

# 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\\_0.0.1](#) zip file  
wget [https://github.com/privaclave-internal/privaclave-setup/raw/main/privaclave\\_setup\\_0.0.1.zip](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

Type : `vi AwsConfig.properties`

Press **Insert** button -> 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 technical team so no need to change that.
- \* Press **Escape** -> `:wq` (Write and Quit) and save the changes.

### Step 3: Obtain AWS Access Key and Secret Access Key

Sign in to the AWS Management Console:

- Open [AWS Management Console](#).
- Sign in with your AWS account credentials.

Navigate to the IAM Console:

In the AWS Management Console, type **IAM** in the search bar and select **IAM**.

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.

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/
```

- Run the setup script

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

This will install the followings

- **JDK 1.8.341** : verify installation using '**java -version**' command.
- **Tomcat Web Server 8.5.100** : It will be installed at **/opt/tomcat** folder.

## Step 5: Install MariaDB

- 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>.jar** 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.