复杂容器云场景下云底座操作系统的探索与实践

麒麟软件有限公司 研发工程师 李剑

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

目录

- 容器云场景的现状与挑战
- 云底座操作系统 NestOS
- 容器云集群与操作系统一体化运维工具 NKD
- Q&A

容器云场景的现状与挑战

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

容器云场景的现状与挑战

Kubernetes，容器云场景的主流技术

推动 Kubernetes 采用的主要因素

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

容器云场景的现状与挑战

Kubernetes，容器云场景的主流技术

1

提高资源利用率

2

简化了应用升级和维护

3

实现了向云环境的迁移

4

在公有云和本地部署之间实现了混合模式

运行 Kubernetes 带来的运维优势

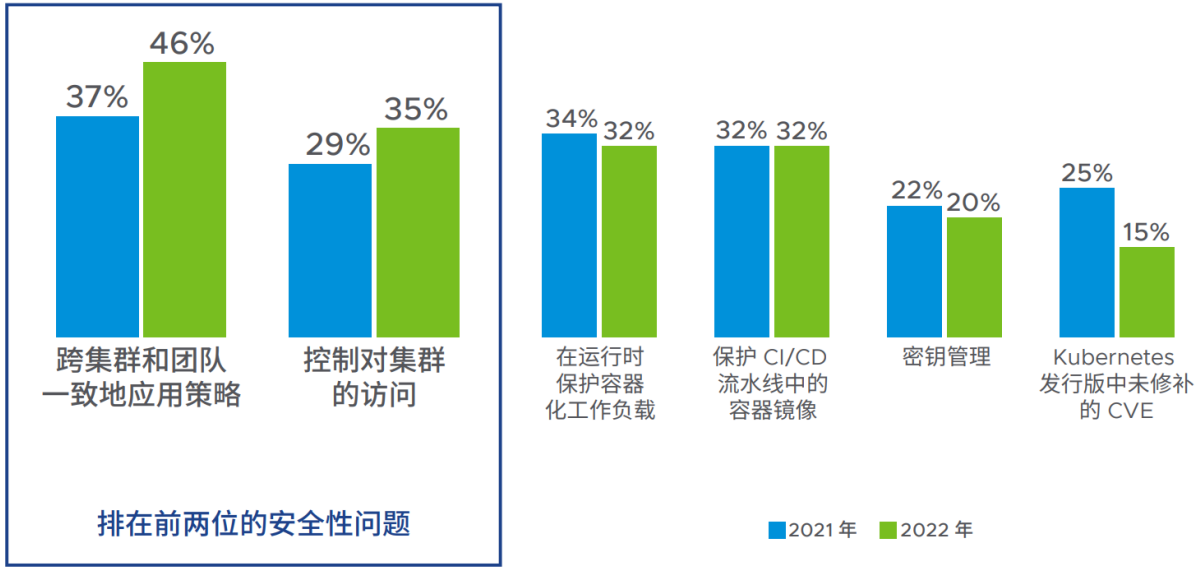
开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

容器云场景的现状与挑战

安全性问题成为重要挑战

哪些工具对运维快速增长的 Kubernetes 环境至关重要?

- 数据安全性、保护和加密
- 集群生命周期管理
- 平台监控和警示
- 自动化



摘自《Kubernetes 使用现状 2022 - 使用 Kubernetes 的最大安全性问题》

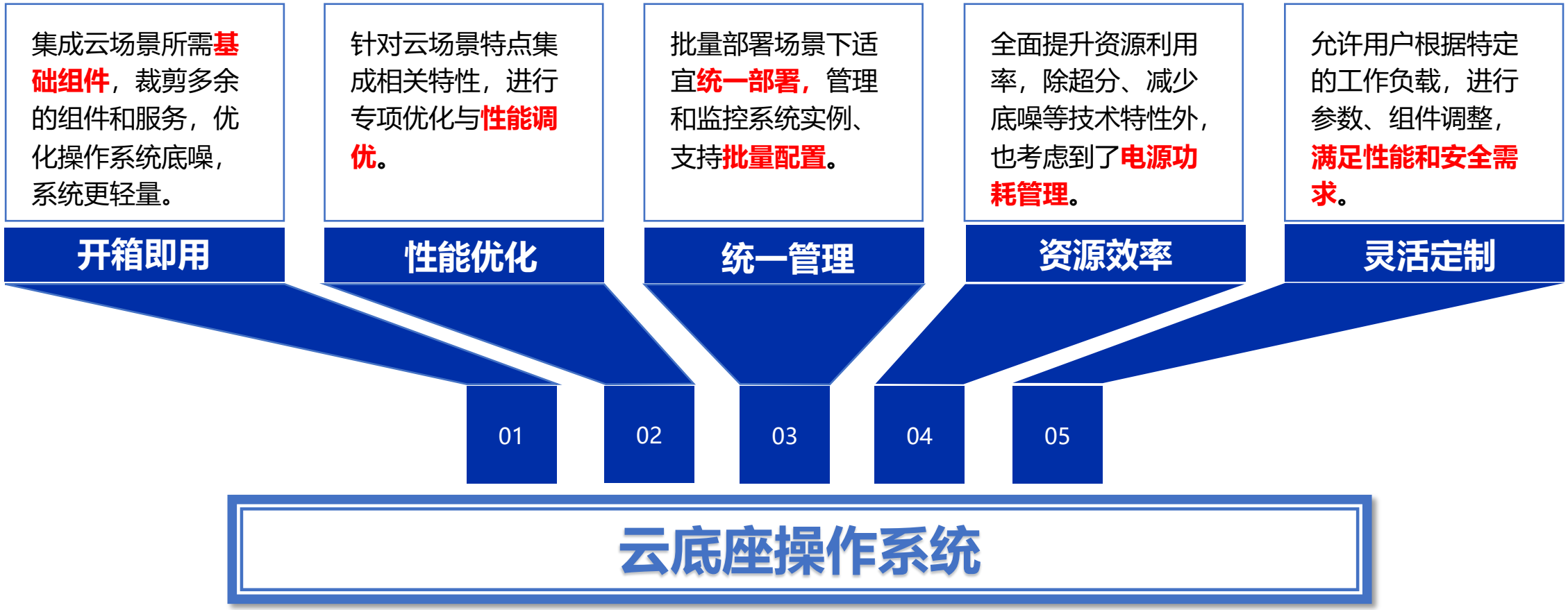
因此，结合 Kubernetes 集群数量和多云部署的增长的现状，以及网络威胁的持续增加，应对安全性方面的挑战成为 Kubernetes 部署和管理的首要任务，多集群和多云部署也成为影响 Kubernetes 安全性的主导因素。

云底座操作系统 NestOS

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

云底座操作系统 NestOS

为什么要选择云底座操作系统?

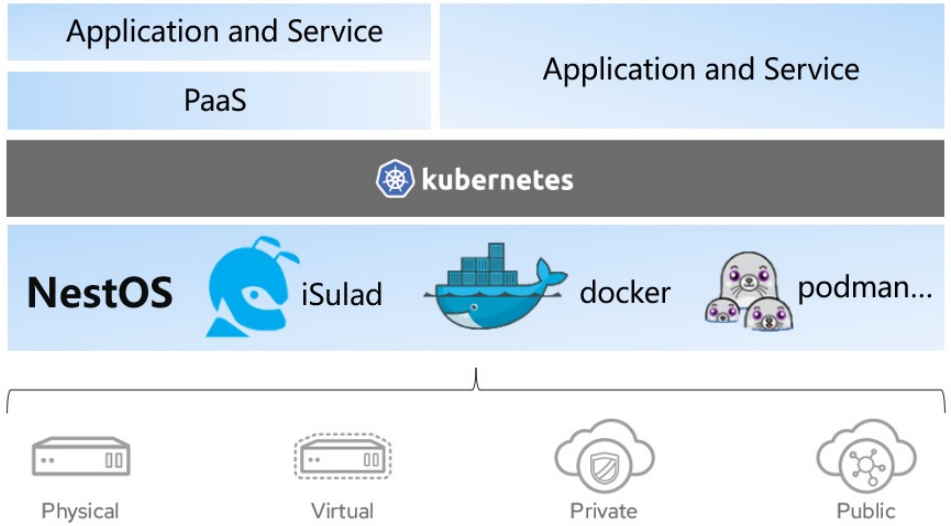


开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

云底座操作系统 NestOS

容器化场景 NestOS for Container

NestOS for Container （以下简称 NFC）专注于以容器化应用为代表的云原生业务场景，采用双根文件系统、原子化更新的设计理念，支持 rpm-ostree、ignition 配置等先进技术，可通过 nestos-assembler 快速集成构建。



NFC 秉承不可变基础设施思想，支持以容器镜像的方式管理操作系统，可自主构建应用系统镜像。此外，NFC 还针对 Kubernetes、OpenStack 等平台进行了适配，优化容器运行性能，使操作系统能够轻松地构建集群，同时高效安全地承载大规模容器化工作负载。

虚拟化场景 NestOS for Virt

NestOS for Virt（以下简称 NFV） 专注于以虚拟化为主的云计算业务场景，采用通用的 RPM 包管理方式，并经过系统裁剪、性能优化和虚拟化增强等方面的精心设计。NFV 预先安装了虚拟化的关键组件，旨在使用户能够轻松创建和管理虚拟机。

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

云底座操作系统 NestOS

NestOS for Container （NFC）特性

1

开箱即用的容器平台

NFC 集成适配了 iSulad、Docker、Podman 等主流容器引擎，为用户提供轻量级、定制化的云场景 OS。

2

简单易用的配置过程

NFC 通过 ignition 技术，可以以相同的配置方便地完成大批量集群节点的安装配置工作。

3

安全可靠的包管理

NFC 使用 rpm-ostree 进行软件包管理，搭配 openEuler 软件包源，确保原子化更新的安全稳定状态。

4

友好可控的更新机制

NFC 使用 zincati 提供自动更新服务，可实现节点自动更新与重新引导，实现集群节点有序升级而服务不中断。

5

紧密配合的双系统分区

NFC 采用双系统分区设计，确保 NestOS 运行期间的完整性与安全性。

云底座操作系统 NestOS

新 NestOS，新特性

01 x2nestos：不可变模式转换工具

x2nestos 是一款将通用形态操作系统转换为 NestOS For Container 版本的快捷部署工具。该工具基于 kexec 动态加载内核特性，实现跳过引导阶段完成操作系统部署，有效降低现有操作系统转换为 NestOS For Container 的难度和成本。

02 支持轻松定制系统镜像

NestOS For Container 已集成 ostree native container 特性，容器云场景用户只需编写一个 ContainerFile（Dockerfile）文件，即可轻松构建定制版镜像，用于自定义集成组件和后续的升级维护工作。

03 内核特性增强

目前，NestOS 已对 nestos-kernel 进行了独立维护，并基于 openEuler-22.03-sp2 内核版本进行开发，主要专注于改进 mm、cpu、cgroup 等方面的内核特性。

04 支持 Rubik 在离线混部

Rubik 是一个自适应单机算力调优和服务质量保障的容器混部引擎，NestOS For Container 版本已预开启 Rubik 在离线混部相关内核特性，支持基于 Rubik 容器混部引擎的整体解决方案，通过对资源进行合理调度与隔离，在保障关键业务服务质量的前提下极大提升容器云场景资源利用率。

容器云集群与操作系统一体化运维工具 NKD

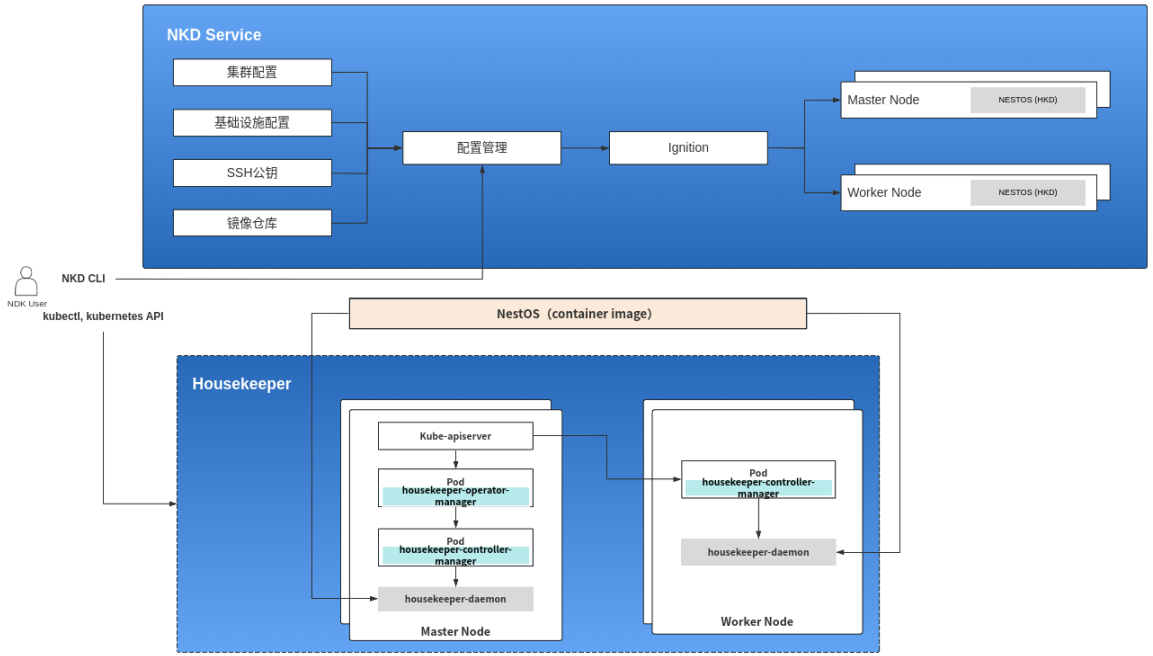
开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

容器云集群与操作系统一体化运维工具 NKD

基于 NestOS for Container 部署的 Kubernetes 集群运维解决方案

NKD，全称为 NestOS-Kubernetes-Deployer，是一套基于 NestOS 设计，NestOS for Container 上独有的容器云部署和运维工具，旨在为容器云业务和云底座操作系统提供一致性的运维解决方案。

NKD 的设计初衷是提供在集群外部署、更新和配置管理等服务的能力，涵盖集群基础设施，包括操作系统以及 Kubernetes 核心组件。



NKD 部署升级流程图

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

容器云集群与操作系统一体化运维工具 NKD

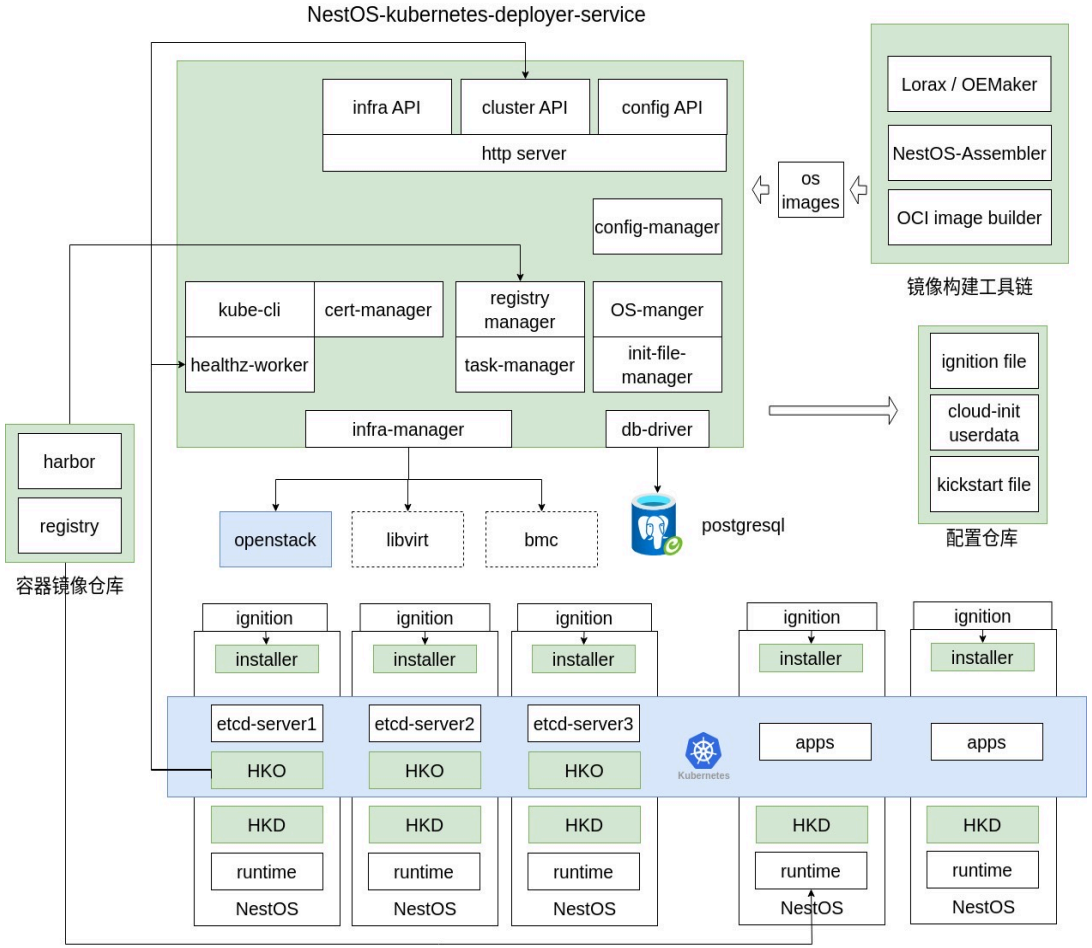
NKD 助力容器云场景运维

- 集群基础设施创建
  - NKD 可根据集群需求，连接基础设施提供商动态创建所需的 IaaS 资源，支持裸金属和虚拟化场景，目前优先实现 OpenStack、Libvirt 场景。
- 操作系统镜像构建
  - NestOS for Container 提供了完善的镜像构建工具链，可轻松集成到用户现有的 CICD 流程中。
- 集中配置管理
  - 在部署 NestOS for Container 时，可通过 Ignition 点火机制传入系统部署后所需的动态配置。
- Kubernetes 集群部署
  - Kubernetes 集群部署是 NKD 的核心功能，将所需配置合并到 .ign 文件中，使得节点在部署完成操作系统引导后自动开始部署集群，无需手动干预。
- 操作系统 & Kubernetes 组件升级维护
  - NKD 会监测 Kubernetes 集群状态，一旦集群创建完成，向用户提供访问凭据，并部署 Housekeeper 服务；
  - 当操作系统或 Kubernetes 组件需要升级维护时，NKD 可使用镜像构建工具构建新版系统镜像，并在查询到新版镜像后，向集群创建 Housekeeper CR 资源。集群中的 Housekeeper 服务将按照配置逐次对集群节点进行升级，完成整个集群的升级工作。

容器云集群与操作系统一体化运维工具 NKD

NKD 的整体规划

- NestOS-kubernetes-deployer-service（简称 NKDS）
  - NKDS 作为 NKD 项目的主体，包含基础设施管理、配置管理、系统镜像管理、证书管理和健康监测等模块。
- Housekeeper
  - 面向集群的 Housekeeper Operator（简称 HKO） 组件；
  - 集成在 NestOS for Container 镜像中的 Housekeeper Daemon（简称 HKD）组件。
- NestOS Installer
  - 主要负责在 NestOS for Container 系统点火阶段部署创建 Kubernetes 集群。
- 其它组件
  - NestOS for Container 镜像构建工具链；
  - 配置管理仓库；
  - 容器镜像仓库。



NestOS 整体架构与集群交互全景

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

Q&A

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

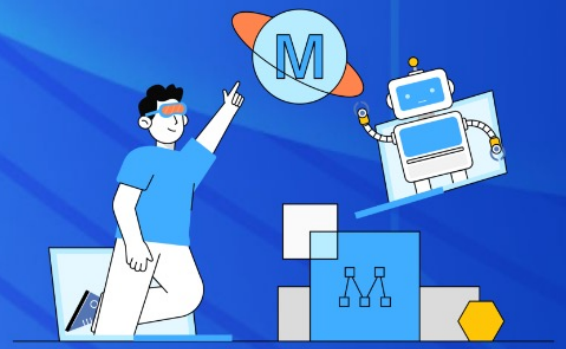
NestOS 官网 — nestos.openeuler.org

OpenEuler

DISCOVERY

NestOS

基于欧拉开源操作系统的云底座操作系统



开启NestOS之旅

在不断演进的云原生世界中，容器化和虚拟化技术已经成为了现代应用程序交付和管理的关键组成部分。为满足这个不断增长的需求，我们基于NestOS-22.03-LTS-SP2版本全新出发，正式推出双模式版本， **该版本整合了NestOS For Container 和 NestOS For Virt这两个模式到一个ISO镜像中，** 旨在满足云场景中容器化和虚拟化两种主要场景下用户的多样需求，专注于提供最佳的容器主机和虚拟化解决方案。

目前NestOS已发布全新版本，欢迎大家下载体验，或者有什么说给NestOS听。

THANKS