Container Platform

白皮书

发布日期 2019-06-21

北京凌云雀科技有限公司

目 录

1 概述 1

1.1 产品背景 1

1.2 产品简介 1

1.3 产品特点 4

1.4 系列产品介绍 6

2 核心功能介绍 7

2.1 平台管理 7

2.2 项目管理 7

2.3 视图拆分 8

2.4 基础设施 10

2.5 容器服务 11

2.6 智能运维 13

3 客户价值 14

版权所有©北京凌云雀科技有限公司

1 概述

1.1 产品背景

由于传统的应用管理工具和模式无法满足企业快速创新的需求，数字化转型成为了国内众多企业持续发展的必经之路。在数字化转型的大背景下，传统外包的做法正在逐渐改变。灵雀云于 2019 年第一季度发起的“企业 IT 应用现状和云原生技术落地情况”调研结果显示，企业开始不再将大部分业务系统，尤其是核心业务需求开发外包。而是更倾向于自建软件研发团队并主导 IT 应用的研发。软件能力将成为企业的核心竞争力，而软件能力正是数字化转型的核心。只有企业自己主导 IT 研发，才能够打造 IT 核心竞争力。

通过调研，灵雀云认为数字化转型的最终目标是实现客户满意度的提升、打造差异化竞争优势、加速产品上市。而以下三个方面可以作为衡量企业数字化转型成功与否的标准：

- IT 部门由成本中心转为收入中心；
- 企业自己主导 IT 产品的研发；
- 改进工具、流程、文化来提高交付速度和质量。

随着 Docker 容器、Kubernetes、微服务等热门技术的兴起和逐渐成熟，为企业数字化转型提供了更具可行性、更容易落地的云原生解决方案。而通过容器技术搭建 PaaS（Platform-as-a-Service）平台来建设、运行、管理业务应用或系统，已经成为了企业数字化转型的主流趋势。

为了满足更加广泛的企业云原生需求，灵雀云借助多年来服务不同领域头部客户的相关技术实践经验，于 2019 年，在企业级 PaaS 平台 ACE（Alauda Cloud Enterprise）的基础上，推出了新一代的聚焦于使用场景的企业级云原生容器 PaaS 平台 Alauda Container Platform（以下简称 ACP 或平台）。

1.2 产品简介

ACP 拥抱云原生（Cloud Native）技术，通过整合 Docker 容器、Kubernetes 原生架构、微服务等相关新技术和新理念，可实现业务应用从开发、测试，到部署、运维的全生命周期平台化管理，能有效帮助企业实现数字化转型，提升企业的 IT 交付能力和竞争力。

版权所有©北京凌云雀科技有限公司

ACP 作为企业级的云原生容器平台，可服务于不同规模的企业，支持管理各种复杂度的基础设施环境（单台机器或多个异构的数据中心）、组织结构清晰的部门建制和人员团队。

ACP 能够满足企业级应用逐步向容器化、微服务化过渡的广泛需求，支持企业建立一个覆盖内外部各环节和组织结构的私有云平台。提升企业 IT 资源利用率，加快应用迭代速度，降低应用交付成本，实现业务应用的智能运维，从而助力企业获得持续创新的核心能力。

ACP 的产品结构如图 1-1 所示。

版权所有©北京凌云雀科技有限公司

图 1-1 产品结构图

ACP 能有效助力企业数字化转型，智能化 IT 基础架构，通过**平台化的基础设施、敏捷化的应用交付、自动化运维管理、服务化的 IT 治理**，赋能中小型企业的 IT 部门，使其同时扮演业务支撑者和业务驱动者的双重角色。

- **平台化的基础设施管理**

版权所有©北京凌云雀科技有限公司

全面集成 Kubernetes 容器编排引擎，在 Kubernetes 业务集群与平台对接后，执行统一管理，并提供健全的容器网络与容器存储解决方案，形成平台化的基础设施。

- **高效的容器服务**

灵活的应用编排和交付，保证在多场景下交付应用。同时，使用 Docker 容器管理应用，占用空间小、资源利用率高，且通过 Docker 命令就可实现轻松快捷地部署。

- **自动化运维管理**

分别从用户视角和管理视角，提供以应用为中心的智能运维体验，屏蔽基础运维架构，使用户更专注于核心业务。

- **服务化的 IT 治理**

支持中小型企业的多租户管理场景，实现细粒度权限控制和自助 IT 治理。统一管理和监控不同基础设施环境上的资源，通过安全审计机制，保障系统安全性。

1.3 产品特点

ACP 是结合最前沿的先进技术，以用户体验优先的设计理念打造的云原生容器平台，具有以下重要特点。

- **无缝对接 Kubernetes**

深度集成 Kubernetes 容器编排引擎，提供标准的 Kubernetes 容器编排服务。平台更好的发挥了 Kubernetes 的产品特性，支持一键部署业务集群和网络；支持容器应用的自动化部署、扩展和管理；可按需集成存储、监控、日志等解决方案；容器化管理工作负载，让整个平台可以像管理产品一样管理应用，进一步提高资源利用率。

把 Kubernetes 原生架构当做开发框架，基于 Kubernetes 扩展机制开发平台功能。在平台性能、稳定性和可扩展性得到保证的同时，支持标准的 Kubernetes API，兼容 Kubernetes 生态工具和系统，支持集成 Kubernetes 原生插件。

- **多集群管理**

版权所有©北京凌云雀科技有限公司

支持接入通过 AKE （Alauda Kubernetes Engine，Kubernetes 安装器）部署的或其他第三方平台部署的原生 Kubernetes 集群，统一管理不同云端上的 Kubernetes 集群。

统一多集群管理不同基础设施环境中的集群和主机，保障了故障迁移，使企业能快速有效并低成本的跨区域、跨平台运行集群。

- **企业级多租户管理**

在支持搭建自由用户体系的基础之上，对接 LDAP（Lightweight Directory Access Protoco，轻量级目录访问协议）或 OAuth 2.0 协议，纳入企业已有的用户体系，可通过 RBAC 细粒度设置用户权限。

支持基于多租户的项目管理，项目可共享平台的基础设施资源，并根据项目需求分配资源。

平台的企业级多租户管理能力，大大简化了为角色相同成员分配相同资源权限的重复工作，利于项目内外部的资源隔离，也增强了数据的保密性。

- **基于用户画像的优化设计**

ACP 的整体设计紧密贴合用户搭建 PaaS 容器平台的使用场景，精准服务于数字化转型的企业客户。在符合用户业务逻辑的同时，根据企业常见角色的具体使用场景拆分用户视角，为用户提供更简单、高效的交互体验。

- **标准化交付**

灵雀云借助于多年来服务不同领域头部客户的经验，打造标准化的产品旨在服务于更加广泛的领域和更多的企业客户，助力企业客户数字化转型落地，获得持续创新的核心能力。标准化交付的 ACP 还具有部署、实施、运维、升级标准化以及可以和第三方容器平台进行融合的特点。为目标客户和合作客户提供了更多的便利性和可能性，也将推动 PaaS 容器平台的普及和落地。

同时，标准化交付的 ACP 可单独使用为企业提供容器服务，也可以结合灵雀云的其他产品（例如：Alauda DevOps、Alauda Service Mesh）提供更为丰富的 PaaS 生态体验，或接入第三方容器平台帮助容器化产品落地。

版权所有©北京凌云雀科技有限公司

1.4 系列产品介绍

灵雀云为了满足企业客户的不同需求，在 ACP 的基础上还延伸出了能够和 ACP 组合使用的系列产品。包含：Alauda DevOps、Alauda Service Mesh。

用户可单独订阅 ACP 作为容器 PaaS 平台为企业提供企业场景的多集群、多租户管理、智能运维，支持用户基于本平台实践 PaaS 生态集成，也可以同时订阅系列产品和 ACP 组合使用，为大型企业的复杂业务应用管理提供完整的 PaaS 平台体验。

- **Alauda DevOps**

DevOps 平台是一款基于容器的 DevOps 研发云应用平台，支持多集群统一管理，容器负载统一调度，细粒度的用户权限系统。平台为企业提供包含需求管理、项目管理、研发、测试、运维等服务在内的开箱即用一站式服务，使软件的构建、测试和发布变得更加快捷、频繁和可靠。

通过完整的 DevOps 工具链，深度集成代码仓库、制品仓库、持续集成等类别中的主流工具，实现零成本迁移，快速实践 DevOps。DevOps 强调产品管理、自动化软件交付和基础设施变更的过程。缩短开发周期，增加部署频率，实现更可靠的发布。支撑应用的全生命周期，旨在建立一套快速、频繁、稳定地进行构建、测试、发布软件的文化与环境，与业务目标紧密结合。

基于 DevOps 理念，即重视软件开发人员（Dev）和 IT 运维技术人员（Ops）之间沟通合作的文化和惯例，DevOps 平台对应用研发流程中的多租户、代码、持续集成和交付等方面分别进行了优化。

- **Alauda Service Mesh**

Service Mesh 是基于容器和 Istio 框架的微服务治理平台。平台提供了环境部署、Istio 配置、Istio 监控、应用管理、服务注册发现、服务拓扑、调用链追踪、路由管理、Istio 网关、流量策略、安全策略等服务的开箱即用一站式服务。

Service Mesh 是分布式服务架构，基于 Istio，支持分布式服务发布、服务注册发现、调用链跟踪、智能路由、流量策略、安全策略、Istio 配置、Istio 监控等功能。

版权所有©北京凌云雀科技有限公司

2 核心功能介绍

2.1 平台管理

- **用户管理**

平台的 IDP (Identity Provider)配置，支持通过同步 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）导入企业已有用户体系；支持 OIDC（OpenId Connect）协议，可使用平台认可的第三方账号登录平台。

- **角色管理**

平台支持基于角色的权限访问控制（RBAC，Role-Based Access Control），根据不同的企业使用场景，系统设置了五大权限角色：平台管理员、平台审计人员、项目管理员、命名空间管理员、命名空间成员。

- **权限管理**

通过给不同的用户分配不同的角色，从而得到不同的权限，简化了权限管理，优化了权限隔离。

2.2 项目管理

平台的项目之间可以灵活的划分出独立且相互隔离的资源空间，每个项目都拥有独立的项目环境，能够代表企业中不同的子公司、部门或项目组。通过项目管理，能够轻松实现项目组之间的资源隔离、租户内的配额管理以及项目下的人员管理。如图 2-1、图 2-2 所示。

一个项目支持绑定多个集群，并管理计算资源配额，提高了资源利用率。

同时，支持为项目绑定多个企业私有的域名，以便通过域名访问项目下应用。

版权所有©北京凌云雀科技有限公司

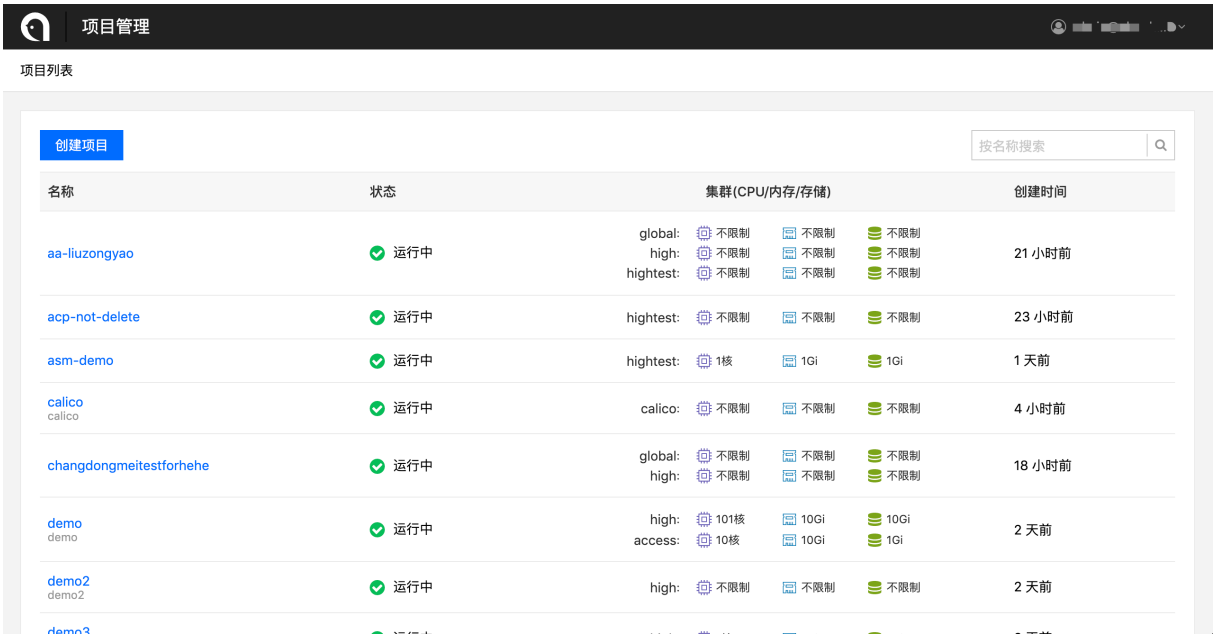

图 2-1 项目列表

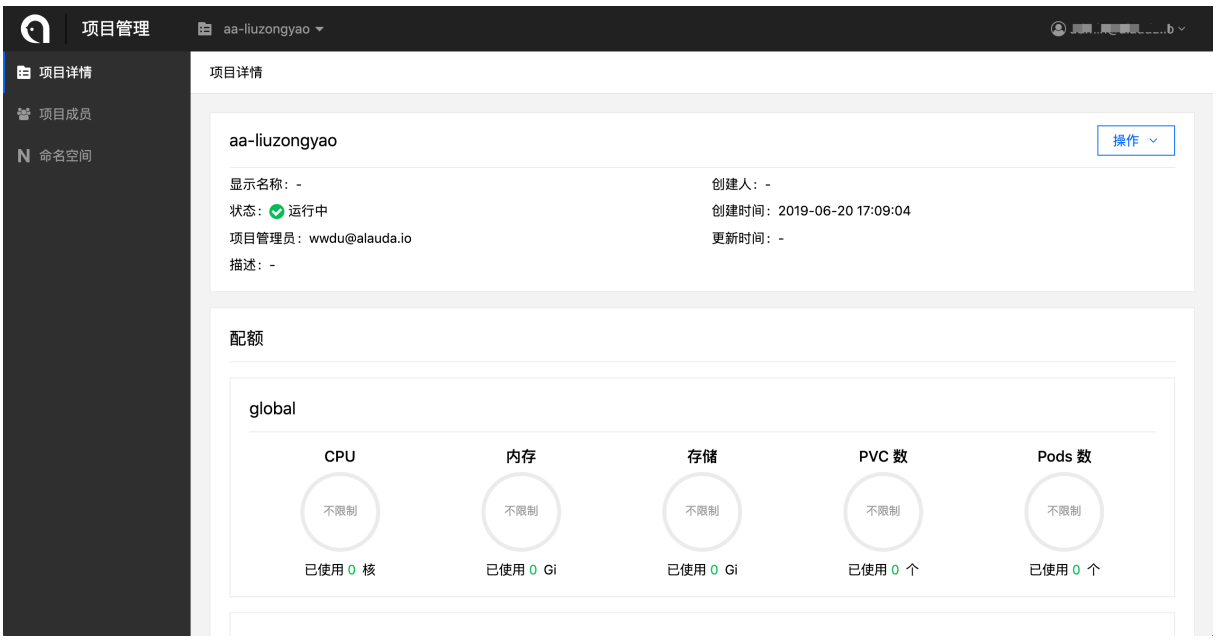

图 2-2 项目管理

2.3 视图拆分

为了进一步提升用户体验，平台根据用户画像，针对企业中应用的基础环境维护人员、管理者、研发人员的日常工作区和习惯，为使用者提供了独有的操作视角，即管理视图和业务视图。每个视图针对该角色的使用场景进行了优化，同时可通过权限控制视图的切换。

- **管理视图**

管理视图主要面向平台管理员，负责管理集群和平台运维，如图 2-3 所示。

平台管理员和具有查看管理视图权限的用户，可以进入管理视图。

在管理视图中，用户可以管理平台共享资源，以及集群下的资源；并对平台、集群或项目实施运维监控。

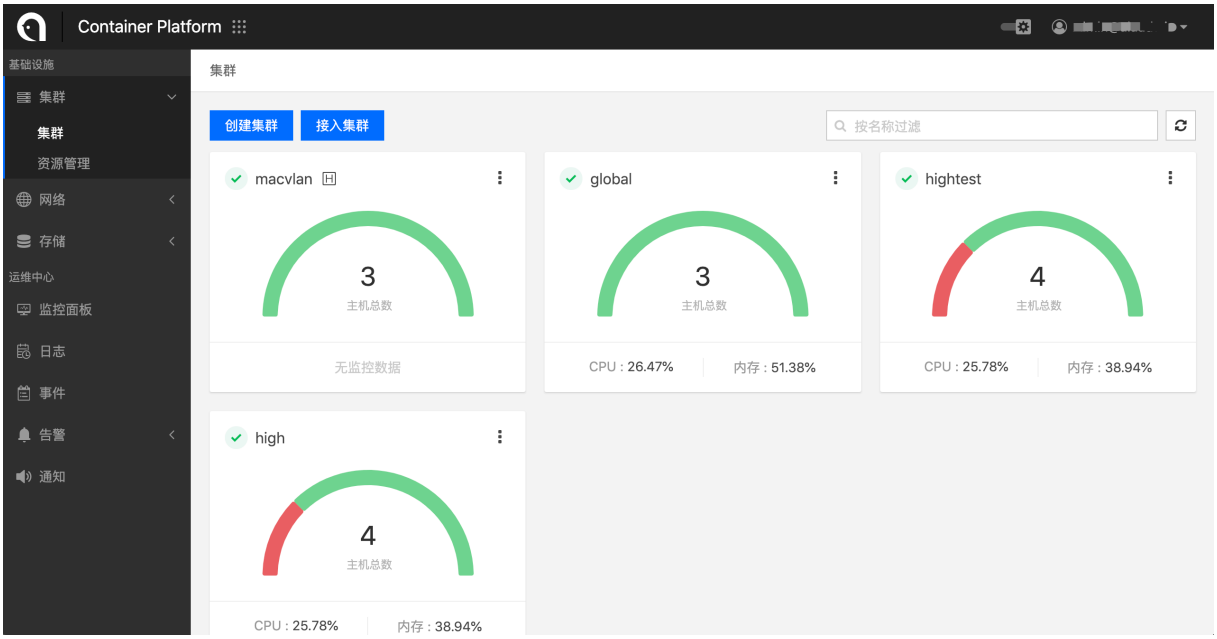

图 2-3 管理视图

- **业务视图**

业务视图主要面向项目管理员以及一般的开发、测试人员，如图 2-4、图 2-5 所示。

作为项目成员的大部分用户，不能查看管理视图，只具有查看业务视图的权限。

在业务视图中，用户可以开发、部署、维护应用；管理配置文件、存储卷、内部路由等项目下资源；对应用实施运维监控。

版权所有©北京凌云雀科技有限公司

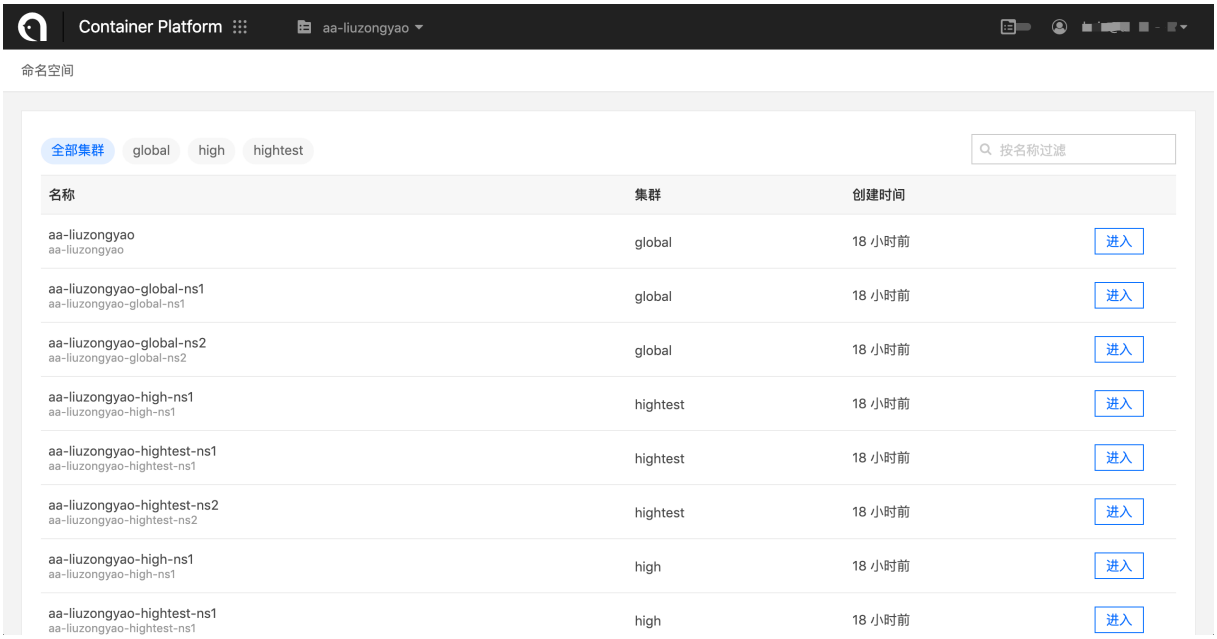

图 2-4 业务视图-命名空间列表

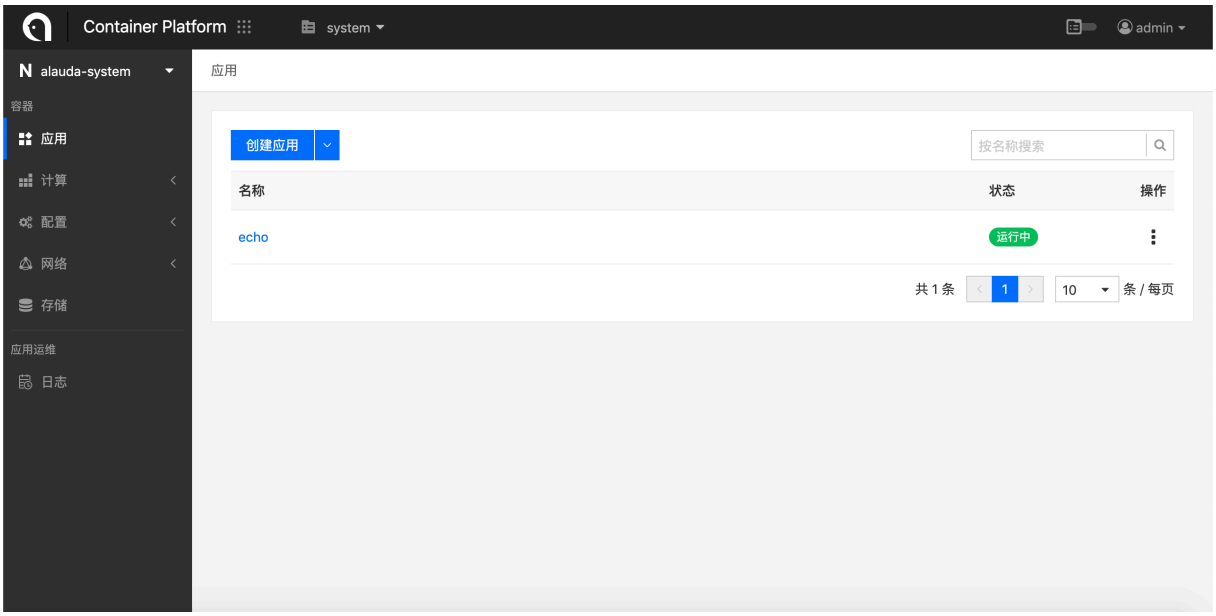

图 2-5 业务视图-进入命名空间

2.4 基础设施

平台以统一多集群管理为核心，可对接稳定快速的物理机服务器、资源利用率高的虚拟机、不同云环境（公有云或托管云）下的云主机创建 Kubernetes 集群。

多集群管理

支持运行多集群，即跨集群容器资源池统一管理运行在多个云端上 Kubernetes 集群，保证集群的高可用。提供跨云的多集群统一管理，解决多云灾备问题，并支持全局集群监控仪表盘。通过多云容器平台的多集群统一管理入口可以实现统一部署、统一发布及统一运维。

支持对集群中的主机执行变更调度状态、标签管理等操作；支持在集群中创建命名空间并划分资源配额。

支持通过平台上的 SSH 主机入口，实现远程登录主机，方便运维管理人员管理主机、排查主机故障和问题。

支持为项目创建多个命名空间，多个命名空间可以分布在不同的集群，一个命名空间只能在一个集群中。

2.5 容器服务

深度集成 Kubernetes 容器编排引擎。支持类型多样的容器调度设置，例如：通过设置主机亲和性可将容器调度到指定的主机上运行；支持 Flannel、Calico 等多种主流的容器网络模式；支持对接不同类型的存储资源。

- **资源管理**

无缝对接 Kubernetes，使用 Kubernetes 原生资源或将平台资源以 CRD（Custom Resource Definition，自定义资源类型）的形式下沉到 Kubernetes，统一由 Kubernetes 进行管理。在减少资源数据量过大对平台性能和稳定性影响的同时，降低了平台维护的成本。

可以通过平台使用自定义的 YAML 编排文件，创建 Kubernetes 资源。也可以查看和更新集群或命名空间下的 Kubernetes 资源，提供 Kubernetes 集群的深度使用体验。

- **容器调度**

全面深度支持 Kubernetes 容器编排引擎的管理功能特性，解决安装 Kubernetes 部署难的问题以及更好的发挥其产品特性，容器化管理工作负载。

提供标准的 Kubernetes 容器编排服务，实现容器应用的自动化部署、扩展和管理。

版权所有©北京凌云雀科技有限公司

- **容器网络**

提供强大的容器网络功能，支持 Kubernetes 的 Flannel 覆盖网络（VXLAN 和 Host-GW）、Calico 网络。

负载均衡功能支持灵雀云负载均衡器 ALB (Alauda Load Balancer)方案，支持 Nginx 七层负载均衡，支持实现多种复杂规则的灰度发布。配置负载均衡，把应用组件中的容器实例，挂载到负载均衡器上，把负载均衡器的服务地址作为统一访问入口。

支持统一管理客户企业私有的域名资源，可以与集群进行绑定并分配给指定的项目使用。

- **容器存储**

管理员可通过 Kubernetes 的存储类对接不同类型的存储资源。支持实施 Ceph 分布式存储方案。

普通用户通过为应用关联持久卷声明（PVC）请求持久卷（PV），或挂载主机本地存储的方式，实现容器持久存储。

- **容器配置**

通过 Kubernetes ConfigMap 统一管理容器配置，并支持在更新配置字典后，通过自定义命令，热更新业务容器中的相关配置，不重启容器即可实现配置的即时生效。

- **应用编排&应用治理**

支持通过 UI 编辑模式或 YAML 编排文件创建应用，在研发、运维、测试或生产环境中运行不同类型的业务。

业务的连续性需要长期稳定运行的环境，应用治理是一项持续的工作。平台的应用（Application）作为 Kubernetes 的 CRD 资源，由一个或多个关联的计算组件构成，支持根据不同的部署和使用需求，选择对应的部署模式：Deployment，DaemonSet 和 StatefulSet，并关联网络、存储、监控、健康检查以及其它配置。支持对比不同应用版本 YAML 上的差异，可回滚到指定历史版本。

结合实时监控和 Kubernetes 原生资源 HPA（Horizontal Pod Autoscaler，自动扩缩容），支持在部署类型为 Deployment 的组件中，根据 CPU 的利用率设置自动扩缩容规则。

版权所有©北京凌云雀科技有限公司

- **开发测试**

  通过镜像启动容器应用，能够快速的部署开发、测试环境。同时，使用相同的镜像能保持开发、测试、运维环境一致，减少错误。

2.6 智能运维

基于平台自身的特性，同时结合 Prometheus 监控和 Grafana 可视化的优势，支持对平台管理的集群、节点、应用、Pod、容器等进行实时监控。支持快捷设置集群、节点、计算组件层面的监控指标告警和日志告警（仅计算组件），也可以根据实际需求自定义监控指标算法，增加需要的告警指标及规则。

全面集成 Kubernetes 的审计和事件，可以查看平台上所有的用户操作信息（审计）和 Kubernetes 事件信息。支持查看平台上所有资源的日志信息。能够帮助用户快速地排查和解决问题。

版权所有©北京凌云雀科技有限公司

3 客户价值

- **快速搭建 PaaS 容器平台**

  为各领域更多的企业客户快速搭建 PaaS 容器平台将现有的基础设施一键升级成新一代的容器云平台，管理容器的全生命周期。为容器应用创造一个灵活轻便、高效稳定、高可用的资源调度管理平台。帮助企业客户轻松实现数字化转型，获得持续创新的核心能力。

- **持续扩展、集成 Kubernetes 生态工具的能力**

  在 Kubernetes 越来越流行、成熟的趋势下，必将建立起更全面、更具扩展性的生态圈。平台深度对接 Kubernetes，以 Kubernetes 原生架构作为开发框架，可兼容或集成越来越多的 Kubernetes 生态工具、系统、插件和解决方案，将源源不断的为使用平台的企业提供最前沿、最具竞争力的技术，从而保证企业的核心竞争力。

- **容器化应用的全生命周期管理**

  实现从测试环境到生产环境的平滑过渡。帮助企业节省环境部署、迁移和运维成本。

- **专业化的智能运维体验**

  提供专业化智能运维，多维度、全方位的收集日志、监控指标、事件、审计，帮助企业客户提升运维质量，降低运维成本。

- **高效的 IT 治理**

  基于角色设计权限管理模型，实现多租户间的资源隔离，租户内的配额管理，建立完备的平台租户和权限管理体系，真正帮助企业客户实现高效的 IT 治理。

版权所有©北京凌云雀科技有限公司