出品方：

IBM

安全混合云

傻瓜系列

Wiley 出品

借助混合云推动转型

发现 API，释放
核心服务的价值

优化 IBM Z®，用作
混合云平台

Judith Hurwitz

Daniel Kirsch

IBM 限量版

安全混合云

IBM 限量版

作者：Judith Hurwitz
和 Daniel Kirsch

傻瓜系列
Wiley 出品

《“傻瓜系列”之安全混合云®》，IBM 限量版

出版商：

John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN：978-1-119-52795-4 (pbk); ISBN：978-1-119-52798-5 (ebk)

美国印刷

10 9 8 7 6 5 4 3 2 1

出版商致谢

感谢以下人员为将本书推向市场提供大力帮助和支持：

项目编辑：Carrie A. Burchfield

编辑主任：Rev Mengle

策划编辑：Steve Hayes

业务开发代表：Sue Blessing

IBM 贡献者：Sherri Hanna、Mark Schultz、Rosalind Radcliffe、Kyle Charlet、Nathan Dotson、Diana Henderson 和 Dan Weigand

制作编辑：Magesh Elangovan

目录

导言

欢迎阅读*《傻瓜系列之安全混合云》*IBM 限量版。越来越多的企业借助混合云实现业务转型，以满足不断变化的客户需求。企业发现，要想满足客户需求，必须利用高度安全的 IBM Z 平台，支持任务关键型工作负载，例如事务管理应用。Z 平台多年来一直都在不断变革。z/OS、LinuxONE、开放式 API 以及 Kubernetes 的强强组合，使 IBM Z 成为混合云领域的关键合作伙伴。企业可以将 IBM Z 环境转变成安全的私有云。此外，在 IBM 的公有云中，企业也可以借助 IBM Z 的安全服务，保护数据和应用。

关于本书

本书旨在帮助读者了解安全云的价值，以及安全云如何支持企业实现技术和业务目标。本书介绍了在混合云环境中确保安全的重要意义，以及 IBM Z 平台及其服务如何在这方面为企业保驾护航。

假定事项

本书中的信息对许多人而言都非常有用，不过我们认为，这些信息对于满足以下条件的读者可能更为有用：

- 熟悉云计算，需要了解混合云的作用及其与数据中心和 IBM Z 的关系。
- 正在规划长期云战略，想要了解私有云的价值以及私有云如何支持企业实现业务目标。

- 希望了解安全服务如何在企业迁移至混合云的过程中提供帮助。
- 希望了解云计算的所有要素是如何组合在一起的，是如何支持软件开发、部署、安全及合规的。
- 作为业务领导，希望采用最重要的新兴云技术，尽可能地发挥创造力和创新性。

本书中的图标

在整本书中，以下图标用于指示重要信息：


牢记

该图标用于标示您需要记住的重要信息。


提示

该图标用于标示您需要特别注意的信息。


警告

该图标用于标示为避免某些问题您需要特别注意的内容。

参考资料

本书篇幅有限，无法提供有关某个主题的所有详细信息，如欲了解本书范围之外的更多信息，请参考以下资料：

- **混合云：**http://ibm.biz/ZHybridCloud
- **数据安全性：**http://ibm.biz/DataSecurity
- **DevOps：**http://ibm.biz/ZDevOps
- **IT 卓越运营：**http://ibm.biz/ITOpExcel
- **Z 案例研究：**http://ibm.biz/ZCaseStudies
- **互联大型机：**http://ibm.biz/TheConnected Mainframe

本章概要

» 定义混合云
» 使用混合云作为战略模式
» 借助大型机推动混合云战略

第 1 章
混合云的商业价值

企业计算的格局不断迅速发展变化。仅仅几年前，许多企业还在犹豫是继续使用数据中心，还是迁移到公有云或私有云。而现在，他们已经认识到，要实现持续创新，需要支持多种计算模式。

业务颠覆大潮为混合云的采用推波助澜。纵观各行各业，与规模较大的传统企业相比，新型竞争对手善于利用各种技术，更迅速、更敏捷地采取行动。当然，这些技术同样也使传统企业受益，支持他们充分发挥自己在知识产权、行业知识和现有客户群等方面的优势。

混合云现已成为架构框架，支持企业选择最适合业务需求的部署模式。混合计算的灵活性使企业能够随着业务需求的变化而改变部署模式。

为了不输给敏捷的竞争对手，企业需要重新思考传统的服务交付方式。要想实现这种转变，关键在于优化 IT 环境，获得所需的安全性、高速度和灵活性。而混合云就是企业发展与变革的有力保障。

在本章中，我们将定义混合云，说明它为何对于企业至关重要。然后，我们将介绍成功混合云战略的关键组成部分，以及大型机为何是该战略的主要要素。

何为混合云?

当今的企业需要应对诸多复杂的问题，包括服务级别要求、安全与合规，以及内部数据存储规则等。公有云服务并不总能提供必要的监督，保护业务完整性。

而混合云则可以满足现代业务需求，分布式系统支持企业为各种任务选择合适的服务。这种环境称为*混合云架构*，如图 1-1 所示。

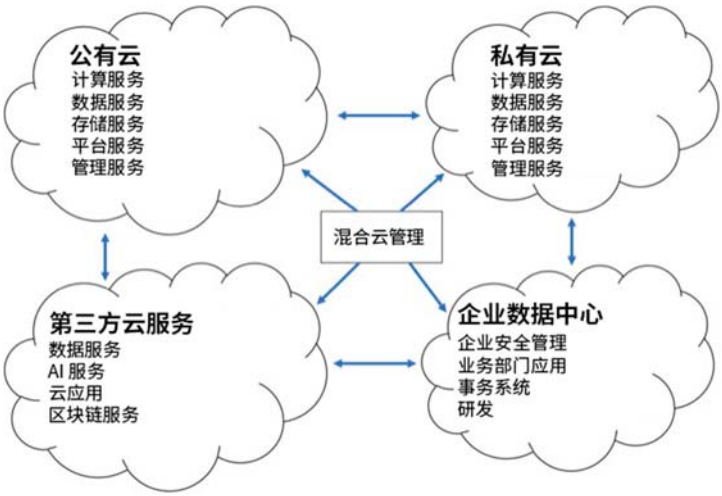

图 1-1： 混合云架构。

牢记

混合云环境将公共、私有或管理计算服务的组合与传统 IT 整合在一起，构成了虚拟计算环境。该环境的目标是在服务与灵活性之间取得平衡，以满足客户期望。所有服务都必须接受统一管理，就像它们是单一环境一样。

混合计算模式既具备卓越的灵活性，又表现出高性能，这种独特的优势使其成为众多企业的首选平台。混合架构将公有云的开放性、私有云的安全性以及数据中心的强大能力结合在一起。这种强强组合使企业能够将现有投资与易于扩展、高度灵活的模块化服务融合在一起，满足客户期望，支持创新和效率需求。

公有云与私有云之比较

所有云各不相同。公有云服务可从市场上获得，任何人都可以按需购买服务包。私有云服务则位于防火墙后面的企业数据中心内。而管理服务则可以存在于这两种环境中。

定义公有云

公有云已经发展了很多年。早期的公有云用例旨在帮助开发人员或企业根据当前需求，逐步增加计算或存储能力。然而，在过去五年中，公有云提供商增加了大量的服务，包括安全性、镜像磁盘、DevOps 等，范围十分广泛。

这些服务在公有云背景下均属于管理服务范畴。与传统的公有云一样，这些管理服务也采用托管模式，使用者按使用量付费，使用服务执行特定功能。

定义私有云

私有云是在防火墙之后提供单一平台的企业级解决方案。与传统的数据中心环境不同，私有云通常基于软件定义的接口，支持其中的服务以模块化、可扩展的方式运行。由于私有云位于防火墙之后，因此提供了可控保护层；它自身包含所需的功能，能够提供众多客户要求的服务级别保证。

例如，IBM Cloud Private (ICP) 平台中包含统一的安装程序，可用于快速建立由主节点、工作节点和代理节点组成的基于 Kubernetes 的集群。它旨在管理和控制环境中的应用。

混合云使企业告别“一体适用”模式，转而根据每个业务部门的具体需求做出适当选择。例如，某个业务部门中的开发人员可能发现某个公有云服务与自己手头的任务非常匹配。而另一个部门的专业知识和经验决定了他们可能需要不同的公有云。混合云方法使每个部门能够根据自身需求选择合适的云服务。在整个企业中，一个组织可以使用多达五到六个不同的公有云，并在众多云平台上运行多个 SaaS 应用。

借助混合云，企业可将数据、应用、业务规则和安全服务作为一组相关功能和服务进行管理。这种方法支持一组服务协同工作，以满足业务需求。混合云支持企业在不影响安全性、治理或性能的前提下灵活地进行创新和转型。

混合云即战略模式

大多数企业都致力于实施多云战略。许多企业利用各种公有云和管理服务来开发应用、分析数据和运行关键工作负载。此外，这些企业还出于安全和成本的考虑，使用私有云服务。对于大多数企业而言，云不再是达成目标的手段，而是一种成熟的战略性职能。

精心制定的混合云战略必须要考虑如何保护企业的知识产权以及遵守企业和政府的法律规章。还必须考虑以下因素：

- 财务限制和预算
- 安全性
- 可扩展性
- 运营管理
- 与 DevOps 和 DevSecOps 环境的整合
- 战略数据的管理

考虑到所有这些因素，必须采用灵活的框架，支持混合云环境。该平台必须能够以始终如一、可预测的方式管理云端的所有要素。这样反过来又会推动及时交付服务和快速实现创新，从而满足客户需求，在竞争中不落下风。

牢记

混合框架必须是可扩展的。随着企业对数据需求的不断增长，平台也必须与时俱进，持续扩展。这既适用于本地数据，也包括公有云和私有云中的数据。平台必须能够确保数据安全。数据泄露会让企业失去客户信任，并造成严重的经济损失。而支持混合云的平台则能够围绕所有敏感数据建立一道坚不可摧的防线。最后，该平台必须通过简化并加速整个平台中新应用的开发与实施，为创新提供强大动力。

了解为何大型机对于混合云战略至关重要

IBM Z 大型机是支持混合云的关键平台。它通过以下方式，助推混合云战略的实施：

- **确保实现一致、稳定的环境：**大型机具备 99.999% 的高可用性，支持云应用所需的稳定性和可靠性。
- **提供可扩展性：**大型机可向上扩展而非向外扩展，因此，当平台因混合云创新而发展壮大时，互动系统可实现无缝的数据扩展。
- **保证数据安全：**IBM Z 在硬件、软件和云服务层面对所有数据进行普遍加密 — 涵盖静态存储的数据和动态传输中的数据，从而给云环境带来无与伦比的安全性。
- **提供快速开发能力，为创新赋能：**IBM Z 提供一个框架，用于支持跨平台快速开发、测试和部署云服务和应用。

目前的大型机旨在与公有云、私有云和其他开放技术协同工作。作为互联生态系统的组成部分，IBM Z 可与外部系统轻松整合，而且与新的应用开发和部署模式兼容。

如果在 IBM Z 上运行核心记录系统，那么在该平台上很可能已经积累了数十年的宝贵数据。通过将 IBM Z 与混合云整合，就可以利用这些数据构建新应用，推出新的创新服务，以及提高客户参与度。混合云正迅速成为部署新服务的标准平台。互联大型机有助于增强计算环境的安全性、稳定性和灵活性。

本章概要

- 了解需要安全云的理由
- 保护数据安全
- 了解安全云的优点
- 利用 IBM Z 安全服务

第 2 章
IBM Z 即安全云平台

管理数据和知识产权对于企业的生存和发展至关重要。因此，安全必须在所有企业战略和计划中占据核心位置。无论是从监管还是法律的角度而言，客户和员工数据都必须受到妥善保护。如果客户感到自己的数据没有得到保护，就不会再与相关企业开展业务往来。随着云基础架构成为诸多企业的主要开发和部署平台，安全和治理自然成为重中之重的任务。

为何需要安全云

企业越来越担心针对信息的网络安全威胁，而信息是决定企业与客户及合作伙伴关系的命脉。企业中的宝贵数据分布广泛，无处不在，包括内部和云端的电子表格、文档、应用和数据库等。因此，安全不再只是首席安全官操心的问题。安全现已成为所有企业的董事会层面关注的主要问题。企业关注安全的主要原因有二：担心数据泄露和企业品牌声誉受损。

数据泄密的后果

数据泄密可能带来灾难性的经济损失。以一家可再生能源公司为例，该公司发明了一种设计太阳能电池板的新方法，使用这种方法制造出的太阳能电池板比竞争对手的产品更轻巧、更高效。与提供商和各种供应商共享工程计划固然重要，但数据安全也必须考虑。如果此类计划落入不法之徒手中，该公司可能会尽失知识产权（IP）。如果该公司未能妥善保护知识产权，很有可能在一夜之间破产。

名誉受损的影响

警告

名誉损失的后果几乎与直接的财务和知识产权损失一样严重。由于需要保护数据，越来越多的合作伙伴和客户持续重新评估业务往来企业。如果某企业遭遇数据泄密，许多客户及合作伙伴会重新考虑是否继续与之开展业务。

以某银行为例，他们成为一场极为狡猾而且针对性很强的网络攻击的受害者。即使客户没有遭受任何经济损失，也很有可能会重新考虑是否继续与该银行进行合作。如果您在该银行开设了账户，并正在考虑房屋抵押贷款，在发生这样的数据泄密事件后，还愿意与之有业务往来吗？

保护数据安全

在保护企业数据方面，仅将全部精力集中在合规与审计上是不够的。虽然有关安全事故的大多数新闻报道都聚焦于第三方恶意攻击；但是，企业还需要关注与实现云安全相关的各种其他问题。

意外泄密

并非所有的数据泄露都是恶意行为造成的。实际上，在许多情况下，善意的员工或合作伙伴也会在无意间泄露数据。某些情况下，员工可能会因为使用公有云服务而将敏感数据暴露给未经授权的用户。例如，员工可能为了便于协作和共享大型文件而使用云共享应用。

此外，还必须考虑数据集是否可以在开发环境中查看或复制，以便可由内部测试团队使用。尽管真正的客户数据集可能是理想的测试对象，但这种做法可能会泄露客户的私人数据。

内部攻击

尽管绝大多数员工与合同工都希望为企业贡献自己的力量，但也不乏居心叵测之人。员工可能会因为被解雇或者未能加薪或晋升而感到不满。某些情况下，有些人会滋生出售企业数据的想法。解决这个问题的关键在于了解谁有权访问哪些数据，并能够完全追溯谁在什么时候接触了哪些数据。

恶意第三方攻击

企业通常会针对最敏感的数据部署各种各样的“护城河”（防火墙）、“大门”和加密机制。然而，企业中的数据分布在不同的部门和地点，这种情况日益普遍。此外，为了帮助员工根据数据做出决策，企业逐渐将宝贵的数据交到越来越多的员工手中。除了“皇冠上的宝石”外，企业的大部分数据从不加密，任何侵入单个终端的黑客都可以轻松得到它们。犯罪分子在寻找企业数据防护的薄弱环节方面变得越来越老练和狡猾。例如，某员工成为电子邮件网络钓鱼攻击的受害者，就很可能导致客户和企业数据曝光。

监管与合规

必须满足法律法规、行业标准和审计要求，一直都是企业确保安全的主要推动因素。特定的行业需要遵守特定的要求，例如，面向医疗保健行业的《健康保险可移植性和责任法案》(HIPAA) 以及面向零售行业的《支付卡行业数据安全标准》(PCI-DSS)。此外，随着欧盟《通用数据保护条例》(GDPR) 的生效，为避免处罚，几乎所有企业都在重新思考自己的安全措施。违反这些法律法规可能会受到严厉的处罚。例如，违反 PCI-DSS 可能意味着零售商不能再接受信用卡付款。

拥有安全云有何意义？

企业认为，将数据和应用托付给云提供商后，就不再需要负责安全工作，这其实是普遍存在的误解。事实并不是这样。企业依然需要负责跟踪这些高度分散的数据以及是否符合相关法律法规要求。

提示

为满足企业的安全要求，请遵循以下最佳实践：

- 制定计划，跟踪所有数据所在的位置以及用于保护数据的安全机制。
- 确保安全性已内置到应用和数据平台中，而不是依赖于各种第三方工具。
- 安全措施必须融入计算系统的每一层中，包括硬件、固件、虚拟机管理器、操作系统、中间件和应用。
- 在混合云环境中实施身份管理。在复杂的多云环境中，必须采用始终如一、可预测的方式，确保安全解决方案保持最新状态，有效保护环境免受攻击。
- 多云环境要求企业扮演系统整合者的角色，通过始终如一、可预测的方式保护计算平台中的所有要素。

IBM 在 IBM Z 和 LinuxONE 上实施安全云的方法

IBM Z 的优势之一在于该平台固有的高水平安全性。通常，企业会担心将高度敏感的工作负载放到云端所带来的风险。那么如何才能在安全要求与云灵活性之间实现平衡呢？答案将在本部分中揭晓。

普遍加密

根据 IBM Z 的架构设计，安全性已预先整合到硬件和软件组合的每个层面，因此，用户无需再为管理种类繁多的第三方安全服务而劳心费神。这种安全能力的基础，就是对数据进行整体加密。因此，可以对与某个应用或数据库相关的所有数据进行加密。

在每个层面实施加密与普通的加密方法截然不同。大多数企业只加密少量数据，大部分数据都处于完全未加密状态。未加密的数据可能会因为无心之失或犯罪行为而泄露或被窃。如果对所有数据加密，即使数据暴露给了企业外部的人员，没有密钥，数据就毫无意义。

普遍加密既可以对静态存储的数据加密，也对动态传输的数据加密，可用于保护本地私有云和公有云服务。此外，加密不需要更改应用。

读者可能很好奇，系统如何能够实时加密和解密数据，而不显著增加开销和降低性能。IBM 开发出了特定的硬件，用于高效快速地执行加密任务。芯片中加密处理功能每秒可通过每个芯片加密高达 13 GB 的数据。

企业可通过各种不同的方法访问 Z 安全服务。例如，客户可基于 IBM Z 架构在本地构建自己的云，从而确保云环境继承所有的内置安全功能。或者，客户可访问 IBM Cloud 中的 Hyper Protect（请参阅后面的“IBM Hyper Protect Services”部分）或安全服务。我们将在下一节中讨论这些选项。

私有云选项

可将 IBM Z 和 LinuxONE 服务器配置为运行 IBM Cloud Private 软件 — 通过 ICP 平台，可轻松将 DevOps 功能与针对云优化的软件整合。IBM Cloud Private on Linux on IBM Z and LinuxONE 帮助团队在安全的云环境中借助容器和微服务，充分利用 IBM 软件组合的强大能力。通过在 Linux on IBM Z 或 LinuxONE 平台上部署 IBM Cloud Private 环境，客户就能够充分享受大型机安全服务带来的优势。例如，客户可使用 IBM Secure Service Container，自动加密所有数据，无论是静态存储的数据，还是动态传输的数据。这种自动化加密技术能够保护应用和数据免受攻击，防止攻击者利用特权管理员凭证获得应用和数据的访问权限。通过利用这些安全功能，客户能够在本地安全地构建和运行自己的混合云和私有云部署项目。

IBM Hyper Protect Services

IBM Cloud 中运行着各种各样的 Z 安全服务。目前，IBM 将 Z 整合到全球公有云数据中心，提供内置了主机级数据保护功能的 IBM Hyper Protect Services。开发人员和客户可以利用行业领先的数据保护功能，构建、部署和托管应用，轻松加密内存中、传输中以及静态存储中的信息。该技术旨在抵御来自企业内外的各种威胁。以下几个部分将详细介绍 IBM Cloud Hyper Protect 系列，该产品目前提供三种服务，并且还将继续扩展，包含更多旨在提供云保护功能的关键服务。

普遍加密保护知识产权和客户数据

对所有数据加密是一种全新理念。在几乎所有在线互动中，数据都会在过程的某个环节处于未加密状态。这就让罪犯窃取数据有了可乘之机。

以在线保险互动为例。客户的浏览会话被加密，以保护客户免受各种攻击技术的侵害 — 客户输入的所有数据（包括用户名、密码等）都将加密。但是，在保险公司的后端应用和网络系统上，这些会话很可能在某个环节未被加密。无论未加密的数据位于何处，都会成为薄弱环节。比如，如果应用性能测试小组可以访问该浏览会话，他们的系统就很可能成为被犯罪分子利用的攻击载体。

IBM Cloud Hyper Protect Crypto 和密钥管理

IBM Cloud Hyper Protect Crypto Services 是一种加密服务，旨在利用一套完整的加密和密钥管理服务以及专用名称空间，在云端提供基于 IBM Z 的安全功能。IBM Hyper Protect Crypto Services 借助“硬件安全模块”(HSM) 生态系统中最高水平的安全能力，保障云原生解决方案的安全，满足高度受监管行业的要求。该系统为高密度的独特事务提供动态和静态保护功能，可通过 IBM Cloud Hyper Protect Crypto Services 在云端访问。该功能以前在银行和金融服务机构比较常见，它将 IBM Z 的安全服务移植到 IBM Cloud 中。

牢记

IBM Cloud Hyper Protect Crypto Services 与多个 IBM Cloud 数据服务整合，包括用于帮助客户在 IBM Z 上保护密钥的 IBM Cloud 服务 IBM Key Protect。此外，这些服务均可通过多种流行的编程语言进行访问，包括 Java、JavaScript 和 Swift。

IBM Cloud Hyper Protect Database Services (DBaaS)

IBM Cloud Hyper Protect DBaaS 是云服务，旨在按需提供数据库。例如，提供 MongoDB Enterprise Edition 数据库集群，支持客户快速配置、管理和保护敏感的数据工作负载。该服务采用了 LinuxONE 的普遍加密服务。这样，客户即使不具备专业技能，也能将客户数据保存到完全加密的数据库中。此外，它还支持 IBM Cloud Hyper Protect Containers（请参阅下一部分），帮助客户部署安全的 Kubernetes 工作负载。借助 IBM Cloud Hyper Protect DBaaS，客户能够在 IBM Cloud 中部署数据库集群；利用应用编程接口 (API)、命令行界面 (CLI) 或用户界面 (UI) 管理数据库实例；管理数据库内容；以及监控数据库环境。

IBM Cloud Hyper Protect Container Services

IBM Cloud Hyper Protect Containers 与安全服务容器一起部署，提供 Kubernetes 集群和标准化的应用打包方法。此过程在 IBM Cloud 中实现了可移植性及可扩展性。随着 Z 架构的普及，容器级安全性的优势变得越来越重要。

无处不在安全服务的重要性

随着企业快速迁移到云部署，他们必须在计算基础架构的所有层面都提供安全防护措施。单层加密或安全保护远远无法起到保护核心资产安全的作用。客户无论是利用自己的 IBM Z 私有云平台，还是使用基于 IBM Z 云的加密功能和 Hyper Protect 服务，IBM Z 安全服务都能从源头提供完善的保护。

本章概要

- 了解敏捷 DevOps 的价值
- 创建流畅的 DevOps 流程
- 了解 DevOps 的实际运用
- 在大型机环境中管理 DevOps

第 3 章

通过 DevOps 在云端创建敏捷软件

云服务现已成为支持企业快速高效地进行数字化转型的关键基础。公有云和私有云的优点之一在于，能为开发组织提供创建创新应用所需的敏捷性。云端的 DevOps 解决方案可帮助企业使用合适的平台以及一组通用工具来实现业务目标。

在本章中，我们将讨论多云环境如何改变了 DevOps，从而使企业能够根据安全和数据位置需求选择合适的的平台。

说明敏捷 DevOps 的价值

业务发展的步伐不断加快，企业希望加速实现价值。数十年来，IT 部门一直在寻找可预测而且安全灵活的方法，用于创建、部署和管理应用。可视化开发方法、自动代码生成和微服务方法的发展，为企业提供了巨大帮助。

数字化转型和云计算对敏捷流程和方法带来的改变，深刻影响了应用的开发、部署、保护、管理和变更方式。由容器和微服务推动的云原生应用开发领域的最新进步就是一个很好的例子，说明了云计算如何推广用于创建应用的新方法。市场动态和快速变化的业务需求是最终推动因素。

在高度分布式的多云环境中，通过 DevOps 生成的软件必须持续更新和管理。为了取得成功，应用开发团队必须快速创建新代码，以便设计和部署新的应用服务，满足不断变化的客户期望。以前那种开发团队与测试人员、部署人员以及负责推动应用取得成功的业务部门隔离，单独编写应用的模式已不再可行。

牢记

DevOps 的目标是在整个企业范围缩短从构思到交付的周期。开始实施企业级 DevOps 之后，要关注的重点是团队能够以多快的速度完成从应用构思到交付给客户的过程。通过正确践行 DevOps 文化，企业就能够显著缩短准备时间和流程周期，加速创造价值。持续交付 (CD) 必须与企业的业务价值相结合。

创建无缝的 DevOps 环境

在不断变化的业务需求和旨在满足这些需求的新技术（包括云）所共同创造的环境中，持续创新和产品面市速度已成为关键的成功指标。要想在这些指标方面交出亮丽的成绩单，必须建立持续开发与集成的过程。

作为最基本的要求，不能再使用“孤岛式”的开发生命周期来创建软件。不能再将生命周期中的各个步骤（包括开发、部署和测试）视为单独的任务；而是应将它们视为整合的流程步骤，必须能够平稳顺畅地从上一步过渡到下一步。

DevOps 实践的理想成果包括：

- 共同努力，采用整合方法实施软件开发生命周期，加快创新速度
- 通过自动执行软件交付流程，提高开发效率和生产力，实现源源不断的创新
- 将用户和客户反馈用作软件创新优化机制

在云基础架构时代，企业必须根据不断变化的客户需求，以及来自新兴网络原生解决方案提供商的威胁，持续对软件进行修改。为了保持竞争优势，流程必须做到标准化、一致而且可重复。如果企业使用各种公有云、私有云和数据中心资源来运行软件环境，这一点就显得尤其重要。敏捷软件开发方法可令 DevOps 开发过程变得更为稳健；而设计思维方法可确保开发团队集中精力解决实际问题；因此，两者结合，有助于显著提高 DevOps 工作的有效性。关键在于充分利用各种有效的流程和方法，促进强有力的团队协作和最终用户的积极参与。

DevOps 实际运用

DevOps 强调的是企业文化转变。许多成功的企业在其整个 IT 基础架构中实施 DevOps，涵盖云环境、分布式环境和大型机环境。通过将云服务模式与大型机的可扩展性、可靠性和安全性优势相结合，有助于实现更出色的敏捷性。

DevOps 团队必须积极参与分享一种共同的企业文化：强调整个生命周期中各个步骤之间的平稳顺畅过渡 — 从设计、开发到生产，涵盖各个平台。DevOps 应该是一个完全整合的生命周期。整合式 DevOps 生命周期有助于将人员与这些实践结合起来，而不是形成新的孤岛。该生命周期的组成部分如下所示（见图 3-1）：

- **持续业务规划：**要实现持续创新，就需要高度灵活的业务规划方法，能够迅速响应客户反馈。在该步骤中，需要不断根据客户反馈梳理待办任务，坚持协作式开发并持续进行测试。

- **协作开发：**协作无疑是确保满足服务需求和服务级别的必要条件。团队可以基于微服务架构构建服务和应用。在生命周期的所有阶段都必须聚焦于客户体验，从而确保所有利益相关方始终紧盯共同的目标。
- **持续测试：**开发完成后才开始测试的日子已成为历史。通过在开发生命周期中及早测试、全程测试，可以及早检测到错误，从而更容易发现、诊断和修复问题。
- **持续发布和部署：**确保应用保持最新状态，是当今企业的一项必备实践，也是 DevOps 方法的主要优势。通过持续发布更新，团队可迭代式地改进应用，积极响应客户反馈。
- **持续监控：**通过在整个开发过程中持续监控应用性能，可以确保它们为生产部署做好准备。
- **持续客户反馈：**为满足持续交付以及由此产生的快速部署的要求，企业迫切需要获得并整合客户反馈。此外，实时监控应用性能还有助于确保满足客户期望。

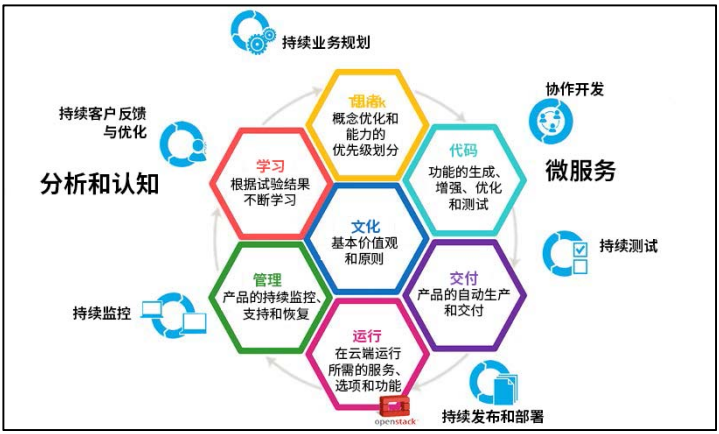

图 3-1：DevOps 周期。

持续交付并不意味着杂乱无章

有人误以为，采用 DevOps 和持续交付就是工作人员在计划外不断地将代码部署到生产环境，从而对业务产生干扰。其实并不是这样，DevOps 和持续交付是持续向某个平台交付代码，比如首先向登台环境交付代码，待准备就绪后才会投入生产环境。在复杂的商业环境中，要确定新代码投入生产环境的最佳时机并不容易。例如，在某些情有可原的情况下，可能需要先完成整个作业之后再添加新代码。因此，最好选择在事务处理量较少的晚间执行这项任务。显然，需要充分考虑事务性系统的流程，谨慎选择更新时机。我们肯定不希望在白天更改事务性系统的功能，因为这可能会对最终的计算产生影响。可先在登台环境中持续部署代码，等待时机成熟再对生产环境实施更新。

DevOps 框架

牢记

DevOps 是一种必须贯穿整个企业的文化，而不仅仅是一套开发者工具。当企业过渡到 DevOps 文化后，这些框架有助于为应用创建一致的结构。通过使用框架，整个应用交付生命周期将得到显著改进。

可将各种服务整合到 DevOps 开发框架中。例如，开发人员可使用配置管理服务，跟踪在软件开发生命周期中创建的版本、变更和代码模块。这些配置管理信息存储在在线存储库中，供所有开发人员共享。

构建应用的流程涉及到编写、编译、运行和测试代码。在 DevOps 环境中，开发人员会生成许多代码模块，每个模块都有自己的一系列依赖项。因此，DevOps 框架还应包含支持所有这些步骤的构建服务。

DevOps 和云

随着云计算的出现，DevOps 发生了巨大的变化。例如，移动和 Web 应用通常会每周更新多次。越来越多新兴的网络原生型企业具备了接近实时的创新能力。客户希望企业倾听自己的反馈，并根据意见改进应用。传统的领先企业不能吃老本；必须坚持不懈地创新。与此同时，企业还需要提供复杂服务（如事务管理）所需的安全性及可扩展性。

如果针对 DevOps 实践采用一致的方法，那么，无论使用哪种平台，都能够形成持续改进的文化。相同的最佳实践适用于移动应用、云服务和大型机。因此，应将 DevOps 视为一个连续体，包含适用于所有部署平台的通用 API、开发工具、安全服务和运营管理。

提示

有了这一系列适用于所有部署模式的通用服务，企业就能够高效地为工作负载选择最合适的平台。例如，将具有复杂的安全性、可靠性和可扩展性要求的工作负载部署到大型机上进行管理。

牢记

虽然每个企业部署的平台可能在服务质量（QoS）和功能方面各不相同，但它们可以应用相同的 DevOps 流程。事实上，在许多情况下，无论使用哪种平台，DevOps 工具和管道都是相同的。

以开源为核心

越来越多的企业采用开源模式，保护自己免受变化的影响。三十多年来，开源一直是 IBM Z 的基本功能。大型机以为开源为基础，意味着开源 DevOps 工具是大型机与生俱来的能力。因此，大型机可以利用其他部署模型中常用的现代语言。可将大型机简单地想象成基于开源能力、高度安全而且可预测的部署模型。

大型机环境中的 DevOps

我们看到，全新 IT 环境作为业务必不可少的组成部分，必须专注于应用的持续改进与持续交付 (CI/CD)。您可能会认为，大型机并不是创建、部署和管理现代应用的合适环境。毕竟，目前存在一种普遍的看法，公有云和“商用系统”才是数据中心的首选平台。

对大型机做出这样的假设是错误的，因为这忽略了有关企业和大型机的一些重要事实：

- 尽管计算市场已经发展了数十年，但大型机仍在企业数据中心发挥着重要作用。许多关键应用仍在大型机上运行，宝贵的数据仍存储在大型机上。
- 尽管客户认为必须迁移到云端以获得灵活性和可扩展性，但大型机仍是托管各类业务应用的可靠选择。企业可在 IBM Z 上部署各种应用。如果采用 Linux on IBM Z，那么不仅能够获得可在任何平台上使用的 DevOps 功能，还能获得只有大型机提供的额外安全性。大型机的可靠性、高性能和安全性都经过了时间的检验。在许多方面，大型机使企业不必为了将工作负载和数据迁移到数据中心之外而操心。
- 企业依靠应用来开展业务运营，其中许多应用都是在大型机上编写的。尽管其中的许多应用都能与云和移动应用整合，但从成本和业务中断的角度考虑，弃用它们在经济上并不现实（也没有必要）。

提示

IBM 提供多种开发工具，帮助消除单体式应用重构的复杂性，支持企业利用现有资产，在行业竞争中保持优势。

» 大型机应用的优势之一便是它们包含了难以从头开始设计的复杂业务规则和逻辑。新兴企业在尝试复制同等复杂程度的系统方面处于不利地位。以某个银行系统为例，该系统在 IBM Z 中运行完整的欺诈检测系统。银行构建了欺诈检测系统，并创建了自定义规则，用于发现并阻止潜在的欺诈活动。该系统经过全面优化，以客户所需的速度和规模运行。银行的所有业务知识都融入到该系统中。相对于那些必须了解如何从头开始创建欺诈检测系统的初创企业而言，该系统是一个巨大的竞争优势。

目前出现了多种新的开发流程、方法和工具，助力实现大型机应用现代化。但还必须认识到大型机的生命力，这对于为大型机开发新应用也是非常重要的。无论是开发新应用，还是对现有应用进行现代化改造，都必须考虑到云部署和云集成。有两类应用与此有关：

» **原生云应用：**这些应用又称为“*云优先应用*”，通常是为移动和 Web 平台构建的，因此与较为传统的应用相比，在开发过程中需要考虑不同的依赖关系。这些应用倾向于将前面讨论的 Web 服务和微服务作为加速开发过程的一种手段。此外，还需要使用主要功能是将移动应用连接到后端服务的集成服务，为这些应用提供支持。

» **支持云的应用：**在本书的上下文中，基于大型机的传统应用主要用于在企业数据中心内运行，以支持任务关键型业务职能。企业可以通过一致的 API 对这些应用中的宝贵资产进行现代化改造，以使它们能和专为互动系统而建的新型云原生应用协同工作。这些应用对于业务运营至为关键，而且具有许多复杂功能。因此，它们具有较多的依赖关系，需要进行持续投资。

牢记

成功的企业逐渐开始使用一些较为先进的工具和方法，用于部署新的大型机功能。新一代工具帮助团队更加迅速地开发云原生应用。作为一种应用开发方法，DevOps 同时适用于这两类应用，但是对许多企业而言，最大的挑战在于如何为现有大型机应用提供云支持。这些应用的现代化改造需要经济实惠的 DevOps 方法和工具，尤其是对于使用 COBOL 编写的应用。新一代工具可通过多种方式提供帮助：

- 利用在企业的其他地方使用的相同 DevOps 工具和方法

  如果针对大型机利用在其他平台使用的现代 DevOps 管道和工具，就能够满足企业所需的速度和质量要求。这种方法使企业能够支持现代技术，如基于 REST 的应用编程接口 (API)。
- 使用 Java 和其他现代语言（例如 Swift 和 Node.js）构建额外的功能
- 将功能易用性与现代编程方法结合，帮助提高开发人员的工作效率
- 支持持续交付，及时交付新代码和新服务，而不依赖于发布计划
- 尽可能无缝地简化从旧编译器向新编译器的迁移工作

其他要求包括：

- 适当的分析工具，能够有效地分析数据流和“数据使用位置”信息、程序控制流、源代码复杂性、应用清单、批处理控制流、应用逻辑变更影响以及企业应用的其他特征
- 适当的风险评估能力，可在整个开发生命周期中发现性能和资源问题，还能访问并借助使用情况数据和事务数据，预测潜在的生产故障

- 每个层面的自动化测试，从单元测试到性能测试全覆盖，能够在整个生命周期中尽早发现问题
- 自动化的应用交付，支持应用性能分析，缩短在线事务处理和批处理周期

理想情况下，这些工具会提供可视化功能，使开发人员可以轻松查看并了解所需的分析。

与任何 DevOps 工作一样，团队也必须分享并支持共同的文化，促进开发生命周期中所有步骤的平稳整合与过渡。在许多情况下，运营人员可与开发团队使用相同的工具，以促进这些过渡。成功的 DevOps 工作以持续的流程改进为基础，当然，这离不开精心策划的方法。

本章概要

» 从 API 经济获利

» 了解大型机作为中枢的价值

» 了解大型机上的数据和应用服务

第 4 章
让安全云环境成为数据和应用中枢

IBM Z 平台日益成为诸多企业的云战略核心，这些企业将大型机作为主要的事务引擎，用于和客户及合作伙伴开展商业往来。海量的复杂业务数据也保存在大型机上。其中一些是历史数据，另一些则来自企业与客户正在进行的业务事务。此外，基于大型机的战略性应用乃是业务运营的核心。目前，已经能够公开包括“信息管理系统”(IMS) 或“客户信息控制系统”(CICS) 在内的诸多 IBM Z 服务，作为云服务供广大用户使用。这项新功能意味着，当我们进入混合计算领域时，务必将大型机视为整体云战略的一个战略性要素。

在本章中，我们将探讨将大型机用作数据和应用中枢所需的方法。要想在这次转型中取得成功，需要使用应用编程接口 (API) 和 API 管理。

了解 API 经济

API 经济帮助企业通过全新方式，使用核心应用服务进行创新，以满足不断变化的客户需求。尽管 API 已存在数十年之久，但现在，企业通过提供一系列标准的 API，就能够以创新的新方式成功管理混合云环境。事实上，API 标准化正在改变混合云的格局。

REST API 便是用于创建移动和云应用的事实标准。这些 API 也是 IBM Z 平台的核心要素。随着 REST 扩展到大型机，云开发人员可以利用关键的业务数据和事务，让 IBM Z 成为混合云环境的焦点。借助名为 z/OS Connect Enterprise Edition 的服务，开发人员无需具备 Z 子系统知识，即可使用开放标准，将 CICS、Db2、IMS 数据和应用或者虚拟存储访问方法 (VSAM) 数据作为 API 公开。

IBM API Connect 是一种 API 管理解决方案，旨在实现四个目标：创建、运行、管理和保护 API。IBM API Connect 的主要功能是管理 API 的生命周期 — 这既包括内部创建的 API，也包括通过订购模式使用的 API。API 管理解决方案使开发人员能够复用现有资产来创建新应用，以及将现有服务链接在一起，从而推出新产品和新服务，创造新收入。

提示

要想获得成功，必须能够管理 API 的整个生命周期。API 管理服务可用于实施安全策略，提供整合指南，并帮助在移动、Web、云和大型机环境中测试 API 服务。借助一致而且可预测的 API，企业就能够迅速从应用逻辑和客户数据中获得经济效益。

介绍到这里，读者可能想问，这种现代 API 管理方法与面向服务架构 (SOA) 有何不同。本世纪初 SOA 的出现标志着企业应用构建和使用方式发生了巨大变化。但在 SOA 出现的头几年，几乎没有标准可循，也没有服务或 API 的管理方法。如果没有周密规划的管理方案，随着服务器和 API 数量的增加，确保高质量和找到合适服务就会变得非常困难。缺乏对服务和 API 的监督与管理带来了诸多问题，这也催生出 API 管理平台和 API 经济。

大型机作为数据和应用中枢的价值

大型机应用是许多企业开展运营的基础。这些应用中通常包含对于业务运营至关重要的业务流程和规则。但是，这些应用背后的代码都是在现代编码标准出台之前编写的，因此很难维护或进行现代化改造。通常，企业因为缺少精心设计的 API 而无法将现有系统与其他服务和数据源整合。同样，大型机数据虽然可在数据中心使用，但并未转换成开发人员能够通过一致方式轻松访问的格式。大型机架构专用于大规模管理和执行复杂的业务流程，提供高水平的安全性。

借助 IBM Application Discovery and Delivery Intelligence 等现代工具，企业就能够分析代码，发现依赖关系，从而可以轻松重构代码，使之实现现代化，并发展成一系列服务，用于提供精心设计的 API。要想取得成功，企业需要将这些安全牢靠的记录系统与灵活的互动系统结合起来。互动系统（例如创新型服务）是用于直接与客户建立亲密关系的应用。例如旅游服务，帮助客户通过移动设备选择酒店或其他服务。又如金融服务应用，通过与客户进行互动，接近实时地提供账户余额等数据。

借助 z/OS Connect Enterprise 和 IBM API Connect 转变大型机应用后，大型机就可以公开 API，以连接可以使用这些服务的云原生应用，而具有这些公开 API 的大型机应用也可以请求和使用云原生服务。

将大型机用作数据和应用中枢

核心记录系统、互动系统和 API 之间的连接是业务成功的关键所在。目前企业的现实情况是，需要将位于大型机上的记录系统组合起来，以便与通常具有云原生性质的互动系统进行互动。

提示

为了在不断变化的业务环境中有效开展竞争，企业必须具备能够支持数据与应用服务整合的中枢。对许多企业而言，将海量数据和关键应用服务从大型机迁移到云服务是不切实际的。通过使用大型机平台作为数据和应用服务的中枢，不仅能够提高安全性，还能促进客户参与度。

数据服务

IBM 提供多种工具，用于在大型机与云数据之间建立无缝连接。例如，z/OS Connect 支持没有大型机经验的用户访问大型机数据。此外，大型机 Linux on Z 客户的开发人员可通过 RESTful API 访问大型机数据。借助这些标准 API，即使不具备大型机背景，开发人员也可轻松创建各种 Web 和移动应用，用于调用大型机功能，将数据写入大型机。

应用服务

在大型机上运行的众多任务关键型应用都具有核心规则与流程，对于实现一致而且可预测的业务运营不可或缺。如果不大规模中断运营，就无法轻松将这些应用服务转变为其他应用和服务。但是，这些核心应用有时需要进行现代化改造。完成改造之后，它们将成为在记录系统与互动系统之间建立业务连接的中枢。

IBM 提供名为 Application Discovery and Delivery Intelligence (ADDI) 的分析平台，用于支持对现有应用进行转变。ADDI 服务是用于对应用进行现代化改造的分析平台。ADDI 通过分析所有程序以及这些程序的技术依赖关系（例如数据库和第三方应用），改进应用服务。该平台采用 AI 算法，分析大型机应用，以发现依赖关系以及更改服务对计算平台运行的影响。ADDI 提供了许多核心分析和可视化工具，包括数据流和使用位置分析、程序控制流分析、源代码复杂性分析和影响分析等。这些工具有助于确定哪些程序对业务至关重要，哪些服务不再使用。

分析完成后，开发人员可以更轻松地对现有代码进行现代化改造，将以前的单体式应用转变为服务。此时，可添加 RESTful API，以便将这些服务整合并连接到云服务，从而提高业务敏捷性。

大型机中枢的目标

通过添加基于标准的 API 和连接服务以及实现应用现代化，大型机可以成为支持企业可扩展性的实用平台。对于将 IBM Z 平台用作业务事务管理核心的企业而言，这一点尤其重要。这些企业通常存储着数十年的宝贵数据，这些数据中蕴藏着丰富的历史背景信息以及客户趋势和模式信息。

通过支持容器和现代数据整合服务，大型机已经发生了显著变化。因此，大型机同时具备了卓越的可扩展性、性能和安全性，这意味着，大型机不再只是高度安全、易于管理的代名词，现在还能满足各种混合云需求。由于大型机是数据中枢，因此可在数据源处执行分析，这样企业就无需移动数据，因此消除了延迟，改善了客户体验。在大型机和多云系统之间引入通用 API，对于创建无缝计算环境至关重要。

本章概要

» 具有云的可预测性

» 了解运营智能的实际应用

» 应用机器学习和预测性算法

» 通过 IBM Z 获得运营智能

第 5 章
认识运营洞察的重要性

业务部门（LoB）的领导越来越希望能够掌控自己与客户及合作伙伴之间的互动。但是，要享受自由，就要承担责任。他们要对服务级别协议（SLA）负责，确保关键应用和基础架构的运营完整性。组织必须在各种可预测、易管理的混合云平台中确保服务的性能和运营。为了改善客户体验，管理层必须能够接近实时地了解分析结果并据此迅速采取行动。

在本章中，我们将讨论组织应如何利用运营数据和客户数据，更深入地洞察混合云环境。

云可预测性的重要性

越来越多的企业提供新服务来管理客户互动，借助新的云产品让大型机变得更开放。人工流程已不再适合管理这种混合环境。这种环境因为涉及太多平台，所以太过复杂。企业希望能够根据服务级别和安全级别提供适当的服务，以满足企业和政府的要求。仅仅管理各个工作负载是不够的；还需要对服务进行协调和管理。

在考虑云服务管理时，有许多选项可用于管理各种工作负载。在混合计算环境中，企业通常必须操心各种平台，包括大型机、部门级系统、公有云和私有云，等等。业务服务通常分散在 IT 组织的多个孤岛之中，因此难以通过一致、可预测的方式提供给客户。

对 IT 组织而言，最大的问题之一便是缺乏经验丰富的专家，帮助企业全面了解所有平台的状况。无论是服务器、大型机、云还是网络，每个平台都有自己独特的管理服务。要想获得成功，运营团队必须证明他们有能力提高用户满意度、降低成本并且保证运营完整性。

IT 运营管理的目标是确保所有计算服务都能以可预测的方式运行，就好像它们是一个统一计算环境一样。从运营的角度而言，IT 团队必须能够支持快速增长的任务关键型事务性工作负载。这些基于大型机的工作负载必须能与各种混合云工作负载无缝协同工作。

运营智能的实际应用

常见的 IT 运营管理问题可通过传统的自动化方法得到解决。一般而言，传统的自动化工作足以应对用户已充分了解的单一工作负载。但是，当企业开始管理涉及多个环境的众多工作负载时，就必须使用智能 IT 运营平台，以便对混合计算环境进行管理和控制。

当今的 IT 运营主管在人手有限的情况下，不仅必须管理日益复杂的物理环境，还要管理越来越多的数据。从经济可行性角度而言，企业不可能拥有足够的财力和技术资源来了解混合环境中每个要素的各种细微差别，以便通过可预测的方式对其进行管理。

数据来自各种不同的系统，包括大型机上的事务管理系统、业务应用、云环境以及机器生成的日志。此外，为了更好地持续改善用户体验，企业收集的有关应用使用情况的信息也越来越多。要想转变为这种预测性管理环境，必须分析性能数据以了解性能模式。

应用机器学习和预测性算法

高级分析和机器学习算法使搜索复杂数据中的隐藏模式成为可能，帮助企业轻松决定 IT 性能的改进是否有助于增强客户体验。首先，需要对系统性能的要求和期望有一个基本了解。企业需要的服务级别有多高？当整合来自大型机和各种云服务的数据和流程后，日志数据是否表明合并后服务的性能满足了要求？是否存在预示着问题的异常现象？

除了生成有关客户体验的数据外，每个底层系统还会生成与软硬件环境工况和运行相关的大量数据。然而，由于信息量太大，导致无法从中轻松获得切实可行的洞察，因此此类机器数据常常被束之高阁。

这些数据由涵盖大型机、虚拟服务器、云环境、存储设备、网络设备和各种传感器的众多系统生成。如果能够将它们组合在一起，提供有用的背景信息，就能有效帮助用户采取最佳行动，提高性能。

因此，有效简化 IT 运营管理的唯一方法是应用机器学习和预测性算法。通过运营智能，该系统能够持续监控混合环境的行为。

牢记

最好的解决方案莫过于将不同来源的数据整合在一起。基于机器学习的模型可用于分析和关联数据，以了解发生了什么、可能发生什么以及如何补救。例如，如果存在系统或网络中断问题，经过训练的分析模型可发现此类问题并提出纠正建议，或者自动采取纠正措施。

IBM Z 上的运营智能

在 IBM Z 平台方面拥有深厚专业知识的企业可以使用多种工具，监控和管理混合计算环境的整体性能。这些运营智能能力包括：

- **IBM Application Discovery and Delivery Intelligence (ADDI)：** 该服务能够快速分析并直观呈现应用组件、数据和作业之间的关系，安全高效地实施所需的变更。该服务可以自动记录文档。此外，ADDI 还能确定并保证 API 的完整性。
- **IBM Common Data Provider for z Systems：** 该解决方案以流方式，实时将各种 IBM Z 运营数据传输至多个分析平台。
- **IBM Z Operations Analytics：** 该解决方案通过多个分析平台，深入洞察 IBM Z 运营数据。内置的 IBM zAware 负责检测并诊断 IBM Z 运营消息中的异常情况。
- **IBM Z APM Connect：** 该解决方案旨在帮助企业全面深入地了解涉及多个 IBM Z 子系统的多个 APM 解决方案中的事务。

如果混合环境中包含 IBM Z 平台，企业就可获得卓越的可视性、自动化能力和洞察力，轻松管理多个云环境。

本章概要

» 制定云战略

» 遵循最佳实践，规划混合云

» 建立 Z 云基础

第 6 章
开始实施企业云战略

大多数大型企业都以大型机为中心运行大量事务，并确保事务安全。考虑到大型机应用的重要性以及平台的稳定性、安全性和高性能，企业需要构建强大的混合云环境。大型机逐渐转变成更灵活的平台，支持卓越的企业安全性、容器、微服务以及混合云。

这些记录系统是企业 IT 整体架构中不可或缺的组成部分。在云场景中，它们可以继续发挥自己的传统作用和用途，无论是作为私有云的一部分向内外部利益相关方提供服务，还是作为混合云中的本地组成部分发挥作用。最终结果是大型机和云环境的最佳能力兼容并蓄，各展所长。

企业云战略

随着 IBM Z 发展成为企业云中不可或缺的要素，它必须支持混合计算模式。这种级别的整合与互操作性正是 IBM Z 的价值所在。

IBM Z 的优点在于，它旨在支持记录系统和互动系统（包括公有云服务和软件即服务应用）的组合。IT 必须打破应用孤岛，成为以共享业务服务的形式构建和部署新功能的行家里手。为满足客户目标，IT 资产不能再各自为战。

因此，为支持客户，应首先制定包含 IBM Z 的混合云战略。要推进这种云战略，必须解决各种问题和需求。

提示

创建可在更复杂的云环境中发挥作用的安全架构框架。大型机提供的安全和治理水平可满足严格的业务管理和法规要求。在开展安全评估工作时，应深入了解混合云战略的参与者如何维持保护企业所需的安全级别。

规划混合云战略

规划安全云战略没有捷径可走。在混合云时代，必须统一规划所有服务和平台。本部分所描述的五项最佳实践是成功的有力保证。

仔细评估需求和限制

业务和 IT 部门必须紧密合作，确定云计算的实际需求。当前正在使用的应用能否满足业务需求？是否得到了妥善管理？需要哪些新服务？对于云解决方案的技术和使用，需要对 IT 和业务人员进行哪些培训？存在哪些财务限制？在制定云战略和实施计划之前，必须回答这些及其他问题。

选择适当的云部署模式

部署模式的选择始终是企业迁移到云的重要考虑因素。许多企业都选择使用 IBM Z，将更多的业务关键型工作负载保留在本地。但与此同时，他们也会选择性地使用外部公有云或虚拟私有云来管理其他工作负载。除了安全和管理方面的考虑外，成本方面的考虑，以及选择资本支出还是运营支出也可能会对这一决策产生重大影响。

确定最佳工作负载和数据位置

数据和应用的位置从未像现在这样重要。面对如此众多的应用部署和数据存储位置选项，企业在做出选择时必须考虑各种因素，包括性能、安全、成本和适用的法规等。

在分析企业级应用后，许多企业很快便认识到，将这些应用继续保留在 IBM Z 上对于安全和管理至关重要。但为构建这些应用而制作业务案例通常困难重重。此外，企业逐渐将大型机转变成混合云 API 主机。这意味着，他们需要对大型机上的应用进行现代化改造，将其作为 API 服务提供给云用户。大型机应用 API 在 API 管理门户中托管之后，看起来与任何其他云服务一般无二。企业选择使用 IBM Z 作为 API 主机的原因之一，是大型机 API 具有高度的可扩展性和可用性，其吞吐量也能够满足最终用户的期望。

虽然某些应用可能会随着更大规模的数字化转型而迁移到云端，但是，许多全新和现有的大型机应用仍保留在 IBM Z 上。因此，为了对这些应用进行现代化改造，企业正在大型机上创建软件定义的云。他们并没有将大型机应用迁移到云端，而是将云、DevOps 以及现代移动和 Web 应用整合到 IBM Z 之上。

牢记

鉴于目前企业所使用的数据数量庞大、类型繁多，因此数据位置变得尤为重要。IT 必须有效管控整个云环境中的数据位置和同步，无论在哪里需要和使用这些数据。决定数据存储位置的另一个因素是数据必须尽量靠近需要使用它们的计算资源，这也称之为云“边缘”法则；因此，需要精心设计、妥善执行数据同步和整体数据管理。

了解并管理服务级别、配置和许可

云环境，尤其是混合云，使服务级别协议 (SLA)、配置和许可的管理变得更加复杂。团队必须了解如何在整个云环境中满足服务级别，这可能包括内部策略以及公有云提供商或合作伙伴的外部策略。配置和许可问题让管理工作的复杂性进一步加剧。

在混合云环境中，服务可能由内部提供，也可能来自外部的一个或多个云提供商。为了有效管理这些服务，必须从所有来源收集配置信息，并协调和关联这些信息，实现连贯一致的服务管理。由于“配置管理数据库”(CMDB) 的信息模型种类繁多，以及需要使用多种不同的工具来收集配置详细信息，因此这项管理任务极具挑战性。通过结合使用跨平台工具以及所有提供商都必须遵守的配置管理策略，有助于缓解这方面的复杂性。

最后，考虑到基础架构的动态性质及其“按使用情况付费”的特征，添加云计算会显著加剧许可的复杂性。举个例子，由于需求的激增，必须将托管服务的服务器数量翻倍。这种情况下，最起码预测和购买软件许可存在一定难度。当然，管理许可的可行方法多种多样，包括在主机上托管应用、在云端运行当前核心系统，或者继续将记录系统保留在原地，等等。

将治理作为优先任务

为了保护最关键数据和应用的完整性，使用大型机的企业必须制定大型机治理规程和策略。然而，考虑到时间、预算以及公有云架构等因素，这种精心策划的治理结构很难在云端复制。解决这个复杂问题需要内部 IT 和业务部门 (LoB) 的利益相关方、云提供商甚至政府机构紧密协作。只有这样，才能建立有效的治理框架，确保数据和事务的完整性与安全性。

建立 Z 云基础

Z 云并不是旨在提高效率和灵活性的孤立项目。这种项目只是，而且也只应是整个数字化转型工作的一部分，与其他项目一起推动 IT 成为变革的力量。孤立的业务职能和 IT 资产必须让位给整体方法，通过综合利用云以及现有平台、技术和资产，使 IT 能够更有效地支持业务目标的实现。通过这种新方法开展业务，企业、客户、合作伙伴和提供商就可以更有效地合作，以更为顺畅、更为整体的方式开展业务。

云是实现这种转型的主要推力量，使 IT 资产更便于所有利益相关方访问和使用。如果执行得当，随着时间的推移，迁移到云端可以带来巨大的财务和组织效益。

声明

声明

加速数字化转型

对于同时需要使用本地服务和公有云服务来满足客户、合作伙伴以及提供商需求的企业而言，构建安全的混合云环境是关键所在。为实现蓬勃发展，企业需要建立覆盖多种部署模式的安全云。保护知识产权是企业不可推卸的责任。IBM Z® 平台可为计算基础架构的每一层提供安全防护。在本书中，我们探讨了 IBM Z 在安全混合云领域发挥的关键作用。

本书内容摘要 …

- 实施混合云战略，开展数字化转型
- 了解 IBM Z 在混合云中发挥的作用
- 利用 API 经济推动业务增长
- 了解混合云中的 DevSecOps
- 实现安全的云环境，赢得客户信任

Judith Hurwitz 是 Hurwitz & Associates 总裁、顾问和思维领袖，也是八本书的合著者，其中包括《认知计算与大数据分析》。

Daniel Kirsch 是 Hurwitz & Associates 首席分析师，也是云计算、机器学习和安全领域的研究专家和顾问。

访问 Dummies.com®
获取视频、循序渐进的图片示例、讲解文章或进行购买！

ISBN：978-1-119-52795-4
部件号：54017854USEN-00
非卖品

傻瓜系列
Wiley 出品

本书也提供
电子版本

WILEY 最终用户许可协议

请访问 www.wiley.com/go/eula，阅读 Wiley 最终用户许可协议的电子书版本。