Project implementation

Tech Stack 👷

- Github
- Jenkins
- Sonarqube
- FTP
- Ansible
- App Centre
- Mongo DB
- Postgres DB
- IIS

Continuous Integration (CI) :cicd:

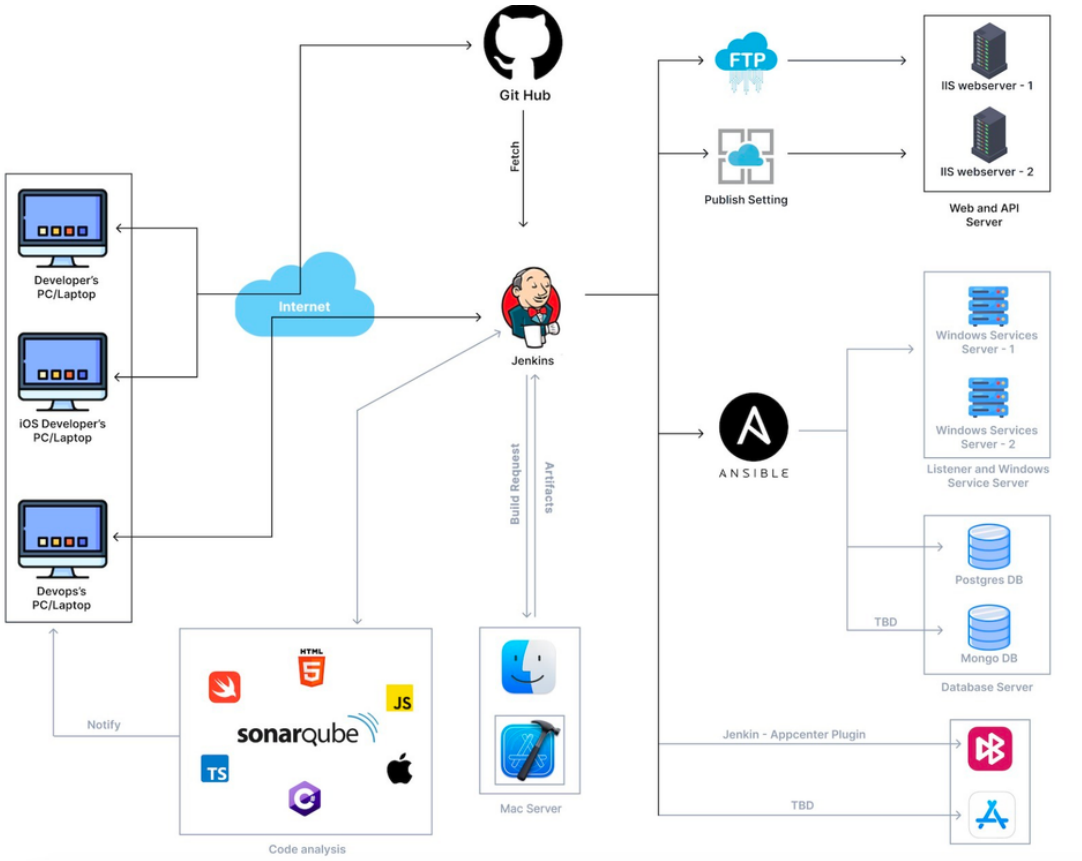
Continuous integration jobs automatically perform the following actions:

- Build the source code to check compilation errors.
- Execute tests when a pull request is created/updated. At present, Dotnet unit tests are executed.

Continuous Delivery (CD) :cicd:

Continuous Delivery (CD) immediately deploys source code to the server after all tests pass successfully. Developers can check their functions quickly and then assign the task to the QA team for review.

As the build executes on the build system, it not only minimizes the deployment downtime, but also reduces the load on the server. As a result, the QA activities, which are happening on the server, are impacted less



The CI/CD process in the previous diagram can be briefly described as follows

- GitHub hosts the Git repository
- For all commit branches, automatically:
  - Execute a standard code scan.
  - Execute a code compiling test.
  - Execute a static code scan With SonarQube
- All scan commits that pass are merged with the target branch
- New deployment is triggered by the deployment engineering team.
  - A deployment job deploys the new package to the target environment.
  - Database structure updates require a pause to take on new requests from the customer.
- The deployment process ends with an email/Slack/Teams notification, sent automatically by the server to the deployment engineering team
- Ios and android build and deploy on App Centre and we can Distribute Release via App Center to App Store or playstore
- Web and Api deploy into IIS Server with Jenkins pipeline
- For automation we use Ansible is used for To deploy th patches into DB and other services that is deployed on Web Server

✍️ Improvement Plan

- WAF monitors traffic at the application layer
- We protect our applications web requests transmitted over HTTP or HTTPS with WAF

- WAF has rules allow to inspect HTTP/S requests coming from both IPv6 and IPv4 addresses
- We have Configured Incident alert so If any critical issue Of Security send on Slack Channel

Web security

- Attack signatures are patterns that may indicate malicious traffic including request types anomalous server responses and known malicious IP addresses
- WE used WAF to rely predominantly on attack pattern databases that were less effective against new or unknown attacks
- involves analyzing the structure of an application, including the typical requests, URLs, values, and permitted data types
- analyzing the structure of an application, including the typical requests, URLs, values, and permitted data types. and AWS WAF to identify and block potentially malicious requests
- protects against distributed denial of service (DDoS) attacks With AWS WAF
- AWS Waf defence against some of the most common DDoS attacks including layer 7 attacks that can Managed WAFs screen the layer 7 traffic and feed data directly to cybersecurity experts who can identify malicious traffic trying to disrupt your services
- WAFs are deployed at the network edge, so WAF can provide a CDN to cache the website and improve its load time

Vulnerability management

- Perform Vulnerability Scan with snyk For Each PR
- Scan network-accessible systems by pinging them or sending them TCP/UDP packets with our internal vulnerability Tool that is build on python
- Identify open ports and services running on scanned systems

Infrastructure Security

- Implement zero-trust security with aws network
- Use multi-factor authentication to secure our account
- Avoid privileged accounts actions that can be taken on specific resources under specific conditions with IAM
- Enforce a strong password policy Do not use the same password for every site, application and service , Contain a mix of uppercase and lowercase letters, punctuation, numbers, and symbols. Contain at least 15 characters

Incident management plan (DATADOG)

- Automated alerts from network and host-based Intrusion Detection and Prevention System (IDPSs), antivirus software, or log analysers
- recognising and reporting events quickly and accurately to ensure that every system issue is caught and sent to the appropriate responders
- identifying the severity of an incident to determine next steps, including how many responders need to be brought in, who needs to be notified, and how soon a solution needs to be provided
- working with teams across the organisation to contain the damage, then sifting through system data—including metrics, logs, and metadata—to find the root cause and troubleshoot potential fixes
- studying the incident to create useful postmortem documentation and take steps to prevent future incidents

Data Protection

- centralised management console for data encryption and encryption key policies and configurations
- Encryption at the file, database and application levels for cloud data
- Role and group-based access controls and audit logging to help address compliance
- Automated key lifecycle processes for cloud encryption keys

Security Shield

- Static threshold DDoS protection of web security
- deterministic packet filtering and priority-based traffic shaping to automatically mitigate basic network layer attacks
- Tailored detection based on application traffic patterns
- Health-based detection
- Automatic application layer DDoS mitigation
- Visibility and attack notification
- Centralized protection management

User Permission Review

- User Need To Enable MFA Use Aws Console
- All the department divided into groups and each department has required access to perform the action
- Password must be 7 characters minimum max30, should have one special character, 1 uppercase, 1lowercase, 1numeric and no white spaces

Identity Management, Password Settings and Security for Staff

- Password must be 7 characters minimum max30, should have one special character, 1 uppercase, 1lowercase, 1numeric and no white spaces
- JWT Authentication is used
- Password is hashed and stored in DynamoDb
- User will be logged out after 1 hour of inactivity

Authorization policy

- Identity-based policies
- Identity-based policies are JSON permissions policy documents that control what actions an identity users, groups of users, and roles can perform
- Resource-based policies for principal permission to perform specific actions on that resource and defines under what conditions this applies

Availability, Business Continuity and Disaster Recovery

- we use canary deployment for eks to reduce the downtime
- Automates the entire release life cycle
- Manages incompatibilities between API versions and database schema changes, supporting a good testing strategy
- Reduces risk of negative outcomes impacting a large percentage of user base when releasing a new functionality to users
- our platform support zero downtime

Backup and Recovery plan for Data and Server

- Data is stored in a S3 bucket that is owned and managed by Amazon RDS service
- We use highly available Multi-AZ deployment so if anything will happened in any region our server work from another region
- Log backups run as frequently as every 5 minutes depending on your workload.

Mobile Application Security (Done)

- Use code obfuscation
- Secured Api with JWT token
- Jailbreak or rooted device detection
- Ensure secure network connection
- Use only required permission

- Secure user data in local memory
- Upto date the dependency plugins