操作系统 通用技术要求

1 范围

本文件规定了操作系统通用技术要求，包括服务器操作系统规范和桌面端操作系统规范两部分。

本文件适用于国家信息技术应用创新工程建设相关服务器操作系统和桌面端操作系统的研制、测评、采购选型和使用维护。

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 2312 信息交换用汉字编码字符集 基本集

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 18031 信息技术 数字键盘汉字输入通用要求

GB/T 19246 信息技术 通用键盘汉字输入通用要求

GB/T 18790 联机手写汉字识别系统技术要求与测试规程

GB/T 21023 中文语音识别系统通用技术规范

GB/T 15732 汉字键盘输入用通用词语集

ISO/IEC 9945 信息技术 可移植操作系统接口（POSIX）基本规范（Information technology-Portable operating system interface (POSIX) Base specification）

3 术语和定义

下列术语和定义适用于本文件。

3.1

控制面板 control panel

是用户查看并操作系统设置的工具，允许用户添加/删除软件，控制用户帐户，更改辅助功能选项等。

3.2

资源管理器 resource manager

是管理系统资源的工具， 能够显示计算机上的文件和文件夹，通过操作资源管理器来对系统文件和文件夹进行操作。

3.3

待机 standby

保存计算机当前工作状态，关闭除内存外所有设备/组件供电，再次唤醒时系统即可恢复到待机前工作状态。

3.4

休眠 hibernate

保存计算机当前工作状态，关闭主机内所有设备/组件的供电，再次唤醒时系统即可恢复到休眠前工作状态。

3.5

注销 logout

结束当前用户任务进程， 退出当前用户运行环境并返回登录界面。

4 缩略语

下列缩略语适用于本文件。

CPU：中央处理器（Central Processing Unit）

DNS：域名系统（Domain Name System）

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）

FAT：文件配置表（File Allocation Table）

HTML：超文本标记语言（HyperText Markup Language）

IP：互联网协议（Internet Protocol）

MPEG：动态图像专家组（Moving Picture Experts Group）

NTFS：新技术文件系统（New Technology File System）

TLS：传输层安全（The Transport Layer Security）

USB：通用串行总线（Universal Serial Bus）

vCPU：虚拟处理器（visual CPU）

5 服务器操作系统规范

5.1 基本功能要求

5.1.1 任务管理

5.1.1.1 任务操作

任务操作功能应包括：

a） 获取任务描述符、任务域数据和任务标识符；

b） 对任务进行创建、终止和状态查询。

5.1.1.2 任务调度

任务调度功能应包括：

a） 支持对设定任务优先级， 优先级可动态调整， 并支持将任务绑定到指定处理器（核）上；

b） 支持实时任务，系统中的实时任务应优先于所有非实时任务，系统应支持实时任务之间采用轮转、先进先出的调度策略。

5.1.1.3 任务间通讯

系统应支持多种任务间通讯方式，包括信号、共享存储器、管道、信号量和消息队列， 语义应遵循ISO/IEC 9945的要求。

5.1.1.4 内核同步机制

系统应提供多种内核同步机制， 包括CPU独立变量、原子操作、内存栅栏、信号量、自旋锁、读拷贝更新（RCU）。

5.1.1.5 中断和异常处理要求

系统的中断和异常处理功能应包括：

a) 提供基于软硬件原因的任务异步中断；

b) 支持实时时钟和定时器；

c) 提供符合 ISO/IEC 9945 的异常处理流程。

5.1.2 内存管理

系统的内存管理功能应包括：

a) 提供页式虚拟内存机制；

b) 具备内存分配、释放、延展功能；

c) 支持物理内存访问， 支持物理地址连续的内存分配；

d) 支持交换分区， 可缓存物理内存以外的虚存数据；

e) 提供共享内存机制， 提供共享内存的挂接和释放；

f) 提供大页支持功能；

g) 提供内存保护机制。

5.1.3 文件系统

文件系统要求应包括；

a) 系统应具备下列文件系统管理功能：

1) 提供对 Ext2、Ext3、Ext4、FAT、NTFS 格式的支持；

2) 支持以文件节点为数据存储和访问单位的虚拟文件系统；

3) 支持分区、目录、文件三级结构；

4) 具备日志功能， 支持查看系统日志文件， 支持对系统日志的日志类型、内容格式、文件大小、保存周期和存储路径的设置，对自定义日志文件的清理和查找；

5) 支持基于页的高速缓；

6) 支持文件系统的挂载、卸载；

7） 提供文件系统一致性检查及错误修复功能。

b） 系统应具备下列卷管理功能：

1） 增加新的物理卷到卷组；

2） 支持逻辑卷容量的动态调整；

3） 支持逻辑卷、卷组、物理卷的动态删除。

c） 系统应具备下列操作功能：

1） 目录操作功能， 包括浏览、新建、删除、复制、移动、重命名、权限设置等；

2) 文件操作功能， 包括读、写、重读、重写、追加写、定位、读文件属性、文件操作属性设置等；

3) 文件管理功能， 包括文件的新建、删除、复制、移动、重命名、权限设置、排序、搜索等功能；

4) 文件链接功能， 包括硬链接和符号链接；

5) 介质操作功能， 包括对光盘、USB 闪存盘、移动硬盘等存储介质的自动识别并挂载功能，对存储介质中的文件和文件夹进行读取、修改和删除的功能，提供卸载存储介质的功能；

6) 已删除文件操作功能，包括存储已删除的文件的功能；对已删除的文件进行恢复和彻底删除的功能； 全部彻底删除已删除文件的功能； 全部恢复已删除文件的功能。

5.1.4 字符集支持

字符集应：

a) 应支持 GB/T 2312 基本集；

b) 应至少应符合 GB 18030 的强制部分， 并应与 GB/T 13000 建立映射关系；

c) 支持 BIG5、UTF8 编码格式的中西文字符；

d) 支持其他有关少数民族文字编码字符集。

5.1.5 中文支持

5.1.5.1 支持中文输入

系统应提供：

a) 提供符合 GB/T 19246 和 GB/T 18031 的键盘输入软件；

b) 提供符合 GB/T 18790 的手写输入法软件；

c) 提供符合 GB/T 21023 的语音输入软件。

5.1.5.2 支持中文字词库

系统应提供至少四种基本的输出字体： 宋体、仿宋、黑体、楷体；提供各种字体的字型变换方式，至少包括常规、倾斜、加粗、倾斜并加粗，其中默认字型为常规字型。

应优先支持GB/T 15732规定的词库导入，在GB/T 15732基础上扩充的词汇应符合我国语言文字规范或习惯， 并应有该词汇来源的依据。

5.1.5.3 支持符合中文习惯的货币/日期/时间格式

系统应提供的格式包括：

a) 货币格式为￥123，456，789.00；

b) 日期格式为 YYYY 年 MM 月 DD 日；

c) 星期格式为星期一、星期二、星期三、星期四、星期五、星期六、星期日；
d) 时间显示格式为 HH：MM：SS。

5.1.5.4 支持中文的打印输出

系统应支持打印输出中文字体和字型。

5.2 图形用户界面

5.2.1 桌面

系统如提供图形用户界面，应提供左键弹出菜单作为系统应用访问集中入口，至少包括以下类别：

a) 用于鼠标点击访问的“计算机”、“主文件夹”和“回收站”图标，其中“计算机”用于文件系统及网络的顶层访问， “主文件夹”用于访问登录用户的“主目录”，“回收站”用于访问被删除而缓存在此的文件及目录；

b) 创建桌面上的应用快捷方式，通过点击该快捷方式可启动相应的应用程序；

c) 右键弹出菜单， 菜单内容与右键选中对象属性有关。

5.2.2 开始菜单

系统如提供图形用户界面，应提供左键弹出菜单作为系统应用访问集中入口，应至少包括以下类别：

a) 应用程序入口，包括系统缺省安装的应用程序，以及由用户安装的附加应用程序的访问入口；

b) 系统环境入口，包括系统资源、控制面板、最近访问历史、文件搜索、屏幕锁定、用户注销、系统关机功能的访问入口；

c) 退出系统入口， 包括注销、重启、关机、待机、休眠、切换用户选项。

5.2.3 系统面板

系统如提供图形用户界面，应提供常驻桌面的系统信息展示区，至少能够显示以下内容：

a) 当前输入法的状态；

b) 当前系统时间；

c) 当前网络连接状态。

5.2.4 快速启动栏

系统如提供图形用户界面，应提供常驻桌面的应用程序快捷方式存放区域，缺省至少提供“显示桌快捷方式， 点击时可将所有当前打开的应用程序窗口最小化。

5.2.5 工作区

系统如提供图形用户界面，应提供常驻桌面的区域，显示当前各个应用程序窗口状态实时分布状态的投影，如果配置有多个工作区，则每个工作区对应一个独立的桌面环境（应用程序窗口不重登），可通过点击在多个工作区间切换。

5.2.6 任务栏

系统如提供图形用户界面，应提供常驻桌面的区域，显示当前各个应用程序窗口的主图标，当鼠标移至图标上时应显示该应用程序的标题， 可通过点击将鼠标、键盘焦点切换到相应窗口。

5.2.7 启动与登录

系统如提供图形用户界面，应提供启动与登录功能，包括：

a) 系统应提供图形化的启动界面和关机界面，启动时显示进度；在图形界面启动和关闭操作系统过程中，系统应能够通过快捷键在字符模式和图形模式间切换；

b) 系统应支持用户通过认证才允许登录系统；

c) 系统登录界面应提供关机与重启计算机功能。

5.3 系统服务管理

5.3.1 命令行工具

应提供命令行工具。

5.3.2 用户管理

用户管理应包括：

a) 支持用户和用户组管理；

b) 支持用户密码设置；

c) 支持用户权限设置；

d) 支持用户密码修改。

5.3.3 网络管理

网络管理应包括：

a) 支持 TCP、UDP、IP（IPv4、IPv6）、 ICMP、ARP、PPPoE、SLIP、PLIP 等网络基本协议；

b) 支持 HTTP、FTP、DNS、NFS、SMTP、NTP、DHCP、SSH、POP3、SOAP、SSL、SNMP 等应用层网络协议；

c) 支持 DNS 设置；

d) 支持 IPv4/IPv6 地址配置；

e) 支持自动获取 IP 地址；

f) 支持网关设置；

g) 支持代理设置等。

5.3.4 系统资源管理

系统应提供下列管理功能：

a) 资源监视功能，对系统的进程、资源（CPU、内存、网络 I/O）、文件系统进行查看，进程信息应至少包括进程名、用户、所占 CPU、进程 ID、所占内存和优先级，资源信息应至少包括 CPU、内存（含物理内存和交换分区）、网络接收和发送的使用情况，文件系统信息应至少包括设备路径、挂载目录、文件系统格式、大小、已用空间和可用空间；

b) 磁盘分区管理功能，可以对磁盘分区进行创建、删除、复制、粘贴、检查、标签更改操作，支持显示硬盘信息，至少包括型号、大小、路径、分区表，提供磁盘容量监控，在磁盘容量限额不足时应显示告警；

c) 软件包分组管理功能，能够实现包的查找、安装、外载功能；

d) 系统服务状态浏览、服务启停及系统服务自动启动配置功能。

5.3.5 时间日期管理

时间日期管理应包括：

a) 支持系统日期、时间设置；

b) 支持设置时区；

c) 支持设置网络时钟同步。

5.3.6 防火墙管理

防火墙管理应包括：

a） 支持开启或关闭防火墙；

b） 支持添加防火墙规则，应至少包括名称、访问策略、协议和端口；

c） 支持不同的访问策略，包括允许、拒绝和限制（部分 IP 允许，部分 IP 拒绝）；

d） 支持显示系统监听报告， 应至少包括访问协议、端口、地址和应用程序；

e） 支持日志记录， 应至少包括系统时间和操作记录；

f） 支持配置文件管理， 支持新建、导出和导入配置文件。

5.3.7 功耗管理

系统应支持对CPU、内存、外存、显示器进行电源管理， 应支持基于CPU体系结构相关的电源管理协议和设备电源控制能力进行能耗管理。

5.4 系统的安全性

5.4.1 身份鉴别

系统应提供下列身份鉴别功能：

a） 操作系统用户标识使用用户名和用户标识，并在操作系统的整个生存周期实现用户标识的唯一性；

b） 支持强口令管理，支持用户密码复杂度配置；

c） 支持用户密码有效期配置；

d） 支持口令认证失败控制；

e） 支持口令加密算法配置。

5.4.2 自主访问控制

系统应提供自主访问控制功能：

a） 允许命名用户以用户的身份规定并控制对客体的访问，并阻止非授权用户对客体的访问；普通用户默认拥有新建、读写和删除私有目录下文件的权限；

b） 应有更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，都应能够实现由客体的创建者以用户指定方式确定其对该客体的访问权限， 而别的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创建者用户授予。

5.4.3 强制访问控制

系统应提供强制访问控制功能：

a） 提供管理员分权机制，实现系统管理员、安全管理员、审计管理员三员管理；

b） 支持主体（包括用户与进程）与程序绑定的访问控制；

c） 支持进程的资源访问限制，资源包括文件系统、网络 IP、网络端口等客体。

5.4.4 私有数据保护

系统应提供用户私有数据保护机制：

a） 支持用户对重要私有数据进行保护， 禁止其他任何用户进行访问；

b） 用户可以将私有数据共享给其他用户，除了用户自己和共享用户外，所有未授权用户（包括管理员权限的用户）都不能访问私有数据；

c） 通过 sudo 或者 su 等提权或切换到本 UID 的用户， 不能访问私有数据。

5.4.5 安全管理工具

应提供系统安全管理工具，文持对系统进行安全功能配置。

5.4.6 国密算法

应支持国密SM2、SM3、SM4算法， 支持对用户登录口令的国密加解密。

5.4.7 运行管控

提供以下程序执行管控功能：

a） 应用程序的白名单配置管理；

b） 应用程序的完整性检查， 禁止被篡改的程序执行；

c） 应用程序来源标记检查， 只有合法安装的软件才可以执行，并能够主动禁止包括网络下载、移动存储拷贝等在内的非合法安装的软件执行；

d） 内核模块的加载控制，确保通过授权的内核模块才允许加载。

5.4.8 关键文件保护

应提供对关键文件的保护机制， 受保护的文件不能被篡改和删除。

5.5 系统的扩展性

5.5.1 虚拟机

系统应提供下列虚拟机支持能力：

a） 支持 CPU 硬件虚拟化技术；

b） 系统中运行的单虚拟机可支持 8 个以上 vCPU，32G 以上内存， 2 个以上网卡；

c） 虚拟机监控器应具有应用隔离能力；

d） 虚拟机监控器应具备动态迁移能力。

5.5.2 容器

系统应提供下列容器支持能力：

a） 支持容器的创建、销毁、运行、停止、重启、信息查看操作；

b） 支持 vCPU、内存、硬盘等资源的配置；

c） 支持镜像的构建、上传、下载、恢复操作；

d） 支持私有容器镜像仓库。

5.5.3 集群

系统应具备以下集群功能：

a) 支持被安装节点以 USB 闪存盘、光盘、网络方式启动安装；

b) 支持 MPI、MPI/OpenMP 混合等并行计算模式， 支持大规模的系统监控和作业管理；

c) 提供集群系统安装镜像定制功能，用户可以根据自己的需求， 定制生成安装镜像。

5.6 高可用的支持