Pràctica de Laboratori: ACL i Grups de Seguretat a AWS

Context

Aquesta pràctica forma part del curs **AWS Cloud Foundations** i té com a objectiu entendre i aplicar els conceptes de **Network Access Control Lists (NACLs)** i **Security Groups** dins d'una VPC d'AWS.

Objectius d'aprenentatge

En finalitzar la pràctica, l'alumne serà capaç de:

- Diferenciar entre **ACLs de xarxa** i **Grups de seguretat**.
- Configurar una **VPC** amb una subxarxa pública.
- Crear i associar una **NACL personalitzada**.
- Crear i configurar **grups de seguretat**.
- Verificar el funcionament mitjançant una instància EC2.

Durada estimada

⏱️ 60 – 90 minuts

Requisits previs

- Compte d'AWS actiu
- Accés a la **AWS Management Console**
- Coneixements bàsics de:
    - VPC
    - EC2
    - Protocols TCP/IP (HTTP, SSH)

Part 1: Creació de la infraestructura bàsica

1. Crear una VPC

1. Accedeix a **VPC > Your VPCs**.
2. Clica **Create VPC**.
3. Configura:
    - Name: Lab-VPC
    - IPv4 CIDR block: 10.0.0.0/16
4. Crea la VPC.

2. Crear una subxarxa pública

1. Ves a **Subnets > Create subnet**.
2. Configura:
    - VPC: Lab-VPC
    - Name: Public-Subnet
    - CIDR block: 10.0.1.0/24
    - Availability Zone: qualsevol
3. Desa els canvis.

3. Internet Gateway i taula de rutes

1. Crea un **Internet Gateway** (Lab-IGW).
2. Associa'l a Lab-VPC.
3. Edita la **Route Table** principal:
    - Afegeix ruta 0.0.0.0/0 → Internet Gateway.

Part 2: Network Access Control List (NACL)

4. Crear una NACL personalitzada

1. Ves a **Network ACLs > Create network ACL**.
2. Configura:
    - Name: Lab-NACL
    - VPC: Lab-VPC

5. Configurar regles d'entrada (Inbound)

Afegeix les següents regles:

Rule #	Type	Protocol	Port	Source	Allow/Deny
100	HTTP	TCP	80	0.0.0.0/0	ALLOW
110	SSH	TCP	22	0.0.0.0/0	ALLOW
*	All traffic	All	All	0.0.0.0/0	DENY

6. Configurar regles de sortida (Outbound)

Rule #	Type	Protocol	Port	Destination	Allow
100	All traffic	All	All	0.0.0.0/0	ALLOW

7. Associar la NACL a la subxarxa

- Associa Lab-NACL a Public-Subnet.

Part 3: Grups de Seguretat

8. Crear un grup de seguretat

1. Ves a **EC2 > Security Groups > Create security group**.
2. Configura:
    - Name: Lab-SG
    - VPC: Lab-VPC

9. Regles d'entrada

Type	Protocol	Port	Source
SSH	TCP	22	La teva IP
HTTP	TCP	80	0.0.0.0/0

Nota: No cal definir regles d'eixida (per defecte estan permeses).

Part 4: Llançar una instància EC2

10. Crear instància

1. Ves a **EC2 > Launch instance**.
2. Configura:
    - AMI: Ubuntu
    - Network: Lab-VPC
    - Subnet: Public-Subnet
    - Security Group: Lab-SG
    - Auto-assign Public IP: Enabled

11. Prova de connectivitat

- Connecta't per **SSH**.
- Instal·la Apache:
- `sudo apt update`
- `sudo service apache2 start`
- Accedeix des del navegador a la IP pública.

Part 5: Validació i experiments

12. Proves recomanades

- Elimina la regla HTTP del **Security Group** → comprova l'accés.
- Elimina la regla HTTP de la **NACL** → comprova l'accés.
- Observa diferències de comportament.

Preguntes de reflexió

1. Quina és la diferència principal entre una NACL i un Security Group?
2. Quin element és **stateful** i quin és **stateless**?
3. Quin recomanaries per controlar accés a nivell d'instància?

Neteja de recursos (IMPORTANT)

- Elimina:
    - Instància EC2
    - Security Group
    - NACL
    - Subxarxa
    - Internet Gateway
    - VPC

Resultat esperat

L'alumne ha de demostrar que entén com **les ACLs controlen el trànsit a nivell de subxarxa** i com **els grups de seguretat protegeixen les instàncies**.
