北京金融科技产业联盟
BEIJING FINTECH INDUSTRY ALLIANCE

金融业上云指引

北京金融科技产业联盟

2022 年 7 月

版权声明

编制委员会

主编

潘润红

编委会成员

聂丽琴　韩　颖　王　鑫

编写组成员

白佳乐　沈震宇　孙凌云　杨晓峰　何鼎铭　邹璐琨　庞　帅
王小琦　李玉玲　孟凡雪　王　蕊　白　阳　陆碧波　王睿超
郝明昊　白鹂莎　陈亚殊　蒋维杰　杜静漪　方佳伟　周鑫立
许小平　许成林　缪栋屹　梅　江　李红亮　国语洋　李　珣
汪宗斌　史广安　凌　威　陈大伟　李　培　阳明亮

主审

黄本涛　周豫齐　陈　斌

统稿

沈震宇　杨晓峰

参编单位：

北京金融科技产业联盟秘书处

中国工商银行股份有限公司

中国银行股份有限公司

中国建设银行股份有限公司

华为技术有限公司

蚂蚁科技集团股份有限公司

阿里云计算有限公司

腾讯云计算（北京）有限责任公司

麒麟软件有限公司

深圳壹账通智能科技有限公司

浙江网商银行股份有限公司

杭州趣链科技有限公司

杭州谐云科技有限公司

迈普通信技术股份有限公司

光大科技有限公司

恒生电子股份有限公司

神州数码信息服务股份有限公司

中电金信软件有限公司

北京信安世纪科技股份有限公司

北京红旗软件有限公司

华夏银行股份有限公司

新华三技术有限公司

摘　要

随着国家“互联网+”的政策落地，云计算加速金融行业的“互联网+”发展，支持云计算发展的政策也相继推出，云计算产业发展、行业推广、应用基础等重要环节的宏观政策环境已基本成型。与此同时，金融行业内的应用规模不断扩大，基于大机技术构建的集中式架构已无法满足弹性扩展需要，所以金融机构积极开展基于云计算的分布式转型探索，以适应业务的快速调整和市场的不断变化。本报告主要从云计算应用现状、金融业上云政策环境、上云准备、上云实施、上云后管理五方面进行描述，同时结合金融机构规模及金融行业监管要求，分别从私有云、金融团体云、混合云（私有云+金融团体云）3 种上云形态进行分析，并提供金融行业上云实践经验，为金融机构业务云化转型提供参考。

目 录

一、金融业云计算应用现状

根据《云计算技术金融应用规范 技术架构》（JR/T 0166—2020）定义，云计算(cloud computing)是一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式，云服务（cloud service）是通过云计算已定义的接口提供的1种或多种能力。云计算本质上是复杂的信息系统，其各个模块保持着技术不断地迭代，以容器、微服务、服务网格为代表的云原生技术逐渐成为当前技术趋势的热点。伴随各行业上云进程的不断深化，及行业云标准发布实施，云化转型进程和数字化转型将进一步加速。

（一）市场情况

1.中国金融云整体市场规模

国际数据公司（IDC）最新发布的《中国金融云市场（2021上半年）跟踪》报告显示，2021上半年，中国金融云市场规模达到26.5亿美元。在逐步消除疫情影响之后，金融机构业务拓展与信息化建设进程重归正轨，金融云市场增速逐步回升，同比增长40.2%。其中，基础设施与解决方案市场增速分别达到38.3%和44.8%。

另外根据IDC研究，目前金融云市场呈现出以下内容。

一方面，线上渠道、营销系统热度不减。在疫情防控成为新常态的背景下，开放银行、远程银行、数字化营销及支持等系统成为2020年金融云增量市场的主要内容；另外，中国率先控制

疫情蔓延并加速复工复产之后，供应链金融、产业链金融亦为金融云市场增长注入新的活力。

另一方面，云服务商技术底座优势进一步显现。“垂直行业信息技术服务提供商+云服务商”组合，已经成为当前金融云项目的标准配置，垂直行业各类应用系统已普遍适配多家云服务商的平台产品，以分布式数据为例，TiDB、OceanBase、PolarDB、TDSQL、GaussDB、GoldenDB 等已成为金融行业新一代核心、销售支持等关键系统的重要支撑。

2. 中国金融云总体市场预测

2020-2025 年中国金融云市场复合增长率预期达到 32.2%，到 2025 年市场规模预期到 186.9 亿美元，见图 1。

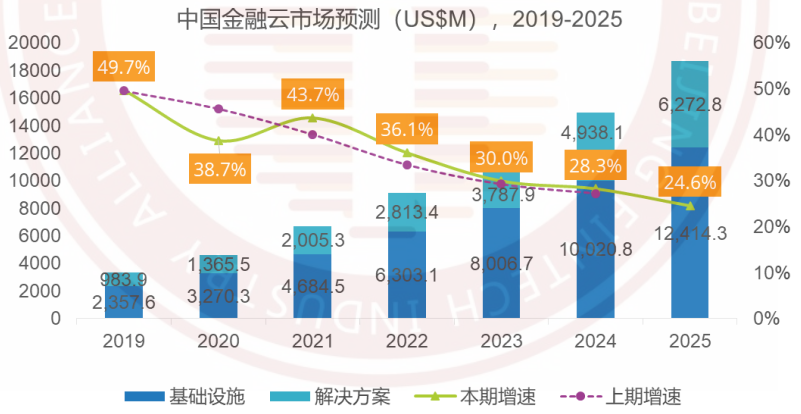

图 1 2019—2025 中国金融云市场预测[1]

3. 金融云解决方案云平台市场

2021 上半年，金融云解决方案云平台市场规模达到 3.3 亿美元，金融云服务商的项目交付能力恢复正常，解决方案市场增

[1] 来源：IDC 中国，2021

速大幅回升。根据 2021 上半年中国金融云平台解决方案市场份额分析报告显示，阿里巴巴、腾讯、华为、百度、京东云位列前五，份额合计达到 79.2%，见图 2。

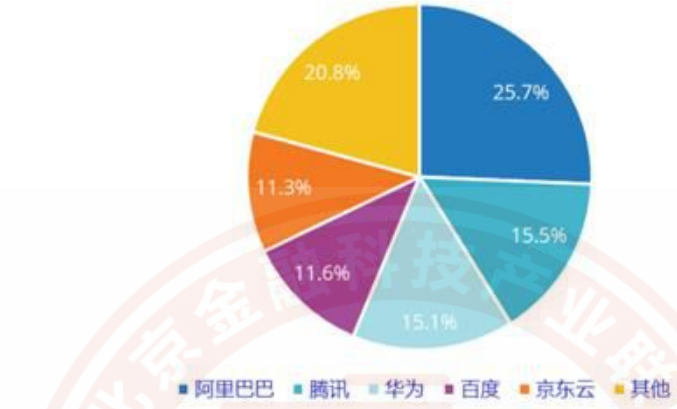

图 2 2021 上半年中国金融云平台解决方案市场份额[2]

（二）技术发展趋势

我国云计算产业上游主要围绕核心硬件研发和创新，芯片产业仍是重中之重，芯片的自主可控能力直接影响着云计算产业安全可信的水平。我国芯片产业整体发展较为薄弱，服务器芯片领域自主研发的有基于 MIPS 的龙芯、基于 x86 的兆芯、基于 ARM 的天津飞腾和华为鲲鹏、以及基于 Alpha 架构的成都申威等，虽然涉及厂商较多，但产业生态仍不完善，直接影响了上层应用生态的成熟度。我国云计算产业下游创新主要围绕云原生、云安全、数据库、数据湖、可信 AI、区块链平台等，加速数字化转型，提升企业生产力。

从金融行业信息基础设施技术路线演进来看，先是从早期的

[2] 来源：IDC 中国，2021

大型机逐步发展至普通 PC 服务器，随后大范围采用服务器虚拟化技术。随着云计算技术的兴起，以基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）、微服务等为代表的云计算理念及技术逐渐成为金融机构的首选。根据中国信通院调查数据显示，目前我国已经应用或计划应用云计算的金融机构已超过 87%，部分金融机构应用云计算已较为成熟。

目前金融机构多根据业务系统的属性、重要程度，选择不同的云部署方式，分别是私有云、团体云、公有云、混合云等。而国内为金融机构提供云服务的厂商有华为、阿里、腾讯等，多提供线上云服务采购模式，也有协助金融机构建设云平台和提供持续升级维保服务。提供的云服务有 IaaS、PaaS、数据库、大数据平台、人工智能等。

（三）金融科技应用

云计算技术近几年发展已经较为成熟，其在各行各业的应用已成为驱动业务增长的重要引擎，企业信息基础设施走向全面云化，且逐步推动业务进一步实现智能化。2020 年 3 月 30 日，国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，指出“数据成为与土地、资本、技术、劳动力并列的第五种生产要素”。相应的，对应到金融业务场景，大致可分为如下 3 个方面。

1.应用全面现代化。从开发到运营，助力金融面向互联网化敏捷创新，促进金融互联网移动 APP 开发、金融传统应用开发、

金融应用微服务全域治理、金融云原生应用开发及运营等。

2.数据全栈智能。发掘金融数据资产价值，加速促进金融行业知识与 AI 结合的模型开发，构建金融级智能数据湖、金融核心交易分布式数据库、金融级数据仓库、金融数据一站式运营平台等。

3.业务全流程安全。构建金融安全合规平台，保证数据可信流通，促进金融云安全、金融数据加密、合规认证、金融同业及跨业多方数据可信计算等。

云计算推动以数据库、数据仓库、大数据、人工智能等为代表的技术云化部署，通过相互融合呈现出更加强大的云创新能力，进而推动企业业务应用系统的智能升级，在业务风险控制、移动支付、精准营销、数字化获客黏客、物流金融、农业金融等均有落地场景。

二、金融业上云政策环境

（一）政策保障

近年来，随着国家“互联网+”政策落地，云计算加速金融行业的“互联网+”发展，支持云计算发展的政策也相继推出，云计算产业发展、行业推广、应用基础等重要环节的宏观政策环境已基本成型。

国务院、工信部等部门近年来出台一系列云计算相关法规标准，指导云计算系统的设计、开发和部署，引导并规范云计算等基础设施建设，提升云计算服务水平，规范市场秩序。

2015 年 1 月，国务院印发《关于促进云计算创新发展培育信息产业新业态的意见》，明确指出云计算是信息化发展的重大变革和必然趋势，促进我国云计算创新发展，积极培育信息产业新业态。

2015 年 7 月，国务院印发《关于积极推进“互联网+”行动的指导意见》，明确提出“互联网+普惠金融”的推进方向，鼓励金融机构利用云计算等技术手段，加快金融产品和服务的创新。

2015 年 8 月，国务院印发《促进大数据发展行动纲要》，推动大数据与云计算、物联网等新一代信息技术融合发展。

2015 年 10 月，工信部印发《云计算综合标准化体系建设指南》，制定由云基础、云资源、云服务和云安全 4 个部分组成的云计算综合标准化体系框架，提出 29 个标准研制方向。

2016 年 7 月，银保监会发布《中国银行业信息科技“十三五”发展规划监管指导意见（征求意见稿）》，提出银行业面向互联网场景的重要信息系统全部迁移至云计算架构平台，其他系统迁移比例不低于 60%。并对银行业云计算明确了监管意见，提出积极开展云计算架构规划，主动和稳步实施架构迁移，支持金融行业上云。

2017 年 7 月，人民银行发布《中国金融业信息技术“十三五”发展规划》，明确要求落实推动新技术应用，促进金融创新发展，稳步推进系统架构和云计算技术应用研究。

2018 年 10 月，国务院标准化制定部门发布《基于云计算的

电子政务公共平台安全规范》（GB/T 34080），从服务分类、应用部署、数据迁移、应用开发设计、运行保障管理等方面为政务云制定了标准。

2019 年 7 月，国家网信办等四部委联合发布《云计算服务安全评估办法》，为提高关键信息基础设施运营者采购使用云计算服务的安全可靠水平，制定了云计算服务安全评估办法。

与此同时，银保监会、人民银行等金融部门也陆续出台相关政策和发展规划，贯彻落实国家云计算发展战略，加速云计算发展进程。

2019 年 8 月，人民银行印发《金融科技（FinTech）发展规划(2019—2021 年)》,提出加快云计算金融应用规范落地实施，充分发挥云计算在资源整合、弹性伸缩等方面的优势，探索利用分布式计算、分布式存储等技术实现根据业务需求自动配置资源、快速部署应用,更好地适应互联网渠道交易瞬时高并发、多频次、大流量的新型金融业务特征，提升金融服务质量。

2021 年 12 月，人民银行印发《金融科技发展规划（2022—2025 年）》,提出加快云计算技术规范应用，稳妥推进信息系统向多节点并行运行、数据分布存储、动态负载均衡的分布式架构转型,为金融业务提供跨地域数据中心资源高效管理、弹性供给、云网联动、多地多活部署能力，实现敏态与稳态双模并存、分布式与集中式互相融合。

从国务院、人民银行、工信部、银保监会等部门发布一系列

政策可以看出，金融业上云在稳步、有序推进。

（二）标准引导

除了政策支持，标准也是云计算发挥其价值的必要基础。云计算标准化工作是推动我国云计算技术、产业及应用发展，以及行业信息化建设的重要基础性工作之一。云计算相关的标准化工作自 2008 年底开始被科研机构、行业协会及企业关注，随后便在全国范围内迅速发展。人民银行 2020 年印发《中国人民银行关于发布金融行业标准强化金融云规范管理的通知》（银发〔2020〕247 号），发布《云计算技术金融应用规范 技术架构》《云计算技术金融应用规范 安全技术要求》《云计算技术金融应用规范 容灾》标准，规范云计算技术在金融行业应用。同年，人民银行发布《金融行业网络安全等级保护实施指引 第 2 部分：基本要求》（JR/T 0071.2—2020），规定云计算部分 4 个等级的安全要求。

（三）市场需求

1.市场竞争优势需求

金融业竞争加剧及互联网企业的跨界渗透，迫使金融单位对业务模式和客户结构产生新的思考，未来金融服务和产品不再是单一或隔绝的，逐渐向场景化、生活化靠拢，同时市场竞争要求金融单位在产品推出效率、客户体验、业务场景创新方面具备更加随需应变、灵活创新的能力，而这一能力需要金融行业借助上云实现。

云计算技术在资源弹性、高效迭代、开放共享等层面具备传统基础设施技术无法比拟的优势。因此，金融单位将借助云计算的运算优势，将自身的数据、客户、流程及系统通过数据中心、客户端等技术手段发布到“云”端，以改善系统体验，提升运算能力、重组数据价值，为客户提供更高水平的金融服务，降低运行成本。

2. 金融服务提质增效的需求

当前金融业人力成本居高不下，整体金融行业运维服务水平完全取决人力投入。而大部分金融单位的运维人员基本处于工作饱和状态，随着业务类型、数据架构、信息系统的演进，运维体系、技术水平、人力成本不堪重负。

以中小银行为例，中小银行是一个严格意义上的银行，拥有全牌照，有权进行全业务拓展，经过监管机构审批后，可以开展银行卡业务、网上银行业务和国际业务等。中小银行为提升自身市场竞争能力，需持续进行新业务系统的研发和建设，这对中小银行信息化建设能力带来较大的挑战。

云计算通过自动化运维和智能化资源调度，能够大大减轻人力负担，有效降低总体运维和运营成本，同时确保风险管理水平不受影响。且云计算的按需供应和横向扩展能力大大缓解了供给不足或资源浪费的矛盾，使金融机构能够付出相对较低的资金来获取足够的信息技术资源，有效降低成本提高效率。金融业上云可以缩短应用部署时间、节约成本和确保业务升级不中断。

（四）技术支撑

1.信息系统架构演进

从 2000 年开始以工商银行为代表的金融企业开启了“数据大集中”的历史进程，金融行业信息系统架构在数据集中式的道路上前行了十多年，取得了骄人成绩，逐步完成了历史使命。随着互联网、移动技术、大数据、社交网络等信息技术的蓬勃发展，基于互联网的金融服务应运而生。这对金融行业的线下网点经营带来了全面的冲击，促使着金融行业向互联网模式逐步转型。一些新兴的民营银行更是没有银行网点，互联网成为了这些机构唯一的客户触点。一个看似简单的愿景：“任何人在任何地点、任何时间、任何场景下，通过多种手段均可使用金融服务”，使得新一代的金融行业系统必须直面来自不同阶层、不同背景的海量客户，以及随之而来的海量交易、海量数据。这将是金融行业共同面对的挑战，而分布式架构和云计算技术已经成为业内公认的解决方案。以谷歌为代表的互联网企业积极探索分布式和云计算，至此整个金融业信息系统架构站在了历史的新起点，朝着更高性能、更大容量、弹性架构、智能化的方向发展。

（1）数据大集中阶段

集中式架构系统的底层一般采用成熟的商业基础软件构建，这种架构的优点是成熟稳定、可用性强、可靠性好，金融行业的技术人员可专注于业务功能开发，无需过多关注底层技术的实现。金融行业经过十多年的集中式架构技术探索和实践形成了丰富

的技术积累，使得底层技术架构基本保持不变，运维手段更为集中统一，有力保障了业务快速发展和生产平稳运行。集中式架构下金融业信息化也经历了以下两个阶段。

第一阶段是以核心业务系统为中心的”大前置”阶段。该阶段围绕着核心系统，建设了信贷系统、国际结算、电子渠道等外围系统，外围系统一般通过直连或大前置的方式接入核心。这种以核心系统为中心节点，外围系统围绕着核心建设的系统架构模式实现了数据的集中管理，也能满足当时的主要业务需求，同时在业务管理和系统管理方面也相对简单。但随着金融业竞争程度的不断加剧，金融业务变革不断加速，业务需求呈现出爆炸性增长，业务流程化、服务多样性、管控精细化等对信息系统都提出了更高更多的要求，这个时候用一个系统、一种技术实现所有需求愈发困难。这种问题集中表现在：一方面经过多年的运行之后，很多旧核心系统已经步履蹒跚，既包罗万象又缺乏足够的弹性，导致每个新需求都需要对旧核心加以改造才能实现，而大部分业务又都耦合在旧核心一个点上，旧核心牵一发动全身，任何修改都可能造成整个系统不可预知的结果。旧核心系统已经成为了金融业信息系统的瓶颈，甚至到了谁都不愿改、不敢动的地步，成为了业务发展的拦路石，同时也为系统的安全稳定运行埋下很多隐患。另一方面越来越多的系统被独立的建设，越来越多的系统需要相互沟通，以完成复杂的业务功能。尽管在一定程度上建立了用于整合的系统，如大前置系统，但往往由于缺乏统一的整合

规范，导致业务的灵活创新并不是一件容易的事。正是这些问题和需求为整个金融业带来了一次信息系统架构的变革。

第二阶段是面向服务的 SOA 架构阶段。面向服务的架构(SOA)不是一种技术，而是人类在探索现实世界的过程中，随着认识的深入，对现实世界不断的进行抽象和建模的一种思想方法。通过SOA，把现实世界的各种实体(组织、客户、存款、贷款...)抽象成一个个独立自洽的“服务”，并对这些实体与外部其他实体之间的关系进行界定和清晰的表述，通过服务识别、分析、设计的建模过程，形成这样一组服务：这组服务是某个特定的现实世界的映射，在这个映射中现实世界及其活动通过服务自身和服务之间的互动得以体现，从而使服务模型得以很好的适应和表述现实世界的演化过程和演化结果。在这个模型里面，每一个服务独立的存在着，对外提供公开的服务界面，服务与服务之间通过这些公开的服务界面进行沟通，沟通的结果将反馈到服务本身；同时每个服务自身的运作机制并不影响其他服务，当某个服务自身发生变化时，只要其对外提供的服务界面不变，对外部系统都将毫无影响。SOA 理念正适合用来解决上述金融业务技术发展过程中所遇到的关键问题，通过 SOA 思想构建一个由不同厂商、不同技术的软件所组合起来的金融信息系统架构，在这个架构体系下，所有的软件能协同工作，发挥出各自的优势，对业务的支撑形成合力。但是随着 SOA 架构的深入，传统集中式大应用开始向微服务小应用拆分，服务粒度变的越来越细，应用的规模变得越来越

小，大量的小应用需要从资源调度、部署运维上提供更灵活、更强大的支持，这些都对传统集中式架构下资源虚拟化和调度能力形成挑战，金融信息系统架构又一次站在历史的新起点，迎接新的变革。

另外，经过多年的运行维护，传统集中式架构的一些根本性问题也慢慢呈现：一是风险度集中，虽然产品比较成熟稳定，但一旦出现软件或者逻辑上的极端异常，有可能导致整个集群不可用，从而引发全局性停业。二是我国人口基数大，随着经济的快速发展，业务量在全球处于领先，性能需求已经逼近传统集中式硬件架构的处理极限。三是成本高昂，集中式架构对基础软硬件产品的可靠性、可用性依赖度高，这些技术产品基本被极少数公司所垄断，缺乏有力的竞争者，信息化成本居高不下。四是核心技术受制于人，供应链风险较大。

（2）云计算和分布式阶段

分布式云计算架构按照一定的维度将系统和数据进行拆分，通过特定的负载均衡机制，将业务分摊到多个节点上处理。这种架构的优点是可以采用更开放的架构，各节点松耦合，对底层产品的可靠性、可用性依赖降低，可以基于廉价的硬件和开源软件构建。分布式和云计算相辅相成，云计算是实现分布式的有效手段和关键基础设施，分布式又是云计算下的必然选择和技术前提。分布式架构本身不只是简单的服务调用的分布式，更重要的是数据的分布式，因为一切服务的基础是数据，数据分布式的粒度直

接决定整个分布式架构的能力。

分布式云架构下的演进大致分为数据垂直拆分，数据水平拆分，数据单元化，数据弹性架构和混合部署等阶段。

数据垂直拆分: 业务系统由很多业务模块构成，垂直切分是指按照业务模块将数据表进行分类，分布到不同的数据库上面，这样也就将数据和服务的压力分担到不同的数据库和应用服务器来完成一定程度的分布式部署。以银行核心业务系统为例，我们一直倡导的“瘦核心”概念就是基于业务模块，把客户信息、产品工厂、费率工厂、存款、贷款、内部账户（异步核算）、公共信息等拆分到不同数据库，降低系统耦合性以及复杂度提升系统整体性能。由于业务系统中的事务主要高度内聚在模块内（比如最常用的客户记账行为中关键的“改余额记流水”需要强事务一致性的数据库操作都在存款模块），模块与模块之间的事务一致性要求不高，因此优化升级的技术成本和挑战不会太大。很多银行已经在这方面取得了丰富的经验和成绩，比如正在进行的“核心主机下移”。

数据水平拆分: 云计算的计算服务器和数据服务器都普遍采用 x86 架构服务器，单机处理能力有限，当单表数据过大（例如账户数据上亿），x86 架构下单机性能不足以支撑高并发请求时（例如上万 TPS），需要将原来一张表的数据进行水平维度拆分为多张表，分开存储在不同的数据库中进行并发处理，水平拆分势在必行。水平拆分虽然能带来处理性能水平扩展，但同时也带

来了数据一致性问题，因此，分布式事务处理能力是数据水平拆分的前提。目前只有极少数互联网公司掌握了成熟的金融级高性能分布式事务框架，很少有金融行业能对其核心记账等关键业务系统做数据水平拆分。

单元化: 单元化是将一个系统的架构按某种数据特征维度进行单元的划分，比如银行有 1 亿用户，如按照用户维度进行划分，则可以分成 20 个单元、每个单元存储 500 万用户信息。每个单元是一个从流量、到应用、到数据形成的完整、自治、独立的生态系统，能为客户提供绝大部分服务，数据访问都尽量封闭在这个单元内，因此可以将一个单元部署到任何地域，单元和单元之间能够互为备份，这为异地多活部署提供了可能。有少量服务确实存在跨单元情况，这就需要单元间的分发和调度能力，以及分布式事务框架能够支持跨单元的事务一致性保障能力。

弹性架构: 云计算讲的弹性架构，通常意义是指 IaaS 层能够实现计算资源（含网络）的弹性扩展和调度。但我们这儿强调的弹性架构，不仅包括 IaaS 层，也包括如何让数据服务也具有弹性。结合前面单元化能力，数据上也实现了单元化，这样辅以数据迁移工具，就能够实现数据服务的弹性，形成整体架构的弹性能力。在类似双十一大促的临时场景时，能够通过整体架构上的弹性，低成本的获取更高容量和处理能力显得非常重要。比如从常规部署的 20 个单元动态变成临时的 100 个单元，这样临时获得更大的并发处理能力，大促活动过后计算资源和单元拆分又

能动态缩容，归还弹性资源节约成本。

混合部署：金融行业系统分为在线交易系统(对客联机服务)和离线大数据处理系统(非直接对客的批量服务)。在线交易系统的特点是日间交易负载压力比较大，凌晨后业务往往处于低峰期，而离线大数据处理平台日间负载低，日终负载高，如能结合上述业务特点根据不同时段进行计算资源混布，就能错峰利用服务器处理能力。延伸开来，线下服务器(开发测试环境)也存在明显的负载低峰期，仅从技术层面考虑，通过混布的方式可以在日终利用线下服务器的计算资源进行离线大数据处理，日终完成后进行归还继续服务日间进行的研发测试工作。混合部署就是让这几套体系中的资源混合部署，综合调度，充分利用硬件计算资源达到节约硬件成本的目的。当然混布方案的挑战是非常巨大的，最核心是解决资源调度问题，需支持不同场景资源混合部署调度，不同在线业务资源需求与多种基础设施的调度、支持针对不同优先级容器的资源进行隔离，还要考虑监管合规的安全性隔离要求等问题。

(3)智能计算阶段

人工智能技术不仅涵盖了语音识别、图像识别、自然语言理解、用户画像、智能预测等，同时与大数据、云计算之间的联系也正变得越来越紧密。2006 年出现的人工智能关键技术——“深度学习”，人工智能至此才有了实用价值，而深度学习正是在云计算和大数据日趋成熟的背景下才取得的实质性进展。因为数据

量越来越大，计算能力越来越强，过去不实用的，逐步进入了实用阶段。这意味着，在通往人工智能的路上，有两个不可或缺的角色：大数据和云计算，三者几乎形成了“铁三角”的关系。人工智能是以算法为核心，硬件和数据为基础。为了提高专业计算性能，很多互联网公司开始大规模通过使用 GPU 代替 CPU、组建 TPU 或 FPGA 集群等基础设施加速计算，搭建算法平台，加速处理大规模且复杂的数据计算，这将引领云计算到达一个新的高度。比如可以通过 FPGA 实现超高网络带宽的智能网卡，能够基于云计算框架的弹性能力轻松创建 FPGA 实例、自定义专用硬件加速器，可以进行快速擦写和重配，达到低时延硬件与弹性伸缩最好的结合。人工智能在金融领域的应用也越来越广泛，已经从传统的征信与风控、反欺诈、智能营销与客服、智能投顾和投资决策五大典型场景应用向账户、流动性预测、增强现实（AR）以及智能运维等方面开展研究和实践，不断推动金融业务的创新和发展。

2.发展趋势及展望

随着云计算、大数据和互联网技术在金融行业的应用逐步深化，金融行业也迎来变化，金融业拥抱云计算技术恰逢其时。金融和产业在云上相遇，将降低金融成本，提升金融覆盖面。

（1）共同打造金融云生态

互联网企业和传统金融机构各自有自身的能力，相互赋能，科技企业给金融机构赋予云计算、大数据等能力，传统企业为科技公司赋予人员优势、对市场生态的深耕和认知。云厂商、金融

机构、传统软件服务企业共同打造金融云生态，促进金融业发展。

（2）分级分类管理

市场上云服务平台种类繁多，云服务商也各有优劣，金融机构可以根据自身业务系统安全级别要求，选择相应安全级别或更高安全级别的云服务平台。

（3）金融业鼓励发展团体云

云平台本身是一种规模经济，只有达到一定规模的云平台才能真正做到计算能力按需弹性扩展。发展团体云可以降低用户成本，节约社会资源，提供专业化的运营和服务。

（五）行业需要

1.上云需要解决的问题

尽管分布式系统架构、云计算已经成为信息技术发展趋势，但是金融行业要实施架构转型，依然面临巨大挑战和困难。

（1）思想观念重塑。金融机构信息技术部门以使用最成熟稳定的技术，保证系统交易的实时一致性作为基本工作原则，从而确保客户和资金安全。因此，金融机构信息系统架构大都使用经典商用软件和体系架构，并培养了大批熟悉应用相关技术的优秀技术人员。而分布式架构与传统架构相比，在架构、设计、开发、运维、管理上需要有不同的思维和技术能力，会对现有技术团队的思想观念和思维模式造成巨大冲击，需要有一个“脱胎换骨”的转变过程。

（2）关键技术攻关。在分布式架构上，为了适应云计算资

源弹性变化和快速部署等需求，必须有一套成熟的金融级分布式架构体系。分布式架构体系的关键不在分布式的服务调用，而在于分布式的数据存储和数据分布后的事务一致性保障，分布式事务框架和分布式数据库将成为金融级分布式架构的核心能力。目前这样的核心技术能力掌握在少数厂商手中，金融机构转型会面临很大的困难，外购的可选性较小，而此类基础能力自研的难度也非常大，不仅面临研发时间周期较长，短时间很难成熟，还面临不成熟技术交付生产可能带来的风险，这对于金融机构来说往往是不能容忍的。

（3）研发测试运维一体化。金融企业在业务上面临互联网金融带来的冲击，技术上又面临云计算和分布式架构转型，这需要在业务产品上强调用户体验、谨慎试错、持续改进，同时技术上需要支持快速迭代、风险可控、故障快速定位等能力。这些对于传统的研发运维体系提出了巨大的挑战，如何在符合监管的条件下实现敏捷研发、DevOps 等研发测试运维一体化的能力，对金融企业而言既是技术挑战也是管理流程挑战。

（4）现有信息基础设施资产保护。金融机构通常都在现有的信息基础设施上投入了巨资，包括服务器、存储设备、数据库和中间件等软件许可，甚至还包括大量的应用软件，如果要实施云计算与分布式架构转型，就意味着前期巨大的投入将面临淘汰。为了避免完全推倒重建，上云的应用与传统架构下的业务系统必然有一个较长的并行期。在这个并行期中，比较难处理好老应用

迁移节奏、老业务自然增量的扩容压力、新增投资方向等问题，因此云架构转型是一项长期的系统性工程，需要非常精准的组织和管控，以达成最佳的现有信息基础设施资产保护，减少转型投入。

（5）团队能力建设与人才培养。云计算相关技术与传统技术发展路径不同，云计算相关技术往往来自于开源技术。由于开源技术的变化很快，研究这些技术的大多为创新型互联网公司。而互联网公司往往对于金融业务的高一致性、高可用和高安全的理解不足，缺乏对金融应用特点的理解和实践经验。因此，金融机构必须培养和拥有一批既掌握新技术又有丰富金融应用经验的技术人才。

2.行业积累和储备

随着云计算产业和基础设施的完善，国内传统金融机构使用云计算技术主要采用有私有云和团体云两种部署模型，近年来增加了混合云的模式。

对于传统的金融机构，尤其是银行业主要采用私有云和团体云的方式，大中型银行类金融机构中主要以私有云为主，例如工商银行、中国银行等。对于互联网相关的边缘性业务，这些大中型金融机构则会选择团体云或者混合云。个别创新型的互联网银行会采用团体云的上云架构。传统的小型银行则还在积极探索业务上云路线。

（1）金融机构部署私有云主要用于存储、运行重要业务系

统，存储敏感数据，一般采用自购硬件设备和解决方案的方式进行搭建，在生产过程中借助外包驻场实施运维。

（2）金融机构部署团体云主要是通过金融机构间在云计算领域的合作，通过资源等方面的共享，在金融行业内形成公共基础设施、公共接口、公共应用等一批公共服务。金融机构部署团体云主要用于对金融机构外部客户的数据处理、服务，或为一定区域内金融机构提供资源共享服务。

（3）金融机构部署混合云主要用于部署互联网相关的边缘性业务。可以根据特定需求，在团体云上部署虚拟环境，结合在私有云上部署的数据存储，满足一定数据安全的前提下，提高相应的成本效益。

三、上云准备

（一）业务规划

金融机构在实施应用系统上云前必须清醒地认识到，上云不是单纯的技术架构变更，更不是科技部门自己的事。技术架构的变更势必会带来业务习惯的改变。上云无论是对科技部门还是对业务部门来说，既存在机遇，同时又充满挑战，需要两者联手协作，目标一致，共同应对新形势带来的新变化。

1. 业务现状梳理

为了帮助业务部门认清上云对业务带来的改变，科技部门首先需要完成业务现状的梳理，对本金融机构的现有信息系统按照服务类型、技术架构、其他关键因素等维度进行全面摸排检查。

（1）按服务类型划分

从服务类型的角度来说，金融机构信息系统一般包括以下 7 种类型。

（a）渠道服务类系统：如手机银行、网上银行、柜面前端、第三方外联系统等。

（b）客户服务类系统：如客户信息系统、客户关系管理系统、押品管理系统等。

（c）产品服务类系统：如信贷管理系统、贸易融资系统、基金、债券、理财系统等。

（d）核心业务系统：如支付结算系统、基础账户管理及存取款等银行基础业务。

（e）决策支持类系统：如经营分析类系统、监管报送类系统等。

（f）基础平台类系统：如总线系统、安全管理平台、运维监控平台等。

（g）内部支持类系统：如办公系统、人力系统、邮件系统等。

（2）按技术架构划分

从技术架构的角度来说，金融机构信息系统大致可以划分为 3 个类型。

（a）基于大型机的超高可用集中化架构类信息系统，大型商业银行的核心业务系统一般采用此类架构。

（b）基于小型机、集中式数据库等设计的高性能高可靠集中化架构类信息系统，传统银行的绝大多数系统，包括各中小银行的核心业务系统一般都采用此类架构。

（c）以 x86 和集中式、分布式数据库为基础的分布式架构，如各银行新兴的互联网金融类系统，以及办公、人力、邮件等系统出于成本考虑也多采用此类架构。

（3）其他关键因素

进行业务现状梳理时，还需针对每个信息系统标注影响上云规划的其他关键因素，包括但不限于业务规模、业务重要性、业务突发性、是否外包、近期是否有较大业务需求变更等因素，最终形成信息系统的分类梳理表。

2. 上云优先级确定

根据业务现状梳理和分类的结果，科技部门需对各类信息系统上云的必要性和可行性进行评估，进行上云优先级划分，并根据评估结果及确定的优先级合理规划上云路线图。对于新建系统，如果没有技术瓶颈及其他特殊情况，通常情况下首选云服务架构，优先级设定为最高。已有系统可以参照高优先级、次优先级、中优先级、低优先级的四级划分标准，将信息系统对应到所属的优先级。

（1）高优先级：此类系统的云化部署不会改变现有业务系统的技术架构，技术成熟度普遍较高，可以直接进行迁移上云，同时会带来较明显的价值效益提升。此类系统一般包括现有运行

在 x86 架构下的互联网金融类系统及内部支持系统。对于渠道服务类系统，要综合考虑系统现状、业务规模及实施难度，可以在高优先级批次实施上云，也可以将其设定为次优先级系统，在积累了一定经验后再行上云。

（2）次优先级：此类系统具有一定的上云改造需求，改造难度相对较低，本身具备分布式架构体系，改造对于总体架构影响不大，通常只需要进行接口对接、数据对接等小范围改造。另外对于有明显的业务负载周期特性，相对短的时间内可能有突发性大业务量的系统，因为对资源横向扩展要求很高，上云的业务收益很大，也应该设定为次优先级。此类系统主要包括客户服务类系统、基础平台类系统中的大部分系统，及决策支持类中的一小部分系统等。

（3）中优先级：此类系统的原有部署模式主要是基于高可靠高性能的小型机和集中式数据库，云化部署之前需完成总体架构改造，从集中式架构转为分布式架构，考虑分布式事务、分布式存储等一系列重要问题，具有一定的改造难度，因此该类系统一般都是在有重大业务需求变化时，随业务的应用设计同时考虑技术架构的变更，另外在实施该类系统的上云方案前，金融机构应该已经完成了高优先级及次优先级信息系统的上云，建立了相对较为完整的上云规范，积累了较多的上云经验。此类系统一般集中在产品服务类系统和决策支持类系统。

（4）低优先级：此类系统通常是金融机构最复杂、集中化

程度最高、一致性及可用性要求最强、改造难度最大的系统，基本上都是基于大型机的超高可用集中化系统。云化部署需要对总体架构进行分布式重构，应充分考虑应用、计算及存储的分布式架构改造、与其他业务及服务对接等，通常需要投入大量资源和较长的改造时间，业界尚无经过长期实践检验的成功案例。此类系统是金融机构的核心业务系统，牵一发动全身，在没有做好万全准备之前不要轻易进行上云尝试。

优先级确定后，科技部门需要跟业务部门积极沟通，向业务部门说明上云改造中及改造后对业务模式的影响，充分听取业务部门的意见，与业务部门达成一致。获得业务部门的支持是信息系统上云成功的重要前提条件。

（二）技术规划

解决了什么系统上云的问题，紧接着要回答的是上什么云、怎么上。这同样不是科技部门自己的事，需要与云服务商通力合作，选择合适的云基础设施及应用的云化改造方案。

1. 云服务商调研

金融机构在选择云服务商之前，需要对云服务商进行充分调研和评估，重点考察云服务商的资质与合规、服务类型、管理能力、技术能力、服务能力、经营能力等关键领域。

（1）资质与合规：评估云服务商是否符合法律法规和监管机构的准入要求，且通过金融云备案，具有面向金融机构提供云产品与云服务所需的各类资质，并满足上云部署前中后各方面的

合规要求，包括《云计算技术金融应用规范 技术架构》《云计算技术金融应用规范 安全技术要求》《云计算技术金融应用规范 容灾》等。

（2）服务类型：评估云服务商能够提供何种类型的云服务，并可参考《云计算技术金融应用规范 技术架构》，评估是否可提供虚拟机、存储、负载均衡、内容分发网络、物理机、虚拟私有云、网络连接、域名等 IaaS 层服务，数据库、中间件、分布式数据处理、容器服务等 PaaS 层服务等。

（3）管理能力：评估云服务商是否具备有效的内部控制机制，明确管理机构与人员职责，建立有效的管理制度，完善管理规范和流程设置，并能够快速响应和处理云客户的需求，满足金融行业监管机构要求的外包管理办法。

（4）技术能力：评估云服务商是否具备面向金融机构提供稳定服务所需的技术能力，包括稳定可靠的云平台、成熟的资源（包括网络、计算与存储）管控能力、高效的运维支撑能力、安全保障能力、金融级业务连续性保障能力、快速响应与应急处置能力、满足业务快速上线、迭代、升级等诉求。

（5）服务能力：评估云服务商是否具有提供持续稳定高质量服务的能力，且服务流程完备，服务团队配置充分，能够提供上云部署前设计和咨询、上云部署的支持和配合、上云部署后的高效运维、快速响应、7*24 小时技术支持等服务能力。

（6）经营能力：评估云服务商是否具有持续经营的能力以

及丰富的云服务运营经验，可从云服务商从业时间、财务状况、市场地位、金融云服务案例、管理规范性、技术成熟度等方面，对云服务商的持续经营能力进行评估。

2.上云方案原则制定

金融业的行业特性决定了强监管、绝对安全是其基本要求，另外提高成本收益比、资源利用率，构建统一调度的计算与存储能力、全网融合的数据资源和高可用共享的平台服务，也是金融机构选择上云的初衷。目标决定原则，基于上述要求，金融机构在制定上云方案时应该遵守以下原则。

（1）监管合规：上云方案需能够满足金融业监管合规要求，根据相应的监管文件来选择私有云、金融团体云、混合云等不同形式的上云方案。监管合规是选择上云方案的底线原则，决不能突破。

（2）安全防护：上云方案对于安全合规要求的满足程度（如等级保护、金融行业安全监管与检查等），着重考虑云化技术引入的新安全风险（如物理资源隔离、虚拟资源隔离、虚拟资源内部安全管控等）。

（3）成本收益：上云方案可以带来明显的价值和效益提升，降低资源投入成本，增强用户使用体验。上云是手段，不是目的，绝不能为了上云而上云，必须考虑成本收益比。

（4）弹性扩展：上云方案可显著提升资源的弹性配置，能够通过很少的改动甚至只是硬件资源的增加，就能实现系统处理

能力的线性增长，支持业务规模的快速扩展，应对业务促销带来的爆发式流量增长。

（5）统一管控：统一规划，建设和选择云数据中心，做好顶层设计和规划，综合考虑当前业务需求及未来发展需求。统一基础资源平台，并打通系统与应用之间的沟通障碍，实现统一集中的运营运维管理。

（6）资源共享：通过共享的平台服务及数据应用，可以不断提升自身的开发效率，整合数据资源。上云方案的设计同样应遵循资源共享原则，尽量利用已有通用服务和数据。

（7）业务可用：上云方案需充分考虑冗余、容错设计，合理规划应用架构和技术架构，保证系统的故障自愈能力、容灾备份能力、按需切换能力，以提升系统的可用性、业务连续性及数据一致性。

（8）承前启后：上云方案既要着眼于新系统的建设，也要关注已有系统的利用和整合，更要重视技术体系的可持续发展及向后兼容性，充分考虑应用现状和未来发展趋势，不盲目追新求快，尽量选用先进成熟技术。

（9）业务敏捷：上云方案要支持业务敏捷性，支持业务应用的敏捷开发、快速迭代、快速上线、支持业务创新。

（三）方案设计

设计上云方案时应全面考虑应用架构、数据架构、技术架构、安全架构，以及与云服务相关的其他各类规划、管理要求、处理

流程，涉及金融机构信息系统建设的方方面面。各机构需结合自身信息化建设现状及治理能力、规章制度，有针对性地制定符合自身业务战略规划、科技发展规律的上云方案。

1.应用架构设计

上云系统的应用架构设计应符合分层模型要求，有清晰明确的分层设计框架，各层之间须确保解耦，层次之间通过接口调用，不强依赖其他层次的组件。严格定义各层级的功能职责和约束，使各层级具有职责单一、功能独立、可复用、易扩展等能力，以便为应用系统云化提供架构支持。对于符合云原生场景的应用，应尽量采用云原生架构进行设计。按照系统内部组件的功能特点，一般可以抽象出接入层、应用层、数据层 3 个层级。

（1）接入层：负责接受用户的数据输入并向用户呈现数据，或接收外部调用请求并返回调用结果，需要与应用层交互。

（2）应用层：针对具体问题的业务逻辑处理，对上承接接入层，处理接入层的请求，返回请求结果；对下是对数据层的抽象操作，将对数据的基础访问逻辑（增删改查）组合起来，完成数据访问。

（3）数据层：也称为持久层，主要负责系统业务数据的持久化和访问，为上层业务逻辑的实现提供数据支持，可以是数据库系统、文件系统、XML 文档或分布式缓存等。

2.数据架构设计

从当前金融行业的应用现状看，以集中式架构为主，传统集

中式架构适用于高度结构化的数据集，所有数据存放在一个数据库，通过一个服务访问，可以实现交易数据强一致性，但是云上需要使用分布式架构，而分布式架构以切分任务及数据达到并行处理的效果，对强一致性要求较低，只能实现最终一致性，且金融行业业务数据量巨大，客户账户数量动辄上亿，无论集中式数据库或分布式数据库均存在容量和连接数上限，因此在数据架构设计时，需要根据分布式架构的特点及业务特性对数据切分策略、数据路由策略、数据库部署、单元划分、服务拆分进行重点考虑，最终目的是在分库分表的基础上，通过流量收敛，突破单库的物理限制和连接数限制，同时减少分布式事务。

（1）数据切分策略：可按客户或机构或者其他业务特性维度进行切分，一批数据归属到一个数据节点进行管理，物理上对应一个数据库实例。

（2）数据路由策略：基于数据访问引擎，根据数据切分要素选择对应的数据库实例（数据分片）。对于采用单元化架构的信息系统，可考虑 2 层路由模式。网关层映射至对应部署单元，单元内再选择数据分片。

（3）数据库部署：根据信息系统的数据量、交易量及其他因素（如数据库产品、技术掌握度等）选用集中式或分布式数据库，考虑主副本个数、部署地及数据复制策略。

3. 技术架构设计

上云系统的技术架构设计极其复杂，涉及基础设施、存储、

网络等一系列考量因素，以及单元化架构、多云设计、云原生等特定技术带来的影响。

（1）云基础设施架构设计：结合金融机构自身业务需求，云服务商需提供定制化的云产品体系、云资源规划、云统一管理，设计符合金融机构未来规划的云基础设施架构体系。

（2）部署架构设计：云平台部署架构需要秉持高弹性、开放性、互通性、高可用性、数据安全性等原则，具体部署设计要求参照《云计算技术金融应用规范 技术架构》。

（3）云存储架构设计：从分布式数据库、分布式文件系统的部署架构、逻辑架构、缓存架构、数据安全等角度综合评估云存储架构方案的设计，需要保障整个存储架构可以在资源池内实现动态扩缩容，以及内部数据动态均衡。

（4）云网络通信设计：网络通信涉及云内、云间、云外 3 种不同分类。每种分类下又有各种不同的典型网络通信场景和部署架构，如云外网络通信涉及云平台与传统数据中心、各分支机构、广域网之间的通讯配置。需要金融机构与云服务商、运营商一起合理规划，统一布局。

（5）云单元化架构设计：按需通过单元化部署使整体架构具备异地多数据中心并行计算能力，同时基于金融级的分布式关系型数据库，通过多机房部署实现城市级故障下数据无损容灾切换。

（6）多云管理设计：对于规模较大的金融机构，可能不止

一朵云，也会存在各类异构资源池，因此需考虑混合云管理、两级云管理、一云多池管理等不同形态的云管方案，实现云管平台的统一纳管、完整视图。对于云原生应用和技术平台，通过云原生的多云管理实现更一致的多云应用管理。

（7）云原生架构设计：可以通过容器化部署、微服务、服务网格、云原生运维等云原生技术提升研发迭代效率，进行更精细化的高可用保障。

4.安全架构设计

相比传统数据中心的信息系统安全，要分析云环境特有的安全威胁及脆弱性，讨论应对云安全威胁的方法以及安全趋势和将来有可能遇到的威胁。全面保障应用系统在网络、操作系统、中间件、业务数据方面的安全。在应用运行的全生命周期中通过链路加密、服务鉴权、数据库鉴权等安全技术实现全链路的安全可信加固。安全架构设计要考虑组网、操作系统、中间件、业务数据等安全策略。

（1）组网安全：组网安全是指应用上云部署时的网络部署策略，需同时考虑应用与外部其他应用之间的组网安全，以及应用内部不同节点间的组网安全。

（2）操作系统安全：操作系统安全是应用安全的基础，操作系统安全包括操作系统与服务、系统访问认证和授权等。

（3）中间件安全：中间件的默认配置一般都存在安全风险，需根据应用安全需求修改相关配置。

（4）业务数据安全：业务数据安全主要包含业务自身的安全措施，包括传输安全、防攻击、敏感数据、数据库安全等。

5.灾备管理设计

云平台容灾系统建设是一项复杂的系统工程，依托于数据复制技术和网络切换恢复策略，把金融企业的重要信息系统在灾备中心重新规划设计。

（1）总体设计原则

容灾系统的设计将遵循技术先进性、可扩充性、高可靠性、高可用性、业务连续性、成熟性、可实施性、可管理性、投资保护的总体设计原则。

（a）技术先进性原则：系统设计采用当前先进且成熟的技术是十分必要的，不仅可以满足金融企业业务连续性需求与策略，同时可以把握未来金融企业的业务及信息科技发展方向。

（b）可扩充性原则：在系统设计时要充分考虑可扩充性，从而确保新功能、新业务在原有的系统平台上顺利扩展和实现。

（c）高可靠性原则：充分保证系统的高扩展能力和高容错能力，具有自动负载均衡能力和性能调节能力，同时提供充分的可靠性指标设计。

（d）高可用性原则：容灾系统在不停机的情况下，实现扩容、维护、升级等服务，提高性能以满足新的业务需求，具备7*24小时连续工作的能力。

（e）业务连续性原则：采用先进的复制技术、主机切换技

术和负载均衡技术，保证生产中心发生灾难时，容灾中心能平滑接管生产中心运行，以满足业务连续性要求。

（f）成熟性原则：尽量选用经过大量运用、成熟可靠的技术和产品系统。

（g）可实施性原则：选用成熟的技术，成熟的案例和最佳实践作为方案设计的出发点，制定详细的技术实施方案。

（h）可管理性原则：为确保容灾系统的可用性，对容灾中心关键硬件设备和系统软件平台进行实时监控是十分必要的，包括对 CPU 使用率、内存使用率、交换区使用情况、I/O 操作、队列状态、磁盘空间、卷磁盘错误、系统事件、系统中各进程对系统资源占用等性能进行实时监控和管理。

（i）投资保护原则：在考虑金融企业容灾系统高性能和高可靠性的同时，还必须考虑投资的合理性，不能一味追求不切实际的先进性。

（2）应用等级划分

上云系统按照不同的服务等级协议（SLA），需确保业务应用系统的连续性设计满足灾备管理的要求，避免出现因可靠性设计偏差导致的服务降级问题，可以按照详细的恢复时间目标（RTO）、恢复点目标（RPO）指标要求对应用等级进一步细分。

（a）关键业务系统：指标要求：RTO≦2 分钟，RPO=0；分级描述：业务系统每年非计划服务中断时间不超过 5 分钟，系统可用性至少达到 99.999%。

（b）一般业务系统：指标要求：RTO≦4 小时，RPO≦1 小时；分级描述：业务系统每年非计划服务中断时间不超过 10 小时，系统可用性至少达到 99.9%。

（c）办公业务系统：指标要求：RTO≦24 小时，RPO≦24 小时；分级描述：业务系统每年非计划服务中断时间不超过 4 天，系统可用性至少达到 99%。

对于关键业务系统，在容灾、实时备份基础上，需要设计双活数据中心的业务模型；对于一般业务系统，需要做好容灾、实时备份；对于办公业务系统需要做好容灾。

四、上云实施

根据不同的上云形态（私有云、金融团体云、混合云），与相应的云服务商合作完成云基础设施平台部署。金融企业需确保与云服务商签订规范的合同，有助于提升服务质量，最大程度地降低对于特定厂商的依赖度，同时重点关注平台自身的管理、资源池、容灾建设和对上层应用提供的支撑服务。

上云实施过程一般分为应用上云、上云测试以及上云后效果评估 3 个阶段。

（一）应用上云

根据不同的应用系统的业务和技术复杂度，确定可行性方案，以分步的方式实施不同的上云策略，可分为：直接上云、改造迁移上云、重构迁移上云、不适合上云。

1.直接上云

云化部署不会改变其现有技术架构的应用，可直接上云。这部分应用需要摒弃传统信息系统架构，采用云原生、微服务、分布式系统架构来构建核心业务系统，以适应快速迭代、高交易量等要求，提升服务效率、改善客户体验，实现应用运行环境标准化。如手机银行、微信银行、第三方支付、积分系统、人力资源系统、流程管理平台等。

2.改造迁移上云

在不影响业务的情况下，应用的总体架构没有太大变化，通过改造接口、工具或数据对接等可以满足应用改造上云的需求，且改造后对应用的管理和价值效益有较大提升的，可以采用改造迁移上云。如客户关系管理系统、营销系统、直销银行、反欺诈系统等。

此类应用在进行改造时要考虑使用云原生相关组件，包括但不限于:

（1）采用容器化平台技术，提供高资源利用率、弹性伸缩、自动化秒级扩展的云平台基础架构。

（2）采用微服务框架，支持灵活、敏捷的业务快速迭代模式。

（3）采用多集群功能管理，支持异地多中心部署方式，实现服务负载分流、故障切换和统一管理。

（4）采用 DevOps 工具集成，包括利用可视化编排工具设计构建流水线，并完成服务更新、负载均衡设置、自动通知等功能。

3.重构迁移上云

现有应用或业务模型无法通过技术改造满足上云条件，需要对业务或者技术架构进行拆分或重构，此类应用需要强有力的技术支持，以云化的方式重新对业务系统进行设计，除此之外，还需要考虑云化架构的性能、业务数据迁移的可行性、需要投入的人力财力和改造时间等其他因素，有一定的业务风险。例如核心系统、卡系统、柜面系统、支付系统等。

4.不适合上云

部分应用由于多种因素导致现有的应用程序无法通过改造或重构的方式实现入云。

（1）硬件限制，如使用加密机等特殊硬件、使用语音板卡等特殊外设或板卡等。

（2）第三方产品限制，如需要固定 IP 地址或固定主机名等。

（3）存在许可问题，如应用 License 跟硬件强相关，云上弹性反而导致 License 失效影响业务。

（4）存在特殊属性要求的应用，如拥有高度机密的数据，上云可能增加数据泄密风险。

（5）对单一计算或存储能力有极高要求，不适合云化部署。

（6）其他限制，依赖其他云平台不支持的技术或服务能力。

（二）上云测试

上云测试包括功能测试、性能测试、可靠性测试、安全测试等。由于私有云、金融团体云、混合云模式下的云服务提供方有

所不同，因此测试所涉及的范围及方法也存在差异。

1.功能测试

上云后依据内部要求针对金融服务业务系统开展功能性测试，确保金融服务业务系统满足业务需求。

（1）私有云：需要私有云厂商提供所交付的私有云环境当中在 IaaS、PaaS、SaaS 等各个层面使用的系统、网络、软件的功能设计文档。并由云服务商提供功能验收测试方案，明确功能验收测试的方式、人员、环境、标准和文档等，由金融机构进行评审并协助进行功能测试，并最终由金融机构对测试结果进行验收。

（2）金融团体云：在金融团体云的模式下，云环境底层的物理设施、网络和系统归属于云服务商，金融机构作为云服务的使用者具备自身租户的管理权限。因此在此种模式下，金融机构需要按照所使用的云平台和云产品的需求，要求云服务商提供云平台所涉及的 IaaS、PaaS、SaaS 等各层面所通过的功能检测认证报告或证明。

（3）混合云模式：在混合云模式下，建议根据混合云的构成，参照私有云、金融团体云的功能测试模式进行分工，并设计整体功能测试方案。

2.性能测试

上云后依据业务需求，对服务网络的网络延时、数据库 IO 读写性能等进行全链路压测，确保信息系统性能满足业务需求。

（1）私有云：需要私有云厂商提供所交付的私有云环境当中在 IaaS、PaaS、SaaS 等各个层面使用的系统、网络、软件的性能设计文档。并由云服务商提供性能验收测试方案，明确功能验收测试的方式、人员、环境、标准和文档等，由金融机构进行评审并协助进行性能测试，并最终由金融机构对测试结果进行验收。

（2）金融团体云：在金融团体云的模式下，云环境底层的物理设施、网络和系统归属于云服务商，金融机构作为云服务的使用者具备自身租户的管理权限。因此在此种模式下，金融机构需要按照所使用的云平台和云产品的需求，要求云服务商提供云平台所涉及的 IaaS、PaaS、SaaS 等各层面所通过的性能检测认证报告或证明。

（3）混合云模式：在混合云模式下，建议根据混合云的构成，参照私有云、金融团体云的性能测试模式进行分工，并设计整体性能测试方案。

3.可靠性测试

上云后针对云计算平台软件、主机、存储、网络节点、数据中心以及业务应用等层面进行可靠性测试，确保金融服务能够从严重故障中快速恢复。

（1）私有云：需要私有云厂商提供所交付的私有云环境当中在 IaaS、PaaS、SaaS 等各个层面使用的系统、网络、软件的可靠性设计文档。并由云服务商提供可靠性验收测试方案，明确

功能验收测试的方式、人员、环境、标准和文档等，由金融机构进行评审并协助进行可靠性测试，并最终由金融机构对测试结果进行验收。

（2）金融团体云：在金融团体云的模式下，云环境底层的物理设施、网络和系统归属于云服务商，金融机构作为云服务的使用者具备自身租户的管理权限。因此在此种模式下，金融机构需要按照所使用的云平台和云产品的需求，要求云服务商提供云平台所涉及的 IaaS、PaaS、SaaS 等各层面所通过的可靠性检测认证报告或证明。

（3）混合云模式：在混合云模式下，建议根据混合云的构成，参照私有云、金融团体云的可靠性测试模式进行分工，并设计整体可靠性测试方案。

4.安全测试

上云后要立即开展安全风险评估以及实战性安全攻防演练，确保信息系统以及云平台本身的安全性。

（1）云平台的安全测试

私有云：需要私有云厂商提供所交付的私有云环境当中在 IaaS、PaaS、SaaS 等各个层面使用的系统、网络、软件的安全设计文档、安全加固文档、安全测试报告及私有云安全产品使用手册和最佳实践指南。并由云服务商提供安全验收测试方案，明确安全验收测试的方式、人员、环境、标准和文档等，由金融机构进行评审并协助进行安全测试，并最终由金融机构对测试结果进

行验收。

金融团体云：在金融团体云的模式下，云环境底层的物理设施、网络和系统归属于云服务商，金融机构紧作为云服务的使用者具备自身租户的管理权限。因此在此种模式下，金融机构需要按照所使用的云平台和云产品的需求，要求云服务商提供云平台所涉及的 IaaS、PaaS、SaaS 等各层面所通过的安全检测认证报告，机构所采购的应用、系统和网络的安全测试报告、安全渗透测试报告等内容，确保机构所购买和使用的云平台、云产品是安全的。并由金融机构根据云服务商提供的材料来评估是否需要制定进一步的测试方案进行测试，以确保所使用的云平台和云产品是符合安全要求的。

混合云模式：在混合云模式下，建议根据混合云的构成，参照私有云、金融团体云的安全测试模式进行分工，并设计整体安全测试方案。

（2）上云后业务的安全测试

私有云：业务在私有云部署模式下，需要重点关注上云之后应用系统提供服务所使用的网络资源、计算资源的差异性，并有针对性的进行安全测试，如上云之后虚拟化、容器化部署模式带来的差异性，在入侵、提权方面是否引入了新的攻击面，以及云平台所提供的安全加固方案和监控措施是否可以有效的防护，防护措施如何和未上云的业务有效配合等，与云服务商制定相应的测试方案和计划进行专项测试，并针对测试内容制定并建立有效

的安全基线和纵深防御机制，定期巡检确保业务上云后的状态是符合安全预期的。

金融团体云：业务在金融团体云的部署模式下建议参照云服务商提供的安全方案和最佳实践进行布防，借助云平台提供的安全能力针对上云后的应用、系统和主机进行定期的安全扫描和测试，防御层面建议借助云服务商提供的防控能力控制风险，发挥出平台所提供能力的最大价值。根据整体的防控方案以及各应用上云后的业务场景制定安全测试和验收方案，确保上云后的业务是符合安全预期的。

混合云模式：混合云模式下建议不同形态的云环境参照如上所述的私有云、金融团体云的模式实施安全测试。

（3）实战检验测试

上云后的业务及云平台需通过实战演练的方式全面验证上云后的业务及关联云平台的安全状况，确保上云后的业务及所使用的云平台的安全性是符合预期的。建议邀请多家有资质及实战经验丰富的安全公司组成专业的测试团队进行验证，并形成最终测试报告，以充分暴露风险并进行整改优化。

（三）效果评估

通过推进金融企业应用上云，将在高可用、性能、自动化、自服务、统一云管等方面带来全面的提升。上云后的效果评估主要从资源利用率、业务效率两方面进行衡量。

1.资源利用率

实现计算资源、存储资源、网络资源集约化处理，借助云平台弹性伸缩能力，可对同等硬件条件下性能、资源利用等方面的提升情况进行评估，主要包括应用系统性能（例如TPS、并发数）、应用节点资源利用率及云平台资源利用率等。

（1）TPS：每秒能处理的事务数量，可以直接体现应用系统性能的承载能力。通过与传统物理环境部署的应用 TPS 指标进行对比，关注应用上云后性能指标差异。

（2）并发数：应用系统同时能处理的事务数，也是反映该系统性能的关键指标。通过与传统物理环境部署的应用事物处理并发数进行对比，关注应用上云后性能指标差异。

（3）应用节点 CPU 利用率：关注应用系统的 CPU 利用率，如果长时间处于高负载，需要考虑进行规格扩容。

（4）应用节点内存利用率：关注应用系统的内存利用率，如果长时间处于高负载，需要考虑进行规格扩容。

（5）云平台资源利用率：关注包括计算、存储、网络等各项资源的使用效率，如计算资源利用率，通过物理 CPU 的平均使用率除以虚拟 CPU 的平均使用率进行计算，值越小表示计算资源利用率越高。

2.业务效率

通过实现对云资源的多渠道、可视化、自助式的服务申请和使用，规范资源管理方式，提升应用高可用能力，使金融企业应用研发更专注于业务开发，降低对基础实施投入，可从应用开发

效率、应用迭代水平等方面进行评估。例如，将上云后通过借助云原生 DevOps 平台形成开发测试运维一体化流程后的研发效能与传统模式下的研发效能进行比对。

五、上云后管理

完成企业应用上云后，需要围绕运维管理、风险管理等方面开展上云后管理工作。

（一）运维管理

运维管理包括监控管理、告警管理、巡检管理、变更管理、容量管理以及资源管理等。

1.监控管理

可以从云计算物理资源、云平台管理组件状态、云化资源 3 个层面进行监控管理，构建一站式、自助化、可视化监控管理能力。

（1）监控管理能力

监控管理能力至少包含以下方面。

（a）监控模板化，内置精炼的监控模板，支持自定义监控项扩展，在满足监控要求的同时，尽可能降低监控采集压力、保证监控高效性。

（b）配置一站式，通过一至两个配置页面完成集中化一站式配置，简化监控告警规则及策略配置，降低使用成本与操作门槛。

（c）支持代理与无代理混合纳管方式，结合主动推送与被

动轮询，实现监控数据灵活采集、高效上送。

（d）可视化，将监控告警通过可视化界面进行呈现。

（2）监控纳管范围

监控纳管范围至少包含以下方面。

（a）带外，支持服务器 IPMI 接口，实现硬件监控。

（b）带内，支持 SNMP、SMI-S、JMS、JDBC、REST 等接口，实现物理网络设备、存储设备、云平台运行组件依赖的数据库、中间件监控。

（c）IaaS，内置面向云管平台和云服务资源的采集适配器，支持灵活扩展，实现计算、存储、网络等云化资源采集与资源监控，满足 IaaS 云监控管理需求。

（d）PaaS，与 IaaS 类似，具备 PaaS 云管接口采集与监控能力，也可以通过容器管理接口，直接对容器资源监控管理。

（e）需与原有监控平台集成，实现监控、告警、资源配置等运维数据信息的共享和联动。

2.告警管理

告警管理要主动探测云环境运行故障，并及时处置。

（1）提供告警生成、通知、操作以及关联分析等告警功能。支持通过统一数据接口集成对接原有监控平台，实现告警的统一管理。

（2）灵活生成云运维监控关注的告警信息。基于静态基线与动态基线的告警配置管理策略，实现告警的过滤、压缩抑制、

丰富、升级、生效时间（或时段）设置等。告警通知策略管理则可以根据时间、告警级别、发生资源等条件选择用户或者用户组，结合短信、邮件或移动运维 APP 等通知方式，实现告警实时通知。

（3）实时呈现告警。告警发生后，及时呈现在告警视图界面，提示云运维管理人员进行告警确认与处置，并实时转派紧急、重要告警。

3. 巡检管理

巡检管理是作为监控管理的补充，通过主动的运行状态检查和合规检查，结合自动化手段，协助定位和分析故障，保障云平台的高可用，有效提升客户感知，主要包括如下内容。

（1）例行检查服务器、网络设备、防火墙、负载均衡设备、控制器运行，对云环境的运行状态进行自动化检测分析，深度感知融合基础架构运行状态。同时实时输出准确、详实的分析报告及改进建议，预防设备运行中可能出现的各种风险，发现设备潜在的性能瓶颈。

（2）根据金融机构业务等保要求，结合云平台运维规定，编排主动检查策略，定期进行云平台软硬件环境合规检查。

（3）对接安全合规检查、第三方安全扫描结果，自动实现安全加固。

4. 变更管理

变更管理是控制变更操作的平台，是进行变更操作的入口，实现变更操作的审批和审计管理。

变更管理通过一个单一的职能流程来控制和管理整个云环境中的一切变更，并支持和资源配置管理建立接口连接。变更管理在实际应用中由管理工具来支持，管理工具提供图形化流程设计器，支持变更流程的自定义设计，通过可视化的流程设计器，快速实现变更流程的在线设计及发布管理。变更审批和变更审计的具体实现如下。

（1）变更审批：可根据变更的优先级，分类等信息，配置变更的审批级别及审批人，当变更执行到审批环节，系统可自动获取审批人，并将工单分派给审批人进行审批，审批结束后，回到变更主流程处理。支持串行审批，并行审批的方式。也可以在提交审批前，单独为工单增加临时审批人或者审批组。

（2）变更审计：支持对历史变更记录进行查询和统计，并对关键的字段设立审计功能，当特定字段发生变化时，自动生成日志，记录何时由谁把哪个字段由原始的什么值改为了新的属性，并由管理员进行查询和审计。通过上述日志系统自动记录事件、问题、变更、配置中特定字段的变化（创建、修改、删除等），对一个处理流程中的所有操作过程都会在日志文件中产生记录，并可以被浏览和审核，同样可以记录每一个资产配置项在整个生命周期内的变化，例如何时由哪个员工对云主机升级了补丁程序等。

5.容量管理

金融业用户上云后，普遍存在容量性能评估难，资源难以有

效分配的问题。一方面，宿主机上的各个虚机之间对宿主机资源是既争用又共享，云化后，原有传统的CPU、内存占用率监控已失去指导意义，不能代表虚拟机是否存在资源瓶颈。另一方面，难以判断物理服务器资源是否得到了充分利用、虚拟机密度是否恰当等。

为解决以上问题，云环境的容量管理分为容量优化管理和容量规划管理两方面。

（1）容量优化管理要关注优化资源配置，提高现有资源利用率。发现并回收低效、未使用的资源，以便合理调整虚拟机大小、回收闲置资源，在不影响业务和性能的情况下，优化资源整合和虚机密度。

（2）容量规划管理要关注容量不足和超额配置情况，以提前规划云资源的扩缩容，指导采购，并规避资源风险。

6.资源管理

资源管理包括资源申请、资源配置、资源回收等资源全生命周期管理。伴随着应用的持续新增和迭代，IP、域名、虚拟机、裸金属、容器、镜像等资源会源源不断的生成，相应的机制能否有效的运用对于应用上线后的风险敞口及风险处置的成本投入起到至关重要的作用。

（a）资源申请阶段，关注资源申请的渠道是否符合安全要求、资源预算消耗等要素，确保新增应用关联的主机、镜像、IP、域名等资源具备安全、合规、有效的管理机制。

（b）资源配置管理贯穿整个运营的所有环节，适时的对变更的内容和场景建立事前、事中和事后的管控和防护机制，包括但不限于变化发生前的安全评估和检查、变化发生中的安全组件集成及防护能力的配置。

（c）资源回收阶段需要建立好充分的关联分析。例如针对应用使用的临时通道及帐号权限进行撤销和回收，保障建设期间的风险是可控的。对已经下线废弃的云主机、数据库进行及时的数据清理及策略的回收，防止造成敏感的信息泄漏及安全策略绕过等风险。基础设施的销毁处置阶段，除了常规的系统、数据的清理和格式化操作外，还需要对上线的安全策略进行回收，确保整个回收过程是完整且安全的。

（二）风险管理

金融业上云需加强上云业务的安全管理措施，体系化的防控方案可有效控制系统上云后的业务连续性风险、信息安全风险及合规性风险等，保障上云业务的风险可控。

1.风险防控措施

风险防控包括业务连续性风险防控和信息安全风险防控两方面。

（1）业务连续性风险防控

金融业上云后需要保障可以给用户提供持续稳定的业务服务，在业务的连续性风险防控体系上建议做到如下几点防控措施。

（a）异地多活，需最大程度发挥上云后分布式架构带来的

优点，例如私有云建设中需将基础设施、计算、存储、网络资源的软硬件部署采用分布而非集中的部署模式，满足灾备建设与业务连续性的要求。

（b）弹性架构，需要具备按需弹性伸缩的能力，在面临流量高峰的时候可以快速弹性扩展，扩充资源和应用处理能力，当应用流量高峰过后，可以快速释放资源，以达到最大程度的资源利用率。弹性业务要具备局部性和临时性特征。

局部性，弹性业务单元只需要包含单元内的部分应用和部分数据即可，通常是高流量链路涉及的相关应用。

临时性，区别于普通业务单元长生命周期的特点，弹性业务单元的生命周期是比较短的，在支持类似“双 11”这样的大促支付高峰后，弹性业务单元的业务请求会弹回到常规业务单元，随后会对弹性业务单元进行释放，以节省成本。

（c）分区发布，需拆分出研发环境、系统集成测试环境、灰度生产环境、生产环境等不同环境。其中灰度生产环境须与和生产环境进行同代码、同配置、同数据库的部署，保障业务处理能力一致。灰度生产环境定位为白名单人员准入，用于验证产品和系统功能，第一时间发现业务和系统问题。

（d）变更防控，需建立与应用重要等级相匹配的变更风险管控机制，根据系统重要性生成不同的审批路径，具备如下特点：对变更前置条件进行校验；通过比对变更参数规避风险；通过代码自动实现人工查看日志、监控、系统指标等，建立全栈的变更

感知能力，一旦出现异常时，可以快速响应及判研，并关联到变更操作，有效缩短应急时间。

（2）信息安全风险防控

金融业上云可以提升数字化转型的进程，提升资源管控和变更效率，在信息安全风险防控体系建设上也需结合上云特点制定安全防控方案，满足金融行业高安全性的要求，规避安全事件的发生。在安全架构设计上建议包含以下部分。

（a）默认安全机制，金融机构上云后的资产及目标实体变更，需具备与上云前一致的变更管控与安全加固能力。需要将上云后的资产通过云平台提供的接口与金融机构的资产及运维平台进行对接，针对云上的运维操作全面感知。同时针对已知的漏洞和风险配置，尤其是上云后引入的新的配置项需进行重点加固。并充分利用上云后新增的云 WAF、云防火墙及态势感知的能力，将变更的资产接入到网络、主机等各个层面，提升整体防护效果。只有当安全准入控制机制做到前面所有的加固措施后，才允许上线。

（b）可信纵深防御，金融机构上云后充分发挥上云后引入的可信计算及云原生技术体系的优势，结合零信任的思想，建立应用及不同资源间的授权、认证、加密能力，通过可信计算能力建立完备的信任链，做到只允许预期内的行为可以成功访问的防护效果。最终建立覆盖终端、网络、应用、数据库等各个层面的信任点，从而形成完备的信任链，打造可信级的纵深防御体系。

（c）数字化与智能化，金融机构需要充分利用云平台提供的数据采集、资源管控和可视化等基础产品能力，将所有目标实体相关的信息进行采集并转换为数字模型，通过任务编排来自动化管理各类安全任务，并沉淀能力朝着智能化的方式转变。

（d）实战演练经验，针对云架构建设的安全防控能力和体系的有效性，需要通过实战化的安全对抗进行检验。因此需对上云后所面临的攻击路径设计攻击演练机制，进行定期演练，验证防控机制的有效性以及风险控制的效果。

2.云服务商管理

针对上云后可能存在的风险，需要同时做好对云服务商的监督管理，并从以下几个方面加强风险管理要求，持续优化风险控制措施。

（1）云服务商要组织评估本金融机构面临的风险状况，找出可能影响金融机构服务结果和服务承诺的风险要素，制定风险管理策略。

（2）云服务商要定期开展风险评估工作，向金融机构提供风险评估结论，并依此决定采取风险防范的措施和方法，对风险进行分级管理。

（3）云服务商要建立健全各项管理与内控制度，设立专门风险管理岗位，监督和检查各项规范、制度、标准和流程的执行情况以及风险管理状况，持续监督风险管理状况，及时预警，将风险控制在可接受水平。

（4）云服务商要建立信息安全事件管理机制，定期向金融机构提供信息安全事件统计和跟踪改进的报告，重大信息安全事件随时报告。

（三）变更及退出

1.服务变更

对于服务变更，需由金融机构发起服务变更请求，云服务商应及时响应，制定变更服务方案、实施计划和恢复方案，提出服务内容相匹配的服务内容说明及服务级别承诺，并提出明确的时间计划，与金融机构协商、审核确认，变更实施要避开金融机构业务运行敏感时间窗口。

2.服务退出

对于服务退出，需满足以下要求。

（1）在服务协议或合同到期前，金融机构以书面方式明确退出服务协议或合同，云服务商应及时响应，并协助金融机构细化服务退出方案，包括但不限于退出实施计划和资源处置方案。

（2）云服务商应协助金融机构在服务退出过程中，保证业务系统的有效运行和数据完整。

六、实践案例

（一）商业银行私有云上云实践

中国工商银行(以下简称工行)是一家国有股份制商业银行，为了提高竞争优势以及快速响应互联网环境下的业务变化，工行在云计算领域持续探索，建成同业领先的云平台，全面支撑包括

核心业务在内的各类应用系统。

为了打造安全可靠的云平台，工行基于业界领先云产品和主流开源技术，结合工行特色实现金融级自主定制和加固。依托基础设施云（IaaS）和应用平台云（PaaS）两大核心云计算技术为支撑，分别建设研发测试云、生产私有云、分行云和金融生态云（SaaS），构建了完善的金融云服务体系。目前，工商银行生产入云应用节点数已接近 10 万规模，其中业务容器近 6 万，关键应用入云比例达到 100%，日均服务调用量超过 100 亿。

基础设施云统筹管理计算、存储、网络资源，实现不同应用间资源共享，提高云上资源利用率。工行通过引入成熟产品并结合生产运营运维需求进行客户化定制，对接各类信息服务管理系统，实现云主机供应、操作系统内配置等全流程自动化，满足大规模私有云场景资源集中供应的需求。工行利用云计算、分布式等新技术，基于开放平台集群系统与大型主机有机结合的基础架构，构建面向未来业务发展的一站式私有云，并通过 API 实现金融生态云对行业开放。同时依托“两地三中心”的资源池布局，设计实现多层次的高可用机制，保障业务连续性。

在应用平台云方面，工行基于业界主流开源技术自主研发，实现容器调度及多集群机制，支持超万级容器集群规模调度运行，并在定时弹性伸缩及手工伸缩的基础上，针对典型应用实现业务监控的自动化弹性伸缩支持，实现秒级弹性伸缩，有效应对业务突发高峰场景。同时，工行在云原生监控、DevOps 等方面持续探

索，构建自动化、可视化、智能化的云运维体系，实现跨平台、跨应用的调用链路分析和应用画像视图，提供云上应用秒级故障预警及实时诊断等能力。

工行金融云作为同业入云规模最大的私有云，曾荣获人民银行科技发展奖一等奖。得益于金融云的建设推广，工商银行的基础设施资源利用效率提升了 2-3 倍，资源供应时间由 2-3 周缩短至分钟级甚至秒级，管理流程基本实现自动化，稳定支撑开放平台核心银行系统建设。通过将微服务与容器技术结合，工行建设了完备的分布式技术体系，构建面向未来业务发展的下一代开放平台全新技术体系框架，实现核心银行业务系统的云化部署，更好地服务工行经营转型和业务发展，并与合作伙伴共同构建开放金融生态。

（二）保险机构金融团体云上云实践

传统的保险业务在系统应变能力上比较弱，比如无法灵活快速的应对大规模疫情这样的突发情况。同时，保险业作为金融服务行业，以“0 风险”为基本准则，对数据库的稳定性和全链路安全有着极高的要求，而传统信息系统无法满足数字化的安全性、稳定性，多数的保险公司都希望借助新技术改变这一现状，而友邦保险正是其中之一。

为加快数字化转型步伐，2015 年年底，友邦保险基于阿里云金融团体云构建了高效、敏捷、弹性、成本优化的数字金融技术平台，并逐步推动业务系统从传统数据中心迁移上云。友邦保险

业务上云后，主要体现以下 3 个特点。

1.**敏捷创新，云技术推动业务发展。**友邦保险在 2019 年底接入云内“智能双录质检”解决方案，在此基础上，仅用 15-20 天时间完成了“空中签单”小程序的开发并投入使用，实现了无需面对面的在线签单，并在极短的时间内全面实现了云培训、云招募、云管理，保障了内部运营以及外部服务的连续性。

2.**极致弹性，支撑行业大促活动。**友邦在 2019 年将核心系统迁移到阿里金融团体云上后，充分利用云计算的弹性伸缩能力，为“开门红”等促销活动提供了便利和保障。云计算的高度弹性能力使得业务能够按需使用计算资源，对资源集群灵活快速调用，少至几台、多至几百台，开机和释放都严谨有序。同时，存算分离的 PolarDB 数据库具有 1 写 15 读甚至更多读的优异读写功能，系统每秒处理上千单，轻松解决系统拥堵问题，订单实时生效。

3.**全面构建云上安全生产体系。**在对客户 APP 以真实数据量级进行全链路压测时，过去通常使用 mock 数据在非生产环境下进行虚拟测试，友邦保险在将业务迁入团体云后，通过使用团体云提供的 PolarDB 数据库在云上设置和生产 1:1 的测试环境，并使用云内应用高可用服务，提升应用面对流量洪峰、服务不稳定时的可用性。

参考文献

[1] 中国人民银行.JR/T 0166—2020 云计算技术金融应用规范 技术架构.国家标准.

[2] 中国人民银行.JR/T 0167—2020 云计算技术金融应用规范 安全技术要求.国家标准.

[3] 中国人民银行.JR/T 0168—2020 云计算技术金融应用规范 容灾.国家标准.

[4] 中华人民共和国工业和信息化部.推动企业上云实施指南（2018—2020）.工业和信息化部印发.http://www.gov.cn/xinwen/2018-08/12/content_5313305.htm.

[5] 中国人民银行. 金融科技（FinTech）发展规划（2019—2021 年）.中国人民银行印发.

[6] 中国信息通信研究院. 中小银行上云白皮书（2018）. http://www.caict.ac.cn/kxyj/qwfb/ztbg/201804/t20180426_158541.htm.

[7] 云原生产业联盟.2020 年云原生发展白皮书.IBM 发布.

[8] 中国人民银行.中国人民银行关于发布金融行业标准强化金融云规范管理的通知.中国人民银行印发.

[9] 国际数据公司(IDC).中国金融云市场（2021 上半年）跟踪.

[10] 中国工商银行.银行信息系统技术体系发展历程及未来趋势展望.中国工商银行发布。

[11] 网商银行技术编委会. 金融级 IT 架构数字银行的云原生架构解密.电子工业出版社.

[12] IBM.银行关键应用云现代化 IBM 观点和建议.IBM 发布.