业 务 系 统 云 化 迁 移 实 施 指 南

（征求意见稿）

常州市工业和信息化局

2022 年 6 月

前　言

本指南依据常州市《市政府办公室关于印发常州市制造业智能化改造和数字化转型行动计划的通知》（常政办发〔2022〕9号）相关要求起草。

本指南起草单位：常州市工业和信息化局、华为云计算技术有限公司、常州市智改数转联盟。

本指南主要起草人：沈新峰、于波、杨书玉、黄启铭、刘立、蒋烨佳、孙永中、单晓明、高雪松、晋红亮、李安详等。

目录

1 概述

1.1.背景

数字化浪潮席卷全球，正在剧烈改变企业产品和服务交付价值的方式与速度，企业正在不断使用软件和技术构建产品，或者受到软件和技术的深度影响。对于数字经济来说，云计算不仅仅是实现 IT 资源池化、提升性能、降低成本和简化管理的工具，更重要的是为产业数字化转型提供丰富的服务。企业将因数字化、智能化而变得灵活、高效、生机勃勃。开放、灵活、易用、安全的数字平台，将成为实现数字化社会的基石和土壤，激发行业创新、推动产业升级，成为企业应对不断提升的客户期望、快速变化的竞争格局以及市场不确定性的关键业务引擎。面对越来越激烈的市场竞争，企业应尽快启动全面云化转型以支撑数字化转型。

为深入贯彻落实《江苏省制造业智能化改造和数字化转型三年行动计划（2022-2024 年）》和《关于大力推进“532”发展战略的实施意见》要求，加快推进常州制造业企业智能化改造和数字化转型（以下简称“智改数转”），助力国际化智造名城建设，打造长三角产业中轴，我们制定了相关行动计划，加快推进企业上云上标识行动，联合运营商、龙头云服务商等组建工作组，编制工业设备上云实施指南、业务系统云化迁移实施指南，分行业制定服务中小型制造企业云化产品目录。编制和推广数据采集经典案例，引导企业对未联网设备进行改造，将研发设计、生产制造、运营管理等核心业务向云平台迁移。推动企业参与江苏省星级上云评定，推进产业链协同、运营分析预测、质量工艺优化等模式创新。支持标识解析节点运营商开发场景应用，鼓励产业链企业参与标识解析推广。

企业全业务上云不仅是一个技术问题，同时也是一场系统性变革，涉及到企业整体治理体系的变化、企业组织架构的适配、企业云化文化和思维的塑造、项目实施管理、持续的运营运维优化等。本迁移实施指南是在企业业务系统云化的背景下，由华为云服务商公有云解决方案团队在帮助大量企业实现全业务上云实践中总结提炼而成，包含了方法论、技术体系、实施步骤等内容，用于指导企业

全业务上云工作的开展，确保上云之路更加顺畅。

1.2.适用范围

本指南主要适用于：

（1）云服务商，参考上云所需各类云资源服务，以及上云建议。

（2）系统集成商，参考上云服务标准流程化建议。

（3）企业信息化部门技术人员，参考上云标准化流程配合内容及验收标准。

（4）企业 CIO，参考业务系统上云整体方案。

1.3.术语定义

云平台 cloud platform

云服务商提供的云基础设施及其上的服务软件的集合。

源云平台 present cloud platform

迁移之前承载业务应用和数据的云平台。

目标云平台 target cloud platform

迁移之后承载业务应用和数据的云平台。

迁移发起方 migration proposer

向目标云平台进行应用和数据迁移的用户方。

迁移实施方 migration implementer

在源云平台和目标云平台间提供应用和数据迁移的服务方。

1.4.缩略语

OA 办公自动化软件（Office Automation）

ERP 企业资源计划管理系统（Enterprise Resource Planning）

MES 制造执行系统（Manufacturing Execution System Association）

IAAS 基础设施即服务。指把 IT 基础设施作为一种服务通过网络对外提供，并根据用户对资源的实际使用量或占用量进行计费的一种服务模式（Infrastructure as a Service）

PAAS 平台即服务。 把服务器平台作为一种服务提供的商业模式（Platform as a Service）

SAAS 为企业搭建信息化所需要的所有网络基础设施及软件、硬件运作平台，并负责所有前期的实施、后期的维护等一系列服务（Software as a Service）

CAAS 通信即服务（Communications as a Service）

GPU 计算机指图形处理器（graphics processing unit）

CPU 计算机中央处理器（central processing unit）

X86 是微处理器执行的计算机语言指令集（The X86 architecture）

I/O 输入/输出（Input/Output）

ACL 是一种基于包过滤的访问控制技术，它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃（Access Control List）

VPN 属于远程访问技术，一般指虚拟专用网络（Virtual Private Network）

AI 人工智能（Artificial Intelligence）

UPS 不间断电源（Uninterruptible Power Supply）

HSM 硬件安全模块（hardware security module）

KMS 主要管理系统（Key Management System）

VPC 专有网络（Virtual Private Cloud）

IPSec 一种协议包（Internet Protocol Security）

2 云化企业价值

2.1.宏观层面

近年来，常州加快智能化改造和数字化转型步伐，成效显著，但部分企业面临智能制造水平薄弱、缺少“智改数转”方案等问题，迫切需要贴近实际的实施指

南。

通过深入企业现场进行实地调查研究，运用先进的智能制造理念和技术评估手段，结合行业特点和工业企业车间现状，围绕生产车间存在问题和建设需求，为企业提供诊断服务，提供切实可行的实施路径，帮助企业建设智能车间，提升自动化、数字化、网络化、智能化水平，实现降本、提质、增效。

具体实施“上云”的核心工作包括：引导企业对未联网设备改造，将研发设计、生产制造、运营管理等核心业务向云平台迁移。推动企业参与省星级上云评定，推动产业链协同、运营分析预测、质量工艺优化等模式创新。

2.2.战略层面

企业业务系统上云可以帮助企业管理数据资产、处理遗留应用、专注核心业务以及创新商业模式。

2.2.1.管理数字资产

上云可以帮助企业更高效的管理数据资产。云化能够方便企业采集数据、存储数据、迁移数据、汇聚数据、分析数据，提高数据处理效率，降低数据存储成本，让企业能够专心聚焦自身的核心业务的发展。

企业通过 OA、ERP、MES 等业务系统上云，可以实现云端数据汇聚。视频、音频、图片等业务附件上云，也可以通过云上提供的技术，实现非结构化数据存储，并能有效的和业务系统相结合。

云上业务系统数据，能够轻松打破各业务部门之间的信息数据孤岛，建立企业级统一数据管理。随着数据不断的积累，数据的价值将会越来越大，数据“集中式”管理的优势会越来越明显。

在当下企业数字化转型的大背景下，数据的有效使用是企业发展的核心要素之一。企业将围绕数据，优化企业流程、变革组织架构、拓展商业模式。

2.2.2.处理遗留应用

企业在经营发展过程中，除了日常使用的业务系统以外，同时也遗留了少量

被遗忘的，使用频率较低的，并且有用的业务系统。这些系统，往往运维人员已经离职或调岗，并且没有软件厂商维保，没有相关文档说明。这类系统，对于企业来说是一个巨大的风险隐患。

通过业务系统上云，引入云服务商先进的分析工具，对系统进行分析；通过云服务商先进的迁移工具，对系统迁移上云。这样既能降低遗留软件系统迁移带来的风险，又能在云服务环境下更好的管理。

2.2.3. 专注核心业务

企业每年在信息化系统建设、机房维护、服务器运维、软件运维方面花费了大量的时间和精力，影响核心优势业务的发展创新，严重情况下导致经营发展陷入停滞。

通过业务系统上云，企业可以将非核心业务的管理运营与基础设施的运维交托于公有云服务商，企业只需专注核心优势业务，提高创新效率的同时，降低经营管理成本，同时不断追求新的业务机会。

2.2.4. 创新商业模式

云服务能够帮助企业实现生产关系与商业模式的创新。通过业务系统上云，传统企业可以不用局限在自身的产品上，而是依托云服务，向“产品+服务”的新业务模式转型。从原来提供单一的产品，转变为通过产品，实现为某个行业提供整套行业解决方案的服务商。

2.3. 应用层面

企业业务系统上云可以推动企业在研发、生产、销售、客服等环节更好地落地数字化实践。

2.3.1. 企业研发

传统的生产制造企业，研发周期长、创新成本高，关键技术或配件等受限，

无法满足日益增长和变化的市场需求。

通过业务系统上云，可以整合云上的资源和技术，弥补企业研发环节的薄弱点，助力企业研发，助力企业转型。

2.3.2. 企业生产

实体经济企业经过多年的流程优化，在生产制造、产品质量控制等方面都处于较高水平，但同时，创新成效边际效用递减，如何优化生产模式成为瓶颈。

通过业务系统上云，企业生产数据可以长期保存在云端，通过这些数据，结合云上云计算、大数据能力和企业的生产经验、知识，可以构造预测模型、监控模型、质量模型等，提升企业生产环节效率。

2.3.3. 企业销售

企业传统的线下销售模式，已经无法满足互联网时代的需求。销售模式的单一、销售渠道的单一，严重制约了企业的发展。

通过业务系统上云，通过云服务商为企业、产品、生态伙伴搭建的云平台，优化企业销售模式，实现由传统销售模式向数字化销售转型升级。

2.3.4. 企业客服

企业的客户信息管理成熟度受多种因素影响，特别是客户群体庞大的企业，对客户相关的数据进行有效整合和精准分析一直是重中之重，客服质量对企业发展有着显著影响。

通过业务系统上云，云上产品和服务能够帮助企业整合客户数据并进行大数据分析，形成清晰精准的客户画像，帮助企业管理客户信息，提升客服质量。

3 上云分析

3.1.难点分析

企业的 IT 基础设施，一般由于历史原因，通常是以部门为单位，系统归属各个部门，呈现烟囱式架构特点，存在技术不统一、资源不统一、数据不统一、无法扩展等问题。业务系统上云，需要从组织架构、部署架构、系统架构三方面分析可行性。

3.1.1.组织架构

企业管理者，首先要从管理思维上接受云，理解云的架构、云的特点、云的能力。根据业务系统云化需要，建立起适合云化发展的组织架构，有计划地配置管理人员和技术人员，为云化转型做好充分的准备。

3.1.2.部署架构

企业原有的 IT 计算、存储、网络环境，通常以自建机房或托管机房为主。软件系统大多委托定制开发或采购软件产品。部署方式通常在物理服务器上或 VMware 虚拟机上。

云架构，大多以虚拟化、开源技术、分布式技术为主。因此将现有业务系统搬上云，必须做好详细的调研工作，了解线下部署方式、网络环境等，参考并设计云上环境。

3.1.3.系统架构

由于历史原因，部分企业的业务系统，系统架构已经落后，无法适配最新的云上环境。这类业务系统则可以考虑重构或升级。重构或升级时，可以采用云化架构，使用适合云部署的技术，如虚拟化、容器化、微服务化，同时可以结合云上的 IAAS、PAAS、SAAS、CAAS 等云服务能力，优化及提升业务系统。

3.2.能力分析

企业业务系统云化，需要结合自身的特点，既要满足政府相关部门监管的要求和企业自身的业务需求，也要考虑自身能力，切不可盲目跟风，超出能力范围。

3.2.1.微型企业

微型企业，对信息系统的投入相对较小，比较适合将业务系统部署在云上，甚至完全托管，将企业的主要精力聚焦在业务发展上，用最小的成本承载最大的业务。

3.2.2.小型企业

小型企业，信息系统有一定投入，对业务系统的稳定性、数据的保密性有一定的要求，建议将业务系统部署在云上，并通过云上的安全产品，实现对系统和数据的保护，降低企业对信息系统运维的投入，节约 IT 投入成本，大力发展企业自身业务。

3.2.3.中大型企业

中大型企业 IT 基础设施投入较大，一般会选择自建机房或托管机房，每年投入大量的人力、物力，进行业务系统维护、机房维护、网络维护等。成本投入方面，每年机房里服务器都存在折旧、损坏、扩容等各类问题。人员储备方面，对企业技术部门人员能力要求较高，要求懂网络、懂计算、懂存储、懂业务。业务系统主要包括核心业务系统、边缘系统等，有大量的文件数据，敏感涉密数据，同时数据根据业务需要存储几年以上。这类企业建议选择部分业务系统上云，充分利用云上资源弹性扩容特性，以及简单便捷的配置方式，降低投入成本、减轻技术人员压力。同时结合业务系统的重要性，建议同步考虑云上容灾。

3.2.4. 强监管企业

强监管企业，主要是受政府职能部门强监管的企业。例如化工企业，环境监测系统数据，需要实时上报政府环保部门；交通运输企业，车辆位置数据，需要实时上报省运管部门；建筑企业，工地视频数据，需要实时上报城管部门等。这类企业的业务系统的公网 IP，一般会提前在政府部门报备，并且对于系统的高可用级别、灾备能力、数据安全等有比较高的要求，同时按照监管机构的要求，业务系统环境需要满足安全等保三级及以上。这些业务系统上云，需要谨慎考虑。上云前期，需要详细的需求调研，完整的方案设计，详尽的上线计划，周密的回退方案。上云期间，需要重点保障。上云结束，需要重点监控，确保系统稳定运行。

3.3 数字化诊断

3.3.1 数字化诊断服务

为推进产业数字化转型输出发展策略和优化建议。基于数字化转型诊断模型，面向企业提供数字化诊断治理解决方案，可以有效解决各方在数字化转型过程中面临的制约因素。面向企业主要提供数字化诊断和数字化治理能力提升。数字化诊断能力是通过有针对性的现状调研和评估工具对企业数字化成熟度进行深度诊断，从组织、管理、核心业务链、资源、数字化基础和应用等维度开展诊断及提出优化策略。数字化治理是基于企业数字化诊断结果，帮助企业策划发展战略、制定顶层设计，涉及商业运行模式、产品研发方式、数字化应用方向、运行管理方法等方面，绘制数字化转型的发展蓝图，并明确具体的建设路径、设计具体的数字化项目。

3.3.2 诊断服务价值体现

通过数字化诊断服务，对企业经营的组织战略、设备自动化、研产供销服等全价值链进行全面梳理，深入探究企业在转型升级中存在的问题与不足，精准评

估、找准差距、研究对策，帮助企业掌握面向高质量发展的不足和系统缺陷，明确数字化转型发展的方向思路；通过量化数据，清晰企业各项发展的可视性、可评测性；深入评估企业全领域发展成熟度水平。引导企业加强云计算、物联网、大数据等新一代信息技术在研发设计、生产制造、运营管理、物流仓储等环节的应用，高起点、高标准、高要求推动企业工业互联网发展，构建企业发展新格局，打造面向数字化时代竞争新优势，帮助企业实现跨越式发展。

4 上云规划策略

企业业务系统上云前，需要了解企业业务系统现状，包括：基础资源、业务系统、业务数据等。

4.1.基础资源上云

4.1.1.计算资源

云计算是最基础的资源池，包括计算资源池、存储资源池、网络资源池等。计算资源池包括 X86 虚拟化资源池、鲲鹏虚拟化资源池、数据库资源池、大数据资源池、GPU 资源池等。

企业业务系统上云前，需要了解业务系统使用的服务器计算资源等情况，梳理云下资源清单，包括 CPU、内存等。结合云上资源，规划设计最优方案。

4.1.2.存储资源

云存储实际上是云计算中有关数据存储、归档、备份的一个部分，是一种创新服务。在面向用户的服务形态方面，它是一种提供按需服务的应用模式，用户可以通过网络连接云端存储资源，在云端随时随地存储数据；在云存储服务构建方面，它是通过分布式、虚拟化、智能配置等技术，实现海量、可弹性扩展、低成本、低能耗的共享存储资源。

企业业务系统上云前，需要了解业务系统使用的存储资源情况等，梳理存储

使用清单，包括大小、读写 I/O 等。结合云上资源，规划设计最优方案。

4.1.3. 网络资源

公有云上为用户建立一块逻辑隔离的虚拟网络空间。在空间内，用户可以自由定义网段划分、IP 地址和路由策略，安全可提供网络 ACL 及安全组的访问控制。即使受到网络攻击，一般也需要经过网关或 VPN 设备，在这些集中的设备上网络流量会更加的可控。

企业业务系统上云前，需要了解业务系统网络规划，根据网络拓扑，识别网络架构。结合云上资源，规划设计最优方案。

4.1.4. 服务资源

4.1.4.1. 大数据服务

基于云服务商提供的云计算和云存储资源，结合云原生数据仓库、数据集成、数据开发、数据治理、数据分析打造一体化的新一代大数据平台，满足企业的高性能海量数据分析诉求。

4.1.4.2. 人工智能服务

基于云服务商提供的 AI 算法，实现云上人工智能服务，包括自然语言、图片、视频、音频、人脸、机器人等高阶服务。同时面向企业提供一站式 AI 平台，为机器学习与深度学习提供海量数据预处理及交互式智能标注、大规模分布式训练、自动化模型生成，及端-边-云模型按需部署能力，帮助企业快速创建和部署模型，管理全周期 AI 工作流。

4.1.4.3. 国产化服务

基于云服务商提供的全国产化服务器、国产化操作系统、国产化数据库，以及开源开放生态体系，帮助企业信息化全面实现国产化。企业需要根据现状分析

和替换需求，做好信息化软、硬件的国产化替代工作。

4.1.4.4 云原生服务

CF 的云原生定义以 Kubernetes (k8s)为主，包含了容器、服务网格、微服务、不可变基础设施和声明式 API 等代表性技术，而 Pivotal 将 DevOps、持续交付、微服务、容器定义为云原生的重点技术。

基于这种云原生定义，可以将云原生技术归为 DevOps（支持了持续交付）、微服务、容器以及云原生基础设施，对应于软件的计划、需求、设计、开发、部署以及运维运营全生命周期流程，可以更清晰的理解云原生技术。

云原生技术有利于各组织在公有云新型动态环境中，构建和运行可弹性扩展的应用，借助平台的全面自动化能力，跨多云构建微服务，持续交付部署业务生产系统。

DevOps 理念提倡开发、测试、运维之间的高度协同，从而在完成高频率部署的同时，提高了生产环境的可靠性、稳定性、弹性以及安全性。

微服务架构使复杂应用的持续交付成为可能，服务拆分是多个业务团队并行开发的基础，微服务把同一业务的人员汇聚在一起，进一步加速了开发效率。

容器技术很好的解决了应用移植过程的环境一致性问题，使微服务实现快速弹性的部署。

云原生服务是使用云原生技术构建的、运行在云上的应用，是可弹性扩展的，具备高容错性、易管理和便于观察的松耦合系统。云原生 12 因子应用（12-Factor）则是针对云原生应用开发的最佳实践原则。12-Factor 包括一份代码，多份部署、依赖、配置、后端服务、构建、发布、运行、进程、端口绑定、并发、易处理、开发与验证环境等价、日志和管理进程。它定义了一个优雅的互联网应用在设计过程中，需要遵循的一些基本原则。而采用云原生可以带来的价值则包括：更高的资源利用率，更快的发放效率，更好的应用治理。

企业业务系统上云前，需要了解业务系统使用的微服务环境，梳理出服务依赖的整体架构，如集群类型、集群规模、实例个数等，容器类型，如 docker、containerd 等，DevOps 交付流程，如 Jenkins、gitlab-ci、Budy 或者清晰的 Pipeline

工作流等，以及现资源的网络模型等。结合云上资源，规划设计最优方案。

4.2.业务系统上云

4.2.1.业务应用上云

依托云服务商公共基础计算资源，建设综合性平台系统，承载工具系统和业务组件，支撑应用软件的高效开发、快速迭代、集成应用以及大数据的挖掘分析，提升系统应用水平和能力。

企业业务系统上云前，需要和实施服务商制定详细的上云方案和计划。

4.2.2.微服务上云

企业业务系统基于微服务架构开发，上云部署运行，需要云底座支撑，包括云容器引擎、云数据库、云缓存、云对象存储、微服务治理、接口网关等多个云组件。目前云服务厂商提供了众多的商业云组件，大部分均可以基于公有云在线应用。

企业业务系统上云前，如果是微服务架构，可以选择云厂商的微服务组件产品使用或在云服务器上自建开源服务。

在微服务上云过程中，充分结合云计算的优势，建议遵守如下关键原则：

- 稳定性原则：保持系统架构相对稳定，并可根据市场发展需要，在系统架构上不断丰富相关业务应用。
- 可靠性原则：系统应支持负载均衡、双机互备等手段，确保安全可靠及7*24 小时不间断运行。
- 开放性原则：系统中的各种网络协议、硬件接口和数据接口等应符合业界开放式标准。应逐步通过服务总线开放系统数据内容和应用功能，全面支持内部运营效率提升，提升平台应用的广度和深度。
- 易用性原则：系统应具备用户可接受的查询效率与响应时间，有良好的客户操作界面，详细的帮助信息，统一维护的错误信息，系统参数维护与管理的可视化，有良好易用的人机接口界面与灵活多样的展现方式。

- 可扩展原则：在保持系统总体架构稳定的基础上，可根据系统规模动态的进行系统资源扩展，以满足不同时期的系统使用要求。应用软件完全支持云化分布式架构部署，系统具备可扩展性，支持数据库混搭部署，便于后续向企业 IT 中台化演进。
- 安全性原则：系统应提供对网络、数据、应用和用户访问的权限控制和轨迹跟踪等安全措施，做到事前可防、事中可控、事后可查，确保系统数据安全。
- 实用性原则：系统应用建设应满足使用人员业务需求，能够解决不同层次使用人员的实际问题。应用开发设计符合使用人员的工作场景，能够对其实际工作进行指导，提高其工作效率。
- 可维护性原则：系统应提供丰富的系统运营管理界面，方便系统日常维护。当系统出现故障时，应能在 15 分钟内进行恢复，并快速定位引起故障的问题和原因。
- 容灾原则：采用标准化、通用性的服务器及网络设备，实现微服务框架和技术组件的异地多活体系架构。

4.2.3. 监管服务上云

企业监管服务系统，公网 IP 等，通常在国家、省、市、区县等政府部门备案。并且由于业务的特殊性，对迁移过程中的停服时间有较高的要求。

企业业务系统上云前，需要提前做备案变更，针对停服时间，在迁移实施前需要做详细的迁移方案和计划，确保业务平稳过渡。

4.2.4. 其它服务上云

对于长于无人运维，且无人了解的业务系统，考虑业务的稳定性，不建议迁移上云。

对于公网 IP 备案无法变更的业务系统，建议考虑转发模式，迁移上云。

对于物理硬件绑定注册信息的软件系统，建议先于厂商沟通，是否能够能上云重新注册。

4.3. 系统数据上云

4.3.1.关系型数据上云

云关系型数据库是一种基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线关系型数据库服务。关系型数据库一般支持以下引擎：MySQL、PostgreSQL、SQL Server。

企业业务系统上云前，需要根据自身关系型数据库的使用情况，考虑使用云上关系型数据库或选择云上服务器自建关系型数据库。

业务数据迁移，一般采用云厂商提供的迁移工具或开源迁移工具，实现数据迁移。

4.3.2.非关系型数据上云

云非关系数据库也常常被成为 NOSQL 数据库，一般都是 Key-Value 形式的，它的查询不需要 SQL 语句支持。常见的非关系型数据库包括：HBase，MongoDb，Neo4J，redis，influx，canssadra 等。

企业业务系统上云前，需要根据自身非关系型数据库的使用情况，考虑使用云上非关系型数据库或选择云上服务器自建非关系型数据库。

业务数据迁移，一般采用云厂商提供的迁移工具或开源迁移工具，实现数据迁移。

4.3.3.文件数据上云

云文件存储是一种在云中存储数据的方法，允许服务器和应用程序通过共享文件系统访问数据。云中的文件系统是一种分层存储系统，允许以共享方式访问文件数据。用户可以创建、删除、修改、读取和写入文件，并在目录树中按逻辑进行整理，以便进行直观访问。

企业业务系统上云前，需要根据自身的业务情况，选择使用云文件存储和云文件系统。

业务文件数据迁移，一般采用云厂商提供的迁移工具或开源迁移工具，实现文件数据迁移。

4.4.云资源费用评估

4.4.1.预付费

云厂商提供的一种包年包月的购买方式，企业可以根据自身对资源的使用需求选择资源包，下单完成后会生成账单。需要注意资源到期的提醒和欠费预警。例如云服务器资源，按包一年的方式购买，一年内使用过程中，无额外费用。

4.4.2.后付费

云厂商提供的一种先使用后付费的购买方式，在到达结算周期时，生成账单的计费模式。客户需要在约定时间内完成缴费，也同样涉及欠费预警。这种对企业来说，用多少付多少，没有资源浪费，更灵活。例如云公网带宽，按需购买，使用多少，付费多少。

4.4.3.资源套餐包

云厂商提供的一种在有效期起止时间，计量项，总量，以及分配规则和结转规则。例如云对象存储包，购买存储套餐包，在套餐包的范围内使用，超出部分，则会按后付费方式计费。

4.4.4.优惠券

云厂商提供各类优惠券、抵用券、现金券等，可以作为购买云资源时使用。具体使用限制，以各个云厂商优惠券说明为准。

4.5.上云工具评估

4.5.1.服务器迁移

云厂商提供各类主机迁移工具，包括镜像、备份等方式。具体采用哪种方式，哪种工具，需要根据企业的信息化水平以及业务系统软件特性决定。

4.5.2.数据库迁移

云厂商提供各类数据库迁移工具，包括结构化数据库、非结构化数据库的迁移。迁移方式包括全量迁移、增量迁移、备份迁移等方式。具体采用哪种方式，需要根据数据量的大小、数据的更新频率等因素来考虑。

4.5.3.对象存储迁移

云厂商提供了各类对象文件存储迁移工具，包括现在迁移、数据快递等方式。具体采用哪种方式，并且成本最低，效率最高，需要根据对象文件的大小、数量综合评估。

5 系统云安全

企业业务系统上云后，系统的安全性会集中暴露出来，不管是云厂商的机房安全、还是云上资源的安全，还是系统安全和数据安全，都需要考虑，同时这也是云的技术特点，决定了云上的安全与传统安全的区别。

5.1.基础设施安全

5.1.1.物理安全

5.1.1.1.机房选址

云服务商数据中心机房选址一律避开自然灾害不利或危险的地区，减少周边环境对数据中心产生的干扰，如 400 米内无实验室、化工厂等危险区域。同时，也要保证数据中心正常运营需要的配套资源，如市电、水、通信线路等。

5.1.1.2.访问控制

在数据中心园区及建筑门口设置全天候安保人员进行登记核查，限制并监控来访人员授权活动范围。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，确保非授权人员不可访问数据中心。

5.1.1.3.安保措施

云服务商采用通用的机房安保技术监控，并消除物理隐患。对机房出入口、走廊、电梯等进行 7*24 小时摄像头监控，并与红外感应、门禁等联动。

5.1.2.环境安全

5.1.2.1.电力保障

云服务商数据中心采用多级保护方案保障业务 7*24 小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市区断电时可启用柴油机供电，以备不时之需。配备了不间断电源（UPS），提供短期备用电力供应。在机房供电线路上配置了稳压器和过压保护设备，在供电设备及线路上设置冗余或并行的电力电缆线路为计算机系统供电。

5.1.2.2.温湿度控制

云服务商数据中心通过精密空调、集中加湿器自动调节，云数据中心机房温湿度保持在设备运行所允许的范围内，使设备元器件处于良好运行状态。机柜冷热通道有合理的布置，利用架空地板下空间作为静压箱来给机柜送风，并设置了冷通道密闭，以防止局部热点。

5.1.2.3.消防能力

云服务商数据中心建筑防火等级均按一级设计施工，使用了 A 级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统，得以控制火情。

5.1.2.4.例行监控

云服务商数据中心的电力、温湿度、消防等环境运行状态通过日常巡检制度实现例行监控，安全隐患能被及时发现并修复，确保设备稳定运行。

5.1.2.5.供水排水

云服务商数据中心的供水和排水系统均有合理规划，保证了总阀门正常可用，确保关键人员知晓阀门位置，以免信息系统受到漏水事故破坏。机房建筑和楼层均有抬高场地，在外围设置了绿化地排水沟，加速排水，以降低场地积水倒灌风险。建筑满足防水一级标准，保证了雨水不能通过屋顶、墙壁向机房渗透。数据中心也配备了及时排水的设施，供水灾时使用。

5.1.2.6.防静电

云服务商数据中心机房铺设了防静电地板，导线连接地板支架与接地网，机

器接地以导走静电。在机房大楼顶部设置了避雷带，供电线路安装了多级避雷器，导走电流。

5.1.3. 网络安全

云服务商数据中心节点众多、功能区域复杂。为了简化网络安全设计，阻止网络攻击在云中的扩散，最小化攻击影响，对云网络进行安全区域、业务层面的划分和隔离。安全区域内部的节点具有相同的安全等级。从网络架构设计、设备选型配置到运行维护诸方面综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保云安全。

5.2. 资源安全

5.2.1. 计算资源安全

5.2.1.1. CPU 隔离

CPU 隔离主要是指虚拟化平台与虚拟机之间的隔离，虚拟机内部的权限分配和虚拟机与虚拟机之间的隔离。CPU 隔离是通过 Root 和 Non-Root 两种运行模式的切换、各运行模式下的运行权限分配以及以虚拟处理器的形式呈现的虚拟计算资源的分配与切换等方式来实现的。通过 CPU 隔离机制，网络欠电压保护可以控制虚拟机对物理设备以及虚拟化运行环境的访问权限，从而实现虚拟化平台与虚拟机之间以及不同虚拟机之间在信息和资源上的隔离，也就是说，一个虚拟机无法获取到其他虚拟机或虚拟化平台的信息和资源。

5.2.1.2. 内存隔离

虚拟化平台还负责为虚拟机提供内存资源，保证每个虚拟机只能访问到其自身的内存。为实现这个目标，虚拟化平台管理虚拟机内存与真实物理内存之间的映射关系。保证虚拟机内存与物理内存之间形成一一映射关系。虚拟机对内存的

访问都会经过虚拟化层的地址转换，保证每个虚拟机只能访问到分配给它的物理内存，无法访问属于其他虚拟机或虚拟化平台自身使用的内存。

5.2.1.3.I/O 隔离

虚拟化平台还给虚拟机提供了虚拟 I/O 设备，包括磁盘、网卡、鼠标、键盘等。虚拟化平台为每个虚拟机提供独立的设备，避免多个虚拟机共享设备造成的信息泄露。每个虚拟磁盘对应虚拟化平台上的一个镜像文件或逻辑卷，虚拟化平台控制只有一个虚拟机的一个虚拟磁盘设备跟一个镜像文件关联。实现了虚拟机使用的虚拟设备与虚拟化平台 I/O 管理对象之间一一对应的关系，保证虚拟机之间无法相互访问 I/O 设备，实现 I/O 路径的隔离。

5.2.2.存储资源安全

5.2.2.1.密钥保护和管理

密钥管理服务是一种安全、可靠、简单易用的密钥托管服务，帮助用户集中管理密钥，保护密钥安全。它通过使用硬件安全模块，为租户创建和管理密钥，防止密钥明文暴漏在 HSM 之外，从而防止密钥泄露。HSM 是一种安全产生、存储、管理及使用密钥并提供加密处理服务的硬件设备。为保护租户密钥安全，减少密钥外泄风险，云服务商提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云 HSM 供租户选择，满足不同租户的实际需求。目前已对接 KMS 服务的云服务包括：云硬盘、对象存储、云硬盘备份及镜像服务等。

5.2.2.2.专属加密

专属加密满足租户更高合规性要求的加密场景，采用通过国家密码局认证或硬件加密机，对租户业务进行专属加密，默认双机架构以提高可靠性。

5.2.2.3.数据删除和销毁

在用户确认删除数据后，云服务商会彻底删除用户数据，确保数据不泄露：

（1）内存删除：云服务商在云操作系统将内存重新分配给用户之前，会对分配的内存进行清零操作，即写“零”处理，防止通过物理内存恢复删除数据造成的数据泄露。

（2）加密数据防泄露：云服务商建议租户对要上云的重要数据进行加密存储，数据需要删除时，通过直接删除相关数据加密密钥，防止数据在被彻底删除前被恢复为明文后造成泄露。

（3）存储数据删除：当租户删除数据时，数据和对应的元数据在系统中一并删除，底层存储区域被回收以供系统重新覆盖写入，数据无法再被读取。但是针对客户误删除的操作场景，通过云硬盘服务的回收站功能、对象存储服务的多版本控制功能，用户可以最终决定数据的恢复或彻底删除。

（4）磁盘数据删除：云服务商对删除虚拟卷采用清零措施，确保数据不可恢复，有效防止被恶意租户使用数据恢复软件读出磁盘数据，杜绝信息泄漏风险。

（5）物理磁盘报废：当物理磁盘报废时，云服务商通过对存储介质进行消磁、折弯或破碎等方式清除数据，并对数据清除操作保存完整记录，满足行业标准，确保用户隐私和数据不受未授权访问。

5.2.3.网络资源安全

5.2.3.1.虚拟专用网络

VPN 用于在远端网络和 VPC 之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到云上，为租户提供端到端的数据传输机密性保障。通过 VPN 在传统数据中心与 VPC 之间建立通信隧道，租户可方便地使用云服务器、块存储等资源，通过将应用程序转移到云上、启动额外的 Web 服务器来增加网络的计算容量，实现了企业的混合云架构的同时，也降低了企业核心数据非法扩散的风险。目前，云厂商通常采用硬件实现的密钥交换协议和 IPSec

VPN 结合的方法对数据传输通道进行加密，确保传输安全。

5.2.3.2.证书管理

云服务商的服务提供 REST 和 Highway 方式进行数据传输：REST 网络通道是将服务以标准 RESTful 的形式向外发布，调用端直接使用 HTTP 客户端，通过标准 RESTful 形式对 API 进行调用，实现数据传输； Highway 通道是高性能私有协议通道，在有特殊性能需求场景时可选用。上述两种数据传输方式均支持使用传输层安全协议进行加密传输，同时也支持基于 X.509 证书的目标网站身份认证。云服务商为用户提供的一站式证书的全生命周期管理服务，实现目标网站的可信身份认证与安全数据传输。

5.2.3.3 云上网络安全的划分原则

基于业界最佳安全实践，使用以下的安全原则进行针对性的业务安全域划分。

- **基于对外提供逻辑架构的功能网络隔离：**按照客户的不同业务域，可以将网络分为接入域、公共服务域、安全管理域，其中接入域为了提供访问终端访问业务系统的安全保障，根据不同的网络路径可能分为互联网业务接入/出口、专线接入、运维接入等不同的接入域；安全管理域是部署统一的安全管理产品用于统一安全运维的区域，即云上的管理流量。
- **业务域基于应用系统逻辑架构的网络隔离，即根据对外提供服务的层次关系进行隔离：**业务应用一般按照逻辑架构划分，可以划分为接入层、应用层、数据层，每一层级部署若干弹性云服务器。考虑到每一层级的实际功能，同一应用相同层级内部的弹性云服务器建议二层互通。不同的业务系统部署在不同的子网，同一子网内仅部署一种应用。应用的不同层级，通过安全组进行隔离。
- **根据接入网络的不同做区域隔离：**某些应用系统部署在内部区域作为中台应用提供服务，某些应用系统对互联网开放需要调用该类型的中台应用；可以考虑多个网络区域内分别部署接对内对外的业务系统，对于业务交换通过跨网络区域进行应用互访请求，不同的网络区域做好严格的安全限制

5.3.系统和数据安全

5.3.1.应用系统安全

由于云环境的灵活性、开放性以及公众可用性等特性，云服务商充分考虑应用系统的安全风险，提供漏洞管理、防篡改、防渗透安全防护。企业在使用云服务的过程中，也要提高安全意识，采取必要措施。具体包括通讯加密，定期更新机制，及时为应用打补丁或更新版本等。

漏洞管理，云服务商构建了完善的漏洞管理体系，实现漏洞感知、漏洞处理、漏洞披露等全流程的跟踪和管理，处理好云平台各服务产品和组件的漏洞。

5.3.2.系统数据安全

在云环境下，企业业务系统数据直接在云端计算和存储，企业拥有其云上数据的所有权和控制权，同时企业需要对自身的业务数据安全负责。云服务商提供了丰富的服务，供企业自主选择，帮助企业提升安全防护水平，消减数据安全风险。

数据隔离，云服务商承载了众多企业数据，各个服务产品和组件在设计之初就规划并实现了隔离机制，避免客户间有意或无意非授权访问、篡改等行为，降低数据泄露风险。

数据加密，云服务商的多个服务采用与密钥管理服务集成设计，方便企业管理密钥，企业可以通过简单的加密设置，实现数据的存储加密。

数据冗余，云服务商数据存储采用多副本备份和纠删码设计，通过冗余和校验机制来判断数据的损坏并快速进行修复，确保即使一定数量的物理设备发生故障，也不会影响业务的运行。

隐私保护设计，云服务商产品的设计遵循《隐私保护设计规范》，建立隐私基线、维护隐私的完整性和指导隐私风险分析，制定对应措施并作为需求落入服务产品开发设计流程。

5.4.业务系统安全上云

5.4.1.基础资源安全上云

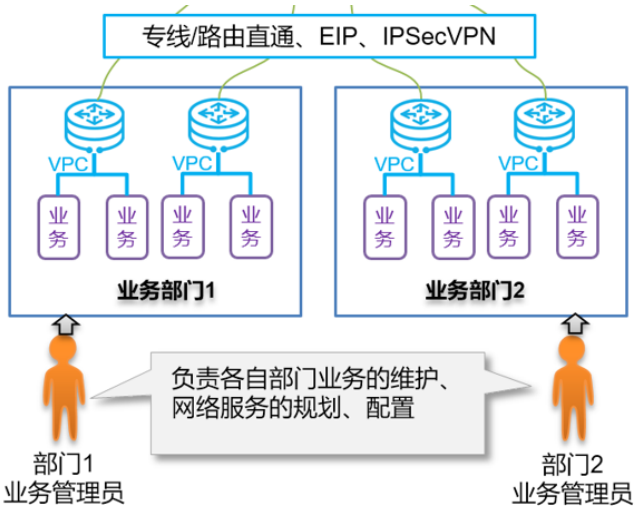
企业业务系统上云前，需要根据自身的业务情况，做好网络规划以及安全隔离、安全接入、负载保护等措施，才能保障业务系统安全稳定的运行

1）网络资源安全隔离：从历史发展的角度看，安全隔离一直是传统安全领域广泛采用的防御手段，目的为了形成对内、对外两个安全域，以便于实施统一的防护策略。

企业上云之后，传统的网络规划的维度，需要考虑虚拟私有云（VPC）的维度的网络规划。业务都部署在 VPC 内，每个 VPC 与其他 VPC、外部网络默认完全隔离。业务可以通过专线、EIP、VPN 这些方式，接入到云外的企业网络。

为了做好前期的安全隔离措施，企业上云之前需要做好至少如下的前期准备工作：

1：根据业务之间的互访关系以及业务属性，明确业务 VPC 的数量以及规划方式。



2： 配置 VPC 之间的网络互通关系以及明确对应的安全隔离措施（如基于云防火墙对进出 VPC 南北向流量进行访问控制）；对 VPC 的内部应基于接入、应用、数据库进行分层，利用安全组进行隔离。

3：对于远程管理或者业务安全访问的需求，规划安全管理 VPC 以及边界防

护 VPC 用于部署堡垒机等安全产品，并明确安全相关的 VPC 与业务 VPC 之间的互访关系，明确对应的安全隔离措施。

2）网络资源可用性保障：对于暴露在互联网的业务系统，在遭受大流量 DDoS 攻击会导致服务出现不可用的情况（带宽被恶意流量占用，导致业务系统无法被正常访问），而该类型的攻击在互联网上极为普遍。

因此对于对外提供服务的业务系统，需要配置云原生防护或者高防 IP，将攻击流量引流到 DDoS 服务清洗系统，来确保源站业务稳定可靠，能够正常对外提供服务。

3）计算负载的安全防护：对于承载业务系统的计算资源，需要考虑“勒索/挖矿病毒”等新型攻击形式的影响，该类攻击除了导致中断之外，会产生严重的业务损失(如数据丢失不可恢复)与经济损失（例如向黑客支付赎金），该类风险是企业业务系统上云前需要解决的重要问题。

业务可以通过加固和修复资产管理、基线检查、漏洞管理等功能发现与解决安全问题，能够使主机减少 90%被攻击的概率；可以通过选择使用云主机安全的产品来进行实现。

4）数据负载的安全防护：

为了保障业务数据的机密性，云上多个存储服务与密钥管理服务集成设计，方便企业管理密钥，企业可以通过简单的加密设置，实现数据的存储加密。建议企业通过密钥管理服务配置自己的专属数据加密密钥，保障自己的数据机密性，其他非企业人员无法查看自己相关的数据。

同时对于大数据类型的业务系统，由于数据的集中化以及数据共享交换的流通性，数据的可控可管是需要考虑的问题。例如数据隐私中涉及到的敏感数据在何处，数据流转过程的监管以及数据共享泄露之后的溯源的问题。在数据治理的过程中，数据的分类需要结合数据的安全分级同步进行考虑，针对不同级别的业务数据制定不同的安全防护策略。

5.4.2.业务系统安全上云

业务系统开发态安全：为保障业务系统自身的安全性，建议将安全的工作融

入到整个开发流水线，例如代码的安全开发规范、第三方开源组件管理、白盒测试、黑盒测试等等，并对代码进行安全审计，保障企业上云的业务系统自身的安全健壮性。

业务系统运行态安全：对于 web 类型的对外业务系统，需要考虑 web 应用方防火墙防止对 web 系统的 SQL 注入等安全攻击，并启用专业的网站安全证书，保障传输链路的安全性；同时建议业务上线前进行专业的渗透测试，保障无重大的安全风险问题。

5.4.3. 系统数据上云

对于数据库类型的上云，企业需要考虑对数据库层面的操作与访问行为进行监控，让数据库的访问行为变得可见、可查。有效的识别出数据库访问行为中的可疑行为并实时触发告警，避免业务数据上云之后因为恶意人员或者系统遭到攻击，导致业务数据出现泄露的事件。

6 系统云运维

传统运维与云运维都是为用户提供 IT 运维服务，云运维其实相当于传统运维借助监控、告警、日志等工具及云计算新技术，解放和提高运维的生产力。

云运维面向的是整个系统，包括数据、应用程序等等。云运维具备主动快速部署的特点，企业可以按需进行交付和扩展，底层的设备也可以由云服务商完成，集中式的处理帮助企业降低人力成本。

因此，依托云厂商提供的强大的平台作为支撑，通过自动化部署进行生命周期阶段的操作，按需配置与更新云端资源，对现有的维护模式进行延伸，解决云运维环境的困难，保障业务持续发展。

6.1. 资源告警

通过配置告警阈值的方式创建告警规则，一旦资源使用量超过告警阈值，资源告警系统将告警信息推送给用户。

6.2.风险发现

用户可以及时发现系统存在的安全风险、系统漏洞、加固系统，提高系统安全性。

6.3.云堡垒机

通过云堡垒机纳管云计算资源，依托其云原生特性，支持对主机、网络存储设备管理，同时也支持云资源操作审计等。

7 上云实践步骤

7.1.需求现状调研分析

迁移需求和现状调研分析活动中，**企业需要协助上云实施方完成：**

（1）协助完成业务迁移需求的调研；

（2）协助完成应用系统的信息收集和调研；

（3）如果业务应用系统由第三方厂商提供，企业应协调第三方厂商完成应用系统的信息收集和调研；

（4）评审并验收迁移需求和现状调研分析报告。

7.2.上云方案设计

7.2.1.业务迁移方案设计

业务迁移方案设计活动中，**上云实施方应完成：**

（1）设计制定业务迁移方案，方案内容包括但不限于迁移方式、迁移工具、迁移流程、迁移批次等；

（2）规划设计目标云平台上业务系统的技术架构和部署架构；

（3）规划设计云网络以及目标云平台上业务使用的网路能力，如专线、可用区、VPC 及子网等；

（4）规划目标云平台上业务使用的资源，如业务所需资源的能力和容量、资源利用率、业务访问流量模型、业务特殊资源需求等；

（5）规划设计业务应用在目标云平台的可靠性和连续性，如主备、双活、多可用区和异地容灾等；

（6）规划设计业务应用在目标云平台的安全防护能力，如加密、防病毒、漏洞管理等。

业务迁移方案设计活动中，**企业应协助上云实施方完成：**

（1）协助完成业务迁移方案的设计制定；

（2）评审迁移方案的合理性以及是否满足业务迁移需求。

7.2.2.业务切换演练方案设计

业务切换演练方案设计活动中，**上云实施方应完成：**

（1）提供业务切换演练的方案选型，包括但不限于演练方式、演练时长、演练流程等；

（2）提供业务切换演练的实施规划，包括相关方的配合方式、演练指导书、演练总结等；

（3）提供业务切换演练交付的验收标准；

（4）提供目标云平台上资源、服务和任务的变更操作指南，如资源、服务、任务的启动、变更等。

业务切换演练方案设计活动中，**企业应协助上云实施方完成：**

（1）协助完成业务切换演练方案的设计制定；

（2）评审迁移方案的合理性以及是否满足业务迁移需求。

7.2.3.业务切换实施方案设计

业务切换实施方案设计活动中，**上云实施方应完成：**

（1）提供业务切换策略、实施规划和交付验收标准，包括但不限于业务切换方

式、切换时长、压力测试、数据迁移方式、数据一致性等；

（2）根据业务影响因素，选择业务应用停止服务或不停止服务方式进行迁移，如业务复杂度和规模、业务重要性和敏感性、业务系统耦合度等；

（3）提供目标云平台资源、服务和任务的配置规划，包括但不限于资源、服务清单和配置等；

（4）提供目标云平台业务系统的切换评估标准和规则。

业务切换实施方案设计活动中，**企业应协助上云实施方完成：**

（1）协助完成业务切换实施方案的设计制定；

（2）评审迁移方案的合理性以及是否满足业务迁移需求。

7.2.4.迁移风险应对方案设计

迁移风险应对方案设计活动中，**上云实施方应完成：**

（1）识别迁移流程、工具中的风险关键点并划分不同的风险等级；

（2）针对不同类型的风险提供相应的措施；

（3）对于方案或流程缺失所导致的风险类别，方案设计采用标准化的作业和方案设计流程；

（4）对于无法完善的风险类别，制定尽可能减少风险的规避方案；

（5）对于一定条件下触发的风险类别，制定相应的回退计划，如配置一致性风险；

（6）对于迁移过程中无法预知的风险，制定应急方案包括人、流程、事件通报机制等。

迁移风险应对方案设计活动中，**企业应协助上云实施方完成：**

（1）协助完成迁移风险应对方案的设计制定；

（2）评审迁移方案的合理性以及是否满足业务迁移需求。

7.3.可行性和风险评估

迁移可行性和风险评估活动中，**企业应协助上云实施方完成：**

（1）协助完成各系统/应用之间依赖性的评估；

（2）协助完成目标云平台的资源及服务的满足度和兼容性评估；

（3）协助完成对上云迁移网络的互通性评估；

（4）协助完成对迁移过程涉及的人力、资源、服务等费用的评估；

（5）协助完成对上云迁移周期和切换中断时长等时间的评估；

（6）协助完成对迁移带来的业务改造、业务可用性/可靠性、组织变革等方面风险的评估；

（7）协助完成对迁移过程的信息安全评估，如网络通道安全、敏感业务系统登录安全等；

（8）评审并验收上云迁移可行性和风险评估报告。

7.4.迁移实施准备

7.4.1.云网络连接准备

跨云网络连接准备活动中，**上云实施方应完成：**

（1）专线资源准备；

（2）其它网络连接准备。

跨云网络连接准备活动中，**企业应协助上云实施方完成：**

（1）提供源环境的登录信息和环境信息。

7.4.2.目标云平台服务准备

目标云平台服务准备活动中，**上云实施方应完成：**

（1）迁移演练之前完成目标云平台资源的报备和预留，避免出现资源不足；

（2）按照业务迁移方案批量发放业务需要的资源和服务；

（3）按照业务切换演练方案、业务切换实施方案划分和配置生产环境及演练环境；

（4）提供和安装业务应用迁移需要的迁移工具和管理工具；

7.4.3.源环境服务准备

源云平台服务准备活动中，**上云实施方应完成：**

（1）协助企业对源云平台的业务应用信息进行备份，如数据、服务列表、账号等；

（2）协助企业对业务全部数据或关键数据进行备份。

源云平台服务准备活动中，**企业应协助上云实施方完成：**

（1）对在源环境的操作进行监督管控；

（2）对源环境的业务应用信息进行备份，如数据、服务列表、账号等；

（3）对业务全部数据或关键数据进行备份。

7.5.业务切换演练

业务切换演练活动中，**上云实施方应完成：**

（1）查验目标云平台上演练环境的准备情况，包括但不限于资源清单、网络配置等；

（2）启用目标云平台上演练环境的应用和资源配置，根据演练策略将业务访问导向目标云平台的演练环境；

（3）查验目标云平台上演练环境的应用运行和数据一致性情况；

（4）评估业务切换演练效果，并进行切换演练总结。

业务切换演练活动中，**企业应协助上云实施方完成：**

（1）协助解决业务切换演练过程中的问题和故障；

（2）制定并完成目标云平台上的业务能力验证，包括功能、性能、安全等；

（3）对迁移的结果及效果进行验收确认，提出演练方案优化要求。

7.6.业务切换实施

业务切换实施活动中，**上云实施方应完成：**

（1）查验目标云平台的资源、网络准备情况，包括但不限于软硬件资源规格、资源配置、网络资源分配和连接等；

（2）根据业务流量模型、负载情况等因素选择合适的时间窗口进行业务切换，如流量波谷期、业务空闲期等；

（3）按照业务切换方案和流程进行业务切换，使得业务访问导向目标云平台的业务系统；

（4）业务切换后，查验目标云平台上应用是否正常运行和数据一致性。

业务切换实施活动中，**企业应协助上云实施方完成：**

（1）协助解决业务切换实施过程中的问题和故障；

（2）对迁移的结果及效果进行验收确认。

7.7.业务试运行

业务试运行活动中，**上云实施方应完成：**

（1）协助企业制定业务试运行测试计划；

（2）协助企业制定业务试运行测试方案，如功能、性能、可靠性、安全等；

（3）协助提供目标云平台产品和服务相关的测试工具和数据；

（4）协助企业分析和解决测试过程中发现的问题；

（5）协助提供业务试运行报告并完善测试方案。

业务试运行活动中，**企业应协助上云实施方完成：**

（1）制定业务切换后目标云平台上的业务试运行计划及业务故障分级；

（2）制定业务试运行方案，包括业务功能、性能、安全、运维等；

（3）根据业务试运行结果，对试运行方案进行优化和完善；

（4）由目标云平台原因导致的故障，协助解决相应问题。

7.8.业务运行保障

业务运行保障活动中，**上云实施方应完成：**

（1）具备明确的运行保障流程和机制；

（2）定期对业务系统运行的软硬件环境进行巡检；

（3）7*24 小时监控系统运行状况；

（4）根据业务运行状况，协助迁移发起方对业务系统进行优化；

（5）达成业务切换方案的验收标准，输出业务运行保障报告。

7.9.迁移验收交接

迁移验收交接活动中，**上云实施方应完成：**

（1）目标云平台上的业务需正常运行一定时间后，与企业进行交接；

（2）达成业务迁移的项目验收标准；

（3）向企业交接迁移方案、交付过程中的问题及解决方案、迁移遗留问题等信息；

（4）协助企业进行人员技术培训。

迁移验收交接活动中，**企业应协助上云实施方完成：**

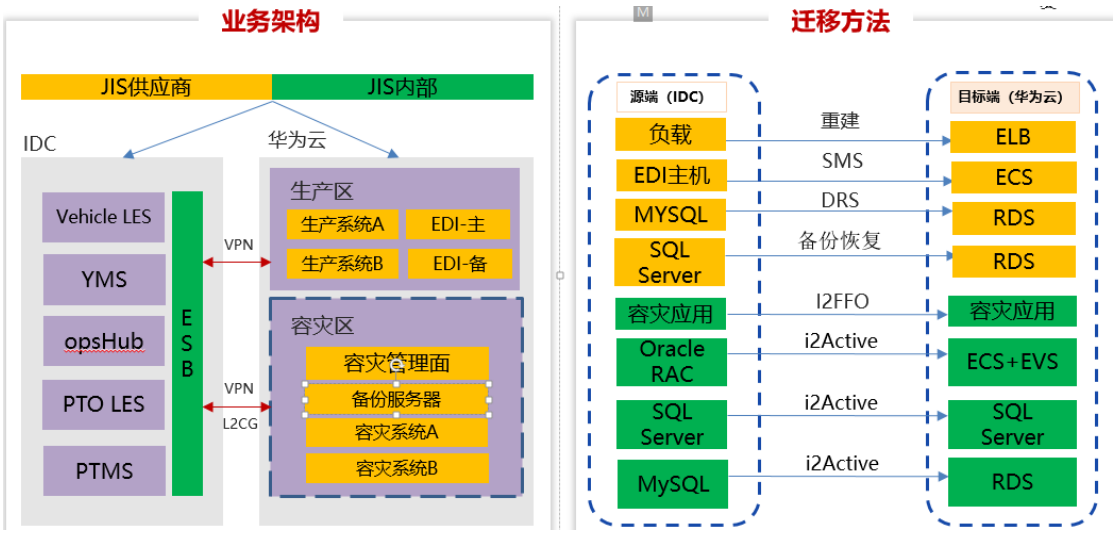
（1）目标云平台上的业务需正常运行一定时间后；

（2）与上云实施方交接迁移方案、交付过程中的问题及解决方案、迁移遗留问题等信息；

（3）参与上云实施方的迁移相关技能培训计划。

8 企业案例

8.1.某汽车生产厂商机房迁移上云



8.1.1.业务上云需求

（1）订单系统希望使用 EDI，但是供应商全接入造成 IDC 带宽吃紧，希望进行云化部署；

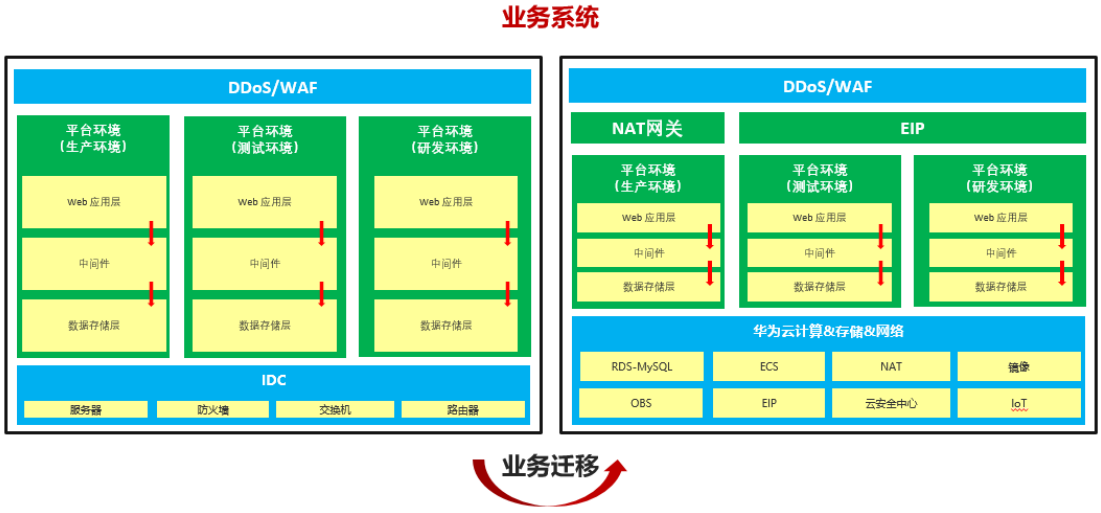
（2）本地 IDC 无容灾系统，每年因为掉电等机房问题造成的数据丢失事件经常发生，SLA 无法保证，且自建容灾机房难度高，投入大。

8.1.2.业务上云效果

（1）云上网络专线，解决了带宽吃紧问题，同时可以根据业务需要，弹性扩容带宽；

（2）容灾上云，构建两地三中心容灾环境，保障业务稳定性。

8.2.某自动化上产服务商 IDC 迁移上云



8.2.1.业务上云需求

（1）线下 IDC 机房管理运维困难，网络架构复杂；

（2）服务器安全，数据库安全性欠佳，对业务的保障支撑能力不足，引发经营风险的可能性较大；且等保等级低，机房等环境未能满足等保认证级别，不适应平台进行等保安全认证等发展需要；

（3）客户内部部门间沟通成本高，办公效率低；

（4）客户系统之间相互独立，形成数据孤岛。

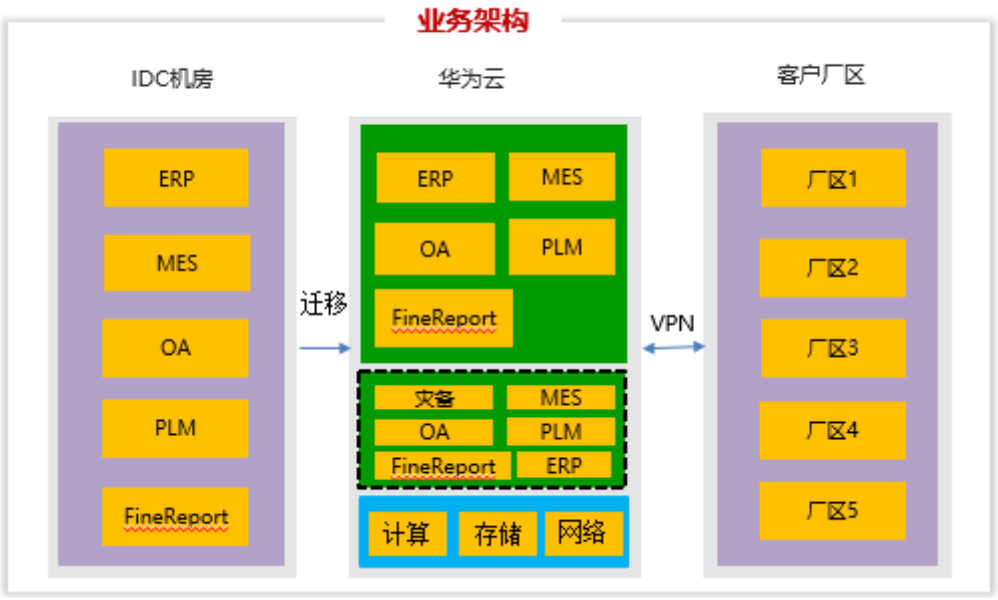
8.2.2.业务上云效果

（1）云上做了安全等保；

（2）打通各个系统业务数据，实现数据中心；

（3）降低运维人员成本，云上可视化运维+自动化运维。

8.3.某汽车零件制造商 IDC 迁移上云



8.3.1.业务上云需求

（1）客户新业务与云服务商合作，资源按需申请，降本增效；

（2）客户本地部署很难满足存储需求，不能弹性快速扩容，管理复杂；

（3）本地机房安全防护弱，云上安全防护系统强，有效保护业务稳定性。

8.3.2.业务上云效果

（1）资源按需购买，降低 IT 资源投入成本；

（2）根据业务量，弹性扩容云资源，节约存储成本；

（3）云上安全防护，包括防火墙、主机安全、防 DDOS 攻击、防恶意脚本注入等，系统运行更稳定。