RELEASE PIPELINE AZURE

Taulant Racaj

AGENDA

- Software and Tools
- High Level Infrastructure Diagram
- Infrastructure Resources
- Kubernetes Scaling Strategy
- Branching Strategy
  - Local Development
- Release Flow
  - Best Practices for Building Software Artifacts

- Quality Gates
- Security
  - Infrastructure Security
  - Microsoft Defender for cloud
- DEMO

SOFTWARE AND TOOLS

GitHub

Bash

Azure (CLI)

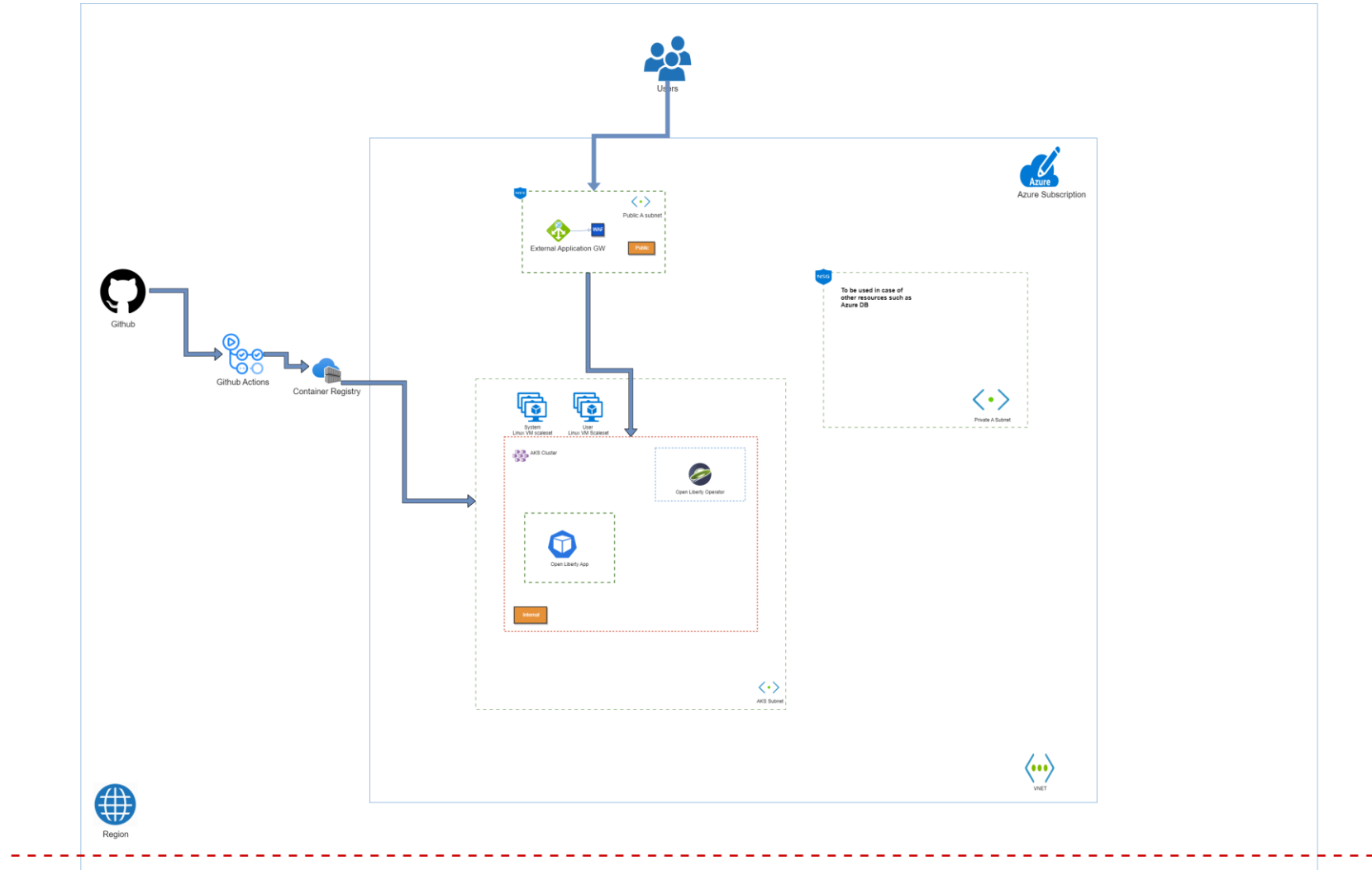Open Liberty

Chocolatey

Kubernetes (CLI)

VS Code

Maven

Terraform

PowerShell

syft

Docker

docker

grype

HELM

sonarqube

HIGH LEVEL INFRASTRUCTURE DIAGRAM

File can be found under -> 1.HighLevel_Infra_Diagram.png file on GitHub
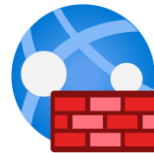
RESOURCES

AKS

Application GW

Vnet

Load Balancer

WAF Policy

Log Analytics
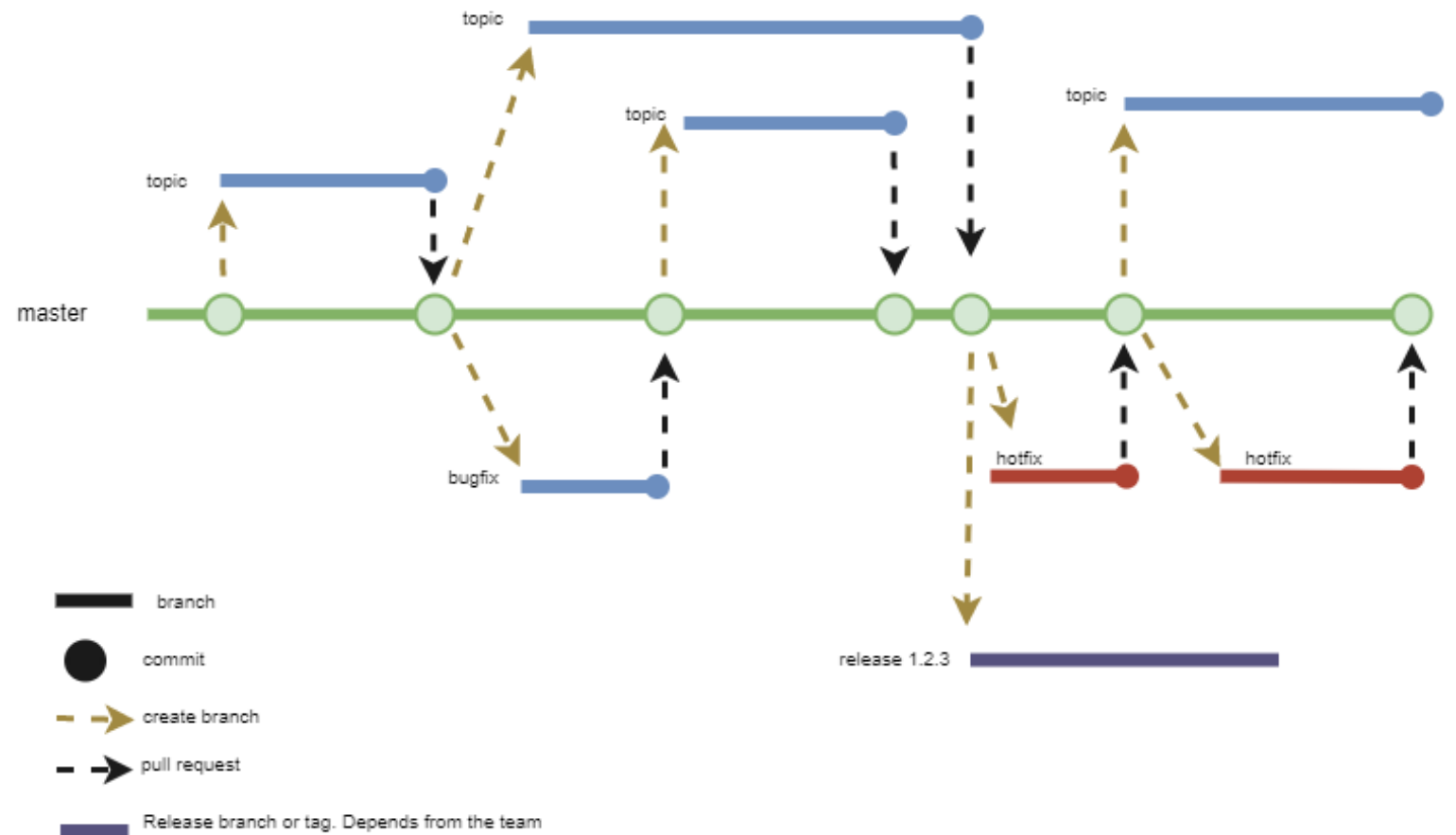
Azure CR

VM Scale set

Key Vault

KUBERNETES SCALING STRATEGY

- Node Autoscale

- Horizontal Pod Autoscaler (HPA)

- Cluster Autoscaler

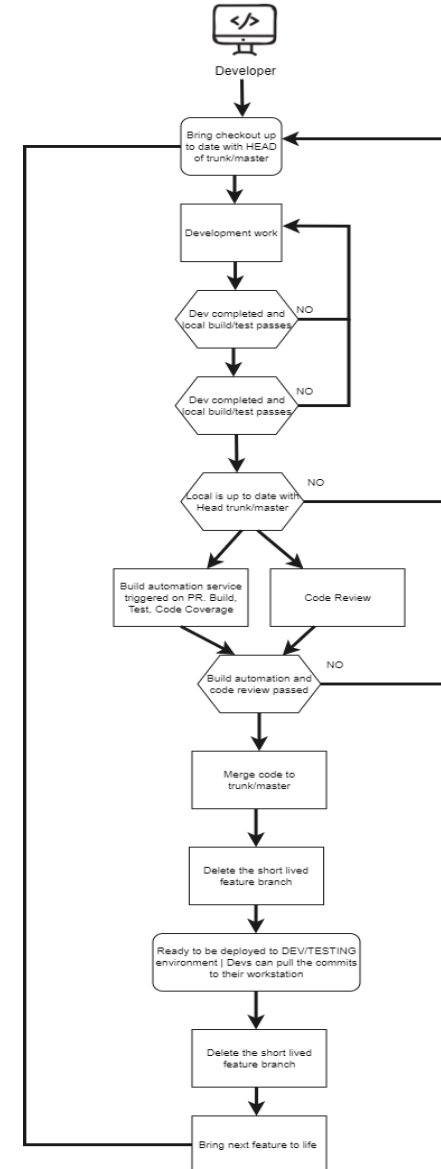- Documentation under -> **Kubernetes scaling strategy.docx file on GitHub**

BRANCHING STRATEGY

High Level Trunk Based Development Strategy

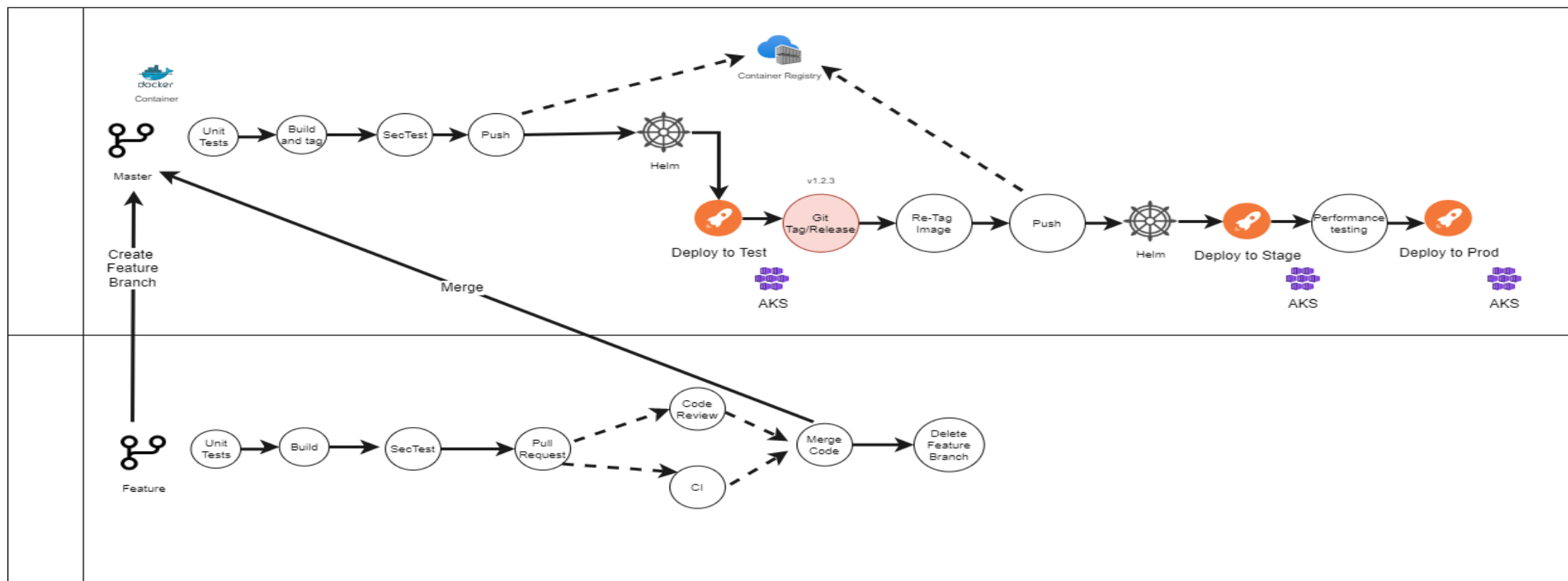File can be found under -> **Branching Strategy.docx file on GitHub**

LOCAL DEVELOPMENT

File can be found under -> 3.LocalDevelopment.drawio.png file on GitHub

RELEASE FLOW

File can be found under -> 4.CI_CD.drawio.png file on GitHub

Conditions		
Metric	Operator	Value
Coverage	->	50-80 %
Duplicated Lines	<	5-10%
Blocker Issues	=	0
Critical Issues	<	5
Cyclomatic Complexity	<	15
Unit test Errors	=	0
Unit test Failures	=	0

QUALITY GATES

SECURITY

- Docker Security - https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html

- Static application Security testing- Analyze the code without executing it https://owasp.org/www-project-top-ten/ Find Vulnerable (e.g. SQL injection) dependencies - Integrate in early stages

- Dynamic application security - Integrate in later stages when application is running on an environment (XSS, SQL injection) - OWASP ZAP tool, HCL App Scan

- Interactive application security testing - Combination of SAST and DAST

- Runtime application self-protection (RASP) - This requires development , in JAVA Instrumentation Interface can be used https://docs.oracle.com/javase/7/docs/api/java/lang/instrument/Instrumentation.html. Tools such as Imperva can help to avoid development.

- Dependency Scanners - Software Composition Analysis (SCA) Tools such as Dependency Track can help here. (SBOM) - Dependency Track

INFRASTRUCTURE SECURITY AKS

WAF	Node Storage • Azure Data Disk – encrypted	Kubernetes Network Policy
Network Security	Node Security • Security patches	Azure Security Benchmark
Cluster Security (API Server)	Pod Management Security (MI)	
Key Vault	Kubernetes Secrets	
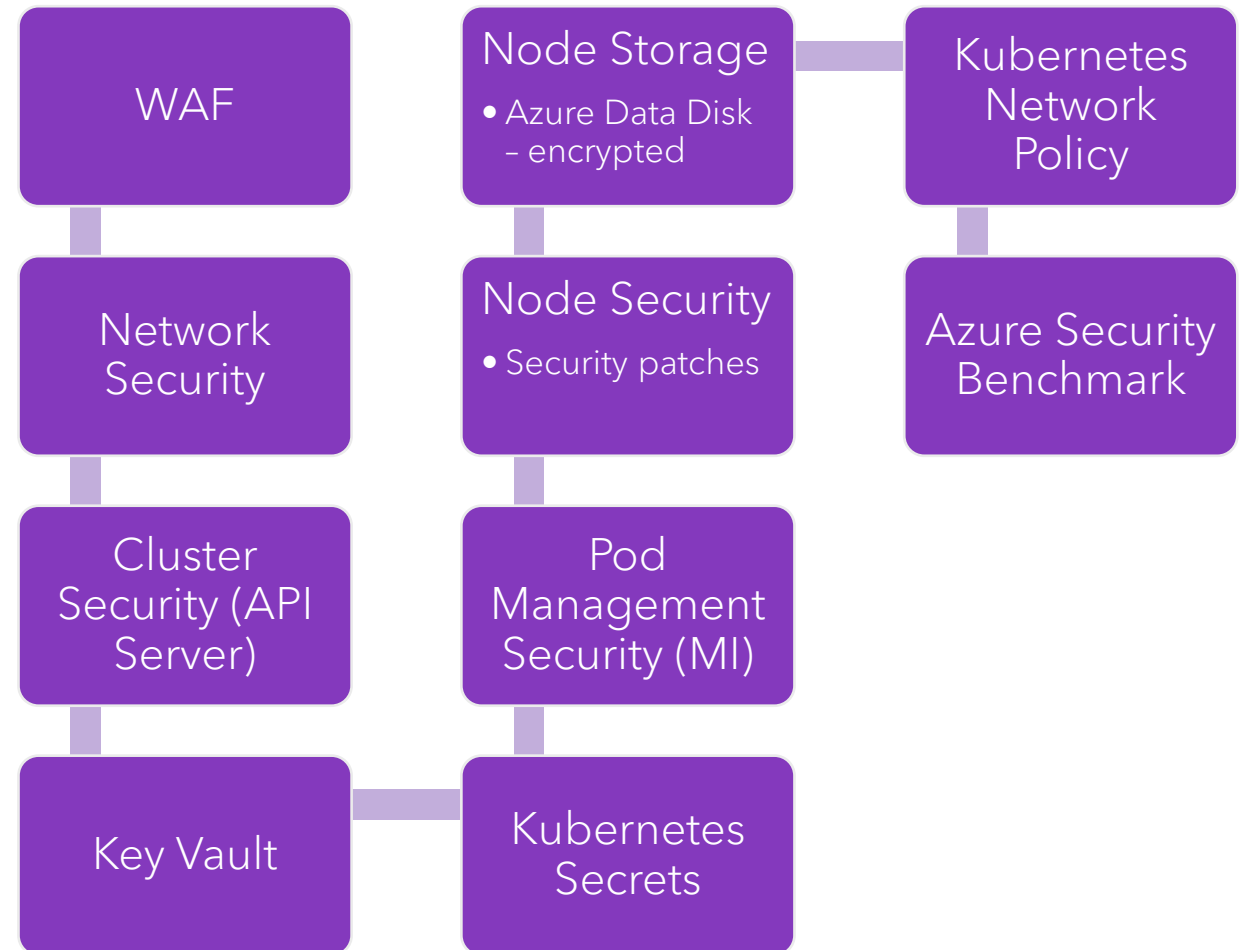
Documentation under -> **AKS Security.docx file on GitHub**

MICROSOFT DEFENDER FOR CLOUD

- Microsoft Defender for Cloud is **cloud-native solution for securing containers,** and it protects almost all significant container resource types.

    - Microsoft Defender for Containers
        - Environment hardening
        - Vulnerability assessment
        - Run-time threat protection for nodes and clusters

    https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction

DEMO

- Terraform Scripts
- Infra Pipeline
- Open Liberty Demo build and deployment