位置、位置、位置：云端数据安全与隐私的重要性

通过提供敏捷的云体验，取悦客户

IBM **Cloud**

IBM

概述

对企业及其客户而言，数据是最有价值的商业资产，他们必须保护数据免于遭受非授权访问。通过结合利用始终可用且安全的数据和富有洞见的数据分析，您可以推动业务创新，提高客户满意度和忠诚度，更重要的是，提高在市场上的竞争力。

在整个生命周期中管理数据，同时满足业务、隐私和安全法规要求，这必须是您在云环境中的头等大事。正因为此，在安全、隐私和云部署方面拥有深厚专业知识的值得信赖的业务合作伙伴至关重要。IBM 通过使用广泛的行业特定产品和服务成功帮助客户迁移到了云端，这些产品和服务背后有 IBM 授权的 2500 多项云技术专利的支持 。

全球云计算的本质意味着数据的物理位置非常重要，并且这种重要性日益凸显。每秒都有跨国商业交易在发生。在一个地区创建的大数据可以跨国界在其他地区进行存储、处理和访问。使用您的数据的最终用户、客户和业务合作伙伴可能来自全球各地。

用户离存储数据的数据中心越近，云工作负载的性能就越高。这条规律同样适用于云提供商。云提供商希望确保您的数据能在全球范围内高效移动，并尽可能降低延迟率。意识到这一点后，IBM 重金投资构建、维护和发展敏捷的全球云网络支柱，该网络可以在全球范围内传输公有和私有流量，帮助您打造卓越的客户体验。

数据的位置至关重要

企业经常将业务工作负载迁移到云端，以确保数据始终可用，同时确保快速、可靠地将数据交付给全球各地的客户。由于不了解通用可访问性、有保证的正常运行时间服务水平协议和高速网络连接等概念，数据的实际位置常被忽视。忽略数据物理位置会导致上传和下载速度变慢、服务延迟、生产力下降、客户和业务流失。更重要的是，数据所在的位置对于您保护数据隐私和满足数据保护监管要求至关重要。

虽然云提供基础架构即服务（IaaS），但存储在云端的数据驻留在物理存储设备上，动态数据也要通过物理网络传输。甚至云应用所用的数据（即，正在使用的数据）也需要得到保护。IBM Cloud 提供内置的安全解决方案，旨在在整个生命周期保护数据。

在评估全球网络的潜在性能时，通常使用光纤中的光速来估计用回程时间（RTT）衡量的最佳潜在响应时间。

云工作负载需要一个灵活、安全、响应迅速并且在全球范围内都有本地支持的基础架构。IBM 了解这些业务云的需求，并为此投资建立了一个全球网络，该网络在 6 大洲 6 个多区域分部提供 60 多个数据中心。IBM 的云网络符合法规要求，确保数据中心内应用工作负载和数据的安全性。IBM 的数据安全解决方案能保护静态数据、动态数据和使用中的数据。

IBM Cloud 提供 IBM Key Protect，后者提供自带密钥 (BYOK) 和 IBM Cloud Hyper Protect Crypto Services 等收益，帮助您保留自己的密钥 (KYOK)，用于加密云数据。

IBM Key Protect (BYOK)

该产品是多租户密钥管理服务（KMS），由 IBM 控制的 FIPS 140-2 Level 3 硬件安全模块（HSM）提供密钥库。借助 IBM Key Protect，客户能够在云端保留和管理他们的密钥，IBM 提供运营保证，确保 IBM 不会访问这些密钥。

IBM Cloud Hyper Protect Crypto Services (KYOK)

提供二合一服务（即，内置硬件安全模块的 KMS）。该产品是单租户密钥管理服务，由客户控制的 FIPS 140-2 Level 4（最高级别的可用性认证）硬件安全模块提供密钥库。借助 IBM Cloud Hyper Protect Crypto Services，客户能利用自己控制和管理的硬件安全模块保护自己保留的密钥；该服务提供 IBM 无法访问密钥的技术保证。

客户场景

在接近客户的地方部署云工作负载，以获得最佳响应时间，这是企业的理想情况。当今的全球数字经济意味着，大多数企业的业务遍布全球各地，他们需要确保客户无论身在何地，都能获得愉快的业务体验。在打造最佳体验时，IBM Cloud 的全球覆盖优势为企业提供了机会，让他们能够将工作负载部署到靠近全球客户群的几个位置。

让我们来看看一家总部位于加州圣何塞、客户位于法国巴黎和新加坡的全球性企业。对于该企业来说，理想情况是将工作负载部署在尽可能靠近这些城市的位置，甚至直接部署在这些城市。或者，企业也可以选择一个不那么理想的解决方案，只在圣何塞部署工作负载；这样，巴黎的客户就会像新加坡的客户一样，延迟响应时间。凭借广泛的网络、多区域分部功能和高速基础架构，IBM Cloud 能帮助该企业以安全、快速和及时的方式服务全球客户。

IBM Cloud 全球数据中心

保护服务安全性，并为客户提供服务

IBM Cloud 数据中心和网络接驳点 (PoP) 与一个全球网络支柱互联，该支柱负责传输往返于服务器的公有、私有和管理流量。这个全球网络在数据中心和网络接驳点之间提供超过 2,600Gbps 的连接速度，以及高达 20TB 的免费出站带宽（出口流量）。

此外，网络接驳点还提供超过 2,500Gbps 的传输速度以及与互联网的对等连接。访问 IBM Cloud 服务器时，该网络能够通过一个网络接驳点将您快速接入 IBM 全球支柱。客户和最终用户可能会经历更少的网络跳点（同时，还能使用 IBM Cloud 控制的更直接的路径）。当用户请求访问 IBM Cloud 服务器的数据时，数据将传输到最近的网络接驳点，然后数据将被传递给另一个提供商，由后者负责其余的数据传输工作。

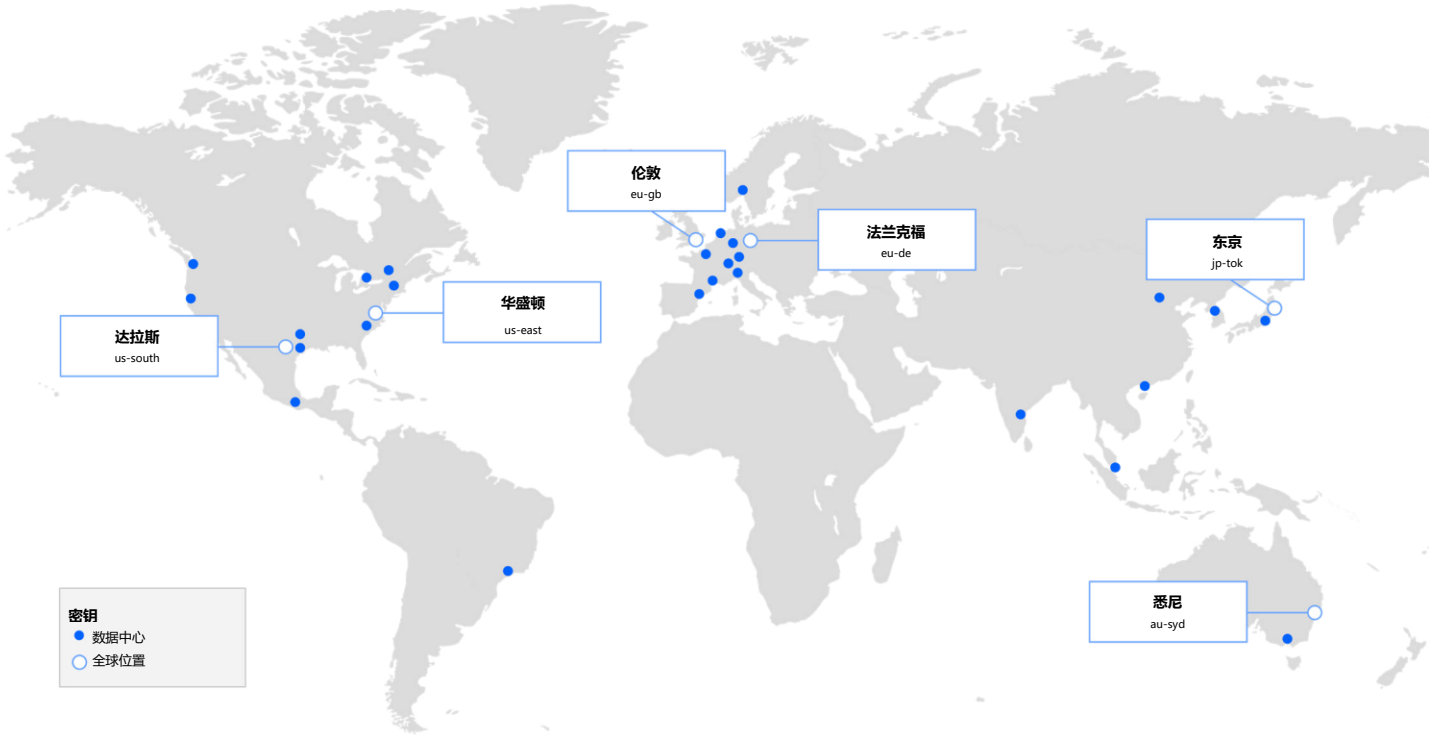


图 1：IBM Cloud 的全球数据中心和多区域分部

安全、快速地移动数据

确保数据在迁移期间以及整个生命周期的安全性并保护数据，这是企业的一项关键优先事项。IBM Cloud 利用与本地基础架构相同的软件技术和专业知识，简化并保护云迁移之旅。IBM Aspera on Cloud 和 IBM Cloud VPC 就是两个技术示例。

IBM Aspera on Cloud

通过利用 IBM Aspera on Cloud，无论网络条件如何，企业都可以以最大速度可靠地移动任意类型和大小的文件和数据集。IBM Aspera on Cloud 利用已获专利的网络优化型专有协议 Fast and Secure Protocol (FASP)，安全地移动数据，其速度通常比 Transmission Control Protocol (TCP) 快一百倍以上。使用 FASP 传输数据是加密的，以保护您的静态数据和动态数据。该解决方案旨在快速、可靠、安全地在云端和本地资源之间移动大型文件和数据集。

IBM Cloud Virtual Private Cloud (VPC)

基于 IBM Cloud Virtual Private Cloud (VPC) 构建云原生三层应用，IBM Cloud VPC 利用私有云的高级安全功能和公有云的敏捷性和便捷性，在 IBM Cloud 中提供了一个受保护的空间。这样，您就能在逻辑隔离网段中控制虚拟网络，快速部署和管理计算资源、存储资源与联网云资源。IBM Cloud VPC 增加了 IBM Cloud 的安全功能，并通过使用安全组和访问控制列表为应用工作负载和数据创建更安全的环境。

为了确保企业工作负载和云原生应用持续可用，IBM Cloud 拥有多区域分部 (MZR)，每个 MZR 由三个可用性区域组成，并添加了容错功能，您可以在单个 VPC 中使用多个子网构建工作负载，从而利用容错功能。此外，IBM Cloud Virtual Server for VPC 还为网络密集型应用、模拟或内存缓存提供了一个优秀的解决方案，其通用概要文件提供高达 80Gpbs 的网络性能。

多区域分部和可用性区域

在 60 多个数据中心中将工作负载部署到 6 个分部和 18 个可用性区域

IBM Cloud 正在不断扩展其全球足迹，确保您能够在客户所在之处与他们会面。我们的 IBM Cloud 多区域分部在周围 6 英里范围内部署了三个甚至更多数据中心。这些数据中心位于邻近位置，以确保高可用性和弹性。它们提供一系列全面、一致的服务来满足企业级工作负载需求。MZR 包括完整的 IBM Watson 和 IBM Cloud 堆栈（IaaS、CaaS、PaaS、认知和数据），并且与两个接驳点互联，以提供最高的接驳点弹性。

高速城区互联将应用的跨区通信延迟缩短到 2 毫秒以内。IBM 云服务（如云对象存储、容器、API 和具有适用权限的反识别数据）可以感知区域，并利用该解决方案减轻应用提供商的负担。

IBM Cloud 多区域分部

可用性和弹性

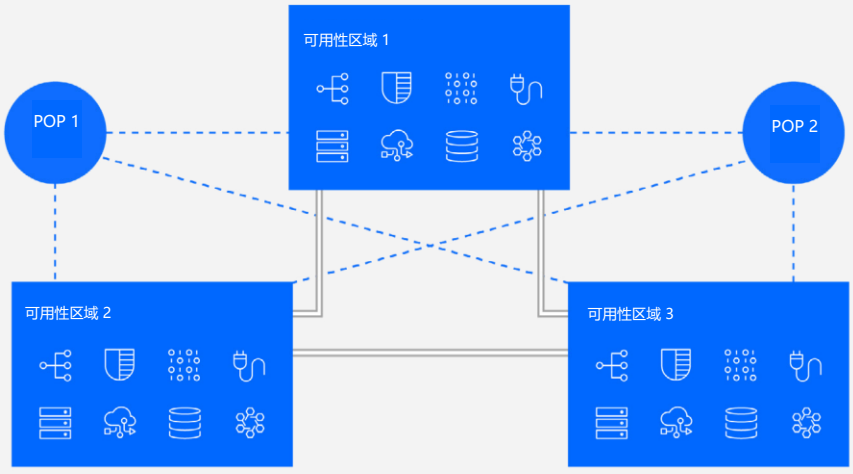
利用全系统容错功能，保持业务运行。

高可扩展性

利用灵活的功能，适应不断变化的企业生产需求。

低延迟

利用响应速度更快的应用，同时更快地移动数据，获得更好的业务结果。



我们的责任

数据是我们这个时代最有价值的商业资产。它是世界上出现的一种新自然资源，且数据的数量、形式和价值都在呈指数级增长。现在，全球任何复杂系统中发生的每个行动和交互、每个决策和关系以及每个事件都用数据表示。面对如此深刻的变革，企业不得不采用基于云的新技术和业务架构以及新的业务流程、技能和互动形式。云提供商争先恐后地利用数据挖掘潜在的商业价值。与此同时，他们也不能忽视个人、企业和社区对安全性、信任、隐私性、工作、技能以及数据的基本期望，这里的数据包括他们自己拥有的数据或者提供商从他们那里收集到的数据。

数据所有权和隐私性

IBM Cloud 相信我们能够将客户数据中挖掘的独特洞察力转化为竞争优势，未经客户明确同意，我们不会共享这些洞察力。我们采用安全实践帮助您保护数据，包括使用加密计算、访问控制方法和专有的同意管理模块，这样，我们能够限制对授权用户的访问。

我们提倡采用强大且创新的手段来加强隐私和数据保护，我们将继续投资加强隐私保护的技术。我们率先实施了针对多款 IBM Cloud 服务和产品的《欧盟云服务提供商数据保护行为守则》，获得了《美国-欧盟隐私法规》和《亚太经合组织跨境隐私规则体系》的安全认证。

IBM 是第一家提供超级数据保护并全力遵守欧盟《通用数据保护条例》的云提供商。IBM Cloud 符合《通用数据保护条例》要求。

数据流和访问

在这个由数据驱动的社会中，保护您的数据隐私至关重要，而这也是 IBM Cloud 重视并为之奋斗的目标。IBM Cloud 投资重金，在全球各地建设云数据中心，让客户能够灵活地决定在何处存储和处理他们的数据。我们认为，这些决定通常应该由客户来做、而非由政府命令驱动。

数据安全性和可信性

IBM Cloud 利用安全实践和技术，帮助您保护工作负载和数据。IBM Cloud 能保护静态数据、动态数据和使用中的数据。我们站在应用人工智能功能的最前沿，以便从容应对新兴的数字威胁。我们不为任何政府机构在我们的产品中设置“后门”，也不向任何政府机构提供源代码或加密密钥。您是唯一拥有加密密钥的一方，甚至 IBM 也不能访问这些密钥。IBM 一直以来都在为全球数千家企业提供经过现场验证和检验的安全解决方案，这也为 IBM Cloud 的安全性奠定了基础。

资源

在本地部署，在全球扩展。有关 IBM Cloud 数据中心的更多信息，敬请访问：

https://www.ibm.com/cloud/data-centers/

Never neglect your network.了解如何设计您的云平台，推动流量、保护数据。了解有关 IBM Cloud Network 的更多信息：

https://www.ibm.com/cloud/network

数据经济正在快速演变。了解我们有关数据责任的观点：

https://www.ibm.com/blogs/policy/dataresponsibility-at-ibm/

免费咨询热线：400-810-1818 转 2395

服务时间：9:00-17:00

IBM Cloud
New Orchard Road
Armonk, NY 10504

美国印刷
2020 年 4 月