操作系统的选择为何仍然如此重要

Linux 助力现代 IT 和业务目标的 8 种方式

Red Hat

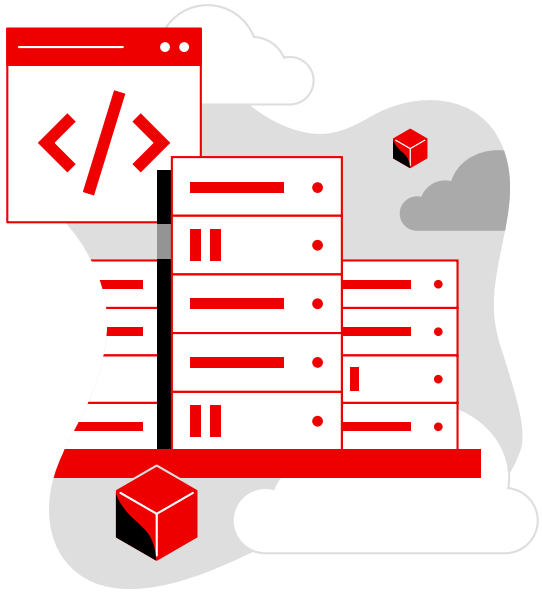
目录

操作系统是现代 IT 的重要组成部分

操作系统一直是 IT 环境中的重要组成部分。

操作系统最初开发于 20 世纪 50 年代，之后便不断改进以满足不断变化的需求。早期的操作系统主要用于批处理和简单的任务调度，一次仅执行一个作业。不过，20 世纪 60 年代，随着分时系统的引入，多个用户可以同时与一台计算机进行交互。在接下来的数十年内，出现了 UNIX 等操作系统，这些操作系统在计算环境中引入了模块化和可移植性。

20 世纪 80 年代，随着个人电脑的普及以及销量的增加，操作系统也逐渐走进大众的视野。图形用户界面（GUI）的出现彻底改变了用户与计算机的交互方式，使计算功能得以面向范围更广的受众。



随着对基于服务器的计算需求的增长，Linux® 成为面向全球企业数据中心的功能强大且可扩展的操作系统。Linux 内核于 1991 年首次发布，是 UNIX 的免费开源替代方案，任何人都可以运行、研究、共享和修改。如今，Linux 已成为全球最受欢迎的操作系统之一，为现代创新型 IT 提供了理想平台。

21 世纪 00 年代，虚拟化技术和容器技术相继出现，这些技术使硬件资源的使用更高效且促成了向云计算的转变。因此，操作系统开始扮演新的管理角色，以实现灵活的应用部署和资源优化。

如今，操作系统的影响范围已超出处于核心的数据中心，覆盖至边缘设备和物联网（IoT）等新兴技术。操作系统可在网络边缘实现高效的数据处理，以缩短延迟时间并提升各种应用场景（从智慧城市到自动驾驶汽车）的性能。

本电子书概述了操作系统（尤其是 Linux 操作系统）在当下仍然如此重要的原因，还介绍了它如何满足现代 IT 和业务的需求。

操作系统的选择在当下仍然如此重要的 8 个原因

随着企业越来越多地采用基于云的分布式 IT 环境，操作系统的重要性也在不断提升。

目前，87% 的企业实施了多云策略，50% 的企业工作负载在公共云中运行。[1] 您的操作系统可作为跨本地和云基础架构、各种硬件和软件以及传统应用及云就绪应用的统一基础。安全性、管理、可移植性和生命周期规划均始于操作系统。如果在数据中心和云环境中的单一运维基础上实现标准化，可以简化 IT 运维、增强灵活性、提高安全性并为创新提供支持。

作为全球最受欢迎的操作系统之一，许多企业都选择将 Linux 作为其 IT 基础。事实上，2022 年，在全球服务器操作系统市场中，Linux 在新物理机和新虚拟机中的部署率分别为 65.6% 和 82.8%。[2]

企业可以在 Linux 操作系统上运行各种生产环境和开发环境的工作负载，包括 IT 和 Web 基础架构、客户关系管理以及企业资源管理。[3] 本章将介绍 Linux 操作系统如何为应用、流程和 IT 环境提供支持，从而为整个企业带来价值。

本章内容：

1 Flexera，“Flexera 2023 年云现状报告”，2023 年 3 月。

2 IDC 市场份额，“2022 年全球服务器操作系统环境市场份额：持续稳步增长”。文档编号：US51038623。2023 年 7 月。

3 IDC 白皮书，由红帽赞助，“红帽企业 Linux：一年内为客户带来 1.7 万亿美元的经济收益”，文档编号：US48931522。2022 年 3 月。

1 操作系统是硬件、应用和用户之间的纽带。

作为软件堆栈中的基础层，操作系统可为硬件和应用之间的交互提供支持，且提供基本的服务和资源。

操作系统可将底层硬件组件抽象化，以便应用在多种基础架构上运行，无需针对特定系统进行修改。它还可以管理资源，其中包括中央处理器（CPU）、内存、存储和网络，从而优化系统性能并防止多个运行中的应用发生冲突。借助操作系统的命令行界面（CLI）和 GUI，您可以更直观地与计算机及其应用交互。用户身份验证、访问控制和加密等安全功能可保护数据和资源免受未经授权的访问。错误和异常处理功能可防止系统崩溃，提升系统的可靠性以及整体用户体验。

Linux 等现代操作系统通常包含两种模式（内核模式和用户模式），这两种模式用于确定哪些应用、组件和用户具有哪些权限。在内核模式下，受信任的核心软件组件（如**操作系统内核**和某些设备驱动程序）可以执行特权操作，直接使用硬件资源以及访问受限的系统内存。

所有其他软件（包括用户应用、库和工具）均在用户模式下运行且对系统资源的访问权限有限。这些应用只能访问用户空间（可防止应用对关键操作系统组件产生干扰的隔离内存区域）。

借助值得信赖的专业能力构建您的 IT 基础

可将 Linux 作为您的所有 IT 工作负载的稳定运维基础，不过，Linux 发行版有多种，每种发行版的工具、服务和支持策略均有所不同。您的业务依赖于 IT 基础，因此，对 Linux 供应商的选择重要且具有战略意义。

应寻找值得信赖且具备您的业务所需的经验和专业能力的 Linux 供应商。关键因素包括：

- 生产级 Linux 发行版，注重满足客户的需求。
- 持续为 Linux 内核做出贡献且处于领先地位。
- 拥有由客户、合作伙伴和专家组成的协作社区。
- 具有生命周期长和安全维护的可靠的商业支持记录。

2 操作系统可确保硬件和软件的兼容性。

操作系统通过管理硬件资源（例如存储、网络和外围设备）来提高系统的稳定性以及软硬件兼容性。

应用和硬件资源通过设备驱动程序实现通信。操作系统通过对这些驱动程序进行管理来确保正确安装、加载和运行，从而提高系统的稳定性以及应用与底层硬件组件之间的兼容性。例如，在系统初始化过程中，Linux 操作系统会对新连接的资源或集成资源进行检测，识别已知设备，然后查找并加载相应的驱动程序。操作系统还提供了硬件抽象层，应用无需获取底层硬件的详细信息即可与硬件设备交互。这些标准化接口可简化应用的开发，提高不同硬件配置下的可移植性。

芯片组、存储和网络是设备驱动程序和操作系统管理所必不可少的要素。人工智能和机器学习（AI/ML）等许多计算密集型工作负载都可从芯片组的硬件加速中受益。操作系统可以将图形处理器（GPU）、系统芯片（SoC）和现场可编程门阵列（FPGA）的功能和加速用于此类工作负载。

还可以通过操作系统以稳定且可靠的方式访问**存储在硬盘上的数据**。操作系统使用经过优化的方法来管理文件组织和存储，最大限度地减少数据碎片，防止命名冲突，并确保跨应用的一致性。

最后，操作系统会对与网络相关的功能进行编排，以实现同一网络中多个系统之间连接的可靠性以及高效的数据交换。操作系统使用网络堆栈管理网络协议的集成，以跨不同网络提供端到端的通信。操作系统可配置和管理网卡（NIC）和无线适配器等网络设备，以支持并加快应用之间的数据传输。操作系统还会实施网络安全措施（包括防火墙和加密协议），以防止未经授权的访问和数据泄露。

从认证合作伙伴生态系统中获得更多选择

测试和认证可确保第三方产品与您的操作系统稳定协作。应寻找与业界领先的硬件、软件和云服务供应商合作的 Linux 供应商，获得更多选择、创新和稳定性。检查所选供应商的合作伙伴生态系统是否包含您当前使用以及将来计划使用的产品和服务。

3 操作系统可增强平台的可靠性和稳定性。

操作系统可检测并处理软件和硬件错误，为应用和用户提供一个稳定、可靠的平台。

应用是许多数字业务的核心，停机往往令人难以接受。许多操作系统都包含可在应用执行过程中捕获和管理运行时错误的先进的错误检测机制。这些机制有助于防止出现系统级崩溃、中断和数据损坏。此外，操作系统还会通过文件完整性检查、校验和以及数字签名来监控关键应用和系统文件，确保仅执行已获授权且未经修改的代码。

硬件错误也是一个问题。通过检测和管理硬件错误（例如内存故障、磁盘错误和处理器故障），操作系统可以提高系统的稳定性，防止灾难性故障的发生。通过与内置于内存和存储设备的纠错码（ECC）和循环冗余校验（CRC）保护功能结合使用，操作系统可以识别并管理出现故障的硬件，从而提高应用所存储和使用数据的可靠性。错误检测和纠正机制（例如日志记录或校验和）有助于操作系统快速准确地检索应用和用户的数据。

了解并解决系统层面的问题也很重要。操作系统提供的日志记录和诊断工具可记录有关错误和系统事件的信息，协助进行故障排除以及主动进行维护操作。借助这些工具，系统管理员可以分析错误模式、识别潜在漏洞并采取纠正措施，从而保持系统的整体稳定性和可靠性。

通过预测性分析和主动修复工具提高稳定性

复杂 IT 环境的管理工作既繁杂又耗时。应寻找包含高级管理和自动化工具的 Linux 发行版有助于您主动管理整个 IT 环境。统一的工具可跨基础架构使用，并监控您的环境中的所有系统，帮助您在问题影响业务的开展之前发现问题。与此同时，借助专注于运维、安全性和业务成果的工具，您可以了解问题和变化对企业的影响，还可确定修复措施的优先顺序。

4 操作系统可提高 IT 运维效率。

一致的操作系统可作为跨 IT 足迹的统一基础，让您可以实现运维的标准化和简化、提高效率并增强安全性。

现代 IT 环境通常由多个基础架构和架构组成。事实上，85% 的企业在运行多个部署环境，31% 的企业在至少 5 个环境中部署应用。[4] 例如，您可以同时使用本地数据中心和公共云提供商，且在基于各种硬件架构（例如 x86、Arm 和 IBM Power 等）的服务器、工作站和边缘设备上部署工作负载。

采用多种环境时，一致性至关重要。借助标准化操作环境，您可以开发通用的程序、策略和配置，从而简化日常运维和管理任务。这为 IT 企业带来了诸多益处：

- **互操作性。**使用通用操作系统可促进不同基础架构之间的互操作性和集成。您可以在大规模环境中部署、管理分布式应用并进行故障排除，从而降低复杂性。
- **可扩展性。**一致的操作系统部署可以简化 IT 服务和环境的扩展，因为新基础架构可以复制经过验证的现有配置。
- **安全性。**借助标准化操作环境，您可以更轻松地跨环境一致地实施安全策略，包括定期进行修补、更新和合规性审核，从而降低安全漏洞的风险。
- **可用性。**在混合云环境中使用一致的操作系统可简化问题的解决过程，从而减少系统停机时间。

标准化可提升效率

操作系统可作为所有基础架构和架构的统一标准化基础。在保持整体一致性的同时，选择能够提供针对不同部署环境进行优化的多种操作系统变体的 Linux 供应商。确保其中包含和关联的管理和自动化工具在所有变体中以相同的方式运行。在其中一种发行版中实现标准化有助于创建统一的内聚型操作环境，从而简化基础架构的管理，提高 IT 效率和生产力，并增强安全性。

4 F5 Networks，“2023 年应用策略状态报告”，2023 年 3 月。

5 操作系统可保护您的基础架构、应用和数据。

操作系统可防范可能危及基础架构、应用和数据的完整性、机密性和可用性的威胁。

Linux 内核包含的许多安全功能有助于保护您的基础架构、应用和数据。例如，Linux 操作系统包含实施**零信任架构**所需的身份验证和授权工具。通过用户名、密码、生物识别信息或安全令牌进行身份验证，可识别想要访问 IT 系统和资产的个人或应用。**安全增强型 Linux（SELinux）**等授权和访问控制机制可定义授予这些用户、群组或应用的权限和特权。这些工具均可用于防止对敏感型资源和系统配置的未经授权的访问。

操作系统的其他主要安全功能包括：

- **加密。**内置加密技术可保护静态以及跨网络传输的机密文件和敏感数据。例如，红帽® 企业 Linux 利用系统级加密策略来自动配置预定义的加密控制并将其应用于系统和应用。它还支持对虚拟机工作负载进行 CPU 辅助加密以实现机密计算。
- **应用白名单。**此功能可建立允许特定用户在系统上运行的已批准应用和可执行文件的索引。
- **硬件信任根。**基于硬件的信任根、远程证明和测量启动技术可验证系统的完整性，确保系统未被修改或篡改。
- **安全性扫描。**开放式安全内容自动化协议（OpenSCAP）等合规性和漏洞扫描工具可简化审核，查找和并复配置错误的系统，帮助您保持合规性。
- **系统日志记录。**审核和日志记录功能可以记录系统内的事件和活动。之后，管理员可以审查并分析这些事件，确定安全漏洞的来源，并实施纠正措施。

为零信任奠定基础

零信任架构可将安全防护应用于每项资产，而非仅在网络边界管理安全防护。尽管 Linux 本身包含构建零信任架构所需的核心功能，某些发行版仍然添加了可简化零信任架构的采用的功能和工具。应寻找通过值得信赖的软件供应链提供的 Linux 发行版，且包含系统级加密设置、硬件信任根功能、内置合规性扫描以及基于策略的身份管理工具。

如需了解更多信息，请阅读**概述**部分。

6 操作系统可管理应用和工作负载性能。

操作系统可管理对 CPU 和内存的使用，以最大限度地提升硬件性能，从而实现卓越的应用、工作负载和用户体验。

操作系统可通过进程调度技术优化对 CPU 和内存使用，在不同资源的工作负载之间实现平衡，并保持系统响应速度。例如，进程调度算法和负载均衡机制可确保 CPU 时间的高效利用和公平分配。调度算法还可以使 CPU 快速在多个进程之间来回切换，实现多个进程同时进行。

通过安排交互式进程的优先顺序，操作系统可以提供响应式体验，让用户感知到的延迟达到最短甚至感知不到延迟。借助实时的进程调度功能，具有严格时间要求的进程（如嵌入式系统或工业控制系统）能够在特定期限内完成并及时响应外部事件。

Linux 还包含内存管理功能，该功能可确保为应用提供充足的内存、避免潜在冲突并优化系统性能。动态的内存分配和解除分配可为进程提供实现最高性能所需的内存。当某个进程结束内存的使用后，操作系统会将内存提供给其他进程使用。

优化工作负载性能

应寻找包含可根据应用、工作负载或应用场景调整、监控和管理系统性能特性的工具和接口的 Linux 发行版。例如，某些供应商提供的工具和服务可让您识别性能问题、剖析应用性能并分析数据，从而帮助您快速解决问题甚至完全避免问题。

操作系统还可通过缓存和缓冲机制提高内存性能，这些机制会将频繁访问的数据存储在速度较快、成本较高的缓存中，将其他数据存储在容量较大、速度较慢的随机存取存储器（RAM）和存储设备中。通过在内存和硬盘之间交换数据，操作系统可利用虚拟内存为进程提供比实际可用地址空间更大的地址空间。虚拟内存可提高多任务处理效率，较大的应用在系统上占用较小的内存即可运行。

7 操作系统可通过虚拟机提高资源利用率。

作为虚拟机技术的重要组成部分，操作系统可优化资源的利用、隔离工作负载并提高跨环境的可扩展性。

虚拟机是自行运行虚拟客户机操作系统的隔离环境，用户和应用可将其视为独立的硬件资源，尽管它们可能会与其他虚拟机共用实际的物理资源。**虚拟机监控程序**是在单个物理服务器上创建和管理虚拟机的专用软件。操作系统和虚拟机监控程序具有许多相同的功能。因此，它们可以共用许多组件，其中包括进程调度程序、内存管理器、设备驱动程序、安全功能和网络堆栈。

扩展虚拟化

Linux 中**基于内核的虚拟机（KVM）**可让您将 Linux 用作虚拟机监控程序。选择能扩展 KVM 功能的商用 Linux 发行版可提高管理效率。

虚拟机监控程序通过执行多种功能为 IT 运维提供支持：

- **分配资源。**虚拟机监控程序可将 CPU 时间和内存等资源分配给虚拟机，在保证服务质量的前提下使多个虚拟机在同一物理硬件上运行。它们还会将物理硬件（网络适配器、存储控制器和显卡等）以虚拟设备的形式提供给虚拟客户机操作系统，使多个虚拟机能够在不会发生冲突的前提下使用相同的资源。
- **创建快照和克隆。**许多虚拟机监控程序都包含虚拟机快照和克隆功能，以提高灵活性、可扩展性和效率。快照可捕获特定时间点的虚拟机状态和数据。它们可用于恢复或回滚至已知配置。克隆功能可复制现有虚拟机，加快新实例的部署。
- **实时迁移和恢复。**实时迁移和高可用性功能有助于平衡工作负载、优化资源的利用，并延长虚拟机的正常运行时间。实时迁移可在不中断服务的前提下在物理主机之间移动运行中的虚拟机。虚拟机保持开机状态，网络连接保持有效状态，且应用可继续运行。如果虚拟机因主机故障而中断，虚拟机监控程序会在数秒内自动将其重启，无需人工干预。
- **安全性和隔离性。**虚拟机监控程序会强制实施严格的边界，防止虚拟机访问分配给其他虚拟机的内存或资源。这些边界有助于增强安全性，遏制潜在漏洞和网络攻击的影响。

8 操作系统可支持现代云原生应用。

Linux 操作系统支持容器技术，该技术在部署和管理现代云原生应用时可实现更高的敏捷性、可扩展性和一致性。

52% 的企业认为“容器化工作负载”是应用现代化工作的重要组成部分。[5] **容器**是将 IT 组件（例如应用、运行时、库和依赖项）打包到轻量级、可移植的隔离环境中的技术。容器技术可高效地将操作系统虚拟化，以便多个容器共用单个操作系统内核，该内核管理着硬件资源以及与物理主机系统的交互。

Linux 操作系统会对与进程空间、文件系统和网络访问相关的内核资源进行分区，从而为每个容器提供独特的专用资源集。与传统的虚拟化一样，这种方法可隔离每个容器，防止容器相互冲突和干扰，且允许多个容器（每个容器均具有唯一的用户空间和运行时环境）在同一主机上执行。为公平且合理地分配资源，操作系统会按每个容器管理和限制对资源的使用，其中包括 CPU、内存和磁盘输入/输出（I/O）。

通过管理容器环境中的网络接口和配置，操作系统可确保容器之间以及容器与外部系统之间能够根据需要进行通信，同时还能使网络保持隔离状态。操作系统还可为容器提供隔离的文件系统，这些文件系统可通过容器存储驱动程序访问共享的数据和持久存储。

最后，操作系统还提供了强制访问控制（MAC）功能，以强制执行严格的预定义资源访问策略。容器只能与指定的系统资源交互，从而提高隔离性并防止普遍存在的安全威胁和漏洞。

扩展您的 IT 环境以及容器技能

您可从 Linux 操作系统开始使用容器。应寻找包含 **Podman**、**Skopeo** 和 **Buildah** 等容器工具的 Linux 发行版，以便您在 Linux 系统上开发、构建、运行和管理容器。选择一家同时提供容器编排平台的 Linux 供应商，您便可以逐渐扩展和扩大容器的使用范围。

5 红帽电子书，“企业如何落实传统应用的现代化升级”，2023 年 2 月 6 日。

利用开源软件的优势

开源社区创建并维护着许多深受欢迎的操作系统（包括 Linux）及相关的工具和软件。

在这些社区中，开发人员提出、贡献并测试新的操作系统功能和特性。版本分为免费的社区发行版和付费的企业发行版。

企业或商用发行版通常以订阅的形式提供，且提供针对业务需求和挑战的额外功能、服务和支持。例如，企业操作系统订阅通常包含全天候生产级技术支持，以加快故障排除速度并减少停机时间。可能还包含培训和教程，以便用户在操作系统中高效管理和优化并排查问题。

较长的生命周期支持可提高 IT 环境中的稳定性。商用操作系统供应商通常遵循可预测的发布周期，因此，企业能够为更新、升级和新功能做好计划和准备。就地升级工具和专业服务有助于顺利、高效地升级到新版本。

企业供应商通常都有安全团队来评估、监控和应对新出现的威胁，以提高操作系统的安全性。某些商用发行版包含的服务可操作系统，并针对安全问题的修复、不合规设置、未修补的系统和配置偏移提供指导。供应商还可以根据行业安全标准对其操作系统进行认证，以帮助保持合规性且受到保护。

最后，许多商用操作系统供应商都会为其操作系统培养认证合作伙伴生态系统，以促进业务的稳定和可靠性。此类生态系统可能包含硬件供应商、软件供应商、公共云提供商和服务机构。

商用开源操作系统的优势

与使用免费替代方案的企业相比，商用操作系统用户可获得以下体验：

23%
3 年内的本地基础架构成本降低幅度。[6]

72%
计划外停机时间减少幅度。[6]

1730 万美元
每企业每年净收入平均增长。[6]

6 IDC 白皮书，由红帽赞助，“红帽解决方案与其他免费开源方案的商业价值对比”，文档编号：US50423523。2023 年 3 月。

简化系统管理

操作系统管理工具有助于更高效地配置、监控和优化 IT 环境。

性能管理

了解系统性能，以识别瓶颈、监控利用率并排查性能问题。

IT 自动化

实现日常任务的自动化，减少人工干预，最大限度地减少错误并确保系统配置的一致性。

安全和访问管理

评估、管理和修复安全漏洞，保护关键应用和数据。强制执行访问控制，管理权限并确保用户拥有其角色所需的权限。

配置管理

应用更新和升级，确保操作系统及时获取最新的安全补丁和增强功能。在多个系统中保持配置的一致性，减少 IT 环境之间的配置偏移。

审核和监控

记录和审核系统事件，简化故障排除、合规性和安全性分析。简化审核活动，确保符合安全和运行标准。监控和优化虚拟资源，确保经济高效地使用资源。

备份和恢复

创建和管理备份，并实施恢复程序，以便在系统出现故障或数据丢失时保护数据。

现代 IT 从红帽企业 Linux 开始

操作系统在 IT 基础架构中起着至关重要的作用。红帽企业 Linux 可为您的企业带来更多价值。

无论您处于 IT 之旅的哪个阶段，红帽企业 Linux 都能帮助您构建高效、安全至上的基础，跨混合云和多云环境实现创新。这款云就绪型操作系统可跨物理、虚拟化、混合云、多云甚至边缘基础架构等提供一致的定制体验。通过红帽企业 Linux 对本地数据中心和云环境进行标准化处理，有助于您完成云迁移，适应高度数字化环境，同时提升工作效率、安全性及运维效率。

- 跨不同基础架构的一致性
- 预测性分析和修复工具
- 高级安全功能
- 值得信赖的软件供应链
- 内置的自动化和管理功能
- 性能优化工具
- 大型认证合作伙伴生态系统
- 适用于多种架构的变体
- 内置的容器技术

进一步了解红帽企业 Linux。

1051224_0324_KVM

Red Hat