Security/Compliance

Identity & Access Management (IAM)

Service global qui couvre toutes les régions

Composants

Users

- Objets identifiant les utilisateurs (personne ou compte pour l'accès d'une application)
- Un utilisateur peut être associé à 10 groupes maximum

Groups

- Objets identifiant plusieurs utilisateurs.
- Sont associés à des policy permissions.
- Par défaut 100 groupes maximum par compte.

Roles

- Objets associés à différentes identités pour leur donner des permissions
- 4 types de roles : AWS Service Role, AWS Service-Linked Role, Role for Cross-Account Access, Role for Identity Provider Access

Policy Permissions

- JSON policies qui définissent quelles ressources peuvent être accédées ou pas.
- Fournis par AWS ou définis par le client.

Access Control Mechanisms

- Mécanismes qui indiquent comment une ressource peut être accédée

Security Status

5 bonnes pratiques vérifiés par AWS sur le compte :

- Activation MFA sur le compte root
- créer des utilisateurs individuels
- utiliser des groupes pour assigner les permissions
- appliquer une IAM password policy
- changer les clés d'accès régulièrement

IAM Policies

Managed Policies

- Peuvent être attachées à plusieurs utilisateurs, groupes ou rôles
- AWS Managed Policies : police préconfigurée proposée par AWS pour les besoins classiques
- Customer Managed Policies : peuvent être créés en modifiant une fournie par AWS, à partir du Policy Genrerator ou manuellement

Inline Policies

- Attachée à un seul utilisateur, groupe ou rôle
- Création par le Policy Generator ou manuellement

Multi-Factor Authentication (MFA)

- Double authentification

Identity Federation

- Permet l'accès sans compte AWS avec une identification tierce d'un Identity Provider (IdP)
- Fonctionne avec 2 type IdP : OpenID Connect (Facebook, Amazon, Google, ...) et SAML (MS Active Directory)

Cross-Account Access

- Permet l'accès aux services d'un autre compte AWS à l'aides des roles
- Trusted account : compte auquel on fait confiance (celui à qui on donne l'accès)
- Trusting account : compte qui fait confiance (celui qui donne l'accès)
- On prend le role en basculant au niveau du compte “switch role”

KMS

Fonctionne au sein d'une région

Cryptographie

symmetric encryption

- une seule clef est utilisée pour crypter et décrypter les données
- Exemples : AES, DES (Digital Encryption Standard), Triple-DES, Blowfish, ...

asymmetric cryptography

- on génère une clef publique et une clef privée
- on donne la clef publique pour crypter les données
- les 2 clefs sont nécessaires pour décrypter, nous seront donc les seuls à pouvoir le faire
- Exemples : RSA (Rivest-Shamir-Adleman), Diffie-Hellman, Digital Signature Algorithm

Composants

Customer Master Keys (CMK)

- Utiliser typiquement pour encrypter les DEK qui sont ensuite utilisées par d'autres services AWS
- 2 types : Customer managed CMKs et AWS managed CMKs

Data Encryption Keys (DEK)

- Créés par par les CMKs et utilisées pour encrypter les données
- Envelope encryption : la clef de cryptage est elle-même cryptée

Key Policies

- Définir les accès aux clefs KMS

Grants

- Délégation d'accès aux clefs KMS à un service AWS

Accès

Via Key Policies

Via Key Policies avec IAM

Via Key Policies avec Grants

Management

Rotation

- Possibilité d'activer une rotation automatique tous les 365 jours (impossible sur une clef importée). Les clefs précédentes sont toujours utilisables sur les données cryptées avant.

Importation

- Importation d'une clef publique

Suppression

- KMS programme l'effacement dans un délai de 7 à 30 jours. La clef est mise dans un état “Pending deletion” où elle ne peut plus servir
- Possibilité d'utiliser CloudTrail pour détecter une utilisation ou bien de programmer une alarme avec CloudWatch
- En cas de doute sur l'absence d'utilisation de la clef il est également possible de la désactiver plutôt que de la supprimer

---

CloudHSM

- HSM : Hardware Security Module, composant physique non partagé

Secret Manager

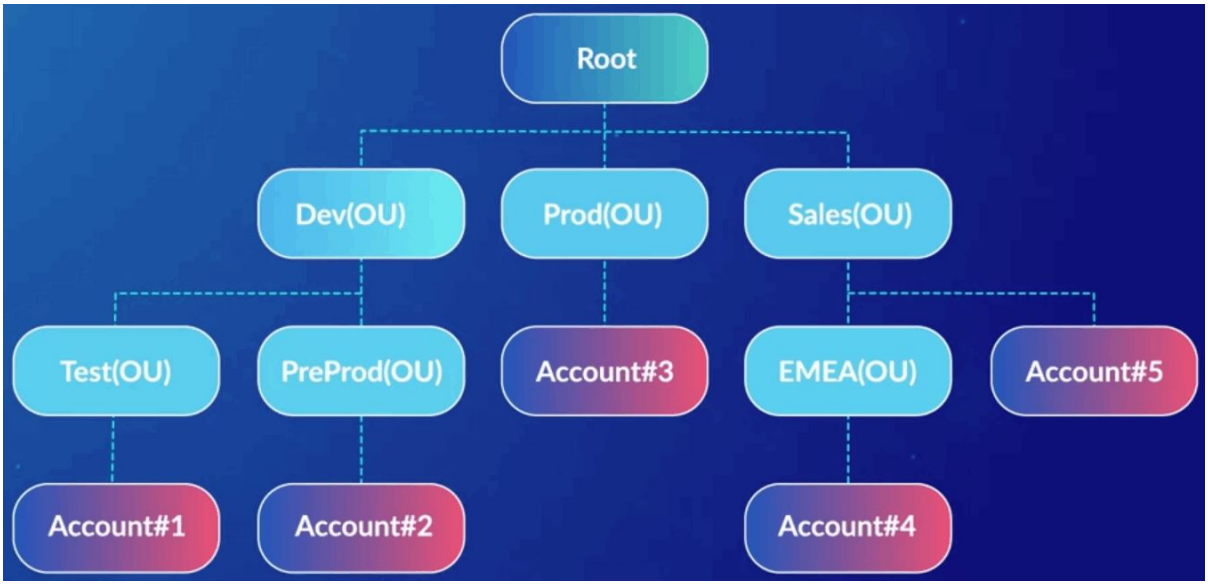
Secret Manager

- Permet le stockage de secrets (mot de passe, clefs d'accès, ...)
- Cryptage systématique
- Possibilité d'activer une rotation automatique pour mettre à jour automatiquement à partir d'une lambda fonction
- Possibilité de partager avec un autre compte AWS
- Jusqu'à 10 Ko, payement pour chaque secret storage plus le nombre d'appels via l'API chaque mois
- Accès défini par des IAM identity-based policies et IAM resource-based policies

Parameter Store

- Permet le stockage de paramètres (qui peuvent être aussi des mots de passe)
- Cryptage optionnel
- Pas de gestion de rotation automatique
- Standard jusqu'à 4Ko (gratuit) ou advanced jusqu'à 8 Ko (payant)

AWS Organizations



- Root :container en haut de l'organisation, tous les éléments se trouvent sous ce root
- Organizational Units : pour catégoriser les account. Rattaché sous root ou une autre OU (jusqu'à 5 niveaux)
- Accounts : ce sont les comptes AWS dans lesquels on peut gérer les ressources
- Service Control Policies : contrôle quels services et fonctionnalités sont accessibles par un compte. Ces SCPs peuvent être associées au niveau root, OU ou account (elles s'appliquent ensuite à tous les objets enfants)

Firewall

Web Application Firewall (WAF)

Conditions

- Cross-site scripting
- Geo match
- IP addresses
- Size constraints

- SQL injection attacks
- String and regex matching

Rules

- Regular Rule : association de conditions (ET logique)
- Rate-based Rule : limite les accès depuis une adresse IP au delà d'un certains nombre de requête par période de 5 mn

ACLs

Association d'une action à chaque règle

- Allow
- Block
- Count

Intégration avec CloudWatch

- Par défaut relevé toutes les minutes et conservés pour 2 semaines
- Les métriques sont : AllowedRequests, BlockedRequests, CountedRequests, PassedRequests (requêtes qui ne correspondent à aucune règle WAF)

Intégration avec CloudFront

- Une fois l'association faite entre une WEB ACL et une distribution CloudFront, cela peut prendre 15mn à se propager à tous les Edge Locations
- Possibilité de customiser l'erreur 403 retourné à l'utilisateur

AWS Firewall Manager

Permet de gérer WAF dans un environnement de plusieurs compte au travers des Organizations.

Prérequis

- Le compte doit faire partie d'une organization
- Un compte doit être défini comme Firewall Manager Admin
- AWS Config doit être activé

Composants

- WAF Rules
- Rules Groups : regroupe des règles qui ont la même action (Block ou Count mais pas Allow). A

créer soi-même ou à acheter sur AWS Marketplace
- Firewall Manager Policies : contient les Rules Groups à assigner aux ressources. 2 Rules groups max par Policy (1 customer et 1 Marketplace)

Coût : 100$ / mois par policy et par région.

AWS Shield

Prévention contre les attaques DDoS (Distributed Denial of Service) qui peuvent être de différents types :

- SYN flood : envoi de SYN et suite au SYN ACK laisse la connexion ouverte
- DNS query flood : attaque du DNS par de multiples requêtes
- HTTP flood/Cache-busting : attaque par requêtes HTTP éventuellement en passant outre du cache pour attaquer le serveur source

AWS Shield Standard

- Gratuit
- Contre les attaques DDoS au niveau 3 (réseau) et niveau 4 (transport)
- Intégré dans CloudFront et Route 53

AWS Shield Advanced

- Protection des applications sur EC2, CloudFront, ELB et Route 53
- Protection plus importante des attaques DDoS niveau 3 (réseau), niveau 4 (transport) et niveau 7 (application)
- Assistance 24/24 d'une équipe spécialisée
- 3 000 $ / mois avec WAF intégré + frais de transfert

AWS Single-Sign On (SSO)

Permet un accès à plusieurs account AWS avec un un accès SSO.

Cognito

Authentication and user management service

User pool

- Pour créer et maintenir l'annuaire des utilisateurs
- Gère les inscription et les connexions

Identity pool

- Permet un accès temporaire à des utilisateurs ou bien des invités
- 2 type d'identités : authentifié et non authentifié
- Chaque identité a un rôle et chaque rôle à une policy attachée qui décrit les permissions

---

From:
https://wiki.iot-acs.fr/ - **Wiki**

Permanent link:
https://wiki.iot-acs.fr/doku.php?id=all:bibles:aws:presentation:8-security

Last update: **2026/07/23 13:30**