ICS 35.060
CCS L 74

中华人民共和国电子行业标准

SJ/T 11936—2024

安全可靠 服务器操作系统技术要求

Safety and reliability—Technical requirement for server operating system

2024-07-19 发布　　2024-10-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息技术标准化技术委员会（SAC/TC 28）提出并归口。

本文件起草单位：中国电子技术标准化研究院、麒麟软件有限公司、统信软件技术有限公司、华为技术有限公司、中科方德软件有限公司、龙芯中科技术股份有限公司、飞腾信息技术有限公司、无锡先进技术研究院、上海兆芯集成电路股份有限公司、海光信息技术股份有限公司、国家工业信息安全发展研究中心、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、工业和信息化部电子第五研究所、中国信息通信研究院。

本文件主要起草人：苗宗利、马承青、刘涛、孟杰、曹晓琦、董建、杨磊、张群、王剑、梁佳男、薛皓琳、郭亮、董军平、王力玉、靳国杰、王洪虎、李超、战茅、王寒冰、李雪、齐宗普、张木梁、刘屹松、胡湘华、崔巍、孙建民、苏卫强、张攀勇。

安全可靠　服务器操作系统技术要求

1　范围

本文件规定了基于Linux内核的在安全性和可靠性方面具有更高要求的服务器操作系统（以下简称“系统”）的CPU架构兼容、系统安装、系统内核、中文支持、系统管理、系统安全、服务支持、常用软硬件支持、应用开发支持、虚拟化支持、可靠性、交付与服务等要求。

本文件适用于服务器操作系统的设计、开发与应用。非Linux操作系统可参照使用。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 13000　信息技术　通用多八位编码字符集（UCS）

GB 18030　信息技术　中文编码字符集

GB/T 32915　信息安全技术　二元序列随机性检测方法

GM/T 0002　SM4分组密码算法

GM/T 0003(所有部分)　SM2椭圆曲线公钥密码算法

GM/T 0004　SM3密码杂凑算法

GM/T 0005　随机性检测规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

独立（或廉价）磁盘冗余阵列　redundant array of independent（or inexpensive） disks（RAID）

把多个硬盘（本文件所述“硬盘”包括“硬磁盘”和“固态盘”）驱动器合并成一组阵列来达到大型驱动器所无法达到的性能或冗余性，访问时一般视作一个逻辑贮存单元或驱动器。

3.2

硬　RAID hard RAID

建立在硬件基础之上，与操作系统和主机无关，管理着RAID子系统。

3.3

软　RAID soft RAID

建立在软件基础上，不需要专门的控制器设备，通过核心硬盘（块设备）代码来执行不同的RAID级别。

3.4

逻辑卷管理　logical volume manager（LVM）

建立在硬盘和分区之上的一个逻辑层，以实现动态调整硬盘分区。

3.5

交换分区　swap partion

一种Linux操作系统虚拟内存管理机制，通过在硬盘上创建系统专用缓存分区，用于存放内存中不经常访问的数据。

4 缩略语

下列缩略语适用于本文件。

ACPI：高级配置和电源接口（advanced configuration and power interface）
AI：人工智能（artificial intelligence）
API：应用编程接口（application programming interface）
ARP：地址解析协议（address resolution protocol）
CA：证书授权（certificate authority）
CD：光盘（compact disk）
CNI：容器网络接口（container network interface）
CIFS：通用网络文件系统（common internet file system）
CNVD：中国国家漏洞数据库（China national vulnerability database）
CPU：中央处理器（central processing unit）
CVE：通用漏洞披露（common vulnerabilities & exposures）
DNS：域名系统（domain name system）
EFI：可扩展固件接口（extensible firmware interface）
ESP：EFI系统分区（EFI system partition）
EXT3：第三代扩展文件系统（third extended filesystem）
EXT4：第四代扩展文件系统（fourth extended filesystem）
Fast CGI：快速通用网关接口（fast common gateway interface）
FAT32：32位文件分配表（32bit file allocation table）
FCoE：以太网光纤通道（fibre channel over ethernet）
FTP：文件传输协议（file transfer protocol）
GNU：GNU计划（GNU is not unix）
GRUB：多操作系统启动程序（grand unified bootloader）
GPT：全局唯一标识分区表（GUID partition table）
GPU：图形处理器（graphics processing unit）
HA：高可用性集群（highly available）
HTTP：超文本传输协议（hypertext transfer protocol）
HTTPS：超文本传输安全协议（hypertext transfer protocol secure）
ID：身份（identity）
IMA：完整性度量架构（integrity measurement architecture）
IMAP：互联网消息访问协议（internet message access protocol）
I/O：输入/输出（input/output）
IP：互联网协议（internet protocol）
IPSec：互联网安全协议（internet protocol security）
IPv4：互联网协议第4版（internet protocol version 4）
IPv6：互联网协议第6版（internet protocol version 6）
iSCSI：互联网小型计算机系统接口（internet small computer system interface）
KAPI：内核应用编程接口（kernel application programming Interface）
KVM：基于内核的虚拟机（kernel-based virtual machine）
LSM：内核安全模块（Linux security module）
MIB：管理信息库（management information base）

NAS：网络附属存储（network attached storage）
NFS：网络文件系统（network file system）
NoSQL：不仅仅是SQL（not only SQL）
NTFS：新技术文件系统（new technology file system）
NTP：网络时间协议（network time protocol）
NVDB：网络安全威胁和漏洞信息共享平台（national vulnerability database）
NVMe：非易失性内存主机控制器接口规范（Non-volatile memory express）
NUMA：非统一内存访问（non uniform memory access）
OCI：开放容器规范（open container initiative）
PCIe：高速串行计算机扩展总线标准（peripheral component interconnect express）
PKI：公钥基础设施（public key infrastructure）
POP3：邮局协议版本3（post office protocol - version 3）
RBAC：基于角色的访问控制（role-based access control）
RDP：远程桌面协议（remote desktop protocol）
RPC：远程过程调用（remote procedure call）
RPM：红帽软件包管理器（Redhat package manager）
SAN：存储区域网络（storage area network）
SBOM：软件物料清单（software bill of materials）
SCSI：小型计算机系统接口（small computer system interface）
SDK：软件开发工具包（software development kit）
SMB：服务器信息块（server message block）
SNMP：简单网络管理协议（simple network management protocol）
SPICE：独立计算环境简单协议（simple protocol for independent computing environment）
SQL：结构化查询语言（structured query language）
SSH：安全外壳协议（secure shell）
SSL：安全套接字协议（secure sockets layer）
TCP：传输控制协议（transmission control protocol）
UDP：用户数据报协议（user datagram protocol）
UEFI：统一的可扩展固件接口（unified extensible firmware interface）
USB：通用串行总线（universal serial bus）
UTC：世界标准时间（coordinated universal time）
VLAN：虚拟局域网（virtual local area network）
VNC：虚拟网络控制台（virtual network console）
XFS：无限（新一代）文件系统（X file system）

5 CPU 架构兼容要求

5.1 CPU 指令架构支持

系统应兼容通过安全可靠测评的 CPU，同源兼容包括但不限于下列 CPU 平台架构：

a) ARM，
b) LoongArch，
c) MIPS，
d) SW64，

e） x86。

5.2 CPU 内置功能支持

系统应支持 CPU 内置功能，满足下列要求。

a） 多核 CPU：
   1） 支持负载均衡，根据负载情况，自动调度程序运行在不同的核心上；
   2） 支持线程绑定，允许限制某个应用运行在指定核心上；
   3） 提供系统访问接口，应用通过访问接口获取运行状态和控制多核调度；
   4） 支持通过硬件指令判别临界区冲突实现自旋锁。

b） CPU 运行频率动态调节，能够根据负载情况，自动调节 CPU 的运行频率。

c） CPU 硬件虚拟化，操作系统内置支持 CPU 虚拟化指令集，以提高虚拟机的运行效率。

d） 物理多路 CPU：
   1） 支持跨路内存访问能力，允许其他路 CPU 访问本路内存；
   2） 支持负载均衡，能够根据负载情况，自动调度程序运行在不同的物理 CPU 之上；
   3） 支持 NUMA 架构，提供 NUMA 驱动编程接口，根据 ACPI 描述的 NUMA 架构内存信息进行进程调度优化，让进程运行在本 NUMA 节点之上。

e） CPU 内置安全功能：
   1） 支持 CPU 硬件密码运算与随机数生成等功能；
   2） 提供编程接口供应用程序调用。

注：仅当硬件支持时要求操作系统支持该特性。

6 系统安装要求

6.1 安装方式

系统应支持光盘、闪存盘和网络安装，满足下列要求：

a） 光盘安装，设置固件从光盘引导后，插入安装光盘，可从光驱引导并进行安装；

b） 闪存盘安装，设置固件从闪存盘引导后，插入安装盘，可从闪存盘引导并进行安装；

c） 网络安装，设置固件从网络引导后，可从网络内已配置好的安装服务器引导并进行安装；

d） 无人值守安装，通过配置文件定制安装策略，包括分区、网络模式、用户名口令、安装形态等，实现系统自动安装，无需人为干预系统安装过程。

注：操作系统安装方式需要固件提供支持，操作性与固件的约定见附录A。

6.2 安装模式

系统安装模式应满足下列要求：

a） 支持图形或文本安装模式；

b） 以图形模式安装时，若不能正常进入图形模式，应能自动切换至文本安装模式或提示用户切换至文本安装模式。

6.3 安装过程配置

系统安装过程配置应满足下列要求：

a） 安装界面文种设置，缺省为简化字方式显示；

注1：“文种设置”常被称为“语言设置”。

注2：“简化字”常被称为“简体中文”。

b） 逻辑分区配置（如 LVM），允许用户不删除数据对硬盘分区大小进行动态调整；

c) 自定义分区，允许创建、删除、修改分区，安装程序能自动检测分区设置的合规性，删除已有分区时应显式告警提示；
d) 安装组件配置，包括服务组件、开发组件、图形界面组件及虚拟化组件等；
e) 时区设置，缺省为东八区（UTC+8）；
f) 键盘布局设置，缺省为汉字键盘布局；
g) 初始用户设置，创建新用户并设置口令，可提供用户口令复杂度检查功能；
h) 计算机名设置，并提供缺省值；
i) 网络设置，缺省为关闭状态；
j) 支持通过闪存盘等方式加载硬件驱动。

6.4 系统引导

系统引导程序应满足下列要求：

a) 支持 UEFI2.0 及以上规范固件引导，计算机以 UEFI 模式启动安装时，安装程序应分配 ESP，并在 ESP 中放置启动引导文件，使系统能以 UEFI 模式引导；
b) 支持 bootloader 引导，支持 GPT；
c) 支持引导程序修复，操作系统安装媒体应提供系统引导修复功能，当已安装的系统引导被破坏时，可重建系统引导；
d) 支持默认启动级别配置，至少包含单用户、多用户字符、多用户图形三种模式；
e) 支持 GRUB 口令保护，修改 GRUB 引导参数时需进行身份鉴别；
f) 支持用户编辑模式，可修改引导参数与配置。

6.5 其它要求

系统安装程序应满足下列要求：

a) 安装程序在安装执行前应明确提示用户可能会删除已有数据，并提供退出/取消功能，当用户取消安装时，不应改变硬盘上已有数据；
b) 系统安装完成后应自动适配显示器最佳分辨率(文本模式除外)；
c) 系统安装和配置过程中，如用户自定义的某些配置可能会影响系统启动或正常使用，应予以明确提示。

7 系统内核要求

7.1 内核版本

基于Linux内核的服务器操作系统应采用6.6版内核。

7.2 进程、线程调度

系统进程、线程调度应满足下列要求：

a) 支持基于 NUMA 的亲和调度；
b) 支持 CPU 多核轮询调度；
c) 具备进程优先级动态调整能力，允许在进程运行时对优先级进行调整；
d) 区分实时进程与非实时进程，分别进行调度；
e) 支持进程运行状态检查。

7.3 内存管理

系统内存管理满足下列要求：

a) 支持的最大内存应不小于 4TB；
b) 应支持内存大页管理，允许应用申请内存大页降低页表转换，优化性能；
c) 应支持 NUMA 近节点优化；
d) 宜支持虚拟内存超分，提升内存的使用率。

7.4 存储管理

系统存储管理应满足下列要求：

a) 支持多种 RAID 实现方式，包括硬件 RAID 和软 RAID；支持多种 RAID 模式，包括 RAID0、RAID1、RAID5、RAID6、RAID10 等；
b) 支持虚拟文件系统，支持将不同功能的外部设备抽象为统一的文件操作接口，包括存储、输入输出设备；
c) 支持文件存储、检索和共享；
d) 支持对可移动外部存储的管理，包括启停、禁用、恢复等；
e) 支持使用外部独立存储设备；
f) 支持存储多路径聚合及 I/O 动态负载均衡；
g) 支持硬盘损坏或老化检测及信息收集；
h) 支持将硬盘的特定分区或文件作为虚拟扩展内存用于存放内存数据，支持虚拟内存压缩；
i) 支持 FCoE、iSCSI，支持将 Ceph 块设备视为常规存储设备挂载到某个目录并作为标准文件系统使用；
j) 支持快速块设备作为慢速块设备缓存以加速 I/O。

7.5 网络管理

系统网络管理应满足下列要求：

a) 支持网络链路故障检测、链路事件通知和链路状态查询；
b) 支持 IPv4、IPv6 协议；
c) 支持多网卡绑定；
d) 支持用户态 TCP/IP 协议栈。

7.6 文件系统

文件系统应满足下列要求：

a) 支持 XFS、EXT3、EXT4、NTFS、FAT32 等文件系统，支持相应格式分区创建、删除、格式化等；
b) 支持日志式文件系统；
c) 最大文件不小于 4TB，最大文件名长度不小于 255 字节；
d) 支持动态调整分区大小，对系统分区容量进行改变。

8 中文支持要求

系统中文支持满足下列要求：

a) 应符合 GB 18030 的要求，并与 GB/T 13000 相应部分建立映射关系；
b) 应内置中文帮助文档；
c) 宜提供中文图形操作界面。

9 系统管理要求

9.1 管理工具

系统应提供管理工具，满足下列要求。

a) 系统信息查看工具，支持查看系统版本、内核版本、内存容量、CPU 型号等信息。

b) 网络管理工具：

1) 支持多网口自动连接、网络地址（常被称为“IP 地址”）设置、DNS 设置、路由设置；

2) 支持多网卡链路聚合，模式类型应包括但不仅限于轮询、主备、802.3AD 动态链路聚合；

3) 支持网络软件桥接、支持 VLAN、策略路由配置、支持虚拟网络设备（veth）配置。

c) 日期和时间管理工具，可设置时间同步服务器地址，支持局域网和广域网的同步设置。

d) 帐户管理工具，支持帐户添加、删除、属性修改等。

e) 存储管理工具，支持硬盘分区创建、删除、查看和修改分区属性，支持 EXT、XFS、NTFS、FAT、SWAP 等多种格式。

f) SNMP 协议工具包，提供 SNMP 设备管理能力，如获取设备信息、设置设备参数、监测设备状态等。

g) 文本终端工具，支持多终端管理。

h) 服务管理工具，支持服务启动与停止，查看服务状态及日志，查询服务启动顺序及依赖关系。

i) 配置管理工具，支持简化任务配置及服务管理。

j) 监控管理工具，支持监控系统资源使用情况，包含 CPU、内存、存储 I/O、网络 I/O 等。

k) 支持启动守护进程，用户可自定义设定需要创建、删除、启动、停止、禁用、启用的守护进程，如遇异常可进行重新加载，实现应用持续运行。

9.2 维护工具

系统维护工具满足下列要求：

a) 应提供远程控制管理工具，支持 RDP、SSH、SPICE、VNC 等协议，方便用户进行文本或图形化形式的远程连接及维护；

b) 应提供文件系统检查工具，对文件系统完整性进行检测和修复；

c) 应提供内核探测工具，支持对内核及用户态程序动态追踪；

d) 应提供性能分析工具，支持对函数层面进行分析；

e) 宜提供性能测试调优工具，按系统工作特点（如计算为主、存储为主等）优化系统配置、库、软件等组件；

f) 宜提供集中管控工具，支持对区域内服务器操作系统进行集中管理维护；

g) 宜提供软件兼容性检查工具，支持依赖库、对外接口等兼容性验证测试；

h) 宜提供硬件兼容性检查工具，支持整机、板卡与操作系统的兼容性验证测试；

i) 提供操作系统跨版本兼容性分析工具，支持依赖包、内核态与用户态接口、内核参数、服务配置等兼容性分析能力。

9.3 系统授权激活

系统可提供授权激活功能，满足下列要求：

a) 支持序列号授权、批量激活服务、场地授权等方式；

b) 未激活期间，系统不得频繁提示，提示间隔宜不小于 7 天；

c) 未激活系统不得影响用户数据安全与完整性。

9.4 日志管理

系统日志管理应满足下列要求：

a) 支持对安全事件的日志记录，包括帐户增删改、成功登录、失败登录、敏感服务开启关闭、配置修改等，日志信息应详实，包括所属用户、访问时间、访问地址等；
b) 支持内核异常日志信息的记录和存储；
c) 支持内核崩溃转储机制，系统崩溃时可收集整个内存信息；
d) 支持配置远程日志功能，可将指定日志内容归档到日志服务器；
e) 支持对日志功能进行访问控制，防止未经授权的访问；
f) 提供日志管理工具，包括系统日志、内核日志、启动日志、安装日志、显示日志和安全日志等；
g) 提供系统错误问题回溯分析工具，对系统崩溃问题及错误问题进行回溯；
h) 支持日志切分、轮替、转储、同步。

9.5 功耗管理

在硬件支持情况下，系统宜提供功耗管理能力，包括功耗控制、状态监控。

10 系统安全要求

10.1 通用要求

系统一般安全要求满足下列要求：

a) 应通过安全可靠测评；
b) 应支持关闭指定服务和端口，包括但不限于关闭远程访问、共享访问等；
c) 应提供防火墙配置管理工具，支持基于协议、网络地址、端口的访问控制规则配置，规则修改后立即生效；
d) 应支持防止 ARP 欺骗攻击；
e) 应支持 GM/T 0002、GM/T 0003 和 GM/T 0004 规定的密码算法运算；
f) 应支持随机数生成，随机数质量通过 GM/T 0005 或 GB/T 32915 的符合性测试；
g) 应提供 LSM 统一访问控制安全框架；
h) 应内置国家电子认证根 CA 的根证书；
i) 宜支持系统管理员、安全管理员、审计管理员分权管理；
j) 宜支持静态文件度量（如 IMA），保障特定文件及内存中运行程序的完整性；
k) 宜在硬件支持情况下，宜支持机密计算框架，提供机密计算 SDK，能接入 1 种以上可信执行环境；
l) 宜支持内核完整性保护，保障内核不被非授权改变；
m) 宜提供内核模块加载黑名单机制；
n) 宜达到 GB/T 20272—2019 三级及以上要求；
o) 宜提供产品及其组件的 SBOM 信息，包括供应商名称、组件名称、组件版本、唯一标识符、依赖关系、作者、时间戳等。

10.2 身份鉴别

系统身份鉴别满足下列要求：

a) 用户标识应使用帐户名和帐户 ID，在操作系统的整个生存周期内用户标识具有唯一性；
b) 应支持用户口令复杂度校验及强口令管理；
c) 应支持用户口令有效期配置；

d) 应支持口令鉴别失败控制；
e) 应支持口令加密算法配置，用户口令进行加密后以不可逆的密文形式保存；
f) 应支持禁止根帐户（root）远程登录设置；
g) 宜支持电子密码钥匙等硬件身份认证鉴别登录；
h) 宜支持一次性口令设置。

10.3 自主访问控制

系统应支持自主访问控制，满足下列要求：
a) 允许客体拥有者以普通帐户决定并控制对客体的访问，并阻止非授权用户对客体的访问；普通用户缺省拥有新建、读写和删除私有目录下文件的权限；
b) 应支持细粒度的自主访问控制，将访问控制的粒度控制在单个用户，对系统中的每一个客体，应实现由客体拥有者以指定用户方式确定其对该客体的访问权限，而其他同组用户或非同组的用户和用户组对该客体的访问权则应由客体拥有者授予。

10.4 强制访问控制

系统应支持强制访问控制，满足下列要求：
a) 支持对应用程序的访问控制与资源限制，包括对文件、网络等客体的访问控制；
b) 支持应用安装控制、应用执行控制。

10.5 安全审计

系统应支持安全审计，满足下列要求：
a) 系统应能对身份鉴别的使用、自主访问控制、标记和强制访问控制策略的修改等生成审计日志；
b) 审计日志应包括事件类型、事件发生的日期、触发事件的用户、事件成功或失败等字段；
c) 支持审计日志查询和导出。

10.6 漏洞管理

系统厂商应建立漏洞管理机制，满足下列要求：
a) 漏洞编号，每个漏洞独立编号，可直接使用 NVDB、CNVD 或 CVE 编号；
b) 漏洞提醒，发现或获悉漏洞信息时，应通过系统推送、电子邮件或企业网站等方式通知用户；
c) 漏洞修复，对已发现的安全漏洞通过补丁等方式对系统漏洞进行修复；
d) 漏洞列表，提供每个版本已修复的漏洞列表，提供命令或网页等方式方便用户查询漏洞及其修复情况。

10.7 热补丁

系统厂商应建立内核热补丁机制，在内核不停止服务下对内核进行修复，并满足下列要求：
a) 对内核热补丁进行编号，每个热补丁拥有独立编号；
b) 支持增量修复以及回滚机制；
c) 提供热补丁合法性和一致性校验功能；
d) 提供热补丁管理机制和工具，功能至少覆盖补丁查询、安装、移除；
e) 提供热补丁升级和回滚系统日志，便于查询或回溯。

11 服务支持要求

系统服务支持应满足下列要求。

a) 支持 TCP/UDP。
b) 支持基于 NFS、SMB、FTP、CIFS 等协议的数据网络共享服务。
c) 支持基于 HTTP、HTTPS、FastCGI 等协议 WEB 服务。
d) 支持基于 IPSec 和 SSL 协议的隧道加密传输服务。
e) 支持基于 PKI 体系的数字证书服务。
f) 支持基于 RBAC 机制的访问控制服务。
g) 支持基于 NTP 协议网络时间同步服务。
h) 支持 RPC、rsync、SSH 等远程服务。
i) 支持基于 SMTP、POP3、IMAP 等的邮件服务。
j) 支持基于轻量级目录访问协议的统一身份鉴别服务。
k) 支持块、文件、对象等类型的数据存储服务。
l) 支持 SQL、NoSQL 等类型的数据库。
m) 支持多种传输速率和存储协议的 SAN 和 NAS 存储。
n) 支持基于同步、异步请求处理机制的分布式服务。
o) 提供对集群的支持：
   1) 支持分布式集群、高可用集群部署方式；
   2) 支持多种集群配置模式，包括主主模式、主备模式、N+1 模式和 N+M 模式；
   3) 支持资源及节点故障检测；
   4) 支持虚拟路由冗余协议、分布式协议等通信方式。
p) 提供对集群四层、七层、链路负载均衡的支持：
   1) 四层负载均衡支持轮询调度、加权轮询调度、最小连接调度算法；
   2) 七层负载均衡支持轮询调度、加权轮询调度、源地址 hash 调度算法；
   3) 链路负载均衡支持多链路入站负载均衡、出站负载均衡、链路聚合功能。

12 常用软硬件支持要求

12.1 开源组件

系统可通过安装镜像内置、软件仓库或附加光盘等方式提供开源组件，系统厂商应对提供的开源组件进行签名认证，确保组件的安全性、稳定性、可靠性。宜提供的开源组件包括：

a) 开源数据库；
b) 开源中间件；
c) 单机虚拟化管理软件；
d) 容器虚拟化软件；
e) 容器管理工具；
f) 分布式存储软件；
g) 云计算管理平台软件；
h) AI 计算框架。

12.2 软件兼容

系统厂商建立软件兼容性测试体系，满足下列要求。

a) 应发布软件兼容性测试流程。
b) 应发布软件兼容性测试指标、分级规则、评价准则。
c) 应提供软件兼容性测试工具。

d) 宜提供在线测试验证环境。
e) 应通过企业网站等实时发布通过兼容性测试的产品列表。
f) 发布兼容性测试结果时，宜提供兼容性测试报告，报告应给出测试对象、版本/型号（含配置）、测试环境、测试工具、测试项及结果、测试结论、测试时间、测试人员、审核人员等。
g) 软件兼容性测试类别应包括：
   1) 集群软件；
   2) 虚拟化云平台；
   3) 容器云；
   4) 存储软件；
   5) 数据库管理系统；
   6) 中间件；
   7) 运维平台；
   8) 备份恢复软件；
   9) 大数据平台；
   10) 终端防护及杀毒；
   11) 网络防护；
   12) 身份鉴别。
h) 软件兼容性测试类别宜包括 AI SDK。

12.3 硬件兼容

系统厂商建立硬件兼容性测试体系，满足下列要求。
a) 应发布硬件兼容性测试流程。
b) 应发布硬件兼容性测试指标、分级规则、评价准则。
c) 应提供硬件兼容性测试工具。
d) 宜提供在线测试验证环境。
e) 应通过企业网站等实时发布通过兼容性测试的产品列表。
f) 发布兼容性测试结果时，宜提供兼容性测试报告，报告应给出测试对象、版本/型号（含配置）、测试环境、测试工具、测试项及结果、测试结论、测试时间、测试人员、审核人员等。
g) 硬件兼容性测试类别应包括：
   1) 服务器整机（含固件）；
   2) AI 服务器；
   3) 存储；
   4) 关键部件，包括 HBA 卡、RAID 卡、网卡、光纤卡、AI 加速卡、GPU、NPU 等。

13 应用开发支持要求

13.1 基础组件兼容

系统基础组件兼容应满足下列要求：
a) 系统基础运行库或开发环境应向后（向下）兼容，即系统版本升级后，应能兼容上一版本所运行的软件与设备；
b) 系统主版本兼容维护时间自发布之日起不低于 5 年，包括但不限于安全修复、功能升级、新硬件支持等；

c） 支持以增量升级包的方式实现版本更新。

13.2 运行环境

系统应提供满足要求的文件系统层次结构、运行库、命令，具体要求由操作系统厂商给出。

13.3 开发环境与编译开发工具

系统应通过内置、软件仓库或附加光盘等方式，提供下列开发库和工具。

a） 开发工具环境：
   1） Qt 开发工具环境；
   2） Eclipse 开发工具环境；
   3） VSCode 开发工具环境。

b） 开发运行库：
   1） GNU C 开发运行库，2.38；
   2） GNU C++开发运行库，12.3；
   3） LLVM libc++开发运行库，17；
   4） Java 开发运行库，8 和 17；
   5） Qt 开发运行库；
   6） Gtk+开发运行库；
   7） Cairo 开发运行库；
   8） OpenGL 开发运行库；
   9） Perl 开发运行库；
   10） Python 开发运行库；
   11） Ruby 开发运行库；
   12） Rust 开发运行库；
   13） Golang 开发运行库；
   14） JS 开发运行库；
   15） libvirt 开发运行库，9.10；
   16） docker 开发运行库，24。

c） 编译开发工具：
   1） GCC，12.3；
   2） G++；
   3） LLVM，17；
   4） Binutils，2.41；
   5） GDB；
   6） Make；
   7） CMake。

d） 文本编辑工具：
   1） Emacs；
   2） Vim。

e） 宜提供构建工具，将源代码转换为可执行程序，功能包括初始化环境、依赖管理、编译、打包，支持 C、C++、Python 等语言。

注：本文件仅对与CPU密切相关的工具及运行库版本做出要求，鼓励操作系统厂商就其他工具及运行库版本选型达成一致。

13.4 软件包管理

系统应提供软件包管理工具，满足下列要求：

a) 支持查询软件包描述和包含文件，以及软件包依赖；
b) 支持在安装时自动提示并下载安装缺失的依赖软件包。

13.5 开发文档

系统应内置或通过企业网站、产品社区等提供中文开发文档，包括：

a) 软件开发参考文档与开发实例；
b) 驱动开发参考文档与开发实例；
c) 应用移植开发文档与开发实例；
d) API 文档与实例。

14 虚拟化支持要求

14.1 内核虚拟化

系统支持内核虚拟化技术，满足下列要求：

a) 应支持 KVM 虚拟化；
b) 应支持在 KVM 虚拟机上安装部署操作系统；
c) 应支持虚拟机启、停等管理操作；
d) 应支持对虚拟机硬盘做快照并从快照恢复；
e) 应兼容 QEMU、libvirt 标准接口；
f) 应支持 UEFI 方式启动；
g) 应支持虚拟时钟；
h) 应支持虚拟鼠标、键盘、显卡、硬盘、CDROM、串口 pty/pipe/file 等设备；
i) 应支持 VirtIO 协议下的虚拟设备，包括串口、blk 驱动硬盘、SCSI 驱动硬盘、不同后端控制器类型的 VirtIO 网卡(包括内核态、用户态、QEMU)、GPU、vsock 设备等；
j) 在硬件支持情况下，应支持硬盘和网卡选择类型 VFIO 设备；
k) 应支持虚拟机 CPU、内存、网卡、硬盘等离线调整；
l) 应支持虚拟机网卡、硬盘、USB 设备热插拔；
m) 在硬件支持情况下，应支持 PCI/PCIe 设备直通；
n) 应支持虚拟机热迁移和加密传输；
o) 应支持虚拟机远程访问；
p) 应支持虚拟机 CPU 和 I/O 线程绑定；
q) 应提供虚拟机对主机的访问和控制；
r) 虚拟机应拥有独立的物理资源，且各个虚拟机之间应严格隔离；
s) 应支持大页内存运行虚拟机；
t) 在硬件支持情况下，应支持三种 CPU 模拟模式，包括直通、宿主模型、自定义；
u) 应支持虚拟机资源调配控制，包括 NUMA、CPU、内存、I/O、网卡；
v) 应支持 CPU 拓扑模拟和透传；
w) 宜支持 AI 部件虚拟化。

14.2 容器虚拟化

14.2.1 基本要求

系统应支持容器虚拟化技术，满足下列要求：

a) 支持 OCI；
b) 支持进程命名空间隔离技术包括不限于 mnt、pid、ipc、uts、user、network 等；
c) 支持在同 CPU 指令架构下的不同规格硬件上无缝分发，保障运行兼容性；
d) 支持沙箱扩展；
e) 支持面向容器的独立逻辑文件管理，具备在容器创建时指定专用根文件夹，容器内进程文件访问重定向等功能；
f) 支持日志查询功能；
g) 支持通过控制终端对容器内主进程的标准输入输出对接交互；
h) 支持通过控制终端对容器内新建进程的标准输入输出对接交互；
i) 支持容器存储卷管理（新增、删除、卷容量配置、自动回收）、卷共享；
j) 支持面向容器的网络设备资源分配和使用；
k) 支持 CNI；
l) 支持容器获取物理节点资源信息。

14.2.2 镜像和存储管理

系统容器镜像和存储管理应满足下列要求：

a) 支持容器镜像导入、导出；
b) 支持容器镜像分层保存、导入。

14.2.3 资源隔离和调配

系统容器资源隔离和调配应满足下列要求：

a) 支持容器资源在线调整，包括 CPU 资源、内存资源、I/O 资源等；
b) 支持文件配额分配、存储带宽资源使用量监控等机制，实现容器级 I/O 控制能力；
c) 支持面向容器的网络带宽调度策略，实现容器级网络带宽分配、使用量监控等机制；
d) 支持面向容器的存储空间使用监控、分配机制；
e) 支持容器 CPU 核独占；
f) 支持面向容器的 CPU 时间片资源按需划分机制；
g) 支持面向容器的内存分配和回收机制，实现内存使用量跟踪和管理；
h) 支持同一集群在线、离线业务混合部署；
i) 支持对容器的编排、负载均衡、调度等能力；
j) 支持根据容器在线与离线混合部署状态进行资源优先调度，提高计算机资源利用率。

15 可靠性要求

系统可靠性满足下列要求。

a) 在 CPU、内存或 I/O 占用率超过 80%时连续运行 168h 应无故障。
b) 应提供备份还原功能，支持生成系统状态快照及恢复系统状态。
c) 在硬件支持情况下，应支持 DDR3、DDR4 等内存上的 ECC 查错、纠错。
d) 支持热插拔：
   1) 宜支持 CPU 热插拔，可通过命令或接口上线、下线 CPU；
   2) 宜支持内存热插拔，可通过命令或接口上线、下线内存；
   3) 应支持硬盘热插拔。
e) 应提供系统升级功能，满足下列要求：

1） 升级时应给出升级的具体内容，包括升级的软件或组件名称、修复的 BUG、安全漏洞列表等，可通过网络链接等方式提供更详细的信息；
2） 若升级时系统常见 API、KAPI 发生变化并影响软硬件兼容性，应给出具体接口变化信息；
3） 提供系统增量升级功能，对系统组件、安全补丁等升级；
4） 支持在线升级和离线升级；
5） 升级不得修改破坏用户数据；
6） 升级不得影响原有软硬件兼容性，如有影响应显式的提示告知用户；
7） 提供升级回退机制，恢复系统原有状态；
8） 如升级为不可回退，则系统升级前以显式的提示告知用户。

f） 应提供故障管理框架，满足下列要求：
1） 支持硬件主动检测，具备发现错误的能力；
2） 支持故障数据采集，按照预制规则进行紧急处理；
3） 支持故障诊断，提供解决建议，进行系统状态恢复；
4） 提供用户接口，可与外部同类型系统或第三方框架互联，进行故障信息上报。

16 交付与服务要求

16.1 交付方式

系统应提供光盘、闪存盘、镜像文件（下载）等交付方式。操作系统的性能宜由企业标准给出，包括：

a） 进程调度；
b） 网络通信；
c） 内存访问；
d） 文件系统；
e） 应用场景。

16.2 服务周期

系统服务周期应满足下列要求：

a） 产品自发布之日起至产品停止功能升级（包含不限于新特性、新硬件支持、问题修复、安全补丁等）之日止不少于 5 年；
b） 产品停止功能升级之日起至产品停止功能维护（主要包括问题修复、安全补丁等）之日止不少于 5 年；
c） 产品功能维护停止之日起至产品停止安全维护（包括中高风险漏洞修复）之日止不少于 3 年；
d） 自销售之日起，产品售后服务周期不少于 8 年。

16.3 服务保障

系统服务保障满足下列要求：

a） 应提供多种形式中文支持服务，包含电话、电子邮件、公众号、远程连接等；
b） 应提供工作日每日不少于 8h（宜覆盖一般工作时间，具体时间由企业标准给出）技术支持服务，服务周期内最快 0.5h 内响应；
c） 满足“同城 4h、异地 12h”服务响应要求，2 个工作日解决问题，对于未能解决的问题和故障提供可行的升级或替代方案；
d） 应建立全国技术服务体系和服务团队，符合专业服务体系标准要求，可提供原厂中文服务；

e） 发生非人为因素故障，在7日内免费对产品进行补充或更换；

f） 服务期内应支持版本免费更换；

注：更换后不延长服务周期。

g） 可提供现场安装调试服务及所需的工具和设备；

h） 交付产品时应提供配套的技术资料，包括但不限于系统说明文件、用户手册（安装、操作、维护、故障排除）、培训材料、培训视频等；

i） 针对关键客户宜提供代码级定制优化服务；

j） 宜支持通过企业网站、产品社区等进行在线问题反馈，反馈问题应在2个工作日内得到响应。

附 录 A
（资料性）
固件约定

固件宜支持下列功能：

a） 支持光盘、闪存盘、网络、硬盘引导；
b） 支持 FAT32、ISO 9660 文件系统；
c） 支持 CPU 虚拟化开关配置；
d） 符合 UEFI 2.0 及以上兼容版；
e） 内核引导支持 GRUB 2.0 及以上兼容版。

参 考 文 献

[1] GB/T 20008 信息安全技术 操作系统安全评估准则
[2] GB/T 5271 信息技术词汇
[3] GB/T 20272—2019 信息安全技术 操作系统安全技术要求


MINISTRY OF INDUSTRY AND INFORMATION TECHNOLOGY
SJ
STANDARDS

中华人民共和国
电子行业标准

安全可靠 服务器操作系统技术要求

SJ/T 11936—2024

*

中国电子技术标准化研究院 编制
中国电子技术标准化研究院 发行

电话：(010) 64102612 传真：(010) 64102617
地址：北京市安定门东大街1号
邮编：100007
网址：www.cesi.cn

*

开本：880×1230 1/16 印张：1 3/4 字数：12千字

2024年7月第一版 2024年7月第一次印刷
印数：200册 定价：70.00元