



# Services de gouvernance et gestion des couts

Par Lahda Biassou Alphonsine



# Lahda Biassou Alphonsine

## Ingénieure cloud et formatrice





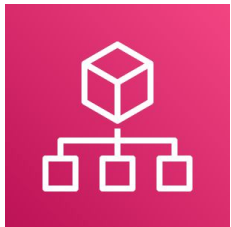
# Plan

- **AWS Organization**
- **AWS Control Tower**
- **AWS Personal Health Dasbord**
- **AWS Config**
- **Amazon GuardDuty**
- **AWS Service Catalog**
- **AWS License Manager**
- **AWS Budget**
- **AWS Cost Explorer**
- **AWS Cost & usage Report**
- **AWS Pricing Calculator**





# AWS Organizatization



AWS  
Organizations

Gestion et application centralisées des politiques sur plusieurs comptes AWS.

- Gestion des comptes par groupe
- Accès aux services AWS basé sur des règles
- Création et gestion automatisées des comptes
- Facturation consolidée
- Basé sur l'API

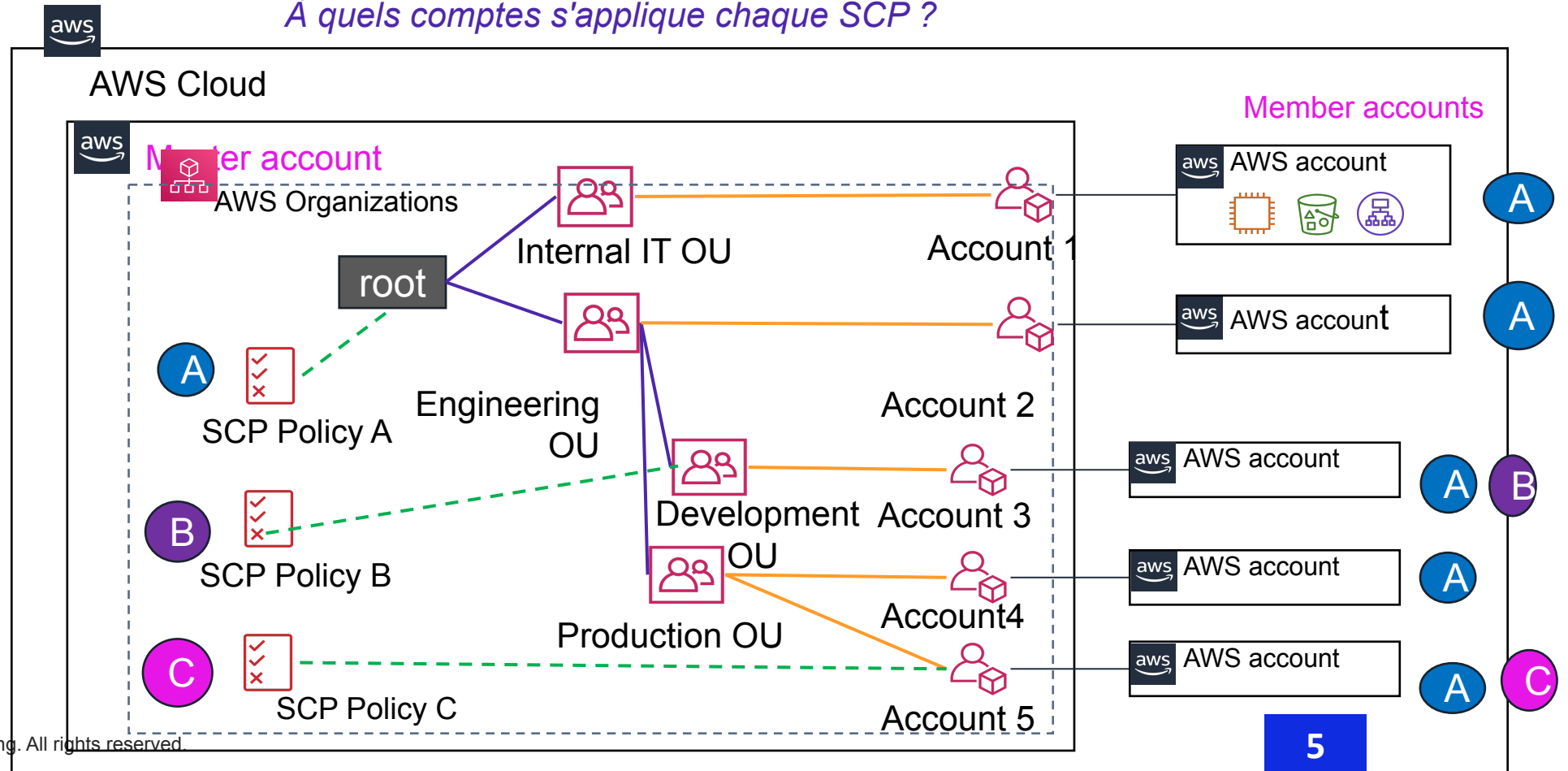


# AWS Organization - illustration

Dans le compte principal AWS Organizations :

1. Créer une hiérarchie d'unités d'organisation (OU)
2. Attribuer des comptes aux OU en tant que comptes membres
3. Définir des politiques de contrôle des services (SCP) qui appliquent des restrictions de permissions à des comptes membres spécifiques.
4. Attacher les SPC à la racine, aux OU ou aux comptes

*À quels comptes s'applique chaque SCP ?*





# Exemple d'utilisation de SCPs

- **Caractéristiques des politiques de contrôle des services (SCP)**
  - Elles permettent de contrôler les services accessibles aux utilisateurs IAM dans les comptes membres.
  - Les SCP ne peuvent pas être remplacées par l'administrateur local.
  - Les politiques IAM définies dans les comptes individuels restent d'application.
- **Exemples d'utilisation des SCP**
  - Créer une politique qui bloque l'accès à un service ou des actions spécifiques
  - Exemple : Interdire aux utilisateurs de désactiver AWS CloudTrail dans tous les comptes membres.
  - Créer une politique qui autorise un accès complet à des services spécifiques
  - Exemple : Autoriser l'accès complet à Amazon EC2 et CloudWatch
  - Créer une politique qui impose le marquage des ressources



# Plan

- AWS Organization
- **AWS Control Tower**
- AWS Personal Health Dashboard
- AWS Config
- Amazon GuardDuty
- AWS Service Catalog
- AWS License Manager
- AWS Budget
- AWS Cost Explorer
- AWS Cost & usage Report
- AWS Pricing Calculator





# AWS Landing Zone

## Définition

C'est une solution qui permet aux entreprises de configurer rapidement un environnement sécurisé, bien architecturé et multi-compte dans AWS

## Composants



AWS Organization

AWS Service Catalog

AWS Single Sign-On

Control Tower





## AWS Landing Zone -composants techniques



Compte Master



Compte Log Archive (CloudTrail, AWS Config, etc.)



Compte Shared Service (VPN, Direct Connect)

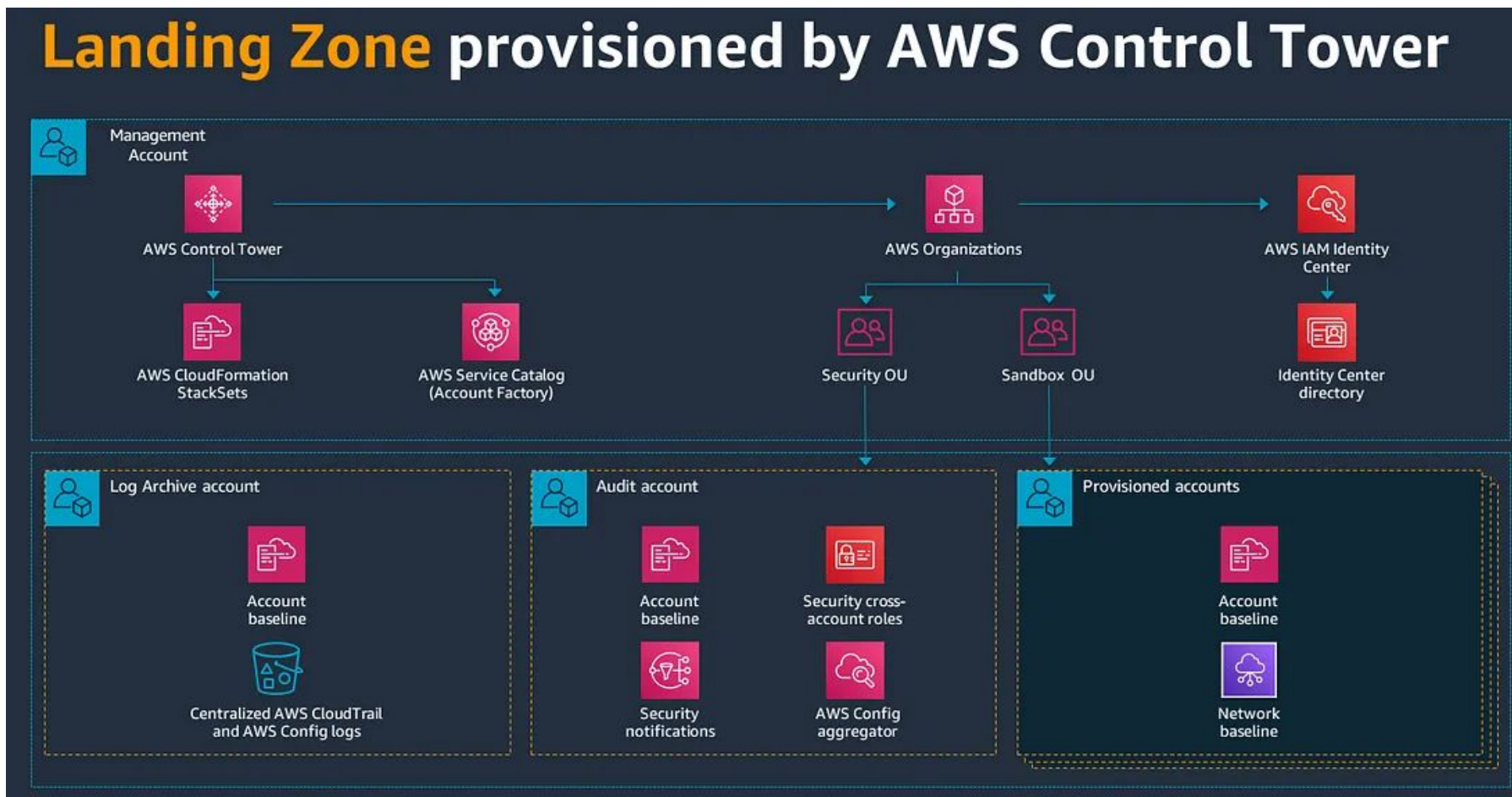


Compte Securite



## AWS Landing Zone -exemple d'architecture

### Landing Zone provisioned by AWS Control Tower





# AWS Control Tower

## Définition

C'est un service qui permet aux entreprises de configurer et de gérer un environnement AWS multi-comptes de manière sécurisée et conforme aux meilleures pratiques. Il automatise le déploiement des environnements multi-comptes, l'application de politiques de sécurité et la surveillance continue de la conformité.

## Fonctionnalités de Control Tower



Landing Zone

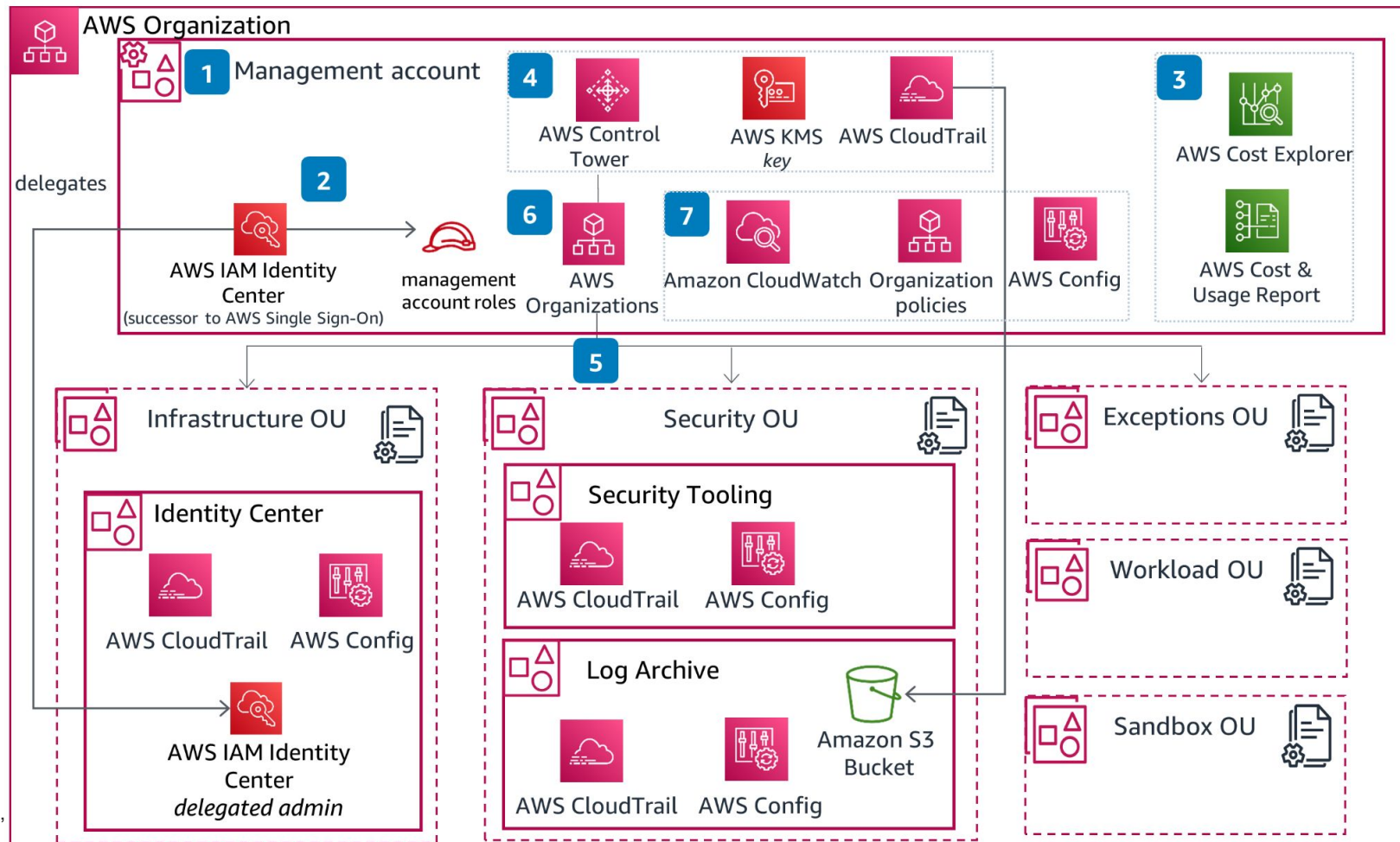
Guardrails

Account Factory

Audit et Conformité



# AWS Control Tower -exemple d'architecture





# Plan

- AWS Organization
- AWS Control Tower
- **AWS Personal Health Dashboard**
- AWS Config
- Amazon GuardDuty
- AWS service Catalog
- AWS License Manager
- AWS Budget
- AWS Cost Explorer
- AWS Cost & usage Report
- **AWS Pricing Calculator**





# AWS Personal Health Dashboard

## Définition



AWS Personal Health Dashboard est un outil qui fournit des alertes et des mesures correctives pour diagnostiquer et résoudre les problèmes liés aux ressources et à l'infrastructure.

## AWS Service Health Dashboard

Tableau de bord de l'état des services AWS permet d'accéder à l'état actuel et à un bilan de santé complet de tous les régions.

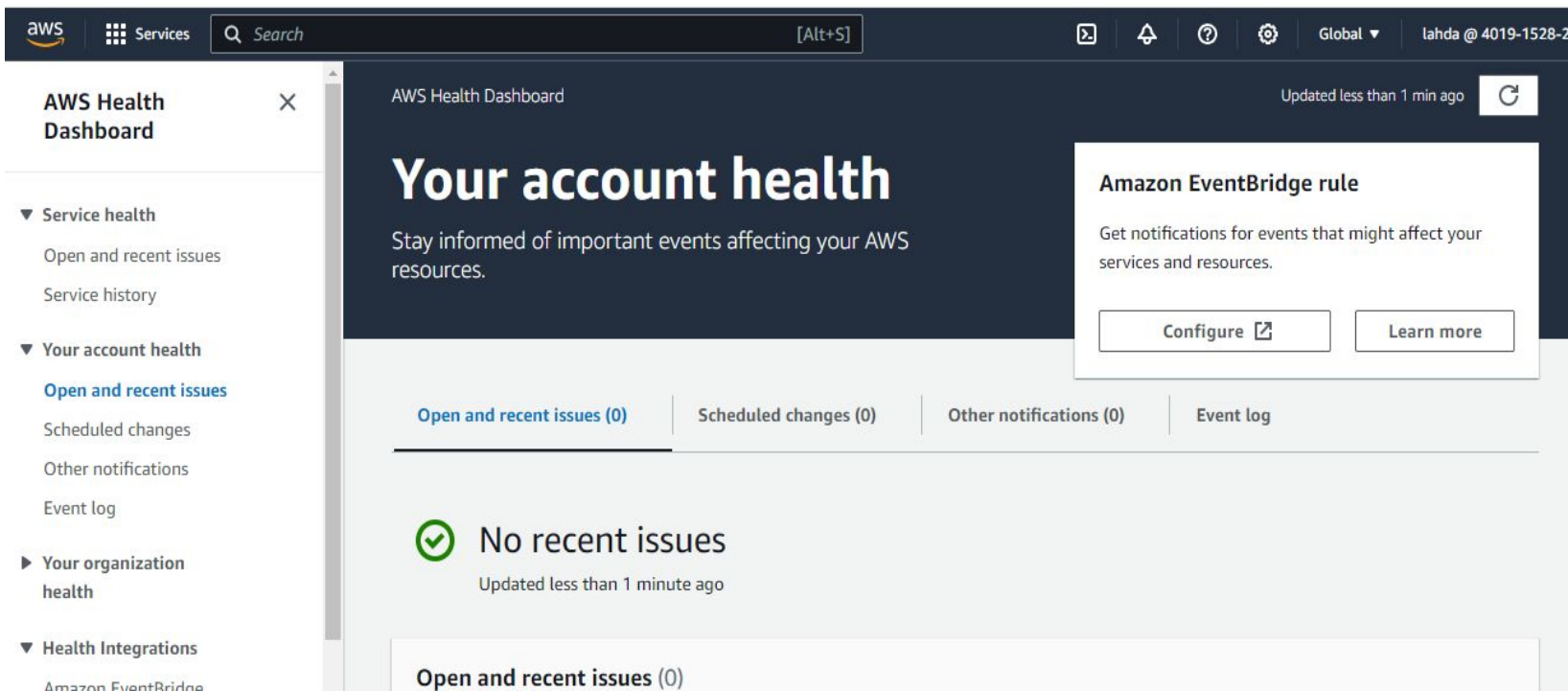
## Personal Health Dashboard

Le tableau de bord de la santé personnelle permet d'être informé de toute interruptions de service susceptibles d'affecter les ressources du compte AWS.



# AWS Personal Health Dashboard

AWS Personal Health Dashboard s'intègre aux événements Amazon CloudWatch Events pour créer des règles personnalisées et spécifier des cibles telles que les fonctions AWS Lambda pour activer les actions de remédiation.



Dans le tableau de bord de la santé personnelle, il y a trois catégories :

- **Problèmes en cours** - affiche les problèmes des sept derniers jours.
- **Changements programmés** - affiche les éléments de tout changement à venir.
- **Autres notifications.**





# Plan

- AWS Organization
- AWS Control Tower
- AWS Personal Health Dashboard
- **AWS Config**
- Amazon GuardDuty
- AWS Service Catalog
- AWS License Manager
- AWS Budget
- AWS Cost Explorer
- AWS Cost & usage Report
- AWS Pricing Calculator







# AWS Config

- Visualiser la conformité d'une ressource dans le temps



- Visualiser la configuration d'une ressource dans le temps



- Afficher les appels à l'API CloudTrail s'ils sont activés



# AWS Config Rules

- Peut utiliser les règles de configuration gérées par AWS (plus de 75)
- Peut créer des règles de configuration personnalisées (doivent être définies dans AWS Lambda)
  - Évaluer si chaque disque EBS est de type gp2
  - Évaluer si chaque instance EC2 est de type t2.micro
- Les règles peuvent être évaluées / déclenchées :
  - Pour chaque changement de configuration
  - Et / ou : à intervalles de temps réguliers
- Déclencher Amazon EventBridge si la règle n'est pas conforme (chaîne avec Lambda)
- Les règles peuvent avoir des remédiations automatiques via SSM Automations
  - Si une ressource n'est pas conforme, vous pouvez déclencher une remédiation automatique
  - Ex : remédier aux règles du groupe de sécurité, arrêter les instances avec des étiquettes non approuvées.



# Plan

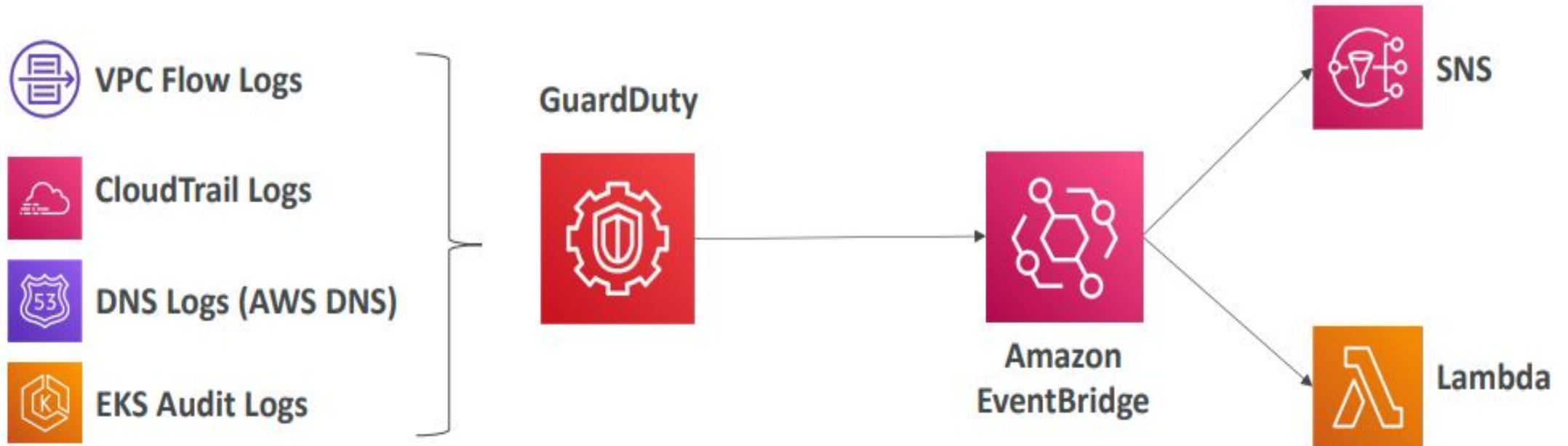
- AWS Organization
- AWS Control Tower
- AWS Personal Health Dashboard
- AWS Config
- **Amazon GuardDuty**
- AWS Service Catalog
- AWS License Manager
- AWS Budget
- AWS Cost Explorer
- AWS Cost & usage Report
- AWS Pricing Calculator





# Amazon GuardDuty

- Découverte intelligente des menaces pour protéger les comptes AWS
- Utilise des algorithmes d'apprentissage automatique, la détection d'anomalies et des données tierces.
- Activation en un clic (30 jours d'essai), pas besoin d'installer de logiciel
- Les données d'entrée comprennent :
  - Journaux d'événements CloudTrail
  - appels API inhabituels, déploiements non autorisés
- Événements de gestion CloudTrail
  - création d'un sous-réseau VPC, création d'une piste, ...
  - Événements de données S3 de CloudTrail - obtenir un objet, lister les objets, supprimer un objet, ...
- VPC Flow Logs - trafic interne inhabituel, adresse IP inhabituelle
- DNS Logs - instances EC2 compromises envoyant des données encodées dans des requêtes DNS
- Journaux d'audit Kubernetes - activités suspectes et compromissions potentielles du cluster EKS
- Possibilité de configurer des règles Amazon EventBridge pour être notifié en cas de découverte.
- Les règles Amazon EventBridge peuvent cibler AWS Lambda ou SNS
- Peut protéger contre les attaques de crypto-monnaies (a une "découverte" dédiée pour cela)





# AWS Service Catalog

- Les utilisateurs qui sont nouveaux dans AWS ont tellement d'options, et peuvent créer un stack ou piles non conformes au reste de l'organisation. Créer des piles qui ne sont pas conformes/en ligne avec le reste de l'organisation.
- Certains utilisateurs veulent simplement un **portail libre-service** rapide pour lancer un ensemble de **produits autorisés prédéfinis par les administrateurs**
- Comprend : machines virtuelles, bases de données, options de stockage, etc...
- Entrez dans le catalogue de services AWS



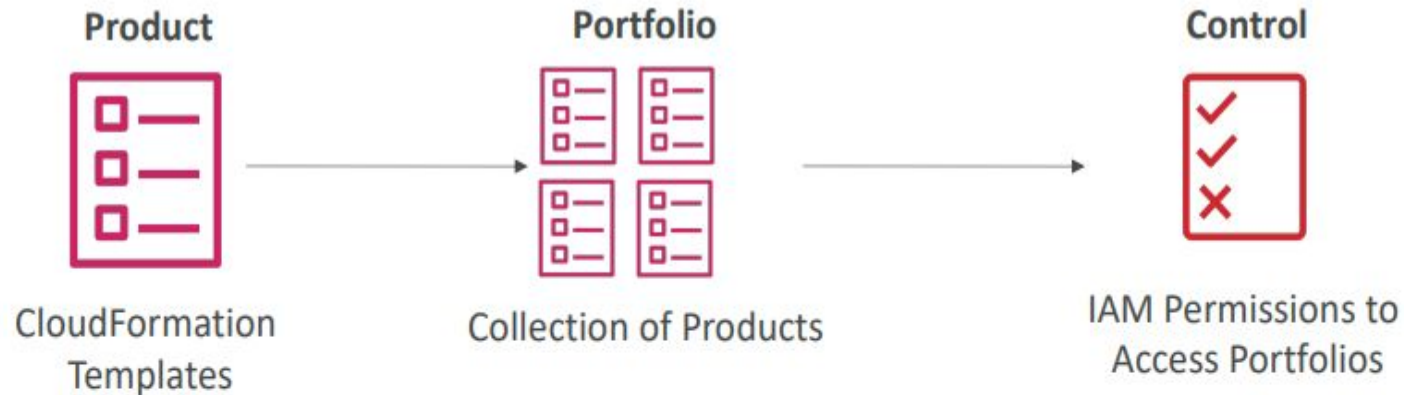
# AWS Service Catalog

- Créer et gérer des catalogues de services informatiques approuvés sur AWS.
- Les " produits " sont des templates CloudFormation
- Ex : images de machines virtuelles, serveurs, logiciels, bases de données, régions, plages d'adresses IP.
- **CloudFormation aide à assurer la cohérence et la normalisation par les administrateurs.**
- Ils sont affectés à des portefeuilles (équipes).
- Les équipes disposent d'un portail en libre-service où elles peuvent lancer les produits.
- Tous les produits déployés sont des services déployés gérés de manière centralisée.
- **Aide à la gouvernance, à la conformité et à la cohérence**
- Peut donner à l'utilisateur l'accès au lancement de produits sans exiger une connaissance approfondie d'AWS.
- Intégrations avec des "portails en libre-service" tels que ServiceNow

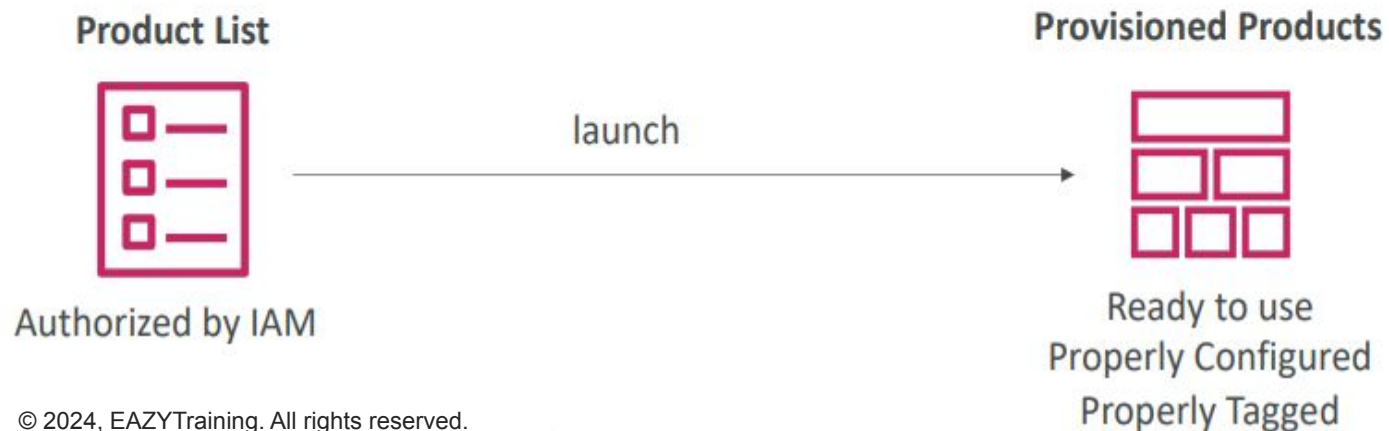


# AWS Service Catalog -diagramme

## ADMIN TASKS



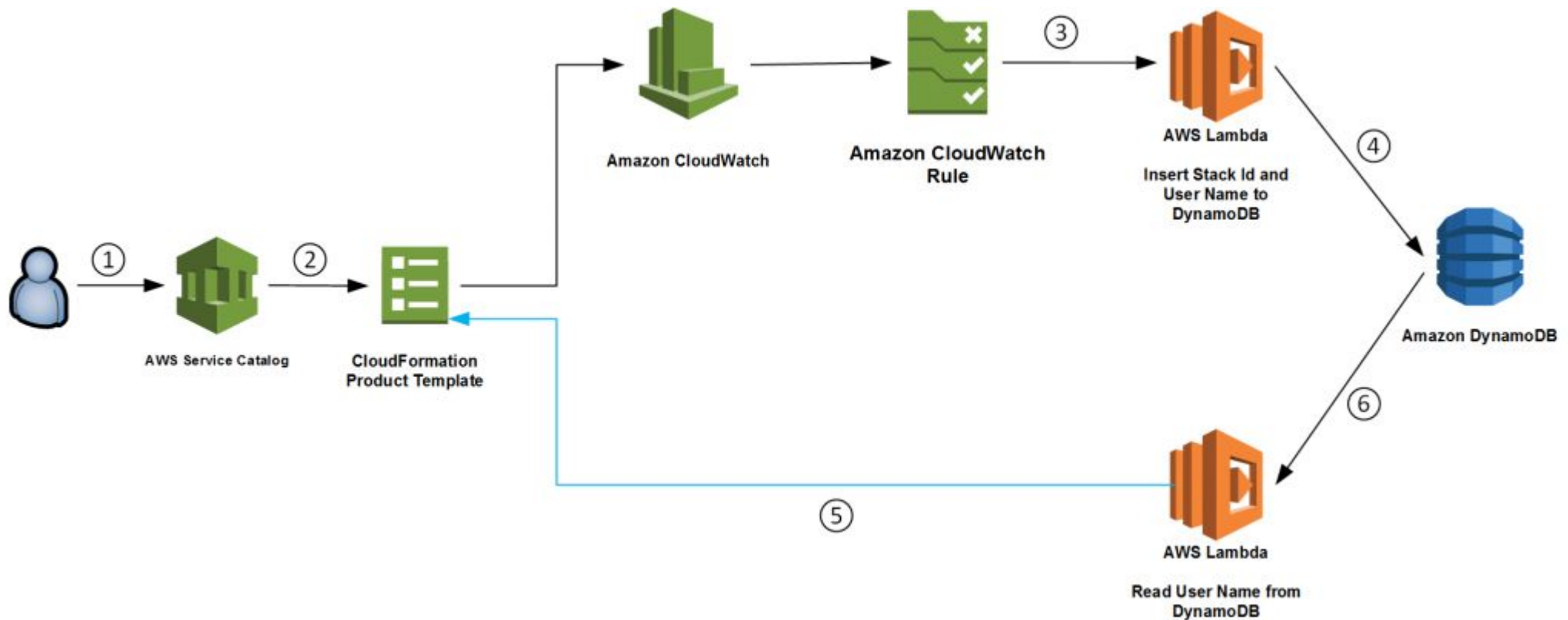
## USER TASKS







# AWS Service Catalog -diagramme





# Plan

- AWS Organization
- AWS Control Tower
- AWS Personal Health Dashboard
- AWS Config
- Amazon GuardDuty
- AWS Service Catalog
- **AWS License Manager**
- AWS Budget
- AWS Cost Explorer
- AWS Cost & usage Report
- **AWS Pricing Calculator**





# AWS License Manager

## Définition

AWS License Manager est un service utilisé pour centraliser l'utilisation des licences logicielles dans l'environnement.

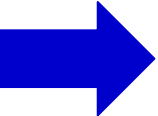


**AWS License Manager**

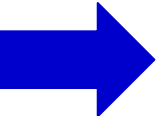
- ❖ Il prend en charge la fonction **Bring-Your-Own-License (BYOL)**, ce qui signifie que les utilisateurs peuvent gérer les licences existantes pour des charges de travail tierces (Microsoft Windows Server, SQL, etc.).
- ❖ Il permet aux administrateurs de créer des règles de licence personnalisées qui aident à prévenir les violations de licence (utilisation d'un nombre de licences par rapport à l'accord).
- ❖ Il fournit un tableau de bord permettant de contrôler la visibilité de toutes les licences aux administrateurs.



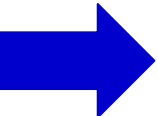
# AWS License Manager



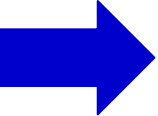
Il permet aux administrateurs de spécifier les préférences de gestion des hôtes dédiés pour l'allocation et l'utilisation de la capacité.



Les droits gérés par AWS License Manager fournissent des contrôles intégrés aux fournisseurs de logiciels (ISV) et aux administrateurs afin qu'ils puissent attribuer des licences aux utilisateurs et aux charges de travail approuvés.



AWS Systems Manager peut gérer les licences sur des serveurs physiques ou virtuels hébergés en dehors d'AWS à l'aide d'AWS License Manager.



Les organisations AWS et le gestionnaire de licences AWS permettent de divulguer les ressources informatiques de l'organisation d'un compte à l'autre.



# Plan

- AWS Organization
- AWS Control Tower
- AWS Personal Health Dashboard
- AWS Config
- Amazon GuardDuty
- AWS Service Catalog
- AWS License Manager
- **AWS Budget**
- AWS Cost Explorer
- AWS Cost & usage Report
- AWS Pricing Calculator





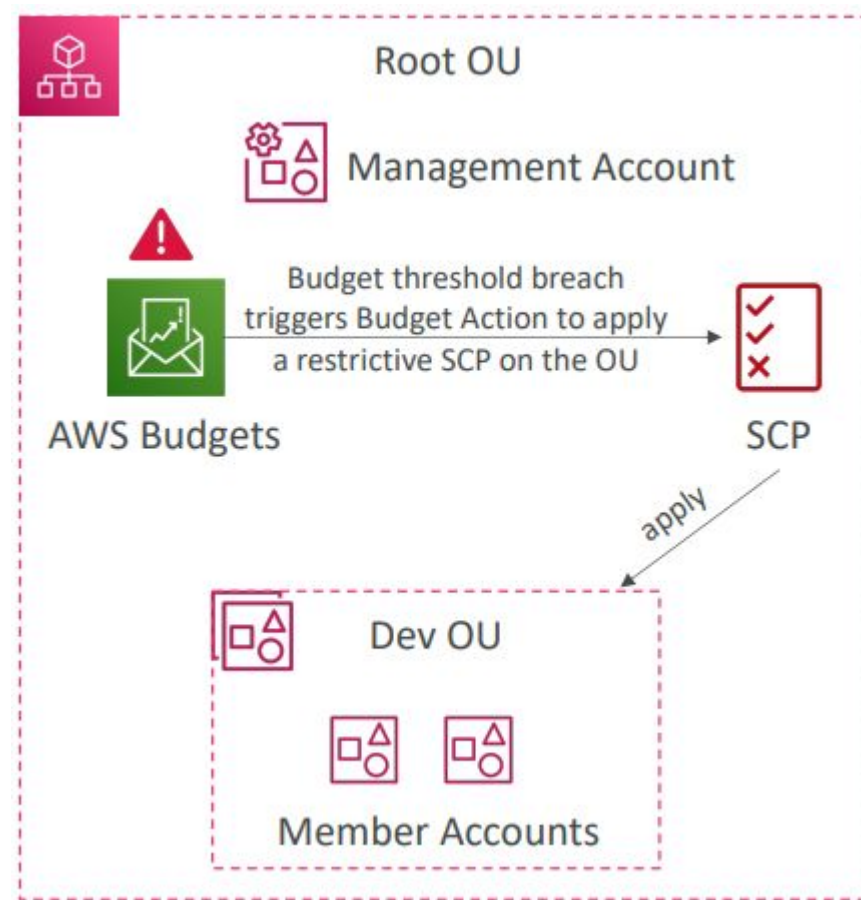
# AWS Budget

- 4 types de budgets : Utilisation, Coût, Réserveation, Plans d'épargne
- Pour les instances réservées (RI)
  - Suivi de l'utilisation
  - Supporte EC2, ElastiCache, RDS, Redshift
- Jusqu'à 5 notifications SNS par budget
  - Peut être filtré par : Service, compte lié, étiquette, option d'achat, type d'instance, région, zone de disponibilité, opération API, etc. Type d'instance, région, zone de disponibilité, opération API, etc...
- Mêmes options que AWS Cost Explorer !
- 2 budgets sont gratuits, puis 0.02\$/jour/budg



# AWS Budget -actions

- Exécuter des actions en votre nom lorsqu'un budget dépasse un certain seuil de coût ou d'utilisation
- Supporte 3 types d'actions :
  - Appliquer une politique IAM à un utilisateur, un groupe ou un rôle IAM
  - Appliquer une politique de contrôle des services (SCP) à une OU
  - Arrêter les instances EC2 ou RDS
- Les actions peuvent être exécutées automatiquement ou nécessiter un processus d'approbation du flux de travail
- Réduit les dépassements de budget involontaires dans votre compte





# Plan

- AWS Organization
- AWS Control Tower
- AWS Personal Health Dashboard
- AWS Config
- Amazon GuardDuty
- AWS Service Catalog
- AWS License Manager
- AWS Budget
- **AWS Cost Explorer**
- AWS Cost & usage Report
- AWS Pricing Calculator







# AWS Cost Explorer

## Définition

AWS Cost Explorer est un outil d'interface utilisateur qui permet aux utilisateurs d'analyser les coûts et l'utilisation à l'aide d'un graphique, des rapports de coûts et d'utilisation de Cost Explorer et le rapport Cost Explorer RI. Il est accessible à partir de la console Billing et de la console de gestion des coûts

La première fois que l'utilisateur s'inscrit à Cost Explorer, il est dirigé vers les principales parties de la console.

Il prépare les données relatives aux coûts et à l'utilisation et affiche jusqu'à 12 mois de données historiques (qui peuvent être moins si l'utilisation est moindre), les données du mois en cours, puis calcule les données prévisionnelles pour les 12 prochains mois.

Les rapports par défaut fournis par Cost Explorer sont les suivants: **Cost and Usage Report, Reserved Instance Report**



# Plan

- AWS Organization
- AWS Control Tower
- AWS Personal Health Dashboard
- AWS Config
- Amazon GuardDuty
- AWS Service Catalog
- AWS License Manager
- AWS Budget
- AWS Cost Explorer
- **AWS Cost & usage Report**
- **AWS Pricing Calculator**





# AWS Cost & Usage Report

## Définition

Le rapport sur les coûts et l'utilisation d'AWS est un service qui permet aux utilisateurs d'accéder à un ensemble détaillé de coûts et d'utilisation d'AWS, y compris les métadonnées sur les ressources AWS, la tarification, les instances réservées et les Plans d'économies.

Si le compte principal d'une organisation AWS souhaite bloquer l'accès aux comptes membres pour établir un rapport sur les coûts et l'utilisation, il est possible d'utiliser une politique de contrôle des services (SCP).

Pour la visualisation, les rapports peuvent être téléchargés à partir de la console Amazon S3 ; pour l'analyse du rapport, Amazon Athena peut être utilisé ou charger le rapport dans Amazon Redshift ou Amazon QuickSight.

Les utilisateurs disposant d'autorisations IAM ou de rôles IAM peuvent accéder aux rapports et les consulter.

si un compte membre d'une organisation possède ou crée un rapport de coûts et d'utilisation, il ne peut avoir accès qu'à la facturation, tant qu'il est membre de l'organisation.



# Plan

- AWS Organization
- AWS Control Tower
- AWS Personal Health Dashboard
- AWS Config
- Amazon GuardDuty
- AWS Service Catalog
- AWS License Manager
- AWS Budget
- AWS Cost Explorer
- AWS Cost & usage Report
- **AWS Pricing Calculator**





# AWS Pricing Calculator

## Définition

C' est un outil gratuit qui permet de créer des estimations de coûts pour l'utilisation des services AWS. Il est conçu pour aider les utilisateurs à modéliser leurs solutions avant de les construire, explorer les prix des services, et planifier leurs dépenses sur AWS

Accédez à AWS Pricing Calculator : Rendez-vous sur le site [AWS Pricing Calculator](https://calculator.aws/).

Estimation des coûts

Transparence des prix

Groupes d'estimations

Exportation



## AWS Pricing Calculator -dashboard

The screenshot shows the AWS Pricing Calculator dashboard. At the top, there's a navigation bar with the AWS logo and 'pricing calculator' text on the left, and links for 'Feedback', 'Language: English' (with a dropdown arrow), 'Contact Sales' (with an external link icon), and a 'Create an AWS Account' button on the right. The main content area has a dark blue background. It features the title 'AWS Pricing Calculator' in large white text, followed by the subtitle 'Estimate the cost for your architecture solution.' Below this, a paragraph states: 'Configure a cost estimate that fits your unique business or personal needs with AWS products and services.' To the right, a white box titled 'Create an estimate' contains the text: 'Start your estimate with no commitment, and explore AWS services and pricing for your architecture needs.' Below this text is an orange button labeled 'Create estimate'. At the bottom of the dashboard, there are two light gray buttons: 'How it works' on the left and 'More resources' (with an external link icon) on the right.

aws pricing calculator

Feedback Language: English ▼ Contact Sales ↗ Create an AWS Account

# AWS Pricing Calculator

Estimate the cost for your architecture solution.

Configure a cost estimate that fits your unique business or personal needs with AWS products and services.

**Create an estimate**

Start your estimate with no commitment, and explore AWS services and pricing for your architecture needs.

Create estimate

How it works More resources ↗

MERCI POUR VOTRE AIMABLE  
ATTENTION!



**Lahda Biassou Alphonsine**

Ingénieure cloud et Formatrice