InCloud OS 6.8.0

产品白皮书

济南浪潮数据技术有限公司

2023 年 6 月

法律声明

您购买的产品、服务或特性等应受商业合同和条款的约束。本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。

除非合同另有约定 ,济南浪潮数据技术有限公司对本文档内容不做任何明示或默示的声明或保证。任何单位、公司以及个人因为下载、使用或信赖本文档而发生任何差错或经济损失的 , 济南浪潮数据技术有限公司不承担任何法律责任 , 不对使用和信赖本文档而遭受的利益损失承担责任。

本文档的内容视为济南浪潮数据技术有限公司的的保密信息 ,您应当严格遵守保密义务 ; 未经济南浪潮数据技术有限公司书面同意 , 您不得向任何第三方披露本文档内容或提供任何第三方使用。

由于产品版本升级、调整或其他原因 , 本文档内容有可能变更。济南浪潮数据技术有限公司保留在任何通知或提示下对本文档的内容进行修改的权利 ,并在济南浪潮数据技术有限公司授权通道中不时发布更新后的文档。您可通过下方技术支持部分联系获得最新版文档。

部分高级功能对于部署有一定依赖，规划请事先同技术服务人员确认。

联系方式

购买咨询：400-860-6708

800-860-6708（固话拨打）

技术服务咨询：400-860-0011 （转 4 号键）

地址：中国济南市浪潮路 1036 号

济南浪潮数据技术有限公司

邮箱：incloudsupport@inspur.com

邮编：250101

目录

1 前言

安全声明

您购买的产品在业务运营或故障定位的过程中可能会获取或使用用户的某些个人数据（如告警邮件接收地址、IP 地址），因此您有义务根据所适用国家或地区的法律法规制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

本公司将一如既往的严密关注产品与解决方案的安全性，为客户提供更满意的服务。本公司已全面建立产品安全漏洞应急和处理机制，确保第一时间处理产品安全问题。若您在本产品使用过程中发现任何安全问题，或者寻求有关产品安全漏洞的必要支持，请直接联系我司客户服务人员。

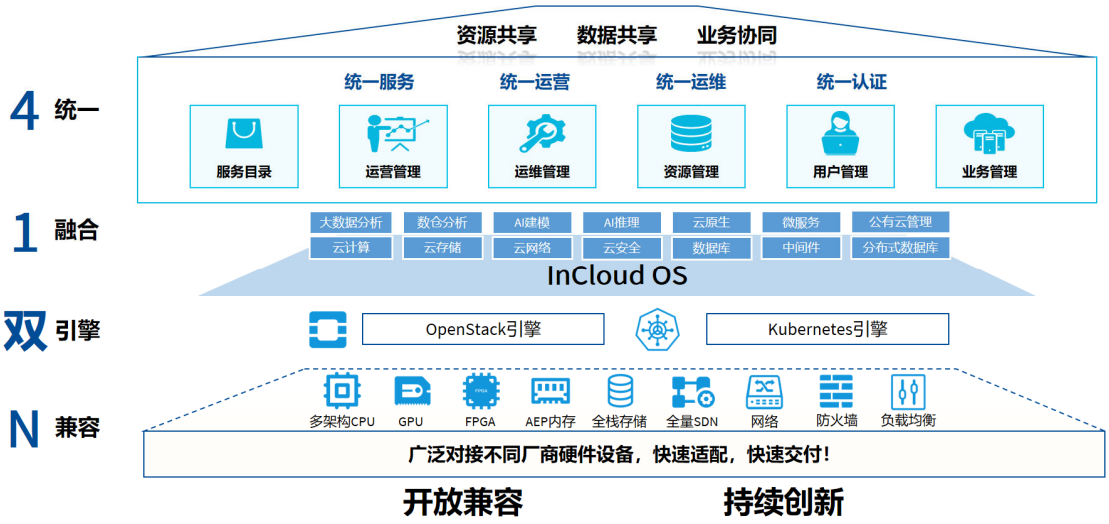
客服电话 400-860-0011（转 4 号键）

2 产品概述

2.1 产品简介

浪潮云海云操作系统（InCloud OS）是国内领先的基于开源开放架构的一款功能丰富、安全可靠的私有云平台，实现了云数据中心底层计算、存储、网络、安全等资源的统一调度管理，业务的动态变更，资源的智能管理，提供稳定可靠的私有云“交钥匙”解决方案。基于开放架构，兼容多元异构平台，可以混合纳管 X86、ARM、LoongArch 等架构的资源，实现单集群内不同 CPU 指令集的统一调度，细粒度的资源混合管理，最大程度的释放异构多元算力。

基于浪潮在数据中心领域多年研发积累以及对云业务场景的深入理解，打造出的云海云操作系统可全面支撑企业云、行业云、政务云建设。InCloud OS 通过对大规模硬件资源的有效监控、灵活的调度策略，实现资源的动态流转与伸缩，在提高整个数据中心资源利用率的同时，极大地提升 IT 资产价值和提高 IT 运营维护效率，降低数据中心的维护成本；异构融合通用算力、智能算力、超算算力，敏捷应对不同应用场景的算力需求，向下负责将物理设备真实算力转化为资源服务，向上对接各类应用需求，以智能驱动创新，最终交付智慧服务。



2.2 产品架构

产品采用微服务的架构设计理念，利用精简化的服务组件构建一个个子系统，各个子系统之间采用 REST API 进行交互，每个子系统可以独立运行，从而取代大集成式的传统基础架构，每一种服务被拆分成最小的组件，各组件可做到高内聚低耦合，彼此独立，因此每项服务都能独立扩展，并能根据业务需求，快速灵活的做到精简部署和配置，从而满足各种复杂的业务场景。同时，独立化组件服务具备故障隔离功能，可将各种服务问题（例如计算服务故障或存储服务故障）的影响限制在一定范围内，以确保不对其他服务产生影响。

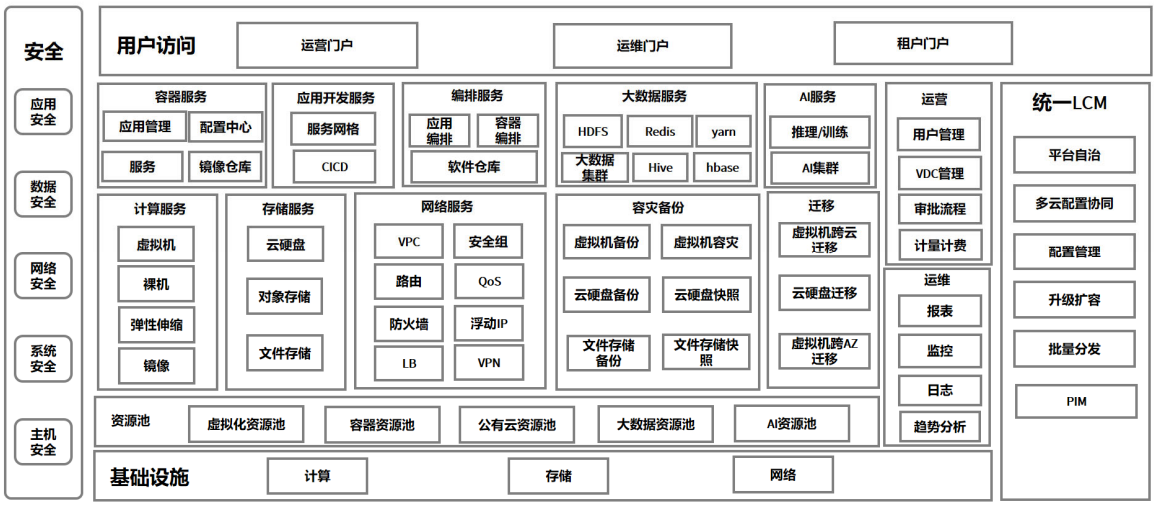
InCloud OS 包括云管理平台、虚拟化云、容器云三大核心子系统。

云管理子系统采用微服务架构的设计理念，基于 k8s+springboot 的架构模式。每个服务节点可分布式独立部署，UI 通过 Rest API 网关调用功能服务，外可提供符合 REST 规范的 API 接口供第三方集成，支持多服务节点间服务的负载均衡、服务路由、集群容错等机制，使系统具有很强的连通性，健壮性，伸缩性和扩展性，云管

理子系统主要包括统一资源管理、运营管理、智能运维等核心功能模块：

虚拟化云子系统基于开源 OpenStack 架构进行增强与扩展，并对外提供标准的符合 OpenStack 规范的 API 接口。虚拟化云子系统又分为计算服务、网络服务、存储服务三大核心功能模块。

容器云子系统以容器应用管理为中心，具备服务治理、DevOps 等云原生能力，该模块基于开源 Kubernetes 架构实现，并进行增强和扩展，北向提供标准的符合 Kubernetes 规范要求的 REST API，以声明式 API+控制器为核心设计理念。



功能架构图

虚拟化计算服务：包括虚拟机、裸金属、弹性伸缩、镜像等。用户可以根据业务类型选择虚拟机或者裸金属，同时结合 VPC、云硬盘存储等能力，打造一个高效、可靠、安全的计算环境，确保业务稳定运行。

存储服务：平台提供高可靠、高性能、可弹性扩展的云硬盘服务，并支持挂载到云主机或者容器上，提供持久化的能力，并提供文件存储、对象存储，支撑数据库、

企业应用、开发测试等场景。

网络服务：平台可以基于 VPC 网络快速规划构建和规划自己的云端网络环境。在 VPC 内可以自主管理各项网络配置，包括路由、子网划分、网关设置等，还可以通过安全组和防火墙实现网络流量管控。

容灾备份 :通过基本的快照和备份技术，可以实现云主机和云硬盘的快照备份功能，保障数据安全性。通过存储的异步/同步复制技术，可以实现业务虚拟机的容灾备份，保证业务高可靠，能够将云主机系统盘、数据盘备份至第三方存储设备，并且能够支持新建云平台对备份数据的纳管和还原。

迁移服务：支持云主机 AZ 内冷热迁移、跨资源池迁移，支持将虚拟机从传统的 VMWare 平台迁移到 InCloud OS 平台，迁移过程无侵入、MAC 和 IP 同步迁移，并保证最大限度降低业务风险。

容器服务：提供高性能的容器应用管理服务，支持企业级 Kubernetes 容器化应用的生命周期管理，通过容器虚拟化、多集群管理技术，用户可以便捷地获取租户隔离的容器应用，轻松高效地在云端运行 Kubernetes 容器化应用。

应用开发服务：通过 CI/CD 自动化流转技术，用户可以实现从源码到容器镜像快速构建，环境快速部署/更新；通过服务网格技术，用户可以实现复杂应用的各微服务之间的流量观测、流量治理、流量追踪，实现应用级智能化管理与运维。

虚拟化编排服务：提供可视化虚拟化编排服务，通过可视化图形界面，用户以拖拽的形式进行规划、构建所需的云服务，包括云主机、网络、云硬盘等。实现快速部

署业务应用系统，同时支持预制场景化模板和模板复用。

容器编排服务：提供了对云平台中工作负载、配置存储卷、访问地址的资源信息以拓扑关系的图形化管理，用户可以通过拖拽的形式将需要的组件关联起来编排对应的蓝图，提高了编排文件编写的效率，解决了容器编排文件编写的繁琐性的问题，提高了用户上云的效率。

大数据服务：大数据计算服务基于 Hadoop 集群之上，采用分布式计算框架实现大规模存储与计算,支持 Hive SQL、Map/Reduce、Spark、parkSql 等计算模型,提供可视化的客户端开发工具对集群进行文件管理、任务提交、定时任务调度、日志分析等。提供 Zookeeper、Kafka、Redis 等企业级中间件服务等。

AI 服务：提供共享型的人工智能服务，针对 AI 计算资源（CPU/GPU）提供高效的资源分配、管理和监控。集成业界流行的计算框架实现数据的推理和训练。

容器大数据 AI 集群服务：集群服务可以方便快捷的为用户提供租户级的 AI、大数据、容器集群服务，集群服务可以基于虚拟机或者裸机的形式统一由云平台供应。让用户从集群的复杂部署和运维困境中解脱出来，为用户应用持续创新带来很大的便利。

运营服务：实现对统一用户权限管理、VDC 管理、操作审计、计量计费、流程审批等功能，现云服务的统一运营，云平台统一管理、维护和配置。

运维服务：实现平台统一的运维管理，提供针对平台资源、系统服务、业务虚拟机、业务容器等的统一监控告警功能，提供系统日志和应用日志的集中索引分析功

能，提供基于多种算法的趋势预测、无阈值检测、根因分析等智能运维功能。

统一 LCM 服务：统一可视化生命周期管理以图形交互式向导完成多云建设和管理。多云管理建设可以完成云平台软件的安装部署与扩容改配，通过统一标准完成系统部署，提高云平台交付速度，使交付变得顺畅容易。

资源池管理：提供对 OpenStack、容器、公有云资源池的接入，为上层各类服务提供基础。

3 产品特点

3.1 开放

3.1.1 源于开源，优于开源

开源 OpenStack、Kubernetes 等技术框架已经成为私有云事实上的行业标准，是行业云构建的优先选择，InCloud OS 始终坚持“源于开源，优于开源”的产品构建理念，依托开源构建区别其他厂商的差异化商业产品和服务，将开源技术商业产品化，充分吸收开源技术方向的引领和指引，加强对于技术源头的掌控能力，加大 OpenStack 开源技术的投入和社区的参与，浪潮在社区贡献的 5 项关键指标中均位列中国第一；充分融合发挥浪潮体系的竞争力，形成“人无我有、人有我优”的差异化竞争能力，我们的产品规划需要聚焦核心客户场景，真正解决目标客户群体的核心痛点，为客户提供浪潮特色的有效解决方案。

3.1.2 坚持分层解耦、架构开放，避免厂商绑定

InCloud OS 坚定的走开放路线，推进分层解耦，持续夯实云平台能力，通过平台发展生态，构建有竞争力的行业解决方案，产品通过多项云标准化测评，从产品功能、方案能力等方面达到国家标准要求，能够满足行业客户对于云计算相关技术的专业要求，符合安全可控的行业标准，提供面向下一代云数据中心和云原生应用的智算中心云操作系统。产品持续强化开放、广泛兼容的平台竞争力，北向可被多个 PaaS、SaaS 厂商兼容，南向兼容主流存储及 SDN 厂商，东西向兼容第三方安全、灾备产品等；基于开源架构实现了从不同芯片架构到不同虚拟化技术（裸机、虚拟机、容器），以及不同应用场景的全面支持；开放标准能够实现标准化、模块化“装配式”建

设，提升智算中心建设效率；对外提供社区标准 RESTful API，为客户提供在现有平台功能上进行二次开发能力，开放架构让不同的智算中心能够互联互通，在管理上互操作、业务上互连接和数据上互流通。

3.1.3 平台+生态战略构建完善的生态体系

产品一直践行“平台+生态”的战略，未来智算中心操作系统是多种算力共享、多种服务共存、多种场景同时支持的多样化系统，加强同合作伙伴之间的联系与合作就变得尤为重要，支持与不同的硬件（芯片、存储、网络）、软件（中间件、数据库、ERP、办公）及 ISV 合作伙伴广泛合作，不断推进云图生态建设。

构建支撑云图体系的 InCloud Lab，与合作伙伴在技术创新、方案孵化、场景优化方面，进行全方位的深度合作，支撑产品在云计算、大数据、人工智能等前瞻性技术研究领域，与合作伙伴及客户进行方案创新、孵化和开发，联合推出经过严格验证的行业云整合方案，保证方案的落地性和可实施性。

产品支持纳管多种异构处理器架构的云平台，支持部署在异构处理器架构的服务器，支持 X86、飞腾、龙芯等处理器架构平台。

采用分层安全加固设计，从 Hypervisor 系统、虚拟机和业务访问等维度对云平台进行安全加固。基于三方安全合作伙伴，可为云平台及租户提供虚拟防火墙、堡垒机、漏扫、日志审计等以 VM 方式运行的安全资源服务，支持有/无代理杀毒，保证客户业务数据安全；访问控制、统一用户管理与特权用户权限管理、多租户环境下资源隔离、虚拟网络安全防护、镜像完整性保护、虚拟平台运行时完整性等保护措施实现边界防护，能够快速提升整体安全水平，减少安全风险。

3.1.4 大规模场景支撑能力

在大规模集群环境中，性能、可用性、功能性等方面出现的波动很有可能对整个行业云数据中心的运行带来影响，集群升级扩容是否平滑、平台运行是否稳定高效、性能是否能够满足业务需求等都将成为用户关注的重要问题。基于开源技术的大规模行业云对于基础设施的构建与优化提出了新的要求。首先，开源应用的快速增长带来了工作负载的提升，越来越高的开源技术堆栈对性能带来了极大的影响，在大规模行业云中，这种影响尤为突出。行业云基础设施需要提供超高的数据处理与存储性能，以满足关键应用的需求，并为数据管理、模型训练、模型部署等高负载应用提供支撑。敏捷基础设施成为重要趋势，大规模的行业云将千倍放大单节点的成本支出，因此，对于性能进行持续优化、并增强成本的控制能力至关重要，需要在软件定义层面实现性能、QoS、TCO 的轻松调配。

基于大规模行业云的应用及运维特点，InCloud OS 在功能性、可靠性、安全性、支撑工具等方面全面优化了 OpenStack，全面优化各领域核心组件，并根据实际需求自研了部分组件，解决了开源架构下各种模块与组件的不足，InCloud OS 在单一集群部署规模上不断突破，助力用户构建简单、高速、高可扩展的开源云基础设施，以支撑快速、灵活和大规模的业务创新与部署，借助先进的数据中心架构，核心业务实现了弹性计算资源及稳定的平台，保证了服务的高可用、高性能、可扩展，有效提升数据中心运维保障效率。

产品在金融、广电、政府、能源等多个行业中实现大规模私有云落地：

- **落地某大行近 2000 节点最大规模生产金融云**：经过三年多的持续建设，目前总体规模接近 2000 节点，涉及两地三中心，业务持续上云，目前已承载

60%交易业务，整体运行稳定，2019 年双十一承载峰值 9000 万笔。

- **落地 2000+节点全国最大规模的创新云平台 :**通过全省“一朵云”的建设模式，完成全国首个支撑省、市、县三级的创新政务云平台的建设，该项目同时纳管飞腾、鲲鹏、龙芯等国产化 CPU 服务器，提供包含虚拟化、容器、微服务、开发平台、云管理平台等全栈云服务，支撑应用系统的迁移、适配、上线。
- **落地广电行业 1500 节点大规模云平台 :**两地三中心云平台架构，一期规模近 1500 节点，首批支撑 5 大核心业务；单集群突破 1000 台服务器规模，业界前二；深度融合统一 SDN 及安全服务链。

3.2 敏捷

3.2.1 面向未来应用的云原生平台

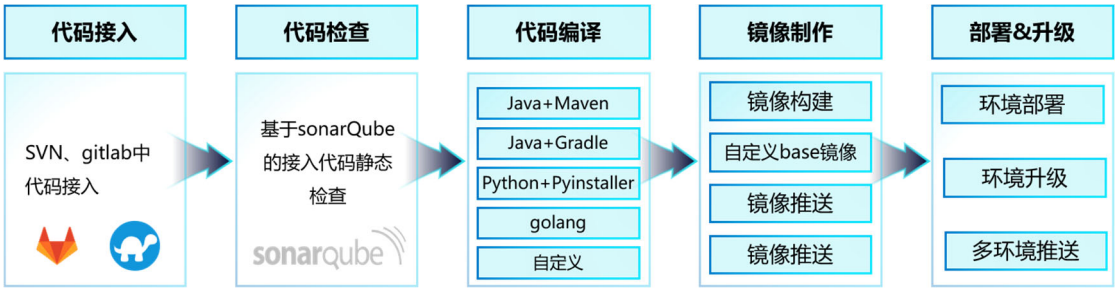
以简化企业应用管理为设计理念，提供基础设施管理能力，提供应用市场、持续集成、持续发布、弹性伸缩、智能监控、多集群管理等功能特性，屏蔽基础运维架构，使客户更专注于核心业务，缩短业务上线周期，优化资源利用率，提高服务响应效率。满足客户应用高可靠及高安全等各种场景。云平台在容器调度、容器网络和存储方面，为客户提供了高效快速、灵活便捷、持久可靠的解决方案。同时支持多集群管理，保证了故障迁移，使企业能快速有效并低成本的跨区域、跨平台运行集群，保证工作负载的不间断运行，最大程度地实现了集群的容灾和多活。

DevOps 特性：

- 一站式容器化交付：基于代码源自动完成代码编译、镜像构建、灰度发布、

容器化部署流程。对接已有 CI/CD，完成传统应用的容器化改造和部署。

- 高效流程管理：更优的流程交互设计，脚本编写量较传统 CI/CD 流水线减少 80%以上，让 CI/CD 管理更高效。
- 灵活的集成方式：提供丰富的接口便于与企业已有 CI/CD 系统进行集成，灵活适配企业的个性化诉求。
- 高性能：全容器化架构设计，任务调度更灵活，执行效率更高。
- 微服务治理 :实现各个微服务实例的自动化注册和发现 ,构建微服务度量能力，支持微服务的健康度分析、故障定界定位、容量规划、根因分析、趋势预测等，支持服务限流、降级、容错、弹性伸缩、安全管控等管控手段，通过应急预案、故障演练、混沌工程等稳定性能力建设来来提升线上微服务的可靠性。



DevOps

3.2.2 可视化蓝图编排

实现对云资源组件 (包括：云主机、网络、子网、安全组、浮动 IP、端口、路由器等) 及脚本、自定义软件的可视化的抽象建模，通过界面拖拽的方式，形成一系列资源组件以及组件之间关系的拓扑结构模型，并结合服务实例功能实现了一键式开通的服务模式。支持图形化拖拽进行编排，简化客户操作；支持多种应用混合编排，

如数据库、中间件，满足应用的各种要求。

InCloud OS 将应用作为一个整体，以应用的服务和管理为核心，提供灵活丰富的编排服务，可以自动生成所需资源和服务，进一步提升云服务的便捷性和易用性。

3.2.3 高效的业务支撑

支持在不影响用户业务的情况下，产品允许动态为云主机增加如 VCPU、内存、磁盘容量等规格，从而实现云主机计算资源的在线向上调整，极大满足了不中断业务情况下实时扩容的场景需求。

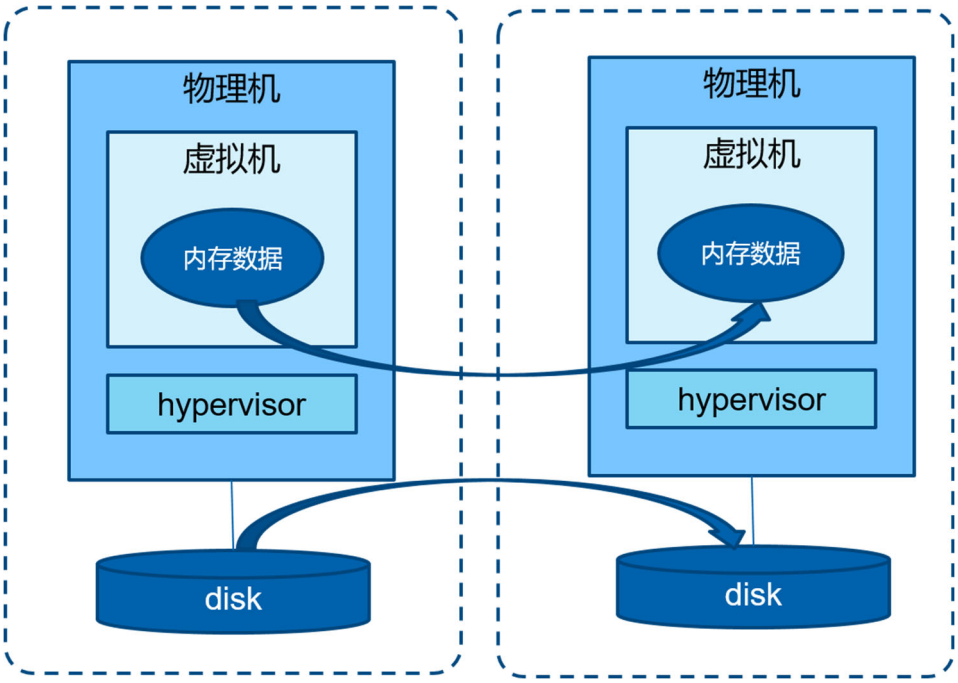
根据用户的业务需求和策略可以自动调整资源，在业务需求增长时无缝增加资源以满足计算需求，在业务需求下降时自动减少资源以节约成本，进而提高用户的资源使用效率，支持资源弹性应对业务负载。

灵活的运营支持，根据自身业务情况，灵活添加资源类型、流程节点以及审批人；支持灵活的自定义流程，支持串行、并行审批流程；实现订单历史全称可追溯，各审批环节实时提醒；精细化运营管理，针对资源的计量计费细粒度至小时级别，并提供多维度的报表导出，供运营者分析；支持自定义报表，用户可按照实际的应用场景自定义数据报表信息，并对报表进行直观的展现、导出。

3.2.4 支持灵活的跨云迁移

产品提供跨云迁移能力，为用户提供跨多个云平台进行各类云资源统一管控的功能，可实现 VMWare 向云平台迁移，以及不同 InCloud OS 数据中心互相迁移，当某个物理主机资源竞争非常激烈而其他物理主机资源空闲率高时，用户可以选择在线将压力较大的云主机迁移到合适的物理主机上，可以高效的调度资源：

- VMWare 虚拟机向 InCloudOS 一键在线迁移，全过程无人工干预，业务无感知 ,帮助用户把原有的 VMWare 平台资源 ,便捷地迁移到现有云平台中。
- 支持跨云迁移虚拟机，打破平台界限，使得不同平台版本，不同地域的数据中心资源的维护与更加便利。虚拟机迁移支持在线迁移和离线迁移。
- 平滑迁移：免代理、不停机在线迁移，最大程度消除业务风险。
- 广泛兼容：兼容 VMWare 多版本（6.0、6.5、6.7 等），兼容市面上主流 Windows、Linux 操作系统。
- 简单易用：提供友好的交互界面，虚拟机一键迁移，迁移任务可视化，迁移详细日志记录，提升用户体验。



跨云迁移

3.3 融合

3.3.1 异构算力统一管理能力

支持虚拟机、云物理机、容器资源统一管理，可以有效满足客户对计算资源多种需求场景需求；云物理机可以提供数据库、大数据等高性能场景，容器可以有效帮助客户解决快速开发部署、微服务等业务场景，云主机可以为用户提供传统虚拟化服务。

具备丰富的异构设备加速能力，提供 GPU、NVMe、USB、光驱等广泛的硬件设备的直通接入服务，满足 AI、图像处理、CDN、大数据等场景的使用要求，促进云数智融合发展。

全面的异构 CPU 兼容能力，支持多种 CPU 架构为业务多样化提供最佳算力选择，支持单集群混合统管异构 CPU，极大提高不同业务场景的需求满足度。

3.3.2 支持异构多云管理

支持多数据中心管理能力，能够实现将分布在不同城市、不同地域的数据中心进行统一管理，满足客户资源统一管理、统一运营的诉求，分散的异地数据中心可以协同管理，高效运管；支持跨数据中心的应用和数据保护支撑，保护业务和数据；

支持混合云管理能力，支持对阿里云的虚拟机、网络、对象存储、负载均衡器等资源进行统一管理，集中监控。满足客户私有云和公有云资源统一管理、运营运维的业务需求。

3.3.3 融合的丰富服务目录

目前在服务目录方提供丰富的全栈服务：

提供 IaaS+高级服务，包括了云主机服务、裸机服务、镜像服务、网络服务、VPN、EIP、安全组、负载均衡服务等。

提供云原生服务和 DevOps 服务。

云数据库服务 :提供了基于虚拟化或容器化的数据库服务能力 ,比如 :MySQL、Oracle、SQL Server、KDB、MariaDB 以及国产化数据库（瀚高、达梦、神通、人大金仓、南大通用等）, 同时支持提供 Redis、Mariadb 高可用的集群化服务。

中间件服务：提供了基于虚拟化或容器化的中间件服务能力，可提供 Tomcat、WebLogic 等中间件服务，也可同时提供出包括东方通、中创、宝兰德、金蝶等在内的国产化中间件服务，充分满足用户国产化需求。

大数据服务：大数据服务基于浪潮自研的大数据 Insight 管理平台和多租户 Dataspace 平台提供服务。

云安全服务 :云安全服务 ,基于第三方云安全平台 ,可为云平台及租户提供虚拟防火墙、堡垒机、漏扫、日志审计等以内置服务运行的安全资源服务。

AI 服务：AI 服务基于 AIStation 平台提供，可提供面向人工智能企业训练场景的人工智能开发资源平台。

第三方服务：遵循 Open Service Broker API（简称 OSB API）标准，将各种对象统一进行服务化的封装，允许第三方实现 Service Broker 接口完成第三方服务的

对接。

系统管理员在 InCloud OS 端启用服务后，组织管理员或组织用户即可在租户端申请使用管理员所发布的服务。管理员可以审批该申请，也可以驳回，申请通过之后，租户即可使用自己的服务实例，并可对所拥有的服务实例进行管理。

3.3.4 提供统一的灾备管理能力

支持容灾服务，通过创建保护组的方式实现云主机、存储资源跨数据中心的容灾保护，将需要保护的虚拟机加入到保护组中，设置虚拟机启动的优先级并配置虚拟机容灾保护脚本，当备用虚拟机启动时可以运行容灾脚本，保证备份虚拟机的正常运行，提高业务的高可用性。

通过存储复制，可以实现对一组相同业务的云主机进行异地备份，当生产中心发生灾难时，可在异地灾备中心恢复受保护的云主机，实现对重要业务和数据的保护，实现业务的连续性，数据零丢失，业务不中断。不仅保护业务数据，也能保证业务的连续性。容灾的最高等级可实现 RPO=0。故障情况下（例如地震、火灾），容灾系统的切换时间可降低至几分钟。

多种级别的策略和管理功能确保不同的租户、业务能获得适当的灾备能力。针对租户的虚拟机、卷等资源细粒度备份可实现精细的用户业务连续性，定时任务、手动触发等能力保证灾备的实时性。

3.4 智能

3.4.1 云数智融合管理

InCloud OS 为用户提供了强大的云数智融合管理能力，将云、数、智进行打通；

InCloud OS 基于服务目录提供大数据处理服务、AI 训练理服务，实现了在云平台上快速构建 AI 和 InsightHD 开发环境和运行环境，为 AI 和 InsightHD 等新兴业务场景提供安全可靠的云基础设施平台，InCloud OS 坚持“融合、智能、敏捷、开放”的原则，能够将管理复杂性降低 30%；数智融合有效帮助 AI 计算效率提升 20%，将数和智数据上进行打通。

AI 服务基于 AIStation 平台提供，提供面向人工智能企业训练场景的人工智能开发资源平台，InCloud OS 服务目录可无缝接入用户已部署的人工智能平台（AIStation），为上云用户提供开发环境、训练任务等一系列 AI 服务，拉通用户开发环境、计算资源、数据资源，构建一体化 AI 开发平台。

大数据服务基于浪潮自研的大数据 Insight 管理平台和多租户 Dataspace 平台提供服务，InCloud OS 服务目录可快速接入用户已部署的一个大数据分布式计算环境（Insight），为上云用户提供 Hadoop、HBase 等一系列大数据服务。

3.4.2 智能化的运营分析

运营优化建议：针对集群、宿主机、云主机和存储等的优化建议和资源分析，参考指标包括 CPU 使用率和内存使用率，以最近三天的监控数据作为采样数据，自动识别使用率低的闲置资源，自动发现负荷过高的资源，建议管理员及时对集群、宿主机、云主机和存储及时进行扩容或减容。

运营趋势预测：预测资源池的未来使用趋势，为管理员运营提供参考，参考指标包括 CPU 使用率、内存使用率、存储使用率等。智能评估云平台、集群等资源的可支撑时间，以图形化方式展示预测曲线，协助管理员拟定扩容计划。

3.4.3 可预见的智能运维

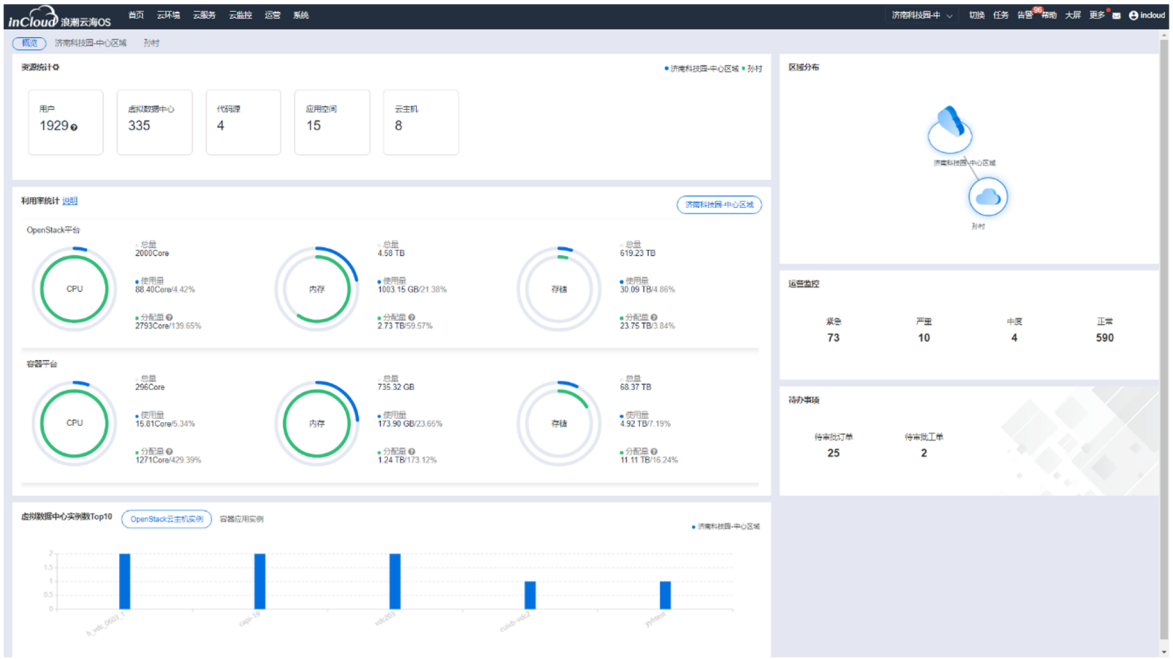
产品支持预见性智能运维模式，通过可视化、图形化数据展现模式，实现清晰认知现在精准预知未来，满足大规模数据中心智能运维需求，提高用户使用体验。支持智能监控，目前已经覆盖了 OpenStack 平台、虚拟化平台、容器平台、公有云平台，包括云主机、主机、文件系统、CPU、内存、磁盘 IO、网卡等监控项，准实时、细粒度的监测项设置，自定义的阈值、告警通知设置，让用户随时随地了解业务系统运行情况，异常情况预先告警，有效降低业务宕机风险。

4 产品功能

4.1 起始页&大屏

InCloud OS 拥有优秀的 UI 视图，为用户提供易用性极佳的使用体验。起始页与数字可视化大屏应用图形化显示模式，集中展示与集群资源相关的 CPU、内存、存储等使用情况，直观反映云平台运行态势，增强用户体验。

起始页，展示系统整体的资源情况、告警情况、待处理事项及常用操作入口。一云多芯场景下支持展示不同资源池下的架构集群资源统计信息。多地域（region）部署情况下可以在首页自由切换使用 region，统一展现不同地域资源使用情况，最大限度提升运营管理员运营效率。



为适配客户大屏展示需求，方便客户方领导快速了解云平台的建设、运行情况，浪潮云海 OS 针对客户实际使用场景进行充分调研，设计开发了虚拟资源、容器资源、监控三个大屏展示功能，从全局视角对系统资源总量、使用情况、告警信息进行

展示。

虚拟化大屏

监控大屏

提供 C/S 客户端的下载，C/S 客户端可用于对 OpenStack 平台内云主机的简单管理，包括：查询、开/关机、删除、访问控制台。

4.2 云环境

4.2.1 OpenStack 平台管理

对 OpenStack 平台类型的物理资源、网络资源、存储资源等进行统一管理，包括资源池(可用分区、主机、裸机、云主机管理、云物理机管理)、虚拟网络管理(VPC、网络、路由器、防火墙、负载均衡、浮动 IP、安全组)、存储管理 (存储池、云硬盘、文件存储、镜像)、快照&备份管理、密钥对管理、云主机规格管理等全面的管理功能，管理人员可将通过直观的操作面板，对虚拟化平台云资源进行创建、分配、编辑等操作。

OpenStack 平台管理

4.2.1.1 资源池管理

资源池是面向物理资源划分的概念，如一个虚拟化资源池是指共享一套 API 节点 (控制节点)、数据库节点和消息队列节点的物理服务器资源，包含控制节点、数据库节点、消息队列节点、计算节点、网络节点、存储管理节点等不同类型的角色。

管理资源池以提供 OpenStack 资源与服务，包括添加、修改、更新访问凭证、移除等功能，当资源池被移除后，无法使用其集群资源新建 VDC、云主机等。

可查看资源池的详情信息：

基本信息：可查看资源池的名称、状态、IP 等基本信息。

性能曲线：可查看当前资源池的资源使用情况，包括 CPU、内存、存储和网络的使用情况。

历史曲线：可查看当前资源池的历史资源使用情况，包括 CPU、内存、存储和网络的历史使用情况。

- 主机：可查看当前资源池下的主机列表信息。
- 可用分区：可查看当前资源池下的可用分区信息。
- 主机组：可查看当前资源池下的主机组信息。
- 主机 HA：可查看当前资源池下的主机 HA 信息。
- 虚拟数据中心：可查看当前资源池下的虚拟数据中心信息。
- 云主机：可查看当前资源池下的云主机列表信息。
- 服务列表：可以选择并查看 OpenStack 服务，包括 Nova 服务、Cinder 服务或者 Neutron 服务等。
- 任务：可查看当前资源池的任务记录。
- 操作日志：可查看当前资源池的操作日志。
- 资源审计：可查看当前资源池的资源审计信息，记录操作时间、操作者、操作的具体内容。

支持对 Openstack 资源池的添加、修改、移除和更新访问凭证。

可用分区管理

可用分区是用云规划的一个物理概念,可以简单理解为一组节点的集合,这组节点具有独立的电力供应设备,比如一个个独立供电的机房,一个个独立供电的机架都可以被划分成可用分区。在同一地域下,电力、网络隔离的物理区域,可用分区中的计算、存储、网络资源是全互通的。

主机管理

主机是运行了虚拟化软件的物理服务器，用以运行云主机。主机为云主机提供 CPU 和内存资源，以及网络连接和存储访问等能力。云平台提供了基于 IPMI 技术的主机生命周期远程控制能力。这些远程控制包括开启主机、关闭主机、重启主机、配置 BMC、开启/关闭服务、进入/退出维护模式。主机远程控制使用户不需进入机房，通过云平台就能轻松管理主机，提高了运维效率。

主机组管理

主机组是根据硬件资源的某一属性对指定可用分区中的主机划分的分组，比如按照地理位置分组、按照是否使用固态硬盘分组等等。

主机 HA 管理

主机 HA（高可用）是为了限定故障转移的范围而设定的主机集合。当集合内某个或多个主机故障时，可按设定的策略将故障主机上的云主机迁移到集合内其他正常的主机上运行。支持主机故障聚合分析,在发生故障时能够按照主机或云主机聚合规则进行故障恢复。

外部网络

外部网络是用于连接系统外部网络,以实现系统内外通信的网络,网络类型支持

FLAT、VLAN、GENEVE。

在外部网络列表中可创建、修改、删除外部网络。

外部网络详情页上可查看该外部网络的基本信息、IPv4 或 IPv6 地址配置信息、虚拟或预留 IP 地址、操作日志等信息；可对预留 IP 地址进行配置管理。

4.2.1.2 存储池管理

管理运维存储池、云硬盘、镜像、文件存储下的相关存储资源。

存储池是统一给云硬盘、镜像、文件存储、对象存储提供存储空间的地方，在这里会划分出对个不同类型、不同性能规格的池子给不同资源去使用。

云硬盘存储池管理

云硬盘存储池是为云硬盘提供存储空间的后端存储，支持划分出多个不同类型、不同性能规格的存储卷给不同资源使用。

云硬盘资源池在平台部署时进行配置，支持云硬盘存储池的查询、删除和设置资源等级以及详情等功能，以方便云硬盘存储池的运维和使用。

利用资源标签设置云硬盘存储池资源等级：不同性能的云硬盘存储池对应不同的资源等级，管理员可根据实际的物理环境配置，为云硬盘存储池指定对应的资源等级。

文件存储池管理

文件存储池展示 OpenStack 中文件存储服务状态的 SDS 信息。

平台提供文件存储池的查询、启用、禁用、删除 SDS 信息以及详情等功能，以

方便文件存储池的运维和使用。

4.2.2 容器平台管理

4.2.2.1 资源池管理

容器资源池(即容器集群)是容器化的管理系统 ,是容器运行所需云资源的集合。它由若干工作主机 (云主机或物理机)、负载均衡、网络等资源组成 , 为容器化的应用提供了资源调度、部署运行和服务发现等丰富多样的功能。

支持多架构、多版本、多资源池的托管服务 , 用户可以在 OpenStack 资源池中创建容器资源池 (即非自定义资源池), 也可通过资源池证书配置实现与自定义资源池的对接及统一管理 , 并实现资源池弹性伸缩、主机管理、组件监控、存储类型对接等功能特性。

支持集群类型：

- 多架构：支持 X86、ARM64 等多种架构服务器，且支持混合架构。
- 多资源池：可将不同资源池分配给不同组织使用，满足容器云多资源池场景。
- 多版本 : 实现对多种版本 Kubernetes 资源池的纳管 , 以兼容用户已有资源池。

资源池管理：

- 支持查看资源池基本信息、组件状态、健康检查以及资源使用情况等信息
- 主机列表：支持查看资源池中工作主机的信息，并进行主机管理。

主机是组成资源池的基本元素，主机取决于业务，可以是云主机或物理机；每个主机中都包含运行容器组所需要的基本组件，包括 Kubelet、Kube-proxy 等。

支持查看主机标签，主机的状态、IP 地址、调度、操作系统类型的主机详细信息，查看主机中资源的使用情况及该主机的运行状态，支持查看运行在该主机上的容器组及容器信息，支持查看主机事件信息，主机节点支持配置 NUMA 亲和。

调度管理功能，可支持开启、关闭主机调度。

标签管理：标签是 k8s 特色的管理方式，便于分类管理资源对象。一个标签可以对应多个资源，一个资源也可以有多个标签，他们是多对多的关系。通过管理节点标签，可以在部署时配置按照节点标签进行调度。修改标签会影响到已经配置该标签进行节点调度的资源。支持添加、修改、删除标签。

- 存储池：支持查看资源池内可用存储池（hostpath 存储池除外）的数据信息。
- ETCD 监控：支持查看 ETCD 监控信息，包括 ETCD 主机、底层数据库大小、客户端接收/发送的流量等等。
- ETCD 是一个分布式、可靠 Key-Value 存储的分布式系统，提供配置共享和服务发现功能，用于维护和保持整个资源池内各工作主机的状态。
- API Server 监控：支持查看 API Server 的监控指标数据，即请求延迟和每秒请求数。
- API Server 是整个资源池管理的 API 接口和资源池内部各个模块之间通信的枢纽。
- 调度器监控：支持查看资源池调度器的监控指标，包括调度次数、调度速率

和调度延迟。

- 组件状态：可查看资源池中监控、日志、资源池等各项服务组件的健康状态监控情况，用户可按需重启服务组件或查看其运行日志。
- 插件实例：可查看当前资源池中已部署的插件实例，即扩展性功能。
- 当不再使用的某个扩展功能时，可通过“卸载”按钮卸载指定的插件实例。
- 健康检查：提供对用户在资源池中自定义应用空间内的各类资源状态及运行情况的健康检查服务，检查报告详细展示各检查类别内各工作负载状态和配置的检查内容。若出现异常项，自动分析异常级别、异常原因并给出修复建议。

支持查询、查看运行资源池，支持查看平台运行概览，查看平台运行中资源和用量的统计信息。查看主机列表、节点详情；支持查看运行环境中的虚拟数据中心信息；支持查看和管理存储类型；支持修改资源池，仅支持修改运行环境的名称和描述信息；支持删除资源池，不允许删除已被绑定的运行环境；支持资源池的扩（缩）容；基于 OpenStack 资源池创建的容器资源池，支持自动弹性伸缩，同时能够查看伸缩记录。

支持导入资源池，提供直连纳管和代理纳管两种模式。如果 CMP 可以直接访问 K8S 集群 kube-apiserver 地址，则可以采用直连纳管。如果 CMP 无法直接访问集群 kube-apiserver 地址，但是容器资源池可以访问 CMP 地址，则可以采用代理进行纳管。

导入资源池

主机管理

主机（Node）是应用实例（Pod）运行所在的工作主机，为资源池提供计算能力，可以是物理机也可以是云主机。

主机分为可用和不可用两种类型。其中，可用包括可调度、关闭调度、进入维护模式中、维护模式四种调度状态；不可用对应不可用状态。

可调度：主机能够正常提供服务，调度器可以将容器调度到该主机运行。

关闭调度：主机能够正常提供服务，但调度器不能将容器调度到该主机运行。

进入维护模式中：指用户进行进入维护模式操作的中间状态。此状态下，主机能

够正常提供服务，但调度器不能将容器调度到该主机运行。

维护模式 :指用户对当前主机进行诸如操作系统版本升级、硬件维护等业务场景的操作 ,对当前主机进行进入维护模式操作。此状态下 ,主机也能够正常提供服务，调度器不能将容器调度到该主机运行。

不可用：主机所在的物理机或者云主机存在故障、网络异常不可达等业务场景时，主机 kubelet 服务不可用的状态。

主机详情页面内可以查看主机的概览、运行状态、容器组、事件、历史曲线，也可以进行相应的调度管理、标签管理以及维护模式的进入。

4.2.2.2 存储池管理

存储池统一为块存储、文件存储和本地存储等提供对接存储资源池和存储空间；存储池支持对接多种类型的存储，包括分布式存储、集中式存储、本地硬盘等；根据存储的提供形式将其分为块存储池、文件存储池和本地存储池 ,可以划分不同类型、不能性能规格的存储卷给不同资源使用。

支持块存储池、文件存储池、本地存储池的创建、管理等操作。

块存储池

为用户提供块存储系统，支持对接的存储池包 Inspur AS5300G2、Inspur AS5500G5-C、InspurAS13000 块存储、OpenStack 块存储、SDS-X 存储。其中，OpenStack 块存储仅为非自定义容器资源池提供存储服务，其他类型的存储池仅为自定义容器资源池提供存储服务。

块存储池（SDS-X 除外）支持配置文件系统类型。

文件存储池

为用户提供文件存储系统，目前仅支持对接的存储类型为 Inspur 高速共享存储。另外，非自定义资源池不支持文件存储服务。

本地存储池

为用户提供本地存储系统，支持对接的存储类型为 hostpath。

4.2.2.3 插件管理

安装部署系统时，默认只安装部署平台的核心组件。插件管理用于管理容器资源池的扩展功能，以支持选择性扩展满足特定需求的功能。在插件中心中已为用户集成了一组基于 Chart 的编排镜像，包括微服务组件、日志组件、存储组件等。管理人员可根据实际业务需求，安装上述扩展组件，以提供相关扩展功能。在插件实例中支持对于已部署的浪潮分布式存储/浪潮集中式存储插件实例修改。部署 MetalLB 时，支持配置多个网段，MetalLB 支持 BGP 模式，支持根据节点标签进行调度。

部署插件：可支持对应资源池方能提供相应的扩展功能。

卸载插件实例：资源池底层环境中删除该组件，其所对应的功能模块不可使用；其中，卸载存储类插件时请先删除资源池下对应的存储池；卸载微服务插件时请确保当前资源池下不存在启用服务治理的应用；支持修改已部署的浪潮分布式存储/浪潮集中式存储（IP-SAN 和 FC-SAN）插件实例。

4.2.3 虚拟化平台管理

InCloud OS 可实现异构虚拟化管理，包扩 VMware Sphere 5.5 及以上版本、自研服务器虚拟化产品 InCloud Sphere V6 版本 ,可通过添加 VMWare vCenter、Inspur iCenter 等实现资源池的添加 ,通过统一视图为用户展示虚拟化资源池中资源(集群、主机、云主机）的使用情况。

4.2.4 大数据平台管理

InCloud OS 可对大数据平台类型的物理资源、网络资源、存储资源等进行统一管理，通过添加大数据资源池，以提供大数据服务，目前仅支持浪潮 Insight。

4.2.5 AI 平台管理

InCloud OS 可对 AI 平台（AIStation）类型的物理资源、网络资源、存储资源等进行统一管理 ,支持添加 AI 资源池 ,以提供人工智能服务 ,目前仅支持浪潮 AIStation。

4.2.6 公有云平台管理

用户再资源池添加公有云（阿里云）环境，阿里云输入对应 AccessKey ID、AccessKey Secret 即可将云环境接入到平台管理，进行云主机、网络、LB、对象存储等虚拟资源管理。

支持公有云环境的添加、修改、更新访问凭证、移除等操作。

4.2.7 对象存储平台管理

对象存储平台提供对平台物理存储和对象存储的管理。物理存储是指将已有的存储系统（AS13000）添加到系统中，为用户提供对象存储资源。对象存储是提供对象存储账号配置管理功能，为用户分配对象存储空间。

4.2.8 平台设置管理

可在此模块对 OpenStack 云主机的快照和备份保存策略、生命周期到期提醒及处理策略进行配置管理。

生命周期

可以对云主机生命周期到期时的提醒策略及处理方式进行统一配置。

支持云主机生命周期策略配置，配置云主机生命周期到期的提醒方式：邮件提醒，短信提醒。

备份设置

通过备份设置对云主机备份保存策略进行配置管理。

支持设置 OpenStack 云主机备份保存策略，当定时备份的数量超出限制时，系

统将自动删除创建时间最早的定时备份。

支持设置云硬盘全量备份保存策略，当备份的数量超出限制时，系统将自动删除创建时间最早的定时全量备份。

快照设置

通过快照设置对云主机快照策略进行配置管理。

支持设置云主机快照保存策略，当定时快照的数量超出限制时，系统将自动删除创建时间最早的定时快照。

云硬盘快照保存策略

当定时快照的数量超出限制时，系统将自动删除创建时间最早的定时快照。

4.3 云服务

4.3.1 计算管理

4.3.1.1 云主机管理

云主机管理模块提供云主机以及云主机模板的创建、操作、管理等功能。C/S 客户端支持云主机查询、开/关机、删除、访问云主机控制台功能。

创建云主机

多样化云主机来源，可通过镜像、云硬盘、云硬盘快照、云主机快照创建云主机。在创建云主机的过程中可以对系统盘进行配置，支持设置系统盘的大小、存储等级、卷类型、系统盘删除策略；也可以对相应网络进行配置，支持自定义网络和网络配置模板、指定 ip 地址、指定端口、mac 地址、网络 QOS 策略；通过镜像创建云主机

时，可选择是否创建云硬盘。

创建过程中可以配置云主机的虚拟数据中心、用户、资源池、可用分区、主机、主机等级、标签、数量、描述信息等；创建时使用原密码、修改新密码、随机密码、注入密钥；支持创建过程中“创建新云硬盘”，也可以“指定云硬盘”；支持用户自定义系统规格、元数据、QoS，挂载 vmtools 工具，并且提供可视化的方式挂载文件存储。

云主机 SLA

云主机 QoS，在使用云主机的过程中，同一个物理主机或者同一个聚合内的多台云主机如果读写负荷较大，可能会导致其他云主机因为抢占不到资源而运行卡顿，从而影响业务的正常运行。InCloud OS 提供针对 CPU、内存、磁盘、网卡的 QoS 设置，用户可以根据业务场景的不同设置不同的 QoS 规则，从而保证不同类型的云主机根据业务场景可以获取不同的资源。

云主机在线扩容，在不影响用户业务的情况下，InCloud OS 允许动态为云主机增加如 VCPU、内存、磁盘容量等，实现云主机计算资源的在线动态调整。该功能满足了在业务场景要求高、不能中断情况下实时扩容云主机的诉求。

云主机安全

平台提供在创建云主机时设置蓝屏策略，用来处理云主机发生蓝屏事件的场景，预先设置好蓝屏策略，当云主机出现蓝屏时，云平台自动相应，支持“关机”和“重启”设置。

云主机安全配置：从镜像、云主机快照创建云主机支持多种登录方式，使用来源原始密码、密钥对、指定密码、随机密码。

云主机密钥对功能主要用于安全登录云主机的场景，用户需要提前准备好密钥对，使用密钥对有两种方式，可以在创建云主机时选择密钥对，也可以在云主机创建成功后在线挂载、卸载密钥对。

在云主机使用过程中，用户可能需要在不影响正常业务的情况下修改云主机密码，并且一台云主机可能有多个用户角色权限，在修改某个用户密码时，不能影响其他用户正常访问，为此 InCloud OS 开发了在线修改云主机用户密码功能。

快速创建云主机

可以通过快速创建云主机方式，批量分发云主机，可指定云主机所属不同区域数据中心，实现一键资源分发，满足边缘场景下，中心节点和边缘节点资源快速分发的需求。

模板创建云主机

支持通过导入配置文件（yaml 文件或 Excel 文件）来快速创建云主机，并提供对应的快速批量模板。

来源为镜像、云主机快照时，指定创建新的云硬盘时，可指定云硬盘存储等级，例如指定“高速”存储等级，创建的云主机硬盘会自动调度到高速存储上，实现存储资源管控。

可视化规格选择：支持选择 CPU、内存、硬盘规格。

网络配置：可指定特定网络创建云主机，IP 分配可指定静态 IP 或者 DHCP 方式。

云主机生命周期管理

可对云主机执行开启、关闭、强制重启、挂起、恢复、暂停、取消暂停、重建、重命名、克隆、删除、配置 SN 号（序列号）等生命周期管理。

暂停：暂停状态时不能提供服务。且暂停状态的云主机可以通过恢复操作，快速恢复为暂停前的状态。运行在云主机中的进程并不能感知自己被暂停过。

挂起：云主机的挂起状态与暂停状态很相似，暂停是将云主机的状态保存在内存中，而挂起是将云主机状态保存到硬盘中，云主机占用的主机资源已经释放。

重建：用选择的镜像或快照更新云主机，更新后的云主机中的业务数据为所选择镜像或快照中的业务数据。

云主机更改生命周期

可修改云主机到期时间，当云主机到期后可按照平台中设置的回收策略对云主机进行处理。

更改所有者

具有更改所有者权限的管理员可以更改云主机的所有者，并将云主机指定给某个用户使用。

更改云主机配置

- 对开机或关机状态的云主机的规格进行更改。
- 云主机开机状态下，CPU 和内存不支持减小。
- 云主机开机和关机状态下，硬盘都不支持减小。
- 云主机来源为云硬盘时，更改配置无法更改硬盘大小。

云主机 CPU 绑定

CPU 绑定是将用户云主机 vCPU 直接绑定到物理服务器的 CPU 上，从而改善云主机的 CPU 调度精确度并提升云主机的性能。当启用 CPU 绑定后，云主机将被限定在宿主机的某些特定 CPU 上，以提升云主机的性能，对于 NUMA 类型的云主机，CPU 绑定使得进程仅访问就近内存，提升性能，避免进程之间相互影响，比如防止繁忙的进程过多的占用资源，影响其他的进程。

云主机大页内存

随着计算需求规模的不断增大，应用程序对内存的需求也越来越大。为了实现虚拟内存管理机制，操作系统对内存实行分页管理。Linux 默认内存页大小为 4KB，如应用内存较大，则需要加载的内存页较多，导致内核加载更多的映射表，引起性能下降。

支持的内存页大小依赖 CPU 支持特性。

异构设备加速

异构加速设备直通是把物理服务器上的加速设备，包括 GPU、FPGA、NVMe SSD 等资源直通到云主机上使用，使得云主机可以拥有高计算、快存储的处理能力。用户可以在创建云主机的时候选择加速器规格，加速器规格中包含 GPU、FPGA、NVMe SSD 等一系列加速资源的组合，也可以对已有的云主机执行绑定、解绑加速器设备的操作。

加速器设备直通要求云主机绑定的加速器设备必须是所在计算节点的物理资源，因此所有涉及到云主机更改所在计算节点的操作都不被允许，否则会因为绑定不到加速设备而启动失败。所以对绑定有加速设备的云主机暂时不允许的操作有暂停、挂起、迁移、在线迁移、更改配置、重建、疏散等。

当对绑定有加速器设备的云主机进行暂停、挂起、迁移、在线迁移、更改配置、重建、疏散等操作时，平台会予以拦截，给出错误提示信息，不允许用户进行以上操作。

硬盘直通

虚拟硬盘的实现分为全虚拟化、半虚拟化和直通三种方式。这三种方式的特点可以用下面的表格总结。

虚拟硬盘实现方式	示例	优点	缺点
全虚拟化	IDE、SATA、SCSI	兼容性好、灵活	性能差
半虚拟化	virtio-blk、virtio-scsi	性能较好、比较灵活	兼容性一般
直通	PCI 直通、SCSI 直通	性能最好	灵活性差、兼容性一般

当前仅支持服务器本地盘和集中式存储服务。

挂载 ISO 镜像

InCloud OS 支持云主机在线挂载/卸载 ISO 镜像，用户可以将自己的 ISO 镜像文件上传到 InCloud OS 上，然后将镜像挂载给指定的云主机。该功能让用户可以在云主机中，获得相当于使用真实光盘的体验。

一个云主机只允许同时挂载一个 ISO 镜像。

SRIOV 网卡

通过 SR-IOV 网卡可以从虚拟机中动态添加和卸载，可以实现对 SR-IOV 更加灵活地使用和释放。通过 SR-IOV 网卡热添加技术，可以以允许一个虚拟机在

运行中可以同时挂载多个 SR-IOV 网卡；不再使用 SR-IOV 网卡时，可以进行热卸载操作；特别是针对 VFIO 设备资源比较紧缺的情况下，实现 VFIO 设备资源更加灵活的应用。

目前该功能约束条件：

1、保证宿主机上打开 VF 设备，并确保计算服务识别到这些 VF 设备；

2、暂不支持自动获取 IP 信息。

USB 网络映射

USB 网络映射功能可以管理 InCloud OS 集群内所有计算节点上的 usb 设备，相比于 usb 直通功能，不再有云主机只能挂载本主机的 usb 设备的限制，而且挂载网络 usb 设备的云主机支持热迁移、冷迁移、疏散功能。

一个网络 usb 设备只允许挂载给一个云主机。

云主机控制台管理

可连接处于开启状态的云主机 VNC 控制台，在控制台中可操作该云主机。同时支持文本远程粘贴。

云主机快照管理

通过云主机快照、内存快照与还原功能可以实现云主机中云硬盘信息的安全快照。虚拟机生命周期中，通过快照和还原操作，可以对虚拟机数据安全保存和恢复。可以极大提高用户数据的安全性，特别是出现宕机等系统损坏的情况，通过快照恢复功能，可以快速恢复运行业务。以最大程度减少对用户业务的影响程度。

云主机备份管理

云主机整机备份与还原，可以有效对客户云主机系统硬盘数据进行有效保存和恢复,有效避免因为误操作或者黑客攻击导致的数据丢失问题,实现云主机在实际生产运行当中的高可用。

云主机克隆

云主机克隆,可以使客户能够以现有云主机为模板,快速复制出多台相同的虚拟机,也可以先创建一台云主机进行软件和系统配置,然后以该云主机为模板批量的创建出相同规格、属性和状态的云主机,实现了对虚拟机数据、属性以及状态的快速复制。

云主机标签管理

在云主机使用过程中,云主机的数量可能达到成千上万台,且每台云主机有着不同的功能,这就需要对云主机进行区分,如果能给云主机做上标记,这在很大程度上便于对云主机进行管理。

云主机迁移

当某个物理主机资源竞争非常激烈而其他物理主机资源空闲率高时，用户可以选择在线将压力较大的虚拟机迁移到合适的物理主机上,期间并不影响业务的运行，这样可以保证虚拟机更加高效的运行。

支持云主机在线迁移,将一台云主机从一个宿主机迁移至另一个宿主机,而迁移过程中云主机继续执行原有指令而不会中断。受限于每种迁移加速技术都有其约束性，InCloud OS 引入了自适应迁移加速策略，自动识别当前情况下何种加速策略最佳，提升在线迁移的易用性。

约束：

1. 云主机与宿主机存在设备映射时不允许在线迁移，如存在 GPU 直通、大页内存、裸磁盘直通等约束时不允许在线迁移。
2. 目标主机资源不足时，会导致在线迁移失败。
3. 云主机在不同指令集的宿主机之间在线迁移，会导致在线迁移失败。
4. 源主机和目标主机大页内存配置不相同时无法进行热迁移。
5. 跨代迁移时云主机 CPU mode 为自适应模式(qemu 默认的 CPU mode)。

云主机详情查看

- 基本属性：可查看云主机的名称、标签、状态、告警状态、虚拟数据中心、虚拟化类型、操作系统、主机、集群、所有者、创建时间、结束时间、资源域、描述等信息。
- 系统配置：可查看 CPU 核数、内存容量等信息。
- 性能监控：可查看云主机的 CPU、内存、硬盘和网卡使用情况。
- 历史曲线：可查看云主机指定时间段内的 CPU、内存、硬盘和网卡使用情况。
- 快照：可查看云主机快照列表，并支持快照的创建、恢复、编辑、删除以及图形化展示操作。
- 硬件配置：展示硬盘信息和网卡信息。
- 任务：展示云主机相关的任务。
- 定时任务：展示云主机相关的定时任务以及定时任务的创建。

- 资源审计：展云主机相关的资源审计信息。
- 操作日志：展示云主机的操作日志。

可多条件组合查询云主机列表。

更新密码：

支持为“开机”状态的云主机重置虚拟机密码。

重置密码时，请先保证该云主机中已安装 QGA 代理（Qemu-guest-agent），并且 QGA 代理正常运行。

亲和性调度策略

亲和性调度策略主要用在批量创建云主机调度主机的场景中，用户既可以选择亲和性策略，在批量创建云主机的时候，会将云主机调度到同一个主机上也可以选择反亲和性策略，批量云主机将被调度到不同主机上，也可选择按交换机、机柜、机柜列等进行反亲和性、软反亲和性调度，实现业务在交换机、机柜、机柜列粒度的高可用。

在按交换机、机柜、机柜列进行强反亲和性调度时，同一机柜里的主机交换机必须一致，不同机柜可以使用同一个交换机。

多样化调度策略

InCloud OS 支持配置多种资源调度策略保证云主机创建到适合的物理主机上。当前支持通过可用域、主机聚合、CPU 核数、内存大小、磁盘大小、Numa 拓扑、PCI 直通以及亲和性调度等策略进行筛选主机，也支持根据规范自定义分配策略满足主机选择需求，从而能够保证云主机自主创建到合适的主机上。

4.3.1.2 云主机规格管理

云主机规格模块提供云主机规格的创建、修改、删除等功能。

支持云主机和云物理机规格；可设置云主机规格的 CPU、内存、磁盘的 QoS；

可配置云主机规格的元数据。

4.3.1.3 云物理机管理

在某些特定场景下，用户需要更多的硬件访问权以及更高的机器性能，比如，高性能计算服务、数据库主机服务等。业内传统做法是将物理服务器放置在机房。每次对物理机服务器进行开关机操作或者安装操作系统等操作，几乎都需要去机房；缺乏对机器的统一管理和调度，既浪费时间又耗费精力。为此，InCloud OS 提供裸金属服务，直接为用户提供独占式的物理服务器资源，满足用户特定需求的可行性及高效性。

InCloud OS 裸金属服务支持物理服务器的批量模板注册等状态管理；支持裸金属 RAID 配置；批量化电源管理及安装部署；支持对裸金属网卡的网络类型添加标签进行标识；也能够实现对云物理机和云主机的统一管理和调度，实现快速安装系统，实现硬件基础设施资源分钟级快速交付。它支持各种网络类型，能够实现多租户下的网络隔离；IP 分配支持自动分配及手动指定两种方式、裸金属调度支持自动调度及手动指定两种方式，能够广泛应用于高性能计算服务、数据库主机服务等场合。

云物理机生命周期管理

可创建、修改、删除云物理机、对云物理机执行开关机、强制重启云物理机等操作；为云物理绑定浮动 IP、解绑浮动 IP，以便云物理与外部网络互通。

云物理控制台管理

处于运行状态的云物理可以打开控制台，通过控制台直接操作云物理机。

云物理机挂载云硬盘：

InCloud OS 支持云物理机挂载 iscsi 链路以及 FCSAN 协议的云硬盘，以满足当本地物理磁盘不足时，可以灵活地按需挂载远端存储的需求。并且依托于后端存储对共享盘的支持，云物理机也支持共享云硬盘的挂载，实现多台云主机/云物理机间存储共享，大大增强云物理机存储的灵活性及可靠性。同时，InCloud OS 也支持云物理机卸载已挂载的云硬盘，且可选择云硬盘是否跟随云物理机删除。

4.3.1.4 弹性伸缩

弹性伸缩能够根据用户的业务需求和策略自动调整资源，在业务需求增长时无缝增加资源以满足计算需求，在业务需求下降时自动减少资源以节约成本，进而提高用户的资源使用效率，并保障业务健康稳健运行。

弹性伸缩的触发规则

自动扩展：只要满足任意一个增加类型的伸缩规则即可触发。

自动收缩：必须满足伸缩组中所有减少类型的伸缩规则才会触发。

弹性伸缩的执行策略

自动扩展时，检查伸缩组的云主机成员中是否存在关机状态云主机：如果有则开启云主机；若无则按照伸缩组中云主机的配置重新创建云主机，同时将云主机的受保护属性置为否。

自动收缩时，按照伸缩策略优先关闭不受保护的云主机，然后再关闭受保护的云

主机；针对相同状态的云主机，减少云主机时需要遵守云主机减少策略。

弹性伸缩组管理：支持伸缩组的创建、修改、删除、启用、禁用等操作；支持将云主机移入伸缩组，将云主机移出伸缩组，将云主机移出伸缩组并删除云主机，修改已加入伸缩组的云主机；支持为当前伸缩组添加/修改伸缩规则；支持查看伸缩历史，操作日志，审计日志。

- 支持为伸缩组添加多个伸缩规则，可以设置弹性伸缩组的最大最小虚拟机个数、关联的负载均衡器，支持配置虚拟机减少策略。
- 支持伸缩主机配置可选择创建虚拟机的镜像、规格、可用分区、分配用户；
- 支持设置伸缩网络信息，包括网络、安全组等。
- 支持弹性伸缩参数的配置，包括调整方式（增加、缩小）、调整数量、监控时间间隔。

伸缩组管理

- 支持弹性伸缩规则的创建、修改、删除操作；支持查看对应操作日志和审计日志。
- 支持弹性规则触发条件的配置，包括 CPU 使用率、内存使用率。
- 支持弹性伸缩参数的配置，包括调整方式（增加、缩小）、调整数量、监控时间间隔。

4.3.1.5 镜像管理

镜像是一个包含了软件及必要配置的云主机模板，包含操作系统、预装的公共应用、用户的私有应用或用户的业务数据。镜像分为公共镜像、私有镜像和共享镜像，

镜像用来创建云主机或者给云主机安装操作系统。

镜像服务提供简单方便的镜像自助管理功能。用户可以灵活便捷的使用公共镜像、私有镜像或共享镜像申请云主机。同时，用户还能通过云主机或外部镜像文件创建私有镜像。

支持多种格式镜像：

- QCOW2、RAW、ISO 格式镜像-创建云主机使用。
- AKI、ARI 格式镜像-创建云物理使用。

可上传、修改、删除镜像。

在多云纳管的场景中，一个云平台中的镜像，可以被其他云平台复用，为了简化客户的操作，提供镜像复制功能。提供镜像下载能力，方便的将云上的镜像下载到本地使用。

InCloud OS 支持用户将证书上传至云平台并对镜像数据做签名，在创建镜像时 InCloud OS 镜像管理服务会对上传至云平台的镜像数据做签名校验，从而保证用户镜像数据的可靠性和完整性。

镜像数据属于用户关键数据，镜像管理服务支持用户在上传镜像时对镜像进行加密存储，确保用户镜像数据安全性和机密性。

镜像上传时，用户如果中间因故中断了上传过程，用户可以重新选择该镜像，接续之前上传的进度继续上传。

4.3.1.6 密钥对管理

密钥对是一种安全便捷的登录认证方式,有加密算法生成的公钥和私钥组成,仅支持 Linux 实例。使用前需绑定密钥对，然后使用私钥连接实例。

可创建新的密钥对用域云主机实例访问，可删除密钥对。

可查看密钥对详情：包括名称、所属资源池、所有者、创建时间、指纹、公钥、私钥等。

4.3.1.7 回收站

回收站用于暂时存放删除的资源,包括云主机、云硬盘等,以便用户及时恢复误删或仍可用的资源。同时,用户可以通过回收站设置,配置回收站中资源可以保存的时间，到期后自动删除，及时释放资源。

- 支持在回收站中查询、恢复、彻底删除云主机,并通过清空回收站一键清空云主机。
- 支持在回收站中查询、恢复、彻底删除云硬盘,并通过清空回收站一键清空云硬盘。
- 支持回收周期设置,可以配置回收站中资源的暂存时长,回收周期仅对在设置更新后放入回收站的资源有效。

若回收站的回收周期不为 0,则删除的云主机会放入回收站(云主机中运行的业务不受影响),可根据实际情况在回收站中选择恢复或彻底删除或到设置的删除时间后自动彻底删除。

若回收站的回收周期为 0,当该云主机是通过云硬盘创建的且配置为删除时删除

云硬盘（在没有创建快照前提下），删除非共享云硬盘；当云硬盘为共享云硬盘且云主机为其挂载的唯一云主机，则删除共享云硬盘；否则挂载的数据盘仅会卸载。

4.3.2 存储管理

4.3.2.1 云硬盘管理

云硬盘是一种高可靠、低成本、高可用、可定制化的存储设备，可以作为云主机和裸金属的独立可扩展硬盘使用。云硬盘是 InCloud OS 平台不可或缺的一部分，为云主机和镜像提供持久的存储资源，不仅可以用作系统盘存放镜像文件来启动云主机，还可以作为云主机的数据盘。

可创建、修改、删除、迁移、重建、转让云硬盘；将云硬盘挂载/卸载到云主机/云物理机。

支持云硬盘扩容、云硬盘克隆、创建备份、创建镜像、创建快照、快照恢复。

可查看云硬盘的基本信息及其相关的云主机、任务、操作日志、资源审计等信息。

支持基于云主机快照创建云硬盘，也可以基于现有云硬盘创建镜像。

云硬盘迁移

满足用户的利旧或提升高优先级业务存储性能的需求，实现云平台存储数据平稳地无缝迁移。

离线迁移：针对可用状态的卷，从云平台通过 dd 方式拷贝数据到目标存储上，支持所有存储产品。

在线迁移：针对使用中的卷，在无需关闭云主机的情况下，通过 libvirt 的 rebase

接口，最终利用 QEMU 的 live block copy 技术，实现数据跨存储迁移。

离线迁移、在线迁移功能都支持迁移限速，可选高、中、低、自定义、不限速，默认不限速。

云硬盘类型

云硬盘类型是一组云硬盘共同属性的标签。使用同一云硬盘类型创建的云硬盘，具备共同的属性。

- 可创建、修改、删除云硬盘类型，支持对云硬盘类型进行加密配置。
- 可为云硬盘类型关联关联 QoS 规格：关联 QoS 后，该云硬盘类型所关联的云硬盘将增加 QoS 属性限制。
- 可为云硬盘类型取消关联 QoS 规格：解除后该云硬盘类型相关的云硬盘类型将不受 QoS 限制。

云硬盘 QoS

云硬盘 QoS 通过云硬盘类型来对云硬盘进行一定属性的限制。当前限制规格属性分为两类：IOPS 和吞吐量，具体如下：

属性	说明
read_bytes_sec	读吞吐量，只读场景下的吞吐量，取值范围 0~99999999Bytes。
write_bytes_sec	写吞吐量，只写场景下的吞吐量，取值范围 0~99999999Bytes。
total_bytes_sec	总吞吐量，读写场景下的吞吐量，取值范围 0~99999999Bytes。

属性	说明
read_iops_sec	读 IOPS，只读场景下的 iops，取值范围 0~99999。
write_iops_sec	写 IOPS，只写场景下的 iops，取值范围 0~99999。
total_iops_sec	总 IOPS，读写场景下的 iops，取值范围 0~99999。

可创建、删除、管理 QoS 规格。

云硬盘纳管

纳管是一种云硬盘管理手段，主要是通过云平台进行管理在底层存储上已存在的 LUN 的技术。

基于用户希望将底层资源统一到一个云平台内进行管理的需求，需要将已运行的业务从其他云平台迁移到当前云平台，后端数据的拷贝将是一件很棘手且耗时的工作，InCloud OS 中的纳管存储云硬盘功能巧妙地解决了此问题。

云硬盘加密

在非加密场景下，数据是通过明文存储在云硬盘中，有造成数据泄露的风险。

云硬盘加密功能，利用宿主机操作系统加密组件，通过唯一的加密 key 将数据加密成密文之后，再存储到云硬盘，这样即使拿到云硬盘数据，在不知道加密方式、及加密 key 的前提下，也无法将数据解密出来。

云硬盘加密层在宿主机与虚拟化层之间，屏蔽了云主机层面的感知，所以在实际业务场景里，不影响虚拟机内部应用对云硬盘数据的读写，将对业务的影响降到最

低。

4.3.2.2 文件存储管理

InCloud OS 通过 OpenStack Manila 提供文件存储服务，可支持 NFS 和 CIFS 协议，通过 Manila 创建的文件存储，可以在云主机内通过挂载文件存储来使用网络存储空间，从而达到扩容的目的。多个云主机挂载同一个文件存储即可实现文件共享，并同时支持快照、ACL 控制

文件存储实例

可创建、修改、删除文件存储实例；可为文件存储实例扩容；可配置文件存储实例的访问权限；可为文件存储实例创建快照。

文件存储类型

可创建、修改、删除文件存储类型。

4.3.2.3 对象存储管理

对象存储是一个基于对象的海量存储服务，为用户提供安全、可靠、低成本的数据存储能力。包括创建、修改、删除桶，上传、下载、删除对象等。对象存储服务能够存放任意类型的文件，适用于普通用户、网站、企业和开发者用户。

支持通过 S3 API 的方式对接 AS13000 分布式存储系统提供对象存储服务，也可以直接通过 AWS SDK 的方式来直接调用 AS13000 存储系统的对象存储网关。

对象存储账号是对象存储系统中的顶级资源，每个账号之间的数据是隔离的。账号下包含存储桶和对象两级。用户可以通过管理网络管理对象存储账号、存储桶和对

象构建的数据结构树 ,通过数据网络进行数据的传输。第三方系统可以通过对象存储账号的公私钥对或者密码来直接通过数据网络操作账号下的存储桶和对象等数据。对象存储账号下存储桶和对象的管理支持标准的 S3 API。

4.3.2.4 快照&备份管理

快照用于记录资源的当前数据状态；备份用于对云主机进行整机备份。

云主机快照

提供云主机快照统一管理界面，可对云主机快照进行编辑、删除操作。

可查看云主机快照的基本属性、资源审计和操作日志信息。

云硬盘快照

云硬盘快照是对现在的云硬盘进行快速数据备份的机制。

提供云硬盘快照统一管理界面，可对云硬盘快照进行编辑、删除操作。

可从云硬盘快照创建云硬盘。

文件存储快照

文件存储快照主要用于文件存储在线数据的备份与恢复。

提供文件存储快照统一管理界面，可对文件存储快照进行编辑、删除操作。

可基于文件存储快照创建文件存储实例。

云主机备份

云主机备份用于对云主机进行整机备份。

提供云主机备份统一管理界面，可对云主机备份进行编辑、删除操作。

可基于云主机备份还原云主机。

云硬盘备份

云硬盘备份是对云硬盘数据的备份，可根据备份恢复到备份时刻的状态或根据备份创建新的云硬盘，创建后的云硬盘数据和备份状态的数据内容相同。

可修改、删除云硬盘备份；可从云硬盘备份恢复云硬盘。

4.3.3 网络管理

4.3.3.1 全栈网络技术路线

InCloudOS 支持多种网络技术路线，包括软硬解耦的软件 SDN、基于浪潮网络 ICE 的硬件 SDN、基于传统经典网络的 underlay 以及对接第三方硬件 SDN 技术路线。

	Type1： 纯软分布式 SDN	Type2 :基于浪潮网络 ICE 的硬件 SDN	Type3：基于经典网络的 Underlay 路线	第三方硬件 SDN
描述	基于纯软 SDN 构建，可以解耦网络硬件 主机 overlay	基于浪潮网络 SDN 构建云平台网络 网络 overlay：全部采用浪思设备	基于传统 vlan 网络构建	基于第三方 SDN，面向第三方网络设备

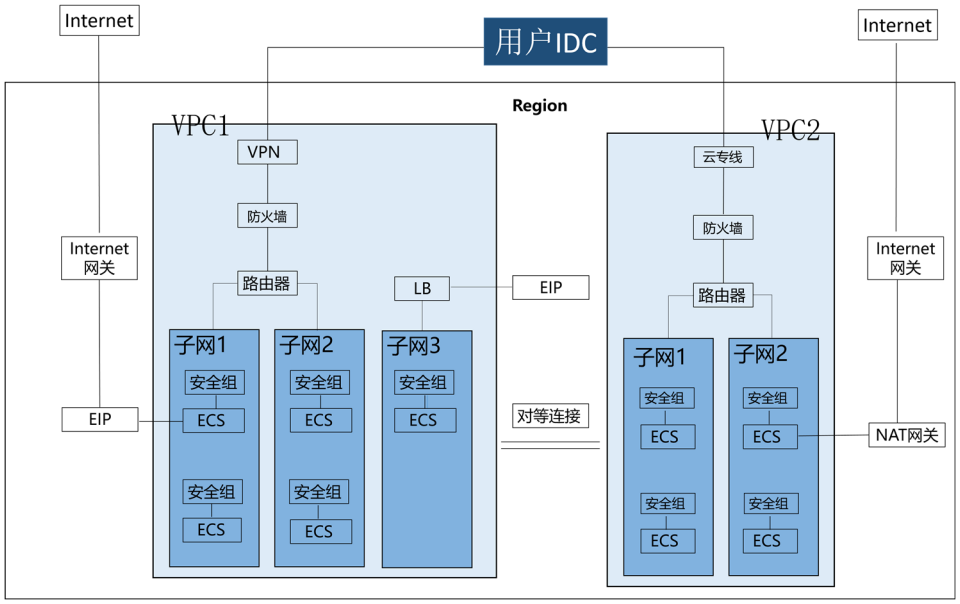
适用场景	所有场景	需要采用浪潮网络设备	对网络模型无要求 客户推荐VLAN	客户采用其它厂商网络设备
优势	解耦网络设备技术架构先进，对标 vmware NSX-T 基于 DPDK 等实现高性能网络	数据面基于硬件转发，性能高 对接商用防火墙，云内外安全措施完善 对云外设备的引流可以在交换机手动配置，补齐特殊场景	对已有网络无需改造 借助硬件交换机实现三层高性能网络	兼容最多厂商 SDN 控制器

注：具体网络功依赖以上三种 Type 模型关系见《技术白皮书》。

4.3.3.2 虚拟私有云

虚拟私有云（Virtual Private Cloud）是一个逻辑隔离的网络空间。租户可拥有一个或多个 VPC ,VPC 之间网络隔离 ,用户在使用的时候不受其他用户的影响 ,VPC 内可包含私有云上的多种网络资源 ,如网络、路由器、防火墙、VPN、负载均衡器等，用户可使用 VPC 自主构建管理隔离的虚拟网络环境 ,提升用户在私有云中资源的安全性。VPC 能简化用户的网络部署，在灵活部署、安全隔离、丰富接入、访问控制等诸多方面具备独到的优势。通过 VPC，用户可以完全掌控自己的虚拟网络，包括创建子网、创建路由、防火墙、配置 DHCP 等 ,使用户能够在保证网络隔离的同时，

更加科学的划分网络范围，部署灵活、管理方便，满足不同的业务需求。



VPC 网络模型

支持 VPC 的创建、修改、删除、设置配额等操作，创建 VPC 的同时创建默认路由器以连通子网 ,删除时默认删除路由 ;可查看 VPC 的基本信息、网络资源数据、操作日志和资源审计信息。

VPC 的数量如果超过虚拟数据中心的 VPC 配额 ,则不允许创建。互联模式 VPC，创建成功之后自动创建默认路由器。精简模式 VPC，创建成功之后则不会自动创建默认路由器。

4.3.3.3 分布式路由

在 InCloud OS 的网络环境中，跨子网的云主机通信需要通过 InCloud OS 的路由器。这既包括不同子网的云主机之间的通信，又包括云主机与外网之间的通信。

传统网络模型下，虚拟路由器会部署在集中式的网络节点或交换机下，从而产

生了两个问题，其一是网络节点/集中式三层交换机将成为整个网络的瓶颈，其二是单点失败的问题。

4.3.3.4 子网

构建统一的虚拟网络管理功能，管理二三层虚拟网络，包括子网和端口，保障各虚拟数据中心的各类云主机均可使用异构的虚拟化网络环境。

可新建、修改、删除、虚拟网络；可查看网络的基本信息、子网、端口组、IP 详情、IP 预留、操作日志、资源审计等信息。

支持对网络的子网和端口组进行操作管理。

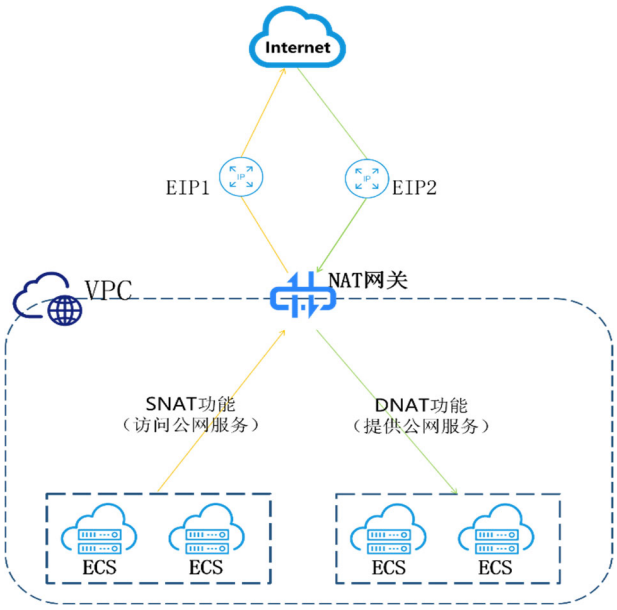
支持设置预留 IP 地址。

可创建、修改、删除子网；可查看子网的基本信息、操作日志、资源审计等信息。

4.3.3.5 NAT 网关

NAT 网关提供网络地址转换服务。包括 SNAT 和 DNAT，SNAT 通过将私有 IP 向外网 IP 转换，实现 VPC 内云主机访问外部网络。DNAT 通过端口映射，实现 VPC 内云主机为外部网络提供服务。

不支持精简模式 VPC。

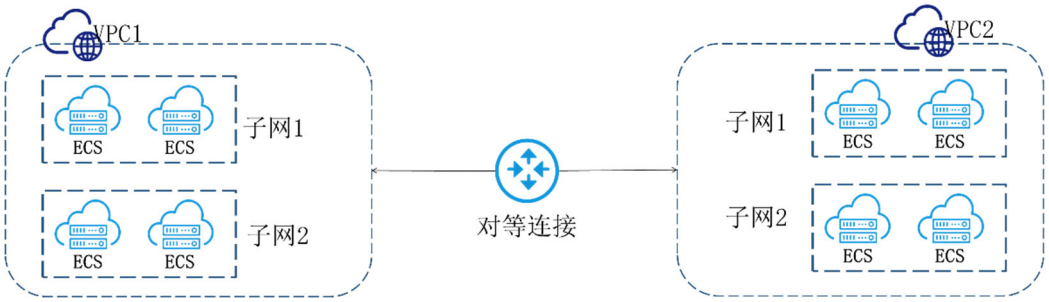


4.3.3.6 对等连接

对等连接可以连接同一租户同一区域内两个相互隔离的 VPC，可以通过在两个不同 VPC 之间建立对等连接实现资源互通，实现私有网络资源与其它云资源的互通。

可以在对等连接详情页面看到对等连接的基本信息、关联的子网、操作日志等。

不支持精简模式 VPC。



4.3.3.7 浮动 IP

浮动 IP 即外部网络中的 IP，云主机等设备绑定浮动 IP 后可以与外界互相通信。

浮动 IP 服务是创建一个可直接访问 Internet 的 IP 地址，并将该地址与虚拟网络的云主机虚拟网卡、云物理机或负载均衡绑定后，实现云资源通过浮动 IP 地址与互联网通信。

虚拟网络中各个云主机配置的 IP 地址都是私有 IP 地址，无法访问互联网。当云主机上的应用需要访问外部网络时，可以通过绑定浮动 IP 的方式来实现虚拟网络中的云主机通过固定的公网 IP 地址与互联网互通。

一个浮动 IP 只能给一个云主机虚拟网卡、云物理机或负载均衡使用。

可分配、释放、绑定、解绑浮动 IP；支持 QoS 配置。

4.3.3.8 安全组

安全组对云主机网卡的网络流量进行过滤，保护云主机通信安全。

安全组是面向云主机的安全防护策略，对防护规则逻辑上分组，为同一个项目内具有相同安全保护需求并相互信任的云主机提供访问策略，支持白名单（指允许策略）。安全组创建后，用户可以在安全组中定义各种访问规则，当云主机加入该安全组后，即受到这些访问规则的保护。

启用安全组服务后，任何一个云主机都必须属于一个或多个安全组。用户可以创建自定义的安全组，如果用户在创建云主机时没有指定自定义安全组，云平台将为该云主机自动生成并分配一个默认安全组。用户可以通过添加或删除安全规则的方式修改用户自有安全组和默认安全组的安全策略。

用户可以任意配置安全组规则，安全控制云主机入和出方向的所有流量，在云主机迁移（云主机 HA、手动迁移）等各种场景下，安全组规则也会伴随云主机自动迁

移。

4.3.3.9 防火墙

InCloudOS 可以实现对防火墙的配置管理，防火墙是分租户的，也可以在多个租户之间共享。云平台主要通过以下概念来实现对防火墙的管理：

- 规则（Rule）：允许用户指定所要匹配的名称、描述、针对的协议（TCP，UDP，ANY）、行为（Allow，Drop）、源/目的 IP 地址/子网和端口号/端口号区间。

  与 Neutron 安全组中的规则的区别：防火墙规则需要指定规则的处理行为是允许（Allow）、丢弃（Drop），安全组是白名单机制、不能指定处理动作；防火墙应用于 vRouter、防护 vRouter 的流量，安全组则应用于虚拟机的虚拟网卡、防护虚拟网卡进出流量安全。
- 策略（Policy）规则的逻辑集合。Policy 可以是共享的和被审计的（Audited）。
- 防火墙（Firewall）：策略的逻辑集合，可以关联作用到的虚拟路由器。

防火墙对象组：

Type2 硬 SDN 技术路线下，InCloud OS 支持防火墙对象组功能，通过对象组可以实现对防火墙规则中 IP 地址和端口的批量管理，提高管理效率。对象组包含地址簿和端口簿两个子功能：

- 地址簿：地址簿中可以添加 IP、CIDR 或 IP 范围，创建或更新防火墙规则时，如果源/目地址选择了地址簿，则该地址簿中的 IP、CIDR、IP 范围都会生效。

- 端口簿：端口簿中可以添加端口或端口范围，创建或更新防火墙规则时，如果 源/目端口选择了端口簿，则该端口簿中的端口、端口范围都会生效。

4.3.3.10 云专线

InCloud OS 提供了云专线功能，实现 vpc 网络与云外网络的打通。云专线包括专线网关和关联子网两个模块。

专线网关：用户可以通过云专线网关动态扩展专线网关数量，进而借由 ECMP 技术，实现提升云专线带宽的目的；

关联子网：配置云内子网和云外 CIDR，都支持多选。

4.3.3.11 云连接

InCloud OS 提供了云连接功能，用户能够快速打通跨区域 vpc 三层网络。云连接主要包括云连接实例管理、云连接子网管理两个模块。

云连接实例管理：为每个资源池的 OVN 层创建互联路由器，OVN 层将内联网络和中转网络以接口形式添加到互联路由器上，内联网络添加到 VPC 路由器，完成了整个互通的链路的创建。

云连接子网管理：本端子网 CIDR 下发至 OVN 层，OVN 层在 vpc 路由器和互联路由器上配置静态路由；同时跨 Region 调用完成对端子网 CIDR 的下发以及相关路由的下发。

4.3.3.12 VPN

VPN（Virtual Private Network）又叫做虚拟专用网络。它是在公用网络上建立

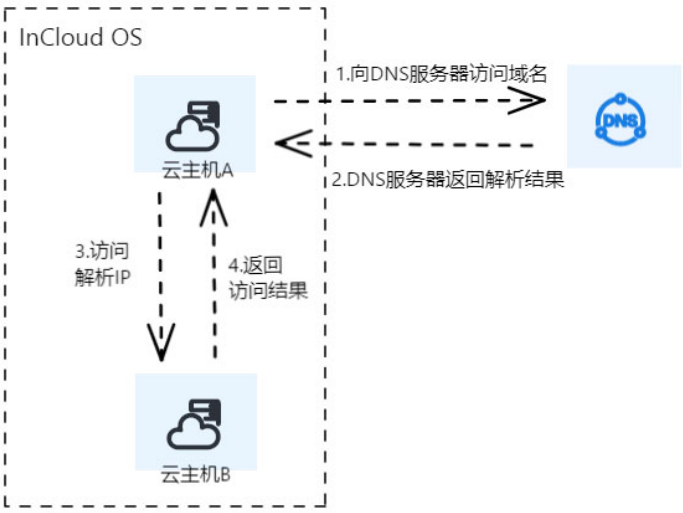
的专用网络，进行加密通讯。InCloud OS 提供 VPN 功能，VPC 内云主机可以通过 IPSec 隧道与对端云主机或设备进行安全加密的通信。

VPN 功能包括 IKE 策略、IPSec 策略、VPN 服务、Endpoint 组，以及 IPSec 站点连接五个子功能模块。

4.3.3.13 DNS

DNS（Domain Name System）又叫做域名系统，它是一个将域名和 IP 地址相互映射的一个分布式数据库，能够使用户通过直接访问域名来访问网站或者 Web 应用程序。

InCloud OS 提供 DNS 服务，云主机访问域名时，集群内对接的 DNS 服务器对该域名进行解析，向云主机返回被访问域名对应的 IP 地址，云主机可根据解析 IP 访问目标云主机或相应服务。



4.3.3.14 负载均衡

负载均衡（Server Load Balancer）是将访问流量根据转发策略分发到后端资源池（资源池，可包含云物理机，云主机）的流量分发控制服务。负载均衡扩展了应用的服务能力，增强了应用的可用性。负载均衡通过设置虚拟服务地址，将添加的资源池成员虚拟成一个高性能、高可用的应用服务池，并根据转发规则，将来自客户端的请求分发给资源池中的成员。负载均衡器对于 IPv4 与 IPv6 都有着较好的兼容能力与流量处理能力，支持使用 IPv4 或 IPv6 的网络创建负载均衡器，并且将流量分发至不同的资源池成员。

负载均衡由 4 部分组成：

- 负载均衡器：承载业务的实体，用于接收并向资源池成员转发客户端请求。
- 监听器：根据监听协议和端口检查客户端请求，并根据分配策略将请求转发给资源池成员处理。一个负载均衡器中可添加一个或多个监听器。
- 资源池：每个监听器会绑定一个资源池。资源池由一个或多个云主机组成，用于接收和处理客户端请求。
- 健康检查器：定期对资源池成员的运行状态进行健康检查。

4.3.3.15 网络 QoS

QoS（Quality of Service，服务质量）策略来解决网络延迟和阻塞等问题，为指定网络的通信提供更好的服务能力。网络 QoS 作用在云主机的网卡上，用来限制云主机网卡的流量大小。

支持自定义 QoS，配置网卡出入方向的带宽峰值及数据包突发大小。

4.3.3.16 流量镜像

nCloud OS 支持流量镜像服务，可以将出、入云主机网卡的流量拷贝一份送到另一台云主机，以便于对流量进行监控、分析、备份等，此服务既不影响源云主机的网络转发，又能在流量的镜像过程中能保持报文内容（包括报文头）的原始性。

流量镜像由底层 OVS 完成，和源云主机占用相同的网络资源，可能会影响相应节点上网络性能

配置流量镜像的虚机在迁移到其它节点后会导致流量镜像失效。

4.3.3.17 网络策略模板

网络策略模板提供子网、网络 QoS 策略、安全组等统一配置，创建云主机时可使用模板快速配置云主机的网络。

4.3.4 容器平台管理

提供容器平台类型的资源进行统一管理，管理人员可将通过直观的操作面板，对云资源、应用、服务等进行创建、分配、编辑等操作。

4.3.4.1 容器服务

4.3.4.1.1 应用中心

为用户提供基于容器镜像、应用模板、应用包等多种交付件创建的应用服务；同时，为用户提供数据隔离的应用空间，实现根据实际应用场景管理业务资源及数据。

自制应用

自制应用管理提供容器应用的全生命周期管理，支撑应用的创建、状态变更、应

用组件部署、访问地址或安全组设置、资源审计等一系列功能。

应用管理服务提供可视化的应用系统管理功能，用户可根据实际需求通过页面操作应用组件的部署、整合多个应用组件间的关联关系，解决微服务形式下多个服务模块批量容器化运行所需要的复杂操作及繁琐配置的问题，支撑应用组件在底层 Kubernetes 集群上的快速部署和灵活的调度策略、精细的访问控制管理，同时结合系统多层级、多维度的角色设置实现应用的分层级、分权限管理。

Helm 应用

Helm 应用管理提供基于标准 helm Chart 模板进行应用的创建、升级、改配、详情查看、监控等标准 Helm 应用的生命周期管理。该功能主要面向如下场景：

场景一：熟悉容器的客户/ISV 其业务系统的交付部署方式基于 K8S，则可直接将 chart 模板上传到 InCloud OS 容器服务/应用商店，通过本功能进行一键化部署和管理。

场景二：面向云原生场景，客户一些通用能力组件，例如：中间件、数据库、技术中台组件等，可基于镜像部署的基础上，逐步形成 Helm 模板，上传至应用商店，后续新项目或者搭建新的环境可快速部署。

一云多芯应用

在同一资源池不同 CPU 架构主机混合部署的基础上，为实现容器应用跨架构低成本切换或自由切换，平台以一云多芯应用形式支持容器应用进行跨架构编排部署，并支持按架构自定义副本数和流量切分比例。

- 支持一键部署一云多芯应用，支持创建时指定不同架构对应的应用容器镜像。

- 支持通过修改自定义副本数和流量切分比例 ,实现一云多芯应用跨架构切换/迁移。
- 支持一云多芯应用跨两种及以上架构进行部署。

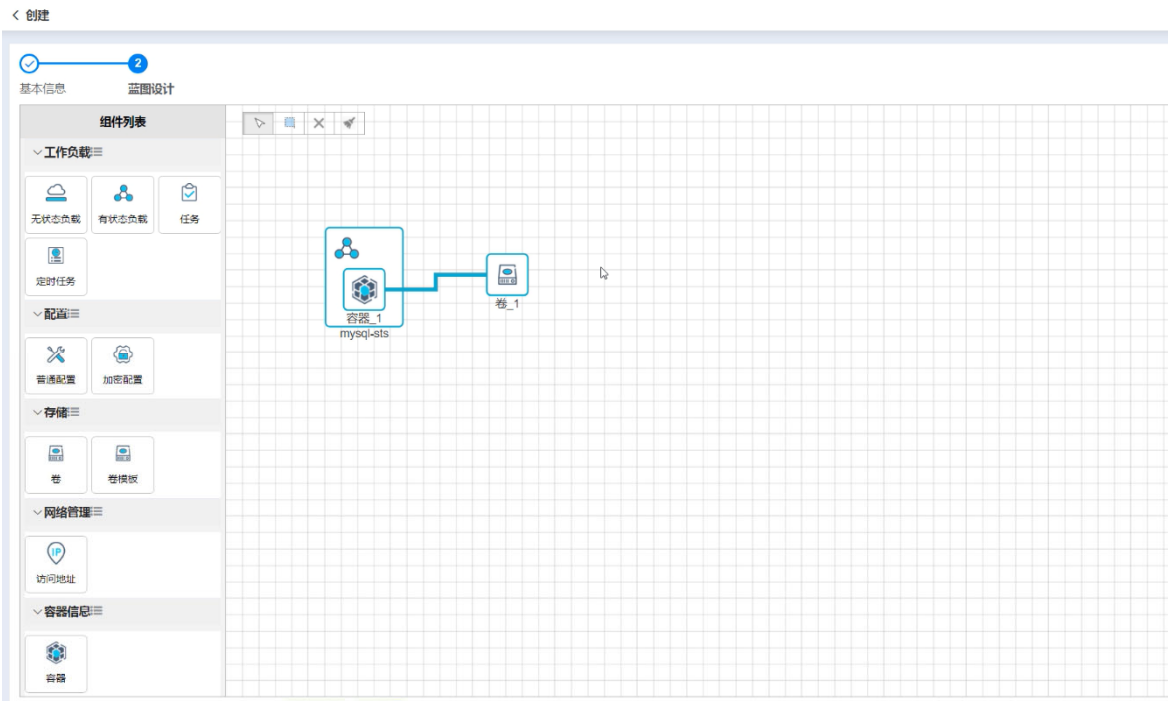
应用拓扑

以图形化形式直观展示应用组件间复杂的关联关系 ,支持可拖拽动态展示 ,支持组件信息的快速查看。拓扑关系中可以展示应用内的各组件的名称、类型、状态以及组件间的依赖关系。

应用实例转蓝图

支持一键转为蓝图功能，适用于多组件复杂关系的应用快速转换成可图形化拖拽式编排、可共享、可重复部署的应用蓝图。

该功能可基于应用的配置、应用组件及组件间的依赖关系形成应用模板 ,并可进一步发布到私有或公有的应用中心，实现应用的快速复制和部署。



升级与回滚

升级功能支持无状态负载、有状态负载、任务、定时任务的升级，升级内容主要包含容器属性（镜像、CPU/内存限制、容器端口、启动命令、参数、环境变量等）、存储卷配置、健康检查配置和调度策略。升级时需要记录版本升级记录。

回滚支持展示无状态负载、有状态负载、任务、定时任务的升级记录，支持用户选择某个版本进行回滚。

应用空间

应用空间（Namespace）是一组资源的抽象整合，可基于应用空间实现平台的多租户模式。在同一资源池内可以创建不同的应用空间，每个应用空间相当于一个相对独立的虚拟空间，默认不同应用空间内的资源彼此隔离；资源数量可以通过配额来限制，且同一应用空间中的资源默认具有相同的访问控制策略，使其既可以共享资源池服务，又可以互不干扰。应用空间的 CPU、内存配额支持设置为不限制。

应用商店

应用商店提供包括开源软件、行业软件、基础数据库及中间件在内的应用模板，形成生态汇聚，实现多组件复杂应用的快速、一致性下发、差异化配置部署，推动业务系统快速、复制化上云。应用商店提供了一组基于 Helm 的应用模版和可视化的快捷应用部署功能，用户可以根据实际需求通过页面操作，配置简单的参数，实现快速部署应用。

应用包管理

应用包管理服务提供应用包的上传、修改、更新、列表展示等功能，并且支持将

应用包直接部署成应用。

应用包管理服务提供可视化的包管理界面，用户可根据自身需求将其项目编译打包成 Jar 包或者 War 包上传到系统进行管理，并可直接部署成应用，进行后续的应用工作负载组件、访问地址或安全组设置、资源审计等一系列功能的整合。满足了用户在特殊场景下将现有的项目快速部署的需求，大大加速了企业整体容器化进程。

4.3.4.1.2 工作负载

工作负载是Kubernetes对一组应用实例的抽象模型，用于描述业务的运行载体，包括无状态负载、有状态负载、任务和定时任务等，是应用软件在服务器上的实际部署形态，也可作为应用组件通过应用管理服务统一管理。

工作负载管理整合容器的状态管理、升级与回滚、访问控制、调度策略、资源监控、日志、控制台等功能，并能够支持可视化设置副本数、自动弹性伸缩、健康检查、镜像拉取策略等特性，能够最大程度的实现应用软件的快速部署与升级、智能监控、自动运维等一系列操作，保障应用软件服务的可持续性、高可用性，提高资源利用率，减少用户在运维管理上的人力与时间成本。

无状态负载

无状态负载（Deployment）为容器组（Pod）提供了一个声明式（declarative）方法来管理应用，各容器组之间完全独立且功能相同。典型的应用场景包括定义无状态负载来创建应用实例（Pod）、滚动更新和回滚、弹性伸缩以及开启/关闭无状态负载。适用于实例完全独立、功能相同的场景，例如：Nginx、web 服务。支持主机路径挂载/卸载，查看/编辑 YAML 配置。

支持无状态工作负载如下操作：

- 查询、查看无状态负载信息；修改、升级、回滚、开启、关闭、删除无状态工作负载。
- 可更新运行中、关闭、错误、忙碌状态无状态负载的配置，包括概览、查看资源状态、容器配置、查看事件、访问地址、网络策略、调度策略、查看日志、控制台访问、资源审计、历史曲线。
- 弹性伸缩支持水平伸缩、定时水平伸缩、垂直伸缩三种方式，能够根据设置好的资源(CPU、内存)和实例数阈值自动/定时调整副本数，帮助应用自动应对波峰波谷，保证工作负载高可用的前提下提高资源使用率。
- 网络策略配置：可访问出规则中的组件，并允许被入规则中的组件访问。
- 主机路径挂载/卸载；
- 查看/编辑 YAML 配置
- 配置调度策略：

开启实例分散策略，开启后，实例将平均分散到每个节点上；当实例数超过资源池中实际可调度的节点数时，超出部分的实例将被挂起。

开启主机节点亲和性策略，开启后，当前组件将按所配置的调度条件运行在通过节点选择策略所选择的节点上。

开启组件间亲和策略，开启后，当前组件将与所满足条件的组件调度到同一节点上。

有状态负载

有状态负载（StatefulSet）是为解决有状态服务问题，在运行过程中会保存数据和状态的工作负载。有状态负载的各容器组之间不完全独立，拥有固定的名称和启停顺序，具有稳定的持久化存储、网络标志、有序部署及扩展等功能特性。适用于实例按顺序启动的场景，例如：mysql 服务、etcd 服务。支持主机路径挂载/卸载，查看/编辑 YAML 配置。

支持有状态工作负载如下操作：

- 查看有状态负载信息，可查看有状态负载的名称、虚拟数据中心等基本属性，以及资源状态、容器配置、事件、访问地址、日志、资源审计、历史曲线等详细信息。
- 可修改、升级、回滚、开启、关闭、删除有状态工作负载。
- 更新配置与调度策略：可对运行中、关闭、错误、忙碌状态的有状态负载进行配置更新及调度策略配置，其配置操作与无状态负载的相同。
- 可对运行中、关闭、错误、忙碌状态的有状态负载进行回滚操作。
- 支持访问地址管理：访问地址的添加、地址修改等相关管理操作。
- 支持网络策略管理。
- 支持主机路径挂载/卸载
- 支持查看/编辑 YAML 配置
- 支持访问控制台。
- 支持垂直伸缩。

任务

任务（Job），即仅执行一次的任务。在 Kubernetes 中用来控制批处理型任务的资源对象，保证批处理任务的一个或多个容器组（Pod）成功结束。任务管理的容器组会根据用户设置的运行规则（重复执行次数、并行数、重启策略等）执行任务，任务结束后就自动退出。例如：创建工作负载前，执行任务；将镜像上传至镜像仓库等一次性任务。可用于数据分析、批量计算等场景。查看 YAML 配置。

任务执行完后，不再创建新的容器组，也不会自动删除已有容器组，用户可在日志中查看已完成的任务日志。若用户删除了任务，那么将同时删除执行任务时创建的容器组及其日志记录。

支持开启并行任务分散策略，开启后，并行任务将平均分散到每个节点上。当并行任务数超过资源池中实际可调度的节点数时，超出部分的并行任务将被挂起。

支持开启主机节点亲和性策略。开启后，当前组件将按所配置的调度条件运行在通过节点选择策略所选择的节点上。

支持开启组件间亲和策略，开启后，当前组件将与所满足条件的组件调度到同一节点上。单击右侧“添加”按钮，即可添加配置的策略。

支持网络策略管理、控制台访问。

定时任务

定时任务（cronJob）是基于时间策略控制的任务（Job）。类似于 Linux 中的 crontab，系统根据用户配置的定时计划（即任务的执行周期），在给定的时间点自动执行指定任务，任务执行完后容器组便会停止，直至下一次触发执行，如此周期性执行该任务。查看、编辑 YAML 配置。

可查看/编辑当前定时任务的名称、用户等基本信息以及标签、资源状态、事件、容器配置等详细信息。

可更新运行中、停用状态定时任务内容器的镜像、CPU、内存、日志采集等属性配置。

4.3.4.1.3 网络管理

网络管理服务提供应用或工作负载的访问地址创建、修改、删除、变更内外部访问、设置外部访问方式、配置域名信息等一系列功能，提供应用或工作负载的安全组的创建、配置安全组规则、关联或移除组件等一系列功能。

服务

服务是应用组件可以对外访问或提供对外访问以及访问限制等一系列属性的集合，在实际使用场景中对应应用或工作负载的访问地址与安全组功能。

服务整合多类型服务包括内部访问、外部固定 IP 访问、外接负载均衡访问的创建，并支持服务的类型转换，同时支持详细地址的增删改，支持实时获取容器端口进行相应的端口映射关系修改，能够最大程度减少用户配置应用的访问入口的时间成本。网络管理服务还提供应用加入安全组以实现限制应用访问的功能，安全组规则设置支持方向类型、端口号、授权组件、端口协议的配置，安全组关联组件多个组件批量加入，在保证应用安全的前提下最大程度的节约了用户在运维管理上的人力与时间成本。

应用路由

应用路由是用来聚合容器资源池内服务的方式，对应于 Kubernetes 的 Ingress

资源。可以通过一个外部可访问 IP 地址将资源池内部访问地址暴露给外部。

子网

容器平台支持为不同的应用空间分配单独的子网并可以预留部分 IP 地址，实现客户对网络地址更精细化的管理，以及更强的隔离性。

网络策略

网络策略用来实现容器服务间的网络访问控制，能够从应用组件、网络协议、网络端口三个层面限定应用的入方向和出方向流量，精准细粒度控制应用网络隔离策略，并支持图形化直观展示网络策略的应用范围、入方向、出方向规则。

容器网络双栈

容器平台支持 IPV4 和 IPV6 双栈，意味着容器组 Pod、服务 Service 和节点 Node 可以获取 IPv4 地址和 IPv6 地址， 客户端可以通过 IPV4 或 IPV6 地址直接访问集群中的服务或容器组，满足用户对容器网络双栈的需求。

Qos

平台支持对 Pod 网卡出入带宽的限速配置，从而实现对网络带宽资源的精细化控制。

固定 IP

容器平台支持为 Pod 分配固定的 IP 地址段或单个 IP，可以使 IP 地址作为业务组件实例唯一的标识。Pod 重建后，IP 地址段或单个 IP 可保持不变。

RDMA

容器服务支持为应用添加 RDMA 高性能网络，能够满足 HPC、AI、存储、大数据等基于 RDMA 编程体系的应用间高速数据读取需求。基于 SR-IOV+容器多网卡技术，提供给容器 RDMA 网络+标准 K8S 网络的双重能力。

目前 RDMA 网络支持 IB 和 RoCE 两种模式。

4.3.4.1.4 存储管理

存储管理模块可为用户提供块存储、文件存储和本地存储等多种存储方式。用户可根据业务需求，创建所需类型的存储卷，以供存储工作负载中的业务数据，实现基于 PVC 的持久化存储。

存储卷管理

存储卷管理提供存储卷的全生命周期管理，支撑存储卷的创建、挂载、卸载、扩容、存储卷共享、卷模板、查看事件、资源审计、监控使用量、使用率、历史曲线等一系列功能。

InCloud OS 容器服务提供可视化的存储卷管理功能，能够屏蔽不同厂商、不同类型的存储产品复杂的设置及对接过程。

根据存储文件系统的管理方式以及卷的特性，将存储分为块存储、文件存储、本地存储，更加方便用户查找使用。

存储卷快照

随着大中型企业快速的发展，企业用户规模不断扩大，数据的增长速度也越来越快，需要缩短备份窗口，以在线的方式对存储数据进行保护，提高数据保护过程中的

应用感知能力。快照是对块存储卷某时刻数据状态的记录,可以作为一种数据容灾方案。当数据丢失时，可通过快照及时将业务数据完整地恢复到快照创建点的状态

存储卷克隆

克隆是基于存储卷已经写入数据进行复制。InCloud OS 容器服务支持块存储卷进行克隆。支持块存储进行克隆，克隆时可以选择新存储卷的名称和描述信息。

块存储卷弹性扩容

容器块存储卷弹性扩容设计的目标旨在实现容器存储卷的动态扩容功能，帮助用户解决手动扩容卷的高运维成本,因扩容滞后导致的业务中断,以及存储资源使用率等问题，容器块存储卷弹性扩容要实现如下特性：

- 当存储卷使用率到达设定的阈值后，可自动触发容器卷扩容至目标容量，能支持按固定容量扩容或按照扩容前容量的百分比为扩容步长进行扩容。
- 根据智能预测算法预测的剩余容量耗尽时长，可自动触发容器卷扩容至目智能预测算法推算出的足够设定天数使用的容量。
- 能根据设定的时间，自动触发容器卷的扩容至目标容量，能支持按固定容量扩容或按照扩容前容量的百分比为扩容步长进行扩容。
- 能对自动扩容操作进行事件记录。

4.3.4.1.5 配置中心

通过配置中心提供普通配置和加密配置，为用户提供工作负载中所需的配置信息以及配置文件。在工作负载中以卷或者环境变量的方式使用普通配置和加密配置。

普通配置

普通配置（ConfigMap）在 Kubernetes 中可以保存工作负载中所需的配置信息以及配置文件，将配置和运行的镜像进行解耦，使得应用程序具有更高的可移植性。普通配置为用户提供向容器中注入配置信息的机制，既可用来保存单个属性，又可用于保存整个配置文件，在工作负载中作为文件或者环境变量使用：

- 以卷的方式，在存储卷配置时，通过“存储卷配置”选择创建的普通配置。
- 以环境变量的方式，在配置容器时，通过“引用配置中心”选择创建的普通配置。

加密配置

加密配置（Secret）是 Kubernetes 中一种加密存储的资源对象，可用于保存认证信息、证书、私钥等敏感信息，降低直接对外暴露的风险。可在工作负载中以存储卷或者环境变量的形式使用加密配置：

- 以卷的方式，在存储卷配置时，通过“存储卷配置”选择创建的加密配置。
- 以环境变量的方式，在配置容器时，通过“引用配置中心”选择创建的加密配置。

4.3.4.1.6 本地备份

越来越多的业务系统会部署到基于 K8S 的容器中，当业务系统在数据损坏、误删等异常场景时，如何快速恢复客户业务系统，并能够保留业务数据，是用户急迫的关键需求。本平台的容器应用备份恢复功能，能够将容器业务系统整体进行备份，包括元数据和业务数据，也可以对整个 Namespace 的业务系统进行备份，在需要时，

能够进行一键快速恢复。同时，为了满足不同的业务场景，支持只备份元数据或者卷数据，也可同时备份两者。

备份服务为容器应用资源提供对 K8S 元数据及 PV 用户数据的一次性备份服务，以便还原容器应用，同事基于对象存储提供备份文件的保存服务。

4.3.4.1.7 跨存储容灾备份

当业务系统在资源池升级、硬件故障等场景时，如何快速恢复客户业务系统，并能够保留业务数据，是用户急迫的关键需求。本平台的容器应用跨资源池容灾备份功能，能够将容器应用元数据进行备份，同时对存储卷数据进行跨集群近实时复制，在需要时，能够通过主备切换/故障切换快速恢复业务。同时，为了满足不同的业务场景，支持只备份元数据，也可同时备份两者。

4.3.4.1.8 容器集群服务

K8S 作为容器基础设施的事实标准，已经被广泛的应用到各行各业的云平台中，随着业务的不断扩展和更新，用户有按需不断创建新集群满足新业务，销毁旧集群替换掉旧业务的诉求，而搭建容器集群相对复杂、运维成本高，提供一种 K8S as Service 的服务，可以方便的按需获取 K8S 容器集群。

按照使用模式可分为资源池共享模式和租户专享模式，资源池共享模式下，管理员一键创建 K8S 容器集群，并自动加入资源池供所有租户使用；在租户专享模式下，租户可以自行一键创建一个集群，为自己规划的业务使用，对整个集群拥有完整的生命周期管理权限用，并且与其他租户进行完全隔离。

4.3.4.1.9 容器资源池管理

在云平台中，容器资源池是一个 K8S 集群，需要纳管到 CMP 管理平台进行统一管理和使用，纳管的方式有两种，包括直连（也称为直接）纳管和代理纳管。如果 CMP 可以直接访问 K8S 集群 kube-apiserver 地址，则可以采用直连纳管。如果 CMP 无法直接访问集群 kube-apiserver 地址，但是容器资源池可以访问 CMP 地址，则可以采用代理进行纳管。通过在 CMP 管理平台中暴露资源池纳管的代理服务地址，让资源池通过代理连接到 CMP。当容器资源池部署在虚拟化环境（CMP 管理节点无法直接访问虚拟机 IP 地址，但虚拟机可以通过 NAT 访问 CMP 地址）或者边缘环境（资源池处于一个局域网内，与 CMP 管理节点处于不同的局域网内）时，适用采用代理纳管。

4.3.4.1.10 GPU 管理和调度

原 GPU 资源共享模式只是在资源申请和调度阶段限制容器应用程序的 GPU 资源配额，做不到运行阶段资源限制和隔离，本版本基于 MIG 做到硬件层面的算力隔离和基于 CUDA 劫持的技术达到软件层面 GPU 隔离的目标。

- 设计灵活的 GPU 配额管理模型，支持 GPU 独享、GPU MIG 共享、GPU 共享等多种 GPU 使用模式。
- 基于 MIG 技术实现 GPU 共享，以多实例的形式提供给 POD 使用，每个实例都有独立于各自的显存、缓存和计算核心。

  基于 CUDA 劫持的 GPU 资源共享技术方案实现 GPU 资源的共享，实现容器应用内部实际运行时 GPU 核心和显存的限制，同时对容器应用无感知。

4.3.4.2 镜像服务

镜像服务提供了一种基于 Harbor 实现的镜像服务，包括内置镜像仓库和第三方仓库，用于存放和管理可用于部署应用服务的容器镜像；基于漏洞数据库的全架构镜像无差别安全扫描，提供镜像版本的安全性监控，并可对高危镜像的取用进行限制，保障用户应用服务的安全性；为用户提供多架构的应用包，包括 Jar 包、War 包，支持各类应用包的全生命周期管理。支持内置仓库和接入第三方仓库。

4.3.4.2.1 镜像中心

镜像仓库

镜像仓库提供了一组基于 helm 的应用模板，应用模板中已编排配置好环境变量等参数，用户仅需简单配置 CPU、内存等基本参数即可轻松一键式部署应用。

目前平台支持的架构环境中已集成 MariaDB、MySQL、Tomcat、SonarQube 和 WordPress 五个公有应用模板；同时 CPU 架构为 ARM 和 MIPS 的环境中，还集成了瀚高数据库、tongweb、宝蓝德 web 应用。

- 支持应用部署、应用修改、上架、下架。
- 支持多架构镜像仓库以一个内置镜像仓库的形式呈现。
- 支持公有、私有镜像管理及列表展示。
- 按分类展示已有镜像：可添加、编辑、删除分类。
- 支持以文件形式上传镜像，并可查看命令行形式推送、拉取镜像操作指引。
- 支持基于镜像一键部署应用。

- 查询、修改镜像分类、镜像版本管理。
- 镜像详情查看，展示基本信息、版本列表、挂载点及环境变量等详细信息、漏洞扫描详情。

漏洞扫描

支持开启/关闭漏洞扫描。

基于漏洞数据库的镜像安全扫描：可一键扫描内置镜像仓库中不同版本的各类镜像。

支持单个镜像扫描、自定义扫描配置。

查看管理扫描结果、重新扫描、删除具有安全漏洞的镜像。

4.3.4.2.2 第三方仓库

可将第三方仓库（Harbor）导入到平台内，进行仓库统一纳管和镜像管理使用。

公有第三方仓库：由超级管理员导入，供所有用户使用。

私有镜像仓库：由管理员创建和管理，供指定虚拟数据中心使用；且一个虚拟数据中心仅可有一个私有镜像仓库。

4.3.4.2.3 应用仓库

平台适配异构 CPU，提供相应架构的内置镜像仓库；不仅内置用户可开箱即用的常用应用镜像，并且供用户分类管理私有镜像。

- 支持上传应用包，支持 war、jar 两种形式；支持应用包版本管理。
- 支持基于上传的 war 包或 jar 包部署应用。

应用包

应用包是指可在本地运行的 Jar 包和 War 包。用户可根据业务需求自定义和配置所需要的应用包 ,通过上传应用包 ,在应用中心以及应用包列表可通过选择应用包快速创建对应的应用。

- 支持应用包部署&上传&删除&更新等操作。
- 支持查询&查看应用包信息。

4.3.4.2.4 镜像复制

镜像复制是指通过手动、定时或事件触发三种模式将镜像中心的镜像远程复制到第三方全局仓库。

支持创建镜像复制规则；修改、删除、立即执行、启用、停止镜像复制规则。

4.3.4.3 服务网格

服务网格是一个提供连接、保护、版本发布控制及观测服务的功能模块。为用户提供无侵入式微服务治理方案 ,支持全生命周期管理及流量治理能力。在已部署微服务插件的前提下 ,创建应用时可一键开启服务网格 ,开启后即可提供无侵入的智能流量治理解决方案 , 其功能包括负载均衡、熔断、限流等多种治理能力 ; 同时 , 服务网格内置金丝雀、蓝绿等多种灰度发布策略 , 提供一站式自动化的发布管理 ; 基于无侵入的监控数据采集 ,提供实时流量拓扑、调用链路等服务性能监控和运行诊断功能 , 构建全景的服务运行视图。

4.3.4.3.1 灰度发布

灰度发布是一种使得应用服务从旧版本平滑升级到新版本的发布方式，包含多种发布策略。可在软件产品快速迭代的过程中，根据发布任务中设置的策略规则，将符合引流规则的流量引入特定的应用版本，保障应用服务的平滑演进，以降低产品版本迭代对业务所带来的风险和影响。

金丝雀发布：在原版本可用的情况下，在生产环境中分出一部分节点运行新版本，并将一部分实际流量引入一个新版本进行测试，测试新版本的性能和表现，以在保证系统整体稳定运行的前提下，尽早发现和解决新版本在实际环境的问题；待验证无问题后，再将其他节点升级为新版本，并将全部流量引入到新版本。

蓝绿发布：提供了一种零宕机的部署方式，在保留旧版本的同时部署新版本，将两个版本同时在线，新版本和旧版本是相互热备的，如果有问题可以快速的回滚到老版本。

A/B Test：为同一个产品目标制定两个甚至多个方案（版本），通过个性化的流量策略设置，引导流量分配至不同的版本，测试不同版本的表现，得出最符合预期的测试结果作为可以最终上线的版本。

流量镜像：在不影响线上应用的情况下，将生产流量引入即将上线新版本进行验证，将应用上线风险降到最低。

4.3.4.3.2 流量治理

微服务系统在设计之初就需要考虑容错机制，需要引入流量治理的架构，当系统负载过高时，可以确保核心业务不被破坏，以及当某个服务出错时，把影响范围降低

到最小，避免整个系统不可用。

InCloud OS 的流量治理支持多种负载均衡路由策略配置，支持对访问请求进行不同维度的流量控制，可以根据客户的需求对微服务的流量分发进行动态的配置与修改。

InCloud OS 的流量治理支持图形化应用拓扑展示 ,实时的展现应用的流量监控、异常请求、超长时延响应、服务健康状态等 ,并支持基于拓扑图对服务进行负载均衡、并发控制、熔断隔离、故障注入等流量治理规则配置 , 实现真正意义上的实时、可视化的微服务流量治理。

4.3.4.3.3 服务追踪

服务追踪为分布式应用的开发者提供了完整的调用链路还原、调用请求量统计、链路拓扑、应用依赖分析等工具 , 可以帮助开发者快速分析和诊断分布式应用架构下的性能瓶颈，提高微服务时代下的开发诊断效率。

InCloud OS 的服务追踪兼容 Opentracing 规范，支持 jaeger、zipkin 等链路追踪与展示工具 , 支持应用级别链路请求最高耗时、错误请求数、总请求数概览展示，支持服务之间链路追踪信息的可视化展示与详细查询。

4.3.4.3.4 方法级链路跟踪

InCloud OS 基于 skywalking 架构 , 支持方法级链路追踪功能 , 可以实时展示应用请求途径的各组件内部自定义方法的执行情况，满足用户更细粒度问题故障及性能瓶颈定位的需求。

方法级链追踪特性功能包括：

- 支持多种语言方法级链路追踪信息的收集、展示和配置，包括 java、php 等常用语言。
- 支持 Java、Nodejs 服务启动时自动注入 skywalking agent 的方式实现方法级链路追踪，对业务无感知。
- 支持应用随时开启或关闭方法级链路追踪。

方法级链路追踪(简称方法追踪)是在分布式全链路追踪的基础上进行更深层次下探到编程语言方法层面的追踪。当这个方法被调用时，APM 探针会按照用户配置的方法追踪规则采集当前方法的调用数据，并将调用数据展示到列表中。方法跟踪主要用来帮助应用开发人员快速分析和诊断方法级别的性能问题。

4.3.4.3.5 参数设置

提供服务追踪和方法级链路追踪数据保存策略的配置管理。

4.3.5 软件开发服务

软件开发服务是一组过程、方法与系统的统称，用于促进研发内部以及研发和运维、质量保障部门之前的沟通协作及整合。为解决日益流行的敏捷开发模式所带来的软件快速开发、交付和质量问题，基于 DevOps 理念，平台支持绑定代码仓库，提供基于 Jenkins 的流水线编排，实现多语言的持续集成和持续交付（CI/CD），提供业务应用的自动化构建、集成、测试和发布等一站式服务。

4.3.5.1 代码源

用户可在此处完成构建前的准备工作：首先添加业务代码所在的代码仓库，然后关联目标代码源，以便后续构建流水线时作为代码源使用。

目前支持的代码仓库：GitLab 和 SVN。

4.3.5.2 流水线

流水线（Pipeline）是基于 Jenkins 的一系列插件集合，结合 Pipeline DSL，将简单到复杂的逻辑通过图形界面呈现给用户。用户可以通过自定义流水线来实现应用的持续集成和持续交付，提高研发效率，降低运维成本。

同时，提供多种流水线内置任务、常见场景的流水线模板，以及流水线克隆功能，用户可根据实际需求自由组合定义流水线，满足用户不同场景的使用需求。

创建流水线后，可定义流水线中的各个阶段和任务。另外，正在执行的流水线不能增加阶段和任务。

阶段：一个流水线可以划分为多个阶段，每个阶段可由一组任务组成。

任务：任务是流水线最基本的操作单元，小到创建一个目录，大到构建一个 Docker 镜像。

系统除提供一些典型的执行任务、发布任务外，同时提供用户自定义任务的功能。其中，目前典型任务包括：

- 构建类：Maven 环境、Gradle 环境、Pyinstaller 环境、Golang 环境
- 其中，Maven 环境和 Gradle 环境均为 Java 的编译构建环境
- 代码扫描：SonarQube 代码检查
- 发布类：Docker 镜像
- 部署类：部署
- 其他：克隆代码

支持查看流水线的执行记录,包括流水线各阶段的执行过程;平台支持系统显示对应的执行记录窗口，查看对应阶段的执行记录信息。

4.3.6 可视化编排

4.3.6.1 云主机应用编排

平台提供可视化编排功能,实现了对云资源组件(包括:云主机、网络、子网、安全组、浮动 IP、端口、路由器)的可视化的抽象建模，通过界面拖拽的方式，形成一系列资源组件以及组件之间关系的拓扑结构模型，并结合服务实例功能实现了一键式开通云资源的服务模式。

- 支持图形化拖拽进行编排，简化客户操作。
- 支持多种应用混合编排，如数据库、中间件，满足应用的各种要求。
- 支持设置编排元素的属性设置，如云硬盘大小、虚拟机规格等。

应用蓝图

蓝图是描述一系列资源组件以及组件之间关系的拓扑结构。为用户提供蓝图(即服务模板)的创建和管理功能,用户可在模板中自定义云主机、网络、应用等组件之间的依赖和引用关系。基于蓝图编排控制器,提供多种应用蓝图设计方案:用户既可自定义应用蓝图,也可基于系统内置模板创建应用蓝图,还可以基于已有蓝图创建新应用蓝图。

支持蓝图设计创建、修改、发布、取消发布、上传、下载、查看拓扑图、关联服务目录、删除、直接部署、蓝图模板等操作。

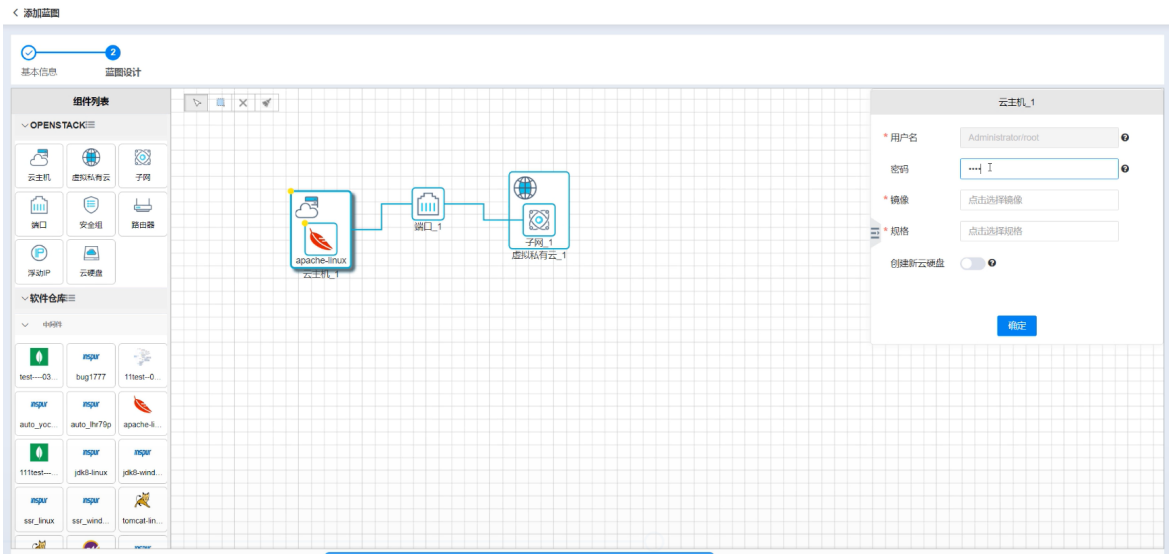
从零开始创建:可以通过拖拽的方式实现资源从无到有的构建,以及资源组件的

配置、编排等操作。

基于模板创建 :系统推荐模板将为你推荐多种常用业务场景模板 ,可以使用任意推荐模板为基础，完成资源拓扑的创建、配置、编排。

基于已有蓝图 :可以从保存的蓝图设计中选择任意模板导入图布 ,对其进行资源拓扑的配置、编排等操作，原有模板不受影响。

平台支持拖拽式蓝图构建功能 ,将需要的云主机组件拖拽到画布上 ,通过连接线编排各个组件间的依赖和引用关系，双击组件或连接线，可在显示的组件属性窗口中，配置其属性参数。



蓝图拓扑

系统为用户提供内置的蓝图模板，以供用户取用。

应用商店

应用商店中存放应用蓝图发布后生成的应用，用户可以一键式部署应用服务。

支持应用查看、部署应用、下架应用等。

软件仓库

软件仓库是用户常用软件的存储仓库，同时可进行软件安装脚本的配置管理，大大简化了云主机安装软件的过程。

支持软件的上传、下载、修改、删除及脚本管理等操作。

脚本管理：运维人员可对上传的软件的初始化脚本进行统一管理，为软件配置安装、初始化配置等脚本，实现编排服务的自动化配置操作。

支持添加、导入、修改、删除软件的脚本。

部署日志

部署日志用于记录在基于蓝图的服务实例部署过程中创建资源的日志信息，以便用户通过部署日志了解部署过程，或者定位部署过程中出现的问题。

编排控制器

编排控制器是部署有编排引擎服务的云主机或者外部主机，用于创建或者部署蓝图内的资源组件。

编排控制器是实现服务编排的核心组件，只有为资源池添加编排控制器后，平台才可以提供服务编排功能。

可为资源池添加编排控制器，提供服务编排功能。一个资源池中只能添加一个编排控制器。

支持编排控制器的添加、修改、删除等操作。

4.3.6.2 容器应用编排

容器应用编排实现从容器应用的可视化编排、容器应用模板到应用商店的发布与下架以及通过应用模板创建应用实例的全周期的应用编排管理，用户可以通过拖拽的形式将需要的组件关联起来编排对应的蓝图，提高了编排文件编写的效率，解决了容器编排文件编写的繁琐性的问题，提高了用户上云的效率。

应用蓝图

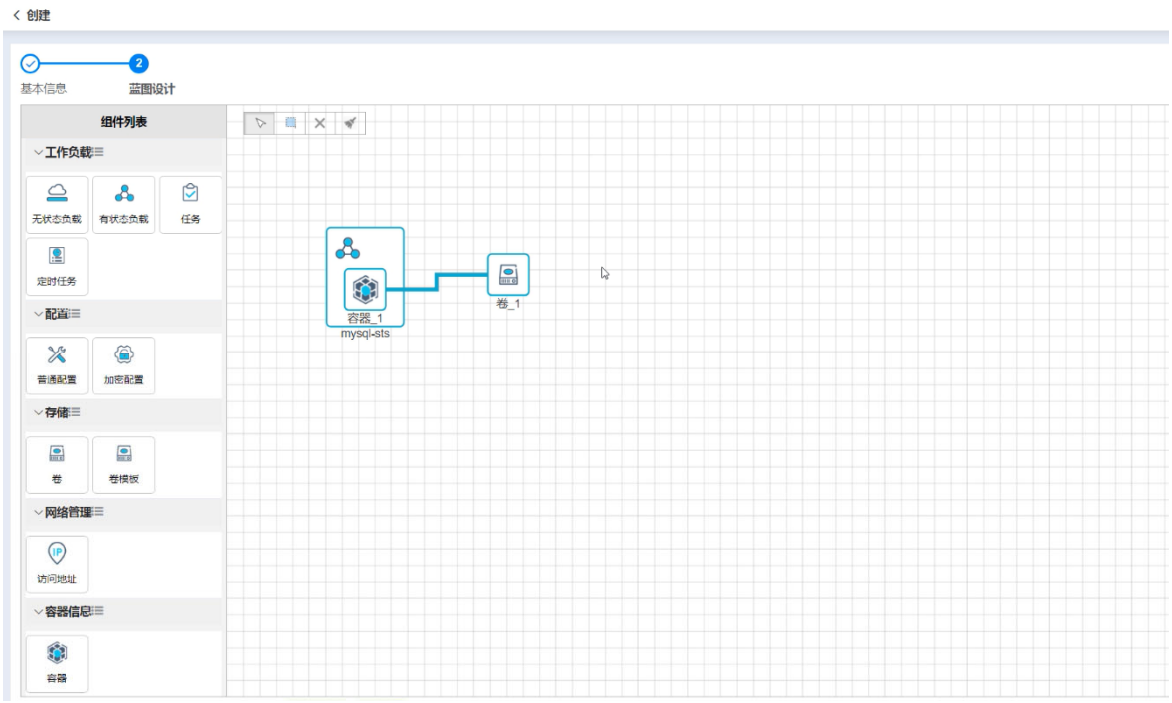
蓝图是描述一系列资源组件以及组件之间关系的拓扑结构。为用户提供蓝图(即应用模板)的全生命周期管理，包括创建、修改、删除等。用户可在模板中自定义工作负载、配置等组件及其之间的依赖和引用关系，并通过蓝图编排引擎将应用蓝图解析为 helm 模板并上传到 Harbor 进行持久化保存。

查看蓝图：可查看该蓝图的名称、版本等基本信息，以及蓝图的详细介绍和拓扑图（仅限于创建蓝图的拓扑）。

发布蓝图：可发布草稿状态的蓝图，发布后生成的应用模板将展示在“应用商店”中，供用户使用。

复制蓝图：复制蓝图时会复制目标蓝图的所有参数，用户可根据实际需求进行修改。

编排设计蓝图，通过拉拽的方式将组件拖至画布，连接线编排各个组件间的依赖和引用关系，双击组件或连接线，可在显示的组件属性窗口中，配置其属性参数。



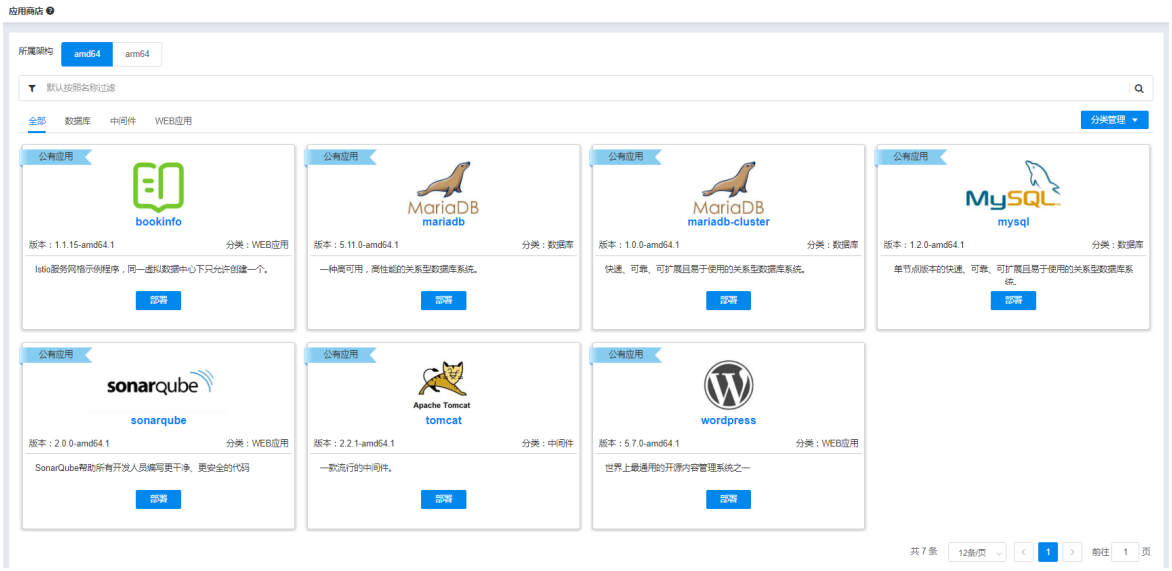
蓝图设计

在应用商店中可以部署设计的应用蓝图。

应用商店

应用商店是平台中应用模板的存储、交付和管理途径，为用户提供了一组基于 Helm 的应用模板，包括开源软件、行业软件、基础数据库及中间件等不同类别的常用应用模板。各应用模板均已编排配置好环境变量等参数，用户仅需简单配置 CPU、内存等基本参数即可轻松一键式部署应用。

目前平台支持的架构环境中已集成的公有应用模板包括：MariaDB、MySQL、Tomcat、SonarQube、bookinfo 和 WordPress。



应用商店

4.3.7 纳管虚拟化平台

4.3.7.1 云主机管理

云主机管理模块提供云主机的创建、操作、查询、管理等功能。可同步已纳管的底层虚拟化平台（ICS、VMWare）中的 VM 状态，云海支持查看整个虚拟化环境中所有 VM 的状态、资源配置及使用情况、所属等基本信息。可以创建指定配置的空云主机，空云主机没有操作系统，需要后期自己安装，将云主机分配给指定 VDC 或用户使用。支持云主机的开启、关闭、移除、强制关闭、删除、编辑、快照、打开控制台、挂载 VMtools 等操作。

4.3.7.2 镜像库

镜像库针对 VMware 和 ICS，用于提供创建云主机或者给云主机安装操作系统时所使用的镜像。镜像库包括公共镜像库和私有镜像库两种类型，公共镜像库可供属于同一个资源池的所有成员使用，私有镜像库仅限一个 VDC 使用。可按需添加和删

除镜像库，并对镜像库信息进行编辑。镜像库中可对镜像文件进行管理，包含上传、下载、删除等。

4.3.7.3 网络管理

可对 VMware、ICS 平台设置基础网络，提供二层 VLAN 隔离网络，创建基础网络，配置网络所使用的交换机、VLAN ID、网络地址等功能，创建好的基础网络可修改。

对 ICS 纳管，平台提供虚拟私有网络（Virtual Private Cloud，简称 VPC），可以通过软件定义的方式构建一个由子网、路由、ACL、弹性 IP 等组成的灵活、安全的私有云网络空间。用户使用 VPC 管理自己的网络资源，不同的 VPC 之间网络隔离，为用户提供独立的封闭的网络。每个 VPC 都有一个 vlan 范围和网段，属于 VPC 的虚拟网络，必须在 VPC 和 vlan 和网段范围内。两个 VPC 之前可以通过对等链接进行网络互联，建立对等连接后，在 VPC 之间可以使用私有 IP 地址通信，两个 VPC 中云主机之间的通信就像在同一个网络中一样。用户可按需创建子网，批量设置 DNS 信息。通过 ACL 规则提供 VPC 网络的访问控制服务。通过端口映射，让 VPC 网络内云主机对外提供服务。提供对弹性 IP 和弹性 IP 池的创建、管理、查询，弹性 IP 是指外部网络的 IP 地址，一般是从运营商购买的公网 IP 地址，系统内的云主机可通过弹性 IP 访问外网。弹性 IP 池是弹性 IP 的集合，包含一组弹性 IP，弹性 IP 池关联一个线路类型。

4.3.8 跨云迁移

4.3.8.1 VMWare 迁移

平台提供跨云迁移能力，通过便捷的界面操作，可将利旧的 VMWare 资源迁移到浪潮云平台，无需再目标虚拟机安装代理。跨云迁移虚拟机，打破平台界限，使得不同平台版本，不同地域的数据中心资源的维护与更加便利。

VMWare to Inspur 简称 V2I，实现 VMWare 虚拟机向 InCloud OS 一键在线迁移，全过程无人工干预，业务无感知，帮助用户把原有的 VMWare 平台资源。

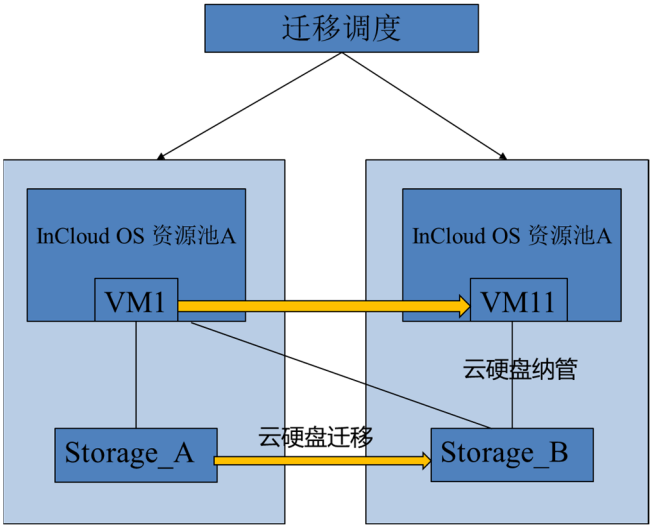
虚拟机迁移支持在线迁移和离线迁移，其中虚拟机在线迁移过程中业务不会中断，亦无需购买额外的第三方迁移服务。支持迁移限速。

迁移前需确保 OpenStack 资源池中已具有迁移代理云主机以及已配置迁移站点。迁移代理即部署有跨云迁移代理程序的云主机，用来拷贝云主机数据；站点即需要迁移云主机的 VMWare vCenter。

新建站点

4.3.8.2 OpenStack 迁移

在同一区域(Region)下 ,把业务虚拟机从一个云资源池离线迁移到另一个资源池（跨 OpenStack 资源池迁移），平台提供虚拟机跨 Openstack 资源池的迁移功能，无需借助第三方工具、无需在源云主机安装代理 ,在平台管理界面内即可将其它资源池虚拟机迁移到本平台内，迁移后可以保证云主机的 IP 和 MAC 保持不变。



跨资源池迁移

4.3.9 服务工厂

通过服务工厂，用户可以创建和集中管理平台中部署的云服务，实现云服务的一致性管理和配置，提供计算、网络、存储、容器、数据库、中间件、大数据、AI、云安全等核心服务能力，全方面满足用户各种应用场景。

在服务工厂中，可定义和上线多种类型、多种规格的服务供租户端申请使用，包括基于传统应用包定义常用服务（MariaDB、MongoDB、Mysql、Redis 等）、基于服务镜像创建的安全服务（堡垒机、日志审计、漏洞扫描等）、线下服务、外接第三方大数据和人工智能服务。

4.3.9.1 服务实例

服务实例即是一个具体的数据库等服务，根据服务规格创建服务实例，为使用者提供一个通用的服务操作管理界面。它是根据服务目录和规格创建的服务，本页面为用户了提供一个通用的服务操作管理入口。

4.3.9.2 服务目录

服务目录是一个云计算环境中的应用交付与运营管理门户，包含用户发布的适用于各种应用场景且开箱即用的服务。让用户聚焦具体应用场景，一键部署场景化业务服务。

4.3.9.3 服务定义

服务定义是一个云计算环境中的应用交付与运营管理门户，包含一整套用来开发云应用及云化已有应用的框架。让用户聚焦具体应用场景，快速组装场景化业务服务。帮助用户高效的开发、部署、运维及管理所提供的应用。

服务包

为用户提供基于云主机的一系列常用集群版和单机版应用服务，如 MySQL 数据库服务云主机版、MariaDB 数据库服务单机版和主从版，Zookeeper、Tomcat 中间件，Kafka 消息队列等。支持访问软件包仓库控制台，配置浮动 IP；支持同源异构，根据架构信息动态筛选镜像和服务安装包；支持 NamedManager-DNS 服务。

用户创建服务的流程如下：

6. 将已备好的基础镜像和仓库镜像上传至系统中。

7. 基于仓库镜像创建软件包仓库。

   软件包仓库中初始包含内置服务所需的软件包，若用户需要其他服务时，可将所需软件包上传至软件包仓库。

8. 基于服务定义文件创建服务。

服务定义文件中定义了服务的基本属性，以及基于服务创建实例所需要的基础镜像、软件包、服务规格、执行的脚本及操作等等。

9. 将服务发布上线，租户端才可以看到并申请使用服务。

服务列表：

服务列表是一个应用交付与运营管理门户，包含一整套用来开发常用云应用及云化已有常用应用的框架，让用户聚焦具体应用场景，快速组装场景化业务服务，帮助用户高效的开发、部署、运维及管理所提供的常用应用。

支持查看服务的基本信息、实例列表、规格列表、操作日志等信息。

支持创建服务、边界服务、发布服务、下架服务、删除服务。

白名单：只有在白名单中的 VDC 用户可以成功申请创建该服务实例，支持开启/关闭服务白名单。

仓库配置：

通过仓库配置，集中配置管理镜像及软件包仓库。

基础镜像：仓库镜像用于创建软件包仓库；软件包仓库本质上是一台云主机，用于存放内置服务所需要的软件包，包括 Redis、MariaDB。基础镜像用于创建服务实例，基础镜像上传后会自动关联到内置服务。目前，系统只支持使用随版本发布的仓库镜像和基础镜像，可联系运维支持人员获取镜像的存放路径。

软件包仓库：软件包仓库是基于仓库镜像创建的云主机，用于统一存放系统内置服务所需的应用软件包，以便用户创建内置服务实例时获取和使用。

服务镜像：

针对安全合作厂商提供的基于云主机的服务镜像,提供内置的安全服务目录,包括堡垒机、WAF、漏洞扫描等。根据架构信息动态筛选镜像，服务镜像修改为“服务镜像”。

使得安全服务目录可用的流程如下：

1. 将已备好的服务镜像上传至镜像仓库中，待系统自动同步安全服务的状态。

2. 将安全服务发布上线，租户端才可以看到并申请使用服务。

安全服务列表：

包含一整套用来开发云应用及云化已有安全应用的框架，让用户聚焦具体应用场景,快速组装场景化安全服务,帮助用户高效的开发、部署、运维及管理所提供的安全应用。

支持查看服务的基本信息、实例列表、规格列表、操作日志等信息。

支持发布服务、下架服务、删除服务。

白名单：只有在白名单中的 VDC 用户可以成功申请创建该服务实例，支持开启/关闭服务白名单。

镜像仓库：

系统提供服务镜像管理功能，以便统一管理用于创建安全服务目录的镜像。

支持上传镜像、删除镜像；

服务中介

服务中介，又称 Service Broker，可以接入符合 OSB（Open Service Broker）

规范的第三方开放服务。系统预置了基于浪潮大数据 Insight 和人工智能 AIStation 平台所提供大数据服务和 AI 服务；也提供专享容器集群，无缝接入已部署的容器平台 Kubernetes ,为用户提供开源容器服务。注册镜像支持标注芯片架构和芯片厂商。

内置专享 Insight/AI 集群服务，使用前，需要先在 OpenStack 资源池中使用命令行上传镜像到 glance，上传后，注册镜像以正式提供对应服务。

支持发布、下架专享 Insight/AI 集群服务。

- 支持查看服务的基本信息、实例列表、规格列表、操作日志等信息。
- 支持发布服务、下架服务、删除服务。
- 支持开启/关闭服务白名单。

线下产品

线下服务（Offline Service）是基于线下产品所提供的线下服务。针对一些不能在 InCloud OS 上自动编排发放的服务，提供在 InCloud OS 线上申请、审批，执行结果反馈，线下开通执行的功能。具体的服务实施在线下进行，与 InCloud OS 没有任何关系，InCloud OS 只是为用户提供了一个统一申请、审批、结果反馈和线下资源管理的平台。

- 支持查看服务的基本信息、实例列表、规格列表、操作日志等信息；
- 支持创建线下服务、发布服务、下架服务、删除服务；
- 支持对服务可使用的规格进行统一配置管理；
- 支持开启/关闭服务白名单。

生态服务

提供内置生态服务，包括云原生数据库服务、AI 训练服务、AI 推理服务、大数据服务，配置系统连接信息，以对接服务，发布服务，开通服务，下架服务，查看服务详情，包括基本信息、已开通服务的 VDC、资源审计、操作日志。

为用户提供一系列第三方生态服务，包括：

云原生数据库服务：对接基于云原生技术研发的多数据库应用平台——沃趣数据库 QFusion，提供标准的、统一的、可扩展的数据库平台级服务。

大数据服务：对接浪潮大数据平台 Insight，提供分布式大数据平台服务，支持海量数据的存储以及离线处理、实时流处理、搜索、在线查询、数据挖掘。

AI 推理服务 :对接浪潮人工智能推理平台 AIStation ,为企业 AI 用户提供可靠、易用、灵活的推理服务部署及计算资源管理平台，提升 AI 计算设备的利用效率，通过统一网关管控、应用业务流编排、边端扩展打通等策略，加速 AI 应用的场景化、规模化落地。

AI 训练服务：对接浪潮人工智能训练平台 AIStation，面向训练场景的人工智能开发资源平台服务 ,为用户提供极致高性能的 AI 计算资源 ,实现高效的计算力支撑、精准的资源管理和调度、敏捷的数据整合及加速、流程化的 AI 场景及业务整合，有效打通开发环境、计算资源与数据资源。

4.3.10 大数据服务

依赖于浪潮大数据平台 Insight。

大数据服务提供针对海量（TB/PB 级）数据的分布式处理服务。可以使用户能够轻松跨越大数据分布式计算环境搭建、运维的技术门槛和繁琐工作 ,直接专注于数

据分析、数据挖掘、商业智能等应用场景。服务包含了大数据处理的主流技术组件，如 Hadoop、HBase、Hive、Yarn 等，提供了从自动化部署运维、性能优化、资源隔离、资源调度、数据计算任务执行及跟踪等全套解决方案。

支持一键创建 EMR 服务，EMR 服务支持存储扩容，启动/关闭 EMR 服务。

专享大数据集群：

支持一键创建专享的大数据集群。

共享大数据集群：

可无缝接入用户已部署的一个大数据分布式计算环境（Insight），基于该环境提供以下功能特性：

- SSO 登录：支持单点登录，实现统一纳管。
- 秒级发放：通过逻辑多租户，在线申请，实现一键发放，即开即用。
- 组合隔离：支持 YARN 资源（CPU 和内存）、HDFS 存储资配额申请，租户间的资源相互隔离互不干扰。支持 Hbase、Hive 等数据权限隔离。
- 简单易用：开发人员和 ISV 无需关注大数据平台的搭建和运维；轻松使用 Hadoop、HBase、Kafka 等大数据组件。

4.3.11 AI 服务

支持基于浪潮 AIStation(面向人工智能企业训练场景的人工智能开发资源平台）发布人工智能服务 ,租户可在自服务门户申请人工智能服务 ,支持 TensorFlow、Caffe、MxNET、PyTorch、Paddlepaddle 等多种深度学习框架，支持训练任务的提交和开发环境的管理、训练任务的可视化管理。

专享 AI 集群：

支持一键创建租户专享的 AI 集群。

共享 AI 集群：

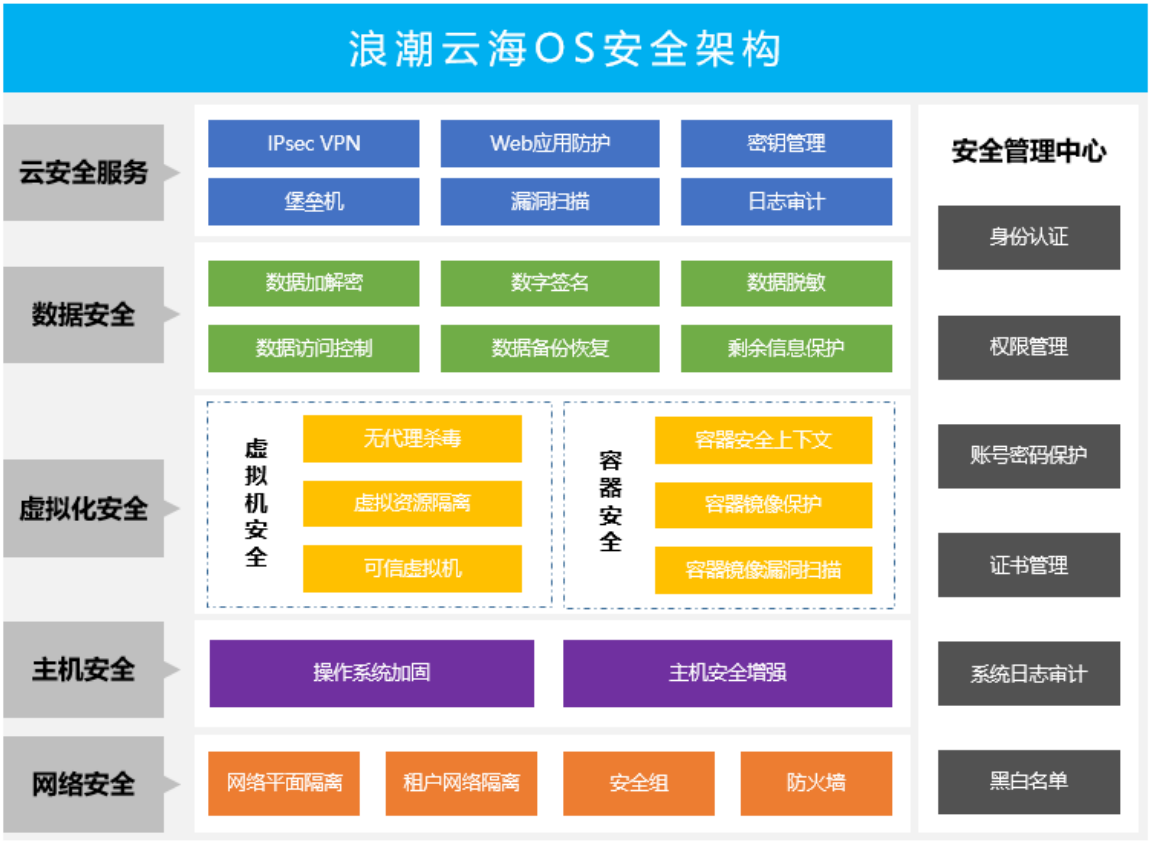
可无缝接入用户已部署的人工智能平台（AIStation），基于该环境提供以下功能特性：

- 支持单点登录，实现统一纳管。
- 统计个人 Cpu/Gpu/存储的已用情况。
- 查看用户组和集群资源情况。
- 个人开发环境资源统计和列表信息。
- 个人训练任务的提交、结果查看等。

面向 AI 企业训练场景，拉通用户开发环境、计算资源、数据资源，构建一体化 AI 开发平台，为 AI 工程师提供计算资源和开发训练服务。

4.3.12 云安全服务

云安全服务是浪潮云海平台“平台+生态”的能力体现，通过“开放、融合”的标准规范，将经过云化的安全产品与基于浪潮云管理平台服务目录相融合，可为云平台及租户提供虚拟化版的 WEB 防火墙、漏洞扫描系统、密钥管理系统、日志审计系统等以 VM 方式运行的安全资源服务。



浪潮云海 OS 总体安全架构

总体支持以下功能特性：

- **资源隔离的服务实例管理**

服务实例是独立的安全实例，独占 CPU、内存和磁盘 IO。允许用户创建属于自己的服务实例，并可对每个服务实例进行启停、配置修改、规格调整、授权激活和删除等管理操作。

- **可视化监控及报警**

开发者可以通过可视化界面查看资源使用情况，当 CPU、内存、存储超过指定值时，会发送报警消息给指定联系人。

- **可信登录**

云平台和每个通过安全服务创建的实例支持双向身份验证和密钥校验，从而实现身份的可信任性,用户可通过云平台登录接口,直接免认证登录第三方安全产品的访问控制台。

4.3.12.1 密钥管理

InCloud OS 集成的虚拟化密钥管理系统服务是三未信安基于云海平台标准规范深度定制化的云化安全产品,系统支持对称密钥、非对称密钥、数字证书和认证令牌等多种加密对象的管理，通过提供丰富的加密接口类型和密钥管理互操作协议（KMIP）,云用户只需部署一套密钥管理系统就可以管理VDC内部中所有加密系统。

- 提供海量密钥管理，可支持千万级密钥量。
- 提供密钥生命周期管理,支持国密和国际算法,提供基于 KMIP 协议的密钥全生命周期管理，包括密钥生成、存储、使用、导入/导出、轮转、备份/恢复、归档和销毁等。
- 支持 KMIP 协议，可与所有支持 KMIP 的加密客户端无缝对接。
- 具备丰富的密钥接口 API,包括国密、JCE、PKCS#11、REST 等,供云上业务系统调用。
- 支持对称密钥、非对称密钥、数字证书和 CA 等多种对象的有效管理。
- 提供加解密、签名验证等密码运算功能。
- 支持基于 Ukey、口令、证书对用户做身份认证。
- 支持设定访问策略实现对密钥的访问与授权。
- 支持对数据库、存储、大数据、应用做加密扩展方案。

注意：该系统使用需要配置密码机或者密码卡。

4.3.12.2 漏洞扫描

InCloud OS 集成的虚拟化漏洞扫描系统服务是绿盟科技基于云海平台标准规范深度定制化的云化安全产品，可为云资产提供高效、全方位的检测，发现网络中的各类脆弱性风险，并提供专业、有效的安全分析和修补建议，贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面，是租户做安全漏洞管理的专业技术工具。

漏洞库支持：漏兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准。

操作系统漏扫：支持对传统 X86 操作系统、创新操作系统，及相关应用及软件的远程安全评估。

DNS 服务漏扫：支持对 DNS 服务的安全漏洞的专门检测功能。

数据库漏扫：支持 DB2、Oracle、MySQL、MSSQL、Sybase 数据库漏洞检查。

弱口令检测：具备专门的口令猜测扫描功能，可对多种协议的口令猜测方式进行扫描，包括利用 SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQLSERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP 等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。

Web 应用漏扫：提供多种 Web 应用漏洞的安全检测，如 SQL 注入、跨站脚本、网站挂马、网页木马、CGI 漏洞等。

补丁联动：支持和微软 WSUS 补丁系统的联动，能够在发给主机管理员的邮件中附带自动配置 WSUS 的注册表文件，方便进行自动化的补丁修补。

支持扩展大数据、物联网、云计算、容器等漏洞扫描。

4.3.12.3 日志审计

InCloud OS 集成的虚拟化漏洞扫描系统服务是绿盟科技基于云海平台标准规范深度定制化的云化安全产品，可为云租户的异构日志进行高效采集、统一管理、集中存储、统计分析，可协助租户满足等保合规要求、高效统一管理资产日志并为安全事件的事后取证提供依据。

满足合规性要求：满足《中华人民共和国网络安全法》、《网络安全等级保护基本要求》等法律法规的安全监管要求。

支持多种采集方式：支持 SYSLOG、SNMP Trap、FTP、JDBC 等多种日志采集方式。

支持异构日志管理：基于主流协议实时采集的安全、网络、虚拟机以及各种应用系统产生的日志信息，解决日志分散存储、数据量大、格式不统一带来的日志分析困难的问题。

支持数据强化：通过数据的过滤和强化，丢弃无用信息，提升日志查询和分析效率。

海量日志处理：使用并发内存内处理机制和离线计算引擎，在小时级别内可完成海量日志处理。

4.3.12.4 WAF

InCloud OS 集成的虚拟化 WEB 防火墙服务是联合绿盟科技基于云海平台标准

规范深度定制化的云化安全产品，产品将客户资产作为组织 Web 安全解决方案的依据，采用黑、白名单机制相结合的完整防护体系，通过精细的配置将多种 Web 安全检测方法连结成一套完整的解决方案，并整合成熟的 DDoS 攻击抵御机制，能够在 IPV4、IPV6 及二者混合环境中抵御 OWSASP Top10 等各类 Web 安全威胁和拒绝服务攻击，保卫您的 Web 应用免遭当前和未来的安全威胁。

1. WEB 基础防护：支持 XSS、CSRF、SQL 注入、命令注入、VM 漏洞利用等 Web 攻击防护，全面覆盖 OWASP TOP10 的攻击类型。
2. Web 流量检测防护：支持 XML 实体攻击防护、XML DDOS 防护，对 XML 文件、SOAP 流量进行合规检测，保障 API 的安全调用。
3. 0day 防护：具备云上海量威胁情报能力，实时感知最新攻击手段变化。
4. 自学习+白名单：基于自学习技术呈现业务逻辑关系和流量模型，协助管理员构建白名单。
5. Web 防篡改：自动检测网页是否被篡改，一旦篡改，对外仍显示正常页面。

4.3.13 公有云平台管理

提供公有云（阿里云）平台管理模块，支持对公有云（阿里）的虚拟机、网络、对象存储、负载均衡器等资源进行统一管理，集中监控。

可将已有公有云资源一键导入系统管理，且平台支持公有云平台中资源的概览，通过资源概览可一览阿里云中各类资源的数量、云主机的监控情况和近一个月内云主机的数量曲线图。

资源概览

4.3.13.1 云主机

云主机管理模块提供阿里云 ECS 实例管理能力 ,包括 ECS 实例的创建、导入、开关机、重启、删除、移除修改 VNC 密码等操作。

系统支持创建阿里云 ECS 实例，且支持批量创建，创建时可指定可用区域、配置系统盘（高效云盘、SSD 云盘）、配置多达 16 块高效云盘作为数据盘、配置 VNC 密码、配置 VPC 以及公网带宽收费标准等。

导入 ECS 实例：支持将用户在阿里云上已有的云主机导入到系统中进行统一管理。

ECS 生命周期管理：支持 ECS 实例开关机、删除、移除操作。

修改 ECS 实例 VNC 密码：支持修改已创建/纳管的 ECS 实例的 VNC 密码。

4.3.13.2 虚拟私有云

系统提供了公有公有云(阿里云)网络管理能力 ,用户可以在系统上创建阿里云的 VPC 网络，设置 VPC 的 CIDR 范围，用来限制 L3 层网络的 IP 地址范围，支持 VPC 网络内添加虚拟交换机给阿里云虚拟机使用。

支持创建、删除网络资源 ,VPC 网络指定地域和一个大的 IP 段 ,支持查看对应操作日志、审计日志。

支持创建、删除交换机资源 ,交换机属于网络 ,交换机指定了可用区和一个小范围的 IP 地址段，支持查看对应操作日志、审计日志。

4.3.13.3 安全组

用户可通过安全组中安全组规则的配置对流入和流出云主机网卡的网络流量进行检测和过滤，以保护云主机通信安全。

支持安全组的创建、修改、删除，创建和删除安全组规则。

4.3.13.4 负载均衡

负载均衡是一种流量分发控制服务，可根据转发策略将访问流量分发到后端多台实例 (云主机), 系统提供阿里云负载均衡管理模块，用户可以在系统上创建阿里云的负载均衡器。

支持负载均衡的创建、修改、删除操作 ,可查看对应操作日志、审计日志。可以选择创建的实例规格 ,支持按照流量计费或者按固定带宽计费 ;可以设置负载均衡的地址类型，比如：公网、私网；调度算法支持加权轮询、最小连接数、轮询；支持

TCP/UDP/HTTP 三种协议。

可以在负载均衡内添加监听器，并设置监听端口；为负载均衡添加控制器；为负载均衡器添加后端虚拟节点，并可以设置虚拟机的端口和权重；设置默认服务器组。

默认服务器组是一组用来接收负载均衡实例中监听器转发的前端请求的云主机。若监听器中仅配置了默认服务器组，则默认将请求转发至默认服务器组中的云主机。

4.3.13.5 对象存储

对象存储为公有云平台中的资源数据提供海量的存储空间，系统提供阿里云对象存储管理模块，用户可以在系统上创建并管理阿里云的对下存储。

支持对象存储的创建、导入、修改、删除操作，可查看对应操作日志、审计日志。

对象存储桶的管理包括桶的创建、删除、修改、查询和导入，可设置桶的读写权限，包括私有、公有读、公有读写。支持选择存储类型包括标准存储、低频存储，可设置桶内对象个数和容量（单位 G）。

支持桶内创建目录、上传文件、删除文件、修改文件、下载文件、返回上一级等操作。支持按照名称模糊查询。

读写权限：设置文件的读写权限。

继承 Bucket：文件的读写权限与存储桶的读写权限一致。

私有：仅允许存储桶的所有者对该文件进行读写操作。

公共读：仅允许存储桶的所有者对文件进行写操作；所有用户均可读取该文件。

公共读写：所有用户均可对该文件进行读写操作。

存储类型：文件的存储类型。

标准存储：高可靠、高可用、高性能，经常被访问到。

低频存储：长期存储，较少访问，存储单价低于标准存储。

归档存储：长期存储，基本不访问，存储单价低于低频存储。

4.3.14 数据库服务

数据库服务提供稳定可靠、高效易用、资源弹性可伸缩的云数据库服务，支持MySQL、MongoDB、Redis 等多种数据库引擎。

数据库服务支持多租户模式，可为每个用户创建一到多个实例。提供资源隔离的服务实例管理，用户可通过提供的访问链接访问数据库服务器，可自主控制访问数据集、操作方便的数据库管理。支持对数据库节点的监控与告警。

4.4 容灾

4.4.1 单中心双活卷

通过单个 InCloud OS 资源池对接两个存储设备，部署为一套双活存储集群，当主存储意外宕机时，双活存储集群通过内部的主备故障切换，持续提供存储 IO，做到云硬盘对应的云主机业务无中断、无感知，数据零丢失。做到 RPO=0，RTO=0。

4.4.2 同城双中心主备

建设两个中心：一个生产中心，一个灾备中心；两个中心建议建设在同城，在同城内可以保证存储数据同步和网络通信。主中心承载全部业务，备中心承载核心业务的备份，业务运行在主中心，在主中心故障时，在备中心恢复容灾保护的业务，对外

提供服务，主备模式支持存储的同步复制（RPO=0）或异步复制（RPO 约等于零）。

主备中心存储系统通过波分设备或者 IP 专线进行数据的远程复制，云管理平台通过三层网络管理双中心的资源，客户通过互联网或者企业网访问业务系统，并能够基于负载均衡进行故障切换后继续访问。

4.4.3 双中心双活

双中心双活利用存储双活技术，通过双中心的两套 G5 存储部署双活集群时间数据在双中心的双活，配合业务双活，通过上层全局负载均衡，实现真正的双中心业务双活。

在双活中心任意中心发生故障时，底层数据通过双活存储集群自动进行故障切换，保证数据零丢失，IO 不中断。上层全局负载均衡通过故障监测，切断故障中心云主机的负载，保证业务持续提供服务，RPO=0，RTO=0。

4.4.4 本地双活卷+异地远程复制双中心

高级双中心灾备在单中心双活的基础上增加远程容灾能力，在主中心一个存储设备意外宕机时故障自动切换，启用容灾保护的云主机可做到数据零丢失，业务无中断无感知，在主中心整体故障时或计划内维护时，最大限度保障业务连续性，保障客户关键数据不丢失，启用容灾保护的云主机可在备中心一键拉起，对外提供服务。

主中心单个存储故障时可做到 RPO=0，RTO=0，主中心整体故障时可做到 RPO>0,RTO>0，其中 RPO 取决于主中心到备中心异步复制的周期（1 分钟-7 天，可根据客户实际情况配置），RTO 为发现主中心业务失败时间加上拉起备中心业务云主机的总时间。

4.4.5 两地三中心

两地三中心在同城环境双中心中任意中心发生故障能够保障客户关键数据不丢失，最大限度保障业务连续性，在同城双中心均发生故障或发生大规模灾难时，可通过异地第三中心拉起业务云主机，持续对外提供服务，最大限度的保障客户关键数据。

两地三中心可在同城双中心灾备或者同城双中心双活的基础上部署，增加异地第三中心，通过异步复制周期性向异地第三中心同步数据。

其中同城双中心灾备方式的场景下：

同城一个中心发生故障或者意外宕机，可在备中心一键拉起业务云主机，实现RPO=0,RTO>0；同城双中心均发生故障时，可拉起异地容灾云主机，实现RPO>0,RTP>0。

同城双中心为双活的场景下：

因为同城双中心双活与业务紧密结合，配合全局负载均衡，可做到主中心故障时自动切换，RPO=0，RTO=0；在同城双中心均发生故障时，可通过拉起异地容灾云主机，持续对外提供服务，实现 RTO>0，RPO>0。

异地容灾 RTO 为发现主中心业务失败时间加上拉起备中心业务云主机的总时间；RPO 容灾策略的同步周期间隔（可根据用户场景配置，1 分钟-7 天）。

4.4.6 容灾服务

当系统的主运行环境因意外（火灾、地震等）停止工作时，可将整个系统切换到

拎一个运行环境工作,使得系统可以继续正常提供服务。容灾服务以保护组为单位进行相关业务处理，将同一虚拟数据中心下的一个或多个云主机根据实际情况创建为保护组。

平台提供计划性切换，容灾演练等高级能力。CMP（云管平台）主备容灾，即在生成中心和灾备中心各部署一套云管平台,通过数据复制技术,将生产环境数据复制到灾备环境，保证两侧数据一致。生产环境 CMP 承载正常的业务操作，备 CMP 正常情况下不启用，上面不进行任务操作。当生产环境 CMP 由于各种原因（病毒、硬件故障、断电、火灾、地震等）发生故障时，备 CMP 启用，接管原有应用，对外提供服务。

可进行相关操作：

- 保护组创建&查询&删除&修改；
- 对保护实例执行开启保护&关闭保护&主备切换&故障切换&重保护。
- 计划性切换，对保护组的主备切换进行计划性管理。

容灾演练

当保护组处于对“保护中”状态时，可对其容灾站点内的备云主机进行容灾演练，验证备云主机的可用性。

容灾脚本管理

为用户提供容灾脚本及脚本的管理能力。

用户可根据业务需求创建对应脚本用于容灾业务的自启动、服务管理等,实现容灾业务的自定义。

可进行相关操作：

容灾演练历史

记录容灾演练的历史记录，支持导出报表、报告。

容灾参数配置

容灾服务使用前必须在此配置主备资源池的对应关系，且两个资源池所使用的云硬盘存储池必须已在底层建立了远程复制连接。

置容灾名称、主备资源池、主备云硬盘类型等。

4.5 云监控

随着客户系统和业务规模的快速提升,对如何高效、快速及灵活的实现对系统和业务进行监控和告警的需求越来越迫切。一方面要保证服务的高可用、高性能、可扩展，另一面要定制灵活、用户友好，提高异常处理效率，降低损失。

InCloud OS 监控告警系统提供大规模系统的监控、告警、通知和数据分析等服务，具有高可用、高性能、精细化、可扩展、智能化和用户友好等特点，帮助用户打造稳定可靠、定制灵活、准实时的监控告警服务。

监控告警系统提供精细化功能服务，包括数据展示、业务管理、数据处理、数据存储和数据采集等,及时准确地监控整个系统运行情况,提高系统异常处理的响应速度，提升运维效率，降低系统维护成本，有效保证用户业务的高可靠性。

- 数据展示包括大屏展示、性能数据展示、告警记录、实时通知和分析报表等。
- 业务管理包括资源管理、配置管理、模板管理、脚本管理、告警管理、通知

管理，拥有良好的用户操作界面和业务自动化的处理方式。

- 数据处理包括支持采集、告警、通知配置生成和分发；告警、通知、数据接口和任务调度的业务功能；数据挖掘和智能处理。其中告警通知采用常规模式、智能模式通过设置告警阀值合理解决问题；智能处理中引入人工智能和机器学习算法，支持异常检测、定位、分析、预警和故障发现、止损、修复、归并等处理流程。
- 数据存储采用时序数据库实现数据快速存储，采用数据流分层处理的方式加快数据处理速度，采用分布式缓存、消息队列等技术解决大数据并发传输。
- 数据采集包括带内、集中采集、代理采集等多种方式，拥有异构设备的数据采集能力，采用插件的方式，实现采集、告警、分析的可扩展性；支持批量上传采集端数据以缓解数据存储的压力。

4.5.1 大规模监控

InCloud OS 监控系统支持丰富的采集插件，可以采集到集群中关键数据，具体包括 InCloud OS 系统本身（宿主机、云主机、集群、容器、核心服务、虚拟路由器）、原生 OpenStack（宿主机、云主机、集群、核心服务）、原生 K8S（宿主机、容器、容器组、应用、核心服务）、操作系统、数据库、存储服务、中间件、CEPH 存储等

此外，集成 ISPIM 后 InCloud OS 支持面向行业数据中心的硬件智能运维管理，具备资源管理、故障监控、性能监控、能耗管理、 报表统计、拓扑展示等功能，可以实现服务器、 机柜、刀箱、一体机、边缘设备、 网络设备、 安全设备、存储等设备的统一管理。

InCloud OS 通过提供全面、统一、多维度的管理监控子系统，可以管理监控数据中心的海量异构资源，包括服务器、存储、网络设备等硬件资源，各种操作系统、数据库、虚拟资源等软件资源；并且能够及时发现故障产生的告警，有效提高故障处理响应速度，降低运维成本。

运营管理员配置各平台及服务实例资源的监控项及告警策略。系统将基于监控告警策略，自动进行资源监控和告警。

4.5.2 趋势预测

云平台往往需要根据业务的诉求对未来做出合理的规划，包括扩容的预测，缩容的预测等。以往基本采用人工预测的方式，但运维人员的能力可能存在差异，使得结果不尽如人意。云平台的性能数据多为平稳时间序列或可转换为平稳时间序列，可以进行预测。但另一方面单一的预测算法，对一种数据预测效果可能很好，对另一种可能很差。趋势预测包含对云平台的重点指标与对单一资源指标进行曲线拟合，实现了时间序列数据的预测，从而实现了云平台重点指标提前异常预警的效果。

4.5.3 无阈值异常检测

传统云平台的性能监控都采用阈值告警，即运维人员根据经验设置告警阈值，当监控数据达到此阈值时，产生告警。但实际的应用过程中发现，阈值设置太依赖于经验，阈值太高，漏掉的告警过多，质量隐患难以发现；阈值太低，告警太多往往引发告警风暴，干扰运维人员的判断。另外，对于一些性能数据抖动的情况，阈值告警也无法检测，产生漏报。InCloud OS 监控将无阈值检测作为阈值告警的补充，很好的解决了上述问题。

4.5.4 日志系统

随着客户系统和业务规模的快速提升，对如何高效、快速及灵活的实现对系统和业务日志进行管理、检索和分析的需求越来越迫切。当系统发生故障或出现性能瓶颈时，需要通过分析各种日志来定位故障原因，找出导致系统性能瓶颈。

平台通过提供全面、多维度的日志系统，可以管理 OpenStack/K8S 集群的海量日志数据，包括操作系统日志、核心服务日志（如 Mysql、RabbitMQ 集群）、OpenStack 组件日志和 K8S 组件日志，在此基础上支持主机日志分析、组件日志分析、主要组件调用错误、主要组件 RabbitMQ 调用错误、主要组件 MYSQL 调用错误和云主机创建调用链等核心分析功能，有效提高故障处理响应速度，节省运维成本。

同时，日志系统也具备日志上报功能。在云平台的日志采集客户端通过配置目标 syslog 服务器的主机和端口将格式化后的日志发送到指定位置。

4.5.5 资源画像

如何资源规格一直以来都是困扰应用运维人员的关键问题，过高的资源规格会导致大量的资源浪费，而过低的规格又会为应用带来潜在的稳定性风险。InCloudOS 为负载提供了资源画像的能力，实现容器粒度的资源规格推荐，可以有效降低为 Pod 配置 Request 和 Limit 的复杂度。同时也可为物理资源提供画像，防止资源过度使用，为用户进行扩容、迁移负载等操作提供依据。

4.5.6 通知管理

通知管理提供联系人、时间表和通知历史的配置管理功能，当发生告警时，系统将在指定的时间以邮件或短信的方式通知相关联系人，以便其及时处理相关告警，保

障业务正常运行。

联系人管理

- 可添加新的或者导入平台中已有的用户为资源告警联系。
- 可设置联系人通知时间表。
- 自定义联系人通知方式，包括邮件和短信。
- 可设置通知状态，哪些级别告警需要通知到联系人。
- 设置通知策略，发送一定次数后不再发送。

时间表管理

可自定义时间表：持月、星期、时间段或者自定义时间范围，灵活的方式进行通知时间管理。

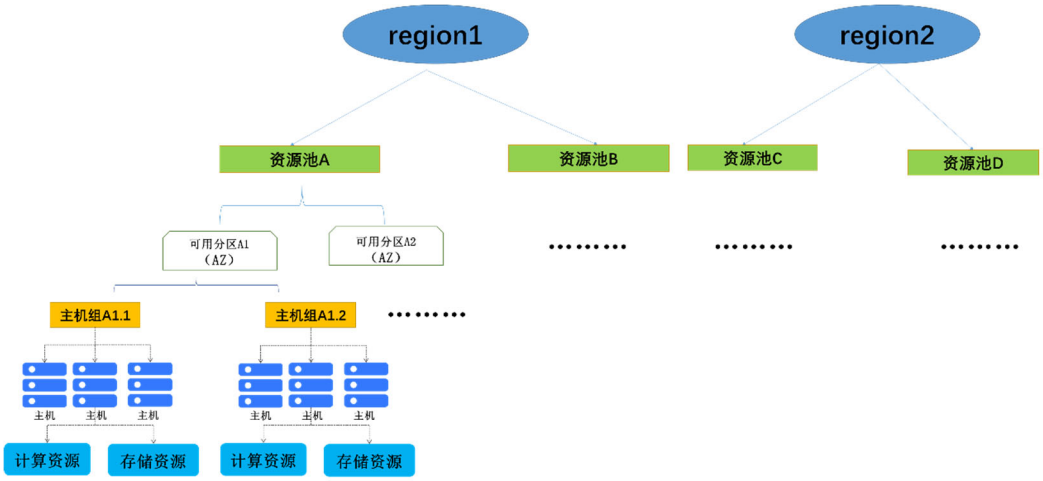
通知历史

对历史通知信息进行查询和管理操作。

4.6 运营管理

为用户提供系统内各类资源的分类统计，以便于其了解系统内资源的整体使用情况，同时可根据历史数据提资源的供优化建议和对未来资源消耗趋势预测，帮助客户对数据中心进行智能运营，及时调整资源。

4.6.1 资源组织



资源模型层级关系图

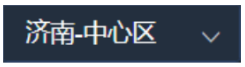
资源池是面向物理资源划分的概念。一个虚拟化资源池或者容器资源池是由共用一套控制平面的一组物理节点组成。

可用分区是用云规划的一个物理概念，可以简单理解为一组节点的集合，这组节点具有独立的电力供应设备，比如一个个独立供电的机房，一个个独立供电的机架都可以被划分成可用分区。

主机组是管理员用来根据硬件资源的某一属性来对硬件进行划分的功能，只对管理员可见，主要用来给 nova-scheduler 通过某一属性来进行虚拟机的调度。其主要功能就是实现根据某一属性来划分宿主机。

4.6.1.1 区域管理

区域（Region）是一个地理区域的概念，其覆盖范围为满足用户服务质量的一个物理数据中心，超出此区域则需要考虑另外建设一个数据中心来满足业务需求。一般情况下，不同的区域位于不同的地理位置，具有地理容灾等级，彼此之间互不影响。

	当系统为多区域部署时，可通过此功能进行区域切换，以查看和管理目标区域下的资源。

每个区域都有自己完整的部署环境，多个区域共享同一套用户和认证体系，用户可以在多个区域之间自由切换。 多区域部署的情况下，仅中心区域的运营管理员可进行区域管理。

运营管理员可切换或登录到指定区域，以查看指定区域首页内展示的资源统计数据。

4.6.1.2 用户管理

包括用户的添加、修改、删除、密码重置、启用、禁用、解锁、赋权、查看详情、自动同步 LDAP 用户信息等操作。

添加用户有两种方式：

（1）输入用户名、密码等信息添加用户，并为用户赋权。

（2）从 LDAP 选择一个或多个用户导入，并为导入的用户赋权。

用户分权分域管理：

一个用户可被赋予多个角色，可通过切换资源域或虚拟数据中心进入不同的管理界面，实现用户对不同域/虚拟数据中心的资源具有不同的操作权限。

LDAP 服务器配置管理支持添加、编辑、删除 LDAP 服务器，以同步管理 LDAP 用户；同时也支持手动同步功能。

4.6.1.3 虚拟数据中心

虚拟数据中心（VDC）是面向租户的从一个或者多个资源池中划分的资源和用户的集合。VDC 包含用户、资源、配额等信息。户所有的资源都是在某个 VDC 内，不同 VDC 之间的资源在逻辑上互相隔离。VDC 可以关联一个或多个资源池中的项目（Project）或命名空间（Namespace），项目或命名空间是 VDC 内资源组织和管理的最小单位。创建子级 VDC 时，只能继承父级 VDC 的资源配额和用户，必须新建项目或命名空间，而不能继承父级 VDC 的项目或命名空间。配置区域范围：添加、移除区域。

- 平台支持虚拟数据中心的添加、修改、删除、维护成员、启用、禁用、修改配额、资源绑定、查看详情等操作，支持树形展示所有用户、按条件查询本地用户和 LDAP 用户。
- 可按照用户的实际组织结构划分多级虚拟数据中心，支持 VDC 分级。VDC 管理员可以根据组织内部架构，划分子 VDC。支持为不同的 VDC 分配资源配额，配额包括 CPU、内存、云主机个数等。

4.6.1.4 角色管理

内置 7 大角色：运营管理员、域管理员、虚拟数据中心管理员、虚拟数据中心用户、安全管理员、审计管理员、运维管理员。

- 运维管理员是负责云平台日常运维管理的角色，包括平台资源监控告警、健康巡检、日志分析、根因分析等，保障平台稳定运行。平台默认有一个全局的运维管理员，统一运维所有资源，满足统维需求。

- 运营管理员是负责平台资源和服务运营管理的角色,包括资源池管理、服务生命周期管理、运营流程设计和审批、组织机构定义、项目配额及平台的管理部分。
- 域管理员是负责本域内运营管理的角色,由运营管理员创建,只对本域内资源具备管理权限，实现分域分营。
- 安全管理员（三权分立模式部署）: 拥有管理端的用户赋权、角色管理、虚拟数据中心成员维护以及操作日志查询权限。
- 审计管理员（三权分立模式部署）: 拥有管理端的操作日志管理和日志设置权限，对系统的操作日志进行审计、维护。
- VDC 管理员是负责所属 VDC 及下级 VDC 资源管理的角色，对 VDC 下所有资源具有管理权限，包括 VDC 下的服务管理、资源监控告警、运营管理及 VDC 内的系统管理等。
- VDC 用户是当前用户资源管理的角色，只能管理和使用自己的资源，包括服务管理、资源监控告警、运营管理等。

角色的创建：

可自定义系统的管理员角色、某资源域的管理员角色,某虚拟数据中心的管理员角色及虚拟数据中心用户角色。

支持灵活的角色权限自定义。

角色定义

4.6.1.5 部门管理

部门为人员的组织单位，一个部门可以包含下级部门和用户；

支持本地部门、也可导入 LDAP 部门；查看本地部门和 LDAP 部门详情，包括基本信息及用户列表。

4.6.2 业务流程

4.6.2.1 订单管理

以审批人的角度展示系统中待审批处理的订单数据，并可进行相应的审批处理。

审批流程自动跳转，审批流程上的节点用户依次审批，申请产生后，系统自动发送邮件提醒审批人，并支持审批历史数据的查询。待审批流程到达最后一个节点，审批通过，资源即在后台被自动创建。打回申请支持驳回到发起人或者到审批上一节点。

以申请人角度，可以查询、展示提交的订单；查看订单信息详情，包括基本信息、详细信息、审批历史等，对订单也可以做出编辑、撤销、提交、删除的操作。

订单可追溯

从提交到资源创建完成，详细记录订单处理历史。

提供订单统计，支持从申请人、资源类型等不同方面统计。

流程管理

流程管理实现了系统中资源申请审批流程以及用户订单的管理，包括申请审批流程的增删改查、用户订单的流转及审批、各种维度的用户订单数据展示及统计。

可查询、展示业务流程，包括全局流程（全局可见）、域流程（域内可见）、VDC 流程（所属 VDC 可见），查看流程详情，包括基本信息和流程关系图。

平台内置一个系统流程：可修改，但禁止删除，缺省包含所有业务类型并由内置运营管理员账户审批。

流程自定义：

- 支持资源类型、流程节点以及审批人的自定义扩充。
- 支持串行、并行审批
- 可支持不少于 30 个审批节点。
- 支持按资源及人的维度统计、查询。
- 绑定业务类型并启用流程，以便租户可申请相关业务资源。

丰富的业务流程：

系统提供了申请服务实例、服务实例续期、申请虚拟数据中心、申请虚拟数据中心展期、申请云主机、申请云物理机、申请云硬盘、申请网络资源、申请文件存储、申请对象存储资源、申请注册用户等业务流程，可以每个流程自定义流程模板，管理员也可以设置一个全局模板，供租户使用。

平台支持实时提醒，通过邮件方式提醒用户进行处理，并对处理结果进行通知。

4.6.2.2 业务统计

可查看以业务类型、虚拟数据中心为统计单位汇总统计的系统中所有未被删除的订单数据。

4.6.2.3 购物车

平台提供购物车能力，并可管理购物车内业务，让用户（非管理者）能够根据自己的业务逻辑灵活的选择订单申请方式，可以订单直接提交，也可以暂存到购物车，方便后续统一处理预定业务资源。

购物车实现了批量提交功能，提高了订单申请、审批的效率。

4.6.3 工单管理

平台提供工单和工单类型的创建、修改、删除、查询等工单管理功能，以便用户客户快捷地提交相关问题及产品需求。

工单类型

运营管理员创建特定的工单类型（如虚拟机故障、网络故障、存储故障等），租户管理员/租户用户提交该类型工单，报告相关问题。

运营管理员可修改、删除已有工单类型。

工单

添加好工单类型之后，租户管理管理员可向运营管理员提交工单，租户用户可向租户管理员提交工单。

上级角色可接受待处理工单并处理，处理后可将工单置为解决状态。

上级角色接受待处理工单后可否决下级角色提交的工单。

租户管理管理员可将租户用户提交的工单向上转发给运营管理员进行处理。

当前用户可以在工单列表中查询、新建、撤回、删除工单。

处理历史

展示管理员/租户管理员处理过用户提交的工单记录。

4.6.4 报表管理

通过报表管理模块对系统资源的使用情况进行统计管理，并生成对应报表可供

用户历史存档。**报表中心**

云管理平台提供了云平台中各种资源（虚拟控制中心、集群、主机、云主机、存储、网络、负载均衡）的综合信息报表；云主机、虚拟机等资源的监控信息报表；多维度（虚拟数据中心、部门、个人）计量计费报表、业务订单报表、租户信息报表等多种报表类型。

- 云平台可以根据类别、资源以及对应的不同的查询维度生成对应的的报表信息。
- 云平台支持立即生成报表或指定生成时间生成对应的报表文件。
- 云平台支持生成 excel、pdf 或 PNG 格式的报表文件。

4.6.4.1.2 下载中心

报表生成后，用户可在下载中心下载对应的报表，可以设置报表保留天数；对于已经生成的报表可以删除。

4.6.4.1.3 自定义报表

支持自定义报表能力，用户可以按照实际的应用场景自定义数据报表，并对报表进行图形化的展现（饼图、柱状图、曲线、环形图、表格）。

能够更好的满足用户报表自定义场景。用户可按照自身的业务逻辑，快速准确的生产业务所需报表，满足决策者的各项动态需求。

支持报表的图形化展示和图形化导出，可以导出饼图、柱状图、曲线、环形图、表格，提升智能化运维能力。

4.6.5 计量计费

计量计费模块实现对部门、部门用户所使用系统资源(计算资源和存储资源)的统计，根据系统设置的单价、折扣等信息进行计费，以及出账后账单展示、余额查询及充值等功能。

支持多层次的资源使用情况统计，包括 CPU、内存、存储、网络、卷的实时使用量及历史使用量统计；让用户及时掌握自身资源使用情况，帮助 IT 部门实现由成本中心向价值中心的角色转变。

可设置不同资源的计费单价以及对不同虚拟数据中心不同资源设置计费优惠，设置余额提醒策略及欠费处理方式，帮助 IT 部门构建资源的价值体系、计费策略。

4.6.5.1 概览页

用户可通过“起始页”一览部门、用户和虚拟数据中心的消费情况，并查阅整体消费趋势；同时可以设置和查看部门、虚拟数据中心费用 TopN、用户费用占比 TopN 及费用趋势情况。

可设置时间范围、部门查询消费趋势。

4.6.5.2 账单

- 部门账单

提供统一管理界面，查看部门总账及消费详情：即用户、使用的资源、产生的费用及费用占比信息。

- 虚拟数据中心账单

提供统一管理界面，查看虚拟数据中心总账及消费详情：即资源、资源的指标、产生的费用及费用占比信息。

提供该虚拟数据中心下所有用户的账单消费详情。

- 用户账单

提供统一管理界面，查看用户总账及消费详情：即用户、虚拟数据中心、资源、资源的指标、产生的费用及费用占比信息。

4.6.5.3 资源计量

提供统一管理界面，查看以虚拟数据中心、部门、用户为统计单位统计的资源使用量信息。

可查看目标的资源使用量详细信息，如统计单位（虚拟数据中心、部门或用户）、资源、用量等。

4.6.5.4 余额&充值

提供统一管理界面，可查询用户账户余额、账户充值、查询充值记录。

支持同时为多个账户批量充值。

4.6.5.5 计费策略

平台提供计费参数和计费策略的配置管理功能，包括资源单价、余额提醒、欠费处理策略、折扣设置、资源标签折扣、系统设置。

4.6.5.6 阿里云账单

以资源池为单位，查看阿里云资源池的消费概况，包括账单金额、账户余额。

查看阿里云资源池的消费详情，包括至指定账期的近半年消费趋势、产品消费分布情况、消费明细和账单明细等。

阿里云账单

4.6.5.7 成本分析

成本分析可以从部门、虚拟数据中心、用户维度，统计分析系统内最近一周内各类资源的整体消费情况，以便对资源进行合理优化，降低成本。

4.6.6 任务&资源审计

通过任务管理模块实现对系统任务的管理，用户可通过任务管理查看任务执行情况，帮助用户运维系统。

普通任务普通任务是指对系统资源进行的一次性操作任务。

定时任务是对系统资源设置一次或者循环多次执行的操作任务。

在资源审计模块下，以资源为单位，汇总统计所有资源的审计记录，可查询、查

看资源从创建到删除过程中所有成功的审计日志；可以按需删除指定时间的历史审计记录。提供云账户下资源的操作记录 ,通过操作记录可以实现安全分析、资源变更、问题定位等场景，方便用户追踪资源的历史变化情况。

- 资源审计完美记录资源创建到删除整个生命周期内所有成功操作。
- 记录操作引起资源数据变化信息。
- 记录操作者信息。
- 按照时间轴方式展示资源生命周期内的操作信息。

4.6.7 用户行为分析

用户行为分析为了客户精细化运营 ,打造更符合用户需求的业务系统 ,为客户提供用户行为分析服务。云平台操作中存在大量用户操作日志 ,包含管理员与云平台租户的操作日志 ,通过对其分析 ,可以发现大量用户操作习惯 ,从中发现用户访问与操作的规律 ,将这些用户行为模型与业务相结合 ,从而可能发现云平台业务系统中存在的问题，并为进一步修正或重新制定业务流程规划提供依据。

用户高频操作针对用户在系统内各种操作的成功日志进行分析，以得到用户高频操作。

用户习惯操作排除用户登录、查看项目等操作 ,获取用户每天执行某些操作的概率。

用户关联操作对用户操作中两个操作共同发生的概率作统计，统计时定义时间窗口，在这个时间窗口内发生的所有操作即为可能有关联的操作，基于整体事件序列，统计两个操作共同发生的概率。

关联操作次数：操作 A 与操作 B 共同发生的次数。

支持度=关联操作发生次数/（操作 A 发生次数+操作 B 发生次数+关联操作发生次数）

A 对 B 置信度即是操作 A 发生的前提下操作 B 发生的概率：关联操作发生次数/操作 A 发生次数。

B 对 A 置信度即是操作 B 发生的前提下操作 A 发生的概率：关联操作发生次数/操作 B 发生次数。

4.6.8 管理与治理

4.6.8.1 一致性审计

4.6.8.1.1 任务管理

创建任务，以提供定制化检测服务，配置管理任务：查询、修改、启用、停用、执行、删除，查看任务详情，包括基本信息、检测统计、检测结果、操作日志，审计项配置管理：添加、移除、禁用、启用、验证，查看审计项详情，包括审计项基本信息、检测描述、威胁影响、指导方案。

4.6.8.1.2 任务执行历史

查询任务执行历史，查看任务执行历史详情，包括基本信息、检测统计、检测结果等，查看审计项详情，包括审计项基本信息、检测描述、威胁影响、验证历史、指导方案，删除任务执行历史。

4.6.9 双因子认证

双因子认证服务,是一种基于证书安全认证技术,除了常规的用户名和密码的认证之后，增加了一种基于证书的身份认证方式，该方式的认证使得系统的安全性更高。当系统开启了双因子认证之后,即使用户的用户名密码被盗取了,没有证书仍然无法登录系统，这样将大大提高系统的安全性。

用户若要访问系统,应该首先获取证书。系统管理员作为系统的证书管理员,需要线下给用户颁发证书,该证书由用户自行妥善保管。颁发的证书形式包含两种:一种是电子版的数字证书,管理员线下给到用户后,用户需要自行保存,并安装到客户端;另一种是 Ukey 形式,管理员通过 Ukey 厂商提供的工具将证书写入到 Ukey 中，交由用户使用，用户妥善保管 Ukey。后续用户访问系统时，浏览器自动读取客户端的数字证书（不区分是否装在 Ukey 中）用于登录系统。

4.7 系统管理

功能涵盖安全策略、系统匹配值、序列号管理、第三方系统管理、证书管理、信息中心、平台监控、操作日志,平台提供完善的配置管理功能,满足私有平台的管控需求。

4.7.1 系统配置

系统配置提供日志保存策略、系统页面风格个性化配置、功能菜单管理等系统维护功能。用户可根据业务需求对系统进行灵活配置管理。

通知设置

邮箱服务器设置适用于用户注册、订单通知、告警通知、云主机到期通知等需邮

件通知的业务场景，支持 SMTP 协议。

短信服务器设置适用于用户注册、订单通知、告警通知、云主机到期通知等需短信通知的业务场景。

系统中预置了常用的通知提醒短信和邮件模板，用户仅按需调整即可使用，提高了通知内容的规范性和通知的发送效率。

日志设置

通过日志设置，可对日志的保存时间、告警策略以及日志删除策略等进行灵活配置。

操作日志是用户对系统的操作行为记录。三权分立时，仅审计管理员具有操作日志设置的权限，非三权分立时，仅运营管理员具有操作日志设置的权限。

自动删除日志功能下可以设置相应的日志保留时间，单位为天。

开启日志告警后，达到设定的告警阈值时进行告警，支持设置告警阈值，显示目前日志条数，告警通知方式有邮件和短信两种。三权分立时，将告警通知发送给审计管理员；非三权分立时，将告警通知发送给运营管理员。另外，24 小时内仅发送一次告警通知。

模块开关

通过模块开关对系统各类角色，包括运营管理员、域管理员、虚拟数据中心管理员、虚拟数据中心用户所能操作的功能菜单进行管理配置。

页面配置

系统为用户提供系统页面风格定制服务。用户可根据实际应用场景或个人习惯对系统进行个性化配置，包括登录页面、主页面和大屏页面的 LOGO、标题、版权信息等等。

标签管理

用户可以按需创建标签,将标签与资源关联后,便于用户识别和筛选管理相应资源,标签分业务标签和资源标签两种。业务标签用于云资源进行个性化标记,以便识别和筛选;资源标签用于按主机、存储等资源进行性能等级进行标记,系统内置主机标签（性能型、高性能、超高性能）和存储标签（低速、中速、高速）。

元数据标签

通过配置元数据可以为系统提供可配置的具有层级关系的参数(根元数据)及取值（子级元数据）。系统中已内置了一些常用的元数据供用户取用，例如芯片厂商、CPU 架构、操作系统、平台类型等等。

支持元数据的创建、修改、删除、隐藏操作。

4.7.2 序列号管理

产品序列号包含功能序列号和维保序列号两种序列号。这两种序列号都是预先生成的,在产品部署完成后,可根据产品的机器码和购买的序列号申请对应的功能激活码和维保激活码,并添加到产品中以激活相应的功能。运营管理员可在此页面查看机器码和序列号信息，并进行激活或作废操作。

客户购买软件的产品密钥,激活产品时需要使用,包括功能序列号和维保序列号两种。功能序列号是系统中各功能模块的使用许可,用于控制可选功能范围和可支持

的最大物理节点数量。系统中可支持的物理节点数不允许超过序列号所允许的范围。维保序列号是为用户提供系统维保服务的许可，用于规定维保的节点数量和维保时间限制。

序列号管理中可以设置到期提醒,设置序列号到期提醒天数,包含功能序列号和维保序列号。

4.7.3 第三方系统管理

系统可以作为业务集成方，为第三方系统提供单点登录入口，例如 SDN 服务、大数据服务等。还可对第三方系统进行访问、添加、编辑和删除的操作。

4.7.4 证书管理

证书管理提供了负载均衡器证书的存储管理功能，以便创建负载均衡器时获取使用。可对证书进行添加、查询和删除,需要注意的是选择上传证书的文件大小不能超过 7KB。

4.7.5 消息中心

消息中心是云平台为更好的建立与用户的联系而建设的服务，可以为云平台用户提供各类通知消息的接收,用户可以及时快捷的接收消息,从而更好的维护自己的虚拟资源，以及避免信息遗漏造成平台使用的不便以及不必要的损失。

消息中心主要包括发送消息和消息接收管理两大功能。

能够根据管理员的需求,向云平台用户主动广播推送消息。例如系统公告、停机维护、新产品上线、安全通知等。

已登录用户可以通过 websocket 即时接收到运营管理员广播推送的消息；对于未登录用户，在下次登录后，在消息中心会接收到运营管理员广播推送的消息。

发布消息

仅运营管理员可向系统内所有用户发布通知消息，以便及时提醒用户需要注意的事项。消息内容的大小不可超过 5MB，内容中的图片大小不可超过 1MB。

消息列表

在消息列表中查看系统中所发布的消息明细，包括已读和未读消息。

4.7.6 操作日志

系统所有用户的所有操作 ,包括登录、退出、告警、操作等 ,都要记录在日志中，以便用户操作问题定位和故障排查 ,为用户提供多维度的日志查询功能 ,并支持将操作日志下载到本地进行备份和统计。根据日志数量而采用不同下载策略。

4.7.7 安全策略

设置云平台的安全策略 , 包含登录会话设置、多因子认证、脱敏、密码策略和黑白名单等。三权分立状态下只有安全管理员能看到该界面。

登录会话设置

配置登录策略 , 包括错误登录次数、锁定时间、首次登录验证码是否显示、最大用户登录数 ; 配置会话策略 , 包括会话超时时间、是否允许同时多点登录、最大活跃会话数量。

多因子认证

多因子认证是用两种及以上的条件对用户进行身份认证的方法。为有效提升用户身份认证和访问的安全性，可配置用户证书、手机验证码和邮箱验证码等认证策略对登录用户进行强身份认证。

用户证书认证是一种安全验证过程，认证服务默认关闭。启用用户证书认证后，用户还需要携带预先颁发的证书方可成功登录，管理员可跳转至证书管理平台登录页面，创建并下载用户证书。证书的有效期为一年，且只会颁发一次，遗失后无法找回，请务必妥善保存。

证书密码与用户账号的初始密码相同，且需保证用户的初始密码长度大于5位，否则用户将无法使用证书。用户证书到期之后会自动生成新证书，用户需再次下载后安装使用。

验证码登录：在已配置邮件服务器或短信服务器的前提下，支持通过邮件或短信获取验证码以登录系统。

敏感信息保护

为保护用户姓名、邮箱、手机号码等个人信息，可通过配置脱敏策略来实现对敏感隐私信息的隐藏保护，以保障用户数据的安全性。

密码策略

可以灵活配置密码复杂度和更换策略，当不满足密码规则时，能给出告警提示，可适用不同场景下的密码配置策略。

黑白名单

白名单就是值得信任允许访问或者允许通过验证的名单。通过 IP 地址白名单，配置允许访问系统的 IP 地址范围。

黑名单就是拒绝的名单。通过 IP 地址设置黑名单，配置不允许访问系统的 IP 地址范围，黑名单以主动的方式拒绝恶意 IP 的访问。

4.8 安全管理

4.8.1 IP 白名单黑名单

白名单就是值得信任允许访问或者允许通过验证的名单。通过 IP 地址白名单，配置允许访问系统的 IP 地址范围。

黑名单就是拒绝的名单。通过 IP 地址设置黑名单，配置不允许访问系统的 IP 地址范围，黑名单以主动的方式拒绝恶意 IP 的访问。

4.8.2 安全控制

用户锁定与解锁

可设置允许用户连续登录失败次数及锁定时长；错误登录次数到达允许的最大值时，用户被锁定，超过锁定时长，用户被自动解锁。在锁定时间内，上级用户可为下级用户解锁。

密码策略

可设置用户密码修改策略，包括：密码最小字符数，最大字符数，是否必须包含特殊字符，是否允许包含正序或逆序用户名，密码重复使用次数，密码有效期，是否启用强修改策略，密码修改最短时间间隔，密码到期预先提醒。

会话连接设置。是否启用多会话连接，会话超时时间设置。

4.8.3 安全认证

当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。除支持用户名密码身份认证外，也支持与数字证书相结合的认证方式。

云计算平台不但要实现自身的安全防护，还要具有向其上租户系统提供安全防护的能力。例如：当远程管理云计算平台设备时，管理终端和云计算平台之间应建立双向身份验证机制；应能检测到对虚拟网络节点的网络攻击行为和云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量等等。

4.8.4 web 安全

所有 REST 接口符合云操作系统安全检验规范的要求，包括 Web 应用系统本身的安全和 Web 内容安全，能防范 SQL 注入、xss 跨站脚本、跨站点请求伪造、不安全的加密存储、跨站脚本漏洞、篡改网页内容、植入恶意代码等安全事件。

4.8.5 资源审计

资源审计服务提供云账户下资源的操作记录，通过操作记录可以实现安全分析、资源变更、问题定位等场景，方便用户追踪资源的历史变化情况。

资源审计通过数据的云存储，实现各类的数字化，使各种审计资源，包括审计人员、程序和相关的硬件设备，通过云来协同工作，使审计资源得到充分优化利用，以促进信息的交流和共享。在云审计过程中，审计人员可以按照自己的时间、方式进行审计，无需关注使用何种计算机程序，也无需关注数据的存储、共享和工作时效性问

题 ,惟一需要关注的就是审计任务本身 ,而云端看不见的繁琐技术全部留给技术后台来解决，并不需要知晓后台是如何运作的。

4.8.6 安全审计与日志管理

审计管理员负责系统所有日志的审计管理工作 ,包括查询、清除、导出等功能；其他用户只能查看自身相关的日志数据 ,但不能执行其他操作。系统所有用户的所有操作，包括登录、退出、告警、操作等，都要记录在日志中。

4.8.7 三权分立

三权分立

支持管理、审计、安全三权分立 ,要求三类角色的权限设置应相互独立、相互制约，安全保密管理员和安全审计员不得由一人兼任。

在三权分立模式下 ,用户授权等安全操作只能由安全管理员进行操作 ;所有日志的审计管理工作只能有审计管理员进行操作。系统所有用户的所有操作 ,都要记录在日志中。

日志应包括操作时间、操作者、操作对象、登录用户 IP、日志级别、操作成功/失败、事件详细信息等字段。

4.8.8 安全指数

安全指数服务是 InCloud OS V6 中引入的一种安全运营服务，旨在通过安全基线检查的方式评估平台的安全状态，并根据检查项的得分情况将平台风险等级分为高、中、低三个级别，总分值为 100 分，最终得分情况及风险等级以图表形式展示在服务首页，让用户对平台的安全态势一目了然，用户可以查看扣分项，并依据本服务提供的建议进行修复和加固，实现平台安全运营生命周期的闭环。

安全指数服务的业务流程主要包含四个方面，即检查项配置、检查平台配置、检查虚拟数据中心、检查虚拟数据中心配置。其中检查虚拟数据中心和检查虚拟数据中心配置存在以下区别：

检查虚拟数据中心检查对象是虚拟数据中心，选择一个或多个虚拟数据中心执行检查后，会对这些虚拟数据中心中所有的检查项执行检查，并计算安全评分和检查通过率。

检查虚拟数据中心配置检查对象是虚拟数据中心内的配置，可以选择部分检查项进行检查。

5 典型应用场景

5.1 传统 IT 架构业务上云

经过多年的发展，以政务云为代表的私有云在国家政策的大力支持下发展迅速。

金融、医疗等传统行业上云进程加快，私有云市场逐渐得到云服务商、系统集成商、IDC 服务商以及各行业用户的广泛关注。传统行业正在走向全面云化，这其中基于 Openstack 云架构获得普遍认可，成为云化“事实标准”；与此同时，全球各大运营商在电信网络和业务云化的战略高度驱励，强调 NFVI 及 VIM 必须独立于多家 VNF，硬件 COTS 化，VNF 与硬件及 Cloud OS 彻底解耦，NFV 扩展的 Openstack/KVM 开源的趋势不可阻挡；软件定义存储、软件定义网络成熟度得到普遍认知和广泛接受，企业开始启动分布式软件定义存储对传统存储进行革新改造及创新合作。

但是传统行业经过多年建设，积累了各种品牌、各种类型的硬件设备和复杂的软件设备，这些设备和软件都需要在上云的过程中得到很好的平滑迁移和继承，而不是重起炉灶，重新建设。同时，设备和软件的异构复杂还带来迁移过程的困难。不仅应用要进行迁移，数据和网络拓扑也要同步迁移；迁移后资源集中度提高，管理和维护的压力也会相应增大。

因此，通过软件定义实现整个数据中心内基础设施资源的抽象、池化、部署和管理，满足定制化、差异化的应用和业务需求，有效交付云服务，为企业业务的全面云化提供支撑。

InCloud OS 通过对硬件虚拟化，软件版本的标准化，系统管理服务化和流程一体化等手段，把企业信息平台建设成一个以服务为中心的云平台。从原有的独占方式转变为共享方式，运行环境可以自动的部署，资源环境可以进行灵活的分配与调整，从而帮助我们建立一个基于业务资源共享、服务集中和资源开放的一个平台。

InCloud OS 可以为用户提供虚拟私有云租用服务，租户可以配置自己的子网、云主机 IP 地址和 ACL，管理自己的网络资源。需要数据中心网络支持虚拟多租户能

力，支持大量的租户部署，实现租户的隔离和安全保障。

基于InCloud OS的云服务平台,可以实现资源的动态迁移。一方面是主动迁移，另一方面是动迁移。如果说前者偏重于管理用户,那么后者则偏重于业务保障,当某个设备发生故障，将会直接迁移到另外一台设备上去，而业务是没有受到任何的干扰。

InCloud OS 通过区分功能调用的内外部 API 和独立运行的认证管理模块，确保数据的安全;通过虚拟资源的多重备份和智能化调度保证企业云业务的稳定运行,同时能够达到智能备份和恢复的效果。

5.2 大规模云数据中心管理

云计算的日渐普及、大数据的兴起、5G 时代的到来以及人工智能在各个领域的应用,使得数据和应用双轮驱动,均呈现爆发式增长。因此,支撑数据及应用的数据中心计算量越来越大，数据中心也呈现集中化和规模化趋势。

传统的数据中心通常采用“一机一业务”的部署模式,但是随着数据中心规模不断扩大，传统 ICT 资源构建方式的低效和高成本弊端日益突出，架构复杂且缺乏灵活性,业务与基础设施紧耦合,应用系统受制于软硬件之间的依赖关系,复杂度越来越高、进一步提升了管理运营成本、降低了业务上线速度。

面对上述问题，业内通用的做法是通过引入虚拟化技术把数据中心物理设备进行资源池化,使得资源使用和部署更加灵活,进而提升业务部署效率、降低业务迁移的难度。

虚拟化后单台主机上运行着多台云主机,多个业务系统,而大型云计算数据中心

普遍具有数千乃至上万台物理服务器、十万量级规模的云主机。这也带来了如何对虚拟化平台乃至整个数据中心进行智能监控和统一管理的新问题。云平台的整体管理能力以及监控的效率、准确率对维持虚拟资源池可靠运行尤为重要。

基于对数据中心计算资源的池化和统一管理，InCloud OS 可以协助 IT 部门更加灵活而弹性的控制数据中心的各种资源，为业务部门提供更好的支持和服务。通过提供全面、统一、多维度的管理监控子系统，管理监控数据中心的海量异构资源，包括服务器、存储、网络设备等硬件资源，各种操作系统、数据库、虚拟资源等软件资源；并利用多级阈值设置和智能警报功能，可以自动而更加准确地分析各种类型的数据，剔除短时异常数据，并且能够判断性能变化的趋势，从而能够在终端用户抱怨和普通的监控工具报警前，报告系统性能问题，节省运维成本。InCloud OS 监控集群支持上千种数据采集，系统可支持 10 万级别的监控项和告警项，可以为用户实现精细化、可扩展的监控告警服务。

5.3 云原生应用创新

随着云计算、大数据、人工智能的发展，企业级应用的复杂性越来越高，也越来越呈现出双模态并存的特点，企业传统业务以稳定发展为中心，力求稳健，而其互联网业务则以创新驱动为中心，力求敏捷；而作为驱动业务的技术手段，IT 架构也表现为双态 IT 架构并存。具体表现为应用架构由单体架构变成微服务架构，而应用部署模式上也由单一节点走向分布式云化。

基于 Kubernetes 容器编排技术，采用微服务架构，兼容 X86、MIPS、ARM 等多架构 CPU，以应用为中心，面向企业私有云市场提供包括全方位应用管理、智能监控运维、微服务治理、DevOps、多租户管理、安全审计等云平台服务，能够帮助

企业加速应用上云，实现业务的高可用性、弹性伸缩，并对应用的全生命周期进行自动化管理。

5.4 云数智融合

在数据中心不断的更新和发展过程中，越来越多的用户对于数据中心的智能化提出了更高的要求，智慧城市、智慧校园、智慧制造等领域快速兴起。尤其是在后疫情时代，大数据分析、远程办公、在线教育的概念越来越深入人心。用户希望融合云、数、智、网、端，依靠大数据分析、AI 训练推理平台，实现智能模型的统一更新、应用分发，以更低的成本、更高的效率发掘潜藏在数据中的趋势价值，建设无人化、网联化、智能化、数字化的行业系统。

围绕云融数智的需求，InCloud OS 依托云计算、大数据、人工智能等技术手段，构建 AI 云计算平台，为用户的 AI 应用提供孵化、统一管理以及算力支持、加速用户内外部数据的采集、加工和治理，并持续赋能 AI 应用，全面提升行业智慧化能力。云计算、人工智能与大数据全面融合，业务从传统的数据生产方开始接受数据的反哺并全面智能化演进，更好的支撑技术与数据、业务的融合与多层级跨越，能够更好的降低运行成本、提高工作效能、提升服务体验，更好的满足业务需求。

6 缩略语

中文全称	英文缩写	英文全称
应用程序编程接口	API	Application Programming Interface
中央处理器	CPU	Central Processing Unit
动态主机配置协议	DHCP	Dynamic Host Configuration Protocol
域名系统	DNS	Domain Name System
分布式虚拟路由	DVR	Distributed Virtual Router
光纤通道	FC	Fiber Channel
简单文件传输协议	TFTP	Trivial File Transfer Protocol
图形处理器	GPU	Graphics Processing Unit
高可靠性	HA	High Availability
超文本传输协议	HTTP	Hypertext Transfer Protocol
基础设施即服务	IaaS	Infrastructure as a Service
互联网数据中心	IDC	Internet Data Center

中文全称	英文缩写	英文全称
输入输出	I/O	Input and Output
每秒读写（I/O）操作次数	IOPS	Input/Output Operations Per Second
网络互连协议	IP	Internet Protocol
智能平台管理接口	IPMI	Intelligent Platform Management Interface
互联网传输协议安全性	IPSec	Internet Protocol Security
因特网小型计算机系统接口	iSCSI	Internet Small Computer Systems Interface
基于内核的云主机	KVM	Kernel-based Virtual Machine
模型-视图-视图模型	MVVM	Model-View-ViewModel
网络附属存储	NAS	Network Attached Storage
网络地址转换	NAT	Network Address Translation
网络文件系统	NFS	Network File System
操作系统	OS	Operating System
平台即服务	PaaS	Platform as a Service

中文全称	英文缩写	英文全称
预启动执行环境	PXE	Preboot Execute Environment
独立冗余磁盘阵列	RAID	Redundant Array of Independent Disks
服务质量	QoS	Quality of Service
内存	RAM	Random Access Memory
基于角色的访问控制	RBAC	Role-Based Access Control
表示状态转移	REST	Representational State Transfer
软件即服务	SaaS	Software as a Service
存储区域网络	SAN	Storage Area Network
服务器信息块	SMB	Server Message Block
软件定义网络	SDN	Software Defined Network
源地址转换	SNAT	Source Network Address Translation
传输控制协议	TCP	Transmission Control Protocol
用户数据报协议	UDP	User Datagram Protocol

中文全称	英文缩写	英文全称
用户界面	UI	User Interface
通用串行总线	USB	Universal Serial Bus
虚拟图形处理单元	vGPU	Virtual Graphics Processing Unit
虚拟 IP	VIP	Virtual Internet Protocol
虚拟局域网	VLAN	Virtual Local Area Network
云主机	VM	Universal Serial Bus
云主机监控器	VMM	Virtual Machine Monitor
虚拟路由冗余协议	VRRP	Virtual Router Redundancy Protocol
可扩展虚拟局域网	VXLAN	Virtual Extensible Local Area Network
虚拟私有云	VPC	Virtual Private Cloud
虚拟私有网络	VPN	Virtual Private Network
扩展标记语言	XML	Extensible Markup Language
复原时间目标	RTO	Recovery Time Objective

中文全称	英文缩写	英文全称
复原点目标	RPO	Recovery Point Objective
基于角色的访问控制	RBAC	Role-Based Access Control
安全应用交付系统	SSA	—
运维安全管控系统	SSC	—
生命周期管理	LCM	Life Cycle Management