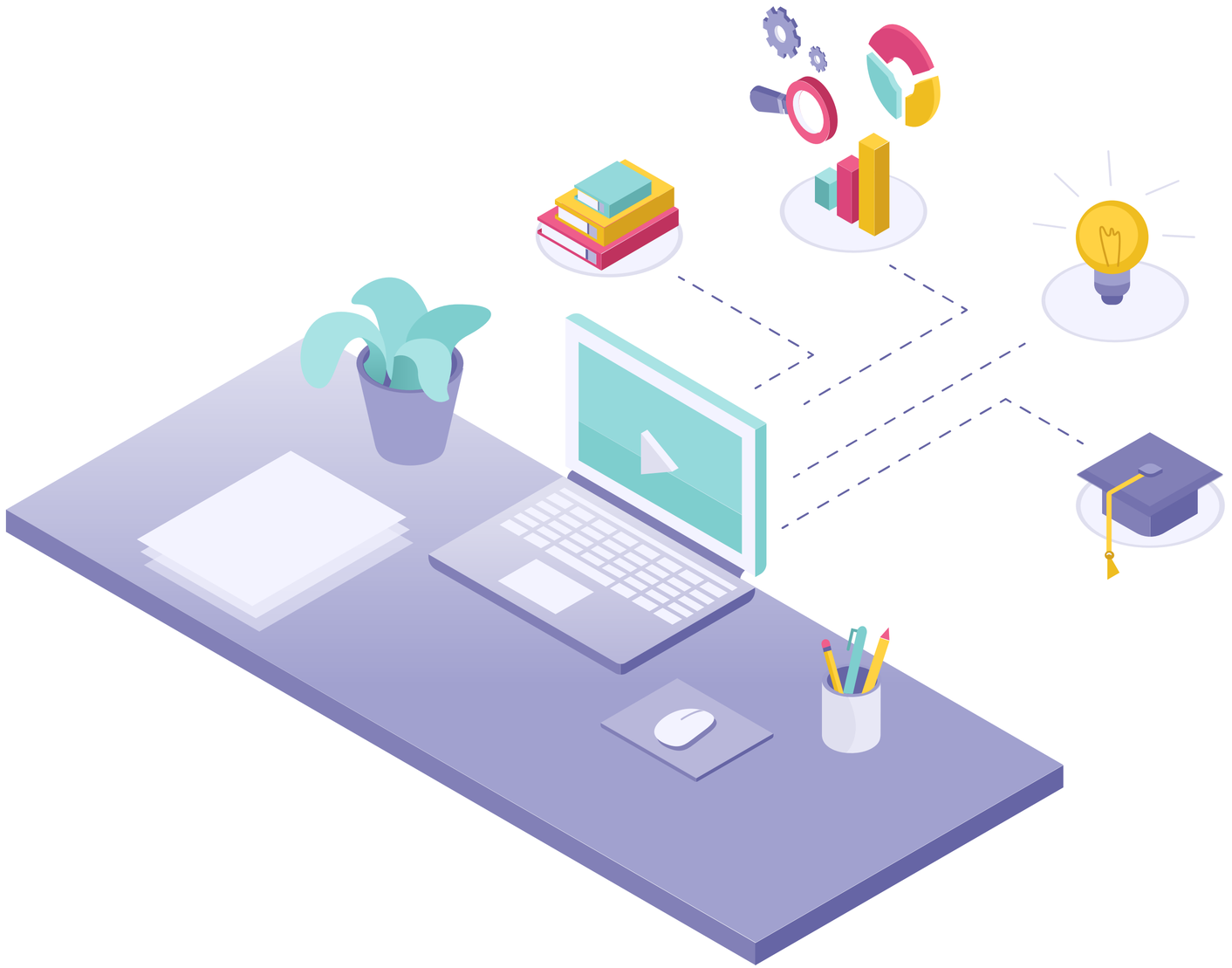
Outils similaires : *Tableau, PowerBI, Looker...*

LeCloudFacile.com

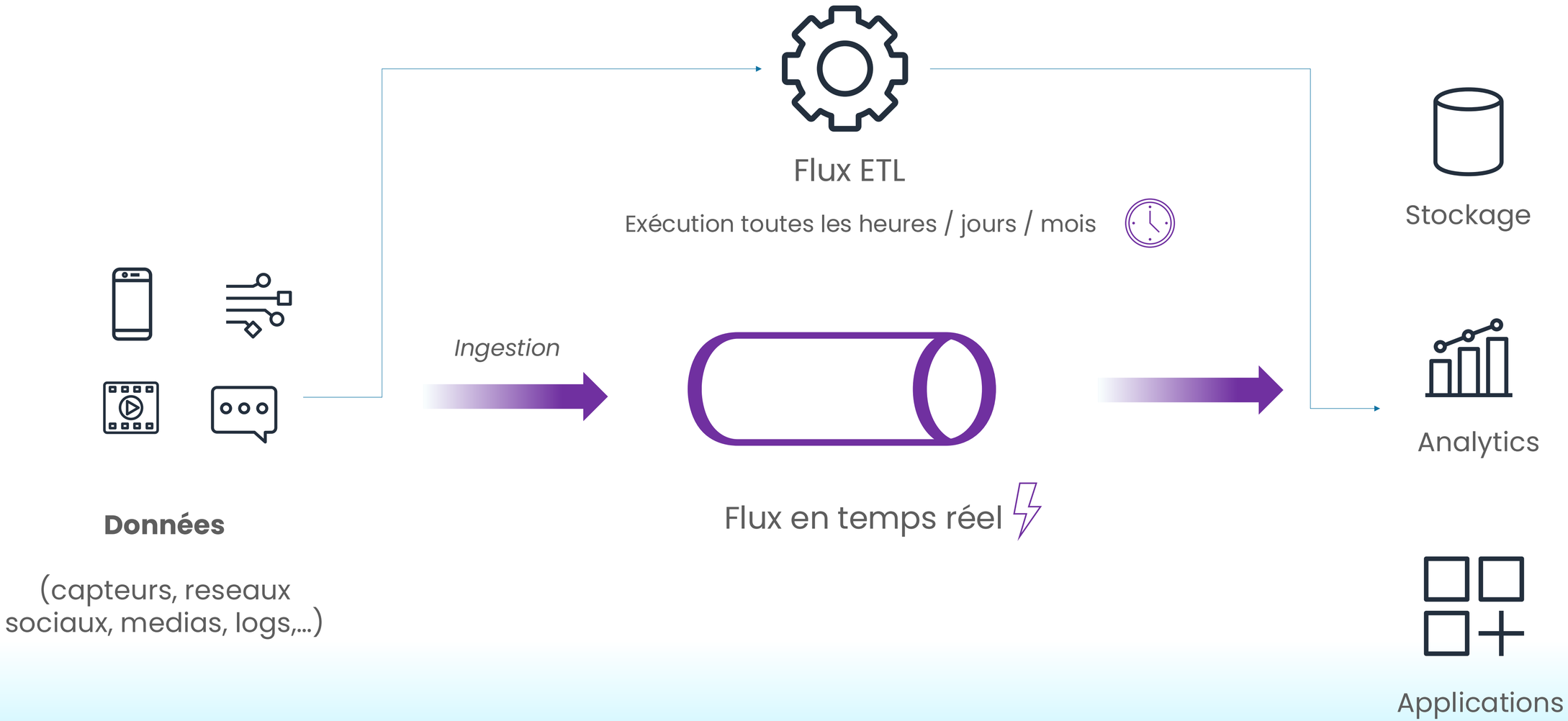
Exemple d'utilisation d'Amazon QuickSight



Amazon Kinesis



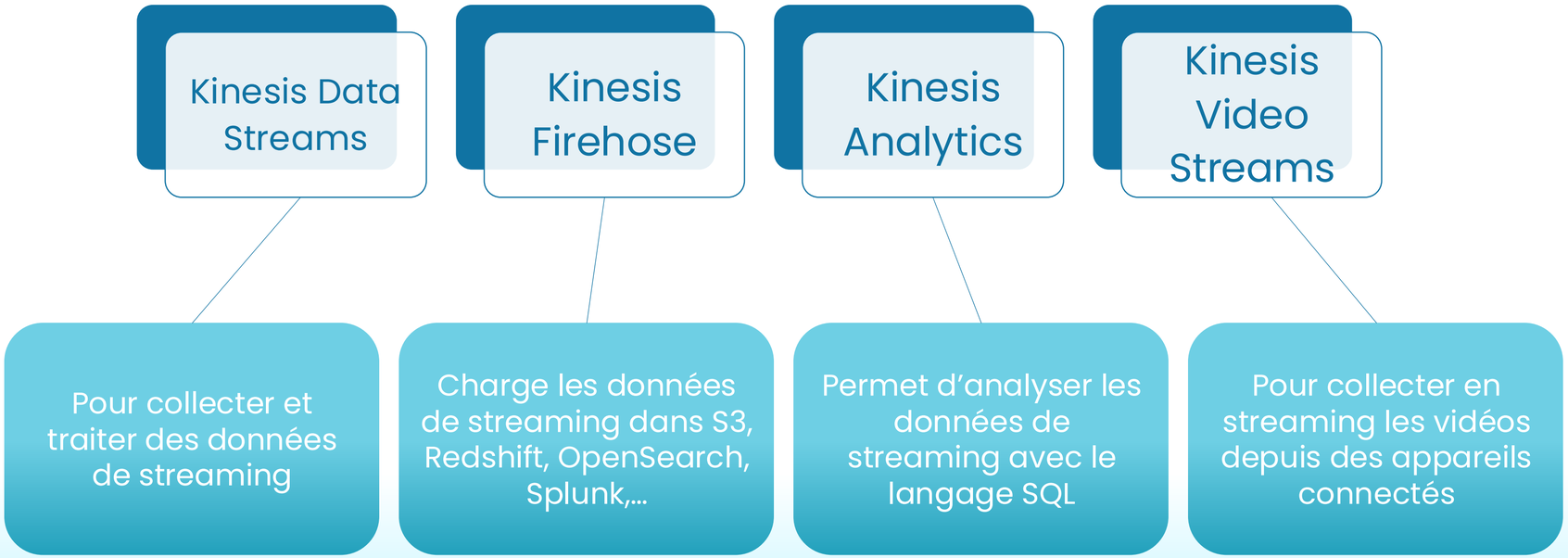
Traitement des données de Streaming



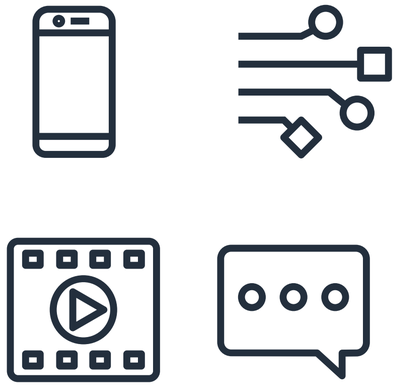
Amazon Kinesis

Famille de services permettant de collecter et traiter en temps réel **les données de streaming**

Exemples de ***données de streaming*** : logs d'applications, données de capteurs, IOT, Clickstream, évènements systèmes/applicatifs...



Exemple



Données

(capteurs, reseaux sociaux, medias, logs,...)

streaming

Amazon Kinesis

chargement

Amazon Rekognition Video

Amazon DynamoDB

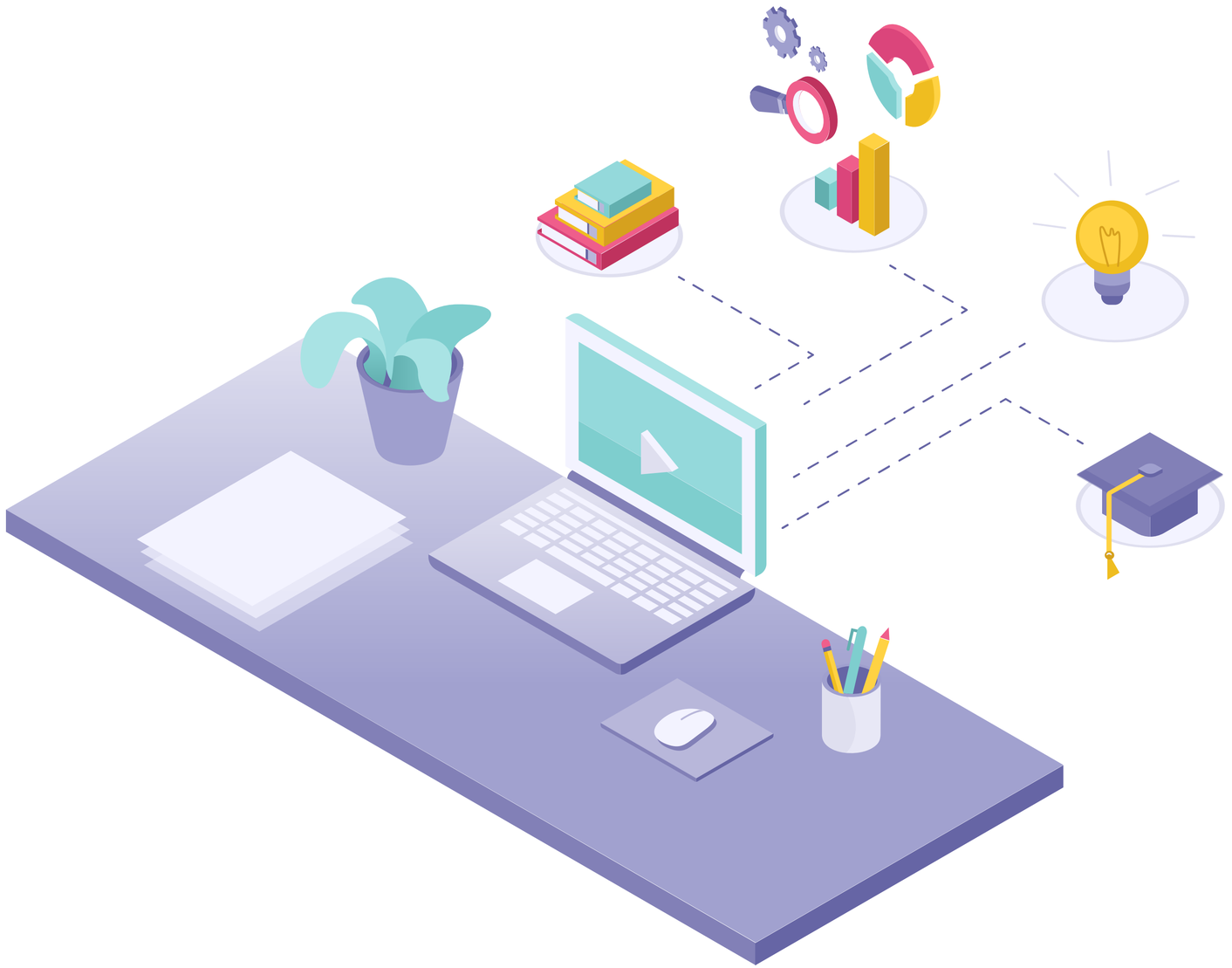
Amazon EC2

AWS Lambda

Amazon S3

Amazon Redshift

Amazon MSK



Amazon Managed Streaming for Kafka (MSK)



Permet de créer des clusters **Kafka** gérés par AWS

Apache Kafka est une plateforme open-source de streaming de données

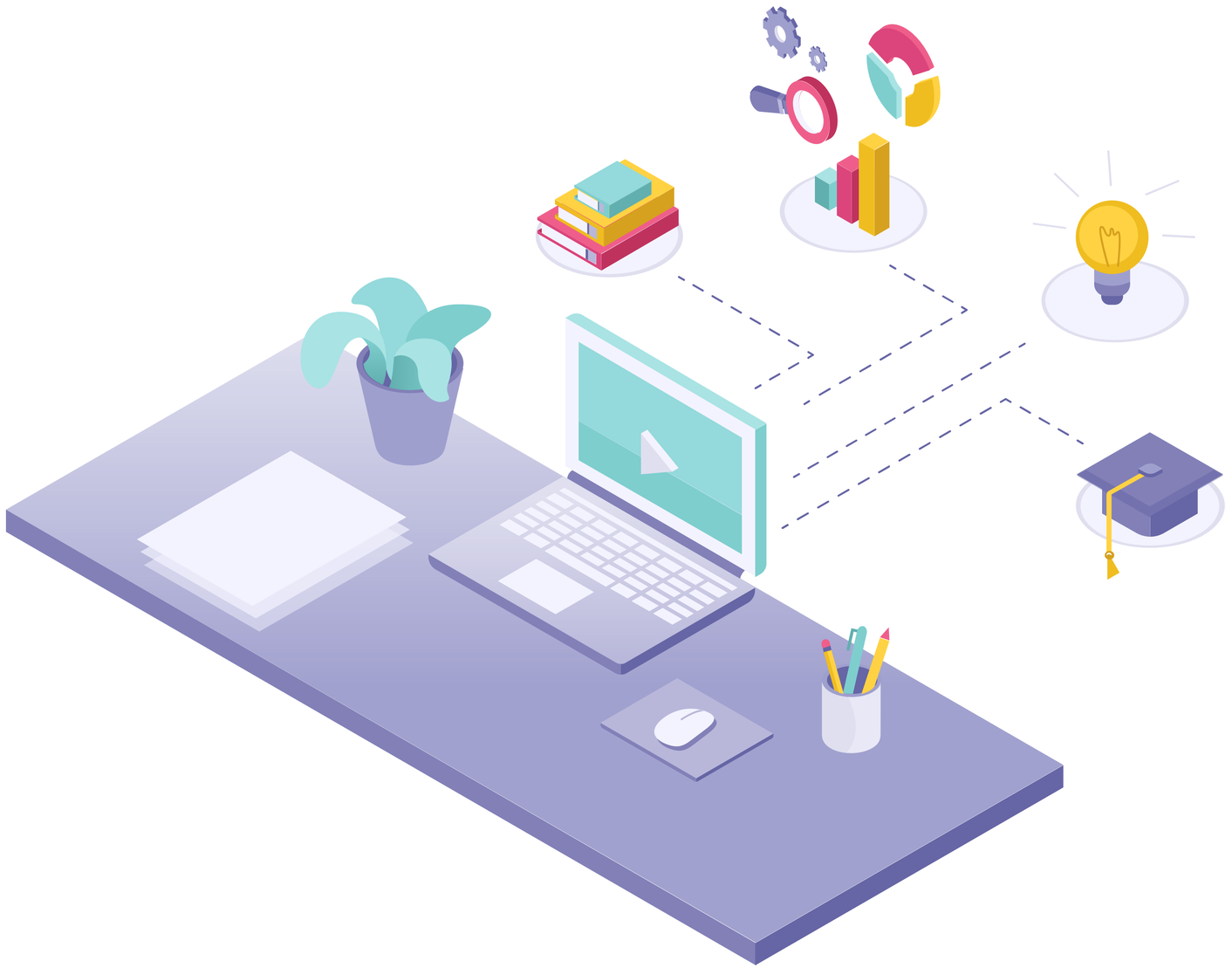
Permet de collecter et traiter en temps réel **les données de streaming**

-> Similaire à Amazon Kinesis Streams

Choix entre *Managed* ou *Serverless*



En résumé



Analytique sur AWS : Exemples d'Architecture

Site e-commerce

Bases de données de production

Option 1

Read replica

Option 2

Amazon Redshift

export

Fichiers plats (CSV, Json, XML,..)

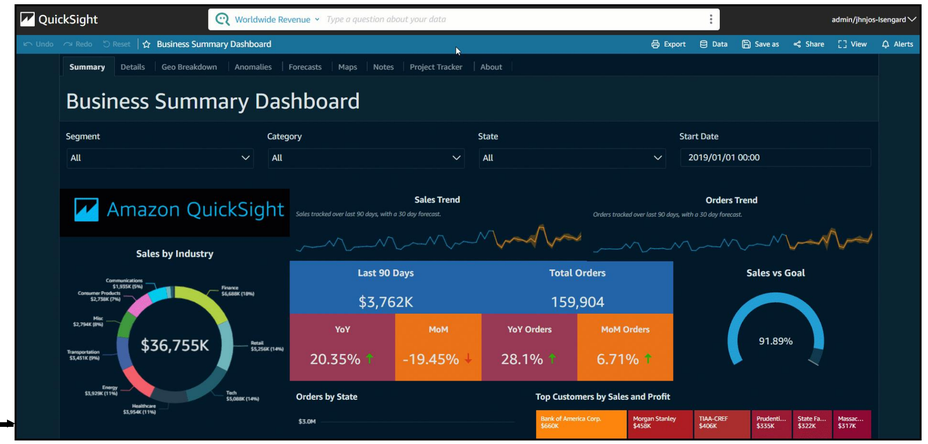
Option 3

Amazon Simple Storage Service (Amazon S3)

Amazon Athena

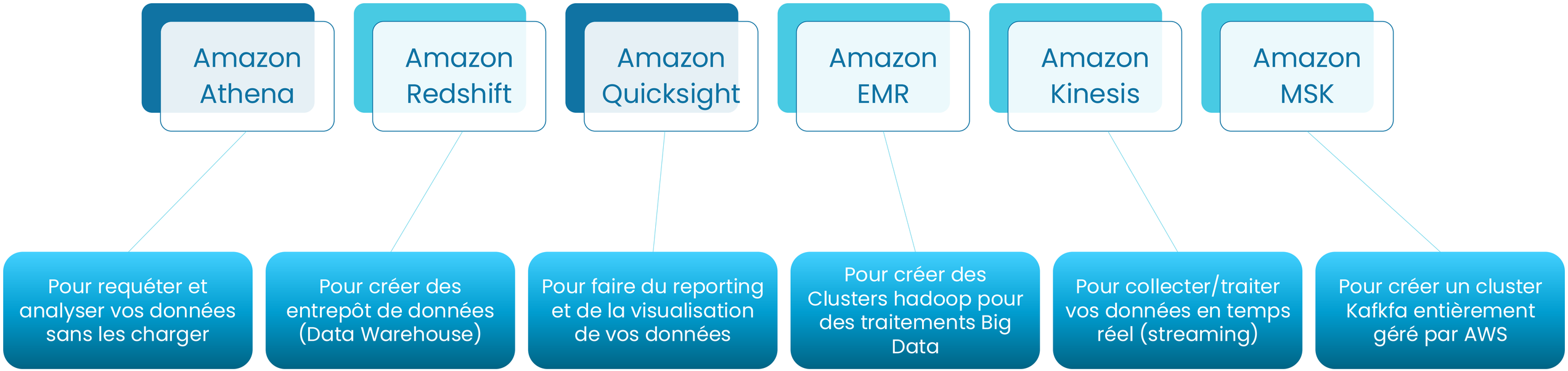
Equipe Business Intelligence (BI)

reporting

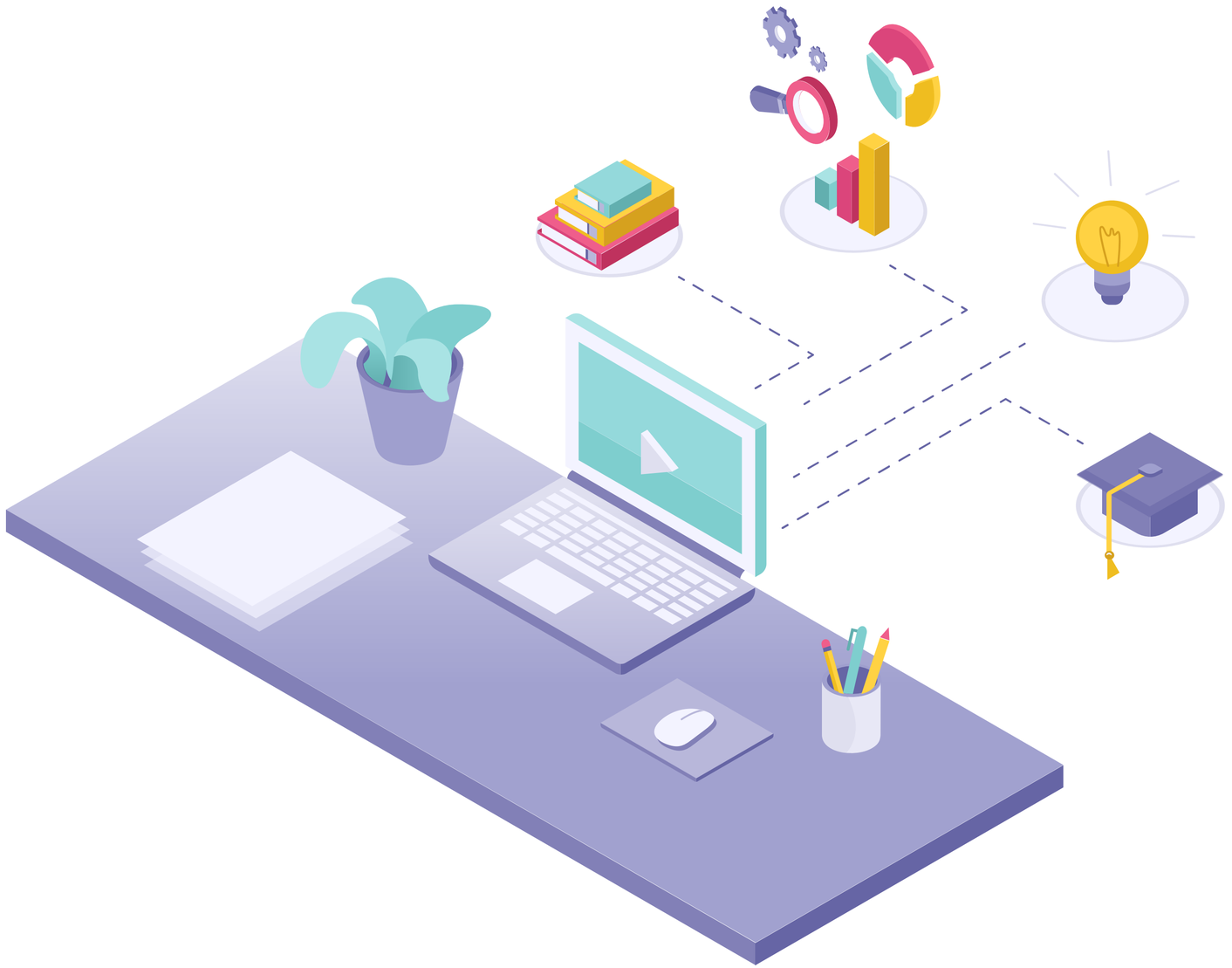


Amazon Quicksight

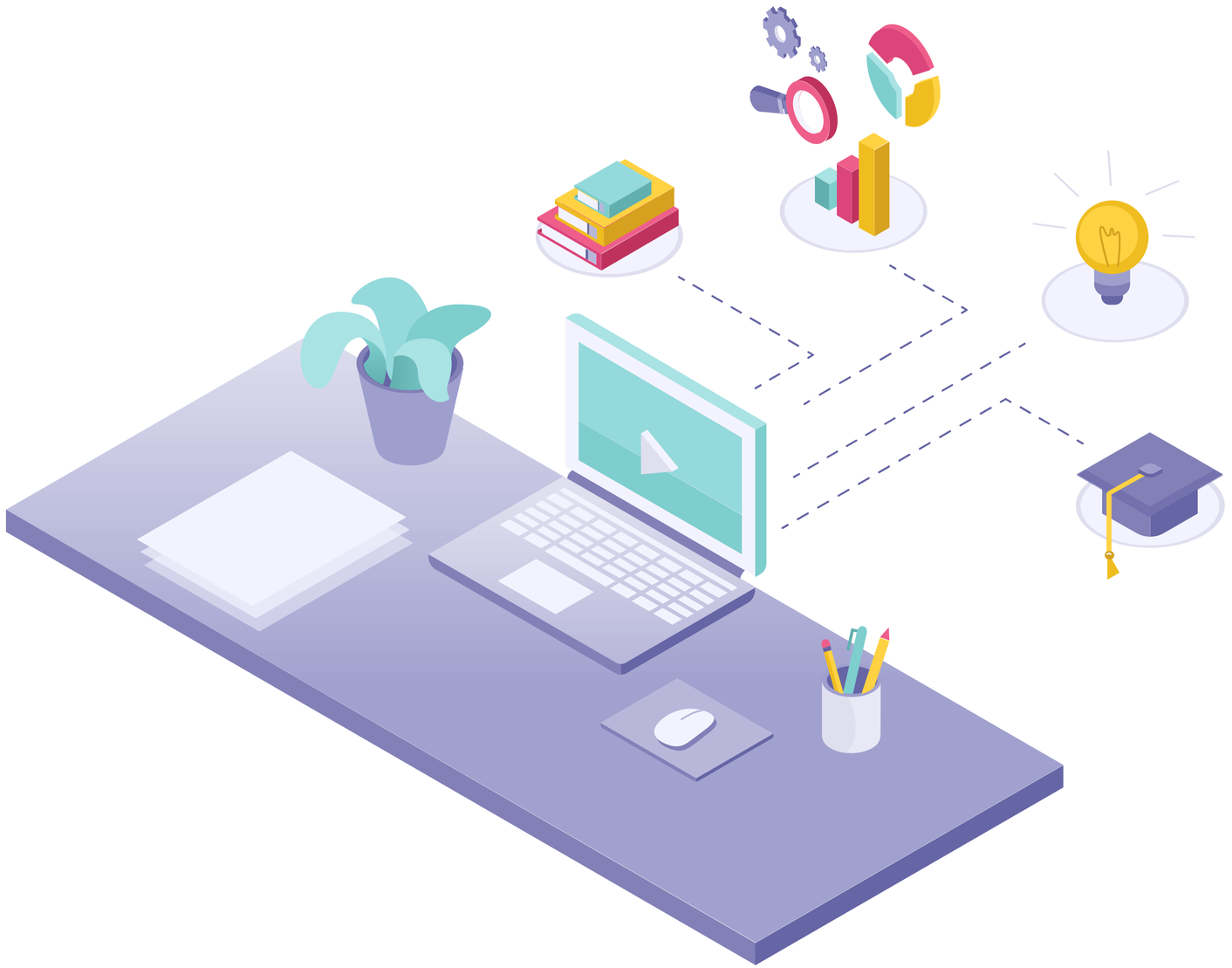
Choisir le bon service



Artificial Intelligence & Machine Learning (AI/ML)



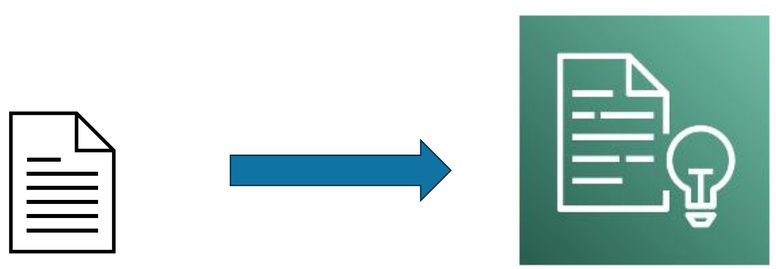
Amazon Comprehend



Amazon Comprehend

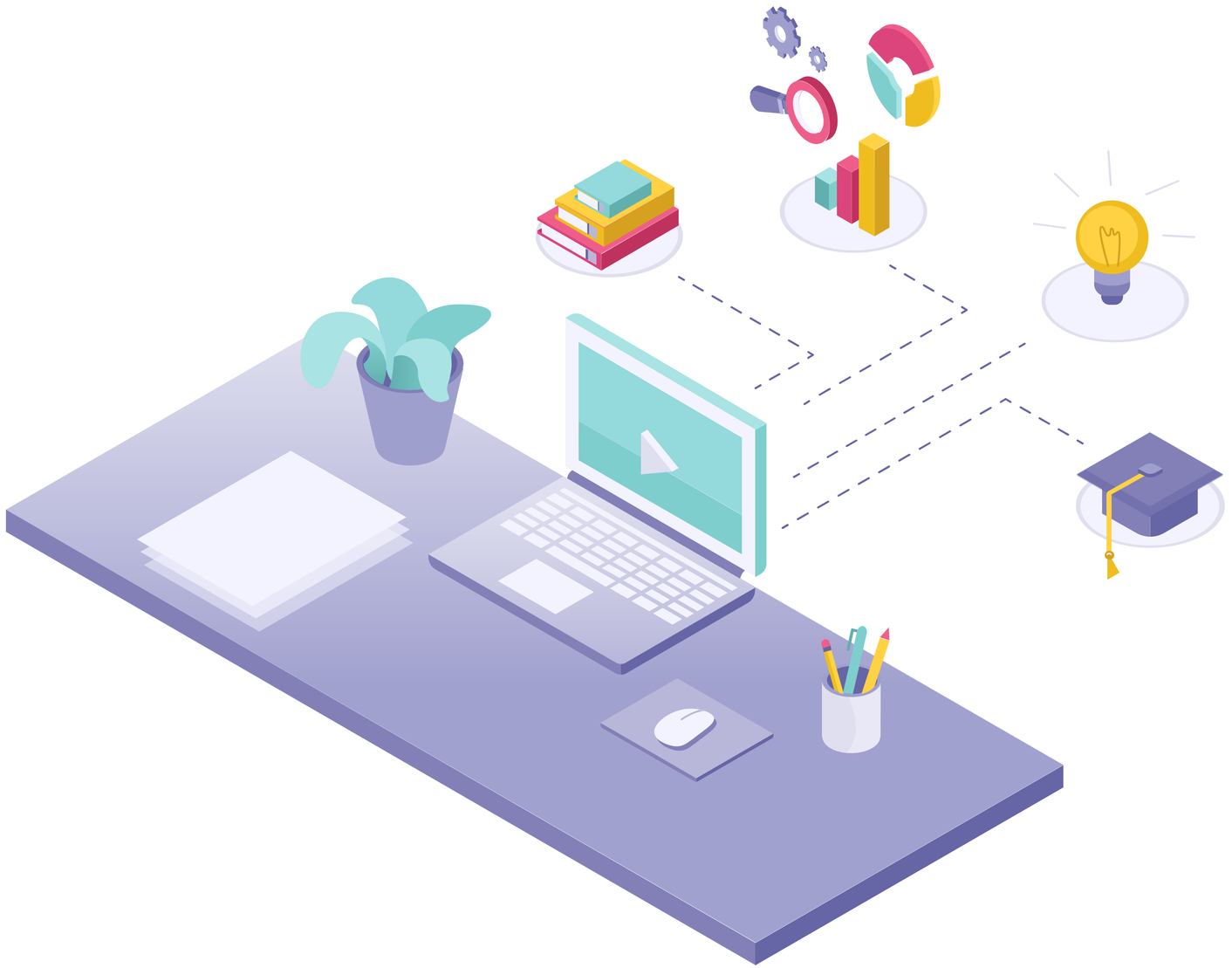
Service de traitement du langage naturel (**Natural Langage Processing**)

Utilise le Machine Learning pour **analyser et comprendre du texte**



- *Langue*
- *Sentiment (positif, neutre, négatif)*
- *Entités : personnes, marques, évènements, dates, ….*

Amazon Polly



Amazon Polly

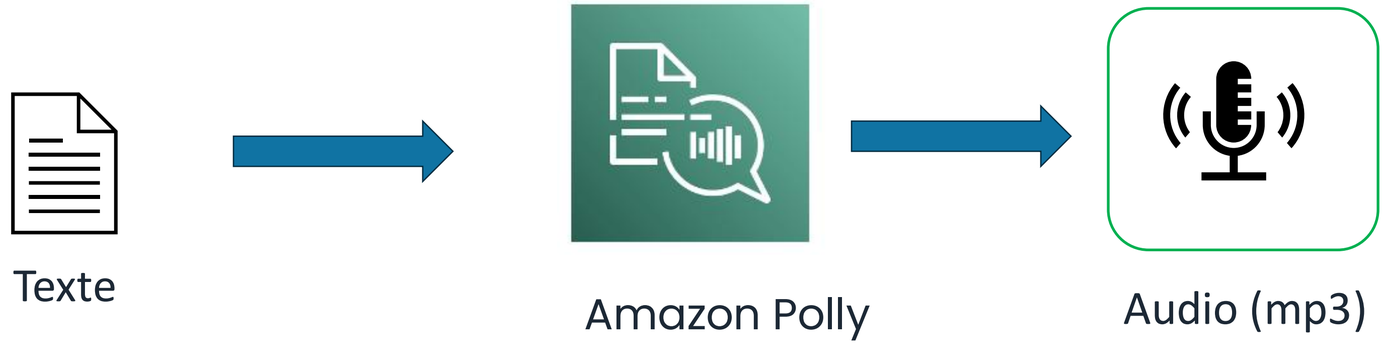


Permet de convertir du texte en discours audio (***Text-to-speech)***

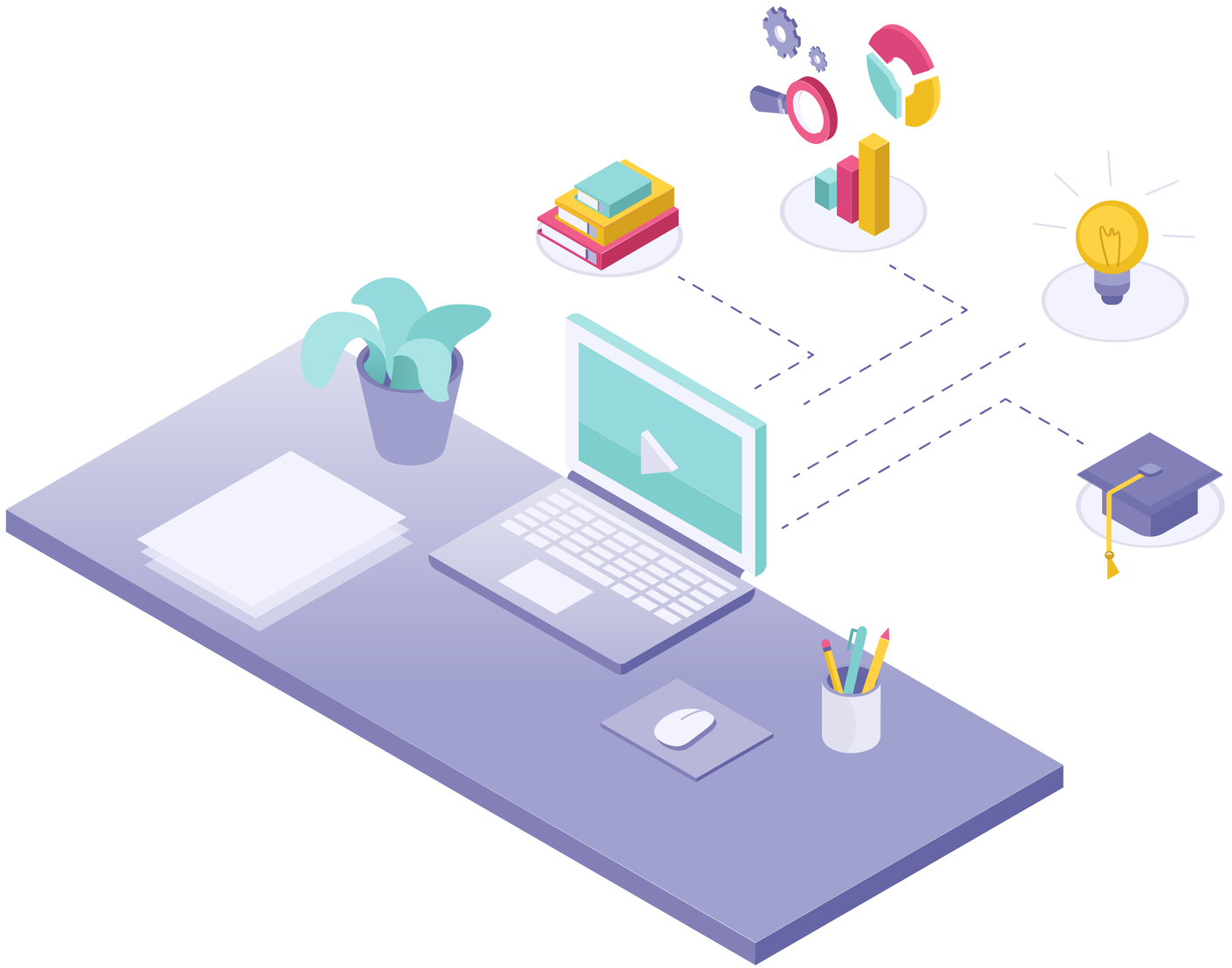
Propose des ***douzaines de voix réalistes***

Supporte plus d'une ***douzaine de langues*** *y compris Anglais et Français*

Personnalisation possible *: débit, ton, volume…*



Amazon Rekognition



Amazon Rekognition



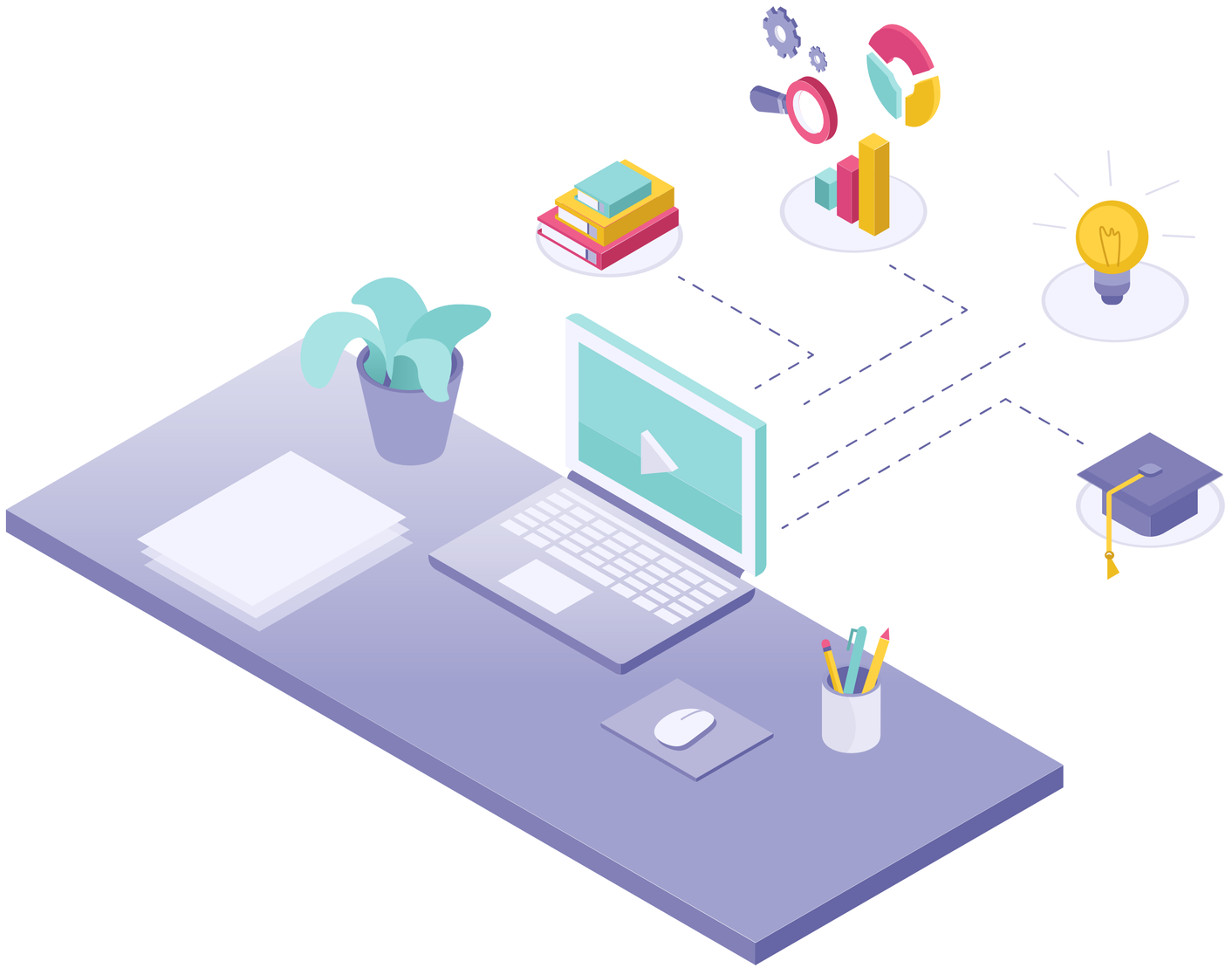
Service de **reconnaissance d'images et de vidéos**

Basé sur du **Deep Learning**

- Rekognition Image -> Analyse les images et détecte les objets, scènes, activités, visages, personnalités, textes, ...

- **Rekognition Video** -> Analyse les vidéos et détecte les mouvements de personnes, objets, célébrités, contenu inapproprié, ...

Amazon Transcribe



Amazon Transcribe



Service AI/ML qui **convertit du contenu audio en texte** -> Speech-to-Text

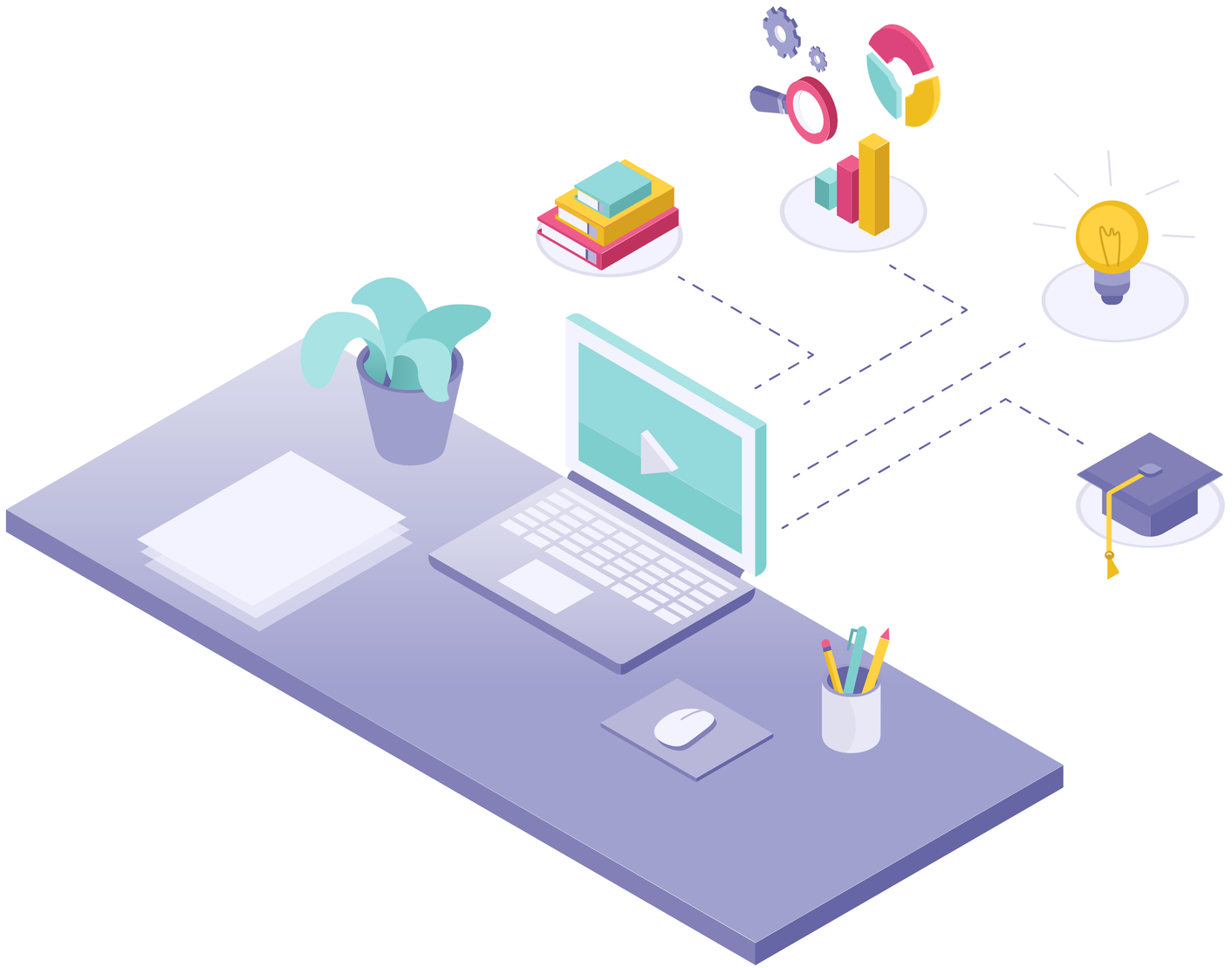
Fichiers audio (dans Amazon S3) ou flux audio en temps réel

Supporte des **dizaines de langues** dont l'anglais et le français

Formats supportés : mp3, mp4, Ogg, WebM, WAV...



Amazon Textract



Amazon Textract

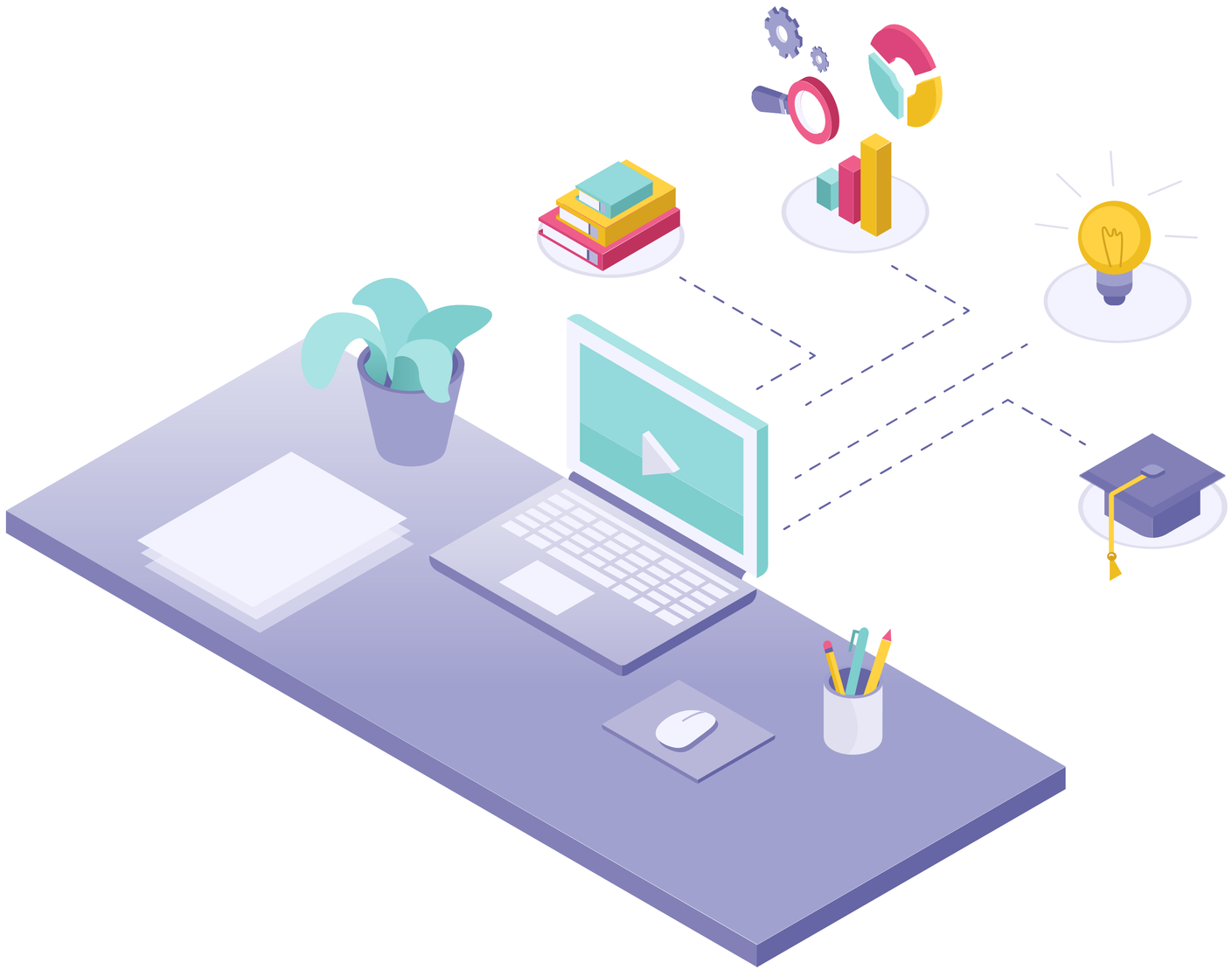
Détecte et extrait le texte imprimé, l'écriture manuscrite, les données structurées à partir d'images ou de documents numérisés

Formats supportés : Images (PNG, JPEG, TIFF), PDF, images, tableaux, formulaires

Synchrone ou **asynchrone** (documents volumineux)



Amazon SageMaker



Amazon Sagemaker



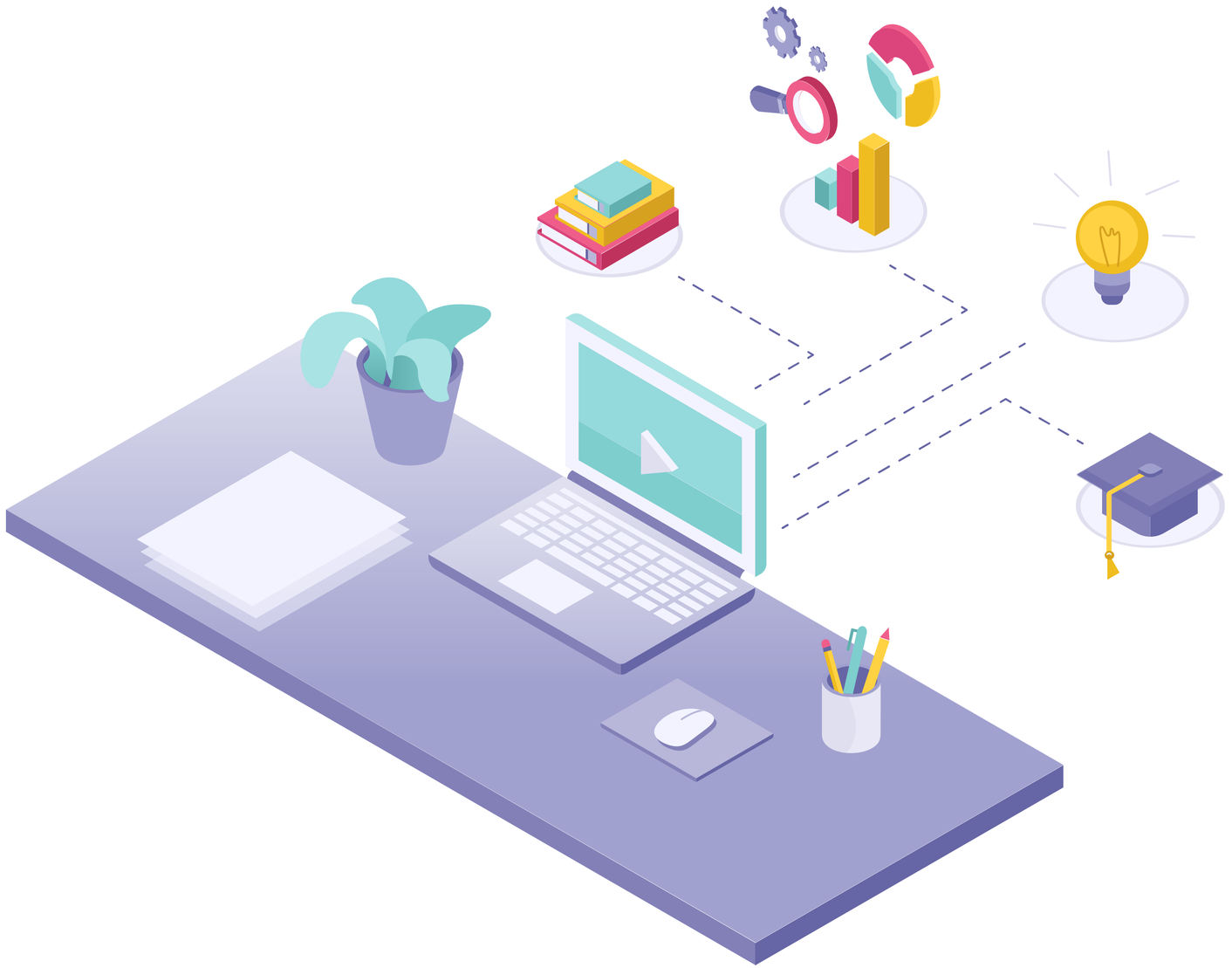
Permet de **créer, entrainer et déployer** des modèles de Machine Learning

Offre une **suite complète d'outils** pour les Data Scientists

Fonctionnalités clés

- Construction et entrainement des modèles
- Déploiement des modèles en production
- Gestion du cycle de vie des modèles
- Notebooks de développement
- Préparation de données

Les services AI/ML



En résumé



Amazon Comprehend

Service de traitement NLP (Natural Language Processing)



Amazon Polly

Service de text-to-speech



Amazon Rekognition

Service d'analyse et reconnaissance d'images et vidéos



Amazon Transcribe

Service de speech-to-text



Amazon Textract

Service d'extraction automatique de texte imprimé ou manuscrit

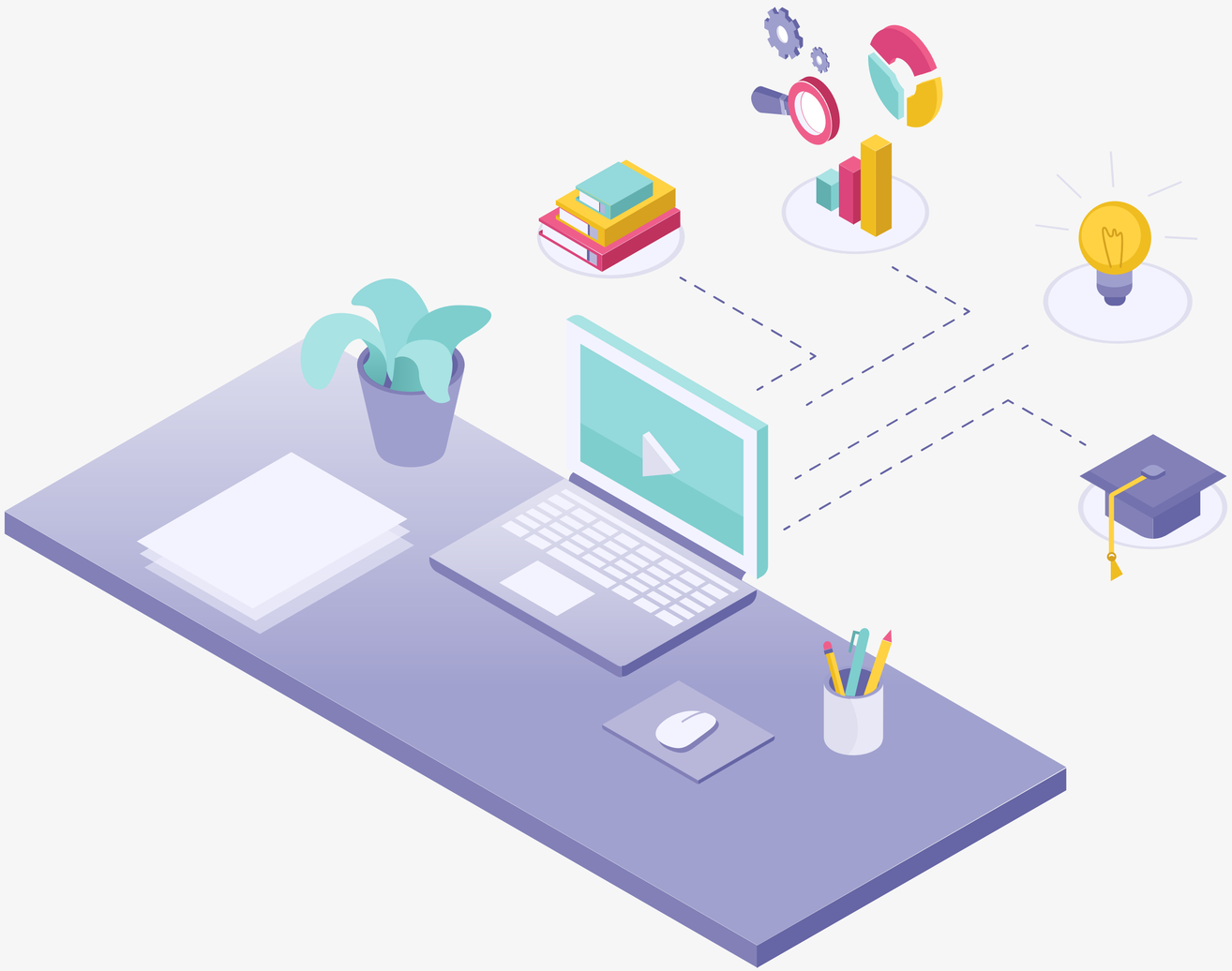


Amazon Sagemaker

Service pour créer, entrainer et déployer des modèles de Machine Learning

AI/ML sur AWS : Quiz

Permet d'identifier le sentiment à partir d'un texte en entrée	Amazon Comprehend
Extraire automatiquement le texte à partir d'un fichier PDF	Amazon Textract
Permet de créer, entraîner et de déployer des modèles Machine Learning	Amazon SageMaker
Développer une application qui convertit du texte en enregistrement audio	Amazon Polly
Permettre de reconnaître des célébrités dans des images et flux vidéos	Amazon Rekognition
Développer une application de génération de sous-titres pour un contenu audio	Amazon Transcribe



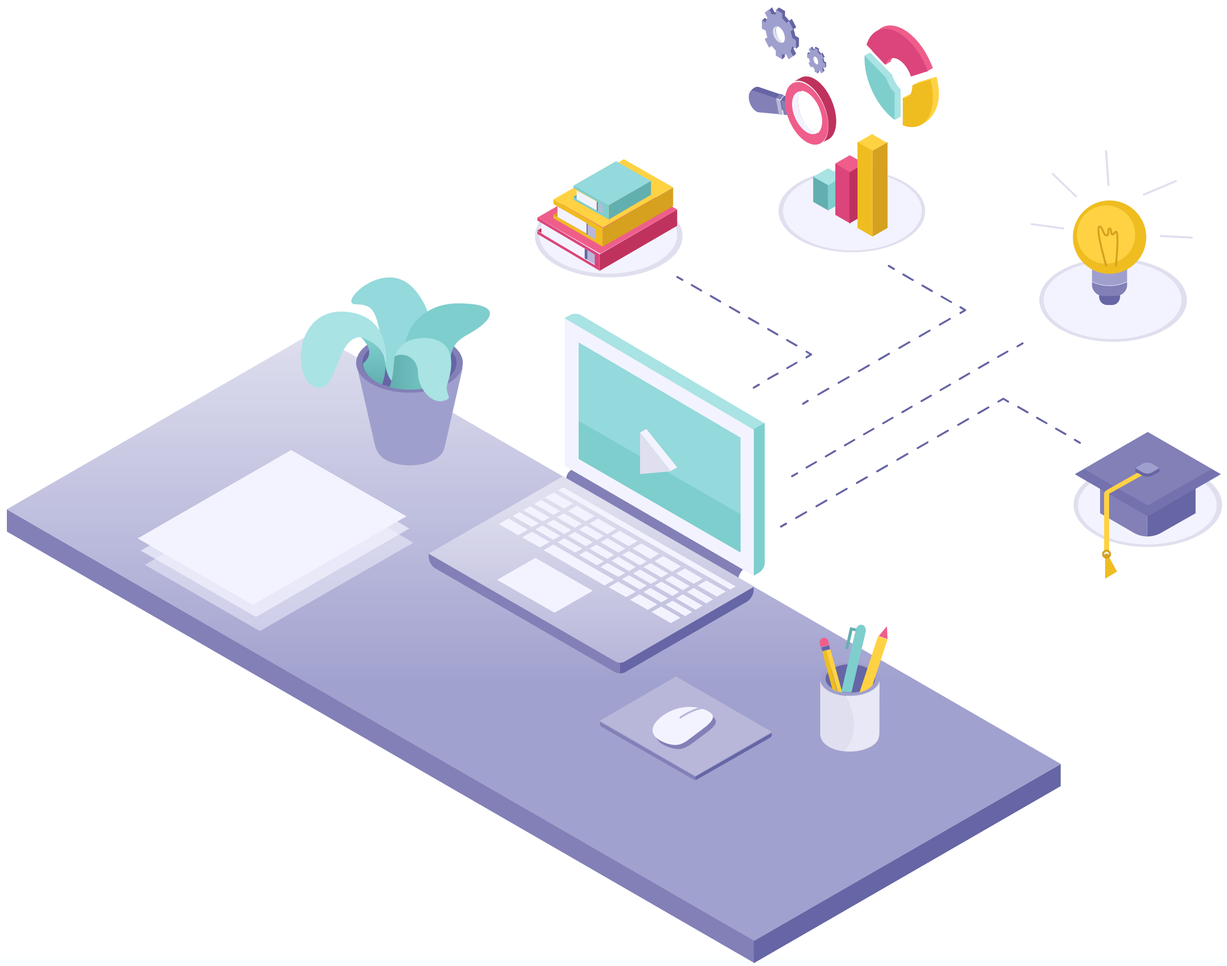
FIN DU MODULE

Lab : Analyser des logs CloudFront avec Amazon Athena

1. Explorer les logs dans Amazon S3
2. Créer une base de données dans Amazon Athena
3. Créer une table dans Amazon Athena
4. Analyser les logs CloudFront avec Amazon Athena

Module 10 : Intégration d'applications

Intégrez des systèmes distribués et des applications sans serveur avec moins de code



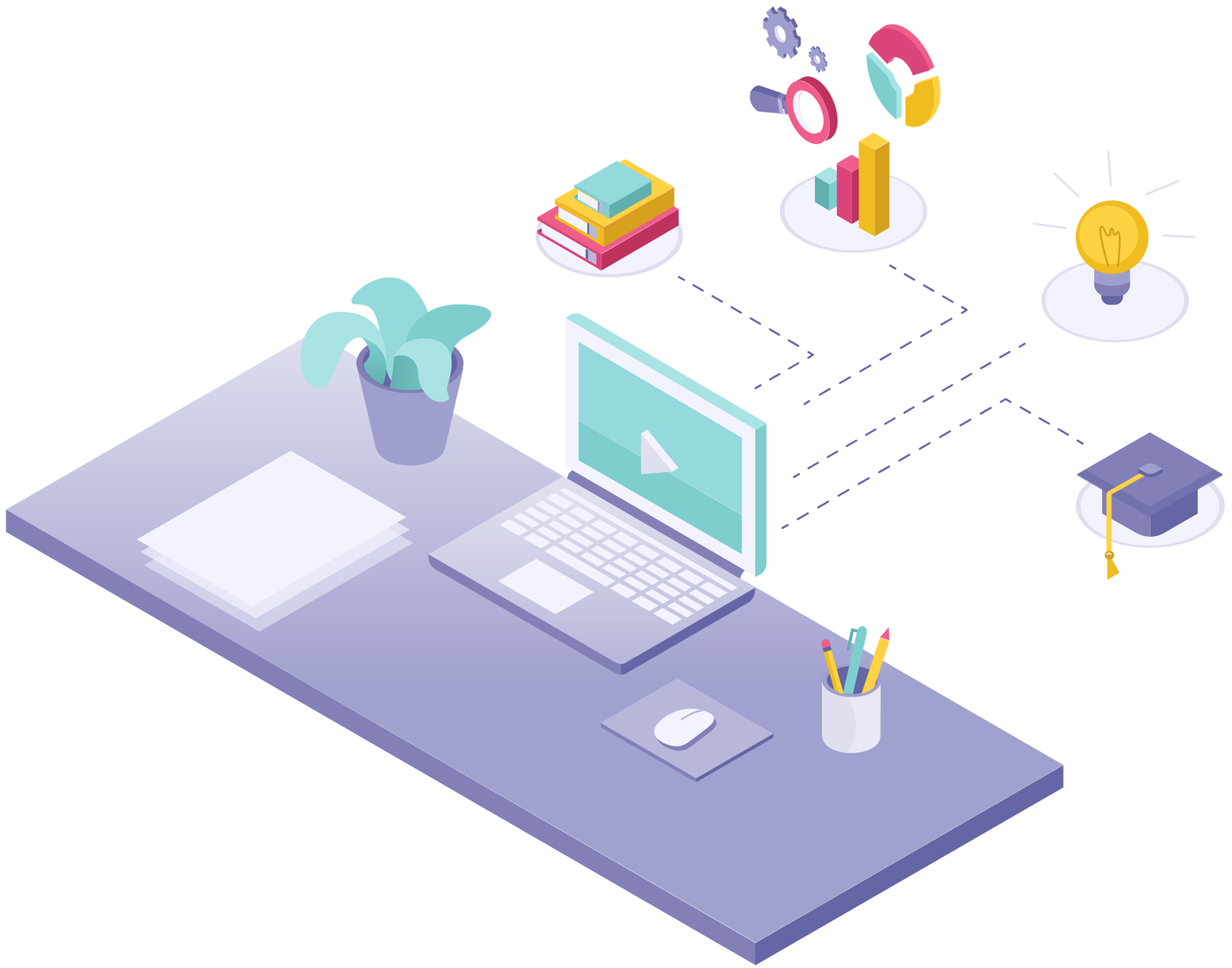
Quels sont les services de messagerie entre applications ?

Comment envoyer des notifications (SMS, E-Mail, ..) avec le Cloud AWS ?

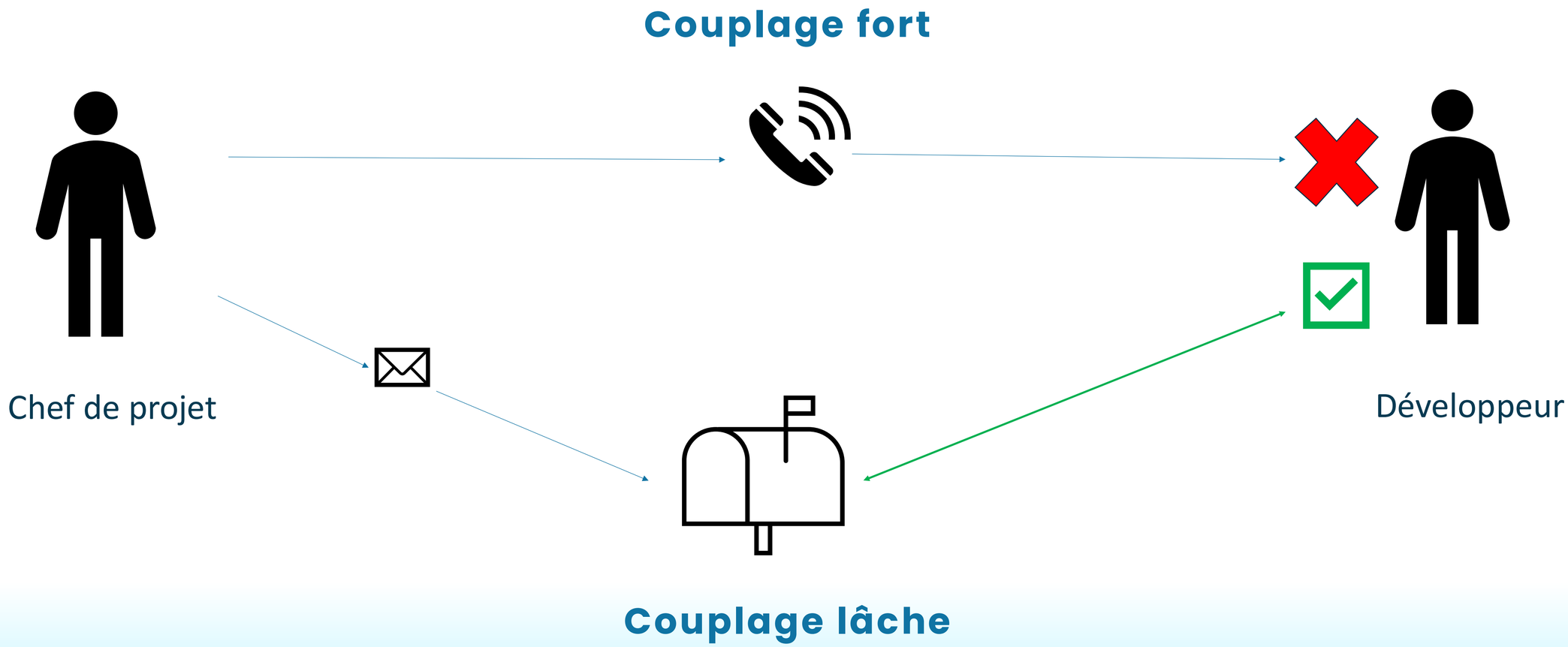
Quels sont les services de mise en file de messages sur le cloud AWS ?



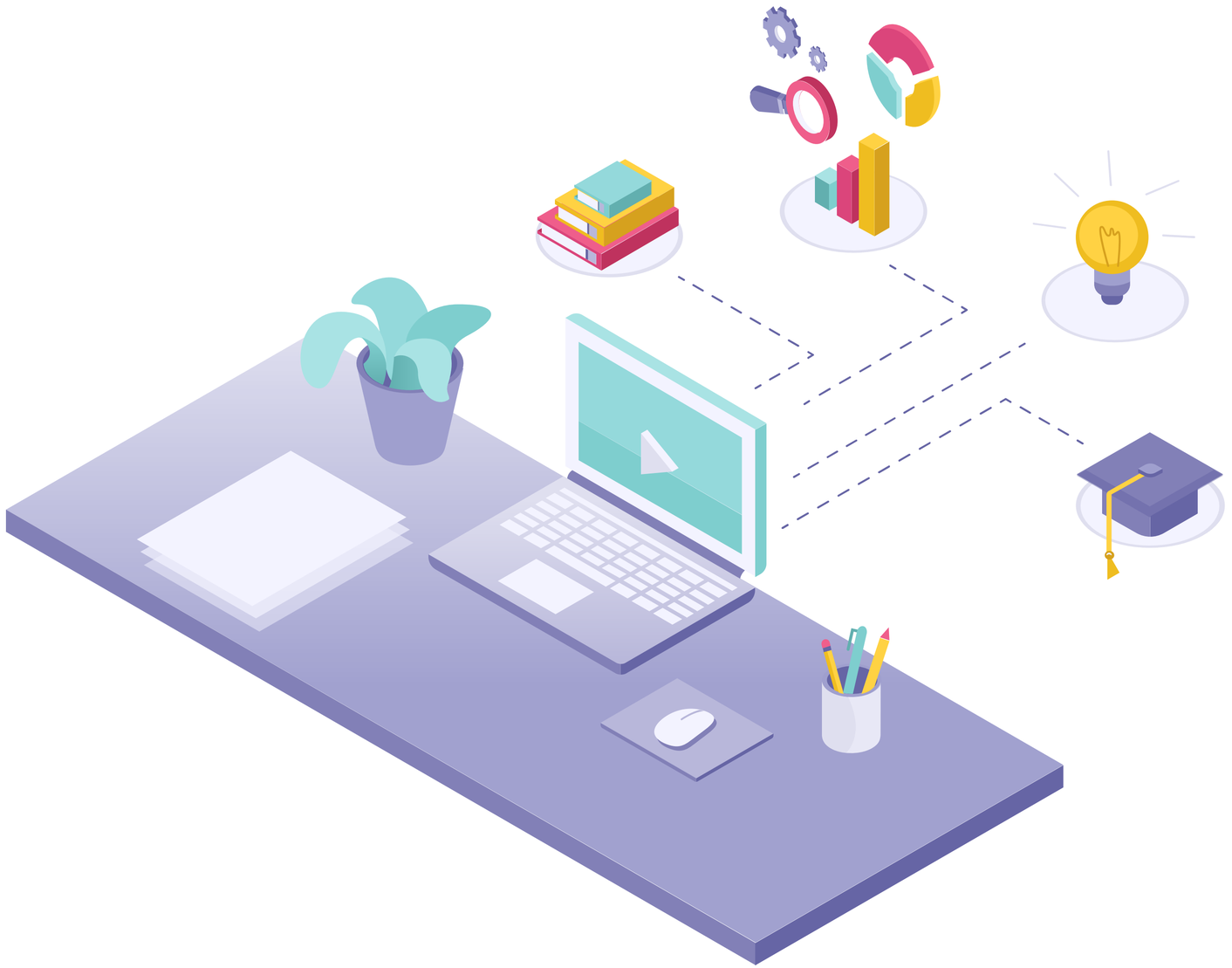
Concepts IT



Couplage entre applications



Amazon Simple Queue Service (SQS)



Amazon SQS



Service de **files de messages** (Mode **Polling**)

Permet le **couplage lâche** d'applications

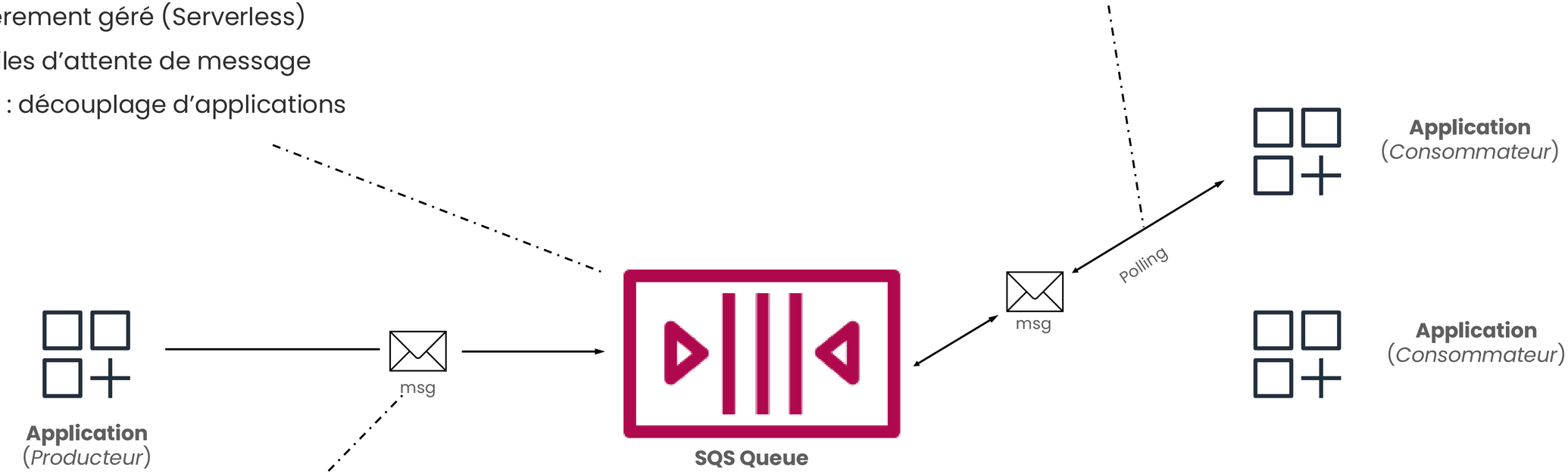
Période de **rétention des messages** : 4 jours par défaut (14 jours max)

Message :

- Taille <= 256 KB
- Format : texte, xml, json

Architecture

- Service entièrement géré (Serverless)
- Fournit des files d'attente de message
- Cas d'usage : découplage d'applications

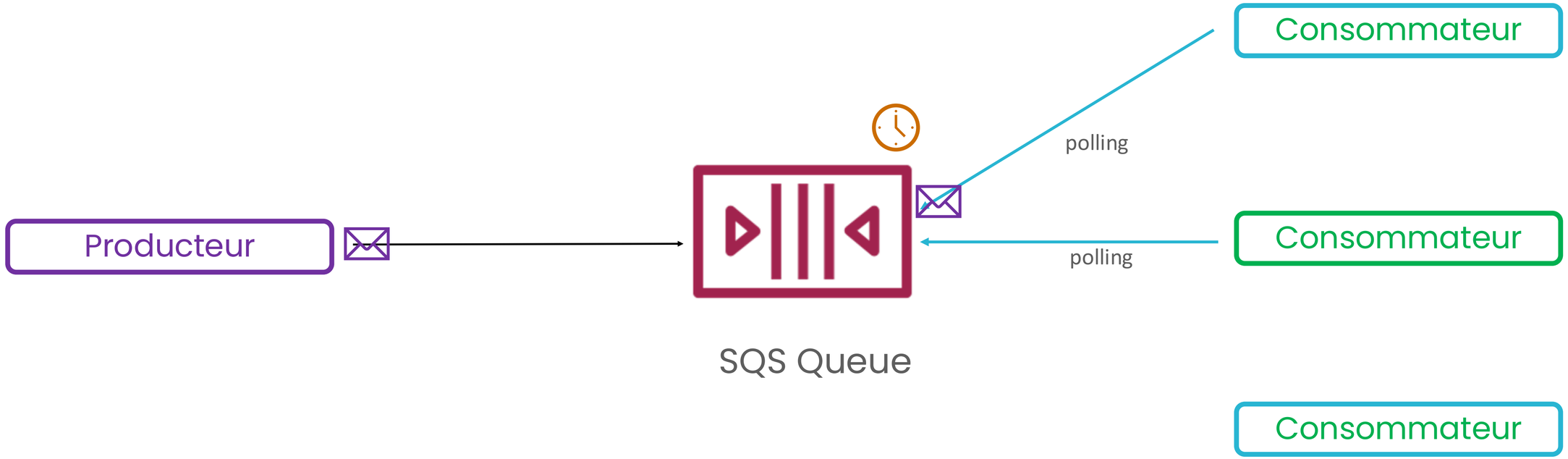


- Modèle de Polling
- 1 file peut avoir plusieurs consommateurs
- Le message est traité par 1 seul consommateur

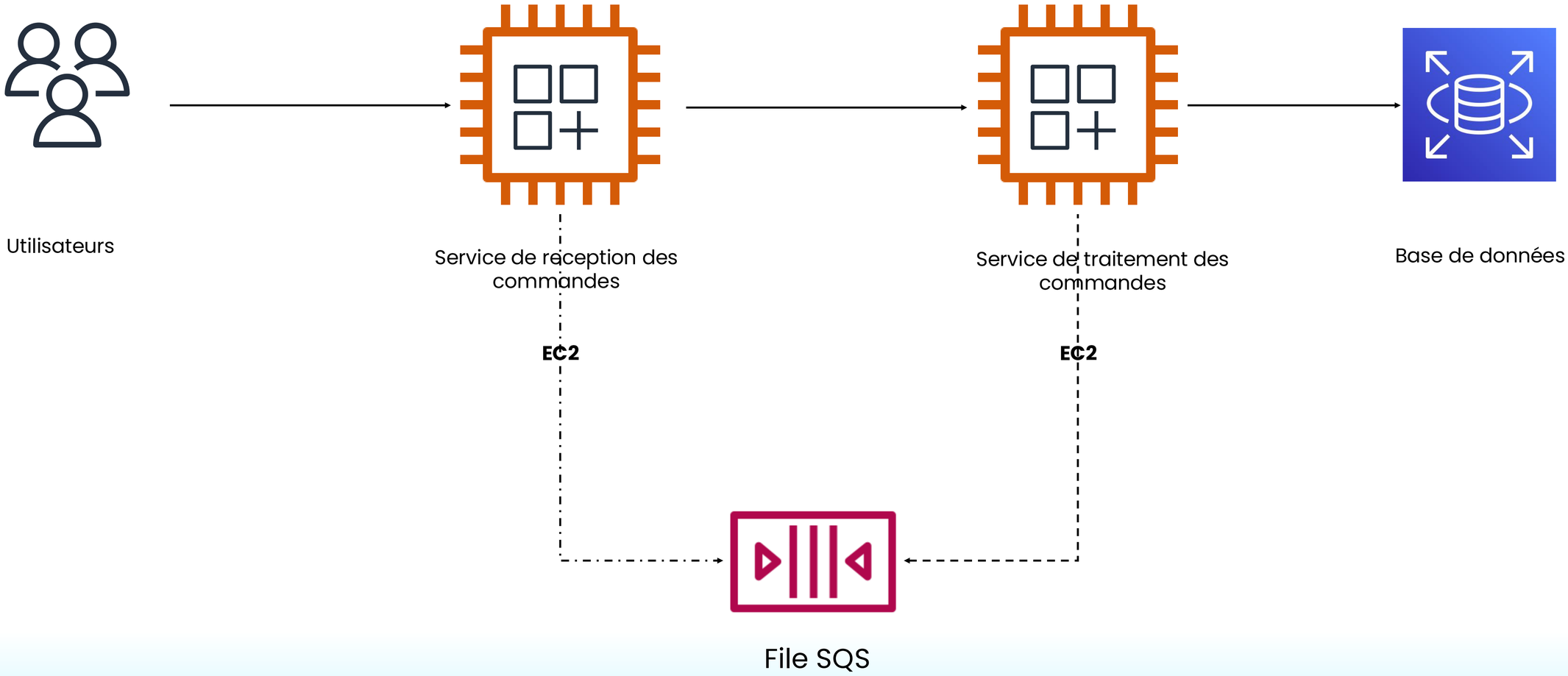
- Période de rétention : 4 jours par défaut (14 jours max)
- Queue Standard ou FIFO

- Taille <= 256 KB
- Format : texte, xml, json

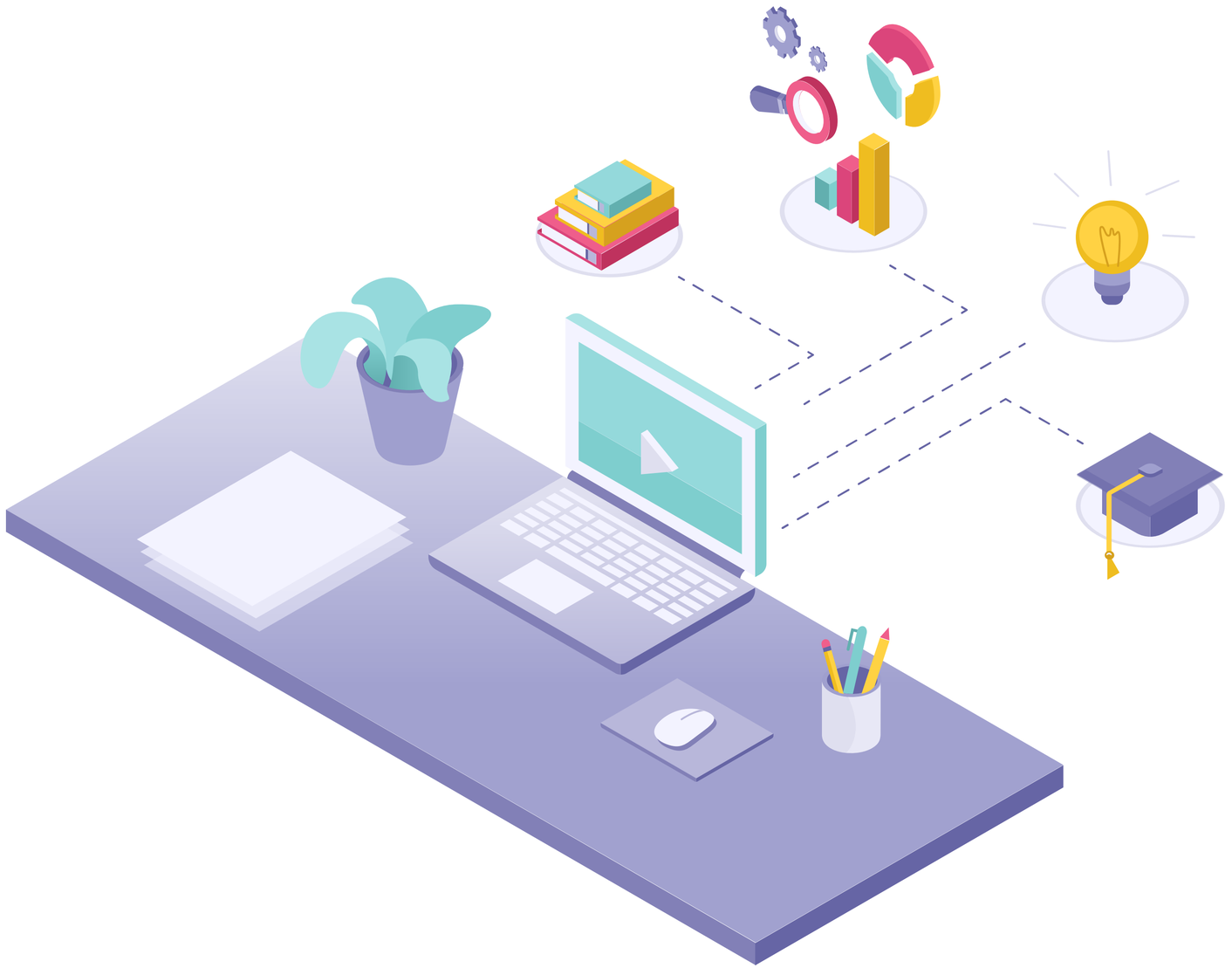
Exemple avec plusieurs consommateurs



Couplage lâche d'applications avec Amazon SQS



Amazon Simple Notification Service (SNS)



Amazon SNS



Service ***Serverless*** d'**envoi de notifications** (Mode **Publish/Subscribe**)

Similaire à une **Newsletter** avec des abonnés -> ***Push***

SNS peut envoyer des notifications :

- **À des abonnés** : par e-mail, SMS, HTTP/HTTPs
- **à d'autres services AWS**. Exemple : SQS, Lambda,...

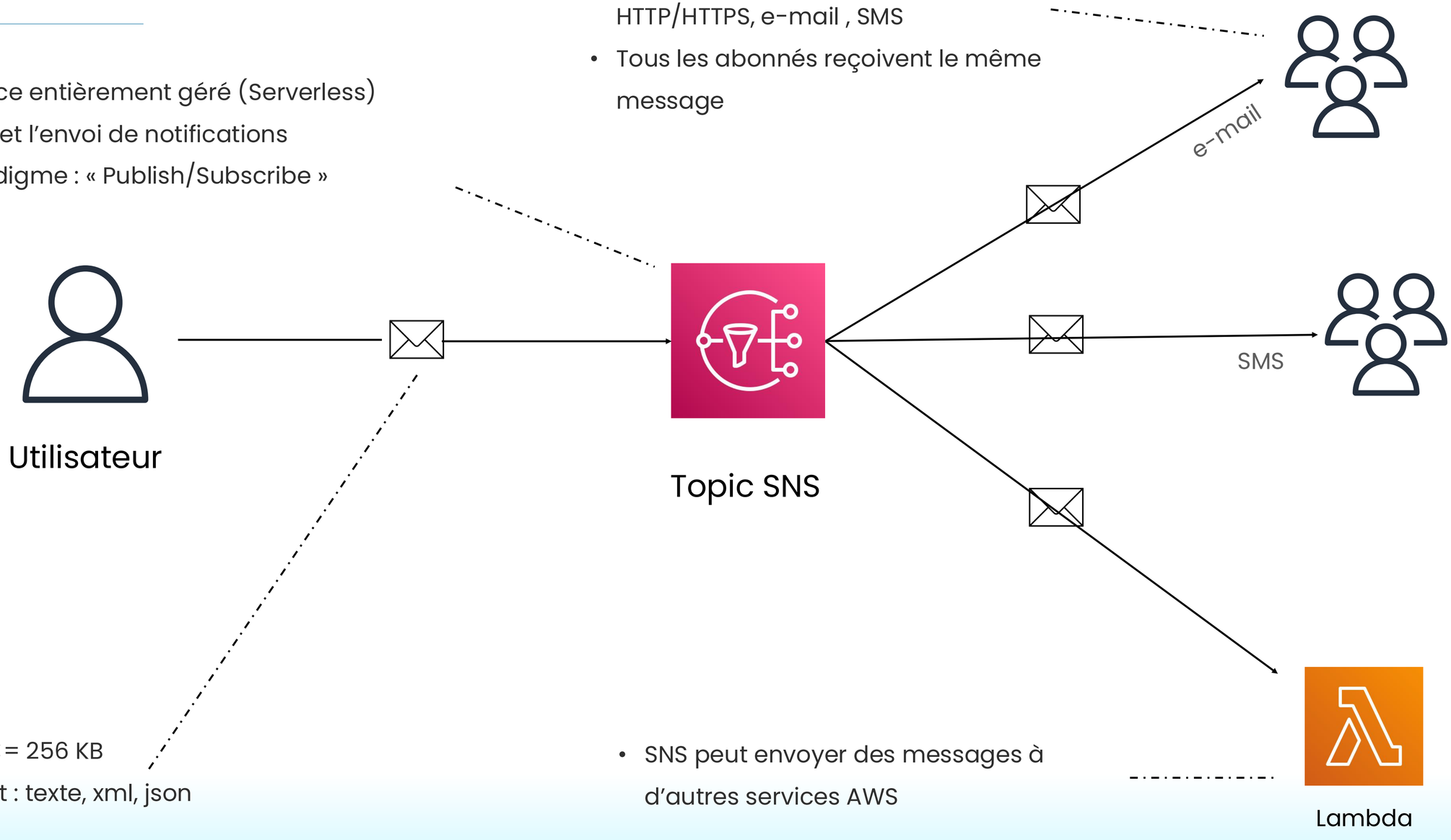
Message :

- Taille <= 256 KB
- Format : texte, xml, json

Architecture

- Service entièrement géré (Serverless)
- Permet l'envoi de notifications
- Paradigme : « Publish/Subscribe »

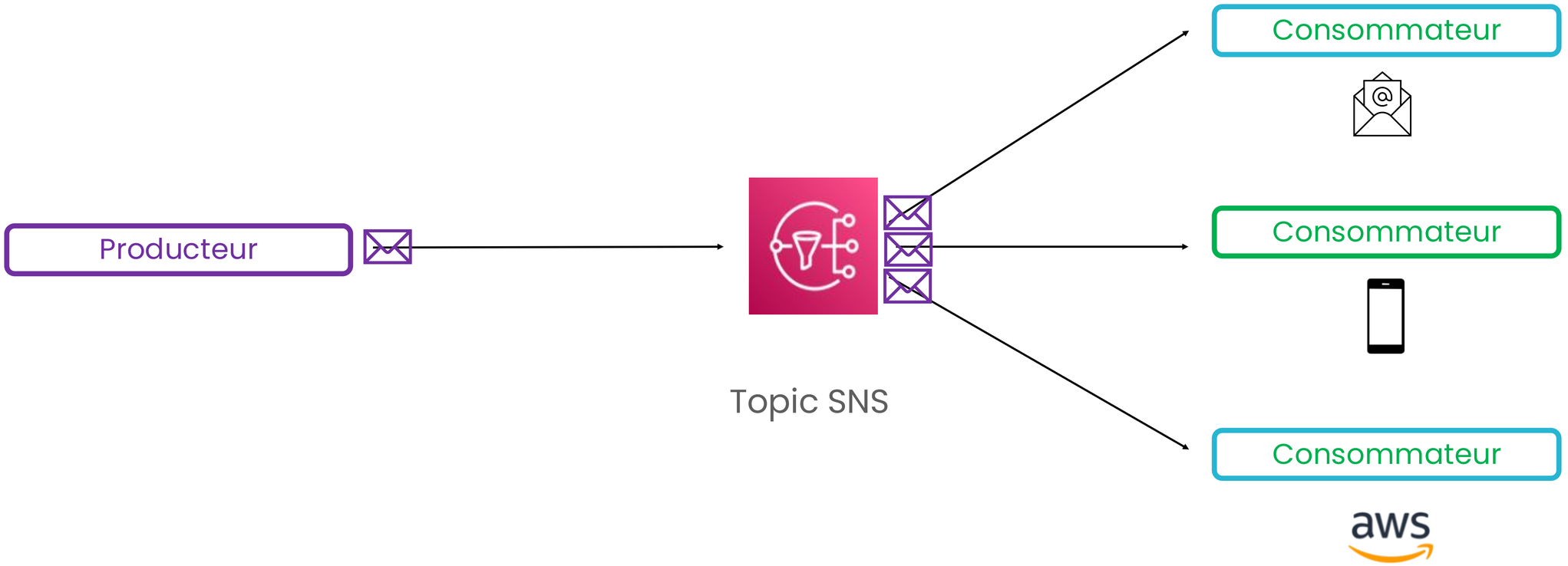
- Multiples abonnés
- Plusieurs protocoles de notification : HTTP/HTTPS, e-mail , SMS
- Tous les abonnés reçoivent le même message



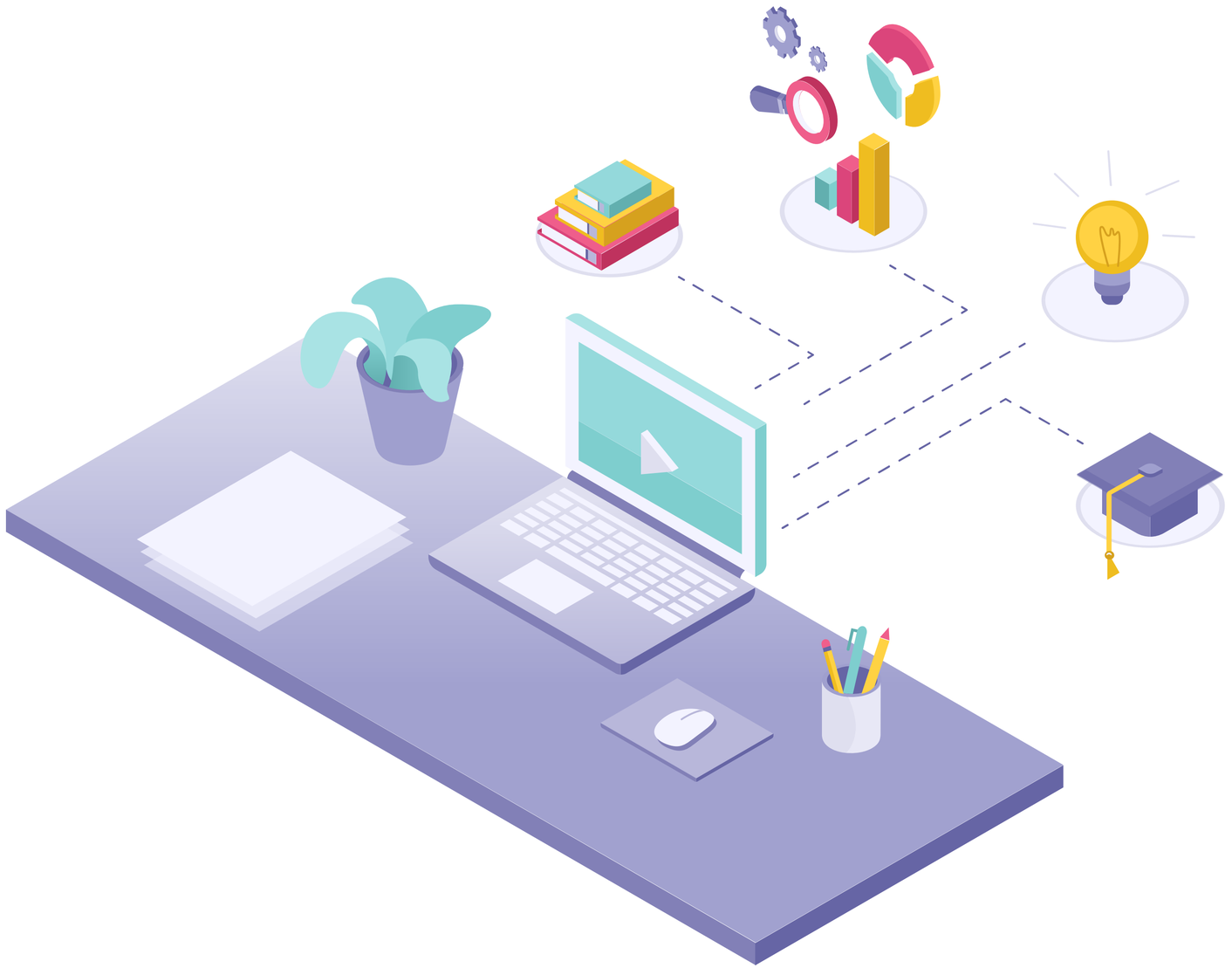
- Taille <= 256 KB
- Format : texte, xml, json

- SNS peut envoyer des messages à d'autres services AWS

Exemple avec plusieurs abonnés



Amazon EventBridge



Amazon EventBridge



Bus d’évènements 100% **Serverless**

Permet de connecter différentes applications et services AWS en utilisant des événements ou des triggers

Permet de créer des architectures *Event-driven*

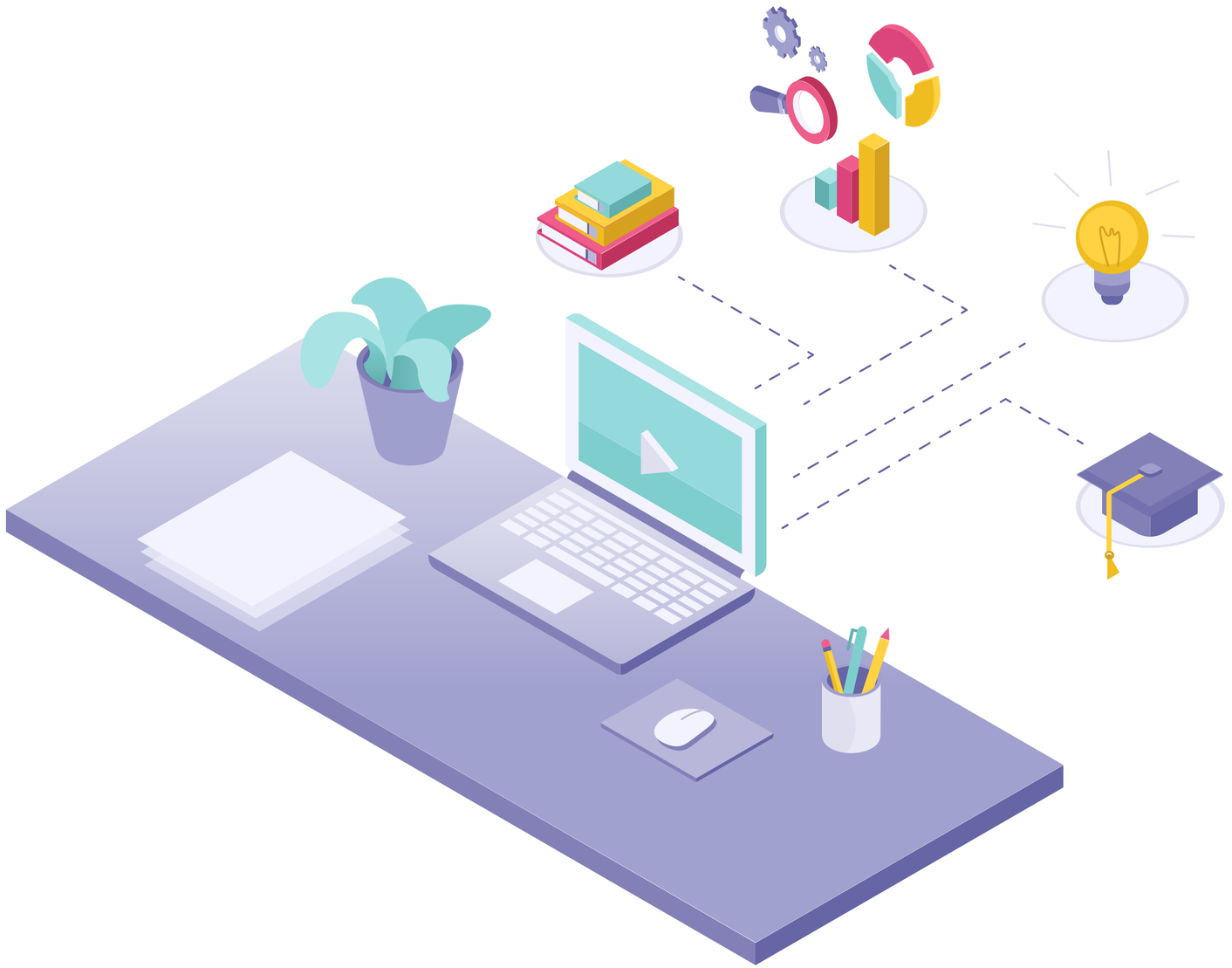
***Concepts clés* :**

- ***Sources*** : Amazon S3, AWS Lambda, EC2, CloudWatch,...
- ***Cibles*** : appeler une fonction Lambda, envoyer une notification SNS,...
- ***Règles*** : expressions de filtrage pour déclencher des actions

Amazon EventBridge



Amazon MQ



Amazon MQ



Fournit des services de **messagerie** entre applications

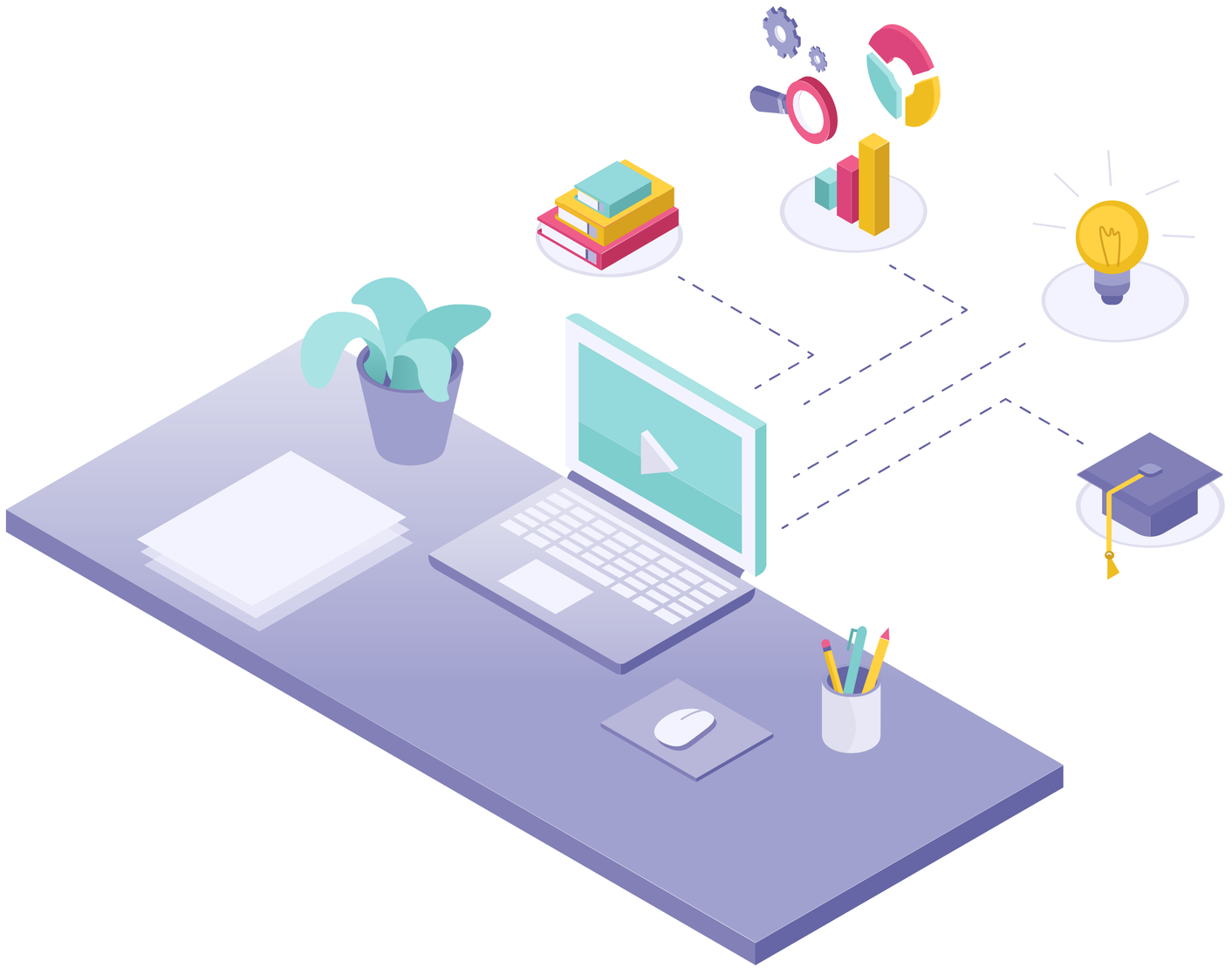
Brokers supportés : **Apache ActiveMQ** ou **RabbitMQ**

Entièrement géré par AWS

Cas d'usage

- Couplage lâche d'applications (comme avec Amazon SQS)
- Migration de brokers existants sur le cloud AWS

Amazon Simple Email Service (SES)



Amazon Simple Email Service (SES)



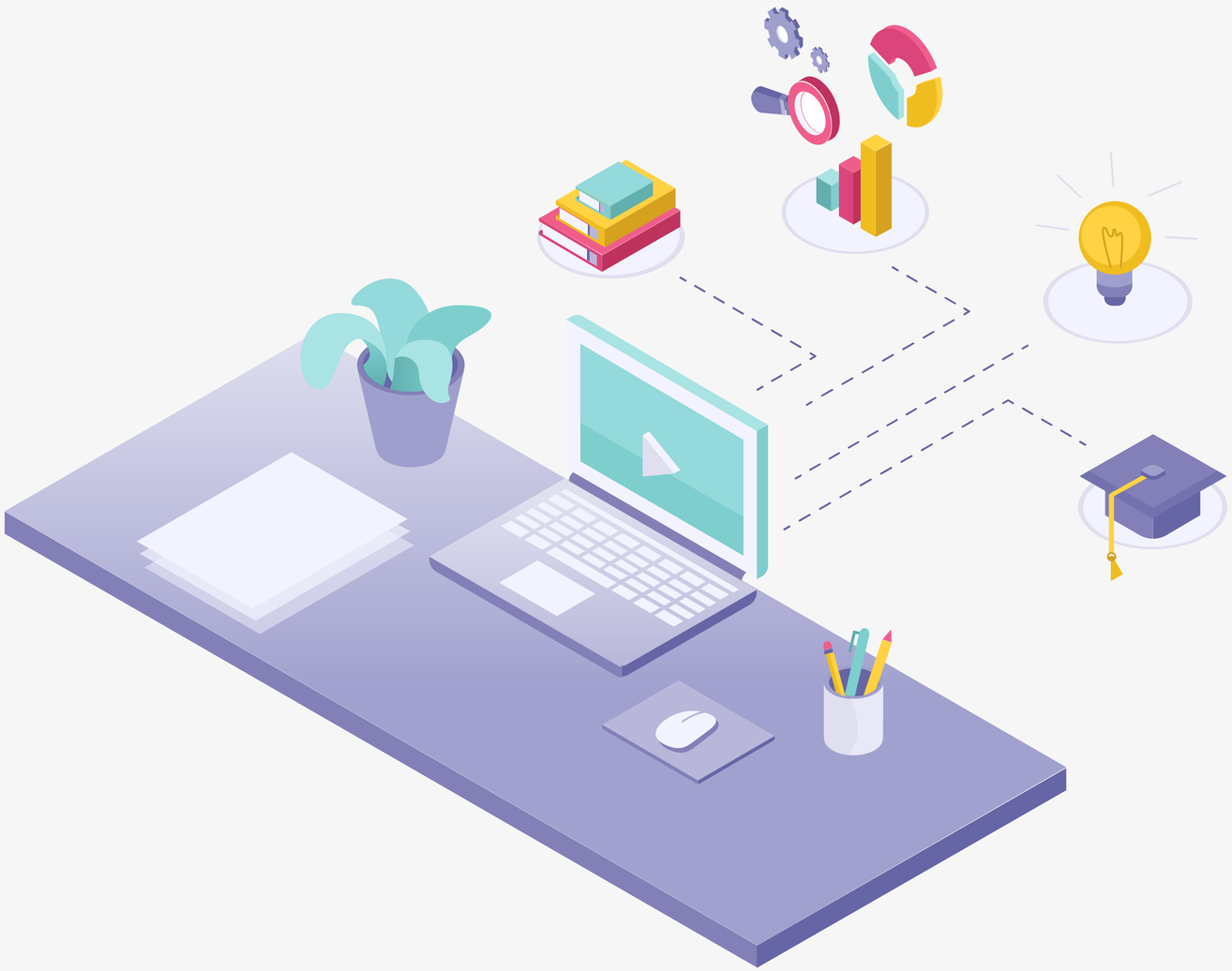
Service de **messagerie électronique** (**e-mail**) entièrement géré

Permet d'envoyer des e-mails **transactionnels ou en masse**

Supporte **SMTP**

Cas d'usage

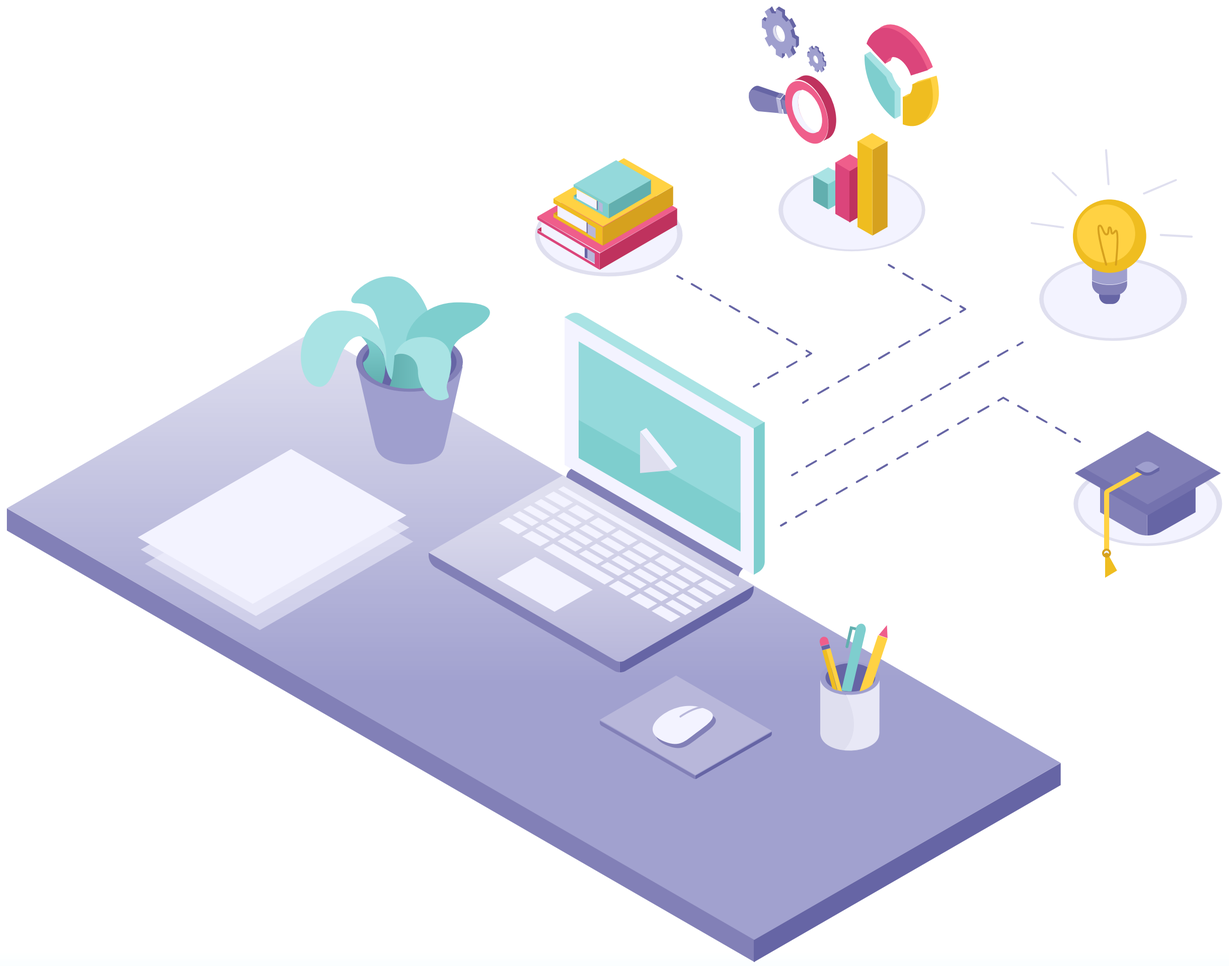
- E-mails transactionnels
- E-mails en masse : marketing, newsletter,..



FIN DU MODULE

Module 11 : AWS IAM

Gérer de façon sécurisée les identités et l'accès aux services et ressources AWS



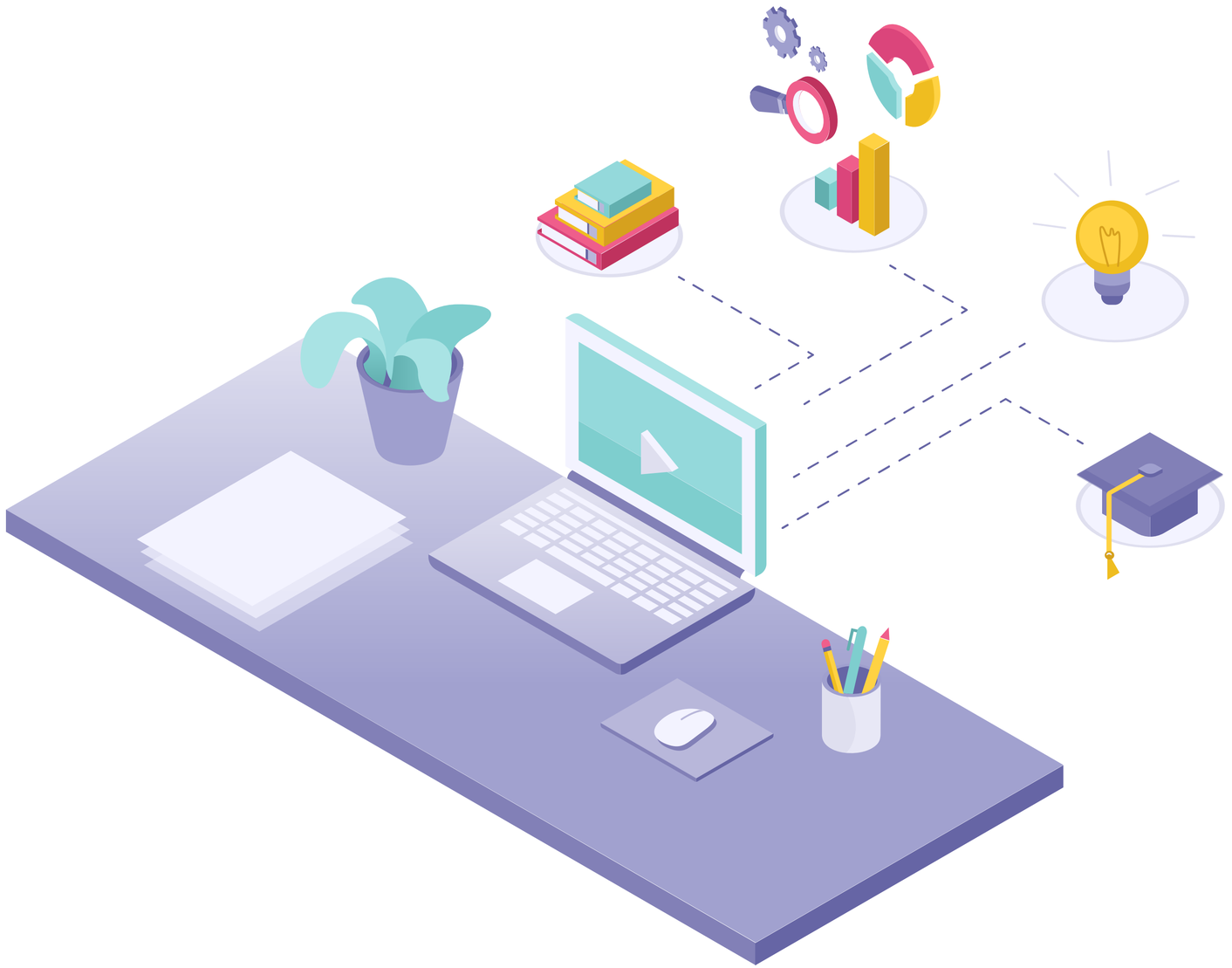
Comment marche la sécurité dans le cloud ?

Comment gérer les identités et les autorisations d'accès ?

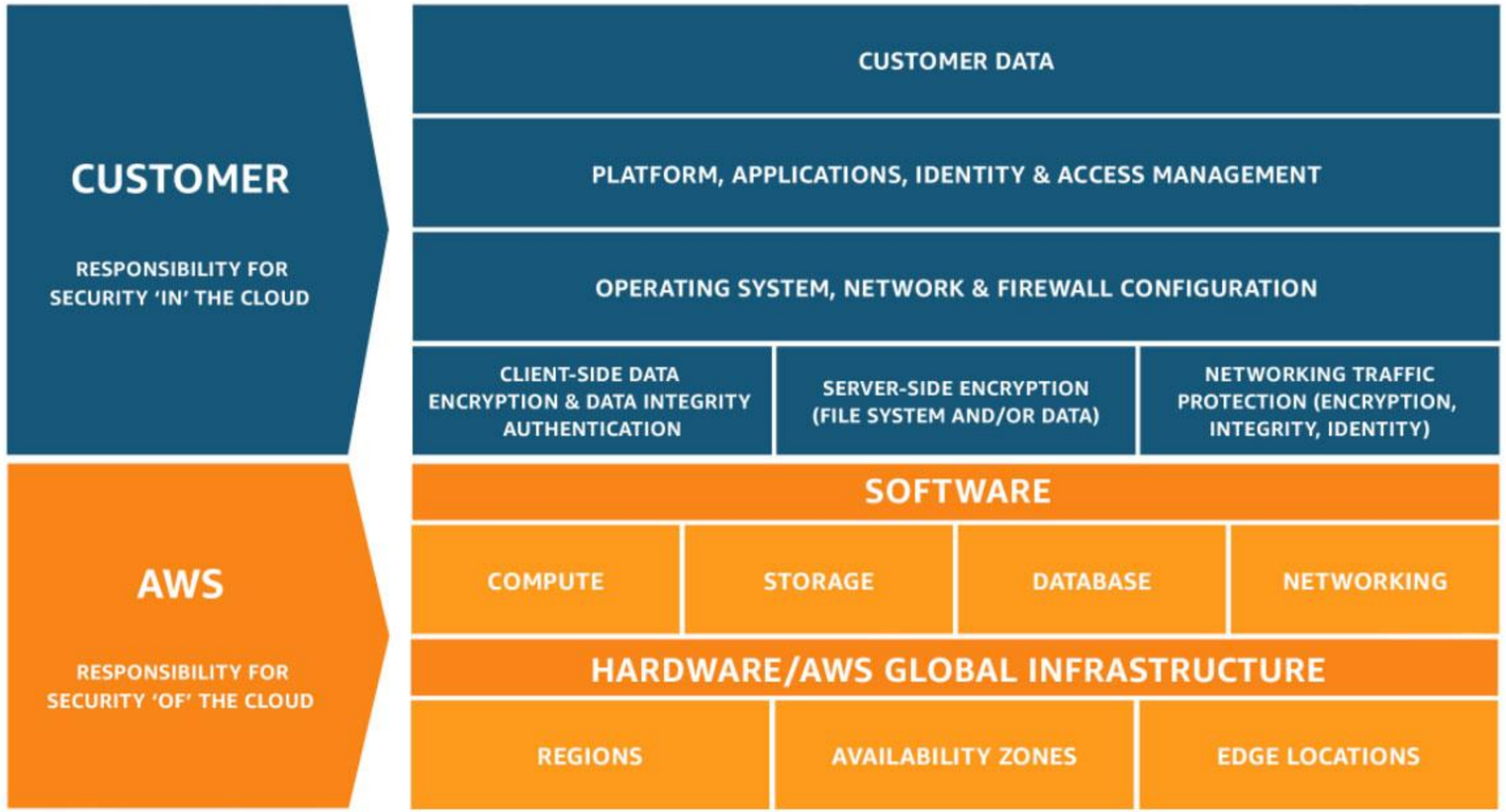
Comment administrer efficacement les utilisateurs?

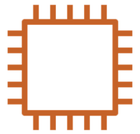


Modèle de responsabilité partagée



Modèle de responsabilité partagée





Instances EC2



Base de données RDS

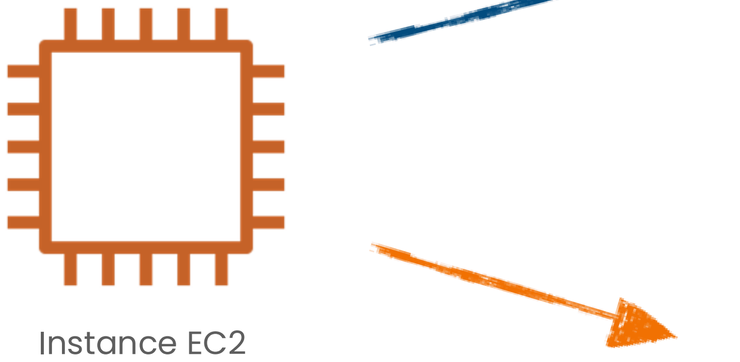


Utilisateurs IAM



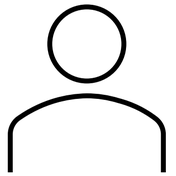
Data Center

Exemple Amazon EC2



Instance EC2

- ✓ Gestion des données (chiffrement, accès, classification)
- ✓ Gestion des logiciels et applications
- ✓ Gestion de la sécurité (groupes de sécurité, NACL,…)
- ✓ Gestion du système d'exploitation (mise à jour, antivirus,…)



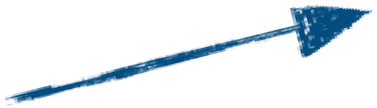
Vous

- ✓ Gestion de l'hyperviseur
- ✓ Gestion de l'infrastructure sous-jacente
- ✓ Gestion et protection des data centers

Exemple Amazon RDS

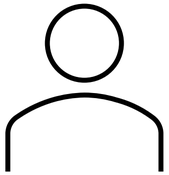


Amazon RDS





- ✓ Gestion des données (chiffrement, accès, classification)
- ✓ Gestion de la sécurité : groupes de sécurité…

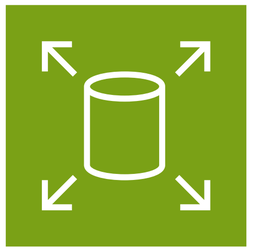


Vous

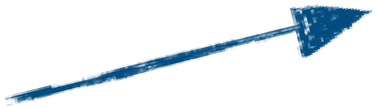
- ✓ Gestion des logiciels et applications
- ✓ Gestion du système d'exploitation (mise à jour, sécurité)
- ✓ Gestion du matériel sous-jacent
- ✓ Gestion de l'hyperviseur
- ✓ Gestion et protection des data centers



Exemple Amazon S3

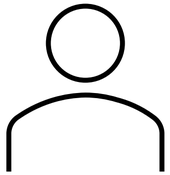


Amazon S3





✓ Gestion des données (chiffrement, accès, classification)



Vous

✓ Gestion des logiciels et applicatifs

✓ Gestion du système d’exploitation

✓ Gestion de l’hyperviseur

✓ Gestion de l’infrastructure sous-jacente

✓ Gestion et protection des data centers

QUIZ : Qui est responsable de la sécurité ?

Qui est responsable de la maintenance matérielle des serveurs ?



Qui est responsable de la gestion des autorisations d'accès aux data centers physiques ?

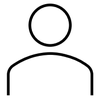


Qui est responsable de la gestion des correctifs de sécurité des instances EC2 ?



Vous

Qui est responsable des logiciels et applications installées sur les EC2 ?

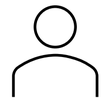


Vous

Qui est responsable de la gestion des correctifs de sécurité sur Amazon S3 ?



Qui est responsable de la bonne configuration des groupes de sécurité ?



Vous

Avec Amazon DynamoDB et Amazon S3, qui est responsable des options de chiffrement des données ?

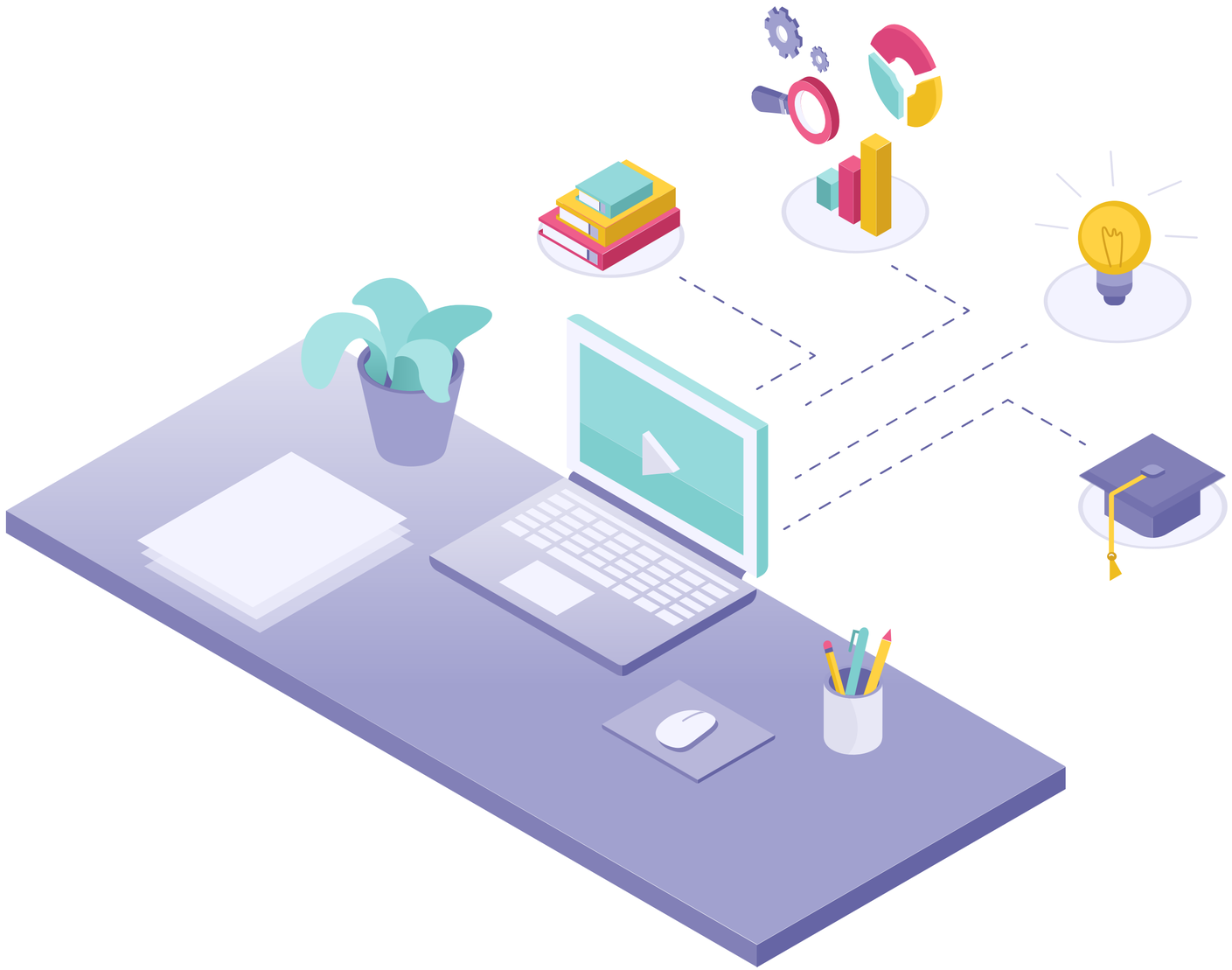


Vous

Qui est responsable de l'hyperviseur et de la correction des défauts liés ?



AWS Identity and Access Management (IAM)

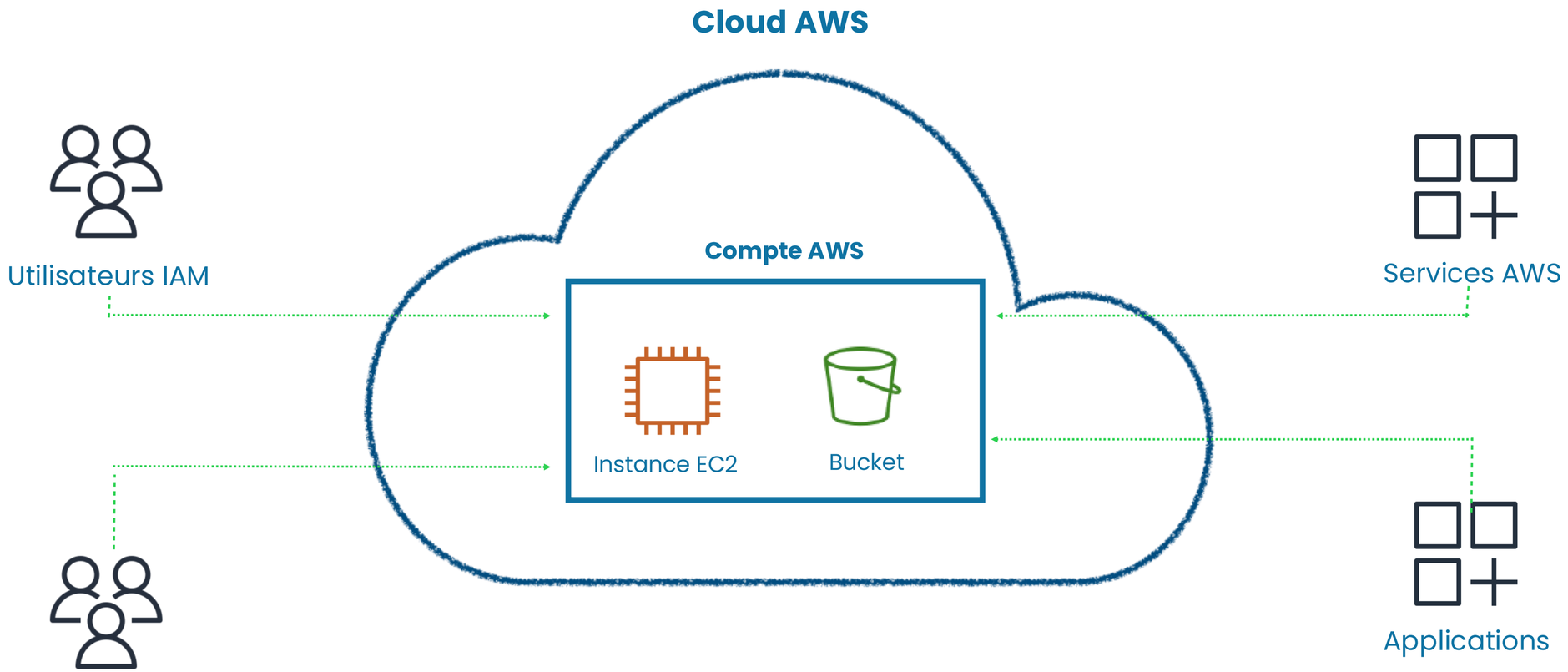


LeCloudFacile.com

Question

Qui a accès aux ressources dans votre compte AWS ?

Qui a accès à vos ressources ?



Par défaut personne, sauf si vous l'y autorisez

AWS IAM



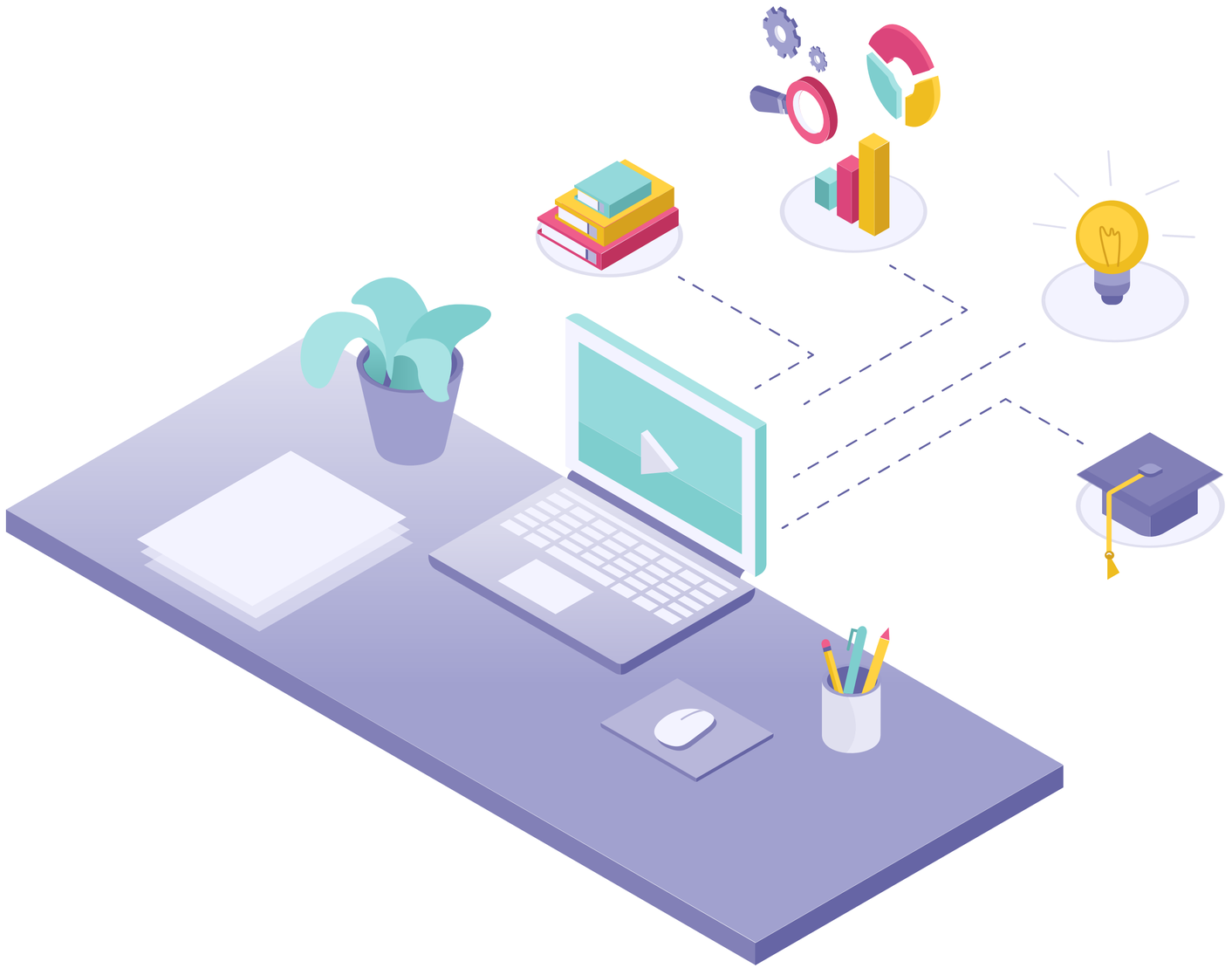
Permet de gérer l'**authentification** (identités) et l'**autorisation** (permissions)

dans votre compte AWS

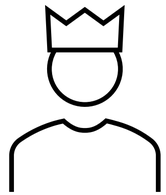
Permet d'administrer

- Les **utilisateurs** et les **groupes**
- Les **permissions** et les **rôles**
- Les **fédérations d'identité**

Utilisateurs et Groupes IAM



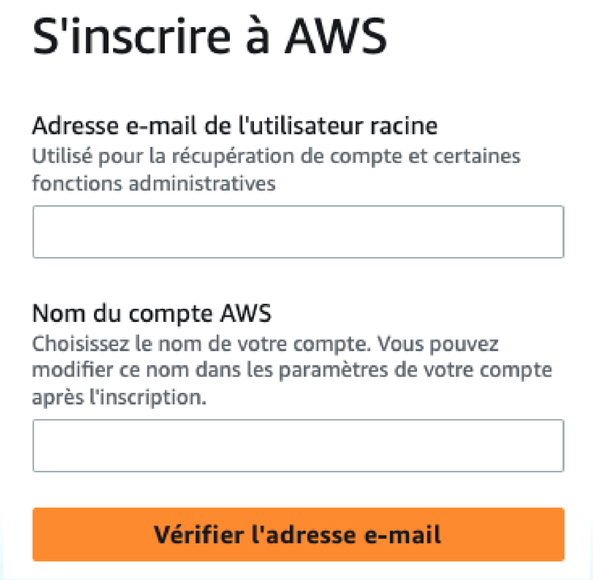
Utilisateur racine



En anglais : ***Root user***

C'est l'**email** qui a servi à créer le compte AWS

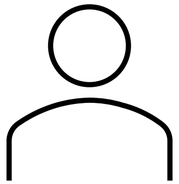
A tous les **privilèges et permissions**. Exemple : *fermer le compte AWS*



Bonnes pratiques

- Ne pas l'utiliser au quotidien !!
- L'utiliser uniquement pour créer des Administrateurs
- Associer un MFA

Utilisateur IAM



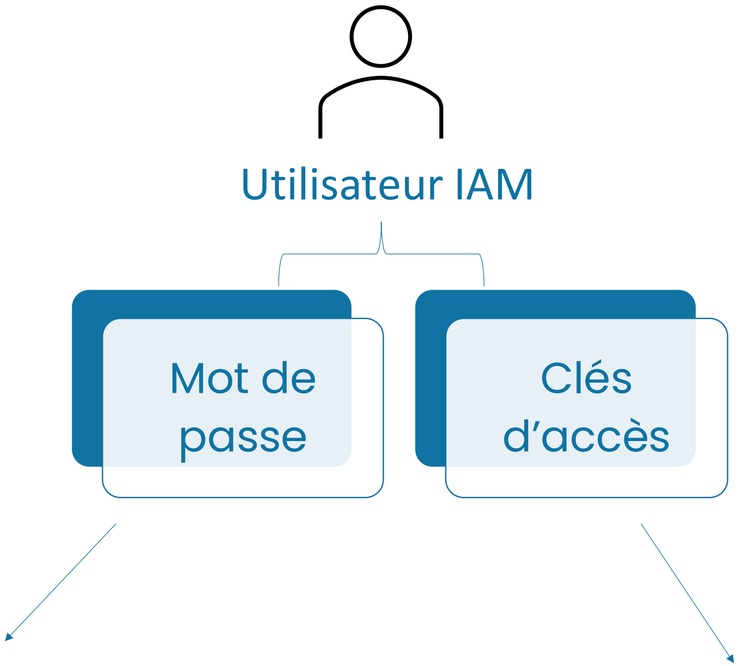
Représente une **entité** qui accède à votre compte AWS

Utilisateur humain *ou* ***Programme***

Possède un **nom** et des informations d'identification (*credentials*)

Par défaut, il ne possède **aucune autorisation (*permission*)** à sa création

Utilisateur IAM : Informations d'identification (*Credentials*)



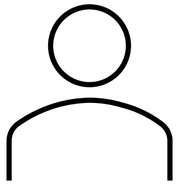
- S'utilise via la **Console AWS**
- Politique de mot de passe robuste
- MFA fortement recommandé

- S'utilise via **AWS CLI, AWS SDK ou API**
- En anglais : ***Access Key***
  - *Composé de* : ***{Access Key Id / Secret Access Key}***
- Bonne pratique : rotation régulière ou préférer les rôles IAM

Utilisateur IAM : Multi-Factor Authentication (MFA)

Facteur supplémentaire d'authentification en plus du mot de passe

[Bonne pratique] A activer pour le ***Root use***r et tous les ***utilisateurs IAM***



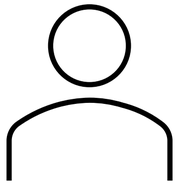


Google Authenticator

AUTHY



Utilisateur IAM : Autorisations (*Permissions*)

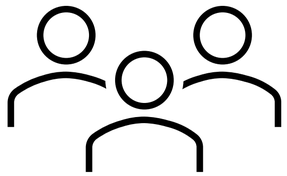


Par défaut, un utilisateur a **zéro autorisation** à la création

Assigner une **Politique IAM** pour accorder une autorisation (*permission*)

[**Grant Least Privilege**] Accordez des **autorisations uniquement** pour les tâches qu'il doit accomplir

Groupes IAM



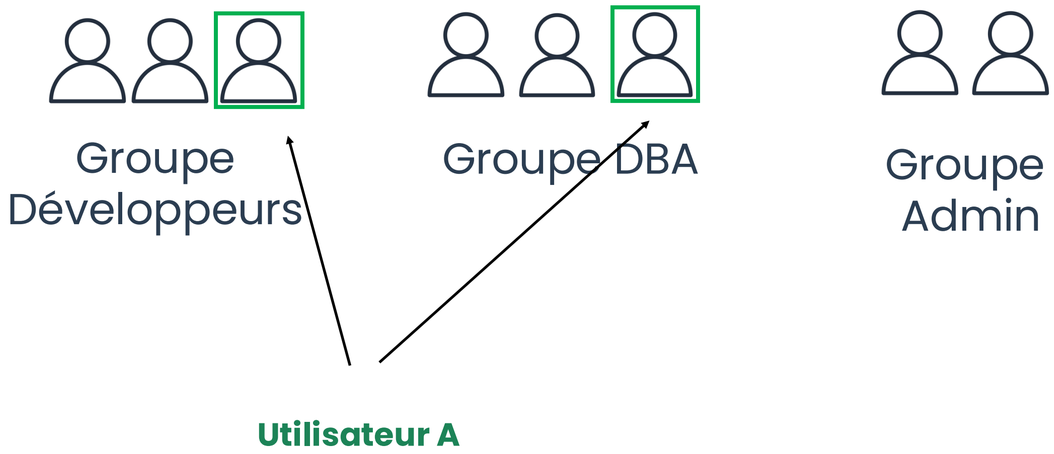
Permet de **regrouper** des utilisateurs qui ont des fonctions similaires.

Exemple : Admin, Développeurs, DBA, Finance

Permet de **simplifier** l'administration des autorisations d'un ensemble d'utilisateurs

Les utilisateurs héritent des **autorisations attachées au groupe**

Groupes IAM

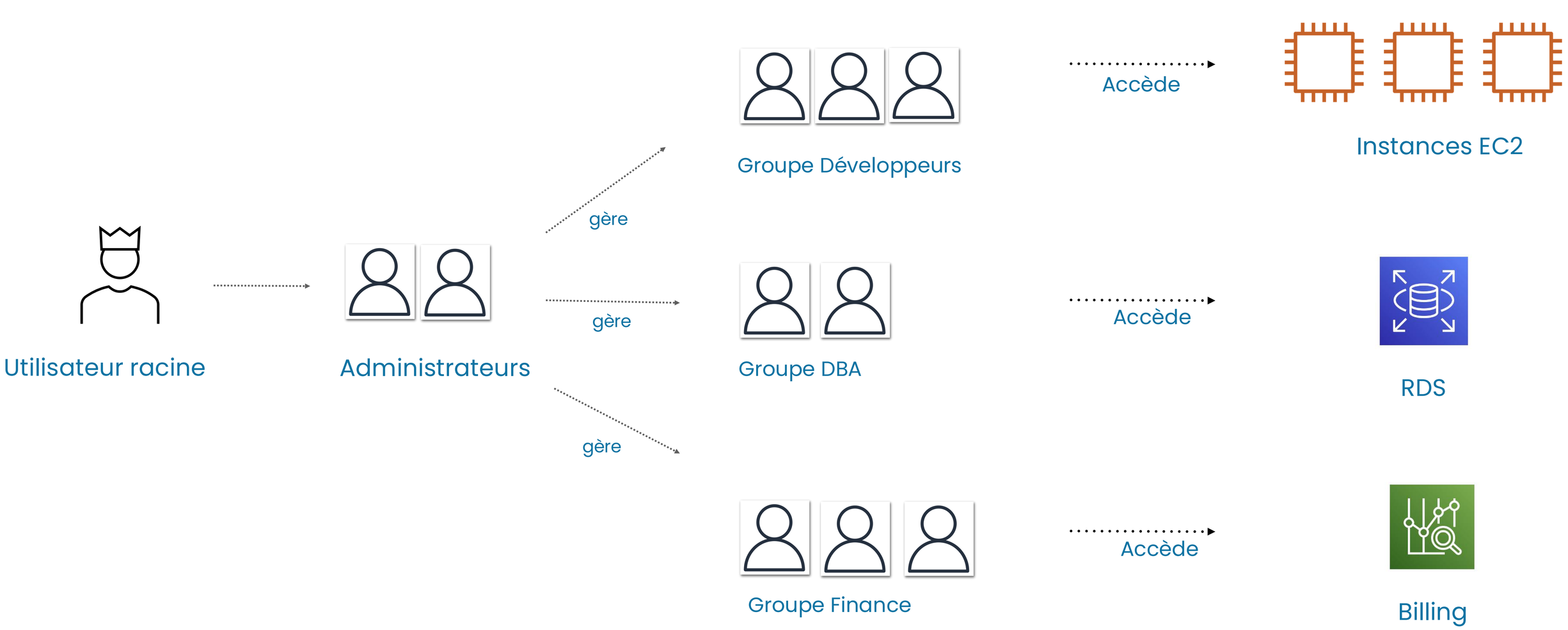


Un **groupe** peut contenir plusieurs utilisateurs

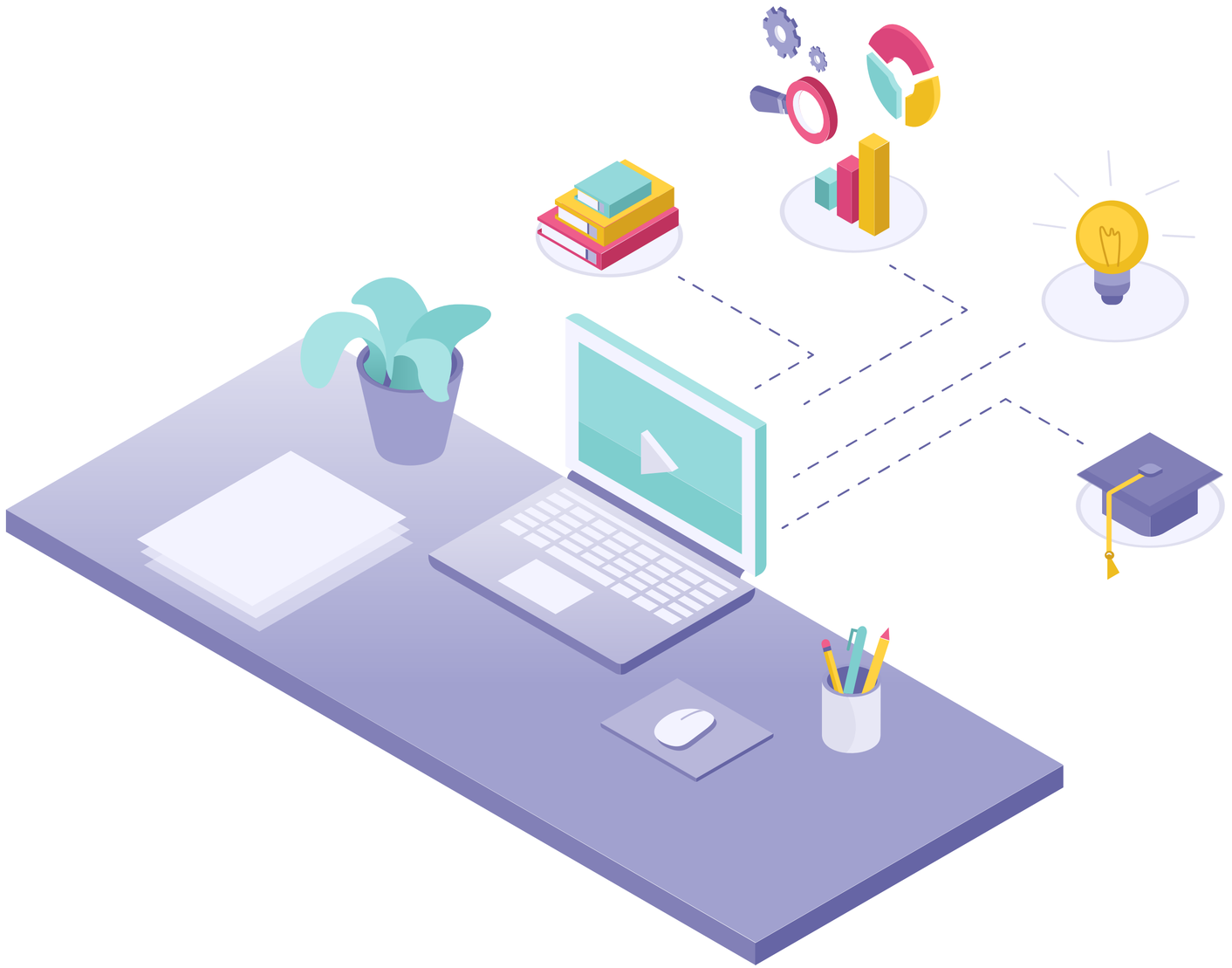
Un **groupe** ne peut pas contenir un autre groupe

Un **utilisateur** peut appartenir à plusieurs groupes -> Il hérite de toutes les permissions

Gestion des utilisateurs et groupes



Politiques IAM



Politiques IAM



En anglais : « ***Policies*** »

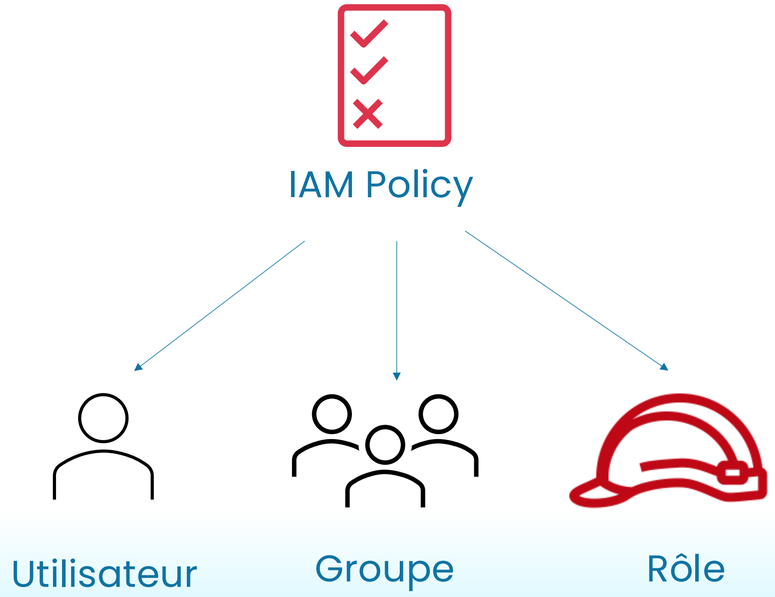
Permettent de gérer les **autorisations (*permissions*)**

Documents **JSON** attachés à des **entités** : utilisateurs, groupes, rôles,...

Effet possible : ***Allow*** ou ***Deny***

AWS Managed

Customer Managed



Exemple de politique IAM

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": "ec2:*",
         "Resource": "*",
         "Effect": "Allow",
         "Condition": {
            "StringEquals": {
               "ec2:Region": "us-east-2"
            }
         }
      }
   ]
}
```

Version

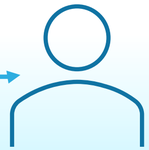
Actions autorisées ou refusées

Ressources concernées

Autorisation (ALLOW) ou Refus (DENY)

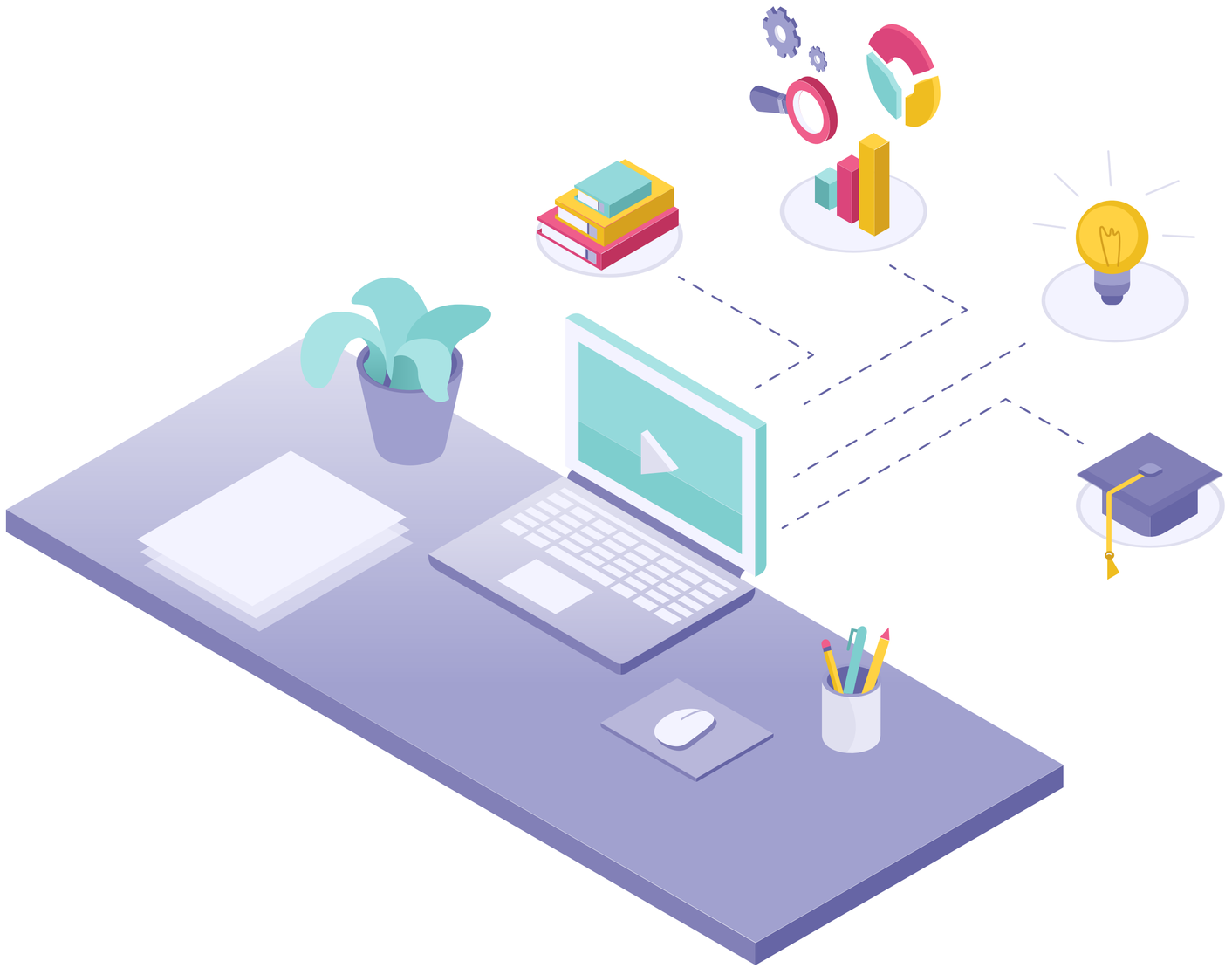
(Facultatif) Conditions

assigné



« Cet utilisateur a toutes les **autorisations** sur les instances EC2 dans la région us-east-2 (Ohio) »

Rôle IAM



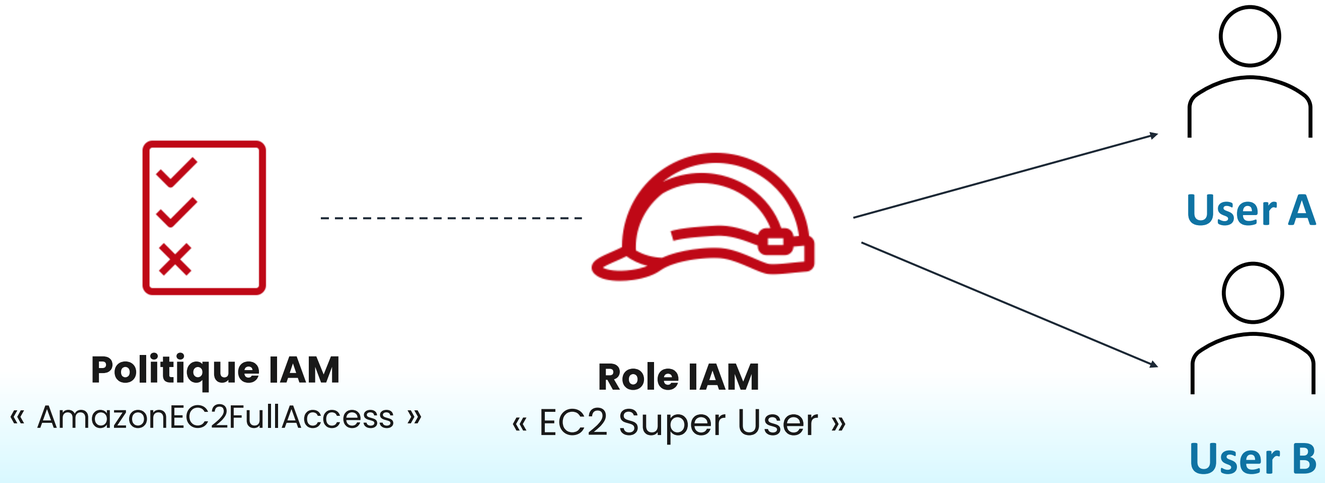
Rôle IAM

Permet un **accès temporaire** à des services ou ressources AWS

Vient avec des **autorisations spécifiques**

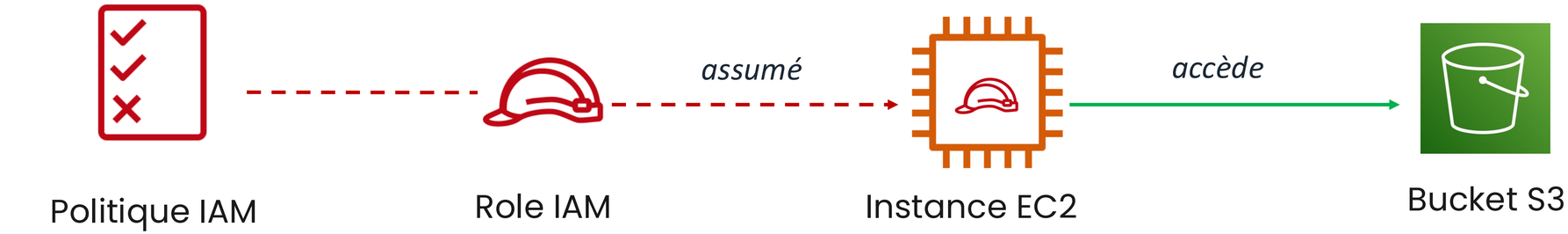
Fournit des informations de sécurité **temporaires**

Peut-être **endossé** par tout utilisateur ou service qui en a besoin

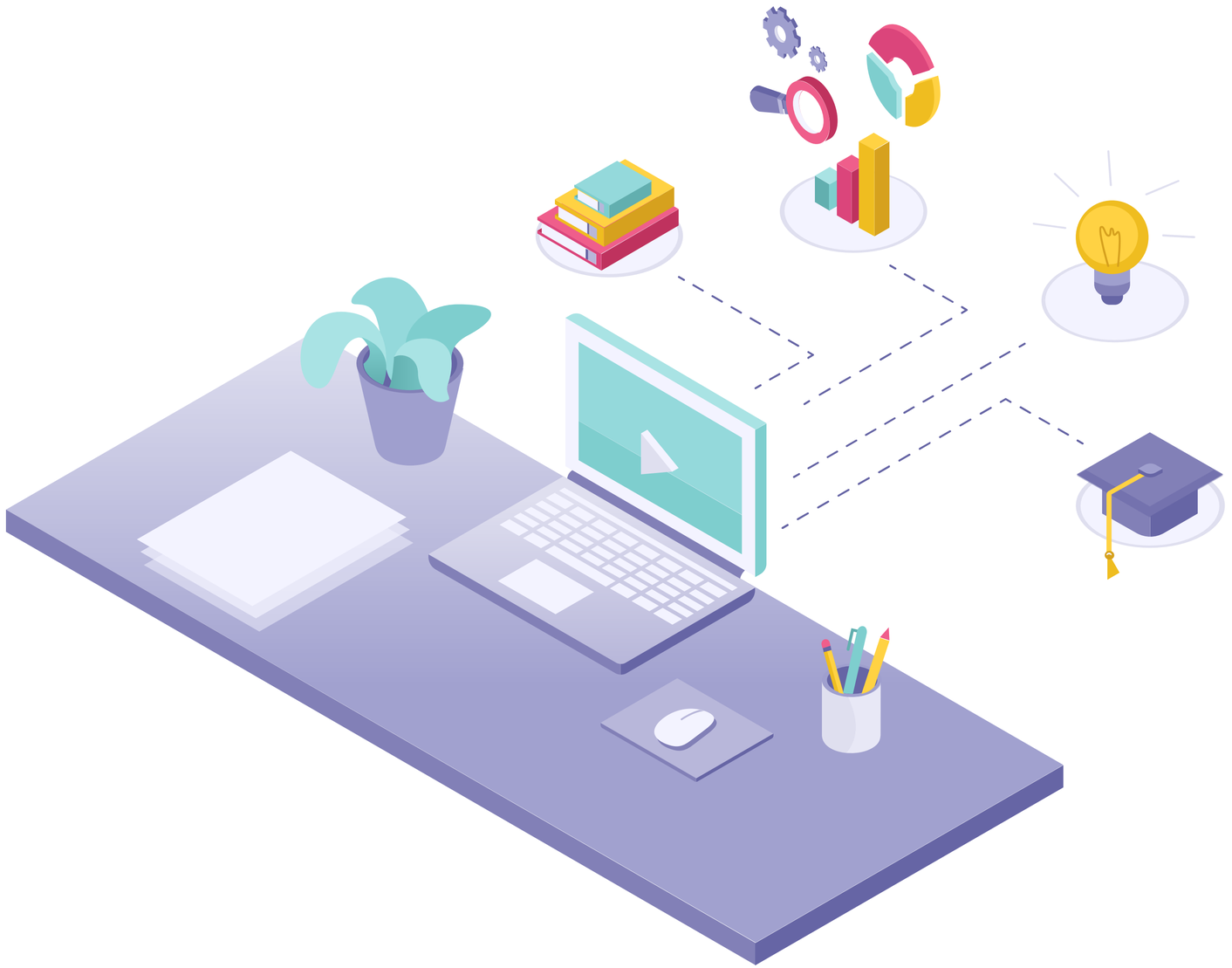


Rôle IAM : Exemple avec un service AWS

Scénario : « Assigner un **rôle** à une **instance EC2** pour qu'elle ait **tous les privilèges** d'accès à vos **buckets S3**»

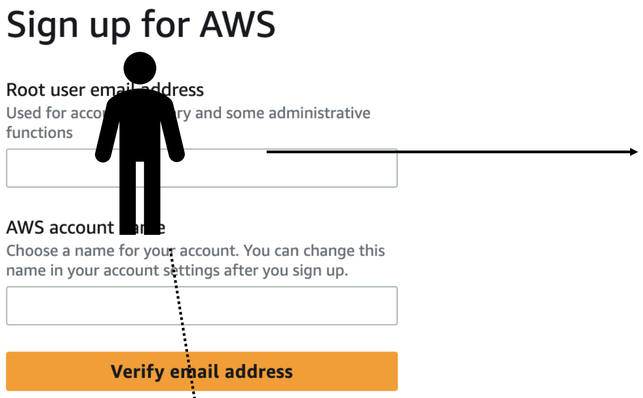


Résumé & Bonnes pratiques

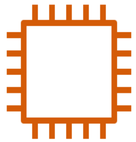


En résumé

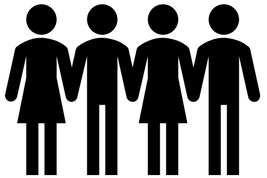




Crée







Utilisateur racine

- Utilisateur super puissant qui a créé le compte AWS
- Accès complet à tous les services

Utilisateur IAM

- Représente un utilisateur humain ou une application
- Accède aux ressources du compte AWS

Groupe IAM

- Ensemble d'utilisateurs IAM qui ont des fonctions similaires
- Simplifie la gestion des permissions

IAM Credentials

- Informations d'identification de sécurité
- Mot de passe ou Clés d'accès (Access Key)
- MFA

Politiques IAM

- Documents JSON utilisés pour définir les autorisations
- Assignées à des utilisateurs, groupes ou des rôles

Role IAM

- Peut-être endossé par un utilisateur ou un service AWS (Exp: Instance EC2)
- Fournit des informations d'identification temporaire

Bonnes pratiques



N'utilisez pas ***l'utilisateur Root*** au quotidien

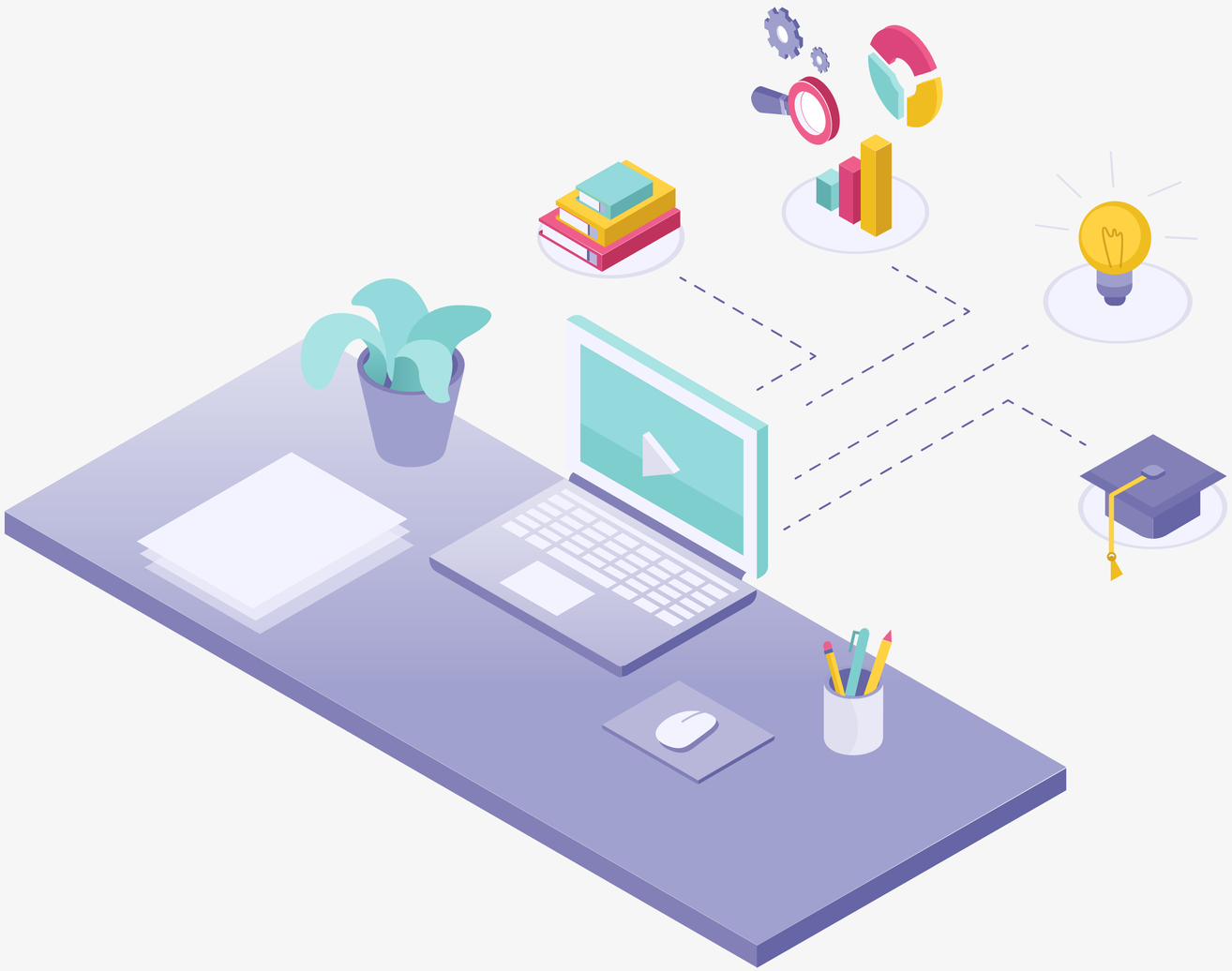
Appliquez le **principe** du « ***Grant least privilege*** »

Encourager **l'utilisation** du ***MFA***

Faites la **rotation régulière** des ***Access Key et mots de passe***

Définissez une **politique robuste** pour les ***mots de passe***

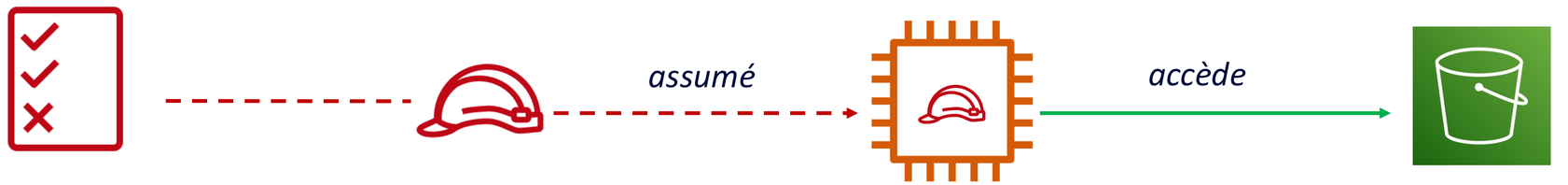
Interdisez le ***partage d'identifiants*** entre utilisateurs



FIN DU MODULE

Lab : Comprendre les *rôles* IAM

Scénario : « Autoriser l'**instance EC2** à accéder en lecture seule aux objets dans votre **bucket S3**»



Politique IAM

AmazonS3ReadOnlyAccess

Role IAM

Instance EC2

Site web

Bucket S3

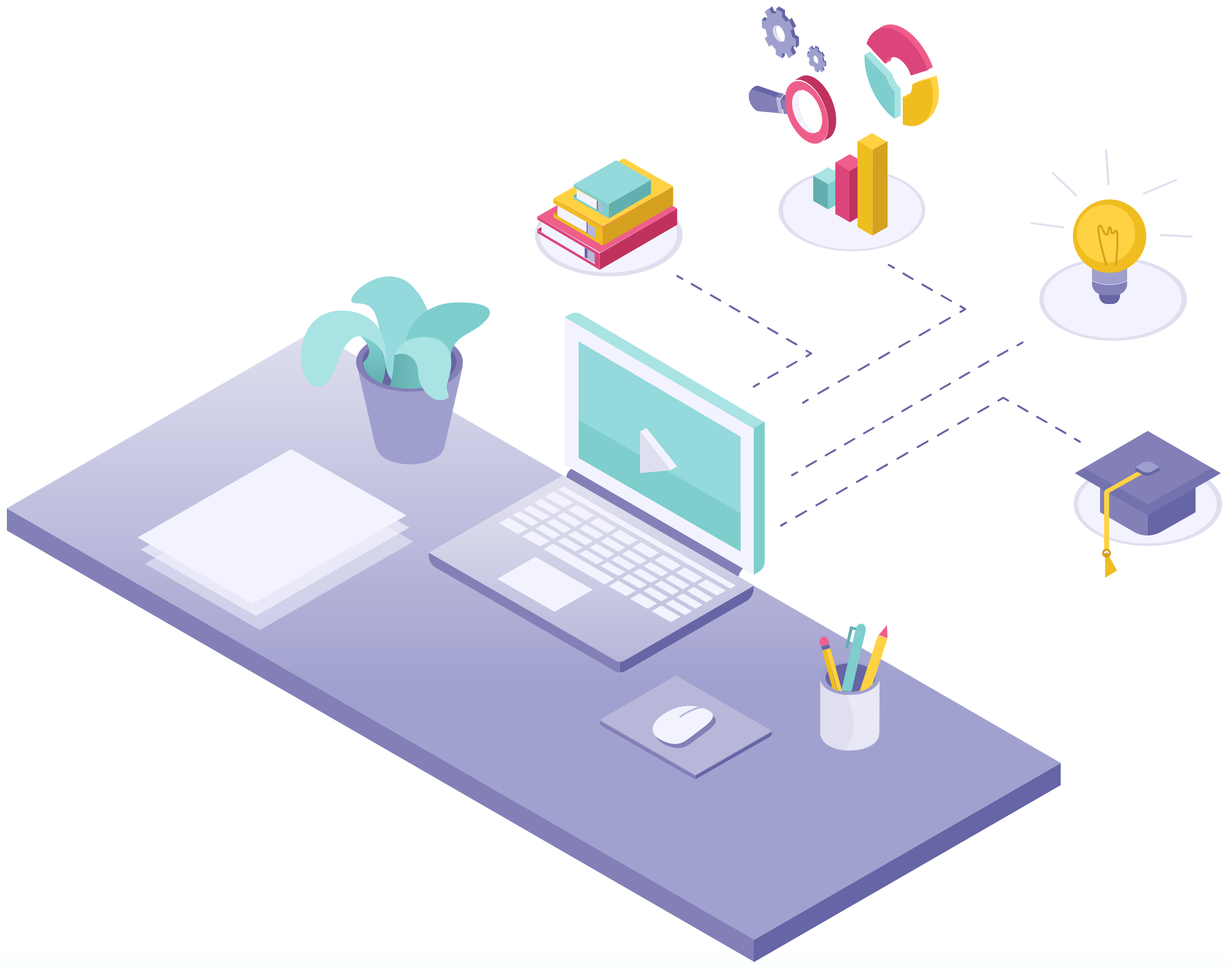
Photos

Lab : Comprendre les *rôles* IAM

1. Explorer l’architecture (Instance EC2, Bucket S3)
2. Créer un Rôle IAM et l’attacher à l’EC2
3. Tester les accès au bucket S3

Module 12 : Autres services de sécurité

Gérer de façon sécurisée les identités et l'accès aux services et ressources AWS



Todo



Services AWS dédiés à la sécurité, à l'identité et à la conformité

Gestion des identités et des accès


AWS IAM


AWS Organizations


AWS IAM Identity Center (SSO)


Amazon Cognito


AWS Directory Service

Détection et réponse


AWS Config


Amazon Inspector


Amazon GuardDuty


AWS Security Hub


Amazon Detective

Protection du réseau et des applications


AWS WAF


AWS Shield


AWS Firewall Manager


AWS Network Firewall

Protection des données


AWS KMS


AWS CloudHSM


AWS Secrets Manager


AWS Certificate Manager

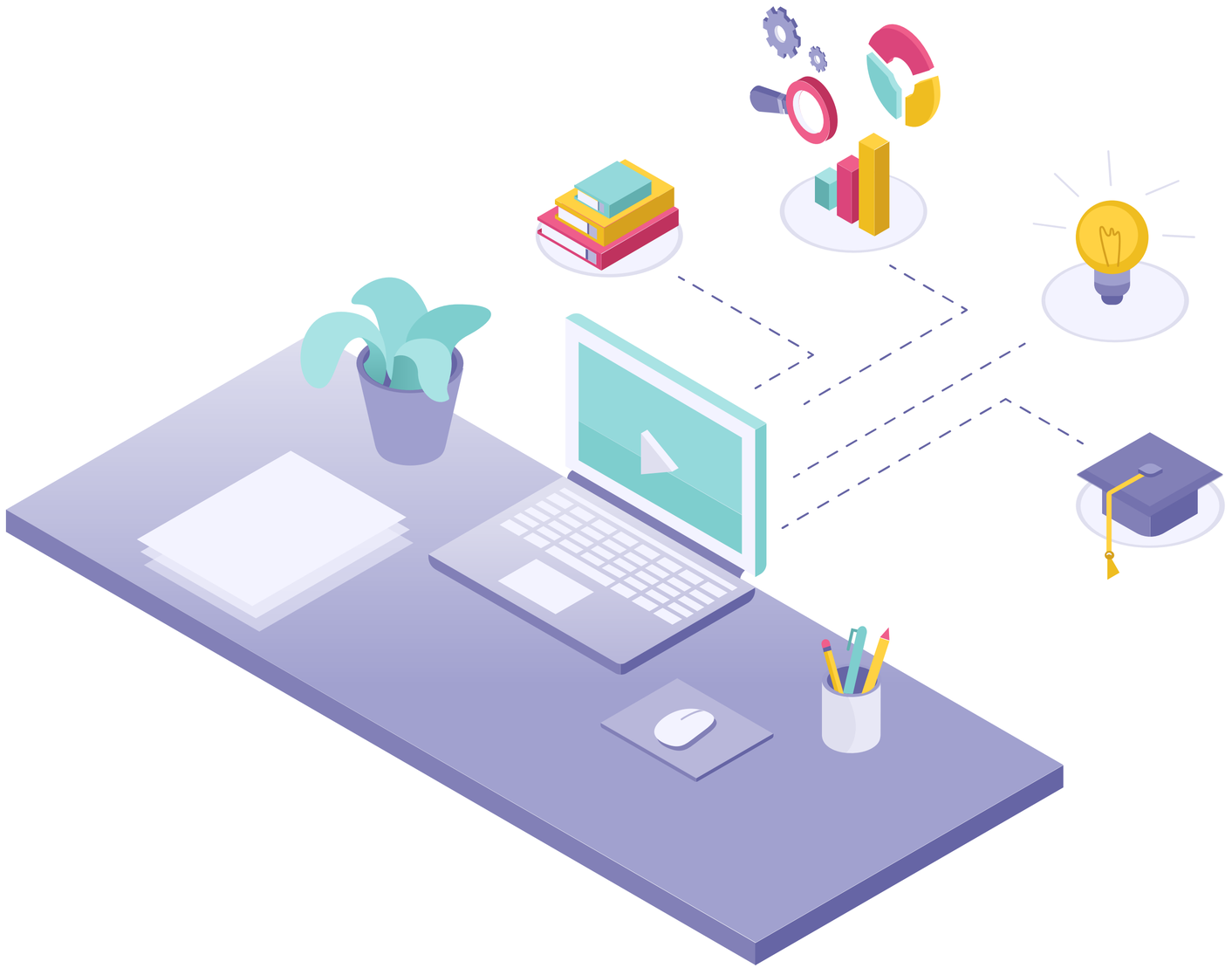

Amazon Macie

Conformité


AWS Artifact


AWS License Manager

AWS Organizations

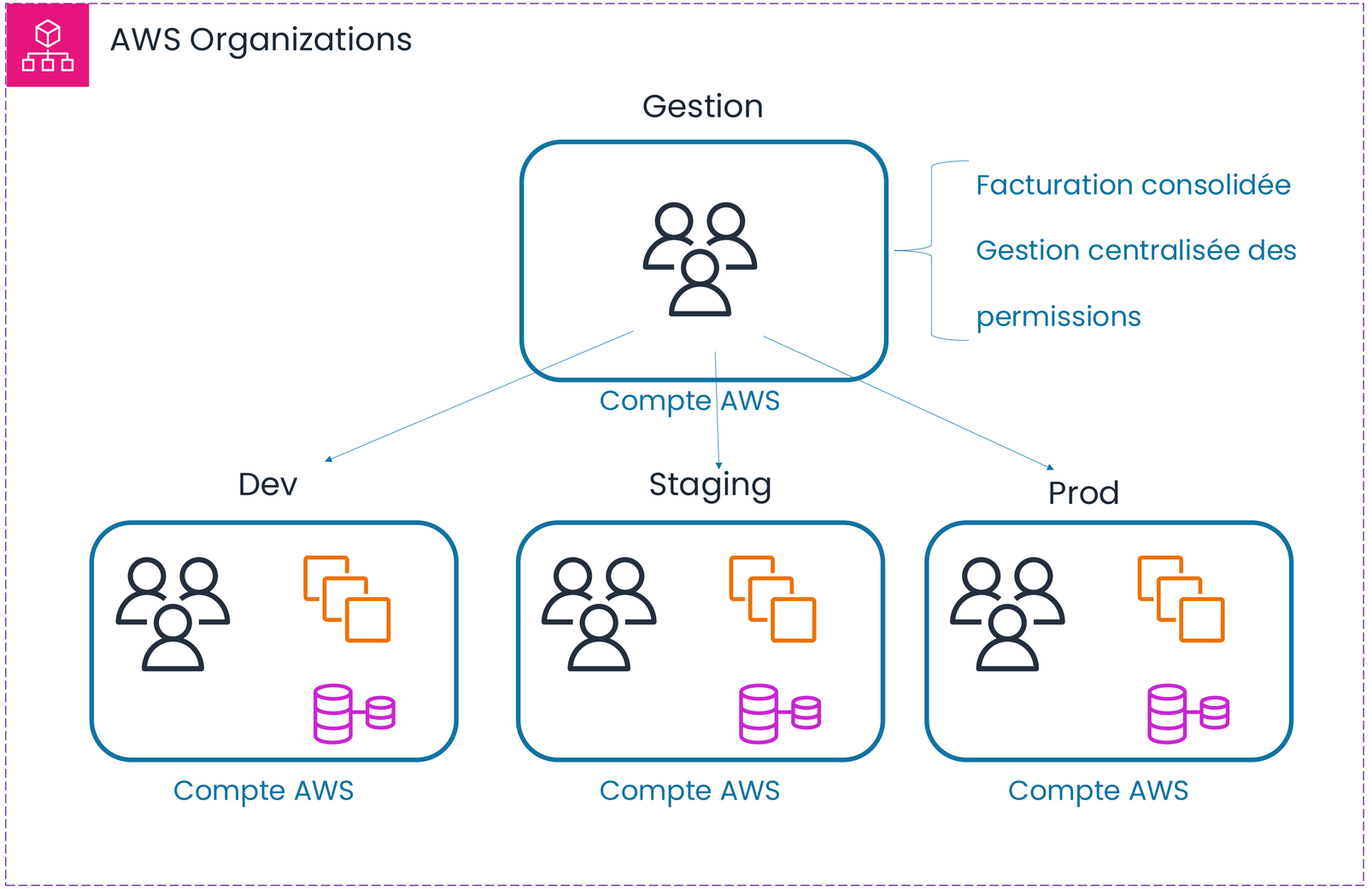


Gestion des comptes AWS

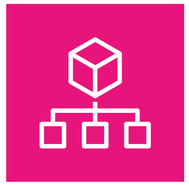
Vous souhaitez

- Déployer des ressources AWS
- Isoler les environnements
- Centraliser les identités des utilisateurs
- Avoir une facturation consolidée & une stratégie centralisée des permissions

Utilisez AWS Organizations



AWS Organizations

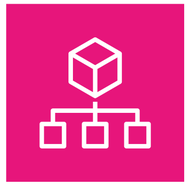


Permet de gérer de façon centralisée **plusieurs comptes AWS**

Quelques Avantages :

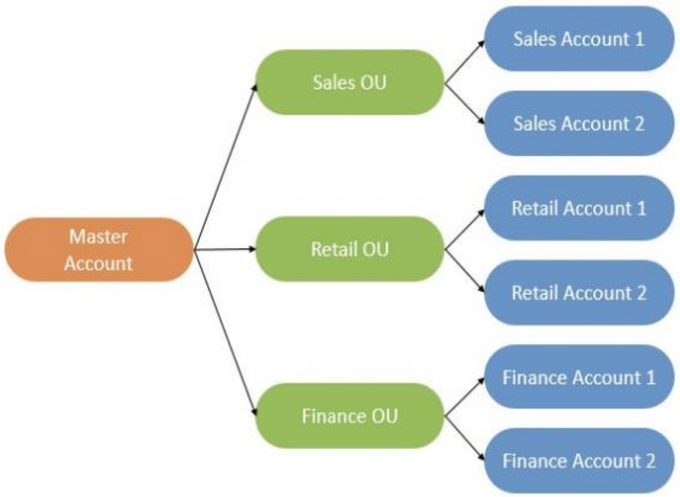
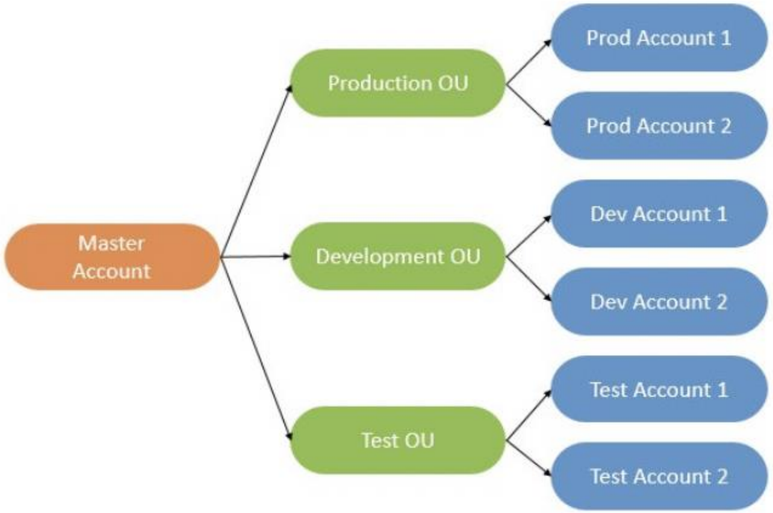
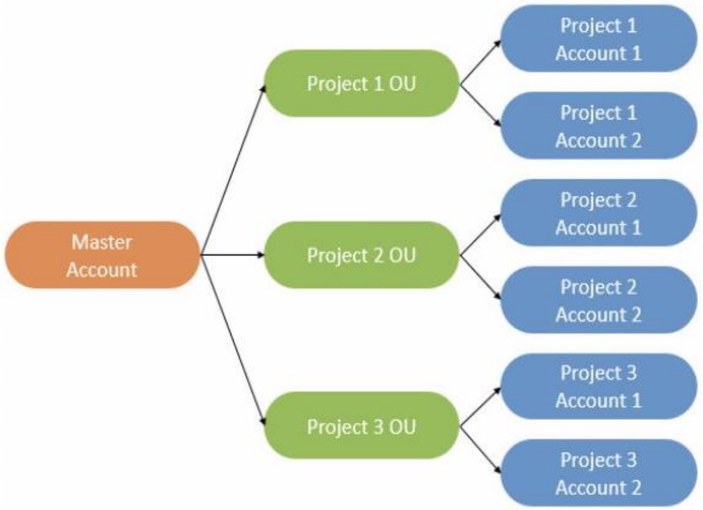
- **Séparation des environnements** en utilisant des comptes AWS distincts
- **Facturation consolidée** de l'ensemble des comptes AWS
- Stratégies de contrôle d'accès avec les ***SCP*** (Service Control Policies)
- Augmentation des **limites de services**

Terminologie et concepts

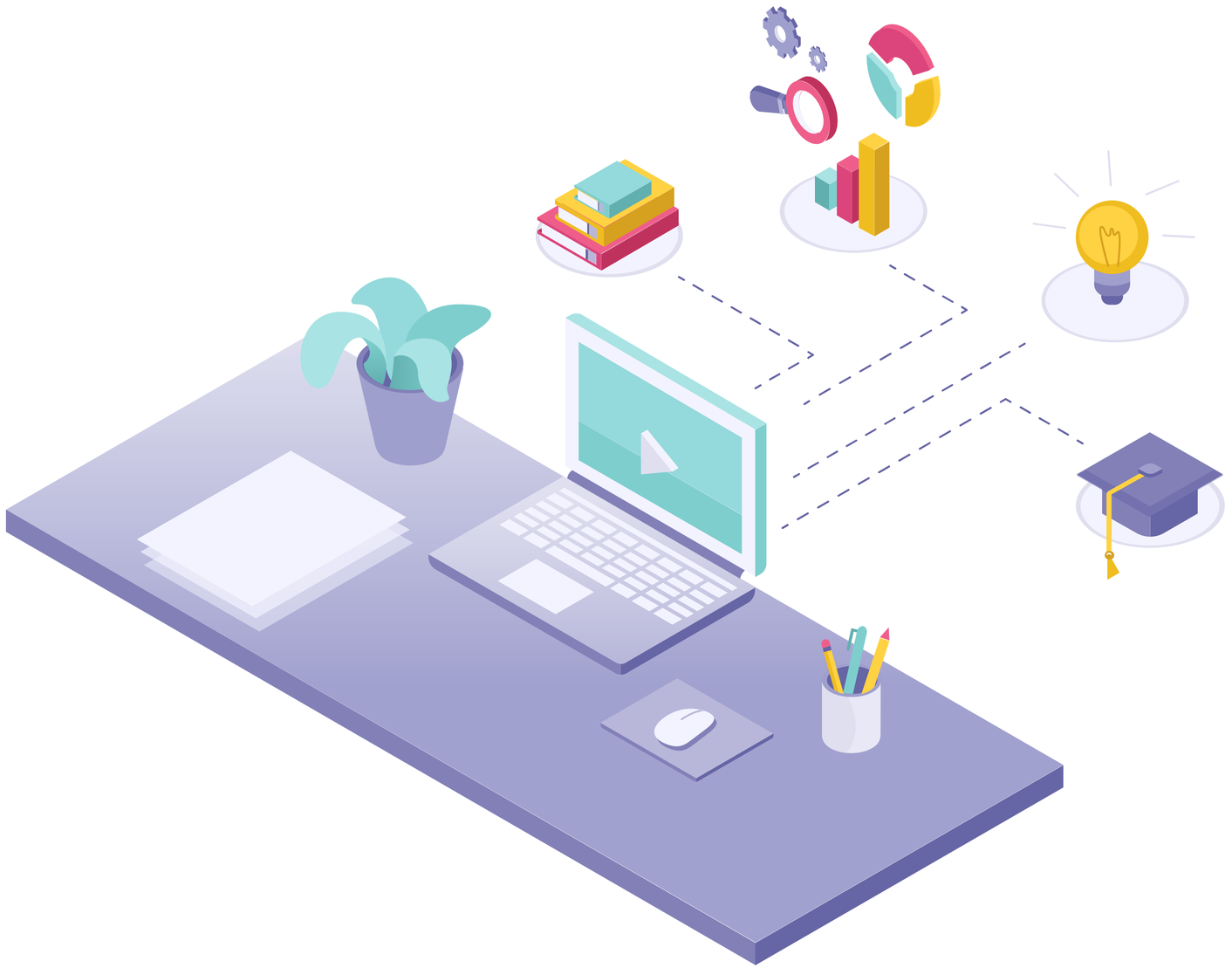


- **Organization**
  - Collection de plusieurs comptes AWS
- **Unité Organisationnelle** (OU)
  - En anglais : *Organizational Unit*
  - Permet de regrouper un ensemble de comptes au sein d'une organisation
- **Compte gestionnaire**
  - En anglais : *Management Account* (anciennement *Master Account*)
  - Compte AWS qui a créé l'organisation
- **Politique de contrôle de services (SCP)**
  - En anglais : *Service Control Policies*
  - Politiques permettant de contrôler les limites de permissions des comptes AWS

Exemples de stratégie multi comptes AWS

BU Account Structure	*Environmental Lifecycle Account Structure*	*Project-Based Account Structure*
		

Amazon Cognito

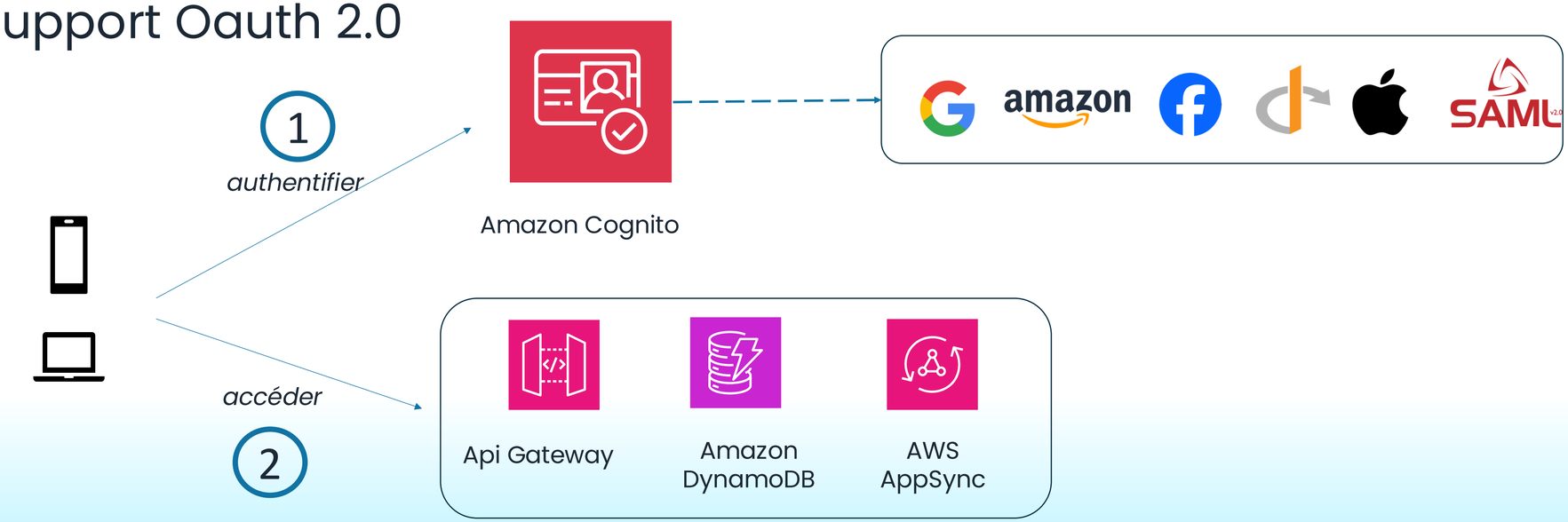


Amazon Cognito

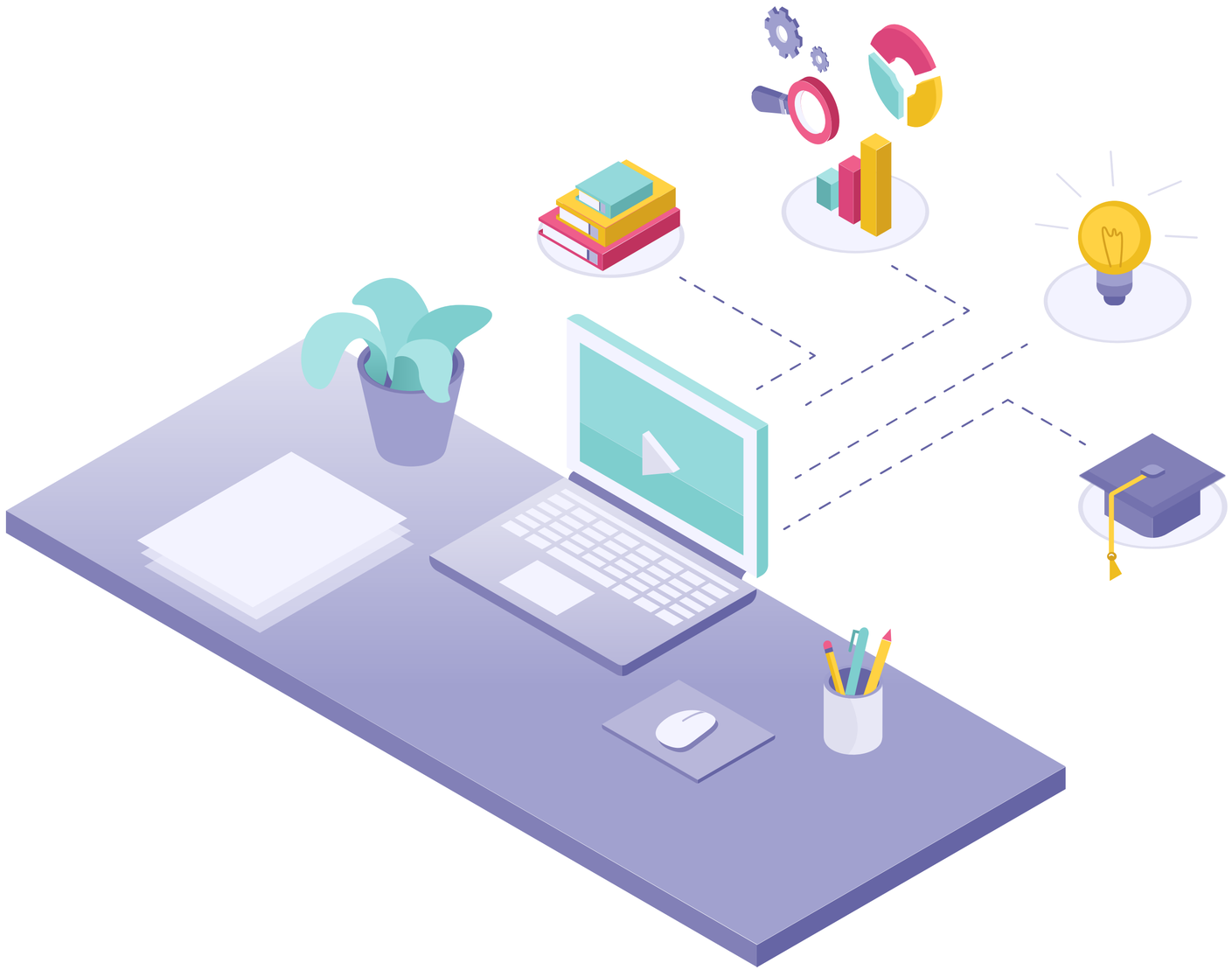
Permet de gestion des identités pour vos **applications web et mobiles**

Les fonctionnalités clés

- Gestion des inscriptions, utilisateurs et groupes d'utilisateurs
- Login avec Facebook, Google, Amazon, Apple, SAML, OpenID
- Support Oauth 2.0



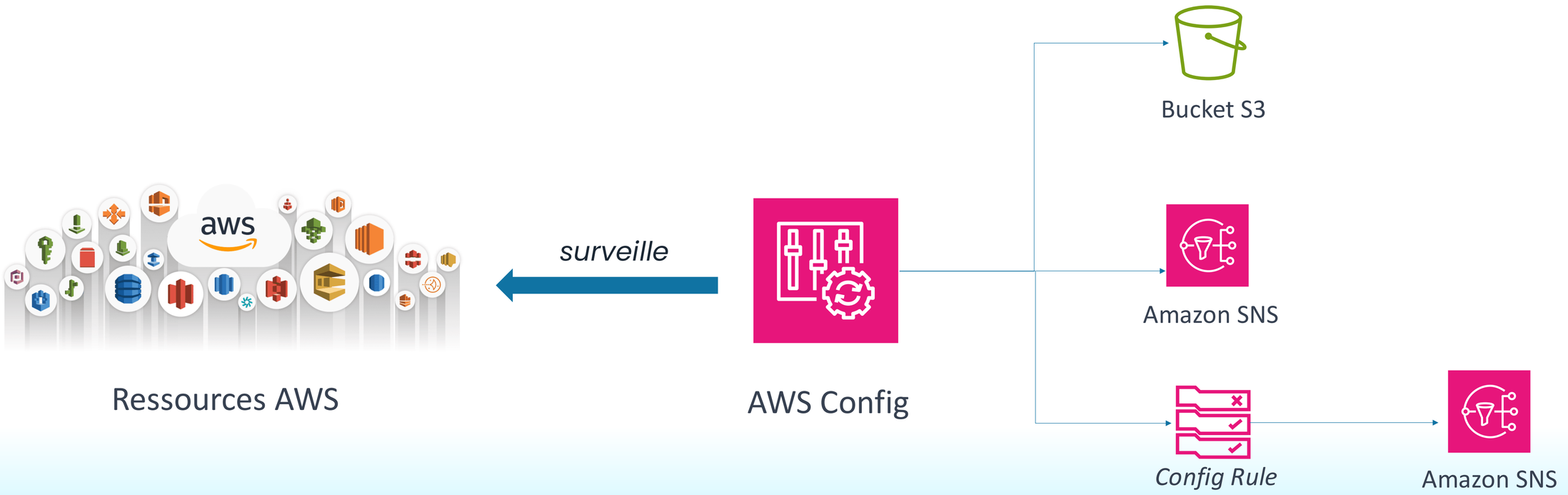
AWS Config



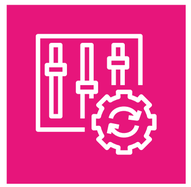
AWS Config

Permet de surveiller la **configuration de vos ressources AWS** au fil du temps

Fournit des informations détaillées sur **l'historique des changements de configuration** de vos ressources AWS



AWS Config Rules



Règles qui évaluent si vos **ressources sont conformes**

- Exemples:
  - *db-instance-backup-enabled*
  - *desired-instance-type*
  - *ec2-volume-inuse-check*

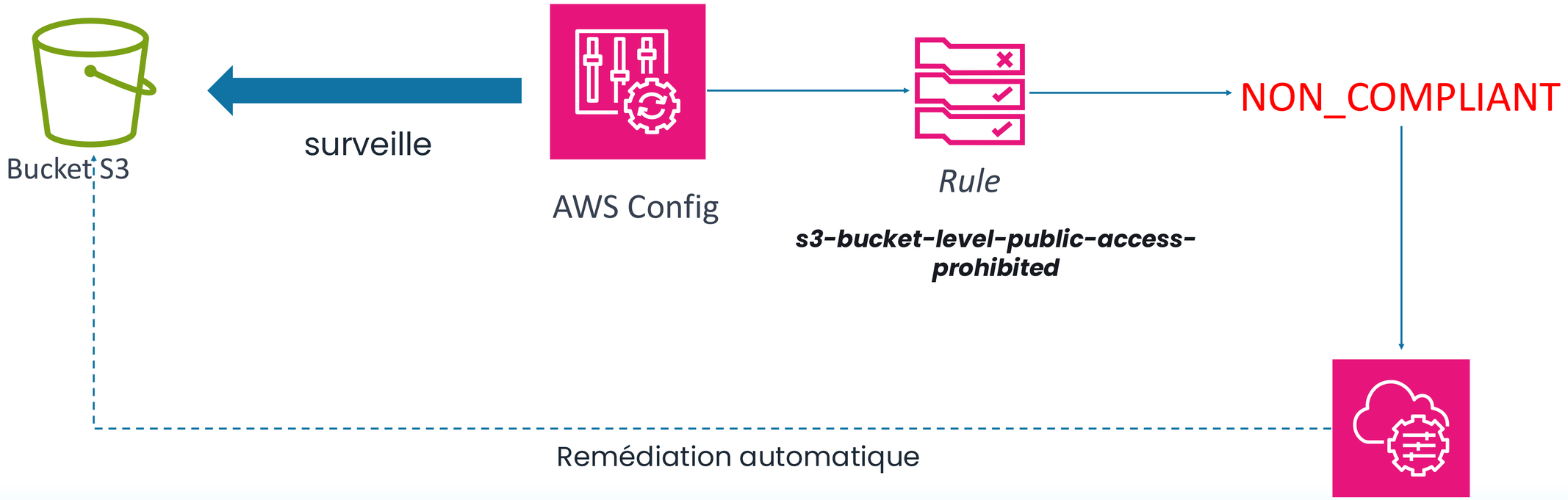
Remédiation automatique si une ressource n'est pas conforme à une règle.

LeCloudFacile.com

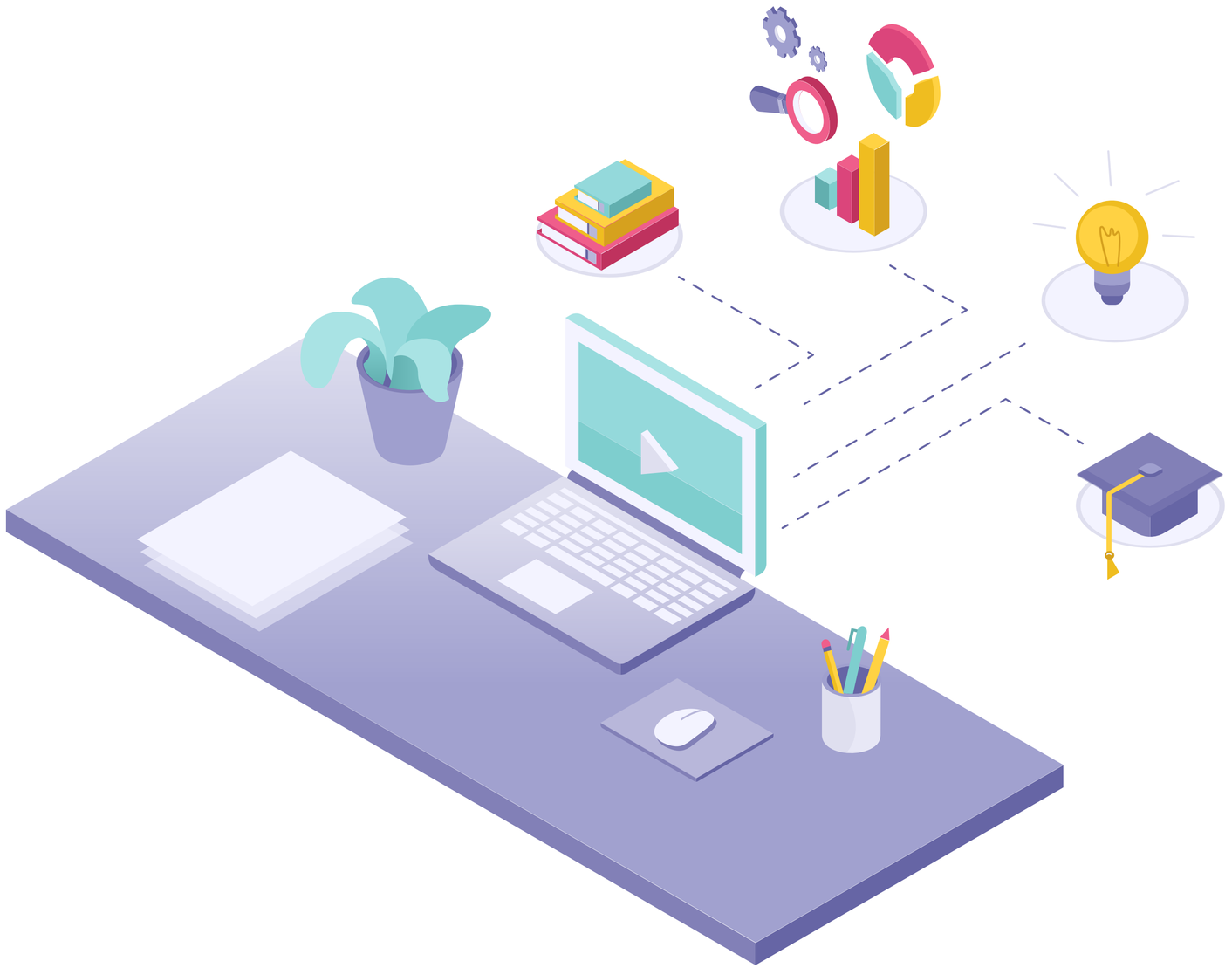
AWS Config Rules : Exemple de mise en oeuvre

Cas d'usage :

Vérifier si un bucket S3 est accessible publiquement et faire de la remédiation automatique



Amazon Inspector



Amazon Inspector



Analyse vos **ressources** pour **détecter les vulnérabilités logicielles (CVE)** et les expositions réseau involontaires

Ressources supportées : instances EC2, images ECR, Fonctions AWS Lambda

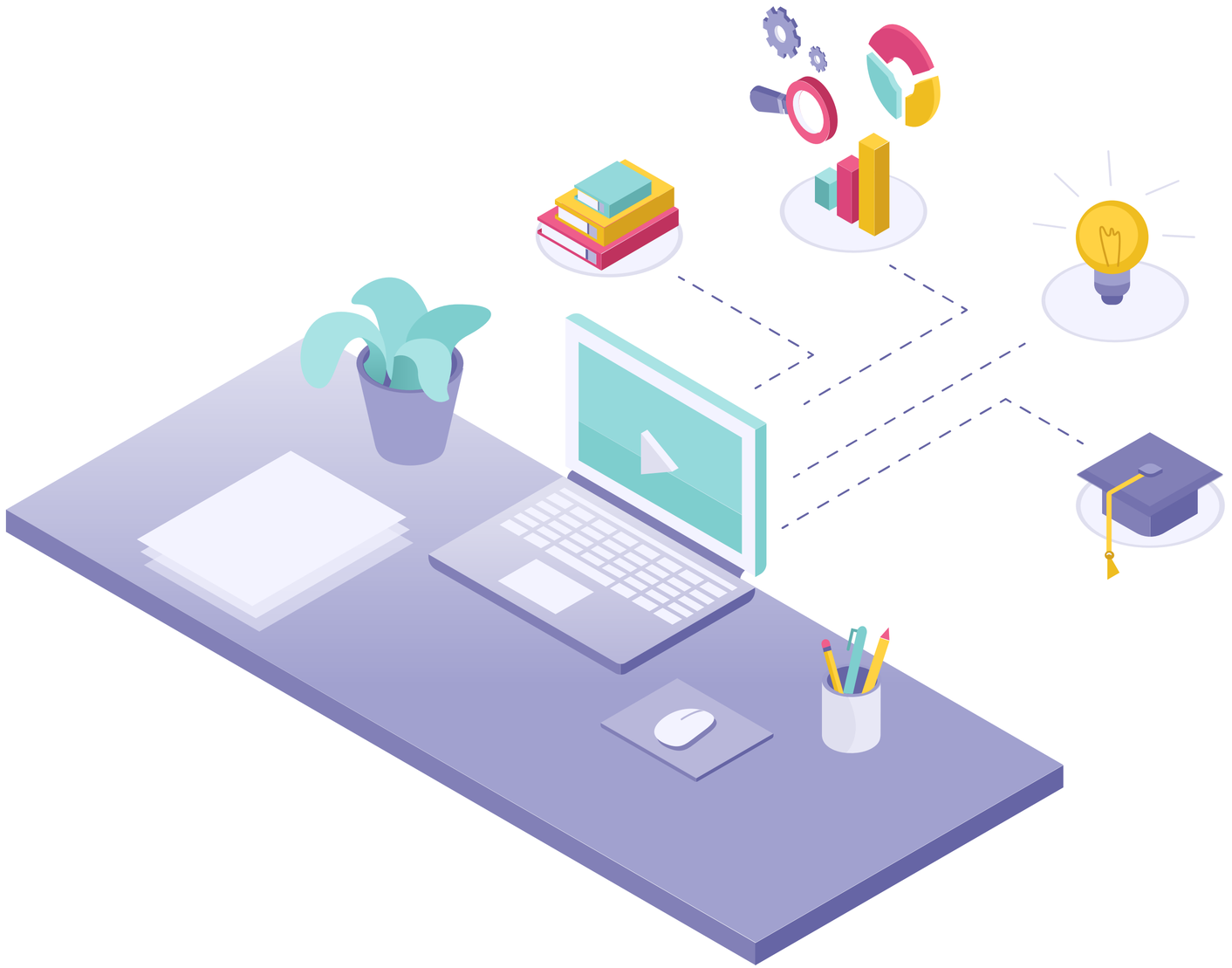
Fonctionnalités clés

1. **Scans Automatisés**
2. **Rapports de Vulnérabilité**
3. **Intégration avec Security Hub**

Amazon Inspector



Amazon GuardDuty



Amazon GuardDuty



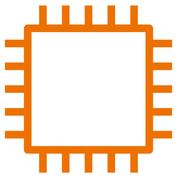
Surveille en continu les **activités malveillantes** et les **comportements suspects** au sein de votre compte AWS

Sources de données : AWS CloudTrail, VPC flow log & journaux DNS, …

Peut détecter

- Port scanning
- Instances EC2 ou Compte AWS compromis
- Logiciels malveillants (malware) dans les EC2 ou conteneurs
- Appels APIs avec des comportements ou emplacements inhabituels

Amazon GuardDuty



Amazon EC2



AWS Lambda



Amazon EKS



Amazon Aurora



Amazon S3

inspecte

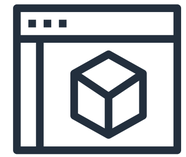


Amazon GuardDuty



Résultats (Findings)

- Comportement anormal
- Exfiltration d'informations
- Exposition réseau
- *Malware*
- ….



Console GuardDuty

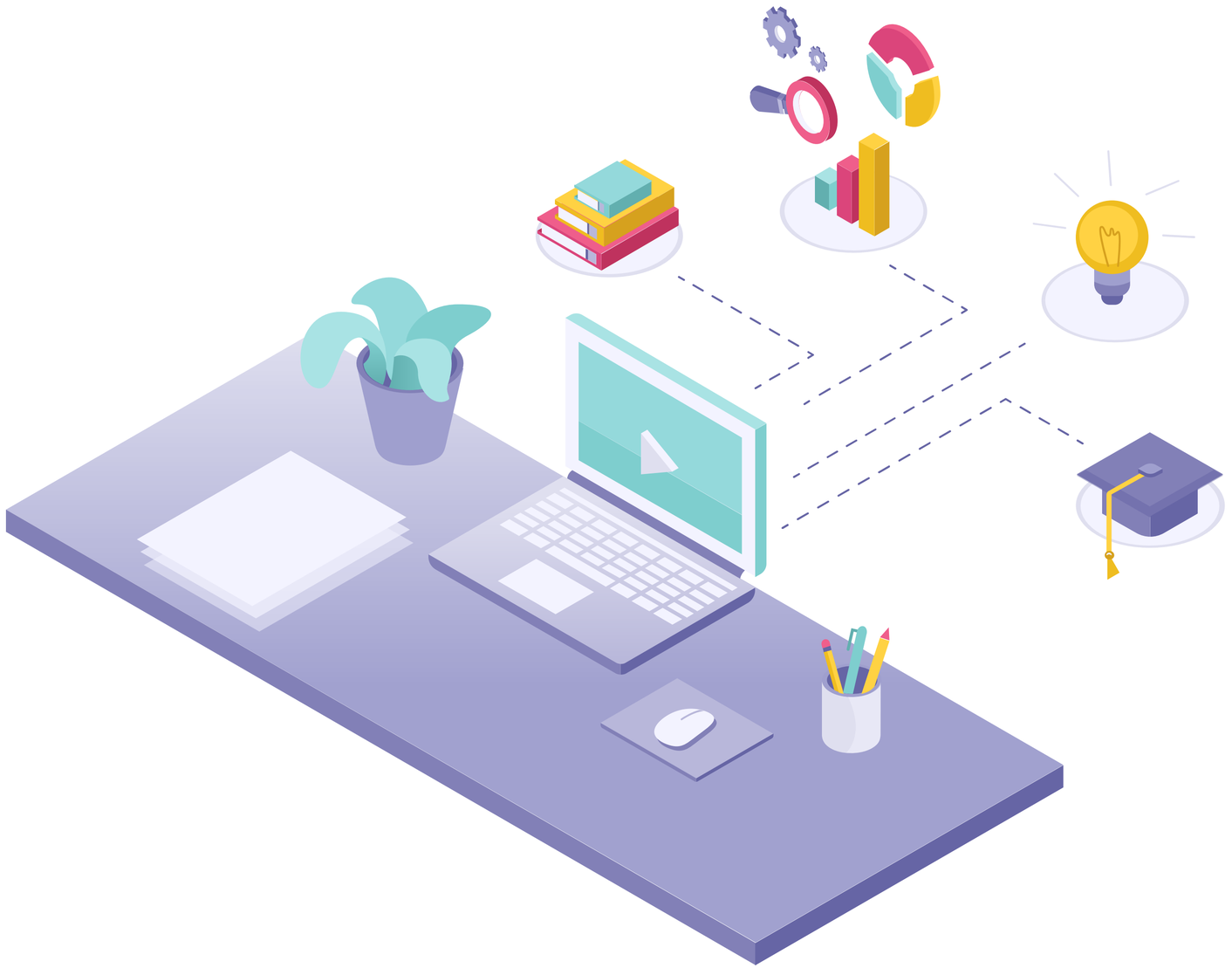


Amazon EventBridge



AWS Security Hub

AWS Security Hub



AWS Security Hub



Permet d'avoir une **vue centralisée et agrégée de la sécurité** de vos comptes AWS

Regroupe les alertes provenant des services AWS tels que GuardDuty, Amazon Inspector, Amazon Macie ainsi que des logiciels tiers

Effectue également des vérifications par rapport à des **normes de sécurité** :

AWS Foundational Security Best Practices, Center for Internet Security (CIS), PCI DSS, NIST…

AWS Security Hub

AWS Services de sécurité

AWS Config

Amazon Macie

Amazon Inspector

Amazon GuardDuty

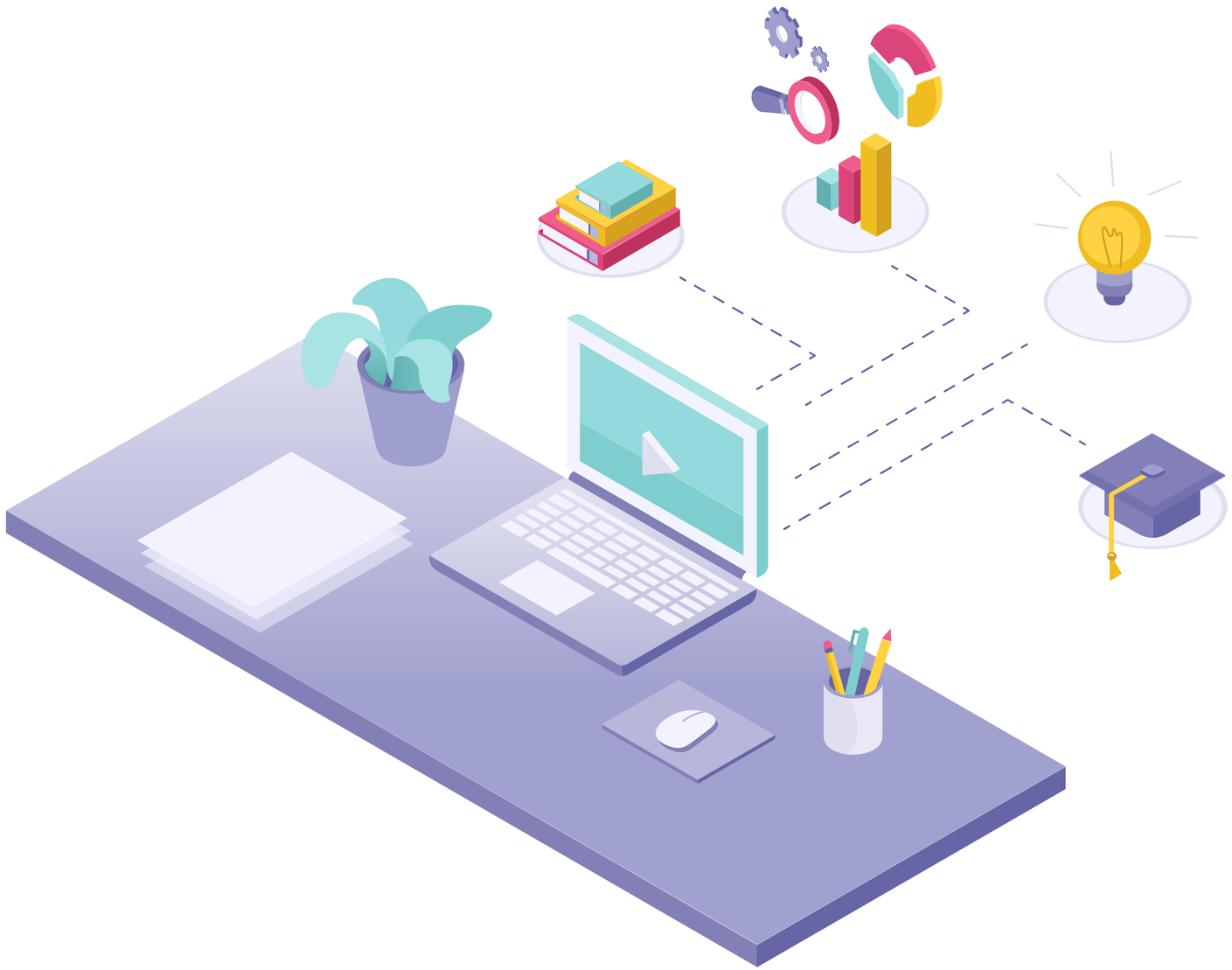
Produits tiers (SIEM, Firewalls,..)

Les autres services AWS



AWS Security Hub

AWS WAF



AWS WAF (Web Application Firewall)



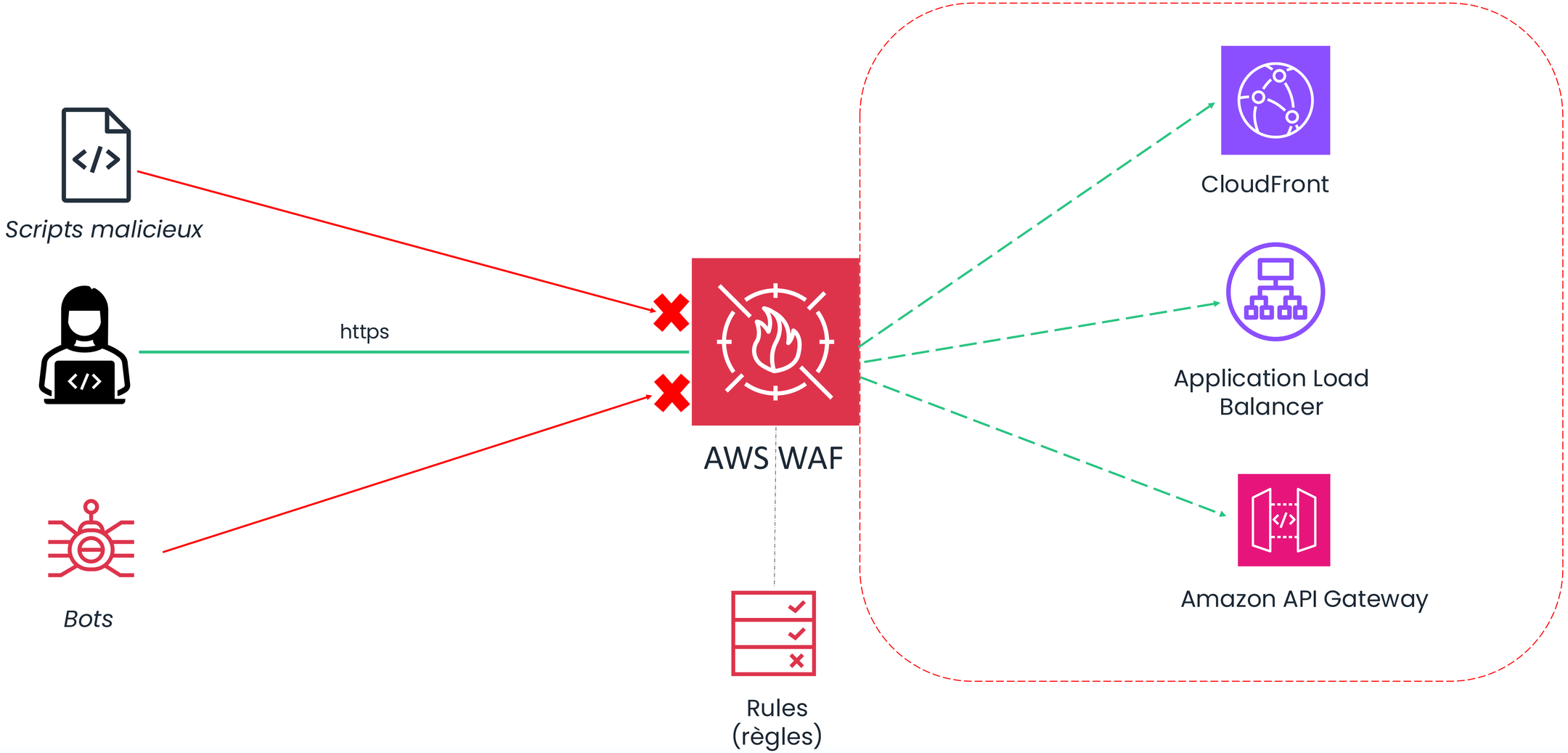
Protège vos applications web contre les attaques malveillantes et bots

Inspecte le trafic **HTTP/HTTPS** (Couche 7)

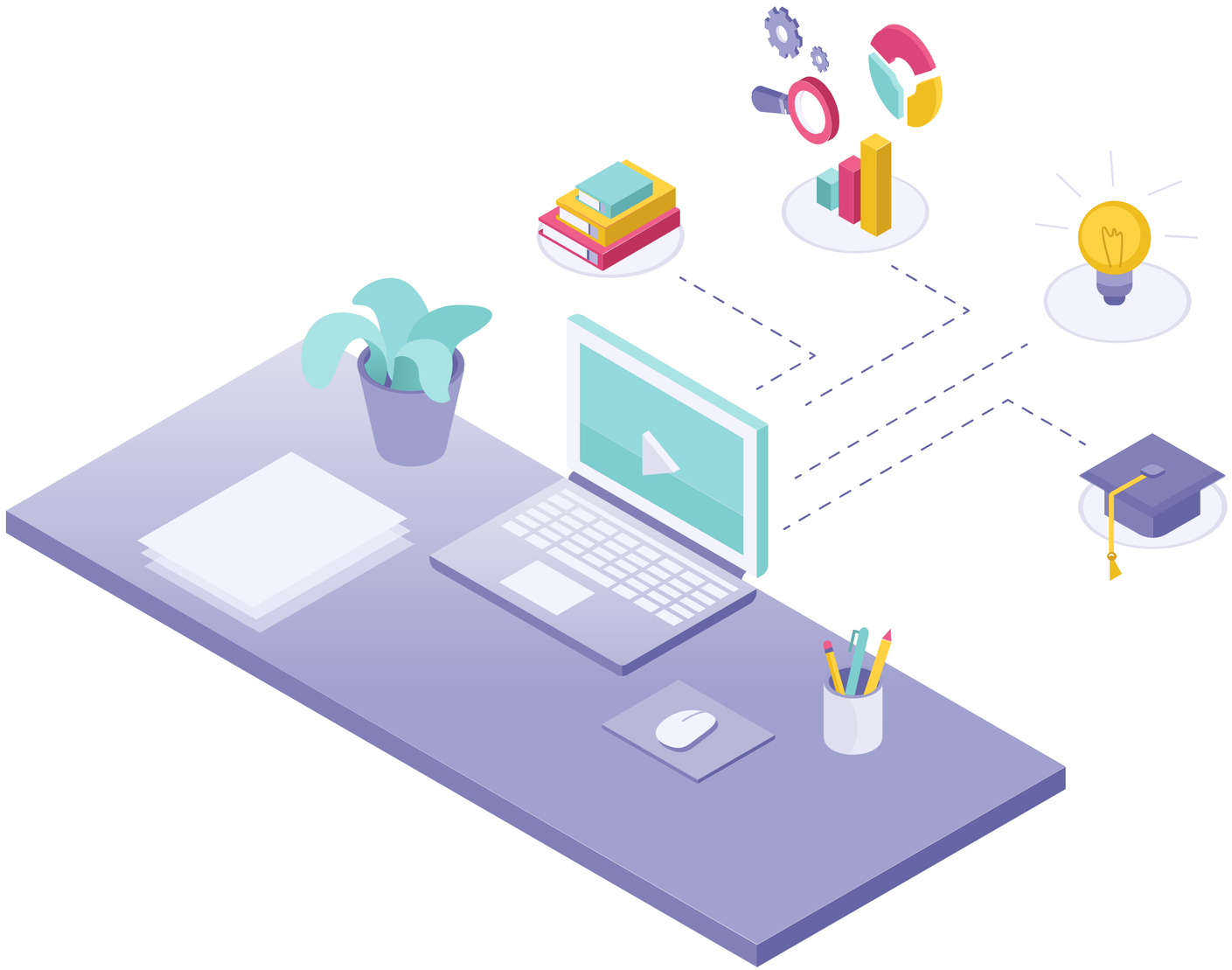
Protections contre : *injection de code SQL, cross-site scripting, volume important de requêtes,...*

Vous définissez des **règles** avec des conditions pour autoriser ou bloquer le trafic web entrant en fonction de conditions

AWS WAF (Web Application Firewall)



AWS Shield

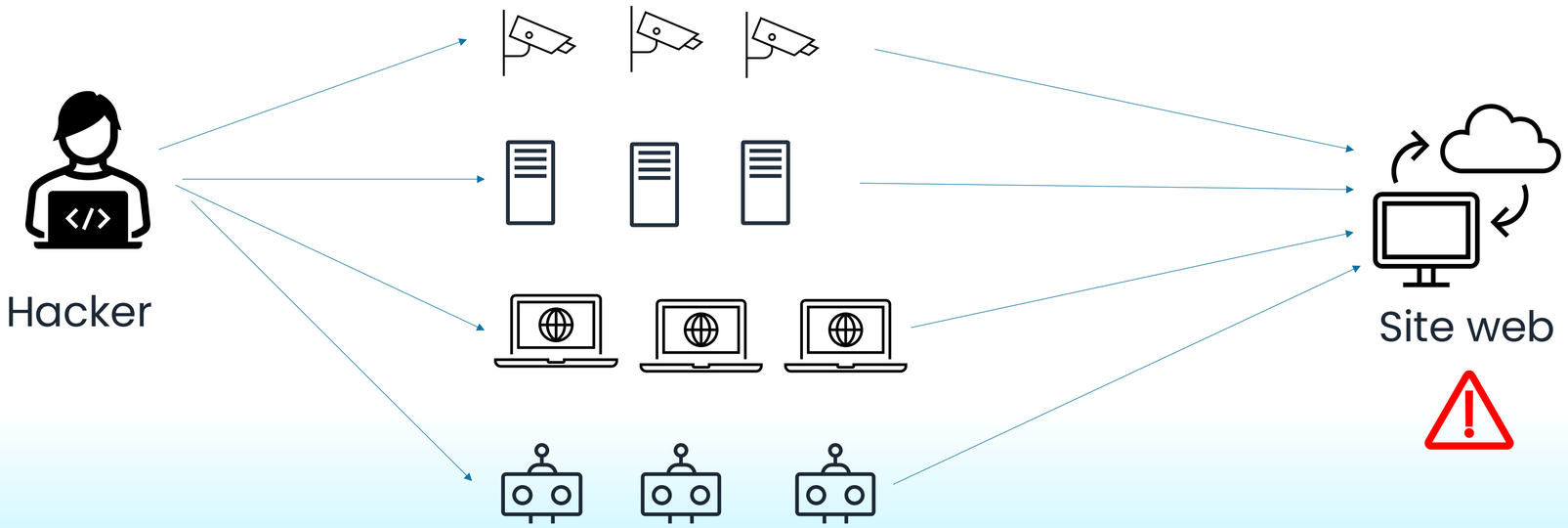


DDoS

Attaque par **déni de service distribué** (DDoS)

Tentative **malveillante** de submerger une cible pour la rendre inopérante

Volume de requêtes peut atteindre plusieurs centaines de Gbps !!

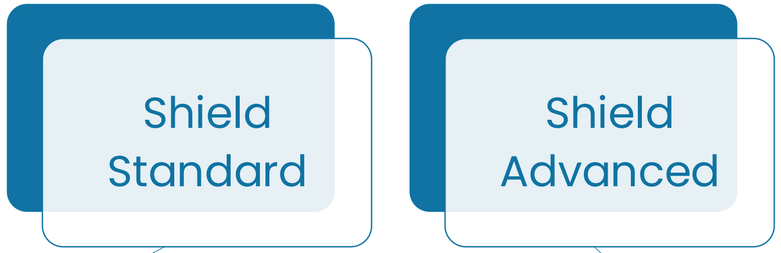


AWS Shield

Service qui **protège vos ressources** AWS contre les attaques DDoS

2 options : Shield **Standard** (gratuit) & Shield **Advanced** (payant)

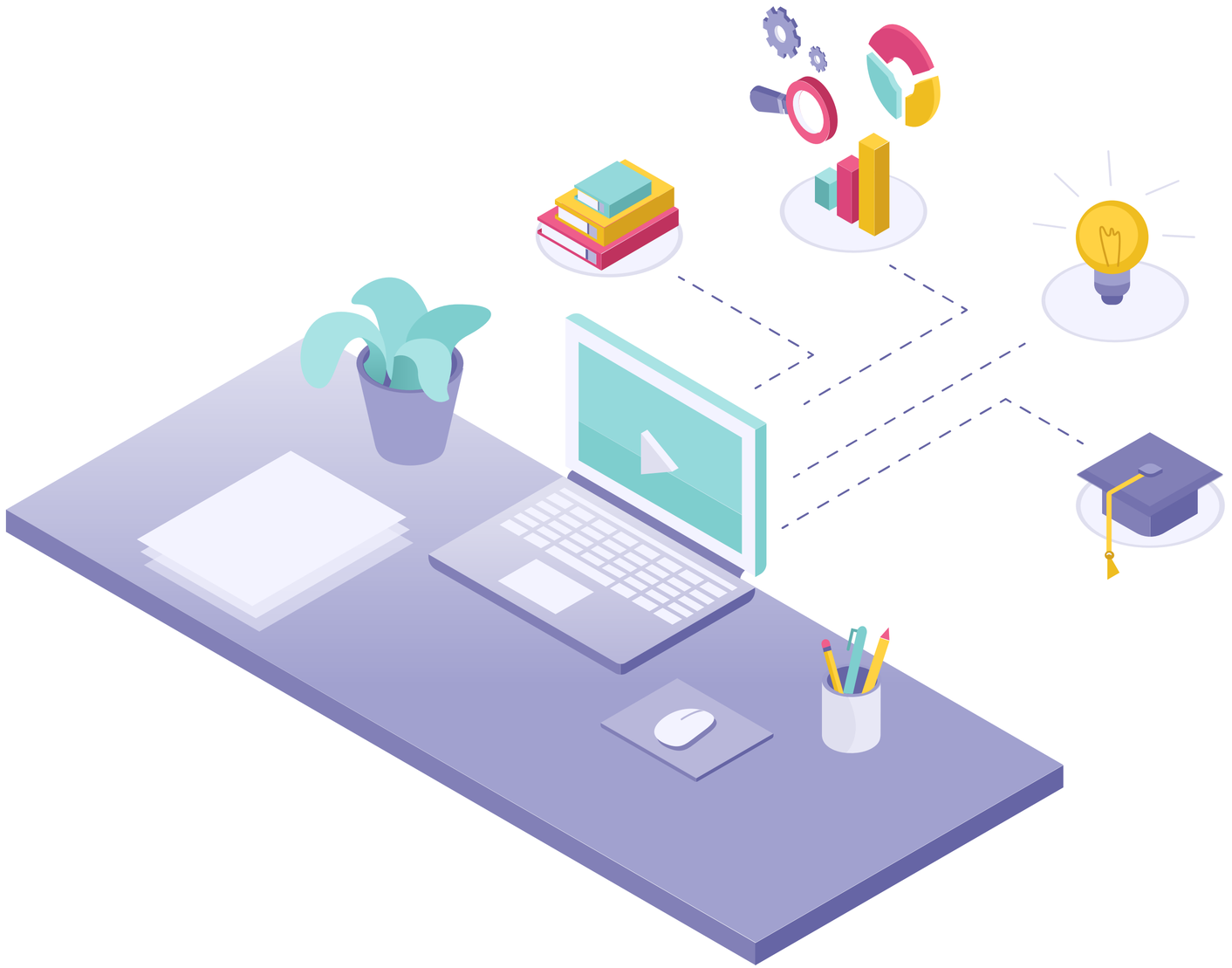




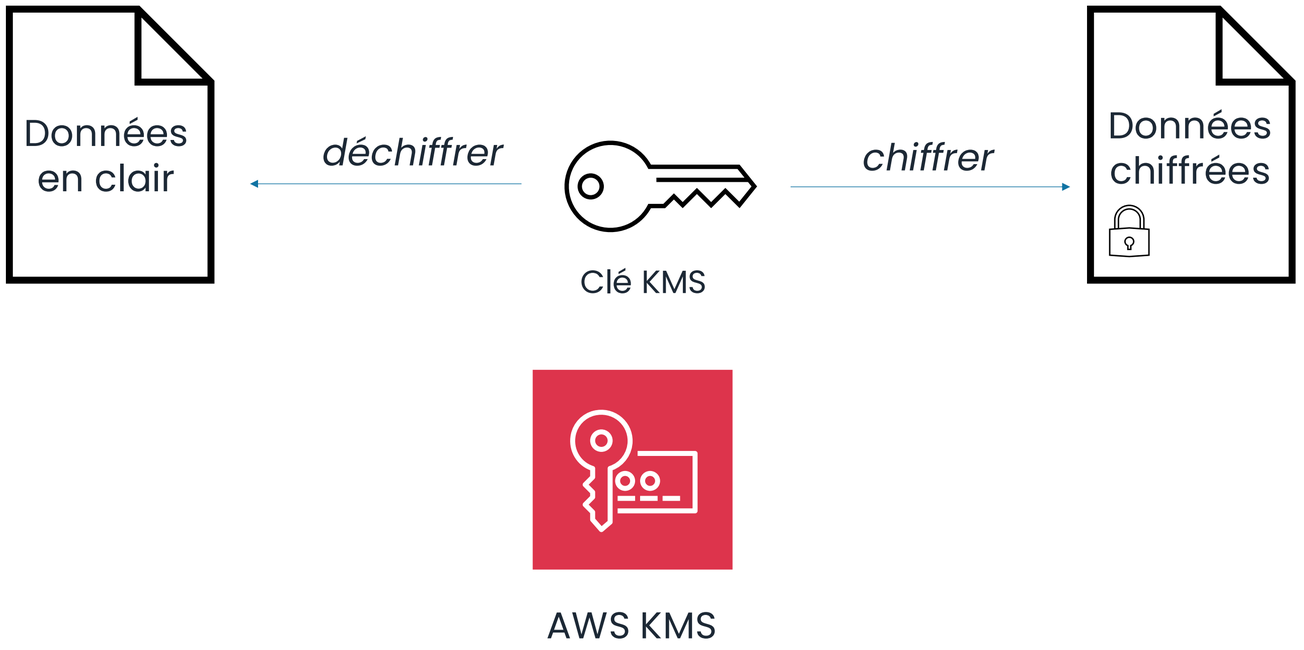
- Gratuit -> Protection Couches 3 et 4 (modèle OSI)
- Types d'attaques : SYN/UDP flood, attaques par réflexion....

- Payant -> Protection Couche 7
- Intégration avec AWS WAF
- Accès au Shield Response Team (SRT)
- Protection contre les coûts liés aux attaques DDoS

AWS Key Management Service (KMS)



AWS Key Management Service (KMS)



AWS Key Management Service (KMS)



Service de gestion de **clés de chiffrement**

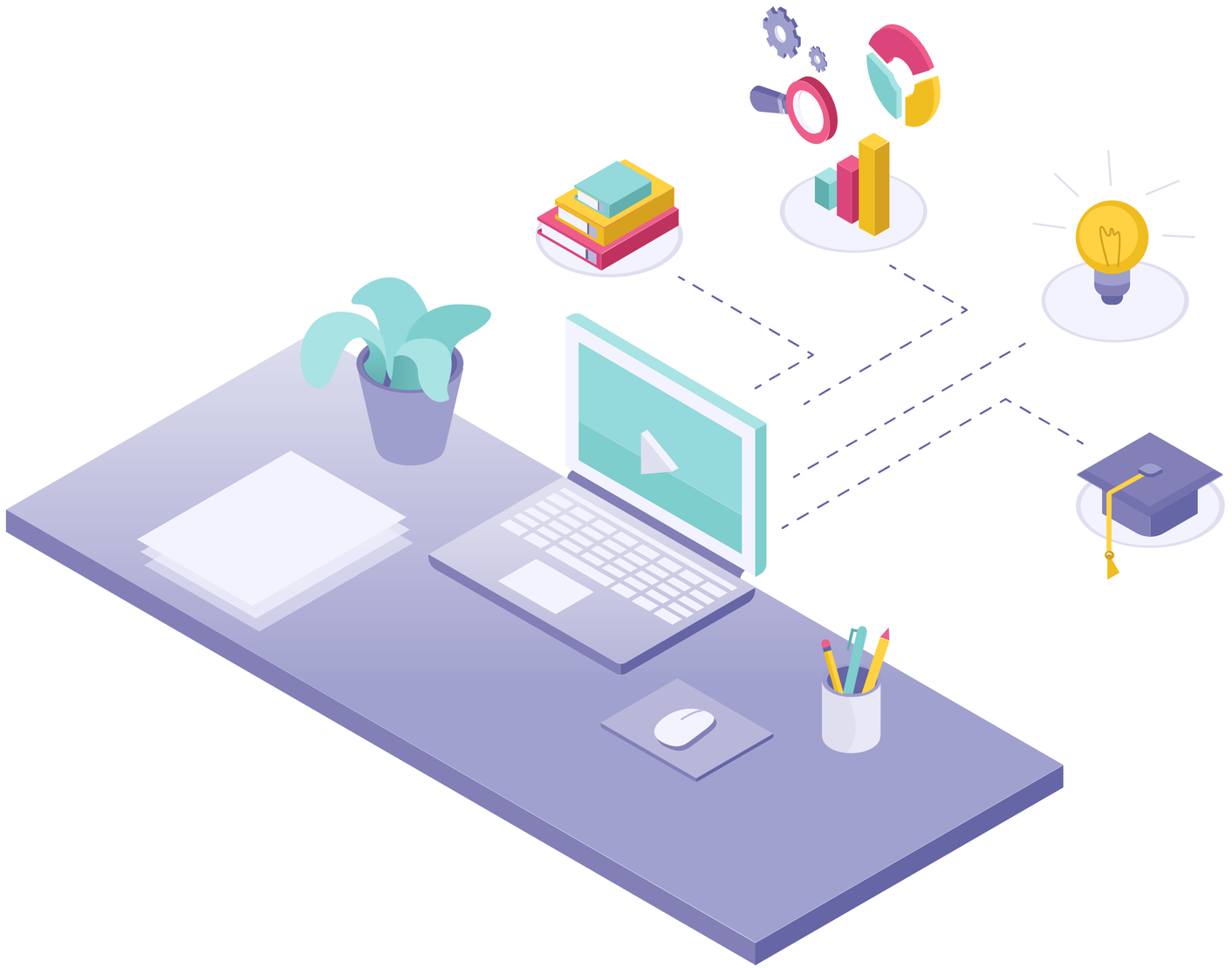
Vous aide à chiffrer vos données **au repos**

Avec AWS KMS, vous pouvez

- **Créer** et administrer des clés de chiffrement
- **Utiliser** les clés KMS pour chiffrer/déchiffrer vos données
- Accorder les **permissions** à des services AWS d'utiliser les clés
- Définir la **rotation automatique**

Intégration avec les **services AWS** (Amazon S3, Amazon EBS, Redshift…)

AWS Secrets Manager



AWS Secrets Manager



Permet de stocker et gérer de façon centralisée vos secrets.

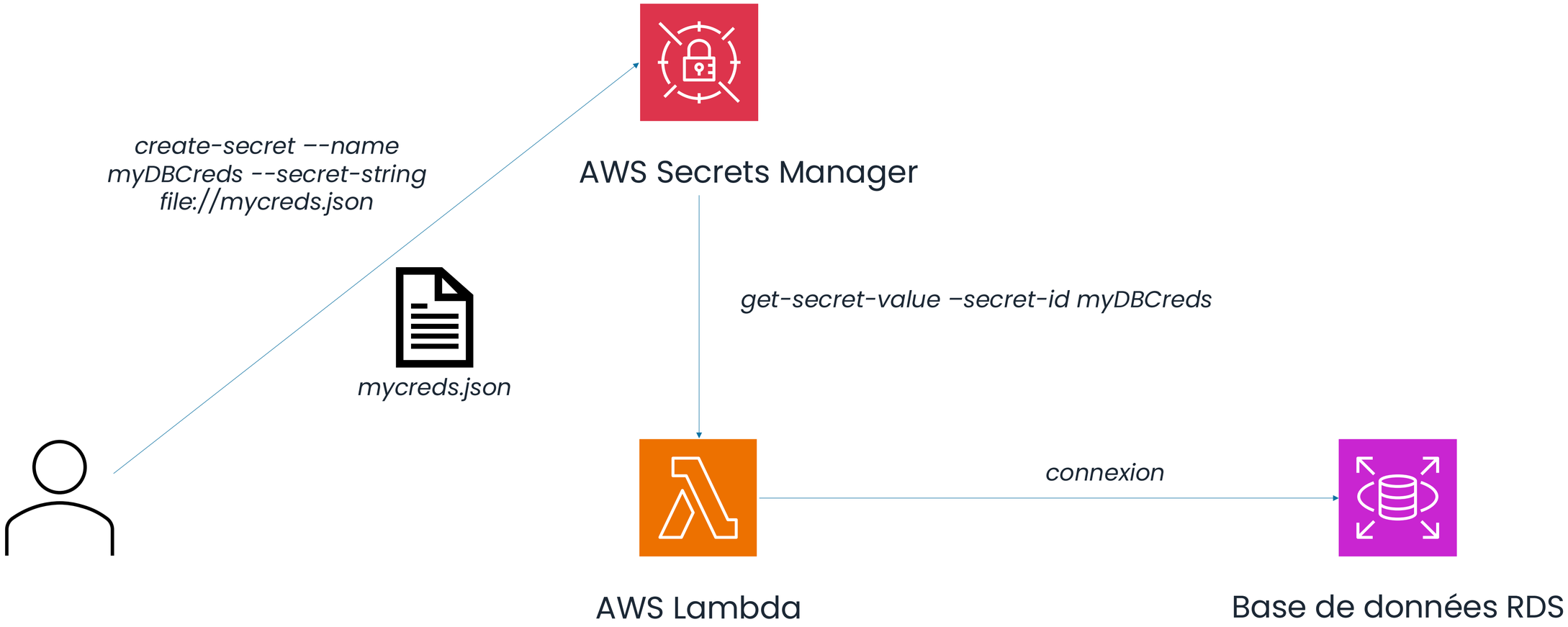
Secrets -> mots de passe, informations d'identification, clés d'API, jetons Oauth...

Avec AWS Secrets Manager, vous pouvez

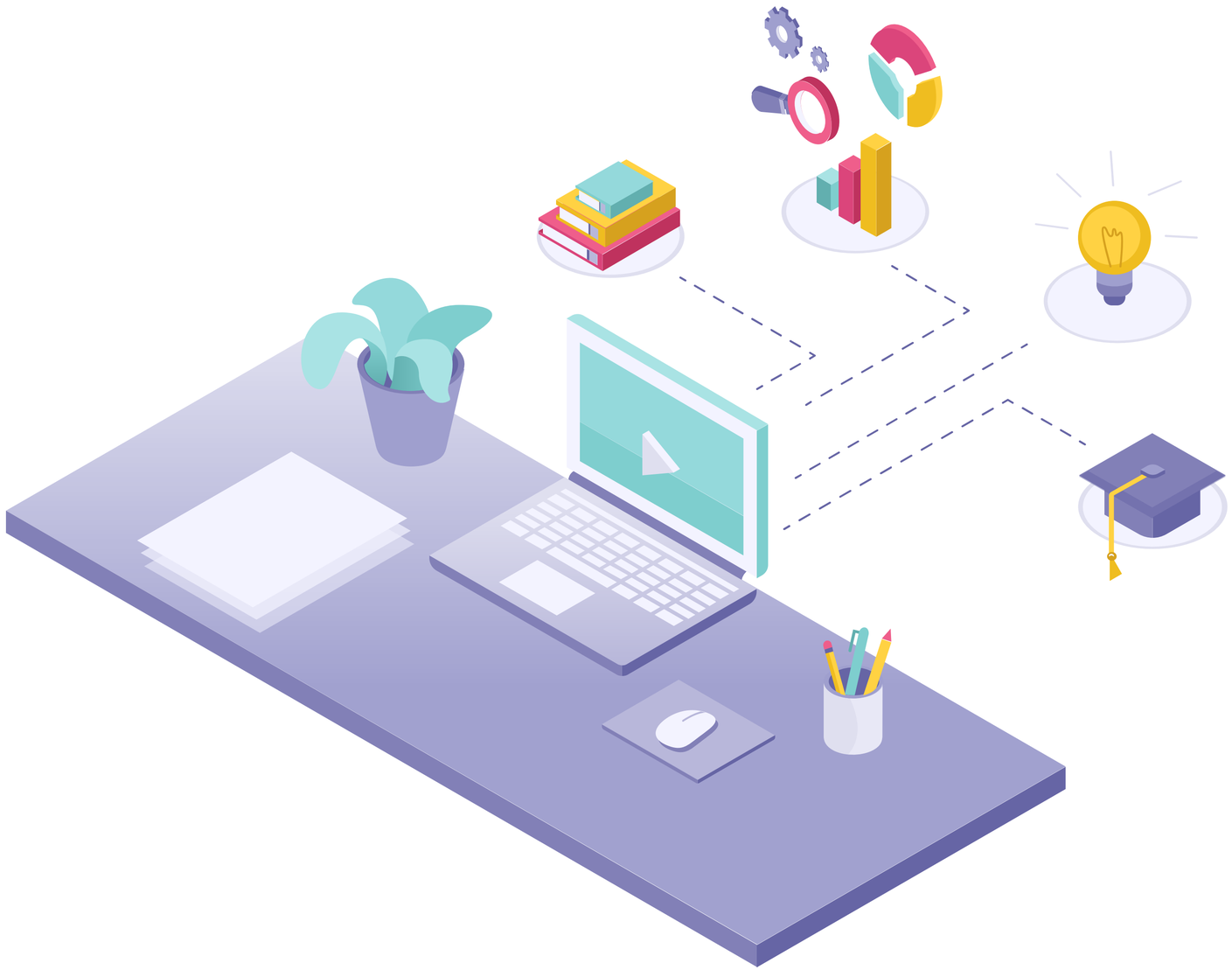
- Stocker et administrer vos secrets
- Gérer la rotation automatique de vos secrets
- Utiliser AWS IAM pour contrôler les permissions d'accès

LeCloudFacile.com

Comment ça marche ?



AWS Certificate Manager



AWS Certificate Manager (ACM)



Permet de créer, d'administrer et déployer facilement des **certificats SSL/TLS**

Chiffrement **en transit**

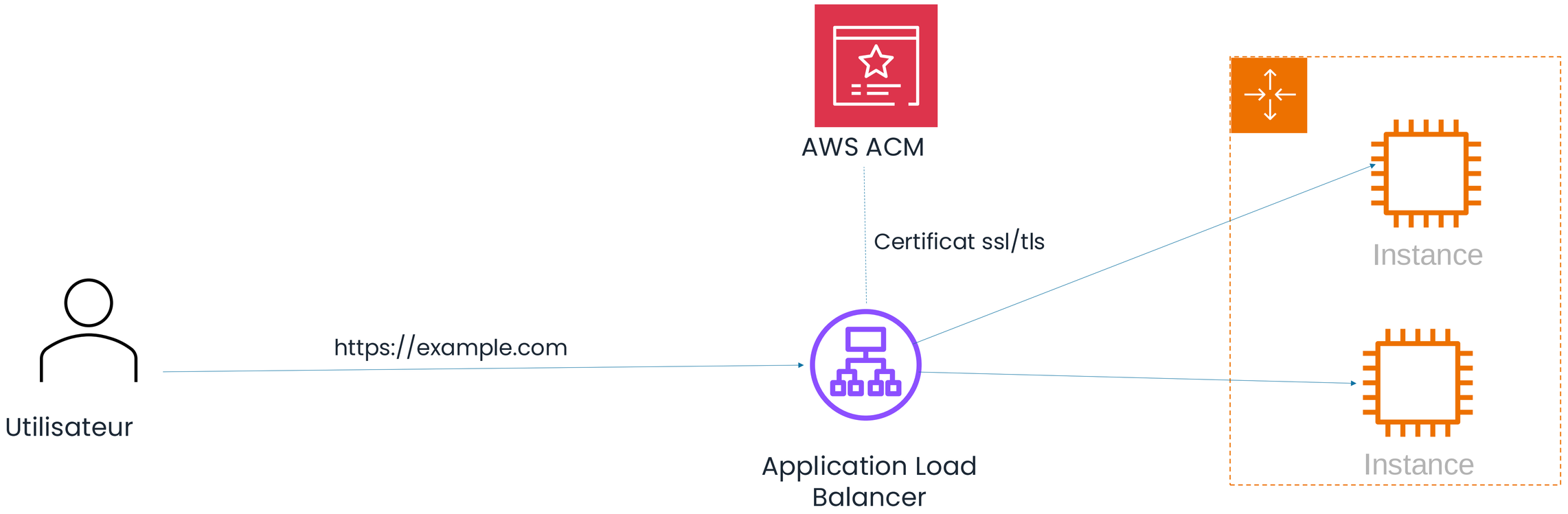
Fournit des certificats

- ***publics*** *(gratuits)*ou ***privés***
- Utilisables **uniquement** avec les services AWS ou dans vos VPC

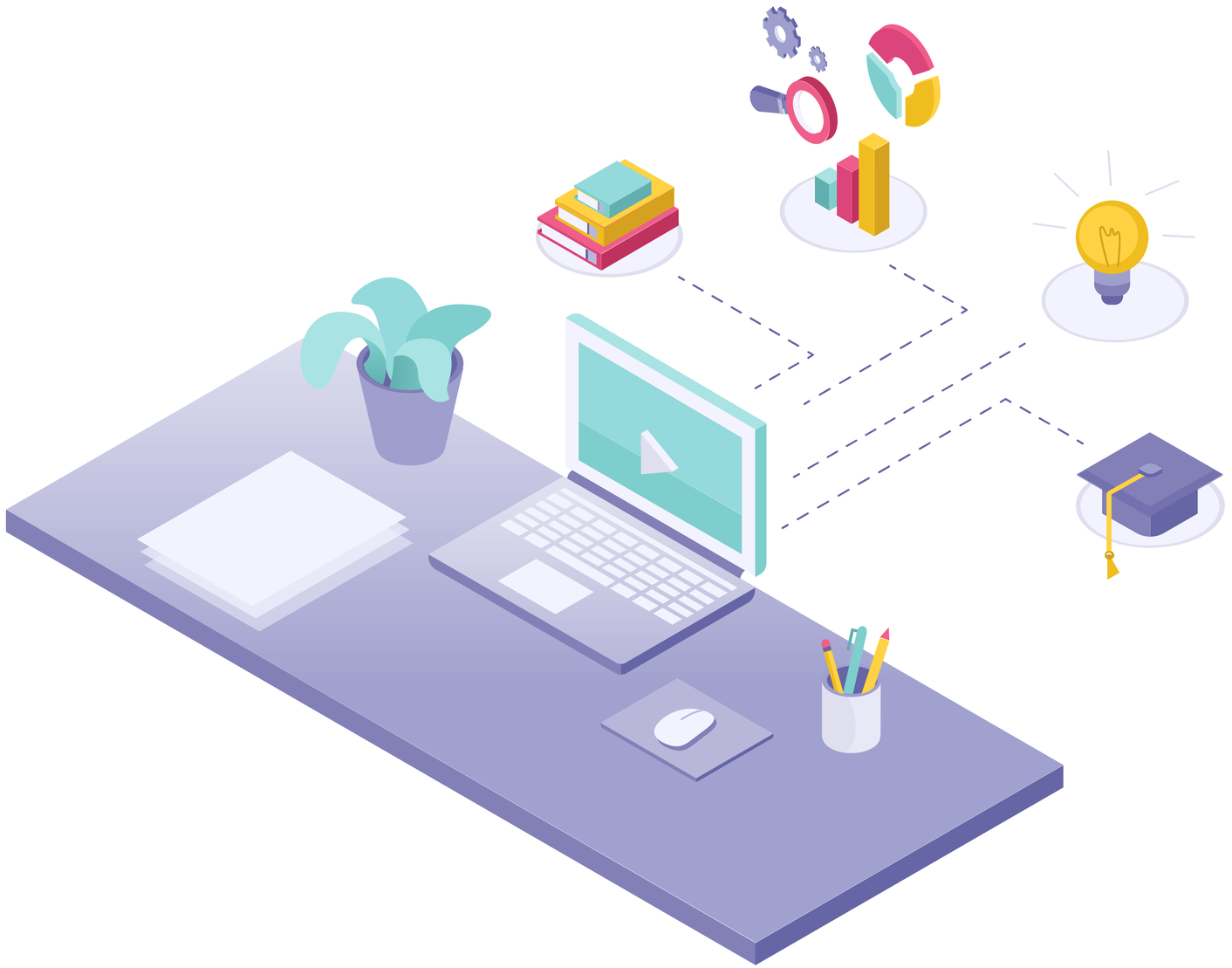
S'intègre avec les Elastic Load Balancers, CloudFront et Amazon API Gateway

Renouvellement automatique des certificats

Mise en place d'un site web sécurisé



Amazon Macie



Amazon Macie

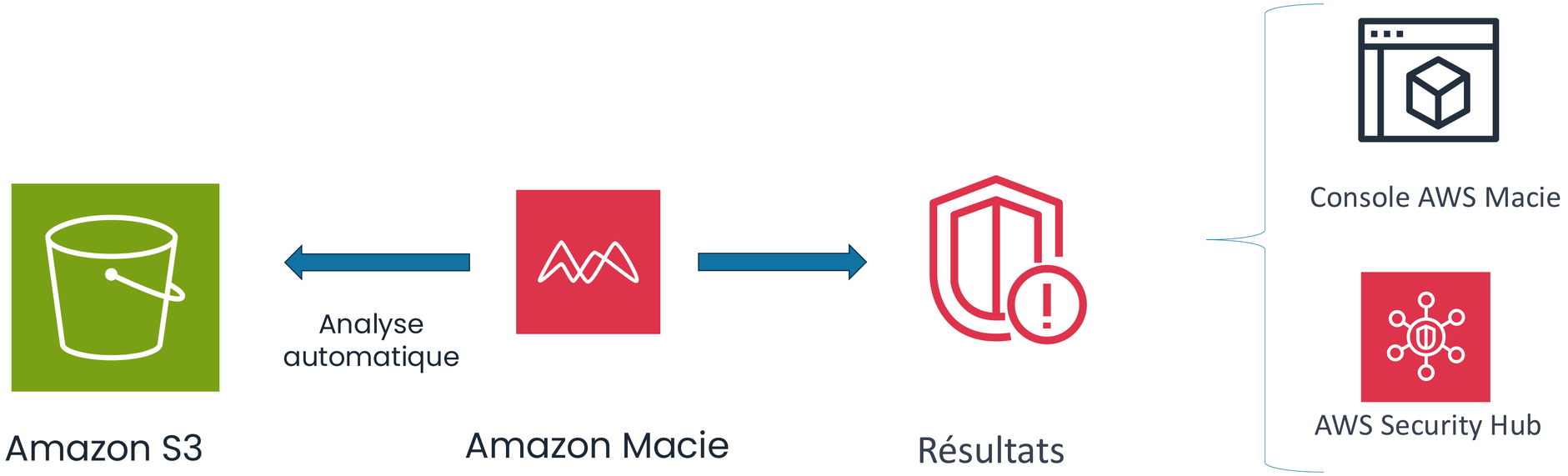


Identifie et protège vos données sensibles stockées dans Amazon S3

Utilise le Machine Learning et la correspondance de modèles

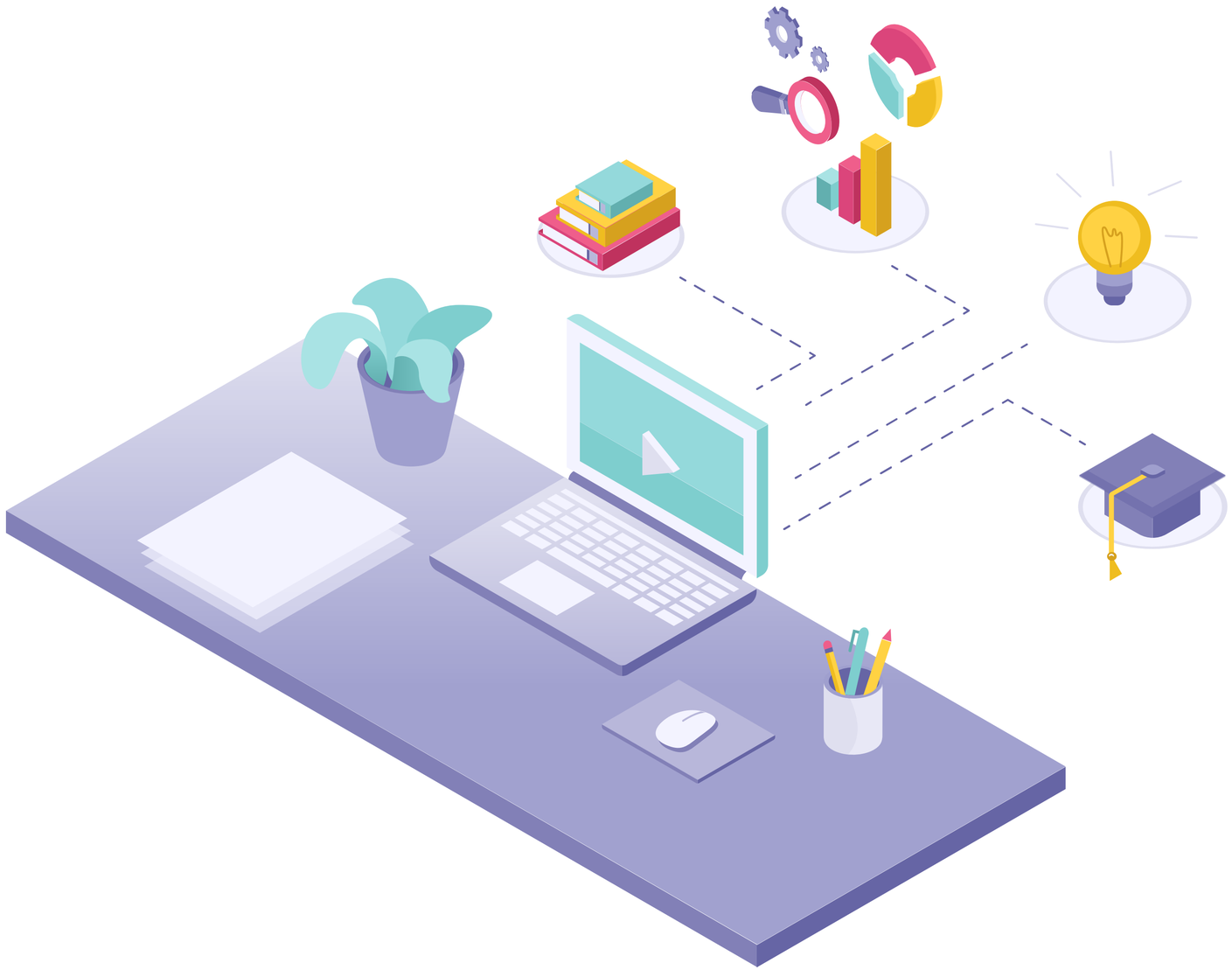
Données sensibles = Données PII -> prénoms, noms, adresses, numéros de cartes de crédit...

Comment ça marche ?



- Données sensibles
- Numéros cartes crédits
- Bucket public

AWS Artifact



AWS Artifact

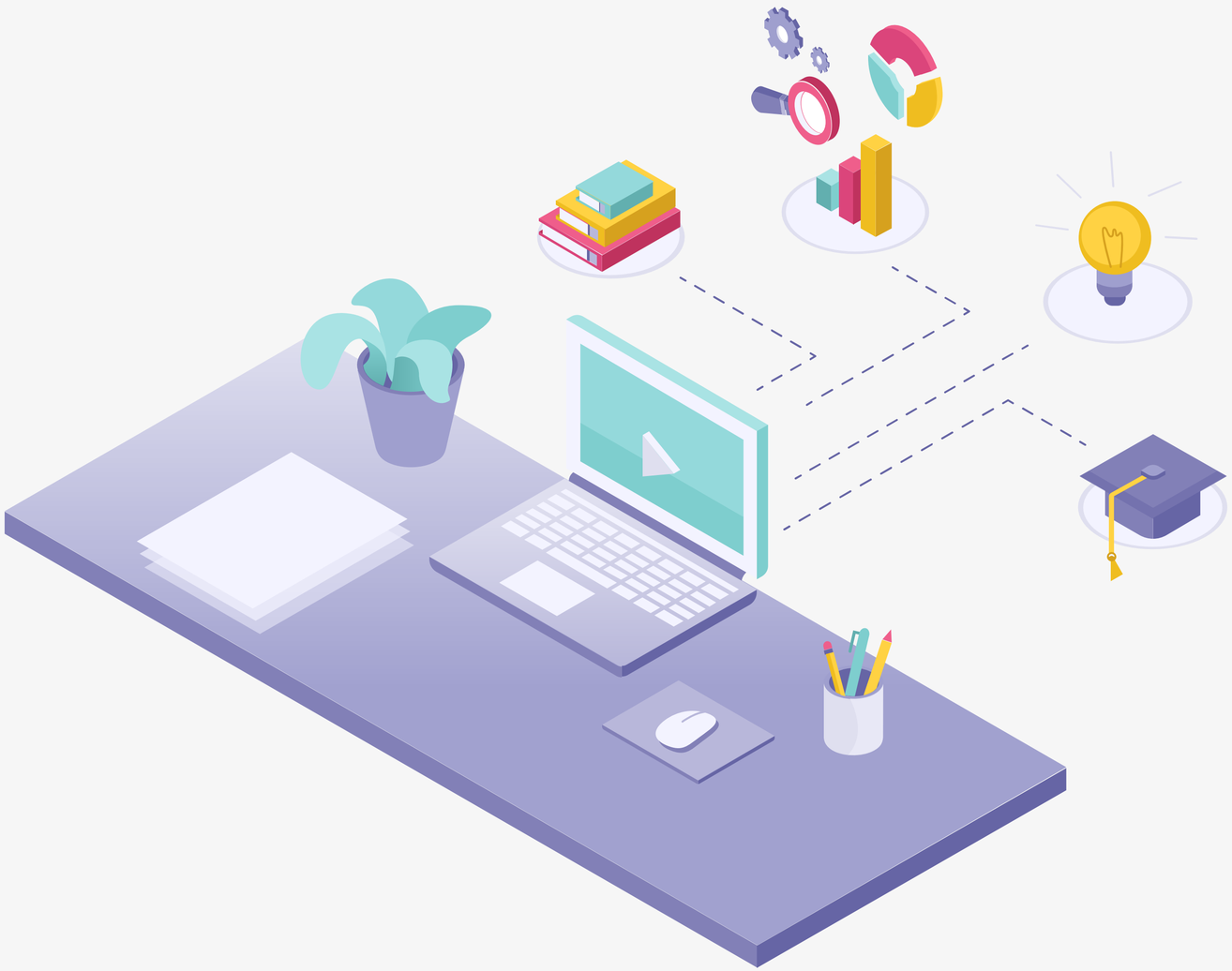


Offre un accès à la demande **aux rapports de sécurité et conformité** d'AWS

Disponible en **libre-service** dans la console, pour tous les **clients AWS**

Vous pouvez télécharger par exemple

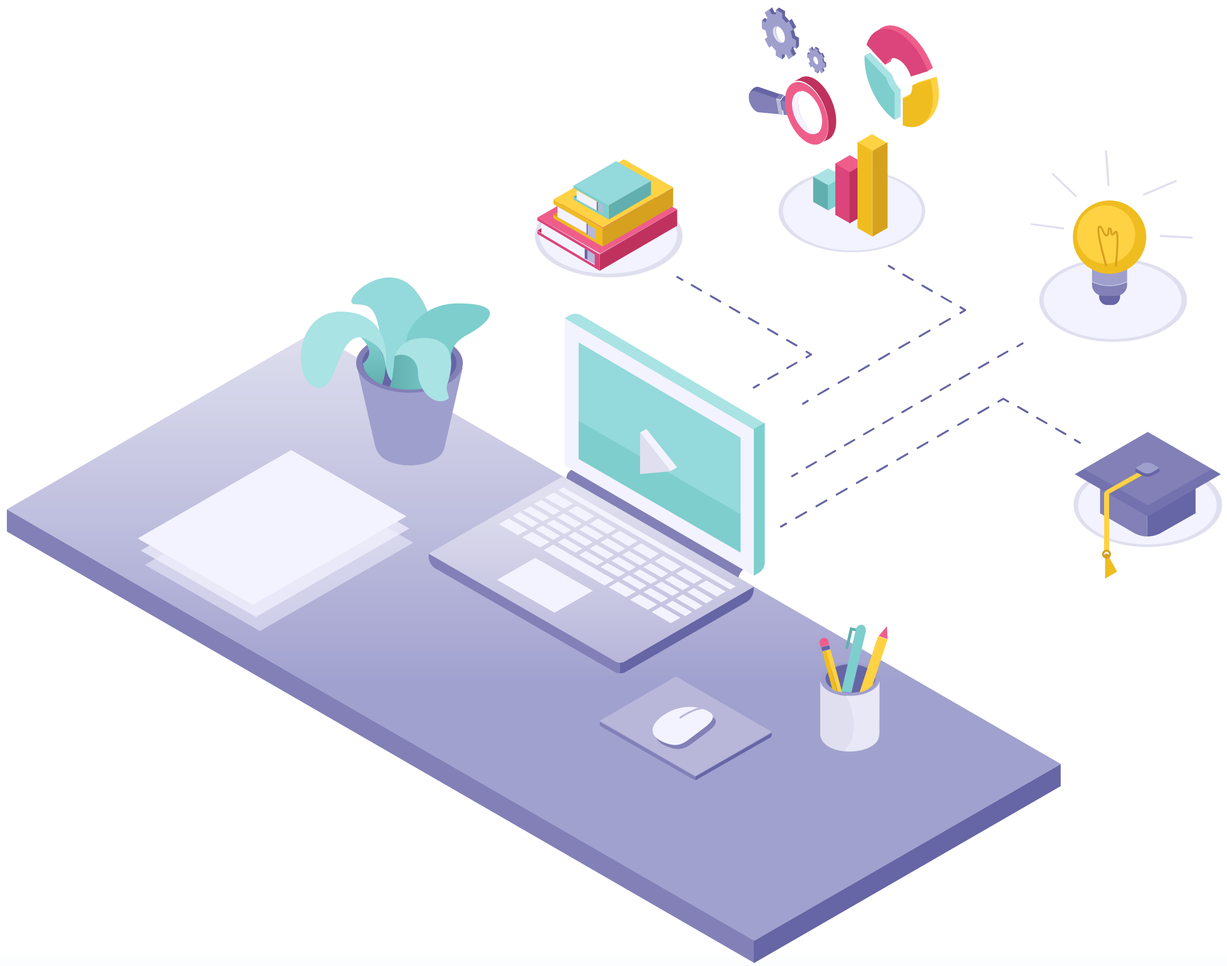
- Les certifications ISO d'AWS
- Rapport PCI-DSS
- Rapports SOC



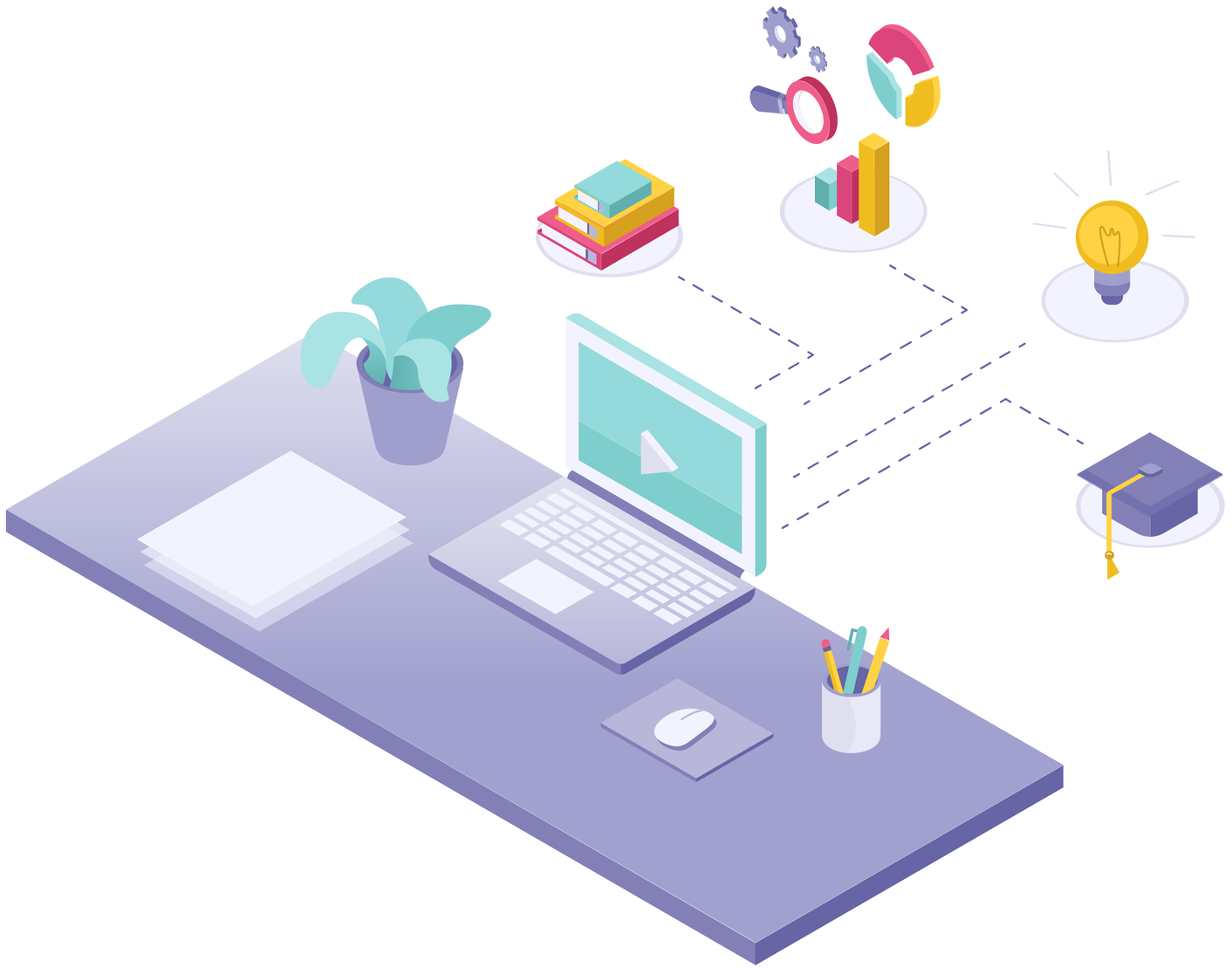
FIN DU MODULE

Module 13 : Développer des applications

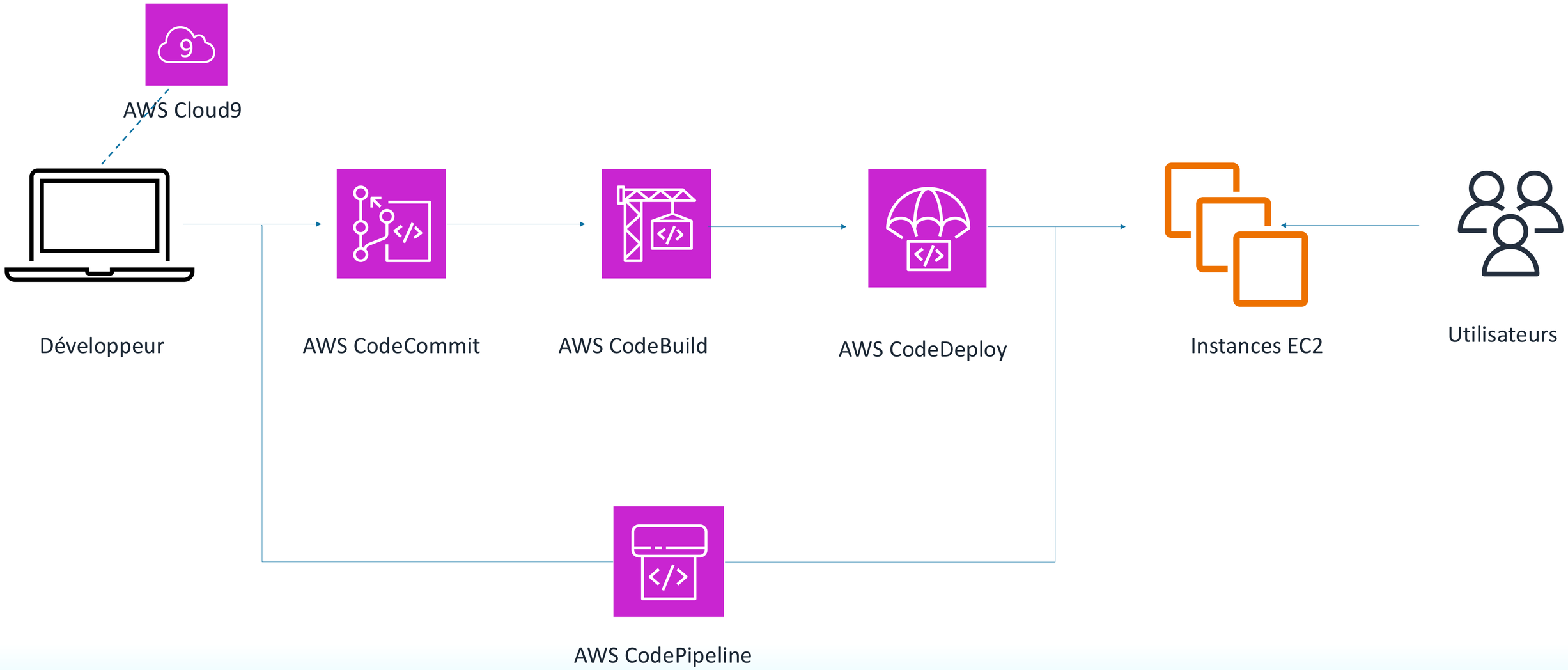
Développer des applications sur AWS plus rapidement et plus facilement



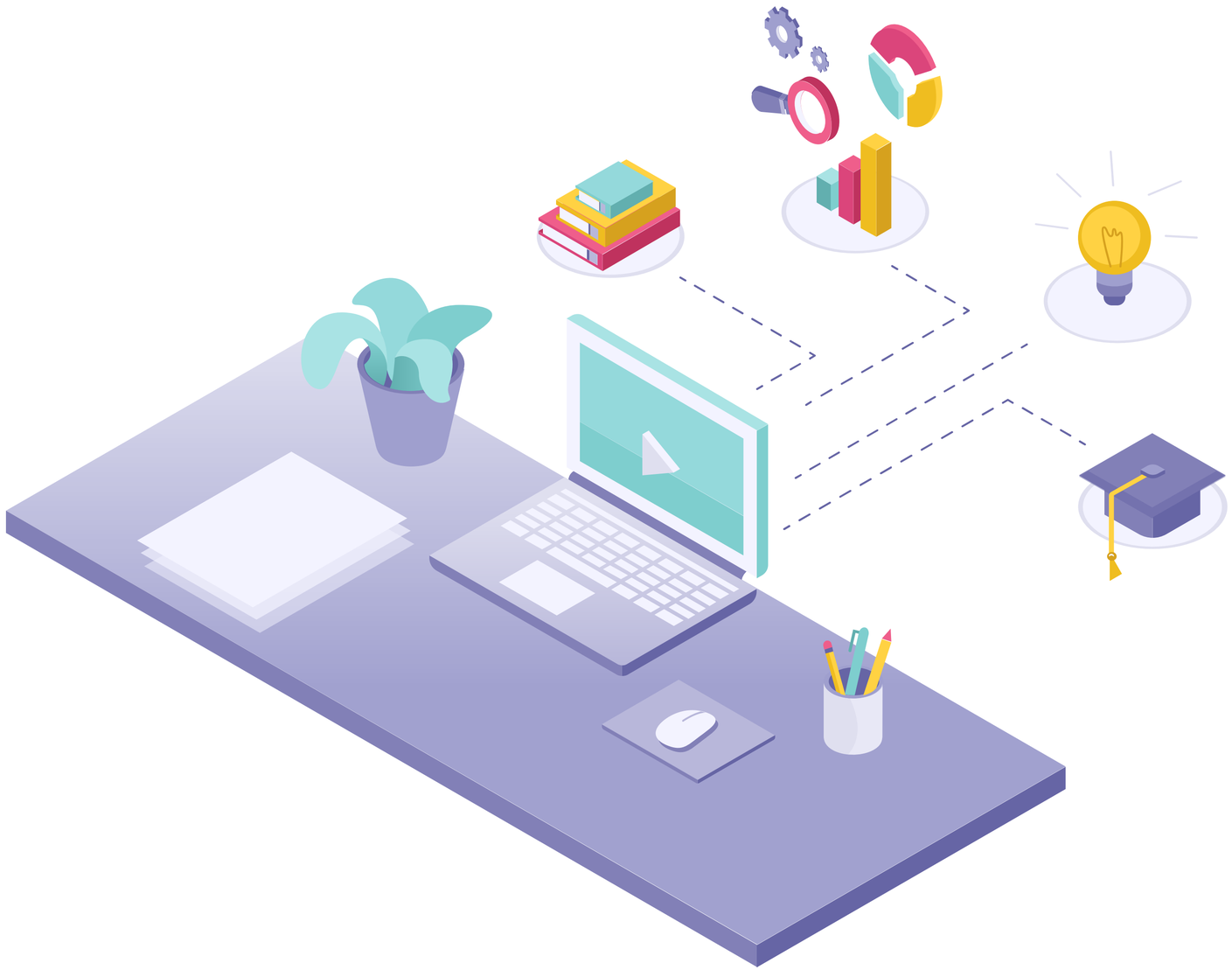
Développer sur AWS



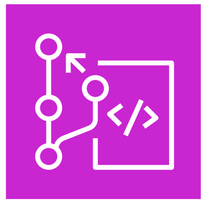
Développer sur AWS



AWS CodeCommit



AWS CodeCommit



Permet d'héberger des **référentiels Git privés** sur AWS

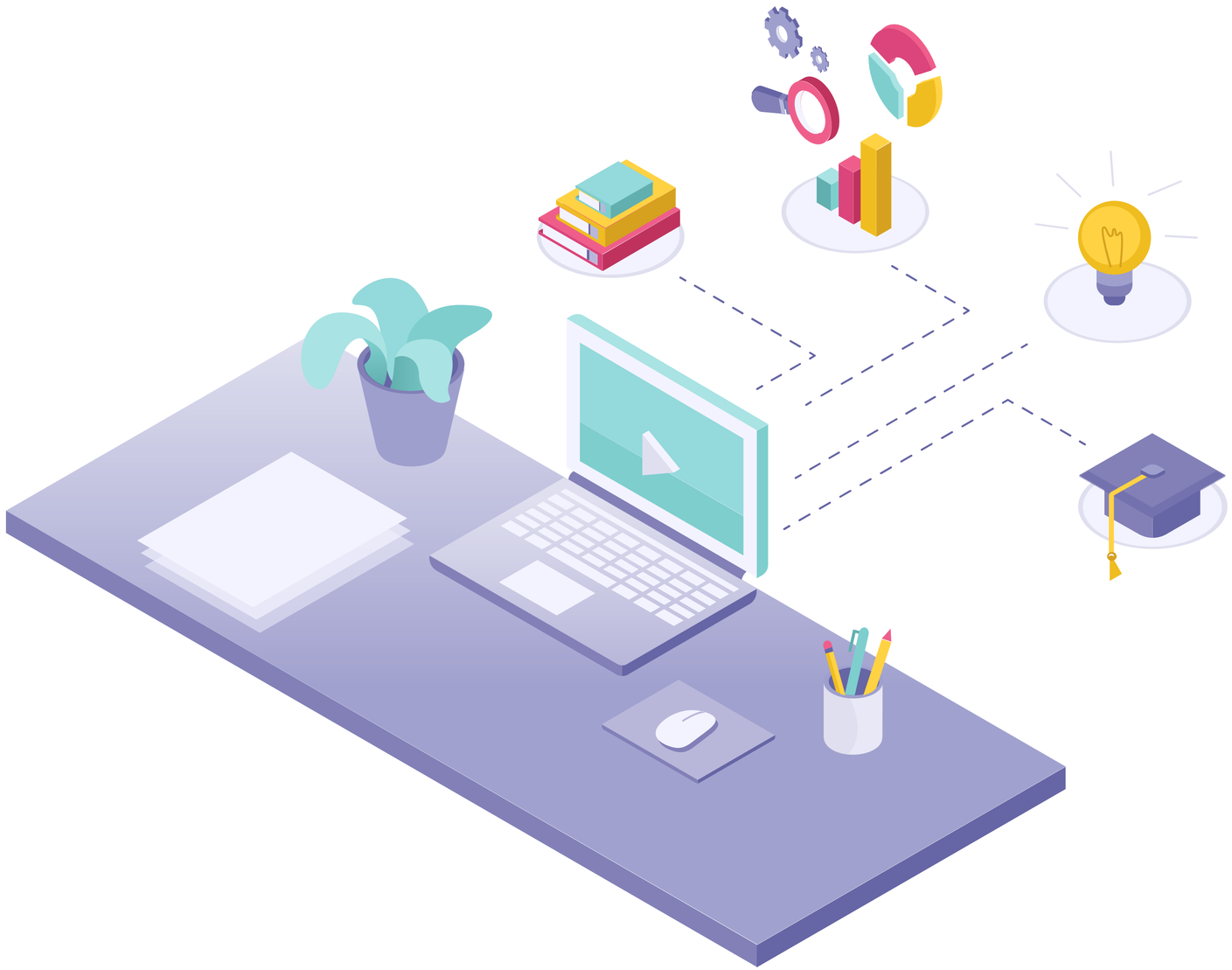
Git = système de contrôle de version distribué open source

Alternative à Github…

Fonctionnalités clés

- Stocker et **versionner** du code
- Référentiel **entièrement géré** par AWS
- Intégration avec les **autres services AWS** (CodeBuild, CodePipeline,…)

AWS CodeBuild

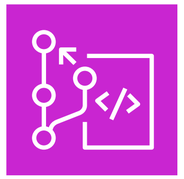


LeCloudFacile.com

AWS CodeBuild

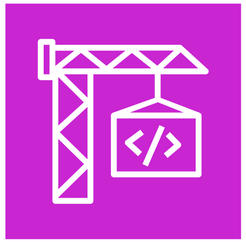


Amazon S3



AWS CodeCommit





AWS CodeBuild



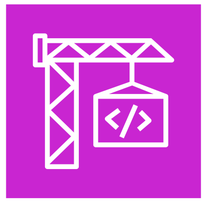


Amazon S3



Github,...

AWS CodeBuild



Service de **compilation** entièrement géré sur AWS

Vous libère de la gestion des **serveurs de *build***

Permet d'automatiser

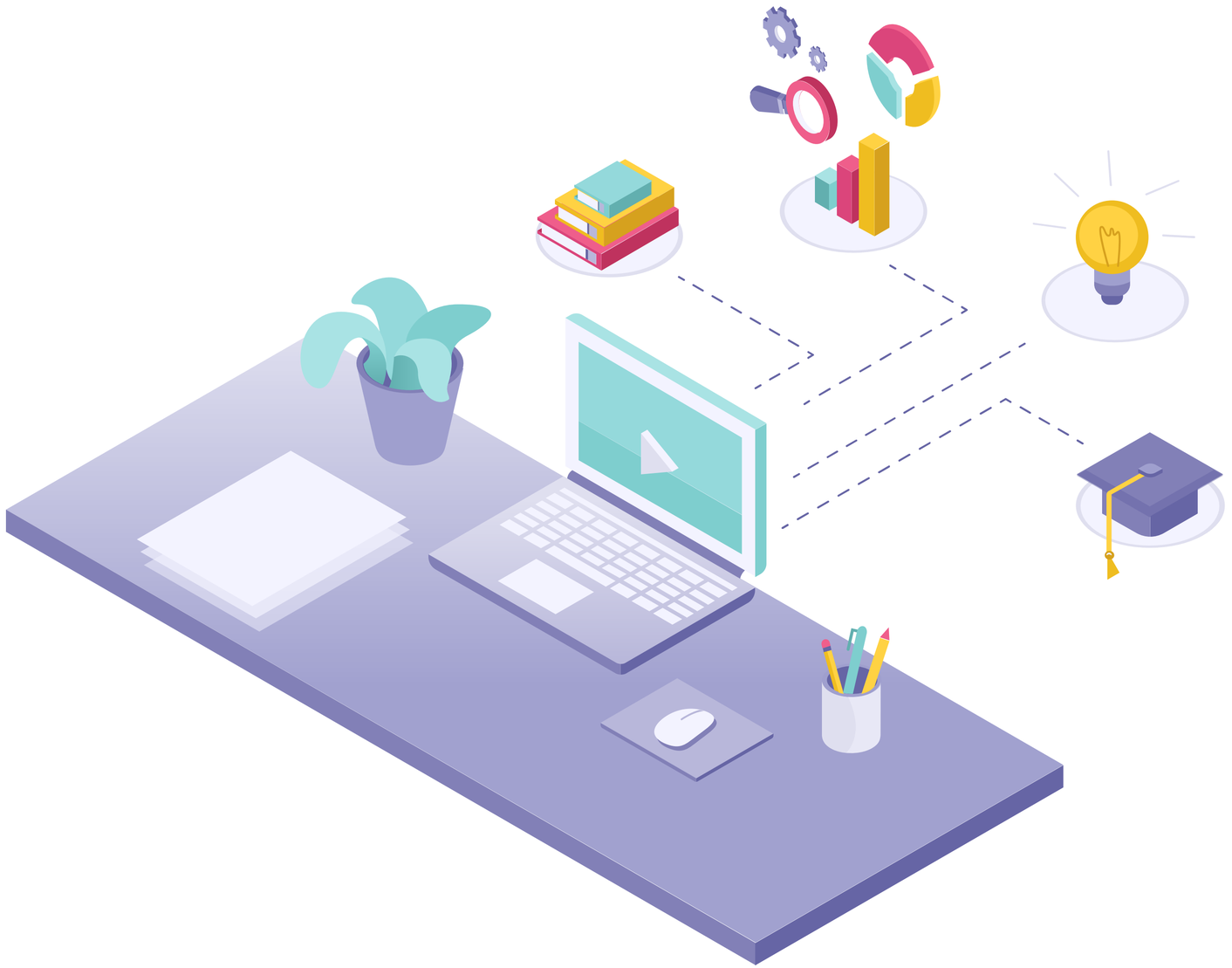
- la compilation de votre code source
- L'exécution des tests
- Le packaging des applications

Sources supportées : AWS CodeCommit, S3, Github,...

Environnements supportés : Java, Ruby, Python, Go, Node.js, Android,

.NET Core, PHP, Images Docker personnalisées...

AWS CodeDeploy

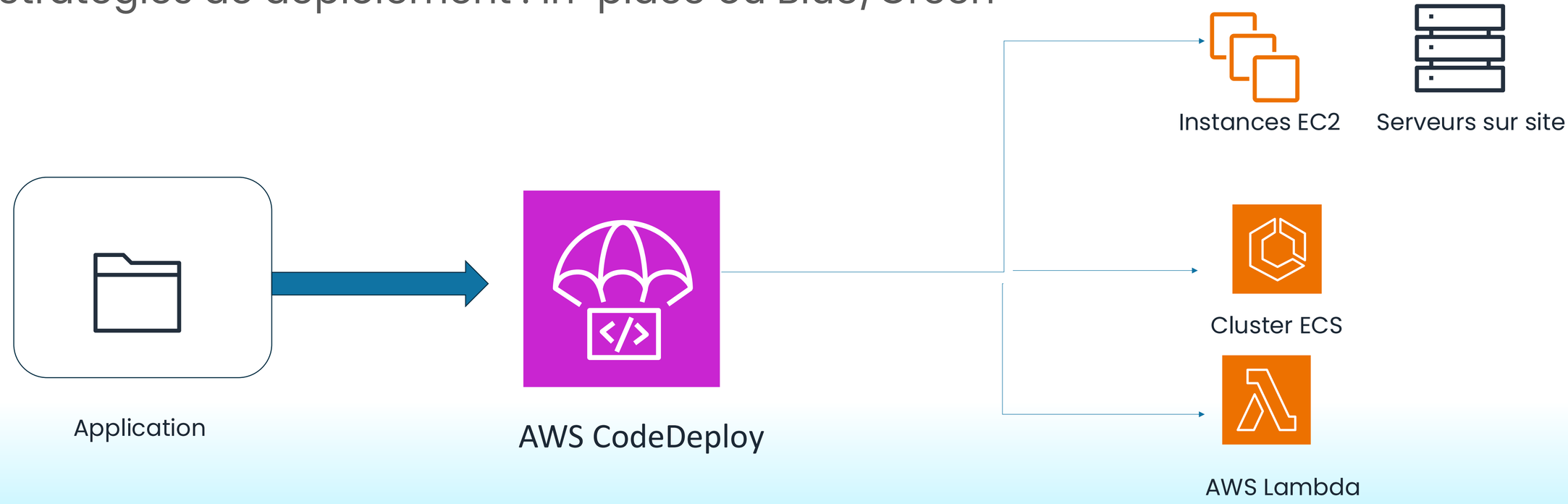


AWS CodeDeploy

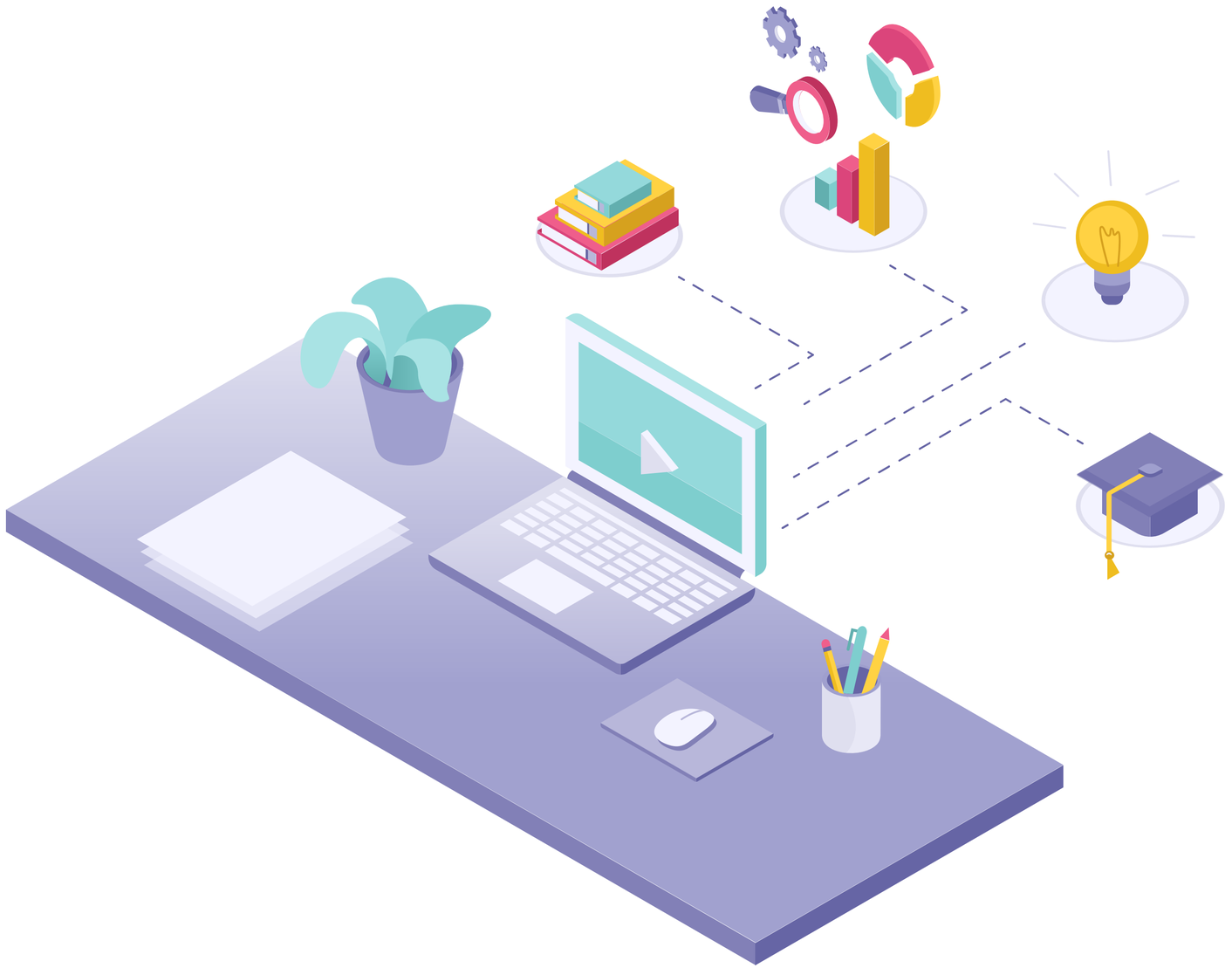
Permet **d'automatiser le déploiement** de votre code applicatif

Environnements supportés : Instances EC2, Cluster ECS, Fonctions AWS Lambda ou environnements on-premises (sur site)

Stratégies de déploiement : In-place ou Blue/Green

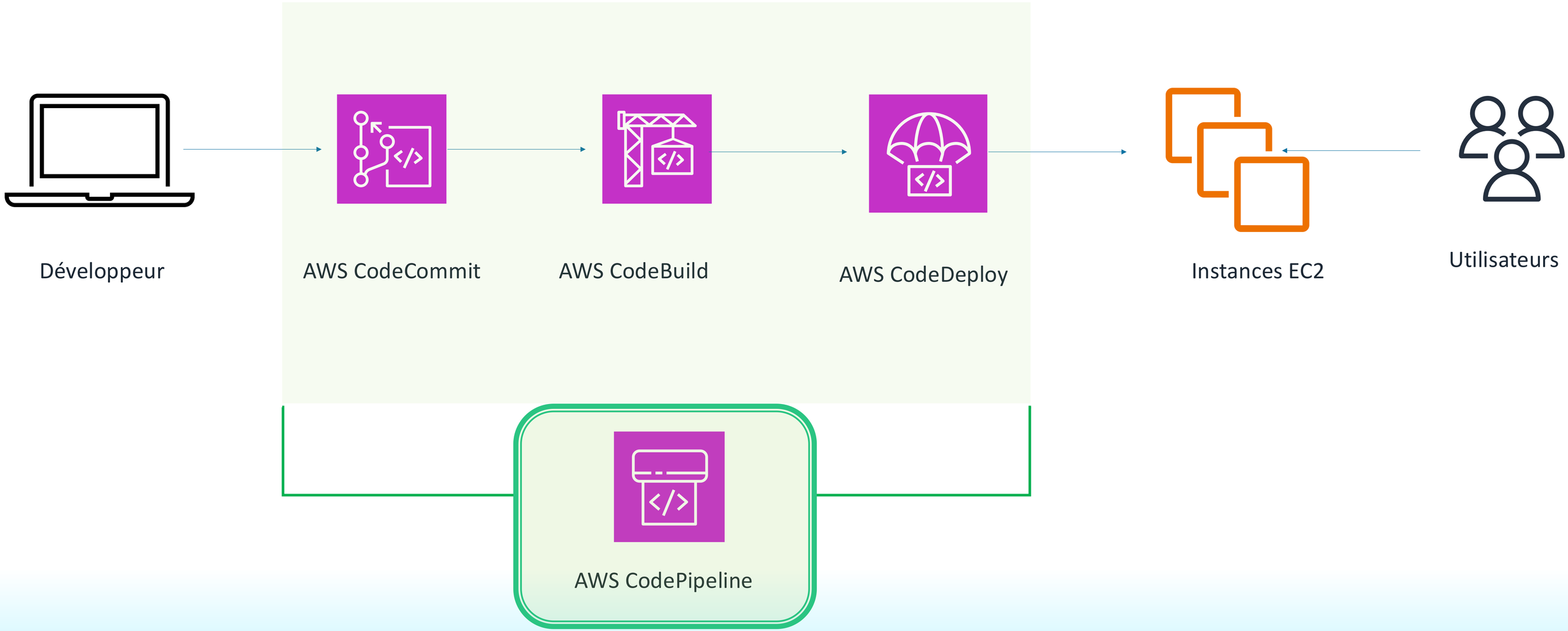


AWS CodePipeline



LeCloudFacile.com

AWS CodePipeline



AWS CodePipeline



Permet de créer des **pipelines** de livraison continue (CI/CD)

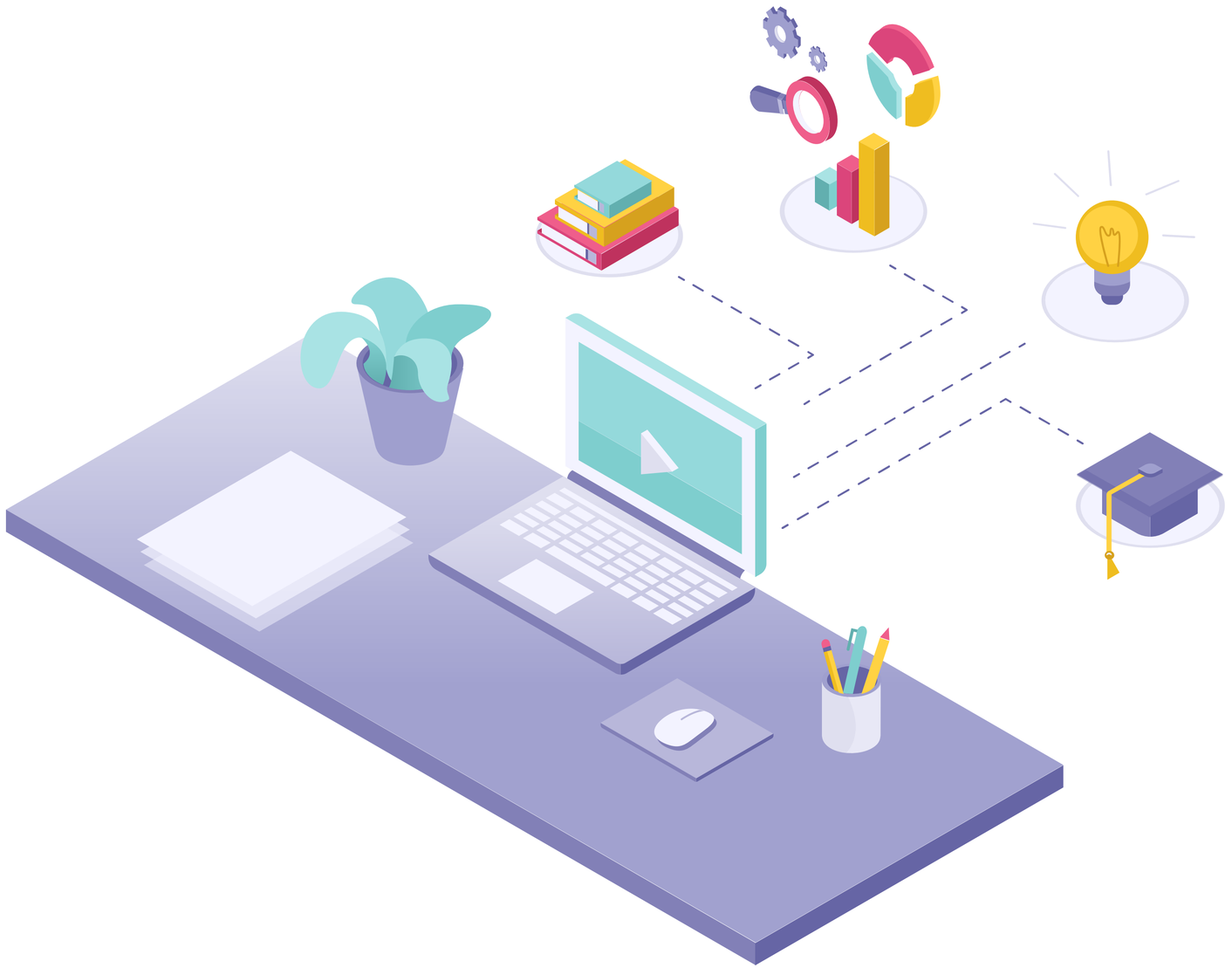
Pipeline -> série d'étapes qui constituent le flux de travail.

- Exp : Code source -> Compilation -> Tests Unitaires -> Déploiement

Alternative à **Jenkins, Gitlab CI/CD**

Intégration avec les **services AWS** : CodeCommit, CodeBuild, CodeDeploy…

AWS Cloud9



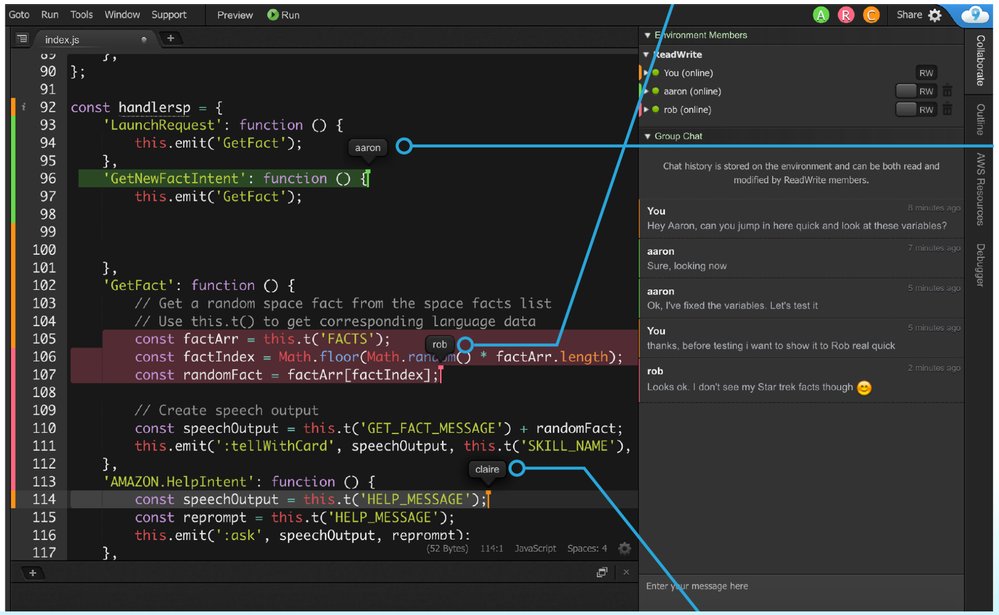
AWS Cloud9

Environnement de développement intégré (IDE) dans le Cloud AWS

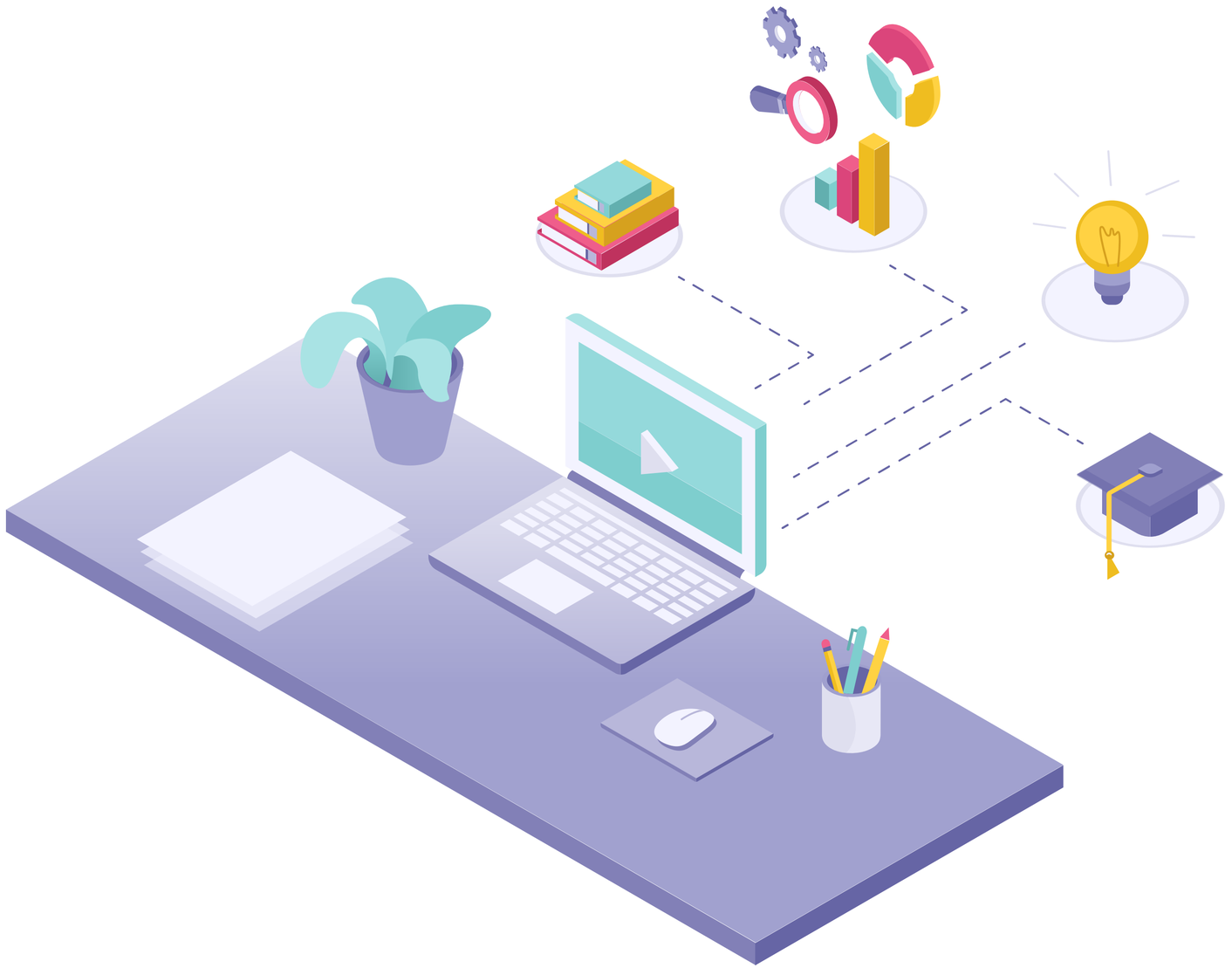
Permet de **développer** du code depuis un navigateur web

+40 langages supportés dont Node.js, Python, PHP, Ruby, Go, C++

Outils **également inclus** : AWS CLI, Docker, Git…



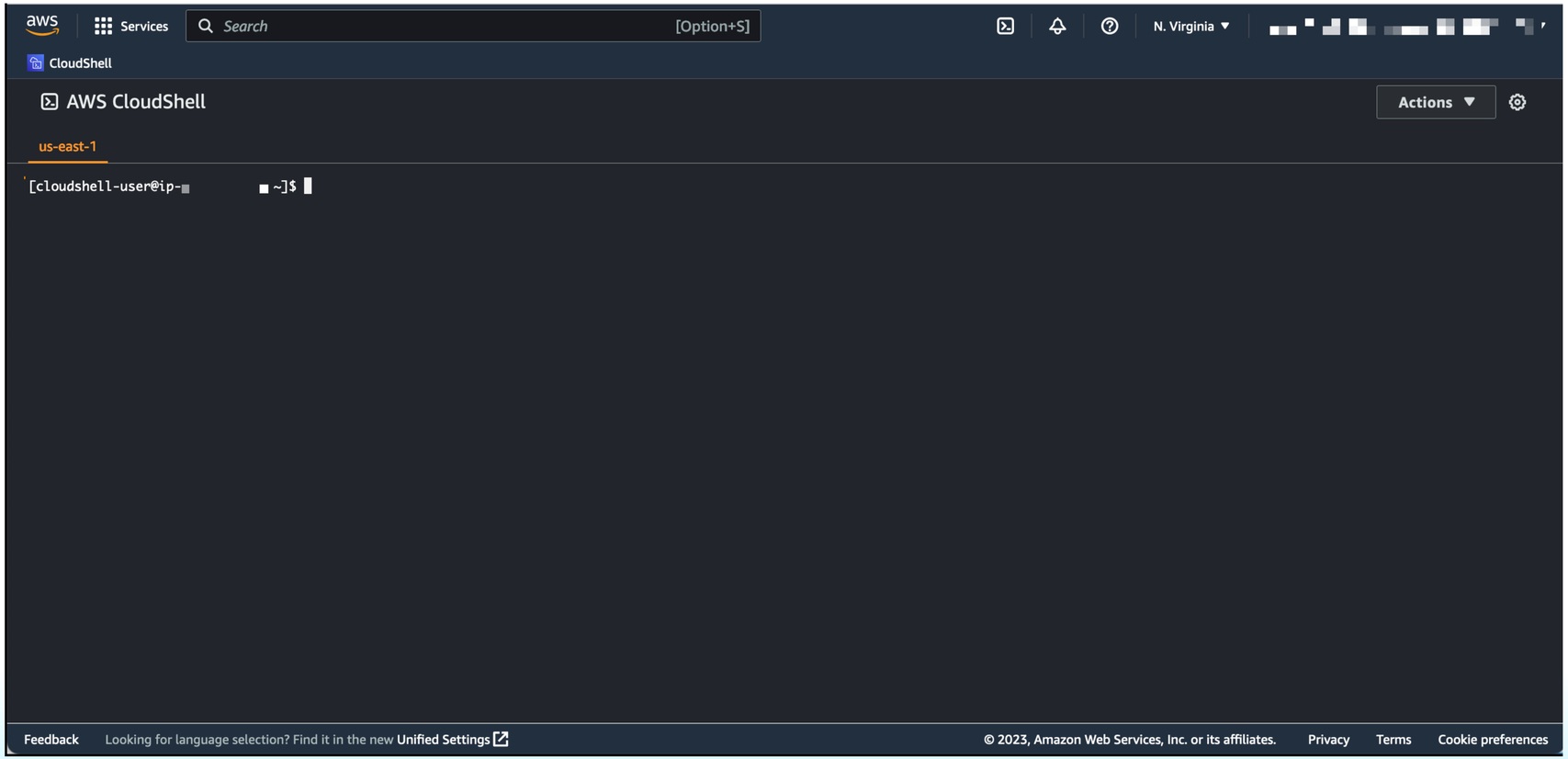
AWS CloudShell



AWS CloudShell

Environnement de ligne de commande (CLI) directement dans la console AWS

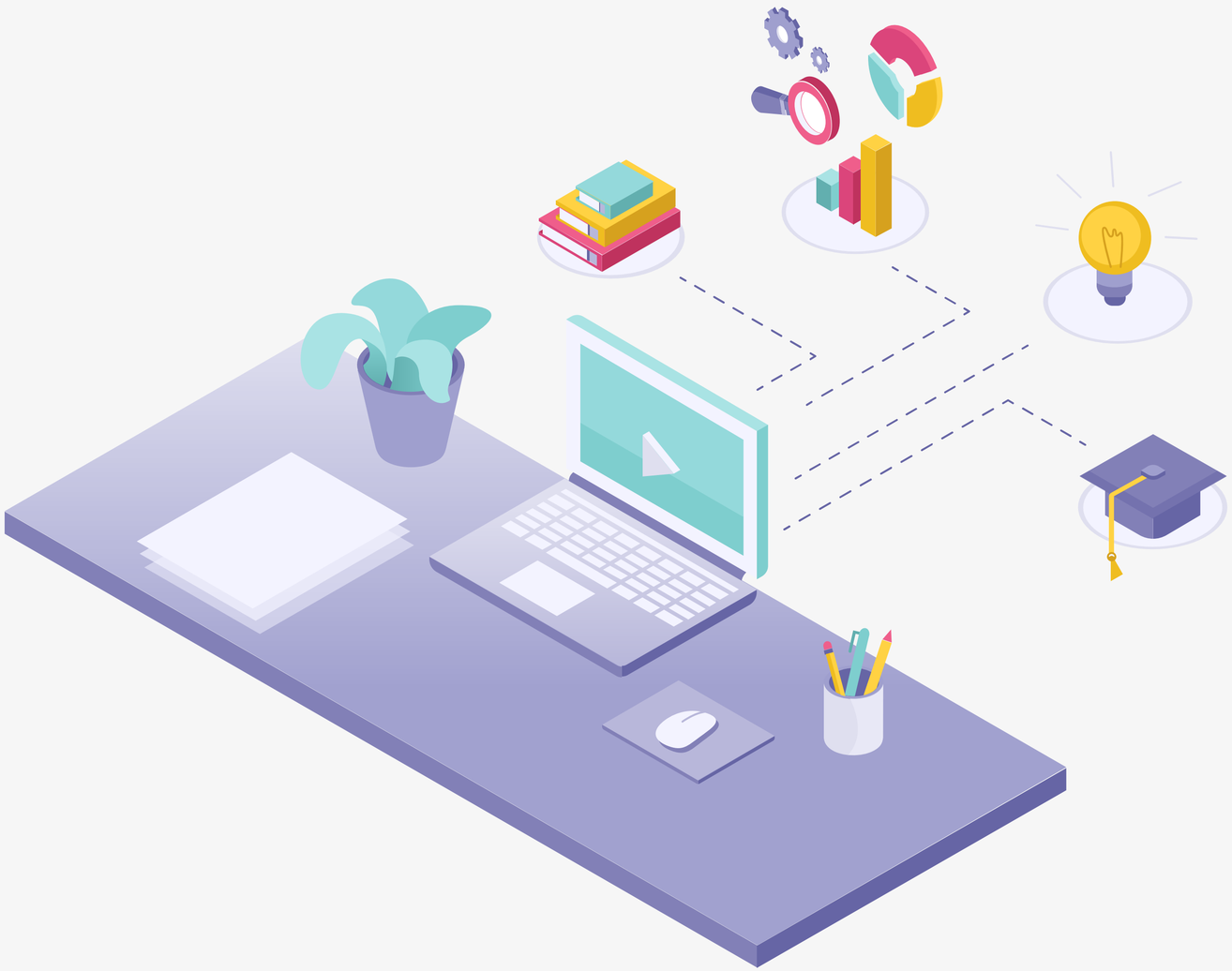
AWS CLI est préinstallé et pré-authentifié



AWS CloudShell

LeCloudFacile.com

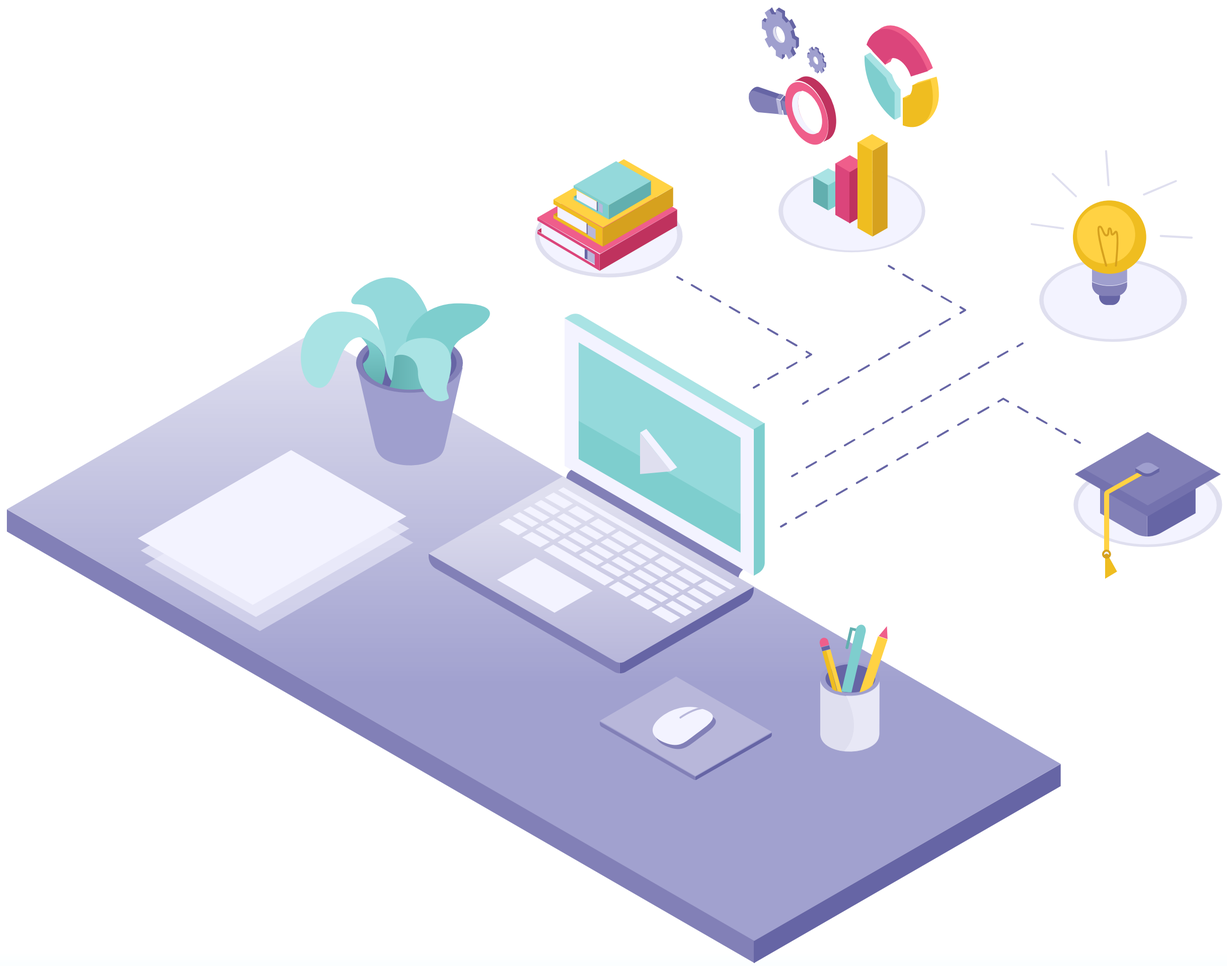
DEMO



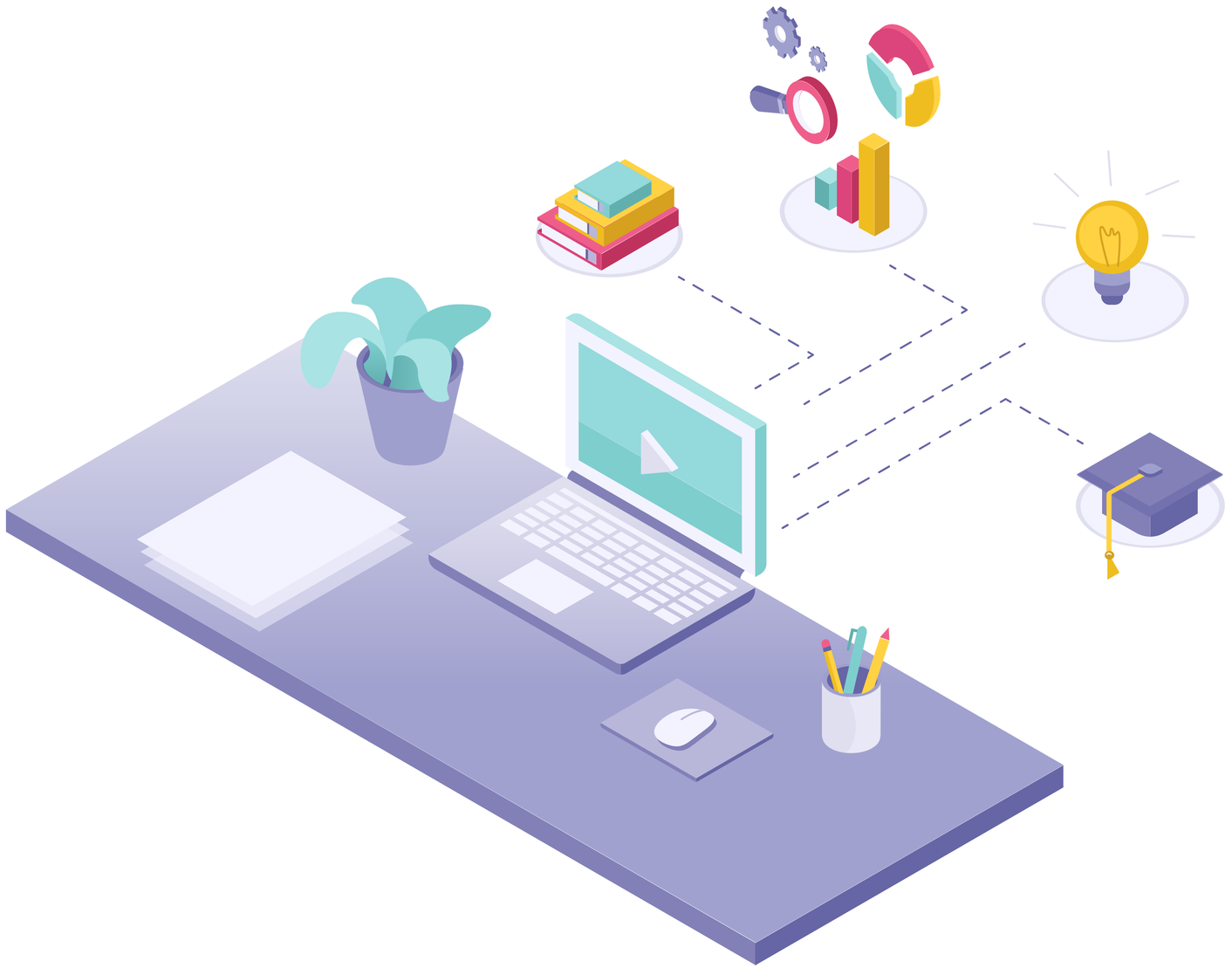
FIN DU MODULE

Module 14 : Déployer des applications

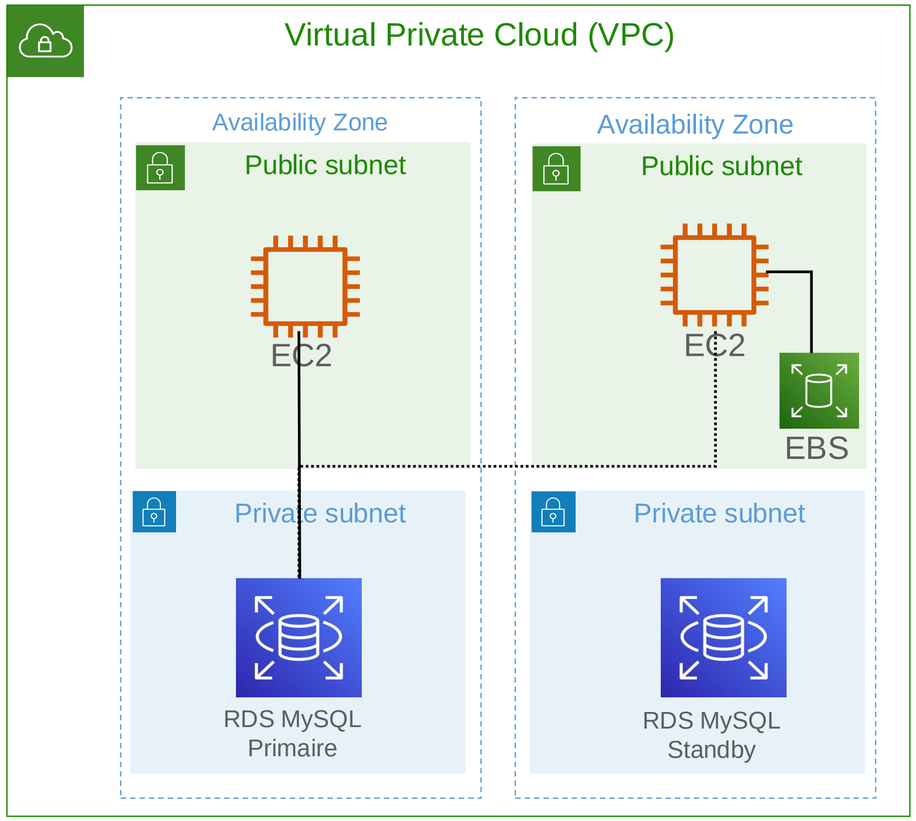
Todo



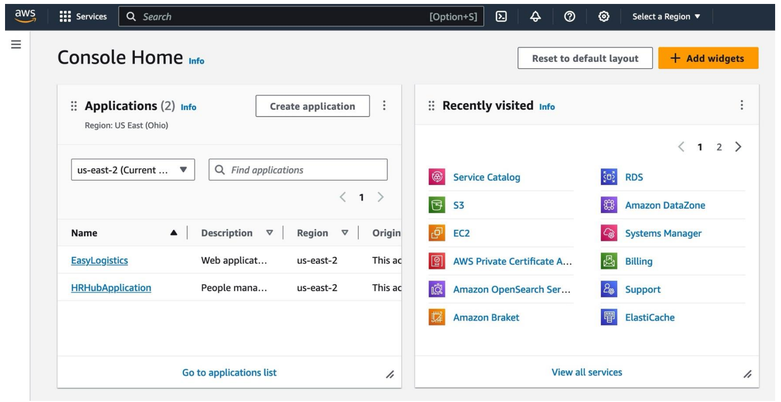
AWS CloudFormation



Déployer votre infrastructure AWS



Option 1



AWS Console

Option 2

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",

  "Description" : "AWS CloudFormation Sample Template ElasticBeanstalkSample: Configure and

  "Parameters" : {
    "KeyName" : {
      "Description" : "Name of an existing EC2 KeyPair to enable SSH access to the AWS Elast
      "Type" : "String"
    }
  },

  "Resources" : {
    "sampleApplication" : {
      "Type" : "AWS::ElasticBeanstalk::Application",
      "Properties" : {
        "Description" : "AWS Elastic Beanstalk Sample Application",
        "ApplicationVersions" : [{
          "VersionLabel" : "Initial Version",
          "Description" : "Version 1.0",
          "SourceBundle" : {
            "S3Bucket" : { "Fn::Join" : ["-", ["elasticbeanstalk-samples", { "Ref" : "AWS::R
            "S3Key" : "elasticbeanstalk-sampleapp.war"
          }
        }],
        "ConfigurationTemplates" : [{
          "TemplateName" : "DefaultConfiguration",
          "Description" : "Default Configuration Version 1.0 - with SSH access",
          "SolutionStackName" : "64bit Amazon Linux running Tomcat 7",
```

Infrastructure as Code (IaC)

AWS CloudFormation

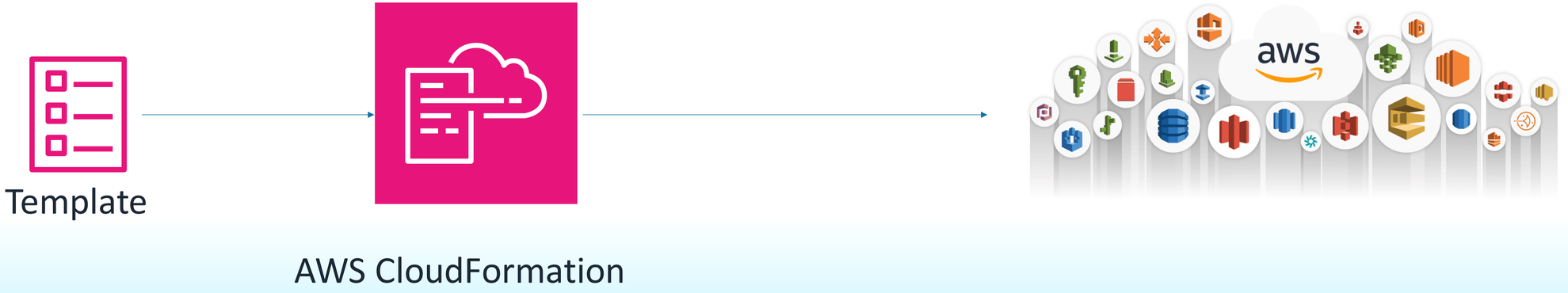


Service AWS pour faire de l'**Infrastructure as Code** (IaC)

Permet d'automatiser la création de vos ressources AWS

Modèle (*Template*) = Fichier (JSON ou YAML) qui liste les ressources à créer

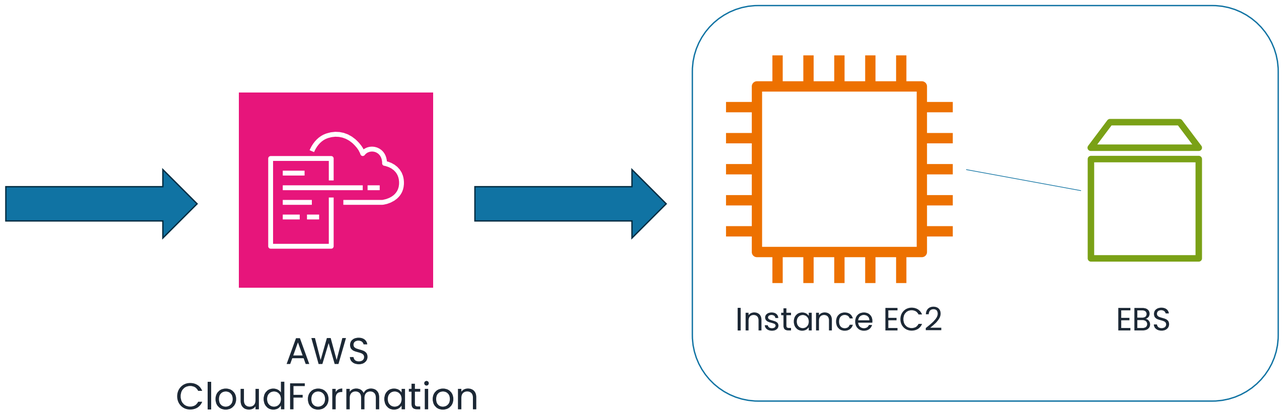
Avantages : *Déploiement automatisé, Versioning, Réplication rapide de votre infrastructure,...*



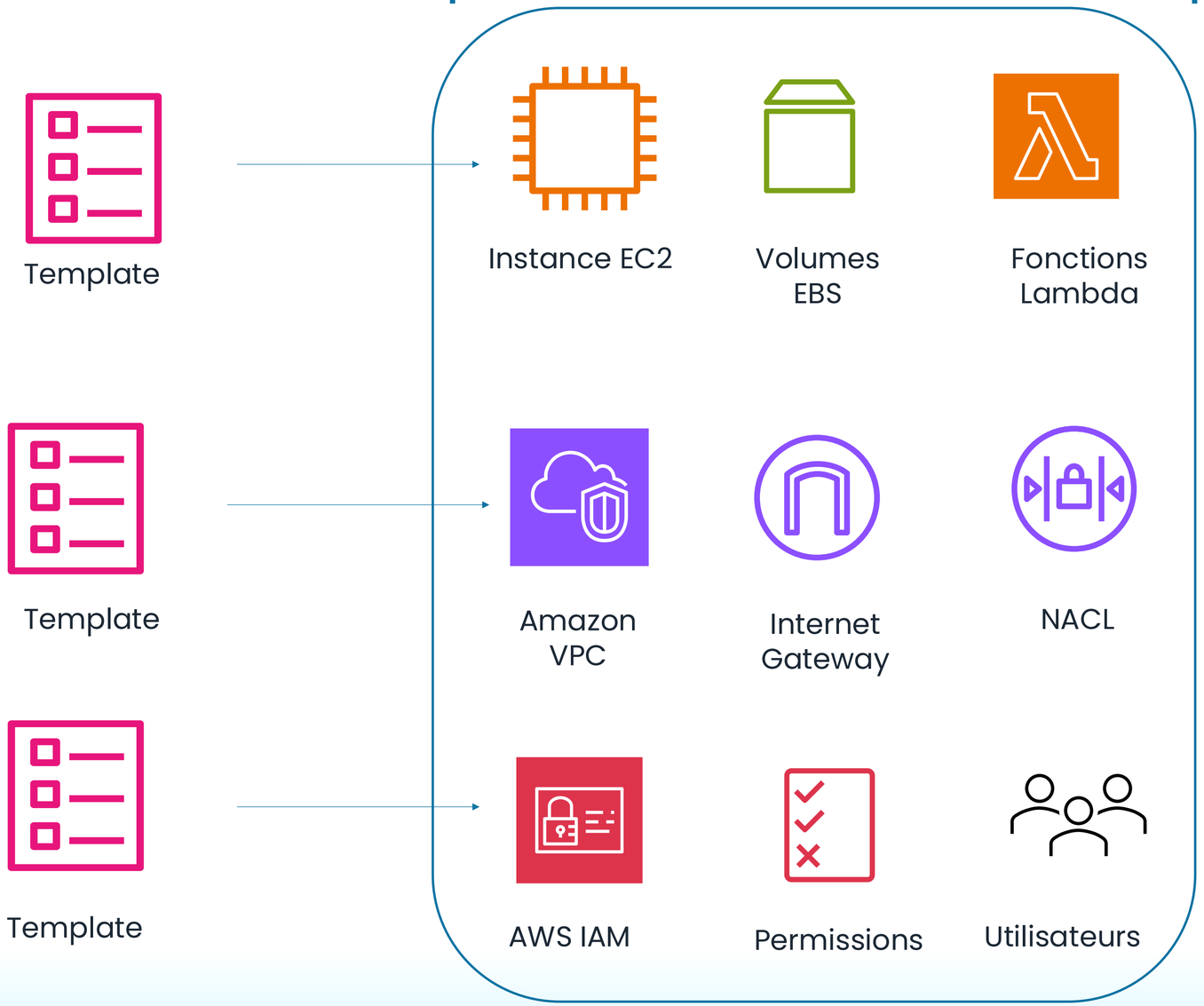
Exemple avec AWS CloudFormation : Déploiement d'une instance EC2

```
AWSTemplateFormatVersion: 2010-09-09
Description: A sample template
Resources:
  MyEC2Instance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: ami-0ff8a91507f77f867
      InstanceType: t2.micro
      KeyName: testkey
      BlockDeviceMappings:
        - DeviceName: /dev/sdm
          Ebs:
            VolumeType: io1
            Iops: 200
            DeleteOnTermination: false
            VolumeSize: 20
```

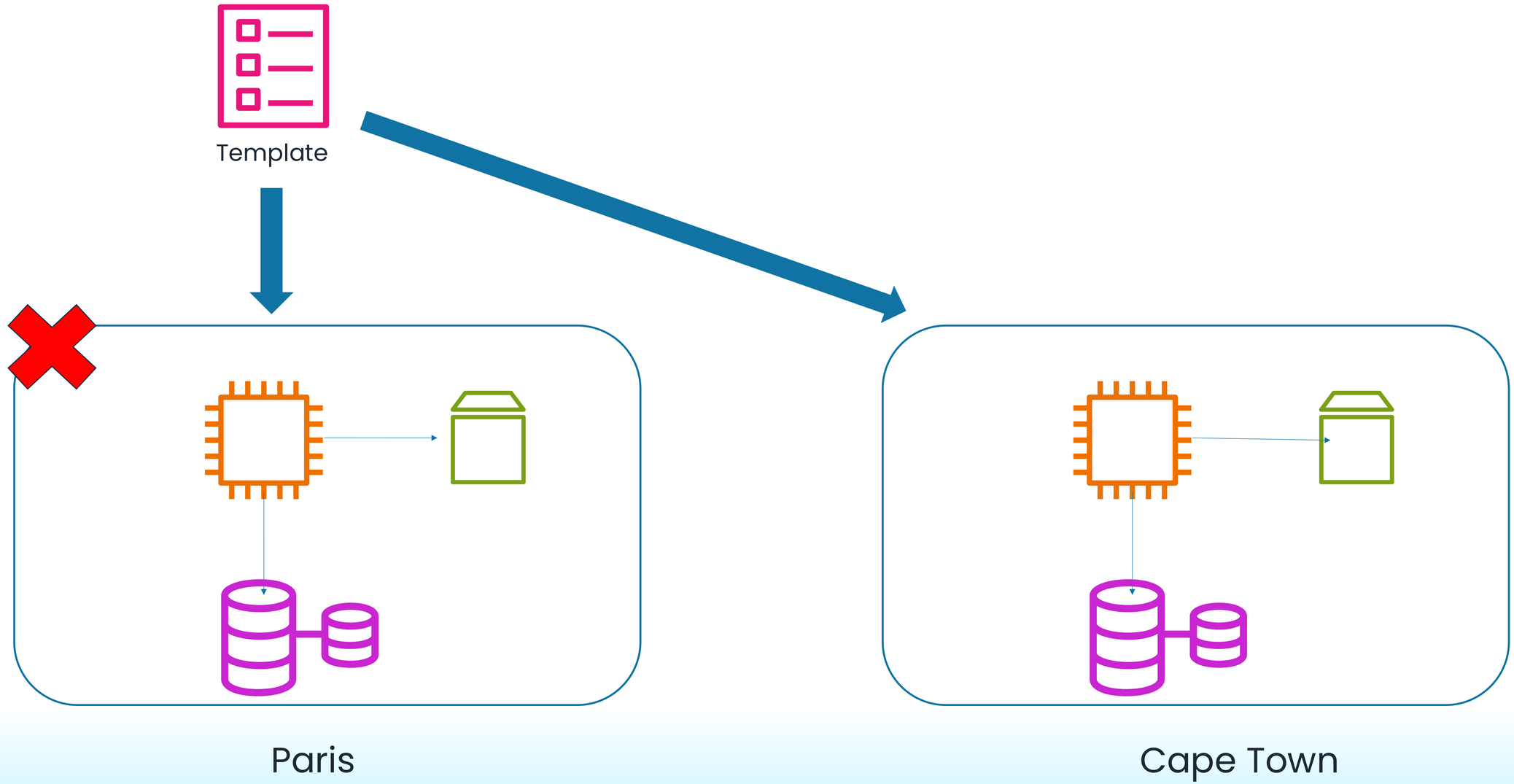
Template YAML



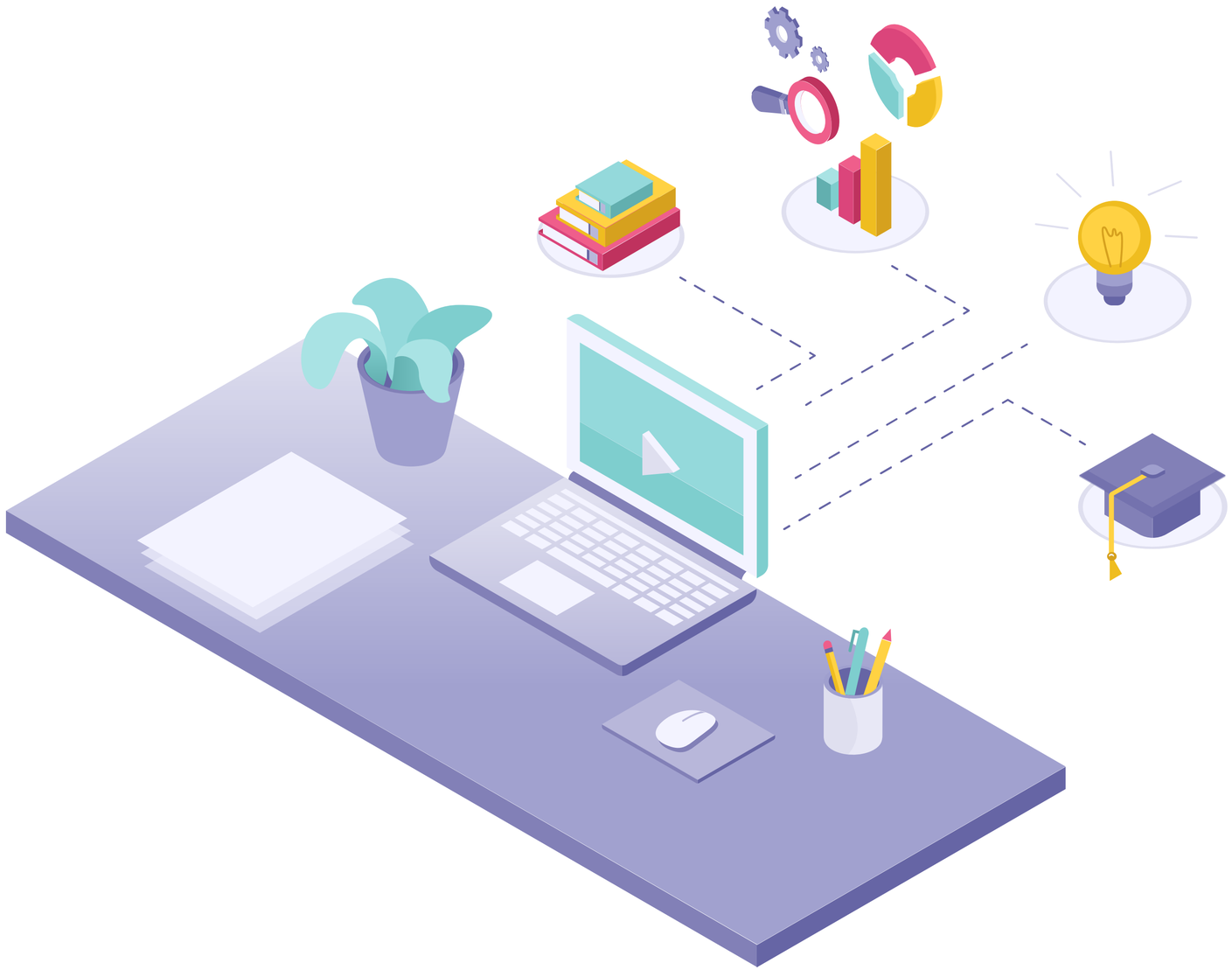
Exemple avec AWS CloudFormation : Déploiement infrastructure complète



Exemple avec AWS CloudFormation : Disaster Recovery



AWS CDK



AWS CDK (Cloud Development Kit)



Framework IaC plutôt orienté pour les **développeurs**

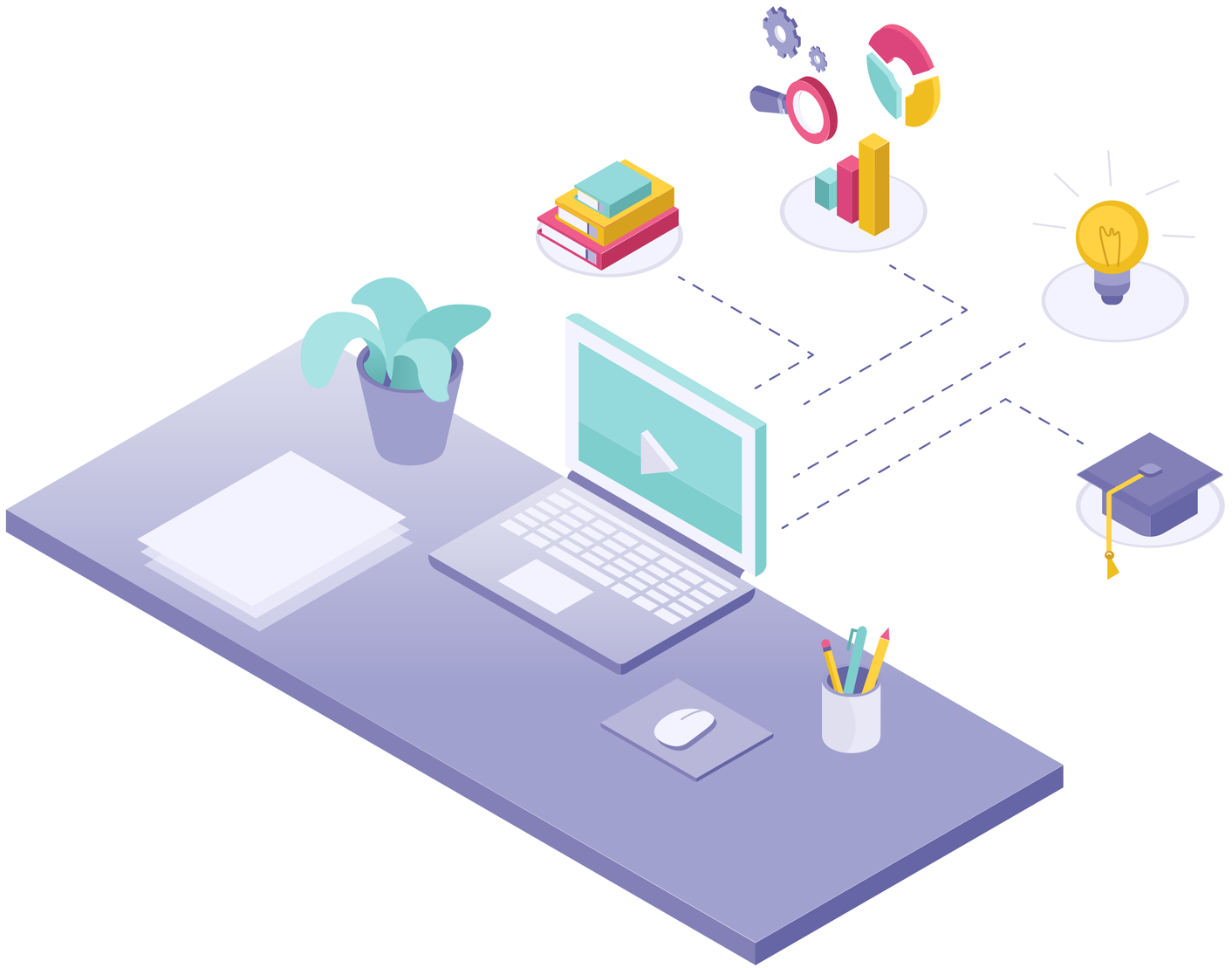
Permet de créer les ressources AWS à l'aide **langages de programmation**

Langages supportés : JavaScript, TypeScript, Python, Java, C#

Avantages de CDK

- Utilisation de **Constructs** de haut niveau basés sur des bonnes pratiques
- Utilisation d'un **langage de programmation familier** pour l'IaC
- S'appuie sur **CloudFormation**

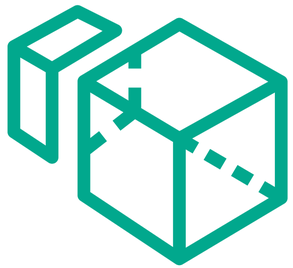
Amazon WorkSpaces



Amazon WorkSpaces

Fournit des **bureaux virtuels** hébergés -> VDI (Virtual Desktop Infrastructure)

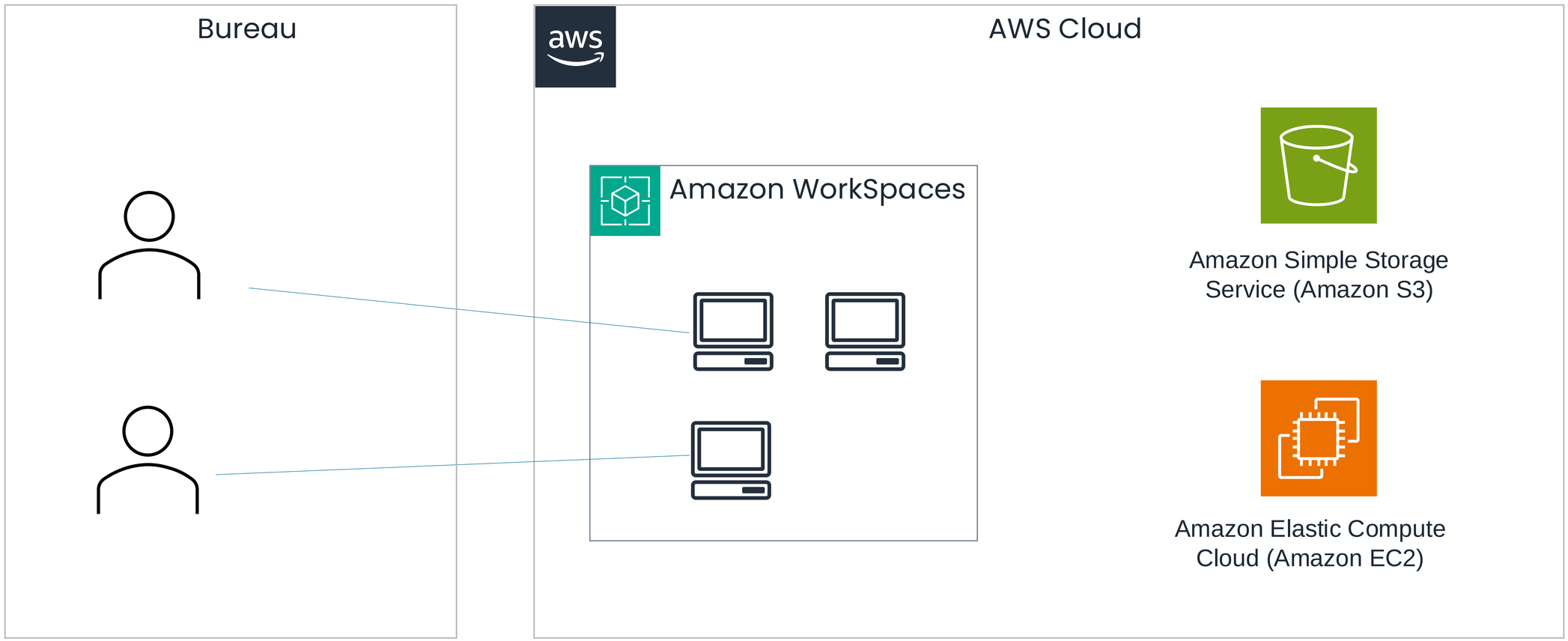
Permet à vos collaborateurs d'accéder à distance à **leur environnement de travail dans votre VPC AWS**

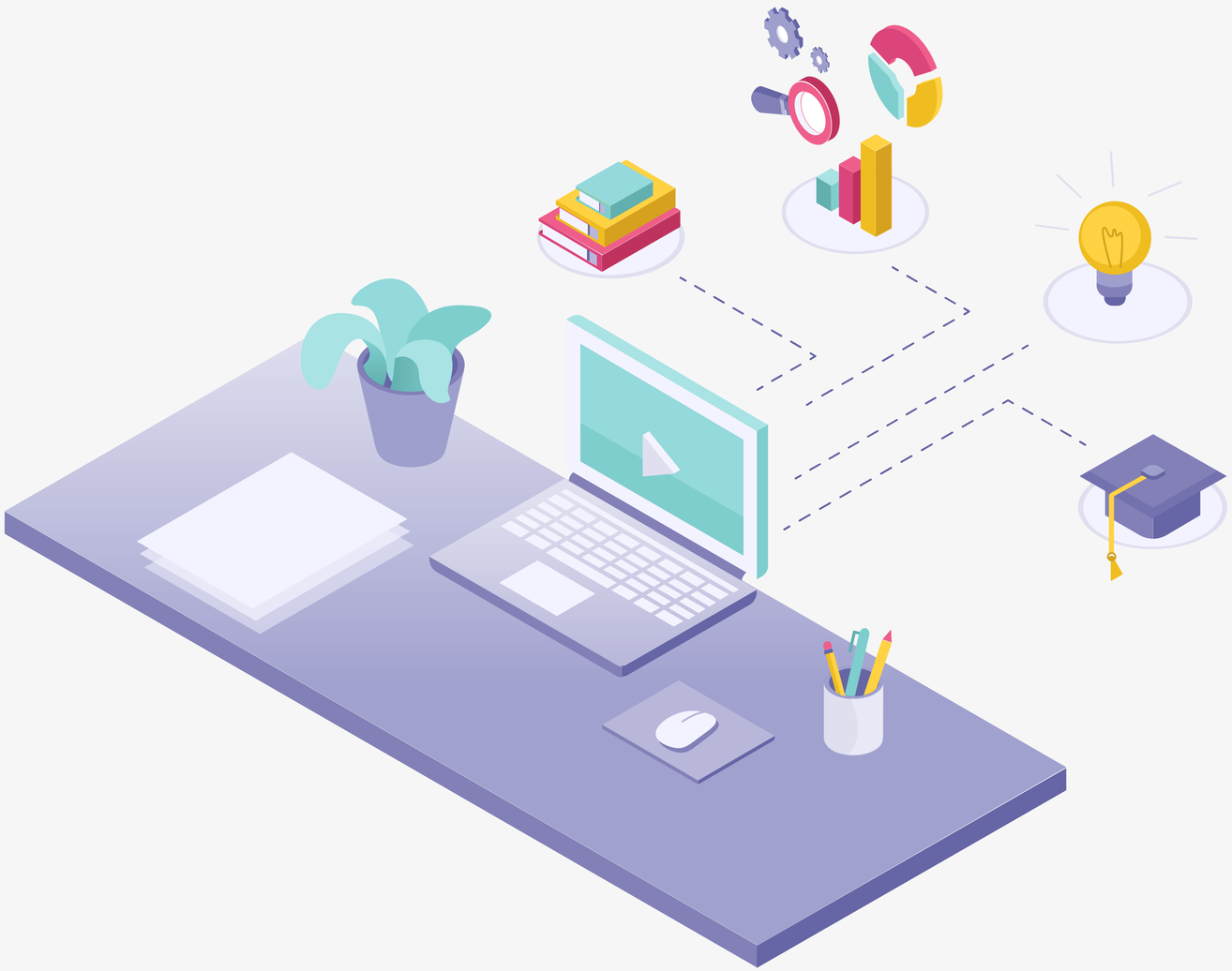


Fonctionnalités clés

- **Choix de l'OS** : Windows, Ubuntu, Amazon Linux
- Choix de la **configuration** matérielle (CPU,...)
- Intégration avec AWS Directory Service
- **Tarification** à l'heure ou au mois

Amazon WorkSpaces





FIN DU MODULE

Lab Créer 1 VPC avec AWS CloudFormation

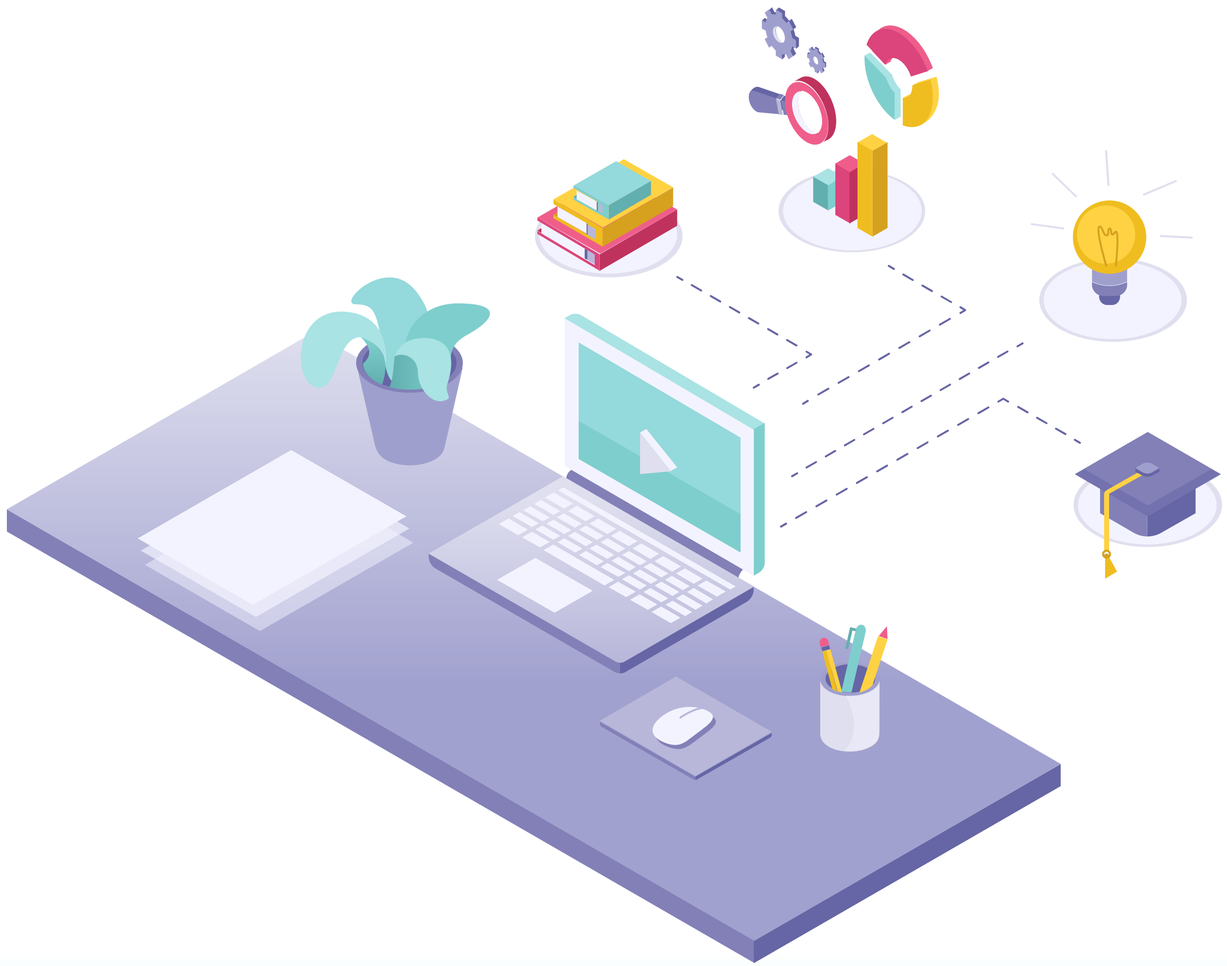




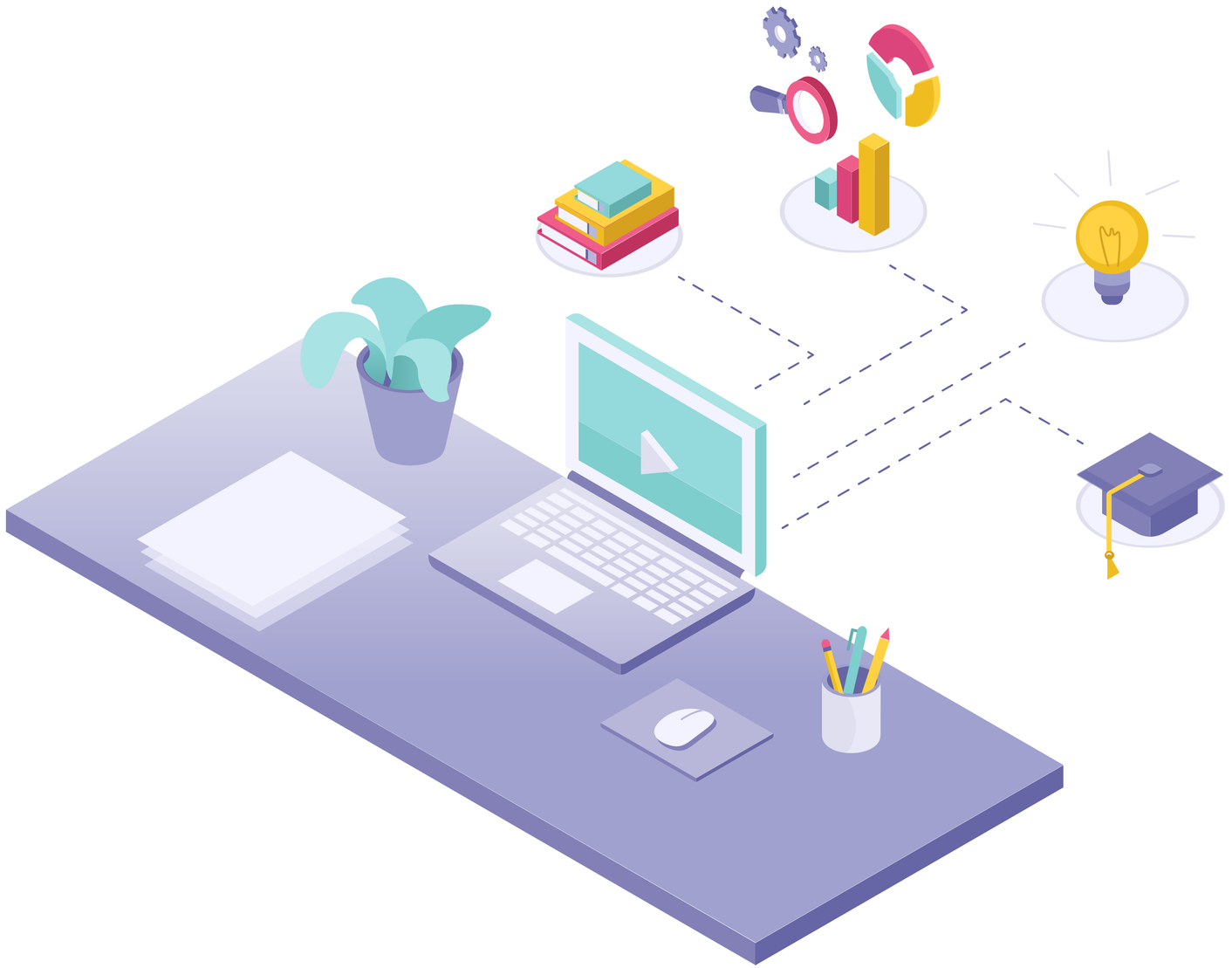
VPC avec 2 sous-réseaux publics et 2 privés

Module 15 : Surveillance & Analyse

Obtenez des informations et améliorez les performances de vos applications et de votre infrastructure



Amazon CloudWatch



Amazon CloudWatch



Services AWS

Agent CloudWatch

Vos Applications

Amazon CloudWatch

Métriques

Alarmes

Logs

Evénements

Amazon SNS

EC2 Auto Scaling

Amazon CloudWatch

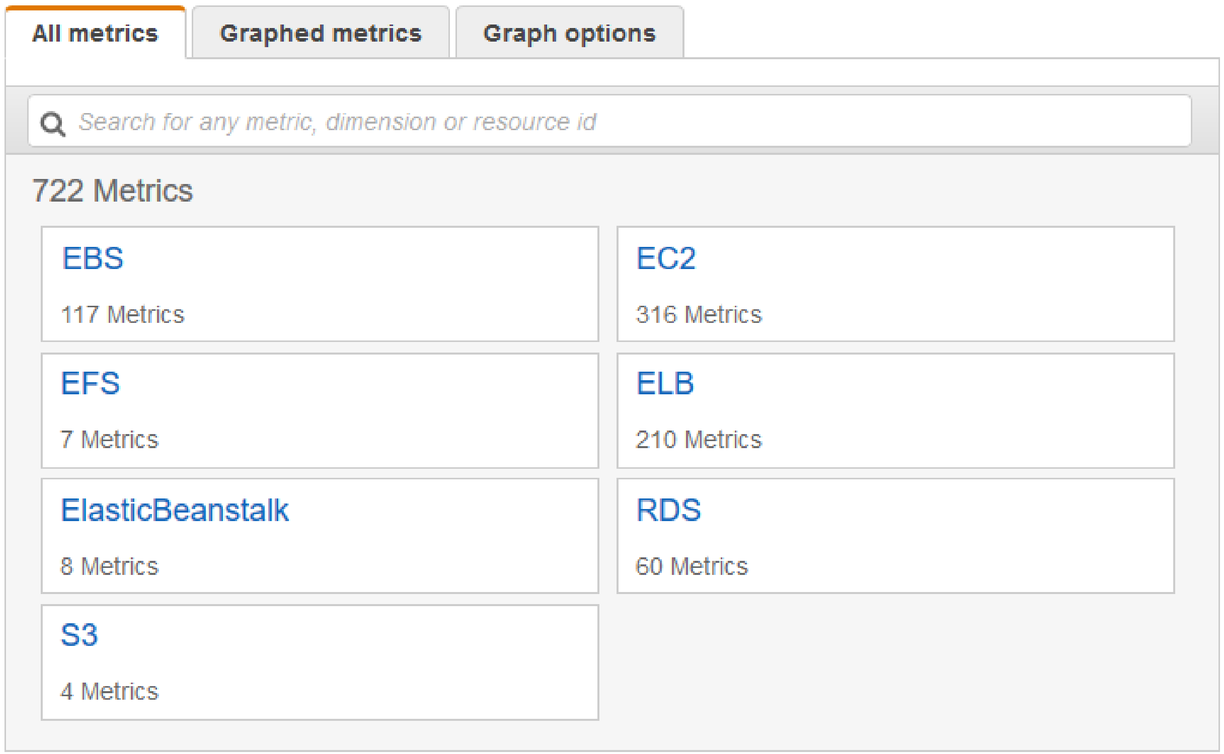


Service de supervision de vos ressources AWS

Fournit

- ***Métriques*** (cpu, réseau, disque,..) sur l'utilisation des services AWS
  - -> *Données sur les performances de vos systèmes*
- ***Alarmes*** *(Alertes)***.** Exp: Alarme si CPU > 70% pendant 5 minutes...
  - -> *Permet de surveiller une métrique CloudWatch*
- ***Centralisation des logs***
  - -> *Permet de centraliser vos fichiers de logs*

Métriques

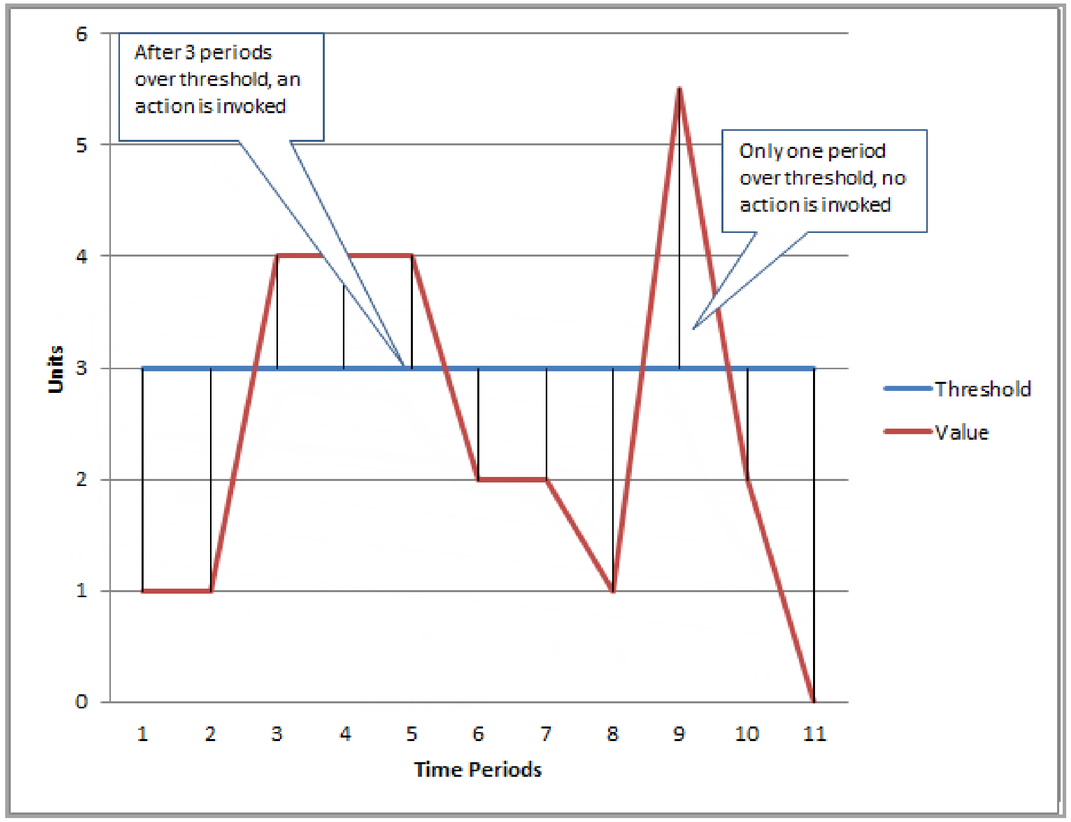


Représente un ensemble de points de données d'une **variable à surveiller**

Exemple

- EC2 : NetworkOut, NetworkIn, CPU Utilization
- EBS : Disk Read /Writes
- ELB : RequestCount, TargetResponseTime

Alarmes



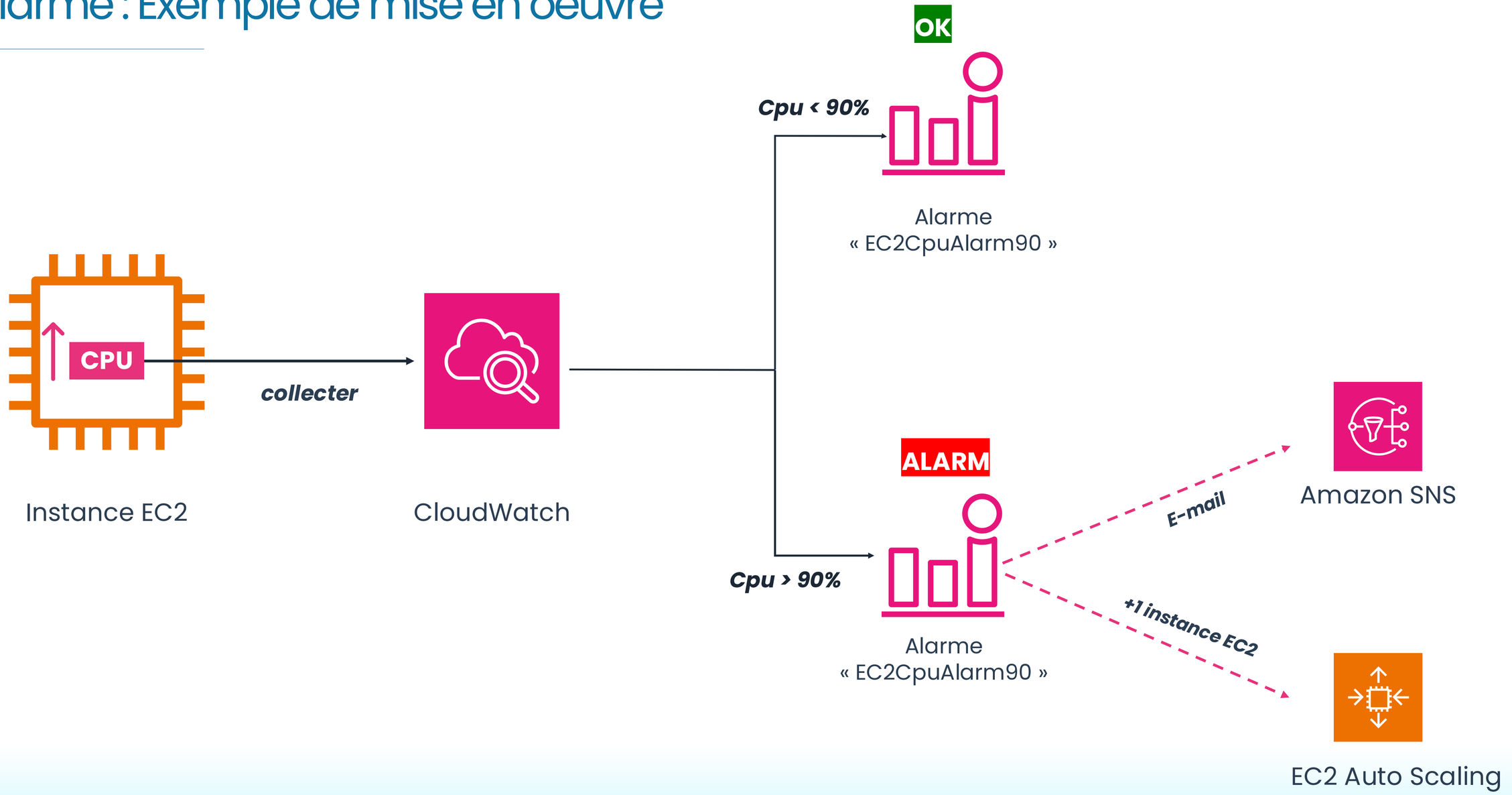
Surveillent les **métriques** CloudWatch

Permettent de déclencher des **notifications ou actions**

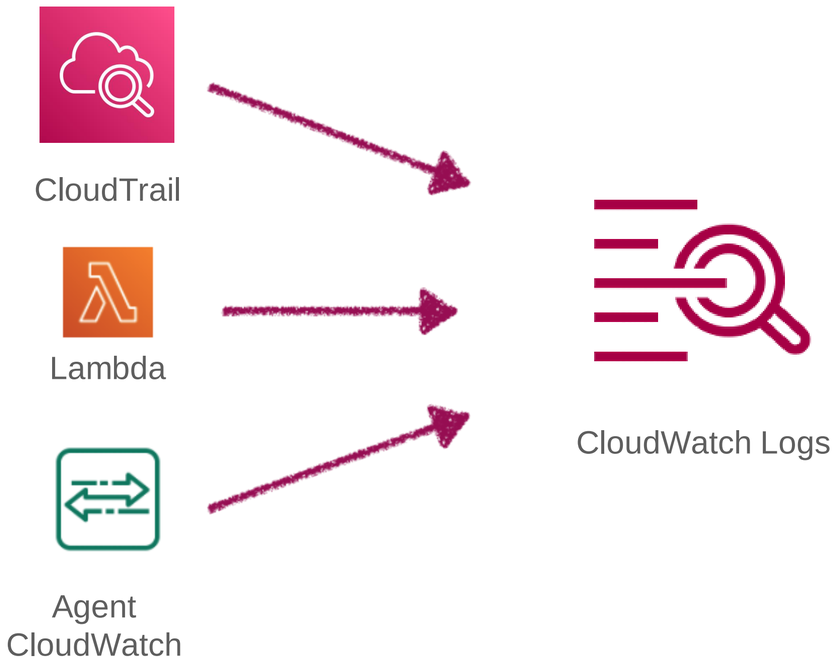
Statuts:

- INSUFFICIENT_DATA : Données insuffisantes.
  - Exp : nouvelle alarme
- OK : La métrique est dans le seuil défini/attendu.
  - Exp : CPUUtilization < 90%
- ALARM : La métrique a dépassé le seuil défini
  - Exp : CPUUtilization > 90% pendant 2 x 5 minutes

Alarme : Exemple de mise en oeuvre



CloudWatch Logs

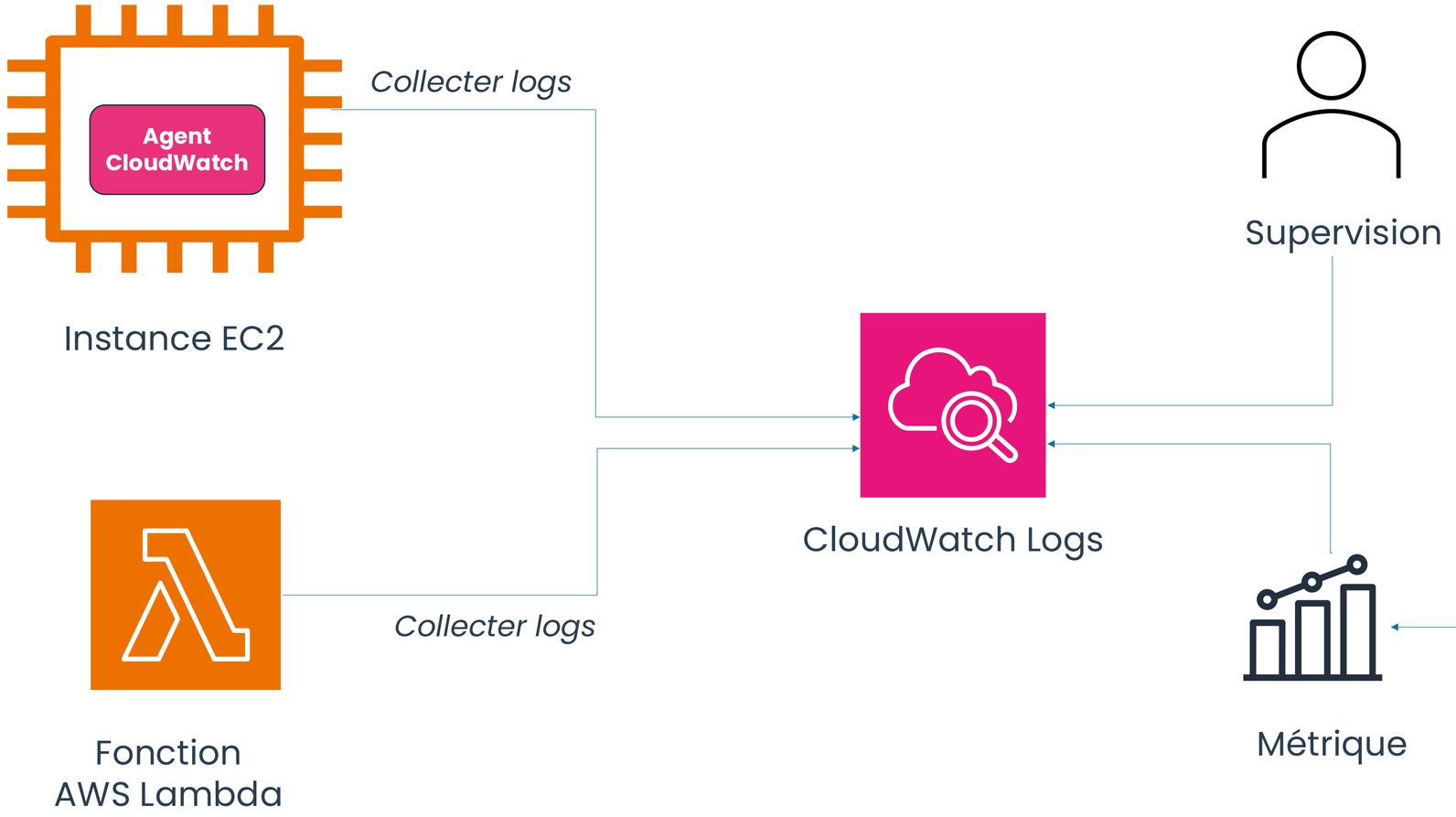


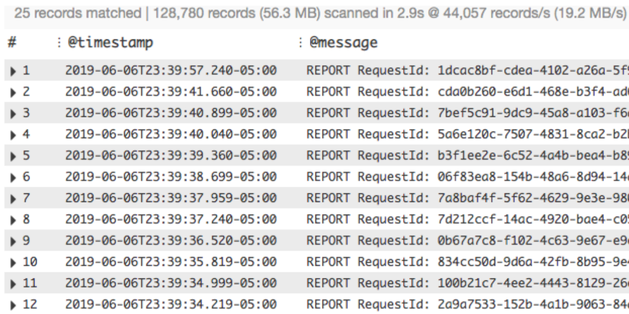
Permet la centralisation des **logs** de vos applications et services AWS

Vous pouvez :

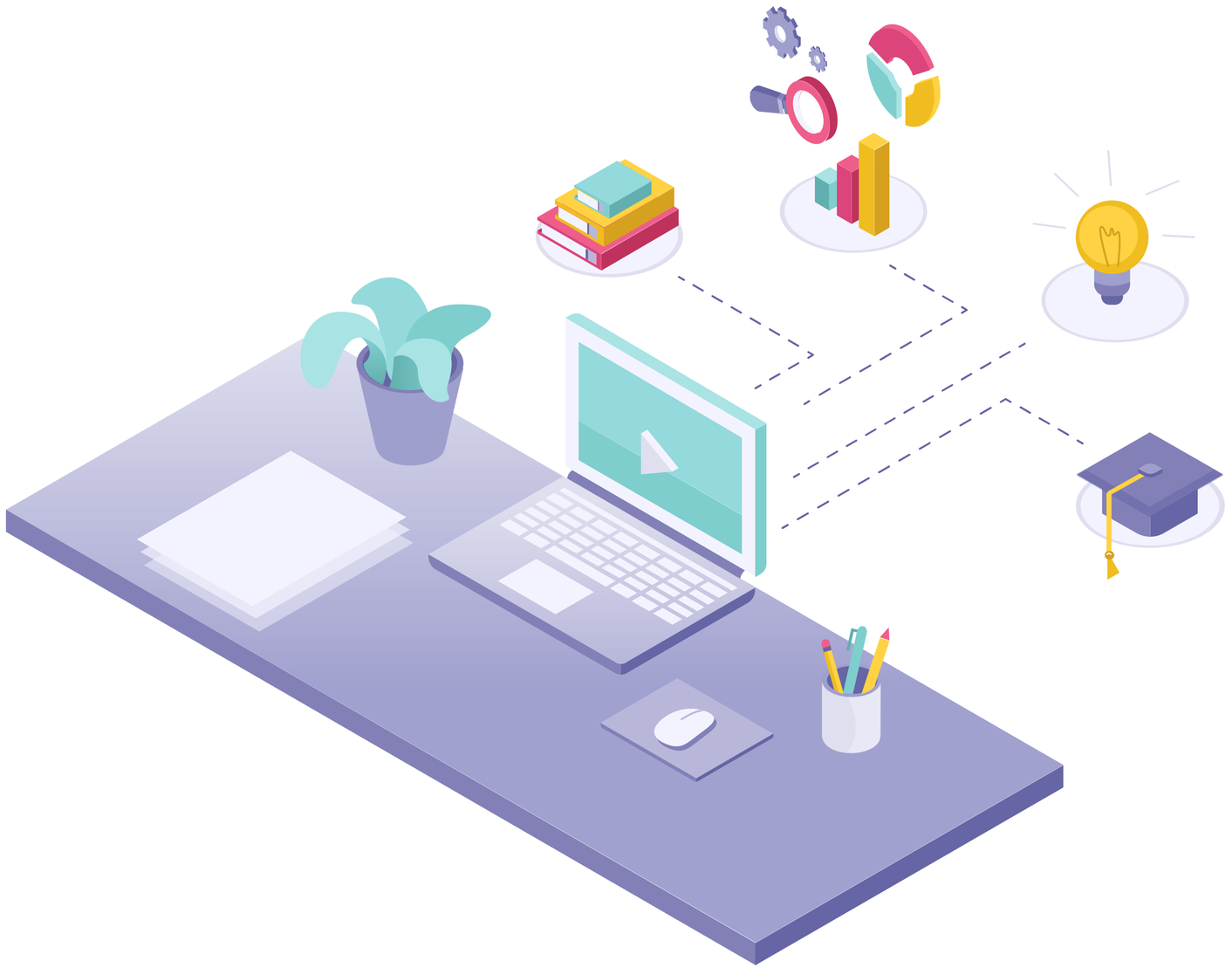
- Collecter les logs des services AWS : Lambda, ECS, Route 53,…
- Collecter les logs de vos instances Amazon EC2
- Créer des métriques et des alarmes basées sur les logs.
    - Exp: Nombre d'occurrence du message « ERROR » dans les logs

CloudWatch Logs : Exemple de mise en oeuvre





AWS CloudTrail



AWS CloudTrail



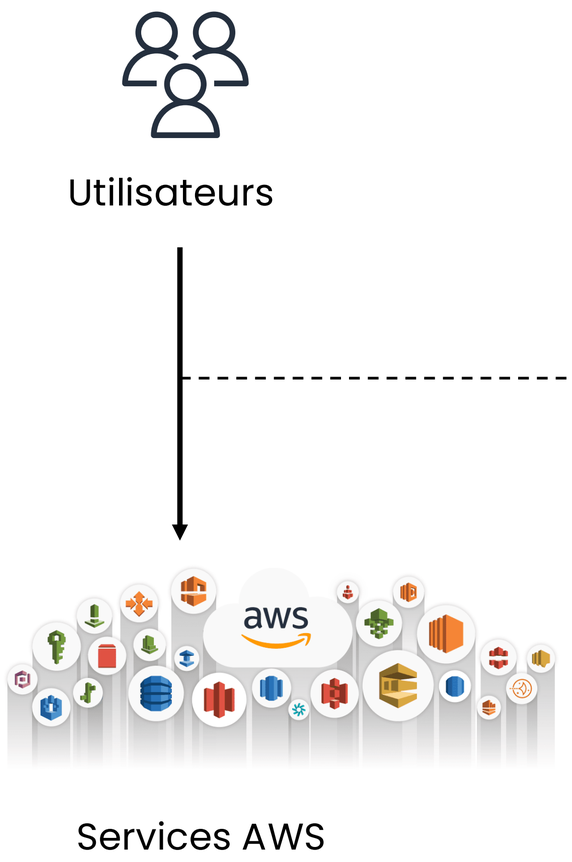
Trace les activités dans votre compte AWS

Contient **l'historique de tous les appels APIs** sur vos ressources AWS.

Permet de répondre à des questions telles que :

- *« Qui a arrêté telle instance EC2 »*
- *« Qui a changé tel Groupe de sécurité »*
- *« Qui a modifié tel bucket S3 »*

AWS CloudTrail



AWS CloudTrail

Cas d'usage

- Permet l'audit et la surveillance de la sécurité
- Suit l'activité des utilisateurs, rôles, service AWS
- Aide à prouver la conformité

Evénement

- Enregistrement d'une activité dans un compte AWS
- Activité API (AWS SDK, CLI,..) ou non API (console)

Console

- Affichage des événements récents (90 derniers jours)

AWS CloudTrail

Exemple d’évènement Cloudtrail


```
{"Records": [{
   "eventVersion": "1.0",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "EX_PRINCIPAL_ID",
      "arn": "arn:aws:iam::123456789012:user/Alice",
      "accessKeyId": "EXAMPLE_KEY_ID",
      "accountId": "123456789012",
      "userName": "Alice"
   },
   "eventTime": "2014-03-06T21:22:54Z",
   "eventSource": "ec2.amazonaws.com",
   "eventName": "StartInstances",
   "awsRegion": "us-east-2",
   "sourceIPAddress": "205.251.233.176",
   "userAgent": "ec2-api-tools 1.6.12.2",
   "requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]}},
   "responseElements": {"instancesSet": {"items": [{
      "instanceId": "i-ebeaf9e2",
      "currentState": {
         "code": 0,
         "name": "pending"
      },
      "previousState": {
         "code": 80,
         "name": "stopped"
      }
   }]}}
}]}
```

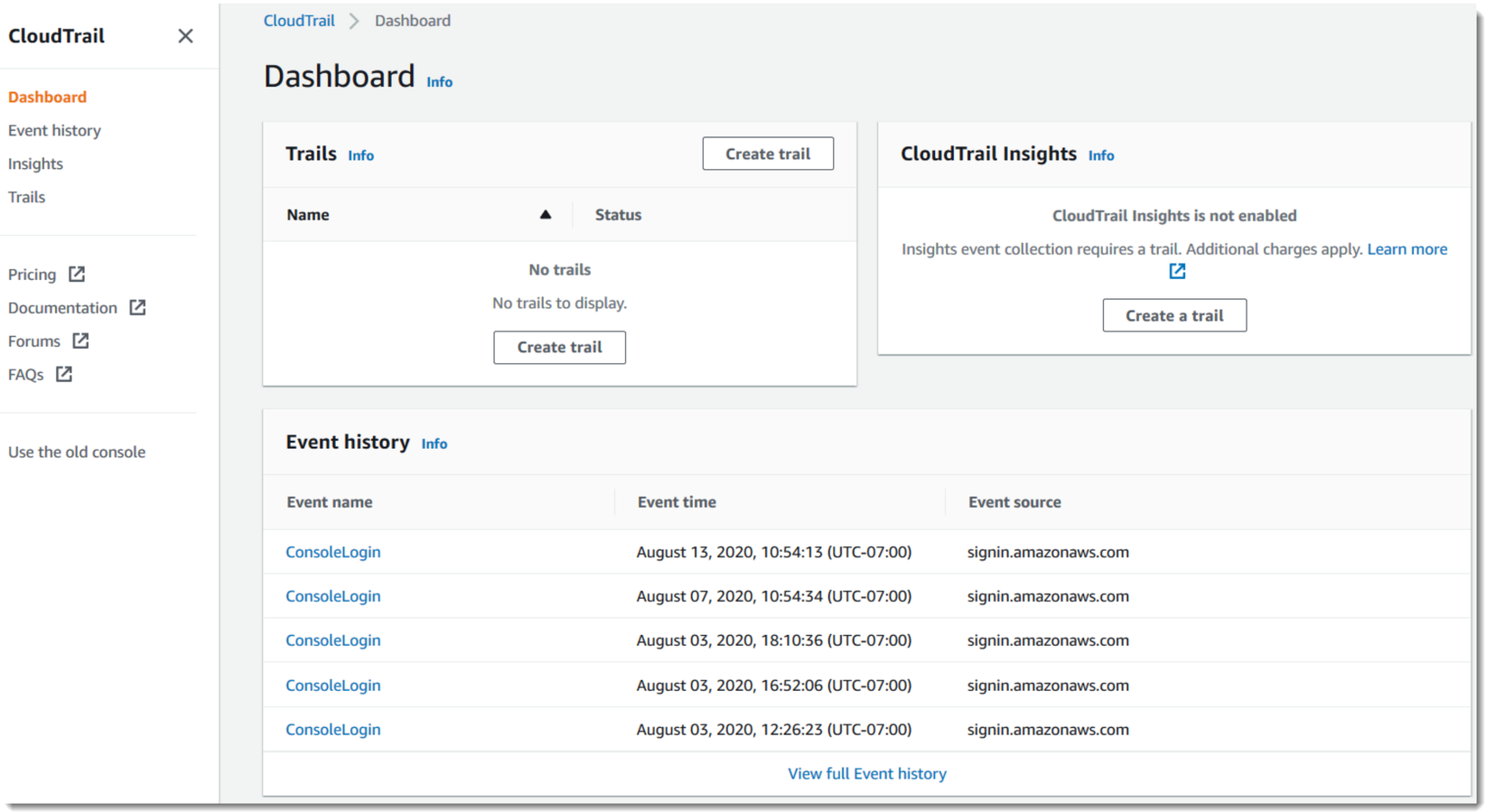

Un utilisateur IAM nommé Alice

a executé la commande ec2-start-instances

pour démarrer l'instance i-ebeaf9e2

dans la région us-east-2

Console AWS CloudTrail



Cloudtrail est activé par défaut dans votre compte AWS

La Console (Event History) affiche les évènements des 90 derniers jours

Journal de suivi (*Trail*)

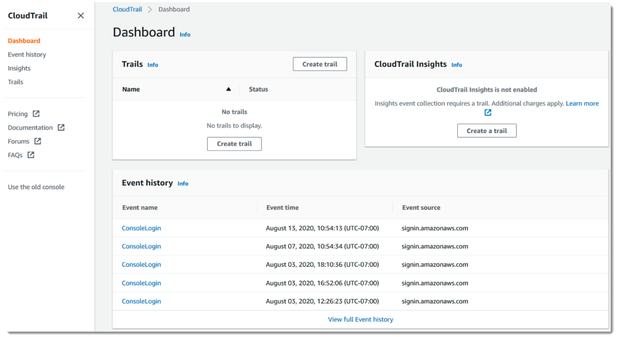


Services AWS

Activités



AWS CloudTrail



Console CloudTrail
(retention : 90 jours)



Journal de suivi
(Trail)



Amazon S3



Amazon EventBridge

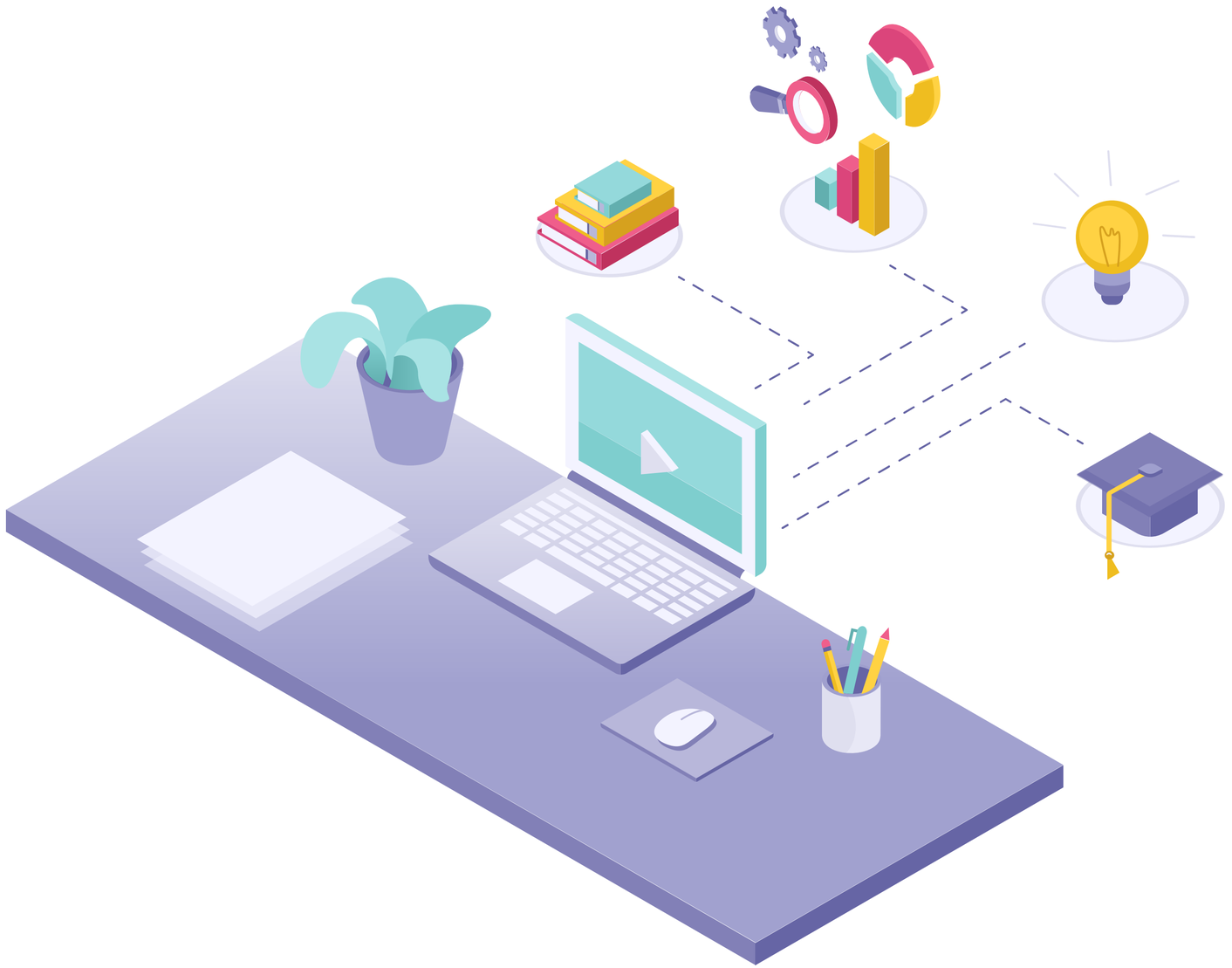


CloudWatch Logs

Quiz AWS CloudTrail ou Amazon CloudWatch

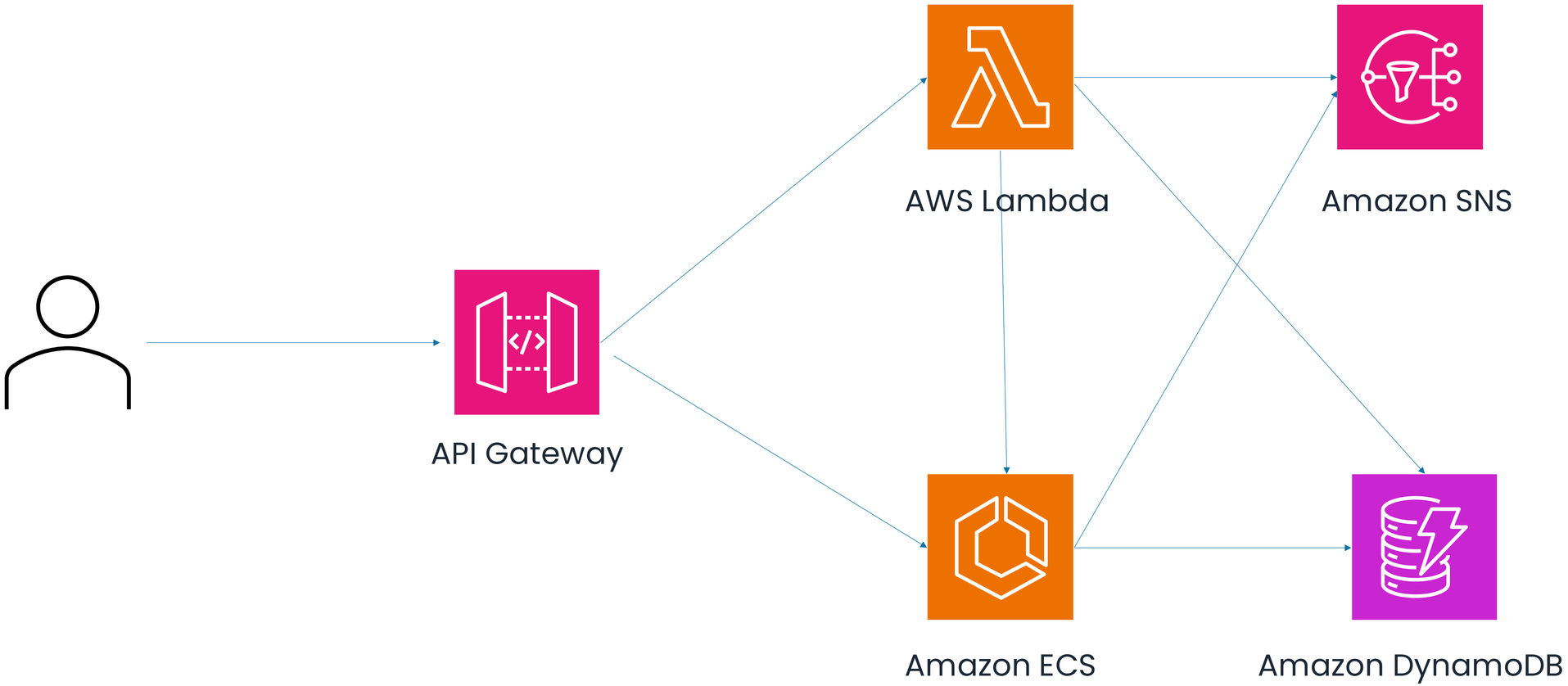
Savoir qui a modifié un groupe de sécurité	AWS CloudTrail
Être notifié lorsque le Root User se connecte	AWS CloudTrail
Visualiser les métriques des volumes EBS	Amazon CloudWatch
Envoyer une notification lorsque le CPU de mon EC2 > 70%	Amazon CloudWatch
Rajouter automatiquement des EC2 lorsque la charge augmente	Amazon CloudWatch
Collecter et visualiser les logs des instances EC2	Amazon CloudWatch

AWS X-Ray

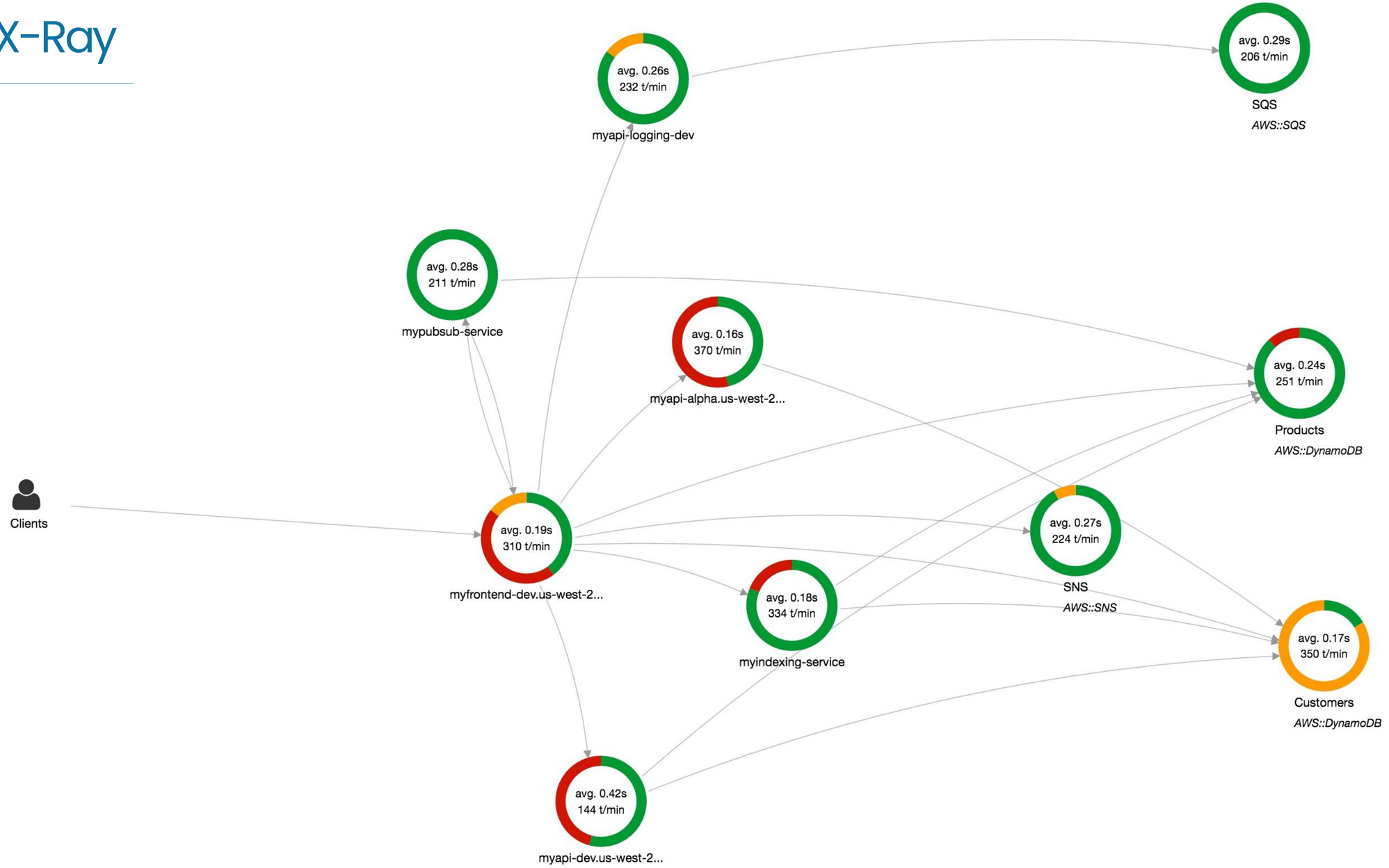


LeCloudFacile.com

AWS X-Ray



AWS X-Ray


avg. 0.26s
232 t/min
myapi-logging-dev
avg. 0.29s
206 t/min
SQS
AWS::SQS
avg. 0.28s
211 t/min
mypubsub-service
avg. 0.16s
370 t/min
myapi-alpha.us-west-2...
avg. 0.24s
251 t/min
Products
AWS::DynamoDB
Clients
avg. 0.19s
310 t/min
myfrontend-dev.us-west-2...
avg. 0.27s
224 t/min
SNS
AWS::SNS
avg. 0.18s
334 t/min
myindexing-service
avg. 0.17s
350 t/min
Customers
AWS::DynamoDB
avg. 0.42s
144 t/min
myapi-dev.us-west-2...

AWS X-Ray



Service de surveillance et de diagnostic **distribué**

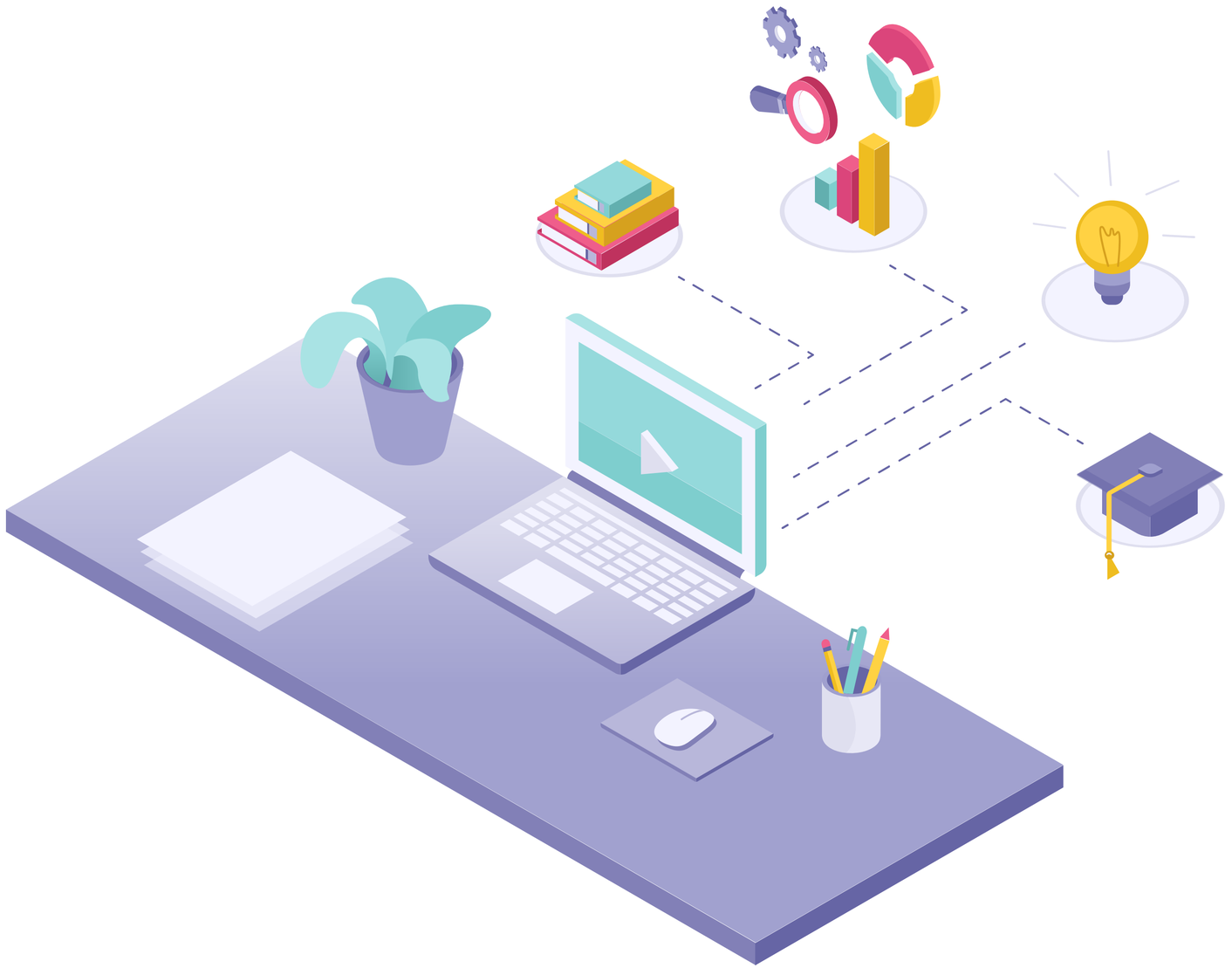
Permet aux développeurs de déboguer les applications basées sur des ***microservices***

Intégration *avec les services AWS : AWS Lambda, Amazon ECS, DynamoDB, Amazon SQS,...*

Fonctionnalités clés

- *Suivi des requêtes distribuées*
- *Cartographie visuelle des services*
- *Analyses des performances*
- *Détection des erreurs*

Health Dashboard



AWS Health Dashboard



Fournit des alertes/notifications sur des évènements (incidents,…)

Intégration avec Amazon EventBridge pour traiter automatiquement les notifications

Service Health Dashboard

Montre les évènements publics

Montre l'état général des services AWS

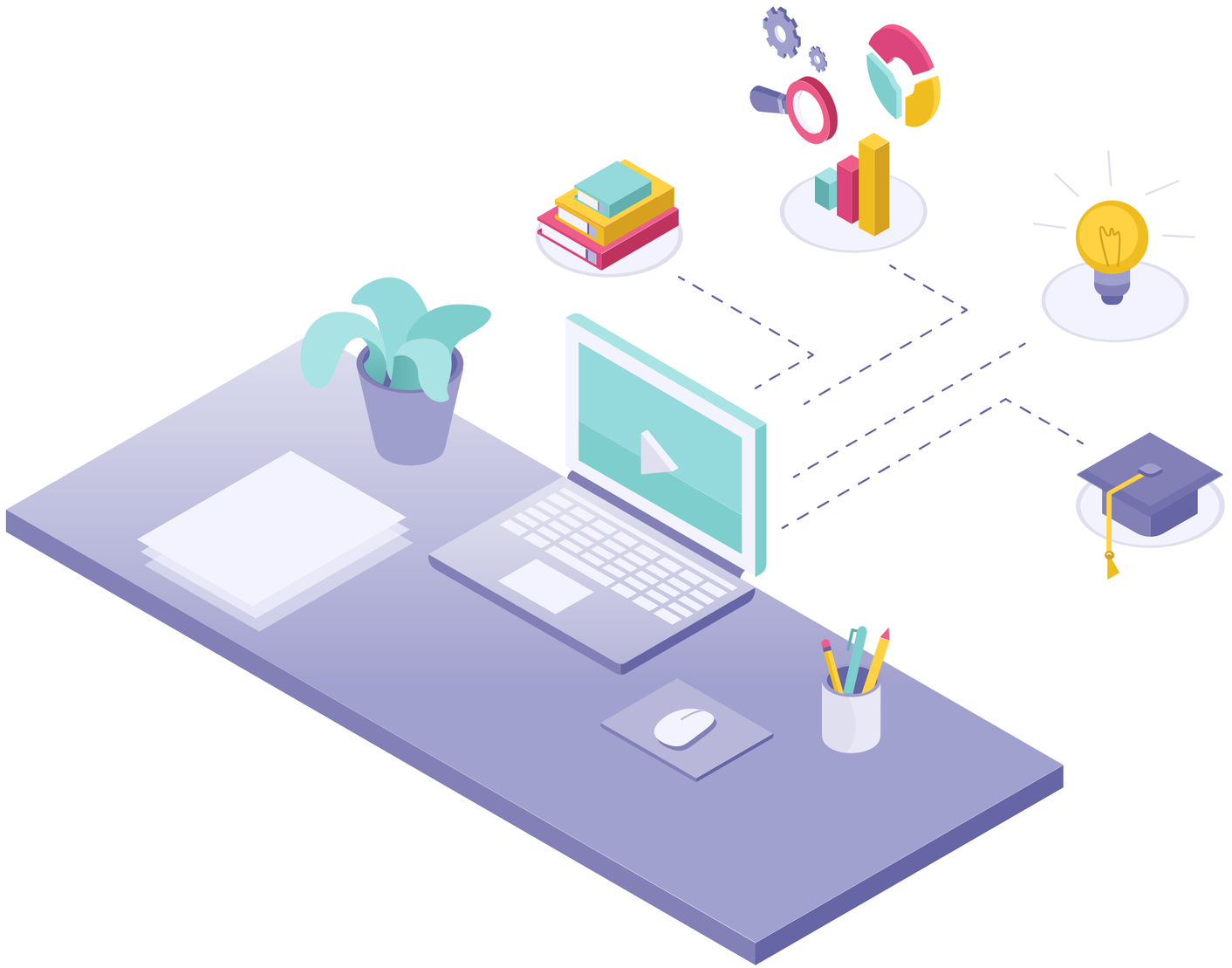
Exemple : Incident Amazon S3 dans une région AWS

Personal Health Dashboard

Montre les évènements spécifiques à votre environnement AWS

Fournit des alertes/conseils pour les évènements AWS susceptibles d'affecter votre environnement

AWS Trusted Advisor



AWS Trusted Advisor

Inspecte votre environnement AWS et émet des recommandations

Contrôles dans **6 catégories : Coûts, Performance, Sécurité, Tolérance aux pannes, Service limits, Excellence opérationnelle**

Les recommandations accessibles dépendent de votre **niveau de support AWS**



AWS Trusted Advisor

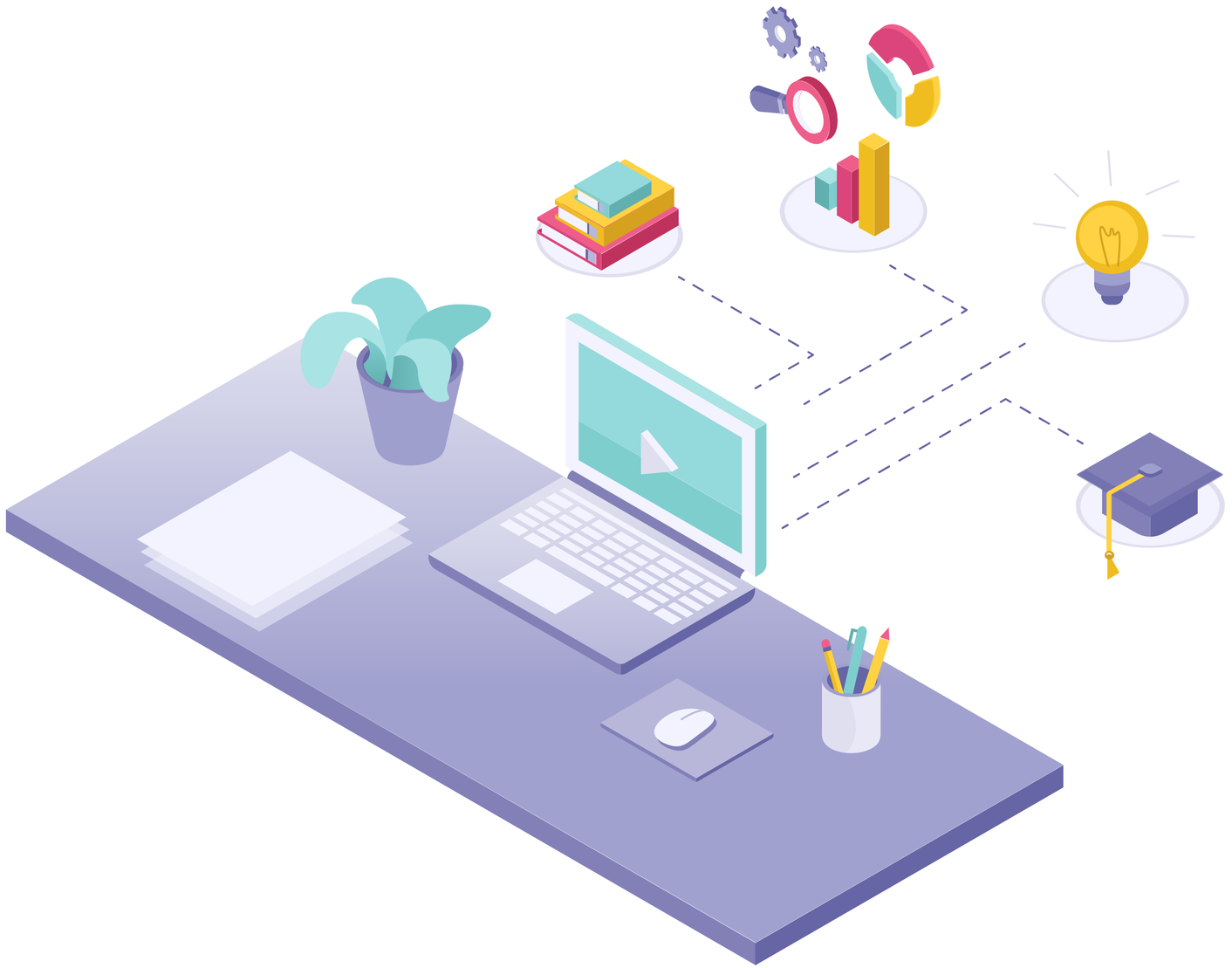
Clients avec **AWS Support Basic/Developper** -> 6 vérifications de **sécurité** + 50 **vérifications de limites de services**

Clients avec **AWS Support Business / Enterprise / Enterprise On-ramp** ->

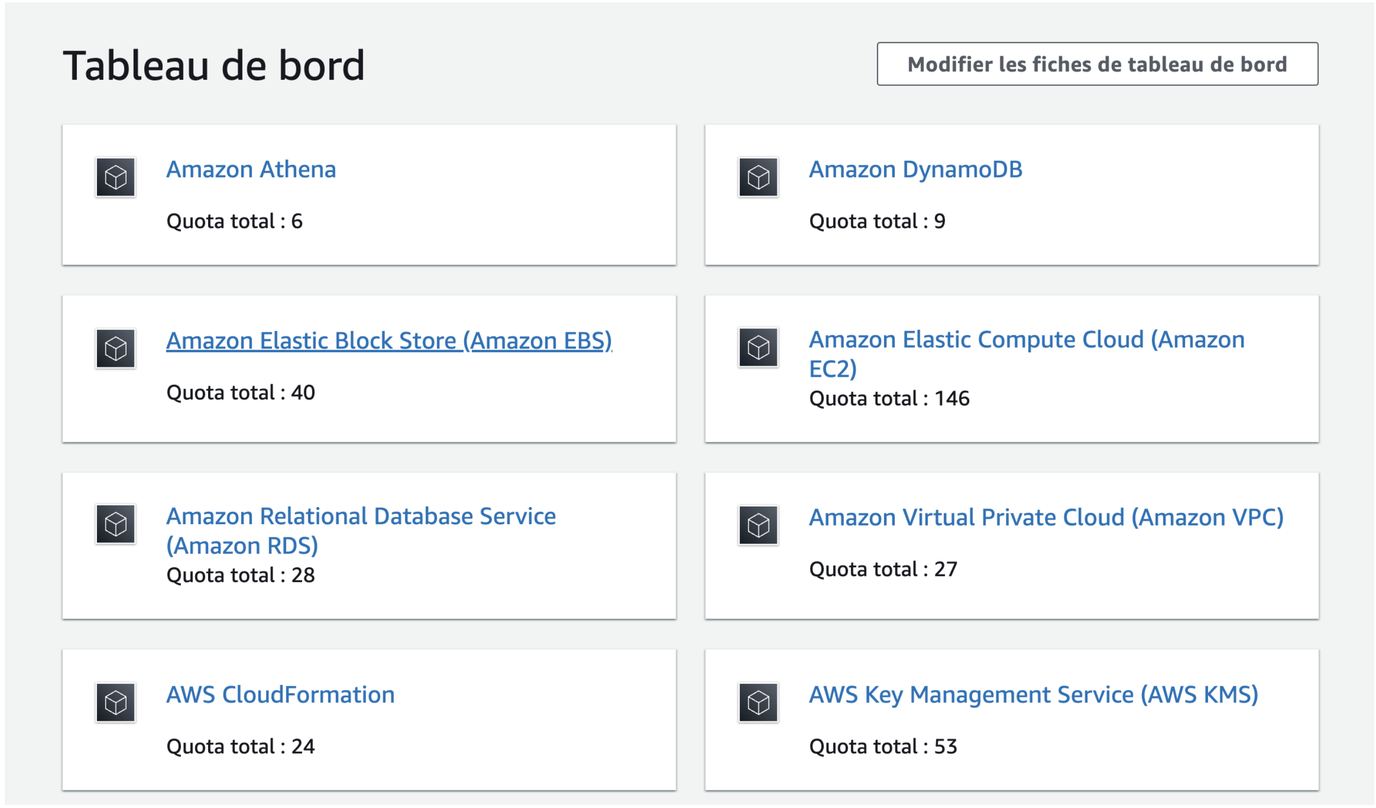
+115 vérifications Trusted Advisor

- **Sécurité**
- **Service limits**
- ***Optimisation des coûts***
- **Tolérance aux pannes**
- **Performances**
- **Excellence opérationnelle**

AWS Service quotas



AWS Service Quotas

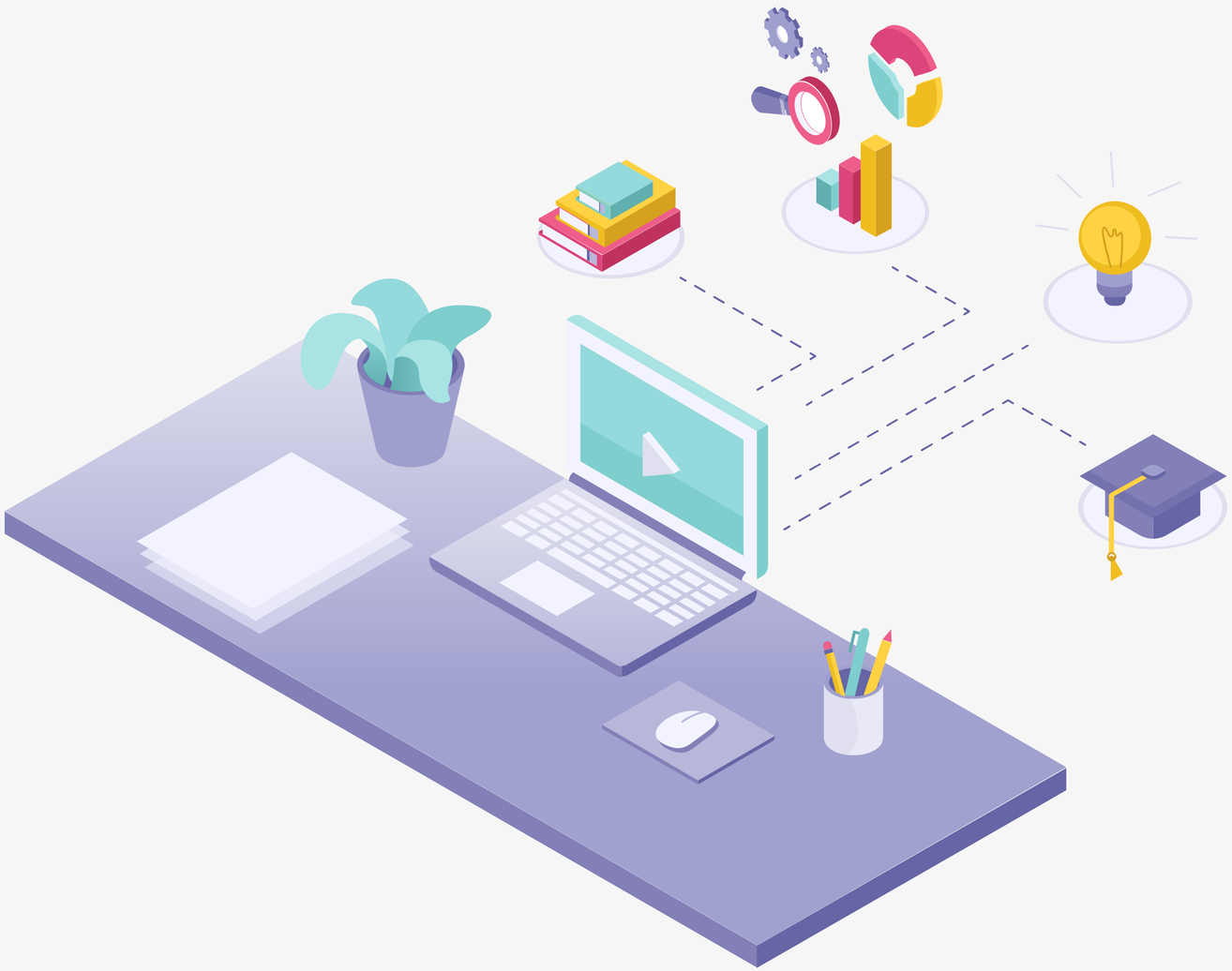


Les services ont des **quotas** (*limites*) par défaut

Quotas par compte AWS et par **région**

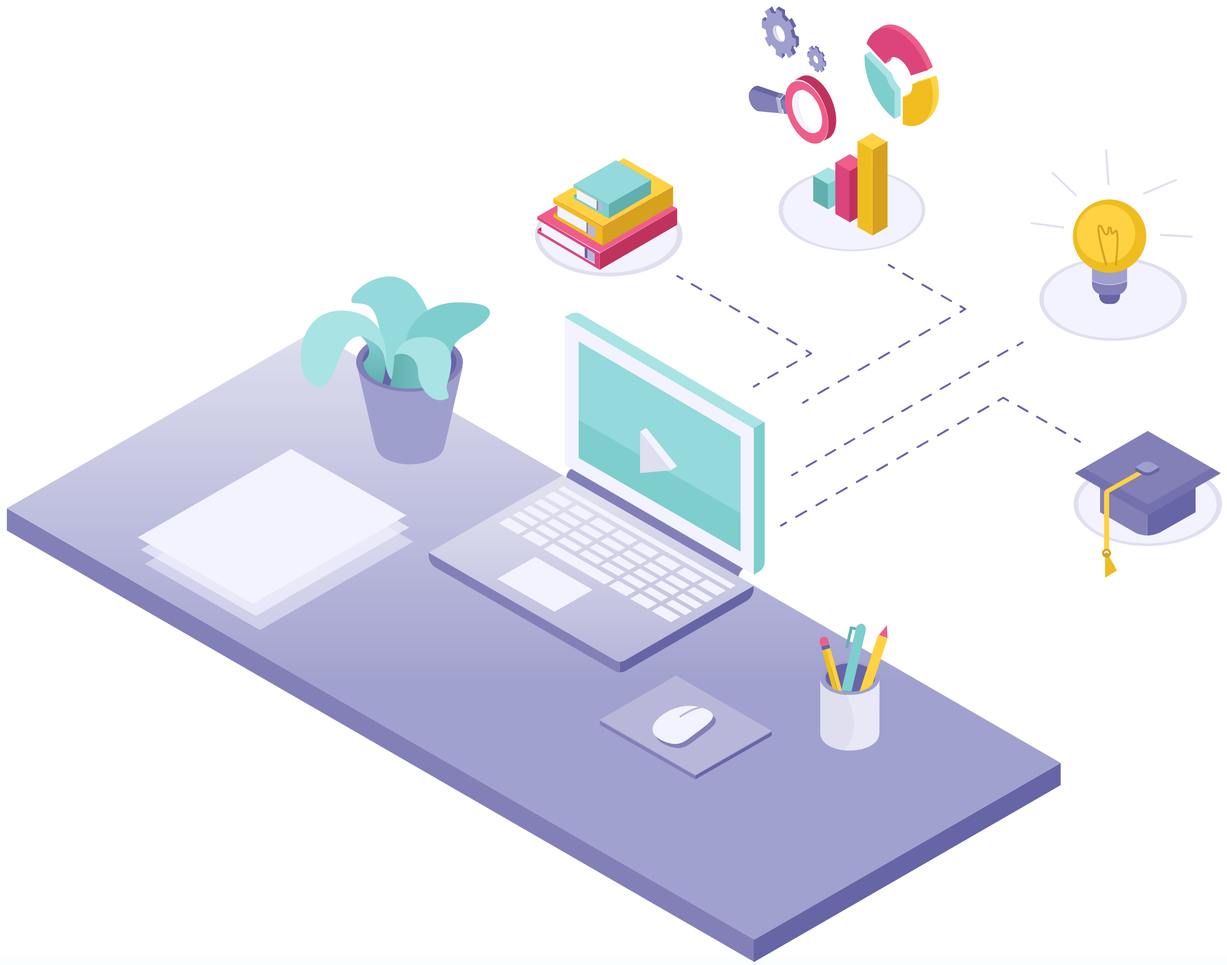
Surveillance avec **AWS Trusted Advisor**

Vous pouvez **demander des augmentations**

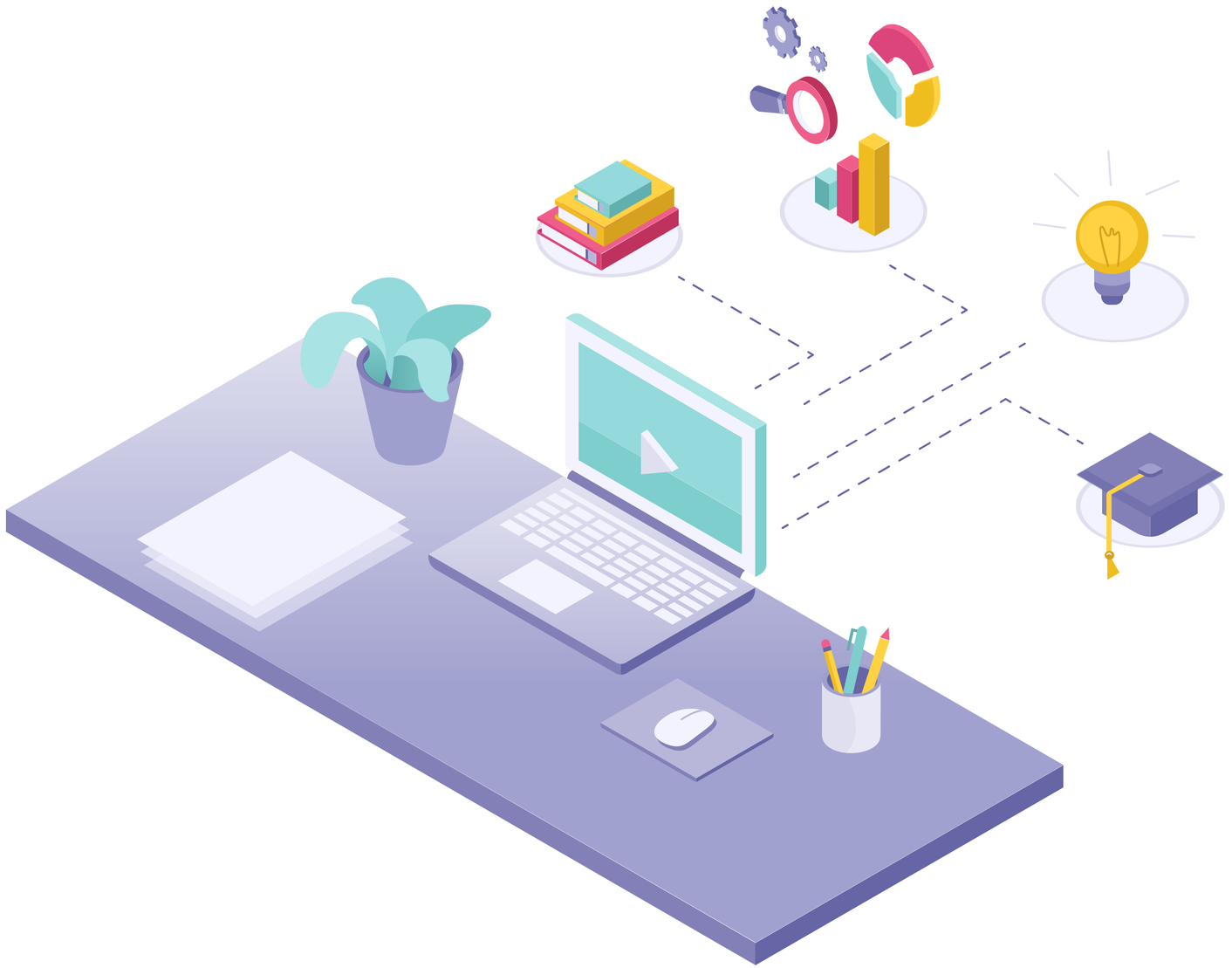


FIN DU MODULE

Module 16 : Billing & Gouvernance



Tarification AWS



Tarification AWS



Paiement de la capacité à l'heure ou à la seconde

Modèle le plus flexible, et le plus cher

Exemples de services
- EC2
- Lambda
- DynamoDB
- RDS
- ...

Engagement sur 1 ou 3 ans à utiliser une capacité spécifique

Permet de réduire votre facture jusqu'à 72% du prix On-Demand

Options de paiement : All Upfront / Partial Upfront / No Upfront

Exemple de services
- EC2
- RDS

Préférez les Savings Plans pour les EC2 !!

Engagement sur 1 ou 3 ans à dépenser un montant ($)

Permet de réduire votre facture jusqu'à 72% du prix On-Demand

Options de paiement : All Upfront / Partial Upfront / No Upfront

Exemple de services
- EC2
- Lambda
- Fargate
- SageMaker

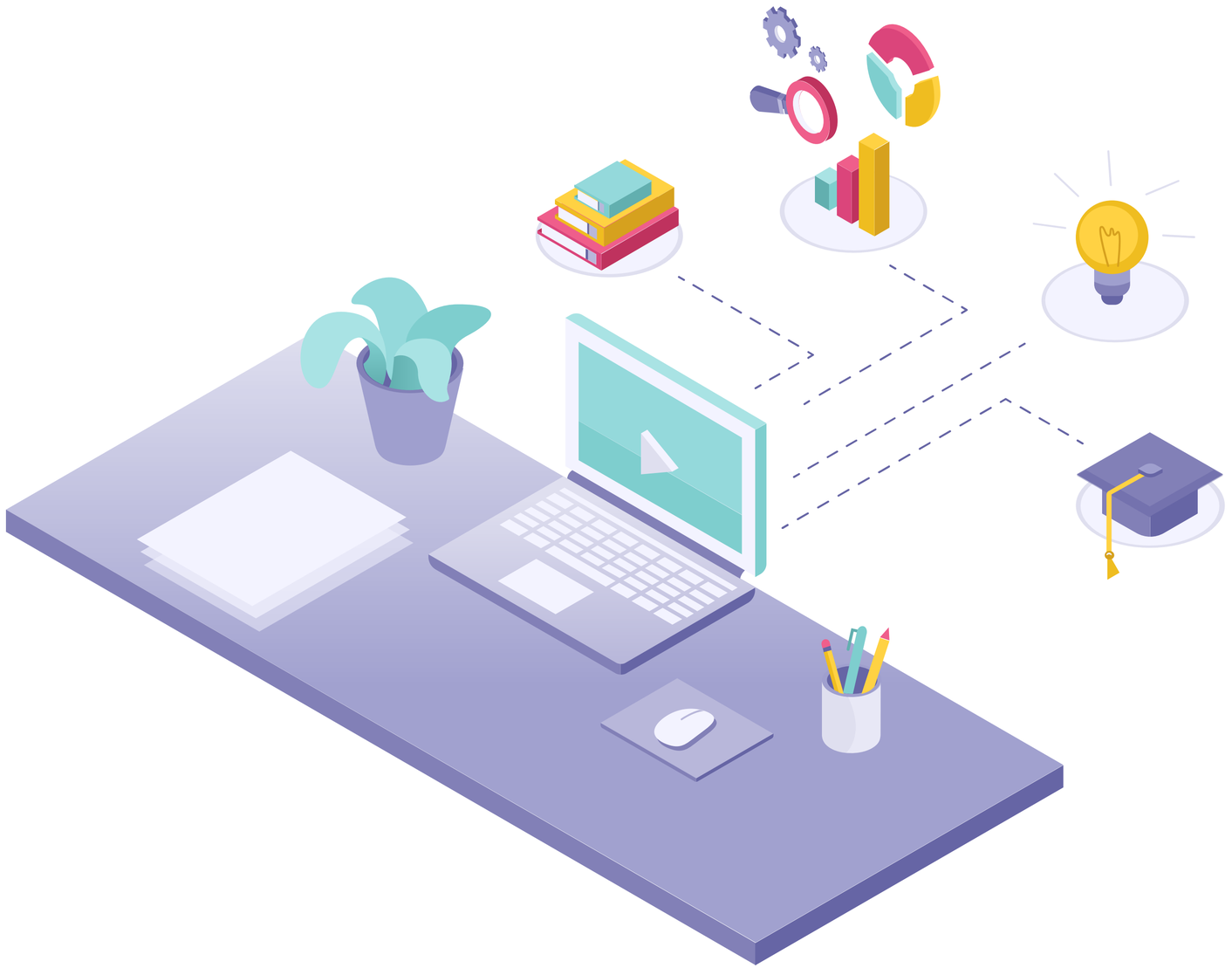
Capacité non utilisée, disponible aux enchères

Permet de réduire votre facture jusqu'à 90 % du prix On-Demand

AWS peut récupérer la capacité à tout moment (2 minutes de notification)

Exemple de services
- EC2
- Fargate

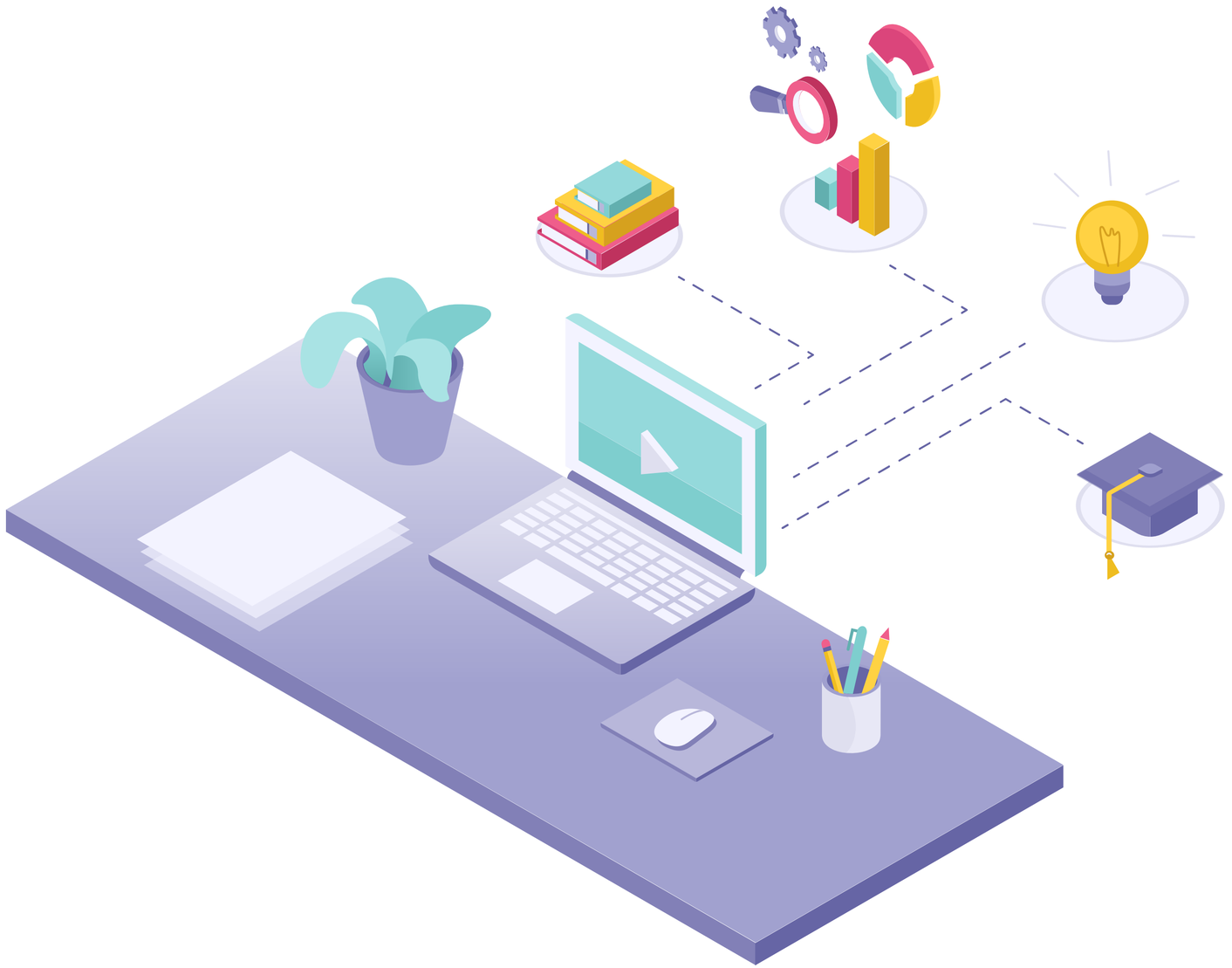
Quiz Tarification AWS



Quiz : choisir le bon modèle de tarification AWS

Offre jusqu'à 90% de réduction par rapport au modèle On-Demand	Instances Spot
Modèle de facturation flexible, sans engagement	On-Demand
Demande de s'engager sur un montant ($) à dépenser sur 1 ou 3 ans	Savings Plans
Modèle de facturation recommandé pour une nouvelle application en cours de déploiement	On-Demand
Instances peu chères, mais peuvent être reprises à tout moment	Instances Spot
Offre une réduction pouvant aller jusqu'à 72% du prix On-Demand	Savings Plans / Reserved Instances

AWS Billing and Cost Management



AWS Billing and Cost Management

Suite de **fonctionnalités** pour vous aider à gérer vos **coûts** sur AWS

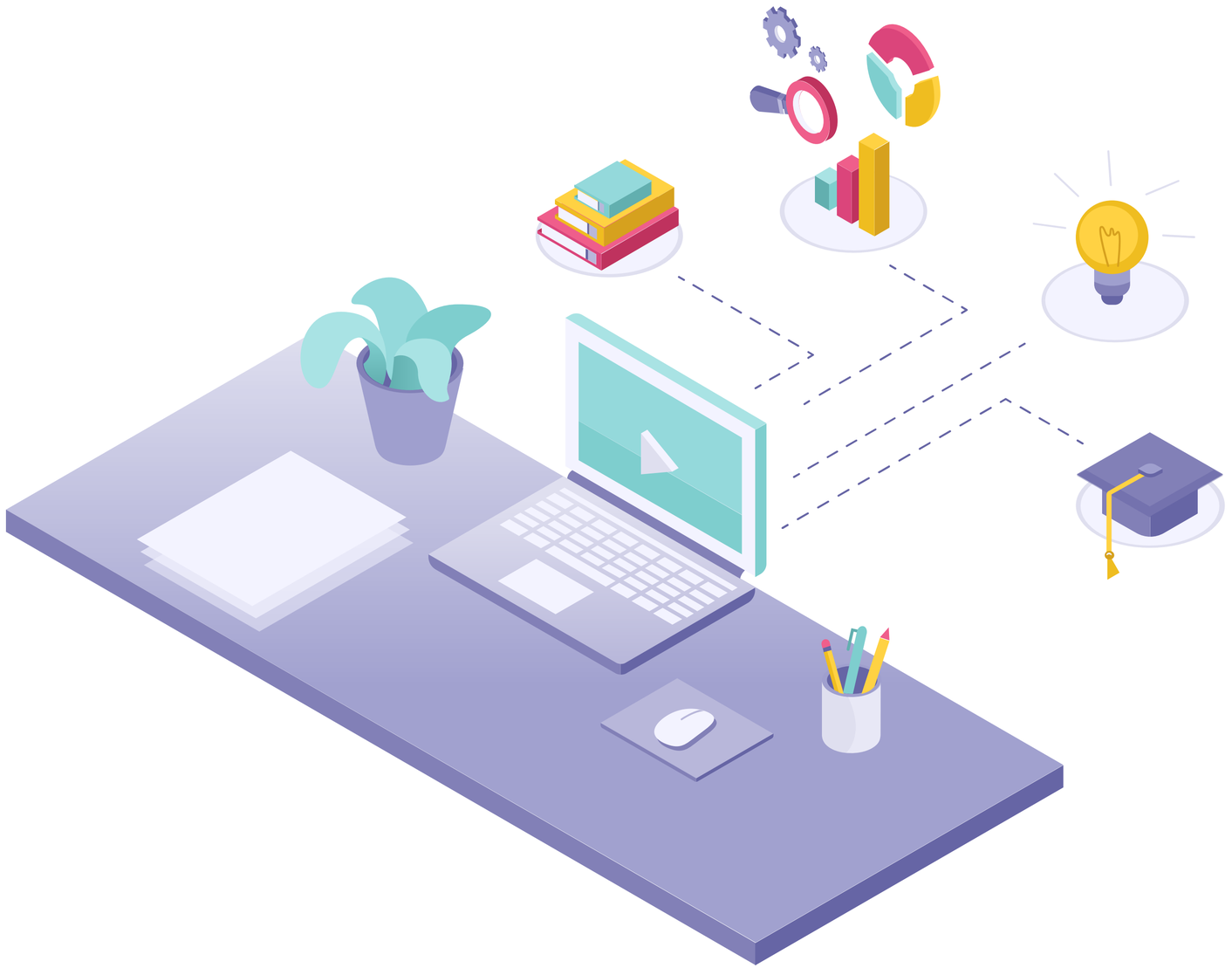
Accessible via la console AWS ou les APIs



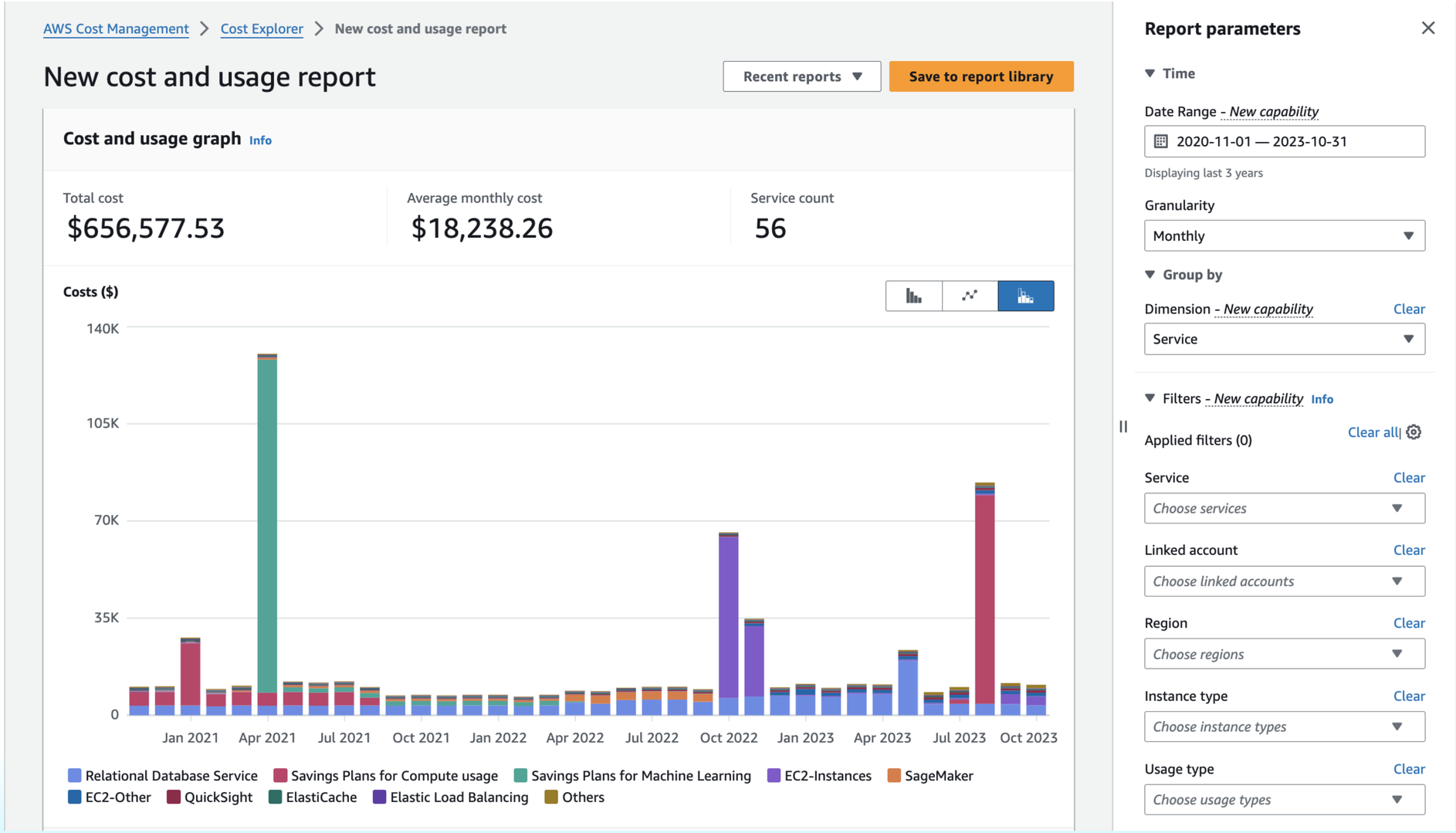
Fonctionnalités

- **Tableau de bord de facturation** : factures, paiement, crédits
- **Analyse et organisation des coûts** : AWS Cost Explorer, Rapports CUR, AWS Cost Anomaly Detection, Suivi Free Tiers, *Cost Allocation tags,…*
- **Gestion des Savings Plans :** Rapports d'utilisation, souscriptions, recommandations…
- **Gestion de budgets** : AWS Budgets
- **Préférences :** moyens de paiement, facturation, taxe….

AWS Cost Explorer



AWS Cost Explorer



AWS Cost Explorer



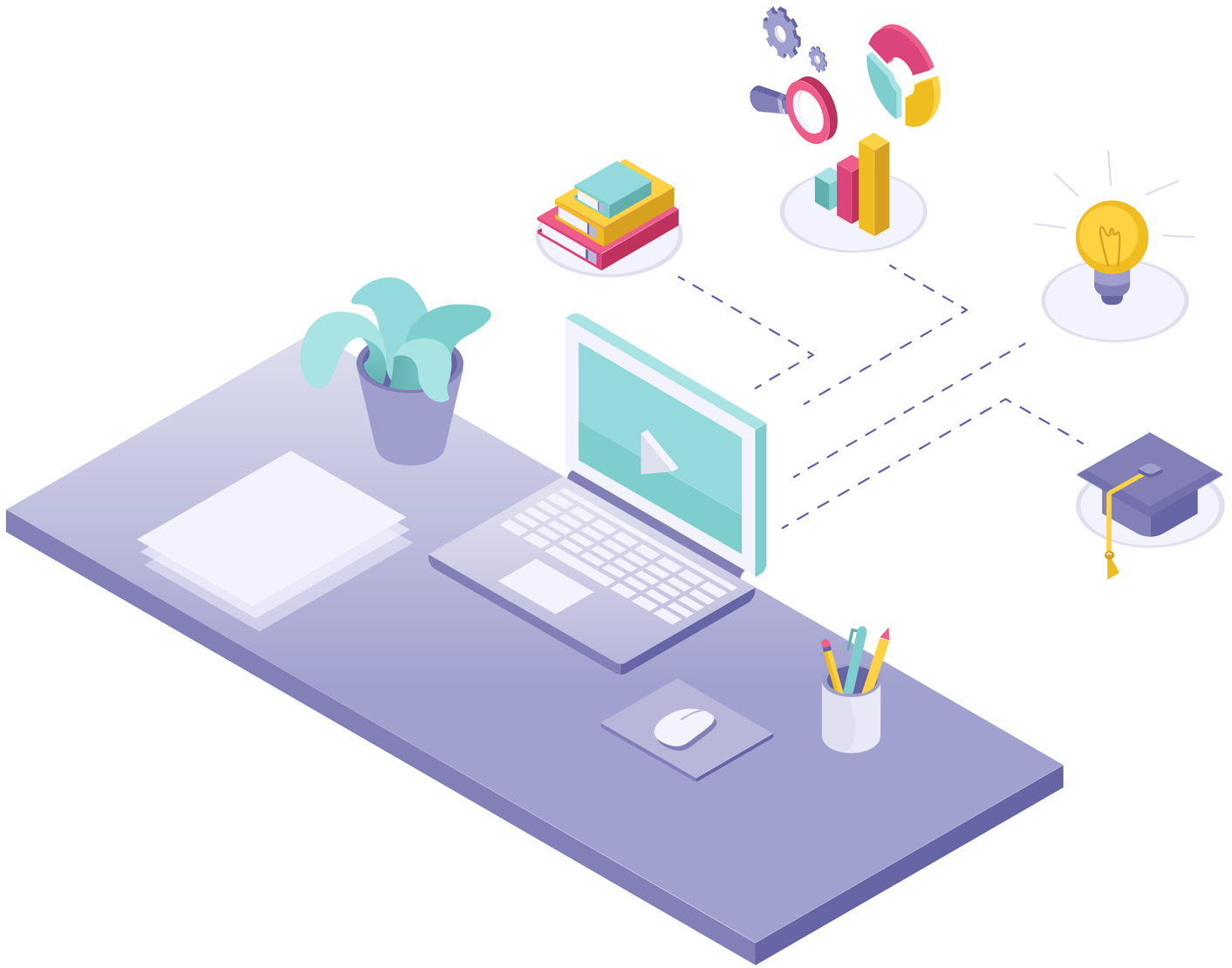
Permet de visualiser et comprendre **vos coûts** sur le Cloud AWS

Il faut l'activer avant de pouvoir l'utiliser

Fonctionnalités clés

- **Historique** des coûts sur les 12 derniers mois
- ***Forecast*** (prévisions de coûts) sur les 12 prochains mois
- **Graphiques** de visualisation des coûts
- Filtrage, recherche, aggrégation…
- Création de rapports personnalisés

Cost Allocation Tags



Cost Allocation Tags

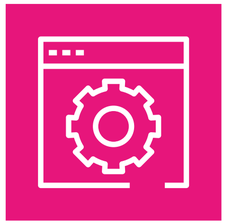
Fonctionnalité de **répartition des coûts basée sur les tags**

Tags = étiquette que vous affectez à vos ressources AWS

Permet donc le suivi des coûts par projet, application, utilisateur, Business Unit…

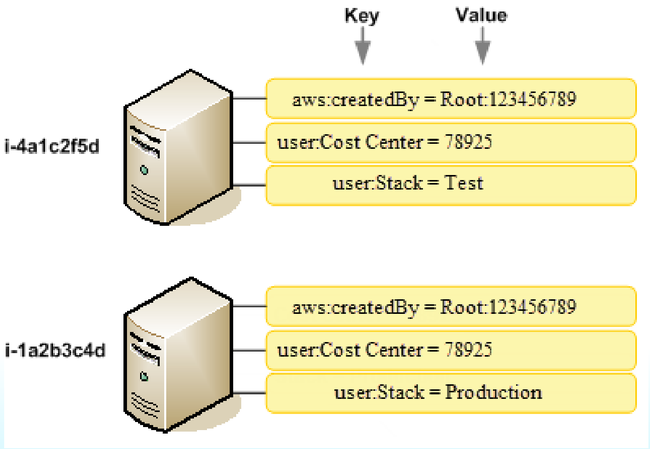
1

Activer *Cost Allocation Tags*



2

Tagguer vos ressources AWS

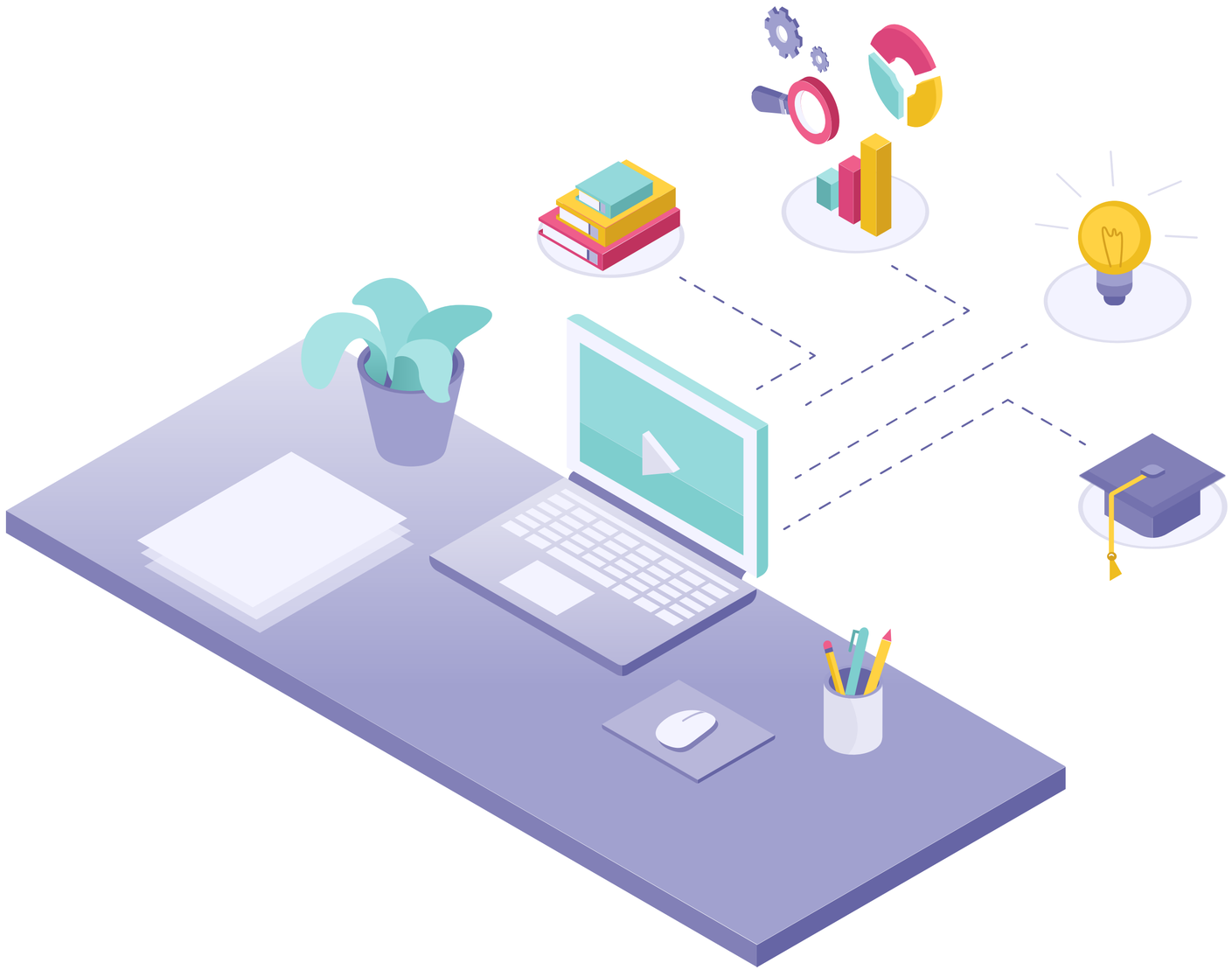


3

Les tags sont visibles dans les rapports de coûts & AWS Cost Explorer

Total Cost	user:Owner	user:Stack	user:Cost Center	user:Application
0.95	DbAdmin	Test	80432	Widget2
0.01	DbAdmin	Test	80432	Widget2
3.84	DbAdmin	Prod	80432	Widget2
6.00	DbAdmin	Test	78925	Widget1
234.63	SysEng	Prod	78925	Widget1
0.73	DbAdmin	Test	78925	Widget1
0.00	DbAdmin	Prod	80432	Portal
2.47	DbAdmin	Prod	78925	Portal

AWS Budgets



AWS Budgets

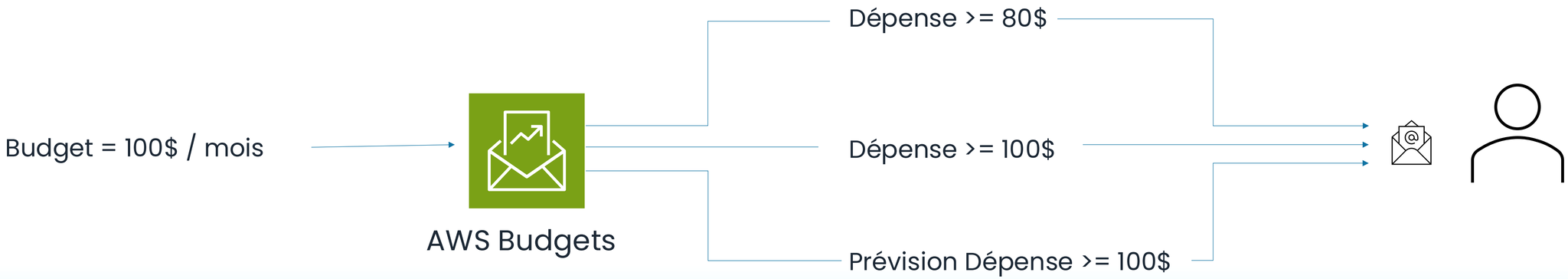


Permet de définir des **budgets personnalisés** pour surveiller vos dépenses

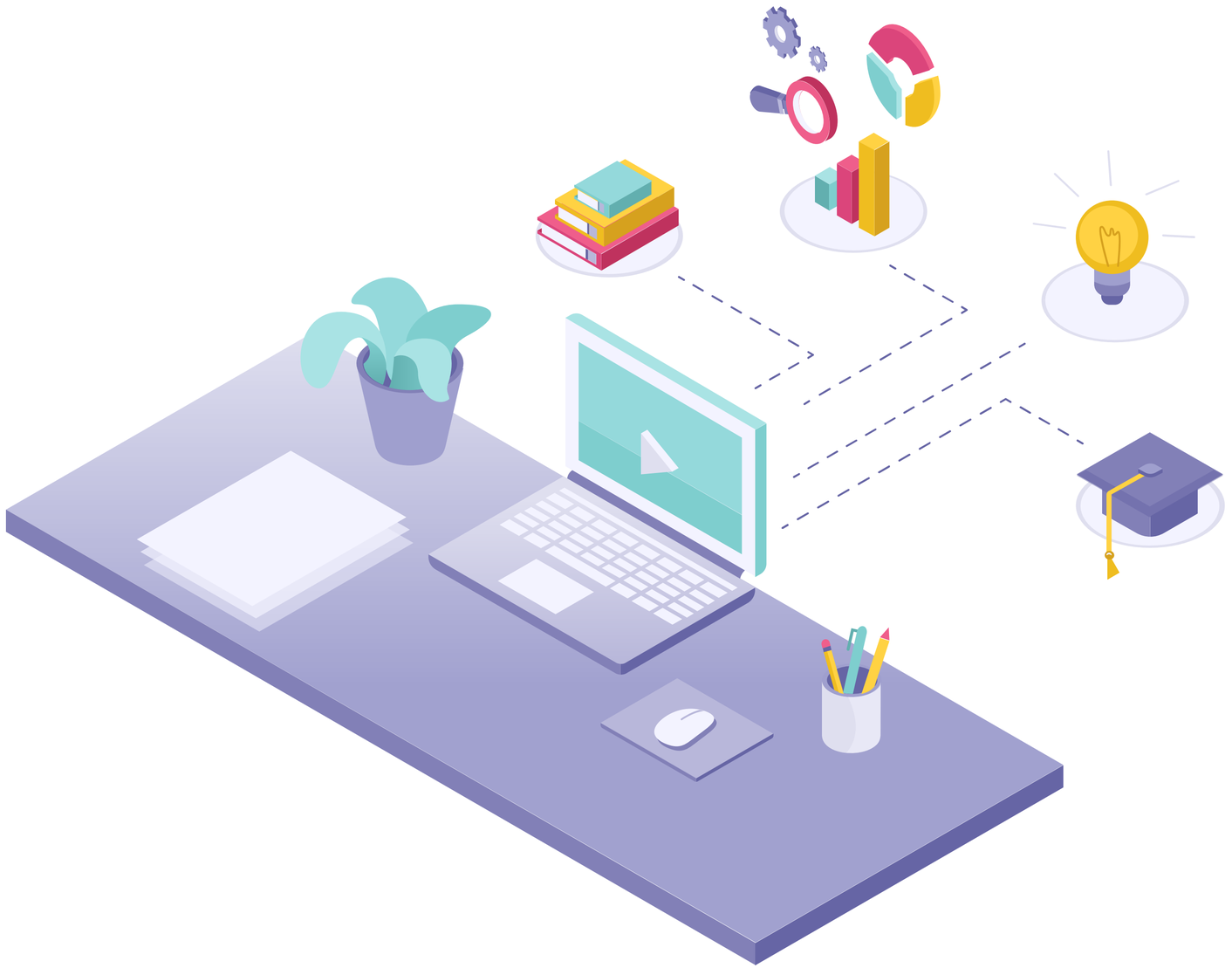
Permet de définir des **limites de dépenses**

Alertes lorsque vous approchez ou dépassez ces limites

Types alertes : e-mail ou notification SNS



AWS Compute Optimizer



AWS Compute Optimizer



Vous aide à **optimiser la configuration** de vos ressources AWS

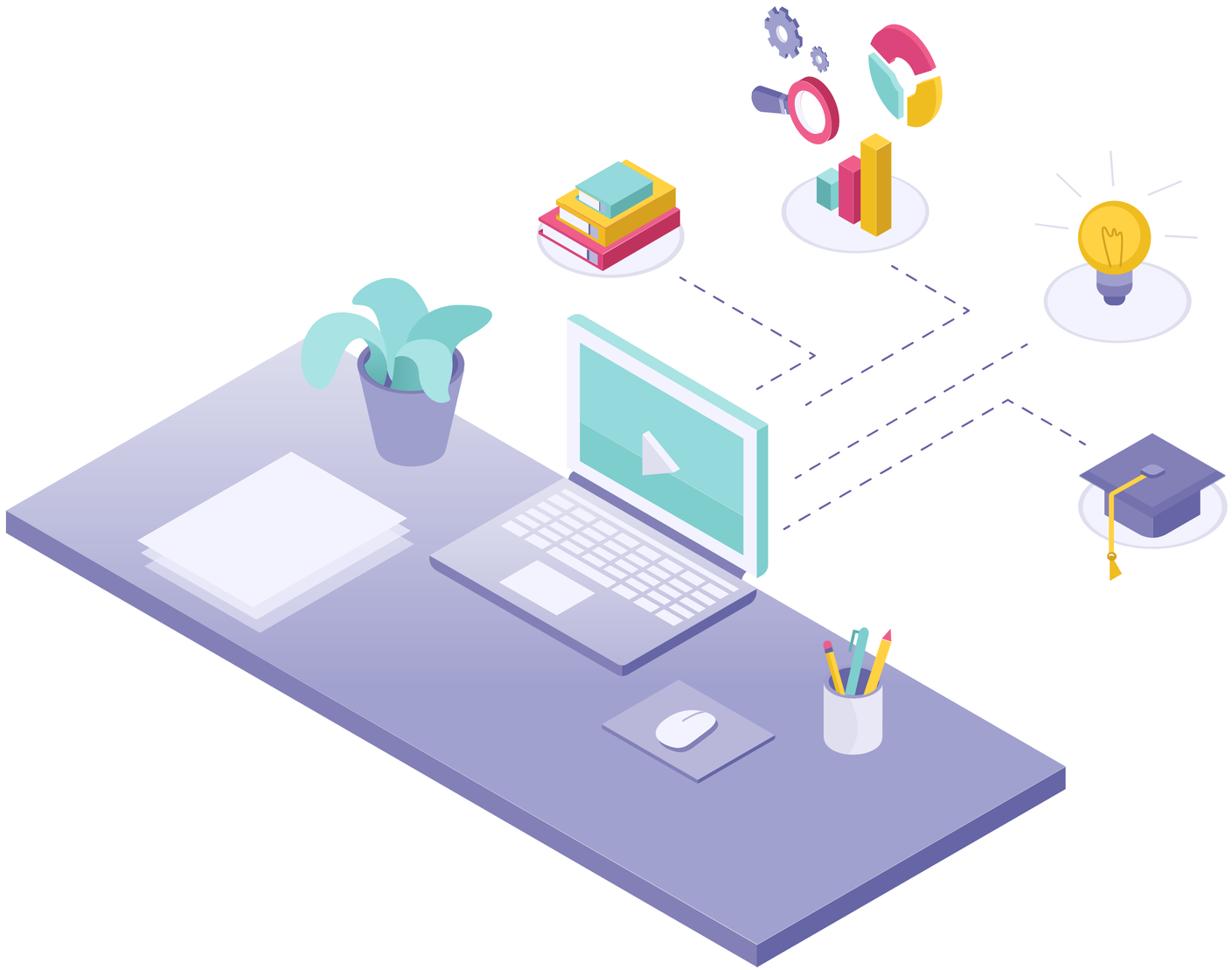
Utilise le ***Machine Learning*** pour analyser l'historique d'utilisation et fournir des **recommandations**

Ressources supportées : Instances EC2, volumes EBS, Conteneurs ECS, Fonctions AWS Lambda

Données analysées : Configuration des ressources, métriques CloudWatch

Avantages : vous permet de faire des économies et d'améliorer les performances

AWS Pricing Calculator



AWS Pricing Calculator

Outil en ligne gratuit qui permet de calculer des estimations de coûts

Permet d'estimer les coûts avant de commencer à utiliser les ressources AWS

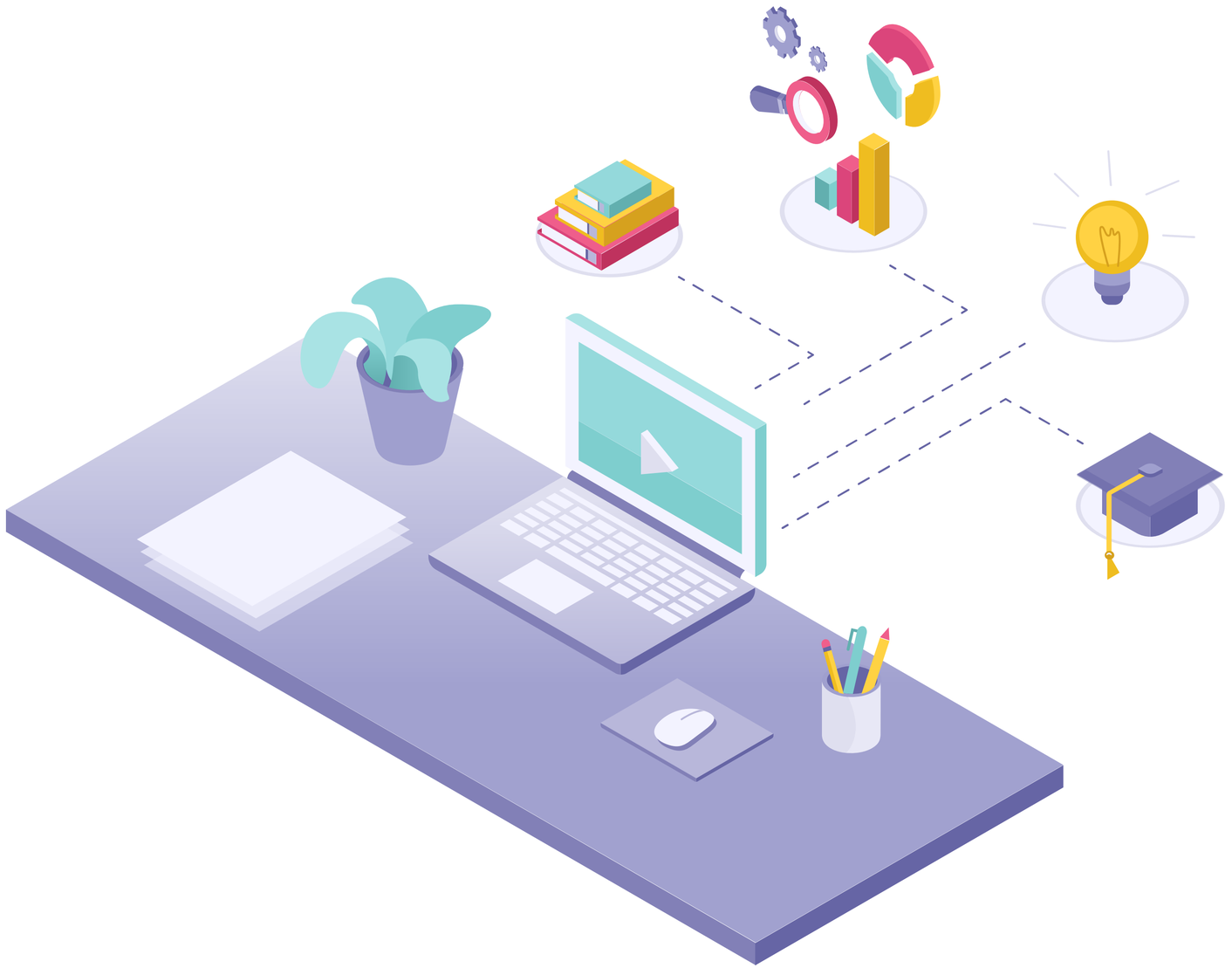
Accessible à tout le monde (pas seulement les clients AWS)

Migration vers AWS -> Utile pour les calculs de TCO (*Total Cost of Ownership*)

Quelques fonctionnalités clés

- Créer des estimations de coûts pour une vaste gamme de services AWS
- Exporter des estimations (CSV, PDF)
- Partagez vos estimations avec des liens publics

Le suivi des coûts en résumé



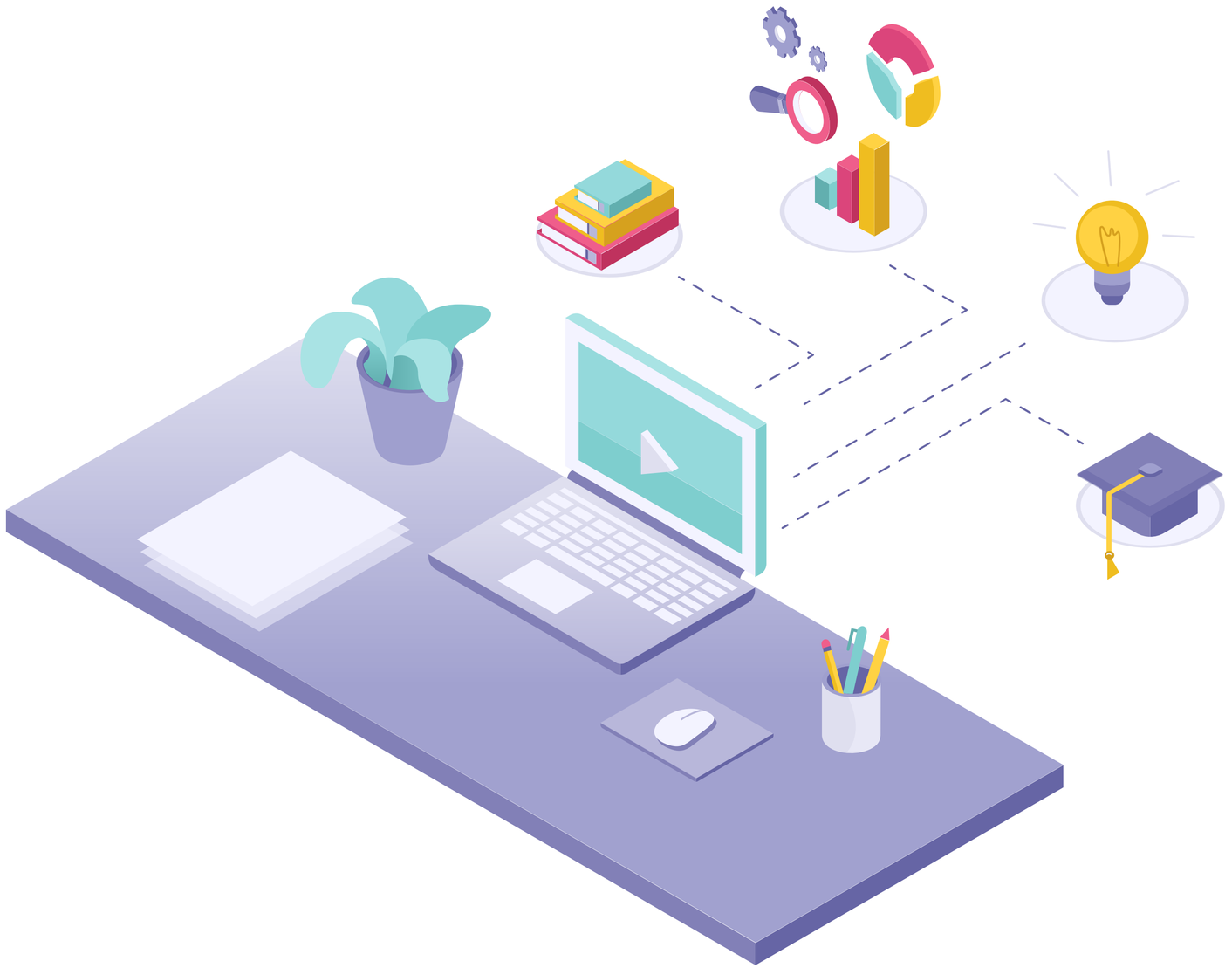
Les coûts sur AWS : choisir le bon service

Billing & Cost Management	AWS Cost Explorer	Cost Allocation Tags	AWS Budgets	AWS Compute Optimizer	AWS Pricing Calculator
Regroupe les outils/fonctionnalités de suivi de vos coûts	Permet de visualiser et explorer vos coûts	Permet d'utiliser les tags pour catégoriser et suivre vos coûts	Permet de définir des budgets personnalisés	Propose des recommandations de configurations optimales	Permet aux utilisateurs d'estimer les coûts

Les coûts sur AWS : Quiz

Permet de suivre et répartir les coûts par projet, équipe ou utilisateur	Cost Allocation Tags
Être alerté lorsque mes coûts AWS dépassent un budget mensuel de 50$	AWS Budgets
Permet de comprendre l'augmentation des coûts AWS sur 1 mois donné	AWS Cost Explorer
Avoir une estimation des coûts de l'application qui sera migrée sur AWS	AWS Pricing Calculator
Avoir des recommandations pour réduire les configurations des instances EC2	AWS Compute Optimizer
Consulter mes factures et modifier mes préférences de facturation	AWS Billing & Cost Management

AWS Support



AWS Support

Ingénieurs AWS qui vous assistent en cas de problèmes techniques

Niveaux d'assistance : *Basic*, Developer, Business, **Enterprise** (On-Ramp), **Enterprise**



Exemples de problèmes pris en charge par le support AWS

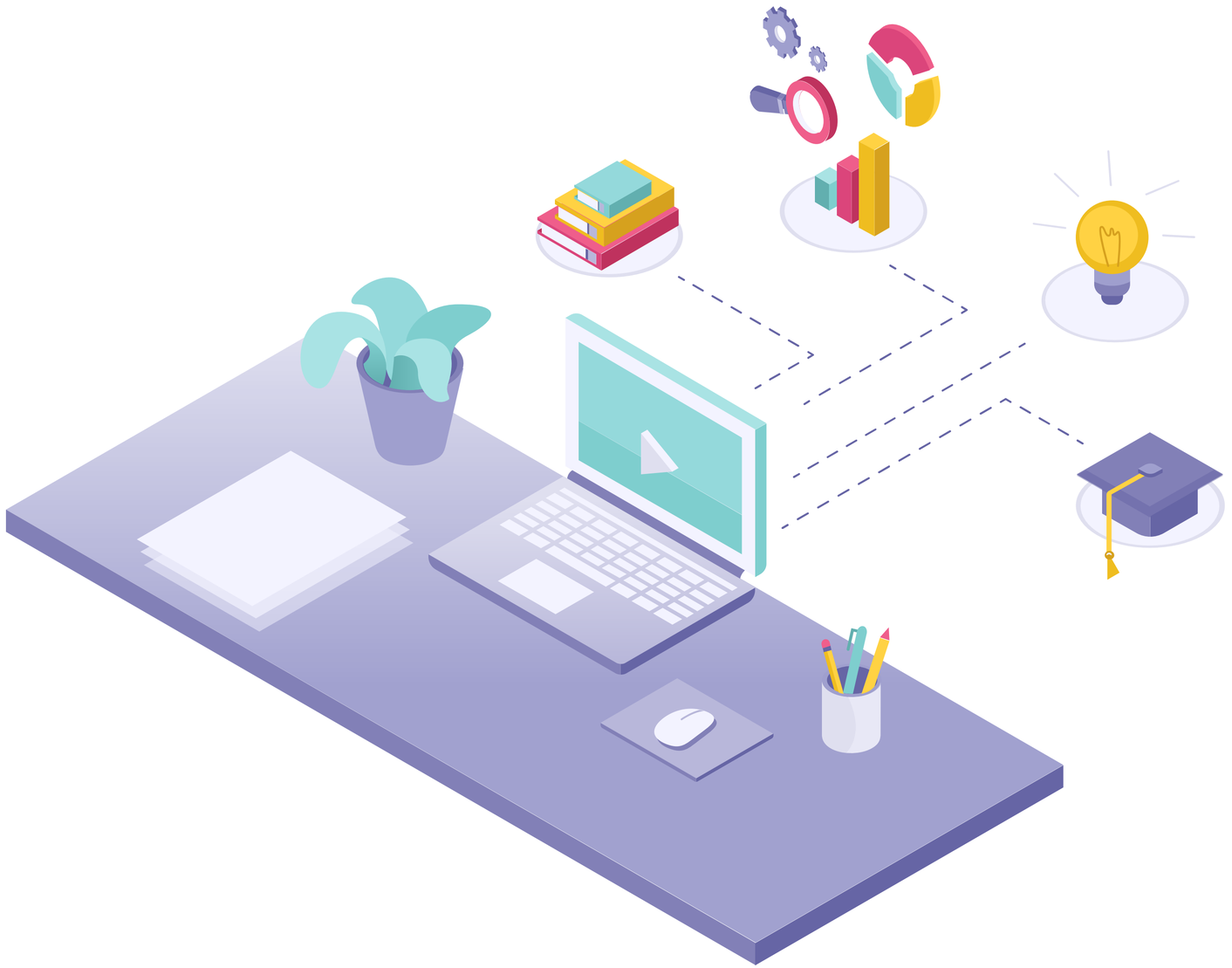
- Problèmes liés au fonctionnement des services AWS
- Demandes de bonnes pratiques de déploiement
- Dépannage sur des problèmes avec AWS SDK ou APIs
- Conseils d'architecture

!!! Non inclus : développement de code, dépannage de vos applications…

AWS Support

	Basic	Developer	Business	Enterprise On-Ramp	Enterprise
Description	-	Accès **web** au service technique aux heures ouvrables** Recommandé si vous expérimentez ou testez dans AWS	Accès 24 h/24 et 7 j7 par téléphone, web et chat Minimum recommandé si vous disposez de charges de travail de production dans AWS	Accès 24 h/24 et 7 j7 par téléphone, web et chat Recommandé si vous disposez de charges de travail critiques de production et/ou métier dans AWS	Accès 24 h/24 et 7 j7 par téléphone, web et chat Recommandé si vous disposez de charges de travail critiques de production et/ou métier dans AWS
Sévérité du cas/temps de réponse*	-	Système affecté : < 12 heures**	Système de production inopérant : < 1 heure	Système vital inopérant : < 30 minutes	Système métier/stratégique inopérant : < 15 minutes
Directives d'architecture	-	Questions d'ordre général	Adapté à vos cas d'utilisation	Conseils basés sur vos applications (un par an)	Conseils basés sur vos applications
TAM dédié (Technical Account Manager)	-			Un groupe de Gestionnaires de compte technique (TAM) pour fournir des conseils proactifs	**Un Gestionnaire de compte technique (TAM) attitré** pour surveiller de manière proactive votre environnement
Tarification	Gratuit	A partir de 29 USD par mois	A partir de 100 USD par mois	A partir de 5 500 USD	A partir de 15 000 USD

AWS Marketplace

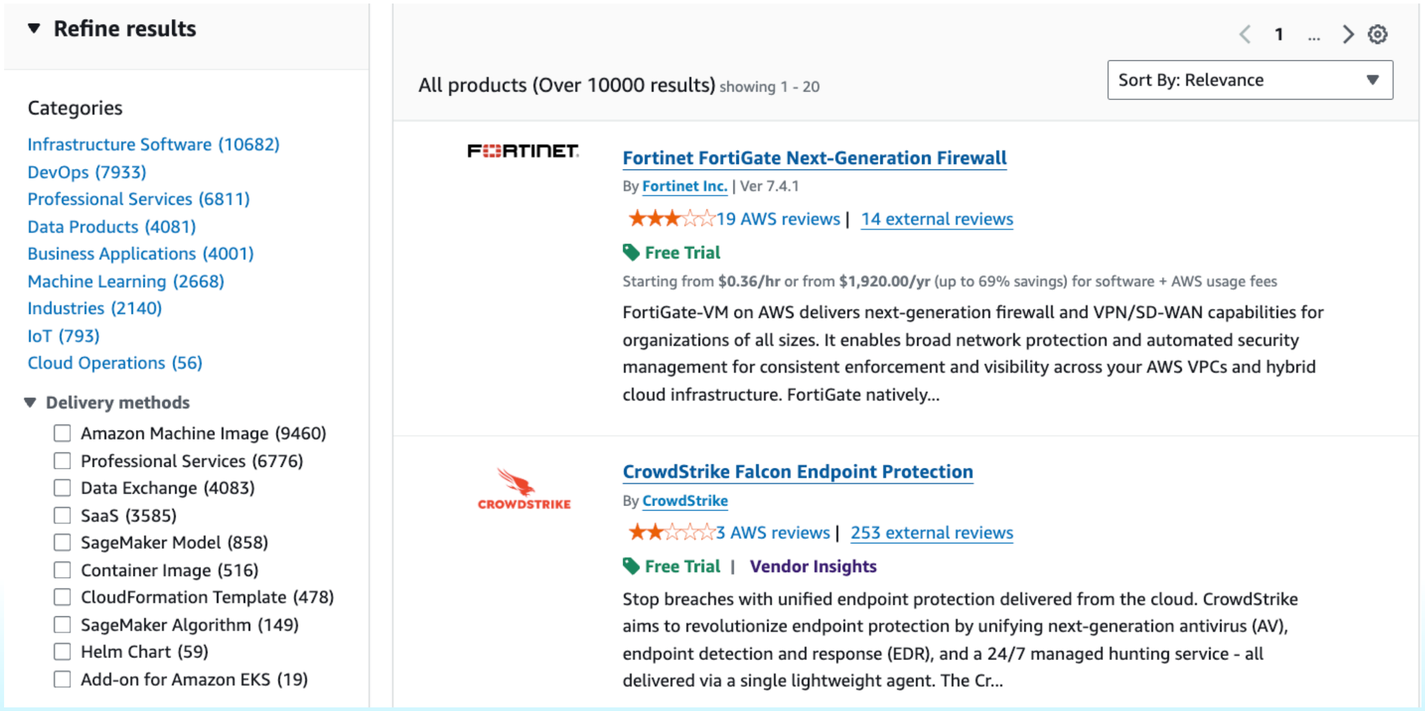


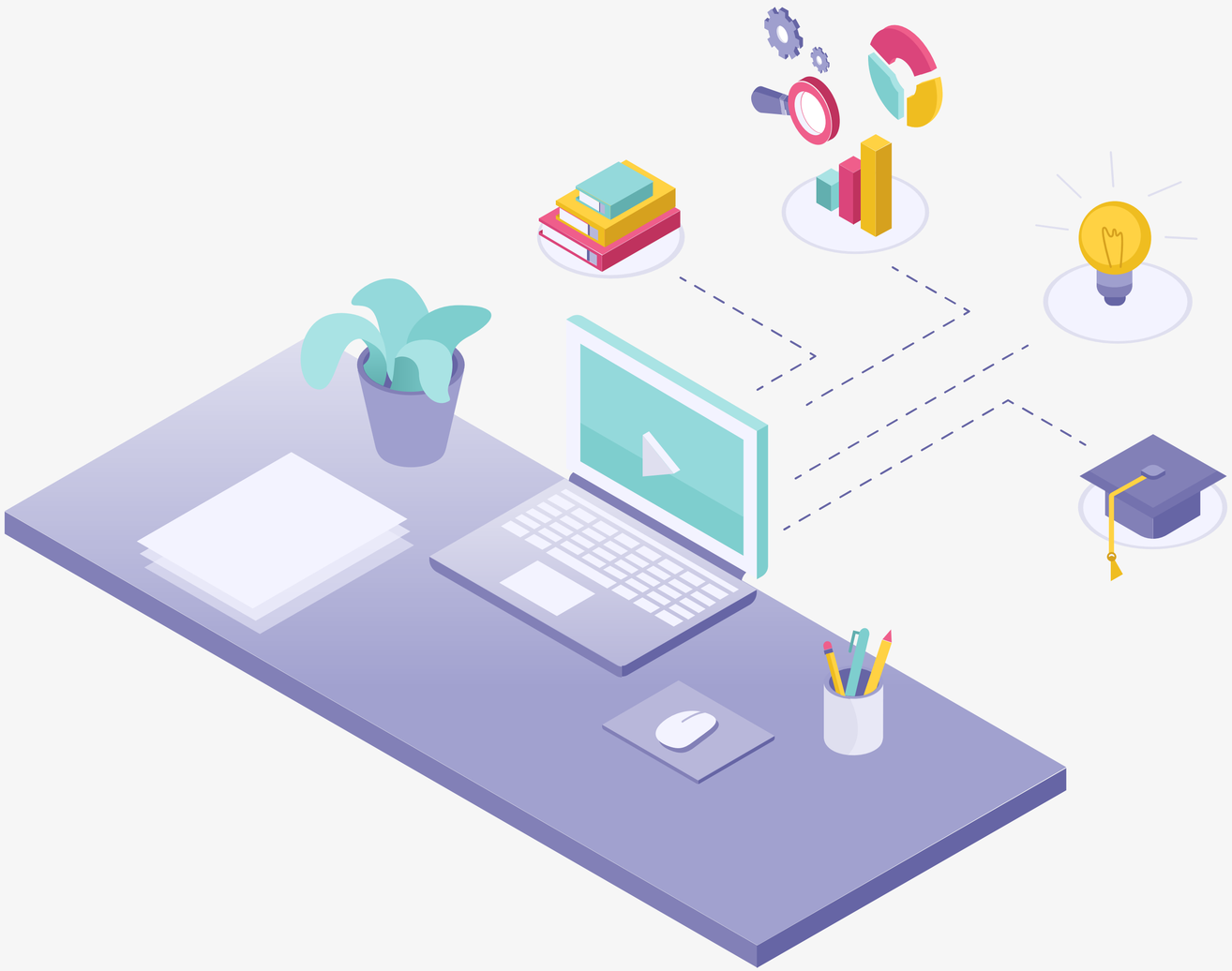
AWS Marketplace

Permet d'**acheter et déployer des logiciels** directement sur le cloud AWS

Inclut des **milliers de logiciels** : Applications métier, Réseau, Devops, Sécurité,...

Simplifie le **processus d'achat** de nouveaux logiciels

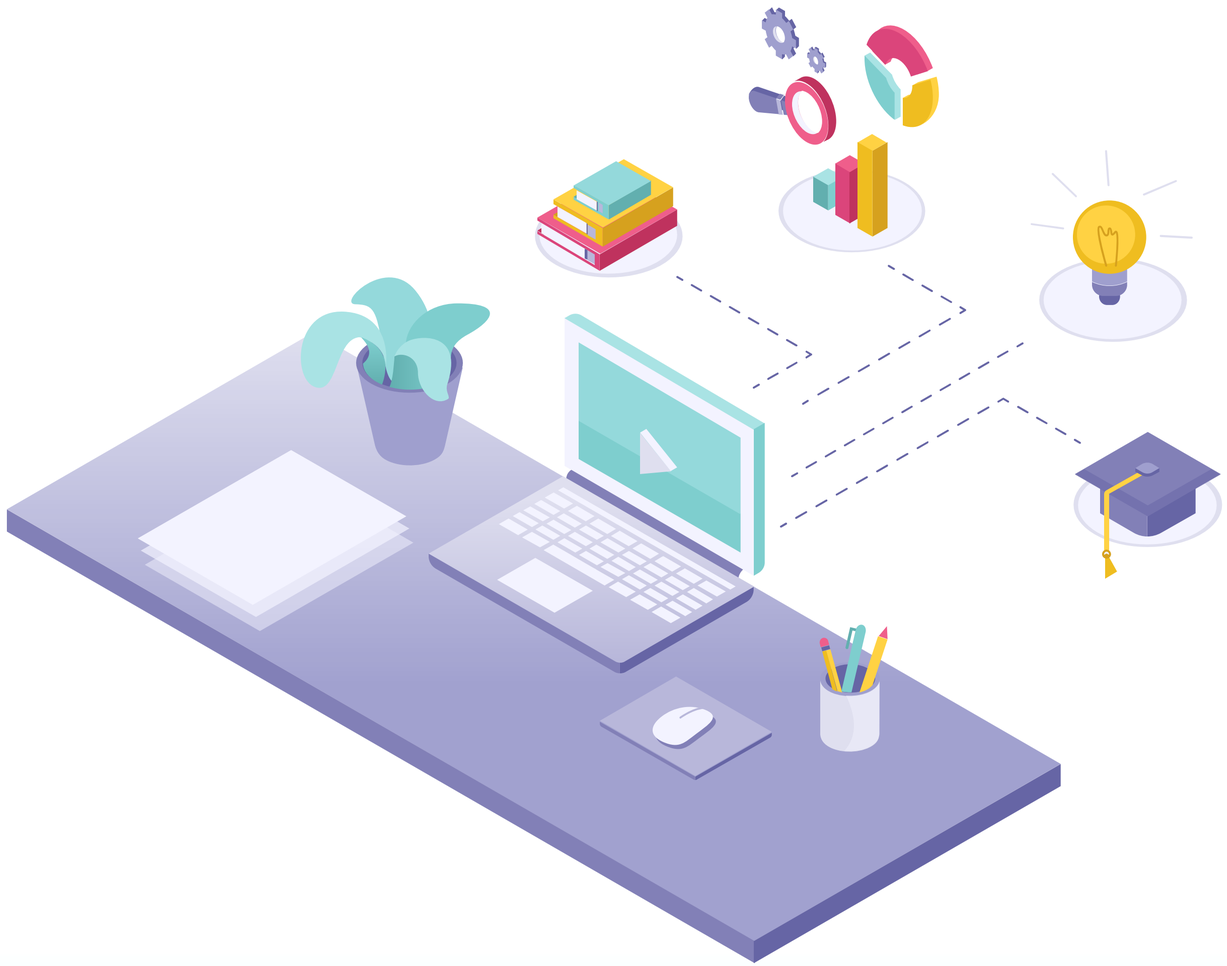




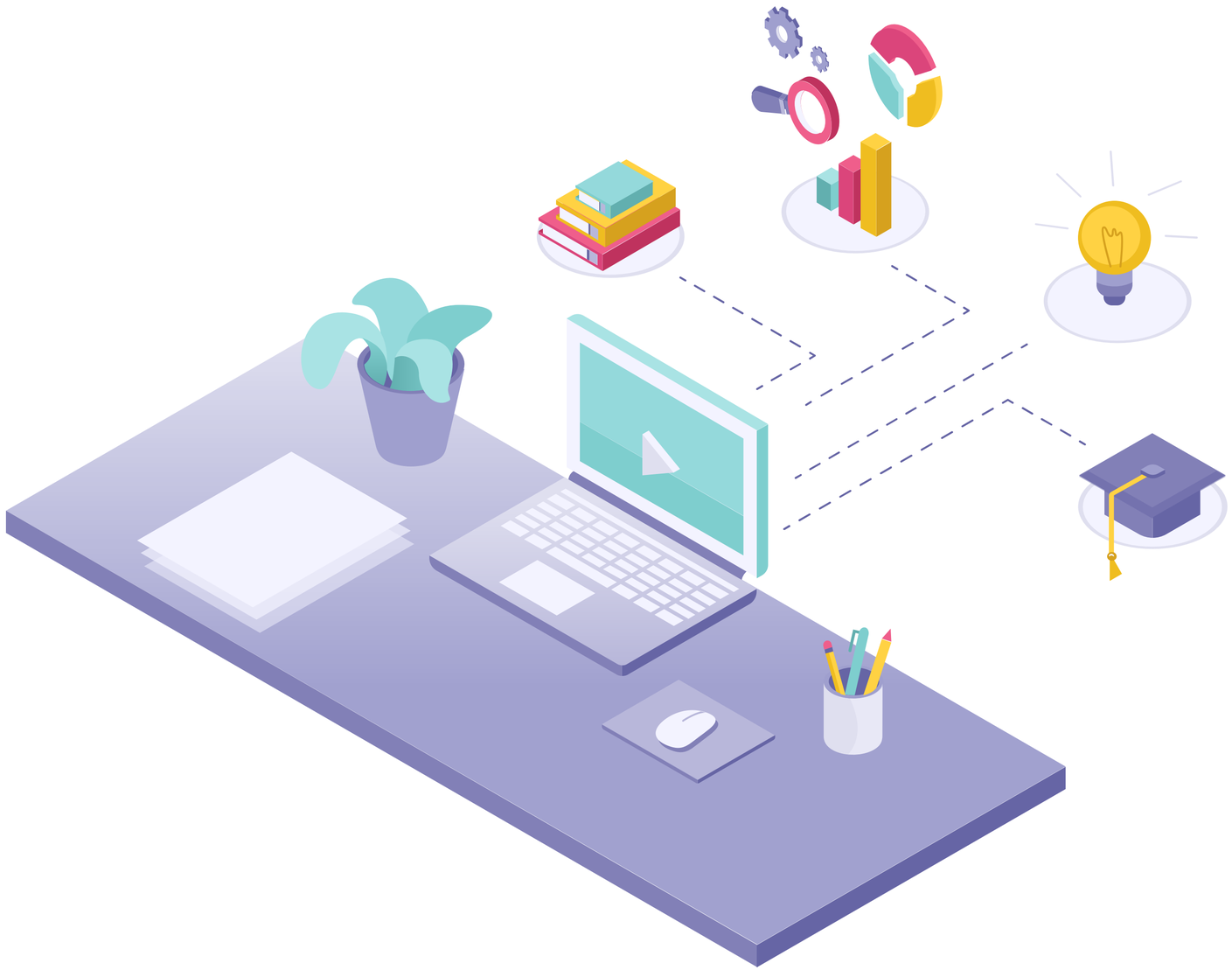
FIN DU MODULE

Module 17 : Migration et Sauvegarde

Todo

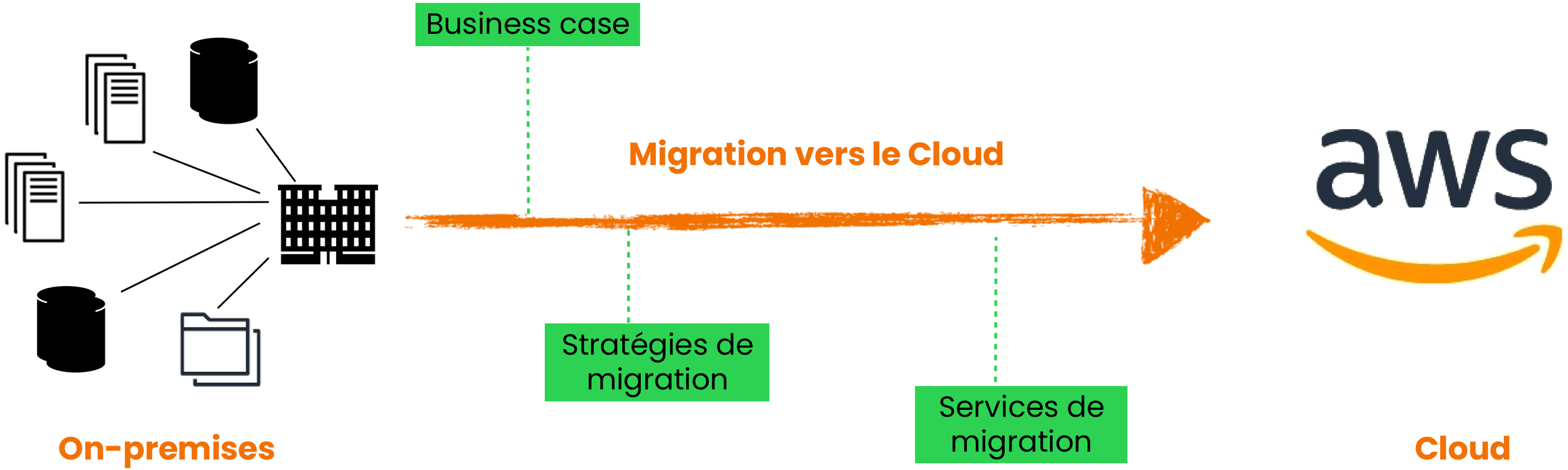


Migration vers le Cloud AWS

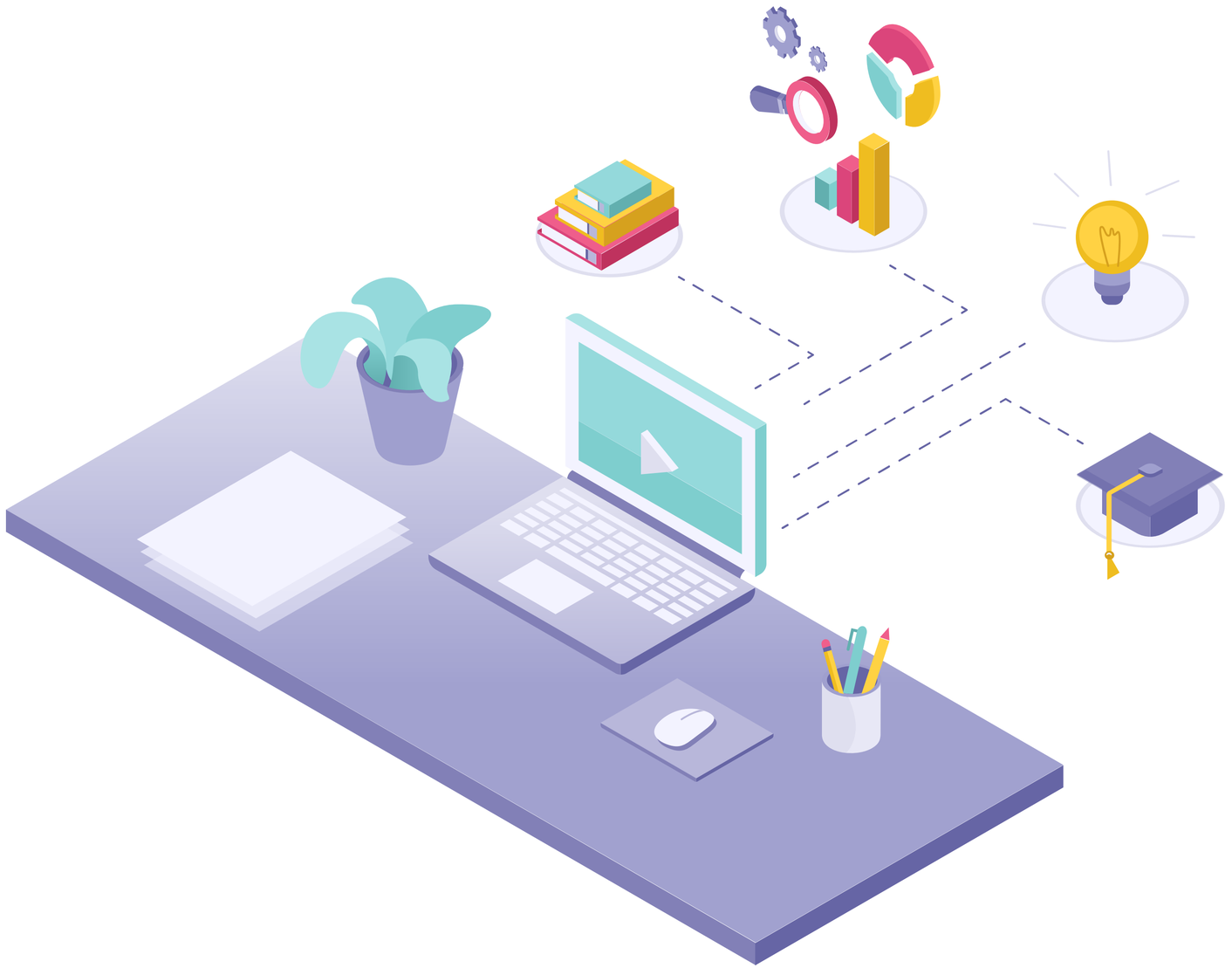


LeCloudFacile.com

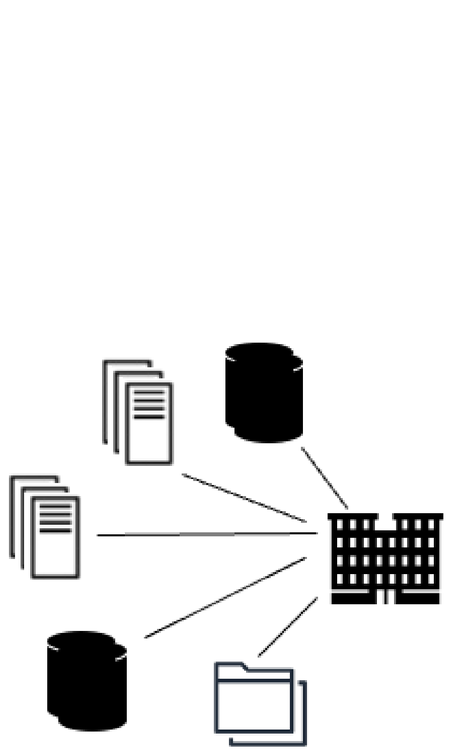
Migration vers le Cloud AWS



Stratégies de migration



Stratégies de migration : les 6 R



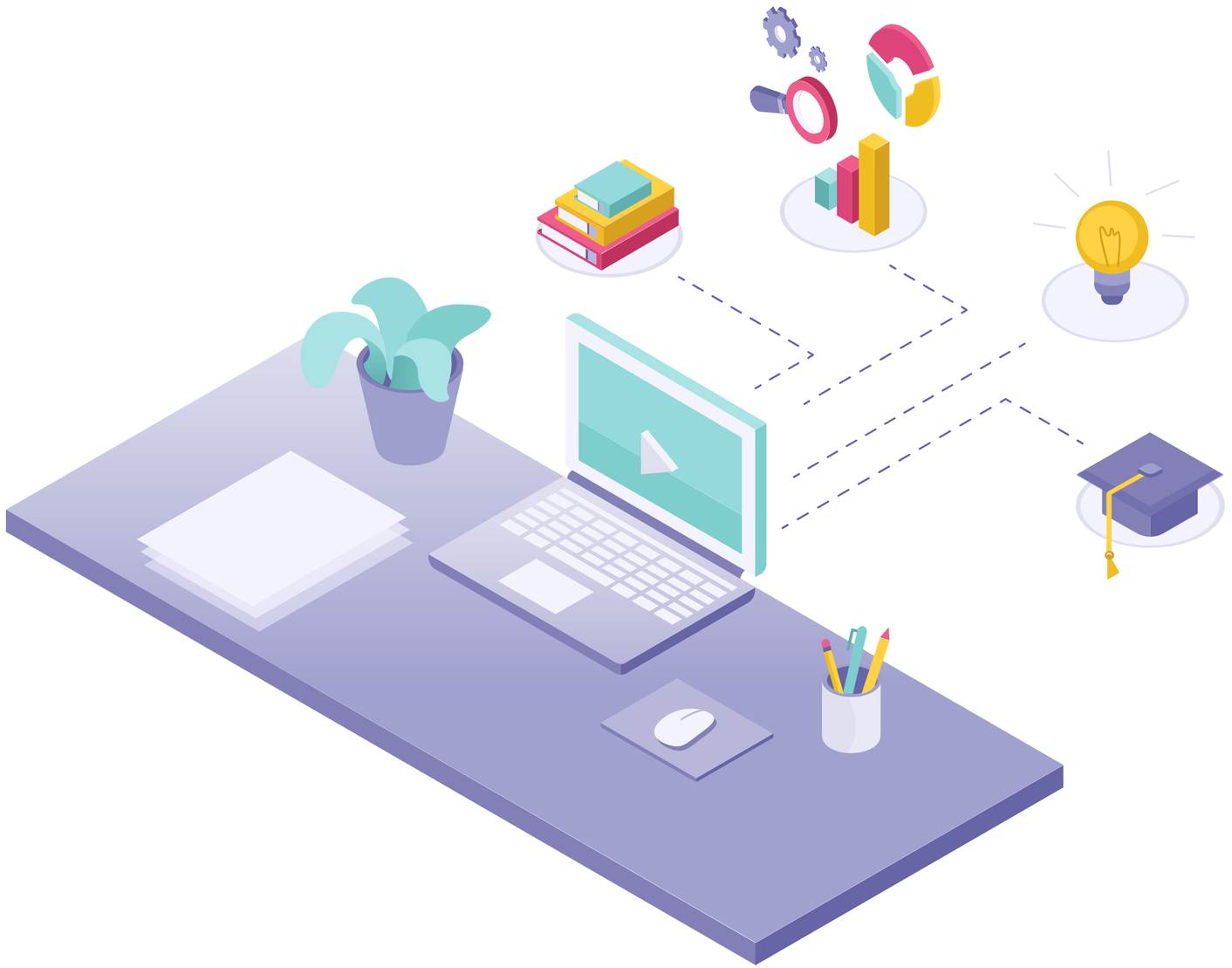
On-premises

Determine

- Rehosting → Lift-and-shift Migration sans changement
- Replatforming → Changement de plateforme
- Refactoring / Re-architecting → Changement d'architecture et/ou re-développement
- Repurchase → Achat d'une nouvelle solution Cloud
- Retain → L'application ne sera pas migrée X
- Retire → L'application sera arrêtée (obsolète,...) X

aws

Services de migration



Migration des bases de données



Base de données

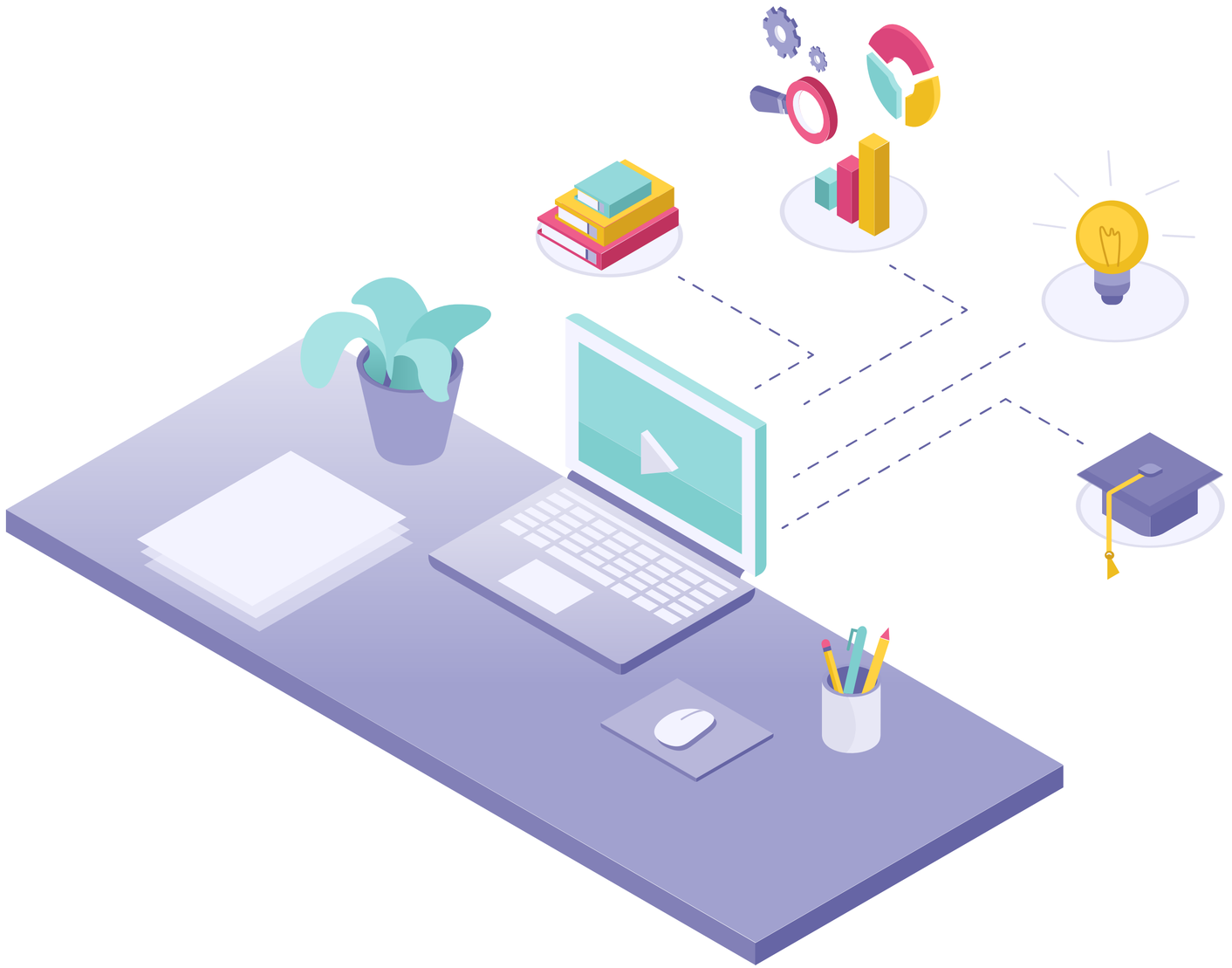
AWS Database Migration Service (DMS)

Amazon RDS

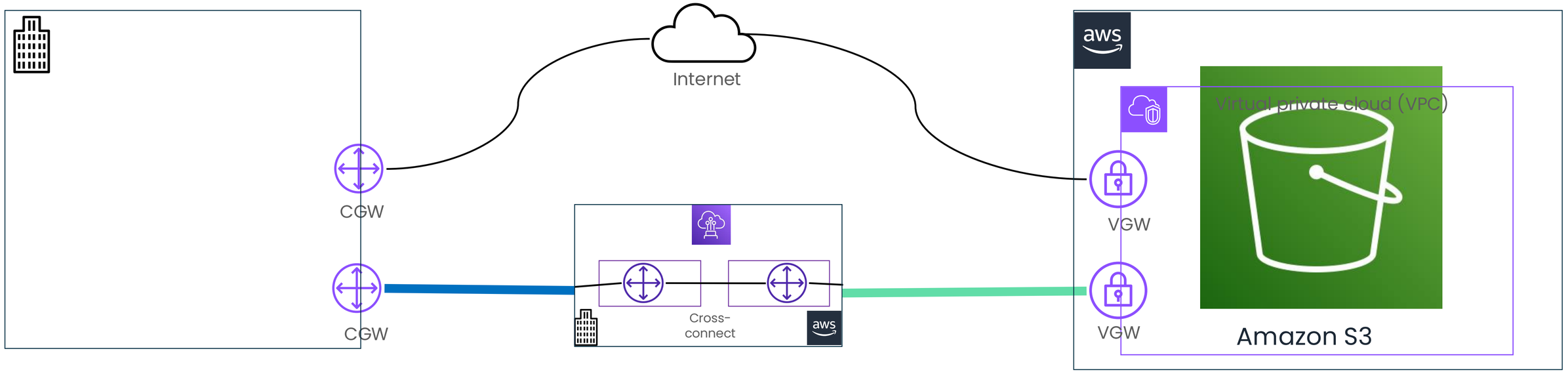
On-premises

- Service de réplication et de migration de bases de données
- Prend en charge les migrations **homogènes** et **hétérogènes**.
- Migration **hétérogène** -> AWS Schema Conversion Tool (SCT) pour la conversions de schémas + AWS DMS pour migrer les données

Migration des données



Migration des données



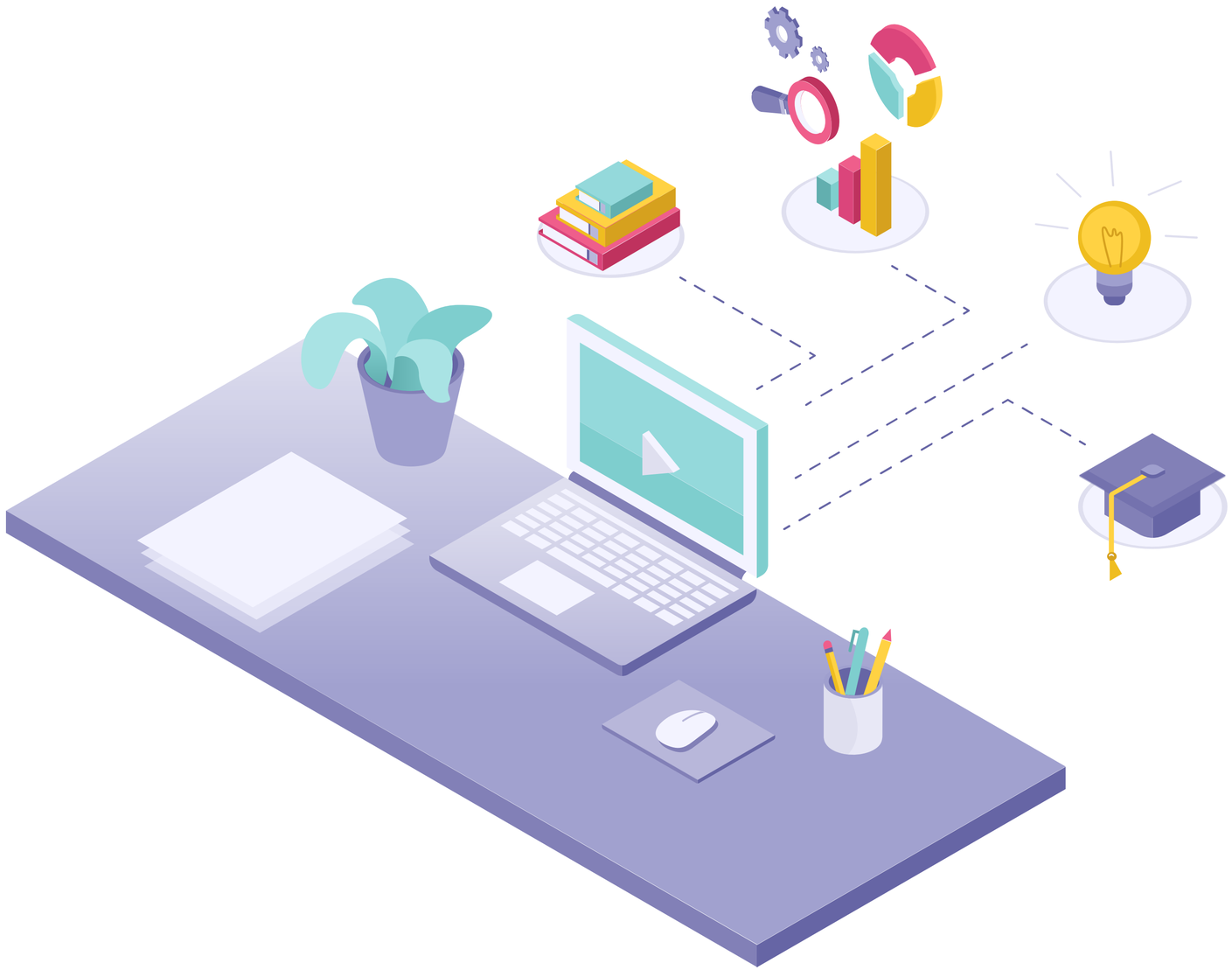


La famille Snow*

AWS Site-to-Site VPN

AWS Direct Connect

La famille AWS Snow



La famille Snow



AWS Snowball Edge

(Compute Optimized ou Storage Optimized)

Plusieurs dizaines de To



AWS Snowcone

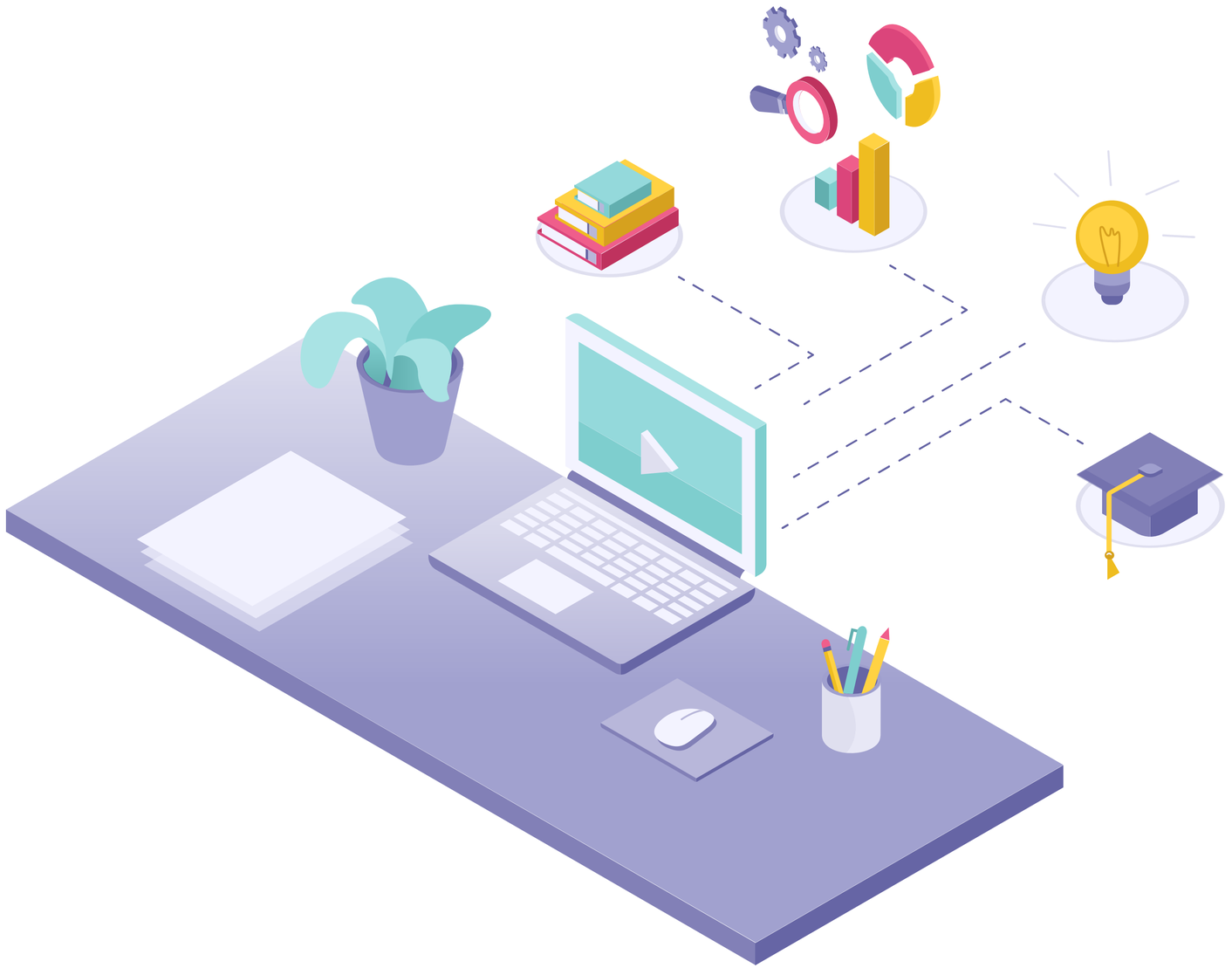
Environ une dizaine de To



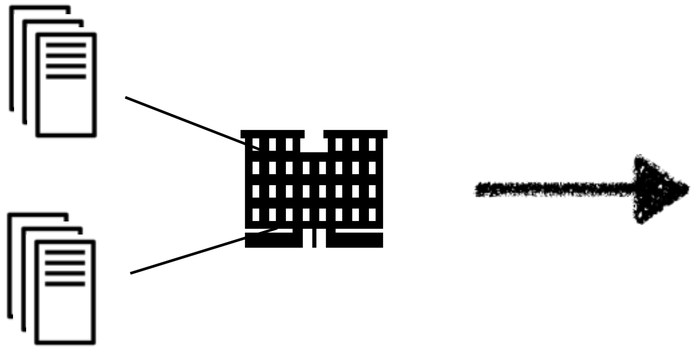
AWS Snowmobile

Une centaine de Po

AWS Application Migration Service

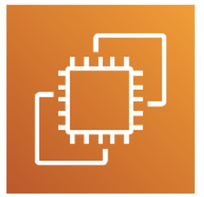


Migration des serveurs





AWS Application Migration Service

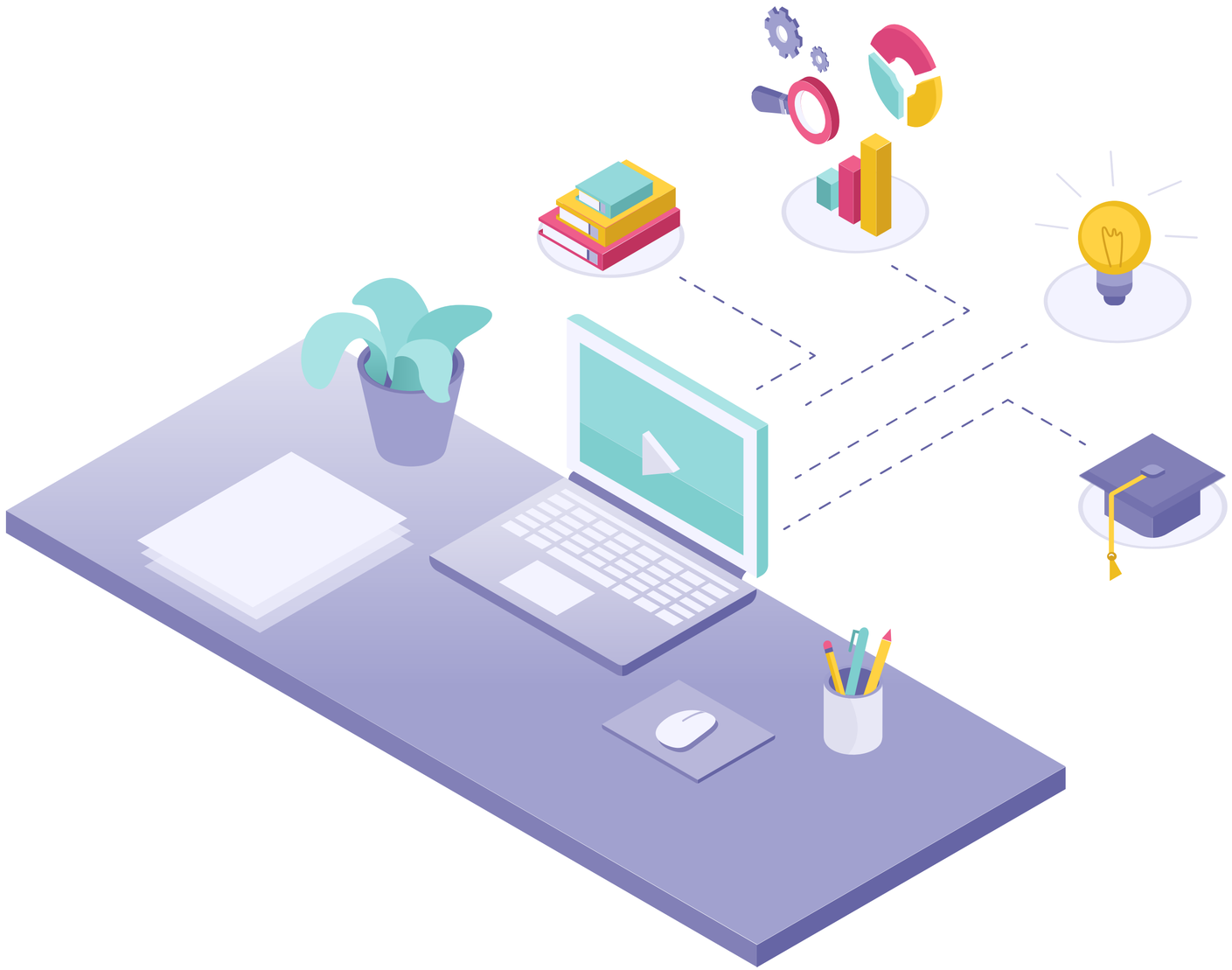


Amazon EC2

On-premises

- Service de migrations d'application et serveurs vers le Cloud AWS, une courte fenêtre de basculement, généralement mesurée en minutes
- Prend en charge les serveurs physiques, VMWare vSphere, Microsoft Hyper-V…

AWS Transfer Family

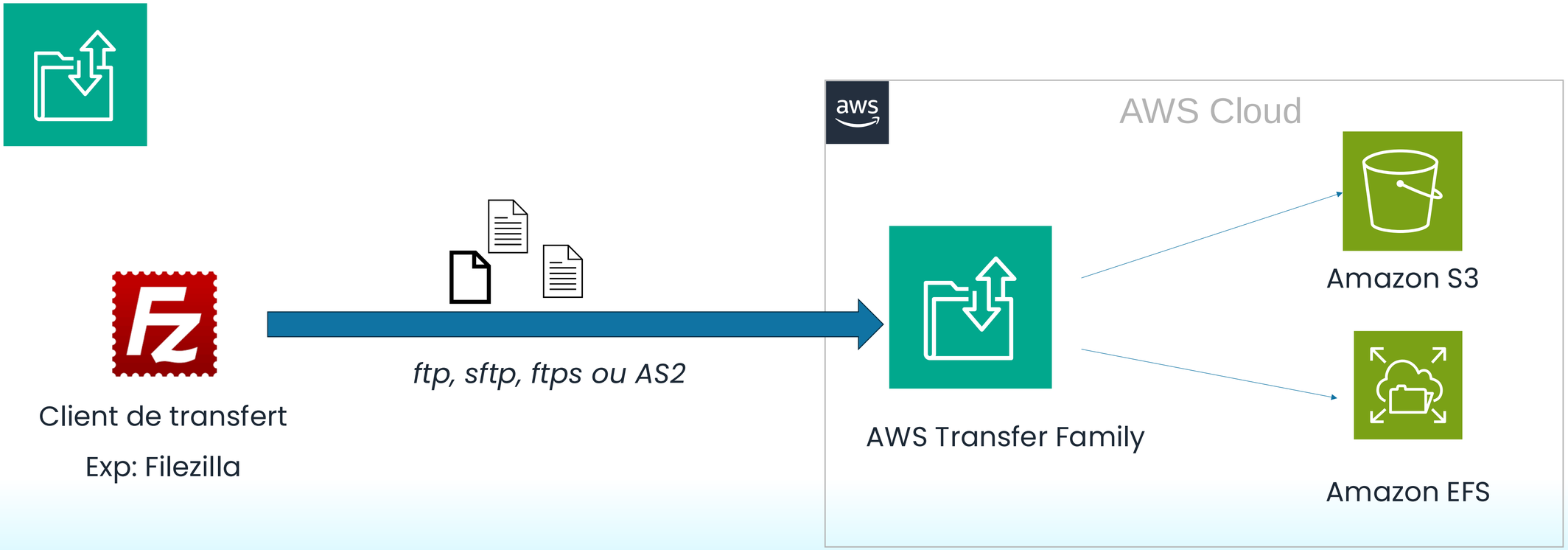


AWS Transfer Family

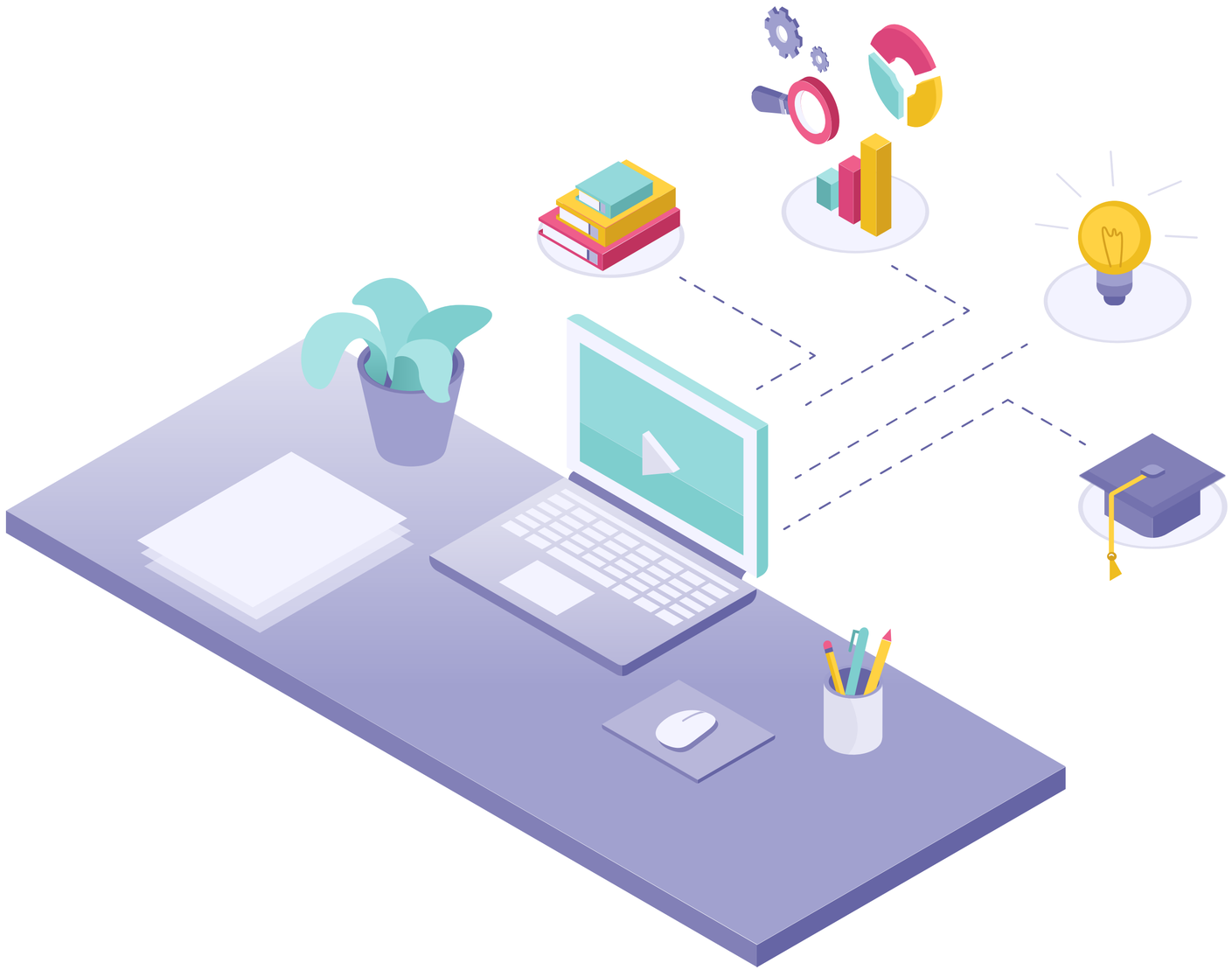
Service géré pour transférer vos fichiers dans le Cloud AWS via les protocoles

FTP, SFTP, FTPS et AS2

Prend en charge les services AWS : Amazon S3, Amazon EFS

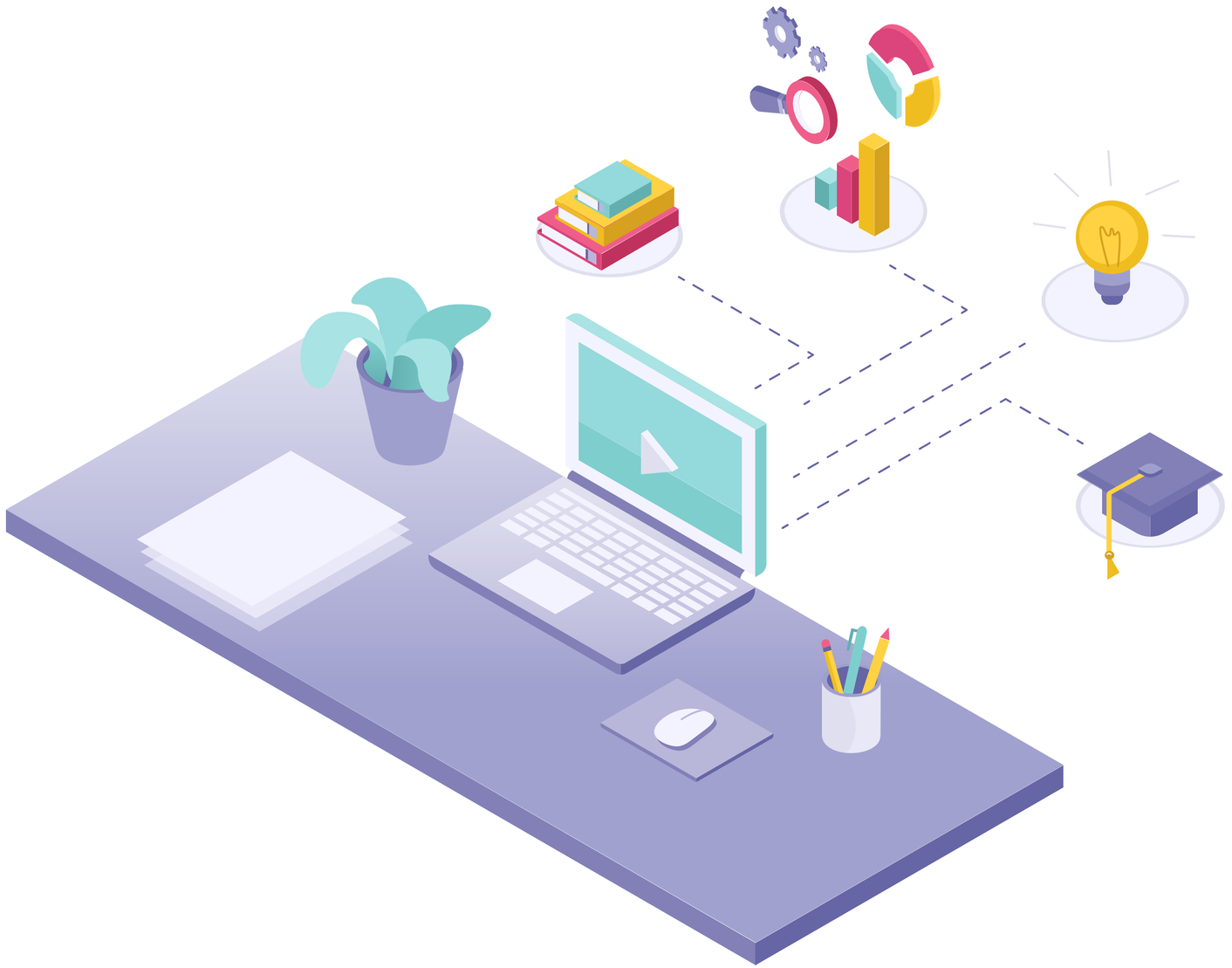


AWS DataSync



AWS DataSync

Disaster Recovery



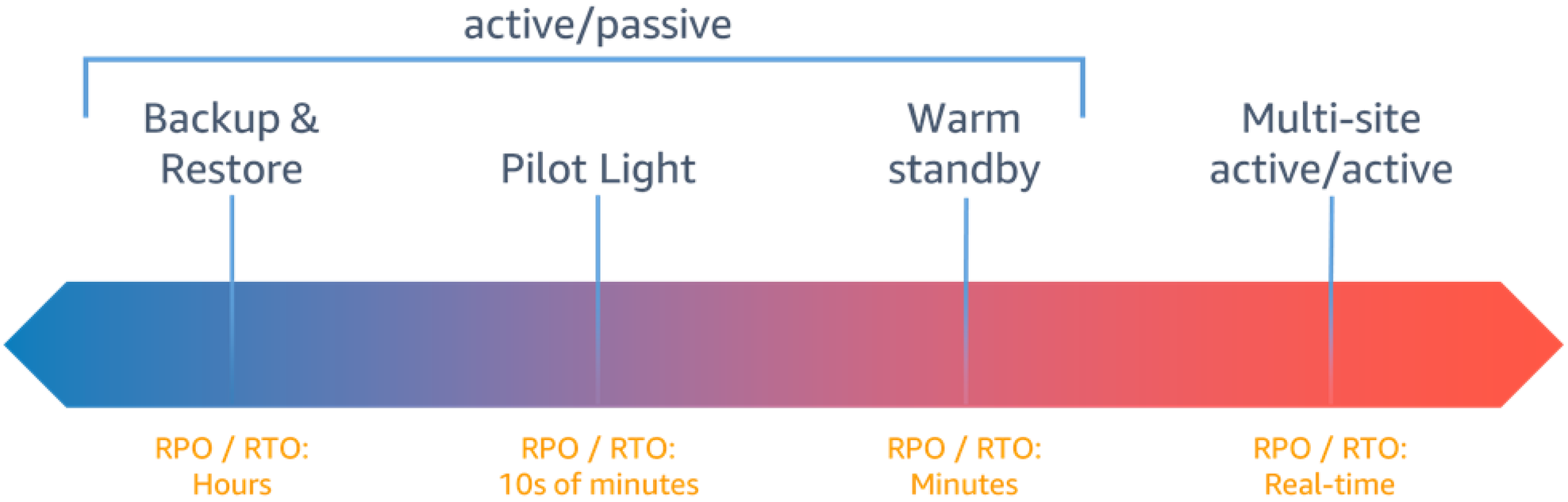
Disaster Recovery

En français : « Reprise après sinistre »

Sinistre : catastrophe naturelle, défaillance technique, panne régionale, erreur humaine,...

Disaster Recovery -> « processus de préparation et de récupération après un sinistre »

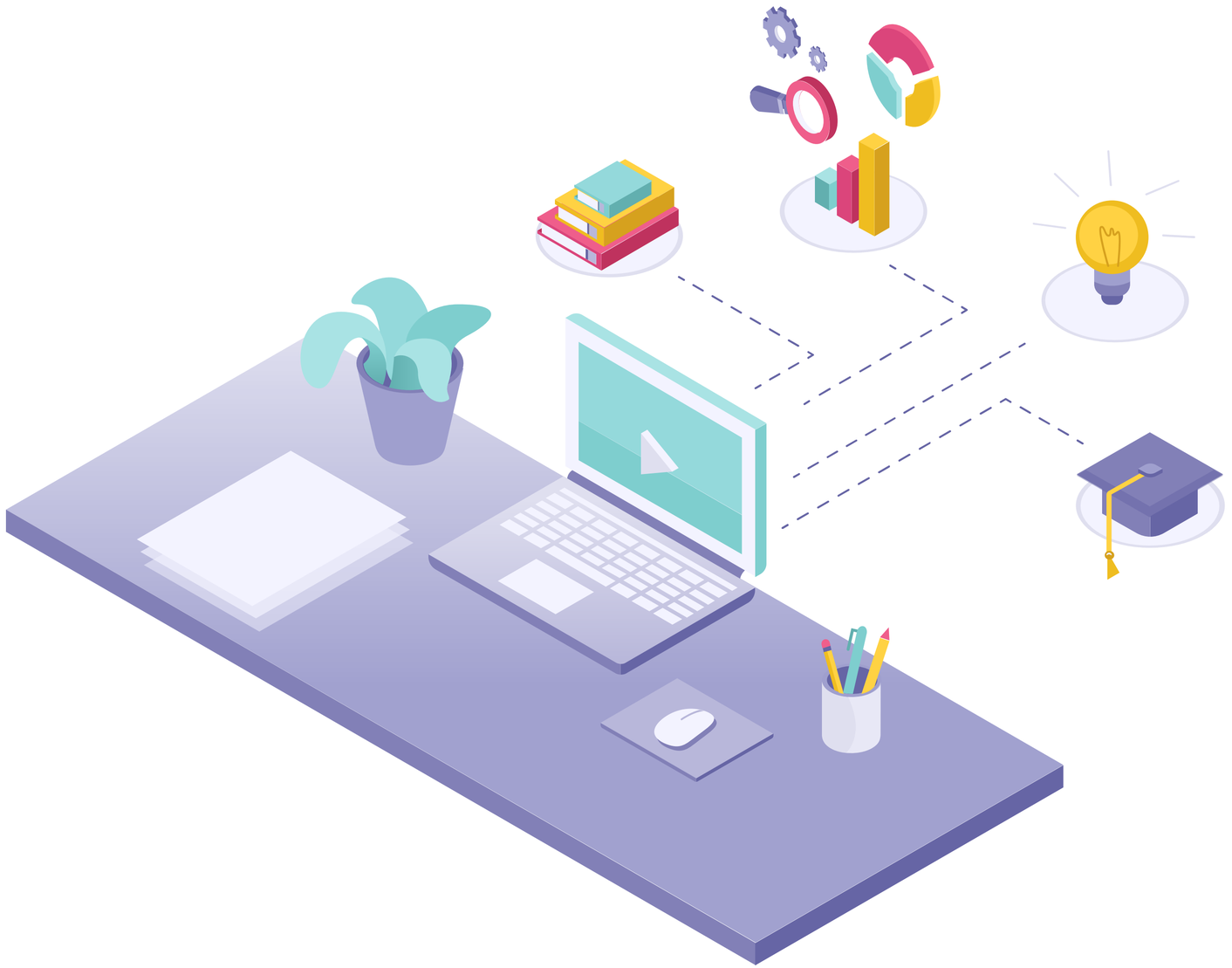
Disaster Recovery : les différentes approches



RTO = Recovery Time Objective

RPO = Recovery Point Objective

Disaster Recovery : les différentes approches



Backup & Restore

En français : « **Sauvegarde et Restauration** »

Les **Backups** sont copiés dans une région secondaire

Option **la moins couteuse** mais RPO/RTO plus élevés -> **Démarrage à froid**

RPO/RTO : Heures



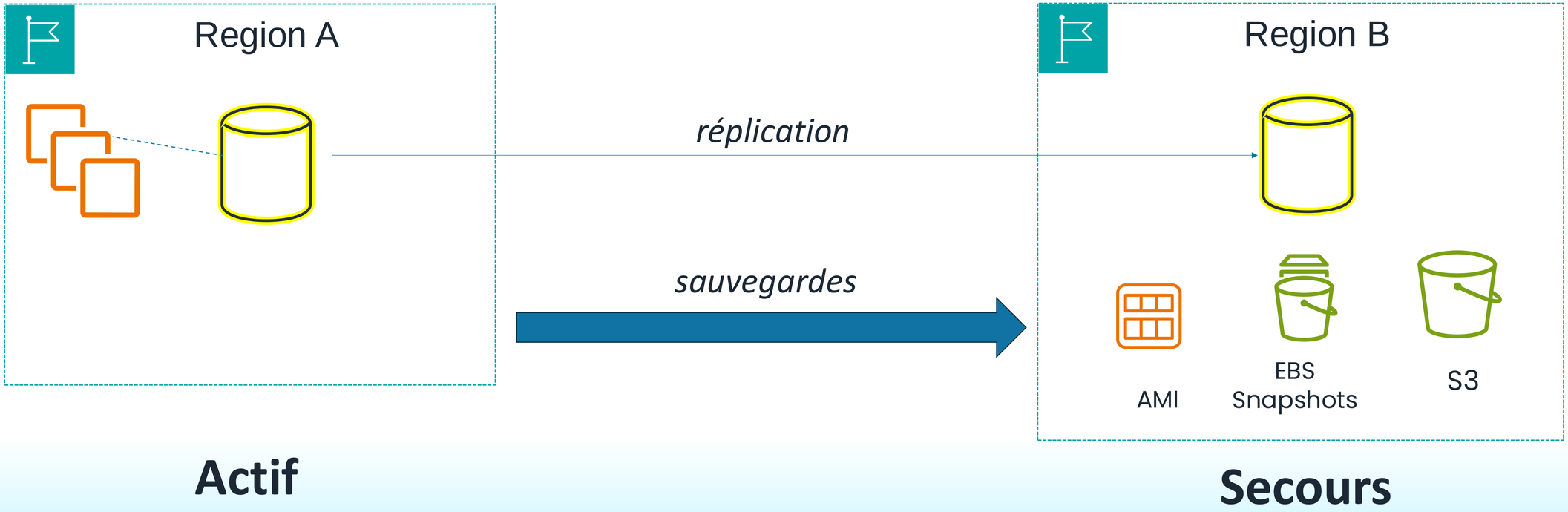
Pilot Light

En français : « **Environnement de veille** »

Les données sont **répliquées** vers la région de secours

L'élément principal de l'application est démarré. Exp : base de données

RPO/RTO : Dizaines de minutes



Warm Standby

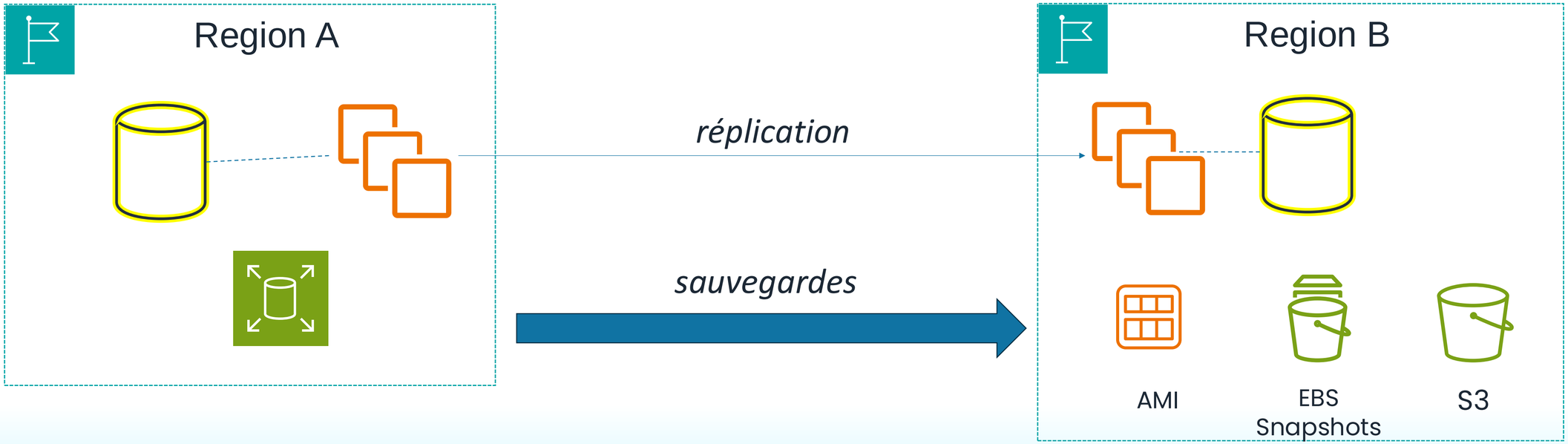
En français : « ***Secours à chaud*** »

Les données sont répliquées vers la région de secours

Une **copie réduite** de votre application est active dans la région de secours

L'environnement de secours peut traiter des requêtes à tout moment

RPO/RTO : quelques minutes



Muti-Site Active/Active

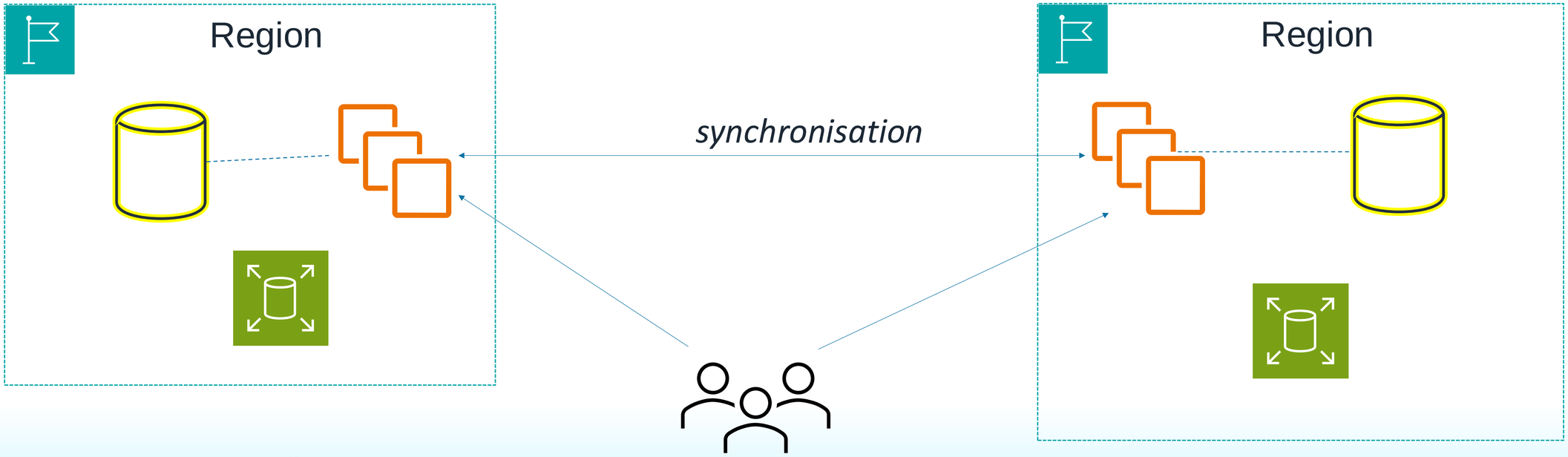
En français : « ***Actif/Actif multi-site***»

Les données sont **synchronisées** entre les deux régions

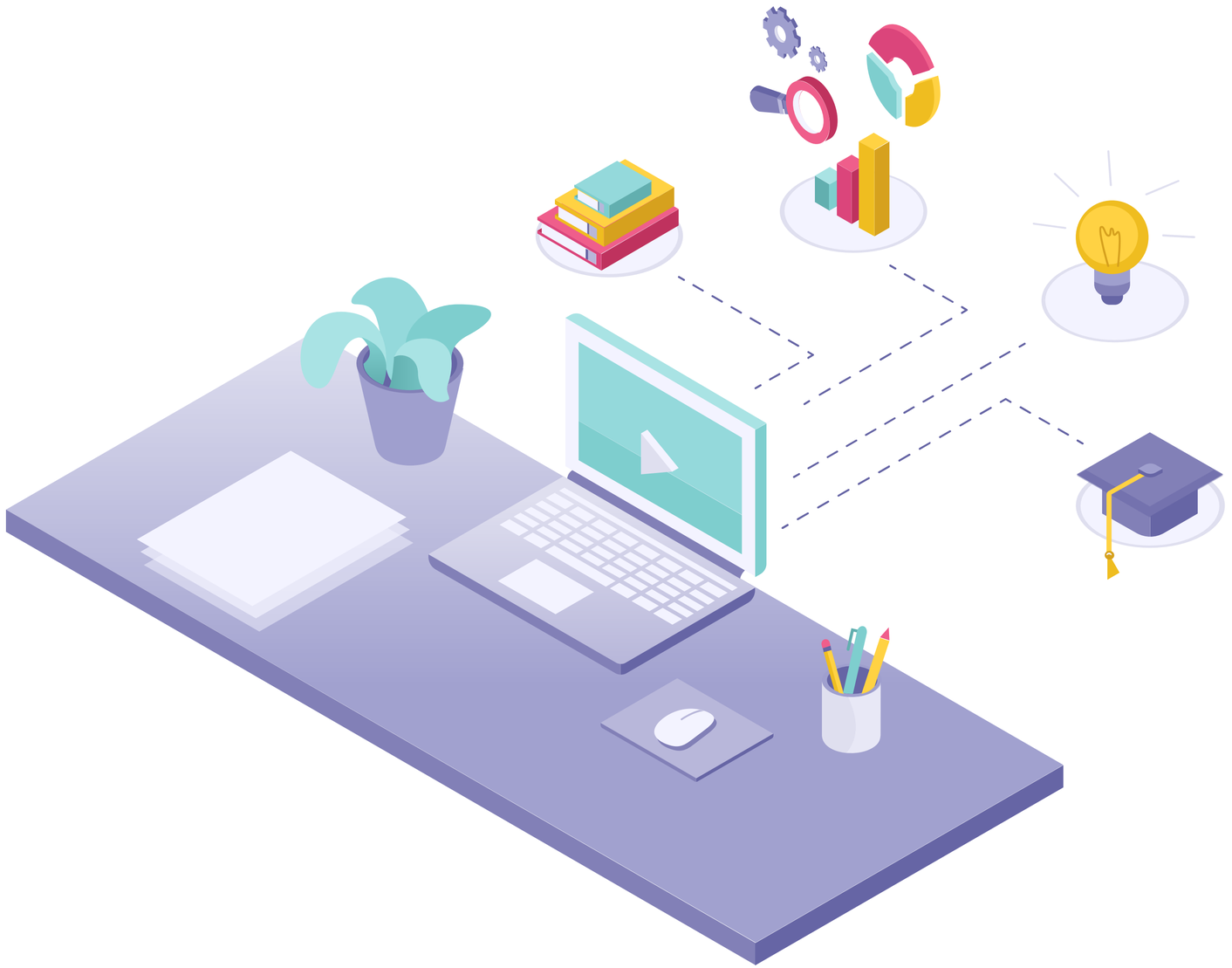
Les deux régions sont **actives** et reçoivent du trafic

RPO/RTO : temps réel

Approche la plus couteuse et complexe



AWS Backup



AWS Backup

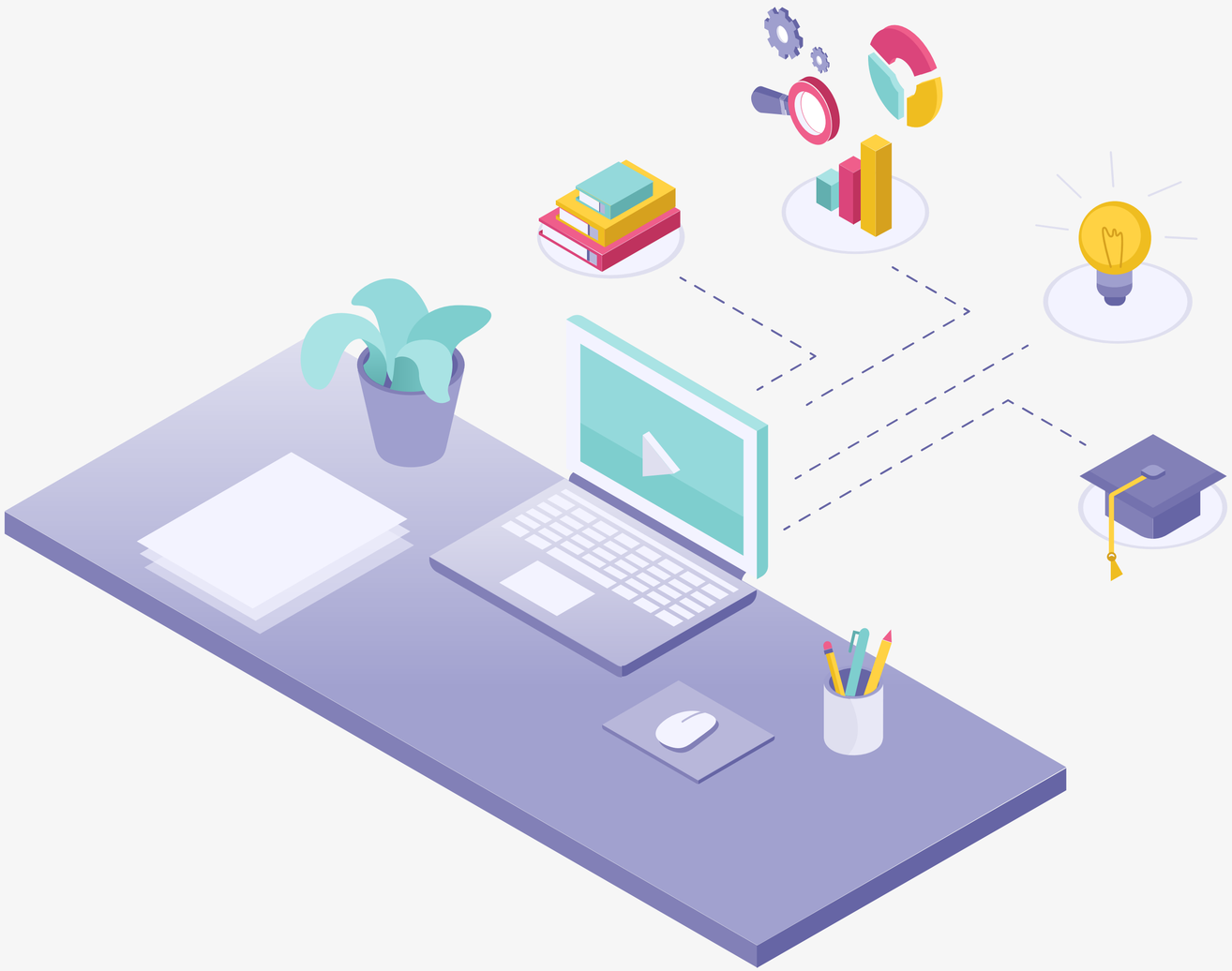


Permet **d'automatiser les sauvegardes** (*backups*) de vos ressources

Services AWS supportés : Amazon S3, Amazon FSx, Amazon EC2, Amazon RDS, Amazon EBS, Amazon EFS, Vmware (sur site & Cloud),...

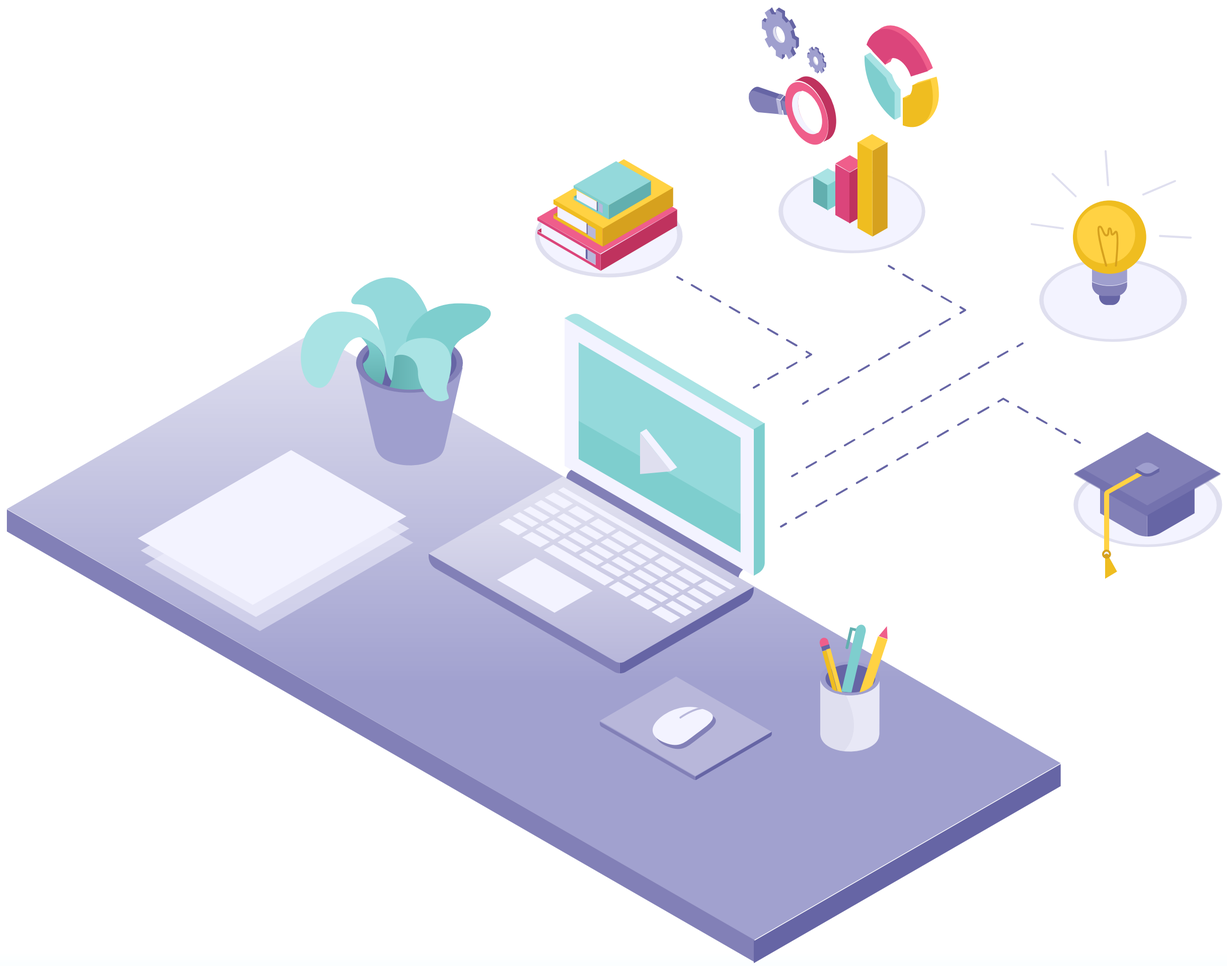
Fonctionnalités clés

- Création de **plans de sauvegarde** (fréquence, rétention,...)
- **Vue centralisée** de toutes vos sauvegardes
- Politiques de **rétention**
- Opérations de **restauration**
- .....

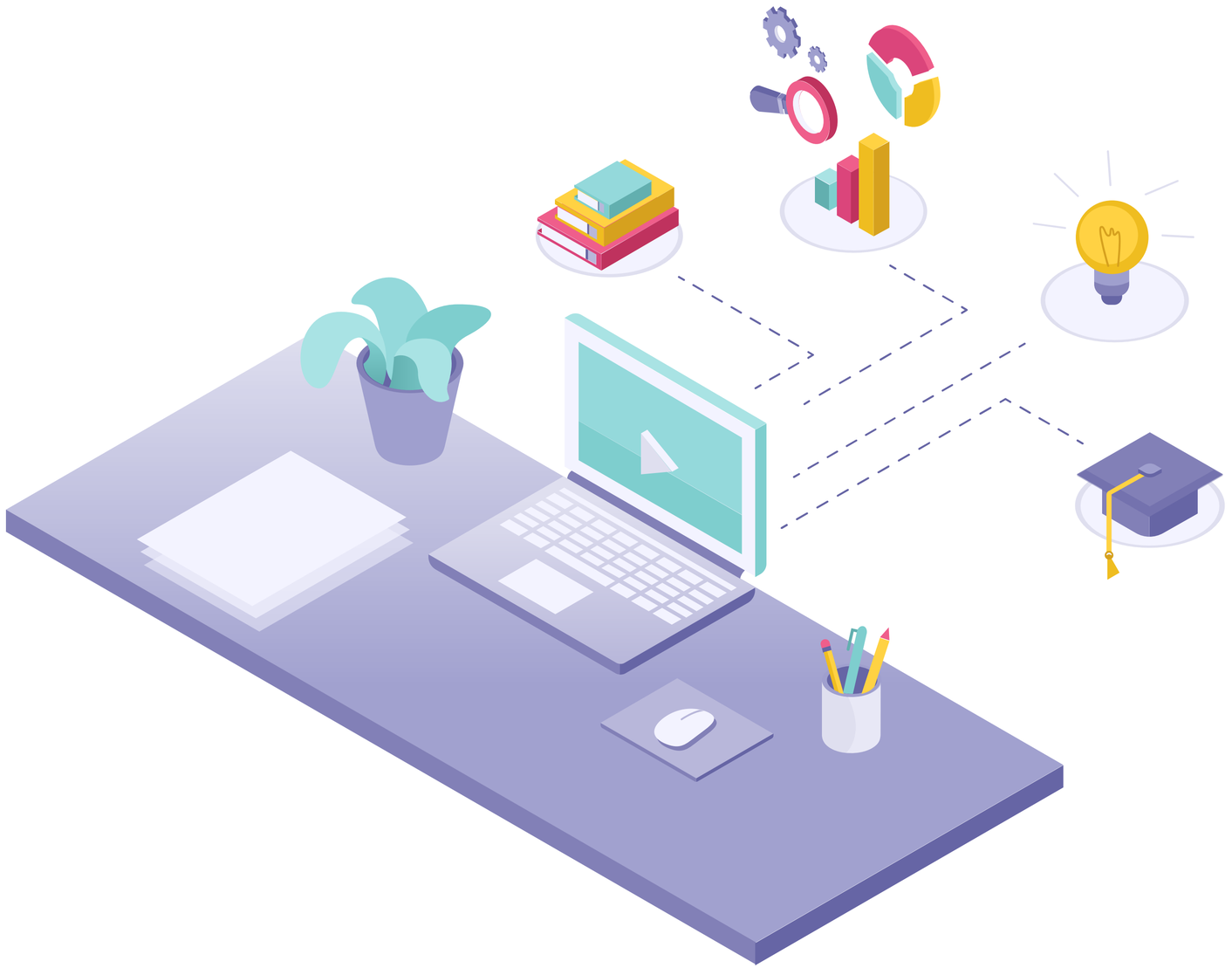


FIN DU MODULE

Module 14 : Architecture & Bonnes pratiques



AWS Well-Architected Framework



LeCloudFacile.com

AWS Well-Architected Framework

Décrit les concepts clés, les principes de conception et les bonnes pratiques architecturales pour concevoir et exécuter des charges de travail dans le cloud.

1

Pilier Excellence opérationnelle

Le pilier Excellence opérationnelle est axé sur l'exécution et la supervision des systèmes et sur le perfectionnement permanent des processus et des procédures.

2

Pilier Sécurité

Le pilier Sécurité est axé sur la protection des informations et des systèmes.

3

Pilier Fiabilité

Le pilier fiabilité met l'accent sur le fait que les charges de travail remplissent leur fonction d'origine et sur la récupération rapide après sinistre pour répondre à la demande.

4

Pilier Efficacité des performances

Le pilier Efficacité des performances donne priorité à l'allocation structurée et optimisée des TI et des ressources de calcul.

5

Pilier Optimisation des coûts

Le pilier Optimisation des coûts est axé sur l'évitement des coûts inutiles.

6

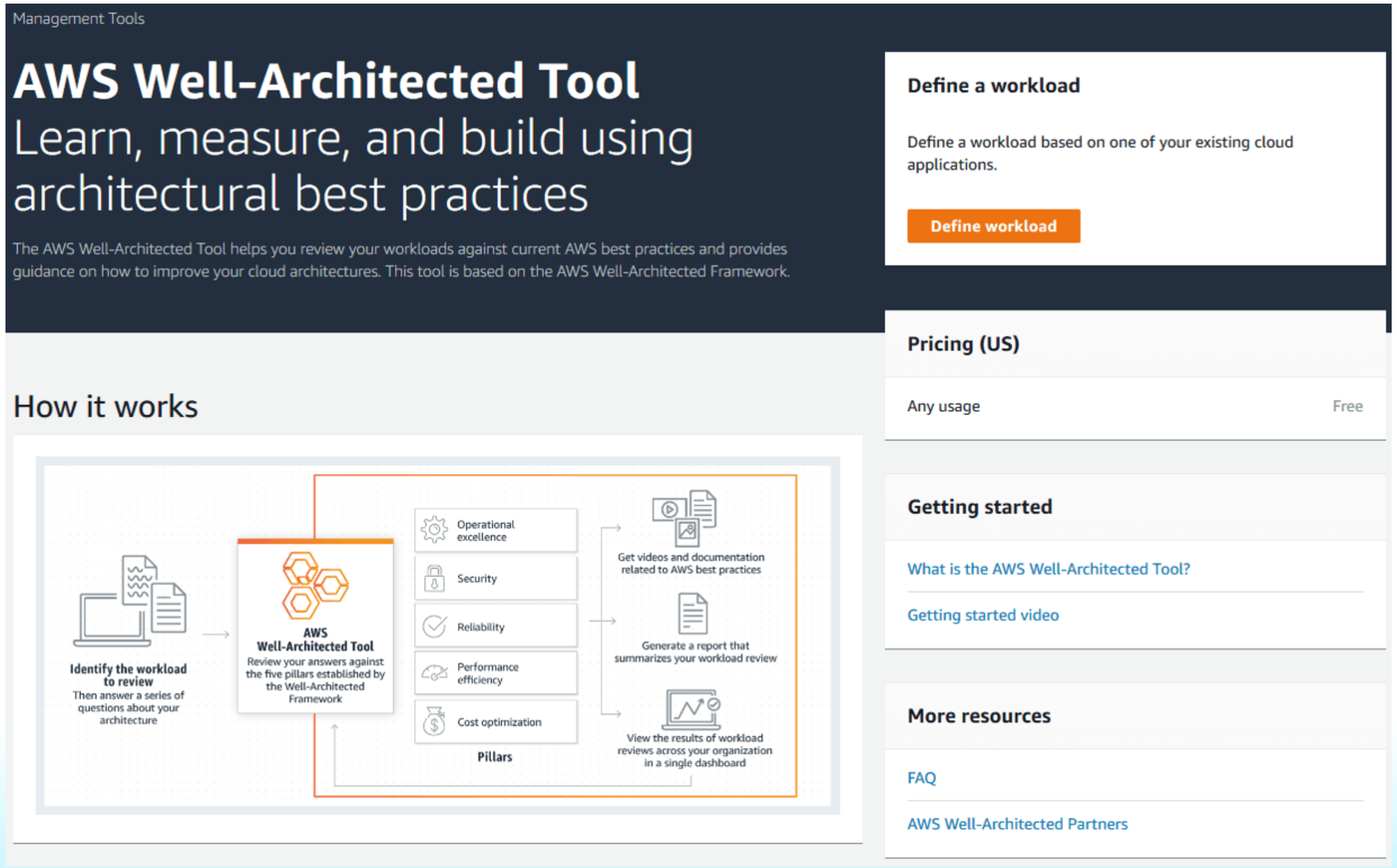
Pilier Développement durable

Le pilier Développement durable met l'accent sur la réduction des impacts sur l'environnement de l'exécution des charges de travail dans le cloud.

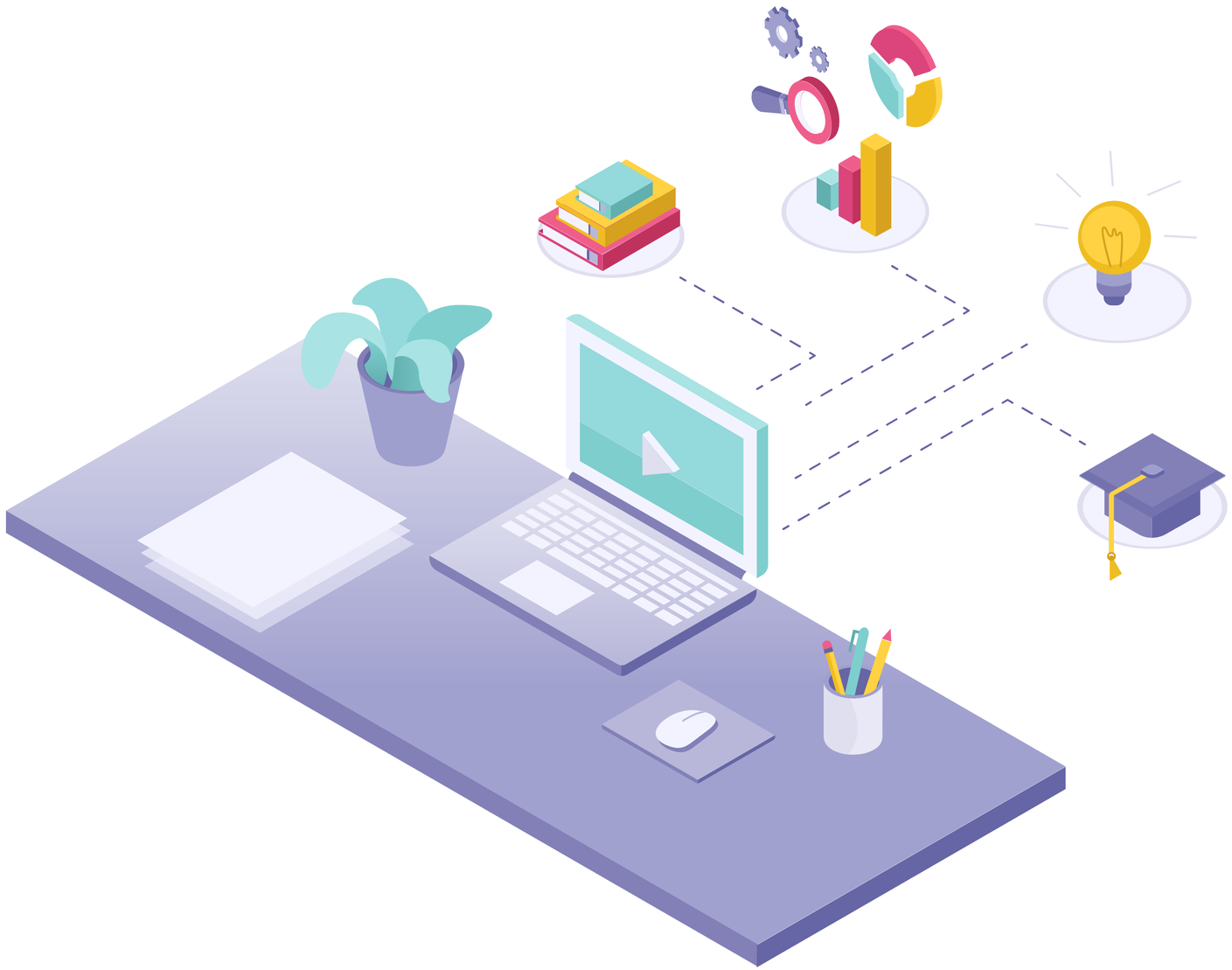
AWS Well-Architected Tool

Outil qui permet de faire des revues de vos charges de travail (workloads)

Basé sur les bonnes pratiques du cadre AWS Well-Architected



Bonnes Pratiques AWS



LeCloudFacile.com

Quelques bonnes pratiques de sécurité



- **Séparation** des comptes AWS (AWS Organizations)
- Principe du **Grant Least privilege**
- **MFA** pour l'utilisateur racine et tous les utilisateurs IAM
- Préférez les informations d'identification **temporaires** (Exp: IAM Role)
- **Chiffrez** vos données au repos (KMS) et en transit (ACM)
- Activez **CloudTrail**
- **Segmentation** réseau (subnets public/privés,..)

Quelques bonnes pratiques de fiabilité



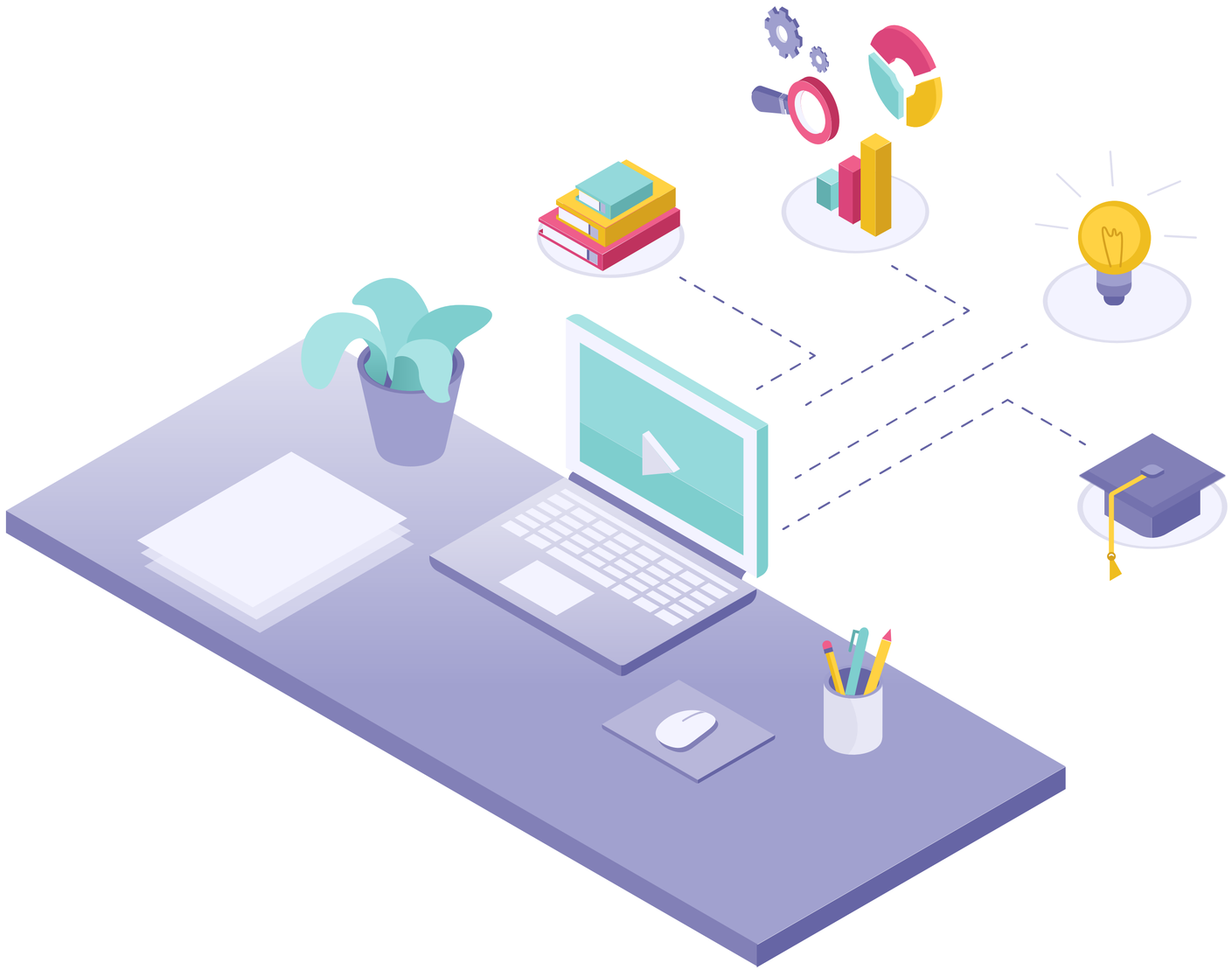
- Répartissez vos serveurs sur plusieurs **AZ**
- Privilégiez la **mise à l'échelle horizontale** (EC2 Auto Scaling) plutôt que verticale
- Surveiller les limites de services avec Trusted Advisor (AWS Qotas pour les augmenter)
- Sauvegarder vos données et applications : Snapshots (EBS, RDS, AMI,...), AWS Backup,...
- Avoir un plan de reprise après sinistre (**Disaster Recovery**) et le tester

Quelques bonnes pratiques de gestion des coûts



- Mettez en place la **facturation consolidée** et activez **Cost Allocation Tags**
- **Optimisation technique** : AWS Compute Optimizer, Right-sizing (métriques CloudWatch), Serverless
- **Optimisation financière** : Savings Plans (1 ou 3 ans)
- Surveillez vos coûts avec **AWS Budgets**
- **Analysez vos dépenses** avec AWS Cost Explorer
- **Prévoyez vos coûts** avec AWS Pricing Calculator, AWS Cost Explorer (Forecast)

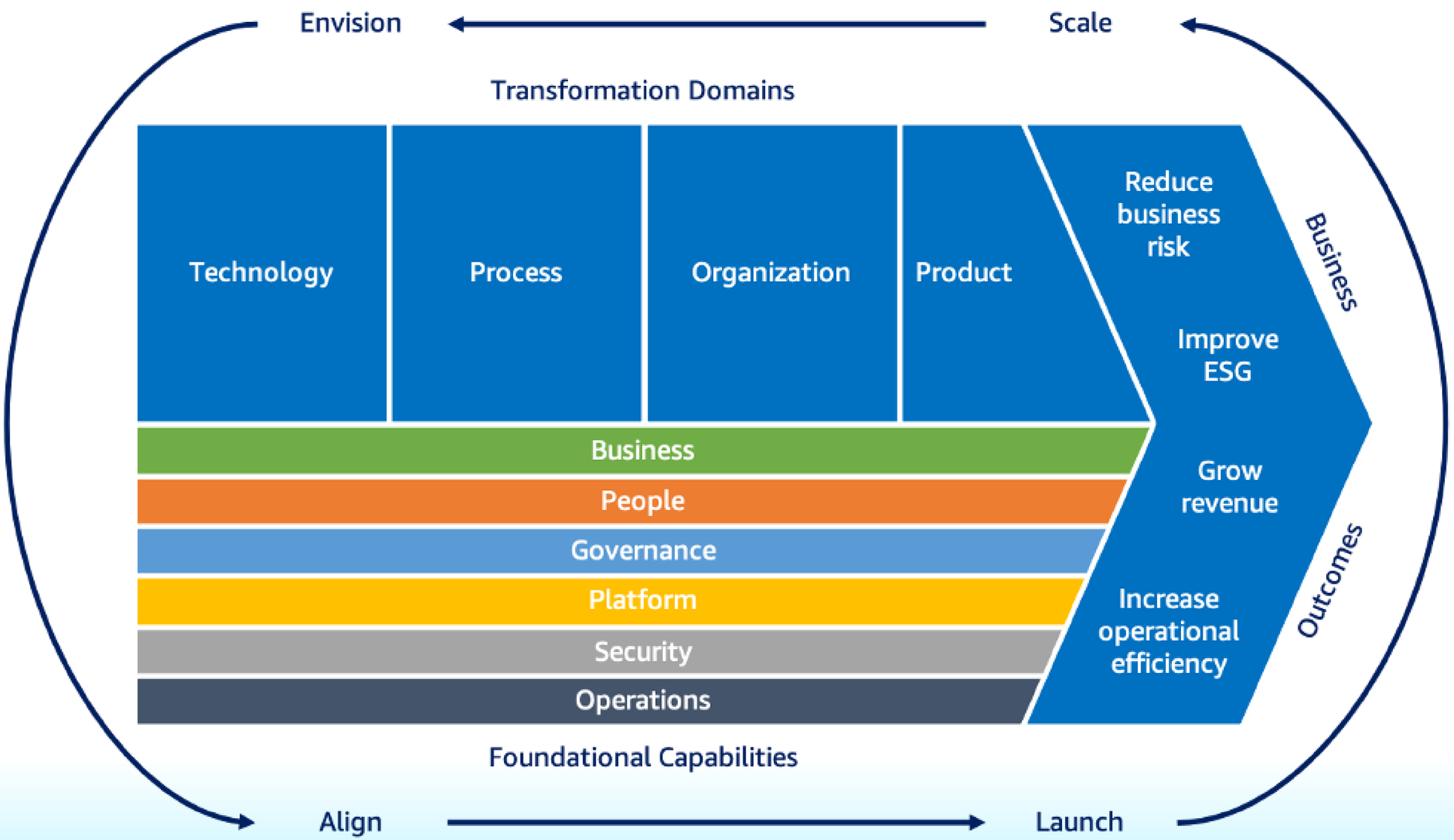
AWS CAF



AWS CAF (Cloud Adoption Framework)

- Ensemble de **bonnes pratiques/outils/conseils** qui aident les entreprises à migrer vers le Cloud
- **Avantages** : Réduire les risques, Accélérer l'innovation, Améliorer l'agilité
- **AWS CAF permet aux entreprises :**
- -> D'obtenir des **Résultats** : ESG, Revenus, Risque --, Efficacité +++
- -> grâce à l'adoption de **capacités fondamentales**
- -> regroupées en **6 Perspectives**
- -> qui permettent la transformation dans **plusieurs Domaines**
- -> selon un **modèle itératif**

Parcours de transformation vers le Cloud



Capacités fondamentales

- AWS CAF identifie un ensemble de **capacités** (« *capabilities* ») essentielles à toute transformation Cloud réussie pour une entreprise
- -> Ces **capacités** (« *capabilities* ») sont regroupées en **6 perspectives** :

Business Perspective	People Perspective	Governance Perspective
Platform Perspective	Security Perspective	Operations Perspective

AWS CAF : Perspectives

1 Business perspective

« La perspective **Business** permet de s'assurer que vos investissements dans le cloud accélèrent vos **ambitions de transformation numérique et les résultats de l'entreprise**. »



AWS CAF : Perspectives

2 People perspective

« La perspective **People** jette une passerelle entre la technologie et l'entreprise, accélérant la transition vers le cloud pour aider les organisations à évoluer plus rapidement vers une culture de croissance continue, de formation, où le changement devient normal, en mettant **l'accent sur la culture, la structure organisationnelle, le leadership et la main-d'œuvre**. »



AWS CAF : Perspectives

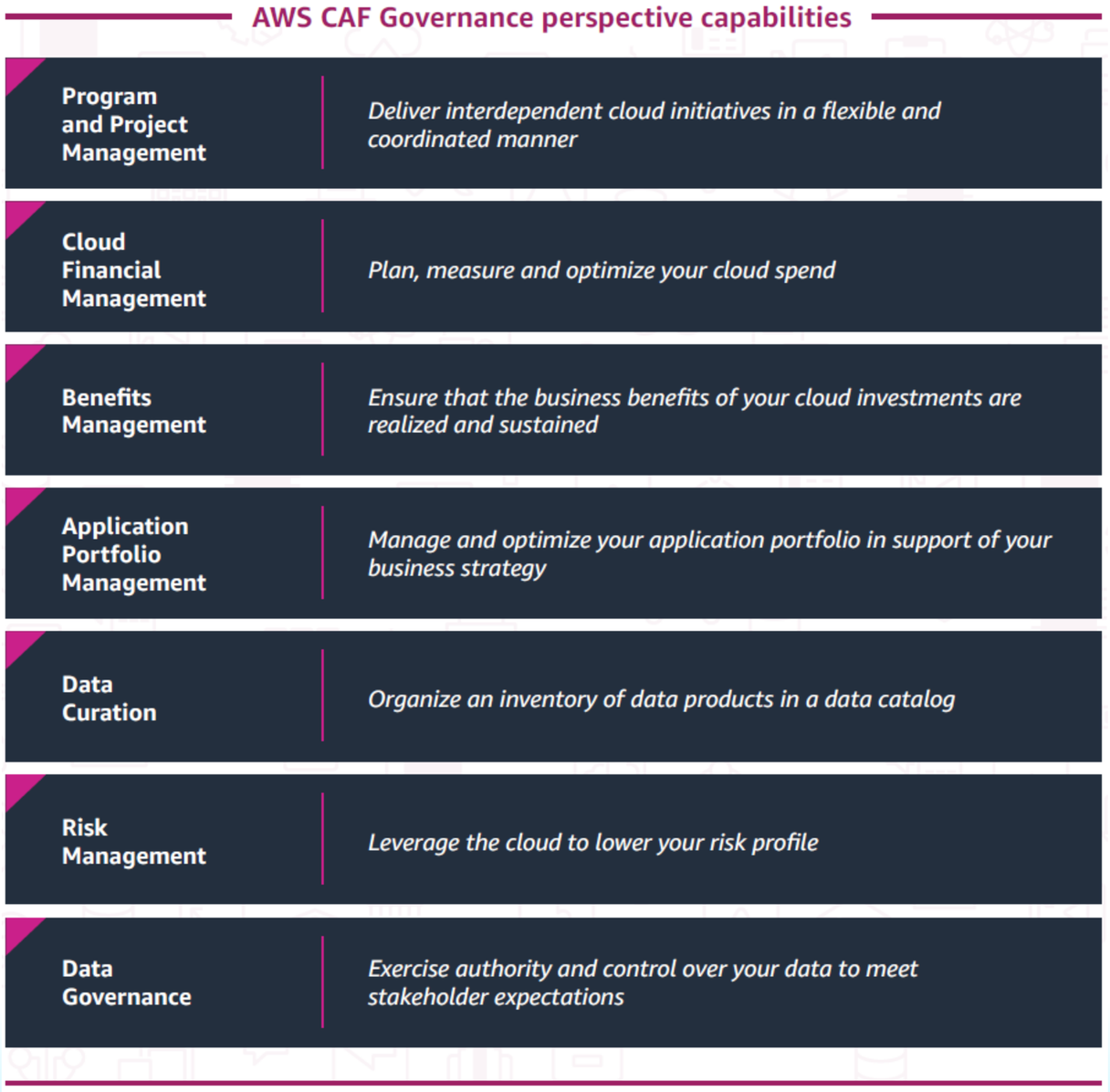
3 Governance perspective

« La perspective **Gouvernance** vous permet

d'orchestrer vos initiatives de cloud computing

tout en maximisant les avantages organisationnels

et en réduisant les risques liés à la transformation. »



AWS CAF : Perspectives

4 Platform perspective

« La perspective **Plateforme** vous aide à **construire une plateforme de cloud hybride, évolutive et d'entreprise**, à moderniser les charges de travail existantes et à mettre en œuvre de nouvelles solutions cloud natives. »



AWS CAF : Perspectives

5 Security perspective

« La perspective **Sécurité** permet d'assurer la **confidentialité, l'intégrité et la disponibilité de vos données et de vos charges de travail** dans le cloud. »



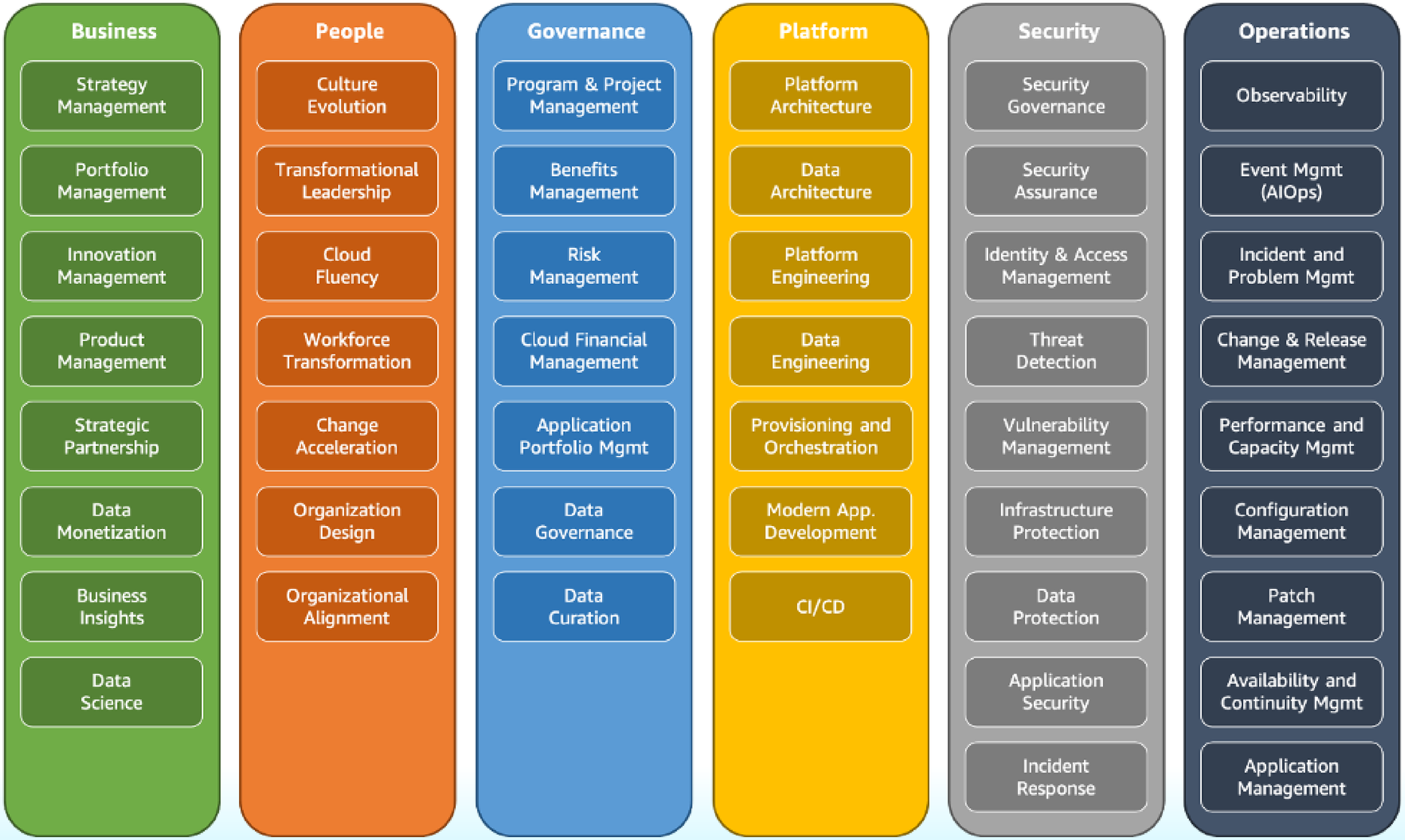
AWS CAF : Perspectives

6 Operations perspective

« La perspective **Opérations** permet de garantir que **vos services cloud sont fournis à un niveau** qui répond aux besoins de votre entreprise. »



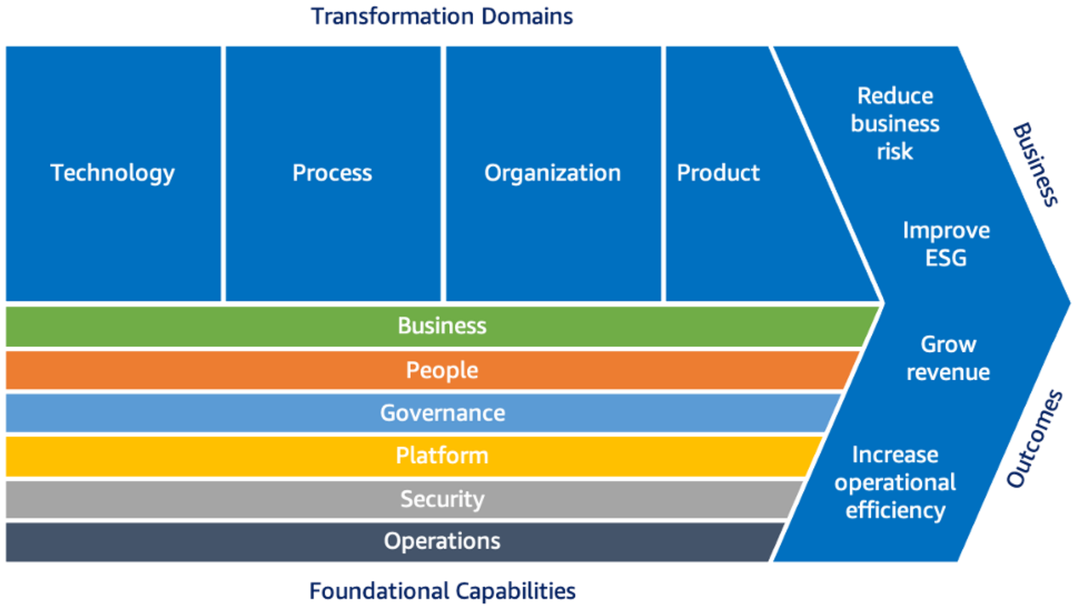
AWS CAF : Perspectives



Domaines de transformation

4 Domaines de transformation

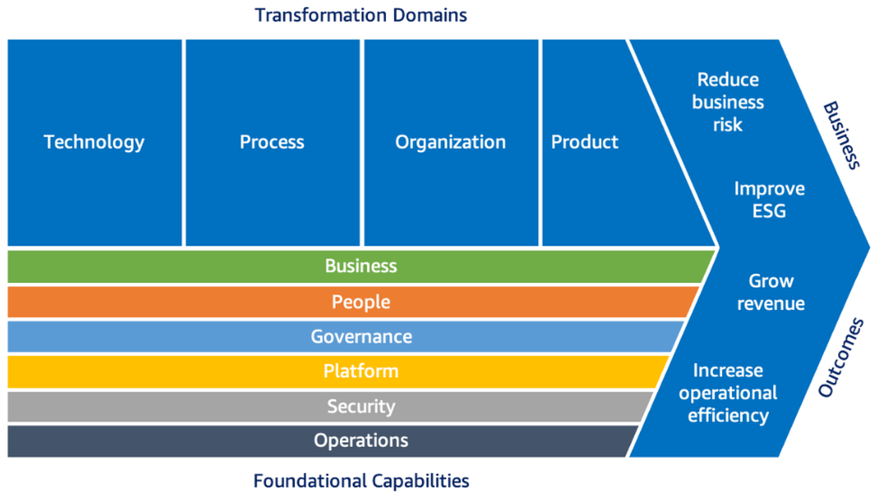
1. Technology
2. Process
3. Organization
4. Product



Domaines de transformation

Domaine Technology

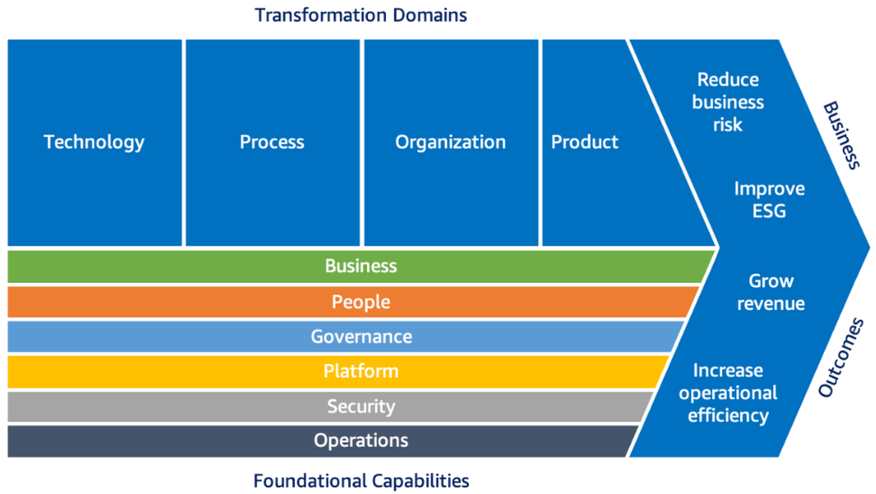
- La transformation technologique se concentre sur l'utilisation du cloud pour migrer et moderniser l'infrastructure, les applications et les plateformes
de données et d'analytique héritées.



Domaines de transformation

Domaine Process

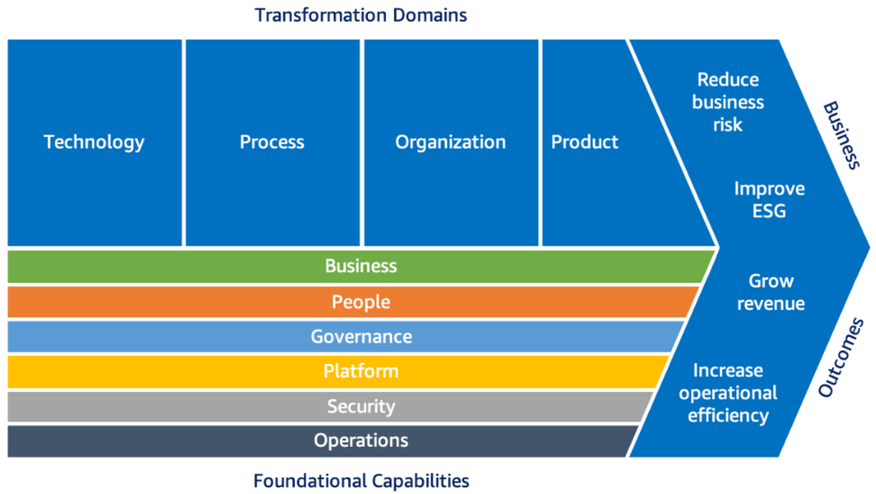
- Se concentre sur la numérisation, l'automatisation et l'optimisation de vos opérations métier.



Domaines de transformation

Domaine Organization

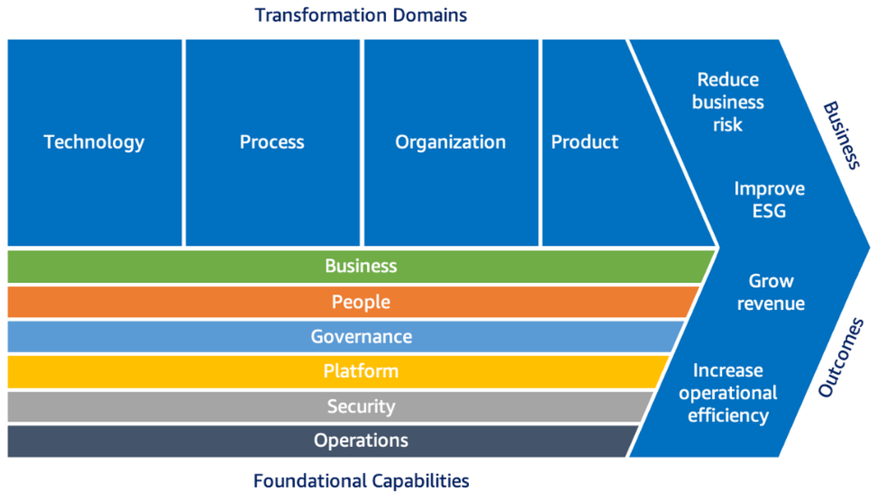
- Se concentre sur la réinvention de votre modèle d'exploitation, la façon dont vos équipes commerciales et technologiques orchestrent leurs efforts afin de créer de la valeur pour le client



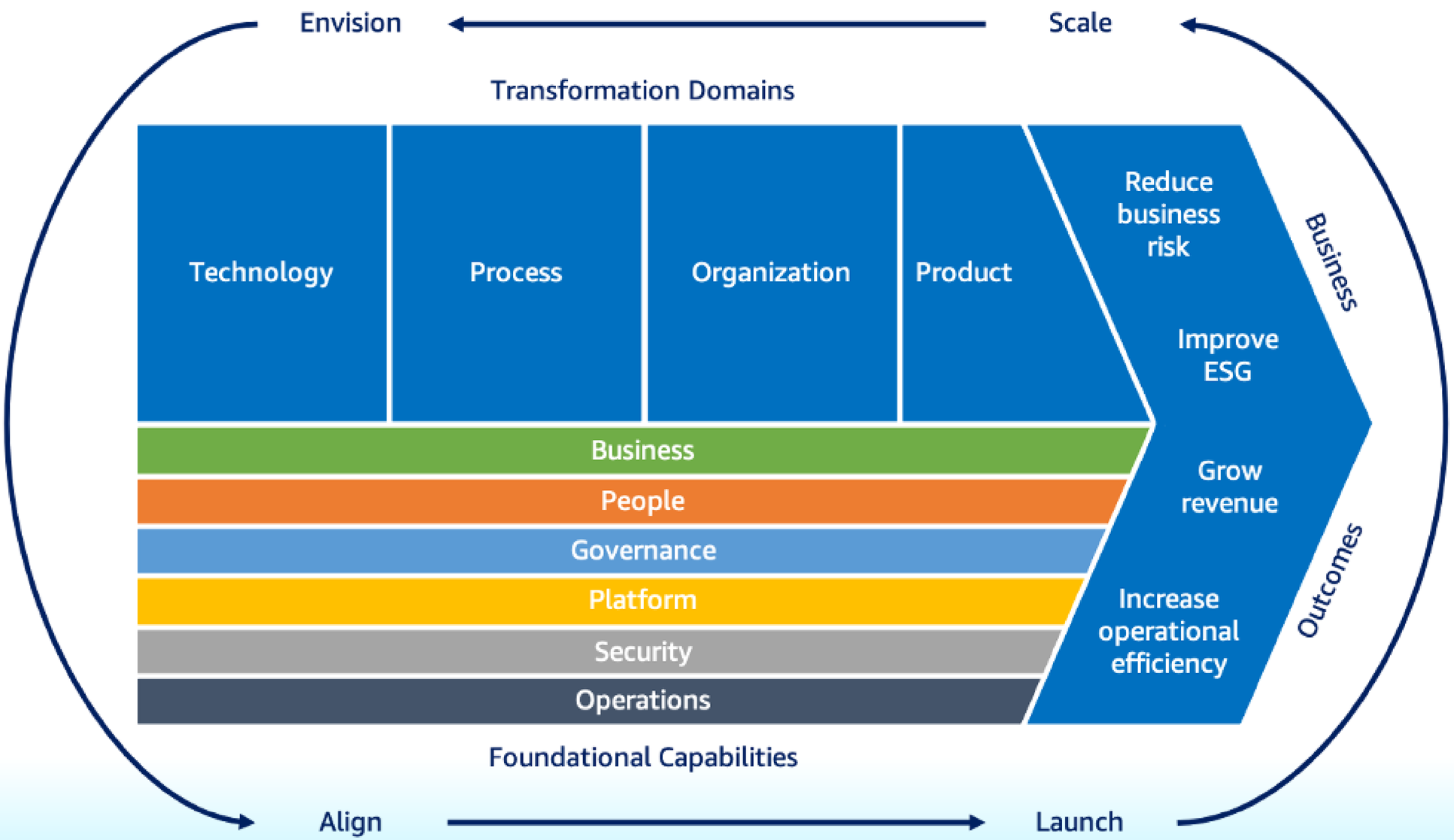
Domaines de transformation

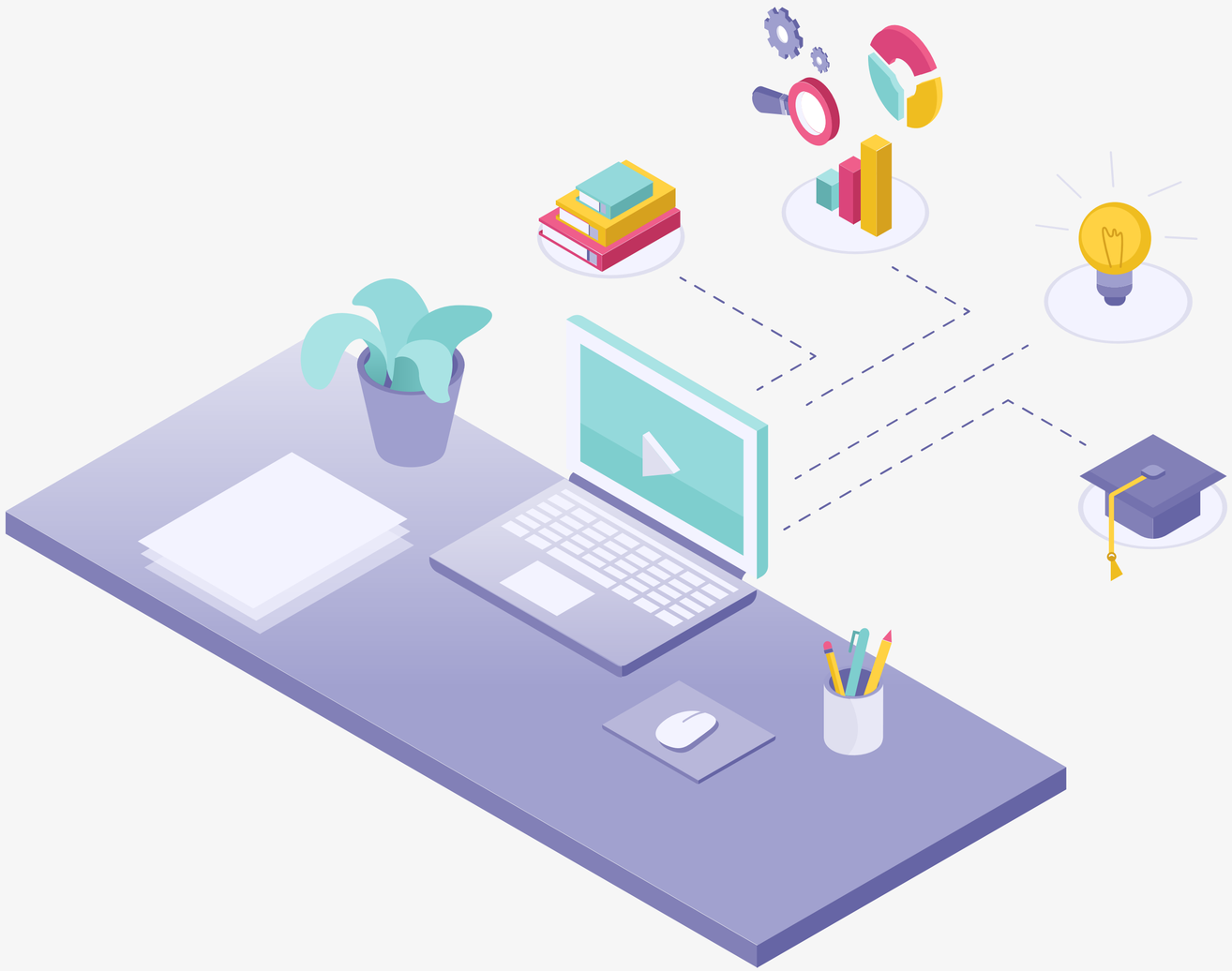
Domaine Product

- Vise à réinventer votre business model en créant de nouvelles propositions de valeur (produits, services) et des modèles de revenus.

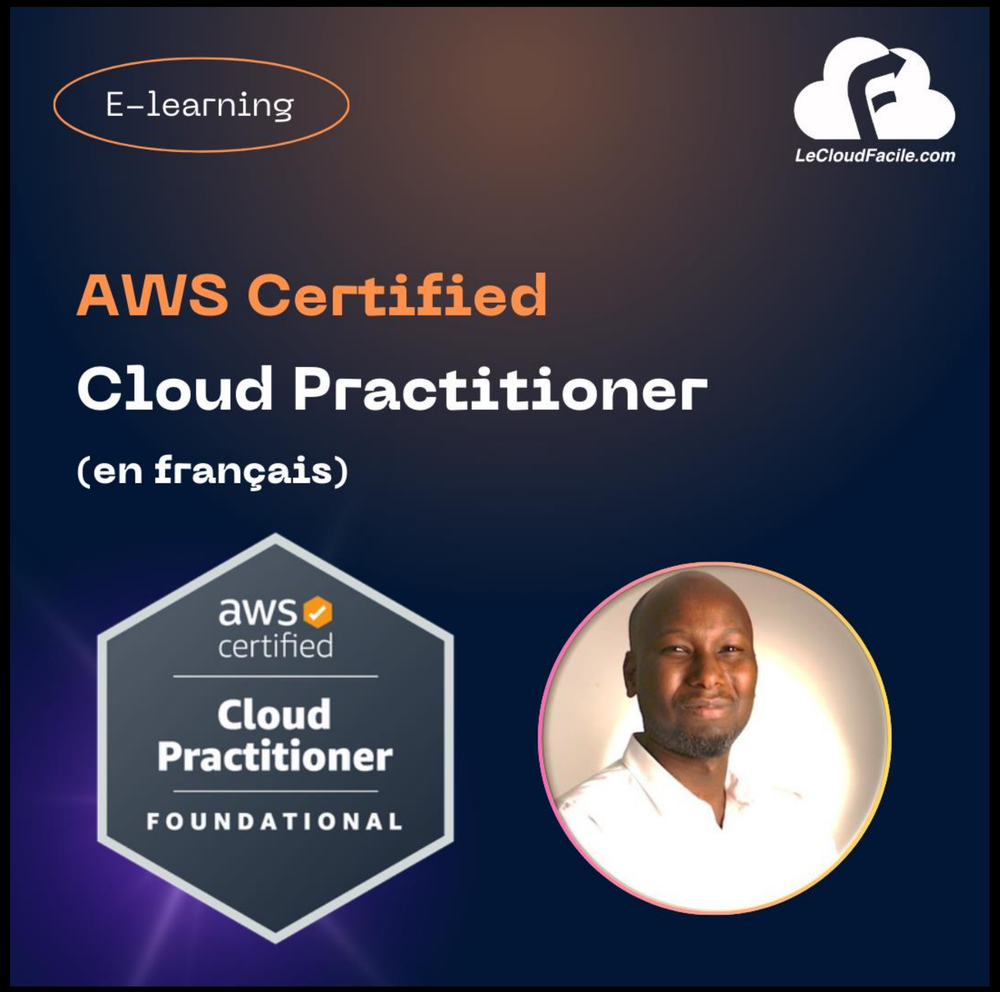


Parcours de transformation vers le Cloud





FIN DU MODULE



www.lecloudfacile.com