Approche Zero Trust

1. Définition

Le modèle Zero Trust repose sur le principe suivant :

- Ne jamais faire confiance par défaut
- Toujours vérifier
- Appliquer le principe du moindre privilège
- Considérer qu'une compromission est possible

Contrairement au modèle périmétrique traditionnel (pare-feu en frontière et réseau interne de confiance), le Zero Trust considère que :

- Le réseau interne n'est pas intrinsèquement fiable
- L'identité devient le nouveau périmètre de sécurité
- Chaque requête doit être authentifiée et autorisée
- La vérification doit être continue

Ce modèle est particulièrement adapté aux environnements Cloud, hybrides et multi-cloud.

2. Limites du modèle périmétrique traditionnel

2.1 Architecture classique on-premise

- Pare-feu en frontière
- Réseau interne considéré comme sûr
- VPN pour accès distant
- Segmentation interne limitée

2.2 Problèmes majeurs

- Mouvement latéral facilité en cas de compromission
- Confiance excessive dans le réseau interne
- Difficulté à sécuriser le télétravail
- Visibilité limitée des flux internes
- Inadapté aux architectures dynamiques (microservices, conteneurs)

Dans le Cloud :

- Il n'existe plus de périmètre fixe
- Les ressources sont accessibles via API
- Les identités remplacent les adresses IP comme point central de contrôle

3. Principes fondamentaux du Zero Trust

3.1 Vérification explicite

Chaque demande d'accès doit être :

- Authentifiée
- Autorisée
- Journalisée

Exemples :

- MFA obligatoire
- Vérification du terminal
- Analyse du contexte (IP, géolocalisation, comportement)

3.2 Principe du moindre privilège

Un utilisateur ou service ne dispose que :

- Des permissions strictement nécessaires
- Sur les ressources strictement nécessaires
- Pour une durée limitée

Application sur AWS :

- Policies IAM granulaires
- Utilisation de rôles plutôt que d'utilisateurs IAM
- Accès temporaires via STS
- Suppression des clés d'accès permanentes

3.3 Micro-segmentation

Objectif : limiter les mouvements latéraux.

Mise en œuvre sur AWS :

- Security Groups restrictifs
- Network ACL
- Segmentation par VPC
- Sous-réseaux publics et privés
- Stratégie multi-comptes via AWS Organizations

3.4 Hypothèse de compromission

Le modèle Zero Trust considère qu'une intrusion peut déjà être présente.

Conséquences :

- Surveillance continue
- Centralisation des journaux
- Détection comportementale
- Rotation régulière des clés
- Automatisation des réponses aux incidents

4. Zero Trust et responsabilité partagée AWS

Dans AWS :

- AWS sécurise l'infrastructure physique
- Le client sécurise :
    - Les identités
    - Les configurations
    - Les données
    - Les permissions IAM
    - Les flux réseau

Le Zero Trust s'applique donc principalement aux responsabilités du client.

5. Mise en œuvre du Zero Trust sur AWS

5.1 L'identité comme nouveau périmètre

Services concernés :

- AWS IAM
- IAM Identity Center
- AWS Organizations
- AWS STS

Bonnes pratiques :

- MFA obligatoire
- Compte root protégé et non utilisé
- Accès temporaires
- Rôles plutôt qu'utilisateurs IAM

5.2 Sécurisation des accès réseau

- Ne pas exposer inutilement les instances sur Internet
- Utiliser un bastion ou Session Manager
- Mettre en place des VPC Endpoints privés
- Utiliser AWS WAF et AWS Shield

5.3 Protection des workloads et des données

- Chiffrement au repos et en transit
- AWS KMS pour la gestion des clés
- AWS Secrets Manager pour les secrets
- Rotation automatique des secrets
- Restriction d'accès aux métadonnées EC2

5.4 Surveillance continue

Services AWS mobilisables :

- AWS CloudTrail
- Amazon CloudWatch
- Amazon GuardDuty
- AWS Security Hub

- AWS Config

Objectifs :

- Détection d'anomalies
- Détection d'escalade de privilèges
- Identification d'accès suspects
- Vérification de conformité continue

6. Étude de cas pédagogique

Contexte :

Une entreprise migre son SI vers AWS :

- Développeurs en télétravail
- API exposée publiquement
- Base de données en sous-réseau privé

Questions :

1. Quels sont les points faibles d'un modèle périmétrique dans ce contexte ?
2. Comment appliquer concrètement le Zero Trust ?
3. Quels services AWS utiliser ?
4. Où appliquer le principe du moindre privilège ?
5. Comment limiter le mouvement latéral ?

7. Synthèse

Le Zero Trust n'est pas un produit mais :

- Un modèle d'architecture
- Une stratégie de sécurité
- Une approche adaptée aux environnements Cloud modernes

Dans AWS, cela implique :

- Identité centrale
- Contrôle d'accès granulaire
- Segmentation forte
- Chiffrement systématique
- Surveillance continue
- Automatisation de la réponse aux incidents

From:
http://slamwiki2.kobject.net/ - **SlamWiki 2.1**

Permanent link:
http://slamwiki2.kobject.net/eadl/bloc4/fm4/zero-trust

Last update: **2026/02/28 17:15**