
DEVOPS_UMANIS





Module 3:

Sécurité du cloud AWS



Contenu de ce Module

- Part 1: Modèle de responsabilité partagée AWS
- Part 2: Gestion des identités et des accès AWS (IAM)
- Part 3: AWS Trusted Advisor
- Part 4: AWS CloudTrail
- Part 5: AWS Config
- Part 6: AWS Day One Best Practice Review
- Part 7: AWS Security and Compliance Programs
- Part 8: AWS Security Resources
- Optional: AWS Day One Demonstration

Objectifs du module

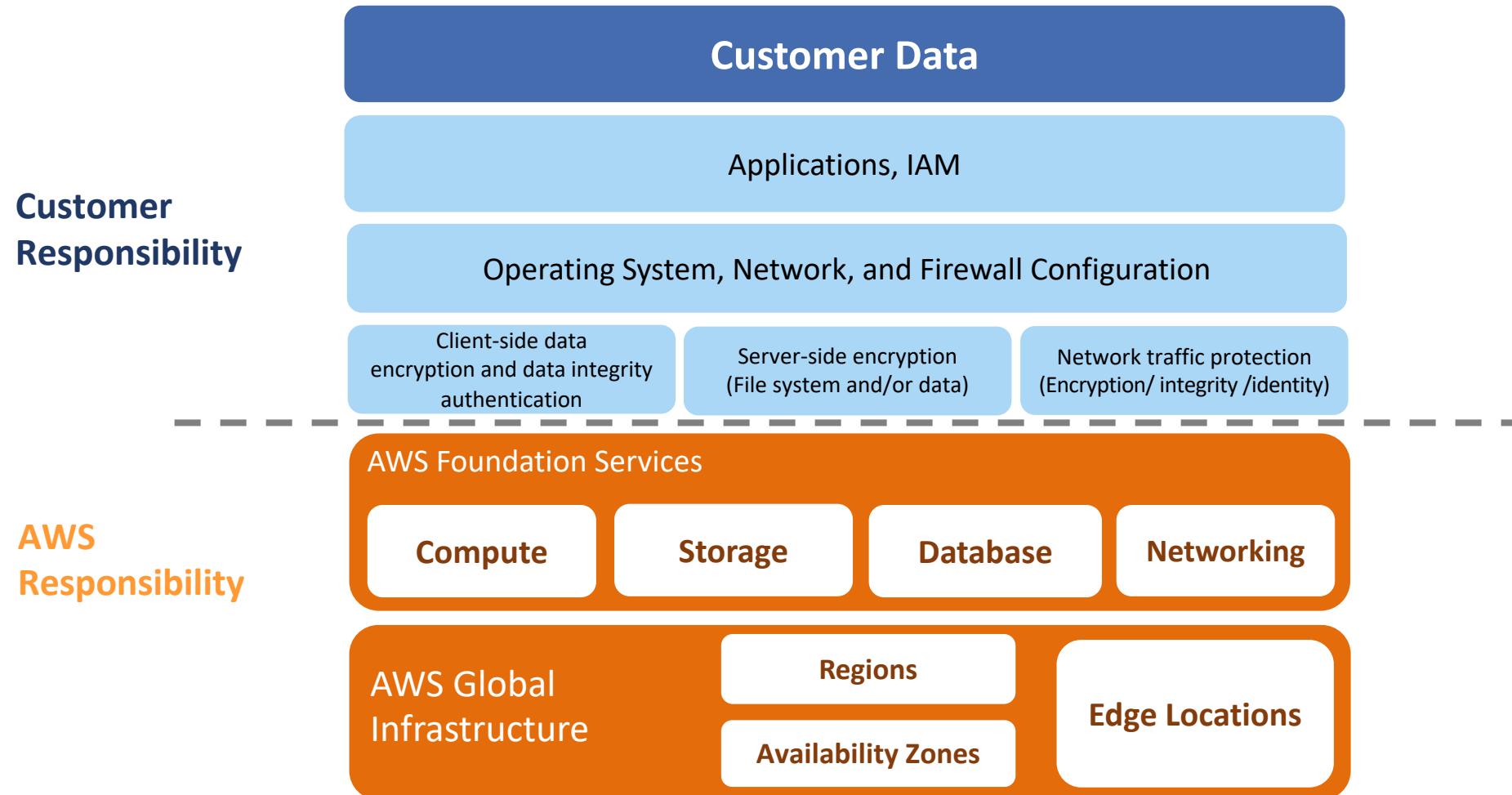
Examiner et comprendre les concepts de sécurité clés liés au partage Modèle de responsabilité et IAM :

- Décrire le modèle de responsabilité partagé AWS
- Examiner les utilisateurs, les groupes et les rôles IAM.



Part 1: Modèle de responsabilité partagée AWS

Modèle de responsabilité partagée



Responsabilités AWS en matière de sécurité : sécurité du cloud



Sécurité physique des centres de données:

- Accès contrôlé et basé sur les besoins

Infrastructure matérielle et logicielle:

- Gestion du matériel, journalisation des accès au système d'exploitation hôte et audit

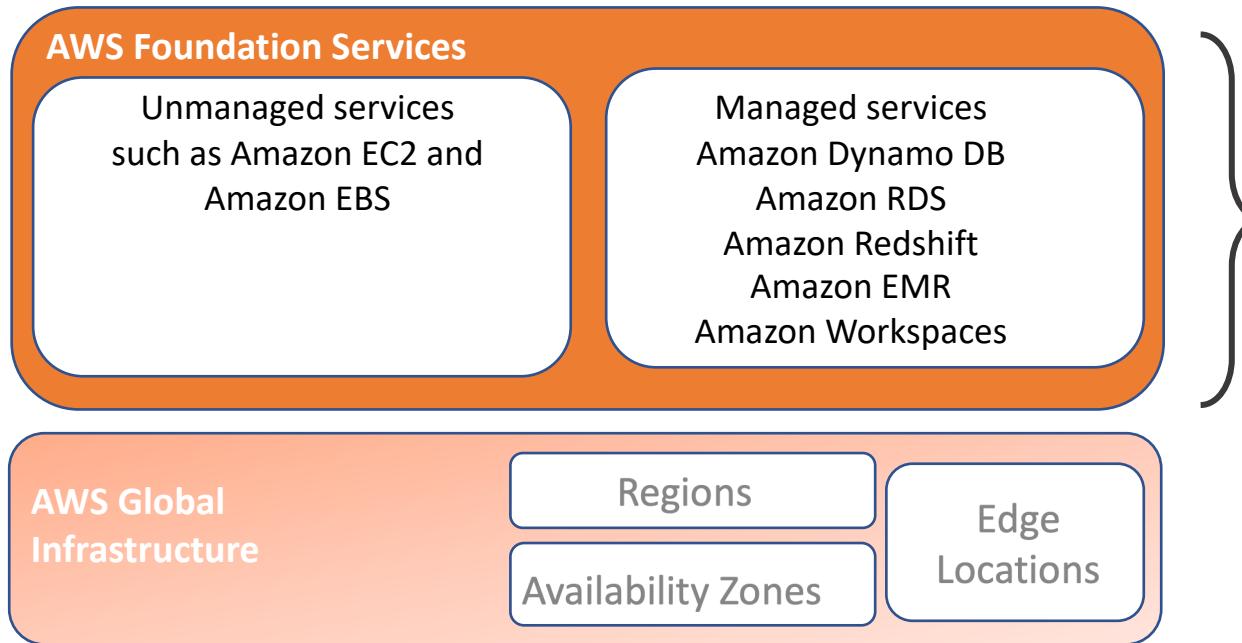
Infrastructure de réseau:

- Détection d'intrusion

Infrastructure de virtualisation:

- Isolement des instances

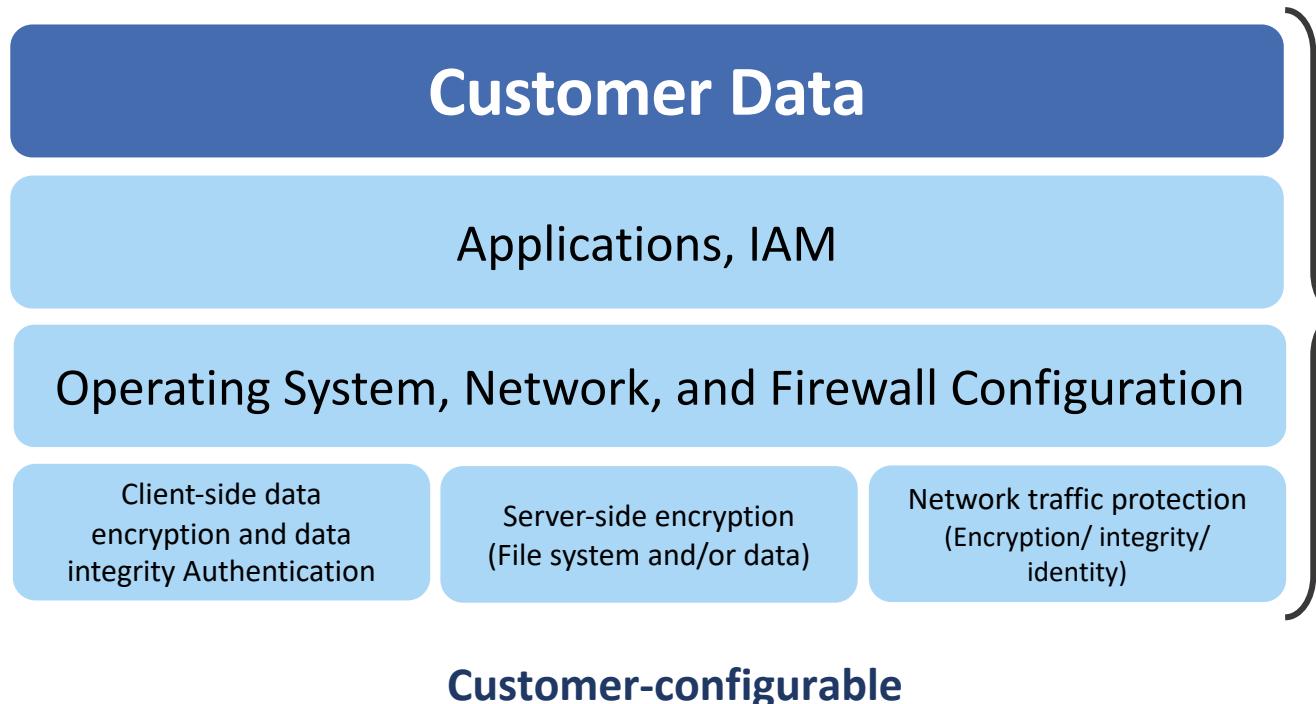
Responsabilités de Sécurité AWS: Sécurité du Cloud



Service gérés

- 📦 **AWS:**
 - Système d'exploitation (OS) et correctifs de base de données
 - Paramétrage du pare-feu
 - Reprise après sinistre
- 📦 **Client:**
 - Contrôles d'accès logiques
 - Protéger les informations d'identification du compte

Responsabilités du client en matière de sécurité: la sécurité dans le cloud



Système d'exploitation de l'instance:

- Y compris les correctifs, la maintenance

Application:

- Mots de passe, accès basé sur les rôles, etc.

Security Groups

Pare-feu basés sur le système d'exploitation/hôte :

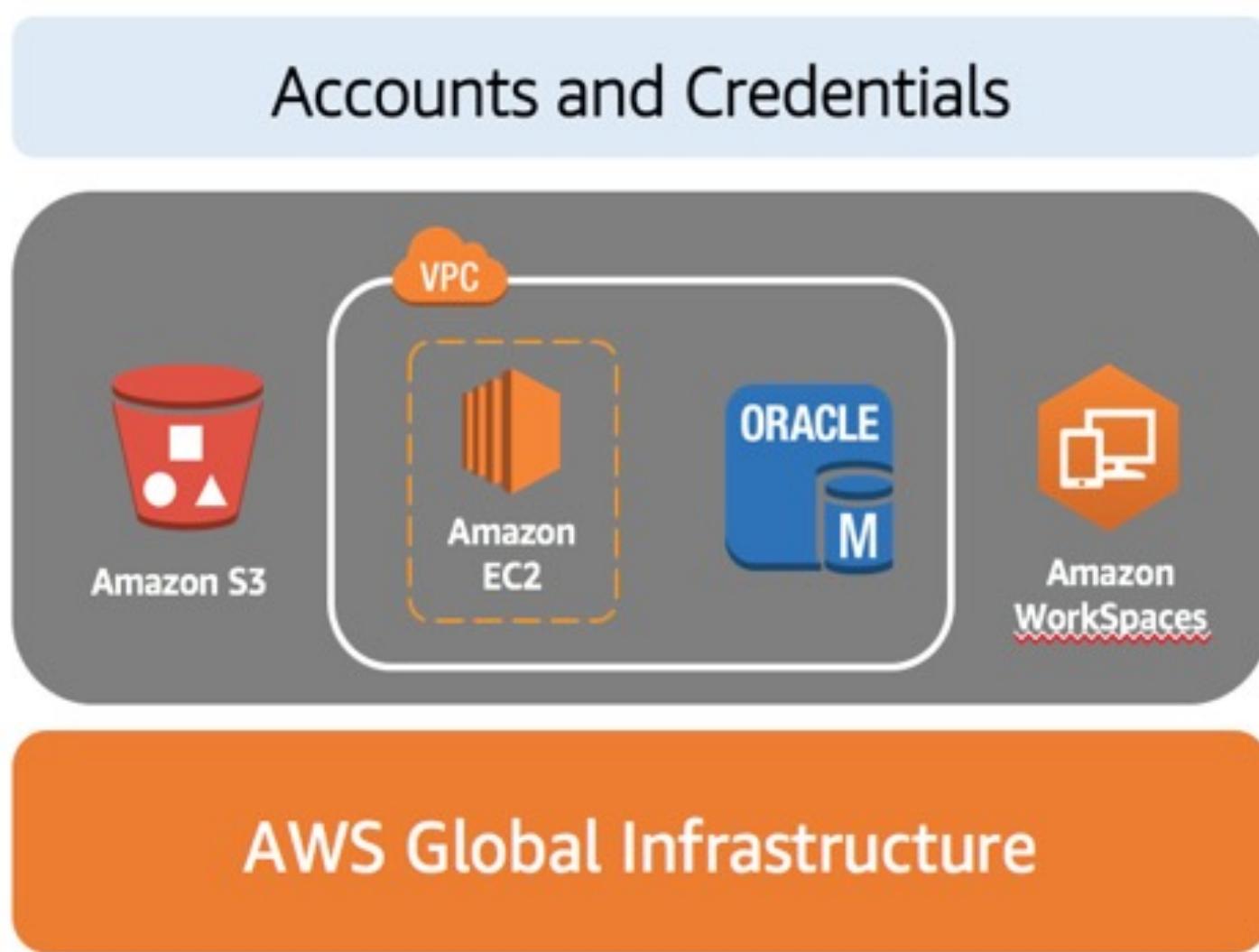
- Y compris intrusion
- systèmes de détection/prévention

Configuration du réseau

Account Management:

- Separation of access

Exemple de responsabilité partagée



Résumé des responsabilités partagées



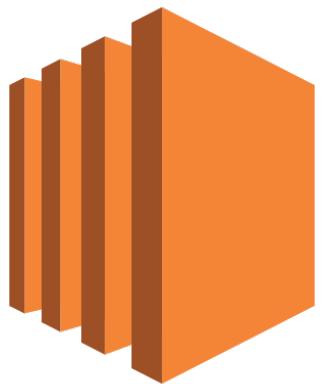
- AWS et le client partagent les responsabilités en matière de sécurité :
 - **AWS est responsable de la sécurité du cloud**
 - **Le client est responsable de la sécurité dans le cloud**
- Les clients ont un contrôle total sur les mesures de sécurité qu'ils choisissent de mettre en œuvre.
- Les clients peuvent utiliser AWS Service Catalog pour gérer des catalogues de services informatiques.
- Les configurations de sécurité des services d'infrastructure sont entièrement sous le contrôle du client.

Part 2: Identity and Access Management (IAM)

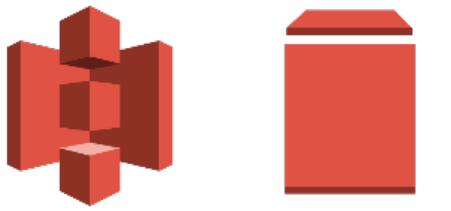
Core AWS Services: IAM



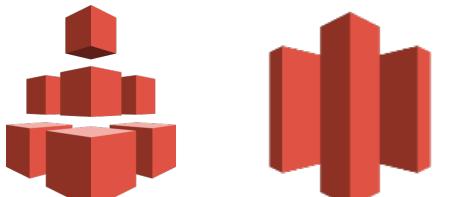
**Amazon
VPC**



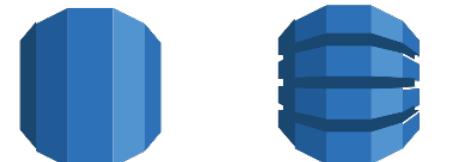
Amazon EC2



Amazon S3 Amazon EBS



Amazon
EFS Amazon
Glacier



Amazon
RDS Amazon
DynamoDB



Storage

Gérez de manière centralisée **l'accès et l'authentification** de vos utilisateurs à vos ressources AWS.

- Offert en tant que fonctionnalité de votre compte AWS sans frais.
- Créez des **utilisateurs**, des **groupes** et des **rôles**, et attachez-leur des **stratégies** pour contrôler leur accès aux ressources AWS.
- Gérez les ressources; accessibles par qui et comment elles sont accessibles.
- Définissez les informations d'identification requises en fonction du contexte (par exemple, qui accède à quel service et qu'essayent-ils de faire ?).



Types d'informations d'identification de sécurité



Email address and password

Associé à votre compte AWS (root).

IAM user name and password

Utilisé pour accéder à la AWS Management Console.

Access and Secret Access keys

Généralement utilisé avec l'interface de ligne de commande (CLI) et les requêtes programmatiques telles que les API et le kit de développement logiciel (SDK).

Multi-Factor Authentication

Couche de sécurité supplémentaire.

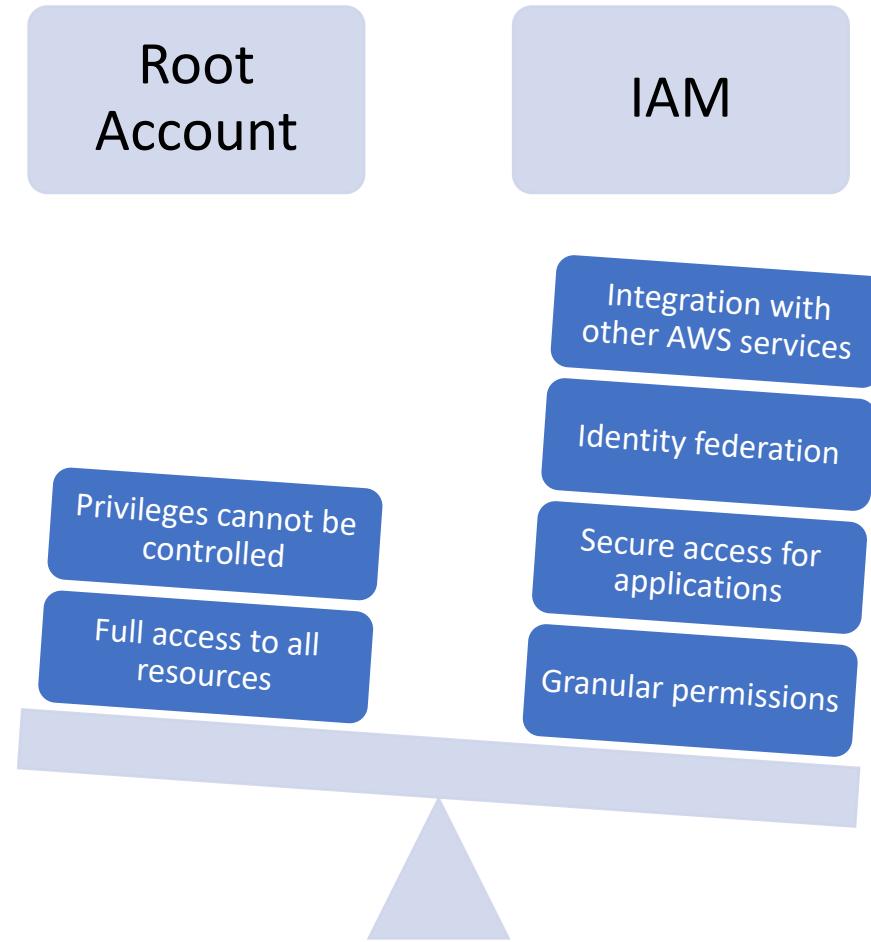
Peut être activé pour les utilisateurs du compte racine et de la gestion des identités et des accès (IAM).

Key pairs

Utilisé uniquement pour des services AWS spécifiques comme Amazon EC2.



Root Account Access vs. IAM Access

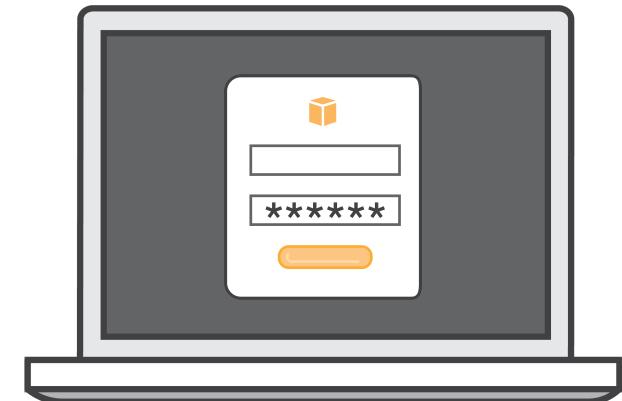


- IAM vous permet de suivre le principe du **moindre privilège**.
- **Best practices:**
 - Supprimer les clés d'accès de l'utilisateur root.
 - Créer un utilisateur IAM.
 - Accorder l'accès administrateur.
 - Activer l'authentification multifacteur (MFA).
 - Utiliser les informations d'identification IAM pour interagir avec AWS.



cube Accès programmatique:

- cube Authentifie l'ID de clé d'accès et la clé d'accès secrète.
- cube Fournit un accès à l'API, à l'interface de ligne de commande, au SDK et à d'autres outils de développement.



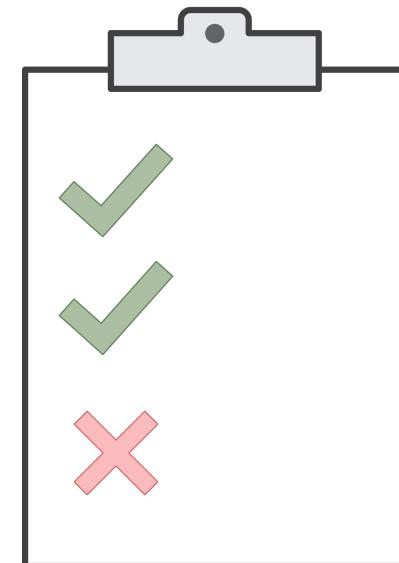
cube Accès aux consoles:

- cube Utilise l'identifiant ou l'alias du compte, le nom d'utilisateur et le mot de passe IAM.
- cube Si activé, MFA demande le code d'authentification.



IAM: Authorization

- Permet aux utilisateurs d'accéder aux services AWS en accordant une autorisation
- Attribuer des autorisations en créant une stratégie IAM.
- Les autorisations déterminent quelles ressources et opérations sont autorisées à être utilisées:
 - Toutes les autorisations sont implicitement refusées par défaut.
 - Si quelque chose est explicitement refusé, il ne peut jamais être autorisé.



Best practice: Suivre le principe du moindre privilège.

NOTE: IAM est **mondial**. Ce n'est pas par région. Il s'applique à toutes les régions.



IAM Multi-Factor Authentication (MFA)



- MFA offre une sécurité accrue.
 - En plus du nom d'utilisateur et du mot de passe, MFA requiert un code d'authentification unique pour accéder aux services AWS.

Account: [REDACTED]

User Name: [REDACTED]

Password: [REDACTED]

MFA users, enter your code on the next screen.



AWS Services Edit awsstudent@ Singapore Support

Amazon Web Services

Compute

 **EC2**
Virtual Machines in the Cloud

 **EC Container Service**
Run and Manage Docker Containers

 **Elastic Beanstalk**
Run and Manage Web Apps

 **Lambda**
Run Code in Response to Events

Storage & Content Delivery

 **S3**
Object Storage in the Cloud

 **CloudFront**
Global Content Delivery Network

 **Elastic File System**
Managed File System for EC2

 **Glacier**
Archive Storage in the Cloud

 **importExport**
Snowball and Terrestrial Transport

 **Storage Gateway**
Hybrid Storage Integration

Database

 **RDS**
Managed Relational Database Service

 **DynamoDB**
Reliable, Scalable, Database

 **ElastiCache**
In-Memory Cache

 **Redshift**
Fast, Cost-Effective Data Warehousing

 **DMS** 
Managed Database Migration Service

Networking

 **VPC**
Virtualized Cloud Resources

 **Direct Connect**
Seamless Dedicated Connection to AWS

 **Route 53**
Scalable DNS and Domain Name Registration

Developer Tools

 **CodeCommit**
Store Code in Private Git Repositories

 **CodeDeploy**
Automate Application Deployments

 **CodePipeline**
Release Software using Continuous Delivery

Management Tools

 **CloudWatch**
Monitor Resources and Applications

 **CloudFormation**
Create and Manage Resources with Templates

 **CloudTrail**
Trace User Activity and API Usage

 **Config**
Compliance Inventory and Changes

 **OpsWorks**
Automate Operations with Chef

 **Service Catalog**
Discover and Utilize Products

 **Trusted Advisor**
Optimize Performance and Security

Security & Identity

 **Identity & Access Management**
Manage User Access and Encryption Keys

 **Directory Service**
AWS-managed Active Directory

 **Inspector** 
Analyze Application Security

 **WAF**
Mitigate Malicious Web Traffic

 **Certificate Manager**
Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

 **EMR**
Managed Hadoop Framework

 **Data Pipeline**
Build Data Pipelines for Data-Driven Workflows

 **Elasticsearch Service**
Run and Scale Elasticsearch Clusters

 **Kinesis**
Stream and Process Real-Time Streaming Data

 **Machine Learning**
Build Smart Applications Quickly and Easily

Internet of Things

 **AWS IoT**
Connect Devices to the Cloud

Mobile Services

 **Mobile Hub** 
Build, Test, and Monitor Mobile Apps

 **Cognito**
User Pools and App Sync

 **Device Farm**
Test Android, iOS, and WebGL Apps on Real Devices in the Cloud

 **Mobile Analytics**
Collect, View and Export App Analytics

 **SNS**
Push Notification Service

Application Services

 **API Gateway**
Build, Deploy and Manage APIs

 **AppStream**
Live Stream Application Streaming

 **CloudSearch**
Managed Search Service

 **Elastic Transcoder**
Encode and Resize Media on the Fly

 **SES**
Email Sending and Receiving Service

 **SQS**
Message Queue Service

 **SWF**
Workflow Service for Coordinating Application Components

Enterprise Applications

 **WorkSpaces**
Desktops in the Cloud

 **WordDocs**
Edit Microsoft Word Documents in the Cloud

 **WorkMail**
Secure Email and Calendering Service

Resource Groups

[Learn more](#)

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

[Create a Group](#)

[Tag Editor](#)

Additional Resources

[Getting Started](#) 

Read our documentation or view our training to learn more about AWS.

[AWS Console Mobile App](#) 

View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

[AWS Marketplace](#) 

Find and buy software, launch with 1-Click and pay by the hour.

[AWS In-Flight Announcements](#) 

Explore the next generation of AWS cloud capabilities. See what's new.

Service Health

 All services operating normally.

Updated: Jan 29 2016 14:59 (2 QMT+0600)

[Service Health Dashboard](#)

 [Feedback](#)

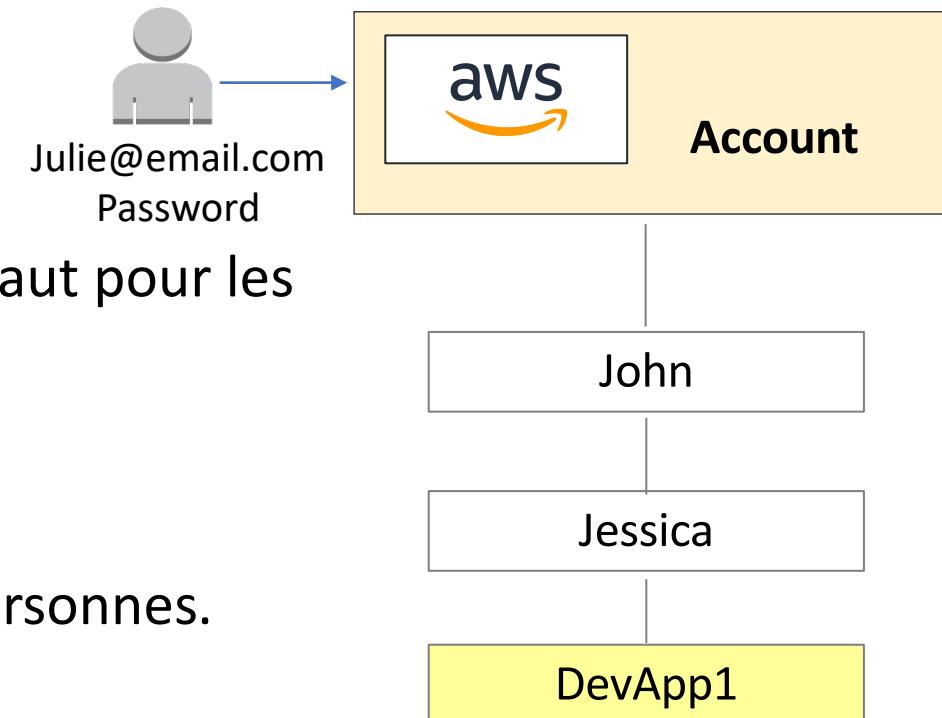
 [English](#)

© 2016 - 2017 Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)



IAM Users

- Une entité que vous créez dans AWS.
- Fournit un moyen d'interagir avec AWS.
- Aucune information d'identification de sécurité par défaut pour les utilisateurs IAM:
 - Vous devez les affecter spécifiquement.
- Les utilisateurs IAM ne sont pas nécessairement des personnes.

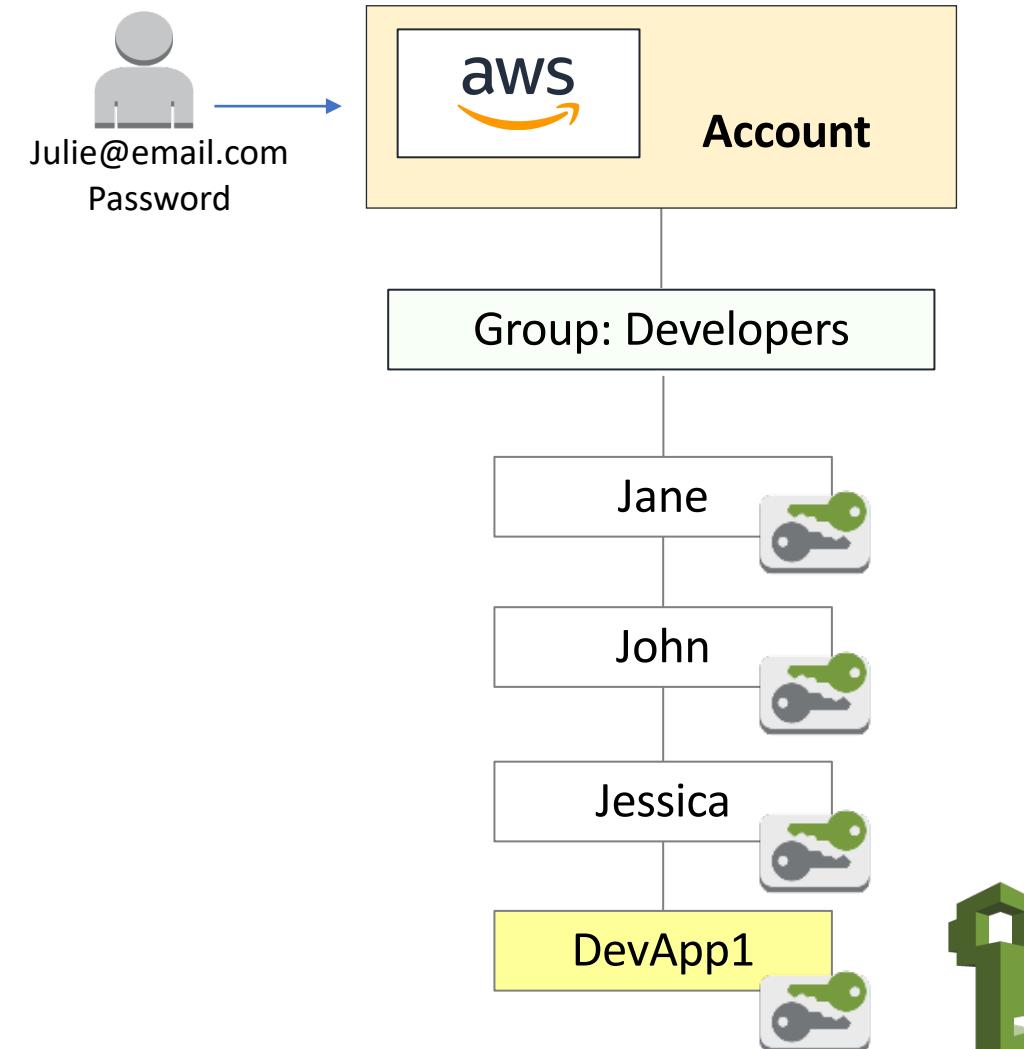


Best practice: Créez un compte d'utilisateur IAM distinct avec des priviléges administratifs au lieu d'utiliser l'utilisateur du compte racine.



IAM Groups

- Collection ou groupe d'utilisateurs IAM.
- Spécifier les autorisations pour l'ensemble du groupe.
- Aucun groupe par défaut.
- Les groupes ne peuvent pas être imbriqués.
- Un utilisateur peut appartenir à plusieurs groupes.
- Les autorisations sont définies à l'aide de stratégies IAM.

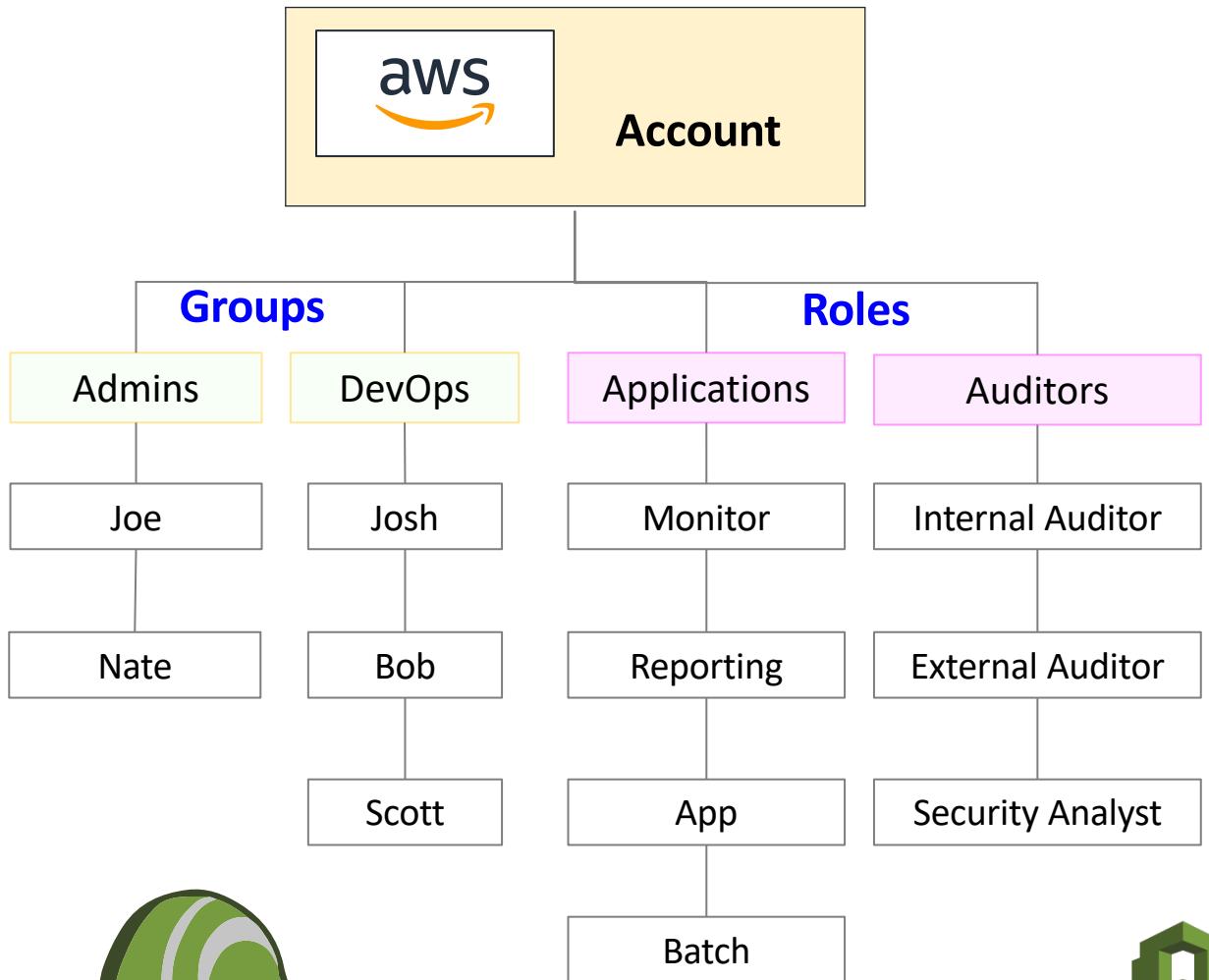


- Utilisé pour déléguer l'accès aux ressources AWS:

- Fournit un accès temporaire.
- Élimine le besoin d'informations d'identification AWS statiques.

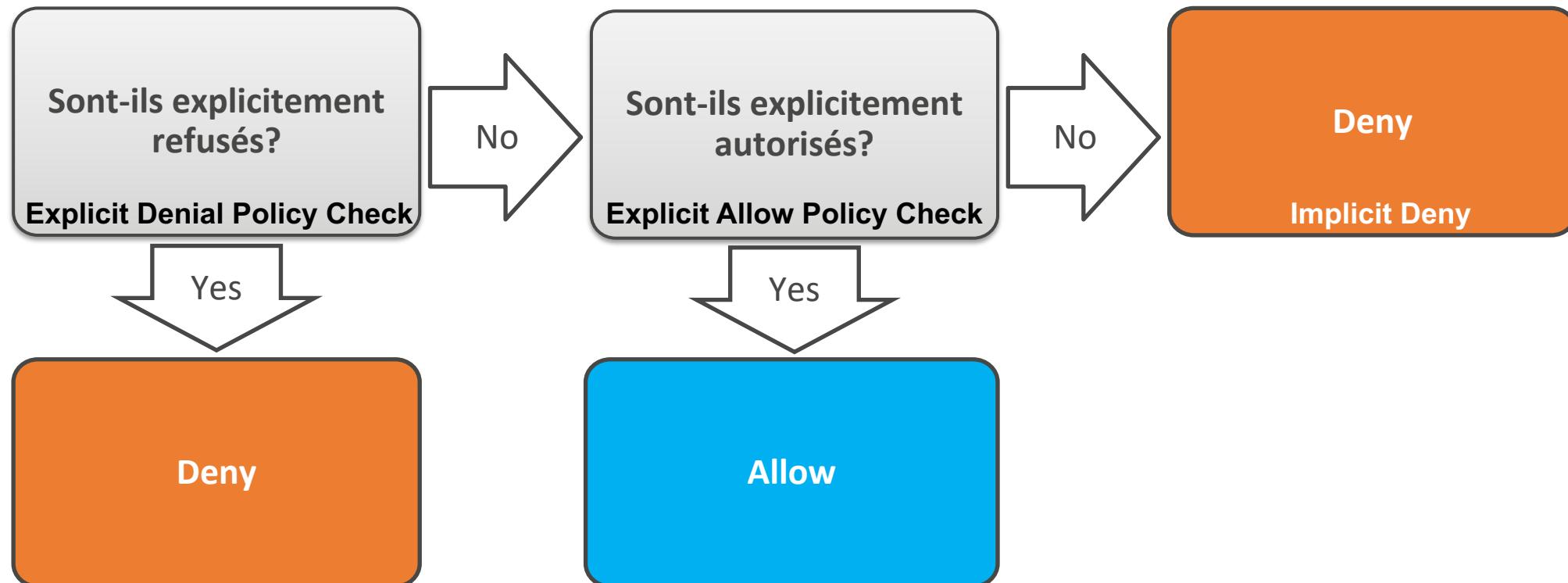
- Les autorisations sont:

- Défini à l'aide de stratégies IAM.
- Attaché au rôle, pas à un utilisateur ou à un groupe IAM.



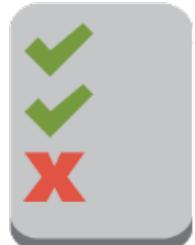
IAM Permissions

Comment IAM détermine les autorisations:



Une stratégie (Policies) IAM est une déclaration formelle d'une ou plusieurs autorisations:

- Vous attachez une stratégie à n'importe quelle entité IAM, telle qu'un utilisateur, un groupe ou un rôle.
- Les policies autorisent les actions qui peuvent ou non être effectuées par l'entité qui permet un contrôle d'accès précis.
- Une même policy peut être attachée à plusieurs entités.
- Une même entité peut être associée à plusieurs stratégies.



Best practice: Lorsque vous attachez la même stratégie à plusieurs utilisateurs IAM, placez les utilisateurs dans un groupe et attachez la stratégie au groupe à la place.



IAM Policy Example

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": ["DynamoDB:*", "s3:*"],  
      "Resource": ["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",  
                   "arn:aws:s3:::bucket-name",  
                   "arn:aws:s3:::bucket-name/*"]  
    },  
    {  
      "Effect": "Deny",  
      "Action": ["dynamodb:*", "s3:*"],  
      "NotResource": ["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",  
                     "arn:aws:s3:::bucket-name",  
                     "arn:aws:s3:::bucket-name/*"]  
    }  
  ]  
}
```

Explicit allow gives users access to a specific DynamoDB table and...

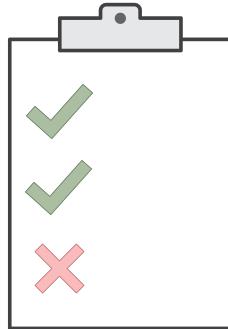
...Amazon S3 buckets.

Explicit deny ensures that the users cannot use any other AWS actions or resources other than that table and those buckets.

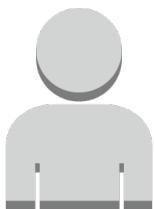
An explicit deny statement **takes precedence** over an allow statement.



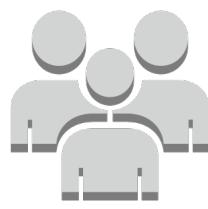
IAM: Policy Assignment



IAM Policy



IAM User



IAM Group



IAM Roles

Part 3: AWS Trusted Advisor

Introduction to Trusted Advisor



AWS Trusted Advisor provides best practices, or checks, in five categories:

Cost Optimization



0 ✓ 9 ▲ 0 !

\$7,516.85

Potential monthly savings

Performance



3 ✓ 7 ▲ 0 !

Security



2 ✓ 4 ▲ 11 !

Fault Tolerance



0 ✓ 15 ▲ 5 !

Service Limits



37 ✓ 0 ▲ 1 !



Green: No problem detected. Yellow: Investigation recommended. Red: Action recommended.

Using AWS Trusted Advisor



💡 Six bonnes pratiques valables pour tous les clients AWS:

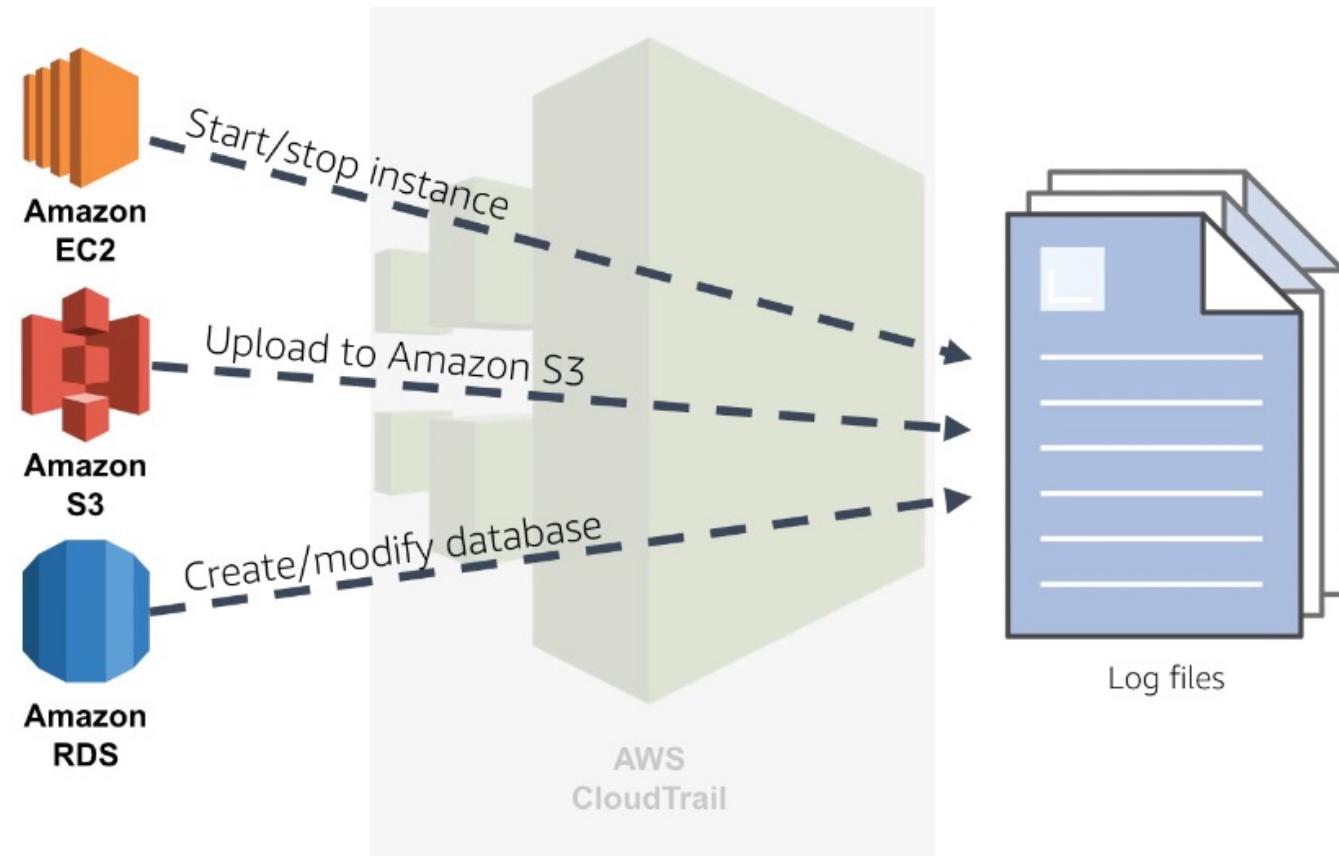
1. Service Limits
2. Security Groups – Specific Ports Unrestricted
3. IAM Use
4. Multi-Factor Authentication (MFA) on Root Account
5. Elastic Block Store (EBS) Public Snapshots
6. Relational Database Service (RDS) Public Snapshots

- Le conseiller de confiance est un expert du cloud personnalisé:
 - Vous aide à suivre les meilleures pratiques
 - Inspecte votre environnement AWS
 - Aide à combler les failles de sécurité
- Trouve les opportunités et les meilleures pratiques dans:
 - Optimisation des coûts
 - Performance
- Security:
 - Tolérance aux pannes
 - Service limits

Part 4: AWS CloudTrail

Introduction to CloudTrail

CloudTrail est un service Web qui enregistre les appels d'API pour votre compte et vous fournit des fichiers journaux.



AWS CloudTrail Benefits



User and Resource
Activity



Simplified
Compliance



Always
On

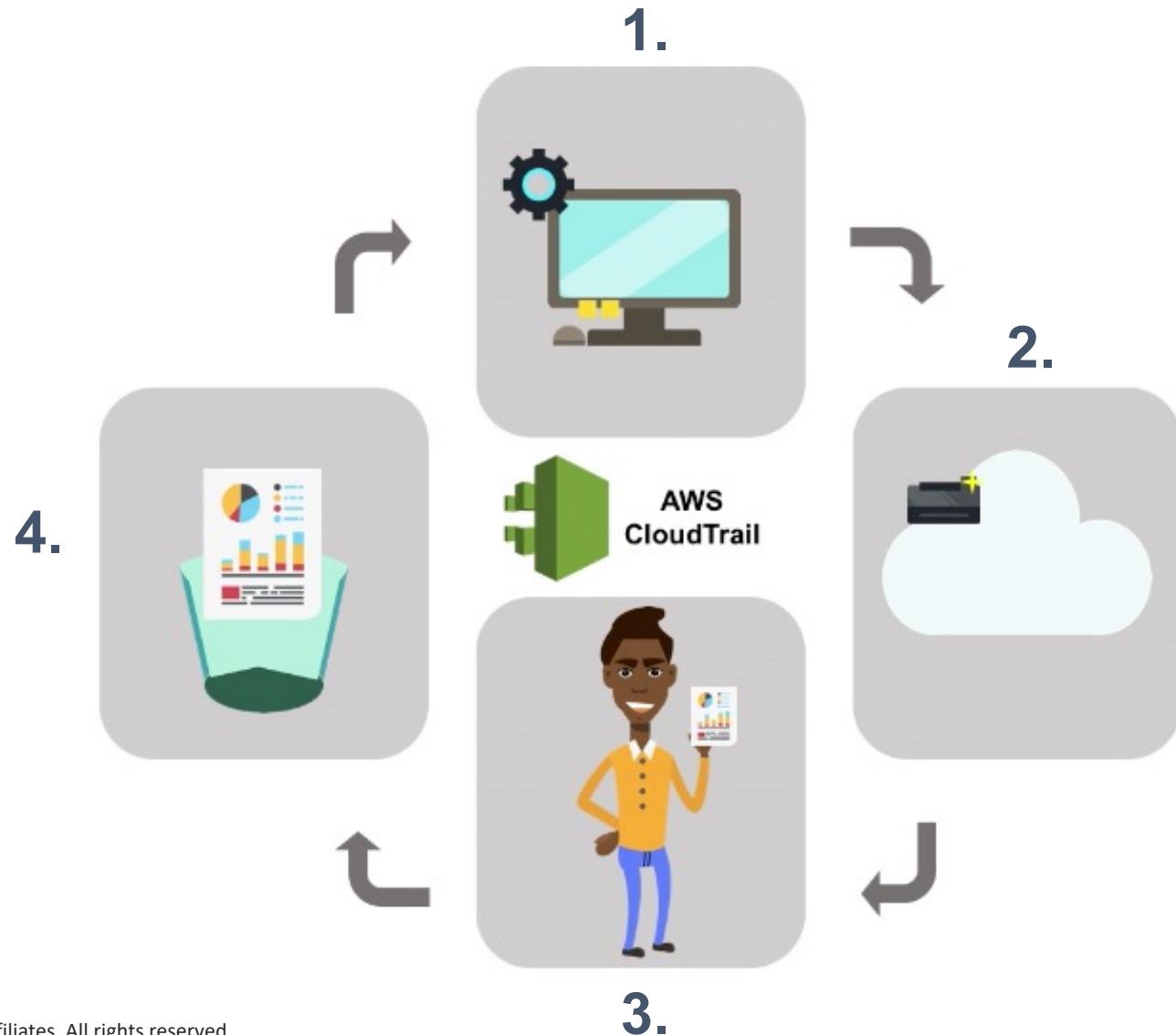


Security
Automation



Analysis and
Troubleshooting

Présentation d'AWS CloudTrail



Utiliser les meilleures pratiques CloudTrail



- 💡 Activer la validation du fichier journal CloudTrail.
- 💡 Agréger les fichiers journaux dans un seul compartiment Amazon S3.
- 💡 Assurez-vous qu'il est activé sur AWS dans le monde.
- 💡 Restreindre l'accès aux compartiments CloudTrail Amazon S3.
- 💡 Intégration avec Amazon CloudWatch.

Part 5: AWS Config

Introduction to AWS Config



AWS Config est un service entièrement géré qui vous permet d'auditer et d'évaluer la configuration de vos ressources AWS.



- Monitoring en continu
- Évaluation continue
- La gestion du changement
- Aide au troubleshooting

Suivre les modifications apportées aux ressources avec AWS Config



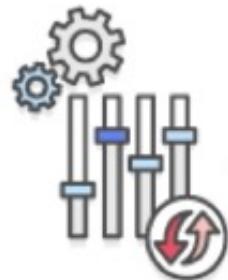
- Fournit l'inventaire des ressources AWS, l'historique de configuration et les notifications de changement de configuration.
- Fournit des détails continus sur toutes les modifications de configuration associées aux ressources AWS.
- Se combine avec CloudTrail pour une visibilité complète sur ce qui a contribué à un changement.
- Permet l'audit de conformité, l'analyse de la sécurité, le suivi des modifications des ressources et le dépannage.



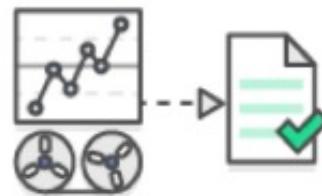
AWS Config Overview



How It Works



Configuration change occurs in your AWS resources



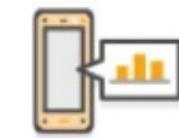
Config records and normalizes the changes into a consistent format



Normalized changes are delivered to your S3 bucket, accessed through Config APIs, and optionally sent via SNS.



Config automatically evaluates the recorded configurations against your desired configurations



Evaluations are displayed on a dashboard, accessed through Config APIs, and optionally sent via SNS

AWS Config Summary



Simple setup



Customize rules



Continuous compliance

Part 6: Jour 1 avec un nouveau compte AWS



1

Arrêtez d'utiliser le compte root le plus tôt possible.

Le compte root a un accès totalement illimité à vos ressources.

Pour arrêter d'utiliser le compte root, procédez comme suit:

- 1) Avec le compte root, créez vous-même un utilisateur IAM.
- 2) Créez un groupe IAM, accordez-lui des autorisations d'administrateur complètes et ajoutez l'utilisateur IAM au groupe.
- 3) Connectez-vous avec vos informations d'identification d'utilisateur IAM.
- 4) Stockez les informations d'identification de votre compte racine dans un endroit très sécurisé. Désactivez et supprimez les clés d'accès de votre compte racine, si vous en avez.



2

Exiger **Multi-Factor Authentication (MFA)**.

- a. Exiger l'authentification MFA pour votre compte racine et tous les utilisateurs IAM.
- b. Vous pouvez également utiliser MFA pour contrôler l'accès aux API de service AWS.

Software MFA options: AWS Virtual MFA, Google Authenticator, Authy Authenticator (application pour téléphone Windows) ou notification par SMS.

Hardware MFA options: Porte-clés ou carte présentoir offert par Gemalto:
<https://safenet.gemalto.com/multi-factor-authentication/>



3

Activer **CloudTrail**.

CloudTrail enregistre toutes les demandes d'API vers les ressources de votre compte:

- 1) Via la console CloudTrail : créez un suivi, donnez-lui un nom, appliquez-le à toutes les régions et saisissez un nom pour le nouveau compartiment Amazon S3 dans lequel les journaux seront stockés.
- 2) Assurez-vous que le compartiment Amazon S3 que vous utilisez pour CloudTrail a son accès limité à ceux qui devraient y avoir accès, tels que les administrateurs.



4

Activer un **rapport de facturation (billing report)**, comme AWS Cost and Usage Report:

- a) Les rapports de facturation fournissent des informations sur votre utilisation des ressources AWS et les coûts estimés pour cette utilisation.
- b) AWS fournit les rapports à un compartiment Amazon S3 que vous spécifiez et met à jour les rapports au moins une fois par jour.
- c) Le rapport sur les coûts et l'utilisation d'AWS suit votre utilisation d'AWS et fournit une estimation des frais associés à votre compte AWS, à l'heure ou à la journée..

IAM Best Practices Summary



- **Supprimer** Clés d'accès au compte AWS (racine).
- Creer un utilisateur IAM **individuel** .
- **Utiliser les groupes** pour assigner les autorisations au utilisateurs IAM.
- Accorder le **moindre privilege**.
- Utiliser une **stratégie de mot de passe forte**.
- Activer **MFA** pour les utilisateurs importants.
- Utiliser les **roles pour les applications** qui tournent sur une instance Amazon EC2 .
- Déleguer en utilisant les **roles** au lieu de partager les informations d'identification.
- **Modifier les identifiants** regulièrement
- **Supprimer** les utilisateurs et identifiants plus nécessaires.
- **Monitored l'activité** dans votre compte AWS.



- AWS can be accessed in three ways:
 - Via the AWS Management Console
 - Programmatically (using the CLI)
 - Using the SDK
- Root account is the email address used to set up the AWS account and *always* has full administrator access.
 - These credentials should never be given to anyone.
 - The AWS Account Root User access keys should be deleted after login.
 - A user should be created for each individual within the organization.
 - The root account should always be secured with MFA.



- 💡 Un utilisateur IAM est une entité que vous créez dans AWS pour représenter la personne ou le service qui interagit avec AWS.
- 💡 Un rôle IAM est similaire à un utilisateur en ce sens qu'il s'agit d'une identité AWS avec des stratégies d'autorisation qui déterminent les actions que le rôle peut effectuer et utilisées pour déléguer l'accès aux utilisateurs.
- 💡 Un groupe IAM est un endroit pour stocker vos utilisateurs:
 - 💡 Identités qui représentent l'utilisateur.
 - 💡 Est un moyen simple d'attacher des politiques à plusieurs utilisateurs.
- 💡 Les stratégies IAM sont construites avec Java Script Notation (JSON):
 - 💡 Contenir des paires clé-valeur qui contiennent un nom et une valeur.
 - 💡 Exemple: {"name": "George Washington"}



Up Next: Module 4 – Cloud Architecting

- Part 1: Introduction to the Well-Architected Framework
- Part 2: Well-Architected Design Principles
- Part 3: Understanding Reliability and High Availability
- Part 4: Scaling
- Part 5: Example - Transitioning a Data Center to the Cloud



Thanks for participating!

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. Corrections or feedback on the course, please email us at: aws-course-feedback@amazon.com. For all other questions, contact us at: <https://aws.amazon.com/contact-us/aws-training/>. All trademarks are the property of their owners.