方德高可信服务器操作系统 V4.0-G320

产品白皮书

地址：北京市海淀区知春路 113 号银网中心 A 座 9 层

电话：400-118-5115

技术支持邮箱：os_support@nfschina.com

官方网站：http://www.nfschina.com

——微信公众号——　　——产品及服务——

目录

1 引言 4
1.1 标识 4
1.2 文档概述 4
2 产品介绍 4
2.1 产品简介 4
2.2 产品优势 6
2.3 核心技术 7
2.4 产品主要功能 8
2.5 产品技术指标 23
2.6 应用领域 24
3 解决方案 25
3.1 高可用集群 25
3.2 负载均衡 26
3.3 安全邮件 27
3.4 安全接管 29
3.5 系统迁移 29
4 典型应用服务器 30
4.1 Web 服务器 31
4.2 邮件服务器 31
4.3 打印服务器 31
4.4 域名解析服务器 31
4.5 FTP 服务器 31
4.6 代理服务器 31
4.7 SSH 服务器 31
4.8 DHCP 服务器 31
4.9 NFS 服务器 31
4.10 数据库服务器 32
5 生态适配 32
6 服务与支持 33
6.1 服务体系 33

6.2 服务周期 34
6.3 服务内容 34
6.4 服务网络 35

1 引言

1.1 标识

标识号：NFSChina Server V4.0-G320

产品名称：方德高可信服务器操作系统 V4.0-G320

版本号：V4.0-G320

1.2 文档概述

本文档说明了方德高可信服务器操作系统 V4.0-G320（以下简称“方德高可信服务器操作系统 V4.0”）的技术功能和服务支撑。

2 产品介绍

2.1 产品简介

方德高可信服务器操作系统 V4.0 集成多重安全增强机制，提供高可信支持，为企业级用户提供稳定、高效的运行环境支撑，满足系统安全性、稳定性、可靠性等要求，全面支持海光、兆芯、飞腾、鲲鹏、龙芯、申威等国产处理器平台和 Intel、AMD 等国际主流处理器平台。

方德高可信服务器操作系统内核以 Linux 内核为基础，提供包括 CPU 架构支持、驱动、进程管理、文件系统、内存管理、进程通信管理、安全管理、网络管理等各方面操作系统核心功能。方德高可信服务器操作系统内核层研发重点是系统安全加固，包含强制访问控制、系统完整性保护、系统关键模块保护等，并提供对应的服务层或应用层模块支持。此外，进行了系统性能调优，国产 CPU 架构适配及硬件部件适配，包括 RAID 卡、HBA 卡、网卡、显卡、硬盘、USB 等硬件设备的适配支持。

方德高可信服务器操作系统服务层主要包括基础运行库、开发库、图形库、网络库、安全库、多媒体库、国际化支持等。基础库和基础服务对应用程序运行环境提供基本方法的实现支持，基础库对应不同硬件平台提供不同版本，尽可能保持同一套源码。基础桌面环境包含服务器桌面等基本应用，是提供用户交互操作的关键模块。

方德高可信服务器操作系统集成了一系列关键应用，基础应用包括浏览器、输入法、文档编译器、文档查看器、归档管理器等。系统管理工具包括系统监视器、磁盘分区工具、虚拟系统管理器、系统升级工具、磁盘挂载工具等；扩展应用包括运方德维管理系统、方德系统迁移平台、日志分析管理工具、方德设备管理器、方德字体管

理器和安全防护软件（方德杀毒）等。系统集成开发环境包含 C/C++ 开发环境、Python 开发环境、Java 开发环境等，支持从软件仓库下载安装。

方德高可信服务器操作系统整体结构图如图 2-1 所示。

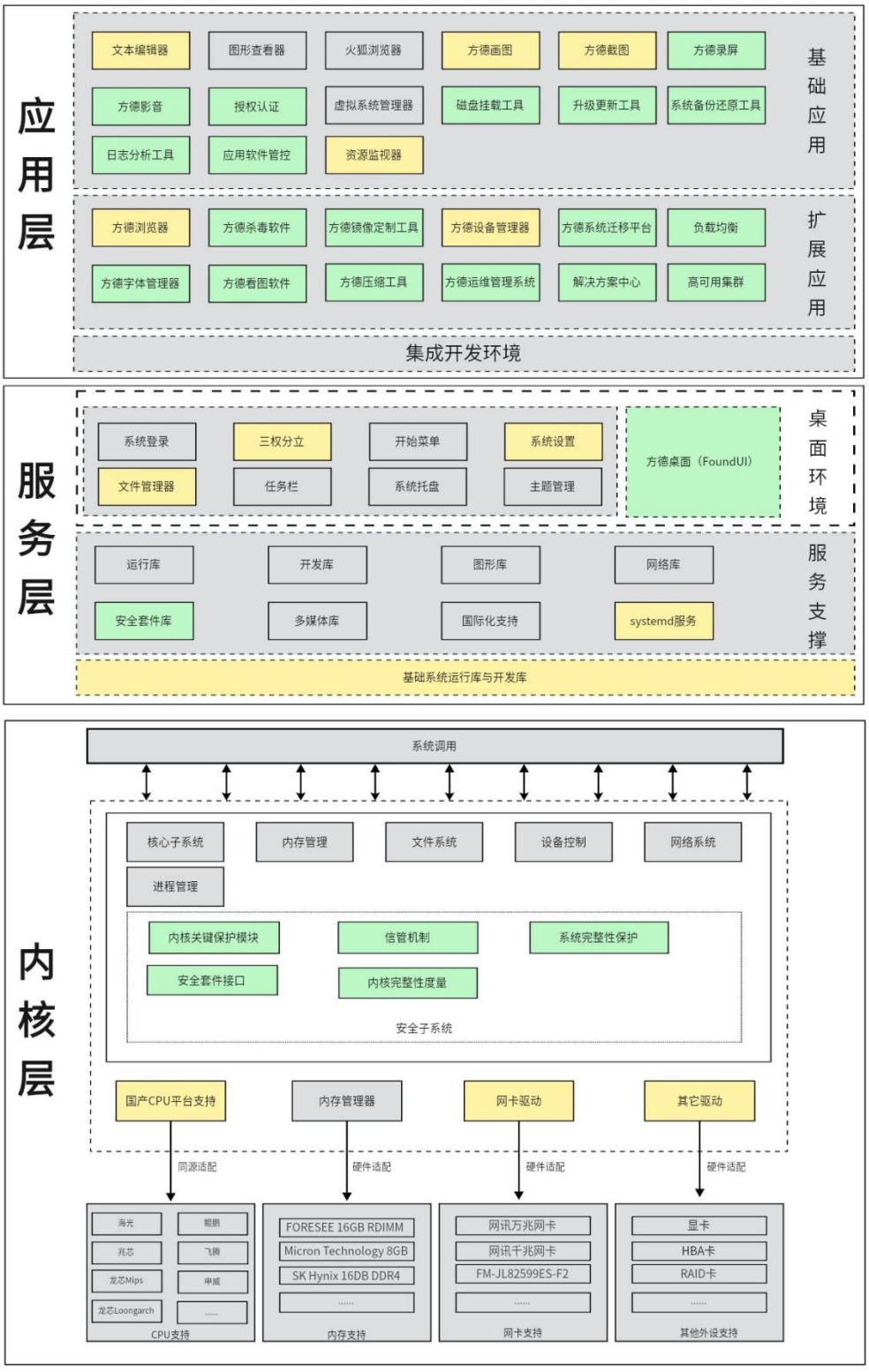

图 2-1 方德高可信服务器操作系统结构图

2.2 产品优势

2.2.1 性能优

方德高可信服务器操作系统 V4.0 在海光平台 Unixbench 综合性能测试方面，测试结果明显优于其它同类产品。

2.2.2 安全性高

1) 集成多重安全增强机制，提供包括漏洞发现、修复和发布全过程的系统安全服务。

2) 支持海光 CCP 和可信计算平台，支持国密 SM2/3/4。

3) 全系统备份还原支持，可根据需要任意创建备份节点和选择还原节点。

4) 支持自研内核统一访问控制安全框架 NFSsec。

2.2.3 生态兼容性好

1) 与 RedHat/CentOS 生态兼容，已适配 CentOS 平台的上层应用可直接迁移到方德平台。

2) 可提供 CentOS 系统迁移方案和迁移工具，实现 CentOS 系统平滑迁移到方德系统平台。

2.2.4 通过《NVME over RoCEv2 网络控制优化技术要求与测试规范》认证

中科方德是首批通过 NVMe over RoCEv2 网络控制优化技术规范的厂商。

2.2.5 国内主流云平台适配支持良好

完成与曙光云、阿里云、百度云、华为云等国内主流云平台的兼容认证适配。

2.2.6 多解决方案及工具支持

方德高可信服务器操作系统 V4.0 兼容适配 CentOS 开源解决方案；支持方德高可用集群、负载均衡、安全电子邮件、文件共享、网盘等自研解决方案；提供方德磁盘挂载配置工具、方德日志收集工具、方德运维管理工具、方德杀毒、方德浏览器等自研工具，方便系统管理和运维；良好的上下游生态，广泛支持主流国产整机、数据库、中间件。

2.2.7 虚拟化、云平台支持

方德高可信服务器操作系统 V4.0 内置开源虚拟化技术 KVM，借助图形化的安装与配置工具，可方便的搭建虚拟化环境；提供对 VirtualBox、VMware、Hyper-V、Xen

等的虚拟化支持；全面支持方德自研云平台和云桌面，适配支持国内主流云平台；提供容器虚拟化支持，提供高性能可弹性伸缩的安全容器应用管理平台。

2.3 核心技术

2.3.1 多硬件平台支持

方德高可信服务器操作系统 V4.0 同源支持海光（海光二号、海光三号、海光四号）、兆芯（兆芯 C，兆芯 D、兆芯 E 和兆芯 KH-40000）、Intel、AMD、华为鲲鹏（鲲鹏 920）、飞腾（FTS2500 系列、FT2000 系列、FTS5000C 系列）、龙芯（龙芯 3C5000、龙芯 3D5000）、申威（申威 3231）等多个硬件平台；提供对主流网络设备、存储设备等的驱动支持。

2.3.2 关键模块保护技术

关键模块保护技术是针对操作系统关键模块被误操作删除情况自研的一款工具，该工具集成到内核中，提供用户态命令可动态修改需要保护的模块列表名，系统内核在执行 rmmod 操作时会对比要删除的模块是否为受保护模块，从而确保受保护模块不会被误操作删除，保护操作系统安全及稳定可靠。

2.3.3 信管机制

信管机制是一款基于方德高可信服务器操作系统的安全机制，是一款自研工具。通过配置进行管控，可以对进出主机的网络数据进行审查管控，也可以对本机文件进行访问读写权限管控，保证系统安全。信管机制主要用于网络管控和文件管控，通过对文件、进程、用户、网络数据等各种对象的 label 标记，进行系统的安全审查控制。文件管控服务器的服务的进程只能操作对应 Label 的经运算许可的文件夹和文件。网络管控服务器的服务的进程 Label 能够发送和接收特定 Label 的数据，以及进出本机网卡的数据管控。

2.3.4 软硬件深度融合优化技术

针对海光等国产 CPU，从操作系统层面和硬件层面进行深度适配与联合调优，有效提升方德高可信服务器操作系统在海光平台上 unixbench、Steam、Iozone、Netperf 等系统性能，形成海光服务器+方德服务器操作系统的最优组合。

2.3.5 系统迁移技术

系统迁移平台基于 flask 框架，包括服务器管理、迁移规则管理、迁移方案管理、迁移仓库管理、迁移实施、迁移审核、工单管理、用户管理等功能，提供页面友好的整体迁移概览和单台迁移进度展示；使用动作服务的方式监控配置的迁移方案，通过

数据触发的形式可自动对批量机器进行扫描、分析及迁移操作，减少复杂的命令操作，有效提升迁移效率，保证可靠迁移。

2.3.6 系统备份还原技术

系统备份还原技术包括使用独立系统实现一键备份还原方案和以开机服务方式实现一键系统还原方案，所述用独立系统实现一键备份还原方案包括独立系统和独立存储分区，所述独立系统包括管理器和备份还原小系统，所述独立存储分区用于储存备份还原小系统的备份文件。本发明通过设有独立系统实现一键备份还原和以开机服务方式实现一键系统还原两种方案，可应对不同的场景需求，两种方案不互斥，可同时使用，提升系统遇到故障时的恢复能力，减小使用者使用系统的难度，且该方法简单直观、易于上手、快捷高效，可在系统发生故障时能够快速高效地将系统还原成备份状态，来解决误操作之后恢复的问题。

2.3.7 方德高性能集群运维管理系统

方德高性能集群运维管理系统为自研的超算管理系统，支持用户权限管理、磁盘配额管理、任务批量下发和执行、节点状态监控，有效简化集群的使用和运维。是一款自研的运维管理工具。

2.3.8 NFSsec 安全框架

NFSsec 以访问控制为核心，可信计算为基础，围绕安全操作系统四级的要求，构建了操作系统的安全防御体系。通过对操作系统主客体进行安全标记，增加强制访问控制、完整性保护等技术手段，与硬件安全芯片结合，从多维度、多层次上提供全面的安全防护，为用户构建一个安全、可信赖的操作系统环境。

2.4 产品主要功能

2.4.1 存储与文件系统

2.4.1.1 存储

1） LUKS2 支持

方德高可信服务器操作系统 V4.0 采用 LUKS2 格式代替了旧版 LUKS(LUKS1)格式，并且使用 LUKS2 作为加密卷的默认格式。LUKS2 在部分元数据损坏的情况下为加密卷提供元数据冗余和自动恢复支持。另外，anaconda 安装程序可使用 LUKS2 磁盘加密，支持 NVDIMM 设备。

2） LVM 缓存支持

方德高可信服务器操作系统 V4.0 提供 LVM 缓存支持，该功能可让用户创建逻辑卷，使用一个小的快速设备作为较大的慢速设备的缓存。它可以让 PCIE SSD 设备作为直连式存储（DAS）或者网络接入存储（SAN）的缓存使用，以提高文件系统性能。

3) NVMe 新增支持

- 实现“NVMe TP 4005a 命名空间写保护”中介绍的命名空间写保护功能；
- 添加对 NVMe 1.3 TP 4004 中指定的异步命名空间访问的支持；
- NVMeT-RDMA 支持最大（16KB，PAGE_SIZE）内联数据；
- NVMeT 添加受支持的命令并影响日志页面。

4) 使用 LibStorageMgmt API 进行存储阵列管理

方德高可信服务器操作系统 V4.0 支持存储阵列管理。LibStorageMgmt 是独立于存储阵列的应用程序编程接口（API）。使用这个 API 可让开发人员以编程方式管理不同的存储阵列，并利用所提供的硬件加速功能。

5) 支持并行 NFS

并行网络文件系统（pNFS）是 NFS V4.1 标准的一部分，允许客户端直接并行访问存储设备。pNFS 机制解决了传统 NFS 的性能瓶颈问题，从而使得系统获得高性能和高扩展性的特性。

6) Ceph 块设备支持

在内核中添加了 libceph.ko 和 rbd.ko 模块。这些内核模块使 Linux 主机可以将 Ceph 块设备视为常规磁盘设备，挂载到某个目录并使用标准文件系统格式化，比如 XFS 或者 EXT4。

2.4.1.2 文件系统

1) 默认文件系统 XFS，单个文件最大支持 1024TiB

方德高可信服务器操作系统 V4.0 默认使用文件系统是 XFS，XFS 文件系统最大大小已从 500TiB 增加为 1024TiB。XFS 是高度可扩展、高性能文件系统，支持高达 16EB（约 1600 万 TB）的文件系统，多达 8 艾字节（约 800 万 TB）以及包含数千万条目的目录结构。XFS 支持元数据日志，它可加快崩溃的恢复。XFS 文件系统还可在挂载且活跃的情况下进行清理碎片和扩展操作。

2) 文件系统新增支持

- 为 SMB3.1.1 POSIX 扩展添加对 STATFS 的支持；
- 向 EXT4 的超级块字段添加 64 位时间戳支持；
- 添加对异步服务器端 COPY 操作的支持；

- 堆栈文件操作：允许从 VFS 中删除一些漏洞，允许只读打开的文件与复制进行适当的交互，可以实现 FS 正确修改 IOCTL。

2.4.2 内核

方德高可信服务器操作系统 V4.0 采用 4.19.113 内核版本，该版本增加了许多新功能，具体说明如下。

1) 基于异步 I/O 的轮询接口

4.19.113 版本新增一个简单的一次性轮询接口 io_submit，用于 AIO 子系统轮询文件系统描述符的情况。与 epoll 不同，它无需其他上下文切换即可达到轮询目的。

2) Overlayfs 内存使用提升

当 Overlayfs（例如容器）的用户修改文件的元数据时，Overlayfs 将复制整个文件的上层缓存。这意味着某些行为（例如 chown()）会大大增加内存使用量。此版本允许延迟拷贝：当低层文件仅修改元数据时，内核将仅仅复制元数据并继续使用低层的数据，直到打开文件进行写操作。

3) L1TF 漏洞补丁

增加对 L1TF（L1TerminalFault）的保护。L1TF 是一个硬件漏洞，允许对 1 级数据缓存中可用的数据进行无特权的推测性访问。

4) 块设备 I/O 延迟控制器

添加新的 controller 以保证 cgroup 的最小延迟值。如果每个设备延迟都没超过设置值，那么控制器不会干涉，但是一旦某个 cgroup 组中延迟超过设定值，它将会降低允许到达磁盘的写的数量，从而降低超过设定值的 cgroup 组的 IO 延迟，其目的是尽量让平均 IO 延迟保持在配置值以下。

5) Common Applications Kept Enhanced (CAKE)队列管理算法

这是一种新的网络包调度规则，其设计目的是替换或者提升当前简单的队列规则在复杂层次结构的抓取 bufferbloat 的问题，以提供更好的网络体验。CAKE 以家用路由为例，可以从最慢的 ISP links 和 routes 中压榨出更多的带宽和延迟，同时提供简单的 API，甚至 ISP 也可以初始化它。

6) Wi-Fi 6 (802.11ax) 初步支持

在无线协议栈中增加了对未来 802.11ax 标准（也称为 Wi-Fi 6）现有草案的初步支持。

7) Intel 缓存伪锁定

增加了对 Intel 特定 CPU 功能的支持。它允许用户指定应用程序可以填充的 CPU 缓存空间量，它隔离 CPU 缓存的那个区域并“锁定”它。从那时起，将只提供缓存命中。缓存伪锁定内存可供用户空间访问，应用程序可在其中将其映射到其虚拟地址空间，从而具有一个内存区域，减少平均读取延迟。

2.4.2.1 动态内核补丁

方德高可信服务器操作系统 V4.0 采用 Kpatch 动态内核补丁管理程序。用户可使用 Kpatch 管理二进制补丁集合，它可在不重启的情况下动态为内核打补丁。

Kpatch 主要包含以下 4 个组件：

1) kpatch-build：用来将 source diff patch 转换成 hot patch module；
2) hot patch module：包含替代函数及原始函数元数据的内核模块；
3) kpatch core module：为 hot patch 注册新的函数以用于替换提供接口的内核模块；
4) kpatch utility：允许用户管理 hot patch 模块的命令行工具。

Kpatch 运行时并不将内核调用重定向到老版本。相反，它会等待所有函数调用都停止时，再切换到新内核。这种方法安全，且容易维护，缺点是在打补丁的过程中会带来一定的延迟。

2.4.2.2 采用 NUMA 进行调度和内存分配

NUMA 系统的结点通常是由一组 CPU 和本地内存组成，有的结点可能还有 I/O 子系统。由于每个结点都有自己的本地内存，因此全系统的内存在物理上是分布的，每个结点访问本地内存和访问其它结点的远地内存的延迟是不同的，为了减少非一致性访存对系统的影响，在硬件设计时应尽量降低远地内存访存延迟（如通过 Cache 一致性设计等），而操作系统也必须能感知硬件的拓扑结构，优化系统的访存。

在方德高可信服务器操作系统 V4.0 中，内核会在同一系统的不同 NUMA 节点间自动重置进程和内存，以提高 NUMA 系统的性能。

2.4.2.3 Swap 内存压缩

方德高可信服务器操作系统 V4.0 提供 Swap 内存压缩功能，Swap 压缩由 Zswap 执行。Zswap 是一种新的轻量化后端构架，将进程中交换出的页面压缩，并存储在一个基于 RAM 的内存缓冲池中。除一些为低内存环境预留的一小部分外，Zswap 缓冲池不预先分配，按需增加，最大尺寸可用户自定义。Zswap 启动存在于主线程中的一个前端，称为 frontswap，zswap/frontswap 进程在页面真正交换出之前监听正常交换路径，所以现有的交换页面选择机理不变。

2.4.2.4 内核模块黑名单

对内核模块来说，黑名单是指禁止某个模块装入的机制。

方德高可信服务器操作系统 V4.0 提供 modprobe 程序可让用户在安装时将内核模块放入黑名单。要禁用自动载入一个模块，可运行以下命令：modprobe.blacklist=module，或者在 /etc/modprobe.d/中创建 .conf 文件，使用 blacklist 关键字屏蔽不需要的模块。

2.4.2.5 支持大内存的内核崩溃转储

当系统出现 panic 的时候，kdump（内核崩溃转储机制）会通过调用 kexec 来快速的启动预先准备好的 dump-capture kernel。该启动方式与快速启动机制类似，不会经过 BIOS，属于热启动。dump-capture kernel 启动后，前一个内核运行时的内存镜像会被保存到 /proc/vmcore，可以通过 cp 或者 scp 将其 vmcore 文件拷贝到磁盘上。重启系统后，即可通过分析工具对刚才保存的 vmcore 文件进行分析，查找导致 panic 的原因。

方德高可信服务器操作系统 V4.0 支持在有大内存（最大为 3TB）的系统中使用 kdump 崩溃 dump 转储机制。

2.4.2.6 APIC 虚拟化

通过利用处理器的新的硬件功能，支持高级可编程中断控制器（APIC）注册的虚拟化，从而提高了虚拟机监视器（VMM）中断处理能力。

2.4.2.7 硬件错误报告机制

方德高可信服务器操作系统 V4.0 提供硬件事件报告机制，可捕获并处理所有来自内核追踪架构的可依赖性、可用性及可服务性（RAS）出错事件，并记录它们。

2.4.2.8 内核安全

安全加固平台建立在操作系统内核层面，既能准确全面的截获应用层的访问请求，又降低了系统安全机制被旁路的危险，为操作系统的安全构筑了坚固的防线。

方德高可信服务器操作系统 V4.0 内置私有数据隔离保护技术，通过该技术包括管理员（root）在内的任何其他用户都不能进行非授权访问，支持内核和核外统一的自主研发的安全框架（NFSsec 框架），提供方德高可信服务器操作系统 V4.0 主动防御能力，保证了操作系统的运行安全和数据安全，为系统提供全面的保护。

2.4.2.9 内核更新

1) 提供超大页面微优化。复制大页面时最后复制目标子页面，因为在复制大页面之后应用程序可能访问大页面的开头，在最后复制目标子页面将使 CPU 缓存对应用程序比较友好。

2) 新增一个 cgroup-aware-OOM-killer 的实现，它增加了将 cgroup 作为单个单元杀死的能力，从而保证了工作负载的完整性。

3) 引入 blk-iolatency io 控制器，这是一个基于延迟的 io 控制器，用于 cgroups。

4) dm 完整性：增加了将 DM 完整性元数据存储在单独设备上的功能。可使用选项 meta_device 激活此功能：/dev/device。

5) 支持要求签名的系统范围策略。允许客户定义一个策略，对 kexec 的内核映像、固件和/或内核模块进行签名。此外，该补丁集还具有配置构建时 IMA 策略的功能，该 IMA 策略会在运行时自动加载，而无需在启动命令行中进行指定，并且在加载自定义内核策略。

6) 支持智能卡和硬件安全模块（HSM）的 PKCS。

7) 支持基于列表的套接字缓冲区的批处理和堆栈遍历。它允许网络堆栈接收数据包列表并将其作为一个单元进行处理，而不是按顺序分别处理每个数据包。

8) 路由添加对定向广播转发的支持。它实现了 rfc1812-5.3.5.2 节和 rfc2644 中描述的功能，允许路由器转发定向广播时的 sysctl bc_forwarding 启用。

9) 网络过滤器 nftables，提供轻量级隧道支持；添加本地 tproxy 支持；实现被动操作系统指纹；允许通过 nft objref 基础结构添加、列出和删除连接跟踪超时策略，并通过 nft 规则配置超时。

10) 异步 I/O：实现 IOCB_CMD_POLL 支持。

11) 锁定：实现 Wound-Wait 互斥体的算法选择。

12) 任务计划程序：删除未使用的 sched_time_avg_ms sysctl。

13) 添加对空闲页面跟踪的支持，并包括共享地图计数。

14) 电源管理：添加一个新的空闲注入框架，供将来内核中的所有空闲注入代码使用。

15) 允许延迟的驱动程序探测超时。

16) 优化 epoll：在可能的情况下放松 irq 安全。

17) 优化 cpufreq / schedutil：考虑中断花费的时间。

18) 优化 page_alloc：双区域的 batchsize。

2.4.3 虚拟化及容器

2.4.3.1 基于内核的虚拟化

1) Hyper-V

为了在崩溃期间收集更多可操作的数据，比如堆栈跟踪，建议在分配的页面上写入一页的 kmsg 数据，并通过 MSR 通知 Hypervisor 页面地址。

2) 使用 virtio-blk-data-plane 提高 I/O 性能

在方德高可信服务器操作系统 V4.0 中使用 virtio-blk-data-plane I/O 虚拟化功能，且添加 XDP 相关的属性，添加 kick stats。它为每个块设备单独分配一个线程用于 I/O 处理，在效率上有一定的提升。

3) PCI 桥接

以往 QEMU 最多可支持 32 个 PCI 插槽。方德高可信服务器操作系统 V4.0 采用 PCI 桥接技术，可让用户配置 32 个以上的 PCI 设备。

> **说明：**
>
> 不支持桥接后的设备热插拔。

4) QEMU 沙盒

方德高可信服务器操作系统 V4.0 使用内核系统调用，过滤加强 KVM 虚拟化安全性，这提高了主机系统与虚拟机之间的独立性。

5) 支持 QEMU 虚拟 CPU 热添加

方德高可信服务器操作系统 V4.0 中的 QEMU 提供虚拟 CPU（vCPU）热添加支持。可在运行的虚拟机中添加虚拟 CPU（vCPUS），满足与负载关联的负载要求。

6) 半虚拟化驱动 Virtio

多队列 virtio_net 及 virtio_scsi 提供更好的可扩展性。每个虚拟 CPU 都有独立的传输或者接收队列以及可在不影响其他虚拟 CPU 的情况下使用的独立中断。

7) VPC 和 VHDX 文件格式

方德高可信服务器操作系统 V4.0 中的 KVM 包括对微软虚拟 PC（VPC）和微软 Hyper-V 虚拟硬盘（VHDX）文件格式的支持。

8) 在线迁移的内存页 Delta 压缩

Delta 压缩算法通过压缩虚拟机内存页并减小传输的迁移数据大小，提高 KVM 在线迁移功能。这个功能可让迁移至集合更迅速。

9) KVM 中集成 Hyper-VEnlightenment 功能

KVM 中已使用多项微软 Hyper-V 功能，例如：支持内存管理单元（MMU）和虚拟中断控制程序。微软在虚拟机和主机之间提供半虚拟 API，通过在主机中使用这个功能的一部分，并根据微软的说明对其进行控制，提高微软 Windows 虚拟机的性能。

10) 高带宽 I/O 的 EOI 加速

方德高可信服务器操作系统 V4.0 在高级可编程中断控制程序（APIC）中使用 Intel 和 AMD 的改进，加速中断结束（EOI）处理。对于老旧的芯片组来说，方德高可信服务器操作系统 V4.0 为 EOI 加速提供了半虚拟化选项。

11) KVM 虚拟机的 USB 3.0 支持

方德高可信服务器操作系统 V4.0 通过添加 USB 3.0 主机适配器（xHCI）模拟作为技术预览提供改进的 USB 支持。

12) Windows 8 和 Windows Server 2012 虚拟机支持

方德高可信服务器操作系统 V4.0 支持在 KVM 虚拟机中运行的微软 Windows 8 和 Windows Server 2012 系统。

13) QEMU 虚拟机的 I/O 节流

这个功能为 QEMU 虚拟机块设备提供 I/O 节流。I/O 节流会延缓 I/O 内存请求的处理。这样会延迟系统但可防止其死机。

说明：

不能节流数据层。

14) 已配置 PCIE 设备的错误处理

如果在将使用高级出错报告（Advanced Error Reporting，AER）的 PCIE 分配给虚拟机时出错，则受到影响的虚拟机会关机，但不影响其他正在运行的虚拟机或者主机。该设备的主机驱动程序从错误中恢复后就可以让该虚拟机重新运行。

15) 基于 VFIO 的 PCI 设备分配

虚拟功能 I/O（VFIO）用户空间驱动程序页面为 KVM 虚拟机提供改进的 PCI 设备分配解决方案。VFIO 提供内核级设备分离强化，提高设备访问的安全性，并与安全引导等功能兼容。

16) Intel VT-d 大页面支持

在方德高可信服务器操作系统 V4.0 中，KVM 虚拟机使用虚拟功能 I/O（VFIO）进行设备分配时，使用 2MB 页面作为输入/输出内存管理单位（IOMMU），因此可减少 I/O 操作的转译后备缓存（translation lookaside buffer，TLB）的消耗。计划在方德高可信服务器操作系统 V4.0 中提供 1GB 页面支持。VT-d 大页面功能支持目前仅限于 Intel 的平台。

17) KVM 时钟获取时间性能

在方德高可信服务器操作系统 V4.0 中加强了 vsyscall 机制以支持 KVM 虚拟机更迅速地从用户控件读取时钟。方德高可信服务器操作系统 V4.0 主机中运行的方德高可信服务器操作系统 V4.0 虚拟机可体验到经常读取时间的应用程序的性能提高。

18) 图像格式的 QCOW2 版本 3

方德高可信服务器操作系统 V4.0 添加对图像格式的 QCOW2 版本 3 的支持。

19) 改进的实时迁移报表

现在可使用实时迁移的有关信息分析和调试性能。改进的报表包括预期关机、关机或者脏页面比例。

20) 在线迁移线程

已将 KVM 在线迁移功能改进为支持线程处理。

21) 字符设备和串行端口的热插拔

目前方德高可信服务器操作系统 V4.0 支持新的字符设备及串行端口的热插拔。

22) 模拟 AMD Opteron G5

KVM 现在可以模拟 AMD Opteron G5 处理器。

23) Libguestfs 新功能

Libguestfs 是一组访问和修改虚拟机磁盘映像的工具。方德服务器 4 中的 Libguestfs 包括大量改进，最主要的包括：

- 使用 SELinux 或者 sVirt 包含的安全虚拟化，保证加强针对恶意和畸形磁盘映像的安全性。
- 可检查和修改远程磁盘，最开始是使用网络块设备（NBD）。
- 在某些程序中可进行磁盘热插拔以便获得更好的性能。

2.4.3.2 Xen

方德高可信服务器操作系统 V4.0 可在 Xen 环境中作为客机操作系统(guestOS)使用。

2.4.3.3 Hyper-V

方德高可信服务器操作系统 V4.0 可在 Microsoft Hyper-V Server 2012 R2 主机系统中作为客机操作系统(guestOS)使用。

2.4.3.4 VMware

方德高可信服务器操作系统 V4.0 可在 VMware ESX 中作为客机操作系统(guestOS)使用。

2.4.3.5 Docker 容器

方德高可信服务器操作系统 V4.0 提供 Docker 容器支持，还提供用于编排容器的 Kubernetes。Docker 容器是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的容器中，然后发布到任何流行的 Linux 机器上，也可以实现虚拟化。

2.4.3.6 KVM

方德高可信服务器操作系统 V4.0 提供 KVM(qemu-kvm 4.2.0)支持，包括：

- 5 级分页功能，扩展了虚拟地址的大小，增加了可寻址的虚拟内存。
- 用户模式指令预防(UMIP)，一种将对用户空间应用程序的访问限制为系统级设置的安全特性。
- Ceph 存储，在所有支持的处理器架构上提供块存储功能。
- NVIDIA vGPU 和 VNC 控制台之间的兼容性。
- QEMU 仿真器引入的沙箱特性，以确保安全的代码测试。

2.4.4 桌面环境

2.4.4.1 GNOME 桌面

方德高可信服务器操作系统 V4.0 默认桌面环境是 GNOME 3.32，且 GNOME 显示管理器使用 Wayland 作为默认的显示服务器。新的 GNOME 包括许多有用的功能，包括：

1) 扩展设备支持

GNOME 集成了 Thunderbolt 3 连接支持。每当 Thunderbolt 3 建立连接并激活时，用户将得到通知。该功能允许用户密切监视所有连接，并检测任何安全漏洞或数据泄漏或盗窃企图。

2) 新的盒子特性

GNOME 的应用程序中包含了一些用于管理远程和虚拟机的新特性。该版本通过自动下载操作系统简化了创建虚拟环境的过程。此外，拖放功能可以让用户轻松地在机器之间传输文件。

3) 新的屏幕键盘

GNOME 重新编写了最新版本的屏幕键盘，试图解决紧迫的 UI 问题。目前该功能支持多种布局以支持不同的地区、自动键盘激活和视图切换，因此用户在书写时可以清楚地看到文本。

4) 更新的 UI 页面

新的桌面环境还增加了几个额外的特性来改进 UI 和 UX。这包括多显示器处理，直接窗口处理，改进的缩放等等。

2.4.4.2 Nemo 文件管理器

Nemo 文件管理器是 GNOME Files（以前称为 Nautilus）的一个分支，但在功能方面远远优于 Nautilus。Nemo 基于 Nautilus 3.4，整合了部分 Nautilus 3.6（所有桌面图标，紧凑的视图等）特点，具有完全的导航选项，GTK 书签管理，路径切换，文件操作进度信息和更多的选项配置。方德高可信服务器操作系统 V4.0 针对 Nemo 进行了改进优化，支持重命名、显示容量等，支持磁盘自动挂载，无需手动挂载，并对页面显示效果进行了优化，兼容 Windows 使用习惯。

2.4.4.3 D-Bus

D-Bus 是一种高级的进程间通信机制，它由 freedesktop.org 项目提供，使用 GPL 许可证发行。D-Bus 最主要的用途是在 Linux 桌面环境为进程提供通信，同时能将 Linux 桌面环境和 Linux 内核事件作为消息传递到进程。D-Bus 的主要概念为总线，注册后的进程可通过总线接收或传递消息，进程也可注册后等待内核事件响应，例如等待网络状态的转变或者计算机发出关机指令。开发者可使用 D-Bus 实现各种复杂的进程间通信任务。

2.4.5 编译工具及开发环境

2.4.5.1 工具链及开发库

GCC 编译器更新到 8.5.0 版本，支持更多 C++标准，更好的优化以及代码增强技术、提升告警和硬件特性支持。

Glibc 库升级到 2.28，支持 Unicode11，更新的 Linux 系统调用，提升 DNS stub resolver、额外的安全加强和性能提升。

提供 Binutils-2.30 工具链、C++ 标准库、Boost 库、QT 库、KDE 开发框架等、OpenJDK8、icedtea-web 及不同的 Java 工具。

2.4.5.2 调试及开发环境

在方德高可信服务器操作系统 V4.0 中，GDB 调试程序发行版本是 gdb-8.2。另外提供一个新软件包 gdb-doc，该软件包包含 PDF、HTML 以及信息格式的 GDB 手册。提供 Qt-creator、Eclipse 等开发 IDE 环境。提供 Git、SVN、CVS 等版本管理工具。

2.4.5.3 性能工具

方德高可信服务器操作系统 V4.0 中包含一些性能工具的最新版本，比如 Oprofile、Papi 和 Elfutils，提供性能、可移植性及功能性改进。提供 Performance Co-Pilot，这是一个用来对系统级性能测定进行采集、归档和分析的工具、服务及库套件。提供 SystemTap 内核探测工具，可用来监控和跟踪运行中的 Linux 内核的操作。提供 Valgrind，这是一款用于内存调试、内存泄漏检测以及性能分析的软件开发工具。

2.4.5.4 编程语言

方德高可信服务器操作系统 V4.0 提供最新的 Ruby、Python、Perl、Java 版本。提供多个 JDK 版本，将 OpenJDK8 作为默认 Java 开发套件（JDK）。另外允许同时平行安装多个 Java 版本(OpenJDK7 等)。平行安装的功能可让用户同时尝试多个 JDK 版本，以便在需要时调优性能并解决问题。

Python 版本默认 3.6.8，同时提供 python2.7 支持。

2.4.6 联网与认证

2.4.6.1 网络分组

引进网络分组技术作为链路聚集的捆绑备用方法。该技术旨在轻松管理、调试和扩展。

2.4.6.2 网络管理 NetworkManager

NetworkManager 由如下几部分组成：一个管理系统网络连接、通过 D-BUS 进行状态报告的后台服务，以及一个允许用户管理网络连接的客户端程序。

NetworkManager 的优点：简化网络连接的工作，让桌面本身和其他应用程序能感知网络。

2.4.6.3 时钟同步 Chrony 套件

Chrony 能保持系统时钟与时钟服务器（NTP）同步，让时间保持精确。Chrony 套件适用于所有经常挂起的系统中，或者间歇性断开并重新连接到网络的系统。例如：移动系统和虚拟系统。

2.4.6.4 动态防火墙守护进程 Firewalld

方德高可信服务器操作系统 V4.0 提供动态防火墙守护进程 Firewalld，它可提供一个动态管理的防火墙，并支持网络“区域”以便为网络及其相关链接和接口分配可信度。它还支持 IPv4 和 IPv6 防火墙设置。它支持以太网桥接并有独立的运行时和持久配置选项。它还有一个可直接添加防火墙规则的服务或者应用程序接口。

2.4.6.5 DNSSEC

DNSSEC 是一组域名系统安全扩展（DNSSEC），允许 DNS 客户端认证和检查来自 DNS 名称服务器响应的完整性以便确认其起始点，并确定在中转过程中是否受到影响。

2.4.6.6 FreeRADIUS

方德高可信服务器操作系统 V4.0 包含 FreeRADIUS 版本 3，FreerRADIUS 一般用来进行账户认证管理，记账管理，常见的电信运营商的宽带账户，上网账户管理，记账，都是使用的 Radius 服务器进行鉴权记账的。

2.4.6.7 包过滤框架

方德高可信服务器操作系统 V4.0 默认使用 nftables 包过滤框架。nftables 是一个 netfilter 项目，旨在替换现有的 {ip,ip6,arp,eb}tables 框架，为 {ip,ip6}tables 提供一个新的包过滤框架、一个新的用户空间实用程序（nft）和一个兼容层。它使用现有的钩子、链接跟踪系统、用户空间排队组件和 netfilter 日志子系统。

nftables 主要由三个组件组成：内核实现、libnl netlink 通信和 nftables 用户空间。 其中内核提供了一个 netlink 配置接口以及运行时规则集评估，libnl 包含了与内核通信的基本函数，用户空间可以通过 nft 和用户进行交互。

2.4.7 互操作性

2.4.7.1 Samba

Samba 是在 Linux 和 UNIX 系统上实现 SMB 协议的一款软件，由服务器及客户端程序构成。SMB（Server Messages Block，信息服务块）是一种在局域网上共享文件和打印机的一种通信协议，它为局域网内的不同计算机之间提供文件及打印机等资源的共享服务。SMB 协议是客户机/服务器型协议，客户机通过该协议可以访问服务器上的共享文件系统、打印机及其他资源。通过设置“NetBIOS over TCP/IP”使得 Samba 不但能与局域网络主机分享资源，还能与全世界的电脑分享资源。

2.4.7.2 IPA 域

提供 FreeIPA 组件，它集成了 Ldap+Kerberos（Kerberos 认证是在身份认证的时候不传输密码，而是在传输票据，更加安全可靠）+Web 管理的集中式用户认证管理系统（系统级别的单点登录 SSO，可以对 apache，ftp，nfs，ldap，smtp，ssh 做身份认证）,可以与微软的 AD 域进行用户信息的同步，提供可与 AD 域间的跨域信任机制，实现 AD 域和 FreeIPA 域用户之间的访问。

2.4.8 安全

所有的软件都包含 Bug，通常这些 Bug 会造成漏洞让恶意用户侵入您的系统。未更新软件包是造成电脑入侵的共同原因。及时地安装安全补丁能及时封堵系统的漏洞，保证系统安全。

2.4.8.1 系统提供的安全产品、工具及服务

方德系统中提供了大量安全相关的产品、工具及服务，有效利用他们可增强系统的安全性，这些产品、工具和服务有：

1) 安全加固平台，在通用操作系统的基础上，通过对操作系统主客体进行安全标记、增加强制访问控制、完整性保护等技术手段，对操作系统进行安全功能增强，弥补通用操作系统安全性不高的缺陷，提高了操作系统的安全保护能力。支持主机信息、加固方案、完整性度量、访问控制、系统保护、安全审计 6 个功能模块。具体技术方案信息详见《方德操作系统安全加固平台 V1.1-产品白皮书》，请直接联系中科方德相关部门进行获取。
2) 方德文件保险箱，提供文件加密保护，对存储在加密文件系统中的文件和目录，提供透明加解密，同时具备用户间数据隔离和加密保护功能，支持一箱一密。增加支持基于硬件信任根的可信存储支持，支持国密算法。
3) 用户密码安全，系统默认安装了 Cracklib PAM 模块，能提供额外的密码检查能力，支持设置最短密码长度、密码复杂度、密码过期期限等功能、错误密码帐户锁定等。
4) 控制 Root 访问：提供 setuid、sudo、su 等工具，提供禁止 root ssh 登录、PAM 限制 Root 登录、自动注销空闲用户、不允许交互式启动等机制。
5) 网络安全访问：提供保护网络安全的 TCP Wrappers 、xinetd、netstat 等工具，提供使用禁止源路由、反向路径过滤等控制命令。
6) 动态防火墙 Firewalld，动态防火墙后台程序 Firewalld 支持对 IPv4 和 IPv6 防火墙设置。它支持以太网桥，并有分离运行时间和永久性配置选择。它

还具备一个通向服务或者应用程序以直接增加防火墙规则的接口。用户对防火墙策略进行适当配置，增强系统网络安全。

7) 用 DNSSEC 保护 DNS 流量，域名系统安全扩展 DNSSEC（Domain Name System Security Extensions）能让 DNS（Domain Name System）客户端进行身份验证，以及检查来自 DNS 域名服务器响应的完整性，以此鉴定它们的来源并判断它们是否在传输过程中被篡改过。

8) VPN（Virtual Private Network）支持，提供 VPN 的配置工具 Libreswan。支持 IPsec 协议的 VPN 配置。

9) 提供磁盘 Linux 分区加密、目录手动加密，提供 GPG（GNU Privacy Guard）密钥创建工具，用于识别您的身份以及进行通信的身份验证，提供公钥密码 openCryptoki 工具，它是一个 Linux 下的 PKCS11 开源实现。

2.4.8.2 SELinux 框架

SELinux（Security-Enhanced Linux）是美国国家安全局(NSA)对于强制访问控制的实现，是 Linux 历史上最杰出的新安全子系统。NSA 是在 Linux 社区的帮助下开发了一种访问控制体系，在这种访问控制体系的限制下，进程只能访问那些在他的任务中所需要文件。方德高可信服务器操作系统 V4.0 提供 SELinux 的最稳定的版本。

2.4.8.3 Audit 审计

安全审计服务子系统 Audit 可以记录操作系统中文件变化、用户对文件的读写、系统调用、文件变化通知等，并将相关记录形成日志信息存放到指定目录。方德高可信服务器操作系统 V4.0 提供 Audit 的所需的服务及查看管理工具，如 Audit 系统管理工具 auditctl，用来获取状态，增加删除监控规则。

查询 Audit Log 工具 ausearch，输出 Audit 系统报告 aureport 等，并额外提供安全审计报警及对审计出的重大危险进程进行限制或中止的功能。

2.4.8.4 日志收集 Rsyslog

系统管理一般都需要收集服务器的日志信息用于及时发现错误，处理故障。Rsyslog 是一个快速处理收集系统日志的程序，提供了高性能、安全功能和模块化设计，可以收集业务日志，并可定制和过滤、筛选。

2.4.8.5 国密算法

支持硬件国密算法，系统内核层 Crypto API 提供 SM2/SM3/SM4 国密算法支持，用户态通过预装 openssl、gmssl 支持国密算法；支持标准格式的国密证书，符合 GMT

0028《密码模块安全技术要求》第二级要求，具备商用密码产品认证证书，支持国密 TLCP 协议。

2.5 产品技术指标

表 2-1 产品技术指标

指标项	指标要求
核心参数	Kernel 4.19.113
	Gnome 3.32.2
	Glibc 2.28
	GCC 8.5.0
	llvm 12.0.1
	Golang 1.16.12
标准符合度	符合 POSIX 标准
	CGL 4.0
	LSB 4.1
	ODCC-2020-05016《NVME over RoCEv2 网络控制优化技术要求与测试规范》认证
架构支持	支持 X86、ARM 等处理器架构，包括海光、兆芯、飞腾、鲲鹏等。
	支持多路多核处理器，最大支持 32 路 CPU，物理内存最大支持 64T，单个分区最大支持 1EB。
硬件支持	支持主流存储设备如 SATA、RAID、iSCSI 等各种存储设备。
	支持主流 Raid 卡、HBA 卡、SCSI 卡、Infiniband 卡等。
	支持各种 LAN 卡、调制解调器、打印机、USB 接口和其它外设如键盘鼠标等。
	支持 GPU 通用计算加速卡。
	支持网卡 bonding；适配支持商用网卡。
	支持硬件系统的扩容和升级，支持设备驱动程序的卸载和安装。
文件系统	支持 EXT2、EXT3、EXT4、XFS、GFS、NTFS、FAT 等文件系统，单个文件最大支持 16TB，文件名长度最大支持 255 个字符。
安装及升级	提供中文化的图形操作页面，具有详细的帮助信息。
	支持多种安装方式，可采用 U 盘安装，光盘安装，网络安装等。
	支持全部安装、最小安装、定制安装等安装方式。
	提供图形化软件包升级工具，支持远程和本地在线升级，支持系统补丁包的及时更新。
多语言支持	支持简体中文、英文等多种语言。
	支持多种中文输入法，包括智能拼音输入法、海峰五笔输入法等。
	支持宋体、黑体、楷体等常见字体类型。
	采用 I18N（国际化）技术和标准。
	支持的字符编码方式不限于 GB2312、GBK、GB18030、UTF8、UTF16 等。
	支持矢量字体打印。
功能指标	支持网络负载平衡技术。
	支持 LVM 逻辑卷管理。

指标项	指标要求
	支持传统的异步 I/O，支持 POSIX 标准的异步 I/O。
	支持分布式文件系统产品，能够实现将多台 PC 服务器的磁盘聚合成一个存储设备。
	提供全面的服务器应用软件包，包括 Web 服务器、邮件服务器、FTP 服务器、DNS 服务器、打印服务器以及 NTP 网络校时服务等软件包。
	支持 TCP/IP 等常用网络协议。支持 IPv4 和 IPv6，端口号支持 0-65535。
	支持裸设备访问。
	图形化的内核参数配置工具。
	提供图形化的安全配置工具，提供图形化的 SELinux、防火墙以及 VPN 的配置管理工具。
	提供图形化的运维监控管理工具，提供系统运行状况监控、性能监控、软硬件资源监控、统一升级部署管理、数据备份、故障诊断及恢复等功能。
	提供 perf、top、iostat、sar、free 等性能分析优化工具。
	提供 Trace 等故障诊断工具，提供 Audit 记录故障信息。
	提供常用的系统工具，包括：VsFtpd 图形配置工具、日志查看工具、内核崩溃转储工具（Kdump）。
安全特性	支持自研内核统一访问控制安全框架 NFSsec。
	提供安全审计机制，可以对系统事件进行审计。
	支持文件系统加密。
	支持文件完整性检查，能够监视重要文件和目录发生的变化。
	支持 nftables 和 iptables，有效管理 Linux 防火墙。
	支持基于 SELinux 的多种安全策略。
	支持基于 SSL/TLS 对 HTTP、SMTP 等的加密、验证，支持 IPSec、支持安全优化的 SSH，保证安全的远程登录、支持网络监控及入侵检测工具。
	支持系统安全启动。
可信计算	支持 LSM、可信计算 TPCM/TCM、TCM2.0、TPM2.0，内置国密算法，支持基于国密算法的加解密应用，支持可信计算。
虚拟化支持	支持 KVM 虚拟化，提供对 VMware、Hyper-V、KVM、Xen、VirtualBox 等的虚拟化支持。
	提供虚拟化管理工具，实现单机、多机环境下的虚拟机的创建、配置与管理。
高可用性	支持负载均衡； 支持多种网卡 Bonding，提高可用性； 支持存储多路径并提供国际标准 multipath 驱动。
集群部署	支持大规模图形化快速安装部署物理机、虚拟机服务器集群。
备份恢复	支持对整个已安装操作系统及数据分区的镜像备份和恢复。
	支持基于本地网络和异地网络的数据备份。
开发工具	提供了丰富的开发工具和完整的 Linux 开发环境。
云原生支持	支持 Ceph、GlusterFS、OpenStack、K8S 等原生技术生态，提供对容器、虚拟化、云平台、大数据等云原生应用的良好支持。
开源生态	兼容 CentOS 生态和 openEuler（欧拉）生态。

2.6 应用领域

方德高可信服务器操作系统 V4.0 主要面向党政军、金融、电信、医疗、教育、能源等重点行业，为企业级用户提供稳定、可靠、安全的运行环境支撑。

3 解决方案

3.1 高可用集群

方德高可用集群是基于 Linux 系统的集群解决方案，是以减少服务中断时间为目的的服务器集群技术，它通过保护用户的业务程序对外不间断提供服务，把因软件/硬件/人为造成的故障对业务的影响降低到最小程度。方德高可用集群方案可提供多种集群高可用策略，能够有效避免单点故障，确保企业级应用的持续性。企业的服务程序和服务器系统始终处于被监控的状态，当服务器的硬件或软件发生故障导致运行出错时，会根据用户预定义的集群策略将业务应用服务自动切换到备机中运行，从而保证业务应用的可持续运行，并能将业务应用的中断时间限制在最小程度。

方德高可用集群解决方案可稳定运行在国产兆芯、海光、鲲鹏、飞腾、龙芯和 Intel X86 等处理器架构，全面保障系统可靠、数据可靠、应用可靠。满足政府、金融、电力、医疗、运输、制造业等行业的自主可控和安全可靠的应用需求。

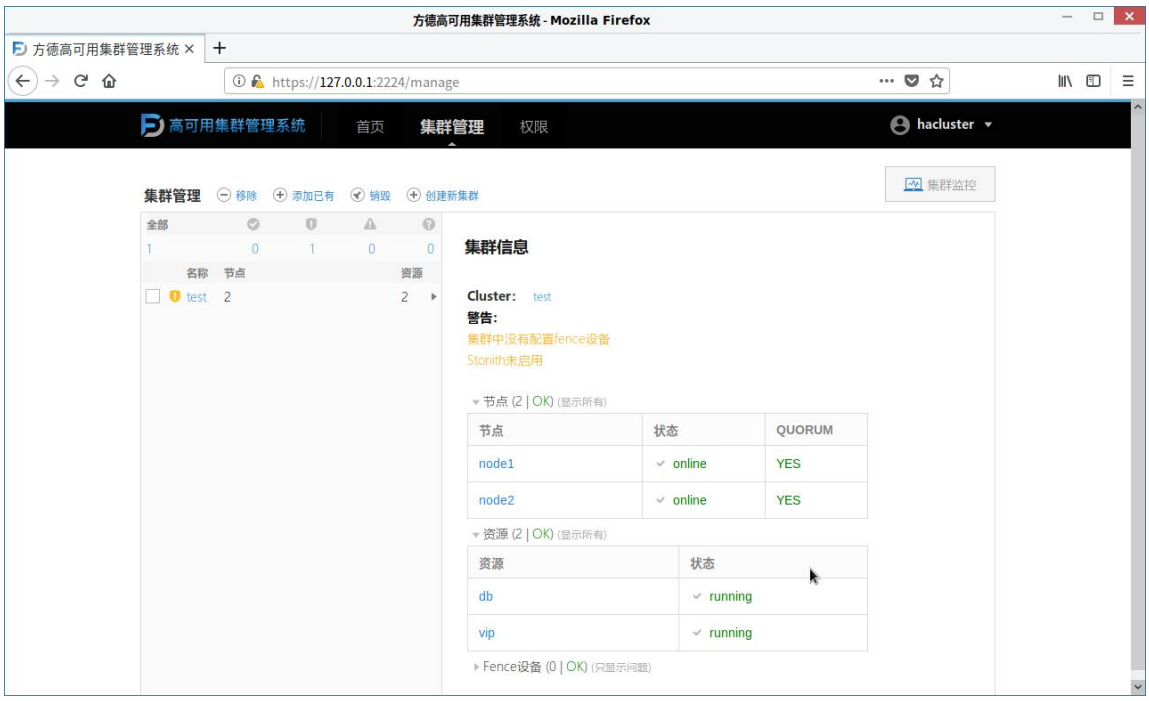

图 3-1 高可用集群

方德高可用集群特性：

1） 图形化管理页面

方德高可用集群软件提供友好、直观、易用的图形化管理工具。

2） 智能可靠的切换策略

方德高可用集群软件提供完善的保护机制及丰富的应用程序代理，针对目前市场主流应用进行优化，保障服务器系统在被监控的硬件或资源出现故障时能及时切换备机。任何一个节点出现故障，都可以在极短的时间内进行自动切换，当故障排除后，服务自动回迁，提供 7 × 24 小时永不停机的企业级应用可靠保障。

3） 多样化的集群模式

方德高可用集群软件 支持双机热备、双机互备、多机备份等多种运行保护方式。还可支持容错方案，能够在秒级完成切换被保护的服务资源任务，满足对中断时间有苛刻要求的用户需求。

4） 确保数据一致性

方德高可用集群软件实时监控共享数据资源，利用磁盘心跳、仲裁设备、心跳网络 bond、共享磁盘锁机制以及参考 IP 服务机制，保证在极端的情况下数据的一致性。

5） 多处理器架构及存储方式支持

方德高可用集群软件不仅支持 X86 架构，对国产海光、兆芯、飞腾、鲲鹏、龙芯处理器架构也有良好支持，最大限度的满足用户对不同平台应用的需求，支持多种文件系统及主流存储设备，支持共享磁盘及镜像磁盘方式，使其可以灵活的根据用户实际情况部署高可用系统。

6） 快速多样的报错预警

方德高可用集群软件在系统出现故障切换时，可以通过本机的蜂鸣预警，并通过发送邮件及短信的方式提醒管理员，使管理员能够快速定位故障主机。

7） 全面丰富的应用监控

方德高可用集群软件除了可以对诸多国际知名应用软件进行高可用保护外，还可监控国产数据库、中间件软件，同时对各种硬件资源进行深入的故障检测。另外，方德提供对用户自定义资源的定制化支持，可提供个性化服务，确保用户系统处于全盘监控之下。

8） 快速响应

方德高可用集群软件能够实现业务的秒级保护切换。

3.2 负载均衡

方德负载均衡软件是基于 Nginx 定制研发的一款负载均衡软件产品。方德负载均衡软件可实现四层或七层负载均衡，将大量的并发访问请求转发到后端多个服务节点进行处理，减小用户等待响应的时间，可以有效的扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。

方德负载均衡软件具有高并发连接、内存消耗少和稳定性高的特点，除此之外，在功能方面，还具有以下特点：

1) 可以支持针对 web、email、ftp 等多种服务的负载均衡；
2) 可以支持七层协议和四层协议的负载均衡；
3) 支持热部署和动态扩容；
4) 支持轮询、加权轮询、ip_hash、least_hash、url_hash、sticky 等多种负载均衡调度算法；
5) 内置健康检查功能，可以方便的查看后端应用服务器的监控状态；
6) 支持远程管理，提供图形化管理工具，方便管理用户的配置工作；
7) 支持软件授权和试用功能，保证软件安全性；
8) 与方德高可用集群软件相结合，支持高可用集群部署，进一步确保服务的高可用性。

3.3 安全邮件

方德安全增强电子邮件系统是专门针对互联网信息技术的特点，综合多行业多领域不同类型单位自身信息管理发展的特点和多年研发经验而开发的一套专门针对涉密行业的、拥有自主知识产权的专业电子邮件系统。

方德安全增强电子邮件系统提供基于集中管理平台、Webmail 系统等整套安全电子邮件系统的解决方案，配合国产高可信服务器操作系统，可全面构建邮件系统服务端、客户端架构，增强信息安全保障，以用户为中心，提供快捷高效、友好的操作体验。

方德安全增强电子邮件系统除具备传统 Webmail 的各项功能外，安全方面增加了许多特性。独特的密级设置，可防止邮件发送的误操作导致的信息泄露；基于 PKI 的用户认证系统，可对用户身份进行鉴别，防止盗发邮件；使用公钥加密，保证邮件在服务器上安全存储，即使邮件泄露，也无法获得有用信息。同时集中管理系统提供了丰富的管理工具，用浏览器即可调整优化系统的各项功能和配置参数，方便开展邮件服务器的运维工作。

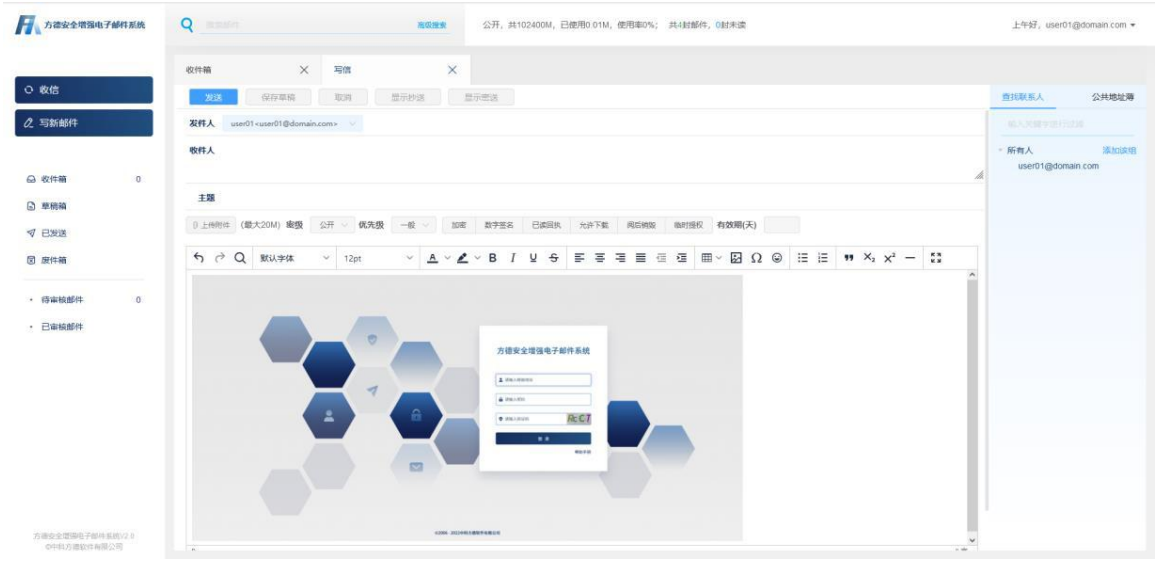

图 3-2 方德安全增强电子邮件系统

方德安全增强电子邮件系统特性：

1) 高安全性

- 与密标、运管和审计等基础安全平台紧密结合，保证系统整体安全。
- 基于数字证书的身份认证机制，保证用户登录安全。
- 邮件可加密存储、数字签名，保证数据安全完整。
- 支持加密安全传输，保证邮件传输过程安全。
- 密级设置、审核机制以及收发监控，控制保密信息流转，防止敏感信息外泄。
- 严格的权限审核，全面的安全审计，保证操作可追溯。
- 管理员三权分立，相互协作、相互制约，保证管理的安全性。

2) 高易用性

- 良好的人机交互体验，收发邮件更轻松。
- GB 级大附件传输，信息交流更通畅。
- 公共地址薄管理，自定义顺序，查找邮箱地址更方便。
- 新邮件到达自动提醒，防止遗漏重要信息。
- 邮件撤回功能，有效解决错发、误发问题。
- 远程监控系统运行状态，管理更轻松。

3) 高可靠性

- 高可用部署，保障邮件服务的可靠。
- 负载均衡部署，保障超大用户量时系统的可靠。
- 备份还原机制，保障全部数据的可靠。

4） 高兼容性

- 兼容国内外主流数据库。
- 符合 J2EE 标准，适配支持各主流中间件。
- 支持国产终端与非国产终端混合部署模式。
- 支持海光、兆芯、龙芯、飞腾、鲲鹏、申威等国产处理器平台。

3.4 安全接管

方德安全接管方案是一项安全解决方案，针对部分无法完成 CentOS 迁移，在停服后仍使用 CentOS7、8 版本系统的用户，可提供安全加固产品和可信软件仓库产品两个产品，安全加固策略配置服务、漏洞订阅服务和系统运维服务三种服务，方案模式为“2 个产品+3 种服务+N 个行业场景”。

安全接管方案包括四个阶段：环境收集阶段、规划设计阶段、实施阶段和维护阶段。

针对在迁移过程中的“老旧系统”、由于迁移时间过长造成的存量 CentOS 系统或对于因技术原因暂难以替换的 CentOS 系统的用户，方德安全接管方案提供产品+服务的支持，为 CentOS5、6、7、8 的用户提供安全加固产品为系统进行安全加固；为 CentOS 7、8 的用户，可切换到方德可信软件仓库，提供安全漏洞补丁修复；为 CentOS 5、6 的用户，可提供定制化的运维服务。

表 3-1 方德安全接管方案服务

CentOS 版本	停服时间	安全接管服务		
		安全加固	可信仓库	运维服务
CentOS 8	2021/12/31	√	√	√
CentOS 7	2024/06/30	√	√	√
CentOS 6	2020/11/30	√	-	√
CentOS 5	2017/03/31	√	-	√

3.5 系统迁移

随着 CentOS 的停服、国家政策“应替尽替”和“国产替代”的推动，方德高可信服务器操作系统 V4.0 提供了系统迁移方案，推出了方德系统迁移平台，帮助客户快速、平滑、稳定、安全地完成系统迁移。

针对用户存量迁移和新建迁移两种场景，方德高可信服务器操作系统制定了不同的迁移方案。在方德系统迁移平台的支持下，通过评估、准备、实施、验证的一系列服务，顺利完成系统迁移，保证用户业务系统的正常运行。

方德系统迁移平台的特性如下：

- 简单易操作，友好的图形界面，步骤引导式交互，一键批量迁移。
- 实时迁移日志，全面的评估分析，信息入库存储，迁移可溯源。
- 差异信息 diff 比对，兼容主流开源软件、商用软件、及用户自研软件。

方德系统迁移平台的主要功能如下：

1) 迁移源管理
   - 支持使用公网、离线仓库进行迁移、支持自定义仓库地址，一次性配置、重复使用。
   - 一键批量绑定迁移源。
2) 迁移前评估
   - 自动检查旧系统环境信息。
   - 提供新、旧系统 rpm 包相关信息及对比列表。
   - 提供新旧系统 ABI 差异对比列表。
3) 环境检查
   - 自动检测系统版本、系统内核、磁盘可用空间、系统架构、等其他与迁移相关的系统环境信息。
   - 迁移过程中自动检查迁移前置条件是否满足、提供逐步引导式使用流程。
4) 一键批量迁移
   - 一键完成当前任务下关联的所有主机新、旧系统迁移，无需重复多次操作。
   - 实时查看各主机新、旧系统迁移日志。
5) 任务管理
   - 任务管理支持批量关联主机，统一绑定迁移源，支持两种迁移方案选择。
   - 提供迁移状态管理，中断后可根据迁移状态节点继续之前的操作进度。
6) 迁移后检查
   - 可查看各主机迁移后环境信息及迁移结果与完成情况。

4 典型应用服务器

方德高可信服务器操作系统 V4.0 支持多种服务器应用，典型的服务器应用有：Web 服务器、邮件服务器、打印服务器、域名解析服务器、FTP 服务器、代理服务器、SSH 服务器、DHCP 服务器、NFS 服务器、数据库服务器。

4.1 Web 服务器

方德高可信服务器操作系统 V4.0 中提供 Apache HTTP 服务器，Apache-Tomcat HTTP 服务器。

4.2 邮件服务器

方德高可信服务器操作系统 V4.0 中提供 sendmail、postfix 等服务，可搭建邮件服务器，同时方德有自研的邮件服务器产品。

4.3 打印服务器

方德高可信服务器操作系统 V4.0 中提供 cups 及 samba 服务，可搭建不同需求的打印服务器应用。

4.4 域名解析服务器

方德高可信服务器操作系统 V4.0 中提供 bind 服务，可搭建域名解析 DNS 服务器。

4.5 FTP 服务器

方德高可信服务器操作系统 V4.0 中提供 vsftpd 服务，可搭建 FTP 服务器。

4.6 代理服务器

方德高可信服务器操作系统 V4.0 中提供 squid 服务，Squid 可以代理 HTTP、FTP、GOPHER、SSL 和 WAIS 等协议，根据不同需要，可搭建正向代理和反向代理，正向代理中，根据实现方式的不同，又可以分为普通代理和透明代理。

4.7 SSH 服务器

方德高可信服务器操作系统 V4.0 中提供 sshd 服务,可向外提供 ssh 服务，此时一般要配置防火墙。

4.8 DHCP 服务器

方德高可信服务器操作系统 V4.0 中提供 DHCP（Dynamic Host Configuration Protocol 动态主机配置协议）服务，可搭建 DHCP 服务器。

4.9 NFS 服务器

NFS（Network File System）网络文件系统是 FreeBSD 支持的文件系统中的一种，NFS 允许一个系统在网络上与他人共享目录和文件。通过使用 NFS，用户和程序可以像访问本地文件一样访问远端系统上的文件。方德高可信服务器操作系统 V4.0 中提供 rpcbind 及 nfs 服务，可搭建 NFS 服务器。

4.10 数据库服务器

方德高可信服务器操作系统 V4.0 提供 MariaDB 及 PostgreSQL 数据库服务，可搭建数据库服务器使用。MariaDB 是替代 MySQL 的产品。MariaDB 保留了与 MySQL 的 API 和 ABI 兼容性，并添加了一些新功能。例如：未阻断的客户端 API 库，有加强性能的 Aria 和 XtraDB 存储引擎，更优的服务器状态变量或者改进的复制功能。

PostgreSQL 是一个高级对象关系数据库管理系统（DBMS）。PostgreSQL 软件包包括 PostgreSQL 服务器软件包及访问 PostgreSQL DBMS 服务器所需客户端程序和库。

5 生态适配

表 5-1 整机适配列表（部分）

厂商	型号	架构
曙光信息产业（北京）有限公司	曙光 H620-G30A 服务器	海光
	曙光 H620-G35A 服务器	海光
	曙光 H520-G30A 服务器	海光
	曙光 H520-G35A 服务器	海光
	曙光 H420-G30A 服务器	海光
北京同方信息安全技术股份有限公司	超强 K620 系列	鲲鹏
	超强 K640 系列	鲲鹏
	超强 K820 系列	鲲鹏
安擎（天津）计算机有限公司	EG940F-G20	飞腾
	EG921F-G20	飞腾
	EG950F-G20	飞腾
	EG940A-G21	飞腾
	EG990A-G20	飞腾
上海华诚金锐信息技术有限公司	申威服务器 GS208S1	申威
	申威服务器 GS212S2	申威
…	…	…

表 5-2 数据库适配列表（部分）

厂商或社区	产品名称及版本	产品类型
MySQL 社区	MySQL 5.x，MySQL8.x 等主流版本	开源
PostgreSQL 社区	PostgreSQL 主流版本	开源
openGauss 社区	OceanBase 3.1	开源
	OpenGauss 2.0	开源
武汉达梦数据库有限公司	达梦数据库管理系统 V7	商业
	达梦数据库管理系统 V8	商业
	达梦数据库管理系统 V8.4	商业
瀚高基础软件股份有限公司	瀚高数据库系统 V4.3.5	商业
	瀚高安全数据库管理系统 V4.5	商业

厂商或社区	产品名称及版本	产品类型
	瀚高企业版数据库系统 V6.0	商业
北京人大金仓信息技术股份有限公司	金仓数据库管理系统 KingbaseES V8	商业
天津南大通用数据技术股份有限公司	大规模分布式并行数据库集群系统 GBase 8a MPP Cluster V9	商业
…	…	…

表 5-3 中间件适配列表（部分）

厂商或社区	产品名称及版本	产品类型
Apache 软件基金会	Tomcat6 7 8 等主流版本	开源
Nginx 社区	Nginx 主流版本	开源
Redis 社区	Redis 主流版本	开源
金蝶天燕云计算股份有限公司	金蝶 Apusic 应用服务器软件 V10	商业
	金蝶 Apusic 应用服务器软件 V9	商业
北京东方通科技股份有限公司	东方通应用服务器软件 TongWeb V7.0	商业
北京宝兰德软件股份有限公司	宝兰德应用服务器软件【简称：BES Application Server】V9.5	商业
北京宝兰德软件股份有限公司	BES 消息中间件软件【简称：BES MQ】V1.2	商业
…	…	…

更多的整机、数据库、中间件等适配情况请访问中科方德官网（http://www.nfschina.com/）生态合作-互认证产品清单查询。

6 服务与支持

6.1 服务体系

中科方德建立了本部支持中心、区域支持中心、授权服务商三位一体的服务体系，由本部支持中心提供呼叫中心服务、服务质量培训与管理，区域支持中心进行区域支持服务、问题/需求管理，授权服务商进行约定范围内的服务。

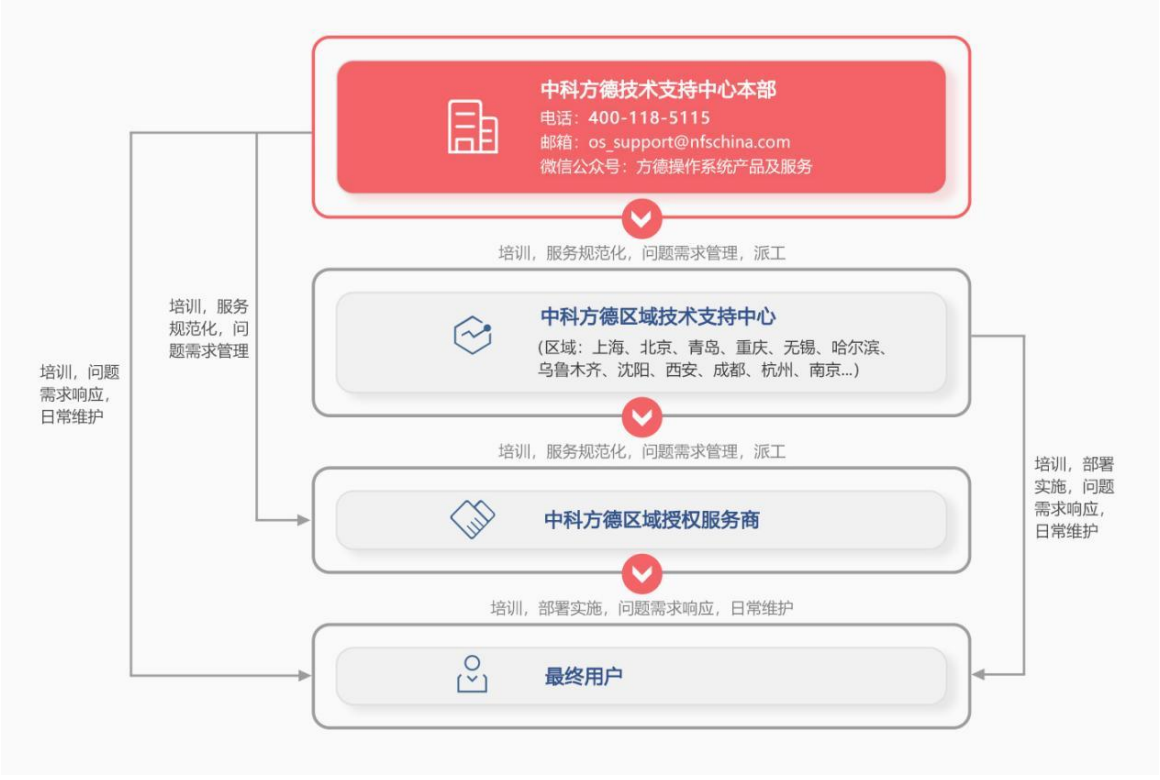

图 6-1 服务体系

6.2 服务周期

方德高可信服务器操作系统默认生命周期为 13 年，包含 5 年标准服务期 + 5 年扩展服务期 + 3 年延长服务期。

标准服务期					扩展服务期					延长服务期		
1 年	2 年	3 年	4 年	5 年	6 年	7 年	8 年	9 年	10 年	11 年	12 年	13 年

- 标准服务期内，提供技术支持、系统 bug 修复补丁和安全漏洞补丁，定期推送小版本升级，包含新功能和新特性；
- 扩展服务期内，提供技术支持、系统 bug 修复补丁和安全漏洞补丁；
- 延长服务期内，提供技术支持、系统关键 bug 修复补丁和关键安全漏洞补丁。

6.3 服务内容

中科方德遵循 ITIL/ISO20000“IT 服务标准化”管理体系的技术服务标准，建立成熟的操作系统产品服务体系。中科方德将竭力保证用户系统的正常运行。

图 6-2 服务内容

6.4 服务网络

中科方德总部设在北京，并在上海、重庆、哈尔滨、青岛、成都、深圳、乌鲁木齐、西安、沈阳、长春、无锡等地设有子/分公司，建立了覆盖全国的产品研发、应用推广、适配服务与技术支持协同网络。

图 6-3 服务网络

联系方式：

服务热线：400-118-5115

电子邮件：os_support@nfschina.com

网址：www.nfschina.com

