# 银河麒麟云底座操作系统 V10

# 版本发布说明

麒麟软件有限公司

2024 年 7 月

## 商标声明

KYLINSOFT 麒麟软件和其他麒麟商标均为麒麟软件有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受麒麟软件有限公司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，麒麟软件有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容有可能变更，麒麟软件有限公司保留在没有任何通知或提示的情况下对内容进行修改的权利。除非另有约定，本文档仅作为使用指导，并不确保手册内容完全没有错误。本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 1. 版本概述

此次发布的是银河麒麟云底座操作系统 V10 的更新版本，继续基于 openEuler 22.03 LTS 的优秀技术特色，并结合麒麟针对云场景深入理解，进一步增强优化的云底座操作系统。打造云原生、高性能、高安全、易迁移等产品特性，加速用户业务上云，提升用户的应用创新空间，可替代 CentOS、OpenEuler 等公共镜像。本发布说明列举了云底座操作系统主要特性、社区引入技术及更新内容。

# 2. 版本信息

| 类型 | 版本信息 |
| --- | --- |
| 产品名称 | 银河麒麟云底座操作系统 V10 |
| ISO 名称 | （11584） Kylin-HostOS-V10-2406-Release-20240719-ARM64<br>（11590） Kylin-HostOS-V10-2406-Release-20240719-X86_64 |
| 源代码 | （11591） Kylin-HostOS-V10-2406-Release-Source-20240719-all |
| 发布时间 | 2024 年 08 月 19 日 |
| 发布格式 | ISO、源代码 |
| 版本查询方式 | 终端：输入 cat /etc/.kyinfo 查询 |

# 3. 技术参数

| 类型 | 参数信息 |
| --- | --- |
| 支持架构 | ARM 和 X86 |
| 支持处理器类型 | 飞腾：FT-2000+/64、腾云 S2500<br>鲲鹏：920、920 V200<br>海光：海光 C86-3G、海光 C86-4G<br>Intel/AMD 等服务器平台 |
| 支持固件类型 | BIOS/UEFI |
| 内核版本 | 5.10.0 |
| glibc 版本 | 2.34 |
| gcc 版本 | 10.3.1 |
| 开发语言支持 | c/c++、java、go、python 等 |
| 中文支持 | GB18030-2005 |

| | |
|---|---|
| **授权方式** | 在线、离线、KMS 机制、订阅 |
| **补丁更新** | 每周 |
| **虚拟化版本** | edk2-202011、qemu-6.2.0、libvirt-6.2.0 |
| **openstack 版本** | Train、Wallaby |
| **kubernetes 版本** | 1.23.12、1.24.16、1.25.12、1.26.7、1.28.10、1.29.5 |
| **边缘计算版本** | kubeedege-1.14.2、k3s-1.24.2 |
| **容器运行时版本** | docker-engine 18.09.0-325、docker-ce 20.10.24<br>crio 1.24.6、1.25.3、1.26.4<br>containerd 1.2.0-309、1.6.20 |
| **客户群体** | 云厂商、自建云 |
| **配套文档** | 银河麒麟云底座操作系统 V10 安装手册<br>银河麒麟云底座操作系统 V10 系统管理员手册<br>银河麒麟云底座操作系统 V10 产品白皮书<br>银河麒麟云底座操作系统 V10 技术白皮书 |

## 4. 主要更新

- 英特尔®至强® 6 处理器支持：新增对英特尔®至强® 6 处理器的支持，确保系统与最新硬件架构无缝对接；
- 新增支持澜起的国密加密算法硬件卸载能力；
- 海光 C86-4G 芯片架构优化：增强对海光 C86-4G 芯片的兼容性，引入 cache 和仿存 QoS，以及 L3 Perf/PMU 功能，提升系统响应速度与资源分配效率。
- iSCSI 链路切换效能升级：优化 iSCSI 链路切换机制，缩短多路径存储场景下的故障恢复时间，保障数据传输的连贯性与稳定性。
- 大块 IO 限流精进：在大块 IO 场景下，内核 IOPS 限流功能得到优化，实现更稳定的限流控制与更精确的 BPS 统计，确保系统性能的均衡与高效。
- 内存动态隔离与释放机制：引入安全、稳定的内存页面动态隔离与解除隔离功能，支持隔离状态下原内存的安全迁移。
- 核隔离技术深化：强化核隔离特性，有效抑制 HPC（高性能计算）场景下磁盘中

断产生的噪声，进一步净化系统底噪，提升整体计算效能与用户体验。

- 容器场景下的在离线混部技术增强：引入动态频率调节，实现高频 CPU 动态扩展，优化功耗；新增 psi 感知内存回收机制，动态平衡在线与离线业务内存需求，提升资源利用率。
- 虚拟化技术升级：新增支持虚拟机跨系统热迁移功能，支持将虚拟机从 openEuler 22.03 系列及 RHEL 8 系列系统热迁移到银河麒麟云底座操作系统 V10；新增通过 dirty-limit 的方式迁移正在运行的虚拟机，缩短迁移时间；MCE 内存故障定位，精准识别受影响虚拟机，加速故障响应。
- 新增低时延高性能网络协议栈：支持基于 dpdk 在用户态直接读写网卡报文，共享内存传递报文，配合轻量级 lwip 协议栈大幅提高应用的网络 I/O 吞吐能力；新增低时延高性能网络协议栈 gazelle 的观测工具，支持输出指定协议下的 rx 和 tx 方向的包数量累计信息，优化网络流量管理。
- 一键式性能调优：集成指标采集、性能分析与静态调优，智能识别瓶颈，提供典型场景调优建议，简化运维流程。
- 系统级故障智能分析：一键日志收集，系统体检与监控，主动检测安全漏洞、异常服务与不合理配置，强化系统安全与稳定性。
- 不可变 NestOS 操作系统创新：支持用户自定义不可变操作系统构建，简化集成与升级流程。
- 动态度量安全保障：周期性 hash 检测，实时监控关键软件信息完整性，根据策略配置响应篡改事件，强化系统安全防御。
- 支持安全启动：新增国密算法支持，支持 shim、grub 和内核文件使用国密算法签名，支持物理机和虚拟机环境下使用国密和非国密进行安全启动

# 5. 附录 I 更新内容

## 5.1. 内核

支持 5.10.0-182.9.v2406 版本 。

支持英特尔®至强® 6 处理器。

支持海光 C86-4G：支持海光 C86-4G 芯片架构，新增支持 cache 和仿存 QoS，新增支持 L3 Perf/PMU 功能。

iSCSI 链路切换时间优化：降低 iSCSI+多路径存储场景下的链路故障切换恢复时长。

内核大块 IO 限速优化： 优化在大块 IO 场景下内核的 IOPS 限流功能，使限流更稳定， BPS 统计更准确。

内存动态隔离和释放：提供安全、稳定的内存页面动态隔离与解除隔离的功能，支持隔离时安全迁移原内存。

核隔离增强：在 Linux 原有核隔离机制的基础上，进一步消除核隔离场景下磁盘中断的噪声，降低 HPC 场景系统底噪。

支持 CPU 在线巡检：静默数据损坏（SDC）可能导致数据丢失和数据被破坏。通过执行巡检指令，发现存在静默故障的核，提前对故障核进行隔离，避免出现更严重的故障，提高系统可靠性。

支持功耗感知调度：面向业务层面收集访存带宽，CPU 负载等数据，确保业务关键线程资源得到满足；面向平台层面，引入物理拓扑调压域感知新的维度，减少单 DIE 调频、 调压带来的调频降功耗的局限，保障在低负载下能最小化功耗。

支持对资源竞争度量及处理性能监控单元指标低负载采集：将 PSI 能力从 cgroup v2 移植到 cgroup v1，在此基础上增加在离线混部资源争抢的压力指标，以及常用压力细粒度指标。

支持 KVM TDP MMU：相较于传统的 KVM MMU，TDP MMU 提供了更高效的并发 Page Fault 处理机制，从而使得 KVM 对大型虚拟机（多 vCPU，大内存）有了更好的支持。

提供基于 memcg 的细粒度 swap 控制：实现不同业务的 swap 功能差异化配置，在保障关键业务的性能的同时，降低低优先级业务的内存资源。

新增云脉芯联 XSC 系列网卡驱动适配与支持。

新增华为自研 SPxxx 系列 RAID 卡适配与支持。

新增沐创网卡驱动适配与支持。

新增澜起科技 TSSE 驱动适配与支持：支持澜起的国密加密算法硬件卸载能力。

新增 AX99100 TPM2.0 驱动适配和支持。

## 5.2. 系统组件

### 5.2.1. bcc：

支持 0.23.0-4.p01 版本；

bcc-tools/tcpaccept: 增加对 kernels v5.6+的支持。

### 5.2.2. blktrace:

支持 1.3.0-2 版本；

提供 iowatcher，用于创建可视化图表。

### 5.2.3. CLI11:

支持 1.9.1-1 版本；

提供命令行参数解析支持。

### 5.2.4. linux-firmware:

支持 20211027-2.p03 版本；

支持 Mont-TSSE 加密算法加速器固件。

### 5.2.5. ltrace：

支持 0.7.91-31 版本；

提供系统调用跟踪支持进程监控。

### 5.2.6. pcp：

支持 5.3.7-3.p02 版本；

提供系统性能采集工具。

#### 5.2.7. mcelog：

支持 179-5.p01 版本；

支持在检测到系统 MCE 报错时，输出内存报错信息到指定端口，便于 libvirt 从该端口获取 MCE 内存报错地址。

### 5.3. 安全

#### 5.3.1. crypto-policies：

支持 20200619-3.git781bbd4.p01 版本；

提供国密签名支持。

#### 5.3.2. lkrg-kyextend：

支持 0.9.6-01.se.21 版本；

提供动态度量内核组组件。

#### 5.3.3. libkydima：

支持 1.1.0-14 版本；

提供动态度量配置及查询命令工具，及策略导出保存功能。

#### 5.3.4. pesign:

支持 115-5.p01 版本；

提供国密签名支持。

#### 5.3.5. nss：

支持 3.72.0-9.p01 版本；

提供国密签名支持。

#### 5.3.6. shim：

支持 15.6-9.p12 版本；

支持国密算法签名验签。

#### 5.3.7. grub2：

支持 2.06-30.se.01.p03 版本；

支持国密算法签名验签。

#### 5.3.8. swtpm：

支持 0.3.3-7.p01 版本；

基于 libtpms 构建的 TPM 模拟器，为 QEMU 虚拟机提供 TPM 功能。

#### 5.3.9. tpm2-tools：

支持 5.0-5.p02 版本；

TPM2.0 可信软件栈对应的工具。

#### 5.3.10. tpm2-tss：

支持 3.1.0-3.p02 版本；

TPM2.0 可信软件栈。

#### 5.3.11. trousers-tcm：

支持 0.3.15-06 版本；

TCM1.2 可信软件栈。

#### 5.3.12. trousers-tcm-tools：

支持 1.3.4-07 版本；

TCM1.2 可信软件栈对应的工具。

### 5.4. 网络

#### 5.4.1. dpdk：

支持 21.11-63.p01 版本；

支持使用 weak-modules 实现 igb_uio.ko/rte_kni.ko 对内核版本解耦。

#### 5.4.2. lwip:

支持 2.2.0-1.p14 版本；

wip 用较少量的资源消耗实现一个较为完整的 TCP/IP 协议栈。

#### 5.4.3. gazelle:

支持 1.0.2-27.p12 版本；

gazelle 是一款高性能用户态协议栈，能够大幅提高应用的网络 I/O 吞吐能力；

新增输出 gazelle 模式下指定协议包收发方向信息统计功能。

### 5.5. 虚拟化

#### 5.5.1. qemu：

支持 6.2.0-78.p18 版本：

新增支持虚拟机跨系统热迁移功能，支持原系统为 openEuler 22.03 系列以及 RHEL 8 系列系统。

#### 5.5.2. edk2：

支持 202011-13.p06 版本：

解决了 GCC 12.3.0 的编译失败问题。

#### 5.5.3. libvirt：

支持 6.2.0-59.p07 版本；

支持通过外部接口获取 MCE 内存报错信息，定位受内存错误影响的虚拟机的功能；

新增虚拟机 xml 配置文件 dirty-ring-size 配置。该配置可以控制虚拟机内存脏页产生速度计算方式和 dirty-limit 热迁移节流算法。

## 5.6. 容器

### 5.6.1. kata-containers：

支持 1.11.1-26-p03；

支持 ARM64 架构；

支持适配海光 CPU。

### 5.6.2. rubik：

支持 2.0.0-3.p08 版本；

新增内存超分、动态调频和 psi 信息采集功能；

支持海光 L3 Cache 和仿存带宽 QoS 控制能力。

## 5.7. nestos 不可变构建能力

### 5.7.1. nestos-assembler:

支持 v0.13.0.4-2.p07 版本；

提供云底座不可变操作系统构建工具；

提供构建工具容器镜像制作脚本；

提供构建工具运行脚本。

### 5.7.2. nestos-installer:

支持 0.16.0-4.p02 版本；

提供云底座不可变操作系统安装部署工具；

支持将 ign 点火文件集成到 iso 或 pxe 镜像中。

### 5.7.3. nestos-config:

支持 22.03LTS_SP3-2.p03 版本；

提供构建云底座不可变操作系统默认构建配置信息。

#### 5.7.4. butane:

支持 0.17.0-1.p01 版本；

提供部署云底座不可变操作系统用户配置校验及转换点火文件功能；

支持 nestos 1.0.0 版本变种规范。

#### 5.7.5. ignition:

支持 2.14.0-2 版本；

提供部署云底座不可变操作系统应用用户配置初始化功能。

#### 5.7.6. rpm-ostree:

支持 2022.16-1.p01 版本；

提供云底座不可变模式构建能力关键依赖组件。

#### 5.7.7. ostree:

支持 2023.5-4 版本；

提供云底座不可变模式构建能力关键依赖组件。

### 5.8. 云组件

#### 5.8.1. kubernetes：

支持 1.28，1.29 版本；

cpu-manager 中新增 S2500 架构下绑核优化算法。

### 5.9. 其他

#### 5.9.1. extuner：

支持 1.1.0-1 版本；

提供系统性能指标采集、分析、静态调优功能。

#### 5.9.2. kylin-sysassist：

支持 1.3-4 版本；

支持系统体验，检测系统 cve 漏洞及 bug；

支持检测系统服务状态、配置等；

支持日志收集，一键收集全量日志信息或部分日志信息；

支持系统监控，对进程、文件、内存、网络进行监控。

### 5.9.3. pytorch：

支持 1.11.0-2 版本；

提供了 TorchData 和 functorch 两个全新的库，增强了 DDP 静态图的功能，为用户提供了更加灵活、高效和强大的深度学习工具。

## 6. 附录 II 安全漏洞修复

CVE-2022-4065, CVE-2022-27378, CVE-2023-45803, CVE-2023-5341, CVE-2022-24050, CVE-2023-3823, CVE-2022-27452, CVE-2020-0452, CVE-2023-3824, CVE-2023-45853, CVE-2023-6693, CVE-2022-26592, CVE-2021-46668, CVE-2023-45866, CVE-2023-45231, CVE-2024-21733, CVE-2024-21626, CVE-2023-46049, CVE-2020-23804, CVE-2023-43785, CVE-2024-24259, CVE-2022-24052, CVE-2023-0664, CVE-2023-36054, CVE-2021-33391, CVE-2022-40896, CVE-2024-1441, CVE-2022-24834, CVE-2023-32700, CVE-2024-24474, CVE-2020-18651, CVE-2023-49994, CVE-2023-43804, CVE-2023-4016, CVE-2022-27376, CVE-2022-27386, CVE-2021-23210, CVE-2023-37732, CVE-2023-2861, CVE-2024-22365, CVE-2023-38471, CVE-2023-38546, CVE-2023-37327, CVE-2022-41853, CVE-2023-50447, CVE-2023-5157, CVE-2022-43357, CVE-2023-3961, CVE-2023-43788, CVE-2023-7008, CVE-2022-27385, CVE-2023-4641, CVE-2021-46310, CVE-2024-28085, CVE-2024-24577, CVE-2023-35789, CVE-2023-34454, CVE-2023-43642, CVE-2023-39325, CVE-2023-32002, CVE-2023-27043, CVE-2023-38472, CVE-2022-3479, CVE-2023-32001, CVE-2022-27387, CVE-2023-2976, CVE-2023-48795, CVE-2023-42465, CVE-2023-43115, CVE-2022-45198, CVE-2022-27447, CVE-2023-30861, CVE-2023-0330, CVE-2023-42670, CVE-2023-40217, CVE-2022-40898, CVE-2023-49992, CVE-2023-47100, CVE-2023-4504, CVE-2023-7104,

CVE-2022-27380, CVE-2023-3019, CVE-2022-24048, CVE-2023-36328, CVE-2023-4863, CVE-2023-42795, CVE-2023-38469, CVE-2022-27381, CVE-2023-45234, CVE-2023-5380, CVE-2022-27449, CVE-2022-27377, CVE-2023-1544, CVE-2023-35887, CVE-2023-4091, CVE-2022-27379, CVE-2023-45233, CVE-2023-22742, CVE-2023-37920, CVE-2024-2496, CVE-2022-27458, CVE-2023-0437, CVE-2024-24258, CVE-2022-27445, CVE-2013-4235, CVE-2022-32087, CVE-2021-46312, CVE-2023-38545, CVE-2023-51385, CVE-2024-1013, CVE-2022-27448, CVE-2023-47038, CVE-2023-6377, CVE-2023-34455, CVE-2022-40151, CVE-2023-6683, CVE-2020-18652, CVE-2022-27456, CVE-2023-40660, CVE-2023-36191, CVE-2023-5367, CVE-2022-48522, CVE-2023-42669, CVE-2022-24051, CVE-2023-6478, CVE-2020-18770, CVE-2023-43787, CVE-2024-2494, CVE-2020-0556, CVE-2023-38473, CVE-2023-5217, CVE-2022-32085, CVE-2023-49991, CVE-2022-41966, CVE-2022-43358, CVE-2023-28709, CVE-2023-47039, CVE-2023-25577, CVE-2023-46218, CVE-2023-43789, CVE-2023-38408, CVE-2023-6277, CVE-2023-31975, CVE-2023-49993, CVE-2023-49990, CVE-2023-3255, CVE-2022-27383, CVE-2023-43786, CVE-2020-21528, CVE-2024-3447, CVE-2021-25786, CVE-2022-27384, CVE-2023-45235, CVE-2024-24806, CVE-2023-4504, CVE-2023-4911, CVE-2023-29406, CVE-2023-39326, CVE-2023-45285, CVE-2023-39325, CVE-2023-39323, CVE-2023-39318, CVE-2023-39319, CVE-2023-29409, CVE-2023-22025, CVE-2024-20926, CVE-2024-20919, CVE-2024-20945, CVE-2024-20918, CVE-2024-20952, CVE-2024-20921, CVE-2023-22081, CVE-2023-44487, CVE-2022-40982, CVE-2022-38090, CVE-2023-39368, CVE-2023-23583, CVE-2023-50495, CVE-2023-29491, CVE-2023-3966, CVE-2023-5366, CVE-2024-0727, CVE-2023-3817, CVE-2023-5678, CVE-2023-40217, CVE-2023-27043