白皮书

LinuxONE：一款高度安全、易于扩展的数据服务基础架构，可加速数字化转型

作者：IBM

Peter Rutten　　Ashish Nadkarni

2017 年 8 月

IDC 观点

技术支持的业务战略，如数字化转型（DX），让企业能够拓展其在市场上的竞争优势。尽管数字化转型是一场颠覆性变革，仍需要企业将（技术）平台、（业务）流程、（数据）治理和（人员）人才有效且高效地组合在一起，从数据中收集深入及时的洞察，利用这些洞察优化业务运营，开发新颖的创新型产品和服务，提高客户忠诚度。

要从大型多样化的数据集中获取深入、及时、切实可行的洞察，需要企业采取创新方法来搭建技术平台。建议方法是在现代化的基础架构平台上部署当前及下一代的应用程序（应用）。当前一代的应用大多数是采购的现成应用，需要传统基础架构方法，并支持已确立的创收的业务运营。下一代应用专门针对面向未来的数字化转型计划开发，设计为云原生应用，使用更先进的开发方法，且通常依托更加前沿的计算技术进行部署。这意味着能够托管当前和下一代应用的现代基础架构解决方案必须支持卓越的性能和可扩展性，经过优化以实现数据整合与服务，支持普遍安全性，敏捷可靠，支持传统和更为先进的计算、开发和部署模型；且本机支持现代开源框架。

IBM 的 LinuxONE 是高度安全的数据服务基础架构平台的一个示例，旨在满足当前一代以及下一代应用的需求。IBM LinuxONE 是有以下诉求的企业的理想之选：

- **极致的安全性：**将数据隐私和法规监管问题视为最高需求的企业会发现，LinuxONE 内含业内一流的安全功能，如 EAL5+ 隔离、加密密钥保护和安全服务容器框架。
- **不折不扣的数据服务功能：**LinuxONE 专为支持结构化和非结构化数据整合而设计，且经过优化，可运行现代化的关系型和非关系型数据库。企业可以从“唯一事实来源”获得深入及时的洞察。
- **独特的均衡系统架构：**LinuxONE 拥有独特的共享内存和垂直扩展架构，因此性能不会降级并实现了扩展功能，适用于数据库和记录系统等工作负载，以及区块链等安全交易应用。

一些企业及外包服务和云服务提供商需要高性能、极致扩展和高度安全的数据服务和整合基础架构平台，以便运行对其数字化转型计划至关重要的当前和下一代应用，而 LinuxONE 将是他们的绝佳选择。

市场概况

企业着手开展数字化转型计划，以期扩展当前及未来其在市场中的竞争优势。数字化转型是一项技术支持的业务战略，但通常极具颠覆性，因为它需要企业“在继续照常运营业务的同时对自身进行重塑”（即在维持现有来源的同时搜寻新的收入和优势来源）。数字化转型要求企业不仅能处理尽可能多的数据，还能够将（技术）平台、（业务）流程、（数据）治理和（人员）人才有效且高效地组合在一起，从数据中收集深入及时的洞察。此外，还要能够利用这些洞察优化业务运营，开发新的创新型产品和服务，提高客户忠诚度。对于大多数企业而言，选择数字化转型只是时间问题。它不再是特大型企业的特权，而是同样适用于金融和保险服务、制造、零售及医疗保健等行业中的企业。缺乏以数据为中心的战略会让任何企业面临严重的生存威胁，无论是大型企业还是小型企业，提供产品还是提供服务。

数字化转型的基础架构

要从大型多样化的数据集中获取深入、及时、切实可行的洞察，需要企业采取创新型方法来搭建技术平台，其中包含应用程序和基础架构。从应用程序角度来说：

- 重塑公司意味着开发新的高端应用（也称为下一代应用）。下一代应用专门针对面向未来的数字化转型计划开发，设计为云原生应用，使用更先进的开发方法，且通常依托更加前沿的计算技术进行部署。
- 维持现有收入流意味着保留现行业务应用（也称为当前一代应用）。当前一代的应用大多数是采购的现成应用，需要传统基础架构方法，并支持已确立的创收的业务运营。

公司以现代化的共享方式投资于数据管理和基础架构并从中受益，此类基础架构特定于其应用程序产品组合的性质及其数字化转型计划的性质和目标。这种基础架构必须支持：

- 极致的性能和可扩展性
- 数据整合及应用间的数据共享
- 严苛的服务级别目标
- 普遍安全性，不仅仅局限于数据加密
- 多种计算模型，如裸机、虚拟化和容器
- 更先进的开发和部署模型，如 DevOps
- 开源云框架，如 OpenStack，以及自动化工具，如 Puppet 和 Chef

基础架构安全性包含加密及更多内容

多项 IDC 调研结果表明，在数据和基础架构方面，安全性是企业高管们最为关注的问题。现代基础架构的安全范式绝不仅仅是数据加密，而是具备普遍性和永续安全性，能够识别风险，抵御内部和外部威胁。企业从最近引起广泛关注的事件中（不乏一些惨痛教训）了解到，采取全面的安全方法意味着不光

要重视外部威胁，也要同样重视内部威胁。也就是说要确保能够未经授权访问基础架构各部分的任何人都不得“携带大量敏感数据离开”。企业的基础架构安全性应该是一个错综复杂的制衡系统，包括：

- 多层安全性 - 授权和认证模式，实时拦截、授权和/或阻止内部和外部用户、应用程序或网络级别的访问
- 水平隔离 - 限制对内部数据或者可从虚拟机 (VM)、容器或服务器实例及其备份和快照中访问的数据的管理访问权（现行做法和技术限制让 VM 管理员在获得管理权限后能够广泛访问敏感度极高的信息。）
- 垂直隔离 - 保护数据免遭同级环境中的访问，同时免遭此类环境的上级管理员的访问
- 访问匹配 - 将“需知内容”与数据的“敏感性指数”和可访问此类数据的系统的“实际访问权”相匹配
- 永续审计机制 - 检测模式，并可提醒管理员出现系统或数据违规情况，从而快速遏制违规范围
- 数据加密 - 数据加密，后跟与用户、应用和网络认证和授权模式分离的严格密钥管理模式

数据中心型基础架构方法的垂直扩展

IT 行业中有个说法，采取水平方式扩展到下一代应用程序架构是一个无所不能的终极解决方案，无论是在本地部署还是公共云中，当前一代应用程序面临的所有性能和扩展问题都将迎刃而解。水平扩展具有明显优势，但同时让企业面临风险，如：

- **数据一致性和资源利用率：**许多水平扩展应用，包括利用基于服务器的存储的应用以及云中运行的应用，均利用以异步副本或擦除编码副本的形式实施的终极数据一致性方案。这意味着，在任何时间的快照中，如果出现任何类型的中断或故障（如安全事件），都可能存在多个事实来源。此外，这类应用程序需要添加节点来扩展容量并提升性能，而这些节点彼此独立，这将导致资源未充分利用，长期下来会造成额外的运营开支。
- **集群缺陷：**使用内置或第三方集群软件让数据一致性和资源利用状况变得更加复杂，这些联网节点以自动化的主动-被动或主动-主动运营方式互相连接。正常情况下软件应该采取纠正措施，但往往做不到。另外，在快速操作让事态变得异常复杂时，人为引入的错误还会雪上加霜。

对于托管关键记录系统和高性能数据服务平台的某些应用程序组件的系统，采取垂直扩展方法具有一些优势。此类系统将更加便于：

- 在数据一致性和安全性方面管理单一事实来源，即便是处理内置终极数据一致性的数据库和应用程序也是如此
- 通过添加更多“核心”，缩短响应时间，支持随需应变的性能，且无需任何外部供应活动，便于在整个系统中实施单一的安全范式
- 通过跨所有虚拟机共享资源，更高效地利用系统

IBM LINUXONE

IBM 依托 Linux-only 技术推出了 LinuxONE 品牌，专门面向寻求全面设计解决方案的买方，该解决方案拥有独特的均衡多租户系统架构和行业领先的普遍安全性，并针对数据服务和任务关键型工作负载和应用程序进行了优化。因此，LinuxONE 最适合：

- 因数据隐私和法规监管要求，或因公共云服务提供商达不到其严苛的可用性、性能和可扩展性目标，选择在本地运行业务应用程序的公司
- 需要安全的多租户平台来托管应用程序，希望通过提供非凡的服务质量从大型公共 CSP 中脱颖而出的 MSP 和 CSP

最后，IBM 还展示了 LinuxONE 能够充当在云中运行区块链的理想平台。例如，运行在 IBM Cloud 中的 LinuxONE 系统展示了 LinuxONE 能够充当区块链的绝对安全且功能强大的数据服务云平台。

LinuxONE 架构

IBM 将 LinuxONE 设计为一款高度可扩展的数据服务和事务处理平台，与运行 Linux 的基于 x86 的标准服务器截然不同。相反，LinuxONE 实现了以下两方面的强强联合 - IBM Z 平台的企业品质和 Linux 及开源软件的开放性。

基于 IBM Z 平台设计

LinuxONE 是一款经过检验的任务关键型硬件平台（IBM Z），具有独特的共享内存和垂直扩展架构。I/O 通道中专用的 Power 和 RAS 核心以及用于 I/O 编排的 SAP 使平台能够在不延长等待时间的情况下处理大量 I/O，毫不费力地应对每秒数百万的事务量。这让 LinuxONE 非常适合运行有状态的工作负载，如数据库和记录系统。

基于 Linux 的开源软件堆栈

LinuxONE 基于 Linux 的强大软件堆栈可运行大多数开源软件包，如数据库和数据管理（如 MariaDB、PostgreSQL、MongoDB 和 Apache Spark）、虚拟化和容器平台（如 KVM、Docker）、自动化和编排软件（如 OpenStack、Puppet、Node.js、Juju 和 Chef）以及计算密集型工作负载（如区块链）。

LinuxONE 性能和扩展功能不会降级（即使利用率已达 100%），能够简化解决方案，削减额外成本，而许多 IT 架构认为需要这些额外开销来应对利用率达 50% 时的性能降级情况。此外，LinuxONE 采用 Ubuntu 系统，支持轻松构建、建模、部署和管理企业级向外扩展的集群和可扩展的云架构。最后，IBM 将 LinuxONE 设计为可根据公司规范进行定制订购，且 LinuxONE 已经过全面测试，能够抵御地震、火灾和洪水等灾难。

LinuxONE 安全性

LinuxONE 是市场上为数不多的内置安全性的平台之一，且“始终可用”，客户购得系统后可享受全部的安全功能。固件级别的安全性可从组合风险中排出一级风险。我们会在后面的章节中讨论这些功能，正是它们让 LinuxONE 在多个领域独树一帜。

LPAR 级别的 EAL5+ 隔离

此安全的多租户功能在同级环境之间提供隔离，让企业和服务提供商受益匪浅。此外，LinuxONE 通过 4 级 FIPS 140-2 认证，这意味着，如果防篡改封条遭到破坏，系统会自动写入零来覆盖数据，从而保护密钥。

IBM Secure Service Container

IBM Secure Service Container (SSC) 是一款用于在 LinuxONE 上安全部署软件设备的框架。Secure Service Container 设备部署在以“SSC 方式”配置的 LinuxONE LPAR 上。Secure Service Container 技术将提供：

- **业界领先的同级隔离：**Secure Service Container 技术利用 LinuxONE 的 EAL5+ 认证的 LPAR 隔离，在单一空间内实现了设备环境的近乎“空隙”的隔离，模糊了底层基础架构的工作负载。
- **垂直隔离和保护数据免遭特权用户访问：**对于以“SSC 方式”LPAR 配置的设备，在设计时禁用了通过 shell 和命令行界面的直接 (SSH) 操作系统访问。仅允许通过明确定义的 RESTful API 和 Web 界面进行设备管理和通信，阻止具有较高系统权限的用户访问，仅获得 Secure Service Container LPAR 及其中运行的设备授权的用户有权访问，从而，保护设备的数据和执行环境免遭无意或恶意内部威胁。
- **传输中和静止的数据和代码的机密性：**禁止对 Secure Service Container 设备的直接内存访问，实施了多层加密和签名，确保在未加密的情况下任何数据位都不会离开设备。
- **验证设备代码，以降低篡改或恶意软件风险：**Secure Service Container 设备在软件部署前，在可靠的固件引导序列中创建之初就便受到保护，可通过签名验证防止篡改。

Secure Service Container 框架在初始阶段就启用了 IBM 提供的解决方案，如 IBM Cloud 中的 IBM Blockchain Platform，其中包含用于托管任务关键型企业级区块链数据和链代码的业务网络所需的加密和数据隐私。

未来，Secure Service Container 框架旨在供用户在 LinuxONE 上的 Secure Service Container 实例中本地部署基于 Docker 容器的应用程序。这使得用户的应用程序能够利用 Secure Service Container 技术，同时在单一 LinuxONE 空间内动态向上扩展至数百万个 Docker 容器，并将这些容器与用户的企业级、跨平台 Docker 和 DevOps 策略相集成。

创新型 LinuxONE 用例

LinuxONE 是一款设计复杂的解决方案，在数据服务和有状态的应用程序方面表现卓著，其拥有垂直扩展环境，内含共享内存及通过高速光纤网的共享处理，而非运行于通用 Linux 服务器或虚拟机的水平扩展集群上。后续章节中讨论的用例展现了 LinuxONE 的实力。

LinuxONE 上的数据库即服务

最近，采用开源关系型和非关系型数据库的企业数量激增，很大程度上是因为要加速开发下一代应用。IBM 正在将 LinuxONE 推向那些希望为结构化和非结构化数据管理部署“即服务”环境的公司。LinuxONE 的安全性、可扩展性和高性能使其成为部署数据库即服务（DBaaS）的理想平台。客户可以从多个角度看待 DBaaS：

- **对 DBaaS 环境的完全控制：**这是一个自助服务模型。IBM 提供了参考架构，帮助客户利用 Trove 在本地部署的 OpenStack 环境中设置 DBaaS。客户可利用此参考架构快速启用 DBaaS，并运行 DB2、PostgreSQL 和 MongoDB。客户还可以选择利用 LinuxONE 平台上的其他开源和技术选项创建自己的 DBaaS 路径。
- **预配置的本地私有云：**这将是一个比之前更加规范的解决方案，因为它会切实加速部署，并利用 IBM LinuxONE Secure Service Container 框架。IBM 正在探寻在 LinuxONE 上交付此解决方案。
- **托管的外部云：**这本质上是一个自助服务模型，其中数据托管在 LinuxONE 上以实现卓越的扩展和安全功能。IBM 正在探寻在 LinuxONE 上交付此解决方案。

LinuxONE 上的区块链

区块链在受到严格监管的行业中兴起（如金融技术），在这些行业中，不折不扣的交易安全性是重中之重。因此，这些行业需要一个面向交易的（即高度可扩展的）计算基础架构平台，此类平台围绕严苛、普遍的安全模式设计，而这些正是端到端区块链部署所必需的。

IBM Blockchain Platform 是 IBM Cloud 上的一款 IBM 管理的区块链即服务。IBM Blockchain Platform 是基于 Hyperledger Fabric V1.0（Linux Foundation 托管的一个 Hyperledger 项目）的企业就绪型区块链服务。该服务支持开发者在 IBM Cloud 上快速构建和托管高度安全的生产区块链网络。此服务基于 LinuxONE，在安全性、性能和数据隔离规范方面均达到业内最佳水平。它提供经验证的审计环境以实现合规性和取证。

Cognition Foundry 帮助初创企业利用企业技术开拓创新

Cognition Foundry 致力于指导初创企业和小型企业获取架构设计洞察，进行应用程序开发，同时支持他们访问 LinuxONE 上可用的丰富计算资源，最终为积极开拓进取的创业者提供公平的竞争环境。Cognition Foundry 将其方法描述为“推动企业 IT 访问民主化”，允许小型用户从一开始就使用与政府和财富 500 强企业相同的技术。

Cognition Foundry 的开发者团队帮助初创企业开发和测试代码，确保他们从设计精密的开放式 IT 基础架构中获得最大收益。Cognition Foundry 利用其庞大的网络，让企业新星能够访问企业架构、设计和业务技能，帮助他们赢得市场竞争，同时控制 IT 成本。

鉴于开源软件在初创领域的普遍运用，LinuxONE 能够运行开源软件是 Cognition Foundry 的一个巨大优势。能够在平台上垂直扩展，意味着支持在不添加基础架构的情况下大规模扩张。作为聚焦于最优资产管理的服务提供商，它可为企业带来巨大助力。

Cognition Foundry 的客户包括 Plastic Bank 等组织，Plastic Bank 与发展中国家的社区协作回收塑料瓶，以换取一些有用的收益。

IBM 面临的挑战和机遇

有了 LinuxONE，IBM 可以宣称已面向未来的工作负载和应用程序搭建了强大的系统，而其中的两个关键技术便是区块链和开源数据库。通过 LinuxONE，IBM 可以尝试复制 IBM Z 长期以来的成功模式。IBM 现在寻求拓展 LinuxONE 的价值，将其推广到广泛的客户、行业、地理位置和工作负载，让它们尽享如下共同的优势：

- 多租户可扩展性，可在共享相同数据的同一机器上支持多样化的生产和分析工作负载
- 更低的能耗和许可成本，更高的性能和最优的安全性，支持在更小的基础架构空间内整合工作负载
- 可靠且始终可用的数据服务平台，企业可“放心地托管业务”，充分利用数据，并向客户提供更多服务

在与客户的对话中，IBM 应将焦点转离将 LinuxONE 与基于 x86 的通用服务器集群进行直接比较。同时，不应将其仅视为面向一两个工作负载的支持平台，而是一个具有业内领先的安全性、可扩展性和性能功能的全方位平台。此外，不能再将讨论聚焦于 LinuxONE 作为托管所有工作负载的平台，而是应该强调它是一个提供唯一事实来源的数据服务平台，具备最高级别的安全性，在业内独一无二。

结论

不论是本地部署还是云中部署，平台的选择都至关重要。平台必须提供安全的多租户环境，其中凭证得到妥善保护，同级环境间彼此高度隔离，固件级别内置加密，且加密密钥由硬件加以保护。它必须提供垂直安全性，让诸如敏感客户记录和机密信息等数据免遭内外部威胁侵扰。最后，它必须提供普遍的安全性（即整个系统得到全面保护），并提供彼此隔离的硬件分区。

IBM LinuxONE 结合了商用 (IBM Z) 和开源 (Linux) 系统的优势，具备其他产品无可匹敌的安全功能，并且针对记录系统工作负载实现了可扩展性。总而言之，IBM LinuxONE 是一个值得投资的平台。

关于 IDC

International Data Corporation (IDC) 是全球首屈一指的信息技术、电信和消费科技市场情报、咨询和活动服务供应商。IDC 致力于帮助 IT 专业人士、业务高管和投资机构以事实为基础，做出有关技术采购的决策，制定业务发展战略。IDC 在全球拥有超过 1,100 名分析师，他们从全球、区域和本地视角对 110 多个国家或地区的技术与行业机会和趋势提供专业化的指导意见。50 多年来，IDC 一直为客户提供战略洞察，帮助他们实现关键的业务目标。IDC 是 IDG 旗下子公司，IDG 是全球领先的技术、媒体、研究及活动服务公司。

全球总部

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter：@IDC
idc-community.com
www.idc.com