Privaclave AWS Deployment Manual

Pre-requisites:

- Create an **EC2** instance of at least **t3.medium** configuration with **Red Hat Enterprise Linux**.

Step 1: Prepare the Setup

- ✓ Gain root access:

```bash
sudo -i
```

- ✓ Update and install **wget**

```bash
sudo yum update -y
sudo yum install -y wget
```

- ✓ Install **unzip** (if not already installed)**:**

```bash
sudo yum install -y unzip
```

- ✓ Download the **privaclave_setup** zip file**:**

wget https://github.com/privaclave-internal/privaclave-setup/raw/main/privaclave_setup_0.0.1.zip -O privaclave_setup_0.0.1.zip

- ✓ Unzip the setup file:

```bash
unzip privaclave_setup_0.0.1.zip
```

  - Apply (Read , Write and execute) permission → **chmod 777 privaclave_setup_0.0.1**

Step 2: Configure AWS Credentials

- ✓ Navigate to the unzipped privaclave_setup_0.0.1 directory

```bash
cd privaclave_setup_0.0.1
```

✓ Open **AwsConfig.properties** file for editing

```bash
nano AwsConfig.properties
```

***** alternative way : vi AwsConfig.properties (if nano not installed)

✓ Update the file with your **AWS credentials**

```properties
AwsAccessKeyId=YOUR_AWS_ACCESS_KEY_ID
AwsSecretAccessKey=YOUR_AWS_SECRET_ACCESS_KEY
EC2HostedRegion=YOUR_EC2_REGION
privaclaveComponentRoleArn=arn:aws:iam::014223972444:role/thirdpartys3access
```

*** privaclaveComponentRoleArn** role is fixed from Privaclave so no need to change that.

Step 3: Obtain AWS Access Key and Secret Access Key

1. **Sign in to the AWS Management Console:**
   - Open AWS Management Console.
   - Sign in with your AWS account credentials.
2. **Navigate to the IAM Console:**
   - In the AWS Management Console, type **IAM** in the search bar and select **IAM**.
3. **Select the User:**
   - In the IAM console, click on Users in the navigation pane.
   - Click on the name of the user for whom you want to create access keys.
4. **Create Access Keys:**
   - Click on the Security credentials tab.
   - Scroll down to the Access keys section.
   - Click on Create access key.
   - A dialog box will appear showing the **Access key ID and Secret access key**.
   - **Important:***Copy the Secret access key immediately as you will not be able to retrieve it later. Store it securely.*

Step 4: Run the Setup Script

✓ Navigate to the setup directory:

```bash
cd /home/user/privaclave_setup_0.0.1/
```

✓ `chmod +x privaclave_setup0.0.1.sh`

- ✓ `yum install dos2unix`
- ✓ `dos2unix setup.sh`

- ✓ Run the setup script

```bash
./setup.sh
```

This will install:

- **JDK 1.8.341** : verify installation using **'java –version'** command.
- **Tomcat Web Server 8.5.100** : It will be installed at **/opt/tomcat** folder.
- **After Successful installation Inbound security groups need to configure to allow port 8080 and your application will be available at http://<your instace public ip>:8080.**
- 

Step 5: Install MariaDB

- ✓ `chmod +x mariadbinstall.sh`
- ✓ `dos2unix mariadbinstall.sh`

- ✓ Run the MariaDB installation script:

```bash
./mariadbinstall.sh
```

Step 6: Deploy Privaclave Components

- ✓ Run the deployment command

```bash
java -jar PRIVACLAVE_AWS_COMPONENT_DEPLOYER_0.0.1.jar
```

This will perform the following operations :

- ❖ Create Lambda functions as per the defined configuration.
- ❖ Pull **AutoPilot<VERSION_ID>.ja**r from PRIVACLAVE_COMPONENTS_BUCKET and upload it to the Lambda function.
- ❖ Pull **CockpitEngine.war** and **CockpitAgent.war** from PRIVACLAVE_COMPONENTS_BUCKET and deploy them to the **/opt/tomcat/webapps** directory.
- ❖ Configure **Cockpit Engine DB** and related DB Configuration.