# Pilier Security du AWS Well-Architected Framework

## 1. Rappel du cadre

Le AWS Well-Architected Framework est un référentiel de bonnes pratiques permettant d'évaluer et d'améliorer une architecture Cloud.

Il repose sur six piliers :

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization
- Sustainability

Le pilier Security définit les principes permettant de protéger les systèmes, les données et les identités dans le Cloud.

---

## 2. Objectif du pilier Security

L'objectif est de :

- Assurer la confidentialité des données
- Garantir l'intégrité des systèmes
- Maintenir la disponibilité des services
- Détecter les menaces rapidement
- Réagir efficacement aux incidents
- Maintenir la conformité réglementaire

Il s'inscrit dans le modèle de responsabilité partagée entre AWS et le client.

---

## 3. Principes de conception

### 3.1 Mettre en place une base d'identités solide

- Centraliser la gestion des identités
- Appliquer le principe du moindre privilège
- Activer le MFA
- Éviter l'usage quotidien du compte root

### 3.2 Activer la traçabilité

- Journaliser toutes les actions (CloudTrail)

- Surveiller les métriques et événements (CloudWatch)
- Détecter les comportements anormaux (GuardDuty)
- Protéger et conserver les journaux

### 3.3 Appliquer une défense en profondeur

- Sécurité réseau (VPC, Security Groups, NACL)
- Durcissement des systèmes
- Sécurité applicative
- Chiffrement des données en transit et au repos

### 3.4 Automatiser les contrôles de sécurité

- Infrastructure as Code
- Déploiements reproductibles
- Vérification continue de conformité (AWS Config)

### 3.5 Protéger les données

- TLS pour les flux réseau
- Chiffrement au repos
- Gestion des clés avec AWS KMS
- Gestion des secrets avec Secrets Manager
- Rotation régulière des clés

### 3.6 Préparer la réponse aux incidents

- Plan de réponse documenté
- Procédures d’escalade
- Isolation rapide des ressources compromises
- Analyse post-incident et amélioration continue

---

## 4. Synthèse pédagogique

Le pilier Security structure l’ensemble du module :

- Comprendre les risques Cloud
- Maîtriser IAM
- Gérer clés et secrets
- Surveiller et détecter
- Répondre aux incidents
- Sécuriser les données

La sécurité dans AWS n’est pas un paramètre à activer, mais une démarche continue intégrée dès la conception.

---

# Message clé

Sécuriser le Cloud, c’est :

- Concevoir sécurisé dès le départ
- Automatiser les contrôles
- Surveiller en permanence
- Tester régulièrement
- Améliorer en continu

Le Well-Architected Framework est un outil d’évaluation permettant de challenger toute architecture AWS selon des critères structurés et reconnus.