Steps to install Privaclave Generic-K8s on AWS

1. **Prepare the target AWS account for installation**
   - Create the customer's installer role for Privaclave in the target Customer's account:
     - Assign Administrator access to it
   - Create a user with permissions only to assume the installation role
   - Configure the Trust Relationship Policy of the role to allow the user to assume it
   - Create a profile in the local machine with the AWS user's credentials and call it “privaclave"
   - Execute this command to use that profile:
     export AWS_PROFILE=privaclave
   - Create an S3 bucket for the Terraform state files with this name: "privaclave-statefiles-<customer's account_id>"

2. **Pull Privaclave’s images and push them to the target account’s ECR:**
   - Privaclave will grant READ access to the customer's AWS installer role to be able to pull images from all the required ECR repos of Privaclave’s account
   - Login into the Privaclave’s ECR to pull the images by using this command:
     - aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin 298884149928.dkr.ecr.us-east-1.amazonaws.com

   - Pull the required images by using these commands (replace <version> with the desired version’s tag):
     - docker pull 298884149928.dkr.ecr.us-east-1.amazonaws.com/classifier-docker-images/classifier_generic_k8s/master:***<version>***
     - docker pull 298884149928.dkr.ecr.us-east-1.amazonaws.com/classifier-docker-images/classifier_generic_k8s/worker:***<version>***
     - docker pull 298884149928.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_autopilot_service/autopilot_image:***<version>***
     - docker pull 298884149928.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_cockpit_service/cockpit_image:***<version>***
     - docker pull 298884149928.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_openresty_proxy_service/openresty:***<version>***
     - docker pull 298884149928.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_policy_handler_service/policy_handler_image:***<version>***

   - Login into the target’s account ECR to push the pulled images by using this command (replace <target’s account ID> with your target’s AWS account ID):
     - aws ecr get-login-password --region us-east-1 | docker login --username AWS --password-stdin <target’s account ID>.dkr.ecr.us-east-1.amazonaws.com

   - Rename the pulled images to push to the target account’s ECR (replace <target’s account ID> with your target’s AWS account ID and <version> with the desired version’s tag):

     - docker tag 298884149928.dkr.ecr.us-east-1.amazonaws.com/classifier-docker-images/classifier_generic_k8s/master:***<version> <target’s account ID>***.dkr.ecr.us-east-1.amazonaws.com/classifier-docker-images/classifier_generic_k8s/master:***<version>***

     - docker tag 298884149928.dkr.ecr.us-east-1.amazonaws.com/classifier-docker-images/classifier_generic_k8s/worker:***<version> <target’s account ID>***.dkr.ecr.us-east-1.amazonaws.com/classifier-docker-images/classifier_generic_k8s/worker:***<version>***

     - docker tag 298884149928.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_autopilot_service/autopilot_image:***<version> <target’s account ID>***.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_autopilot_service/autopilot_image:***<version>***

- docker tag 298884149928.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_cockpit_service/cockpit_image:***<version> <target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_cockpit_service/cockpit_image:***<version>***

- docker tag 298884149928.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_openresty_proxy_service/openresty:***<version> <target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_openresty_proxy_service/openresty:***<version>***

- docker tag 298884149928.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_policy_handler_service/policy_handler_image:***<version> <target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_policy_handler_service/policy_handler_image:***<version>***

- Push the pulled images to the target account's ECR (replace <target's account ID> with your target's AWS account ID and <version> with the desired version's tag):
  - docker push ***<target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/classifier-docker-images/classifier_generic_k8s/master:***<version>***
  - docker push ***<target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/classifier-docker-images/classifier_generic_k8s/worker:***<version>***
  - docker push ***<target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_autopilot_service/autopilot_image:***<version>***
  - docker push ***<target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_cockpit_service/cockpit_image:***<version>***
  - docker push ***<target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_openresty_proxy_service/openresty:***<version>***
  - docker push ***<target's account ID>***.dkr.ecr.us-east-1.amazonaws.com/policy-engine-and-autopilot-docker-images/generic_k8s_policy_handler_service/policy_handler_image:***<version>***

4. Grant permissions to the target account's services to pull the pushed images by adding this policy to the permissions of each ECR repo in the target account (replace <target's account ID> with your target's AWS account ID):

```
{
 "Version": "2008-10-17",
 "Statement": [
  {
   "Sid": "ECRImageRetrievalPolicyFromRoles",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::<target's account ID>:root"
   },
   "Action": [
    "ecr:BatchGetImage",
    "ecr:GetDownloadUrlForLayer"
   ],
   "Condition": {
    "StringLike": {
     "aws:PrincipalArn": "arn:aws:iam::<target's account ID>:role/*"
    }
   }
  }
 ]
}
```

3. Set variables with customer values

- Clone the privaclave-release repo
- Go to the "iac/generic-k8s/1-deployment_variables/principal-variables.tfvars" file and edit the indicated variables with the customer's values:

```
Version                 = "<desired version>"   # example: Version = "v2025.06.18.213652"
aws_region              = "us-east-1"     # Update with desired region
deploy_networking       = true
deploy_cluster          = true
domain_name             = "qa.privaclave.com"
create_monitoring       = false
ci_artifact_bucket.     = "privaclave-statefiles-<customer's account_id>"
```

- Go to the "./iac/generic-k8s/2-privaclave-base-infra/backend.tf" and "./iac/generic-k8s/2-privaclave-k8s-app/backend.tf" files and set the customer's Terraform state file bucket name (the one created above)

4. Install

- Open a terminal screen at the "iac/generic-k8s" of the release repo
- Execute the first installation script like this:
  sh install-infra.sh <arn of the customer's installer role>
- Follow the ./iac/generic-k8s/2-privaclave-base-infra/README.md file to join the worker nodes to the cluster and get the kubeconfig file to use with kubectl
- Execute the second installation script like this:
  sh install-k8s-app.sh <arn of the customer's installer role>

5. To destroy

- Open a terminal screen at the “iac/generic-k8s/3-privaclave-k8s-app” of the release repo
- Execute the following command to destroy the k8s app installation:

```
terraform destroy \
    -var-file="../1-deployment_variables/principal-variables.tfvars" \
    -var-file="../1-deployment_variables/privaclave-k8s-app.tfvars"
```

- Open a terminal screen at the “iac/generic-k8s/2-privaclave-base-infra" of the release repo
- Execute the following command to destroy the infra installation:

```
terraform destroy \
    -var-file="../1-deployment_variables/principal-variables.tfvars" \
    -var-file="../1-deployment_variables/privaclave-base-infra.tfvars"
```