

# 第五章 技术要求

## 一、项目概述

随着业务应用向微服务架构转型，传统开发运维模式难以满足快速迭代、弹性伸缩和资源集约化的需求。同时，当前异构计算资源（X86、ARM、C86 等）分散管理，算力利用率低，与开发流程脱节，导致应用部署复杂、运维效率低下。为提升微服务应用的开发效率和运维质量，亟需构建一套统一的异构算力纳管平台和标准化的微服务开发平台，实现算力资源的统一调度与精细化管控，并打通从开发到运维的全流程自动化管理，形成开发、部署、运维一体化的闭环能力。

本项目拟基于云原生技术体系，建设微服务开发平台和异构分布式算力统一纳管系统两大核心平台。微服务开发平台提供覆盖项目管理、代码托管、持续集成、持续部署、制品管理和效能度量的一站式工具链；异构分布式算力统一纳管系统采用 Kubernetes 为核心编排引擎，实现对 X86、C86、ARM 等多架构异构节点的统一纳管与调度，构建异构算力资源池，全面适配国产操作系统。两大平台深度协同，实现开发流程与资源管理的无缝对接，形成“开发 部署 运维 优化”的闭环能力，为后续业务系统提供高效、稳定、可扩展的研发运维支撑，降低基础设施成本，提升资源利用率。

## 二、建设要求

### （一）项目目标

本项目拟建设一套符合 DevOps 理念的微服务开发平台和一套异构分布式算力统一纳管系统，实现以下目标：

提供从需求提出到上线运行的全流程闭环管理，支持敏捷项目管理、代码协作、自动化构建与测试、自动化部署、制品管理及效能度量；

支持多语言微服务开发（Java、Python、Go 等），适配 X86、ARM 等多架构算力环境，实现异构部署；

实现异构算力资源的统一纳管与调度，构建异构算力资源池，提升资源利用率；

与底层容器云平台（异构分布式算力统一纳管系统）深度协同，打通开发流程与资源调度，实现资源的按需分配和自动化运维；

建立研发效能度量体系，通过数据驱动持续优化研发流程，提升团队交付效率和质量。

## （二）主要建设内容（主要功能模块）

| 序号 | 系统模块    | 主要功能    | 简要说明                                                                                                                          |
|----|---------|---------|-------------------------------------------------------------------------------------------------------------------------------|
| 1  | 微服务开发平台 | 需求与项目管理 | 支持瀑布模式、敏捷模式的项目管理方式。                                                                                                           |
|    |         |         | 支持项目概览，展示项目实时信息，如项目概况、项目动态、项目进度等信息。                                                                                           |
|    |         |         | 支持多层需求管理模型，支持需求字段属性自定义，支持需求类型开关设置启用状态。                                                                                        |
|    |         |         | 支持需求的多维度创建，包括通过需求列表、版本需求、迭代需求维度创建需求；支持需求的导入和导出。                                                                               |
|    |         |         | 支持需求关联子需求、关联缺陷、关联测试用例；支持需求评论、需求日志功能。                                                                                          |
|    |         |         | 支持甘特图展示，可以通过甘特图查看项目的计划。                                                                                                       |
|    |         |         | 支持敏捷看板展示，支持版本视图和迭代视图，支持默认看板和用户看板；支持看板设置，可以定义看板的列及列展示的状态。                                                                      |
|    |         |         | #支持需求关联代码分支，并以需求维度提交测试单流转给测试人员进行协同。（提供含有需求或代码分支或发起提测关键字的截图）                                                                   |
|    |         |         | #支持自定义项目工作流，如需求工作流、测试单流、分支流程、缺陷流程等，可设置流程的触发器、权限、条件、动作、后处理等内容。<br>（提供含有工作流配置或工作流模板：需求/测试/分支/缺陷等流程或流程转换的触发器/权限/条件/动作/后处理关键字的截图） |
|    |         | 代码管理与协作 | 支持集成 gitlab、svn 代码管理，通过平台可完成代码库的相关操作。                                                                                         |

| 序号 | 系统模块 | 主要功能     | 简要说明                                                                                                                              |
|----|------|----------|-----------------------------------------------------------------------------------------------------------------------------------|
|    |      |          | #支持基于需求创建分支、合并分支、合并审批等操作。（提供含有需求或创建分支或合并审批关键字的截图）                                                                                 |
|    |      |          | 支持在线编辑代码、提交代码、分支对比、提交及合并日志等常规操作。                                                                                                  |
|    |      |          | 支持代码库权限的分配，支持代码库的操作审计。                                                                                                            |
|    |      |          | 支持代码分析和统计，可查看代码量统计、代码趋势、代码提交统计等。                                                                                                  |
|    |      |          | #支持自定义分支策略规范流程，通过流程驱动分支自动化操作、流水线执行；支持分支流程设置卡口，如合并之前检查流水线状态。（提供含有分支策略流程或流水线状态检查关键字的截图）                                             |
|    |      | 自动化构建与测试 | #支持可视化编排流水线，支持应用级、服务级流水线，支持并行/串行处理、设置各种流水线阶段、设置静态参数/动态参数、支持VM/Docker/K8S多模。（提供含有流水线可视化编排或阶段配置或任务配置或静态/动态参数示例的截图，提供支持虚拟机/K8S多模的截图） |
|    |      |          | #支持集成 Jenkins。（提供含有 Jenkins 或任务配置或构建关键字的截图）                                                                                       |
|    |      |          | 支持流水线的复制、克隆、自定义阶段、任务以及参数。                                                                                                         |
|    |      |          | 支持人工审批流水线执行情况，包括或签或者会签。                                                                                                           |
|    |      |          | #支持自定义门禁阈值，如代码扫描、安全检测等，不满足设定阈值的情况下自动停止流水线执行，并触发通知。（提供含有门禁配置或质量门禁或扫描或阈值或流水线关键字的截图）                                                 |
|    |      |          | 支持页面设置工具脚本、静态参数、执行参数等。                                                                                                            |
|    |      |          | 支持流水线权限控制，对单个用户可查看权限、                                                                                                             |
|    |      |          |                                                                                                                                   |
|    |      |          |                                                                                                                                   |
|    |      |          |                                                                                                                                   |
|    |      |          |                                                                                                                                   |
|    |      |          |                                                                                                                                   |
|    |      |          |                                                                                                                                   |

| 序号 | 系统模块 | 主要功能      | 简要说明                                                                                           |
|----|------|-----------|------------------------------------------------------------------------------------------------|
|    |      |           | 可编辑以及运行权限的统一管理。                                                                                |
|    |      |           | 支持测试用例管理，支持用例分组展示；支持测试用例导入导出、批量操作和关联需求功能。                                                      |
|    |      |           | #支持提测单管理，提测单信息包含提测需求、提测执行的构建流水线等关联信息，通过提测单可以追溯提测的需求、代码、流水线、制品和质量等信息。（提供含有提测单或提测需求或构建流水线关键字的截图） |
|    |      |           | #支持提测版本依赖各服务版本的管理，支持图谱和列表展示版本依赖关系。（提供含有提测单或版本图谱或图谱视图或列表视图关键字的截图）                               |
|    |      |           | 支持通过提测版本发起发布申请。                                                                                |
|    |      | 自动化部署     | #支持容器/非容器应用统一发布。（提供含有容器部署或虚拟机部署关键字的截图）                                                         |
|    |      |           | #支持软件发布流程管理，发布流程支持平台审批或集成第三方系统审批，支持制品晋级操作。（提供含有发布流程或审批或制品晋级关键字的截图）                             |
|    |      |           | 支持部署模板管理，可通过部署模板快速定义部署过程脚本；支持设置部署超时、失败跳过、失败重试部署机制。                                             |
|    |      |           | 支持部署单元配置，每个部署单元关联机器范围和配置文件，支持按部署单元进行部署。                                                        |
|    |      |           | 支持部署记录查看和部署；支持部署日志查看。                                                                          |
|    |      |           | 支持容器应用的状态同步、健康检查、异常提醒。                                                                         |
|    |      |           | 支持部署脚本定义，支持通过部署模板或自定义的方式创建部署脚本。                                                                |
|    |      | 制品管理与版本追溯 | 支持在仓库制品维度，在线查看是否存在安全漏洞以及在线报告。                                                                  |
|    |      |           | 提供制品、第三方依赖的安全扫描能力，并对安全漏洞支持平台级别、项目级别等邮件提醒。                                                      |
|    |      |           | #支持制品在同一节点或不同节点之间晋级，支                                                                          |

| 序号 | 系统模块          | 主要功能     | 简要说明                                                                                                                                                                                                                                |
|----|---------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |               |          | 持晋级策略配置。（提供含有制品库或制品晋级或晋级策略关键字的截图）                                                                                                                                                                                                   |
|    |               |          | 支持设置高危、中危险、黑名单设置阻断下载，支持白名单设置并支持白名单放行。                                                                                                                                                                                               |
|    |               |          | 支持漏洞库私有化部署与持久化，支持在线更新或者人工同步。                                                                                                                                                                                                        |
|    |               |          | 支持对接组件安全工具，实现组织级安全策略下发与实施。                                                                                                                                                                                                          |
|    |               | 效能度量与可视化 | 支持通过版本进度、迭代进度、工作项燃尽图等展示当前项目的进度。                                                                                                                                                                                                     |
|    |               |          | 支持通过缺陷的级别、解决情况、占比等查看当前版本的质量概况。                                                                                                                                                                                                      |
|    |               |          | 支持展示项目组成员以及人员、角色的工作项分配概况。                                                                                                                                                                                                           |
|    |               |          | 支持通过需求吞吐量和流水线执行趋势展示工作进行效率。                                                                                                                                                                                                          |
|    |               | 平台协同能力   | 支持与底层异构算力统一纳管系统深度联动，实现开发流程与资源管理的无缝对接，自动化部署可直接调用容器云资源，监控数据互通共享，形成闭环优化。                                                                                                                                                               |
|    |               |          |                                                                                                                                                                                                                                     |
| 2  | 异构分布式算力统一纳管系统 | 异构节点纳管   | #支持 X86、C86、ARM 等异构计算节点的统一纳管，通过 Kubernetes 节点亲和性、污点与容忍等机制实现资源的灵活调度。（提供含有亲和调度/反亲和到底或污点或容忍度关键字的截图）                                                                                                                                    |
|    |               |          | #支持集群、节点、分区、实例（Pod）、容器的交互式列表展示与资源监控，深度监控集群五大核心组件性能指标，支持 Web 端 kubectl 终端、分级 Kubeconfig 权限管理、组件按需安装、事件持久化存储及操作历史追溯，所有关键信息与指标通过可视化呈现，实现集群一体化、精细化运维管控。（提供含有集群或节点或分区或 API Server 或 controller 或 scheduler 或 ETCD 或 Ingress 或 kubectl 或终 |

| 序号 | 系统模块    | 主要功能 | 简要说明                                                                                                                                  |
|----|---------|------|---------------------------------------------------------------------------------------------------------------------------------------|
|    |         |      | 端或 kubeconfig 关键字的截图)                                                                                                                 |
|    |         |      | #支持灵活的分区全生命周期管理能力,支持共享和独享两种分区模式且可动态调整隔离策略。分区的创建、查询、编辑、删除及节点迁入迁出操作,支持配置 CPU/内存等资源超分配比例以提升利用率。(提供含有分区管理或独享分区或共享分区或超配关键字的截图)             |
|    |         |      | 支持灵活的节点污点管理功能,允许管理员为单个或多个节点设置污点,通过键值对和效果标记(如 NoSchedule、PreferNoSchedule 或 NoExecute)精准控制 Pod 调度策略,有效实现节点隔离或专用节点管理,所有污点配置实时生效并支持批量操作。 |
|    | 容器镜像管理  |      | 支持企业级镜像全生命周期管理能力,支持通过可视化界面将容器镜像安全高效地上传至 Harbor、Registry 等仓库并同步至目标集群。                                                                  |
|    |         |      | #支持镜像标识与标签管理、公共/租户私有镜像隔离存储与访问控制、运行容器镜像捕获生成快照、同类型仓库间镜像同步、手动/策略化镜像归档与检索。(提供含有公共镜像目录或租户公共镜像目录或自定义镜像目录或镜像捕获或镜像同步或归档关键字的截图)                |
|    |         |      | #支持完善的镜像保护与清理机制,支持对关键镜像版本单/批量锁定(禁止覆盖删除)、租户级自定义时间/版本数量维度的镜像回收策略、非锁定镜像版本批量清理。(提供含有批量锁定/批量解锁或清理或回收关键字的截图)                                |
|    | 网络与存储适配 |      | 支持 underlay、overlay 网络方案,overlay 网络支持直接路由模式,兼容 IPv4/IPv6 双栈模式,支持跨主机容器互联及容器与外部非 NATIP 直通;支持主机网络模式及集群外部直接访问 PodIP。                      |

| 序号 | 系统模块 | 主要功能 | 简要说明                                                                                                                                                                              |
|----|------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |      |      | #支持租户自行可视化设置 Pod 的入网出网规则配置，配置维度按应用、服务、Pod、命名空间、IP 地址段等。（提供含有入网规则/出网规则或 IP 段或命名空间选择器或 Pod 选择器或应用或服务关键字的截图）                                                                         |
|    |      |      | 支持可视化的 IP 资源管理功能，支持网络创建、IP 地址/地址段分配及使用情况查询，同时具备服务 IP 预约、固定 IP 绑定能力，并支持主机网络模式和集群外部直接访问 PodIP 等高级网络特性。                                                                              |
|    |      |      | 支持在 overlay 网络模式下提供 EgressIP 功能，可为 Namespace 或 Workload 设置统一出站 IP，同时提供固定 IP 绑定能力，确保关键业务 Pod 的 IP 地址持久化，增强网络访问的可控性和可追溯性。                                                           |
|    |      |      | # 支持创建 ClusterIP 、 NodePort 、 LoadBalancer 三种类型的 Service，可配置端口映射、协议类型等基础参数并添加自定义标签，满足不同场景的内部服务暴露与分类管理需求。（提供含有 ClusterIP 或 NodePort 或 LoadBalancer 或 headless 或端口或 TCP/UDP 关键字的截图） |
|    |      |      | #支持 HTTP/HTTPS、TCP/UDP 多协议负载均衡配置与 EWMA 智能流量调度算法选择，能下载 Ingress 配置 YAML 文件用于备份迁移。（提供含有 http 或 https（或 TLS）或 TCP 或 UDP 或 EWMA 均衡算法关键字的截图）                                            |
|    |      |      | #支持基于权重比例的流量分发、基于请求头和 Cookie 的灰度路由规则，可组合多种策略适配复杂发布场景，实现多版本服务并行运行与流量灵活切换。（提供含有权重或 Header 或 Cookie 关键字的截图）                                                                          |
|    |      |      | 支持 StorageClass 可视化全生命周期管理能力，支持管理员通过图形界面完成 SC 的创建、                                                                                                                                |

| 序号 | 系统模块   | 主要功能 | 简要说明                                                                                                                                                    |
|----|--------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |        |      | Provisioner 及参数配置、YAML 文件下载、删除等操作。兼容 NFS、Ceph-rbd、CephFS、Carina 本地存储等多种存储类型，并可设置 Retain/Delete/Recycle 回收策略。                                            |
|    |        |      | 支持 PV 可视化全生命周期管理能力，支持管理员和租户通过图形化界面完成 PV 的创建、配置、YAML 文件下载及日常管理，可删除 release 或 available 状态的闲置 PV，还能一键克隆 available 状态的 PV 以实现存储资源快速复用。                     |
|    |        |      | 支持 PVC 可视化全生命周期管理能力，可以在线扩容存储容量、设置磁盘配额限制，以及快照创建、存储卷克隆、快照恢复等全周期数据保护操作。                                                                                    |
|    |        |      | #支持同时挂载多个 NAS 存储系统，管理员可执行存储卷挂载/卸载操作，并为不同租户分配专属 NAS 资源配额。租户可自主管理存储卷的创建、删除、查看及共享，服务发布时可直接选用 NAS 存储数据，平台会实时监控存储使用情况，在容量达到阈值时自动触发告警。（提供含有 NAS 或挂载/卸载关键字的截图） |
|    | 容器应用管理 |      | #支持以层级树形式展示租户下的所有应用及其下属服务，支持展开/折叠节点，直观呈现应用与服务的归属关系。（提供含有应用中心或应用名称或服务管理或服务名称关键字的截图）                                                                      |
|    |        |      | #支持应用的创建、资源配额编辑、单/批量删除、服务发布、任务创建等基础操作。（提供含有新增或资源限额或批量删除或发布服务或发布任务关键字的截图）                                                                                |
|    |        |      | 支持批量版本变更、应用配置备份为 YAML 模板跨集群复用、临时屏蔽非关键告警等便捷能力。                                                                                                           |
|    |        |      | #支持多集群应用资源拓扑可视化管理能力，支持按应用部署的集群维度自动构建并展示应用                                                                                                               |
|    |        |      |                                                                                                                                                         |
|    |        |      |                                                                                                                                                         |
|    |        |      |                                                                                                                                                         |
|    |        |      |                                                                                                                                                         |

| 序号 | 系统模块 | 主要功能 | 简要说明                                                                                                                                                                                                                                                                                                     |
|----|------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |      |      | 内 Service、Secret、ConfigMap、Job、CronJob、Ingress 等核心资源的拓扑关系图，直观呈现资源间的依赖与关联关系。（提供含有资源拓扑或资源列表或服务或 secret 或 configmap 或 cronjob 或 job 或 service 或 ingress 关键字的截图）                                                                                                                                             |
|    |      |      | 支持通过服务树结构或列表查看服务详情，涵盖基本信息、网络监控、PVC 监控和实例状态，可执行横向和纵向弹性伸缩、版本变更、升级回滚、高级配置、容器启停等全流程运维操作。                                                                                                                                                                                                                     |
|    |      |      | #支持容器驱逐、捕获运行中容器生成自定义镜像、通过 Web 终端访问容器命令行、Debug 等运维操作，可查看容器标准输出日志，实时掌握应用运行状态。（提供含有驱逐或镜像捕获或终端或 Debug 或启动日志关键字的截图）                                                                                                                                                                                           |
|    |      | 运维监控 | #支持多类监控对象与指标实现全面告警，包括基础设施维度（节点、主机、PV、PVC 等，监控 CPU、内存、磁盘、网络及主机存活状态）、K8S 核心组件维度（APIServer、Controller、Ingress，监控运行状态）、工作负载维度（Deployment 副本数、Pod 驱逐/重启/异常等专项指标）、数据库维度（MySQL 连接数、慢查询数量）以及日志维度（基于关键字等匹配规则。（提供含有主机或 deployment 或 statefulset 或 pod 或 pv 或 pvc 或 APIServer 或 Controller 或 Ingress 或日志关键字的告警策略截图） |
|    |      |      | 支持告警触发与恢复双重通知机制，集成邮件、短信、站内信、微信、钉钉及第三方 Webhook 接口等多种通知渠道。                                                                                                                                                                                                                                                 |
|    |      |      | 支持按集群、服务、实例、时间范围及关键字的多维度搜索功能；支持以表格或窗口形式查看日志信息，并可进一步查看单条日志的详细内容，便于快速定位问题和分析应用运行状态。                                                                                                                                                                                                                        |

| 序号 | 系统模块 | 主要功能 | 简要说明                                                                                                                                                                                                        |
|----|------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |      |      | 支持实时查询容器启动日志，可自定义日志窗口展示行数、文件大小限制及查询起始时间，精准筛选目标时段日志内容。                                                                                                                                                       |
|    |      |      | 支持租户全生命周期管理与跨集群资源管控能力，支持平台管理员通过可视化界面进行租户的创建、查询、编辑、删除等操作，所有变更实时生效且记录操作日志，保障管理的安全性与可追溯性。可查看分配的集群分区清单、资源配额使用情况、超配状态及网络流量统计等详情。平台管理员可全局查看所有租户的应用、服务及实例列表，租户管理员仅能查看所属租户资源，且均支持按租户名、集群名等维度快速筛选查询，实现租户资源的多维度可视化管控。 |
|    |      |      | #支持精细化的租户资源配额全维度管理能力，支持跨多个集群为租户统一配置 CPU、内存、存储等资源配额，允许基于分区设置大于 1 倍比例的资源超分配，算力集群可按总资源比例或自定义方案分配配额，且所有配额支持动态调整。（提供含有资源配额或 CPU 或内存或实例或存储或超配比关键字的截图）                                                             |
|    |      |      | 支持多维度智能化报表，自动采集集群、分区、节点、租户、告警、审计、应用七大维度的核心数据，涵盖各维度的基础状态、资源利用率（平均值、峰值、谷值）、业务运行特征及安全审计信息等内容，为报表生成提供完整数据支撑。                                                                                                    |
|    |      | 安全合规 | 支持自动记录用户在平台内的所有关键操作，完整捕获操作时间、执行用户、目标资源、操作类型及参数变更等详情                                                                                                                                                         |
|    |      |      | #支持对容器集群提供安全配置、权限配置、漏洞多维度安全检测，自动生成可视化风险评估报告。每份报告均附带针对性修复建议，支持单个或批量 Excel 格式导出。（提供含有                                                                                                                         |

| 序号 | 系统模块 | 主要功能 | 简要说明                                                                                   |
|----|------|------|----------------------------------------------------------------------------------------|
|    |      |      | K8s-CIS 扫描或 K8s 权限扫描或 K8s 漏洞扫描或扫描报告或修复建议或批量下载关键字的截图)                                   |
|    |      |      | 支持对容器镜像进行深度安全检测（包括 CVE 漏洞、敏感信息泄露、恶意软件等风险）。扫描结果自动标注漏洞等级。                                |
|    |      |      | #支持用户安全参数可视化配置,满足密码安全策略、会话管理策略、用户/密码锁定策略的配置和修改。（提供含有密码安全策略或会话管理策略或账户过期时间或密码过期时间关键字的截图) |

### （三）业务需求

微服务开发平台与异构分布式算力统一纳管系统协同，旨在满足以下业务场景需求：

1. 多团队协同开发：支持不同业务域团队并行开发，通过敏捷项目管理、代码分支隔离和权限控制，保障多人协作的规范性和安全性。
2. 快速迭代与持续交付：通过自动化流水线实现代码提交后自动构建、测试、部署，缩短交付周期，支撑业务快速响应变化。
3. 异构环境适配：平台需支持 X86、ARM 等多种算力架构，确保微服务能够在不同硬件环境下稳定运行，满足未来国产化适配要求。
4. 资源弹性利用：与底层容器云平台协同，实现按需申请开发、测试、生产环境资源，提升资源利用率，降低运维成本。
5. 效能改进：通过数据度量，发现研发流程中的瓶颈，优化开发测试策略，持续提升团队交付能力和软件质量。

### （四）功能需求

系统支持实时过滤数据，快速定位目标服务。

## 1. 微服务开发平台功能需求

### (1). 需求与项目管理

支持瀑布模式、敏捷模式的项目管理方式。

支持项目概览，展示项目实时信息，如项目概况、项目动态、项目进度等信息。

支持多层需求管理模型，支持需求字段属性自定义，支持需求类型开关设置启用状态。

支持需求的多维度创建，包括通过需求列表、版本需求、迭代需求维度创建需求；支持需求的导入和导出。

支持需求关联子需求、关联缺陷、关联测试用例；支持需求评论、需求日志功能。

支持甘特图展示，可以通过甘特图查看项目的计划。

支持敏捷看板展示，支持版本视图和迭代视图，支持默认看板和用户看板；支持看板设置，可以定义看板的列及列展示的状态。

支持需求关联代码分支，并以需求维度提交测试单流转给测试人员进行协同，提交测试过程支持自动分支代码合并、打 tag、执行构建流水线。

支持自定义项目工作流，如需求工作流、测试单流、分支流程、缺陷流程等，可设置流程的条件、触发器、权限、条件、后处理等内容。

### (2). 代码管理与协作

支持集成 gitlab、svn 代码管理，通过平台可完成代码库的相关操作。

支持基于需求创建分支、合并分支、合并审批等操作，支持代码分支规范的灵活配置，用户通过平台可按规范执行分支操作。

支持在线编辑代码、提交代码、分支对比、提交及合并日志等常规操作。

支持代码库权限的分配，支持代码库的操作审计。

支持代码分析和统计，可查看代码量统计、代码趋势、代码提交统计等。

支持自定义分支策略规范流程，通过流程驱动分支自动化操作、流水线执行；支

持分支流程设置卡口，如合并之前检查流水线状态。

### (3). 自动化构建与测试

支持可视化编排流水线，支持应用级、服务级流水线，支持并行/串行处理、设置各种流水线阶段、设置静态参数/动态参数、支持 VM/Docker/K8S 多模。

支持集成 Jenkins、支持可视化页面编排流水线，工具打通。

支持流水线的复制、克隆、自定义阶段、任务以及参数。

支持人工审批流水线执行情况，包括或签或者会签。

支持自定义门禁阈值，如代码扫描、安全检测等，不满足设定阈值的情况下自动停止流水线执行，并触发通知。

支持页面设置工具脚本、静态参数、执行参数等。

支持流水线权限控制，对单个用户可查看权限、可编辑以及运行权限的统一管理。

支持测试用例管理，支持用例分组展示；支持测试用例导入导出、批量操作和关联需求功能。

支持提测单管理，提测单信息包含提测需求、提测执行的构建流水线等关联信息，通过提测单可以追溯提测的需求、代码、流水线、制品和质量等信息。

支持提测版本依赖各服务版本的管理，支持图谱和列表展示版本依赖关系。

支持通过提测版本发起发布申请。

### (4). 自动化部署

支持容器/非容器应用统一发布。

支持软件发布流程管理，发布流程支持平台审批或集成第三方系统审批，支持制品晋级操作。

支持部署模板管理，可通过部署模板快速定义部署过程脚本；支持设置部署超时、失败跳过、失败重试部署机制。

支持部署单元配置，每个部署单元关联机器范围和配置文件，支持按部署单元进

行部署。

支持部署记录查看和部署；支持部署日志查看。

支持容器应用的状态同步、健康检查、异常提醒。

支持部署脚本定义，支持通过部署模板或自定义的方式创建部署脚本。自动化部署支持容器/非容器应用统一发布。

支持软件发布流程管理，发布流程支持平台审批或集成第三方系统审批，支持制品晋级操作。

支持部署模板管理，可通过部署模板快速定义部署过程脚本；支持设置部署超时、失败跳过、失败重试部署机制。

支持部署单元配置，每个部署单元关联机器范围和配置文件，支持按部署单元进行部署。

支持部署记录查看和部署；支持部署日志查看。

支持容器应用的状态同步、健康检查、异常提醒。

支持部署脚本定义，支持通过部署模板或自定义的方式创建部署脚本。

#### (5). 制品管理与版本追溯

支持在仓库制品维度，在线查看是否存在安全漏洞以及在线报告。

提供制品、第三方依赖的安全扫描能力，并对安全漏洞支持平台级别、项目级别等邮件提醒。

支持制品在同一节点或不同节点之间晋级，支持晋级策略配置。

支持设置高危、中危险、黑名单设置阻断下载，支持白名单设置并支持白名单放行。

支持漏洞库私有化部署与持久化，支持在线更新或者人工同步。

支持对接组件安全工具，实现组织级安全策略下发与实施。

#### (6). 效能度量与可视化

支持通过版本进度、迭代进度、工作项燃尽图等展示当前项目的进度。

支持通过缺陷的级别、解决情况、占比等查看当前版本的质量概况。

支持展示项目组成员以及人员、角色的工作项分配概况。

支持通过需求吞吐量和流水线执行趋势展示工作进行效率。

#### (7). 平台协同能力

支持与底层异构算力统一纳管系统深度联动，实现开发流程与资源管理的无缝对接，自动化部署可直接调用容器云资源，监控数据互通共享，形成闭环优化。

### 2. 异构分布式算力统一纳管系统功能需求

#### (1). 异构节点纳管

支持 X86、C86、ARM 等异构计算节点的统一纳管，通过 Kubernetes 节点亲和性、污点与容忍等机制实现资源的灵活调度。

支持集群、节点、分区、实例（Pod）、容器的交互式列表展示与资源监控，深度监控集群五大核心组件性能指标，支持 Web 端 kubectl 终端、分级 Kubeconfig 权限管理、组件按需安装、事件持久化存储及操作历史追溯，所有关键信息与指标通过可视化呈现，实现集群一体化、精细化运维管控。

支持灵活的分区全生命周期管理能力，支持共享和独享两种分区模式且可动态调整隔离策略。分区的创建、查询、编辑、删除及节点迁入迁出操作，支持配置 CPU/内存等资源超分配比例以提升利用率。

支持灵活的节点污点管理功能，允许管理员为单个或多个节点设置污点，通过键值对和效果标记（如 NoSchedule、PreferNoSchedule 或 NoExecute）精准控制 Pod 调度策略，有效实现节点隔离或专用节点管理，所有污点配置实时生效并支持批量操作。

#### (2). 容器镜像管理

支持企业级镜像全生命周期管理能力，支持通过可视化界面将容器镜像安全高效地上传至 Harbor、Registry 等仓库并同步至目标集群。

支持镜像标识与标签管理、公共/租户私有镜像隔离存储与访问控制、运行容器镜像捕获生成快照、同类型仓库间镜像同步、手动/策略化镜像归档与检索。

支持完善的镜像保护与清理机制，支持对关键镜像版本单/批量锁定（禁止覆盖删除）、租户级自定义时间/版本数量维度的镜像回收策略、非锁定镜像版本批量清理。

### (3). 网络与存储适配

支持 underlay、overlay 网络方案，overlay 网络支持直接路由模式，兼容 IPv4/IPv6 双栈模式，支持跨主机容器互联及容器与外部非 NATIP 直通；支持主机网络模式及集群外部直接访问 PodIP。

支持租户自行可视化设置 Pod 的入网出网规则配置，配置维度按应用、服务、Pod、命名空间、IP 地址段等。

支持可视化的 IP 资源管理功能，支持网络创建、IP 地址/地址段分配及使用情况查询，同时具备服务 IP 预约、固定 IP 绑定能力，并支持主机网络模式和集群外部直接访问 PodIP 等高级网络特性。

支持在 overlay 网络模式下提供 EgressIP 功能，可为 Namespace 或 Workload 设置统一出站 IP，同时提供固定 IP 绑定能力，确保关键业务 Pod 的 IP 地址持久化，增强网络访问的可控性和可追溯性。

支持创建 ClusterIP、NodePort、LoadBalancer 三种类型的 Service，可配置端口映射、协议类型等基础参数并添加自定义标签，满足不同场景的内部服务暴露与分类管理需求。

支持 HTTP/HTTPS、TCP/UDP 多协议负载均衡配置与 EWMA 智能流量调度算法选择，能下载 Ingress 配置 YAML 文件用于备份迁移。

支持基于权重比例的流量分发、基于请求头和 Cookie 的灰度路由规则，可组合多种策略适配复杂发布场景，实现多版本服务并行运行与流量灵活切换。

支持 StorageClass 可视化全生命周期管理能力，支持管理员通过图形界面完成

SC 的创建、Provisioner 及参数配置、YAML 文件下载、删除等操作。兼容 NFS、Ceph-rbd、CephFS、Carina 本地存储等多种存储类型，并可设置 Retain/Delete/Recycle 回收策略。

支持 PV 可视化全生命周期管理能力，支持管理员和租户通过图形化界面完成 PV 的创建、配置、YAML 文件下载及日常管理，可删除 release 或 available 状态的闲置 PV，还能一键克隆 available 状态的 PV 以实现存储资源快速复用。

支持 PVC 可视化全生命周期管理能力，可以在线扩容存储容量、设置磁盘配额限制，以及快照创建、存储卷克隆、快照恢复等全周期数据保护操作。

支持同时挂载多个 NAS 存储系统，管理员可执行存储卷挂载/卸载操作，并为不同租户分配专属 NAS 资源配额。租户可自主管理存储卷的创建、删除、查看及共享，服务发布时可直接选用 NAS 存储数据，平台会实时监控存储使用情况，在容量达到阈值时自动触发告警。

#### (4). 容器应用管理

支持以层级树形式展示租户下的所有应用及其下属服务，支持展开/折叠节点，直观呈现应用与服务的归属关系。

支持应用的创建、资源配额编辑、单/批量删除、服务发布、任务创建等基础操作。

支持批量版本变更、应用配置备份为 YAML 模板跨集群复用、临时屏蔽非关键告警等便捷能力。

支持多集群应用资源拓扑可视化管理能力，支持按应用部署的集群维度自动构建并展示应用内 Service、Secret、ConfigMap、Job、CronJob、Ingress 等核心资源的拓扑关系图，直观呈现资源间的依赖与关联关系。

支持通过服务树结构或列表查看服务详情，涵盖基本信息、网络监控、PVC 监控和实例状态，可执行横向和纵向弹性伸缩、版本变更、升级回滚、高级配置、容器启停等全流程运维操作。

支持容器驱逐、捕获运行中容器生成自定义镜像、通过 Web 终端访问容器命令行、Debug 等运维操作，可查看容器标准输出日志，实时掌握应用运行状态。

#### (5). 运维监控

支持多类监控对象与指标实现全面告警，包括基础设施维度（节点、主机、PV、PVC 等，监控 CPU、内存、磁盘、网络及主机存活状态）、K8S 核心组件维度（APIServer、Controller、Ingress，监控运行状态）、工作负载维度（Deployment 副本数、Pod 驱逐/重启/异常等专项指标）、数据库维度（MySQL 连接数、慢查询数量）以及日志维度（基于关键字等匹配规则）。

支持告警触发与恢复双重通知机制，集成邮件、短信、站内信、微信、钉钉及第三方 Webhook 接口等多种通知渠道。

支持按集群、服务、实例、时间范围及关键字的多维度搜索功能；支持以表格或窗口形式查看日志信息，并可进一步查看单条日志的详细内容，便于快速定位问题和分析应用运行状态。支持实时查询容器启动日志，可自定义日志窗口展示行数、文件大小限制及查询起始时间，精准筛选目标时段日志内容。

支持租户全生命周期管理与跨集群资源管控能力，支持平台管理员通过可视化界面进行租户的创建、查询、编辑、删除等操作，所有变更实时生效且记录操作日志，保障管理的安全性与可追溯性。可查看分配的集群分区清单、资源配额使用情况、超配状态及网络流量统计等详情。平台管理员可全局查看所有租户的应用、服务及实例列表，租户管理员仅能查看所属租户资源，且均支持按租户名、集群名等维度快速筛选查询，实现租户资源的多维度可视化管控。

支持精细化的租户资源配额全维度管理能力，支持跨多个集群为租户统一配置 CPU、内存、存储等资源配额，允许基于分区设置大于 1 倍比例的资源超分配，算力集群可按总资源比例或自定义方案分配配额，且所有配额支持动态调整。

支持多维度智能化报表，自动采集集群、分区、节点、租户、告警、审计、应用

七大维度的核心数据，涵盖各维度的基础状态、资源利用率（平均值、峰值、谷值）、业务运行特征及安全审计信息等内容，为报表生成提供完整数据支撑。

#### (6). 安全合规

支持自动记录用户在平台内的所有关键操作，完整捕获操作时间、执行用户、目标资源、操作类型及参数变更等详情

支持对容器集群提供安全配置、权限配置、漏洞多维度安全检测，自动生成可视化风险评估报告。每份报告均附带针对性修复建议，支持单个或批量 Excel 格式导出。

支持对容器镜像进行深度安全检测（包括 CVE 漏洞、敏感信息泄露、恶意软件等风险）。扫描结果自动标注漏洞等级。

支持用户安全参数可视化配置，满足密码安全策略、会话管理策略、用户/密码锁定策略的配置和修改。

#### （五）非功能需求

##### 1. 技术架构技术手段要求

系统应采用微服务架构，遵循云原生设计理念，支持容器化部署；

技术栈应开放、成熟，采用业界主流的 DevOps 工具链（如 Jenkins、GitLab CI），具备良好的扩展性和可维护性；

开发语言主要采用 Java、Python、Go 等，支持多语言扩展；

数据库应支持国产数据库（如达梦、人大金仓、OceanBase 等）；

应与底层容器云平台（基于 Kubernetes）实现 API 级集成。

##### 2. 总体架构说明

平台整体采用三层协同架构：



整体架构采用“三层协同、全链路闭环”设计，自上而下分为业务应用层、平台支撑层、基础设施层，各层级职责清晰、协同联动，依托微服务开发平台与异构分布式算力统一纳管系统的深度融合，实现微服务业务应用从开发到运维的全流程自动化、标准化管理，架构整体呈现“开发-部署-运维-优化”的闭环能力。

核心能力围绕“开发高效化、部署自动化、运维标准化、资源集约化”展开，依托微服务开发平台与异构分布式算力统一纳管系统的协同联动，实现微服务业务应用全生命周期的高效管理，同时发挥异构算力统一纳管的优势，适配多场景业务需求。

### 3. 性能需求

支持至少 200 个并发用户同时使用平台功能（如创建流水线、查看项目进度等），页面平均响应时间 $\leq 2$  秒；

流水线并发执行数：支持至少 50 条流水线同时执行，构建任务平均完成时间不超过 10 分钟（视代码规模而定）；

平台应支持水平扩展，随着用户量和任务量的增加，可通过增加服务实例提升处理能力；

系统需保证  $7 \times 24$  小时稳定运行，年度可用性 $\geq 99.9\%$ 。

单套容器云平台可管理的容器集群总数  $\geq 100$  套

单个容器集群可管理的节点总数  $\geq 500$  台

单个容器集群可承载的 Pod 总数  $\geq 20,000$  个

单个容器集群节点可承载的 Pod 数量  $\geq 50$  个

### 4. 安全需求及等级保护开发要求

平台需提供严格的权限控制，支持基于角色的访问控制（RBAC），确保不同用户只能访问授权范围内的项目和资源；

代码仓库和制品仓库应具备安全扫描能力，及时发现已知漏洞和后门；

平台应防止 SQL 注入、跨站脚本攻击等常见 Web 攻击；

敏感数据（如代码、凭证、配置）在存储和传输过程中需加密；

平台应满足国家等级保护三级要求，配合完成等保测评；

提供完整的操作审计日志，记录用户关键操作，便于追溯；

平台应避免存在任何后门或未公开接口，定期进行安全漏洞扫描和修复。

## 5. 运行环境需求

服务器：Linux 服务器（支持 CentOS 7+、麒麟、统信 UOS 等国产操作系统）；

容器运行时：Containerd 或 Docker；

容器编排：Kubernetes 1.28+；

数据库：MySQL 5.7+ 或国产数据库；

中间件：Redis、Nginx 等；

代码仓库：GitLab（可单独部署或集成）；

制品仓库：Harbor 或 Nexus；

网络：平台内部服务之间需高速网络互通，对外提供 HTTPS 访问。

## 三、项目实施要求

### （一）项目团队要求

为顺利实施本项目，投标人须组建稳定、专业的项目团队，项目团队成员不少于 14 人，其中项目团队核心成员不少于 6 人（包括项目经理和现场服务人员）。现场服务人员不少于 5 人，全部具备本科或以上学历，其中设置技术架构、系统分析、前后端开发、测试、运维等人员角色。核心成员应具有 3 个以上类似微服务开发平台或 DevOps 平台项目的经验，且具备计算机技术与软件专业技术资格（水平）的系统架构设计师（高级），具体要求如下：

1. 项目经理：具有 8 年以上相关经验，具有信息系统项目管理师证书（高级），熟悉 DevOps、微服务、容器架构，具备较强的沟通协调能力。

2. 技术架构师：具有 5 年以上微服务架构设计经验，熟悉 Kubernetes、容器化技

术。

3. 开发工程师：至少 3 名，其中后端开发需熟悉 Java/Go/Python，有 DevOps 工具链开发经验；前端开发需熟悉 Vue/React，有平台类项目开发经验。

4. 测试工程师：具有自动化测试经验，熟悉性能测试、安全测试工具。

5. 现场实施人员：具备 3 年及以上的云原生或持续集成或持续部署的实施运维经验。

团队服务要求：采购人有权对不满足要求的人员要求投标人进行更换，投标人应及时更换相应人员并保证项目进度不受影响；若采购人认为工期和质量无法确保时，投标人须及时增加项目人员。

投标人承诺项目经理及核心人员要在项目正式验收前专职承担本项目相应工作，未经采购人许可不得变更，且承诺承诺所投入的项目团队所有成员均为本单位正式员工。

## （二）知识产权要求

投标人保证采购人在使用合同中的产品或其中任何一部分时，不受第三方提出的侵犯其专利权，商标权、工业设计权和其它受保护的权利的索赔和起诉，如因投标人提供的产品或软件导致版权纠纷，由此给采购人带来任何损失由投标人承担。

结合本项目业务需求定制化开发所形成的软件开发成果，相关知识产权、著作权归采购人所有。投标人或甲乙双方针对本项目需求开发或组织开发的软件、软件模块或其他代码等需在项目正式验收前向采购人提交源代码。未经采购人事先书面许可，投标人不得将之用于商业用途或提供给第三方，否则承担相应的经济 and 法律责任。

本项目招标文件中技术需求书部分相关知识产权、著作权归采购人所有，未经采购人事先书面许可，投标人不得将之用于商业用途或提供给第三方，否则承担相应的经济 and 法律责任。

在本合同生效前已存在的原有产品及其功能模块的著作权及其他知识产权并不因本

合同的签署和履行而转移，但投标人应确保采购人在使用过程中的合法性并应提供相关产品的技术白皮书、帮助手册、应用接口文档等。包括：投标人保证在本项目中所有预装和为本项目安装的系统软件、数据库软件等成品软件是在中国境内具有合法版权的正版软件；若投标人在本项目实施过程中使用投标人自有的软件产品或功能模块，应向采购人开放源代码，采购人有权不限期限地进行二次开发；若投标人在本项目中采用第三方软件或产品，投标人应保证其均是在中国境内具有合法版权的正版软件并获得源代码使用授权且提供源代码。

在项目正式验收前，需协助采购人完成本项目相关功能模块和核心技术的软件著作权申请，并承担所有申请和受理过程的相关费用。

### （三）配合评测要求

微服务开发平台和异构分布式算力统一纳管系统配合上云应用顺利通过三级等保评测工作。

### （四）工期进度要求

本项目自合同签订之日起，总工期不超过 6 个月，具体节点如下：

第一阶段（合同签订后 1 个月内）：完成需求调研、详细方案设计，提交《需求规格说明书》和《详细设计说明书》评审。

第二阶段（合同签订后 2 个月内）：完成关键技术研究验证，包括集群部署与高可用架构验证、网络与存储选型测试、多租户与权限管理机制验证等工作。

第三阶段（合同签订后 4 个月内）：完成平台核心功能开发与信创适配，包括微服务开发平台和异构分布式算力统一纳管系统的功能开发，并进行国产化环境兼容适配。

第四阶段（合同签订后 5 个月内）：完成平台全部功能测试与调优，开展系统集成测试、性能测试、安全测试，部署到试运行环境。

第五阶段（合同签订后 5.5 个月内）：完成现场部署与协同调试工作。

第六阶段（合同签订后 6 个月内）：完成试运行、用户培训、文档整理，完成项目验收。

项目验收合格后，进入为期一年的维护期，所需一切费用均由投标人承担。

#### 四、培训要求

本项目投标人须提供不低于 20 人次的现场培训，培训所产生的费用均视为已经包含在投标报价中，采购人不再支付培训产生的任何费用。具体如下：

1. 维护培训：培训对象为采购人项目组及系统运维相关人员（不少于 5 人）。主要内容包括系统总体架构、部署架构、程序安装配置、模块详解、运维监控、故障处理等。

2. 使用培训：培训对象为采购人使用该应用系统的相关人员（不少于 15 人），包括平台管理员、项目管理员、开发人员、测试人员等。主要内容为平台各功能模块的操作方法、流水线配置、项目管理流程等。

培训需提供配套的培训手册、操作指南等文档，确保培训后用户能独立使用平台。

#### 五、售后及技术支持服务

投标人应提供 1 年的维护服务，所需一切费用均由投标人承担，服务起始时间为终验合格之日。具体要求如下：

服务方式：提供 7×24 小时技术支持服务，包括电话、邮件、远程协助等。

响应时间：故障响应时间不超过 2 小时，修复时间不超过 12 小时。对于严重故障，需立即响应并协调资源解决。

服务内容：包括系统故障排查、性能优化、安全补丁更新、版本升级指导等。如有系统软件升级、系统故障，投标人应进行处理，所需一切费用均由投标人承担。

服务方案：投标人需提供书面的技术支持及售后服务方案，明确服务方式、范围、内容、人员配置等。

## 六、保密要求

投标人必须对技术文件以及由采购人提供的所有内部资料、技术文档和信息予以保密。投标人必须遵守与采购人的相关保密规定，未经采购人书面许可，投标人不得以任何形式向第三方透露本项目的任何内容。（投标人须针对以上要求提供承诺函并加盖投标人公章）。

## 七、成果交付物要求

### 1. 软件成果

微服务开发平台一套（包含全部功能模块），部署在采购人指定环境。

异构分布式算力统一纳管系统一套（包含全部功能模块），部署在采购人指定环境。

平台所有源代码（包括本项目开发的所有代码、配置脚本、数据库脚本等）。

部署包及镜像文件。

### 2. 文档成果

异构分布式算力统一纳管系统升级维护方案 1 份；

微服务开发平台升级维护方案 1 份；

异构分布式算力统一纳管关键技术研究报告 1 份。

### 3. 培训材料

培训课件、操作视频、常见问题解答等。