

浪潮信息



浪潮信息云峦服务器操作系统 KeyarchOS V5.8 技

术白皮书

技术白皮书

浪潮电子信息产业股份有限公司

2024年12月

版权所有 ©2024 浪潮电子信息产业股份有限公司。保留一切权利。
未经本公司事先书面许可，任何单位和个人不得以任何形式复制、传播本手册的部分或全部内容。

技术支持

技术服务电话：400-860-0011

地 址：山东省济南市高新区草山岭南路 801 号 9 层东侧

浪潮电子信息产业股份有限公司

网 址：<https://www.ieisystem.com/keyarchos/>

邮 编：250101

目 录

目 录.....	IV
1 前言.....	1
2 产品介绍.....	1
2.1 产品架构.....	2
2.2 产品关键特性.....	3
2.2.1 安全可靠.....	3
2.2.2 稳定可靠.....	10
2.2.3 高效运维.....	11
2.2.4 极致性能.....	15
2.3 产品技术指标.....	20
3 系统主要功能.....	22
3.1 网络配置.....	22
3.2 软件包管理.....	22
3.3 Systemd 服务管理.....	22
3.4 用户管理.....	23
3.5 磁盘管理.....	24
3.6 LVM 管理.....	24

3.7 日志管理.....	25
3.8 时间配置.....	26
3.9 系统监控.....	26
4 典型应用场景.....	27
4.1 物理裸机服务器.....	27
4.2 虚拟化.....	28
4.3 云计算.....	28
4.4 大数据.....	28
4.5 人工智能.....	29
4.6 边缘计算.....	29
5 服务与支持.....	29

1 前言

浪潮电子信息产业股份有限公司（简称：浪潮信息）是中国领先的云计算、大数据服务商，已经形成涵盖 IaaS、PaaS、SaaS 三个层面的整体解决方案服务能力，凭借浪潮信息高端服务器、海量存储、操作系统、超融合、信息安全技术为客户打造领先的云计算基础架构平台，基于浪潮信息政务、企业、行业信息化软件、终端产品和解决方案，全面支撑智慧政府、企业云、垂直行业云建设。

为了应对智慧时代的新变革、新挑战，浪潮信息提出了“以应用为导向，以系统设计为中心，建立多元异构算力融合、软硬协同优化”的技术发展路线，操作系统是浪潮信息以系统设计为中心技术路线的关键环节。

浪潮信息推出自研服务器操作系统云峦 KeyarchOS，一方面是进一步践行以系统设计为中心的技术路线，持续推动软硬协同创新；另一方面，通过 KeyarchOS 充分发挥浪潮芯片、板卡和服务器的创新成果，为用户提供卓越的整机系统体验；同时，浪潮信息还将依托 KeyarchOS，联合上下游合作伙伴，围绕操作系统，构建操作系统生态标准、规范，以及行业方案，壮大开源社区力量，共同推动操作系统产业生态的繁荣。

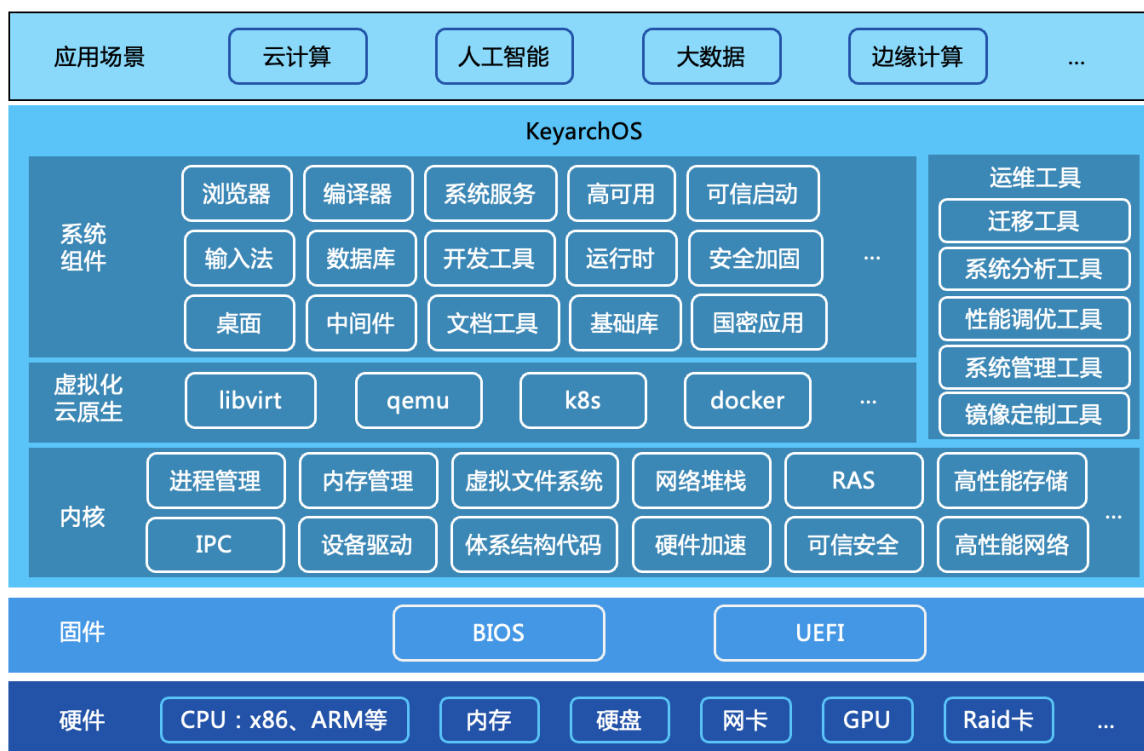
2 产品介绍

KeyarchOS 服务器操作系统是一款面向政企、金融、通信、能源交通等企业级用户的 Linux 服务器操作系统，KeyarchOS 的技术上游为龙蜥操作系统开源社区。基于龙蜥的开源生态基础上进行整合。其稳定性、安全性、兼容性和性能等核心能力均已得到充分验证。

KeyarchOS 服务器操作系统可广泛应用于大数据、云计算、人工智能、海量存储等应用场景，支持光盘、U 盘、PXE 等安装方式，可部署在用户物理裸机服务器、虚拟机和容器等环境，同时为用户提供部署、升级和迁移方案，以及完整的生态支持和专业的技术保障。

2.1 产品架构

KeyarchOS 在龙蜥操作系统开源技术和生态的基础上，进行了软硬件融合优化、安全增强、生态兼容，在具备龙蜥社区的技术架构与广泛生态基础之上，提供全方位的操作系统支持，是一款强安全、高可用、高可靠、高性能、易维护的服务器操作系统，能够为企业用户提供值得信赖的基础设施平台，满足企业用户多应用场景的需求。



产品架构图

2.2 产品关键特性

2.2.1 安全可靠

浪潮信息高度重视产品与解决方案的安全性，为客户提供更满意的服务。服务器产品安全一直是浪潮信息关注的焦点，保障产品安全是浪潮信息的关键战略之一。KeyarchOS 服务器操作系统在 Linux 自有安全特性的基础上，采用 TCM/TPM 可信启动、统一 PAM 认证模块、多因子认证、国密算法、主机加固软件、CVE 漏洞发现与修复等多种安全策略和安全机制，为用户提供全方位的安全防护体系。

1) 安全资质

KeyarchOS 服务器操作系统通过了安全操作系统四级、商密二级、供应链安全等权威安全资质认证。

2) 国密套件

- **国密算法库**：KeyarchOS 服务器操作系统全面支持 SM2、SM3、SM4 国产商用密码算法，实现 openssl、cryptography、libgcrypt、qemu、gnutls、nettle 等基础组件集成国密算法，支持 X86/ARM 两种架构，强化信息安全底座，助力多场景合规应用。
- **加密机适配库**：通过统一接口标准，实现对多厂商、多协议加密机的高效适配，支持 SDF、PKCS#11 等主流协议，提供 C/C++ 和 Java 两种语言版本，满足多业务场景需求。其设计支持加密机的动态切换与灵活扩展，降低开发成本。集成严格的访问控制和日志审计机制，确保操作可追溯和数据安全。加密机适配库全面支持 SM2、SM3、SM4 等国密算法，结合硬件加速技术，提供高性能加解密服务，并符合国家密码合规要求，为业务系统构建安全、可信、便捷

的加密服务解决方案奠定坚实基础。

3) 安全审计

KeyarchOS 服务器操作系统基于内核的安全审计功能，能够记录系统中的各种动作和事件，比如系统调用、文件修改、执行的程序等系统中所有的事件，可以可靠地收集任何与安全相关（或与安全无关）事件的详细信息，来提高系统的安全性。

4) 安全漏洞管理机制

浪潮信息致力于提供安全可靠的产品和服务，目标是及时为客户提供处理漏洞所需的信息、指导意见和风险缓解方案。浪潮信息打造了专业的系统安全漏洞管理机制，浪潮信息产品安全事件响应团队(PSIRT)负责接收、处理和公开披露与浪潮信息产品相关的安全漏洞，浪潮信息专业安全团队会定期发布系统安全补丁，并及时通知客户进行升级。

5) 安全防御模块 KSecure

功能简介

KeyarchOS 内置的轻量化安全防御组件 KSecure，采用 eBPF 技术，可提供轻量级安全检测和防御能力，防止黑客入侵及内部违规操作，有效提升了操作系统安全性和合规性。

技术挑战

传统安全检测和防御方案采用内核模块技术，编写不当的内核模块可能会导致系统崩溃或安全漏洞。相比之下，eBPF (extended Berkeley Packet Filter) 是一种新的内核技术，提供了一种安全、可编程的方式来扩展内核功能，具有“高稳定、高性

能、安全、灵活”的特点，具有深度的系统观测能力，在保障操作系统安全性的同时，最大限度减少对系统稳定性和性能的影响。

功能描述

KSecure 安全防御组件的主要功能如下：

安全基线检测：基于等保和 CIS 标准形成知识库，提供基于模板的基线检测、修复和回退功能；帮忙发现身份鉴别、访问控制、安全审计、入侵防范、剩余信息保护等方面潜在的安全风险，支持基线值自定义和灵活扩展。

关键文件/进程防护：支持文件和目录的防护，防止核心业务文件被篡改、删除等行为；支持关键进程防护，保护核心业务进程不被恶意终止、删除、信息注入；

主机/容器入侵检测：基于规则引擎，提供黑客入侵行为检测和自动处置；基于“诱饵”行为监测的勒索病毒防御，及时发现和阻止勒索病毒加密行为，作为抵御勒索病毒最后一道防线；

安全管理：支持安全特性动态加载、对安全组件 CPU 资源占用限制、安全策略热加载、服务启停和随机启动管理等功能。

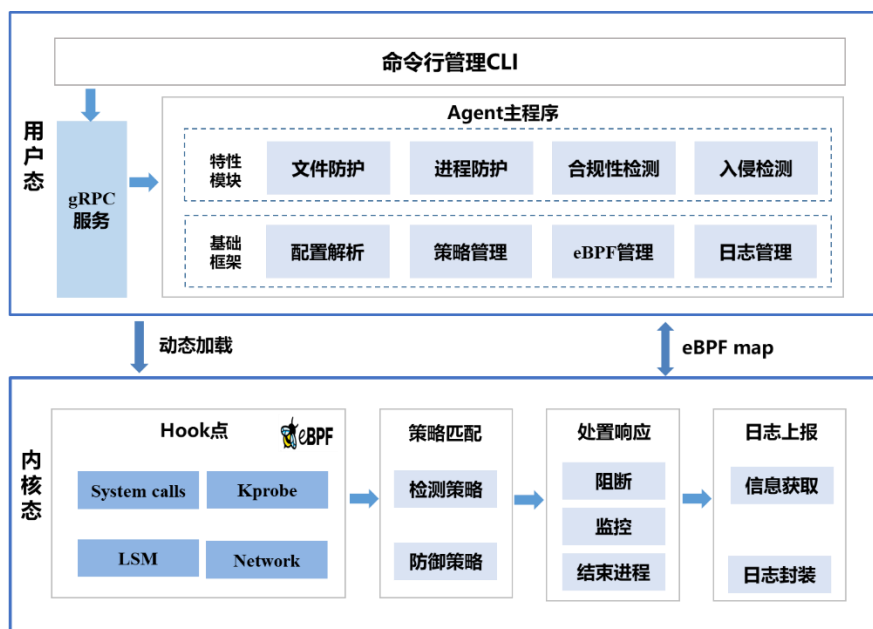
应用场景

应用场景 1：安全合规

基于标准和最佳实践对操作系统配置进行检测和自动修复，提升操作系统的合规性和安全性。支持用户结合实际的安全需求选择实施加固和扩展，以便更好地满足不同用户不同场景的配置安全基准要求。

应用场景 2：防黑客入侵

自动检测黑客入侵检测行为，并及时终止可疑进程。为主机关键业务提供保护，防止关键文件被篡改和内部违规操作。



软件架构图

KSecure 安全组件由用户态和内核态两部分组成：

用户态：KSecure 安全组件的用户接口为 CLI，使用 gRPC 服务实现 CLI 进程和主进程通信。通过基础框架支撑安全特性功能开发，通过特性开关调用 eBPF 函数将 eBPF 字节码程序加载至内核；

内核态：在内核对应事件触发时，运行相应的 eBPF 字节码程序，与配置的安全策略进行匹配，根据策略进行响应并上报安全日志。

6) 可信增强模块

功能简介

KTrusted 是一款基于可信根验证操作系统关键文件完整性的工具，为主流的

操作系统提供可信启动功能，让应用程序运行在安全可信的环境中。

技术挑战

随着云计算和大数据的兴起，计算节点承载越来越多的算力需求。服务器操作系统作为数据中心的基本单元，其上运行着业务系统和用户信息等重要数据，一旦服务器操作系统关键组件被恶意篡改，用户信息、业务数据也将面临被篡改、窃取的风险。

功能描述

KTrusted 基于可信度量功能，构建从服务器上电到操作系统启动的信任链；同时提供基于可信状态的操作系统引导控制、启动控制、可信报告查询等功能；在系统持续运行期间提供基于可信根的内核内存关键数据动态可信验证功能，并提供度量日志、审计日志。

系统启动时信任链构建功能的核心是从服务器硬件上电开始，通过可信根逐级度量服务器启动过程的各组件（BIOS BootBlock、BIOS MainBlock、BootLoader、OS Kernel、OS 模块等），并扩展度量结果到硬件可信根的安全存储空间，同时通过硬件安全芯片提供的密码服务，为上层应用及访问者提供验证平台可信的方法。

系统持续运行期间动态可信验证功能是以可信根为核心，对系统关键程序（如内核）运行时内存中的关键变量及数据（如系统调用表、代码段、中断描述符表、内核模块代码段、只读数据等）、以及属性等进行实时、周期性的可信度量及验证。

应用场景

KTrusted 实现从系统引导阶段到系统持续运行期间的可信验证覆盖，增强系统安全可信能力，适用于对业务系统安全防御要求较高及安全合规要求高的场景，例如金融、能源、电力政企用户等。

软件架构图



功能架构图

7) 机密计算功能

功能简介

KeyarchOS 机密计算功能在 Intel SGX、AMD SEV 等可信硬件基础上为应用提供数据机密性和完整性、代码完整性保护。基于 Intel SGX 可以快速构建进程级机密计算应用，并通过 Occlum 库操作系统可以实现应用无修改运行。

技术挑战

随着云计算和大数据的兴起，服务器操作系统作为数据中心基石，面临日益增长的算力需求与严峻的安全挑战。关键组件一旦被恶意篡改，用户信息与业务数据将受

严重威胁。传统 OS 安全手段难以抵御 bootkit 等启动过程攻击，系统启动安全成为 APT 攻击的主要突破口。

功能描述

KeyarchOS 机密计算功能支持 Intel SGX、AMD SEV/SEV-ES/SEV-SNP、HG CSV 等机密计算硬件。

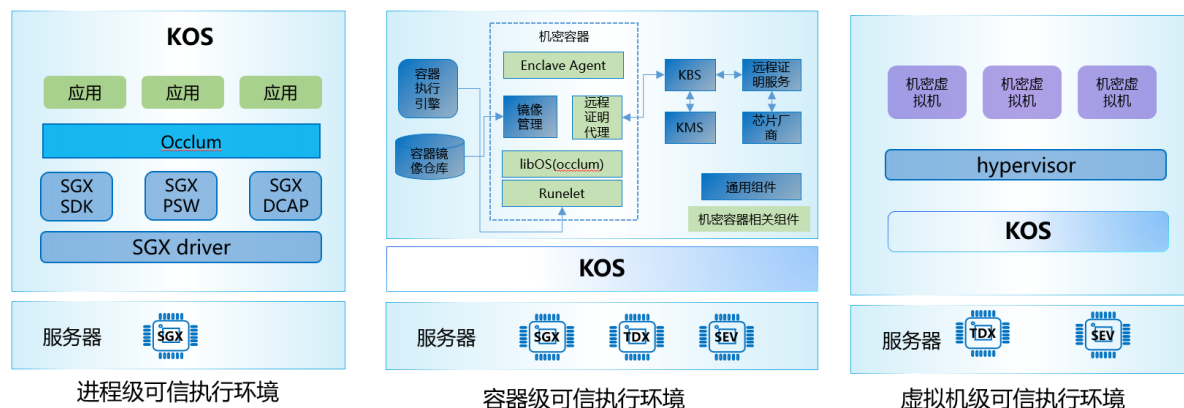
基于英特尔至强系列第三代可扩展处理器的 NF5280M6 服务器，KeyarchOS 机密计算功能最大支持机密计算内存可达 1TB。

KeyarchOS 通过对 Intel SDK、PSW 等软件包进行重新编译适配，已经将机密计算功能内置到 yum 源，实现对机密计算能力的开箱即用。同时，支持 Occlum 等库操作系统，可以通过 yum 源实现快速安装与使用，实现 Intel SGX 进程级机密计算应用无修改运行。

Occlum 库操作系统可以快速将 Nginx、Python、Redis、Sqlite 等应用运行在机密计算环境中，大大降低了机密计算应用的开发成本。

应用场景

机密计算技术有效实现对数据使用时的防护，解决了传统加密技术的短板，实现了对数据存储、数据传输、数据使用的端到端的全生命周期数据安全。机密计算主要应用在金融行业的联合风控、医疗领域的医学研究、商业领域的联合营销、人工智能技术中的联合建模及推理等场景。



系统架构图

2.2.2 稳定可靠

KeyarchOS 服务器操作系统历经近 10 余年自主研发历程，拥有丰富的操作系统产品研发和市场实践经验，在产品选型上采用稳定长期维护版本内核为基础，充分保证操作系统的高可靠运行。

KeyarchOS 支持内核热补丁功能，能够在不停机状态下进行内核漏洞和 bug 的修复，用户可以在 yum 源中安装指定内核版本的热补丁修复 RPM 包，提升 KeyarchOS 系统的不停机时间，保证用户业务高可用。

在业务层面，KeyarchOS 提供完善的集群高可用套件，有效支撑了应用高可用部署、故障无感切换，保障业务连续性。

KeyarchOS 还提供了 rasdaemon 工具用于监测和记录硬件错误事件，rasdaemon 能够捕捉各种硬件错误事件，包括内存错误、处理器错误、总线错误等。rasdaemon 工具不仅能够实现硬件错误的监控，还能实现基于阈值的 UCE 内存故障预测，将即将发生内存故障的内存页隔离，保证系统的可用性。

2.2.3 高效运维

1) 系统异常定位分析模块 KSysAK

模块简介

KSysAK 是一款全方位的系统运维工具集，基于百万量级服务器运维经验抽象总结开发而成，覆盖了日常监控、线上诊断和故障修复等常见运维场景。

技术挑战

在系统运维过程中，资源的监控与利用、问题的排查与解决是核心诉求，满足这些诉求需要一系列的操作系统底层能力与工具，而这些能力与工具目前分散在多个不同的场景。如何有效地整合这些能力与工具，发挥其作用，以及怎样更方便的在系统上部署，目前缺少一个整体的方案，特别是在现代云计算中心中，大规模集群通常含有不同的硬件平台、系统以及业务场景，对这些能力与工具有着较高的要求。在 Linux 操作系统中，现有的运维手段能力有限，具体体现在缺乏持续监控能力、缺乏自动分析诊断能力、缺乏线上问题诊断能力等。解决这些运维问题则面临以下难点：

1. 无侵入的系统能力；
2. 持续、精细化、低负载的监控能力；
3. 自适应不同场景的异常检测、故障判断能力；

功能描述

针对以上问题，KSysAK 包含了若干子工具，如 pingtrace 用于网络分析，memleak 用于内存泄露分析及诊断，ossre 用于检测系统配置指标检查以及系统已知问题识别，sysmonitor 用于系统负载情况。

KSysAK 框架包括监控模式和诊断模式。

监控模式：

- ✓ 系统资源瓶颈指标包括 CPU 瓶颈、内存瓶颈、网络瓶颈、IO 瓶颈，通过对瓶颈的监控可以发现应用运行过程中对资源的依赖度，再通过依赖度有效配合其他数据，对应用做合理的调度和资源分配。除了硬件四大资源之外，系统软件本身也会存在瓶颈，比如 Linux 内核系统实现各种文件、句柄、cache、共享资源的访问过程中都有可能产生并发瓶颈，KSysAK 针对此瓶颈做了很多工作。
- ✓ 干扰是应用运行过程中是比较常见的因素，会引发抖动或运行中断等。云原生的趋势下，KSysAK 实现了容器资源可视化。

诊断模式：

诊断模式指及时发现问题，并根据问题根因做诊断，随用随起。根据用户运维场景，包括但不限于：

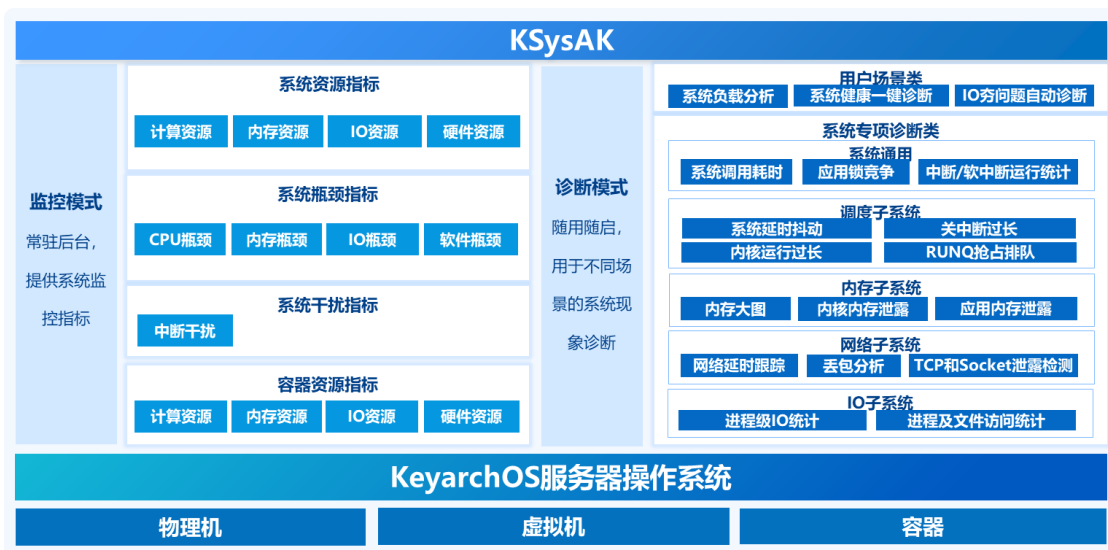
- ✓ 系统负载分析：系统负载是系统运维过程中的典型问题，针对此问题进行根因分析，避免影响进程堆栈。
- ✓ 系统健康一键诊断：对系统各个资源维度进行分析，查看配置是否合理等。
- ✓ IO 问题自动诊断：IO 打满时，自动分析是应用瓶颈还是业务瓶颈导致。

除了用户场景，KSysAK 工具集对高级技术人员提供了更深层次的数据诊断，比如系统调用数据耗时较长的函数、中断运行统计、调度模块、内存模块、延时抖动、内存泄露等，KSysAK 会根据每个子系统的特点做专项功能诊断。

应用场景

KSysAK 在 KeyarchOS 操作系统中主要面向场景包括数据库、分布式存储、虚拟化、云原生等。为金融、电信、互联网等行业客户提供全栈可观测能力，实现操作系统的全方位监控和故障诊断能力。

软件架构图



功能架构图

2) 系统性能调优模块 KTuning

模块简介

KTuning 是一款 AI 算法与专家知识库双轮驱动的操作系统全栈式智能优化产品，为主流的操作系统提供轻量化、跨平台的一键式性能调优，让应用在智能定制的运行环境发挥最优性能。

技术挑战

随着几十年来硬件和软件应用的不断发展，Linux 内核正变得越来越复杂，整个操作系统也变得越来越庞大。大部分使用者只使用了这些参数的默认配置，因此无法充

分发挥系统最佳性能。然而，针对特定的应用场景进行调优面临以下几个难点：

- ✓ 参数数量多，且参数间存在依赖关系
- ✓ 上层应用系统种类多，不同应用系统的参数不同
- ✓ 每个应用的负载也复杂多样，不同负载对应的最优参数值也不同

功能描述

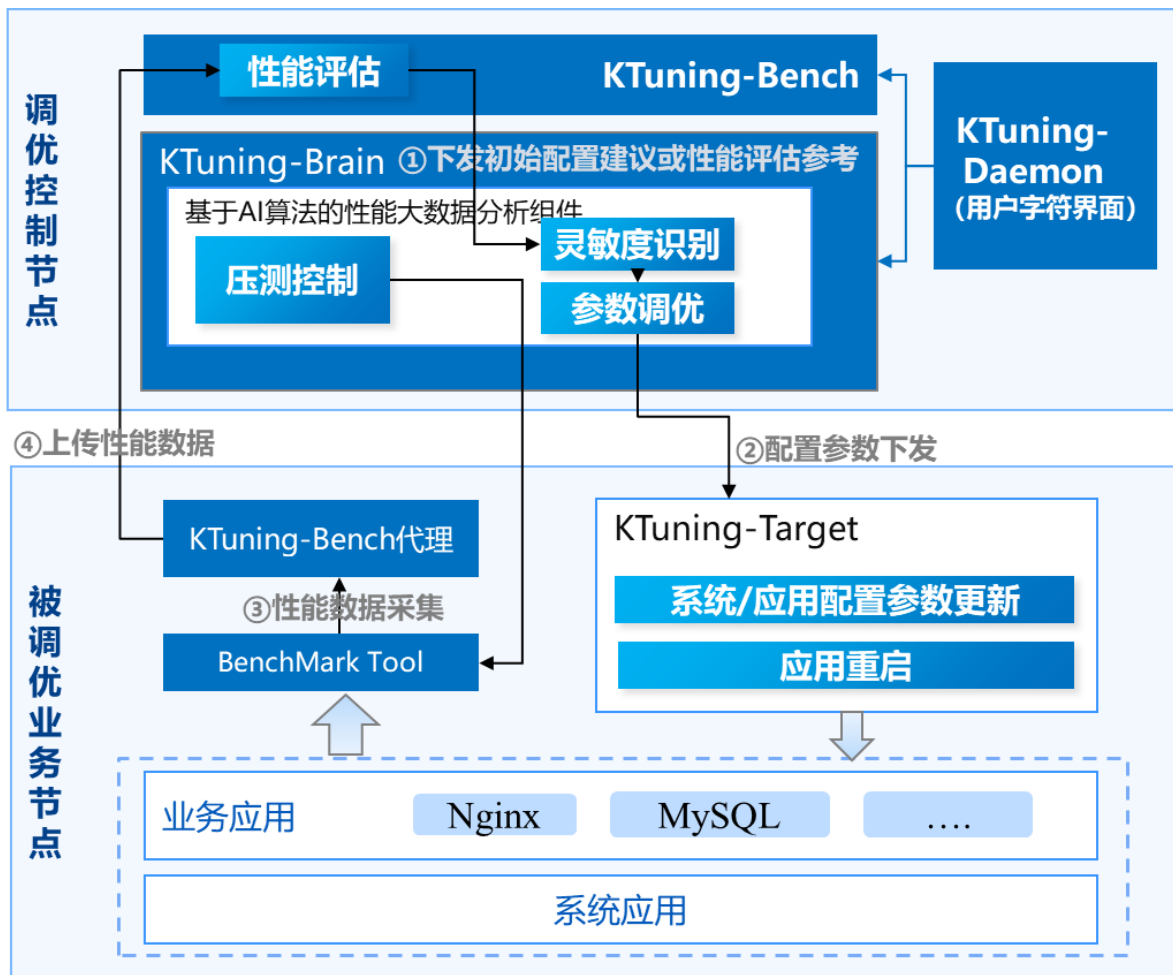
KTuning 最基本的功能是使用操作系统或应用软件提供的配置修改接口修改操作系统或应用软件的配置，使运行参数满足用户的期望。而根据配置参数生成的方式，KTuning 的工作模式又分为动态调优模式和专家调优模式（静态调优模式）。

动态调优模式：KTuning-Brain 组件利用 AI 算法分析 KTuning-Bench 对业务环境压测得到的参数，基于算法计算得出系统/应用运行的最优配置参数，通过 KTuning-Target 修改系统/应用配置参数，达到调优的目的。

专家调优模式：KTuning-Daemon 维护了一组基于经验得到的系统/应用参数配置文件，有用户根据实际的业务场景部署需要的配置文件以达到性能调优的目的。

应用场景

KTuning 可以帮助用户在相同资源的环境下，获取更高的网络吞吐、更低的网络时延、更高效的业务处理能力和更快的业务响应速度。同时，用户可以根据自己的业务需求，减少对硬件资源的需求，从而降低业务运营成本。



软件架构图

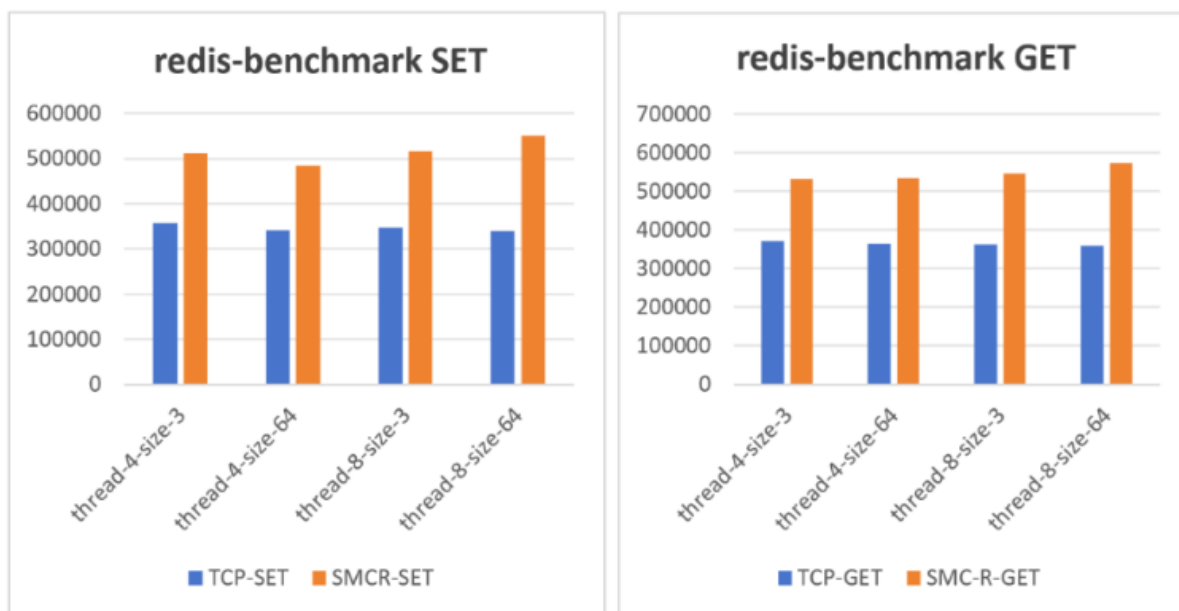
2.2.4 极致性能

KeyarchOS 在保证系统稳定性和安全性的同时，通过软硬协同、上游优秀特性回合等方式持续对性能进行优化，包括但不限于以下功能：

1) SMC-R 高性能网络

RDMA 是一种远程内存直接访问技术，可以显著提升网络通信性能，但为了使用 RDMA 网络需要修改应用程序，这很大程度限制了 RDMA 技术的应用。内核网络协议 SMC-R 在利用 RDMA 技术的同时、又进一步完美兼容了 socket 接口，能够透明无感的为 TCP 应用带来网络性能提升。使用者可以使用 LD_PRELOAD 或 ULP +

eBPF 的方式透明的将应用程序中的 AF_INET 族 socket 替换为 AF_SMC 族 socket, 从而可以实现不修改应用程序就能够使用 RDMA 高性能网络。



Redis 基准性能测试

在 redis-benchmark 测试中, SET 方法使用 TCP 协议, 无论线程数或数据包大小场景下均比较稳定, 使用 SMC 协议, 提升幅度较大, 达到 40%以上, 在线程数 8、数据包大小 64 情况下提升 60%。GET 方法测试结果与 SET 方法相近, 性能提升趋势也基本一致。

2) CXL 分层内存优化

CXL 是目前解决内存扩展瓶颈的最有前景的技术, 但与 DRAM 内存相比, 扩展内存面临高延迟、低带宽的技术挑战, 分层内存可以最优化利用 CXL 内存。分层内存将 DRAM 划分为快速内存、CXL 内存划分为慢速内存, 当 DRAM 内存水位较高时通过优化页回收机制实现 DRAM 上的冷页迁移至 CXL 内存中, 当识别到 CXL 内存中频繁访问的热页时动态将其迁移到 DRAM 内存中, 最终实现频繁访问的热页保持在

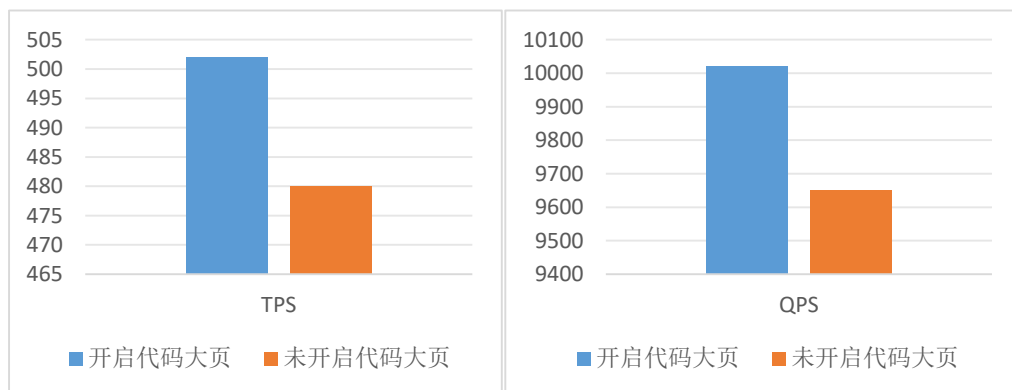
DRAM 中，不经常访问的冷页保持在 CXL 内存中。

以 1:4 的比例混合使用 DRAM 内存和 CXL 内存时，开启分层内存后的 Redis 性能比开启分层内存前提升了大约 12%。

3) 代码大页

透明大页支持通过一次性分配 2M 页填充进程页表，避免多次缺页开销，从硬件角度优化了 TLB 缺失开销，能够提升某些应用的性能。但透明大页也会导致严重的内存碎片化、内存膨胀和内存利用率低等问题，以上问题导致透明大页没有在数据库中被广泛使用。代码大页在透明大页的基础上，将支持扩展到可执行二进制文件，包括进程二进制文件本身、共享库等可执行数据。与透明大页相比，由于代码大页仅将占比较低且有限的可执行文件页部分转换为大页，从根本上避开了内存碎片以及内存不足的问题，所以在数据库场景中使用代码大页相比透明大页更加简单推广。

KeyarchOS 支持了代码大页功能，在 X86 架构下开启代码大页后，mysql 性能提升 3%-5%。



MySQL 性能测试

4) io_uring

io_uring 是内核社区设计的一种全新的异步 IO 框架，应用程序和内核之间通过共享 ring buffer 进行通信，避免了在提交和完成事件中的内存拷贝，从而提升 io 性能。该技术特点包括：a) 简单易用，方便应用集成；b) 可扩展，不仅仅为存储 IO 使用，同样可以用于网络 IO；c) 特性丰富，满足所有应用，如支持 Buffer IO；d) 高效，尤其是针对大部分 512 字节或 4K IO 场景；e) 可伸缩，满足峰值场景的性能需要等。io_uring 可适用于绝大多数对异步 IO 有诉求的业务和应用，目前在主流的应用软件中都已经集成。

基于 fio 进行测试，采用 io_uring 引擎相比于使用 aio 引擎的顺序读写性能提升 150%，随机读写性能提升 100%。

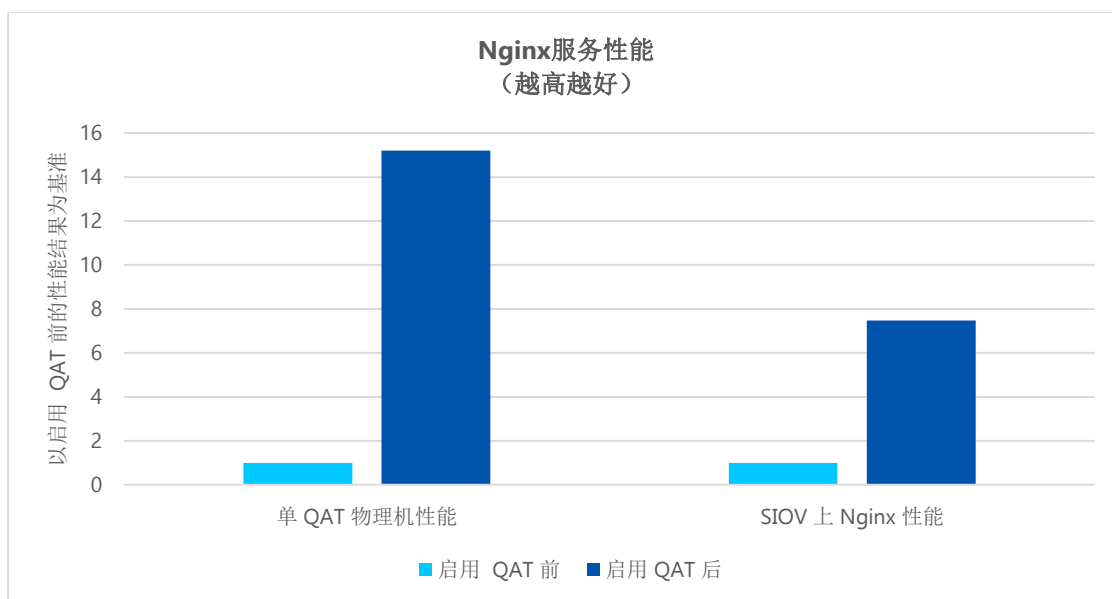
5) 硬件加速

KeyarchOS 和 Intel 等芯片公司深入合作，使能硬件加速特性，进一步提升操作系统性能和效率。

● QAT 加速

英特尔 QAT 能够有效提升应用程序和平台的性能，在数据路径中，QAT 带来的高压缩比特性，能够广泛用于存储、高性能计算和大数据、文件系统、数据库等场景，KeyarchOS 提供了 QAT 的驱动及相关配套工具，方便用户直接使用。

- ✓ 基于 QAT 提升 Nginx 服务性能：测试环境为单个 QAT PF 节点（直通模式），Nginx worker_processes 设置为 2，在启用 Intel QAT 之后，Nginx 服务性能提升到超过 15 倍。



Nginx 性能测试

- ✓ 基于 QAT 加速虚拟机的在线迁移：利用 QAT 硬件提供的算力，对需要传输的内存数据进行压缩和解压缩，将压缩和解压缩功能全部 offload 到 qat 硬件，解放 cpu 资源。针对不同的虚拟机内存规格（32G、48G、64G、96G、128G）分别测试使用 qat 迁移加速和不使用 qat 迁移加速，最终在 libvirt 端使用 qat 迁移加速比不使用 qat 迁移加速块将近 1 倍。

- RDT 资源调配技术

英特尔 RDT 提供了一个由多个组件功能（包括 CMT、CAT、CDP、MBM 和 MBA）组成的框架，用于缓存和内存监控及分配功能。这些技术可以跟踪和控制平台上同时运行的多个应用程序、容器或 VM 使用的共享资源，例如最后一级缓存 (LLC) 和主内存 (DRAM) 带宽。RDT 可以帮助检测“吵闹的邻居”并减少性能干扰，从而确保复杂环境中关键工作负载的性能。

KeyarchOS 在内核中使能了 RDT 技术，并且验证了基于 RDT 保护 OpenStack 和 Redis 关键业务程序，均能获得预期效果。

- ✓ 基于 RDT 保护 OpenStack 关键服务：通过使用 RDT 技术分配 12 路 L3 保护 OpenStack 控制面，创建 300 台虚拟机的性能提升 50%
- ✓ 基于 RDT 保护 Redis 核心业务：存在 Noise Neighbor 干扰的情况下，没有开启 RDT 时，Redis 性能下降约 21%，通过 RDT 技术为 Redis 工作负载分配 80%内存带宽后，Redis 性能可恢复到原来的 95%。

2.3 产品技术指标

指标名称	指标内容
基础核心	Linux Kernel 5.10 LTS
支持芯片	Intel、AMD、Ampere、Hygon、Phytium、Kunpeng等主流处理器
核心参数	最大支持CPU数量：【x86】8192、【arm】256
	最大支持内存：【x86】64TB、【arm】256TB
	文件系统支持：支持XFS, GFS2, EXT3, EXT4、NTFS、FAT32等多种文件系统格式，支持LVM调整分区大小
板卡支持	支持主流网卡、raid卡、SAS卡、GPU、DPU、HBA、HCA、NPU等部件
网络协议支持	支持IPV4/IPV6协议 支持RDP、SSH、VNC等远程控制协议 支持NFS、SMB、FTP、CIFS等数据网络共享服务协议 支持HTTP、HTTPS等web服务协议

指标名称	指标内容
	支持IPSec和SSL的加密协议 支持NTP时间同步协议 支持SNMP、NETCONF等网络管理协议
安装方式支持	光盘、USB等物理存储介质
	支持图形和文本模式安装
	PXE网络安装
虚拟化支持	支持KVM虚拟化
	支持在KVM、Xen、Hyper-V、ESXi 虚拟机上安装部署
开发环境支持	支持QT、Eclipse、VSCode等集成开发环境 支持GNU C/C++、Java、QT、perl、Python、rust、Ruby、Golang、JS等开发库 支持GCC、GDB、Make、Cmake等编译开发工具
开源软件支持	支持MariaDB、Redis、Mongodb、PostgreSQL等开源数据库 支持Tomcat、RabbitMQ、Nginx等开源中间件 支持QEMU、libvirt虚拟化管理软件 支持docker、kubernetes等容器管理软件 支持Ceph、GlusterFS等分布式存储软件 支持OpenStack等云计算管理平台软件

3 系统主要功能

3.1 网络配置

KeyarchOS 支持各种类型的网络接口，包括以太网、Wi-Fi、虚拟接口等，管理员可以使用 nmcli、ip、ifconfig 等工具来管理这些接口，包括启用、禁用、配置 IP 地址等，还可以通过修改/etc/sysconfig/network-scripts/下的网卡配置文件进行网络配置。

KeyarchOS 支持通过 iptables 和 firewalld 工具配置网络访问控制规则，保护系统和网络免受未经授权的访问，提供了 ping、traceroute、netstat 等工具诊断网络问题，辅助进行性能优化。

3.2 软件包管理

KeyarchOS 使用 dnf 命令管理 RPM 软件包，dnf 可以查询软件包信息，从指定软件库获取软件包，自动处理依赖关系以安装或卸载软件包，以及更新系统到最新可用版本。dnf 包管理器克服了 yum 包管理器的一些瓶颈，提升了包括用户体验、内存占用、依赖分析和运行速度等多方面的内容，dnf 使用 rpm、libsolv 和 hawkey 库进行包管理操作，可以与 yum 同时使用。

管理员还可以采用 module(模块)的方式安装软件包，这样可以在一个源或者多个源中存在不同的版本的软件包，采用 module 的方式可以根据需求选择不同版本的软件包，并且安装的时候不会产生冲突。

3.3 Systemd 服务管理

系统管理员可以使用 systemd 管理系统，主要用于控制、报告和系统初始化的工

具和服务，systemd 的主要功能包括：在操作系统启动过程中并行启动系统服务；按需激活或者关闭系统服务。

systemd 主要功能是基于 unit，Unit 由一个名称、类型和配置文件组成，用来定义和管理特定的任务，管理员可以使用单元文件来配置系统行为。

systemd 主要有以下特性：并发启动、按需启动、资源控制、挂载和自动挂载、兼容 SysV、快照功能。

并发启动：Systemd 采用 socket/D-Bus activation 技术启动服务，加快了操作系统的启动速度。

按需启动：Systemd 提供按需启动服务的能力，只有在服务被真正的请求的时候才启动。

资源控制：Systemd 集成了 Cgroup 的资源控制功能。通过 systemd 可以快速灵活的控制进程使用的资源。

挂载：Systemd 提供了系统启动时自动挂载设备的能力和手动配置文件系统挂载的能力。操作系统在启动时能够满足设备和文件系统的挂载需求。

兼容 Sysv：Systemd 兼容 Sysv 服务的脚本，对这些脚本可以不加修改的直接使用。减少了迁移成本。

快照功能：Systemd 提供了对当前运行的服务创建快照的能力。并在需要时可以按需恢复快照。

3.4 用户管理

在 KeyarchOS 中，每个普通用户都有一个账户，包括用户名、密码和主目录等信

息，除此之外，还有一些系统本身创建的特殊用户，它们具有特殊的意义，其中最重要的是管理员账户，默认用户名是 root。同时 Linux 也提供了用户组，每一个用户至少属于一个组，从而便于权限管理。

用户和用户组管理是系统安全管理的重要组成部分，管理员可以使用 `useradd` 命令添加用户、`passwd` 命令修改密码、`usermod` 命令修改用户、`userdel` 命令删除用户、`groupadd` 命令添加用户组、`groupmod` 命令修改用户组、`groupdel` 命令删除用户组等。

3.5 磁盘管理

KeyarchOS 提供图形化的磁盘管理工具和命令行的磁盘管理工具。图形化的磁盘管理工具需要安装 `gnome-disk-utility` 软件包，支持格式化磁盘、创建分区、格式化文件系统、挂载/卸载分区、删除分区、备份/恢复磁盘等功能。磁盘管理相关的命令包括，`lsblk` 命令查询所有可用的块设备、`df` 命令查看系统上文件系统的磁盘使用情况统计、`du` 命令用来展示磁盘使用量的统计信息、`fdisk/parted` 命令进行磁盘分区操作、`mkfs` 命令格式化分区文件系统、`mount` 命令挂载文件系统、`umount` 命令卸载文件系统等。

3.6 LVM 管理

KeyarchOS 支持 LVM 逻辑卷管理，LVM (Logical Volume Manager)，即逻辑卷管理，是 Linux 环境下对磁盘分区进行管理的一种机制，LVM 是建立在硬盘和分区之上的一个逻辑层，来提高磁盘分区管理的灵活性。通过 LVM 系统管理员可以轻松管理磁盘分区，如：将若干个磁盘分区连接为一个整块的卷组 (volume group)，形成一个存储池。管理员可以在卷组上随意创建逻辑卷组 (logical volumes)，并进一步

在逻辑卷组上创建文件系统。管理员通过 LVM 可以方便的调整存储卷组的大小，并且可以对磁盘存储按照组的方式进行命名、管理和分配。当系统添加了新的磁盘，通过 LVM 管理员就不必将磁盘的文件移动到新的磁盘上以充分利用新的存储空间，而是直接扩展文件系统跨越磁盘即可。

dm_mod 模块已经集成到了内核中，管理员可以通过 pvcreate 命令管理物理卷、vgcreate 命令管理卷组、lvcreate 命令管理逻辑卷。

3.7 日志管理

KeyarchOS 的日志文件是包含 kernel, services 和运行在上面的应用软件的消息的合集。不同的日志会存储在不同的文件中，比如 secure 相关日志保存在 /var/log/secure 中，定时任务的日志保存在 /var/log/cron 文件中。

日志文件的 daemon 有两个：rsyslog 和 journal

rsyslog 是基于 syslog 协议的，它提供高性能、极好的安全功能和模块化设计。能够接受来自各种来源的输入，转换它们，并将结果输出到不同的目的地。

Journald 是 systemd 的一个组件。journald 守护进程捕获 Syslog 消息、内核日志消息、初始 RAM 磁盘和早期启动消息以及写入所有服务的标准输出和标准错误输出的消息，对它们进行索引并提供给用户。

为了避免日志文件无限增长并占用过多的磁盘空间，KeyarchOS 提供了 logrotate 工具用于管理日志文件的轮换，它的主要功能是定期或根据一定的条件轮换日志文件，可以配置指定哪些日志文件需要轮换、轮换的频率等，并且支持日志的压缩等功能。

3.8 时间配置

KeyarchOS 提供 `chrony` 用来进行时间同步，`Chrony` 是一款用于时间同步的软件工具，特别针对 Linux 系统设计。它的主要目标是提供高精度和快速的时钟同步服务，确保计算机系统的时钟与标准时间高度一致。相对于传统的 `NTP` 工具，`Chrony` 通常能够更快地实现时钟同步，这对需要高精度时间的应用程序尤为重要。`Chrony` 以系统服务的形式存在，可使用 `systemd` 或其他服务管理工具来启动、停止和监控。

KeyarchOS 同样提供 `date`、`clock`、`hwclock` 等常用的时间设置工具。

3.9 系统监控

KeyarchOS 提供了许多用于监控和管理系统性能的工具，以下是一些常见的系统监控工具：

`perf`: `perf` 用于在 Linux 系统上进行性能分析和调优，可以帮助管理员深入了解应用程序和系统的性能特征。

`bpftrace`: 基于 `eBPF` 技术实现，允许系统管理员在不需要重新编译内核模块的情况下，获取深入的性能和调试信息，能够用于性能调优、故障排除、安全监控等。

`top`: `top` 命令显示实时的系统性能数据，包括 CPU 使用率、内存使用情况、进程列表等。它是一个命令行工具，可通过交互式方式查看信息。

`htop`: `htop` 是 `top` 命令的增强版，提供更多的功能和更直观的界面，使系统监控更方便。

`vmstat`: `vmstat` 命令提供有关系统的虚拟内存、进程、磁盘、CPU 等方面的信息，以及统计数据，可以用于实时监控和分析性能问题。

iostat: iostat 命令用于监控系统的磁盘 I/O 性能，显示磁盘读写速度、I/O 请求和等待时间等信息。

sar: System Activity Reporter (sar) 工具可以记录和报告系统的性能数据，包括 CPU、内存、磁盘、网络等，用于生成性能历史数据和分析。

iftop: iftop 可以监视网络流量，显示实时的网络带宽使用情况，对于分析网络性能非常有用。

mpstat: 用于监视多核/多处理器的性能统计信息。

tcpdump: tcpdump 是一个网络数据包捕获工具，可以用于详细分析网络流量，对网络故障排除和安全审计很有帮助。

4 典型应用场景

KeyarchOS 服务器操作系统提供灵活的安装部署方式，支持行业主流硬件和软件，提供完善的系统功能服务，具有强安全、高可用、高可靠、高性能等关键特性，用户可以将 KeyarchOS 用户物理裸机服务器、虚拟化、容器等环境中，同样面向行业提供服务器操作系统解决方案，满足云计算、大数据、海量存储、人工智能、边缘计算等应用场景需求。

4.1 物理裸机服务器

KeyarchOS 作为服务器操作系统可直接部署于物理裸机服务器上，为用户提供基础的软件服务和可靠的运行环境。

4.2 虚拟化

KeyarchOS 操作系统支持虚拟化技术，既可以作为物理机上的宿主机操作系统也可用作虚拟机上的客户机操作系统。KeyarchOS 提供了常用的 KVM、QEMU、Libvirt 等虚拟化组件，支持硬件辅助虚拟化，能够满足用户不同的虚拟化场景需求，提供常用的虚拟机管理工具(如 virsh、virt-install、virt-manager 等)，方便用户运维和管理虚拟机。

KeyarchOS 操作系统支持容器技术，容器是一种相对于虚拟机来说更加轻量的虚拟化技术，以一种可移植、可重用的方式来打包、分发和运行应用程序。该技术具有敏捷化、轻量安全、可移植性强、资源利率高、易部署等特点，能为用户提供更灵活、高扩展性、高可用性、更高效的业务部署，KeyarchOS 操作系统支持 docker、podman 等主流容器基础平台，实现容器的全生命周期管理。

4.3 云计算

随着云计算及虚拟化技术的成熟，用户越来越多的将应用和业务部署和迁移到云端，KeyarchOS 操作系统不仅适配浪潮信息自研的云计算基础框架平台，也支持 Openstack 等开源虚拟化云计算框架平台，方便用户搭建和部署云计算平台。

4.4 大数据

针对大数据应用场景，KeyarchOS 服务器操作系统提供整套的大数据解决方案，适配了 Hadoop、Hive、Flink 等国内外主流的大数据引擎、数据存储、数据处理等工具套件，提供多源数据集成、高效存储、分布式计算与调度、高并发访问以及分析挖掘能力，可应对 GB-PB 量级的海量异构数据场景，帮助客户轻松构建数据的全生命周期管理体系。

4.5 人工智能

在人工智能在深度学习、计算机视觉、仿真等领域已经取得了广泛应用，作为新一代计算信息技术的核心，基于人工智能的应用和落地越来越多。KeyarchOS 操作系统针对人工智能应用场景，提供相应的软件解决方案，并适配了主流的人工智能框架，包括 Tensorflow、Scikit-learn 等。

4.6 边缘计算

在人工智能和 5G 等技术蓬勃发展的背景之下，边缘计算的应用和落地越来越多。在 ICT 融合、新一代 CDN、智能网联汽车、工业互联网、产业+AI、城市治理、智能物联网等领域应用落地，海量数据在边缘产生、复制、存储、传输及分析应用，边缘计算的价值日益凸显。KeyarchOS 操作系统发布面向边缘计算的版本，同时提供边缘计算软件解决方案。

5 服务与支持

浪潮信息秉承以客户为关注焦点，技术创新是原动力理念，关注客户需求，通过技术创新和产品创新，为客户提供完善的产品和解决方案，KeyarchOS 即是浪潮信息众多产品的核心一员。作为浪潮信息打造的一款基础设施系统软件，KeyarchOS 为用户提供全方位技术服务支持，以满足不同用户、不同场景的技术支持服务需求。