

- 1) Jira/scrum planning
  - creation of multiple tickets with scrum boards, sprints, backlogs etc
  - integration with Slack to get notifications in slack .
  - integration with GitLab, github with the scrum and kanban boards .
  - setup tracking of whole project using jira.
- 2) Creation of multiple accounts using aws control tower and compliance,governance of accounts.
  - AWS Organisation setup with SCP'S
  - AWS control tower, landing zone setup .
  - applying multiple famous SCP and proactive, reactive controls for additional compliance,security.
  - Single Sign on setup
  - Cross-account roles
  - implementing Well architected framework practices.
  - extensive setup of own networking account, security,audit account and shared service account for better account and environment organisation.

Optional-

- Setup of transit gateway to connect multi account vpc's and services .
- terraform account factory setup
- automate creation of multi account with control tower and lamda fuction upto 50+ account with waf practises.

- 3) Setup of some prerequisites before deployment of project
  - Creating some base variables at gitlab group level ex-aws access keys,snyk tokens etc
  - Creation of base AMI'S using packer to distribute to multiple accounts,multiple regions.
  - Creation of Base -Dockerfile with all softwares dumped in.
  - buying base domain name and setup using route53, certifates setup using ACM .
  - creation of s3 buckets, dynamo db for executing terraform remote backend at deployment stages.

Optional –

- base vpc and networking thing defined as per network engineer.
- base ci/cd templates,aws templates etc

- 4) End to End DevSecOps CI Pipeline using Gitlab for openproject repo
  - Gitlab pipeline with components of security scanning and building docker files using some base images to reduce time of build.
  - Integration of Sonarcloud,synk,oswap,trivy for security scans .
  - applying good multi-branching strategy with main,dev,realise branches
  - usage of packager.io at realise braches to effectively realse to multiple linux distributions.
  - trigger pipeline script to change or update docker tags to the Kubernetes manifests.or even argo image updater can be used also.
  - integration with jira for effectively manage vulnerability.

→ Add DAST testing using OSWAP ZAP

Optional-

- Pull request preview option for better dev experience
- Single security/vulnerability dashboard to effectively manage vulnerabilities.
- monitoring the ci/cd pipelines and reduce time of building , optimise it.
- make script to automate update tags from base image.or use (task file ) to automate .
- add unit tests, integration tests, smoke tests for better testing .

5) Deployment of AWS Multi-region, Multi -ENV Infrastructure provisioning using terraform.

- Gitlab pipeline for infra creation using terraform to deploy into prod,staging environments with multi regions.
- Understanding infra that created using terraform .
- Setup of WAF,Route53,Cloudfront,global accelerator etc
- custom sub domain for staging env.
- Aurora based rds database for multi region support .

Optional-

- Configuration of backup with external third party provider or multi cloud strategy.
- implement and deploy into multi cloud strategy.

6) Provisioning EKS cluster with terraform

- Provisioning EKS cluster with terraform
- Adding alb controller configuration for using ingress.
- EBS CSI driver support for usage of pv as ebs volme .
- Custom domain setup with route53 ,ACM.
- Additonal addon's using terraform.
- Terraform remote backend using s3,dynamo db.
- replicate into multi-env, staging,prod etc
- setup of Kubernetes dashboard .

Optional-

- usage of teramate for better terraform management.
- provision using EKCTL.
- usage or setup of onpremises kops Kubernetes.

7) Continuous deployment using argocd.

- setup of argocd controller in Kubernetes as crd.
- Integrating the git repo with argo cd.
- deploying resources into multiple env(clusters) like staging,env .
- custom domains integrations with route53 for both staging,env environments.
- Setup of sealed secrets or hashicorp vault for secret management.

Optional – setup of cloud-native pg for db, k8sgpt for troubleshooting, k9 for good dashboard, trivy for manifest scanning

8) Monitoring and observability

- Infra level monitoring, alerting using cloudwatch and xrays
- configuring Prometheus and Grafana for Kubernetes monitoring of metrics with observability .
- ELK Stack configuration with heartbeats, filebeats etc
- Kernel level observability using ebpf ,otel and visualization using Grafana .