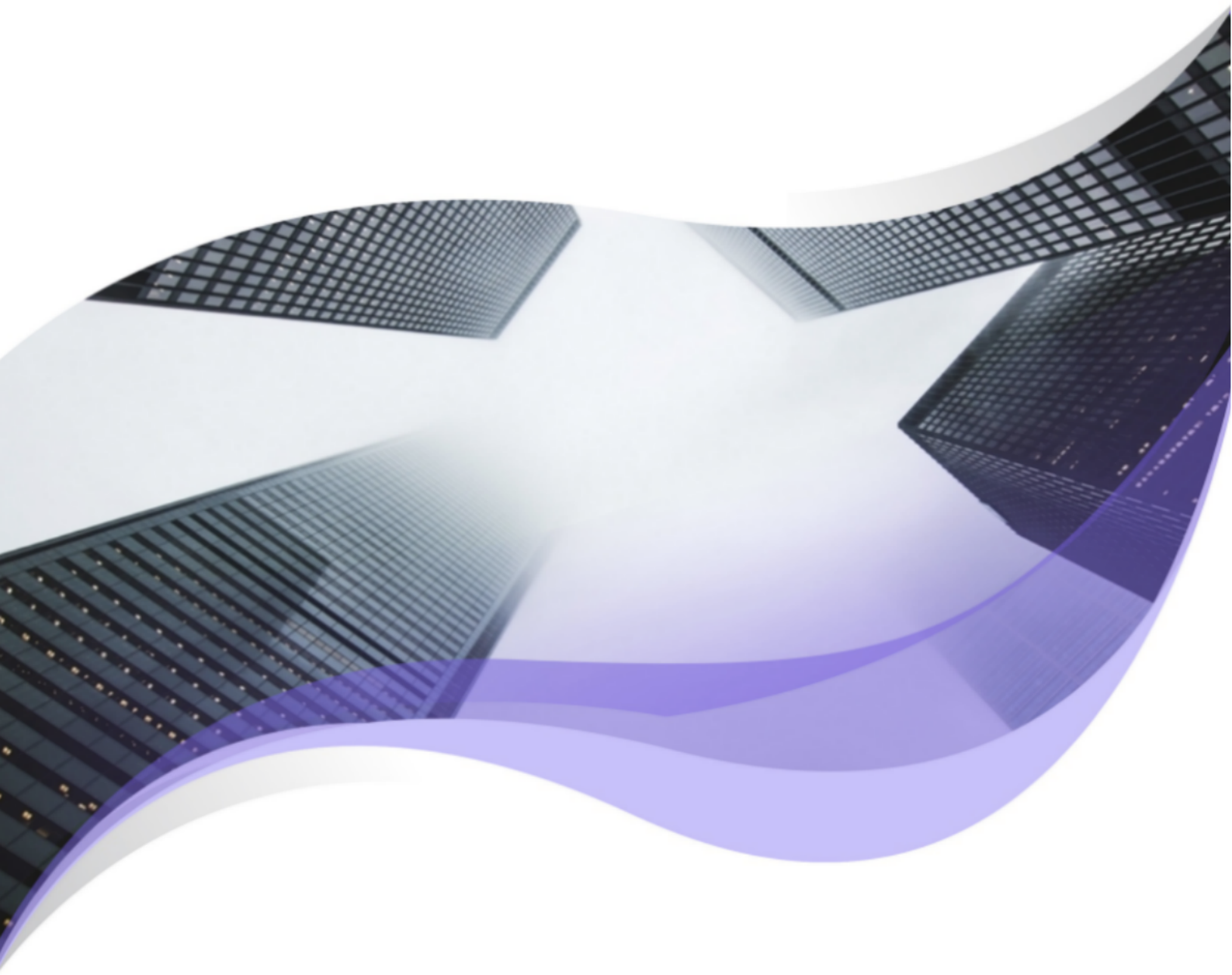
易捷行云
EasyStack

云原生基础设施解决方案

白皮书



文档版本: v1.0.1
发布日期: 2023-06-20

目录

1 解决方案介绍

1.1 概述

概述

现状与问题

过去十年，云计算已经作为支撑基础设施与企业数字化转型的关键技术，并且正在由迁移上云向深度用云过度。多数企业云计算架构的演进已经完成了由单物理主机向虚拟化/超融合的转型，构建了以虚拟机加物理机的IT基础设施资源池，随着企业数字化转型不断加速，业务应用系统形态与技术也在发生改变，从传统应用、容器化应用到微服务化应用，企业IT基础设施也在发生架构与技术上的变化，而企业核心应用架构微服务化带来的复杂性转移到基础设施云原生化，这是IT基础设施数字化转型的核心。随着微服务化的应用系统改造加速，低代码化的业务开发模式的引入，对基础设施平台化的服务沉淀能力提出了新的要求，将云原生服务构建在传统虚拟化基础设施之上的传统IAAS+PAAS解决方案，虽然让云原生/微服务化应用能够运行在企业数据中心中，但也从架构、管理运维与投入产出比上为企业基础设施管理带来了挑战。

- 从架构复杂度上，分层构建虽然带来的软件层面的解耦，但由于云原生应用本身对于操作系统，计算、网络、存储、安全性的紧密依赖，在以上平面的衔接上带来了架构的复杂性，从规模、性能上提出了更多挑战。
- 从管理运维角度上，分层构建意味着大部分将云原生相关的基础设施管理交给应用开发部门负责，企业IT基础设施部门以提供基础设施计算、存储、网络资源为管理与运维边界，但随着云原生/微服务化的应用占比提高，对于基础设施的资源供给速度、利用率、编排效率、性能以及安全性提出了新的挑战，也对基础设施管理者对于云原生技术的掌握提出新的挑战。
- 从投入产出比角度上，云原生基础设施所带来的自运维与故障自愈能力，以及支撑低代码开发的特性，能够将更多云上软件转变为企业自身应用所需的云服务能力，降本增效。

方案概述

易捷行云云原生解决方案以云原生相关技术为核心，通过可进化的架构、将容器、虚拟化、存储、SDN网络、操作系统通过数字原生引擎有机整合，提供面向微服务应用的云原生产品套件 ECNS，包括Kubernetes容器服务、容器应用中心、安全容器实例、DevOps平台、容器镜像服务、裸金属服务等一系列产品，具备云

平台的弹性和分布式优势，实现应用的安全强隔离、快速部署、按需伸缩、持续交付等场景需求，它使设计和开发的应用程序的整个生命周期都能在云中运行。

图1.易捷行云云原生基础设施解决方案整体架构

方案特性

- 多元算力：为满足业务承载的安全性、高性能、信创化、轻量化、多类负载的要求，平台需要通过深度适配实现基于裸金属提供容器集群、云原生虚拟化、安全容器等云原生服务能力。
- 统一网络：平台需要提供软SDN能力，可以为安全容器、云原生云主机提供统一组网能力。

- 开放生态：平台提供标准框架开放接入，统一提供鉴权认证与加密服务，可对接计算、存储、网络、监控、管理、运维、安全等服务。
- 简单易用：提供更加轻量化、自动化的管理基础设施软件，聚焦业务创新，平台需要提供全自动化安装部署、扩容、配置能力。
- 持续迭代：为了持续保障平台功能性满足我司要求，同时兼顾安全性、可靠性、稳定性。平台需要能提供统一升级引擎，支持从操作系统到各类云原生服务的在线升级和迭代，实现渐进建设。
- 规模支撑：当前架构需要可以支持从3节点持续扩展至数千节点，同时可按需提供包括容器集群，DevOps，安全容器，云主机，高性能云存储等。
- 可扩展性：平台具备良好的可扩展性，可提供基于Operator等架构的开发和扩展能力，实现复杂的资源管理和调度需求。

解决方案功能架构

图2.易捷行云云原生基础设施解决方案功能架构

1.2 产品形态

Kubernetes 容器服务产品形态

对比项目	云原生基础设施ECNF解决方案	云基础设施ECF方案附加Kubernetes容器服务
主要特点	直接部署在裸金属上 应用创建时无需准备容器集群 应用直接运行在裸金属上，拥有更好的性能与更细的内核隔离能力 应用负载密度更高 基础设施管理者需要关注云原生基础设施集群的运行情况	部署在IaaS提供的云主机上 多套项目隔离的Kubernetes集群，彼此隔离 申请与回收集群更加灵活 自定义Kubernetes集群的规模与配置 需要自行维护、管理Kubernetes集群
使用场景	使用于基础设施云原生化，大规模多云场景下的云原生应用裸金属部署、批量任务、Serverless、CI/CD、稳定可靠的云原生应用运行环境。	使用于多云云原生应用编排管理、云原生应用开发测试、CI/CD、按需灵活的云原生应用开发测试环境。
资源利用率	资源利用率高，资源分配粒度在0.25vcpu，计算资源直接分配给容器运行时。	利用率一般，资源分配粒度以1vcpu为单位，容器再使用分配给虚拟机的资源进行再次分配，资源利用率需要通过精细化管理才能够提高。
可观测性	同时提供包含操作系统、存储、网络、容器编排引擎、容器运行时一体化监控、日志服务。	同时提供包含操作系统、存储、网络、容器编排引擎、容器运行时一体化监控、日志服务。
是否支持一云多芯	通过统一操作系统可以适配兼容海光、鲲鹏、飞腾多路线，具备一云多芯的能力。	通过统一操作系统可以适配兼容海光、鲲鹏、飞腾多路线，具备一云多芯的能力。

1.3 解决方案产品能力

集群管理

- ECNF 容器集群创建，您可以根据基础设施的规划，通过自动化中心完成集群的规划与配置，更多信息请参见（自动化中心）
- Kubernetes 容器集群创建，您可以根据需求使用平台内产品创建云主机上的租户隔离的容器集群，更多信息请参见（创建容器集群）
- 多集群管理，支持多个独立集群统一权限管理，通过统一的IAM权限与访问管理服务以及多区域服务实现多个集群的统一管理，更多信息参见（多区域管理）
- 集群升级管理，平台提供OTA升级引擎，支持从操作系统到云产品的平滑升级能力，更多信息参见(OTA升级)

多元算力

- 安全容器服务，安全容器实例（Secure Container Instance）提供敏捷安全的容器运行服务，既无需预置和管理云主机，也无需构建Kubernetes容器集群，只需提供打包好的容器镜像，即可运行容器，帮助您专注于业务开发，提升开发效率。产品底层使用安全沙箱容器技术，提供虚拟机级别的安全和资源隔离能力，同时针对容器运行环境进行深度优化，提供比虚拟机更快的启动速度和运行效率，更多信息参见（安全容器服务）
- 云原生云主机（KubeVirt）基于原生Kubernetes，提供以容器为核心的虚拟化工作负载管理服务，支持将已有的虚拟化工作负载与容器化的工作负载结合于一个平台，支持在容器中与已有的虚拟化应用进行有交互的新微服务应用的开发。更多信息参见（云原生云主机）
- 裸金属服务（Baremetal Service）旨在为客户的业务应用提供专属的物理服务器，其兼具虚拟机的弹性优势与物理服务器的性能优势，实现超强超稳的计算能力，保障核心业务卓越的计算性能、稳定性和数据安全，满足客户各类核心应用对高性能及稳定性的需求，同时提供完备的裸金属主机全生命周期管理能力。更多信息参见（裸金属服务）
- 工作负载管理，Kubernetes容器服务提供完整的工作负载管理能力，更多信息详见(工作负载管理)

存储

- 块存储产品可以提供虚拟的块存储资源——云硬盘。云硬盘类似PC机的物理硬盘，需要挂载至云主机等计算实例上使用，用户可以像使用物理硬盘一样对云硬盘进行格式化并建立文件系统。云硬盘可以作为云主机的系统盘或数据盘，由于云硬盘的生命周期独立于云主机，不随云主机的销毁而消失，因此可为用户提供稳定、灵活的持久化存储能力。更多信息参见（块存储）

- 高性能云存储是为云上业务提供高IOPS、高吞吐量、低IO读写时延的云存储服务，适用于企业中的高性能计算、超高数据访问等关键业务。高性能云存储以高性能型云硬盘或性能型存储卷的形式为云主机、容器提供存储服务。更多信息参见（高性能云存储）

SDN网络

- SDN网络服务旨在为云主机、容器、安全容器和裸金属等计算资源构建安全隔离的、自主配置和自主管理的虚拟网络环境，提升云上资源的安全性，简化网络的部署。客户可以按需配置子网、虚拟网卡和安全组等功能，并允许灵活搭配路由器和公网IP，支撑其业务部署。更多信息参见（SDN网络服务）

高级服务

- 容器应用中心基于开源项目Helm开发，提供应用模板的统一管理与调度，用户可以上传模板并基于模板快速部署应用，大幅简化了Kubernetes资源的部署与管理过程。更多信息参见（容器应用中心）

- DevOps源自Development（开发）和Operations（运维）的组合，是一种新的软件工程理念，旨在打破传统软件工程方法中“开发->测试->运维”的割裂模式，强调端到端高效一致的交付流程，实现开发和运维的统一。DevOps云产品，以容器技术的持续集成（CI，Continuous Integration）、持续部署（CD，Continuous Deployment）为基础，面向从源代码获取到应用程序或软件生产上线的全流程，提供运行脚本、构建发布镜像、YAML部署、构建发布Chart模板和Chart模板部署等服务，并通过卡片式的可视化配置页面，提供精益、敏捷、可定制的企业CI/CD流水线创建模式，帮助企业精细化管理交付流程，缩短交付周期，提升交付效率。更多信息参见（DevOps）

运维

- 可观测性

云监控服务（Cloud Monitoring Service，CMS）是面向用户的监控告警服务。通过云监控服务，可以帮助用户快速了解当前云平台的健康状态、容量使用情况以及存储集群使用状态等信息。云监控服务还为用户提供详细的云平台报警信息。当云平台运行状态异常时，可以查看报警信息，快速定位并及时解决问题，恢复云平台。更多信息参见（云监控服务）

Kubernetes容器服务提供自带的日志服务，您可以试试查看日志详情。

安全

- 证书与密钥服务是平台上提供私有CA及数字证书全生命周期管理的服务，帮助企业搭建和维护自己的CA体系，包括根及多级中间CA，同时，支持在企业内部签发和管理私有证书，以及托管企业购买的或第三方生成的证书。证书管理服务帮助企业无需花费高昂费用即可实现企业内部的应用身份认证和数据加解密，从而识别和保护组织内的应用程序、服务、设备和用户等资源。更多信息参见（证书与密钥服务）

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区1号楼1层107-2号
南京易捷思达软件科技有限公司：
江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)