i assume a local image repo is an onprem nexus server so to secure the connection between the jenkins in the vpc and the onprem nexus we use a site to site vpn connection which is encrypted

Corporate Data Center

Nexus Image Repository

Customer gateway

code is checked out of github by jenkins by passing through a nat gateway

GitHub

Region

Virtual Private Cloud

Internet gateway

Public Subnet

NAT gateway

Public Subnet

NAT gateway

VPN Gateway

route53 is used for several reasons:
1.provide a DNS for the alb which is part of the company domain so external users can access it by a logical name like panaya.com
2.provide an internal address for the database so that the jenkins build can access the database to build a new index.html. we use an alias record to point to a private NLB

Load Balancing Application Load Balancer

Amazon Route 53

Private Subnet

Load Balancing Network Load Balancer

ECS Cluster

Private Subnet

Nginx

Terraform

Private Subnet

Jenkins

Terraform

Mysql

upon a git webhook activation the script does the following:
1.checkout code
2.build the docker image without using the cached builder stage of nginx
3. tag and push to nexus ; save tag as jenkins variable
4.deploy ecs terrafrom file,provide the jenkings tag variable you created as a terrafrom variable for the image tag.this will make sure the latest version is deployed