🖥️ Tutorial: Provisionando VM, Load Balancer e WAF na Oracle Cloud (OCI)

🔑 Pré-requisitos

- Acesso ao Console da **OCI** com permissões no compartment Lab-Cloud-App.
- **VCN vcn-labCloud** já criada com a subnet privada private subnet-vcn-labCloud.
- **OCI CloudShell** habilitado (ícone de terminal no canto superior direito do console).

🚀 Parte 1: Criar a VM

1. **Acesse o Console da OCI**
   - Entre em https://cloud.oracle.com.
   - No menu, vá em ☰ **Menu → Compute → Instances**.

2. **Selecione o Compartment**
   - No canto esquerdo, selecione o compartment **Lab-Cloud-App**.

3. **Criar Instância**
   - Clique em **Create instance**.
   - Nome da instância: vm-labcloud-app.

4. **Escolha a Imagem**
   - Clique em **Change Image**.
   - Selecione **Oracle Linux 8**.

5. **Escolha a Forma (Shape)**
   - Clique em **Change Shape**.
   - Escolha **VM.Standard.E4.Flex**.
   - Configure **1 OCPU** e **4 GB RAM**.

6. **Configuração de Rede**
   - **VCN**: vcn-labCloud.
   - **Subnet**: private subnet-vcn-labCloud.
   - **Assign a public IPv4 address**: **desmarcado** (a instância ficará apenas na rede privada).

7. **Gerar e Baixar Chaves SSH**
   - Na seção **SSH Keys**, escolha **Generate a key pair**.
   - Clique em **Save Private Key** e **Save Public Key** → os arquivos serão baixados para o seu computador.

8. **Criar Instância**
   - Clique em **Create** e aguarde até ficar em estado **Running**.

🔗 Parte 2: Preparar o CloudShell

1. **Abrir o CloudShell**
    - No canto superior direito do console, clique no ícone **CloudShell** (terminal).
    -
2. **Fazer Upload da Chave Privada**
    - No CloudShell, clique no botão de **Upload** (ícone de pasta).
    - Envie o arquivo da **chave privada** que você baixou (oci_api_key.pem).
    -
3. **Ajustar Permissões da Chave**
4. chmod 400 <nome_da_chave>.pem

5. **Pinar o CloudShell na Rede Privada**
    - No CloudShell, clique em **⋮ (menu de 3 pontos)** → **Pin to VCN**.
    - Escolha:
        - **VCN**: vcn-labCloud
        - **Subnet**: private subnet-vcn-labCloud
    - Isso conecta o CloudShell à mesma rede da VM.

🔑 Parte 3: Acessar a VM

1. **Pegar o IP Privado da VM**
    - No console, abra os detalhes da instância vm-labcloud-app.
    - Copie o **Private IP Address**.

2. **Conectar via SSH pelo CloudShell**
3. ssh -i <nome_da_chave>.pem opc@<ip_privado_da_vm>

4. **Testar Acesso**
    - Se conectar corretamente, você verá o prompt do usuário opc.
    - Teste rodando:
    - hostname

⚙️ Parte 4: Configurar a Aplicação

1. Dentro da VM, siga o passo a passo do README do workshop.
2. Garanta que a aplicação esteja rodando na porta **8080**:
3. curl http://localhost:8080

🌐 Parte 5: Criar o Load Balancer Público

1. **Criar Load Balancer**
    - Vá em ☰ **Menu → Networking → Load Balancers**.
    - Clique em **Create Load Balancer**.

- Nome: lb-labcloud.
- Tipo: **Public**.
- Forma: **Flexible** (ou 10 Mbps para testes).
- VCN: vcn-labCloud.
- Subnet: escolha **uma subnet pública**.

2. **Listener**
   - Nome: http-listener.
   - Protocolo: HTTP.
   - Porta: 80.

3. **Backend Set**
   - Nome: backend-vm-labcloud.
   - Protocolo: HTTP.
   - **Health Check**:
     - Tipo: TCP
     - Porta: **8080**
     - Intervalo: 10s
     - Timeout: 3s
     - Falhas antes de marcar como unhealthy: 3

4. **Adicionar Backend**
   - Clique em **Add Backend**.
   - Insira o **Private IP** da VM.
   - Porta: **8080**.

5. **Criar LB**
   - Clique em **Create Load Balancer**.

🌐 Parte 6: Configurar o WAF no Load Balancer

1. **Acessar o serviço WAF**
   - No console, vá em ☰ **Menu → Security → Web Application Firewall**.
   - Clique em **Create Web Application Firewall policy**.

2. **Configurar a Policy**
   - Nome: waf-lb-labcloud.
   - Compartment: **Lab-Cloud-App**.
   - Tipo de recurso protegido: **Load Balancer**.
   - Escolha o **lb-labcloud** criado na Parte 5.
   - Clique em **Create Web Application Firewall policy**.

3. **Adicionar Ações Personalizadas (Actions)**
   No menu da policy criada, vá em **Actions → Add Action** e configure as seguintes:
   - **Deny-XSS**
     - Action type: **Return HTTP response**
     - Response code: **403 Forbidden**

        - Content-Type: application/json
        - Response body: vazio (default)

    - **Deny-SQLi**
        - Action type: **Return HTTP response**
        - Response code: **403 Forbidden**
        - Content-Type: application/json
        - Response body:
        - {"code":"403","message":"Blocked by WAF - SQL Injection","RequestId":"${http.request.id}"}

    - **Deny-BigPost**
        - Action type: **Return HTTP response**
        - Response code: **403 Forbidden**
        - Content-Type: application/json

    - **Deny-RateLimit**
        - Action type: **Return HTTP response**
        - Response code: **403 Forbidden**
        - Content-Type: application/json
        - Response body:
        - {"code":"403","message":"Blocked by WAF - RateLimit","RequestId":"${http.request.id}"}

4. **Adicionar Regras de Proteção (Protection Rules)**
    - **XSS**
        - Rule name: XSS
        - Condition: i_equals(http.request.url.path, '/comentarios')
        - Action: Deny-XSS
        - Body inspection: **marcado**
        - Ative as seguintes assinaturas (rule IDs):
            - 941140
            - 9410000
            - 941120
            - 941110

    - **SQLi**
        - Rule name: SQLi
        - Condition: i_equals(http.request.url.path, '/login')
        - Action: Deny-SQLi
        - Body inspection: **marcado**
        - Ative a assinatura (rule ID):
            - 942130

    - **BigPost**
        - Rule name: BigPost
        - Condition: i_equals(http.request.url.path, '/upload')
        - Action: Deny-BigPost

        - Body inspection: **marcado**
        - Ative a assinatura (rule ID):
            - 930120

5. **Adicionar Regra de Rate Limiting**
    - Clique em **Rate Limiting Rules → Add Rule**.
    - Nome: RateLimit-Login.
    - Condition: i_equals(http.request.url.path, '/login')
    - Requests limit: **5**
    - Period in seconds: **10**
    - Action duration in seconds: **30** (opcional).
    - Action: Deny-RateLimit.

6. **Salvar e Ativar**
    - Clique em **Save changes**.
    - Certifique-se de que a policy está **Attached** ao lb-labcloud.