

# Bonnes pratiques pour la gestion des opérations de sécurité AWS

Julien Simon

Principal Technical Evangelist, AWS

[julsimon@amazon.fr](mailto:julsimon@amazon.fr)

@julsimon



# Agenda

- Modèle de sécurité partagée
- Protection des données
- Gestion des utilisateurs et des autorisations
- Journalisation des données
- Automatisation des vérifications
- Questions et réponses

# Modèle de sécurité partagée

# AWS partage avec vous la responsabilité de la sécurité

**Vous**

Applications et contenu client

Gestion de plateforme, d'applications, d'identité et d'accès

Configuration du système d'exploitation, du réseau et du pare-feu

Chiffrement des données côté client

Chiffrement des données côté serveur

Protection du trafic réseau

Vous devez définir vos contrôles **DANS** le cloud



Services de base AWS

Calcul

Stockage

Base de données

Mise en réseau

Infrastructure globale AWS

Zones de disponibilité

Régions

Emplacements périphériques

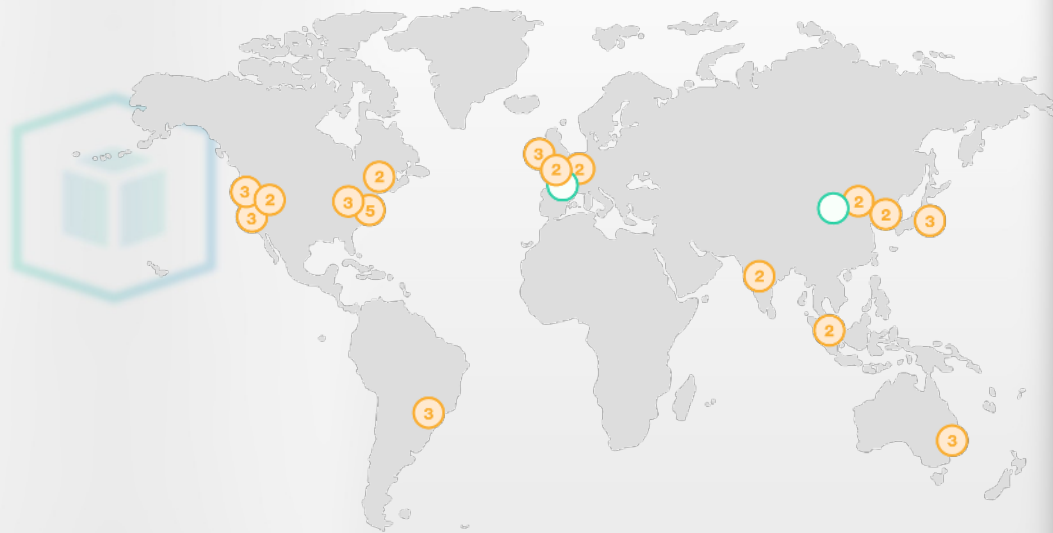
AWS se charge de la sécurité **DU** cloud



# Protection des données

# Vos données restent là où vous les mettez

- 16 régions, 42 zones de disponibilité
- Vous conservez le **contrôle** et la **propriété** complets de vos contenus
- AWS ne déplace **JAMAIS** les données en dehors de la région où **vous** les avez placées.



# Chiffrez vos informations sensibles

Chiffrement **client**

Chiffrement **serveur natif** pour de nombreux services

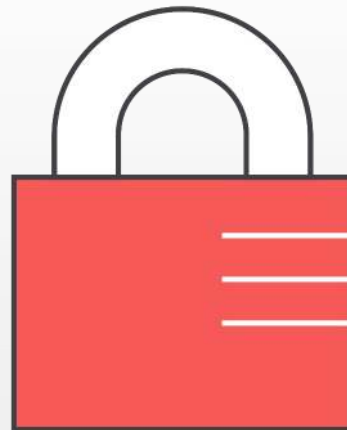
- S3, EBS, RDS, Redshift, etc.
- SSL/TLS de bout en bout

Gestion des clés évolutive

- **AWS Key Management Service** offre une gestion des clés évolutive et à coût réduit
- **AWS CloudHSM** offre une génération, un stockage et une gestion des clés extrêmement fiables et reposant sur le matériel

Options de chiffrement tierces

- Trend Micro, SafeNet, Vormetric, Hytrust, Sophos etc.
- AWS Marketplace : <https://aws.amazon.com/marketplace/>



# Gestion des utilisateurs et des autorisations



# Gestion des utilisateurs et des autorisations

## 1. Créez les utilisateurs



### Avantages

- Informations d'identification uniques
- Rotation des informations d'identification individuelles
- Autorisations individuelles
- Simplifie l'analyse

# Gestion des utilisateurs et des autorisations

1. Créez les utilisateurs
2. Accordez les privilèges les plus faibles possible



## Avantages

- Moins de risques d'erreurs humaines
- Il est plus facile d'assouplir que de durcir
- Contrôle plus détaillé

# Gestion des utilisateurs et des autorisations

1. Créez les utilisateurs
2. Accordez les privilèges les plus faibles possible
3. Gérez les autorisations avec des groupes



## Avantages

- Il est plus simple d'attribuer les mêmes autorisations à plusieurs utilisateurs
- Il est plus simple de réattribuer des autorisations selon les changements de responsabilités
- Un seul changement pour mettre à jour les autorisations de plusieurs utilisateurs

# Gestion des utilisateurs et des autorisations

1. Créez les utilisateurs
2. Accordez les privilèges les plus faibles possible
3. Gérez les autorisations avec des groupes
4. Limitez davantage les accès privilégiés à l'aide de conditions



## Avantages

- Niveau de détail supplémentaire lors de la définition des autorisations
- Possibilité d'activation pour n'importe quelle API de service AWS
- Limite les risques d'exécution d'actions privilégiées par accident

# Gestion des utilisateurs et des autorisations

1. Créez les utilisateurs
2. Accordez les privilèges les plus faibles possible
3. Gérez les autorisations avec des groupes
4. Limitez davantage les accès privilégiés à l'aide de conditions
5. Activez AWS CloudTrail pour obtenir des journaux d'appels d'API

## Avantages

- Visibilité sur votre activité utilisateur en enregistrant les appels d'API AWS dans un compartiment Amazon S3

# Gestion des informations d'identification

## 6. Configurez une stratégie de mot de passe fort

### Avantages

- Veille à ce que les utilisateurs et les données soient protégés



# Gestion des informations d'identification

6. Configurez une stratégie de mot de passe fort
7. Changez régulièrement vos informations d'identification de sécurité

## Avantages

- Bonne pratique classique



# Gestion des informations d'identification

6. Configurez une stratégie de mot de passe fort
7. Changez régulièrement vos informations d'identification de sécurité
8. Activez MFA pour les utilisateurs privilégiés



## Avantages

- Complète la saisie du nom d'utilisateur et du mot de passe en demandant un code unique lors de l'authentification



# Délégation

## 9. Utilisez les rôles IAM pour partager l'accès



### Avantages

- Il n'est pas nécessaire de partager les informations d'identification de sécurité
- Il n'est pas nécessaire de stocker les informations d'identification à long terme
- Cas d'utilisation
  - Accès entre comptes
  - Délégation intracompte
  - Fédération

# Délégation

9. Utilisez les rôles IAM pour partager l'accès
10. Utilisez les rôles IAM pour les instances Amazon EC2



## Avantages

- Facilité de gestion des clés d'accès sur les instances EC2
- Rotation automatique des clés
- Attribution de privilège moindre à l'application
- AWS SDK totalement intégrés
- Interface de ligne de commande AWS totalement intégrée

# Délégation

9. Utilisez les rôles IAM pour partager l'accès
10. Utilisez les rôles IAM pour les instances Amazon EC2
11. Réduisez ou supprimez l'utilisation du compte racine

## Avantages

- Moins de risques d'utilisation erronée des informations d'identification



# 11 bonnes pratiques IAM

1. **Utilisateurs** – Créez des utilisateurs.
2. **Autorisations** – Octroyez le privilège le plus faible.
3. **Groupe** – Gérez les autorisations avec des groupes.
4. **Conditions** – Limitez davantage l'accès privilégié à l'aide de conditions.
5. **Audit** – Activez AWS CloudTrail pour obtenir des journaux d'appels d'API.
6. **Mot de passe** – Configurez une stratégie de mot de passe fort.
7. **Rotation** – Changez régulièrement vos informations d'identification de sécurité.
8. **MFA** – Activez MFA pour les utilisateurs privilégiés.
9. **Partage** – Utilisez les rôles IAM pour partager l'accès.
10. **Rôles** – Utilisez les rôles IAM pour les instances Amazon EC2.
11. **Racine** – Réduisez ou supprimez l'utilisation du compte racine.

# Clés d'accès AWS ou mots de passe ?

Cela dépend de la façon dont les utilisateurs accéderont à AWS

- Console → Mot de passe
- API, CLI, SDK → Clés d'accès

Veillez à changer régulièrement vos informations d'identification

- Utilisez le rapport d'informations d'identification pour effectuer un audit du changement de ces informations
- Configurez une stratégie de mot de passe
- Configurez la stratégie de façon à permettre la rotation des clés d'accès

# Un compte AWS ou plusieurs comptes AWS ?

Utilisez **un compte AWS unique** lorsque :

- Vous souhaitez un contrôle plus simple des actions effectuées dans votre environnement et des personnes à l'origine de ces actions.
- Vous n'avez pas besoin d'isoler les projets, produits ou équipes.
- Vous n'avez pas besoin de dissocier les coûts.

Utilisez **plusieurs comptes AWS** lorsque :

- Vous avez besoin d'un **isolement total** entre les projets, équipes ou environnements.
- Vous souhaitez isoler les données de restauration et/ou les données d'audit (par exemple, en écrivant les journaux CloudTrail dans un autre compte).
- Vous avez besoin d'une seule facture, mais en dissociant le coût et l'utilisation.

# Journalisation des données

# Différentes catégories de journaux

## Journaux d'infrastructure

- AWS CloudTrail
- Journaux de flux VPC

## Journaux des services

- Amazon S3
- AWS Elastic Load Balancing
- Amazon CloudFront
- AWS Lambda
- AWS Elastic Beanstalk
- ...

## Journaux des instances

- Messages
- Sécurité
- NGINX/Apache/IIS
- Journaux d'événements Windows
- Compteurs de performances Windows
- ...



# CloudTrail

1. Activez dans toutes les régions



## Avantages

- Assure également le suivi des régions inutilisées
- Peut être effectué au cours d'une seule étape de configuration

# CloudTrail

1. Activez dans toutes les régions
2. Activez la validation du fichier journal



## Avantages

- Garantit l'intégrité des fichiers journaux
- Les fichiers journaux validés s'avèrent utiles lors d'enquêtes de sécurité et légales
- Créé à l'aide des algorithmes standard du secteur: SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique
- CloudTrail commencera à diffuser les fichiers de valeur de hachage toutes les heures
- Les fichiers de valeur de hachage contiennent les valeurs de hachage des fichiers journaux diffusés et sont signés par CloudTrail

# CloudTrail

1. Activez dans toutes les régions
2. Activez la validation du fichier journal
3. Chiffrez les journaux



## Avantages

- Par défaut, CloudTrail chiffre les fichiers journaux à l'aide du chiffrement côté serveur de S3 (SSE-S3)
- Vous pouvez choisir de chiffrer à l'aide d'AWS Key Management Service (SSE-KMS)
- S3 détermine si vos informations d'identification sont autorisées à déchiffrer

# CloudTrail

1. Activez dans toutes les régions
2. Activez la validation du fichier journal
3. Chiffrez les journaux
4. Intégration aux journaux Amazon CloudWatch



## Avantages

- Recherche simple
- Configuration des alertes sur les événements

# CloudTrail

1. Activez dans toutes les régions
2. Activez la validation du fichier journal
3. Chiffrez les journaux
4. Intégration aux journaux Amazon CloudWatch
5. Centralisez les journaux de tous les comptes

## Avantages

- Configuration de tous les comptes pour envoyer les journaux vers un compte de sécurité centralisé
- Réduction des risques de falsification des journaux
- Possibilité de combinaison avec S3 CRR
- Incluez les comptes de développement/temporaires !

# Journaux de flux VPC

- Stocke les journaux réseaux dans CloudWatch
- Peuvent être activés sur un VPC, un sous-réseau ou une interface réseau
- Filtrez les résultats souhaités en fonction de vos besoins
  - Tout, refuser, accepter
  - Dépannage ou sécurité lié à des besoins d'alerte ?
  - Réfléchissez avant d'activer tout : comment l'utiliserez-vous ?

# Journaux des services AWS

De nombreux services vous permettent d'exporter leurs logs vers CloudWatch Logs, CloudTrail ou S3.

- **Elastic Beanstalk** → CloudWatch Logs

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/AWSHowTo.cloudwatchlogs.html> <https://aws.amazon.com/fr/about-aws/whats-new/2016/12/aws-elastic-beanstalk-supports-application-version-lifecycle-management-and-cloudwatch-logs-streaming/>

- **ECS** (instances & containers) → CloudWatch Logs [http://docs.aws.amazon.com/AmazonECS/latest/developerguide/using\\_awslogs.html](http://docs.aws.amazon.com/AmazonECS/latest/developerguide/using_awslogs.html)

- **Lambda** → CloudWatch Logs

<http://docs.aws.amazon.com/lambda/latest/dg/monitoring-functions-logs.html>

- **S3** → CloudTrail (S3 data events)

- **CloudFront** → S3

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html>

- **ELB / ALB** → S3

<http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

# Journaux des instances EC2

Les journaux CloudWatch vous permettent de collecter toutes les informations de vos instances et de surveiller leur activité

- Le coût du stockage est peu élevé : conservez les journaux
- La collecte est effectuée par l'agent CloudWatch (Linux et Windows)
- Les données peuvent être exportées :
  - Vers S3
  - Vers Amazon ElasticSearch Service ou AWS Lambda
- L'intégration aux métriques et aux alarmes vous permet de continuellement rechercher des événements suspects



# Automatisation de la sécurité

# Plusieurs niveaux d'automatisation

- Automatisation du *provisioning* infrastructure & applicatif
  - AWS CloudFormation
  - AWS OpsWorks
- Autogestion
  - AWS CloudTrail → journaux Amazon CloudWatch → Alertes Amazon CloudWatch
  - AWS CloudTrail → Amazon SNS → AWS Lambda
  - Appels API → Amazon CloudWatch Events → SNS / SQS / Kinesis / AWS Lambda
- Validation de la conformité
  - AWS Inspector (contenu des instances EC2)
  - AWS Config Rules

# Amazon CloudWatch Events

- Déclenchement suite à un événement
  - Cycle de vie EC2, Auto Scaling
  - Appel d'API AWS
  - Ajout régulier de nouvelles sources (AWS Health)
- Déclenchement planifié
  - cron est dans le cloud !
  - Toutes les 5 minutes minimum
- Un événement peut avoir plusieurs cibles



# AWS Config Rules

- Config Rules vérifie la **conformité de la configuration** des ressources AWS.
- Vous pouvez utiliser :
  - Des règles **prédéfinies** par AWS : MFA activé, CloudTrail activé, volumes EBS chiffrés, etc.
  - Des règles **personnalisées**
- Les vérifications peuvent être :
  - **Périodiques** (1, 3, 6, 12 ou 24 heures)
  - **Déclenchées** par les changements de configuration
- Vous pouvez notifier les changements de conformité par SNS...
- ... et réagir avec des fonctions Lambda 😊
  - Par ex: une instance non conforme a été lancée ? On la tue !



# Amazon Inspector




Il vous permet d'analyser le contenu et le comportement des instances EC2 et d'identifier les problèmes de sécurité potentiels

- Evaluation de la sécurité des applications
  - Basé sur un agent
  - 15 min – 24 h
- Règles intégrées
  - CVE (vulnérabilités et expositions courantes)
  - Préparation à PCI DSS 3.0
  - ...
- Résultats de sécurité et conseils pour corriger les vulnérabilités
- Automatisable via les API






# AWS Trusted Advisor



## Recommended Actions

-  **Security Groups - Specific Ports Unrestricted** Updated: 9/29/14 7:19 AM  



Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

2 of 71 security group rules allow unrestricted access to a specific port.
-  **IAM Use** Updated: 9/17/14 12:39 PM  

Checks for your use of AWS Identity and Access Management (IAM).

At least one IAM user, group, or role has been created for this account.
-  **MFA on Root Account** Updated: 9/17/14 12:39 PM 

Checks the root account and warns if multi-factor authentication (MFA) is not enabled.

MFA is enabled on the root account.
-  **Service Limits** Updated: 9/17/14 12:39 PM 

Checks for usage that is more than 80% of the service limit.

0 of 42 items have usage that is more than 80% of the service limit.

**Security**



2

1

0

# Ressources complémentaires

Livre blanc : Overview of AWS Security Processes

<https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>

Livre blanc : AWS Well-Architected Framework

[http://d0.awsstatic.com/whitepapers/architecture/AWS\\_Well-Architected\\_Framework.pdf](http://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)

Livre blanc : Security Best Practices

[https://d0.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Best\\_Practices.pdf](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)

AWS re:Invent 2016: Security Services State of the Union (SEC312)

Steve Schmidt, CISO, Amazon Web Services

<https://www.youtube.com/watch?v=8ZljcKn8FPA>

AWS re:Invent 2016: Automating Security Event Response, from Idea to Code to Execution (SEC313)

<https://www.youtube.com/watch?v=x4GkAGe65vE>

# Merci !

Julien Simon

Principal Technical Evangelist, AWS

[julsimon@amazon.fr](mailto:julsimon@amazon.fr)

@julsimon

