
阿里云
CAICT
Deloitte.
ALL
企业
全面上云
成功路径与实践
ENTERPRISE
CLOUD
ADOPTION
IN
BEST
PRACTICE
ALL IN CLOUD
CLOUD
阿里云研究中心

写在前面...

《企业全面上云成功路径与实践》白皮书全文共7章约13万字，
力图全面覆盖企业全面上云旅程中的各个知识点和实践需求，为了方便读者阅读，我们在此统一作此说明。

首先
First of all

《企业全面上云成功路径与实践》白皮书与过去您读到的类似内容有何不同？

-全面覆盖企业上云7大关键议题，包括上云价值分析、上云障碍解决、上云决策落实、上云规划设计、上云行动事件、云上管理与治理体系以及企业构建云原生架构的方法；

-企业成功上云所需的组织内部策略，上云并非简单地IT行动，它需要在组织内部形成共识并紧密协作，为此我们特别设计了全面上云的成功框架和破除传统企业全面上云的障碍两章内容，帮助企业上云负责人完善组织内部沟通协作策略；

-根植于上云实践的具有可操作性的内容，从上云价值分析、IT上云蓝图规划，到迁移上云、云上IT治理，都来自于阿里云及合作伙伴的一线实践，白皮书不仅仅是指导性原则，丰富了大量经过实际场景和项目验证的实操内容；

-完全本地化团队中文撰写，内容契合中国企业实践，作为一家中国云计算公司，我们深知内容来自于中国云计算市场一线并完全由本土云计算专家撰写的重要性，因此，白皮书完全由本地化专业团队中文撰写，结合中国企业上云特征和需求；

其次
the second

在每一章中您会读到哪些内容？

第一章《启动全面上云策略》：本章主要阐述企业全面上云战略的定义、必要性与价值，以及如果借助全面上云确保与消费者永续连接，驱动企业IT从成本中心向服务中心转型，以及实现新“四化（云化、数据化、AIoT化和移动化）”，此外，我们将为您和您的企业明确阿里云从全面上云到数字原生操作系统的战略愿景。

第二章《上云价值分析》：从业务、治理、平台、安全、运维、IT成本等企业核心视角，帮助上云负责人明确全面上云对企业内、外部的价值，并以此清晰地向上云旅程相关方阐述其能够从上云旅程中获益以及如何获益，并在随后的工作中支持企业全面上云。

第三章《全面上云的成功框架》：这一成功框架的目标是帮助企业上云负责人通过一系列针对组织内部的策略及行动，向公司内部清晰化上云的决策依据和推进流程，形成内部各团队、部门及中高层负责人对上云旅程的准确认知，并结合上云价值分析中的获益情况，对上云负责人给予支持。

第四章《破除传统企业全面上云的障碍》：传统企业全面上云必然会面临阻碍，其中许多并非来自IT，而是来自于经济性、服务等级、技能与组织，乃至数字资产及合规性要求，这一章筛选出常见的6个问题并给出来自实践的建议。

第五章《IT上云蓝图规划》：IT上云是企业全面上云的关键和基础，它将赋予IT前所未有的参与业务的“机遇”，因此完备的目标评估、可行性分析和上云规划必不可少，这正是这一章的重点：来自于一线实践的内容，将为上云负责人提供IT上云前的完整筹备“清单”。

第六章《迁移上云与云上治理》：从IT迁移上云到云上IT治理、云上管理体系，本章在提供迁移上云的行动建议和实操指南之外，帮助上云负责人在上云后持续优化、迭代云上的IT治理与管理体系，确保云上IT仍然能够与企业治理与管理体系及其要求保持一致。

第七章《云原生》：云的时代需要新的技术架构，来帮助企业应用能够更好地利用云计算优势，让业务更敏捷、成本更低的同时又可伸缩性更灵活，这正是云原生，这一章将帮助上云负责人继续企业全面上云的旅程，拥抱云原生架构，用技术加速创新，进一步发挥企业上云的价值。

此次发布的《企业全面上云成功路径与实践》白皮书，只是万里长征的第一步，未来我们将继续修订、补充、迭代，以此为基础为中国企业全面上云提供建议、分享经验，贡献绵薄之力。

目录
CONTENT

导语

2020年 —————————————————— 是不平凡的

我们看到了众多数字化创新不断的涌现，更看到以云为代表的数字基础设施在这一过程中发挥至关重要作用，
云的支撑之下，资源有效调度、数据高速流动、应用便捷开发、系统快速上线，凸显过去10年阿里云及整个中
云计算产业建设的丰硕成果。

可以说，2020年开启了一个“万物皆可云”的新时代。云以在线公共服务的方式，提供安全、可靠的计算和
据处理能力，让计算和人工智能成为普惠科技，成为企业数字化转型的载体，乃至全社会数字化发展的基础。

但我们同样看到，在企业从信息化向云化迁移的过程中，“上云”仍非易事，在云上获得数字化、智能化的能
仍有难度，他们需要一份来自于上云最佳实践、根植于上云成功路径的全面系统且具有可操作性的指导性
册”，但在过去，企业只能参考或缺少最佳实践、或翻译晦涩难懂、或仅有精炼框架的内容。

为此，阿里云研究中心牵头完成这一份《企业全面上云成功路径与实践》白皮书，以一份包含企业上云的成功
架、实施指南和最佳实践的完整集合，帮助企业清晰上云价值、破除上云障碍、落实上云决策、设计上云规划
实施上云行动并形成云上治理体系与创新。

更重要的是，在您所看到的这份白皮书中，蕴藏着阿里云自2009年成立以来，为200多个国家和地区的企业、
发者和政府机构提供服务所积累下来的经验与实践。

在此，我们将之分享出来，希望能够帮助每一家企业加速上云，并拥有平滑、顺畅的上云旅程。

主要阐述企业启动全面上云战略的定义、必要性，以及全面上云的未来愿景。

1 企业全面上云成功路径与实践

启动全面上云战略

1 复杂经济系统驱动企业全面上云

经济系统变得越来越复杂，这种复杂来自于客户的个性化，来自于产品的复合化，来自于场景的多元化，来自于供应链的复杂性等复杂因素。面对经济系统的复杂性，过往形成的传统IT架构以及基于这套架构所形成的解决之道，越来越难以适应经济系统复杂性需求。响应的周期、成本、效率难以满足客户的需求。

基于传统IT架构的解决方案，核心是如何解决企业内部的资源和架构的管理问题，即使进行了面向内部资源的优化，但最终的结果，往往是构建起一套封闭技术体系。

云计算与传统IT架构完全不同，它不再只是提供硬件+软件的解决方案，更多是提供一套以消费者为核心、以服务为形式、以数字技术为手段的完整基础设施。

以云计算为基础，企业可以思考新的问题，即数字化转型，例如如何面向全局优化，实现与供应商等合作伙伴以及客户的数据集成，构建面向全局乃至全产业链优化的开放技术体系，或是利用数字技术结合数据洞察，加速生产、提高效率或是改善成本。

在当下，外部环境的诸多突发事件，在复杂经济系统之上，叠加了前所未有的紧迫性，数字化转型变成必选项，它从原本的“增长轨道”被许多企业切换到“生存之道”，地位和价值产生了根本性的变化。从传统IT架构切换到以云为基础的体系架构就变得更加重要。

因此，无论是为了面对经济系统的复杂性，还是推动企业数字化转型进程，企业构建以云计算为基础的解决方案和新的技术体系成为必然，云计算不再仅仅是一个单纯的IT名词，而是一个企业生存、发展和转型的应对之道。

新消费、新经济是当前复杂经济系统中重要的、以数据为基础的代表，它们代表了算力和智能为手段的新阶段，云计算所提供的极致算力和智能（算法），为数据价值的充分利用提供了可能，也因此成为新消费、新经济以及数字经济的基础设施。

当我们把云计算看作一种基础设施和技术体系建构方式之后，云计算所提供的就不再只是常被提及的经济性和快速响应。云计算为企业在新消费、新经济的市场环境下，提供了五项重要的价值：

第一，云为企业提供新技术和资源的供给。云计算既是数字经济的基础设施，提供算力、存储、网络等资源，更重要的是提供了可靠易用的云平台、全局智能的大数据、云端一体的智联网和随时随地的移动协同，是以高经济性提供新技术的平台。以阿里云为例，243个行业解决方案、37个行业通用方案，其中包含了大量前沿技术，并以云服务的方式供给企业，极大的降低企业的新技术应用门槛。

第二，在云上企业能够更快连接合作伙伴与客户。随着数字经济转型进入深水期，越来越多的非互联网企业将会选择全面上云，云计算的支出正在成为每一个公司的标配，使用云计算的能力，是企业基础能力的重要组成部分和指标。这意味着，在互联网+传统产业的过程中，为了尽快与客户的业务系统、产品平台和技术体系接轨，企业必须尽快上云。同时，在同一套云平台下建立起企业间的数据、技术和产品连接，简化系统架构和业务接口的复杂性，要远比在物理IDC及封闭技术体系上更加简单迅速。

第三，云计算架构在经济学上更加经济。云计算是一种大规模分布式计算的模式，其推动力来自规模化所带来的经济性。在这种模式下，一些抽象的、虚拟化的、可动态扩展和被管理的计算能力、存储、平台和服务汇聚成资源池，通过按需交付给外部用户。

在云计算中，无论是基础设施、平台还是软件，都需要较高的初始固定投入，但是这一初始固定投入一旦建成，就可以反复共用而极少耗损，从而利用分享基础设施、平台和软件来降低边际投入。

在用户侧，对于云上的企业来说，第一，由于云服务商的边际成本的降低，企业可以以更加经济的方式获得基础设施；第二，企业个性化的每项增值业务，只要进行一个较低的边际投入，就可以展开广泛的服务，无须从头开发基础设施、平台和软件；第三，新技术的采用具有不确定性但初始成本较高，云上则为用户提供了按需付费、以租代买的方式，对降低企业的投资有较大的帮助。

第四，技术领先性降低了新技术采用门槛。IT技术发展的趋势一定是加速发展的，其速度要远远超过一般企业IT基础设施迭代的速度，这意味着在下一个更新周期到来之前，企业需要持续为性能、效率和可用性逐渐落后的IT基础设施付费，而竞争对手很可能在通过云上的技术红利获得更优质的IT资源和IT技术。

以AI领域当前炙手可热的GPU算力为例，从2018年9月到2020年5月，GPU单卡算力提升了大约7倍，在特定场景下提升了11倍，8块GPU卡的AI超算系统的峰值算力可达10 PetaOPS。如果一家企业在2019年初投入1000万用于采购GPU算力，那么现在这些算力的价格可能只是原来的几分之一。

第五，云的安全和可用性避免风险支出。2019年，CNCERT接到网络安全事件报告超过10万件，而随着“互联网+”加速与产业融合，安全威胁从线上到线下，意味着企业面临着比以往更加复杂、规模更大的安全问题。

安全能力的滞后会在未来越来越多的造成风险支出的上升，2017年蠕虫式勒索病毒WannaCry在全球造成了超过80亿美元的损失，这其中既包括雷诺、台积电等传统工业制造业企业，也包括互联网、信息技术领域的多家企业。

安全问题不仅仅是依靠技术和产品，安全团队的能力和安全防御经验实际上更为关键，只有足够的安全团队及丰富的安全经验，才能够在物理安全、硬件安全、虚拟化安全、云平台内部身份和访问控制、云平台安全监控和运营等方面进行了全方位安全设计和建设，而这些正是云服务商在努力构建的。

2 启动全面上云战略

1 全面上云战略的定义与必要性

根据《2019中国企业数字转型指数研究》显示，中国企业在数字化转型方面成效显著的比例仅为9%，平均成绩只有45分，数字化程度整体偏低。IT基础设施作为数据这一生产要素的产生、加工和价值挖掘的主要承载工具，直接影响企业数字化进程，IT架构陈旧无力支撑上层应用的多元需求成为转型的一大瓶颈，形成诸多数字化转型中的阻碍。

跨平台异构环境的数据难打通。由于历史原因，早期企业部门间的IT建设缺乏统一管理，应用需求差异较大且开发时间不一致，导多个软硬件平台的信息系统同时运行。这些系统数据相互独立、隔离，应用间的数据天然割裂。随着数字化进入到全新的发展阶段，构建数据驱动的精细化运营体系，需要打通组织内部的数据壁垒，实现生产过程全链条的全量数据汇集，这也成为企业基础设施主要瓶颈。

高并发、不可预测访问需求承载力有限。随着互联网化的进程持续推进，互联网形态的业务日渐丰富。相比较过去传统业务，企业业务具有更强的“在线”形态，在诸如抢购、秒杀、网促等场景下，要求IT架构能更好的支撑高并发、高弹性的业务需求。而现有基础设施架构为应对可能存在的业务峰值，需要储备大量物理资源，造成了严重的资源闲置，随时存在因不可预测流量冲击导致业务中断的风险。

快速响应用户需求变化，推动应用产品迭代更新是数字时代企业最有力的竞争手段，偏稳态的传统基础设施略显乏力。

在数字技术支撑方面，传统基础设施对大数据、区块链、人工智能等新兴数字技术在算力支撑、统一服务编排调度等方面的支持能力有限，难以构建基于数据驱动的交付流程，产品交付的效率大打折扣；

在应用开发方面，基于传统信息系统构建的业务应用，集成了多个业务逻辑，修改其中部分程序也需要对整个程序进行重建和部署，阻碍了应用开发效率；

在运维管理模式方面，传统基础设施架构下企业将开发、IT运营和质量保障分三个各自独立的部门，软件开发和部署涉及组织多部门间的联动合作，沟通协作成本较高，影响应用交付效率。

IDC《全球云计算IT基础设施市场预测报告》数据显示，2019年全球云上的IT基础设施占比超过传统数据中心，成市场主导者，这意味着，云计算市场正在发生一场新的转变。

在过去十年的云计算发展中，企业上云经历了基础IT要素（硬件、软件、数据）上云、企业业务系统云上运行、企业间云端互联三个阶段，随着数字化转型进程的加速，企业进入上云的第四个阶段：全面上云，即企业所有业务都要迁移上云，并在此基础上围绕价值链实现与其他企业的云端互联，云平台功能从企业内部系统集成扩展到产业链上下游企业间资源共享，业务协同，实现更高效的集成应用模式。

除了以上诸多因素，企业全面上云还存在着以下三点必要性：

首先，围绕云计算将建立新型技术体系，全面上云将享有“数字产业上下游技术升级”。以云计算为核心的新型技术体系，将建立起完全不同于传统IT的全新架构体系，硬件从高性能单一系统转向大规模定制化、分布式平台，中间基础软件转变为云操作系统、云原生软件，前端应用向软件即服务的模式转型。

新体系以分布式的极致性能和高可用性为基础，构建起超大规模、超高密度的数字基础设施，并以此驱动对底层硬件（包括但不限于芯片、服务器、存储、网络等）和中间基础软件（包括但不限于数据库、中间件、操作系统等）的重新设计，重塑整个数字经济的产业链和生态体系，因此，企业全面上云将享有“数字产业上下游技术升级”，而不单纯是IT基础设施的改造升级。

其次，数字原生时代的应用与智能将以云为基础爆发，云及云上能力成为企业应对关键。数字原生的生产方式正在推动各个产业升级，伴随数字原生时代到来的是应用大爆发、智能大爆发，以及企业用户的大爆发。据IDC预测，到2023年，将有超过5亿个数字应用程序和服务使用云原生方式开发和部署，相当于过去40年开发的应用程序总数。城市大脑、自动驾驶、科技抗疫、淘宝直播等数字原生的应用越来越广泛，任何传统IT基础设施都已经无法满足数字原生大爆发的需求。

第三，经济增速放缓、市场竞争加剧，在相当长的一段时间内留给“从容上云”的窗口期将越来越少。随着人口、资本和规模三大红利的消失，整体经济增速放缓已经成为事实，市场竞争在低增速背景下正逐渐加剧，在相当长的一段时间内，企业的主要精力将放在生产与营销领域，通过新技术采用、新产品上市和新营销手段拉动企业业务增长。

在云上的业务系统、前端应用乃至业务团队可以专注在商业模式和创新，逐步屏蔽底层的技术建设的需求，在这一过程中为每个创新主体提供便捷、快速、智能的平台，实现数字原生的数智化建设方式，快速实现数字化应用构建和部署，企业IT团队将聚焦于服务这些团队的需求，释放给传统IT基础设施的资源有限且不足，并很难在短期内推动云下系统的上云旅程，“从容上云”的窗口期将越来越少。

2 全面上云确保与消费者永续连接

与消费者保持7x24小时的持续服务一直是全球化企业的重要战略，为此许多企业建立了横跨多个大洲的“日不落式服务”呼叫中心，以某手机品牌为例，其呼叫中心遍及欧洲、美洲、亚洲、非洲，甚至在某些大洲按照一定

的时区间隔来配置呼叫中心站点，但这是一件成本高昂的建设：全球化部署的呼叫中心意味着规模庞大的基础设施建设以及本地（大多数时候还包括多语种）人力资源储备。这是作为全球化企业必须要面对的挑战，但也让企业获得了消费者的极大信任和依赖感，“无论何时、何地，总能够联系到客户服务”成为全球化企业的竞争优势之一。

现在，与消费者持续保持连接意义发生了改变，消费者不再将焦点全都放在是否存在7x24小时的呼叫中心，而是更加关注企业的服务可用性，即是否能够随时随地的获得服务，并时刻关注服务状态和进程是否符合自己的需要和预期，并由此延伸出一个新的需求：接触频次。正如电商网购消费者中的绝大部分客户都会频繁查询发货、物流和配送状态，消费者希望获得永续连接，这种永续连接体现在持续的、高频次的接触上，消费者会持续不断的“Ping”，一旦中断便会产生极大的忧虑。

在保持永续连接方面，数字经济时代有着天然的优势，新技术让数字互动更频繁、摩擦更少和充分定制化，因此企业可以与消费者建立比以往任何时候都更紧密的联系。不可否认的是，数字化与新技术也加重了消费者对接触频次的要求，因为这种接触的单次成本对于企业和消费者来说都比以往有着断崖式的下跌：外派平台只需要提供定位信息，消费者则只需要点击一次刷新按钮。

以接触频次为代表的永续连接是一种全新的消费者连接方式，它高频次、双向低成本、以数字化和新技术作为支撑，它实质上是一种高频次的数据提供按需服务方式，消费者通过网络和数据与企业保持永续连接，但这种连接受到非常大的挑战，全面上云则是确保企业与消费者永续连接的重要支撑。

– **全面上云首先确保了系统持续可用、充分可靠。**提高业务系统的可用性与可靠性是企业IT服务首要目标，但在传统IT架构下，为了保证系统可用性与可靠性需要付出极大的成本建设1:1的冗余保障系统，而且一个节点的冗余也无法完全保证数据与业务的万无一失。在云上确保系统可用性与可靠性不仅能够利用云平台本身的高可靠性获得提升，云的弹性支持建立“不对等”的云上容灾、备份系统——可以从较小的规模进行建设，并在故障发生时快速扩容。

– **全面上云避免因为地域、距离问题而降低服务水平。**对全球化企业来说，几乎可以认为每时每刻都有消费者在使用你的业务服务，这意味着无论是地域、距离还是网络等方面的差异，都不能也不应该成为降低服务水平的借口。选择全球化服务的云服务商，企业全面上云意味着在全球范围内资源规格、服务水平、技术体系都几近统一的云服务，并可以将业务在全球分布式部署，从而避免上述问题所导致的服务水平降低。

– **全面上云帮助企业每一项业务都拥有极致算力和高效智能。**在数字原生时代，企业的每一项业务都将具备数字化的端（无论是内部应用还是外部应用），这必然产生对算力和智能需求。为了更好的提供服务，云与端之间的链路被逐渐打通，云持续向前端延伸，形成云端一体的全新形态。云端一体的融合模式为各种场景提供了最高效能，最低延迟的解决方案，企业每一项应用都将获得云端极致的算力、大规模存储、高效智能、安全等服务，形成数字经济基础设施的企业内普惠。

3 全面上云驱动企业IT从成本中心向服务中心转型

长期以来，企业IT被认为是企业的成本中心，即使是在强依赖IT基础设施的互联网企业，由于其成本范围最广、成本费用发生占比较大、成本支出与业务增长之间关联性不强，以及往往因为业务压力存在持续的、高增长的、高昂的硬件（固定成本）支出，企业IT仍然无法摆脱成本中心的角色定位。因此，企业IT存在只考虑成本费用、只对可控成本承担责任、只对责任成本进行考核和控制的特点。其中，可控成本具备三个条件，即可以预计、可以计量和可以控制。

在以计量和控制为导向的成本中心的角色定位下，企业IT往往会存在过度追求成本效益管理职能，并为了具象化从而获得管理层认可，过度追求IT投入建设后企业所能获得的具体价值与收获，继而出现如下三类常见问题：

1、为支持重点业务，不断增加IT投入。

由于企业信息化时代的IT投入惯性，往往会在部分重点业务上进行资源上的重点投入，以期通过资本和资源红

利，帮助业务快速成长，实现高占比市场份额，并在持续高速增长中获得更多的资本投入，在这一过程中，企业IT经常陷入“大力支持高增长的重点业务”的误区，为该业务配置或新购大量IT资源，甚至会发生超额配置、超期采购的情况，一方面，忽略重点业务的数据洞察，另一方面，忽略IT投资回报率，造成IT资源的浪费；

2、过度计量导致IT资源紧张，无法支撑业务增速且新技术采纳度低。

在缩减成本、降低支出的需求下，企业往往会首先削减IT投入，并要求企业IT进行精细化、实时化和业务分账制的计量，为了符合企业高层的要求，IT团队经常会过度计量，降低IT资源供给速度，以需求最小化的方式进行计量，这会直接体现在减少硬件采购、减缓软件支出、避免新技术采纳等方面，过度管理受短期业务要求和需要驱动的IT项目。此外，IT团队会为了成本导向放弃IT架构指导方针，这些违规行为通常会让IT运营更加复杂，进而增加了长期成本。

3、过度追求投资回报率和业务流程，导致IT建设融合度低。

在企业的高速发展期，IT建设模式一般是以项目式的系统开发，即先由企业里的某个部门提出需求，然后通过招投标确定IT系统建设单位，收集企业里的业务需求，制定开发计划、测试、上线、维护。由于这些IT建设都是以单个部门或业务为导向的，必然会高度追求投资回报率。同时，IT团队为了保证自身责任的清晰，会高度追求业务审批流程的准确性和完备性。这种模式下的系统建设，采用瀑布式开发，严格分级，各系统独立建设，缺乏数据共享，会成为“烟囱式”的建设模式，出现大量独立的计算存储网络设备，资源利用率低，闲置严重，非常依赖容量规划，并且新业务上线周期长。

为了解决上述问题， 企业IT必须快速向服务中心转型，这一转型过程应当与上云路径同步进行，逐渐从IT支持角色转变为IT服务角色，逐渐从以IT技术为核心转变为以IT服务为核心，逐渐从以IT职能为中心转变为以IT服务流程为中心，逐渐从费用分摊的成本中心模式转变为按服务级别收费的利润中心模式。

1、上云驱动了企业IT向服务中心转型，转型加深、加快上云进程。

与过去主要是企业自定义和自定价的面向服务架构（SOA）不同，云计算服务商已经将IT资源和能力服务化，并提供极小颗粒度的配置方式，IT团队可以通过组合配置为内部业务部门提供服务，并建立内外部服务的对应关系，减少从资源到服务的转换。此外，由于云的自动化和自服务特性，IT团队能够将一部分IT工作释放到需求部门，减少大量日常繁杂的技术维护工作。随着IT团队向服务中心转型的加深，会进一步深化现有IT支持的上云进程，从而实现高覆盖度的服务化IT。

2、上云与向服务中心转型实现服务成本的透明度与可信度。

使用云计算服务商所提供的云服务具有标准的公开定价和服务水平定义，具有更加清晰地成本支出定义和服务等级协议，帮助企业IT从费用分摊的成本中心模式转变为按服务资源和级别收费的利润中心模式，从而维持云计算服务长期目标的实现和业务运作良性保持，合理平衡资源，收益和风险之间的平衡，从而创造云计算的最佳价值和长期可持续发展，使得云计算服务业务总体上得到有效的治理和管理，实现端到端的业务服务需求。

3、上云推动企业管理的改善、业务的提高，企业IT重要性随之提高。

在上云的过程中，降低和优化架构复杂性的综合评估势在必行，这将在多数领域发现重大的成本节约机会，可以帮助企业发现大量未使用或重复的应用，重复配置或闲置的资源，以及可供整合的子架构。由于云上服务的按需配置、按量付费，IT团队可以采用可预测性模式和探索性模式来支持业务需要，并通过流程自动化提高业务团队的IT配置自动化、自主化，从而推动企业管理的改善、业务的提高，企业IT重要性随之提高。

此外，IT团队可以应用具体形象直观的数字来描述IT系统投入建设后改善多少管理状况，给公司市场带来多大的成长，产出是否大于投入等，从而取得高管层充分的认可与支持。让高管层认识到IT部门不只是专业技术部门，也是一个创收、迸发经济价值的利润中心。

4、企业IT向服务中心转型没有终点，IT团队调整势在必行。

随着上云和向服务中心转型的进程加深，原本复杂、冗长、占用大量时间和资源的IT运维工作压力必然会持续下降，这意味着将有一定程度上的人力资源空闲。IT团队终于有机会将更多精力聚焦在业务上，而不是基础设施上，IT团队的积极主动调整将变得尤为重要。

在对团队成员进行精确细分的基础上，IT团队的调整有可以考虑如下方向：属于开发型的成员，可以支持其连接业务团队，持续推动DevOps，加深与业务团队的合作，甚至可以选择双线汇报；属于传统运维型的成员，应当鼓励其持续提高IT运维效率，尝试AIOps等新技术；属于复合型的成员，建以优化流程、计量、分账方式为主要方向，进一步提高上云后的IT团队价值测算。

3 以全面上云为起点，带动企业实现新“四化”

在数字经济时代，以大数据，云计算，人工智能，5G，物联网，区块链等新一代信息技术，将构建起支持整个“数字中国”的技术底座，这就是数字基础设施，也就是信息时代里像工业时代高铁和高速公路一样的基础设施，它是企业竞争力的基本能力，体现以数据为关键要素的算力、算法、数据为基础的特点。

未来十年是数字基础设施的安装期。数字基础设施的共同目标，以服务大多数企业和消费者为基础，并不断深化产业数字化的服务，而构建数字基础设施，需要对现有的信息技术基础设施的“四化”。

全面上云即企业IT基础设施的云化。以可靠易用的云为基础，实现IT基础设施的端到端的云化，就像当年工厂自主发电转变成完整的电网电力供应的电力变革一样，让大多数的企业不需要自己去构建数字经济时代最重要的算力基础设施，在云端获得可靠的IT资源、可靠的算力，而且具有很高的经济性。

云化为企业提供五项关键的能力，即数据能力、（资源）调度能力、安全能力、大规模实践和开放的生态，解决企业在数字化转型过程中所面临的传统IT基础设施分散、复杂、昂贵、缓慢和不稳定的情况，向供应电力一样，供应数字经济时代最重要的算力。

第二是数据化，构建全局智能的大数据。企业一直面临充分利用海量数据的压力，数据需要被有效利用、有效的被计算，但在过去，企业没有能力去处理这些海量数据，现在，企业通过强大的云计算平台加上高效算法，能够进一步挖掘数据价值，最大化数据效率，再通过清晰、直接的方式展现给企业的管理者、运营者，形成数据对企业运营、管理的正向循环。

第三是AIoT化，数据不是凭空创造的，更不是自动获得的，我们怎么建立与物理世界的连接和在线化？包括工业、农业、交通运输业等等，这个需要新的支撑，即AIoT。正是因为有了AIoT，我们可以连接物理世界的数据，各种不同维度、越来越细的颗粒度，更重要的是还可以反馈去控制这个世界。

与简单的连接物理设备为主的IoT不同，AIoT把原来离散的设备变成数据的输入端的同时，也让它们变成了在线的智能设备，像停车位、窨井盖、路灯、滴灌系统、生产设备全部在线化，能够自动连接到云上，形成云-端一体的数据流动、智能协同、高效管理、安全管控和全局资源调度。

最后是移动化，移动化已经深刻影响了消费领域，中国现在有9.04亿互联网用户，有6.94亿用户使用在线政务服务，但移动化并不仅仅是在线生活、在线社交，更是在线协同与在线办公、组织管理、高效系统和业务创新，并且沉淀下宝贵的企业数据，更重要的是全过程跨越了时间、地域、系统和移动性的阻碍。

企业在全面上云旅程中，用云逐步替代传统的IT基础设施系统，实现弹性计算、分布式处理、大规模存储计算、还有安全的能力，增强资源调度能力；用云上数据中台、大数据平台等帮助企业数据化，让企业通过数据的采集、清洗、归档、分析数据的同时，实现数据在感知、分析与预测方面的能力建设；云上的AIoT能力借助IoT设备和AI能力服务于企业来感知、认知和决策能力的提升。

最终，企业以全面上云为起点，数据与云深度融合、AIoT与云构建云端一体、云为移动化提供坚实的数字底座，带动企业实现新“四化”。

4 从全面上云到数字原生操作系统，阿里云 2.0 为企业和社会带来本质化改变

在信息化时代，企业利用IT技术实现业务的信息化，结合业务咨询，企业实现了一定程度上的流程优化与再造，并以传统IT基础设施为基础，建立起ERP、CRM等信息系统。

为了持续满足业务增长所带来的系统压力，传统信息化系统通过持续堆叠性能更高的硬件，如CPU、SSD等，提升系统性能，改善服务质量，但这也让系统不断变得更复杂、更昂贵，迭代速度也越来越慢，这被称为纵向扩展（Scale Up）。

当互联网服务这一全新的、以指数级提升性能和资源需求的服务形态出现，用户分布式系统以横向扩展（Scale Out）的方式取代传统信息系统成为必然，可以说，如果没有分布式系统，时至今日就不可能有互联网行业的飞速发展，更不会有互联网应用的大爆炸。

1 全面上云战略的定义与必要性

云服务商以分布式技术为基础，结合资源管控、调度，以及将其产品化和服务化输出能力，诞生了最初始的云计算的概念，并经过十余年的发展，在云操作系统（如阿里云的“飞天”操作系统）的基础上，成功解决了资源云化问题，形成了包括算力、存储、网络和安全等在内的云计算服务，并支持企业实现“四化”。

云计算突破了IT基础设施的物理限制，将算力等资源变成公共服务，这是一次体系性的跃迁，基于云的体系架构屏蔽了大量的底层技术细节，让用户可以通过服务调用的方式调用底层计算资源，从而比信息化时代降低了用户的使用门槛。

以阿里云为例，在为企业的数智化需求提供服务的过程中，用云逐步替代传统的IT基础设施系统，实现了弹性计算、分布式处理、大规模存储计算以及安全服务；用云上数据中台、大数据平台等帮助企业通过数据的采集、清洗、归档、分析数据的同时，实现数据在感知、分析与预测方面的能力建设；云上钉钉则帮助各个机构能够根据用户的使用习惯和需求进行移动协同的建设；云上IoT能力和AI能力服务于企业感知、认知和决策能力的提升。

过去几年，很多大中型企业已经通过上述举措实现了数智化项目的试点与探索。然而，当前外部环境的变化让数字化进程大大加速，很多企业缺少应对数智化需求暴增的开发和服务能力，尤其是大量业务用户的应用需求和大规模用户协作的需求无法得到满足。

为此，云服务商正在为企业提供更加完整的云平台，让云不仅与企业业务形成有效支撑、有机融合，更在屏蔽硬件复杂性的同时，更进一步，通过软件的组件化，提升软件开发效率，进而为企业应用开发提供一个新型平台。

2 云钉一体，让应用开发更容易

以云为基础，结合云上的数字化、智能化、中台化和移动化的能力，跨越传统软件工程中的将功能代码作为组件的“传统组件化”，将能力视作组件，重新定义软件应用的开发方式，帮助企业在建立任何种类的软件应用时可以快速构建，是云在突破IT基础设施的物理限制之后，进入到企业应用开发领域的新使命。

不仅如此，许多企业都拥有数量繁多的应用，超过1000个应用的企业同样屡见不鲜，但过去企业应用的构建时垂直烟囱式的方式，不仅构建过程中没有很好的组件式方法和资源复用，数据连接、应用互联、流程交互等方面更是难以解决，也正因为如此，许多企业根本无暇考虑IT基础设施的云化或是数字化、智能化，仅仅是处理复杂的应

用体系就已经戳捉襟见肘。

阿里云提出“云钉一体（云服务+钉钉）”的目标，即是为那些并非IT技术出身的企业用户提供更为简单易用的云计算服务，就像当年Windows为计算机普及提供了一个普世的操作界面，帮助企业基于“云钉一体”的基础设施更容易的开发企业应用，随着“云钉一体”为开发者提供更便捷、简易的应用开发环境，将极大地扩充企业乃至整个生态中可使用的应用数量，也就是产品数量。

因此，“云钉一体”将在提升企业移动协同水平的基础上，让企业应用开发变得更加敏捷和一体化，形成整体融通、全局最优的应用体系，并基于敏捷性而提升试错、迭代的速度，加速企业创新，从而帮助企业在数字经济时代保持充足的活力。

与此同时，云端一体则让万物皆有算力。云端一体，即云和端的融合，一方面，为PC端、移动端等端提供晕的能力，让端具有云端极致的算力、大规模存储、高度安全的能力；另一方面，即让部分边缘计算的端，在边缘侧提供全栈云计算产品和服务，通过与云进行协同，提供低延时的服务和降低对网络的消耗，以及IoT设备通过智能化的技术，实现数据的处理和采集，并将数据上传到云上进行大规模的计算。

云端一体的融合模式为各种场景提供了最高效能，最低延迟的解决方案，云将和各种各样新型的端，包括IoT的端、IT的端，包括其他新兴的端来组成新的云端一体，真正让全社会都能够获得以及发挥数字化、智能化的能力，让万物皆有算力。

3 阿里云2.0：飞天云平台+数字原生操作系统

很显然，为了更好地实践“云钉一体”，推动云端一体，现有的云计算产品形态和服务能力已经难以满足需要，需要一个基于云，其上具备移动协同、数据智能的、IoT的一体化能力的操作系统。

以阿里云为例，这个操作系统以钉钉、数据中台、业务中台、AIoT中台为核心，为每个创新主体提供数字原

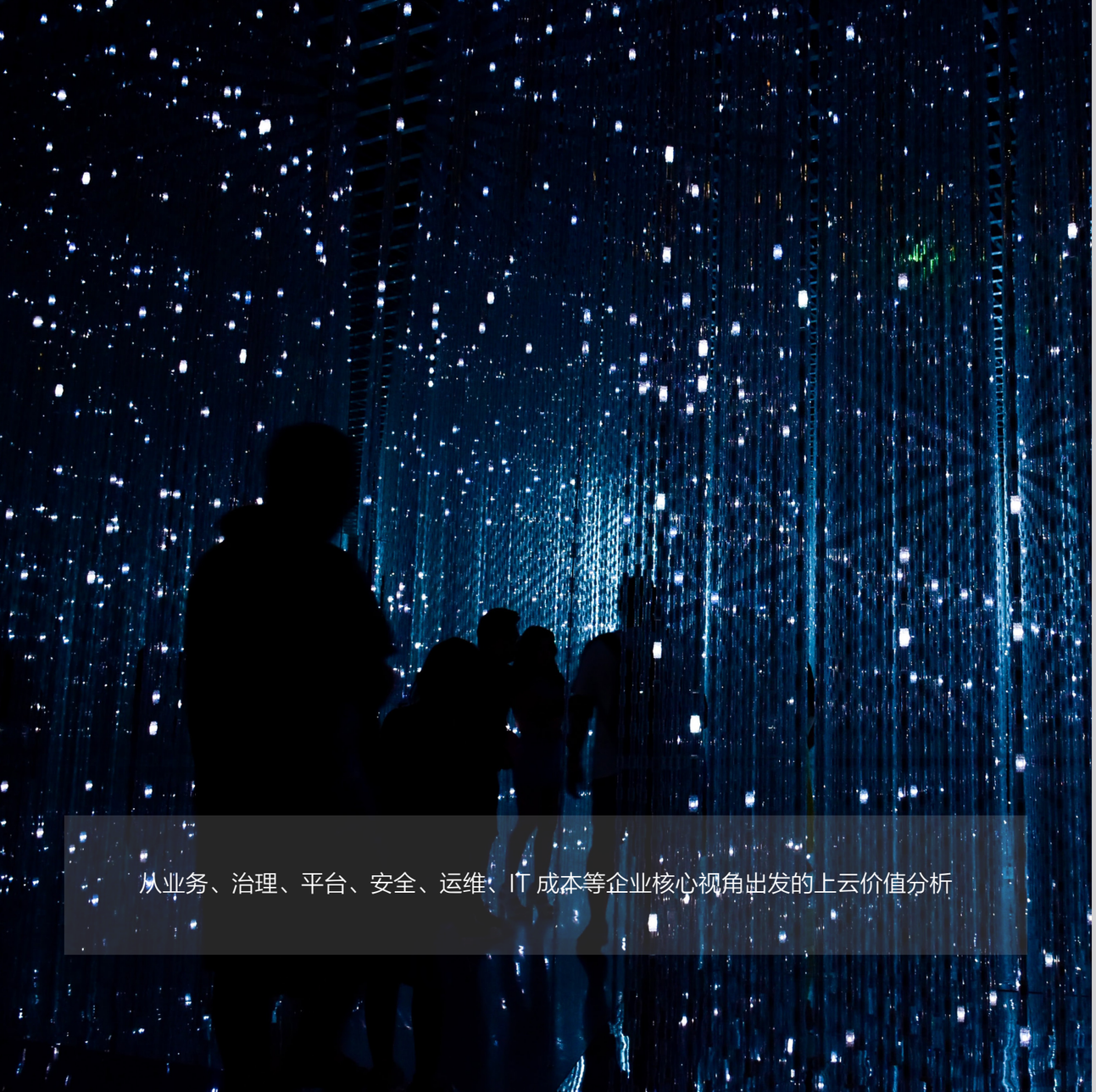
生的数智化建设方式，填补底层算力与数智创新之间的技术鸿沟，它将为每个创新主体提供便捷、快速、智能的平台，这个操作系统将让应用开发变得非常简单，让不会写代码的人也能用低代码开发与应用平台搭建自身所需的操作系统，快速实现数字化应用构建和部署。

企业可以通过这一数字原生操作系统直接调用数据、智能、应用和端的能力，专注在商业模式和创新，逐步屏蔽底层的技术建设的需求，只要通过操作系统就可以调用各种能力。

阿里云飞天云平台和数字原生操作系统将共同组成阿里云2.0，由狭义的云计算平台，成为一个为企业数字原生需求服务的复合型平台，在解决算力等云需求的基础上，把人工智能、移动协同、AIoT、数据与业务流程管理、应用开发等能力进行封装，让上层应用可以直接调用各类能力，普惠每个组织，进一步释放全社会数字化、智能化的创新能力，特别是让中小微企业参与到数字化中，让原来用不起来云的机构，都能得到即开即用的云。

阿里云2.0将实现更强大的平台和组织间的协作，既改变了云的使用方式，也改变了企业开发应用的方式，让云可以向水电煤一样，普及到更多的企业，更多的人，更多的系统中去。

因此，阿里云所提出的全面上云，并非简单的“全站上云”或是IT基础设施的迭代，它将是把未来的信息系统变成一个智能化的、面向未来的数据智能、移动化的新型系统的起点，从全面上云开始，结合数字原生操作系统，为企业和社会带来本质化改变。



2 企业全面上云成功路径与实践
上云价值分析

1 业务视角

企业在价值创造和价值变现的发展过程中，IT基础架构数字化转型主要的矛盾体现在需求与供给上严重不匹配，无法有效应对业务能力全面提升、数字化运营、数字化业务发展的挑战。

首先，如何通过新的业务模式、新的产品影响乃至颠覆当前行业市场？在市场洞察的基础上，如何快速进入新市场并保有当前市场份额?

我们从企业决策层的视角看，企业的关键举措需要最大化股东价值，提升业务敏捷度，以企业战略优势为目标，优化企业投资，全面优化企业运营效能。企业数字化转型要帮助CEO在市场洞察的基础上，快速拓展新业务，进入新市场并保有当前市场份额；能够提升企业创新效能，紧贴市场需求，及时发布新产品与新服务；提高业务敏捷度，使得业务运营与市场反馈相匹配，使服务与产品更快面向市场。

企业数字化转型要帮助COO提升由数据驱动的企业洞察力，使得运营有效性提升，更好推动产品与服务设计过程，使业务运营匹配企业战略；设计全新的企业产品与服务，推动市场需求挖掘，深入理解市场，并迅速响应新

兴市场的需求；通过“服务化”模式，降低运营成本，结合数据分析结果，获取更多运营洞察。

企业数字化转型要帮助CHO在人事计划范围内，及时获得优秀人才资源，优化人才结构，提高人员效能，打造多方共赢的团队文化，打造主动学习的能力与氛围，为员工、团队、企业文化的成长提供更加深入的洞察。

其次，随着新技术的高速发展，企业如何从中获益，如何快速使用新技术，为业务创造价值，如何将技术与业务进行深度融合？

企业全面上云能够促进IT支持业务开展效能，建立并保持企业技术远景洞察力，能够帮助CIO通过IT基础架构数字化转型全面提升企业IT治理水平，降低IT治理成本。为企业提供业务快速开展、产品与服务交付的IT支持，更好地支持业务目标达成，包括：促进业务敏捷性，加强IT资产与企业数据安全性，提升IT效能与生产力，优化对业务的支持水平。

企业全面上云能够帮助CTO明确技术发展方向，企业如何从新技术中获益，为更多新技术的应用提供基础保障；企业如何将技术与业务进行深度融合，帮助企业更加快速有效地跟进技术发展趋势；企业如何降低成本支出，提升技术产出效能，通过新技术，快速开发可落地的实际企业应用。

企业全面上云能够帮助CDO巩固数据质量，保证数据来源的统一性、可靠性，为业务开展提供更好的洞察能力，助力企业决策；提供尖端的数据库技术与数据接入工具，推动业务精益化并提供更好的数据管控与数据治理方法；将机器学习过程融入当前已有的企业分析能力中，为决策者、核心业务流程提供更优质的数据获取方式。

再次，面对不确定的信息安全威胁，如何及时更新升级企业现有安全服务，建立安全防护策略，由被动型向预测性安全感知模式演变？

企业全面上云能够帮助CSO建立立体多维度的安全防护体系，实现IT基础架构安全管控全面升级，规避潜在安全隐患，建立安全防护策略，由被动型向预测性安全感知模式演变，及时更新升级企业现有安全服务，以最小的成

本代价，降低企业安全风险。借助大数据分析与机器学习手段，高效管理并监控企业风险，对企业的全局风险增进识别能力，识别可能存在的风险，以及对企业潜在的影响，当达到安全风险阈值时，主动提示业务风险管理部门。

最后，企业业务主要的痛点与难点是如何聚焦在业务创新本身，如何使用最小的成本，最快的速度，在架构、技术、安全上进行全面提升，在数字化转型过程中，“给飞行中的飞机换引擎”。

云时代的到来，影响到企业运营的方方面面，越来越多新的产品形态和商业模式变为可能，身处云时代的企业领导者，都会受到深远影响。我们看到越来越多的企业正在使用云计算服务，享受云计算带来的业务变革和技术提升的红利。云计算已经不仅仅是作为基础应用，它带来了“一切即服务”的蓝海，使得任何IT能力都可以变成基于云的服务供企业使用。不断开拓新的市场，创造新的价值，满足新的需求。

1 业务支撑

过去十年来，全球企业在数字化转型方面进行了大量投资，数字化转型是增长最快的技术/服务集群之一。IDC预测，到2023年，数字化转型将占全球信息化支出的一半以上。这意味着企业在数字化转型上的投资将有史以来第一次超过在所有其他ICT项目上的投资总和。数字化技术在金融服务、制造业、零售业、交通运输等垂直行业取得长足发展，数字化转型迅速成熟。其他垂直企业也正在取得更有意义的进展。无论他们处于何种状态，所有的行业/垂直行业都在将数字技术整合到他们的业务流程中并不断重塑，以提供非凡的价值。

云计算是这一转型旅程必不可少的第一步，数字化转型中的战略、业务目标及挑战，企业可以由通过构建云能力堆栈实现并带来收益，进一步攫取市场份额并保有当前市场地位，全面推动业务转型，快速拓展新业务，进入新市场，提升企业创新效能，提高业务敏捷度，使服务与产品更快面向市场，为企业建立新的差异化竞争优势。

云计算对业务的支撑可以体现在如下四方面：

业务创新： 通过IT转型引领变革，带领业务创新实现增收。

在业务创新领域，企业通常会面对以下挑战：

- 如何支撑应用从传统架构向云计算架构转型；
- 如何支撑数据驱动的业务创新；
- 如何支撑混合云战略，避免出现影子IT（未被IT部门授权或批准的员工或团队使用的硬件或软件服务）现象；

云计算将从以下方面应对挑战：

- 云计算将支撑稳态与敏态双模应用。在此基础上，通过云计算环境实现应用的快速部署，为业务部门和开发人员提供可靠一致，标准化的开发和测试环境。
- 通过云平台的服务包装能力，将数据服务能力包装成为IaaS、PaaS或SaaS服务。
- 通过云计算的混合云管理能力，实现混合资源统一管理。

提升效率：转型后的IT提升产品交付速度，缩短交付周期。

在交付领域，企业通常会面对以下挑战：

- 如何以服务的形式为业务部门提供更好的运行环境；
- 如何提升业务部门和开发人员使用基础资源和工具的感受和满意度；

云计算将从以下方面应对挑战：

- 利用云计算的弹性和灵活，根据业务负载大小周期，动态调整业务场景的使用资源，保证业务场景的响应速度，从而提升IT用户感受和满意度。

- 利用云计算统一资源治理架构，优化流程，自动化过程环节，缩短资源分配的周期，提升业务部门的满意度。

保障质量：转型后的IT确保应用系统稳定易维，安全合规。

在系统运维领域，企业通常会面对以下挑战：

- 如何提升关键应用场景的可用性和安全性；
- 如何优化灾备系统，扩大灾备覆盖范围；
- 如何快速发现问题，隔离问题；

云计算将从以下方面应对挑战：

- 利用云平台资源管理和高可用功能，减少计划内和计划外的停机时间。
- 利用云平台的高可用特性，优化灾备方案，提升应用高可用的能力，提升SLA水平。
- 优化核心资产的管理与部署，更好的保护企业无形资产。
- 利用云平台的监控与展示能力，统一管理混合云环境，并根据利用率及运行状态实现资源的灵活调配与故障及时处理。

优化成本： IT转型后降本增效，构建服务生态。

在成本控制领域，企业通常会面对以下挑战：

- 如何提高资源利用率；
- 如何降低基础架构运维成本；
- 如何降低服务成本；

云计算将从以下方面应对挑战：

- 通过云计算技术整合现有资源，实现基础架构的模块化与标准化，提高资源利益率，降低运营成本。
- 通过云平台实现更精准的资源配置，提升效率，降低成本。
- 扩大自动化覆盖面，将运维人员从传统的重复劳动中释放，投入到高价值工作中，降低运营成本。
- 结合现有资产，合理规划与利旧，实现物尽其用。

2 服务目录

建设目标

服务目录的主要目的是为所有约定的IT服务提供一个一致信息源和建立其它服务管理组成的基础。本质上,它清晰地定义了业务、研发部门从IT组织可得到的服务列表，以及按商业目标和需求定义的服务内容。服务目录在设计之初，通常具备如下三点目标：

- 建立统一服务列表，其中包含服务的业务描述以及服务的申请方法；
- 提供计费计量方式及相应的服务级别；
- 一个覆盖云服务及产品全部服务请求的独立、综合的信息。

建设意义

设计并实现服务目录，通过以上目标的制定，可带来如下的价值：

- 用户能够充分了解可供自己使用的服务以及如何申请这个服务；
- 用户在对服务有所了解的情况下，能够做出合理的决定；

- 辅助管理客户期望；
- 简化服务订购。

重点考虑内容

服务目录在设计时需要重点考虑的因素包括以下四点：

- 服务定义；
- 费用；
- SLA（服务等级协议）；
- 如何订购。

建设步骤

服务目录的主要目的是为所有约定的IT服务提供一个一致信息源和建立其它服务管理组成的基础。本质上,它清晰地定义了业务、研发部门从IT组织可得到服务列表和按商业目标和需求定义服务内容。服务目录在设计之初，通常具备如下三点目标：

- 服务定义：描述服务的详细信息、功能、优点、价值等信息，为服务请求者提供服务及组件的成本、计费等信息；
- 自助门户：协同门户，实现跨项目、跨组织、跨部门的团队协同；
- 目录视图：提供业务服务目录及技术服务目录视图；
- 系统开发生命周期SDLC：通过系统开发生命周期（或DevOps支撑平台、技术库等）定义关键集成点及流程，以支撑实现业务需求；

- 需求管理：灵活度量及监控服务需求以确保能力能够满足服务等级协议；
- 服务等级协议SLA：服务等级协议包含在服务定义中，SLA提供围绕各层级服务的可用性及关联费用详细信息；
- 安全：包括提供基于角色的访问控制、单点登录、数据安全等功能；
- 服务计量计费：实现基于消费模式的业务使用计费模型，提供IT服务计量和计费功能，服务目录可以通过调整消费行为管理IT成本；
- 服务管理：提供围绕服务设计、实施及运维的支撑流程以实现对服务的评价和监控服务的效率和性能。

3 业务视角的上云价值

在传统的业务战略模型中，IT的通常扮演支撑角色。云计算的兴起，技术正在重新定位并越来越在战略决策中扮演重要的角色，信息技术主要提供的不再是支撑能力，而是创造能力。云计算正逐渐帮助企业提炼信息技术现代化能力，构建企业数字化核心技术体系，成为实现IT供给侧结构性改革的“新基石”。同时，不断构建完善高效敏捷的数字化运营体系，强化“技术应用”与“业务战略”的不断融合，重塑IT来实现管控效率提升，帮助企业迅速回应技术对市场的影响以及相关业务挑战，成为企业发展战略的“新引擎”。

通过云计算重新构建企业IT信息化建设概念体系和运营模式的主要工作包括：

- 确定企业全面上云战略，推动IT基础架构数字化转型；
- 通过云战略愿景、组织影响、财务影响、技术架构、安全、风险与合规等多个维度的结构化模型和经过验证的方法，规划有效和实用的云战略，建立一套完整的云战略指导原则，确定云能提供的价值，保证整体云战略与业务需求相匹配；
- 对现有资源进行进一步优化整合，确定上云路线图，优化人力配备，提升资产利用率与运营效率；
- 实施上云战略，通过云上服务目录和服务编排设计，实现IT基础架构的标准化与服务化，能够支持业务的发展，实现应用层IT资源的灵活调度；
- 对应用/数据充分保护、统一管理，提供便捷、安全的业务体验，为打通全价值链及新业务运营保驾护航。

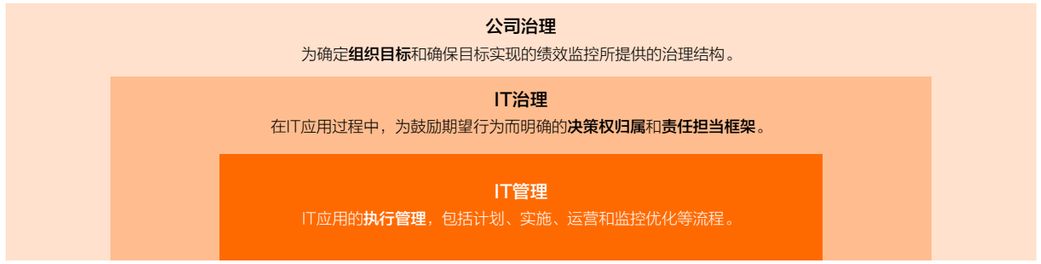
作为构建云计算的主体，企业云管理部门的终极使命是打破IT内部的壁垒，打破IT与业务的壁垒，用最快的时间，最低的成本，最好的质量来实现业务的任意需求，创造业务新场景，最终支持企业转型为融合业务与技术的“数字定义”生态圈经营体。

云的建设过程，是效率革命的过程，也是技术、组织、流程多方面适配业务变革的过程，赋予IT前所未有的参与业务的“机遇”。

2 治理视角

1 IT治理现状

IT治理是公司治理的一部分（如下图*），是通过明确IT决策归属和责任承担机制，确保IT促进企业发展，并管理与IT相关的风险。在IT治理的框架下，企业IT组织实施各项IT管理工作，除了架构管理外，还包括开发管理、测试管理、质量管理、版本管理、生产运行管理、安全管理等组成部分。IT治理的水平影响的是企业IT的质量，架构的质量、模型的质量、数据的质量，当然最终也影响业务的质量。



*来自《IT治理：一流绩效企业的IT治理之道》

2 企业IT治理所遇到的挑战

IT主要关注企业的IT投资是否与战略目标相一致，从而构筑必要的核心竞争力。IT治理要能体现未来信息技术与未来企业组织的战略集成，要尽可能地保持开放性和长远性，以确保系统的稳定性和延续性。通过IT治理方面的制度安排，能有效地推动IT战略与业务战略融合，提高IT投资回报率，降低IT风险。但同时，企业IT治理也面临着诸多挑战：

账号与权限的风险

- 未经授权的访问
- 本地账号依赖（对于本地的账号依赖不利于业务的扩展）
- 多租户多账号导致的管理复杂度
- 无法与外部合作伙伴共享资源（传统的身份验证机制或第三方多重身份验证可能不适用资源共享）

资源配置风险

- 资源浪费
- 资源预配不足
- 管理效率低下
- 业务中断

成本管控的风险

- 预算控制
- 利用率损失
- 支出异常
- 过度预配资产

安全风险

- 数据泄露或丢失
- 服务中断

网络风险

- 不必要的网络成本
- 网络管理效率低下
- 业务中断

③ 治理视角的上云价值

企业IT治理的复杂度通常取决于如下几方面：

- 企业组织架构：如治理机构（如IT治理委员会等）的设置和权限的划分，组织内机构职权的分配以及各机构间的相互协调；
- 管理成熟度：企业公司治理的成熟度是否足以支撑IT治理；
- 企业运维人员数量；
- IT消费数量：包括软/硬件，人工，以及第三方服务消费；
- 资源/服务提供商数量；

可见，在传统的IT格局下，企业规模越大，业务流程越复杂，IT治理的复杂度也会大大增加。如今，通过业务上云，传统的IT治理转化为云治理，企业可以大大简化IT治理复杂度，加速IT治理过程。

企业业务上云通常分为项目试点、构建基础架构、应用迁移、持续治理四个阶段。

在项目试点阶段，主要工作包括评估云计算的收益，采用公共云解决特定的业务问题（例如电商、大数据、物联网等）。此阶段无需治理；

在构建基础架构阶段，主要工作包括把公共云作为企业数据中心的延伸，建立可扩展的云安全、合规、运营体系，并迁移少量应用系统作为试点。在此阶段，云治理主要关注访问控制和资源管理的轻量级治理模式；

在应用迁移阶段，主要工作包括做好在云上长期运营 IT 的准备，迁移现有应用到云（包括关键业务应用，甚至整个数据中心）。在此阶段，云治理主要关注基于组织架构的企业级IT治理模式；

在持续治理阶段，企业开始注重优化业务模型和技术流程，云成为 IT 建设的默认项。在此阶段，云治理主要

关注效能优化治理模式。

综上，通过业务上云，传统的IT治理转化为云治理。后者将大大减少企业对系统运维、IT消费数量、资源/服务提供商等方面的治理工作，使得企业更关注于业务和组织的持续治理及优化本身。因此，我们认为云治理是IT治理的进化形态。

3 平台视角

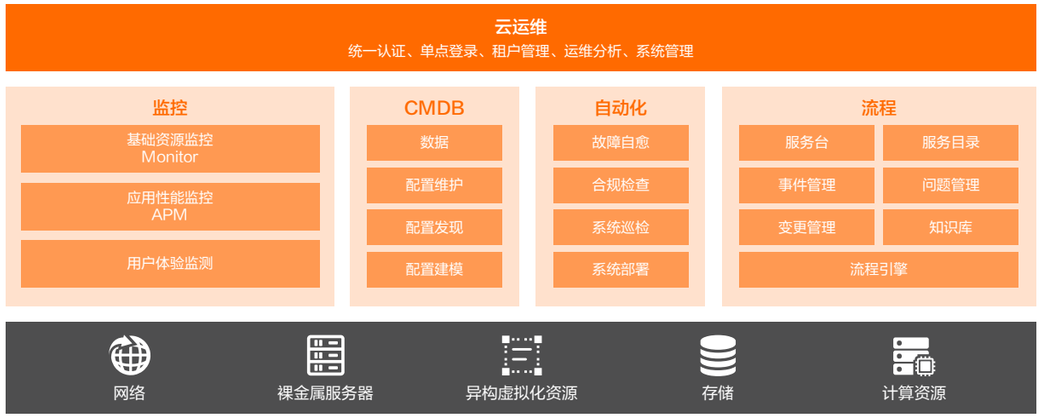
① 资源管理

企业对于IT资源的管理，在过去的二十年中，走过了从离散的雏形，到数据集中处理，到云数据中心三个阶段（如下图）。

分散雏形阶段的特点是：缺乏规划，分割管理、摸索建设。数据中心的建设往往就地取材，没有规划，专业性不强；IT组织以建设任务为导向，常常随IT项目建设边使用边改造；运维专业化程度处于较低的水平，缺乏专门的管理目标和管理手段。

云下数据中心（IDC）阶段的特点是：整体规划，专业运维。数据集中存储、处理，应用和业务集中化；建设依托有效规划，更加现代化，大规模数据中心引入“两地三中心”模式。引入运维流程框架，通过流程实现跨部门的运维任务在各个专业部门之间的贯穿和协同。缺点是应用与基础架构耦合严重，不利于业务的快速增长和变革。

云计算阶段的特点是：应用与基础设施松耦合，资源服务化。公共云在逻辑上成为一个整体，要求运维组织不再按照专业领域进行部门划分，而是按照云服务商设置划分。公共云“高可用性”有了基础级保障，运行维护工作核心开始围绕服务和资源的合理提供、监管和调度。公共云还可以提供一体化的底层计算网络存储的资源管理（专有云/公共云资源管理；裸金属服务器资源管理；计算资源管理；网络资源管理；存储资源管理，异构虚拟化平台管理），如下图。



2 服务输出流程

除了资源管理，企业基于云平台还可以实现多种IT服务流程。

DevOps与应用生命周期管理

通过DevOps与应用生命周期管理，企业可以快速构建代码仓库、部署环境（开发/UAT/生产）、交付流水线（Pipeline），以及运维监控组件，使企业更关注于应用开发本身，缩短产品交付周期。

虽然上面这样的架构在传统IT基础设施上也可以实现，但是与云平台结合的DevOps可以给企业带来更大的收益：

- 更易于自动化

自动化是基础设施管理的一个重要方面。利用云实现流程自动化有助于提高自动化速度，使流程更加可靠、无错误、健壮和高效，最终缩短上市时间。通过云实现IT现代化，实现快速数字化转型。云服务商通常会提供各种服

务（工具），使企业能够管理基础设施并使其现代化。自动化过程包括基础设施配置、构建、运行测试用例、监控报告等等。

・更方便的服务资源复制和备份

通过DevOps，服务资源的复制与备份过程可以自动化，比如，如果需要临时分离环境（创建生产环境的副本）和负载测试，以测量应用程序的稳定性。利用领先的云提供商提供的各种工具，可以轻松地自动执行环境的复制和备份。

・更有效的监控

云服务商通常都会提供一站式的监控服务，比如当任何基础设施行为异常时发出警报。DevOps可以触发自定义警报和各种监视警报，使企业能够更有效地利用资源。

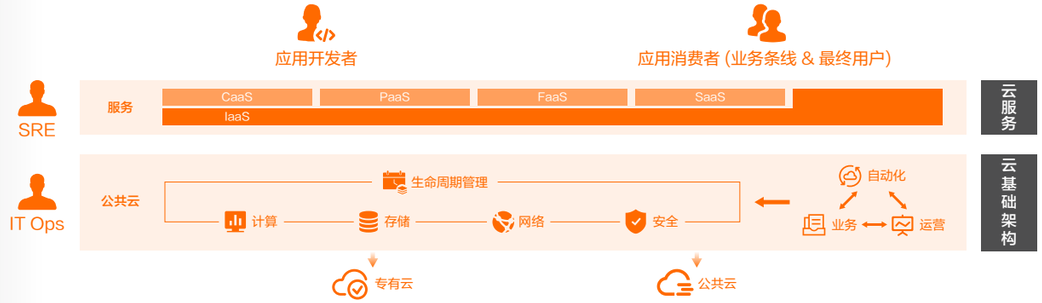
・更快速的开发迭代

云服务商可以帮助企业快速部署环境，但是在没有DevOps的情况下定制它是一个挑战。DevOps专注于通过构建自定义逻辑和编写功能来使用最新工具解决基础设施问题。

综上，在这个数字化和技术不断发展的环境中，云和DevOps很多时候是紧密结合在一起并携手使用的。这种结合不仅增强了软件产品的性能，并使整个基础设施自动化，从而以更快的速度不断改进产品。

资源编排管理

资源编排管理是云数据中心区别于传统数据中心的重要能力之一。资源编排是一种简单易用的云计算资源自动化部署服务。用户可以通过使用Json/Yaml格式的模版描述多个云计算资源的配置、依赖关系等，并自动完成所有云资源在多个不同地域以及多个账户中的部署和配置，实现基础设施即代码（Infrastructure as Code），如下图所示。



与传统的基础架构相比，云服务商提供的资源编排的有如下优势：

・基础设施即代码

基础设施即代码（Infrastructure as Code）。通过资源编排可以帮助企业最快速地实践DevOps中关于IaC的理念，将准备资源所需要做的工作都通过代码来完成。

・可重复部署

无论企业需要部署的环境是开发，测试还是生产环境，都可以使用同一套模板进行创建。指定不同的参数可以满足环境的差异化。如果企业需要进行多地域的部署，使用同一套模板可以进行重复的部署，从而提高部署多地域的效率。

・标准化部署

在实践中，不同环境的细微差异往往带来非常复杂的管理成本，延长了问题诊断的时间，从而影响了业务的正常运转。通过资源编排重复部署，可以将部署环境标准化，减少不同环境的差异，将环境的配置沉淀到模板中。再通过类似代码的严格管理流程，从而保证部署的标准性。

3 平台视角的上云价值

平台视角的上云的价值可以从管理，运营，执行三个层面来得到体现。

首先，对管理层面来说，即从管理者的角度去看，云平台的建设将会给企业的管理价值和管理成本两个方面带来巨大收益。总的来说，通过云技术的发展，必将带来管理价值的最大化和管理成本最小化。具体来讲：第一，管理价值最大化：通过云技术，以信息系统集中应用为目标，合理处理信息化各种资源的集中和分布态势，促进管理价值的最大化；第二，管理成本最小化：通过云技术，合理处理业务对信息化资源的需求，形成弹性和可扩展的业务支撑能力，推进企业信息化资源的精细化管理。

其次，对运营层面来说，即从后期运营、经营相关的角度去看，云平台的建设必将为企业带来如下两点价值：第一，业务高效协同：借助云技术， 实现业务与业务、业务与生产的信息流畅传输，促进纵横向的高效协同；第二，业务高效处理：借助云技术高效计算、海量数据处理能力，实现企业对各类业务的高效处理，满足业务信息及时处理、及时发布的需求。

最后，对执行层面来说，云平台的建设给企业的价值体现在如下方面：第一，生产收益最大化：借助云技术，结合大数据分析技术，实现对海量生产数据的实时感知、实时采集、挖掘分析、实时优化，使生产装置实现最大收益；第二，业务系统快速部署：借助云技术，提供标准、快速交付的IT平台，实现业务应用系统的快速部署，满足业务系统对IT平台的灵活性、可伸缩性要求。

4 安全视角

1 云下数据中心所面临的挑战

随着IT技术的不断发展，以及业务与IT日益密切的联系，云下数据中心面临的安全挑战与日俱增，并正在经历着巨大的转变。

1、管理复杂度提升

企业发展的初期，仅需要几台服务器和有限的机房环境就能满足基本的业务需求。随着企业业务的迅速发展，为了满足上层应用的敏捷性与可持续发展，IT基础架构变得日益复杂，具有多层次、相互依存、分布式、高度网络化等特性，产生的问题层出不穷，影响到上层应用的安全稳定运行。企业要想管理好自己的IT基础架构，保证其安全可靠，就必须引入先进的工具和管理流程，管理复杂度的提升给企业带来巨大的压力。

2、严峻的网络安全威胁

在IT技术迅速发展的同时，网络安全的威胁也与日俱增。从阿里云安全中心2019 年拦截的威胁数据我们看到，过去一年整体安全态势有以下四方面：

- 挖矿病毒依然以33.4% 的高占比成为2019 年的主要安全威胁；
- 2019 年日均发生2000 余次DDoS 攻击，与2018 年基本持平；
- 网络攻击中暴力破解依然是“低成本、高收益“的主流攻击手段；
- 电商等行业将面临黑灰产链条更加完整和专业的Web 攻击。

面对如此严峻的网络安全威胁形势，企业需要不断更新升级自己的安全防护技术和管理手段，才能确保在和黑客们的持续斗争当中立于不败之地。

但与此同时我们也看到，企业对网络安全的认识普遍不足，相关技术、手段和安全人才往往跟不上，这也是导致网络安全威胁日益严峻的重要原因之一。例如，挖矿病毒已经取代勒索病毒成为黑产获利的主要手段，由于挖矿病毒所造成的危害并不像勒索软件那么直接，所以企业往往忽视或者不重视对挖矿病毒的防御，而实际上，挖矿病毒窃取企业计算资源所造成的破坏不可小觑。

另一个导致网络安全威胁日益严峻的重要原因是企业对网络安全的不重视。很多时候，网络安全事件并不是由新的威胁触发，而是之前的漏洞没有被消除。例如，三年前爆发的WannaCry勒索病毒目前依然是给企业带来危害最大的病毒，这说明很多企业没有及时修复该漏洞，对网络安全不重视。

3、业务连续性与灾难恢复

日益提升与复杂的业务需求，对IT基础架构的依赖性和优质服务需求等都要求业务的连续性和灾难恢复。数据中心的正常运行时间和服务的可用性对于企业的业务的成功与否至关重要。以制造业为例，数据中心承载着很多非常重要的应用，包括MES系统，IoT系统，人力与财务系统等。IT基础架构是作为整个系统的重要载体，如果IT基础架构不可靠的话，工厂要停产，财务、客户的订单就都会出现问题。

4、缺乏技能娴熟的IT人才

当前，中国的移动互联网逐步成熟，人工智能、大数据和物联网技术迅猛发展，这一切都使得企业对于中高端IT技术人才需求越来越旺盛。然而与此相矛盾的是，招聘一名技术娴熟的IT专业人员平均要6到12个月，更多的企业难以在短期内招到满足IT技术发展需求的专业人才。IT人才的匮乏使得企业数据中心的安全运营面临重要挑战。

2 安全视角的上云价值

云带来的安全价值是从云本身的规模化优势而来的，它能让安全从偏安一隅的隔离模式，变成集中管控、迅速下发的神经中枢模式，从而增强企业威胁情报模型、更好地抵御攻击，以及加快安全事件的响应。如果企业能用好云，能够改变企业信息安全的结果，让放在云上的业务系统，比云下更安全。

1、技术优势

云下的安全防护技术通常已经过时，它完成了创建时要做的一切，但是它的增长空间不灵活，因此无法适应当前网络风险水平。但是，即使企业确实想使旧的基础设施保持技术上的最新状态，要完成的检查和升级也要经历很多的挑战，因为这方面对企业而言投入巨大。结果，大多数企业的安全防护技术趋于落后。

与此相反的是，公共云解决方案不断更新，并上线最新的安全功能。大型的云服务商的网络安全团队可以确保最新的安全防护技术可以保障企业数据的安全。

2、资源优势

由于具有规模效应，云服务供应商所具有的IT资源和优势是企业所无法比拟的，这使得云服务商可以轻松解决一些企业自身难以解决的安全问题。例如，云服务供应商可以利用自己庞大的机房和服务器等资源为用户提供低成本容灾构建方案，而企业如果自建容灾数据中心，其成本投入通常是巨大的。DDos攻击是网络安全防御中常见的攻击手段，云服务商通常拥有巨大的带宽，可以帮助企业抵御DDos攻击对带宽的消耗，而普通企业通常不可能购买如此巨大的网络带宽。

3、人才优势

上文提到了企业通常缺乏技能娴熟的IT人才。与之不同的是，云服务商通常是IT人才的聚集地，在对IT人的吸引力上和招聘渠道上也具有无可比拟的优势。这使得云服务商拥有足够多优秀的IT人才来确保云的稳定运行，并及时研发出预防和抵御新型安全攻击的技术手段。

4、经验优势

云服务商所面临的安全威胁在数量和严重程度上都远高于企业。在长期与各种病毒和网络攻击的博弈过程中，云服务商也积累了丰富的经验，这些宝贵的经验使得云服务商通常能在第一时间将漏洞封堵住，甚至具有防患于未然的能力。

而对于普通企业来说，经验的不足和知识积累与管理的不到位使得他们对于安全问题的处理能力远不如云服务商经验丰富。

5、加速合规与等保优势

网安法第二十一条规定：国家实行网络安全等级保护制度，等保安全制度适用于境内所有信息系统。企业需按照网络安全等级保护制度履行安全保护义务，按照等保安全制度申报完成网络安全等级评定，根据各级保护制度的要求整改、建设信息系统，是企业应履行的义务，同时可发现自身系统的安全隐患及不足，并及时整改，进而可提高企业整体的行业竞争力。

云服务商通常提供一站式等保安全解决方案，助力企业更高效、专业地完成等保认证。

5 运维视角

1 IT运维的内容和目标

IT运维负责处理系统运行故障，维护服务目录和应对服务请求，对系统进行计划和紧急的变更，其目的是保障IT系统稳定运行，满足业务发展的需求。IT运维的内容大致可分为服务管理和资源管理两部分：

服务管理

面向业务部门，其核心目标是保障服务体验，并有效支撑业务提升，包括用户访问体验，业务交易监控，运维服务水平与效率等。

随着企业的应用系统逐步迁移到云环境中，运维组织的管理模式逐步从传统的IT运维向云运维转型，从IT软硬件系统服务转向系统稳定性保障、业务赋能，全面提升了IT的业务支撑能力。

在IT运维转型过程中，必须考虑深化应用ITSM，结合云服务的特点，对现有的IT运维流程进行优化提升，对现有的工具进行升级，以确保服务继续满足预期。同时，在确定SLA关键服务等级协议时，要充分考虑角色与职责、业务覆盖范围、绩效衡量、安全标准、数据所有权及管理等内容。

资源管理

面向IT基础设施，其核心目标是IT基础设施的高可用、性能、自动化，包括配置管理、监控和巡检、操作自动化、操作审计等。

2 IT 运维的现状与挑战

1、混合云下的应用与IT基础架构松耦合

国内真正意义上集中式、大规模的数据中心（IDC），源于2000年开始的数据集中工程，已从银行业延伸到证券、保险、电力、电信等行业。经过十多年的发展，已从建设分散雏形发展到集中数据中心，并逐步走向多活和混合云环境阶段。

分散雏形阶段

在此阶段，IT运维缺乏整体规划，分割管理，在摸索中建设：

- 数据中心的建设往往就地取材，没有规划，专业性不强；
- IT组织以建设任务为导向，常常随IT项目建设边使用边改造；
- 运维专业化程度处于较低的水平，缺乏专门的管理目标和管理手段。

集中数据中心阶段

在此阶段，有了整体的规划，运维朝着专业化方向发展：

- 数据集中存储、处理，应用和业务集中化；
- 建设依托有效规划，更加现代化，大规模数据中心引入“两地三中心”模式；
- 引入运维流程框架，通过流程实现跨部门的运维任务在各个专业部门之间的贯穿和协同。

多活和混合云环境阶段

在多活和混合云环境下，应用与基础设施开始松耦合，资源服务化：

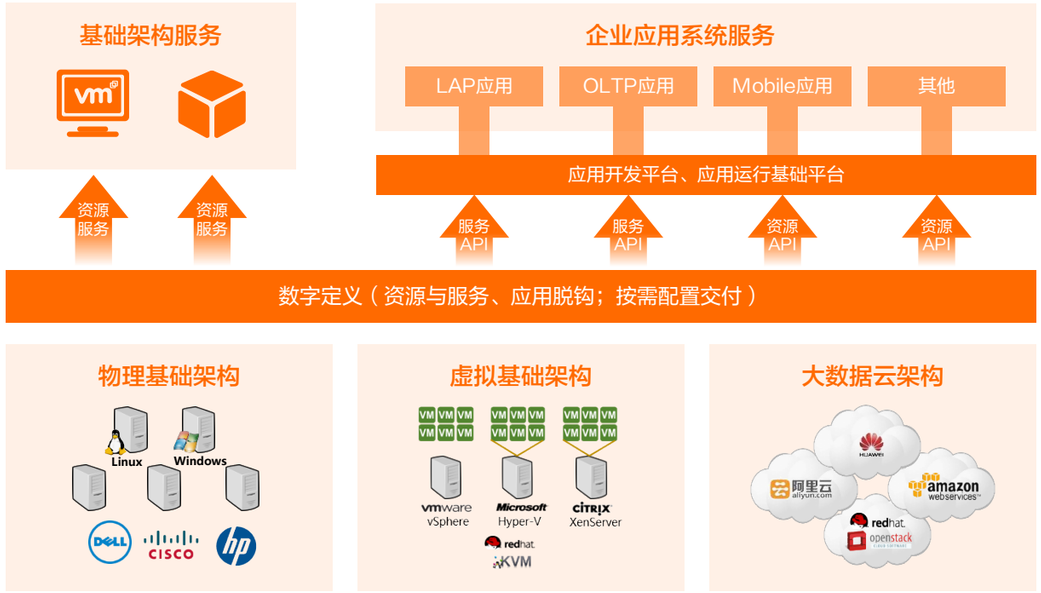
- 信息部门在逻辑上成为一个整体，要求运维组织不再按照专业领域进行部门划分，而是按照物理/逻辑进行部门设置划分；
- 信息部门“高可用性”有了基础级保障，运行维护工作核心开始围绕服务和资源的合理提供、监管和调度。

2、IDC运维复杂度提升

随着云计算的发展，IDC也从大集中逐步发展为区域集中式，再到分布式云IDC。分布式云IDC在计算能力、容灾能力、可扩展等能力上均有优异的表现，但其复杂的架构也给IT运营提出了新的挑战。解决IDC运维的复杂性，提升运维的敏捷性是关键。

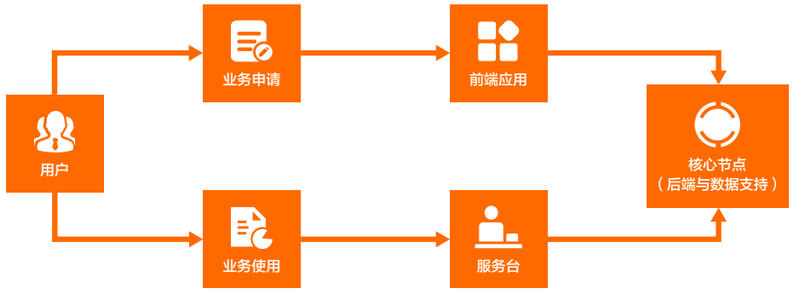
3、混合云架构下的IT系统运维

混合云兼有公共云和私有云的优势，正在被越来越多的企业所采用。信息化架构的不断演变，使得运维管理要兼容多种基础架构（传统物理基础架构，虚拟基础架构，云架构等），通过数字定义的方式向上层应用提供IT基础架构资源服务，并对封装后的信息化基础架构服务和业务应用服务进行保障，驱动组织向主动优化、服务导向的运维模式提升。



4、服务导向

对用户而言，只关注所提出的需求是否在可接受时间内得到处理，为达到这个目标，需要对包括人员、技术和工具在内的一整套能力进行组织和规划，以确保向用户交付满意的服务。对于IT运维而言，满足用户服务性的要求需要关注服务提供的时效性，用户的满意度，以及问题的解决率。



3 运维视角的上云价值

云上运维所带来的价值是驱动传统的人工运维逐步转向自动化运维。传统的企业数据中心运维包含许多重复的运维任务，事件驱动的自动化场景，定时和批量的运维场景，跨地域的运维场景，需要审批的特殊场景等。通过云上的自动化运维，企业可以通过模板来定义执行任务、执行顺序、执行输入和输出，然后通过执行模板来完成任务的自动化运行，实现运维即代码，大大提升运维效率。

云上的自动化运维给企业带来的价值包括：

降低IT成本

自动化运维可以降低人工成本，提升运维效率，减少故障带来的经济损失，从而降低企业IT成本。

提高运维生产力

自动化运维减少了人工操作，不仅可以提高产出，还可以将运维人员从复杂的传统运维工作中解放出来，将其知识和技能应用于更有价值的工作和任务上。此外，通过减少周转时间，每天可处理工作量也提高了。

高可用

IT基础设施的故障可能会使企业蒙受巨额损失，无论是金钱上，还是声誉上。运维优先要保障的便是高可用，这也是自动化运维的一大目标。例如通过自动化备份和恢复机制，全天候系统监控和远程通信，以大幅降低网络故障时间；或是通过备份的快速回滚，减少故障带来的损失。

更可靠

运维常常包括一些重复的工作，这也就是为什么它容易出错。当人为因素从这个过程中消除时，那些人为错误也自然消失了，这对于具有多个操作系统的大型网络尤其有用。自动化运维可以明显提高可靠性，减轻运维人员繁琐的手动任务。

性能优化

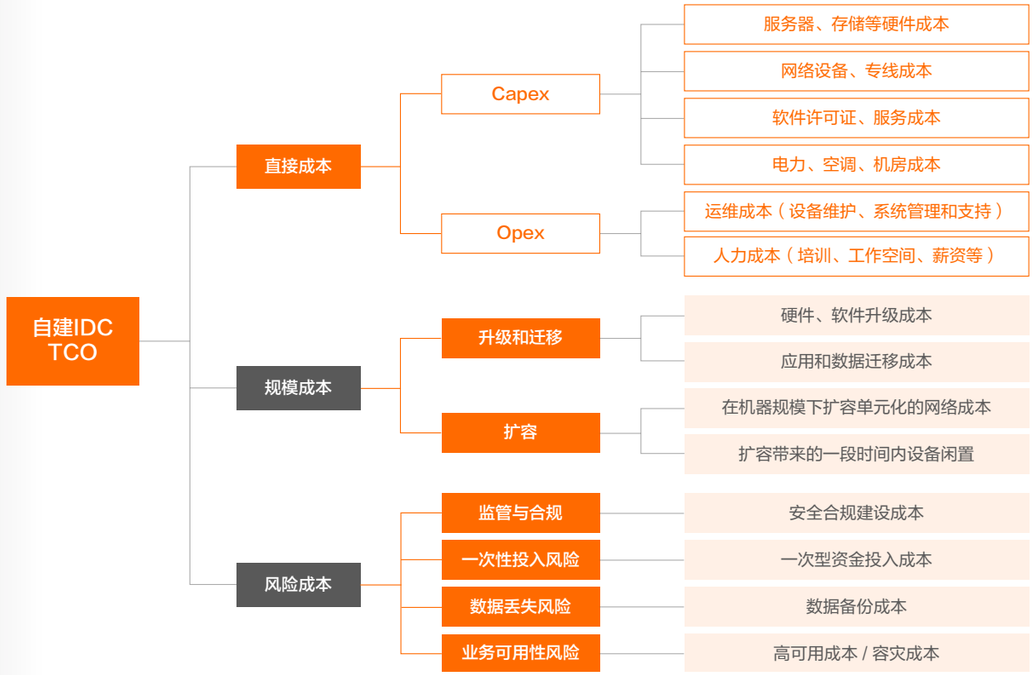
运维专家面临的另一个问题是，让执行任务和工作流程变得更快、更高效、具备更高工作负载。传统运维方式想要满足这些需求是很困难的，而自动化运维工具则可以填补此类需求，在无需雇佣更多员工的情况下，最大限度的提高性能。

6 IT 成本分析

1 TCO分析—自建IDC

传统自建IDC的TCO首先要考虑直接成本，其中资本性支出Capex主要由硬件成本、网络成本、软件和服务成本、基础设施成本组成，运营费用Opex主要由人力成本和运维成本组成。除了这些显性成本，还需要考虑规模

成本和风险成本等隐性成本，比如升级、迁移、扩容等与IT规模相关的活动引发的额外成本，再比如为了满足监管与合规要求，防止数据丢失，提高系统可用性同样需要大量成本投入。最后，自建IDC的一次性资金投入，也是企业需要关注的风险因素。各部分的成本进一步细分如下图：



2 TCO 分析—云数据中心

与于传统IDC不同，云上数据中心的成本模型包括云运行成本和一次性安装成本，而最终目标结果—云上数据中心的的总成本（TCO）为运行成本和一次性安装成本的加和。

其中，运行成本等于云基础设施成本加上云后的新增使用成本，每部分的详细含义如下：

云基础设施成本

- 服务器/容器
- 存储
- 网络
- 数据库
- 中间件
- 许可证

新增使用成本

- 数据传输
- 额外链接
- 监控收费
- 云上应用开发
- 企业支撑

成本模型中的另一部分——次性安装成本等于建设成本和迁移成本的加和，每部分的详细含义如下：

建设成本

- 公共云网络连接
- 云安全工具
- 云监控和管理工具
- 云迁移工具
- 实施成本

迁移成本

- 云管理组织的架构的建立
- 应用迁移
- 运营模式变更
- 人才和技能提升
- 实现集中预算和内部核算机制

3 成本视角的上云价值

前文所述，传统IDC和云上数据中心的成本核算具有不同的计算方式，但两者的区别不仅仅在于核算的方式。在实践中，企业传统IDC有诸多成本方面的挑战：

- 基础设施资源的消耗是波动的、周期性、或者完全没有规律的；

- 因为上面的原因，通常基础设施采购量是实际需求的2-3倍，需要数周/数月的时间进行采购。 结果就是，基础设施的能力在大多数情况下都未得到充分利用；
- 较高的固定成本，导致总成本（TCO）既包含资本支出（CAPEX），又包含运营支出(OPEX)；
- 资源的提供需要很长的时间，必须由特定的团队完成，造成额外的时间和人力成本；
- 基础设施资源的采购是一个耗时的过程，阻碍了业务快速创新，增加了创新成本。

相对的，云上数据中心从以下几个方面应对挑战：

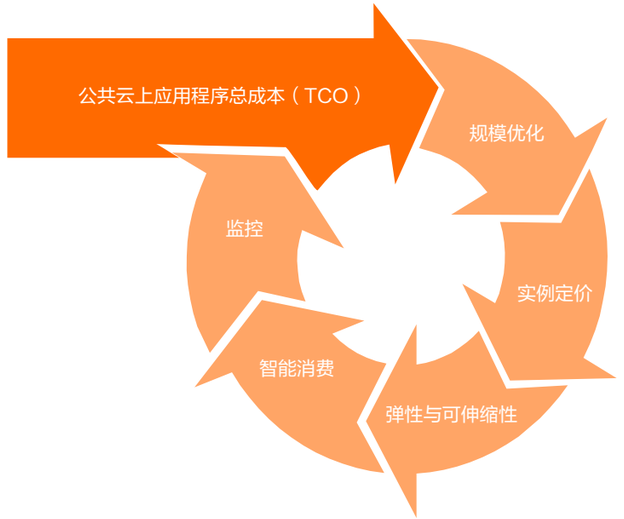
- 无需固定成本。企业只需要根据需求支付必要的基础设施成本；
- 按使用量付费。企业根据基础设施资源使用情况支付运营费用；
- 更快的创新。使用公共云服务商提供的快速迭代的创新功能，降低创新成本；
- 即时资源调配。云基础设施可以在数秒/分钟内配置完毕，提高了业务相应速度。

综上，企业通过上云，改变了成本核算的模式（从CAPEX转化为OPEX），避免了资源的浪费，同时加快了业务创新。

4 云上总体成本持续优化

对于企业而言，可以从以下几方面进行持续性的云上成本优化。

- 实例规模优化：以最低的成本合理确定实例类型的大小，以满足性能和工作负载要求；
- 实例定价模式优化：利用实例定价模型的组合来降低实例计算单位成本——预留实例与按需计算相结合。预留实例定价可以潜在地节省成本;然而，大多数客户不希望被1年或3年的合同束缚住。



- 弹性与可伸缩性：使用自动伸缩功能来根据需求和使用情况(例如业务波峰/波谷工作量)对实例进行扩容或伸缩操作；
- 智能消费： 识别并关闭未使用的实例，例如周末不运行的开发/测试实例；
- 监控：设置指标以持续监控和衡量利用率，以寻求成本优化机会。由于在云上启动实例非常容易，因此，为了限制“云蔓延”（一般指云实例或云服务的不受控制的扩散），清晰地看到服务的实际消费变得比以往任何时候都更加重要。

最后，为了充分优化云计算的使用成本，企业需要对应用程序的成本和收益进行调整并定期检查。必要的时候，应用程序需要重构以在技术层面上充分利用新的功能，来达到增效降本的目的。

一系列针对组织内部的策略及行动，帮助上云负责人在内部形成上云旅程准确认知

3 企业全面上云成功路径与实践

全面上云的成功框架

全面上云的成功框架帮助企业的上云负责人，清晰化上云的推进和决策流程，对上云价值达成共识，实现内部协调、业务有效、组织灵活、进程持续并产生可持续的业务价值。这一框架包括8个主要组成部分，企业可针对自身情况进行周期上的灵活调整，但需要指出的是，这8个阶段的重要性并无明显差异。

1 全面上云战略的必要性认知

云为每一家企业所提供的要素，包括灵活使用、容易扩展、高可用性和极致算力等等，都是面对数字经济中企业所需要的，同时，云也能够确保符合企业的信息安全策略，特别是数据保护、审计功能、访问控制、日志记录、监控以及网络和终端保护。

因此，在确定了企业上云评估流程和定制化的云成功框架之后，在规范监控、事件响应和审计的流程的支持下，企业应当尽快将各种工作负载交由最合适的云来处理，这样可以提高工作效率，并把更多精力放在技术创新上。

企业上云的主要流程往往从基础设施云化开始，完成服务器、存储、网络等硬件设备的云化，逐渐推进到业务

系统、管理系统、工具软件，实现业务应用上云，产品研发上云常被放置在第三阶段，无论是硬件产品还是软件产品，研发能力和流程，智能服务，都实现上云，第四阶段是制造和运营能力上云，包括生产设备、设计流程、资料资源、协同办公、企业运营等方面的上云。

企业上云（包括互联网企业）战略可以被分为“尝试上云-核心上云-全面上云”三个上云阶段，从部分应用、测试业务尝试上云，到数据库、关键业务系统等核心上云，到包括“前、中、后端”的基础设施、业务应用、产品研发、制造和运营能力的全面上云，但对于相当多企业来说，上云是否要到“全面上云”的阶段仍然存在一定的讨论，这一问题可以从两个层面来讨论：

1、技术应用层面：云计算无疑将改变信息技术（IT）产业，也将深刻改变人们工作和公司经营的方式。特别是对企业来说，全面上云是一个技术代际迭代的背景下技术驱动的选择，驱动企业从基础设施上云，到大数据上云，再到云上中台和云上智能，“新技术”的趋势下，全面上云不只是单纯让企业“上云”，更是让企业在云上创造更多新的场景需求。

同时，随着越来越多的前沿技术（比如人工智能）在云上以服务化的方式通过API接口提供（尤其是技术的原子能力），不在云上的企业获得技术赋能实现技术红利的难度将持续加大；

2、IT管理层面：准确来讲，这一层面的关键是“全站”，即完整的从传统IDC迁移到云上，如果停留在全面上云阶段之前，这意味着IT团队要面临两套IT系统之间的鸿沟，不仅被迫维护两套IT系统，造成IT团队与IT能力的割裂，而且因为业务分别部署在云上/传统IT，难以实现多元业务互联互通，业务协同。

2 企业 CEO 的支持

虽然在上云规划初期，CEO往往处于“上云无关者”的周期内，但取得CEO的支持仍然至关重要。企业中驱

动上云的负责人，可以从外部市场环境驱动、竞争对手驱动、行业发展方向驱动、业务内部战略驱动等层面，为CEO呈现上云战略融入业务中所实现的价值，以及如何与业务形成一致性目标，采用方法与业务和组织就绪性保持一致。以下是取得CEO支持时建议使用的驱动要素：

1、重要的IT基础设施选择：包括传统IDC退出、改变IT成本支出模式、对IT服务水平提出更高要求、改善业务发展中的峰值承载能力、响应上一级管理者（如子公司向集团）的要求，这些因素会造成显著的成本量级、支出模式、业务连续性及业务决策影响，是取得CEO支持时的常见且直接的因素；

2、上云的短期获利：弹性缩放应对峰值挑战、在短期内获得新的技术能力、改善客户体验和服务的水平、减缓高速增长业务的IT需求增长、提高IT团队响应速度；

3、长期的云上获益：获得云上技术红利、为出海（全球化）做好准备、长期提高业务灵活性、构建业务部门IT自主化能力、为新产品和服务做好准备；

4、云计算成为数字经济创新平台：云正在从单纯的基础设施走向“数字底座+数字操作系统”的融合，即除了作为数字经济底座（数字经济基础设施）的价值，借助云端一体化发展，云已经具备支撑企业快速业务开发及上线的能力，从而促进企业业务创新。

3 全面上云优先战略

企业全面上云优先战略的制定目标，关键是从技术愿景、业务需求和IT战略三个层面，找到与全面上云之间的结合点和价值点，并在这三个层面产生不同的投资回报，同时考虑全面上云优先战略对企业财务情况和财务模型的影响。

全面上云优先战略的制定中，需要避免三个误区：

1、上云在任何情况下价格都是最优：更高的经济性是上云的主要驱动因素，在制定全面上云优先战略时，CFO可能会要求企业IT在任何情况下，上云都能获得最优的价格，但这并非如此，尤其是在上云迁移转换和应用初期；

2、全面上云应当一切入云、一批入云：全面上云并非一次全部上云，某些业务驱动因素可能会导致选择混合的、分次序的上云解决方案，全面上云是一个企业借助上云实现核心技术的互联网化、应用的数据化和智能化的旅程；

3、忽略数字资产规划： 数字资产包括虚拟机、容器、应用程序、算法和数据等，上云是从物理设备到（虚拟）服务的转变，上云的迁移策略制定过程中，许多企业容易忽略数字（IT）资产规划的建立、盘点和计量，而是仅监控流程，由于云服务的计费分账机制建立仍然需要一定周期，这意味着IT团队将很难统计数字资产与业务收效的映射关系，IT团队应当使用数字资产将业务成果映射到发布计划和技术工作。

制定全面上云优先战略的主要组成成员及架构应当包括：

1、企业CFO：CFO经常是CIO的管理者，即向下管理CIO，向上将IT作为自己工作的一部分向上对CEO负责，肩负这一角色的CFO负担着两个责任：第一，企业财务、投（融）资的第一责任人；第二，将IT作为重要的投资之一，纳入严格的成本管理中。

2、企业COO：全面上云必然对企业运营产生极大地影响，在将业务逐渐云化的过程中，COO将决定如何利用云深度改造和优化现有业务，从而确保在制定业务和技术战略时，将云所供给的资源、能力作为战略发展的参考。此外，COO一般会要求业务项目改造后有明确的成本效益和运营效果要求。

3、企业CIO：CIO需要说服企业管理层接受基于云计算可以重构垂直行业的业务流程和商业模式的巨大潜力，因此CIO必须具备能将复杂的事情简单化，能一句话说清楚云计算给企业带来的新商业模式和结构重组价值。

4、上云办公室：CFO、COO和CIO从财务管理、业务运营和上云规划三个方面作为决策者制定全面上云优先战略，但仍然应当建立混合三个团队的上云办公室，以推进企业全面上云的策略细节、规划步骤和落地执行。此外，上云办公室内应当引入业务团队的负责人或高级别接口人，该角色一般不建议由COO团队代理。

4 全面上云的 TCO 分析

全面上云本质上不是一个可以通过完全量化的指标来衡量的工作，但通过以下三个途径，CIO与CFO之间可以就全面上云的TCO进行融合了准确量化和可信判断的分析。

1、使用云服务商所提供的TCO计算器，如阿里云的TCO计算器（https://tco.aliyun.com/），从服务器、存储、交换机、带宽、人工等方面对现有服务器集群进行TCO分析，并融合折旧年限和软件成本、年化资金成本、容灾和迁移扩容成本等影响因素；

2、为主要IT支出设计3-5年的成本支出路线图：基于第一性原则，拆分IT支出中占比最大的主要成本来源，将其与云上产品进行一一对应，结合其支出情况、折旧年限、规模复杂度等影响因素，设计可供对比的长期成本支出路线图，以确定核心支出是否能够受益于云；

3、在进行全面上云的TCO分析时，如果可以说服CFO和COO参与到TCO和ROI评估中，应当将新的财务计划与企业发展战略联合，充分考虑到云计算按需使用、按需付费、支出灵活的特点（特别是云服务支出入费用，企业级客户通过长约获得优惠，比资产平摊费更低），以及从Capex到Opex的转换等方面的优势；

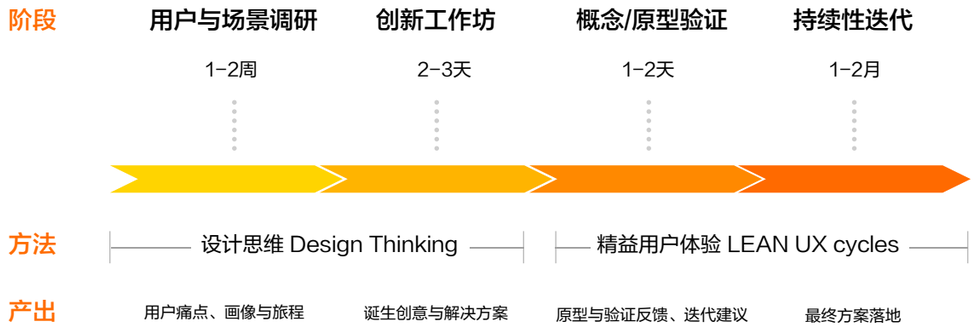
4、需要指出的是，并非所有的云服务都能带来CFO们所期望的弹性和按使用计费的特性，比如SaaS则一般

是按用户数来收费，并且需要签署长期服务协议，很难达成随用随停的目的，通过财务的手段实施上云战略层面的操作，一个非常重要的工作是具备数据分析能力，将来自上云的原始数据碎片整合成有效的数据信息，融入公司战略中。

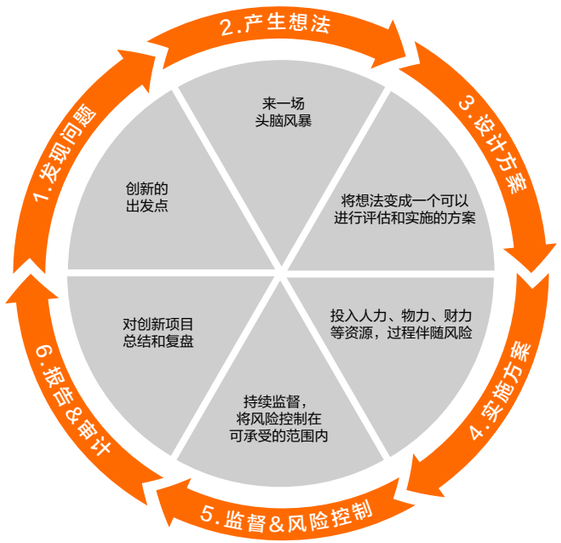
5 开展上云工作坊（Workshop）

数字化转型的事情，大部分都是组织内沟通与共识的事情，开展上云工作坊的主要目的是通过透明的沟通方式，衔接不同组织之间的知识与行动，进而达成组织共识和共创行动计划。

以下流程可供参考：



上云工作坊的创新旅程　来源：ACRC分析



上云工作坊的共创流程　来源：ACRC分析

6 选择卓越的云合作伙伴

全面上云战略应当选择卓越的云合作伙伴，以此尽可能获得来自于合作伙伴在产品、技术、能力和经验上的支持，针对企业在云采用中我们提供了以下参考标准：

1、云服务商具有较强的服务能力：在数字经济时代，企业正在推动新的业务战略，包括全球服务、进入细分市场、从线上到线下，这意味着云服务商必须要地域覆盖、服务深度、线上线下融合等方面提供支持。此外，分布式计算、新一代云数据中心、服务的弹性伸缩等能力决定了云服务商能否服务好企业；

2、业务运行情况和规划：稳定的业绩增长和财务运行状况是最为重要的，云服务商必须要处于良好的财务状况，具有长期顺利运营所需的充足资本。同时，云服务商的管理结构、风险管理策略以及长期的业务规划应当是准确和被长期验证的；

3、支持能力与服务水平：服务水平协议（SLA）是其中的关键，保证云服务商能提供符合要求的服务并给出清晰地性能和能力报告（最好由第三方认证）。需要注意的是，云服务商应当具有足够的控制权，来跟踪和监视提供给客户的服务及对其系统所做的任何更改；其次，能够监视所用资源及其费用，避免产生超出预期之外的费用，并尽可能提供灵活的计费与记账（分账）方式，帮助企业清晰化内部费用分配；

4、持续不断的产品技术演进：云计算仍然处于高速发展期，当前企业所获得的云上的产品、技术、解决方案仍然有极大地演进和升级空间，因此云服务商的迭代能力决定了其是否能够长期为企业提供有效的新技术、新能力和新成本价值的支撑；

5、长期的投资计划：无论是数据中心还是云操作系统、服务器、芯片、网络等重大核心技术研发，云计算必然是一项需要长期投资支撑其发展的业务，尤其是在云正在向下定义数据中心硬件（尤其是芯片）的趋势下，长期的投资计划不仅仅意味着业务持续发展，更在于云服务商的产品技术能力和持续成本优化可能；

6、安全合规及相关资质：符合政府、行业的安全合规和相关的国内及国际性资质。

7 组织变革与目标聚焦

上云战略不止是制定能够帮助企业上云和数字化转型的战略，更是对IT架构的重新调整，不仅包括产品、技术、服务、财务与审计的调整，也包括组织和文化的变革。IT团队及紧密合作的业务团队必须一同勇于接受文化方面的改变，以符合企业的制胜战略要求以及组织结构特点。

需要指出的是，仅仅拿出理想的战略和组织结构并不足够，必须培育企业文化来配合，如果坚持采用传统的工作和思维方式，就会在前进的道路上形成阻碍。

所有级别和部门都要重塑文化，帮助个人、团队和组织实现发展，全体IT领导需要参加定制化的学习，学习如何让文化行为与组织变革保持一致，当然，其中最重要的是由IT领导树立榜样，以身作则为起始。

企业应当准备好实施全新的运营模型，旨在更新和改进我们的IT解决方案和服务交付的方法，这套运营模型的基本要素如下：

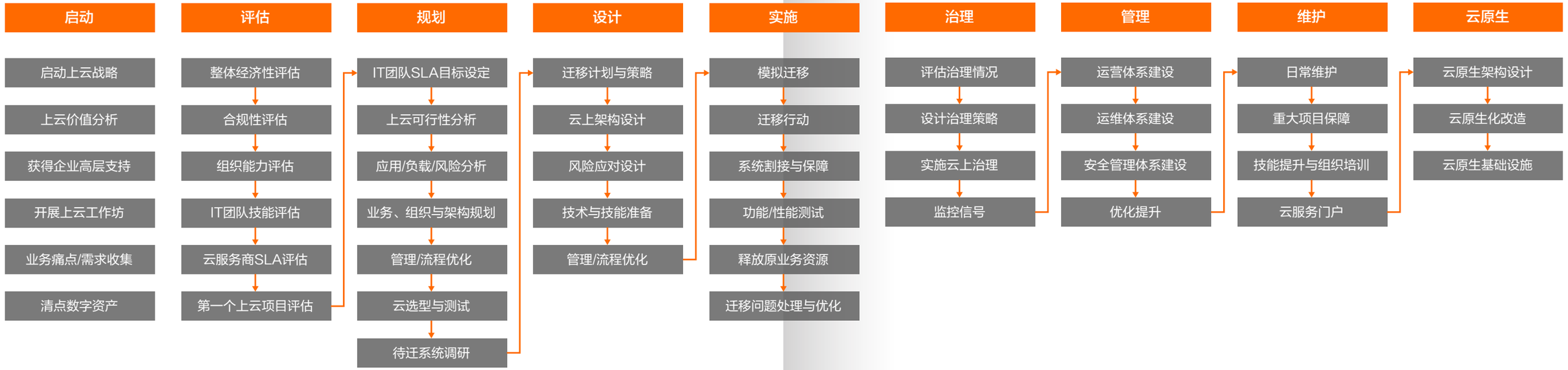
– 矩阵式组织，有垂直和水平解决方案栈，专业知识有侧重且可重复利用；

– 完整价值流，可以强化业务知识和业务协作，优化业务解决方案、数据和商业价值的实现方式，并将各部分关联起来；

– 支持运营模型和交付服务持续改进和整合；

– 交互模型，说明如何完成工作、参与者之间的交接以及每个参与者的角色和职责；

8 循序渐进的上云路线图（可供参考的流程图）



企业全面上云是一个复杂、长期且个性化的旅程，从启动全面上云战略开始，就充满着不确定性，在前三章阐述了启动全面上云战略、上云价值分析和全面上云成功框架之后，为了帮助企业上云负责人更好的理解以上内容，并将本白皮书后续内容更好的应用于实践，我们在此提供可供参考的上云路线图，以供对白皮书内容更好的理解和使用。

筛选出常见的传统企业全面上云障碍，并给出来自实践的建议

4 企业全面上云成功路径与实践

破除传统企业全面上云的障碍

在云计算出现之前，虽然传统IT架构模块之间的耦合度较高导致可扩展性很差，并存在大量的因为供应商、架构设计、产品特性所导致的企业IT孤岛，但信息化建设仍然在企业发展中起到了至关重要的推动作用，并且，由于许多企业的信息化历程往往倡导10~20年，这意味着无论从技术架构、系统构建、成本与预算管理，还是组织经验、管理模式、知识技能等方面，已经形成了一套完整而坚固的体系。

客观来说，传统企业全面上云必然会面临阻碍，这其中最常见的阻碍包括云的安全性、成本问题、运维管理等方面，但对于拥有复杂庞大信息化系统的传统企业来说，上述问题往往都只是点上的问题，为了能够更加系统的破除传统企业全面上云的障碍，则需要全面的关注以下六个问题。

1 整体评估上云的经济性

云计算既是数字经济的基础设施，提供算力、存储、网络等资源，更重要的是提供了可靠易用的云平台、全局智能的大数据、云端一体的智联网和随时随地的移动协同，是以高经济性提供新技术的平台。

与此同时，随着数字经济转型进入深水期，越来越多企业将会选择全面上云，云计算的支出正在成为每一个公司的标配，使用云计算的能力，是企业基础能力的重要组成部分和指标。同时，在同一套云平台下建立起企业间的数据、技术和产品连接，简化系统架构和业务接口的复杂性，要远比在物理IDC及封闭技术体系上更加简单迅速。这意味着，在互联网+传统产业的过程中，为了尽快与客户的业务系统、产品平台和技术体系接轨，企业必须尽快上云。

业界的共识是云计算架构在经济学上更加经济。云计算是一种大规模分布式计算的模式，其推动力来自规模化所带来的经济性。在这种模式下，一些抽象的、虚拟化的、可动态扩展和被管理的计算能力、存储、平台和服务汇聚成资源池，通过互联网按需交付给外部用户。

在用户侧，对于云上的企业来说，第一，由于云服务商的边际成本的降低，可以以更加经济的方式获得基础设施；第二，其个性化的每项增值业务，只要进行一个较低的边际投入，就可以展开，无须从头开发基础设施、平台和软件；第三，由于新技术的采用具有不确定性但初始成本较高，云上则为用户提供了按需付费、以租代买的方式，对降低企业的投资有较大的帮助。

云的经济性不仅限于上面所说的因规模经济和范围经济所带来的经济性，对于企业CXO来说，需要对其预测的云计算经济性有一个明确的处理方式，无论是用于云迁移还是用于新应用。

1 业务改善带来经济价值

在考量云计算的经济性时，最重要的是认识到对云计算帮助各规模企业改善和发展他们的业务，而不是仅仅将云计算的采用所带来的经济性局限在IT业务上。

在许多场景下，云计算可以更快、更有效地为用户提供优质基础资源，智能化协同工作，简化操作，缩短响应时间，获得优异的整体体验。与此同时，云计算帮助企业改变商业过程，深度挖掘潜在的商业价值，为企业创新和颠覆开辟了道路。

VIPKID是知名的青少儿英语国际教育品牌，为了更好的用户体验，VIPKID用完课率来评估在线教室运行质量。VIPKID承诺，若授课过程中网络多次出现卡顿等，外教可以选择结束课程，平台会正常支付老师课时费用的同时，还要向学生赔偿相应的学时。

网络稳定运行对于用户体验有决定性影响。如VIPKID这样1对1授课的模式，授课更密集，对网络质量的要求更高；况且，外教在北美，而学生在中国，天然的地域差距更是让网络稳定性、时延等面临着巨大挑战。

在云服务的广泛覆盖和全球网络互通优化的基础上，VIPKID实现了高清晰度的视频交互通信，保证网络顺畅稳定与信息安全，在最高达3.5万课程实时并发的环境下，网络延时少于200ms，同时让完课率提升到了99.5%，因网络原因而产生的投诉则下降到不足1%。

可以算一笔账，假设每天10万节课，客损从3000节降到500节，2500节/天x200元x365天=1.825亿。这意味着云计算每年为VIPKID节省近2亿元。基于云的业务改善为VIPKID带来了显著的经济价值。

2 创新的云采用方式提高经济性

新消费、新经济是以数据为基础，算力和智能为手段的新阶段，云计算所提供的极致算力和智能（算法），为数据价值的充分利用提供了可能，是数字经济基础设施。

随着数字经济转型进入深水期，越来越多的非互联网企业将会选择全面上云，云计算的支出正在成为每一个公司的标配，使用云计算的能力，是企业基础能力的重要组成部分和指标。

这意味着，在互联网+传统产业的过程中，为了尽快与客户的业务系统、产品平台和技术体系接轨，企业必须尽快上云。

但云计算的采用方式并非是简单地“销售-购买-自用”的模式，创新的云采用方式能够有效实现业务创新，提高云采用的经济性。其中一种方式就是借助云快速构建新模式，将云作为To C和To B业务创新的重要伙伴。

例如，企业借助云获得为中小B端企业提供数字化基础设施和服务C端客户的技术和产品能力，将云及云上技术能力包装成为“创新服务的底座”，形成C（Cloud）2B（提供服务的企业）2B/2C（获得服务的企业或消费者）的新模式。

直播云是好未来旗下专为教育领域提供在线教室的产品，在2020年新冠肺炎疫情期间，好未来面向全国星罗密布的线下培训机构，推出“避风港计划”，将直播云全面免费开放，提供全面的线上直播授课解决方案支持，并提供直播系统、课程内容、运营陪护等“伴跑”支持，帮扶了数万家教培机构。

虽然同样是“云”，但直播云并不是好未来将阿里云资源和能力的一次“转售”。在阿里云所提供的云资源和能力的支撑基础上，好未来直播云融合其对教育培训机构线上教学、管理和服务的理解，从技术层面、产品体系、服务体系、AI赋能四个层级，帮助那些系统建设、研发能力比较弱甚至毫无相关经验的教育培训机构快速实现直播在线教学，而且能够为教学过程提供与一线品牌相近的场景工具和互动体验。

3 云上释放数字技术红利 企业获得更好经济性

云服务商通过核心技术研发，持续提升云服务的资源利用率，扩大云计算规模效应，为企业提供呢高性价比的云服务，通过技术进步、资源优化和技术服务化，云服务商成为技术红利的主要释放渠道，持续降低技术应用与技术创新的门槛。

与此同时，云提供了最稳定的技术基础架构，帮助企业能应对不断变化的业务形态、消费者需求和持续变化的复杂经济体系，从而修炼业务内功。更进一步，云原生将更进一步释放云计算带来的红利，能够使用云上极致弹性的资源交付能力，能够使用云上极为便捷的产品和服务，为资源效率带来极大提升，增强对应用和资源进行编排的能力，并降低运维负担，提高开发效率。

在云本身依靠技术迭代、创新和服务模式所创造的基础设施红利之外，以云为基础，企业将更进一步获得数字技术的红利，获得更好的经济性。

首先，在数字经济时代，数字技术所带来的红利往往不是来自于单点技术，而是“技术组合红利”，需要完整的技术生态，形成技术组合，才能实现技术红利的商业变现。云上的数字技术及其生态的完整性都显著优于一般企业，云上提供的数字技术，可以视作企业的技术“库存”，并在出现数字技术短板时按需使用，从而帮助企业真正获得数字技术红利。

其次，数字技术的投入水平正在持续提升，即使企业在初期支撑起了大规模投资，往往会在迭代过程中因为高昂持续投入而产生新的问题，但数字技术的发展正是在持续的“实践-迭代-再实践-再迭代”中实现的，这导致大量企业的投入无法持续。此外，由于企业的团队能力、行业背景、技术经验等方面的差异，其所产出的数字技术在大量投入下仍然与云服务商所的技术水平有一定差异，在云上直接获得技术并应用于商业获得红利，在时间周期、应用效率、技术水平等方面有显著的经济性。

第三，数字技术具备普惠性，其红利的释放必然是面向最广泛的用户群体，最终通过广泛的市场服务实现，因此在技术红利的生产结构中，最核心的事项就是市场交易，技术红利就是围绕市场交易这一核心事项进行时空重组的结果。云以强大的覆盖能力和服务化特性，支撑企业利用数字技术提升商业服务能力优化高业务效率、降低人力等成本支出。

第四，企业迫切需要释放数据价值，数据不仅是互联网与科技行业的技术红利释放的第一高地，更在传统企业数字化转型中扮演重要角色，云上的数据技术能力已经在中国高速的互联网行业发展中得到验证，可以帮助企业在持续爆炸式增长的大数据中，处理复杂、多样、海量的数据并使全量数据的分析、挖掘成为可能，数据价值能够得到充分释放，企业同时获得经济价值。除此以外，云上包括人工智能在内的多种技术结合，能够更进一步释放数据红利的价值。

2 确认核心云服务的 SLA 服务等级协议

SLA服务等级协议（Service Level Agreement）是服务商与客户之间定义并具体达成了承诺的有关质量、可用性、责任（以及赔偿）等内容的正式约定，在一定开销下为保障服务的性能和可靠性，并且这种开销成为驱动提供服务质量的主要因素。

云服务商将会为客户提供一份预先定义好并广泛适用的SLA服务等级协议（以下简称SLA协议），通常情况下，云服务商与客户签订的SLA协议规定了其想客户提供的云服务（如云服务器、云存储、云网络等）的服务可用性等级指标及赔偿方案。SLA协议内容在其有效期内，一般不会做任何变动，如有云服务的延续订阅，则在续订期开始时所确定的SLA协议将贯穿整个续订周期。

确认核心云服务的SLA协议是企业上云中至关重要的工作，这意味着企业确认了云服务商所提供的云服务的可靠性、可用性等指标，同时包括出现故障之后的解决和赔偿方案，可以满足企业内部的相关要求。一旦确认云服务商的SLA协议，则意味着云服务商交付的服务级别得到企业的认可。

因此，企业应当从如下几个方面确认云服务商的SLA协议，以确保核心云服务在支撑业务连续性上得到有效保护。

确认云服务商的MTBF（平均故障间隔时间）和 MTTR（平均故障恢复时间）：

包括数据中心服务和云服务在内最常用的量化数值标识，MTBF同时被称为平均无故障时间、平均正常使用时间，这一数值越高则证明云服务商所提供的SLA协议的服务水平越高；

MTTR指某个云服务从故障发生到故障修复的的平均修复时间，这一数值越短，则表示云服务恢复速度越快、易恢复性越好，从故障到恢复运行所耗费的时间越短。

确认服务可用性承诺：

云服务的可用性通过MTBF和MTTR的计算得到，即云服务可用性= MTBF/（MTBF+MTTR），这一数值即云服务商在表达可用性时的“X个9”的常见数值。

一般来说，云服务商会为每一项云服务作出不同的服务可用性承诺，如果某项服务未达到前述可用性承诺，客户可以根据SLA协议相应条款约定获得赔偿。

需要注意的是，云服务商所做出的服务可用性承诺普遍包括除外情形，云服务商预先通知客户后进行系统维护所引起的，包括割接、维修、升级和模拟故障演练、客户的疏忽或由客户授权的操作所引起的等情况。

确认云服务“不可用”的定义：

不同的云服务有不同的不可用定义，这一定义并非简单地被标记为“服务不可用”或者是“无法连接服务”，它必须有准确的定义，其中包括及不限于具体的故障状态描述、功能失效描述、无法连接服务以及上述状态延续的时间。

以云服务器为例，常见的对服务不可用的描述如：当一台设置了出入允许规则的云服务器实例以TCP或者UDP协议与任一IP地址的双向（出/入）都无法联通，且该状态持续一分钟以上，视为该分钟内云服务器实例不可用。

确认SLA协议所规定的赔偿规定：

当云所提供服务达不到协议中所约定的可用性标准时，应当对客户因此产生的损失进行赔偿，SLA协议针对赔偿方式、赔偿标准以及客户提出索赔的时限都应当做出详细说明，以便在产生纠纷时有据可依。

赔偿方式和赔偿时效是重要的关注点。云服务商的赔偿方式包括但不限于代金券、使用时长、服务费用减免和

折扣账单，应当在SLA协议中做出规定；其次，云服务商一般要求客户必须在协议规定的时限内向服务商提出索赔，超过时限的索赔要求无效。

在企业全面上云过程中，SLA协议成为阻碍的主要原因存在如下三种常见情况：

– 云服务商的SLA协议与传统IT供应商的SLA协议的差异：云服务商的SLA协议仍然在演进优化过程中，传统IT供应商的SLA协议在全面性、细节性和体系性上存在一定的优势，这往往为企业全面上云带来SLA协议解释上的复杂性；

– 与传统IT供应商所提供的IT产品、解决方案不同，云服务商所提供的服务往往直接服务于业务部门（甚至是某个应用），这意味着业务部门希望对云服务商的SLA协议有所管理和影响；

– 云服务商的SLA协议不仅具有规范的约束作用，同时也意味着需要可量化的指标来衡量IT部门的服务质量，但是，签订这样一份企业内部的协议却是一件比较难的事情；

为了避免SLA协议成为企业全面上云阻碍，在以上对SLA协议的确认之外，如下两个行动非常重要：

首先，IT团队与业务团队可签订企业内部的SLA协议，在云服务的内容与标准上便达成了一致，企业内部的IT服务也将更加标准化与规范化，这不仅让IT团队与业务团队的结合更加紧密，同时有机会将云服务商的SLA协议贯穿到业务服务中去，业务人员就可以清楚地看到，支持某种业务系统的哪些资源存在瓶颈或受到哪些限制，清晰化云服务商在出现问题时的明确责任归属；

其次，选择第三方云服务SLA监控服务或自主建立SLA监控体系尤为重要，且需要形成对内的说明体系，这一体系应当包括不同云服务的指标（需要参考不同云服务的可用性说明）、主动或被动地数据收集方式及频次、数据处理分析及记录、异常情况下的告警机制。此外，云服务商如果提供API方式去获得SLA协议所需要的监控数据，则可以考虑通过第三方监控服务获得持续的报告。

3 从 0 到 1，第一个上云项目

从云计算市场诞生之初，从0到1完成第一个上云项目就是一个关键话题，但随着企业对云计算理解和采用的程度不断加深，企业在选择上云项目的标准在不断变化：在云计算发展初期，不仅是第一个上云项目，大多数的上云项目（或者称之为系统）都是由单个业务部门驱动的单个系统或应用的，将云单纯视为另一种IT资源的云化，即“Cloud Hosting”。此时，上云与传统IT采用方法区别并不显著，或只是“影子IT”或暂时测试。

随着越来越多的企业IT团队将上云作为一项旅程和使命在企业中推动，他们不仅向业务部门提供经过IT批准的云参考体系结构， 以便他们能够安全、受管治和透明地在其上进行创新，更重要的是，上云成为一项受到IT团队支撑、保护、监管和统筹的工作，不仅确保了安全性、合规性、可靠性，更重新改变了从0到1完成第一个上云项目的定义。

但是，这并不意味着第一个上云项目的选择、规划、实施变得更加容易，恰恰相反，第一个上云项目变成必须全面思考的问题，以确保企业全面上云的旅程有一个恰好的开始。因此，第一个上云项目在选择时建议遵循以下原则：

– **明确的云采用动机：**包括但不限于基础设施的重要迭代，如关闭线下数据中心、IT支出降低、关键性技术支持的中断等；技术与业务创新，如获取新的技术能力、改善产品与服务体验、全球化或其他原因驱动的服务需求；

– **短周期内的结果呈现：**中长期的上云项目结果回报并非不可接受，事实上，大多数的上云旅程的回报周期都长达数月甚至1~2年，但对于第一个上云项目来说，IT团队必须尽快获得认可，才能持续的推动企业全面上云的旅程；

– **最小且独立的作用域：**除非有明确的企业高层的命令，否则将第一个上云项目与企业的数字化转型、全局性

业务转型等联系在一起是非常不明智的行为，将范围限制在最小且独立的作用域有助于获得核心动机（及来自利益相关团队的支持）和可衡量的上云效果；

– **与IT架构的颠覆和重构无关：**第一个上云项目是IT团队与业务团队在企业全面上云领域的重要合作机会，将其与IT架构的颠覆和重构联系在一起，不仅会降低业务团队对上云的兴趣度和支持度，更容易降低IT架构受到负面影响；

– **寻找最感兴趣的利益相关者：**在评估第一个上云项目时，寻找最感兴趣的利益相关者与技术、能力、成本、业务理由和成果等要素同等重要，IT团队应该预料到早期的云项目会让一部分人兴奋， 也会让另一部分人感到不适，寻找敢于尝试、好奇心强、对数字经济有所感知的利益相关者不仅能够快速实现从0到1的第一个上云项目实践，而且可以作为未来推动企业全面上云的内部价值传播者和布道官；

– **全面且正向的业务理由：**IT团队必须谨记，第一个上云项目如果没有业务直接促进作用那么就等同于对业务的产生负面影响，无论是业务成本降低、业务流程优化、新技术的创新性使用或是业务灵活性改善，对业务产生直接促进作用非常重要，这将建立一个基线，帮助其他业务团队理解企业全面上云的价值；

– **选择财务情况相对清晰的领域：**复杂的财务情况会导致第一个上云项目价值无法得到准确、显现的计算，从而导致上云重新回到传统IT的成本中心的状态，从而无法获得继续支持；

– **数据和算力需求为主、独立IT系统可供选择：**算力需求和数据容量的暴增有目共睹，传统IT的持续投资意味着将成为数字经济时代的沉默成本，与此同时，这两部分的成本和复杂度都驱动其成为第一个上云项目，将算力和数据移动到云是一种可靠的快速胜利。此外，灾备系统、测试等非生产系统、以及其他简单系统是尝试第一个上云项目的推荐选择；

4 评估业务痛点与收集需求清单

上云的价值正在得到广泛认知，但也存在着一定的误读，并导致部分团队的狂热，许多企业早期的甚至唯一的上云拥护者往往将云认为是“解决一切IT技术、能力、资源和创新问题的灵丹妙药”，并对其在改善业务方面的表现充满希望。

因此，在上云时评估业务痛点并收集需求清单的工作就显得尤为重要，在此建议从如下五个角度评估业务痛点，以确认其成为上云旅程中重点关注的对象。

– **认清提出业务痛点的角色：**评估业务痛点的第一步是与企业内不同角色进行调研对话，包括但不限于财务角色、市场营销角色、客户服务角色（通常为销售）、人力资源与行政角色、管理层角色、产品与技术开发角色，他们会提出基于其自身角色的业务痛点，如财务角色关注提高盈利能力、降低成本并改善合规性；

– **明确解决业务痛点后的结果：**IT团队必须明确业务痛点解决后所能获得的业务结果，包括但不限于财务结果、性能结果、敏捷性结果、组织及创新结果、客户体验结果等，这些结果应当有业务团队的明确承诺和数字指标上的改善，比如在上云之后，业务团队全球客户服务网络的延迟性从秒级提升到毫秒级；

– **定位业务痛点与上云之间的关系：**一定比例的业务团队会夸大业务痛点与上云之间的重要性关系，从而将业务效果、敏捷性等结果与云密切相关，但能否快速响应和推动市场变化并非仅仅依靠上云实现，IT团队必须避免此类“诱惑”，强调业务痛点通过上云得到明确改善，而非受到业务团队其他因素的严重影响；

– **数据和算力驱动改善的业务痛点：**数据和算力驱动的业务痛点改善，包括工作负载表现的优化，是上云可以直接产生的效果。IT团队必须明确业务痛点受限于数据和算力的可获得性，而非其他明确的限制性因素，这些可获得性不仅包括数据和算力的资源储备充足度、易用性，也包括IT团队的支持响应速度。

收集需求清单是企业顺利全面上云的重要工作，在此过程中，以业务痛点的评估为基础，收集支持特定业务的IT需求及资产的列表，以便在上云旅程中持续与业务团队互动，进行业务需求分析及支撑计划。

在收集需求清单时，建议将获得的需求分为以下三类：

第一类，急切需要解决的业务需求，如果该问题不能得到尽快的解决，则会产生显著的业务影响，降低企业业务收入和客户服务水平，上云能够产生显著改善；

第二类，需要改善但短期内不会对业务造成显著影响的需求，该问题必须要得到解决，如持续上升的业务（或IT团队）人力成本，但在短期内可以通过人力增加或自动化工具（如RPA等）进行解决；

第三类，是否需要改善仍然有待商榷的需求，处理这部分需求时IT团队必须与评估业务痛点紧密结合，避免虚假的需求清单（与云无关的）成为上云旅程中的组成部分；

作为需求评估的补充，IT团队不应只面向内部客户（即业务团队）进行需求分析，外部客户的需求（包括引入业务、开发、运营及管理等团队的讨论）是企业全面上云的重点，确保清晰的需求分析是实现全面上云价值最大化的所需要得，并能够确保IT团队充分了解业务团队的业务成果目标及其所需要的IT资源与运营支持。

5 清点数字资产与合规性要求

在长达二十年之久的信息化进程中，无论是互联网公司还是传统企业，在积累物理资产的同时，拥有并积累大量数字资产，包括虚拟机、容器、应用程序、算法和数据等。

需要指出的是，在企业全面上云过程中所统计的数字资产，不包括传统物理资产和无形资产（如专利、商标

等）的数字化表达，数字资产是支撑企业业务及其流程、运营管理、系统运维、安全合规等信息化、数字化工作而存在的技术与数据资产的总集。

在企业从信息化到全面上云的过程中，数字资产将从传统物理基础设施同步迁移到云上基础架构，由于企业全面上云的主要驱动力往往来自于数字化转型，因此，这意味着IT团队在完成数字资产的整体迁移的同时，往往要面对更高的对数字资产可用性、准确性和及时性的要求，形成双重压力。

清点数字资产并形成清单，同时将数字资产与其所支撑的业务进行一一对应，进而完成数字资产与业务的映射关系，确保上云后面向业务的数字资产可用性，是企业全面上云的重要步骤，它确保上云后数字资产的不丢失、业务应用资源的可用以及进一步对数字资产分析及合理化的充足准备。

数字资产清单的收集常被规划为三类：

基础架构资产：通常情况下被定义为提供基础IT能力支撑的数字资产，包括但不限于虚拟机、容器、网络架构等，需要通过系统扫描和支撑业务的基础设施的统计，确保创建的所有基础架构资产都被登记在统一列表上，需要注意的是，网络架构存在映射和依赖关系，也应当一并登记；

应用体系资产：无论是对内还是对外，应用体系都是直接面向“客户（或用户）”的数字资产，满足所服务对象需求并接受其反馈，但应用体系资产并不仅仅包括前端的应用程序，更包括使其发挥作用的API、应用框架、中间件以及应用架构，由于在上云过程中一般不涉及到算法，并不需要包括算法等数字资产；

数据资产：数据资产是企业产生量最大、产生最频繁的数字资产，每时每刻都在发生变化，但总体来说数据资产处在持续高速膨胀之中，企业全面上云的很重要一步就是数据及数据平台全面上云，数据平台包括数据仓库、数据湖以及数据中台体系。因此，数据资产清单的内容不仅应当包括数据，还应当包括数据支撑体系（如数据中台）、数据依赖关系、数据变化流程以及企业数据管理政策规范；

数字资产清单的收集很难在一次流程中完成，IT团队需要和包括业务团队在内的所有相关方进行验证确认，同时，尽可能使用自动化工具进行统计而非单纯的手工作业以确保能够收集到清单所遗漏的数字资产，与此同时，建议遵循以下三个原则：

1、清点数字资产和安全合规性需求清点同步进行，在清点数字资产的同时完成安全及合规性要求的收集，并将两者联系起来，这将帮助IT团队避免重复的安全合规调研工作，并帮助梳理、评估、管理和保护企业的数字资产；

2、清点数字资产同时下线“被遗忘”的基础架构和应用体系资产，清点数字资产的过程同时是抛弃已经被遗忘的数字资产的过程，如长期闲置的虚拟机或操作系统镜像，在清点过程中可以借此降低维护数字资产的成本，并避免将陈旧、冗余和无效的数字资产带入云端；

3、混合的、多步骤的清点数字资产方式：无论是从工作负载入手还是从资产管理入手，亦或是从财务报表开始，都存在一定的不足，清点数字资产方式应当是多种方式的混合，常用的方法是首先从资产管理入手，并通过财务报表进行比对和验证，在此之后通过工作负载开始对前面工作的成果进行验证，并列出业务关键工作负载的数字资产清单以确保上云过程对核心业务不会产生任何负面影响，随后在基础架构资产、应用体系资产和数据资产的上云过程中，不断与财务报表和当前版本的数字资产清单进行比对。

6 上云技能与组织就绪

1 全面上云的技能准备

越来越多的企业将他们的基础设施、应用程序和数据迁移到云中，许多企业全面上云旅程的主要负责人都将迁移作为整个工作中的第一要务，但对于相当多的非互联网企业来说，当企业开始云迁移之后才发现，不仅业务团队

在对云的理解和云技能上严重匮乏，IT团队同样面临云技能方面得诸多短板。

不仅如此，据《云计算发展白皮书（2020）》指出云技能从粗放向精细转型，技能体系日臻成熟，随着云原生的容器、微服务、无服务器等技能，越来越靠近应用层，资源调理的颗粒性、业务耦合性、管理效率和效能利用率都得到了极大提高，但对IT团队的技能要求也越来越高。

企业必须要找到来自内部或外部的合适人选，使用正确的技能集合以优化其上云迁移，但这一人选并不仅仅是一个人，而是应当包括五类具备关键技能的人员：

- **云计算基础设施相关技能**，虽然云服务都基于在线服务和API，但具备基础设施管理、运维和架构经验，并熟悉其在云上映射体系的技能，尤其是虚拟化、云存储和虚拟网络等方面的技术能力，这是搭建云计算基础设施的关键。相关技能应当包括部署实施能力、性能优化能力、架构设计能力、云服务产品配置能力、业务迁移能力和云服务产品对比能力；

- **完整支撑应用程序堆栈的技能**，虽然不是每一个IT团队的成员都需要具备该技能，但是至少有一位团队成员需要熟悉从底层资源（IaaS）到中间件及平台层（PaaS）完整支撑应用程序堆栈的技能，这不仅能够更好地支撑应用程序迁移到云，也可以触类旁通的解决应用体系迁移问题；

- **数据架构设计、构建和支撑的技能**，数据上云能够显著加速企业数字化进程，充分利用云上的分布式、高可用、高性能等特点，设计数据存储架构并构建起数据存储及支撑业务的基础设施的技能尤为重要，这部分包括数据存储技术、数据分析、数据可视化、数据变成、数据项目设计等技能；

- **在云上构建安全体系的技能**，在企业全面上云旅程中，安全体系建设必须同步构建，才能够及时实现安全处理，同时，IT团队必须有专门人员具备相关行业的安全协议和相关的法规的理解和执行能力，这意味着IT团队的安全人员除了熟悉云服务商的DDoS防护、Web应用防火墙、网站威胁相关系统之外，要快速学习云防火墙、云监控等技能；

– **具备同时向IT和业务团队进行上云培训技能**，培训技能常被上云负责团队所忽略，为了帮助IT和业务团队开始上云旅程，必要的培训必不可少，包括上云理念、策略、规划、采用以及就绪等方面的IT技能培训，同时也应加入让业务团队理解上云价值的沟通型培训。

企业全面上云的技能准备可以通过云服务商所提供的认证培训服务获得，并认证培养、挖掘专业人才，提升公司的云上技术能力，在阿里云上亦提供相关服务，具体可参见：阿里云大学–https://edu.aliyun.com/ 。

2 组织就绪为上云提供保障

在企业全面上云的旅程中，组织话题贯穿整个生命周期，但在上云初期，规划恰当的上云组织架构，确保整个企业的组织——而不仅仅是IT组织——的就绪，将为上云提供可靠的保障，同时避免大量经常出现的上云陷阱和难题。

为了实施企业全面上云，应当建立专门的上云组织团队，贯穿整个上云旅程并在企业全面上云之后，转换成为企业的云服务与云创新团队，这一团队的组成、职能和构建建议如下：

– **设置云治理专业岗位甚至小规模独立团队**，从IT治理的概念迁移，云治理是在在企业全面上云过程中，为鼓励期望行为而明确的决策权归属和责任担当框架，企业应当在上云伊始设置云治理专业岗位甚至小规模独立团队。以确保可以正确评估、管理和监控上云的进程、风险及合规性，从最小化可行产品原则开始构建，持续从关注访问控制和资源管理的轻量级治理模式，过渡到基于组织架构的企业级IT模式，并形成效能优化治理模式。

– **建立融合云策略和云采用职责的专业团队**，云策略和云采用团队是上云中必不可少的组成，但与市场上流行的独立构建方式不同，在此我们建议将云策略和云采用团队加以融合。这个团队将不仅负责定义上云驱动力、上云路径、业务合作策略和上云价值结果，还将投入到如何将其付诸实施的工作中去，这将帮助这个团队在云策略与云采用之间达成更实际的可行性与优先级的平衡。

但这一融合团队并非每个人都身兼两种角色，常用的方式是一部分人主要负责云策略但兼顾云采用，另一部分人则与之相反，但团队的负责人应当横跨两个职责，在主要负责云策略的成员中，应当有业务团队的参与，但IT团队仍然不应当缺席。与独立构建两个团队不同，融合团队将实现更及时的协作，并通过云采用过程中的反馈修正云策略，以确保企业全面上云旅程的顺利展开。

– **清点数字资产与合规性的岗位应当长期存在**，正如前述，数字资产清单的收集很难在一次流程中完成，IT团队需要和包括业务团队在内的所有相关方进行验证确认，即使是在企业全面上云之后，为了确保云上数字资产的清晰、准确，这一岗位应当长期存在并扮演重要角色。

– **与应用迁移和业务开发紧密结合的DevOps团队**，DevOps理念强化软件研发运营全周期的管理，从软件需求到生产运维的全流程改进和优化，结合统一工具链，实现文化、流程、工具的一致性，降低组织内部的沟通与管理障碍，加速业务的流程化、自动化。这意味着，在上云初期即建立与应用迁移和业务开发紧密结合的DevOps团队，业务团队和IT团队会有机会将部分业务负载跨越Cloud Hosting阶段直接进入Cloud Native，改变研发运营的生产方式，打破组织壁垒，实现研发与运维的跨域协同。

– **明确一个稳定长期存在的云运维团队并确保低离职率**，虽然许多互联网企业认为“谁构建，谁运维”，其运维工作全部由开发人员完成，只保留极少的 核心角色专门响应和处理严重等级的故障，但是在非互联网企业中，云运维团队仍然非常重要。

云上运维与传统运维有着本质上的区别，并非是运维物理资源向运维云上资源的变化，而是一种全新的以业务为导向、以云的特性为基础的全新运维方式，运维将从IT运维转向云上新基础设施运营，运维人员面对的是一个无法见到任何物理设备，脱离原有工具体系，（云）资源获取速度更快、颗粒度更细、种类更多元，并从硬件基础设施进入操作系统、软件应用程序和云操作系统的全新环境。

因此，在云上，运维人员并不是没有价值，而是会变得更加重要，当前的运维工作不是AIOps 和运维自动化工

具可以独立承担的，但需要指出的是，底层基础设施的运维工作确实可以委托给第三方公共云服务商统一负责，但上层应用的运维工作还需要企业自己来承担。云运维团队将倾向于具备开发能力，尤其是产品能力，某种意义上将是DevOps团队的一部分。

3 CXO的价值体现与角色转变

上云并非简单的IT投资，它所改变的除了企业的IT基础设施、数据基础，影响IT运维团队的运营模式与工作目标，还包括企业的业务系统、信息系统、财务系统等系统平台，并对企业的业务运营、消费者触达、生态连接以及内部的组织和运营模式产生深远影响，因此在上云进程中企业中的CXO（CEO、CFO、CIO）不仅需要起到非常重要的推动作用，发挥其在上云中的关键价值，企业CXO自身也会经历角色的转变。

CEO的价值与角色转变：上云无关者-上云尝试者-上云决策者-上云倡导者

CEO是一个在企业中负责日常经营管理的最高级管理人员。一般意义上认为，作为公司的实际管理者和经营者，IT 投资的政策和策略以及公司 IT 资源的流动、组合和重组只需要经过CEO审核、批准，而无需CEO进行过多参与和干预， 即使是在互联网企业CEO往往具有技术背景（甚至是IT背景）的情况下，CEO对IT建设的参与度也仍然偏低。

在云计算时代，云比传统IT与企业业务的构建、运营和增长的关系更加紧密，这意味着CEO在上云过程中必然经历一个从无关到浅层参与到深度参与的过程。

上云无关者：CEO将上云看作是传统IT基础设施在技术上的升级迭代，简单的将上云理解为从物理基础设施到虚拟化基础设施的转变，对上云过程中出现的新成本支出投以最主要的关注，并要求CFO较多的参与上云进程。

上云尝试者：通过外界及同行业信息的了解，对上云具有一定的理解和兴趣，愿意支持IT团队进行探索，尝试将单个业务项目做上云改造，但仍然将云计算视为IT基础设施的一部分，即将这种改造认为是IT支出和服务方式的

改变，并要求业务项目改造后有明确的成本效益。

上云决策者：认识到IT基础设施的云化只是上云的第一步，认可云计算在企业业务上的巨大价值，决定借助上云来推动企业核心技术的互联网化、应用的数据化和智能化，在将业务逐渐云化的过程中，决定利用云深度改造和优化现有业务，成为企业上云的决策者，将业务团队和IT团队联合在一起推动上云进程。

上云倡导者：要求企业全面上云。在一定期限内100%业务上云，制定通过云上产品、技术和解决方案，加速实现企业业务数据化、AIoT化（智联网）、移动化。在制定业务和技术战略时，将云所供给的资源、能力作为战略发展的参考，向合作伙伴和客户倡导上云，并推动构建云上生态和产业链。

CFO的价值与角色转变：财务审核者-上云狂热者-上云战略参与者-新财务模型设计者

CFO经常是CIO的管理者，即向下管理CIO，向上将IT作为自己工作的一部分向上对CEO负责，肩负这一角色的CFO负担着两个责任：第一，企业财务、投（融）资的第一责任人；第二，将IT作为重要的投资之一，纳入严格的成本管理中。

但更重要的是， CFO应当将新的财务计划与企业发展战略联合，必须做到能够主动的评估当前的技术、财务状况与公司的发展规划之间的有机联系，在这三者之间建立有序的链接，使公司上下协调一致，发挥最大职能。

这样的CFO是对传统CFO功能的一个突破——CFO现在已经愈来愈成为公司战略层面的重要架构，成为管理层的紧要顾问。

财务审核者：受限于专业技能，CFO对云计算的理解速度和深度都处于“慢热”。由于IT建设长期采用项目制并每年审核（极少的企业会制定3-5年的长期IT投资计划）IT支出和预算，CFO在上云初期会将云计算作为一般性投资项目认知，并因为其新增支出的属性加以严格审核，这意味着CFO将只是作为财务审核者的身份参与到上云初期进程中。

上云狂热者：由于自建数据中心及IT基础设施涉及到巨额的资金预支，一次采购长期占用大量资金，并持续贬值，CFO往往会因为硬件、软件一次投入对现金储备的挑战而严格审核IT支持。在上云进程中，随着云计算按需使用、按需付费、支出灵活的特点（特别是云服务支出入费用，企业级客户通过长约获得优惠，比资产平摊费更低），Capex到Opex的转换会让CFO高度认可，并陷入上云狂热期。这意味着CFO将会要求快速实现从传统IT架构向云的转换。

上云战略参与者：经历上云狂热期的CFO会之间发现，并非所有的云服务都能带来CFO们所期望的弹性和按使用计费的特性，比如SaaS则一般是按用户数来收费，并且需要签署长期服务协议，很难达成随用随停的目的，CFO将认识到，自己必须要亲自参与到上云战略中，通过财务的手段实施上云战略层面的操作，一个非常重要的工作，是具备数据分析师的能力，将来自上云的原始数据碎片整合成有效的数据信息，融入公司战略中。

新财务模型设计者：创建一个财务模型用于准确全面反映任何云转换的商业价值的过程可能十分复杂，而且不同组织的财务模型和业务模式往往不尽相同，但是为了更好的了利用云及云上的大数据、人工智能等技术红利，CFO仍然应当从收入及成本增量、运营成本缩减、人员及软性成本减少、云投资收益等方面，设计新财务模型，以更好地支出企业上云进程。与此同时，为上云设计的新财务模型能够在企业数字化转型过程中被复用。

CIO的价值与角色转变：上云诠释者（布道）–上云推动者（协调）–上云流程管理者–业务紧密合作者

随着云计算的采用，企业中越来越多的业务单元将拥有自己的IT采购流程，CIO将花费少得多的时间来担忧IT基础设施的具体细节，但这并非完美的解决方案，IT资源和能力的配给并非只是单纯的“性能、容量和带宽采购”，业务单元的负责人们会面对SLA无法满足最低要求、很难精确预测数据量和贷款卡需求、无法有效管理资源（特别是网络）等问题，这些问题可能会导致长时间的宕机，并放缓应用响应水平，从而影响生产效率并产生不合规和业务损失的风险，同时提高IT成本。

上云诠释者（布道）：为了说服企业高层和内部协作者上云，CIO在上云初期必然会肩负起上云诠释者的角

色，成为最为积极的上云布道师，这其中的关键说服原则基于云计算可以重构垂直行业的业务流程和商业模式的巨大潜力，因此CIO必须具备能将复杂的事情简单化，能一句话说清楚云计算给企业带来的新商业模式和结构重组价值。

上云推动者（协调）： 在这阶段，CIO的主要职责是确立新建IT计划的优先顺序,审核、协调与推进上云计划，从业务优先级、应用复杂度、迁移难度、业务连续性要求等角度，制定包括系统、应用上云顺序在内的上云路线图。CIO需要投入较大的精力在协调工作，并在复杂环境中持续推动上云。

云采用管理者：随着技术在企业运营中变得愈加重要，COO和CIO的角色将合并，业务单元及其服务提供商之间的政策执行、技术布道和调解将成为CIO的关键职责。因此，在企业中CIO的角色演变成为运营职责，更多注重内部咨询，更少涉及基础设施管理，成为拥有较强的云采用自主权的业务单元的云采用的顾问和管理者。

业务紧密合作者：CIO将技术调配战略与业务战略紧密结合在一起，可以在不同的业务单元上推动云与业务的结合使用,以使其保持竞争力和创新性，具有优化、促进甚至是改进企业现有业务的能力，IT团队将有一部分成员成为业务单元的核心成员，CIO自身也将成为业务紧密合作者，将云计算作为业务发展的关键驱动力之一。

5 企业全面上云成功路径与实践
IT 上云蓝图规划

1 设定提升 IT 服务质量的目标

企业云部门的终极使命是打破IT内部的壁垒，打破IT与业务的壁垒，用最快的时间，最低的成本，最好的质量来实现业务的任意需求/创造业务新场景，最终支持企业转型为融合业务与技术的“软件定义”生态圈经营体。

云的建设过程，是效率革命的过程，也是技术、组织、流程多方面适配业务变革的过程，赋予IT前所未有的参与业务的“机遇”。

1 服务等级管理流程

依据业务需求设定可用性等目标，确保未来云服务对外提供服务的管理流程，运营服务等级协议并支持合同满足服务等级协议的要求。

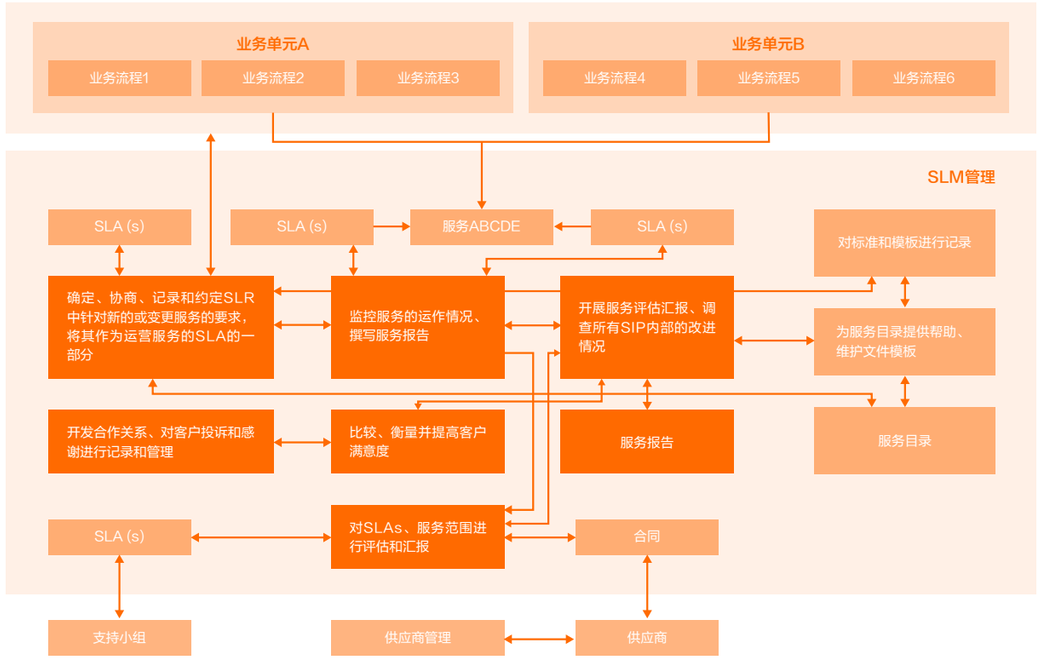


图 服务等级管理流程示意

・设计服务级别需求框架：

服务等级管理应符合企业云部门的服务等级协议的结构，以保证企业业务需要得到及时响应。

・监控服务绩效：

服务等级协议须得到有效的监控，才可以对服务进行衡量及改善。

・考核、测量和改善客户满意度：

有效管理业务满意度。加强对业务满意度的管理，明确改进方向。

・审查和修订基础协议和服务范围：

未来云服务应通过内部技术团队、外部合作伙伴及外部供应商共同对外提供服务。

・服务报告：

在服务等级协议达成一致后，应立即启动服务监控，并定期向业务方提供服务绩效报告。

・在服务改进计划中，审查、改进服务：

定期评审会应组织行业单位人员共同参与，以评估过去一定时期内的服务成就及下一时期的服务目标。

2 SLA指标管理体系

在云服务SLA指标管理体系方面，通过对业务连续性、系统可靠性及系统运营服务等级的定义，来定义不同的指标项去满足服务需求：

・业务连续性：RTO、RPO、其他

在业务连续性方面，通常会根据系统的RTO、RPO来衡量是否满足用户服务需求，根据业务连续性等级的不同，会对RTO、RPO以及其他特殊的参考指标的要求共同去定义容灾指标。

・容灾服务支持：服务支持时间、问题响应时间、问题解决时间

对于容灾服务来讲，一般而言会定义服务的支持时间、问题相应时间和问题解决时间，再根据容灾级别和故障级别定义具体的指标项。

- 整体服务水平：可用性、性能、满意度、服务支持时间、其他

对于未来企业提供的云上服务，根据具体的服务级别，会对服务的可用性、性能、满意度、服务支持时间或者一些服务的特殊指标要求去定义具体的指标项。

- 故障处理效率：问题响应时间、问题解决时间

对于云上服务出现故障的时候，一般来讲我们会通过衡量运维人员的故障的响应时间以及对问题的解决时间两个维度去定义服务的等级。

3 SLA目标设定

根据用户类型和请求类型去定义不同的服务指标。在云服务投入运营后，建议SLA服务水平等级应随时间推移而变化,从基础水平开始,并逐步提高标准。

阶段一：基线

- 收集指针以确定初始服务级别。
- 将服务表现与期望的结果和基准进行比较,以确定具体的服务表现目标。
- 指标不会在云服务外部传达。
- 工具和范本简单，可以是手动进行。

阶段二：实践

- 生成服务表现指标，并传达给企业业务部门。
- 设计简单的服务表现检查方法
- 工具和模板内置于流程中,并作为日常工作的一部分进行更新,自动化程度不断提高。
- 启动常规报告和回馈程序。

阶段三：提高

- 服务确定级别差异并创建具体的改进行动计划。
- 调整服务等级目标，主要为了持续提升以满足业务部门的技术和业务目标。
- 服务表现的管理工具与系统数据连接,且大部分是自动化的。
- 绩效管理流程已投入运行。

阶段四：优化

- 实施改进措施,确定结果,确定新目标。
- 服务表现衡量系统到位。
- 连续测量和数据收集的过程是完全自动化的。
- 基于结果的奖励措施已经到位。

2 上云目标评估要素及可行性分析

伴随企业信息系统的持续建设，各种业务应用会导致某种程度的技术债，并具有各自独特的属性。因此，云的

采用将因产品组合而异。

可借助企业全面上云方法论，通过上云适应性和评估模型及工具，收集企业应用多个维度的特征数据，并加以分析以评估应用对云的兼容性、最佳着陆区和应用上云迁移路径。

需要收集的应用关键信息按其评估目的可分为业务目标评估、安全合规评估、业务运行环境评估和IT基础架构评估。

1 业务目标评估要素

进行业务目标评估所需要收集的业务应用特征数据（关键属性）有：

- 上云收益
- 市场需求
- 可用性要求
- SLA等级
- 高可靠性要求
- 灾备要求
- 功能要求
- 用户数预估
- 业务增长预估
- 对用户的影响
- 组织结构支持
- 合作伙伴支持

2 安全合规评估要素

进行安全合规评估所需要收集的业务应用特征数据（关键属性）有：

- 物理安全
- 硬件安全
- 主机安全
- 网络安全
- 虚拟化安全
- 数据安全
- 账号安全
- 业务安全
- 安全监控
- 国家/地区合规要求
- 行业合规要求
- 企业内审合规要求

3 业务运行环境评估要素

进行业务运行环境评估所需要收集的业务应用特征数据（关键属性）有：

- 技术架构
- 硬件相关性
- 源代码是否可控

- 编程语言
- 程序模块耦合度
- 外部依赖性
- 应用扩展性
- 是否使用分布式架构
- 应用发布流程

4 IT基础架构评估要素

进行IT基础架构评估所需要收集的业务应用特征数据（关键属性）有：

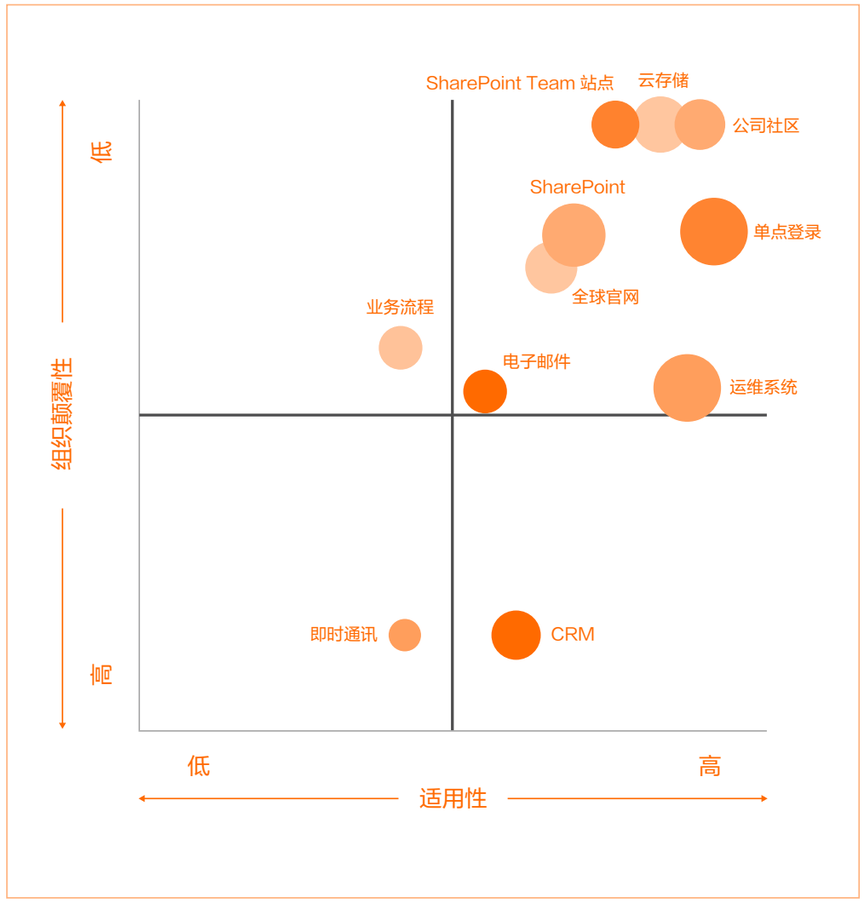
- 部署架构
- 应用稳定性
- 使用虚拟化
- 存储设备使用
- CPU/内存要求
- CPU/内存使用率
- 网络延时
- 物理设备依赖性
- 操作系统上云兼容性
- 中间件上云兼容性
- 数据库上云兼容性

5 上云可行性评估报告

基于收集到的50多个维度的业务类和技术类的业务应用特征数据（关键属性），借助上云适应性和评估模型客观地对客户现有的各个业务领域的应用系统进行量化评估，形成上云可行性评估报告。

评估报告的主要内容包括对于每个应用的上云可行性的简要描述，分析评估的结果以表格和散点图的形式呈现。示例如下：

属性	权重和置信系数		适用性和放置值		
	权重	置信	本地数据中心	中性	公有云
应用程序云就绪性（仅套装软件）	5	5	无云版本	需要升级	支持当前版本
应用程序： 套装软件与否	3	5	套装软件	自定义 Web	
应用架构知识水平	7	5	低	中等	高
应用代码复杂性/规模	8	10	高	低中	低
应用程序硬件依赖项	10	10	是	不可用	否
应用程序操作系统/平台的云适用性	6	5	非云兼容	需要升级	云兼容
应用规范和合同需求	7	10	高	中等	低
应用服务器云就绪性	6	5	非云兼容	需要升级	云兼容
业务关键性	8	10	非常高	中高	低
业务功能就绪性	9	5	否		是
数据库云就绪性	6	10	非云兼容	需要升级	云兼容
数据分类	6	10	高保密	内部	公共



云架构	阶段	1	2	3	4.1	4.2	完成	主要联系人	业务驱动因素	适用性	影响	其他
解决方案1								领导	53%	53%	57%	
解决方案2								领导	6%	32%	33%	
解决方案3								领导	6%	32%	33%	
解决方案4								领导	6%	32%	33%	
解决方案5								领导	6%	32%	33%	
其他机会项		框架步骤										
云架构	阶段	1	2	3	4.1	4.2	完成	主要联系人	业务驱动因素	适用性	影响	其他
特殊情况								领导	6%	32%	33%	

图：上云可行性评估结果示例

阿里云基于成熟的企业客户上云经验，提供上云可行性的快速评估工具供您使用。通过梳理在企业上云前普遍需要关注和评估的问题点，给予企业评估建议报告，助力企业全面上云。

在上云评估阶段，通过上云可行性评估工具可以完成：

- 分析云下业务与技术的痛点，评估云上解决痛点的可行性，作为分类对接方案、人员的依据，为针对不同规模、场景制定有效的迁移方案做准备。
- 以在线调查和评估报告的形式从IT基础设施、上云目标、业务环境和安全合规等维度详细评估，相比线下表格更有利于迁移过程信息化管理和打通服务。

需要说明的是：上云评估越详尽，上云方案就会越具体，整个上云过程也会更快更标准。

获取阿里云企业上云可行性评估工具，前往上云能力中心开始评估（https://cmc.console.aliyun.com/submitAssessment）。在评估过程中，您还可以免费咨询阿里云企业上云专家获得支持。

3 IT 上云规划

1 业务梳理

通过工具和方法，从业务的影响范围、组织范围、重要性、关联度，业务一致性要求、风险及监管要求、应用体系架构、基础技术架构等多个维度，对企业现有的业务进行梳理。评估业务目前的运营状态，确定与未来的业务运营需求的差距，结合发展趋势和领先实践，确定业务上云的规划目标和迁移路线图。

2 负载分析

1、现有负载及业务情况调研/分析

在进行上云规划过程中，要对现有负载及业务情况进行调研分析，可以通过工具和方法来收集应用程序的信息，主要包括以下内容：

应用数据

主要包括所有应用程序组合的完整列表，以及技术和非技术属性。

基础设施数据

主要包括基础设施的架构、应用程序与基础设施的映射数据，工作负载的类型以及软件版本。

性能数据

主要包括应用程序的性能特征、服务属性以及日常的服务请求数量。

财务数据

主要包括与当前基础设施资产有关的财务成本和现行折旧时间表。

安全性和合规性信息

主要是对企业所在区域与网络安全需求相关的法律法规及相关政策进行分析、并遵循行业监管和组织内部对数据安全、隐私保护和透明度的要求。

2、业务与负载上云优先级

我们可以从以下几个维度确定业务与负载上云优先级。

快速降低IT运维成本

将现有应用按照原样迁移到云平台上，利用基础设施资源及服务只做虚拟化部署，不需要进行技术架构和数据架构的变更。

快速的帮助业务增长

把一个旧的原应用系统，或者已经迁移到云上的系统进行改造，对相关的组件、服务进行替换或者部分优化，通过使用PaaS平台资源及服务，将原有的应用系统改造为云应用。

从旧系统投资中挖掘出最大价值

将现有核心应用重新设计成为松耦合、模块化的云原生架构。通过云服务的支撑能力提升系统安全性、可靠性和高性能，并降低业务变革带来的成本。

❸ 应用及关联依赖分析，现状接口与依赖关系梳理

首先是利用应用程序映射工具对应用进行关联依赖性分析，形成依赖树结构，然后是逐一对依赖分支进行识别，确定不被其他应用程序依赖的应用程序，结合业务与负载上云优先级的规划内容，将这些应用程序划分到初始迁移的应用组合中。对于有相互依赖关系的应用程序，要根据其业务的重要性和依赖关系进行识别并分组，形成后续的应用组合。

❹ 业务、组织与架构规划

1、与云相对应的组织架构

业务一对齐型组织

图：业务一对齐型组织模式

业务一对齐型组织概念

- 云团队细分为与业务团队一致的组
- 大部分是联合交付模式,核心团队负责制定标准、选择平台和指导体系结构设计

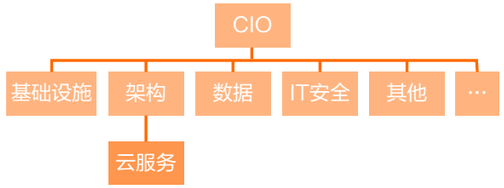
业务一对齐型组织优势

- 支持专门定制的云基础架构解决方案
- 通过端到端业务一致性提高响应能力和成本透明度
- 促进业务单位和IT组织之间的明确责任和界限
- 减少对基础架构团队的依赖和需求

业务一对齐型组织缺点

- 需要强大的跨云治理和采用支持工具来嵌入和自动化风险、合规性和控制机制
- 跨业务部门的重复功能和角色会导致增加员工人数

综合型组织



图：综合型组织模式

综合型组织概念

- 云服务团队作为传统IT基础架构团队的扩展,创建支持混合基础架构的集成功能,提供公共、私有和现有内部基础设施之间的连接

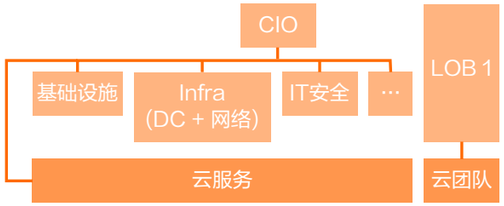
综合性组织优点

- 支持云服务而不增加新的组织结构,实现云服务的有机增长,具体取决于业务需求、风险和控制偏好以及保留内部基础设施
- 受益于现有资本和人力资源的规模、稳定性和协同效应
- 降低整体投资风险,最大化遗留资产回报

综合性组织缺点

- 新的云服务团队 可能受到传统治理的阻碍
- 在云服务管理流程上需要进行妥协让步
- 云服务团队缺少品牌和企业内部感知

领袖型组织



图：领袖型组织模式

领袖型组织概念

- 成立专门的云服务团队，直接向 CIO 报告,云被公认为业务的关键驱动因素
- 此类组织形态在面向产品和技术的企业(例如金融行业、技术型企业)中经常看到

领袖型组织优点

- 一套标准、模式和设计——摆脱以应用程序为中心的方式,提高利用率
- 云业务流程推动正确的需求流程
- 为云服务部门提供机会,创造新的品牌和声誉
- 促进敏捷性和灵活性,以推动支持云的战略计划,创新和生成新的服务和产品
- 使云团队和其他IT职能之间的责任和组织接口更加清晰

领袖型组织缺点

- 需要大量资金来重组现有团队或从零开始构建、达到临界质量并过渡到可持续服务提供商
- 迫使云服务领导层专注于引导,而不是战略领导力

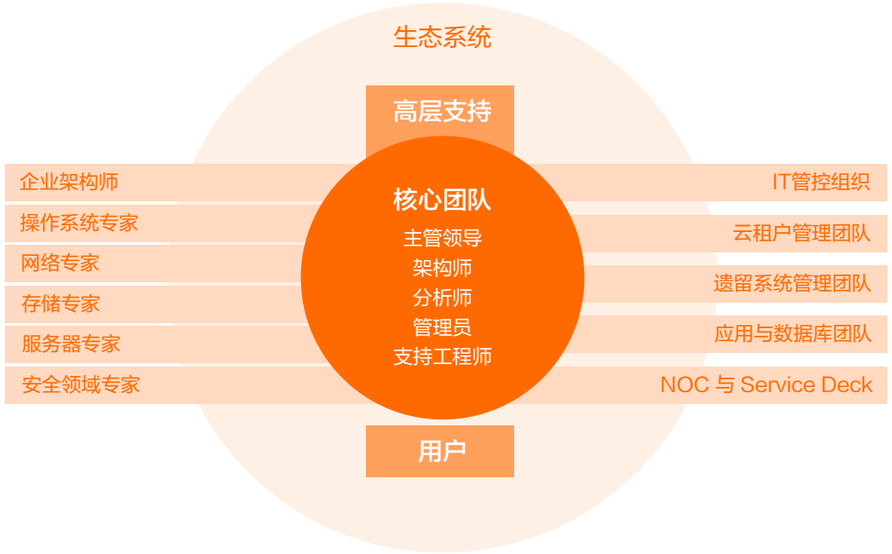
2、建立云COE团队

云服务团队需要具有可衡量，责任清晰的特质，并能够提高云计算运营管理的效率。

云服务团队是由一个云计算核心技术专家（ COE ）团队和相关功能团队组合而成。云计算运营团队为所有云计算环境的决策和行动指明方向。

云服务COE模型定义了在团队角色跨域的云计算运营管理责任。

云服务算运营COE可以不断地开发和实施创新的方法去构建，设计，部署前瞻性云计算基础架构，并追求最大化的效益，同时满足运营水平协议需要，基于云计算环境，提供可靠的服务质量保证。



图：云计算COE团队角色定义

一个完整的云COE团队中，至少应包含四种成员角色。

云架构师

- 负责云基础架构标准制定和执行
- 响应业务需求
- 集成、升级计划
- 容量和性能管理
- 配置与合规管理

云管理员

- 负责云基础架构的管理
- 部署和配置虚拟化组件
- 负责安全、配置、合规管理执行
- 监控并维护云计算环境的稳定运行

云分析师

- 负责容量跟踪、分析、预报
- 性能跟踪、分析，汇报
- 负责安全、配置、合规管理执行
- 维护云计算环境的稳定运行
- 设计云虚拟机基础组件

云支持工程师

- 监控并维护云计算环境的稳定运行
- 负责运行在云计算环境中系统及应用的日常操作

5 管理与优化流程，持续优化机制

企业全面上云，对企业IT来讲是颠覆性的革命，是一个从观念、体系、技术、组织等多方面进行变革，需要持续的对管理流程进行更新和优化，实现资源整合以及分配的高效，敏捷，构建资源整合能力，服务开通能力，实时洞察能力，弹性扩展能力；需要建立新的、高绩效的、敏捷的组织模式，以及新的项目交付方法、新的人才技能培养与创新体系；需要从以业务流程为核心的系统与服务管理，向以数字化为核心的产品与资源管理转变。实现IT即产品，IT即平台，IT即服务，以个性化、体验为导向，灵活，简便，标准化的基础架构组件，实现千人千面的应用组合。

6 云选型与测试

云平台选型主要从整体市场地位、整体能力、获得的专业机构证书与标准、产品生命周期的管理与发布、安全合规、整体安全防护能力、合同、商务条款、SLA、基础设施情况、可靠性、性能、市场影响力、生态合作等方面进行考虑，具体对比项目及参考评判标准请详见下表：

分类	项目	指标	备注
整体市场地位	国内的整体市场IaaS/PaaS份额	排名	参考知名分析机构最新的市场分析报告，例如IDC公共云服务市场报告、Gartner IaaS和IUS市场份额分析报告等。
	亚太的整体市场IaaS/PaaS份额	排名	参考知名分析机构最新的市场分析报告，例如IDC公共云服务市场报告、Gartner IaaS和IUS市场份额分析报告等。
	在IDC和Gartner报告中，阿里云在国内市场和亚太市场份额排名均列首位，全球市场排名第三。		

分类	项目	指标	备注
整体能力地位	中国公有云象限	排名	参考知名分析机构的能力分析报告，例如Forrester中国公有云发展平台报告、Forrester Wave：中国全栈公有云开发平台厂商评测报告等。
	产品/解决方案体系完整度	产品/解决方案数量	
	阿里云在亚太地区综合能力排名第一，拥有超过260款产品、243个行业解决方案和37个行业通用解决方案。		
基础设施	数据中心部署情况	全球/中国/可用区数量	
	阿里云在全球21个地域的63个可用区为全球用户提供云计算服务，覆盖200多个国家和地区，在中国部署多达41个可用区		
	安全合规资质	安全资质认证数量及关键安全资质满足情况	
	重大事件护航能力	国内重大事件安全护航次数、重要级别及规模等综合评价	例如G20、双11、两会、十九大等全国性重大事件护航表现
	全球公共云服务安全评估	排名	参考Forrester Wave全球公共云服务安全评估报告
	国家重点攻防演习行动情况	排名	参考获奖情况，例如公安部护网最佳攻击团队奖、最佳防守单位奖等
	阿里云保护中国超过40%的网站，防御全国50%的大流量DDoS攻击，每天成功抵御50亿次攻击，全年帮助用户修复超过833万个高危漏洞。阿里云先后通过国内外数十家权威机构的认证和审计，全力为客户构建和运行安全可控、可信赖、兼具灵活性的云服务。了解更多关于阿里云安全合规能力的详细信息，请前往阿里云信任中心。		

1、云上产品选型

计算服务选型策略

目前，主流云服务商提供的计算服务主要是弹性计算服务和容器服务，根据各自服务的特点，可以从不同维度对相应服务进行评价，具体如下表所示：

分类	项目	指标
弹性计算	硬件加速虚拟化技术	磁盘IOPS、网络PPS等
	稳定性	单机稳定性、多可用区稳定性
	通用计算实例性能	低载网络平均延时（us）
		云盘读延时（us）
		云盘写延时（us）
	租户隔离	存储实例级别I/O QoS，网络带宽和PPS实例级别隔离
		存储、网络转发卸载，不占用租户资源，租户侧资源和性能强隔离
	弹性能力	资源管理：支持按量、竞价实例、SLB、RDS实例、实例生命周期
		伸缩模式：支持多种模式（简单、步进、目标追踪、预测、定时）
		多可用区扩容策略: 优先级、均衡、成本优化
	全生命周期管理（实例创建、部署、运维）	提供跨售卖方式、跨实例规格族、跨可用区等符合企业需求的不同策略（经济、平衡、高可用等）；自动部署托管、容量管理
	规格丰富度	通用型、存储增强型、网络增强型、计算型、内存型、大数据计算/存储/网络增强型、高主频通用/计算/内存型、GPU计算型、FPGA计算型、NPU计算型等
	售卖方式	按量付费、包周付费、包年包月、预留实例、竞价实例
	运维体验	支持对对云上资源大规模自动化运维，支持自动批量执行日常运维命令
		运维操作模版化编排、支持云上资源批量复杂的自动化运维操作，包括运维任务定义、管理和执行，适合事件驱动运维、批量操作运维、定时运维任务和跨地域运维等典型场景

分类	项目	指标
弹性计算		阿里云云服务器ECS基于弹性计算10年深厚技术积淀，技术领先、性能优异、 稳如磐石。单实例可用性达 99.975%，多可用区多实例可用性达 99.995%，云盘可靠性达 99.9999999%，可实现自动宕机迁移、快照备份；单实例最高可选88vCPU，内存704GB，单实例性能最高可达到700万PPS网络收发包，35Gbps带宽；支持分钟级别创建1000台实例，多种弹性付费选择更贴合业务现状，同时带来弹性的扩容能力，实例与带宽均可随时升降配，云盘可扩容。更多详细信息，请参见云服务器ECS。（注：相关数据随阿里云产品更新而变化，此处仅供参考）
容器服务	资质与认证	Kubernetes认证服务提供商（KCSP）；通过一致性验证，拥有提供专业支持和服务的资质
	报告排名	Gartner竞争格局分析报告、Forrester分析报告
	集群管理	集群规模：单集群最大支持节点数
		支持构建集群联邦，支持联邦集群的应用和服务管理。
		支持集群定制化选项，例如自定义镜像、自定义脚本、自定义节点名称、自定义集群本地域名、自定义安全组等
		支持专有版、托管版、Serverless、边缘多种集群形态，适用不同业务场景
	弹性伸缩	支持应用从容器实例弹性伸缩到Serverless容器服务，无需扩容虚拟机资源
	运行时安全	针对运行中节点、容器实例支持动态安全检测，通知用户并提供修复建议
	应用编排&调度	支持应用生命周期管理，包括应用的创建、配置、修改、删除、伸缩等；应用配置信息应包括实例数、资源配额、服务名、服务端口、环境变量、日志配置、存储配置、自定义容器CMD参数等
		支持标签化的编排调度策略，支持根据应用需求动态调度容器；支持多维度的调度策略选择，例如资源维度（CPU、内存、GPU等）、可用性要求维度、应用的亲和性维度等
		支持容器资源配额（如容器使用的CPU数、内存大小）配置功能
	边缘	边缘端支持边缘节点服务（ENS），支持创建、加入、扩容、自动伸缩等功能
		阿里云容器服务ACK提供高性能可伸缩的容器应用管理能力，支持企业级容器化应用的全生命周期管理。整合阿里云虚拟

分类	项目	指标
容器服务		化、存储、网络和安全能力，打造云端最佳容器化应用运行环境。Gartner竞争格局国内唯一入选，Forrester报告国内排名第一。更多详细信息，请参见容器服务ACK。 阿里云弹性容器实例（Elastic Container Instance）是 Serverless 和容器化的弹性计算服务。企业无需管理底层 ECS 服务器，只需要提供打包好的镜像，即可运行容器，并仅为容器实际运行消耗的资源付费。更多详细信息，请参见弹性容器实例ECI。

存储服务选型策略

目前，主流云服务商提供的存储服务主要是块存储、对象存储、NAS等，根据各自服务的特点，可以从不同维度对相应服务进行评价，具体如下表所示：

分类	项目	指标
整体地位	全球云存储魔力象限	排名
块存储	性能要求	支持不少于三种商业化产品类型，每种类型具备不同的I/O性能
		支持在线调整性能级别，无需停机或迁移数据
		单盘性能上限IOPS、吞吐量
		磁盘读写延迟
		支持实例级别存储性能限速，不同实例规格族与配置具备不同的存储性能
	服务能力	单云盘最大容量
		支持在线扩展容量，扩容期间无需关闭虚拟机、无需卸载云盘
	售卖形态	支持多种售卖形态，例如随实例预付费、随实例按量后付费、单独购买云盘资源包、单独购买按量后付费云盘

分类	项目	指标
块存储	安全能力	支持云盘以及快照加密能力，支持使用指定KMS密钥（BYOK）加密，保证数据安全性
	数据保护	支持针对云盘在线创建快照，支持针对任意快照时间点回滚
	快照策略	支持按照自定义策略定期执行快照功能，单云盘可保留快照数量
	资质认证	GB/T 37737-2019《信息技术云计算分布式块存储系统总体技术要求》国标测试报告证明
	阿里云块存储为云服务器ECS提供的低时延、持久性、高可靠的数据块级随机存储。快存储云盘基于多副本技术，提供99.9999999%的数据可靠性；单盘高达100万随机IOPS、 4000MBps顺序吞吐；单盘支持最大32TB，单台服务器支持16块数据盘，自由配置随时扩容；快照实现简单高效的数据备份，支持云盘加密，满足合规要求。更多详细信息，请参见块存储。	
对象存储	基础功能	存储桶支持申请方付费
		支持RTMP流直推转录
		提供归档存储服务能力，历史归档数据1分钟内解冻
		支持传输加速，可加速跨地域上传和下载访问
	容灾容错	支持跨多可用区冗余能力的存储类型，将数据分散存放在同一地域（Region）的多个可用区；当某个可用区不可用时，仍然能够保障数据的正常访问
	安全合规	支持客户端加密功能
		支持访问日志导出
		支持实时日志查询
		支持WORM特性，允许用户以“不可删除、不可篡改”方式保存和使用数据
		支通过Cohasset Associates审计认证，符合美国证券交易委员会（SEC）和金融业监管局（FINRA）合规要求
	数据管理	支持对象标签，对存储的对象（Object）进行分类，并支持针对同标签的Object设置生命周期规则、访问权限等

分类	项目	指标
对象存储	数据处理	支持从对象中选择内容进行select即时查询，支持CSV、JSON格式
		支持原生图片处理服务，例如获取图片信息、图片格式转换、图片缩放、裁剪、旋转、图片添加图片、文字、图文混合水印、自定义图片处理样式、通过管道顺序调用多种图片处理功能
		支持文档处理（格式转换、文档预览）、视频截帧功能
	阿里云对象存储OSS提供海量、安全、低成本、高可靠的云存储服务，提供99.9999999999%的数据可靠性。通过RESTful API支持在互联网任何位置存储和访问，容量和处理能力弹性扩展，多种存储类型供选择全面优化存储成本。更多详细信息，请参见对象存储OSS。	
NAS	支持协议	支持NFS v3.0/v4.0、SMB2.1/3.0协议
	权限管理	支持对文件系统文件和目录的ACL访问控制
		支持对客户端按IP地址的访问控制
	快照	支持文件系统快照
	性能监控	支持对文件性能进行监控和历史数据统计
	日志审计	支持对文件系统操作进行日志审计
	性能要求	容量型单文件系统IOPS、吞吐量
		性能型单文件系统IOPS、吞吐量
		极速型单文件系统IOPS、吞吐量
	服务能力	容量在线弹性扩展，不中断业务
	售卖形态	支持多种售卖形态，包括按量付费和包年包月
	安全能力	支持文件系统数据存储加密和传输加密
	数据保护	支持文件系统备份
	阿里云文件存储NAS，可共享访问、弹性扩展、高可靠、高性能的分布式文件系统。广泛应用于容器存储、大数据分析、	

分类	项目	指标
NAS	Web 服务和内容管理、应用程序开发和测试、媒体和娱乐工作流程、数据库备份，且支持冷热数据分级存储。更多详细信息，请参见文件存储NAS。	

网络服务选型策略

目前，主流云服务商提供的网络服务，可以从不同维度对相应服务进行评价，具体如下表所示：

分类	项目	指标
云上网络	产品丰富度	产品数量
	网络质量	性能、时延
	网络隔离	网络环境隔离、逻辑隔离
	自定义网络环境	自定义IP 地址范围、网段、路由表和网关等，按需对网络进行规划和管理
	访问控制	网络权限管理、网络访问控制
	阿里云在全球19个地域部署了110多个接入点和1500多个边缘节点，可向企业提供优质的全球网络服务。基于安全隔离的专有网络架构，提供优质、功能齐全的云上网络服务，例如网络地址转换、流量分发、公网访问等。同时，提供共享带宽和共享流量包服务，服务器可以共享流量和带宽，优化网络成本。更多详细信息，请参见专有网络VPC。	
	全球企业级负载均衡网络设备市场份额	排名
	协议支持	支持多种协议的流量分发
	容灾保障	健康检查、多可用区部署、集群部署
	性能保障	性能保障实例、超大性能规格
	阿里云负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务，支持TCP、UDP、HTTP、	

分类	项目	指标
云上网络	HTTPS协议的应用流量转发，通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。更多详细信息，请参见负载均衡。	
网络接入	传输安全	通信数据安全，无私密数据窃取风险，数据安全可靠
	稳定可靠	设备级容灾、链路级容灾、接入点容灾
	接入方式	物理专线接入、Internet接入、4G接入
	阿里云提供高速通道、智能接入网关、VPN网关多种方式，帮助企业打通云上云下系统和数据，消除信息孤岛。为不同规模、不同地域、各行业的企业机构提供云下网络（IDC、总部、分支、门店）到阿里云上安全、可靠、灵活的网络连接。更多详细信息，请参见智能接入网关。 通过将云下IDC、门店、分支等接入和云上网络，阿里云还提供全球跨地域专有网络间互联，帮助企业快速构建合法合规的混合云和分布式业务系统网络。更多详细信息，请参见云企业网。	

数据库服务选型策略

目前，主流云服务商提供的数据库服务，主要包括RDS、Redis、ADB for MySQL、数据库备份、SQL Server等服务，这些服务从不同维度对相应服务进行评价，具体如下表所示：

分类	项目	指标
整体	数据库挑战者象限	排名
	数据生态完备情况	产品、工具、服务体系化布局
	金融级数据安全保障	资质认证
RDS	可用区资源	多可用区（至少两个可用区）
	数据库资源规格	CPU核数、内核空间，最大规格要求CPU超过100核

分类	项目	指标
RDS	用户独有规格	可独有整台物理机器的独占型规格
	存储空间	提供高I/O能力选项存储类型和数据多副本保存的存储类型
	网络连接	支持云环境内网连接，支持公有外网连接
	临时升级	支持临时升级资源规格，到期后自动降回原规格
	实例回收站	支持实例回收站，在实例删除后一段时间内可通过回收站重建实例，数据保持和删除时刻一致
	MySQL版本	支持主流MySQL版本，包含5.5、5.6、5.7、8.0
	群组模式管理资源	支持群组模式管理数据库资源
	在线升级存储空间	支持业务无中断在线方式升级数据库存储空间
	迁移可用区	支持在同地域内不同可用区之间迁移数据库资源
	性能洞察	提供MySQL实例负载监控、关联分析，通过实时会话指标诊断数据库性能糟点，并且能诊断出具体SQL语句
	实时数据库会话管理	支持通过页面结束数据库会话，支持下发数据库限流指令
	空间分析	提供通过页面对数据库空间进行分析、发现异常空间增长表、数据库空间增长趋势和可用时长预测
	全量SQL分析	提供分析数据库全量SQL能力、TOP SQL分析
	SQL优化建议	提供SQL语句优化解决方案，包括改写建议、索引设置建议
	高并发更新	提供高并发更新能力，单行根据主键更新能力
	数据加密	支持数据加密功能，支持透明数据加密、用户自带加密秘钥能力、轮转用户秘钥
	存储盘加密	支持对数据存储盘加密、用户自带加密秘钥
	国密算法SM4	提供使用国密算法SM4加密数据库数据

分类	项目	指标
RDS	数据库备份	支持数据库备份，备份文件可长期保留；支持全量备份实例，支持通过日志增量备份实例；支持手工备份；支持备份文件同步到异地
	自动化库表级恢复	支持自动化备份，且备份粒度精确到库表
	快照备份恢复	支持通过快照备份数据库，支持通过快照恢复数据库，且实现秒级恢复
	等保三级	通过国家等保三级要求
	阿里云关系型数据库RDS基于阿里云分布式文件系统和SSD盘高性能存储，RDS支持MySQL、SQL Server、PostgreSQL和MariaDB TX引擎，并且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案。更多详细信息，请参见云数据库RDS。	
SQL Server	数据库版本	支持MircoSoft SQL Server Web版、标准版、企业版
	数据库连接	支持多个只读实例统一的负载均衡连接地址；支持在只读实例负载均衡连接中，设置每个只读实例的读请求处理权重
	数据库可用性	支持SQL Server实例跨两个可用区（机房）部署主备实例，防范单机房故障
	数据管理	支持SQL Server数据库用户信息管理，包括但不限于创建、删除账号，设置账号对数据库的管理权限；支持SQL Server数据库用户数据管理，包括但不限于数据库创建、删除，数据库字符集选择等
	数据安全性	支持数据写入磁盘后，单独对磁盘进行加密设置
		支持设置TDE数据落盘加密功能
		支持设置SSL链路加密访问
		支持对数据库连接后的SQL 操作行为进行数据审计，包括但不限于执行的账号、SQL 语句及服务器IP
	性能优化	支持磁盘空间分析管理，包括但不限于以图表形式展示实例的空间使用情况，如空间使用率、数据日志比、TOP 5数据库空间占用等数据

分类	项目	指标
SQL Server	性能优化	支持以界面化展示实例中缺失的索引信息，导出创建缺失索引的脚本文件
		支持索引使用率查询功能，包括已经存在的索引的使用率情况、索引的碎片率
		支持实时TOP SQL和历史TOP SQL查询功能
		支持TOP Objcets查询功能，展示SQL Server用户实例中对象级别（存储过程、函数、触发器等）的性能问题
	RDS SQL Server不仅拥有高可用架构和任意时间点的数据恢复功能，强力支撑各种企业应用，同时也包含了微软的License费用，减少额外支出。更多详细信息，请参见云数据库RDS。	
Redis	跨地域容灾	支持构建跨地域容灾架构
	混合存储	支持磁盘缓存，提供冷热数据分离技术，单实例最高支持缓存大小
	性能增强	社区版性能比较
	规格指标	缓存规格、集群架构、QPS
	监控告警	支持全架构监控、告警设置
	端口号	支持端口号修改
	访问控制	支持白名单、访问控制管理能力
	审计日志	支持审计日志服务，内核层面记录所有更新操作，方便追溯，并支持高危命令记录，例如flush all等
	缓存分析	支持大Key缓存分析，能够定位大Key
	持久化	支持RDB、AOF两种持久化模式，AOF支持落盘开关设置及增量备份开关设置
	按时间点恢复	开启增量备份后支持按时间点恢复实例（克隆）
	备份下载	支持RDB、AOF文件下载
	可用区迁移	支持可用区一键迁移，灵活资源调配
	公网访问	支持公网连接

分类	项目	指标
Redis	代理访问	支持代理连接，兼容多Key命令
	免密访问	支持信任网络免密访问，降低内网访问认证成本
	云数据库Redis版兼容开源Redis协议标准、提供混合存储的数据库服务，基于双机热备架构及集群架构，可满足高吞吐、低延迟及弹性变配等业务需求。更多详细信息，请参见云数据库Redis版。	
云原生数据库	集群规模	支持大集群规模
	单集群容量	单集群可支持不少于300个数据库实例（Database）
	单集群容量	单集群可支持单库不少于1PB数据量
	单数据库容量	生产环境单数据库支持1万张表以上
	行列混存	支持表级别配置存储模式
	全索引	支持智能全索引，任意列支持建索引
	性能监控	支持细粒度的运行报表,包括访问量、每秒查询次数、慢查询、超时等指标
	SQL兼容	兼容MySQL协议
	查询性能	生产环境支持万亿级数据表查询
		生产环境支持千亿级数据表关联分析
	写入性能	单节点写入速度
	阿里云云原生数据仓库AnalyticDB MySQL版，全面兼容MySQL协议以及SQL:2003 语法标准，可对海量数据进行即时的多维分析透视和业务探索，快速构建企业云上数据仓库。产品规格按需可选，基础版成本最低，适合BI查询应用；集群版提供高并发数据实时写入和查询能力，适用于高性能应用；弹性模式版本存储廉价按量计费，适用于10TB以上数据上云场景。更多详细信息，请参见云原生数据仓库AnalyticDB MySQL版。同时可参阅云原生数据仓库 AnalyticDB PostgreSQL 版。	
数据库备份	全量备份	支持MySQL逻辑全量备份，支持5.5、5.6、5.7、8.0版本
		支持PPAS逻辑全量备份，支持9.3、10版本
	增量备份	支持MySQL逻辑增量备份

分类	项目	指标
数据库备份	备份特性	支持通过备份工具自动备份到分布式存储
		支持本地机房数据库备份并恢复到云数据库
		支持备份源配置
		支持目标存储配置
		支持备份对象配置，支持整个实例、多个数据库、单个数据库、多张表、单表、视图、存储过程、触发器等
		支持备份频率配置
		支持备份开始时间配置
		支持增量备份开关配置
		支持备份保留时长配置，到期自动删除
		支持备份集转储到低频存储配置，备份集在标准存储中保留超过一定时间后转存到低频访问存储
		支持备份集转储到归档存储配置，备份集在低频访问|标准存储中保留多超过一定时间后转存到归档冷备存储
		支持备份计划运行信息查看
		支持备份计划生命周期查看
		支持全量备份任务列表查看
		支持增量备份任务详情查看
	全量恢复	支持MySQL逻辑全量恢复，支持5.5、5.6、5.7、8.0版本
		支持PPAS逻辑全量恢复，支持9.3、10版本
	增量恢复	支持MySQL逻辑增量恢复

分类	项目	指标
数据库备份	恢复特性	支持恢复时间点配置
		支持恢复目标数据库配置
		支持恢复数据库对象配置
		支持同名表冲突处理功能，例如：遇到同名对象则失败（遇到同名对象，则恢复失败，用户要手工处理目标数据库同名对象）；遇到同名对象则跳过（同名对象不执行恢复，不同名对象正常执行恢复）；遇到同名对象则重命名（同名对象在恢复时会被重命名，恢复目标数据库上原有同名对象不动）
		支持恢复任务列表查看
		支持恢复任务详情查看，包含全量结构前置恢复、全量数据恢复、全量结构后置恢复、增量日志恢复步骤
	阿里云数据库备份DBS为数据库提供连续数据保护、低成本的备份服务。DBS为多种环境的数据提供强有力的保护，包括企业数据中心、其他云厂商、混合云及公共云，可实现实时的数据备份,在线数据发生变化时，数据库备份会获得变更的数据，并将数据实时写入云存储，实现秒级RPO的数据备份。更多详细信息，请参见数据库备份DBS。	

大数据平台选型策略

目前，主流云服务商提供的大数据平台服务，可以从整体情况、架构、数据装载与管理、计算模型、安全性、性能表现、集群资源、授权合规、数据集成平台等方面的不同维度进行评价，具体如下表所示：

分类	项目	指标
整体	大数据数仓产品组合	排名
	大数据计算性能	排名
	成熟度和稳定性优越	商用时长

分类	项目	指标
架构	核心技术	自主研发，拥有核心技术
数据装载与管理	存储压缩	高效数据压缩存储，压缩效率和数据格式相关，压缩比；对冷数据支持归档操作
	生命周期	分区级别的数据生命周期管理功能，过期数据系统自动清理
计算模型	SQL	参数化视图，支持传入任意表或者其它变量，定制视图行为
	MapReduce	支持MapReduce单机调试；支持超多规模计算，最大Mapper支持个数，最大Reduce支持个数；支持扩展MapReduce增强计算过程；支持MapReduce计算的多表输入和输出
	图计算	支持面向迭代的图计算处理框架
	Spark	在统一的计算资源和数据集权限体系之上，支持Spark计算框架，满足更丰富的数据处理分析场景。
安全	细粒度权限控控制	支持列级权限控制
性能测试	TPC-DS测试	相同数据量、相同资源，相同测试集同等标准情况下，整体测试时间性能
集群资源	规模	单集群支持并行作业服务器规模，同一套服务支持多集群调度
授权合规	授权合规	具备国家颁发的软件著作权证书，具备自主知识产品证明
		技术方案应具有不短于3年的实际应用案例
		满足信息系统安全等级保护等级要求（等保三级）
集成平台	数据集成	支持传输速率控制、并发控制
		支持读取数据时数据过滤
		支持脏数据监控
		支持实时同步MySQL、Oracle等
		支持复杂网络情况下对异构的数据源进行数据同步与集成
	数据开发	支持智能代码提示，包括语法关键词、元数据信息等

分类	项目	指标
集成平台	数据开发	支持代码格式化、折叠、缩略图展示
		支持以可视化的形式展现SQL代码的内部结构
		支持代码全文检索
		支持手动触发的手动调度模式（手动业务流程）
		支持业务流程级别、节点级别的参数设置，即用不同的参数输入，运行获得不同的数据分析结果
		支持SQL组件概念，将相同的SQL逻辑写成模板
		支持发布控制，经过审核后方可将代码发布至生产项目，实现开发和生产环境隔离
		支持大数据相关节点ODPS SQL、ODPS MR、Spark on ODPS、SQL组件等
		支持数据集成节点
		支持Shell节点、虚节点
		支持机器学习节点
		支持流程控制节点，包括判断分支、循环、遍历、赋值
		支持跨租户依赖节点
		支持其他引擎扩展（自定义节点）
	数据资产管理	支持跨组织的元数据展示与授权，加速部门间的数据共享
		支持云厂商自研大数据计算服务
		支持数据资产搜索，可对资产名称、描述进行模糊搜索
	数据服务	支持通过可视化配置，将各类数据库中的数据表快速生成API服务；对于复杂API，支持自定义SQL查询语句，支持多表关联查询等能力
		支持API注册，将已有的API统一注册到数据服务平台
		支持统一服务总线，统一发布API，支持鉴权、流控等能力

分类	项目	指标
集成平台	数据服务	支持丰富的数据源，包括MySQL、Oracle、SQL Server、PostgreSQL、RDS等。
	数据安全	支持数据安全等级自定义，包括绝密、机密、秘密数据等定义
		支持根据数据安全等级，发现和定位敏感数据，明确其在数据资源平台上的分布情况，根据定义的敏感数据类型自动发现敏感数据，并为其分级分类
		支持数据访问审计，记录审计特权用户的访问记录，包括访问时间、执行操作等
		支持数据脱敏，包含有敏感信息的数据库，在不限制用户访问的情况下，对敏感信息进行动态遮蔽
	平台管理	支持以工作空间维度管理对象、成员、角色与权限
		工作空间支持设置管理员、开发、运维、部署、访客等角色
		支持简单模式项目
		支持标准模式项目
		支持云厂商自研大数据计算引擎
阿里云飞天大数据平台是阿里巴巴10年大数据建设最佳实践的结晶。从丰富多样的大数据计算引擎，到高效易用的大数据研发平台，飞天大数据平台拥有非常齐全的产品体系，满足各种业务场景下对大数据多方面的需求。飞天大数据平台刷新多项世界纪录，向世界展示中国能力，被称为新一代的“大国重器”。同时对存储与计算进行极致优化，打破性能与成本的线性关系。更多详细信息，请参见飞天大数据平台。		

流量产品选型策略

目前，主流云服务商提供的流量产品，主要有CDN服务和云通信服务，根据这类服务需求，可以从不同维度进行评价，具体如下表所示：

分类	项目	指标
CDN	节点列表	服务节点分布在全球各区域和主要运营商的骨干和边缘节点
	宽带证明	拥有充足的带宽资源和全球加速能力
	宽带储备	拥有充足的带宽和设备处理能力，在必要时能实现及时高效的扩容，能够应对至少20T以上的带宽突发需求，满足重要时期或重要事件的访问需求，并在突发大流量访问的情况下能够保证服务质量不受影响
	技术要求	支持全链路HTTPS、支持HTTPS无证书方案、支持企业级免费证书、支持HTTPS双向加速
		支持图片鉴黄，自动检测通过CDN加速的图片是否涉黄，记录违规图片的URL供用户导出和删除
		回源支持多源优先级设置、私有Bucket回源授权、协议跟随回源
		支持P2P技术CDN分发，以P2P技术为基础，通过挖掘利用边缘网络海量碎片化闲置资源而构建的低成本高品质内容分发网络服务
		拥有全站加速能力，自动分离动静态文件，通过最优路径选择和协议优化提升动态文件的传输能力
		支持四层协议加速，支持TCP和UDP协议加速
		对海外到国内的加速支持专线隧道功能
		支持WebSocket协议
		具备静、动态内容分离技术，对网站静、动态内容分别采用相应加速技术进行CDN加速服务，保证动、静态内容安全、有效的实现快速访问
		动态数据回源实现基于运营商的负载均衡，即某一运营商接入用户优先回同一运营商源站
	安全防护	对于网络安全事件从发现、到告警、再到抵御及事后处理的各项流程应具有明确规范，拥有成熟的安全措施及应急方案
		提供抗DDoS攻击解决方案，可以抵御SYN Flood、UDP Flood、ACK Flood、CC等多种类型的DDoS攻击。必要时可对攻击流量进行清洗，并保证用户的正常访问不受影响

分类	项目	指标
	阿里云CDN服务拥有超过2800全球节点、全网带宽输出能力达130Tbps、覆盖全球六个大洲，支持国内主流运营商，关键性能指标业内领先，包括缓存命中率超过95%、响应时间达到ms级、加速视频时的视频流畅率超过95%。更多详细信息，请参见CDN。	
云通信	短信服务	资源能力（国内短信、国际短信）
		平台并发能力
		安全能力
		注册资本
		公司成立时间
		从事短信业务时间
		社保证明人数
		财务表现（营业收入、短信业务收入）
		行业项目案例
		短信平台软件著作权
		失信情况
		增值电信业务许可证、电信网码号资源使用证书
		相关认证
	阿里云短信服务拥有强大的高并发处理能力，双11期间一天内发送6亿条短信，服务2亿用户。国内验证短信秒级触达，到达率99%；国际/港澳台短信覆盖200多个国家和地区，安全稳定，广受出海企业选用。更多详细信息，请参见短信服务。	

中间件选型策略

目前，主流云服务商提供的中间件服务主要包括分布式应用服务、消息队列、云总线（API）、应用实时监控服务，这些服务可以从不同维度进行评价，具体如下表所示：

分类	项目	指标
分布式应用服务	无缝迁移	支持开源Dubbo和SpringCloud框架，应用无需修改任何代码即可迁入，并且支持服务不中断的迁移方案
	混合云能力	支持混合云的应用部署和集群管理能力，包括管理用户自建IDC以及其他云厂商机器的能力；支持在同一个控制台完成对混合云所有机器和集群的管理和监控，支持应用在混合云的部署和完整生命周期管理
	全链路灰度	在微服务的场景下，支持无代码侵入的全链路的灰度方案，自动对流量进行打标；支持控制灰度流量仅运行在灰度环境中，并支持在灰度环境仅部署发生变更的应用
	多环境逻辑隔离	支持在一个账号下通过命名空间隔离的方式实现多套环境并存，例如多套测试环境的并存；命名空间支持服务名逻辑隔离，不同命名空间里的服务名可以重复但完全隔离，不引起调用混乱，应用无法发现和调用其他命名空间中的服务。
	软件著作全登记	获得国家软件著作权登记
	阿里云企业级分布式应用服务 EDAS提供应用开发、部署、监控、运维等全栈式解决方案，同时支持 Spring Cloud、Apache Dubbo（以下简称 Dubbo ）等微服务运行环境，提供从创建到运行的应用全生命周期管理服务，包括应用的发布、启动、停止、扩容、缩容和删除等服务。更多详细信息，请参见企业级分布式应用服务EDAS。	
消息队列	消息过滤	支持消息的 Tag 过滤方式，提高消费者的消息投递效率并降低资源成本
	多租户管理	集群支持多个虚拟实例管理，实例拥有独立的命名空间
	消息类型	支持顺序消息，按照消息的发布顺序进行顺序消费（FIFO），支持全局顺序与分区顺序；
		支持分布式事务消息，分布事务功能，既实现系统间的解耦，又保证数据的最终一致性
	消息治理	支持全程追踪消息在生产者、消息服务器、消费者之间的流动轨迹，并将数据进行汇聚分析后可视化输出
		支持 Topic、Message ID、Message Key多维度消息查询
		支持对已消费过的消息进行重新回放或清除堆积的消息
	容灾能力	多地域部署，支持高可用互备

分类	项目	指标
	阿里云消息队列提供低延迟、高并发、高可用、高可靠的分布式消息中间件服务，采用Region化、多可用区、分布式集群化部署，确保服务高可用，可用性高达99.95%，即使整个机房不可用仍可正常提供消息服务；同步双写、超三副本数据冗余与快速切换技术确保数据可靠，数据可靠性高达 99.99999999%；支持的消息类型涵盖普通消息、顺序消息（全局顺序/分区顺序）、分布式事务消息、定时消息/延时消息。更多详细信息，请参见消息队列。	
云服务总线	最大吞吐能力	在简单协议场景下，例如把已有HTTP服务开放成HTTP API，假定已有稳定服务加上网络延迟响应非常快，例如≤1毫秒，单个服务请求消息大小为1KB字节，要求API服务节点每CPU核QPS≥1000
	最大处理容量	可水平线性扩展，可管理的产品自身服务节点总数≥1000，支持发布API总数量≥10万个
	多协议适配	支持适配多种协议，包括REST Web Service、SOAP Web Service、Dubbo等
	多个环境级联能力	支持一次发布实现多个产品服务集群之间接力发布，实现服务跨多个环境的快捷发布
	阿里云云服务总线CSB提供平台化的应用集成和服务开放能力，帮助企业打通整合内外新旧业务系统，实现跨环境、跨归属应用系统之间的互通集采用形成组合方案。更多详细信息，请参见云服务总线CSB。	
应用实时监控服务	基础架构监控	支持应用节点的基础性能收集，包括CPU、Memory、Disk、Network等
	RPC框架支持	支持基于主流同步、异步调用框架，例如HSF、Dubbo、HTTP RESTful框架的分布式链路跟踪
	数据库监控	支持抓取SQL语句运行时长和错误，支持抓取绑定变量
	消息队列监控	支持按消息topic维度展示请求数，响应时间和错误数
	诊断能力	支持通过自动线程剖析定位慢调用方法
	报警能力	支持默认提供应用各维度指标的报警
	权限控制能力	支持租户级别应用隔离的能力
	日志关联分析能力	支持根据业务关键字（如用户名）定位出相应的应用日志和应用调用链路
	通过API接口提供应用监控数据	支持通过API接口提供metric指标数据

分类	项目	指标
	应用实时监控服务包含前端监控，应用监控和Prometheus监控三大子产品，涵盖浏览器、小程序、App、分布式应用和容器环境等性能管理，帮助企业实现全栈式的性能监控和端到端的全链路追踪诊断。更多详细信息，请参见应用实时监控服务ARMS。	

安全产品选型策略

目前，主流云服务商提供的安全产品主要包括，WAF、DDoS防护、堡垒机、云安全中心等，这些服务可以从不同维度进行评价，具体如下表所示：

分类	项目	指标
WAF	整体市场地位	排名
	资质/认证	公安部安全产品销售许可证（WAF）
	多协议、多版本防护	支持HTTP、HTTPS、HTTP2、Websocket协议；支持HTTP 0.9/1.0/1.1/2.0版本，支持HTTP2协议流量转发与防护；支持HTTP回源以及HTTPS强制跳转
	支持非标端口的防护	支持常见非标端口防护
	全量访问日志查询	支持网站全量访问日志的存储与在线检索功能；支持通过API接口将日志导出到本地或第三方SIEM平台；支持最近一周的全量访问日志查询；支持基于源IP、URL关键字、Cookie、Referer、User-Agent、X-Forwarded-For、服务器响应状态码、和是否为攻击属性等属性的智能搜索和详情查看功能并提供日志下载功能
	防扫描	支持短时间集中Web攻击的IP自动封禁、防目录遍历、并支持对时间、访问频率；支持封禁时长的自定义设置；支持对常见扫描器的渗透测试拦截；支持无需修改代码修改的滑块验证接入方式
	智能防护引擎	基于深度学习引擎的智能防护算法，有效地防护传统正则引擎不能检测到的未知攻击

分类	项目	指标
WAF	主动防御能力	支持使用大数据智能算法能力对历史的流量进行自动学习分析，形成合法的白流量画像，实现用户流量识别防护
	IPV6地址防护	支持IPv6的业务安全防护、并支持接入网站一键支持IPv6
	阿里云Web应用防火墙通过对网站或者APP的业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。更多详细信息，请参见Web应用防火墙。	
DDoS防护	资质/认证	公安部安全产品销售许可证（DDoS）
	机房/带宽	清洗中心机房数量、支持BGP带宽资源；防护带宽资源，单机房带宽资源；支持机房自动容灾、专线回源，国内平均访问时间延迟20ms以内
	核心能力	DDoS最大防护能力不低于1Tbps
		BGP带宽防护资源，保底防护能力大于600Gbps
		CC防御能力大于100万QPS
	接入能力	网站类业务：支持HTTP/HTTPS、 Websocket/ Websockets协议类型，支持HTTPS协议、HTTP2.0协议版本，支持80、8080、443、8443以外的非标准端口 非网站类业务：支持TCP和UDP协议；支持端口映射，即转发端口和回源端口可以不同
	调度能力	支持CNAME自动调度、支持与CDN、WAF等服务结合使用
	防护选项	支持智能AI防护
		支持针对IP和域名的黑白名单、按区域封禁攻击流量、CC安全防护模式自定义、CC安全防护规则自定义
		支持HTTP协议精准匹配防护规则，可按 IP、URI、Cookie、Referer、User-Agent、X-Forwarded-for、Content-Type、Content-Length、Post-Body、Http-Method、Header、Params等HTTP头部字段进行精准匹配并过滤掉攻击流量

分类	项目	指标
DDoS防护	防护选项	支持黑洞自助解除
		支持弹性扩展防护带宽
	阿里云DDoS防护服务以阿里云覆盖全球的DDoS防护网络为基础，结合阿里巴巴自研的DDoS攻击检测和智能防护体系，向企业提供可管理的DDoS防护服务，自动快速的缓解网络攻击对业务造成的延迟增加、访问受限、业务中断等影响，从而减少业务损失，降低潜在DDoS攻击风险。阿里云DdoS防护在全球建设DdoS清洗中心，防护网络总带宽超过10Tbps，每天平均防护云上DDoS攻击2500次，成功防护1Tbps攻击。更多详细信息，请参见DDoS防护。	
堡垒机	资质/认证	公安部安全产品销售许可证（堡垒机）
	部署要求	支持系统盘与数据盘分离部署，操作系统存储在系统盘中、数据存在数据盘中，防止因操作系统出现故障造成数据损坏
	设备管理要求	支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，支持自动授权
	身份认证要求	支持与GET、POST、SOAP发送方式的HTTP短信网关平台进行联动，实现短信动态口令双因素认证机制
		支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令
	运维方式要求	支持使用本地的winscp/flashFXP/SecureFX等客户端工具登录堡垒机访问SFTP/FTP设备
		支持直接使用登录堡垒机的AD/LDAP用户及密码直接自动登录到服务器
	阿里云堡垒机支持集中管理资产权限，全程记录操作数据，实时还原运维场景，助力企业用户构建云上统一、安全、高效运维通道；保障云端运维工作权限可管控、操作可审计、合规可遵从。更多详细信息，请参见堡垒机。	
云安全中心	安全资质	公安部安全产品销售许可证
	漏洞检测&修复	支持Linux软件漏洞检测&修复、Windows系统漏洞检测&修复
	基线检查	支持Windows、Linux 主机基线检查，符合等级保护2.0、CIS标准
	云平台配置检查	支持云平台安全检查
	二进制病毒检测	支持恶意进程（云查杀）实时检测、本地检测、云端检测
		支持多AV引擎、机器学习、深度学习、安全沙箱等引擎检测能力

分类	项目	指标
云安全中心	入侵检测	支持检测Bash反弹、Powershell异常指令、进程异常写文件操作、进程异常行为、敏感文件篡改、异常网络连接、应用入侵事件、DDoS攻击事件等
	自动化攻击溯源	支持自动化定位攻击源、攻击链、入侵原因，并以可视化的形式展示
	日志分析	支持全量日志分析（网络、主机、云产品）
	安全大屏	安全大屏支持自定义选配场景
	阿里云云安全中心是一个实时识别、分析、预警安全威胁的统一安全管理系统，通过防勒索、防病毒、防篡改、合规检查等安全能力，帮助企业实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产和本地主机并满足监管合规要求。更多详细信息，请参见云安全中心。	

其他产品选型策略

目前，主流云服务商提供的其他产品和服务主要包括，日志服务、账号管理、云防火墙、MongoDB等，这些服务可以从不同维度进行评价，具体如下表所示：

分类	项目	指标
日志服务	功能	支持csv、分隔符、正则表达式等文件采集
		支持客户端对日志进行结构化解析，支持上传原始文件
		支持syslog协议采集
		支持MySQL、Redis、K8S、Windows Event、HTTP Status、系统 (CPU/内存/磁盘/网络) 信息采集
	数据加工	支持采集端进行数据加工
		支持对采集字段名、内容等进行过滤

分类	项目	指标
日志服务	数据加工	对IP等字段提供地理位置信息
		支持对字段进行脱敏
	支持平台	支持多平台,包括Linux、Windows、AIX、容器K8S、嵌入式
	配置管理	支持集中式配置管理
	自动恢复	重启和升级时保证数据不丢，采集连续
	SDK	支持C++、Java、PHP、Go等多语言
	数据加工	支持解析、展开、跳转逻辑、变量赋值等数据解析能力
	监控报警	支持便捷配置监控与报警
	阿里云日志服务是行业领先的日志大数据解决方案，一站式提供数据收集、清洗、分析、可视化和告警功能。更多详细信息，请参见日志服务。	
账号	子账号管理	支持灵活的账号管理分配机制，允许同一个企业帐号下拥有多个用户组和子帐号，并可分配不同权限以控制子帐号对云资源的访问
	多租户隔离	不同部门、不同项目间的云端资源在管理上需互相隔离
	账单管理	管理员可查看单个账号和企业总账号的历史资源消耗清单和余额信息
	SSO单点登录	集成企业自有账号体系
	阿里云访问控制RAM 支持建设子账号体系，帮助企业以更精细的粒度（资源对象级、API操作级）管理云端资源的访问权限，实现最小授权原则。还支持根据请求源IP 地址、日期/时间、资源标签等属性创建更精细的资源访问控制策略。更多详细信息，请参见访问控制RAM。 阿里云应用身份服务（IDaaS）是一个集中式身份管理服务，为企业提供统一的应用门户、用户目录、单点登录、集中授权、以及行为审计等中台服务。IDaaS 支持 SAML、OIDC、CAS 等常见身份联邦协议，也可以与钉钉通讯录、AD、HR系统等身份源打通，做到统一的身份权限管理和应用访问控制。更多详细信息，请参见应用身份服务。	
云防火墙	部署	支持SaaS化部署，无需改变网络结构；支持内置系统冗余；支持性能平滑扩展
	访问控制	支持防火墙安全控制，控制入流量和出流量的访问；支持支持基于域名的访问控制

分类	项目	指标
云防火墙	IPS	支持入侵防御（IPS）功能
	日志	支持安全事件日志、流量日志和系统日志，保存6个月
	流量可视化	支持互联网到业务的访问流量分析
	流量可视化	支持业务主动外联分析
	流量可视化	支持被阻断访问的分析
	可视化	支持基于安全组的流量可视化
	阿里云云防火墙是一款SaaS化云原生防火墙，帮助企业全面梳理云上资产的互联网暴露和风险情况，一键防护；提供IPS虚拟补丁可智能防御高危漏洞；集成威胁情报，支持阻断主动外联行为、业务间访问关系可视，网络流量审计，是企业满足等保合规需求的必备选择。更多详细信息，请参见云防火墙。	
MongoDB	分片管理	支持Sharding
	架构	支持集群、副本集能力
	域名管理	支持域名访问
	vpc免密	支持VPC内免密访问
	秒级监控	支持秒级监控
	版本覆盖	支持3.4/4.0/4.2版本
	数据加密	支持TDE数据加密、支持用户自带密钥，保障数据安全
	审计	支持审计日志服务
	只读实例	支持追加只读实例
	按时间点恢复	支持按时间点恢复、克隆实例，保障数据最大可靠性
	库表级恢复	支持库表级恢复
	性能洞察	提供实时性能展示、性能趋势对比、回话管理、慢查询管理、索引推荐等综合管理能力

分类	项目	指标
MongoDB		阿里云云数据库MongoDB版支持ReplicaSet和Sharding两种部署架构，具备安全审计、时间点备份等多项企业能力。更多详细信息，请参见云数据库MongoDB版。

2、上云验证性测试

为了保证上云效果，需要通过专用的演练工具来执行验证性的测试，以便于提前发现问题并处理，以及应急预案的正确执行。

阿里云的应用高可用服务（AHAS）就是这样一款具备验证性测试功能的演练工具。其主要功能特性介绍如下：

- 一款专注于提高应用高可用能力的SaaS产品，提供应用架构自动探测、故障注入式高可用能力演练和一键应用限流降级等功能，可以快速低成本地提升应用可用性。
- 可提供基于真实线上故障的高可用能力演练计划、实行与复盘服务、根据客户的应用架构智能推荐故障演练场景。

迁移上云的行动建议和实操指南，以及迁移之后如何构建云上 IT 治理、云上管理体系

6 企业全面上云成功路径与实践
迁移上云与云上治理

1 迁移上云

1 待迁系统调研

企业中现有的应用系统具有各自独特的属性，迁移上云时，会对云有各种不同的需求，导致云的采用将因产品组合而异。对待迁移系统进行调研，掌握其现状是将系统迁移上云的至关重要的第一步。

指导系统调研的方法主要包括：

建立程序角色

目的：

- 基于技术和非技术属性构建每个应用程序的多维视图。

关键行为：

- 确定可以用于量化评估的特征值。

- 将范围内的程序数据规范化，以确定应用的角色。
- 与利益相关者验证假设和数据的规范化。

确定影响范围

目的：

- 先了解整个程序集，然后筛选出到可于云适配性量化评估的程序。

关键行为：

- 从各种来源收集数据，以建立程序和基础架构的统一视图。
- 确定云适配性量化评估范围内的程序。

规范化

目的：

- 对程序角色的特征数据应用适配性规则，以对所有评估范围内的程序量化分析。

关键行为：

- 通过基于重要性和数据质量可信度来配置适配性规则。
- 规范化本地和云评分以生成0–10的分数，其中0表示最不适合云实施，10表示最适合云实施。

适配性评估

目的：

- 为范围内的程序生成适应性频谱

关键行为：

- 为每个范围内的程序量化计算单独的本地和云适配性分数。
- 与IT领导人，程序使用者及开发者沟通合作，获取评估反馈。

1、业务类关键属性

业务类关键属性	
业务目标评估	**安全合规评估**
• 上云收益 • 市场需求 • 可用性要求 • 业务连续性要求 • 是否为关键/核心应用 • 业务应用属性 • SLA等级 • 高可靠性要求 • 灾备要求 • 功能要求 • 用户数预估 • 业务增长预估 • 对用户的影响 • 组织结构支持 • 合作伙伴支持	• 物理安全 • 硬件安全 • 主机安全 • 网络安全 • 虚拟化安全 • 数据安全 • 账号安全 • 业务安全 • 安全监控 • 国家/地区合规要求 • 行业合规要求 • 企业内审合规要求

2、技术类关键属性

技术类关键属性		
业务运行环境评估		**IT基础架构评估**
• 技术架构 • 停机窗口 • 高可用 • 灾备架构	• 硬件相关性 • 源代码是否可用 • 编程语言 • 程序模块耦合度	• 外部依赖性 • 应用扩展性 • 是否使用分布式架构 • 应用发布流程 • 部署架构 • 应用稳定性 • 使用虚拟化 • 存储设备使用 • CPU/内存使用率 • 物理设备依赖性 • 操作系统上云兼容性 • 中间件上云云兼容性 • 数据库上云兼容性

应用系统清单

通常在进行云迁移期间，需要通过扫描工具收集应用系统清单，某些工具还可以创建网络映射和依赖项，以帮助定义工作负荷的对齐方式。

如果企业系统非常庞大，应用之间耦合多，各系统的负责部门不同，人工收集的方式难免会有疏漏，难以完整厘清所有应用系统以及系统间的复杂依赖关系。

应用系统清单很难通过一次性的盘点完成。我们强烈建议云COE团队邀请相关业务责任人和用户参与确认系统清单的完整性，也可以使用一些网络流量和依赖关系分析来识别正在运行但不在清单中的应用系统资产。

阿里云提供针对企业上云场景提供应用发现服务（Application Discovery Service），满足企业在迁云阶段的评估、规划、建设、迁移的需求评估。采用无侵入式采集技术，不影响在线业务的性能前提下从主机和进程两个维度构建架构拓扑，自动分析识别主机和进程信息、资源使用水位以及各应用和组件之间的依赖关系。更多详细信息，请参见应用发现服务。

2 迁移计划与策略

1、应用迁移评估

在应用系统迁移过程中，往往无法对所有应用都采用同一种迁移策略，甚至存在一些不能被迁移的应用，因此需要使用云适应性评估模型（6R）进行评估，主要内容如下：

退役Retire

将要退役/结束生命周期的应用，其用户可能会迁移到其它应用上。

保留Retain

保留下来的应用，作为非云基础设施的一部分。

替换Replace

将会被其它应用（或者是应用集）所取代的应用，可以购买和使用商业软件或者第三方服务，作为一个服务进行交付。

移植Rehost

应用组件是“云友好”，也就是说比较容易移植到云环境上，比如在虚拟化以后只需要很少的应用变化。

重建平台Replatform

应用组件不在云上或者不符合成本效益，因此需要对基础设施和平台进行调整。

重构Refactor

应用组件并不适用于云，并且/或者根据业务需求要进行特定的改变。

2、应用迁移方法

将新的应用系统直接部署在云计算环境中或将原有系统迁移到云计算环境中是两种主要信息系统的云化改造路径，对其实现难度的评估是对应用系统进行云化改造风险与收益评估的重要手段。整个业务系统的云化分析过程需要从包括基础设施支撑环境改造、操作系统平台变更、平台软件绑定分析、IP地址依赖性消除、API重构、模块化改造、标准化改造、外部依赖条件等在内的多个层面和维度进行，准确评估业务信息系统云化改造的相关难点与痛点，才能对信息系统云化改造有充分的认识和准备；

新建系统及迁移系统都需要云平台的支撑：新建应用可以充分使用PaaS平台及基础设施资源及服务；迁移系统需进行评估，根据评估结果确定应用迁移的实施方案，选择使用PaaS平台或基础设施资源及服务；

传统应用迁移到云环境策略主要根据应用的评估结果制定应用迁移的实施方案，主要从系统云化后对业务的价值及资源消耗情况（如月结期间对资源消耗很高，月结过后资源消耗很小），以及系统技术层面评估迁移难度及风险，从而制定系统迁移的最佳方案。

传统业务系统特点

传统业务系统多为大型单体应用，系统具有一个数据库,用于整个应用程序，同时具有复杂且较大的且不可重用的代码库，本地进程内呼叫,用于外部通信的 SOAP；每次产品发布必须部署整个应用程序。

业务系统在每个运行时实例中保留的状态，紧密耦合,跨应用程序深度嵌入依赖关系；一个技术堆栈,适用于整个应用程序，系统高度定制,具有有限的可重用性和多年来积累的大量技术债务；经常出现故障、问题或计划外停机，影响应用稳定运行，服务器性能会遇到瓶颈，扩容难度大，影响业务的推广。

系统研发和应用技术支持运维的团队人数多，管理难度高，团队人员对采用旧技术栈的应用系统支持意愿差。

云上业务特点

云上业务系统采用大量粒度可扩展的服务化或微服务化架构，微服务架构是一种架构模式，它提倡将单块架构的应用划分成一组小的服务，服务之间互相协调、互相配合，为用户提供最终价值。

每个服务运行在其独立的进程中，服务与服务间采用HTTP、消息传递或二进制调用等轻量级的通信机制互相沟通。

每个服务都围绕着具体业务进行构建，每个微服务都有自己的数据源，实例无状态保留在分布式数据网格中，

并且能够被独立的部署到生产环境、类生产环境等。

另外，应当尽量避免统一的、集中式的服务管理机制，每种微服务可采用不同的技术选择，对具体的一个服务而言，应更具业务上下文，选择合适的语言、工具对其进行构建。

应用迁移

在企业都在寻求实现跨渠道的数字能力之际，需要建立一个与之匹配的体系结构和交付范式，以促进数字产品和服务的快速构建、测试和部署。在产品数字化改造过程中，我们建议将现有的传统架构应用全面转向云原生应用，以充分适应不断变化的环境。实现产品数字化功能所需的速度和敏捷性包括:

- 开发 API过渡到可扩展并保持传统系统完整性的"微服务"架构和整合模式；
- 拥抱敏捷交付模式迭代构建、测试和验证功能和体验；
- 加快交付周期并缩短上市时间通过整合持续集成和开发(例如 DevOps)实践以及基于云的基础架构；
- 向以产品为中心的方法迈进交付和发布,重点关注客户经验。

3、应用迁移优先级规划

工作负载优先级

在确定工作负载的优先级时，一些因素会加快/推迟应用程序迁移的时间线。这些因素会在模型中被加权来确定迁移的优先级。

首先，需要明确对应用的工作负载进行排序的原因，在收集云应用适应属性、进行云的准备和迁移路线的选择之后，还应基于业务线、应用的复杂性、关键性、业务需求、成本控制以及迁移到目标环境过程中的条件，进行工作负载的优先级的排序。

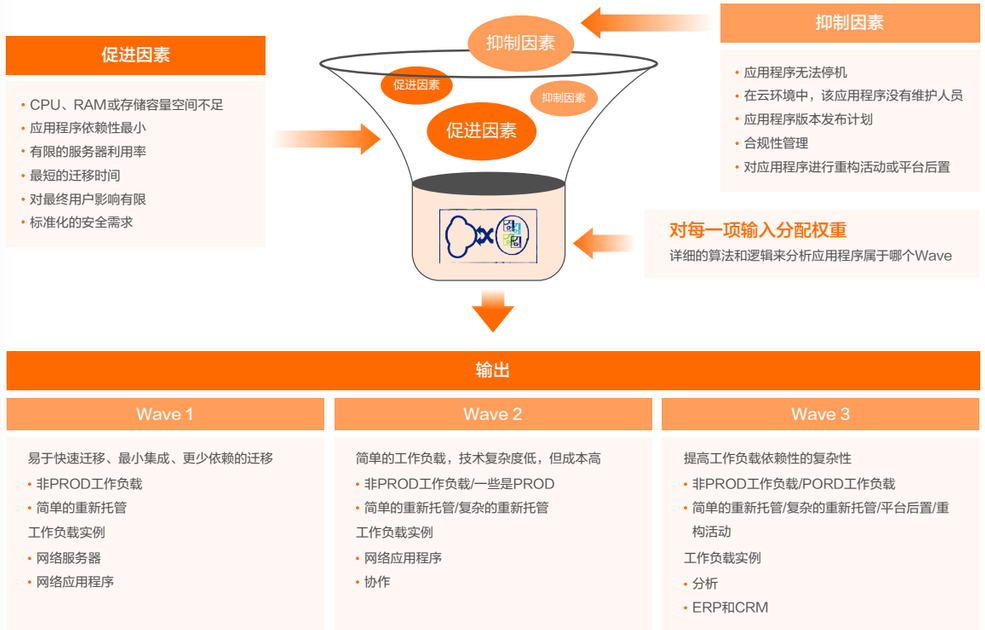
当对工作负载进行优先级排序时，有一些因素会对应用迁移的重要性起促进作用，还有的是会对迁移的时间成本有强制性的抑制作用，对各个促进因素和抑制因素赋予权重，进而分析每个应用属于哪个批次。促进因素和抑制因素分别包括：

促进因素：

- 消耗完CPU、RAM、或者存储容量
- 具有最小依赖性的应用
- 有限的服务器使用率
- 迁移的最短持续时间
- 有限的对终端用户的影响

抑制因素：

- 应用不能有停机时间
- 在云环境中没有应用的支持人员
- 应用版本的发布计划
- 遵从性规章
- 重构或者重建平台



图：迁移优先级规划

过程输出物

在应用迁移的不同阶段，会存在不同的阶段，按照时间顺序和技术上的复杂程度具体分为：

- 批次1

以快速实现、最小化集成、最低依赖性为目标的简单、可行的迁移，主要针对非生产性的工作负载和简单的移植。

・批次2

简单的工作负载，具有低技术复杂性，和大的占用空间，主要针对非生产性的工作负载/一些生产性的和简单的移植/复杂的移植。

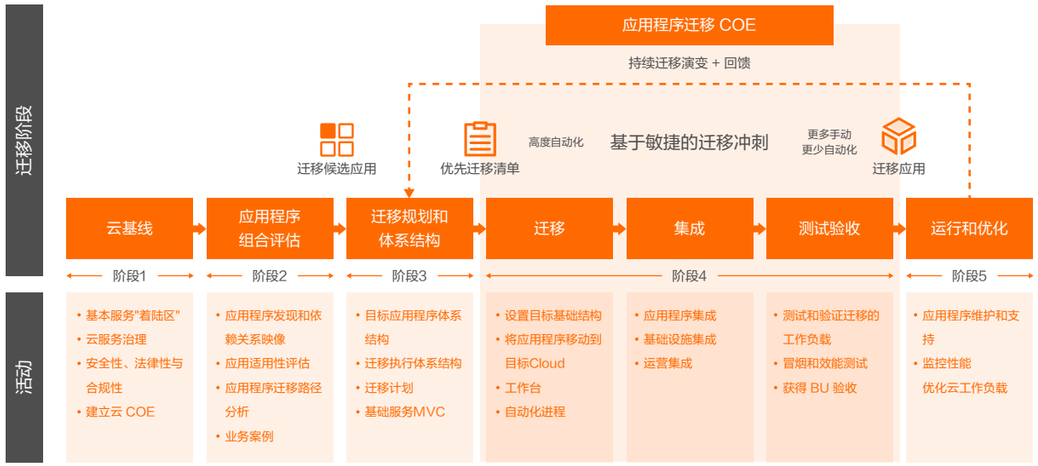
・批次3

增加工作负载依赖性的复杂度，主要针对非生产性/生产性的工作负载和简单/复杂的移植/重建平台/重构的。

4、迁移计划

工作负载优先级

对于大规模迁移,首先应基于云迁移方法论建立应用程序迁移COE,以受益于规模经济和效率。然后，可以采用如下五个步骤，分阶段的制定迁移计划，完成应用迁移工作。应用迁云总体流程如下图所示：



阶段1：云基线

・基本服务"着陆区"
・云服务治理
・安全性、法律性与合规性
・建立云COE

阶段2：应用程序组合评估

・应用程序发现和依赖关系映像
・应用适用性评估
・应用程序迁移路径分析
・业务案例

阶段3：迁移规划和体系结构

・目标应用程序体系结构
・迁移执行体系结构
・迁移计划
・基础服务MVC

阶段4：基于敏捷的迁移冲刺

迁移

・设置目标基础结构
・将应用程序移动到目标Cloud

- 工作台
- 自动化进程

集成

- 应用程序集成
- 基础设施集成
- 运营集成

测试验收

- 测试和验证迁移的工作负载
- 冒烟和效能测试
- 获得验收

阶段5：运行和优化

- 设置目标基础结构
- 将应用程序移动到目标Cloud
- 工作台
- 自动化进程

3 云上架构设计

1、网络组网

云上网络组网原则

云上网络组网的设计，需要遵循以下的设计原则：

- 可用性。为业务系统提供不间断的网络连接和网络服务的能力，确保核心、重要和关键业务系统的高可用；
- 安全性。为满足等保等其他安全体系的合规性要求；
- 稳定性。采用稳定的网络架构和技术，确保稳定性；
- 扩展性。满足未来的性能容量增长、新技术和新功能的需求，可以应对突发业务做业。

网络现状梳理

网络设计的第一步，需要对云数据中心网络现状进行梳理；主要内容包括：

- 企业多数据中心场景下（如典型的两地三中心），各数据中心的功能定位，所运行业务；
- 按数据中心功能定位映射到云上的不同区域或者同区域的不同可用区；
- 数据中心内部网络架构和网络分区梳理；
- 各网络分区内的应用分布和信息梳理，业务的互访关系梳理。

网络规划

- 从应用角度考虑上云后应用的直接迁移，重构，新增等情况，按应用规划出云上的功能分区；
- 基于规划的云上功能分区，考虑云上是否可沿用原有网络分区或是需新增、裁减、整合网络分区；
- 按之前梳理的业务互访关系和上云后的应用规划整理出新的云上业务互访规划。

具体执行云上网络设计时，一个完整的设计，其主要内容应该包括如下几个方面：

1	地域选择	8	基于SLB的高可用设计
2	VPC选择	9	子网访问控制
3	VPC网段	10	互联网访问设计
4	可用区设计	11	多VPC设计——非互联网访问VPC设计
5	单VPC和多VPC网络的选择	12	跨VPC互访设计
6	多VPC网络的规划	13	主机访问控制
7	多VPC设计——互联网接入VPC设计	14	单VPC设计

表：网络设计的关键内容

阿里云最佳实践

在阿里云上构建云上网络，需要提前规划云上网络的网段、交换机部署、路由策略等。更多详细信息，请参见云上网络设计。

阿里云企业级云上组网方案利用专有网络VPC、负载均衡SLB等网络产品，帮助企业用户构建一个支持多业务部署、安全、可靠的云上网络。

组网方案	方案介绍	使用场景	安全防护
单VPC单账号	使用一个VPC，通过交换机划分不同功能区	· 账号管理要求低（团队规模小） · 安全要求低（基本安全防护要求） · 可用性要求中（同城双活）	· 网络ACL · 安全组
单VPC多账号	· 使用一个VPC，通过交换机划分不同功能区 · 使用共享VPC创建多个业务账号	· 账号管理要求高（团队规模大且业务多） · 安全要求低（基本安全防护要求） · 可用性要求中（同城双活）	· 网络ACL · 安全组
多VPC多账号	· 使用多个VPC划分不同功能区和安全域 · 使用共享VPC创建多个业务账号	· 账号管理要求高（团队规模大且业务多） · 安全要求中（需要划分安全域） · 可用性要求中（同城双活）	· 网络ACL · 安全组 · 路由策略 · 云防火墙
多地域负载/容灾	使用多个地域实现异地容灾和负载分担，并通过云企业网实现多地域互通	· 账号管理要求高（团队规模大且业务多） · 安全要求中（需要划分安全域） · 可用性要求高（同城双活和异地容灾）	· 网络ACL · 安全组 · 路由策略 · 云防火墙
多环境隔离	· 使用多个云企业网实现多环境隔离 · 利用中转VPC实现不同环境的数据中转	· 账号管理要求高（团队规模大且业务多） · 安全要求高（不同环境间严格隔离） · 可用性要求中（同城双活）	· 网络ACL · 安全组 · 路由策略 · 云防火墙 · 第三方应用/数据安全能力

更多详细信息，请参见企业级云上网络解决方案。

2、安全设计

上云安全评估

定义与身份验证和基于角色的访问控制相关的最佳实践，包括单点登陆框架、角色与策略识别、AD整合机制等。

识别应用程序在云上应遵循的数据保护和加密，包括数据生命周期管理、加密密钥管理、系统保护进程等。

验证网络架构并确保必要的分区和保护机制到位，包括VLAN隔离、安全组模板、VPN连接、最小特权访问定义等。

评估用于提高云环境中平台服务（PaaS）安全性的附加要求，包括应用程序威胁建模、Web扫描工具、测试数据消毒净化方法等。

评估潜在日志源，并完成分析和日志记录的方法，包括日志收集和存储体系结构、工具选择、日志生命周期管理等。

回顾安全信息和事件管理（SIEM）需求并定义在云上实现它的方法，包括SIEM工具体系结构、脆弱性评估方法、配置监控过程等。

加强基础设施安全的设计修补和更新过程，包括操作系统修补和硬化工具、存储硬化策略、数据库修补方法等。

设计与实现一种增强安全体系结构的持续监测和改进模型，包括定期环境审核、安全测试设计和方法、新安全产品的评估等。

云上安全设计

・网络隔离（纵深防御）

通过云产品的安全隔离和访问控制功能，实现网络、系统、应 用和数据不同维度的隔离以实现纵深防御；

・认证授权（最小权限）

仅授权使用者必须的云账户和子账户权限，并开启双因素认证 措施和关键操作二次认证能力；

・安全加密（开启加密措施）

通过传输加密和存储加密措施实现数据在云上全程加密；

・监控告警

通过日志和监控措施及时发现配置变动、异常登录和操作、数据泄露以及异常攻击等。

阿里云最佳实践

基于云上安全问题，阿里云将云上安全防护体系框架分为以下三部分：

・安全产品提供的安全防护能力：例如，WAF、云安全中心、RAM、KMS等。
・云产品提供的安全防护能力（含红色的数据安全）。例如，VPC隔离、传输和存储加密等。
・用户利用云产品能力进行的安全管理和安全监控活动。例如，日志透明化、云主机安全管理等。

基于该云上安全防护体系框架，我们提出以下云上安全建议：

・启用云上基础防护措施
・云上业务安全防护
・云上应用安全防护
・云上系统安全防护

- 云上隔离措施
- 云上数据生命周期管理
- 云上安全监控措施
- 云上安全运营

更多详细信息，请参见企业上云安全建设解决方案和企业安全最佳实践。

3、业务上云

云上架构设计

云上业务架构采用“厚平台、薄应用”的设计理念，业务服务、数据库遵循“尽可能拆分”的原则，各服务采用组件化完成独立开发、独立部署、独立发布、独立升级；从而满足高扩展、高性能的要求。

遵循“尽可能缓存”原则实现高性能和高可靠。采用分布式架构，有效地消除各种瓶颈，通过分布式横向扩展、缓存技术建设一个真正高性能的平台。

遵循“尽可能异步”原则，通过数据库拆分和消息队列，实现高可用和高可靠。为了缓解随着系统流量增加而带来的数据库压力，需对数据库进行垂直拆分、分库分表、读写分离等操作，通过各数据库之间的异步消费来保证数据一致性。

遵循“尽可能自动化”原则，通过建立完善的监控体系，实现自动化运维。建立完善的监控体系，利用自动化运维工具，实现系统端到端的监控机制。

阿里云最佳实践

业务上云的方式，一种是在云上完全重新部署，另外就是使用服务器迁移工具直接应用迁移。

阿里云拥有丰富的迁云工具和解决方案，阿里云官网已上线260+云产品、200+解决方案，100+上云最佳实践，帮助企业客户快速完成迁云方案评估，迁云实施和生产流量切换，全面提升企业业务的可靠性、安全性。

阿里云解决方案最佳实践，是基于众多客户上云的成功案例萃取而成的最优化企业上云指导。每个最佳实践包括使用场景、多产品部署架构及部署手册。帮助客户更好地理解阿里云的产品和解决方案，降低企业上云门槛的同时满足客户自服务的需求。

- 服务器迁移：使用阿里云提供的迁移工具将物理服务器、虚拟机以及其他云平台云主机一站式地迁移到阿里云ECS。详细实现方案，请参见服务器迁移最佳实践。
- VMware迁移：实现VMware私有云虚拟机迁移至阿里云DDH实例。详细实现方案，请参见VMware迁移DDH最佳实践。
- OpenStack迁移：将OpenStack上的虚拟机迁移到专有宿主机DDH上，大幅降低成本。详细实现方案，请参见OpenStack迁移DDH最佳实践。
- 小型互联网企业业务迁移：面向中小型互联网企业，业务服务器和数据库迁移上云。详细实现方案，请参见小型互联网迁移上阿里云。

更多业务上云最佳实践，请前往企业上云最佳实践频道

（https://www.aliyun.com/acts/best-practice/index）。

4、数据上云

数据上云架构设计

数据在同一业务库中采用多租户隔离机制；为数据服务层建立一套统一的管理规范，所有业务用户账号在完成相关审批流程后对相应的数据字段进行授权安全访问，对数据只有读的权限，不能对原始数据进行直接修改或删除，做

到数据不搬家，可用不可见；建立统一的数据资源视图和数据血缘跟踪能力，能够对所有的数据的生命周期进行溯源查询，用以甄别数据变更过程中的真实性和准确性；根据不同业务场景结合流程节点和风险管控要求，对相关数据进行分析、建模、挖掘，提高数据服务支持。

数据上云安全防护

在企业数据上云的过程中,实施数据分层保护功能已成为一个关键优先事项。同时，数据保护控制必须辅之以强大的监控工具和访问管理控制,以构建数据的整体视图，对数据的全生命周期进行监控。重点考虑以下关键数据保护领域。

- 数据分类：围绕数据识别、清单、标签和分类的功能和流程；
- 静态数据保护：有关加密/令牌化的解决方案和注意事项,包括密钥管理；
- 传输中数据保护：功能包括 TLS/SSL 层保护、数据丢失防护解决方案和安全数据传输；
- 数据监控：通过操作中心 (SOC) 进行日志记录和监视功能；
- 在云环境中,以数据为中心的保护需要在整个数据生命周期中进行。

阿里云最佳实践

- 缓存数据上云

包括Redis、MemCache迁移。迁移前，确定存放的是什么数据，比如session，用户登录信息等，确定存放的哪些数据是可以丢弃的，应用重新从数据库更新，确定需要迁移的数据量；迁移时，使用DTS工具进行迁移，且支持增量；应用和Redis之间如果有代理程序，需要先进行失效处理。

- 数据库上云

以MySQL迁移为例。迁移前，确定每个业务线对应的实例使用情况，实例共享物理机情况，确定端口是否都

使用3306，不同的实例是否都使用不同的域名，MySQL以哪些版本为主，确认云上是否覆盖，统计实例总数，一台物理机多少个实例，每个实例数据量级别，通过POC来熟悉DTS用法；迁移时，使用DTS工具迁移；如果出现异常则可采用回退策略，DTS回流到线下，客户可能做业务改动，比如将IP改成域名，需要提前检查。技术细节可以参考“电商资源建站和数据库迁移最佳实践”。

- 半结构化数据上云

包括MongoDB迁移。迁移前，需要了解有几个集群，总共多少TB数据，需要做云服务POC验证；迁移时，使用云自建方式，加分片方式迁移，也可以使用云服务方式，通过使用DTS工具从自建迁移过来。

DTS的数据迁移功能支持同构或异构数据源之间的数据迁移，同时提供了库表列三级映射、数据过滤等多种ETL特性，适用于数据迁移上云、阿里云实例间迁移、数据迁移下云等多种场景。

迁移场景	源库类型	实现方案
从自建数据库迁移至阿里	MySQL	从自建MySQL迁移至RDS MySQ
		从通过专线、VPN网关或智能接入网关接入的自建MySQL迁移至RDS MySQL
		从通过专线接入的自建MySQL迁移至其他账号下的RDS MySQL
		从自建MySQL迁移至PolarDB MySQL
		从自建MySQL迁移至DRDS
	SQL Server	从自建SQL Server增量迁移至RDS SQL Server
		从自建SQL Server全量迁移至RDS SQL Server

迁移场景	源库类型	实现方案
从自建数据库迁移至阿里	Oracle	Oracle迁移上云推荐方案： · 从自建Oracle迁移至PolarDB-O集群（迁移结构） · 从自建Oracle迁移至PolarDB-O集群（迁移数据）
		从自建Oracle迁移至DRDS
		从自建Oracle迁移至云原生数据仓库AnalyticDB PostgreSQL
		从自建Oracle迁移至RDS MySQL
		从自建Oracle迁移至RDS PPAS
	PostgreSQL	从自建PostgreSQL（10.1-12版本）增量迁移至RDS PostgreSQL
		从自建PostgreSQL（9.4-10.0版本）增量迁移至RDS PostgreSQL
		从自建PostgreSQL全量迁移至RDS PostgreSQL
	Redis	从自建Redis迁移至阿里云Redis
	MongoDB	从单节点架构的自建MongoDB迁移至阿里云
		从副本集架构的自建MongoDB迁移至阿里云
		从分片集群架构的自建MongoDB迁移至阿里云
	TiDB	从自建TiDB增量迁移至RDS MySQL
		从自建TiDB全量迁移至RDS MySQL
	Db2	从自建Db2迁移至RDS MySQL

迁移场景	源库类型	实现方案
从第三方云迁移至阿里云	Amazon RDS	从Amazon RDS MySQL迁移至阿里云
		从Amazon RDS Oracle迁移至阿里云RDS MySQL
		从Amazon RDS Oracle全量迁移至阿里云RDS PPAS
		从Amazon RDS for PostgreSQL增量迁移至阿里云
		从Amazon RDS PostgreSQL全量迁移至阿里云
	Amazon Aurora	从Amazon Aurora MySQL迁移至阿里云
		从Amazon Aurora MySQL迁移至PolarDB MySQL
		从Amazon Aurora PostgreSQL全量迁移至阿里云
	Amazon SQL Server	从Amazon RDS SQL Server全量迁移至阿里云
	Atlas MongoDB	使用DTS将MongoDB Atlas数据库迁移至阿里云
	华为云文档数据库	从华为云文档数据库迁移至阿里云
	腾讯云MySQL	从腾讯云MySQL迁移至阿里云
	腾讯云MongoDB	从腾讯云MongoDB增量迁移至阿里云
		从腾讯云MongoDB全量迁移至阿里云
同一阿里云账号实例间迁移	RDS实例	RDS实例间的数据迁移
	RDS MySQL实例	配置RDS MySQL间的数据集成任务

迁移场景	源库类型	实现方案
同一阿里云账号实例间迁移	RDS MySQL实例	从RDS MySQL迁移至PolarDB MySQL
	RDS MariaDB实例	从RDS MariaDB迁移至RDS MySQL
	PolarDB MySQL集群	PolarDB MySQL集群间的数据迁移
		从PolarDB MySQL迁移至RDS MySQL
	PolarDB兼容Oracle数据库	PolarDB-O集群间的数据迁移
	MongoDB实例	从MongoDB单节点实例迁移至副本集或分片集群实例
		从MongoDB副本集实例迁移至分片集群实例
		迁移MongoDB实例至其他地域
跨阿里云账号实例间迁移	RDS实例	跨阿里云账号迁移RDS实例
	PolarDB MySQL集群	跨阿里云账号迁移PolarDB MySQL集群
	MongoDB实例	跨阿里云账号迁移MongoDB实例
从阿里云迁移至自建数据库	RDS MySQL实例	从RDS MySQL迁移至自建MySQL
	PolarDB MySQL集群	从PolarDB MySQL迁移至自建MySQL
自建数据库间的迁移	Oracle	自建Oracle间的数据迁移

・存储迁移上云

主要指非结构化数据迁移。迁移前，了解现有存储的数据是哪些，含副本数据量和实际数据量，负载情况，读写比例等，需要POC来熟悉产品用法，包括测试使用OSSImport来将IDC文件迁移到OSS；迁移时，历史数据使用闪电立方迁移到OSS，热数据使用OSSImport迁移到OSS云上存储；迁移到OSS需要改应用，需要注意检查避免出错，另外，如果小文件较多，则迁移耗时可能会较长，需要提前做好安排。

阿里云在线迁移服务是阿里云提供的存储产品数据通道。使用在线迁移服务，您可以将第三方数据轻松迁移至阿里云对象存储 OSS，也可以在对象存储 OSS 之间进行灵活的数据迁移。详细存储迁移上云方案，请参见在线迁移服务。

4 迁移行动、割接与上线

为了使迁移按时完成以实现预期的业务目标，建议采用基于工厂的方法。基于工厂的方法使用一套标准的流程和工具以自动、并行的方式执行迁移。它有助于组织形成一套具有标准化流程的模式，通过执行这些流程来完成大规模的迁移活动。

云迁移工厂模式具备以下功能：

功能1——基础服务

・提供了使应用程序迁移到云平台所需的核心能力和服务
・基础服务包括网络、安全、监控、配置管理与计费，以及退款
・在实施阶段迁移团队应该参考基础服务提供的最佳实践。

功能2——流程工作台

- 支持在短时间内将多个应用程序迁移到云
- 通过短时间敏捷的并行运行来完成不同的迁移
- 关键的可重复流程是自动化的，来提高交付速度（例如scrum bots，自动配置脚本生成器等）
- 实施和管理团队是跨职能团队，他们来执行短时间迁移 /定位的迁移步骤（例如，平台后置应用程序）

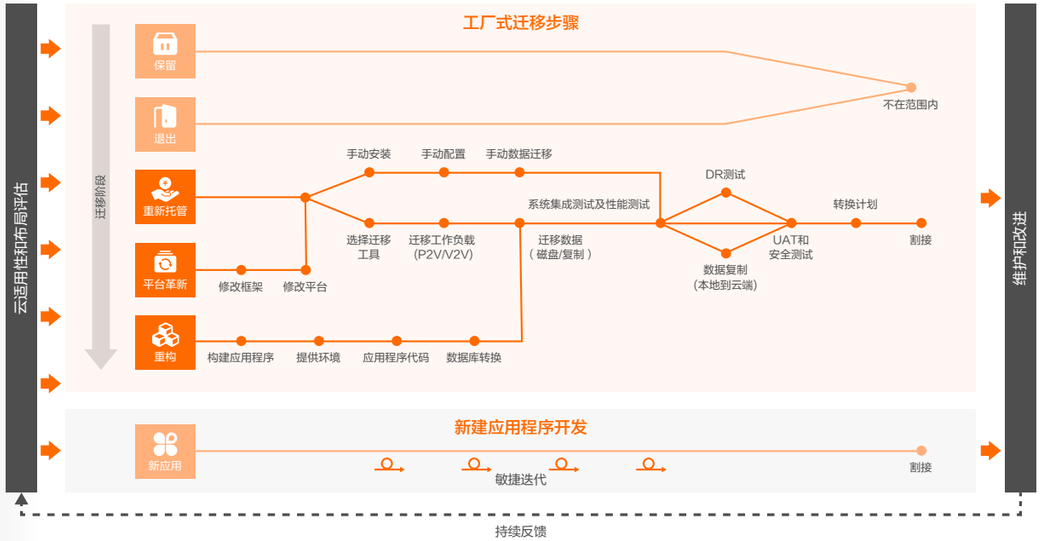
功能3——卓越云中心

- 提炼了使应用程序迁移进程的性能与采用过程中设置的目标一致的业务和技术能力
- 团队与业务功能交互以理解需求并使用合适的指标来度量迁移性能
- 负责管理整个项目，也负责培训迁移团队
- 还会监管安全与合规性需求及事件

1、迁移行动

迁移行动

一旦为应用程序确定并固化了迁移路径，实施和管理团队将使用以下迁移路径之一迁移待迁移的应用程序集。

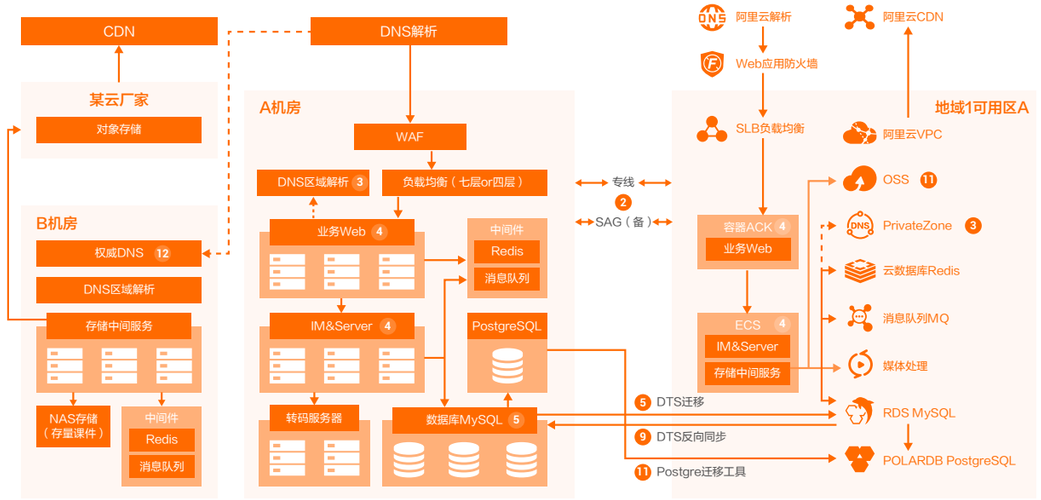


图：应用上云执行迁移 - 迁移活动

阿里云迁移最佳实践

服务器迁移中心（Server Migration Center，简称SMC）是阿里云自主研发的迁移平台。使用SMC，可将单台或多台迁移源迁移至阿里云。迁移源（或源服务器）概指企业待迁移IDC服务器、虚拟机、其他云平台的云主机或其他类型的服务器。

在应用服务迁移过程中，使用SMC服务将在IDC部署的业务应用服务自动、快速、一站式迁移到云上ECS，同时提供工具支持将自建Kubernetes的应用迁移到云上。更多详细信息，请参见SMC最佳实践。



1. 阿里云官网注册
2. IDC和VPC网络打通
3. 区域解析同步到云解析PrivateZone（原企业管控平台集成）
4. Web应用迁移到容器Kubernets（ACK镜像备份及迁移工具）
   C++应用迁移到ECS（SMC迁移服务）
5. DTS服务将MySQL数据同步到云上RDS
6. 中间件MQ直接切换
7. 配置Web应用防火墙
8. 测试（应用调试、数据库连通性、性能压测等）
9. DTS双向同步开启反向同步链路
10. 更改DNS解析，业务流量切换到云上
11. PostgreSQL迁移（PostgreSQL迁移工具）
12. 存储迁移到OSS（在线迁移服务）
13. 切换CDN和存储

阿里云迁移工具

迁移时，可以借助阿里云提供的丰富的上云实施工具（https://www.aliyun.com/solution/cmc/implementationplan），提升上云的效率和效益。

工具名称	功能和用途
混合云备份服务HBR	IDC VMware虚机无代理增量迁云
混合云容灾服务HDR	IDC 物理机、虚拟机容灾上云
离线迁移（闪电立方）	实现本地存储数据迁移上云
在线迁移服务	将第三方数据迁移至OSS
云存储网关	帮助企业应用无缝对接OSS
服务器迁移中心SMC	将服务器迁移至阿里云
Disk2VHD（第三方）	将逻辑磁盘转换为虚拟磁盘
Velero-k8sToACK（第三方）	将云原生K8S迁移至ACK
Image-Syncer镜像迁移	将镜像批量迁移至ACR
Derrick应用容器化	非容器应用快速完成容器化
ack-image-builder	快速制作ACK自定义镜像
数据传输服务DTS	支持多种异构数据间传输
Redis-port（第三方）	将数据自动恢复至目标实例
Redis-shake	将Redis中的数据备份到RDB中
MySQLDump（第三方）	进行数据库备份与恢复
BDS	针对HBase的迁移同步服务

工具名称	功能和用途
搬站迁移工具MMA	将Hadoop开源生态迁移上云
DistCP（第三方）	大规模集群间拷贝工具
离线数据同步工具DataX	异构数据源离线同步工具
资源编排ROS	云资源管理和自动化运维服务
emr-tools	Hadoop迁移数据到OSS
iperf3（第三方）	测试实际网速预估传输时间

表：阿里云上云实施工具

阿里云迁云实施服务

阿里云提供从咨询到实施迁云全周期的专业服务，通过技术支持或协助的方式帮助企业将在线业务系统、数据库及存储等内容迁移到阿里云，并顺利完成业务系统的割接。更多详细信息，请参见迁云实施服务。

2、迁移割接方案与割接保障

应制定详细的割接方案。包括整体割接方案介绍、详细操作步骤的技术方案、回退方案、人员和分工安排、预期效果、割接过程中的信息采集和业务、数据监控、支持资源和保障措施等。

应对制定出的割接方案进行风险和业务营销评估，并对割接系统所涉及的开发、运维团队和用户部门进行宣贯和告知。

割接方案中应重点考虑对业务数据的备份和恢复，确保割接过程中数据得到充分的保护，不会出现丢失或发生错误。

割接过程中和完成后，都应对割接后的业务和数据做好监控和总结回顾。持续观察业务的运行状态，直到确认完全没有问题，割接执行工作才算基本结束。

割接完后，要针对割接过程中出现的问题进行分析，及时改进，并在下一次或后续的割接工作中避免。除了对发现的问题及时改进，也要总结经验并保留下来，供组织内学习使用，从而提升整个组织内人员的技能水平。

3、功能/性能测试

企业上云后，可对云资源、应用架构的安全、性能、稳定性、成本等方面进行全面巡检，针对迁移效果，根据阿里云各产品的最佳实践，基于TAM服务体系的核心能力，提供诊断和优化建议。

功能测试——智能顾问（Advisor）服务

智能顾问是一款开箱即用的风险巡检产品，一键巡检快速识别当前云资源、应用架构的潜在风险并针对性提供解决方案。

智能顾问可根据用户情况，结合阿里云长期以来的客户侧最佳实践，基于TAM服务体系的核心基础能力及阿里生态内SRE的专业能力，以在线的方式全方位地为用户提供云资源、应用架构、业务性能及安全上的自助巡检和治愈优化建议，高效提升客户的业务延续性。

性能测试——性能测试 PTS（Performance Testing Service）服务

PTS是具备强大的分布式压测能力的 SaaS 压测平台，可模拟海量用户的真实业务场景，全方位验证业务站点的性能、容量和稳定性。

PTS 目标是将性能压测本身的工作持续简化，使您可以将更多的精力回归到关注业务和性能问题本身。在 PTS 平台上，您可以用较低的人力和资源成本，构造出最接近真实业务场景的复杂交互式流量，快速衡量系统的

业务性能状况，为性能问题定位、容量最佳配比、全链路压测的流量构造提供最好的帮助。进而提升用户体验，促进业务发展，最大程度实现企业的商业价值。

4、云转型支持灵活的IT系统和服务

应用上云的最终效果，是根据业务需要，以不同的速度交付应用系统及IT服务。在多速IT下，IT组织利用敏捷方法学、持续集成/持续交付、模块化体系结构和其他工具/方法来快速部署更新，加快产品上市时间，迅速响应业务需求。

为了在组织中支持多速IT，可以设计特定的工作流来满足业务需求，这些工作流旨在以不同的速度定义和交付IT服务。

敏捷交付

敏捷交付有助于组织在推动更大的创新和试验的同时关注交付正确的软件和数字产品。

CI/CD和开发运维

CI/CD可以通过持续的构建、测试和部署在很大程度上有助于自动化部署流程，减少了应用程序发布的时间和工作量。

微服务和容器

通过启用微服务，应用程序变得具有弹性和可扩展性，而且通过使用API和容器，应用程序组件相对松散耦合。

认知自动化

IT操作下的流程可以通过使用RPA和认知自动化来实现自动化，以帮助扩展现有的运维团队与流程。

组件提升

重新访问应用程序体系结构，以评估哪些组件可以用适合云的替代方案替换，以增加从云迁移中获得的好处。

5、释放原业务资源

随着企业的应用系统逐步的迁移上云，原有的IT资源将会逐步关停并转，业务资源得到释放，在资产生命周期的结束后，企业的IT成本结构得到了优化和提升。企业能够将原有业务资源释放后产生的价值空间，继续投入到业务模式创新的探索和实验中，不断推动业务的发展。

5 迁移问题处理与优化

在应用系统迁移上云后，需要对上云的业务系统进行全链路的业务功能测试、性能测试、压力测试，对迁移过程中遗留的问题进行处理与优化。需要从全局视角，针对不同的业务场景进行业务功能的完善以及性能优化提升，对云上的系统架构、应用组件、产品服务、资源配置进行适应性调整。从总体上对系统上云后的性能、弹性、稳定性进行提升，以满足未来业务发展的需要。

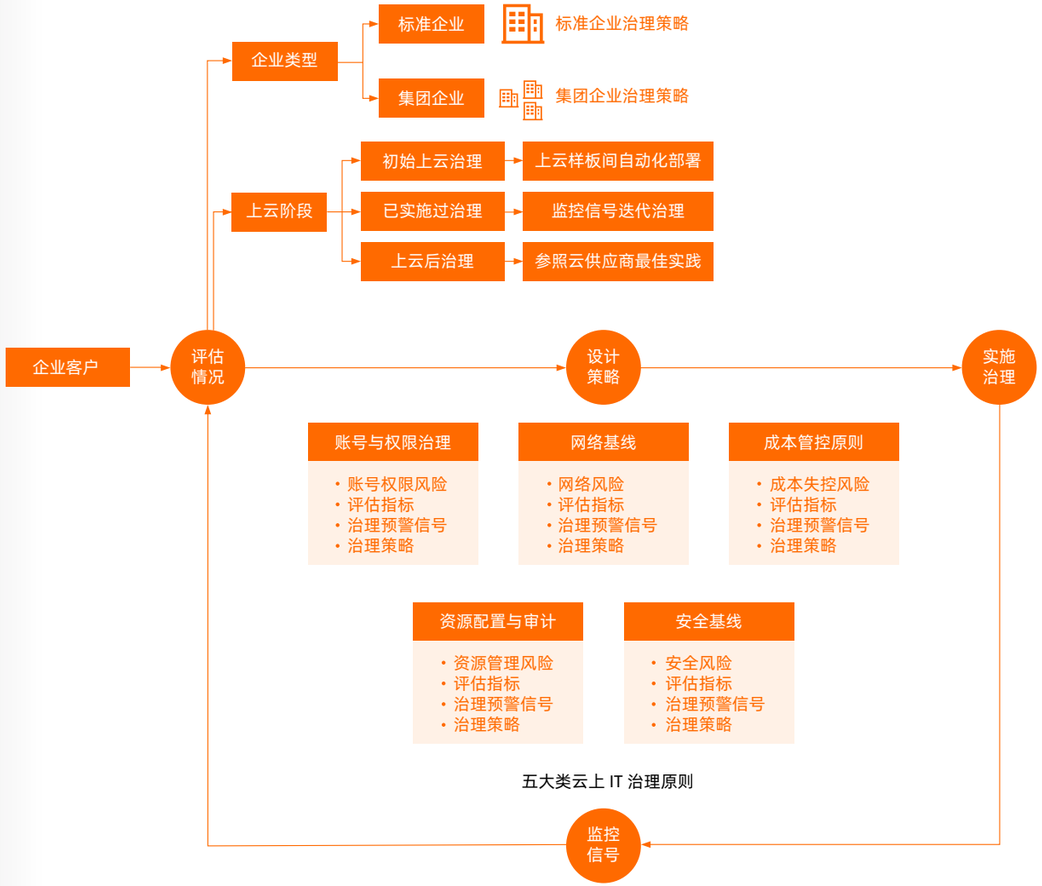
我们还要紧密关注云服务厂商的产品改进与提升，及时关注技术架构演进的方向和最佳实践，持续优化系统的架构和资源配置。

2 云上 IT 治理方法论

1 云上IT治理方法论

开展企业云上IT治理主要有4个步骤：评估情况、设计策略、实施治理和监控信号。云上企业IT治理根据治理原则应对企业上云可能面临5大类风险，包括账号与权限管理风险、成本失控风险、资源合规风险、安全风险、网络稳定与效率风险。针对性地，可以开展企业云治理可以以5大类原则为依据：账号与权限治理原则、成本管控原则、资源管理与审计治理原则、安全合规基线治理、网络基线治理。

上云企业按照企业的规模和上云的IT系统复杂度，可以分为标准企业和复杂的大型集团企业。



1、评估情况

治理原则的选择

不同的企业，从云上IT治理的角度，有不同的需求，按照上云企业的规模和上云的IT系统复杂度，可以分为标准企业和复杂的大型集团企业。

企业特征	标准企业	集团企业
地理区域	客户和员工主要位于同一个国际或地区	客户和员工可能位于多个国际或地区
业务部门	业务共享统一的IT基础设施	多业务部门具有不同的IT基础设施
运维团队规模	2-10人运维人员	10人以上运维人员
IT预算分配	统一IT预算分配	跨部门独立结算

不同类型企业的云上IT系统情况

企业IT系统状况	标准企业	集团企业
云账号	单个生产账号	多个生产账号
云上资源规模	25-1000台计算节点	200台以上计算节点
网络	没有外网服务或者1到2个外网服务	网络复杂，多个外网服务

上云治理阶段的匹配

企业治理目标状态	标准企业	集团企业
账号与权限	同一个的权限策略	各个业务部门有不同的权限策略
成本管控	成本与预算合理分析	支持分账进行成本与预算分析
安全基线	保护企业核心知识产权和财务数据	保护不同业务的知识产权、财务数据，兼顾第三方和合作伙伴等合作的情况
网络基线	业务在一个专有网络下运行	考虑多种网络之间的隔离与互通

从企业IT治理的角度，企业越早开展云上IT治理，一般说治理的工作量越小，治理的效果越好，但实践中企业开展IT治理的时机，往往受自身的业务发展影响。企业开展IT治理的时机，可能处于的不同上云治理阶段，包括：未上云阶段、已上云并实施过云上IT治理、已上云但未实施过云上IT治理。

未上云阶段。这类企业在初始上云规划的时候，就开展云上IT治理，可以从评估情况开始，将云上IT治理策略纳入上云规划的一部分。

已上云并实施过云上IT治理。这类企业已经有部分业务上云，并且已经设计了云上IT治理策略，并实施过治理。

已上云但未实施过云上IT治理。这类企业已经有部分业务上云，但在此前的的上云规划和实施中没有或较少的考虑过云上IT治理。

2、设计策略

云上IT治理策略的内容

云上IT治理策略是企业根据自身情况，制定的IT治理指导性文档，内容包括业务风险、评估指标、治理预警信号和治理原则。

业务风险

业务风险是一系列可能给企业造成业务损失的概率性事件，一旦发生，可能造成企业成本上升、收入下降、服务能力下降甚至完全丧失。企业在设计云上IT治理策略的过程中，首先根据自身业务需要，识别对自己重要的业务风险，并记录在云上IT治理策略中。本文从五个方面列举了一些常见的业务风险，企业可以根据自己的企业规模，结合自身实际业务需求，识别相应的业务风险，并记录在云上IT治理策略中。

风险评估指标

风险评估指标是一系列可以量化的指标，使得通过关注这些指标，可以一定程度上评估企业当前在某个方面的潜在IT治理风险。本文从五个方面列举了一些常见的风险评估指标，企业可以根据自己的企业规模，结合自身实际业务需求，确定自己的风险评估指标，并记录在云上IT治理策略中。

治理预警信号

治理预警信号是一系列企业在云上进行IT运维管理过程中可能出现的场景，遇到这些场景时，企业可以考虑实施相对应的IT治理措施。本文从五个方面列举了一些常见的治理预警信号，企业可以根据自己的企业规模，结合自身实际业务需求，确定自己的治理预警信号，并记录在云上IT治理策略中，并针对信号保持监控，当相应的信号出现时，采取相应的治理措施。

治理原则

治理原则是云上IT治理策略的主要内容，企业针对云上IT运维管理制定的一系列策略声明，是企业实施云上IT

治理的原则指导。本文从五个方面（详细内容将在6.2.2 五大类云上IT治理原则策略中详细阐述）列举了一些常见的云上IT治理原则，企业可以根据自己的企业规模，结合自身实际业务需求，确定自己的治理原则，并参考云提供商给出的相应领域的最佳实践，实施企业云上IT治理。

3、实施治理

企业根据自身的上云治理阶段，实施云上IT治理。对于处于未上云阶段的企业，企业将云上IT治理策略纳入自己的上云规划之中，评估企业所属类型，根据企业所属类型设计企业云上IT治理策略，参考云服务商的最佳实践，实施云上IT治理。有些云服务商针对首次上云企业，设计有针对性的自动化部署模版或样板间，可以自动化地为企业构建起符合主要IT治理要求的云上基础设施。对于已上云并实施过云上IT治理的企业，企业的云上IT业务已经处在可靠稳定的运行阶段，应该根据标准化的云上IT治理策略，随时监控云上IT治理预警信号，相应的场景出现的情况下，评估新的情况并实施治理。对于已上云但未实施过云上IT治理的企业，需要评估企业所属类型和当前企业遇到的业务风险，根据企业所属类型设计企业云上IT治理策略，参考云服务商的最佳实践，实施云上IT治理。

4、监控信号

在实施治理之后，企业保证云上IT服务在当前环境下的可见与可控。此后企业持续监控云上IT运行风险评估指标和来自企业的新的业务需求。当云上IT运行风险评估指标出现大的风险性波动，或者企业有影响治理的新的业务需求，企业可以重新评估治理情况，并实施迭代治理。

2 五大类云上IT治理原则参考策略

1、账号与权限治理原则

概述

账号与权限治理原则是五大类云上IT治理原则之一。这一类治理原则侧重于说明企业应该如何建立适合自己的云上账号体系和权限体系。企业利用云提供商提供的认证与授权系统，建立起匹配自己组织人员结构和资源管理要求的账号与权限治理体系，保证针对云上资源的一切管控操作都可以追踪到获得认证和授权的身份。账号与权限治理原则是企业云上资源管控安全的基础，是对企业安全基线的补充。本框架的这一节主要介绍账号与权限治理所应对的业务风险、常用的评估治理水平的指标、提醒治理团队关注账号与权限问题的预警信号和实施治理的常见原则。这一节的主要读者是企业的云架构师和云治理团队的其他成员。根据这些规则制定决策、策略和流程的过程中，应有负责设计和实施企业账号与权限系统的 IT 团队共同参与和讨论。

业务风险

1、适用于所有企业的业务风险

存在未经授权的资源访问。如果敏感数据和资源可以被未经授权的用户访问，可能会导致数据泄露，违反企业的安全要求，有可能导致企业承担业务或法律责任。

资源访问效率低下或失去服务能力。如果无法有效地授权用户访问数据和资源的操作，可能会导致企业的服务中断，导致企业承担业务损失。

传统账号系统效率低下。传统的身份验证机制或第三方多重身份验证可能不适用于云，因为它们需要将系统迁移到云，或需要将其他账号服务部署到云。账号系统的迁移有可能延迟或阻碍业务应用迁移，并增加成本。

2、主要适用于集团企业的业务风险

多账号解决方案导致效率低下。具有多个部门或多条业务线的企业可能需要多个用户帐号。对于需要牢记多组凭据的用户，以及跨多个系统管理帐号的 IT人员，这可能会导致效率低下。

无法与外部合作伙伴共享资源。难于将外部业务合作伙伴添加到已有的账号解决方案，这可能会阻碍资源共享和业务沟通效率。

风险评估指标

3、适用于所有企业的风险评估指标

- **账号系统大小。**通过账号系统管理的用户、组或其他对象的总数。
- **依赖传统账号系统的业务应用数。**依赖于本地账号系统或第三方或多重身份验证机制的业务应用数。
- **权限越界提升的用户数。**对资源或管理工具拥有越界提升的访问权限的用户数。
- **身份验证次数。**成功和失败的用户身份验证尝试次数。
- **授权次数。**用户访问资源的成功和失败尝试次数。
- **泄露的帐号。**遭到入侵的用户账号数。

4、主要适用于集团企业的风险评估指标

- **账号组织结构的总体大小。**企业账号组织结构使用的目录数、层级数和账号数总体大小。
- **联合账号系统的规模。**与企业联合搭建的账号管理系统的数量。

治理预警信号

5、适用于所有企业的治理预警信号

- 用户帐号管理需求。 如果企业的用户、 组或其他对象统一在账号系统中进行管理，则可能会受益于在账号系统中的投资，以确保对大量帐户的有效管理。
- 传统账号系统预警。如果企业计划将业务应用迁移到需要旧身份验证功能或第三方多重身份验证的云，则应实施账号与权限治理，以减少与重构或其他云基础结构部署相关的风险。
- 发生权限越界提升访问的预警。如果某个企业的用户的管理工具和资源的发生权限越界提升访问次数超过了某个百分比 p% ，则应该考虑投资进行账号与权限治理，以最大程度地降低无意中过度预配用户访问权限的风险。
- 身份验证失败预警。如果身份验证失败的企业的尝试次数超过某个百分数 p% ，则应实施账号与权限治理，以确保身份验证方法不受外部攻击，并且用户可以正确进行身份验证。
- 授权失败预警。 拒绝访问尝试超过某个百分数 p% 的企业应该考虑实施账号与权限治理来改进访问控制的应用程序和更新，并识别潜在的恶意访问尝试。
- 泄露账号系统预警。 具有超过1个泄露帐户的企业应考虑实施账号与权限治理，以提高身份验证机制的强度和安全性，并改进用于修正与受攻击帐户相关的风险的机制。

6、主要适用于集团企业的治理预警信号

- 账号组织结构复杂性预警。 维护超过 N 个代表部门或业务线的目录的企业应考虑设计和实施账号与权限治理，以减少与帐户管理相关的风险，以及在多个系统间分散的多个用户凭据相关的效率问题。
- 联合账号系统预警。 实施具有 N 外部账号管理系统的联合身份验证的企业可以从账号与权限治理中获益，以确保联合成员之间的组织策略一致。

治理原则

- 应该遵循的云厂商的建议注册云账号，云账号应该符合以下要求：

  - 注册可以长期行使管理员职责的手机号作为验证手机号，避免因为人员变动导致验证手机号遗失。
  - 应该根据云厂商要求设置企业实名认证，注意保持注册名称跟法律登记实体名称的一致性，特别是当名称中包含标点符号和字形相近的字词时。
- 企业可以根据规模和IT治理需求分成两类，标准型企业治理模型和复杂型企业治理模型。针对复杂型企业治理模型，选择的云提供商应该提供组织结构管理的解决方案，支持企业按照自身组织结构进行资源和账号管理。
- 对于组织结构管理，选择的云提供商应该支持不同组织级别使用统一的企业实名认证和不同组织级别使用不同的企业实名认证。
- 所有帐号和子账号都应该符合以下要求：
  - 设置足够强度的账号密码，尽量避免使用姓名、手机号、身份证号、银行卡号等隐私信息。
  - 应该使用多因素认证方法登录到受保护的资源。
- 应该为企业创建管理员子账号，用于日常的管理员操作，避免使用云账号进行日常操作。
- 针对复杂型企业治理模型，创建对应企业资源组织结构的资源目录。
- 访问密钥用于云服务API的调用，应该遵循以下规则管理：
  - 当用户权限发生变化时或不再需要通过API访问云资源时，应禁用访问密钥。
  - 当确认已经不再需要使用访问密钥时，可以删除访问密钥，删除前应该通过最后访问时间或操作日志等确认密钥已不再被人使用。
  - 应当创建两个以上访问密钥进行轮换。
- 应该针对企业的账号、用户、用户组和角色的命名制定治理规范，并将规范应用到所有云资产。
- 应该针对关键任务型应用程序或受保护数据所涉及的任何资源，依据最小特权访问模型设计角色，并建立相应的管理员账号。

- 针对拥有本地身份系统的企业，选择的云提供商应该提供一种通过旧身份系统进行身份验证的方式，使得企业可以通过云厂商支持的身份系统（Identity Provider，IdP）与云厂商实现统一登录系统。
- 针对拥有第三方身份认证系统的企业，择的云提供商应该提供一种通过第三方身份认证进行验证的解决方案。
- 企业如果需要部署需要客户身份验证的新应用程序，应该使用与内部身份系统相兼容的身份系统。
- 针对访问控制资源，应该有独立的资源控制权限策略，以应用于访问控制管理员组。
- 针对除访问控制资源以外的系统资源，应该有独立的系统资源控制权限策略，以应用于系统管理员组。
- 针对除数据安全防护资源，应该有独立的数据安全防护控制权限策略，以应用于数据安全防护管理员组。
- 针对网络资源，应该有独立的网络控制权限策略，以应用于网络管理员组。
- 针对数据库资源，应该有独立的数据库控制权限策略，以应用于数据库管理员组。
- 针对财务费用资源，应该有独立的财务费用控制权限策略，以应用于财务费用管理员组。
- 应该把权限提升作为例外进行管理，将所有此类例外以及相关的团队都做记录，并定期审核例外情况。

阿里云的最佳实践

企业需要根据归属项目（或分公司、部门、产品线等维度）对云资源进行分组，并根据云上用户的任务执行，授予相应的操作权限，确保项目间的资源隔离以及用户访问限制。

阿里云提供用户组功能，根据云上用户所承担的执行任务分成运维、开发、财务等角色，并进行操作权限的定义，将用户加到某个用户组中以获得相应的权限；利用资源组功能可以将云资源进行分组管理，并且可以基于资源组将权限授予相应的用户或者用户组。针对标准企业和集团企业两个模式，阿里云提供不同的最佳实践来支撑客户帐号与权限的治理需求。更多详细信息，请参见访问控制RAM。

2、成本管控原则

概述

成本管控原则是五大类云上IT治理原则之一。这一类治理原则侧重于说明企业应该如何建立适合自己的云上成本管控机制。对于很多企业来说，节省IT成本是选择上云的重要因素之一。而随着上云的规模越来越大，业务越来越复杂，云上成本也越来越高，如何在业务规模、系统性能和资源成本之间作出取舍，也称为企业业务成功的重要因素。特别是对于复杂的集团企业来说，首先能够实现云上成本在不同部门的分账解决方案，以达到上云成本的透明化，是对企业能够进一步提升企业上云效率和效果的重要保障。本框架的这一节主要介绍成本管控原则所应对的业务风险、常用的评估治理水平的指标、提醒治理团队关注成本管控问题的预警信号和实施治理的常见原则。这一节的主要读者是企业的云架构师和云治理团队的其他成员。根据这些规则制定决策、策略和流程的过程中，应有负责设计和实施成本管控系统的 IT 团队共同参与和讨论。

业务风险

1、适用于所有企业的业务风险

- **预算失控。**不控制预算可能会导致云服务商支出过多。
- **资源利用率损失。**不在实际使用或使用率很低的资源的可能导致投资损失。
- **支出异常。**任何产品或业务的意外支出峰值，都可能意味着资源没有被正确使用。
- **过度预配资源。**如果业务应用部署在超过应用程序或虚拟机（VM）的需求的配置中，则会产生浪费。

2、主要适用于集团企业的业务风险

- **分账效率低下。**如果缺乏很好的机制对企业的支出进行分账，企业则可能需要大量的人力投入对齐不同部门、不同业务与不同资源支出的匹配关系。

- **分账不清造成的费用失控。**如果缺乏很好的机制对企业的支出进行分账，则可能失去对不同部门、业务应用的资源申请的控制，从而造成预算、资源利用率和资源过度申请的失控。

风险评估指标

3、适用于所有企业的风险评估指标

- **年支出。**云提供商提供的服务的总年成本。
- **每月支出。**云提供商提供的服务的每月总费用。
- **预测与实际比率。**用于比较预测支出和实际支出 (每月或每年) 的比率。
- **环比云采用率。**每月与每月的云成本的增量百分比。
- **当月累计成本。**从月初开始算起的每日当月总累计支出。
- **费用支出趋势。**针对预算的费用支出趋势。

4、主要适用于集团企业的风险评估指标

- **每月分账人力投入。**企业每月直接或间接投入到分账工作的人天。
- **未分账资源类数。**未能实现有效分账的资源类型的数目。
- **未分账支出额。**每月未能实现有效分账的支出费用额度。
- **分账困难资源类数。**实现分账解决方案人力投入极大的资源类型的数目。
- **依赖分账的支出。**每月处于属于分账困难资源类的资源支出的费用额度。

治理预警信号

5、适用于所有企业的治理预警信号

- **成本管控承诺。**企业在云服务商的当年的预算为x元 。他们需要一种成本管理准则来确保企业不超过其支出目标p1%，例如10%，并且他们将支持好至少p2%，例如95%，的业务量。
- **百分比预警。**企业期望其云支出对于其生产系统是稳定的。如果某项业务员支出更改超过某个百分数 p%，则实施成本管控治理是一项明智的选择。
- **过度预配预警。**认为他们部署的解决方案的企业是过度预配的。成本管控治理是一项优先投资，直到正确地调整预配和资产利用率。
- **月度支出预警。**如果每个月的 x元的云支出被认为是一种很高的成本。 那么在给定月份中支出超过该数量，则需要实施成本管控治理。
- **年度支出预警。**具有年 IT R&D 预算的企业，可以在云试验中花费 x元。如果年预算不超过该数量，则采用云可做为一种实验性解决方案。如果超出预算，则需要实施成本管控治理，否则将影响上云项目本身的推进。

6、主要适用于集团企业的治理预警信号

- **分账人力投入预警。**如果每月直接或间接投入到分账工作的人天数超过 N 人天被认为很大，那么超过给定N人天的情况，则应该考虑实施成本管控治理。
- **未分账支出预警。**如果每月未能实现有效分账的支出费用额度超过x元, 则需要考虑实施成本管控治理。
- **分账困难支出预警。**企业每月应用分账解决方案投入的人力资源非常大，反映当前分账方案不具有可扩展性，每月处于属于分账困难资源类的资源支出的费用额度超过 x 元，则应该考虑实施成本管控治理。

治理原则

- 任何云部署都必须分配给具有已批准预算的计费单位和用于预算限制的机制。
- 具有分配的云预算的每个计费单位都将每年进行一次预算申请，以设置预算，每月调整预算，每月为审查计划与实际支出分配时间。每月与记帐单位主管讨论大于 20% 的任何偏差。为进行跟踪，将所有资产都分配

- 给记帐单位。
- 部署到云的任何资产都必须在可以监视利用率的程序中注册，并报告任何容量超过50% 的利用率。 任何部署到云的资产都必须以逻辑方式进行分组或标签，使治理团队成员可以在预配过度资产的任何优化方面与工作负荷所有者进行接洽。
- 直接影响客户体验的任何资产必须通过分组或标签进行账号。 在优化影响客户体验的任何资产之前，云调控团队必须根据至少90天的利用率趋势调整优化。 记录优化资产时考虑的任何季节性或事件驱动突发。
- 应将部署到云的所有资产与计费单元和应用程序或工作负载相关联。 此策略将确保你的成本管理学科有效。 应将部署到云的所有资产与计费单元和应用程序或工作负载相关联。 此策略将确保你的成本管理学科有效。 为进行跟踪，所有资产都必须分配给一个核心业务功能中的应用程序所有者。
- 出现成本问题时，将与财务团队建立附加的监管要求。
- 治理团队应每周对照计划监视一次所有云成本。 应每月与 IT 领导层和财务部门共享一次云成本与计划偏差报告。 IT 领导层和财务部门应每月检查一次所有云成本和计划更新。
- 为了实现问责，必须将所有成本都分配到业务职能部门。
- 应持续监视云资产，以发现优化机会。
- 云管理工具必须将资产大小选项限制为已批准的配置列表。 此工具必须确保所有资产都是可发现的，并受成本监视解决方案跟踪。
- 在部署计划期间，应记录与托管生产工作负载相关的所有必需的云资源。 此项记录有助于优化预算，并做好采用额外自动化的准备，以防使用费用更高的选项。 在此过程中，应考虑云提供商提供的不同折扣工具，如预留实例或许可证成本降低。
- 为了更好地控制云成本，所有应用程序所有者都必须参加关于优化工作负载的实践培训。

阿里云的最佳实践

不同于传统建设模式，云上资源采用按量付费的模式，因此成本管理需要持续地进行。通过资源目录和财务管理服务设定企业管理账号，为组织或单元下所有账号付费并管理账单；通过标签以不同的维度实现分账管理，以企业视角审查与管理云资源的成本和费用；通过成本管家等服务基于用量优化成本；通过API实现资源申请与企业财务流程的整合，不断的进行成本优化。更多详细信息，请参见财务管理与成本管家。

3、资源配置与审计治理

概述

资源配置与审计治理原则是五大类云上IT治理原则之一。这一类治理原则侧重于说明企业应该如何设计自己资源结构、设立标签从而结构化地管理自己的资源以及如何保证云上资源配置的合规性。企业的IT运维团队通常需要随时关注云上的基础设施资源和云上业务运行的情况，以保障业务要求。结构化和标签化地管理企业的云上资源，有助于IT运维人员查找、发现和统一管理云上资源。使用配置管理和审计工具，针对云上资源设定配置审计规则，则有助于企业保证云上所使用的资源与企业合规要求的一致性。本框架的这一节主要介绍资源配置与审计治理所应对的业务风险、常用的评估治理水平的指标、提醒治理团队关注资源配置与审计的预警信号和实施治理的常见原则。这一节的主要读者是企业的云架构师和云治理团队的其他成员。根据这些规则制定决策、策略和流程的过程中，应有负责设计和实施企业账号与权限系统的 IT 团队共同参与和讨论。

业务风险

1、适用于所有企业的业务风险

- 产生不必要的运营成本。已过时或未使用的资源或是在需求较低时间内预配过度的资源会增加不必要的运营成本。
- 预配不足资源。对于这类资源，高于预期需求的体验可能会在云资源不足以应对需求时，导致业务中断。

- 管理效率低下。缺少与资源相关联的一致的命名和标签元数据可能会导致 IT 人员难以查找用于管理任务的资源或账号与资产相关的所有权和计帐信息。 这样会导致管理效率低下，从而可能会增加成本并减慢针对服务中断或其他运营问题的 IT 响应速度。
- 业务中断。违反组织规定的服务等级协议（SLA）的服务中断可能会导致企业损失业务或其他财务成效。

2、主要适用于集团企业的业务风险

- 集团企业管理效率低下。缺少与企业组织账号结构相一致的命名和标签元策略，可能会导致 IT 人员难以针对不同企业部门应用不同的资源管理策略。
- 集团企业分权分账效率低下。缺少与企业组织账号结构相一致的命名和标签元策略，可能会导致 IT 人员难以实施有效的集团企业分权分账治理。

风险评估指标

3、适用于所有企业的风险评估指标

- **云资产。**云部署的资源总数。
- **未标签的资源。**没有所需计帐、业务影响或组织标签的资源数。
- **未充分利用资产。**内存、CPU 或网络功能完全利用的资源数。
- **资源消耗。**内存、CPU 或网络功能被负荷耗尽的资源数。
- **资源生存期。**自上次部署或修改资源以来的时间。
- **处于严重问题状态的虚拟机。**检测到一个或多个关键问题的已部署虚拟机的数量，这些问题必须解决才能恢复正常功能。
- **按严重性列出的警报。**已部署资产上按严重性细分的警报总数。

- **云提供商服务运行状况事件。**云提供程序导致的中断或性能事件数。
- **服务可用性。**云托管工作负荷实际运行时间与预期运行时间的百分比。
- **恢复时间目标（RTO）。**发生某个事件后，可接受应用程序不可用的最长时间。
- **恢复点目标（RPO）。**发生灾难期间，可接受数据丢失的最长持续时间。 例如，如果在单个数据库中存储数据并且未将数据复制到其他数据库，而是执行每小时备份，则最长可能会丢失一小时的数据。
- **恢复（MTTR）的平均时间。**在发生故障后，还原组件所需的平均时间。
- **间隔（MTBF）之间的平均时间。**组件在两次中断之间按预期合理运行的持续时间。可以通过此指标计算服务变得不可用的频率。
- **备份运行状况。**进行主动同步的备份数。
- **恢复运行状况。**成功执行的恢复操作数。

4、主要适用于集团企业的风险评估指标

- **未纳入组织管理的资源数。**没有用组织账号管理起来的资源总数。对于具有多账号的集团型企业，越多账号和相应资源放在组织账号下管理起来，则资源管理效率越高。
- **资源查找、分权分账人力投入预警。**企业每月直接或间接投入到资源查找、分权和分账工作的人天。

5、适用于所有企业的治理预警信号

- **标签和命名预警。** 如果一家企业的资源超出了 N 个资源，而缺少所需的标签信息，或者不是遵守的命名标准，则应该考虑投资于资源一致性学科，以帮助优化这些标准并确保将其应用到云部署的资产。
- **过度预配资源预警。** 如果企业使用少量的可用内存、CPU 或网络功能定期拥有超过某个百分数 p% 的资产，则建议投资资源一致性训练以帮助优化这些项目的资源使用情况。
- **预配不足资源预警。** 如果企业的资产量超过某个百分数 p% ，耗尽大部分可用内存、CPU 或网络功能，则

建议在资源一致性训练中投入投资，以帮助确保这些资产有必要的资源来防止服务中断。

- **资源生存期预警。** 如果企业的资源超过 N 个 ，超过了 N 个月未 更新，则可能会受益于资源一致性原则，旨在确保活动资源的修补和正常运行，同时淘汰过时或未使用的资产。
- **服务等级协议预警。** 不能满足其外部客户或内部合作伙伴的服务等级协议的企业应投资于部署加速规范以减少系统停机时间。
- **恢复时间预警。** 如果企业超过了系统故障后恢复时间所需的阈值，则应投入改进其部署加速规则和系统设计，以减少或消除故障或单个组件停机的影响。
- **虚拟机运行状况预警。** 如果企业有超过某个百分数 p% 的虚拟机遇到严重的运行状况问题，则应投资资源一致性训练来确定问题并提高虚拟机稳定性。
- **网络运行状况预警。** 如果企业的网络子网或终结 点的网络 子网或终结点出现连接问题，则应该投入资源一致性训练来识别和解决网络问题。
- **备份覆盖率预警。** 具有某个百分数 p% 的任务关键型资产且没有最新备份的企业可以从资源一致性训练科目中增加的投资中获益，以确保一致的备份策略。
- **备份运行状况预警。** 如果一家企业遇到超过某个百分数 p% 的还原操作失败，则应投入资源一致性训练来识别备份问题，并确保对重要资源进行保护。

6、主要适用于集团企业的治理预警信号

- **资源组织管理预警。**如果没有将资源按照组织账号结构管理起来，对于具有多账号的集团型企业，则可能影响资源管理效率。
- **资源查找、分权分账效率预警。**如果缺乏很好的标签和资源分组机制，匹集团企业的组织账号结构，则可能影响企业在云上进行资源查找、分权分账的效率。

治理原则

- 应该根据企业的组织结构、业务类型、资产环境等，定义资源分组和标签策略，并对所有资源应用分组和标签。
- 云治理团队应该明确定义建议的云资源部署工具，企业各部门选用的部署工具都必须与云治理团队选用的云资源部署工具兼容。
- 应该根据成本、业务关键性、SLA、应用程序和环境等相关的的属性，对所有资源打标签。所有标签值应该与云治理团队的预定义值保持一致。
- 部署到云的所有资产应该尽可能使用模板或自动化脚本进行部署。将实现以下策略：
  - 将为所有生产系统账号关键指标和诊断度量值，并且将对这些系统应用监视和诊断工具，由操作人员定期监视。
  - 操作将考虑在非生产环境（例如过渡和 QA）中使用监视和诊断工具来确定系统问题，然后在生产环境中出现这些问题。
- 应该激活资源配置审计功能，并根据资源配置策略设置配置审计规则，使用配置审计监控所有的资源配置变更。
- 企业应该利用资源配置审计功能满足两类管控需求。第一类为预防性管控，为符合企业合规准则，而禁止进行某些高危操作，如禁止外网链接，禁止创建未加密的磁盘等。第二类为发现性管控，如设置合规规则并对企业资源进行持续监控，发现不合规资源时，进行记录、报警乃至自动修复。
- 应该定期对资源配置审计告警和历史情况做审查，以确定资源资源配置审计记录下来的不符合规则的资源变更。
- 审计日志持久化：对云上操作、资源变更、网络流量等日志进行持久化保存，以备审计之需。

阿里云的最佳实践

当企业在云上部署业务后，资源管理是云上管理的重点。企业中的应用和云资源通常会按照团队、用途来划分，那么使用资源组便可以很方便的把云资源进行分组管理；同时，可以基于资源组进行授权。当然，在日常运维中可能需要按多个维度对云资源分类，标签Tag就是很好的工具，用于表示该资源的创建者、管理者、成本中心等。更多详细信息，请参见资源管理。

每一次资源变更需确认变更的合规性，若“不合规”需尽快察觉、确认影响范围并迅速修正。面对大量资源每日的运维变更，依赖人工无法保证合规性。阿里云配置审计帮助企业实现云上IT配置合规的持续性自主监管。更多详细信息，请参见配置审计。

4、安全基线

概述

安全基线治理原则是五大类云上IT治理原则之一。这一类治理原则侧重于说明企业应该如何在云上建立自己的安全基线作为企业上云的基础保障。安全性原则包含任何IT系统实施中都要考虑的安全问题，而上云也会引入其特有的安全问题。许多企业的业务有其特有的行业法规提出安全要求，企业上云时要优先考虑这些安全要求，以保护其敏感业务数据不遭受非法访问。安全基线规则目的在于确保将这些需求和约束始终如一地应用于云环境。本框架的这一节主要介绍安全基线治理所应对的业务风险、常用的评估治理水平的指标、提醒治理团队关注安全基线问题的预警信号和实施治理的常见原则。这一节的主要读者是企业的云架构师和云治理团队的其他成员。根据这些规则制定决策、策略和流程的过程中，应有负责设计和实施企业安全系统的IT团队共同参与和讨论。

业务风险

1、适用于所有企业的业务风险

安全基线规则尝试解决安全相关的核心业务风险问题。 与企业合作来确定这些风险，并在规划和实现云部署时监视每个风险的相关性。组织之间的风险有所不同。使用此与安全相关的常见风险列表作为云调控团队中讨论的起点：

- **数据破坏。**无意中泄露或丢失敏感云托管的数据可能会导致客户丢失、发出合同或产生法律后果。
- **服务中断。**由于不安全基础结构中断正常操作而导致的中断和其他性能问题可能会导致生产率损失或业务损失。

风险评估指标

2、适用于所有企业的风险评估指标

- **数据分类。**根据组织的隐私、合规性或业务影响标准，未分类的云存储数据和服务的数量。
- **敏感数据存储的数目。**包含敏感数据并应受保护的存储端点或数据库数。
- **未加密的数据存储的数目。**未加密的敏感数据存储的数目。
- **攻击面。**多少个数据源、服务和应用程序将由云托管。 这些数据源中分类为敏感数据源的数据源占多少百分比？ 这些应用程序和服务中属于任务关键应用程序和服务的应用程序和服务占多少百分比？
- **涵盖的标准。**安全团队定义的安全标准的数目。
- **涵盖的资源。**安全标准涵盖的已部署资产。
- **总体标准符合性。**符合性符合安全标准的比率。
- **受严重性的攻击。**中断云托管服务的多少种协调尝试（例如通过分布式拒绝服务（DDoS）攻击）是否可以进行基础结构体验？ 这些攻击的规模和严重性如何？
- **恶意软件防护。**已部署的虚拟机上安装了所有必需的反恶意软件、防火墙或其他安全软件的已部署虚拟机的

百分比。

- 修补延迟。由于虚拟机已应用操作系统和软件修补程序，因此已有多长时间。
- 安全健康建议。用于解决部署的资源的运行状况标准的安全软件建议数，按严重性进行组织。

治理预警信号

3、适用于所有企业的治理预警信号

- **任务关键型工作负荷预警。**将任务关键工作负荷部署到云的企业应对安全基线规则进行投资，以防止可能的服务中断或敏感数据泄露。
- **受保护的数据预警。**在云中托管可归类为机密、私有的数据或受到监管的数据的企业。他们需要安全基线规则来确保这些数据不会丢失、泄露或被盗。
- **外部攻击预警。**对于其网络基础结构的严重攻击，每月 N 次遭受严重攻击的企业可以从安全基线层面受益。
- **标准符合性预警。**超过超过 p% 个资源的企业的安全标准符合性应投资于安全基线层面，以确保在整个 IT 基础结构中一致地应用标准。
- **Cloud 房产大小预警。**托管 N 多个应用程序、服务或数据源的企业。 大型云部署可以从对安全基线规则的投资中受益，从而确保其整体攻击面得到适当保护，防止未经授权的访问或其他外部威胁。
- **安全软件符合性预警。**低于某个百分数 p% 的已部署虚拟机的企业安装了所有必需的安全软件。 安全基线规则可用于确保在所有软件上一致地安装软件。
- **修补预警。**过去 N 天内未应用 OS 或软件修补程序的已部署虚拟机或服务的企业。 安全基线规则可用于确保在所需时间内使补丁保持最新状态。
- **面向安全性的。**即使对于测试和试验工作负荷，一些企业也具有较高的安全性和数据保密性要求。 这些企业需要对安全基线规则进行投资，然后才能开始任何部署。

治理原则

- 部署到云的任何资产都必须具有已批准的数据分类。
- 在可以批准并实现足够的安全和治理要求之前，无法将任何使用受保护数据级别账号的资产部署到云。
- 在可以验证和控制最低网络安全要求之前，会将云环境视为外围网络，并应满足与其他数据中心或内部网络类似的连接要求。
- 所有已部署的资产必须按照重要程度和数据分类进行分类。 在部署到云之前，将由云调控团队和应用程序所有者查看分类。
- 用于存储或访问受保护数据的应用程序的管理方式不同于已经不使用的应用程序。 至少应对它们进行分段，以避免意外地访问受保护的数据。
- 在任何包含受保护数据的段中提升权限都应属于异常。 任何此类例外都将与云调控团队一起记录并定期审核。
- 治理工具必须仅将虚拟机部署限制为已批准的映像。
- 节点配置管理应尽量将策略要求应用于任何来宾操作系统的配置。节点配置管理应考虑到组策略对象中的现有投资 (资源配置的 GPO) 。
- 治理工具必须强制在所有部署的资产上启用自动更新。 必须同运维管理团队合作评审违反规定的情况，并按照运营策略予以纠正。 不自动更新的资产必须包含在归 IT 运维的流程中。
- 为任何任务关键型应用程序或受保护的数据创建新的订阅或管理组将需要云管理团队进行评审。
- 最小特权访问模型将应用于包含任务关键型应用程序或受保护数据的任何管理组或订阅。
- 安全团队应定期检查可能影响云部署的趋势和攻击，以更新云中使用的安全管理工具。
- 部署工具必须由云调控团队批准，以确保正在进行部署的资产的日常管理。
- 必须将部署脚本保存在云调控团队可访问的中央存储库中，以便进行定期检查和审核。
- 治理流程必须包括部署时的审核和周期性审核，以确保所有资产的一致性。

- 任何需要客户身份验证的应用程序的部署都必须使用与内部用户的主账号提供者兼容的已批准的账号提供者。
- 云治理流程必须包括账号管理团队的季度审查。 这些审查可以帮助识别云资产配置应阻止的恶意参与者或使用模式。
- 云提供商必须能够集成由现有本地解决方案管理的加密密钥。
- 将自动 DDoS 缓解机制部署到所有可公开访问的网络终结点。 不应向 Internet 公开由 IaaS 提供支持的面向公众的网站。

阿里云的最佳实践

虽然有了授权机制让使用者没有权限做不合规的事情，但在权限范围内使用者依然有可能由于多种原因作出错误的操作。因此，操作审计作为最后一道防线，记录所有发生的事情。一旦发生不符合预期的事情，IT部门有可以调出历史记录，追溯事故发生的原因。另一方面，为了避免事故发生，企业根据业界标准和企业过往的最佳实践，制定出内部IT规定，例如密码策略规定，公网访问规定等。通过配置审计配置和执行这些规则，确保企业持续处于“合规”的状态。更多详细信息，请参见操作审计。

在通过访问控制、审计、快照服务等阿里云平台默认安全能力建设企业云上安全基础配置后，应继续建设基础安全防护，帮助企业抵御外部攻击和入侵，提升主动安全防护能力。阿里云提供云安全中心、云防火墙产品实现云上统一安全管理。更多详细信息，请参见云安全中心和云防火墙。在基础安全防护之上，企业应根据具体业务情况进一步构建云上应用的安全能力并满足等保相关合规需求。

5、网络基线

概述

网络基线治理原则是五大类云上IT治理原则之一。这一类治理原则侧重于说明企业应该如何建立适合自己的云上网络架构。企业利用云提供商提供的虚拟网络产品，建立起匹配自己租户和业务要求的网络架构。企业在线下有自己的网络架构隔离不同的办公网络和业务服务网络，这些网络之间或者需要相互安全隔离保证数据安全，或者需要相互建立高速连接满足业务性能需要，上云之后企业也有相应的要求构建相应的网络区域。本框架的这一节主要介绍网络基线治理所应对的业务风险、常用的评估治理水平的指标、提醒治理团队关注网络架构问题的预警信号和实施网络基线治理的常见原则。这一节的主要读者是企业的云架构师和云治理团队的其他成员。根据这些规则制定决策、策略和流程的过程中，应有负责设计和实施云上网络架构的 IT 团队共同参与和讨论。

业务风险

1、适用于所有企业的业务风险

- **不必要的运营成本。** 已过时或未使用的资源或是在需求较低时间内预配过度的资源在某些情况下会增加不必要的运营成本。
- **业务中断。** 违反组织规定的服务等级协议（SLA）的服务中断可能会导致企业损失业务或其他财务成效。

2、主要适用于集团企业的业务风险

- **集团企业内部通信不必要的运营成本。** 已过时或未使用的资源或是在需求较低时间内预配过度的资源在某些情况下会增加不必要的运营成本。
- **集团企业内部通信业务中断。** 违反组织规定的服务等级协议（SLA）的服务中断可能会导致企业损失业务或其他财务成效。

风险评估指标

3、适用于所有企业的风险评估指标

- **公网IP数量。**企业拥有的公网IP数量。
- **对外网提供服务的业务应用数量。**企业对外提供服务的业务应用的数目。
- **VPC数目。**企业在云上所管理的虚拟专有网络（VPC）的数目。
- **子网数目。** 企业在云上所部署的子网的数目。
- **地域数量。**企业业务部署的VPC网络所处于不同的地域，地域越多，复杂性越高。

4、主要适用于集团企业的风险评估指标

- **需要内部打通的VPC链接数目。**企业业务部署的VPC网络所处于不同的地域，地域越多，复杂性越高。
- **企业内部通信造成的公网流量。**为了满足企业内部不同VPC之间通信，产生的公网流量。

治理预警信号

5、适用于所有企业的治理预警信号

- **不正常的网络链接。** 存在网络连接问题的资源数。
- **不正常的服务终结点。** 与外部网络终结点有关的问题数。

6、主要适用于集团企业的治理预警信号

- **企业内部通信造成公网流量预警。**为了满足企业内部不同VPC之间通信，产生的公网流量，每月超过了 N GB。

治理原则

- 云提供商必须能够支持现有的边缘设备解决方案和任何所需的配置，以保护任何公开的网络边界。
- 云提供商必须能够支持与全球 WAN 的共享连接，并通过现有边缘设备解决方案路由数据。
- 不允许通过公共 Internet 或跨数据中心直接访问包含受保护数据的子网。 对这些子网的访问必须通过中间子网进行路由。 所有对这些子网的访问都必须通过可执行包扫描和拦截功能的防火墙解决方案。
- 包含受保护数据的网络子网必须独立于任何其他子网。 将定期审核受保护数据子网之间的网络流。
- 治理工具必须审核和强制执行安全管理团队定义的网络配置要求。

阿里云的最佳实践

对于企业来说，通过网络架构规划，建立网络与业务方分工机制，实现成本和效率的兼顾。对生产网和办公网进行隔离，对不同业务采用隔离或打通。初创企业通过简单的网络结构，中型企业将网络服务化，制定安全路由规则，通过服务化支撑业务。组织更复杂的企业，还将涉及到多集团或多地域的打通。更多详细信息，请参见企业级云上网络解决方案。

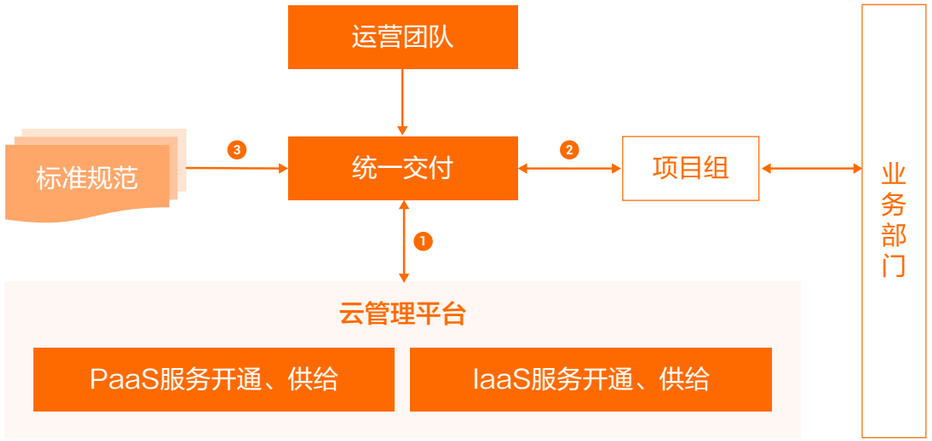
3 云上管理体系

1 云上运营体系建设

1、云上运营管理

统一交付

负责云平台技术服务及基础资源开通及供给。负责云平台统一环境配置及管理。负责云平台测试环境配置及管理，统一生产环境应用部署管理。缩短需求到交付的开发周期，保证交付质量，降低程序部署风险。为开发项目组提供高度集成、自动化的工具，支持组件及应用的敏捷开发以及实施过程管理。



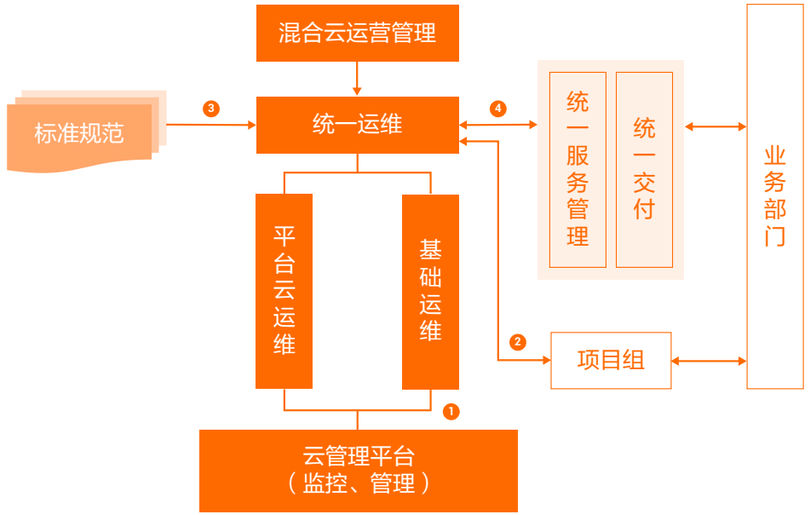
1、管控：负责云平台技术服务及基础资源开通及供给；负责云平台统一环境配置及管理；负责云平台测试环境配置及管理，统一生产环境应用部署管理。采用适合不断变化的能力的体系结构和发展实践；主动监控和管理需求,使基础架构资源与不断变化的业务需求保持一致；在各种压力下定期加载测试应用,为未来做好规划。

2、协同：为各项目组提供需要的工具和技术支持，实现项目开发过程的自动化和可视化。

3、遵循：统一交付服务对项目的开发配置，构建，测试和部署发布均需要遵循云平台管理统一标准规范。

统一运维

云平台云运维（PaaS）以及基础运维（IaaS），负责云平台技术服务运维以及基础资源运维、统一监控，负责云平台相关的网络及安全运维。



1、监控及管理：统一运维能力提供包括云平台云及基础设施的统一监控、管理，负责云平台技术服务运维及基础资源运维，同时配合支持项目组应用运维。收集、存储和分析数据日志,以关联事件,以自动检测问题、隔离根本原因和自动修复。利用更高的自动化、预测性性能分析来制定潜在的补救措施并自动部署解决方案。

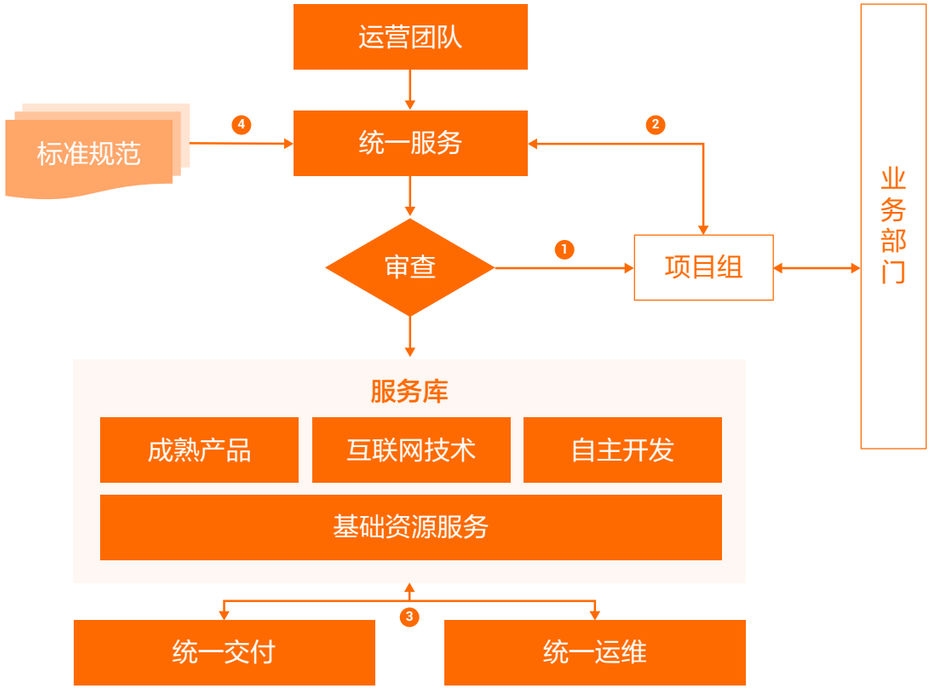
2、协同：为各项目组提供需要的应用相关的监控信息及日志信息，提供各项目组应用运维过程的自动化和可视化能力。

3、遵循：云平台统一运维需要遵循运维管理标准规范。

4、支撑：配合统一服务管理、统一交付管理提供云平台资源、技术服务的相关技术支撑。

统一服务

云服务目录管理以及技术服务和基础资源服务的统一运营，负责云平台运营管控职责，包括服务规划、容量规划，入云标准及技术标准、安全及合规管理，服务订单管理、计量计费及结算、服务目录、服务发布、SLA管理，预算、采购及供应商管理。



1、管控：云运营团队通过统一服务管理对服务内容做全生命周期的管控，基础资源的监控及运维，并对项目组/统一运维/统一交付提供技术服务、基础资源服务统一管理。评估基础架构资源的运行状况和利用率,以避免云资源的浪费,实现有效的成本管理。通过指标和KPI监控和管理应用程序的性能和可用性,以保持服务级别。

2、支撑：对项目组的技术方案及资源申请进行评审，并对日常项目组的协同支持。例如培训、需求管理、方

案审查、评价处理、服务/资源申请管理、技术指导等。

3、协同：统一服务全生命周期，需与统一交付能力及统一运维能力进行协同，统一协调两个组对外提供服务支撑。

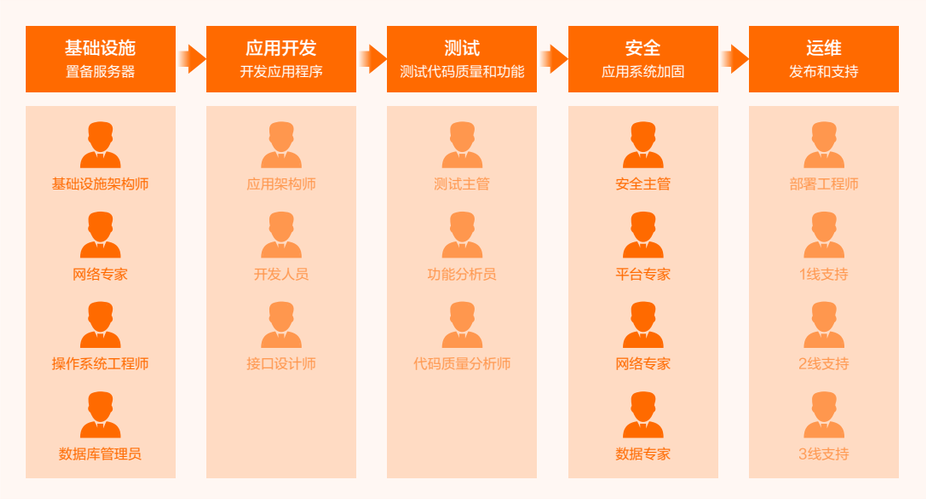
4、遵循：统一服务对项目组的建设方案的审查、基础资源的实施、架构的设计及服务管理均需要遵循云标准规范。

2、云服务组织管理

企业当前IT服务组织的特点

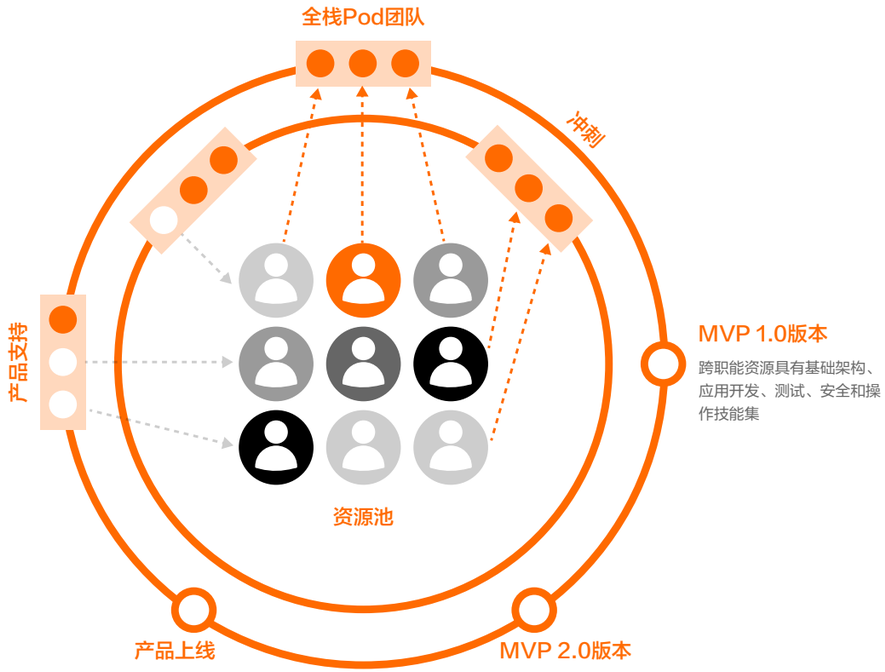
分层的组织结构，导致标准分层地应用程序架构，例如：UI层、应用程序层、数据库层和基础设施层。有限的跨职能协作导致紧耦合的应用程序、缓慢的开发周期和大版本发布应用。当前的客户及业务部门支持模式呈现出一种“竖桶式”孤立的结构，导致各团队包含相同的技能集，关注可靠性而不是创新和变革。

需要新的、高绩效、敏捷的团队和运营模式，敏捷的组织围绕高绩效团队进行协作，以减少协调问题并建立共享责任制。



企业内云服务组织管理的特点

业务、应用程序和基础设施团队组成敏捷的pod团队，从而加强协作（DevOps），和更快速的部署。流畅的团队结构可产生松耦合和高弹性的应用程序，从而更好地满足客户需求。



未来的客户及业务部门的支持模式是动态的、高度行动化的团队结构，侧重于不同团队间包括sprint和个人发展的合作。

建议企业采用新一代云运营模型通过关键职能的划分，为创建与IT组织目标密切相关的运营模式提供了战略框架。基础服务团队从传统的IT基础设施支撑转向交叉协作、高度敏捷的团队来保证资源供给和自动化运维。

随着企业云服务的使用范围扩大，公共云使用逐步深入，基础服务团队将重新分配，因为他们现有的大多数“置备”和“运维”工作将自动化。资源和技术能力将更多的体现在“赋能”和“创新”上。

业务产品团队

- 是敏捷的、以客户为中心的团队拥有跨职能的能力。这些团队将拥有整个产品生命周期，包括设计、交付和运营；
- 从产品待办事项中创建和确定用户情景的优先级；

- 设计应用程序、数据和基础设施架构；
- 实施DevOps/敏捷流程；
- 通过借助平台共享服务（例如API）持续集成和编码用户情景；
- 创建和执行自动测试用例；
- 使用预定义的脚本/模板按需置备。

平台服务团队（云COE团队）

- 支持共享服务，并为组织内的创新领域建立卓越中心；
- 构建产品团队使用的服务型产品；服务型产品的配置、修补和强化;
- 为产品团队建立创新框架，以在整个冲刺（即自动化）中利用；
- 确保产品团队（即IaaS、PaaS、SaaS）的平台产品的可用性和安全性。

基础服务团队

- 是共享的业务功能，在业务产品工程设计期间建立并在产品之间共享；
- 部署产品团队所需的硬件、网络和业务流程组件；
- 用于应用程序项目的基础设施架构;手动配置核心基础设施组件;
- 持续技术和支持;基础设施安装和配置;
- 配置、修补、强化和维护核心基础设施资源。

站点可靠性工程SRE

- 运维自动化；
- 事件管理和产品故障排除；

- 提供主动的稳态支持；
- 创建和执行脚本以自动解决事件；
- 将50%的时间花在工单、待命、手动工作;50%实现现有手工流程自动化。

云业务管理办公室

- 根据业务需求制定IT战略/愿景；
- 定义企业架构；
- 完成项目和治理计划；
- 建立业务和治理控制；
- 定义总体项目计划和路线图。

技术管理办公室

- 设计适用于产品、平台和基础设施的架构标准；
- 实施并推进治理、合规性和安全控制。

阿里云最佳实践

阿里云推出业内领先的面向企业的一站式研发提效平台，历经阿里集团众多业务打磨，覆盖研发测试全流程，通过研发综合效能管理和专项自动化提效工具，提升研发效能，降低研发成本，支撑技术团队实现真正的CI/CD和独立交付。更多详细信息，请参见DevOps解决方案。

3、多云管理策略

企业的多云管理策略

通过实现多云管理，无论在Paas层的云上组件,如消息服务，迁移服务，应用服务，分析，机器学习，管理安全，移动服务，效能管理，IoT，还是基础的数据库，网络，存储，计算，都可以横向再多个云厂商之间进行选择，例如再多个云厂商提供的不同的可用去进行应用部署，实现跨云的高可用架构，进一步提高企业业务的可靠性。通过多云管理策略的实现，可以为企业带来如下优势发送到：

- 减少云服务商锁定;
- 可以设计更适合用途的解决方案/堆栈;
- 不太容易受到产品更改的影响;
- 许多服务中的功能和功能受限;
- 更快地迁移应用程序;
- 需要不断评估保留实例的需要;
- 实现企业业务的快速创新;
- 可重复使用的技术堆栈，更少的内部工程;
- 赋予开发人员权力;
- 减少故障排除和维护;
- 减少复杂on-premsoftware软件维护;
- 跨服务无缝集成。

多云环境下通过容器实现应用可移植性

一组封装的应用程序及其所有的依赖环境，包括数据库、代码、配置文件、以及其他支撑运行的所有服务。利

用标准化容器服务，可实现应用程序在不同的异构环境中迁移。通过容器实现应用的跨云部署，优势体现在下面三个方面：

1.生产力：自动化、标准化的预配置容器和策略驱动的业务流程使开发人员能够专注于日常工作。

2.可移植性：能够在独立于硬件的不同云环境之间对应用系统进行迁移。

3.利用率/轻量：能够根据购买的计算能力容纳更多应用程序,避免资源浪费。

4、云管理平台

企业可以通过统一多云管理平台对企业数据中心和公共云资源进行管理。未来企业基于多云管理模式下的服务，Iaas、Paas及Saas服务，通过统一的运管平台进行管理，用户可以通过云管理门户访问服务目录，去使用这些服务。

云服务统一管理

通过统一云管理平台为企业提供对私有云资源和多个公共有云资源的统一管理能力，例如，资源配额统一划分，统一计量，统一Web控制台。支持纳管资源包括：云主机、云硬盘、私有网络、路由器等。

提供统一视角的混合云管理、容器服务、智能运维、第三方资源纳管，以发挥异构云的优势，提高IT运营效率、优化IT成本。

多云适配

针对不同的云环境，云网关会进行授权验证、路由转发、数据转换、API调用等一系列操作。最终是调用对应云环境的API，将结果数据转换为云管平台的数据模型，来实现不同云资源的操作。

服务编排

通过服务编排实现细粒度的服务组合，提供不同权限级别的自助服务目录设计，提升客户体验。

通过一种通用的编排框架，在目标主机上获取任务，下载脚本，执行并上报结果。实现了基于资源拓扑来编排应用，编排资源，包括虚拟机，端口，网络，路由器，安全组等；编排应用，运行程序或者脚本，搭建，配置和管理应用API网关：请求经过API网关转发到后端编排服务，在转发请求前，验证该用户有无权限。

编排服务：统一管理所有编排模板和它们所生成的实例。根据请求的不同，将请求分发到不同的微服务，如：资源服务，Kubernetes等。

应用/资源编排：负责基础资源的编排（云主机、网络等），对接资源服务和裸机服务。也可以用于更高层的应用编排。

容器编排：负责容器编排，对接KubernetesAPI。

计量计费

统一云管理平台通过计量计费功能实现精细化运营。计量计费模型可实现如下功能：

实现资源维度、计量对象、计量单位等计量模型，计量模型可动态扩展，计量模式可以自定义组合，统一标准计量，方便其他服务使用，灵活的计费方式，计费项可自定义，根据计费项分类，可对计费项进行业务组合，付费方式多样：按使用时间、按使用量，支持计费方式互转，计费报表自定义，多维度展现，支持按数据中心对各类资源设置单价，支持从多个维度统计费用，按数据中心、按资源类型、费用趋势、月账单明细等，统计费用环比，为费用预测提供依据，支持平台全局、数据中心、项目月账单报表导出，通过费用反映资源的使用量及分布情况，为成本支出提供数据，为成本优化提供依据。

2 云上运维体系建设

1、云上运维服务管理

企业云上IT运维服务能力

通过多级服务管理，为客户提供解决方案，全面释放企业云IT运维服务能力。

业务流程与一级服务支持

关键用户自助
服务请求 | 应用操作 | 应用变更 | 资源申请 | 测试

1级呼叫管理
呼叫路由 | 呼叫优先级 | 呼叫监控 | 初步诊断

应用管理

2级应用程序操作支持
系统监控 | 批量作业管理 | 服务台 | 系统技术支持 |系统问题记录

3级应用程序维护
Devops | 配置 | 分析 | 补丁 | 调优 | 性能监控 | 供应商协调

4级应用程序开发
系统生命周期管理 | 架构设计 | 项目开发实施 | 升级项目 | 应用迁移

基础设施、网络与云服务管理

数据中心、云运营和系统管理

安全 | DBA | 备份和恢复 | 资源管理 | 容量管理 |运营分析 |事件和变更管理

基础设施网络管理（LAN/ WAN）

安全管理 | 存储 | 网络配置 | 网络监控 |资源和能力分析 | 性能调整和故障解决

云基础设施平台

基础设施支持 | 事故管理 | 性能管理 | 云服务商协调 | 工单管理 | 成本分析与优化

云上IT运维服务管理

随着企业的应用系统逐步迁移到云环境中，必须考虑深化应用ITSM，以确保服务继续满足预期。IT服务管理（ITSM）是一种以服务为中心的方法，用于设计、交付、监视和改进向业务交付IT服务和功能的方式。ITSM包含所有流程、人员和技术，用于向业务交付高质量的服务，以满足战略目标。主要包括以下内容：

- 促进一种IT管理理念的转变，将企业内部云管理部门视为给生产和销售等业务部门提供的内部服务的支持机构，并将其视为服务供应商来看待和管理；
- 使IT服务和功能与当前的业务需求保持一致，并积极预测其未来的需求；
- 将IT从成本中心重新定位，并逐步演进为将IT视为业务的战略伙伴的运营模型；
- 在设计和交付IT功能时，鼓励IT服务人员从外向内持续关注最终用户的业务视角；
- 为企业内部提供一致的、高质量的IT服务，以成功地管理所有事件、问题、更改和升级。

随着企业全面上云，ITSM和ITIL（即Information Technology Infrastructure Library，信息技术基础架构

库，是全球公认的一系列信息技术（IT）服务管理的最佳实践）的最佳实践仍然是相关的，因为每个组织应该继续关注于使用过程方法来持续交付IT服务。云环境中的IT服务管理主要包括：事件和问题管理、变更和发布管理、资产和配置管理，同样具有云服务的特点。

事件和问题管理

根据ITIL最佳实践的定义，事件管理主要是组织开展相关活动，旨在识别、分析和修复问题/中断，防止将来再次发生。在事件处理过程中，几乎总是一个专门的团队在现场处理事件，记录、分类和调查事件。同时，根据KPI跟踪绩效，例如首次联系解决、每次联系的成本、客户满意度等。

问题管理主要是分析处理一起或多起事件的原因。在创建问题记录时，事件原因通常是不知道的。在问题处理过程中，并不总是有专门的团队来处理问题，调查并记录事件的根本原因。通常，跟踪绩效所根据的KPI不会与事件团队的具有相同颗粒度。

随着企业应用上云，传统事件和问题管理流程在云端发生了变化，需要运营团队进行重新思考。

事件管理关键因素：

- 事件团队主导，与云服务提供商合作，确定在事件发生时相关产品与服务的RACI模型（即RACI Model，是在专案管理或组织改造时常用的工具，主要是用来定义某一项活动参与人员的角色和责任，是一个简单有效的工具）；
- 考虑与云服务提供商深度合作，实施自动化运维服务机器人和虚拟工程师来处理事件，提高事件处理效率；
- 重新评估当前的KPI，并为组织无法直接管理与控制的云上的产品、工具及服务的事件解决指标设定可实现的期望值；
- 仔细审查SLA，以进一步明确云服务提供商和企业云服务团队在事件管理过程中的责任划分。

问题管理关键因素：

- 与云服务提供商加强合作，协商合理的能够满足企业需求的SLA；
- 充分了解云服务提供商的问题管理流程，并与内部问题管理流程进行比较，进行融合与匹配，满足IT服务管理的需要；
- 仔细审查SLA，根据问题原因分析的结果，进一步明确云服务提供商和和企业云服务团队以及企业内部业务部门、云服务使用部门在问题管理过程中的责任划分。

变更和发布管理

变更管理主要是添加、修改或删除任何可能对IT服务产生影响的内容，并利用一套标准流程来控制和监控变更流程，最大限度地降低变更对用户和服务的整体影响。在变更管理过程中，对于提出的变更申请，根据收益和风险评估并确定其优先级；在部署到生产环境之前测试变更内容，并且确保一旦变更失败有应急计划；更新配置管理系统以反映全部变更；记录变更并跟踪变更管理绩效KPI。

发布管理：除了测试和部署发布流程之外，还包括计划、安排和控制系统建设的流程，并利用一套标准流程和步骤确保成功有效地在生产环境中发布。在发布管过程中，采取发布计划并进行影响分析，以确定变更的影响范围和受影响人员；进行可靠的风险分析，并记录潜在影响；测试并部署发布需要与变更管理同步，以确定发布时间表和受影响用户；检查新发布功能的性能，收集用户反馈并跟踪发布绩效KPI(例如成功发布的数量）。

随着企业应用上云，传统变更和发布的管理方法及流程在云端发生了变化，需要运营团队进行重新思考。

变更管理关键因素：

- 与业务开发团队和运营团队合作，收集对当前流程的反馈，以了解潜在变更的影响；
- 在实施变更之前，与主要的IT利益相关方进行调查和圆桌会议，收集反馈并支持对当前变更管理流程的所有

改变；

- 与云服务提供商协作，开发RACI模型并明确沟通、部署和记录变更的流程。

发布管理关键因素：

- 与开发和运营团队合作，识别确定当前流程中的低效率和改进领域，并集体头脑风暴讨论解决方案；
- 收集IT利益相关方的反馈意见，从发布的角度了解其需求，并与云服务提供商合作以满足消费者需求；
- 重新评估当前的KPI，并为组织无法直接控制的工具的发布指标设定可实现的期望值。

资产和配置管理

IT资产管理：管理，优化和跟踪组织内购买，部署，维护，使用和处置软件应用程序的一系列流程。在IT资产管过程中，要确保IT组织控制下的资产在整个资产生命周期内可被识别和控制；同时通过准确的IT资产信息来支持服务管理流程，确保IT资源管理作出明智决策。通常情况下，企业会为IT资产进入环境建立一个单一门户；适当标记IT资产并在部署到组织环境之前更新配置管理数据库(CMDB)；协调CMDB数据与发现数据，以确保准确记录和更新IT库存；实施强健的资产处置/回收流程，确保CMDB反映准确的资产处置信息。

配置管理：系统工程流程，用于在产品的整个生命周期内建立和维护产品的性能，功能和物理属性，设计和操作信息的一致性。配置管理主要是识别，控制，记录，报告，审核和验证服务以及其他配置项，同时在服务生命周期负责、管理和保护资产配置的完整性。在CMDB中记录当前资产的详细清单，针对从CMDB添加，更改或删除的所有配置更改，设计并实施严格的管理政策和程序；监控并记录所有建议的配置更改的状态，并更新CMDB以保持准确性；定期审核CMDB并记录/报告CMDB与当前环境之间的所有不一致之处。

随着企业应用上云，传统IT和配置的管理方法及流程在云端发生了变化，需要运营团队进行重新思考。

变更管理关键因素：

- 实施并执行IT资产，主要是云上的IT资产回收政策，并将变更在原有的范围基础上，传达给更广泛的组织；
- 针对云上的产品与服务，要仔细检查并更新当前的财务管理和退款政策，以确保能够使用性能更好，性价比更高的云产品与服务；
- 审核并优化当前的IT资产需求管理流程，为应用上云做好准备。
- 发布管理关键因素：
- 与云服务提供商合作，了解如何在云环境中管理配置更改；
- 检查并优化CMDB当前的更新流程，并与云服务提供商合作，记录何时进行更改；
- 充分了解云服务提供商的配置管理工具，并进行集成。

阿里云最佳实践

阿里云在全球领先的云基础产品的基础上，提供应用实时监控服务、云监控、应用高可用服务、智能顾问、日志服务等云上运维产品，便于企业了解阿里云上的资源使用情况、业务的运行状况和健康度，在云上进行应用性能管理与端到端的全链路追踪诊断等。

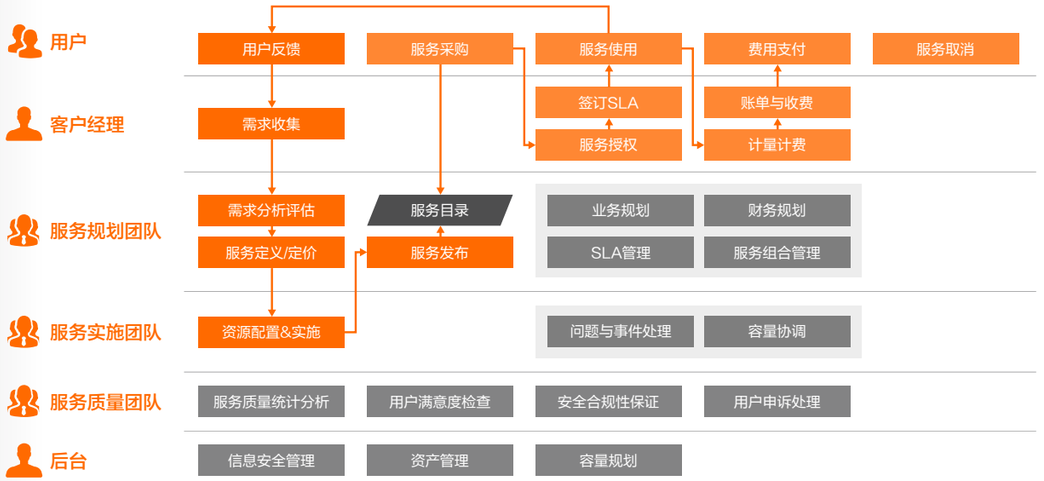
通过帮助企业解决系统运行中遇到的问题，并进行深层次分析，持续进行架构优化，大幅提高企业在阿里云上的运维能力。

更多详细信息，请参见云上运维工具。

同时，阿里云提供运维服务，代表企业客户运营阿里云基础设施，充分利用阿里巴巴集团最佳实践帮助客户做好云上资源运维管理，降低运维开销和风险，提升安全性和稳定性，让客户能够更专注于企业业务发展和战略规划。更多详细信息，请参见运维服务。

流程与服务请求管理涉及用户、客户经理、服务规划团队、服务实施团队、服务质量团队和后台，从前到后共

六个层次。其中用户层主要涵盖服务采购、服务使用、费用支付、用户反馈等。客户经理层主要涵盖服务授权、签订SLA、计量计费、账单与收费、需求收集等；服务规划团队主要涵盖业务规划、财务规划、SLA管理、服务发布等；服务实施团队主要涵盖问题与事件处理、容量协调、资源配置与实施等；服务质量团队主要涵盖统计分析、用户满意度检查、安全合规性保证以及用户申诉处理；后台主要涵盖信息安全管理、资产管理、容量规划等。

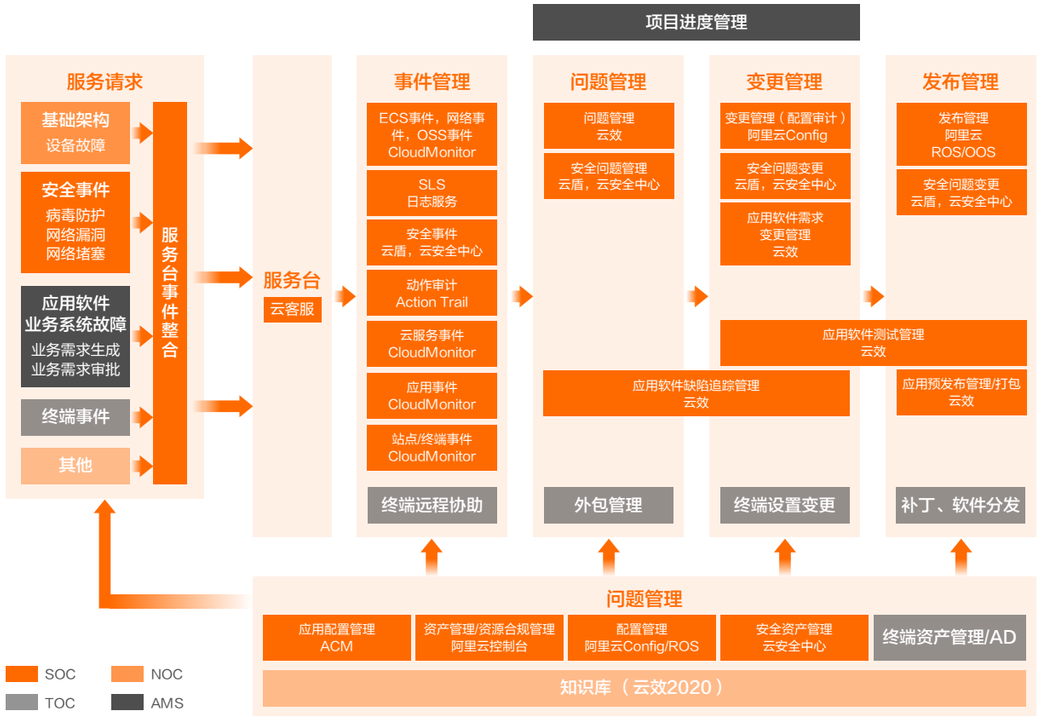


对于事件管理，利用CloudMonitor管理ECS事件、网络事件、OSS事件、云服务事件、应用事件以及站点/终端事件，利用ActionTrail管理动作审计。对于问题管理，利用云效进行问题管理和应用软件缺陷追踪管理，利用云盾和云安全中心进行安全问题管理。

对于变更管理，利用阿里云Config进行变更管理，利用云效进行应用软件需求变更管理和应用软件测试管理。对于发布管理，利用阿里云ROS/OOS进行发布，基于云盾和云安全中心进行安全基线/发布，利用云效进行应用

预发布管理/打包。

对于配置管理，利用ACM进行应用配置管理，利用阿里云控制台进行资产管理/资源合规管理，利用阿里云Config/ROS进行配置管理，利用云安全中心进行安全资产管理，利用云效2020进行知识库管理。



服务支持

阿里云打造完整的服务体系，为用户提供多种技术支持和服务保障，让用户上云更轻松，云上更高效。

阿里云提供7*24小时售后支持服务：

- 智能在线：智能诊断，秒级解答，推荐最佳解决方案或匹配合适的人工渠道。
- 电话咨询：咨询工程师即时解答云产品及业务咨询问题。
- 钉钉咨询：移动端支持小助手提供更便捷的服务体验。
- 技术工单：技术工程师即时解答云产品及工程技术问题。

除此之外，阿里云还拥有多种专家服务和支持计划，为企业提供由专属企业群、专属技术服务经理(TAM)等组成的专属支持与服务。更多详细信息，请前往阿里云支持与服务。

2、云上运维SLA

云运维SLA重点考虑内容

企业云服务团队在进行云上运维过程中，在确定SLA关键服务等级协议时，应重点考虑一下内容：

- 角色与职责

明确规定各方在 SLA中的职责，包括：负责监督合同、审计、绩效管理、运维和安全；定义关键术语,包括激活日期、性能,沟通并确定云计算术语定义中的任何歧义。

- 覆盖领域

明确规定了覆盖范围,包括但不限于数据的可用性、性能、安全性/隐私以及位置、可移植性和可访问性。

- 绩效衡量和报告

明确定义企业云服务团队绩效指标,包括但不限于服务级别、容量和能力、响应时间等，以及云服务提供商将如何监控和报告这些指标；明确指定云服务提供商如何以及何时报告故障和中断，以及提供商如何补救此类情况并降低重复发生的风险。

- 安全标准

明确指定云服务提供商如何管理安全标准；明确指定云服务提供商为保护数据可靠性、数据保留、数据隐私等数据，而必须满足的安全性能指标；明确指定可以执行审核，以确认云服务提供商的性能和安全标准。

- 数据所有权与管理

明确指定数据所有权驻留在请求云服务的组织；明确指定如何在SLA的整个期间管理数据和网络，以及如何在服务退出/终止的情况下将其转换回来。

- 处罚和例外

明确规定可执行后果的范围，如对不遵守 SLA 绩效措施的处罚等。

关于阿里云产品服务等级协议，请参见服务等级协议。

云运维SLA提升

企业云SLA服务水平等级应随时间推移而变化,从基础水平开始,并逐步提高标准。建议整个SLA提升通过四个阶段完成:

- 阶段 1：基线
  - 收集指针以确定初始性能级别
  - 将绩效与期望的结果和基准进行比较,以确定具体的绩效目标
  - 指标不会在 IT 外部传达
  - 工具和范本简单且可能手动
- 阶段2： 实践
  - 生成指标加入商业伙伴关系协议,并传达给企业
  - IT 领导使用简单的指针来确定性能问题
  - 工具和模板内置于流程中,并作为日常工作的一部分进行更新,自动化程度不断提高
  - 启动常规报告和回馈程序
- 阶段3： 提高
  - 服务确定级别差异并创建具体的改进行动计划
  - 服务等级目标进行调整,通常增加以满足客户的 IT 和业务目标
  - 性能管理工具与系统数据系结,且大部分是自动化的
  - 绩效管理流程已投入运行
- 阶段4：优化
  - 实施改进措施,确定结果,确定新目标
  - 单个性能衡量系统到位
  - 连续测量和收集资料是完全自动化的
  - 基于成果的奖励措施已经到位

3、云上运维监控管理

云监控所遇到的挑战

为了建立更好的云服务可视性和管理，健康和性能监控以及报告的基本组件需要适应云运维要求。传统的运维监控方法，在云环境中以下关键因素会遇到相应挑战：

如何进行拓扑搜索？ 部署环境分布在本地和云端。虚拟机在多个服务器间不间断运行，形成承载应用程序服务的基础设施资产的动态拓扑。

如何绩效应用程序性能监控？ 混合云基础架构本质上是动态的，由特定领域的监控工具进行监控和管理–每个工具可自主运行；应用程序可以部署在多重来源（本地、 SaaS, PaaS, IaaS ）上，并且可供分布在不同地理位置的终端用户访问。

如何实现基础设施可视？ 无法直接管理和控制诸如网络、服务器、存储和操作系统等云提供商资产；物理和虚拟单元的资源消耗需要具有可视性；由自助服务和弹性伸缩导致云资源的无节制扩散将使得可视性和控制力的降低，导致云服务散乱。

如何实现数据融合与性能分析？ 混合环境是多层结构，具有多个孤岛和平台；每个供应商提供的数据日志和格式各不相同。

如何实现解决方案自动化？ 如何通过事件驱动的自动化扩展至自动修复，自动化执行基于操作事件（如警报）的操作工作流，并且通过预防、帮助修复或修复问题的操作响应事件。

云监控的重点领域

为全面监控各类资源与服务，需实现针对拓扑搜索监控、应用程序性能监控、基础设施可视、数据融合与性能

分析、解决方案自动化五大领域开展监控。

对于拓扑搜索，基于应用程序组件和端到端依赖关系的自动发现和映射，构建本地和云端资产及其相互关系的整体视图。

对于基础设施可视，利用管理平台监控物理和虚拟计算环境，通过合并工具自动发现添加的新主机和实例并跟踪其KPI，与云服务提供商的API集成以提升云资源性能和利用率的可视性，支持监控并预警云资源利用率。

对于应用程序性能监控，通过集成监控工具充分了解应用程序流，隔离应用程序瓶颈并提供整体视图。

对于数据融合与性能分析，将离散监控系统孤岛数据组合到关联引擎和报告仪表盘中，以提供整体性能的全局性图景。通过自动化监控解决方案实现跨领域洞察，支持关联和分析全部数据，利用智能检测异常避免影响关键应用程序。

对于解决方案自动化，基于性能分析预测功能，主动定义补救措施，并适时支持自动部署解决方案。

云监控报告KPI

建议在云运维中需要对经营业绩和运行性能这个两大类的多个KPI进行监控和追踪，并对KPI进行适当提升。

类别	KPI	描述
经营业绩	增加的业务服务数量	由应用程序监控衍生的洞察带来的新增业务服务数量
	获得的客户数量	由于应用程序性能/可用性增加的新客户数量
	客户流失数量	由于应用程序性能/可用性丢失的新客户数量
	客户留存率	随着时间的推移，保留的客户的百分比

表：上云可行性评估结果示例

类别	KPI	描述
经营业绩	收入增长百分比	由所得洞察带来的总收入增长百分比
	交易/失败的数量	成功/失败的端到端客户交易数量
	客户满意度	由于体验优化带来的客户满意度的提升
运行性能	可用性	应用程序/服务对客户的可用性百分比
	响应时间	从客户发起请求到收到预期响应，完成这一过程所需要的时间
	正常运行时间	应用程序或系统正常运行时间所占的百分比
	利用率	与总计算能力相比实际使用的计算资源量
	MTTD (平均检测时间)	从事件发生（例如计划外中断、服务障碍等）到检测到该事件所需要的平均时间
	MTTR (平均恢复时间)	从事件发生（例如计划外中断、服务障碍等）到解决该事件所需要的平均时间
	MTTB (平均故障间隔时间)	给定时间段内设备故障间隔的平均时间。它表示设备预期故障率的可靠性等级
	事故造成的中断百分比	相对于服务时间，由于云环境中发生事故导致中断（不可用）的百分比

- 云监控成熟度模型

云监控包含资源监控和服务监控。需要实时掌握各种资源和服务的健康状态，帮助企业快速发现与定位问题。云监控成熟度模型是一种重要的分析工具，基于该工具可判断出企业的云监控水平，有利于企业准确定位当前所处阶段，明确下一步云监控工作的改进方向。云监控成熟度模型分为三个阶段，如下表所示：

	阶段一 反应式	阶段二 主动式	阶段三 预测式
报告人	最先由最终用户经常地报告问题	网络操作中心或系统管理员在问题发生之前使用仪表盘发现问题	自主修复工具会在问题发生之前进行调整以解决问题
服务	简单的上/下状态 几乎没有监控功能	基础的网络服务 若干种监控功能	涵盖所有监控能力的详细监控
环境	生产环境的关键部分	生产环境及其他较低级别的环境	生产环境、较低级别环境以及B2B端点
技术	自行生成的脚本 多个非集成工具	集成企业级工具和仪表盘	端点工具集成到企业仪表盘中
操作	缺乏文档 无限制访问	一些文档 变更管理及其他流程	完整的文档 受限制的访问

表：云监控成熟度

- 阿里云最佳实践

阿里云机房是中国最大的5A 级机房之一。2T出口带宽、网络智能调度。避开高负荷通路，承载淘宝双11期间数十亿访问量。机房监控系统覆盖动力类、环境类、安防类、硬件设备类四类监控。

阿里云通过对各类指标（带宽、内存、CPU等）和各类事件（状态、操作、主动运维等）的监控，实现对主机ECS、网络VPC、存储OSS、自定义、站点、服务、日志、事件等基础架构的全方位监控。

阿里云支持10多种第三方中间件，如Spring、Redis、MySQL、Oracle、Dubbo等。支持事务入口、异常事务，异常RPC、慢SQL排查等问题诊断功能。支持本地调用堆栈和Java异常排查。提供ARMS logger API，可通过关联TraceID让用户打印日志，用于业务全息排查。

阿里云基于EDAS+ARMS实现对服务治理、服务监控、全链路跟踪、全链路灰度、服务统计报表的监控。可通过大屏展示服务调用实时拓扑。

阿里云基于ARMS实现业务应用监控。具有丰富的数据接入和输出层，用户接入门槛低。基于可视化编程的实时计算编排，MOLAP存储，智能报警展示的一站式服务，开发效率高。支持高可靠，高性能，秒级响应，数据一致。应用场景丰富，各类行业模板开箱即用。

4、 云上灾备与恢复管理

企业业务连续性管理

业务连续性管理（Business Continuity Management，简称BCM），是一项综合管理流程，它使企业认识到潜在的危机和相关影响，制订响应、业务和连续性的恢复计划，其总体目标是为了提高企业的风险防范能力，以有效地响应非计划的业务破坏并降低不良影响。

我们建议企业根据自身业务需求情况和业务连续性管理要求，制定自己的灾备策略，对不同的系统，确定灾

难标准，明确相应的RTO（当系统不可用时可忍受的恢复时间）和RPO（当系统恢复时可忍受时间内数据丢失数量）。灾难定义标准及相关RTP和RPO要求如下：

灾难恢复能力等级	容灾标准的定义	RTO	RPO
1	基本支持	2天以上	1天至7天
2	备用场地	24小时以上	1天至7天
3	电子传输和部分设备支持	12小时以上	数小时至1天
4	电子设备和完整设备支持	数小时至2天	数小时至1天
5	实时数据传输和完整设备支持	数分钟至2天	0至30分钟
6	数据零丢失和远程集群支持	数分钟	0

根据系统要求的RPO和RTO要求的不同，我们需要采用不同的技术及数据备份策略。RPO要求为秒、分钟级别，需要采用同步复制或者同步镜像技术；RPO要求为小时级别，可以采用异步复制技术；RPO要求为日或者周，可以采用定期复制或者磁带备份技术。RTO要求为秒、分钟级别，需要使用应用级容灾；RTO为分钟、小时级别，需要使用运营级容灾；RTO为日、周级别，则可以采用数据级容灾。

数据完整性向右递增，投入成本技术要求递增。业务连续性向左递增，业务恢复时间运维风险递减。

企业应用上云可实施多种替代处理策略，以满足特定的应用以及数据可用性需求，同时支持灾难恢复策略。对企业云上灾备与恢复管理，可按照同城应用双活、异地高可用、同城应用双活+异地备份恢复这三个层级进行选择。

公共云容灾与恢复

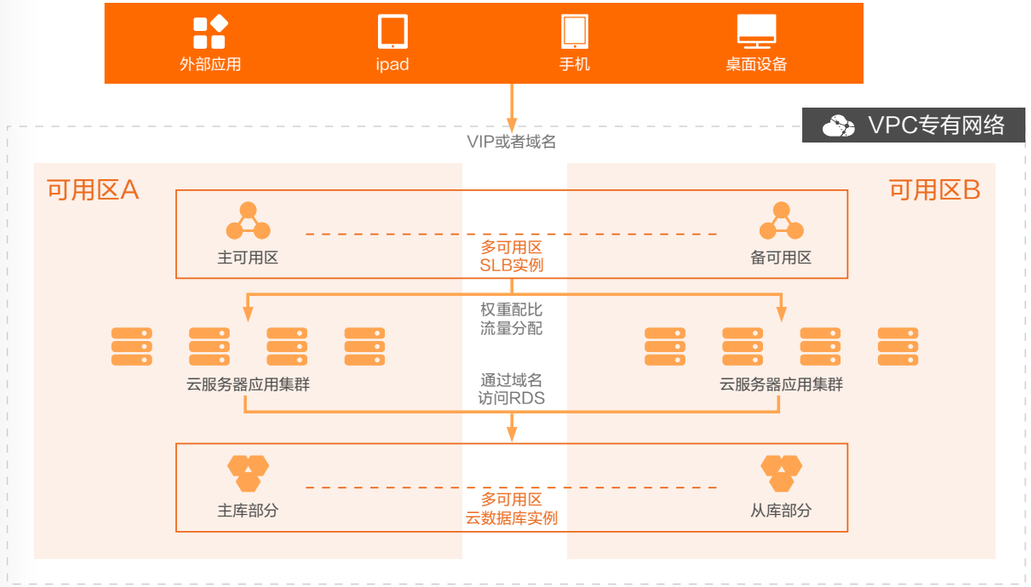
公共云容灾具备基础资源天然的高扩展性和高可靠性优势，可用作为企业现有业务容灾的有效补充，也是未来容灾技术的发展趋势。

根据企业应用系统RPO要求，将传统架构下业务系统生产数据分级备份至公共云数据中心的云存储中。当单位生产数据异常时，可将数据恢复从云容灾中心恢复至企业数据中心。容灾成本低，运维简单。无需硬件维护，云存储扩展性强，备份管理简单。提高业务可靠性。生产数据异地备份，更安全，可根据RPO要求灵活、分级备份数据；云存储具备天然可靠性优势。

阿里云最佳实践

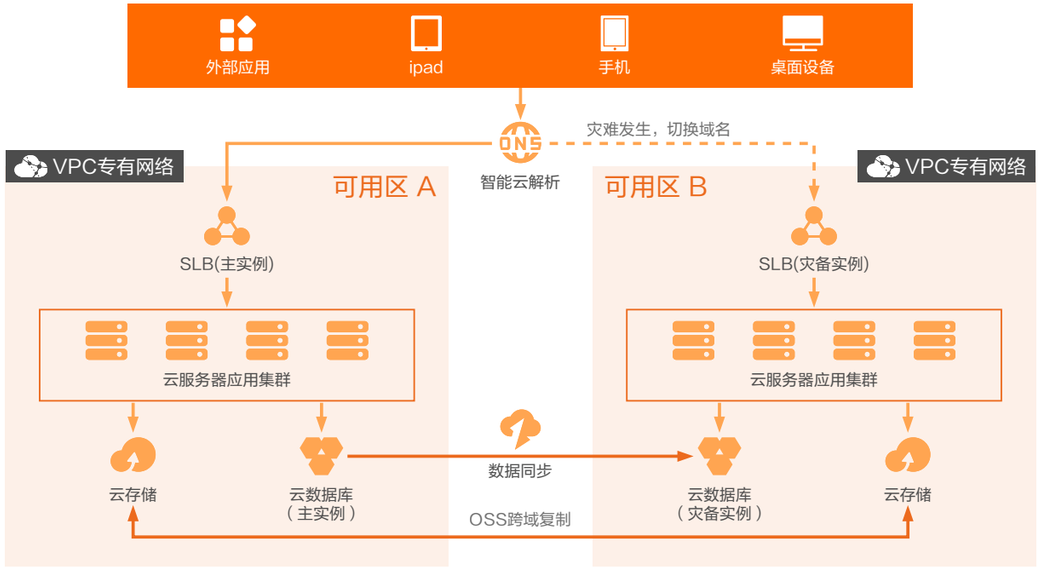
・同城应用双活

对于只部署在公共云上的应用系统，可采用跨可用区高可用灾备架构，当Region下的某个可用区故障，云产品实例不可用，可用区中某个云产品集群级别性能衰减或者不可用，或基础设施故障导致的整个可用区级别故障。可在Region下的多个可用区搭建具备同城容灾能力的系统。



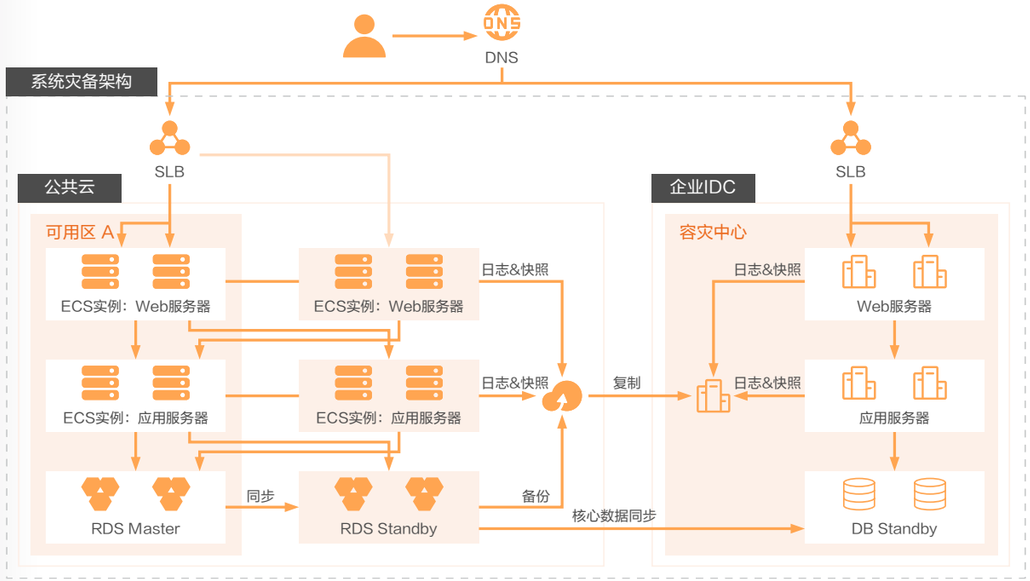
・异地高可用

对部署在公共云上的面向不同区域客户的应用系统，考虑到不同区域的一致性访问，会部署在不同的Region，可采用跨Region高可用灾备架构。但当出现不可抗力或基础设施故障导致整个Region不可用，出现访问故障，需要利用多个Region搭建具备异地高可用、异地容灾能力的系统。



・同城应用双活+异地备份恢复

通常情况下，在混合云环境中，部分的企业应用系统，由于业务特点以及业务连续性、安全性要求高的系统应用可使用混合灾备架构，部署在公共云和企业两地不同地域的两个数据中心中，生产中心处于Active模式，灾备中心处于Standby模式。其中，灾备系统部署在企业IDC私有云环境中。



更多详细信息，请参见阿里云企业级云灾备解决方案和同地域跨可用区容灾最佳实践。

3 云上安全管理体系建设

1、云上安全责任

中华人民共和国国家标准GB/T 35279-2017《信息安全技术-云计算安全参考架构》。基于信息资产和产品功能建立了如下的信息安全责任共担模型，其中不同颜色定义云服务提供商应负责责任部分、客户应负责责任部分，共同承担责任部分。客户实施安全组件的责任在IaaS服务中较大，在PaaS服务中降低，在SaaS服务中最小。而云平台责任从IaaS，PaaS到SaaS分别增加。

ISO/IEC 27017 云计算安全和隐私管理系统安全控制。云服务使用过程中，云服务供应商系统所创建或修改的数据和文件可能对于确保服务运营、恢复和连续性至关重要。 资产所有权以及对于这些资产相关的操作(例如，备份和恢复操作)承担责任的各方应当被定义和记录。否则，将会存在云服务供应商假设云服务客户执行了这些重要任务(反之亦然)的风险，并且可能发生数据丢失。

	IaaS	PaaS	SaaS	
客户的责任	数据安全	数据安全	数据安全	
	终端安全	终端安全	终端安全	责任共担
	访问控制安全	访问控制安全	访问控制安全	
	应用安全	应用安全	应用安全	云平台方责任
	主机和网络安全	主机和网络安全	主机和网络安全	
	物理和基础架构安全	物理和基础架构安全	物理和基础架构安全	

阿里云安全责任共担模型

基于阿里云的客户应用，其安全责任由双方共同承担：阿里云要保障云平台自身安全并提供安全产品和能力给云上客户；客户负责基于阿里云服务构建的应用系统的安全。

阿里云负责基础设施（包括跨地域、多可用区部署的数据中心，以及阿里巴巴骨干传输网络）和物理设备（包括计算、存储和网络设备）的物理和硬件安全，并负责运行在飞天分布式云操作系统之上的虚拟化层和云产品层的安全。同时，阿里云负责平台侧的身份管理和访问控制、监控和运营，从而为客户提供高可用和高安全的云服务平台。

客户负责以安全的方式配置和使用各种云上产品，并基于这些云产品的安全能力以安全可控的方式构建自己的云上应用和业务，保障云上安全。阿里云基于阿里巴巴集团多年攻防技术积累，为客户提供云盾安全服务，保护客户的云上业务和应用系统。阿里云建议客户选择使用云盾安全服务或者阿里云安全生态里的第三方安全厂商的安全产品为其云上应用和业务系统提供全面的安全防护。

安全责任共担模式之下，阿里云保障云平台层面的安全并提供一方集成的云产品安全能力和云盾安全服务给客户使用，让客户降低对安全性的顾虑，更专注于核心业务发展。

2、云平台安全合规

安全合规

安全合规一直是信息化发展过程中的重要命题。在企业迈向全面“云化”的进程中，云的安全合规也成为了企业进行云服务选型的重要考量因素。因此，企业在上云过程中要参考一系列的标准认证、三方审计及评估，更好的分析云服务厂商的合规实践。针对云服务商的合规管理评估主要包括四个维度：

・法律法规

云服务厂商要遵守国家立法机构颁布的法律要求，如《中华人民共和国网络安全法》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》等；

国家行政机关颁布的云服务的准入政策，如《中华人民共和国电信条例》等；

国家信息安全主管部门颁布的管理规定，如《公安机关互联网安全监督检查规定》等。

・国内合规认证

国内信息化、信息安全等主管部门，对云服务经营者进行的服务经营者能力、服务质量、可信度、网络与信息

安全等评测认证，旨在推动云服务经营者加强内部管理，提升服务质量和诚信水平。如公安部《网络安全等级保护》、工信部《云计算服务能力符合性评估》、网信办《党政部门云服务网络安全审查》等。国内其他机构的专业资质认证，作为行业信息化服务准入资质。

・国际规格认证

在不同的国家/地区开展云服务时，需符合当地的法律法规。但由于法务合规的独特性，无法通过证书或审计报告的形式来体现。

管理体系合规，主要包括ISO国际标准认证，体现云服务商自身成熟的管理机制和遵从的行业最佳实践。

体系化合规报告，旨在向客户展示云平台管控的完整性和有效性。主要包括：体系控制是否持续有效，职责分离是否准确，运维操作审计。

阿里云安全合规

阿里云是合规领域的“全满贯”，已通过100多项合规认证和第三方审计为亚洲合规资质最全的云服务商。

同时在个人隐私保护方面，阿里云坚持致力于保护每位客户的个人信息，保证客户对所有提供给阿里云的个人信息拥有所有权和控制权。与此同时，阿里云积极响应国家监管部门对企业承担个人信息保护责任的号召，持续完善内部的个人信息管理和保护体系。

阿里云通过大量权威机构的认证证明个人信息保护能力/数据安全保护能力，详细信息请见ISO 27017、PCI DSS、可信云云服务数据保护认证等。阿里云将持续建设阿里云整体的个人信息保护管理体系，除了关注阿里云作为控制者角色时云平台自身的个人信息保护能力之外，会进一步投入力量建设阿里云作为数据处理者的角色时相应的产品/服务中的个人信息保护能力。

3、用户合规管理

安全合规

根据等保2.0相关要求，企业应用系统在上云过程中，结合云平台功能分层框架和云安全特点，构建云计算安全防护框架包括：用户层、访问层、服务层、资源层、基础设施层和管理层，并以此为基础构建一个中心、三层防护的云安全防护体系。

一个中心指安全管理中心，三重防护包括安全计算环境、安全区域边界和安全通信网络。云上系统的等保要求绝大部分集中在二级和三级系统。

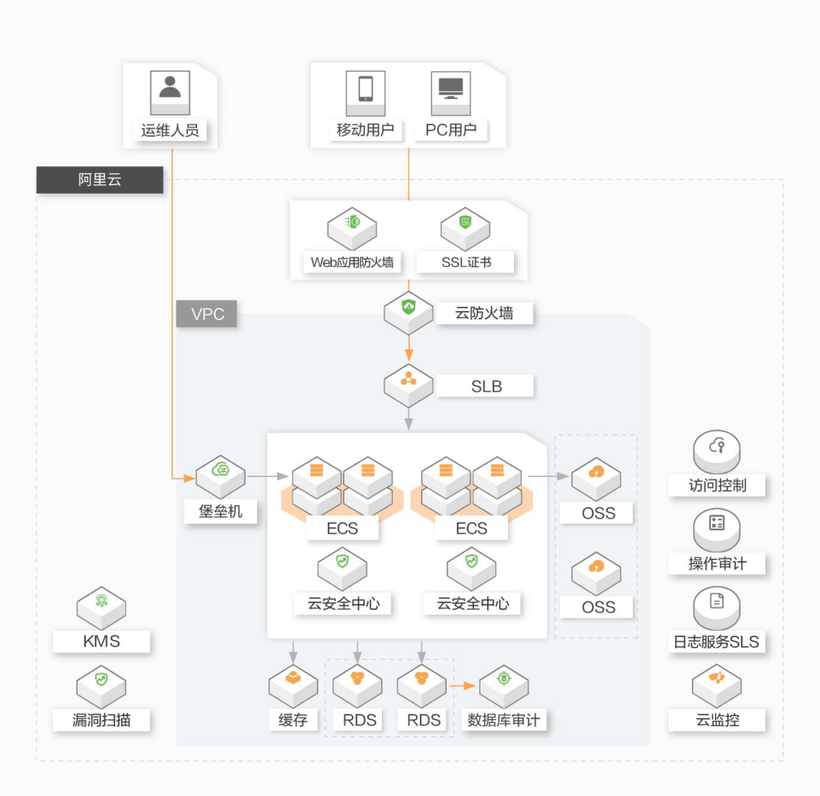
安全领域	基本要求	二级	三级
安全通信网络	应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段	云防火墙	云防火墙
安全区域边界	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为		DDoS高防
	应具有提供访问控制、边界防护、入侵防范等安全机制	Web应用防火墙	Web应用防火墙
	应能对各类安全事件和新型攻击进行分析、识别、报警	云安全中心	云安全中心
安全计算环境	应对用户进行身份鉴别、访问控制、运维审计	堡垒机，KMS，操作审计，日志服务SLS，云监控	堡垒机，KMS，操作审计，日志服务SLS，云监控
	应启用安全审计功能，数据进行安全审计	数据库审计	数据库审计

安全领域	基本要求	二级	三级
安全计算环境	应满足数据完整性和数据保密性的要求	SSL证书	SSL证书
	应能发现已知漏洞，并在经过充分测试评估后，及时修补漏洞	漏洞扫描	漏洞扫描，渗透测试
	应仅采集和保存业务必需的用户个人信息，并对数据安全审计范围进行扩展全机制		敏感数据保护
	应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现别、报警		应用身份服务
安全管理中心	应对系统资源和运行进行配置、控制和管理。包括用户身份、系统资源配置、系统加载和启动、异常处理、数据和设备的备份与恢复等。	安全管家	安全管家

阿里云最佳实践

阿里云按照国家互联网信息办公室、国家发展和改革委员会、工业和信息化部和财政部联合发布的《云计算服务安全评估办法》要求，阿里电子政务云平台在2016年全国首批通过云服务审查增强级要求，为党政机关、关键信息基础设施运营者提供安全可控的云计算服务。

阿里云按照网络安全等级保护制度，不断提升云计算服务的主动防御、动态防御、整体防控和精准防护能力，在2019年5月，《GB/T22239-2019 信息安全技术 网络安全等级保护基本要求》为指导标准的网络安全等级保护办法的等保2.0系列标准正式发布后，阿里云成为全国首家通过等保2.0正式标准测评的云服务商。典型等保三级架构如下图所示：



按照新的云等保要求和监管部门的意见，在具体的云上应用等级保护合规和测评中，涉及阿里云平台侧的相关要求不再进行单独测评，可以直接引用阿里云平台的测评结论。阿里云将提供以下材料，协助租户云上系统通过等

保测评：

- 提供等保定级辅导服务
- 提供备案指引服务
- 提供符合等保2.0合规需求的安全产品
- 提供等保测评服务， 提供阿里云平台的合规资质证明

阿里云为企业提供完善的等保合规2.0安全解决方案，帮助企业云上业务满足安全合规要求。更多详细信息，请参见等保合规2.0安全解决方案。

4、云平台安全

云平台安全主要指云服务厂商的基础安全能力，主要包括：物理安全、基础设备安全、虚拟化安全、云服务产品安全以及云平台内部身份与访问控制、安全监控和运营等内容。

物理安全

云数据中心建设应满足GB 50174《电子信息机房设计规范》A类和TIA 942《数据中心机房通信基础设施标准》中T3+标准。主要包括：机房容灾、人员访问管理、账号和身份认证、运维审计、数据销毁策略与流程、数据擦除、客户数据处置策略、网络隔离策略等内容。

基础设备安全

基础设备安全主要包括：物理网络安全、硬件固件安全，硬件固件基线扫描、高性能GPU实例保护、BIOS固件验签、BMC固件保护；加密计算，所有加密信息只能在可信执行环境中计算和运行，从而提供基于硬件的高等级的数据保护能力；可信计算，通过度量和验证保证云平台运行环境的安全，以及通过对白名单应用的监测管理确

保应用的运行安全。

虚拟化安全

虚拟化安全主要是从提供者视角、管理者视角、使用者视角去看每个视角需要关注的安全因素；从虚拟化的各种资源类别，结合角色视角去分析各类虚拟化资源需要关注及解决的安全点。

根据上述虚拟化安全的设计思路，以及具体参与的用户角色（管理者、使用者、提供者），在计算虚拟化安全、存储虚拟化安全、网络虚拟化虚拟化安全加固、虚拟镜像安全、租户隔离策略、安全架构策略、逃逸检测及补丁修复等安全管理各个方面存在着需要关注的安全管控点。

- 虚拟网络：多租户安全隔离、网络防御、安全域、安全多实例
- 虚拟机：安全补丁、安全漏洞、病毒防御、安全策略迁移、访问控制
- 虚拟存储：存储隔离、存储备份、访问控制
- 虚拟化管理：虚拟镜像安全、授权认证、销毁安全、审计日志、监控管理

云服务产品安全

云服务产品安全主要包括计算、存储、网络类产品安全，服务注册、服务申请及注销、权限认证、服务监控、服务流控、服务路由；云平台环境下的网络安全隔离，通信协议、端口认证、数据加密；数据库产品、大数据产品、组件/服务安全，权限认证、审计日志、代码规范、代码漏洞、数据加密处理、数据验证；组件/服务管理、服务计量计费安全、组件/服务传输安全、服务访问安全、组件/服务集成安全。

内部身份与访问控制

身份与访问控制主要包括：云服务厂商内部用户使用身份认证系统进行账号生命周期管理；统一登陆管理、账

号密码管理策略和访问控制策略；合理分配用户权限，按照权限、角色、用户组、部门和用户进行权限统一管理，每个内部用户通过权限管理系统实行权限申请、使用和回收。

安全监控和运营

云平台安全监控和运营主要包括：云产品安全生命周期管理，在云服务产品推出的过程中，架构、开发、测试、发布等每个节点都有完整的安全审核机制确保产品的安全性能够满足严苛的云上要求，从而有效地提高云产品的安全能力并降低安全风险。

通过云平台侧的安全监控，及时发现平台自身的应用和主机、网络等资源被恶意攻击的安全事件，并在发现安全事件之后，触发云平台内部应急响应流程进行妥善处置，及时消除影响。对于内部监控发现的和外部上报的漏洞和安全事件做出应急处置。

5、 用户安全管理

网络隔离(纵深防御)

通过云产品的安全隔离和访问控制功能，实现网络、系统、应用和数据不同维度的隔离以实现纵深防御。

认证授权(最小权限)

仅授权使用者必须的云账户和子账户权限，并开启双因素认证措施和关键操作二次认证能力

安全加密(开启加密措施)

通过传输加密和存储加密措施实现数据在云上全程加密

监控告警

通过日志和监控措施及时发现配置变动、异常登录和操作、数据泄露以及异常攻击等

6、 阿里云安全架构

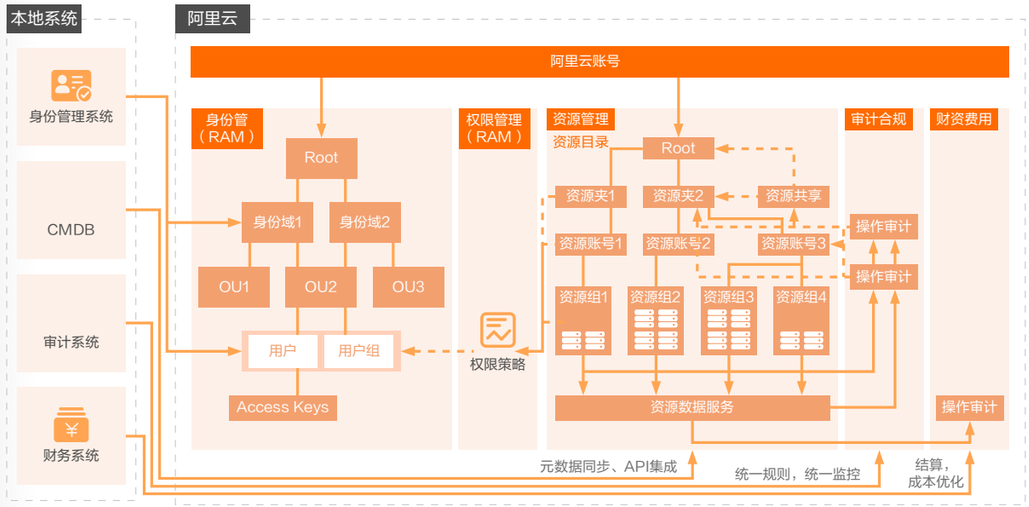
“五横两纵”7个维度的安全架构设计从客户需求出发，覆盖了用户侧和云平台侧的安全架构设计点，用户可以对照判断自身的安全能力是否缺失，强壮安全体系。两个纵向维度为账号安全和安全监控和运营管理，都包括了用户侧和云平台侧的不同实现。五个横向维度从最底层的云平台层面安全，到对外用户侧层面的基础安全、数据安全、应用安全和业务安全。

1、用户账户安全

Resource Access Management(RAM)是阿里云为客户提供的集中式用户管理与资源访问权限控制服务。每个资源有且仅有一个属主(资源 Owner)。该属主必须是一个阿里云账号(又称主账号、根账号、资源 Owner)，是对资源付费的人，对资源拥有完全控制权限。

通过使用 RAM，用户可以在其云账号下为其企业员工、系统或应用程序创建独立的 RAM 用户账号，并可以控制这些用户对其云资源的操作权限。每个 RAM 用户可以拥有独立的登录密码 或 Access Key，可以登录阿里云控制台或以程序方式操作云服务API。RAM 使得一个阿里云账号(主账号)可拥有多个独立的子用户(RAM用户)，并支持多因素认证、强密码策略、控制台用户与API用户分离、自定义细粒度权限策略，用户分组授权、临时授权令牌等功能。

资源目录支持按照基于企业的业务或生态环境，让管理员方便地创建体现业务关系的资源 目录结构，并将企业多个账号分布到这个目录结构中的相应位置，从而形成资源间的多层级关系。



2、用户基础安全

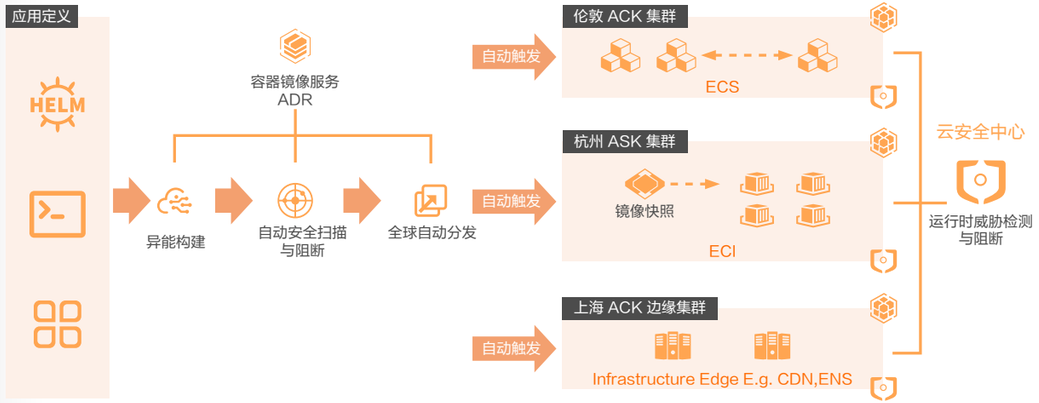
通过采集主机资产、及其弱点数据，实时掌握资产安全状态。

01：资产管理	主机、软件、端口、进程、账号资产动态清点
02：漏洞管理	Windows、Linux、Web-CMS、0day漏洞分钟级定位，一键修复
01：基线检查	Windows、Linux、中间件等保二级/三级基线检查，可定制

基于大数据技术，协同威胁情报，针对威胁进行检测防御，利用全量日志快速检索定位异常。

04：入侵检测	100+异常检测模型，覆盖异常登录、异常进程、异常命令、异常网络连接
05：恶意代码查杀	多引擎检测Webshell、病毒、木马、挖矿软件等恶意代码，一键查杀
06：进程白名单	机器学习算法智能学习生成白名单策略，防范未知威胁代码攻击
07：文件防篡改	实时监控指定目录，文件篡改告警并实时恢复
08：事件响应	采集多种主机入侵分析必需数据，快速检索定位攻击路径和来源

每个安全容器都有独享的内核，对内存、网络、IO 等实现了更强的隔离，可以基于这套框架，在单宿主机上更好的保障用户的多租户安全隔离。容器内 Web-CMS 漏洞检测和修复、Webshell 检测和修复、云查杀、进程异常行为、异 常网络连接、进程启动日志、网络连接日志的功能。扫描镜像相关的最新 CVE 安全漏洞信息，容器镜像的签名和校验可确保仅在 ACK 上部署经过容器使用方签名确认的的容器镜像。



帮助用户基于隧道技术，实现数据链路层的隔离，为每个用户提供一张独立隔离的安全网络环境。实例级别虚拟化防火墙，具备状态检测和数据包过滤功能，可用于在云端划分各个ECS实例(在容器服务中，即各个容器集群)间的安全域。对南北向和东西向访问的网络流量进行分析，并支持全网流量(互联网访问流量，安全组间流量等)可视化，并支持对主动外联行为的分析和阻断。通过全流量代理的方式实现大流量攻击防护和精细化Web应用层资源耗尽型攻击防护。

3、用户数据安全

敏感数据保护是从海量数据中自动发现，记录并分析客户在云上保存的敏感数据的使用情况，及时发现其使用是否存在安全违规并进行风险预警，帮助用户防止数据泄露和满足GDPR等合规要求。

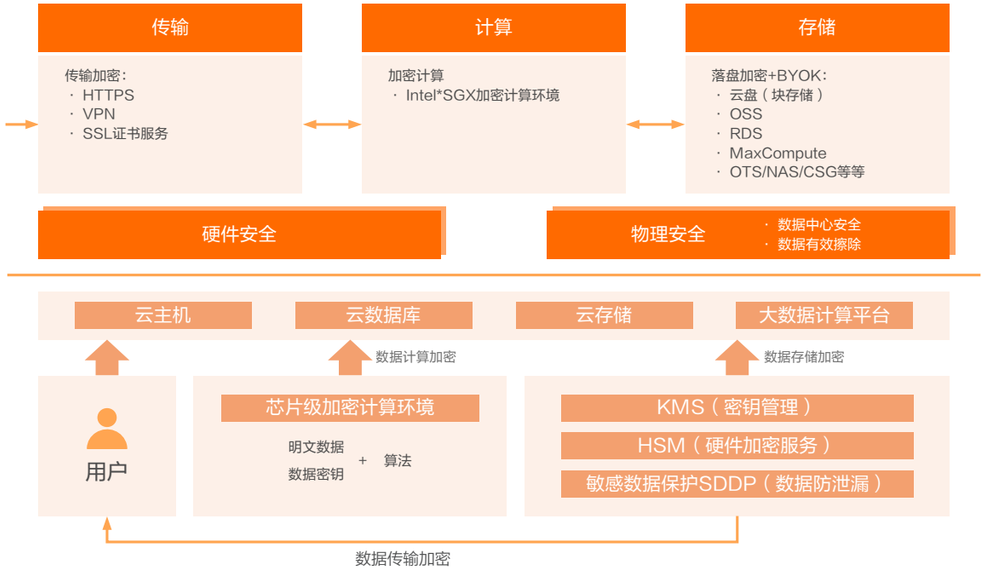
根据系统内置算法规则或客户自定义模型，通过AI、机器学习等方式精准识别敏感数据和文件。支持识别的非结构化文件类型多达180多种，同时内置支持识别7类约40多种敏感数据和图片文件。

以脱敏的方式实现数据的安全分享。支持丰富的脱敏算法与自适应参数配置，确保脱敏结果能适用于开发、测试和分析场景。

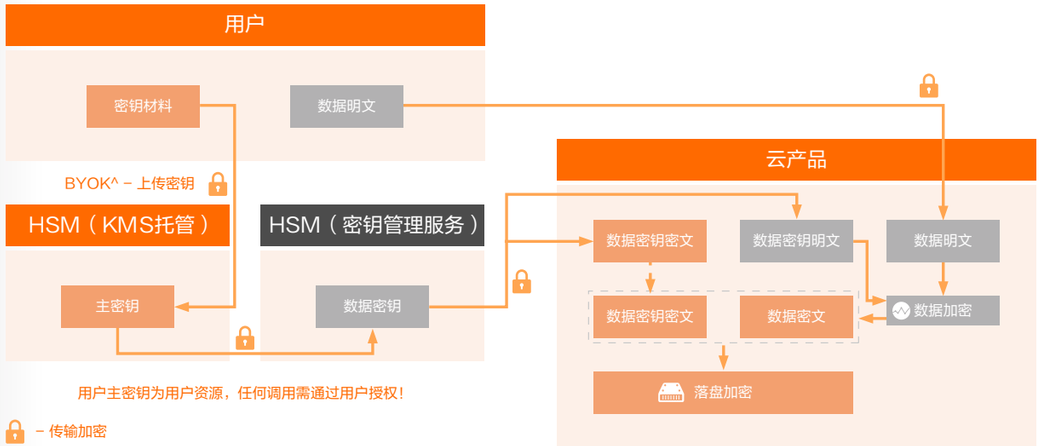
识别数据异常，提供告警能力，降低数据风险。基于大数据的分析与识别能力，对敏感数据与文件的异常访问实现智能检测并针对性的提供保护建议。

审计异常行为，及时告警，提供可追溯能力。对结构化数据和非结构化数据的行为进行审计，提升企业安全风险响应能力，满足合规要求。

阿里云是国内唯一支持SGX加密计算环境的云服务提供商

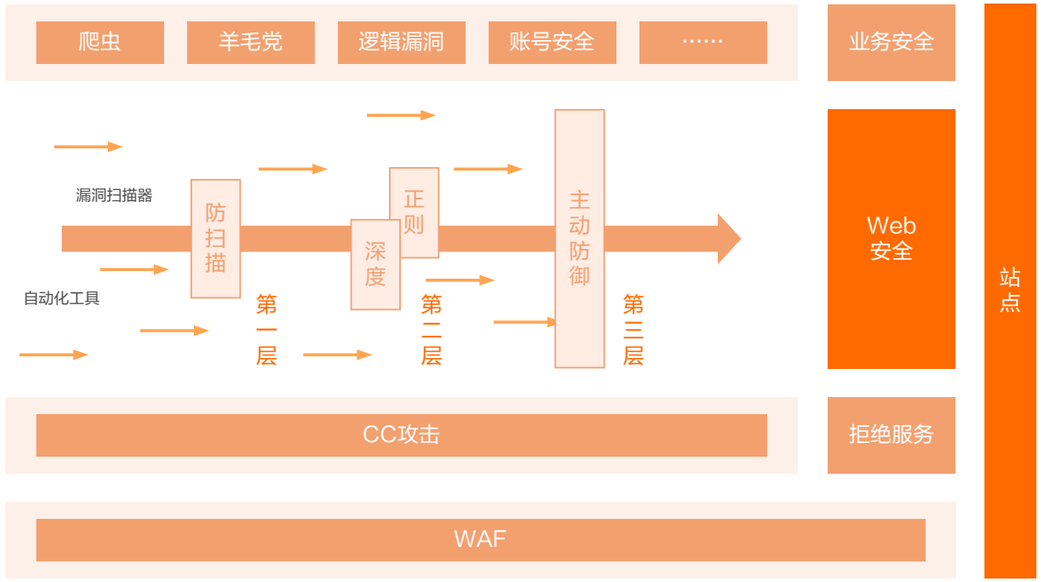


阿里云提供密钥的安全托管、密码运算等基本功能，内置密钥轮转，支持用户数据进行加密保护。



4、用户应用安全

针对攻击者的批量漏洞扫描和故意袭扰行为，采用自动封禁的方式做到攻击处置自动化，并结合情报做到协同防御；针对攻击者使用已知漏洞进行攻击的行为，配置严格的WAF规则和策略针对攻击者进行0day漏洞攻击，采用白名单基线的方式进行防护，即事先对重要系统建立一套合法的流量基线。

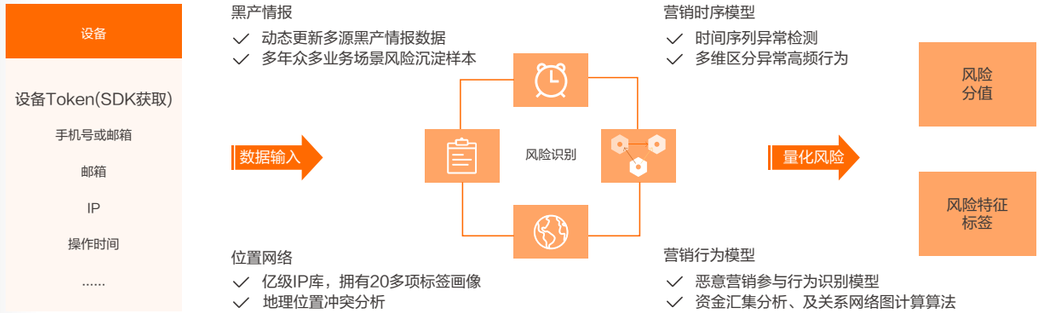


当大量系统上线，如何保存和更新配置文件，如何安全存放配置是云上应用系统面临的重要安全风险。将敏感信息(例如数据库连接串(含密码))存放到生产环境的服务器上的配置文件。将敏感信息做成配置文件打包在软件工程的配置文件里，并发布到各类环境里。在 Docker 编排时，将敏感信息直接存放到环境变量中。配置管理系统自身密钥如何防止暴露。

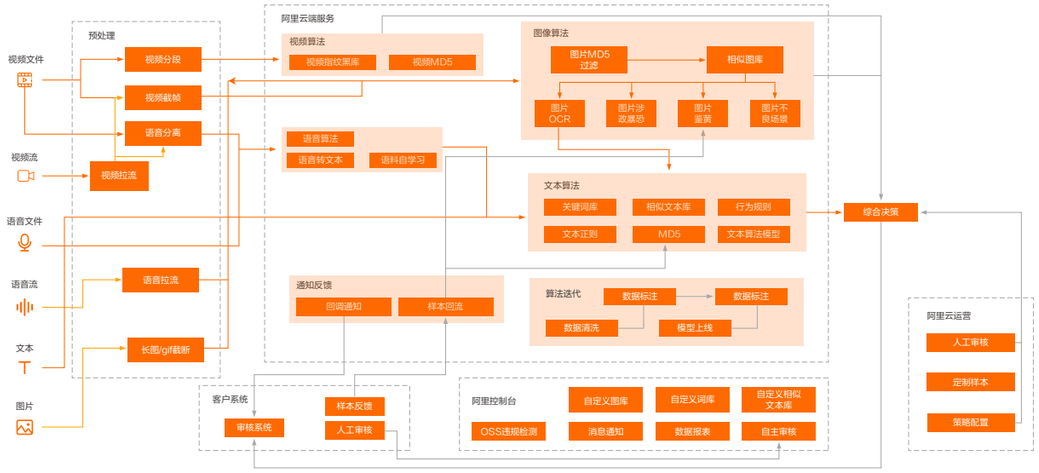
网站关联资产发现，自动化漏洞渗透测试和敏感内容监测，漏洞修复，基线加固和组件升级，对于Git库等云上托管代码，应用最小权限原则。按照安全生命周期，严格审核和评估代码安全，黑白盒代码安全检测。

5、用户业务安全

通过设备风险SDK和API调用结合的方式，有效识别黄牛、薅羊毛、抢秒杀等业务风险，防止营销资金流失，提升活动效果。单次活动即可挽回数十万损失。防止恶意爬虫(Bot)可以有效降低和解决外部恶意自动化工具对用户网站的业务影响。对于Git库等云上托管代码，应用最小权限原则。按照安全生命周期，严格审核和评估代码安全，黑白盒代码安全检测。



降低色情、暴恐、涉政等违规风险，解决广告推广，谩骂等用户体验痛点，而且能大幅度降低人工审核成本。



通过活体检测+身份证ocr技术+人脸比对技术+智能核身决策平台输出综合身份认证结果。

6、用户安全监控与运营

构建纵深立体的威胁检测架构，通过黑客遗留的痕迹感知威胁发生，让一切攻击都有迹可循。

将合规要求实施为规则，在配置审计持续监控资源的变更并自动评估合规性。在线查看合规结果并下载合规报告，订阅资源变更和合规事件，时刻掌握资源动态。为规则设置修正逻辑，自动及时修正不合规。

企业审计日志集中化存储，通过日志服务审计，将公司内部多个账号的云产品，操作记录，应用日志集中存储。满足等保，GDPR等审计合规需求。异常监控自动告警，对接第三方审计、安全运营SOC、备份系统。

将渗透测试集成到安全开发生命周期，能够更早地检测系统缺陷并降低整体业务风险，可以帮助企业挖掘出正常业务流程中的隐藏的安全缺陷和漏洞，并提出修复建议。助力企业先于黑客发现安全风险，防患于未然。

为解决企业上云安全专业人才短缺、安全技术工具少生产效率低、体系化建设不够完善。经用户授权后，安全管家服务专家将依托管家自带运营服务体系，全面接管用户云上资产安全，用户可以将安全聚焦点转移到业务自身安全。

4 优化提升

1、部署加速

企业IT部门可充分利用云服务资源快速供给的优势，利用云服务的扩展能力，实现应用系统与基础设施解耦。通过运营运维效率的不断的优化，进一步加速应用系统及产品的快速迭代和优化更新，提高业务的弹性与敏捷性，响应市场的快速变化和客户需求，逐步形成差异化的竞争优势。

2、工作负载优化

云服务有裸金属服务器、虚拟机、容器、Serverless等不同类型的工作负载资源实例，可以满足不同业务场景的需要。企业IT可以按需访问计算资源，从而以最低限度的管理进行快速配置和发布。

但随着业务的不断拓展，企业的对IT资源需求存在不可预测性，对系统弹性与稳定性的要求越来越高；同时，业务规模的不断扩大，对云的运营管理的复杂度也越来越高。因此，企业IT需要通过持续不断的对工作负载优化，选择性价比更高、运维复杂度更低、性能稳定性更高、架构更加灵活的工作负载，提升整体的运营效率。

3、备份恢复优化

由于云服务的备份恢复策略与企业传统的策略有所不同，企业采用云服务后，需要结合云服务相关产品的架构与特性，重新进行业务影响分析。不断修正评估算法，提高风险识别的准确度，制定相应的风险控制流程以及应急处置与业务恢复策略，有效控制风险。

同时，根据重要性及紧急程度，重新设计完整的应急预案来应对各种业务中断情况，特别是混合架构下，企业

IDC与云服务之间的网络链接的风险评估，有效应对突发事件带来的影响。优化灾备演练方案，检验应急预案完整性、可操作性和有效性，以及验证业务连续性资源的可用性，从而确保提高应对中断事件的综合处置能力。

4、可用性提升

应用系统迁移上云后，应采用先进的互联网思想、领先的架构设计理念持续进行优化。通过云服务提供的分布式服务框架，对各类业务服务进行统一的服务治理，采用组件化完成独立开发、独立部署、独立发布、独立升级，有效地消除各种瓶颈，满足系统高扩展与高可靠的要求；通过云服务提供的缓存服务，有效地缓解业务高峰期用户访问量过大带来的性能问题，保障业务顺利地开展，满足系统高性能要求；通过云服务提供的云原生数据库，缓解随着系统流量增加而带来的数据库压力，对数据库进行垂直拆分、分库分表、读写分离等操作，通过各数据库之间的异步消息来保证数据一致性；通过云服务提供的各种跨可用区的产品和服务，全面提升系统可用性。

5、安全性提升

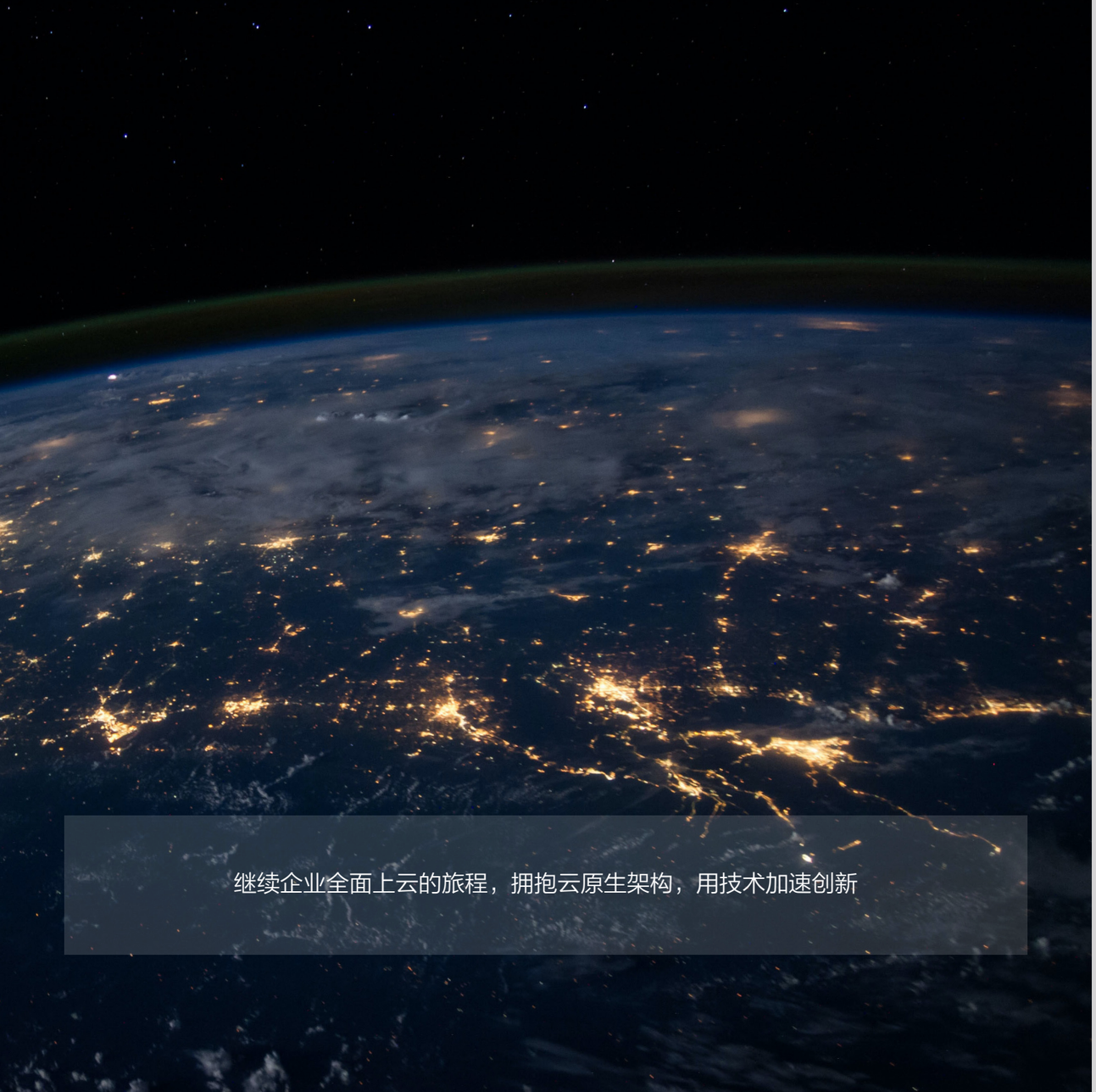
应用系统迁移上云后，根据云安全责任共担模型，其安全责任由双方共同承担，云服务提供方要保障云平台自身安全并提供安全产品和能力给云上客户；客户负责基于云服务构建的应用系统的安全。

首先，作为云服务用户，需要充分利用云服务提供商提供的安全服务，保障自己应用系统或服务的基础安全、数据安全、应用安全和业务安全。这些安全服务主要包括：主机安全、容器安全、密钥、身份认证、VPC、安全组、云防火墙、VPN、堡垒机、DDos防御等。

其次，需要利用云服务的安全防护能力，参考最佳实践，合理的设计和演进系统架构，保护应用系统或服务的安全，对应用系统的安全防护能力进行加固。我们常用的云服务资源特性包括：自定义网络拓扑结构和访问控制、弹性公网IP和自定义路由策略等。

再次，要强化对应用系统或服务本身的安全设计，包括应用环境的安全防护、加强漏洞扫描和代码审计，保障应用系统或服务本身不存在安全问题或漏洞。

最后，要加强云服务安全体系建设，强化信息安全策略，保障业务安全和数据安全；要加强身份认证和访问授权，建立密钥及密码管理规范；要加强数据隐私的保护以及传输、存储过程中的安全管理 ；通过对云上系统的安全优化，使得云上的环境能够得到有效的安全防护。



7 企业全面上云成功路径与实践
云原生

1 云原生概述

1 全面上云对企业IT提出新要求

过去十年国家高度重视我国云计算产业发展，相继出台多项政策提促市场转型升级。历经多年发展，我国云计算产业已得到长足发展，连年保持着较高增长率，产业规模已突破千亿，产业链条趋于完善。云计算已经取代传统IT成为数字时代的信息基础设施，在数字经济时代扮演越来越重要的角色。随着我国在“新基建”领域布局加速，云计算迎来全新的发展机遇，万千企业数字化转型换挡提速。

如前所述，企业上云经历了基础IT要素上云、业务系统上云、企业云端互联、企业全面上云四个阶段，全面上云阶段，企业所有业务都要迁移上云，并在此基础上围绕价值链实现与其他企业的云端互联，云平台功能从企业内部系统集成扩展到产业链上下游企业间资源共享，业务协同，实现更高效的集成应用模式。

企业全面上云对企业IT，特别是IT基础设施，提出了全新要求，**一是快速响应用户需求的持续交付能力**。快速响应市场需求已经成为企业竞争的决胜因素，持续交付使开发人员可以在短时间存在的特性分支上工作，定期向主干合并，同时始终让主干保持可发布状态，能做到在正常工作时段里按需进行一键式发布，提升开发的效率。但复

杂传统应用的单体架构模式在代码维护与集成编译方面困难重重，难以做到持续交付；**二是架构的极致弹性能力**。在部署业务应用时，虚拟机分钟级的弹性不再满足快速扩缩容的需求。更加轻量级的容器技术成为微服务部署的最佳载体，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；**三是自动化的开发运维一体化能力**。敏捷开发带来应用的快速迭代，同时也增加了版本发布的风险与业务运维的复杂度。开发、测试、运维高度协同的一体化理念被提出，需要在完成高频率部署的同时，提高生产环境的可靠性、稳定性、弹性以及安全性，消除频繁发布的风险。

2 云原生加速企业IT架构敏捷化，加速全面上云

1、云原生架构定义及设计原则

云原生架构是基于云原生技术的一组架构原则和设计模式的集合，旨在将云应用中的非业务代码部分进行最大化的剥离，从而让云设施接管应用中原有的大量非功能特性（如弹性、韧性、安全、可观测性、灰度等），使业务不再有非功能性业务中断困扰的同时，具备轻量、敏捷、高度自动化的特点。

云原生架构设计遵循以下几个重要原则，**一是服务化原则**，服务化可将业务模块间的关系高度抽象化、标准化，从而将不同生命周期的模块解耦分离，并行业务迭代加速整体的开发进度和稳定性；**二是弹性原则**，即系统的部署规模可以随着业务量的变化自动伸缩，降低余量规划带来的资源浪费；**三是可观测原则**，充分考虑分布式云计算的环境，引入日志分析、链路跟踪和度量等手段，将跨主机、全链路的服务调用情况进行记录、分析和下钻，极大程度上维持业务健康；**四是韧性原则**，业务所依赖的软硬件组合出现异常时，架构能够进行较大程度的抵抗与自愈，保障业务能够持续提供服务不中断；**五是过程自动化原则**，在软件交付标准化的基础上进行自动化，通过配置数据自描述和面向终态的交付过程，让自动化工具调谐交付目标与环境差异，实现软件交付和运维的自动化；**六是零信任原则**，云原生架构打破传统边界安全思想，聚焦以身份为中心的访问控制，任何内外部的人、设备和系统都需要基于认证和授权重构访问信任。

2、云原生架构与传统架构的差异

新的计算架构正在改变企业搭建和使用计算资源的方式，从物理机到虚拟机，提高了硬件的利用率并使资源的使用和变更变得更加灵活。云原生技术进一步降低了应用对运行操作环境的依赖，提高了应用的可移植性和交付效率。根据Gartner的报告预测，到2021年全球70%的企业实现应用的云原生化部署，传统IT架构向云原生转型是大势所趋。

传统架构依然是稳态业务部署的重要选择。云主机从云计算诞生以来一直是计算基础设施的支柱，它的优缺点早已被广泛认知。在过去的十年中，云主机的性能已经发生了重大转变，**低延迟、可预测的高性能以及更好的隔离环境**，使它成为静态单体架构应用程序和性能敏感的工作负载(如高性能计算应用、视频编码、机器学习等）的部署首选。对于大型应用程序，云主机部署也是最主要选择，特别是强调数据持久性和有状态应用。云主机提供的强大安全性和隔离功能使其成为IT运营、风险管理和开发人员可以达成一致的默认计算载体。

云原生架构是敏态业务部署的最优选择。云原生架构由于其面向应用的扩展方式以及超强的可移植性以及轻量级优势，也逐渐成为应用部署的重要组成部分。**应用微服务化加速大型应用的并行迭代效率**，基于云原生架构的应用具备微服务化特性，即以功能域或逻辑关联将单体应用拆分为松耦合的多个子应用，这些相对独立的微服务研发、测试和部署流程可并行执行，极大的提升了整体迭代效率；**负载容器化保障了应用在异构环境中弹性部署**，容器作为标准化的软件单元，将应用及其所有的依赖项打包，使应用不再受环境限制，在不同计算环境间快速、可靠的运行。同时容器共享内核的技术特点使载体更加轻量，相较于虚拟机分钟级的弹性伸缩能力，秒级的资源弹性伸缩能力能够更加快速灵活的响应不同场景的需求。

3 云原生架构对企业的价值

企业上云不应仅仅是简单粗暴的搬迁上云，应用也需要优化传统的设计方法，从架构设计、开发方式到部署、

维护整个软件生命周期都基于云的特点设计，从而构建原生为云而设计的应用，这样才能充分利用和发挥云平台的弹性以及分布式优势。

1、从IT架构角度看云原生价值

云原生架构最大程度上继承了云的强大功能。云原生极大的释放了云计算的红利，充分继承了云计算的设计思想。基于云原生架构在云环境的应用开发能够在资源编排机制、分布式部署、高可用架构等方面得到较好的基础支撑，通过新的架构、技术保障应用系统变得更加健壮，云原生最大程度发挥了云的优势。

云原生架构具备更加极致的弹性能力。云原生有效解决了异构环境的部署一致性问题，促进了资源的标准化，为服务化、自动化提供了基础。云原生技术体系以容器为基本的调度单元，相比虚拟机资源的切分粒度细化至进程级，共享内核的轻量化设计进一步提升了资源的弹性效率。

云原生架构能够兼容应用开发多元的技术栈。与传统架构下的单体应用强行绑定语言和技术栈相比，云原生架构下的应用在业务域划分上应是相互独立的，这使得不同业务域有不同的技术选择权，比如推荐系统采用Python实现效率可能比Java要高效得多。云原生架构实现了使用多元技术栈做应用开发的兼容统一，使得个业务团队能够根据实际需求灵活的选择最佳技术路线。

云原生架构能够更好的提升业务稳定性。自动化程度高，自愈性高，云原生使得应用本身具有“韧性”，即面对强大压力的缓解能力以及压力过后的恢复能力。通过服务状态、系统健康度、接口调用情况、异常的实时告警等实现可视化及预警化，自动化的量化和监控功能，结合业务健康检测启用容器级别的异常自动恢复，及时规避业务风险。

2、从企业运营角度看云原生价值

云原生架构大幅减少企业IT成本。云原生极致的弹性免除了企业侧因应对峰值业务所带来的预留资源的浪费，提高资源的复合利用率，降低了资源成本。同时传统IT架构下的应用中捆绑嵌入了大量的非业务功能，重复造轮子现象严重，研发成本居高不下。云原生技术标准化的交互方式，应用与应用基础设施（编程框架、中间件等）逐步分离，应用基础设施从专用转为通用，从中心化转为松耦合模块化。应用基础设施下沉与云平台充分融合，将云能力与应用基础设施能力进行整合封装构筑统一的技术中台，向业务应用提供简单、一致、易于使用的应用基础设施能力接口，实现技术中台化，缩减重复开发的人力与资源成本。

云原生架构带来更快速的业务交付速度。数字化转型的紧迫需求下使得企业中越来越多的业务衍变成数字化业务，数字化对于业务渠道、竞争格局、用户体验等诸多方面都来更加严苛的要求，直面用户需求更加快速的响应成为企业的核心竞争优势。应用微服务化开发，服务之间使用标准的API接口进行通信。松耦合架构会减轻因需求变更导致的系统迭代成本，为多团队并行开发提供基础，并加快交付速度。云原生技术实现了应用的敏捷开发，大幅提升交付速度，降低业务试错成本，快速响应用户需求，增强用户体验，加速业务创新。

云原生架构带给企业更低心智负担的使用体验。传统架构下的中间件通常与业务捆绑，不能实现通用中间件的有效复用，在应用部署过程中需要投入大量的精力重复构建且极易出错，用户使用体验较差。基于公共云搭建的云原生架构，基础设施层繁琐的运维工作大部分由云服务商承担，企业用户可一键部署启动云原生集群，搭配平台提供的各种标准化中间件服务，实现应用的快速上线部署，降低了用户使用的心智负担，使用户能够聚焦价值更高业务逻辑，提升研发整体效能。

云原生架构更大程度的降低了内部协同的折耗。通过引入DevOps理念优化软件研发运营全周期的管理，从软件需求到生产运维的全流程改进和优化，结合统一工具链，实现文化、流程、工具的一致性，降低组织内部的沟通与管理障碍，加速业务的流程化、自动化。云原生架构变革了研发运营的生产方式，打破组织壁垒，实现研发与运维的跨域协同，进一步解放生产力。

2 云原生理念、技术

云原生是一系列云计算技术体系和企业管理方法的集合，既包含了实现应用云原生化的方法论，也包含了落地实践的关键技术。云原生应用利用容器、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，来构建容错性好、易于管理和便于观察的松耦合系统，结合可靠的自动化手段可对系统做出频繁、可预测的重大变更，让应用随时处于待发布状态，云原生技术有利于各组织在公共云、私有云和混合云等新型动态环境中，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。

1 容器技术

容器是一种轻量级的虚拟化技术，能够在单一主机上提供多个隔离的操作系统环境，通过一系列namespace进行进程隔离，每个容器都有唯一的可写文件系统和资源配额。容器技术分为运行时和编排两层，运行时负责容器的计算、存储、网络等，编排层负责容器集群的调度、服务发现和资源管理。

容器服务提供高性能可伸缩的容器应用管理服务，容器化应用的生命周期管理可以提供多种应用发布方式。容器服务简化了容器管理集群的搭建工作，整合了调度、配置、存储、网络等，打造云端最佳容器运行环境。使用容器技术，用户可以将微服务及其所需的所有配置、依赖关系和环境变量打包成容器镜像，轻松移植到全新的服务器节点上，而无需重新配置环境，这使得容器成为部署单个微服务的最理想工具。

2 微服务

微服务是指将大型复杂软件应用拆分成多个简单应用，每个简单应用描述着一个小业务，系统中的各个简单应用可被独立部署。 各个微服务之间是松耦合的，可以独立地对每个服务进行升级、部署、扩展和重新启动等流程，从而实现频繁更新而不会对最终用户产生任何影响。相比传统的单体架构，微服务架构具有降低系统复杂度、独立

部署、独立扩展、跨语言编程等特点。

与此同时，架构的灵活、开发的敏捷同时带来了运维的挑战。微服务框架作为微服务开发和运行治理的必要支撑，帮助实现微服务注册、发现、治理等能力，目前，在微服务技术架构实践中主要有侵入式架构和非侵入式架构两种实现形式。侵入式架构是指服务框架嵌入程序代码，实现类的继承，其中以Spring Cloud最为常见。非侵入式架构，如Istio，则是以代理的形式，与应用程序部署在一起，接管应用程序的网络且对其透明。

3 Devops

DevOps是一组过程、方法与系统的统称，用于促进开发（应用程序/软件工程）、技术运营和质量保障（QA）部门之间的沟通、协作与整合。它的出现是由于软件行业日益清晰地认识到：为了按时交付软件产品和服务，开发和运维工作必须紧密合作。

DevOps旨在统一软件开发和软件操作，与业务目标紧密结合，在软件构建、集成、测试、发布到部署和基础设施管理中大力提倡自动化和监控。DevOps的目标是缩短开发周期，增加部署频率，更可靠的发布。用户可通过完整的工具链，深度集成代码仓库、制品仓库、项目管理、自动化测试等类别中的主流工具，实现零成本迁移，快速实践DevOps。

DevOps帮助开发者和运维人员打造了一个全新空间，构建了一种通过持续交付实践去优化资源和扩展应用程序的新方式。DevOps和云原生架构的结合能够实现精益产品开发流程，适应快速变化的市场，更好的服务企业的商业目的。

4 服务网格（Service Mesh）

服务网格（Service Mesh）是一个用于管理、观测、支持工作负载实例之间安全通信的管理层。服务网格通常以轻量级网络代理阵列的形式实现，这些代理与应用程序代码部署在一起，而对应用程序来说无需感知代理的存

在。服务网格通常由控制平面和数据平面两部分组成。数据平面运行在Sidecar中，Sidecar为应用程序提供了一个透明的网络基础设施，让业务在低侵入或者零侵入的情况下获得更健壮的网络通信能力。

服务网格带来了巨大变革，拥有其强大的技术优势，被称为第二代“微服务架构”，为微服务带来新的变革，主要体现在：服务治理与业务逻辑解耦，服务网格把SDK中的大部分能力从应用中剥离出来，拆解为独立进程，以Sidecar的模式部署，将服务通信及相关管控功能从业务程序中分离并下沉到基础设施层，使其和业务系统完全解耦，使开发人员更加专注于业务本身；异构系统的统一治理，通过服务网格技术将主体的服务治理能力下沉到基础设施，可方便地实现多语言、多协议的统一流量管控、监控等需求。

5 无服务器架构技术（Serverless）

Serverless是一种构建和管理基于微服务架构的完整流程，允许你在服务部署级别而不是服务器部署级别来管理你的应用部署。它与传统架构的不同之处在于，完全由第三方管理，由事件触发，存在于无状态（Stateless）、暂存（可能只存在于一次调用的过程中）计算容器内。构建无服务器应用程序意味着开发者可以专注在产品代码上，而无须管理和操作云端或本地的服务器或运行时。Serverless真正做到了部署应用无需涉及基础设施的建设，自动构建、部署和启动服务。

无服务器是一种架构理念，其核心思想是将提供服务资源的基础设施抽象成各种服务，以API接口的方式供给用户按需调用，真正做到按需伸缩、按使用收费。这种架构体系结构消除了对传统的海量持续在线服务器组件的需求，降低了开发和运维的复杂性，降低运营成本并缩短了业务系统的交付周期，使得用户能够专注业务本身。

在无服务器架构的理念和方法下，有很多种无服务器的技术形态，目前成熟落地的有3种形态，函数即服务（FaaS）、后端即服务（BaaS）和Serverless容器。

3 基础设施云原生化建设瓶颈分析

1 企业对云原生技术的接纳度较低，转型云原生存在思想障碍

云平台服务商的建设热情和积极性要远远高于行业企业，存在典型的“一头热一头冷”现象。相比之前“机器换人、设备更新” 立竿见影的成效，云原生技术新动能更多依赖无形的数据要素，更多是推动企业研发运维模式和商业模式变革。大多数实体制造业企业跳不出传统发展模式、依赖原有路径导致企业“不想”云原生化；技术投入风险大、效果不可预知导致企业“不敢”云原生化；能力不足、技术储备不足导致企业“不会”云原生化。另外，行业云应用的新业态、新模式、新技术还处于喷薄欲出的竞争阶段而为进入稳定应用阶段，技术选型一旦错误将面临被淘汰和重建的风险，而且行业企业上云的案例实施效果显性化呈现不够、一般行业企业家看不懂、摸不着，案例聚焦到具体行业、规模、阶段、场景不够深入、不好借鉴，案例实施方案在技术、安全、投资、时间等方面刻画得不清晰，特别在没有成功案例参考和市场检验成功的情况下，主动尝试的意愿不强，观望的多行动的少，亟需相关场景需求的标杆示范案例。

2 云原生技术栈技术路线繁多，技术实践存在选型障碍

云原生的理念经过几年发展，不断丰富、落地、实践，云原生已经渡过了概念普及阶段，进入了快速发展期。云原生热点技术井喷式爆发，细分领域发展趋于多元。

云原生技术涵盖云原生底层技术、云原生编排及管理技术、云原生应用、云原生安全等方面，每部分又包含多项技术选择。底层技术包含云原生服务器、云原生存储、云原生网络和容器技术；云原生编排及管理技术包括云原生消息队列、服务网格、无服务器架构技术、云原生调度系统、多云容器编排、有状态应用管理、云原生数据库等；云原生应用包括大数据、人工智能、边缘计算等；云原生安全包括保密计算、容器平台安全、基于服务网格的安全等。

总体看来，云原生技术生态日趋完善，细分项目不断涌现。相较于早年的云原生技术生态主要集中在容器、微服务、DevOps等技术领域，现如今的技术生态已扩展至底层技术、编排及管理技术、安全技术、监测分析技术以及场景化应用等众多分支，初步形成了支撑应用云原生化构建的全生命周期技术链。同时细分领域的技术也趋于多元化发展，如在容器技术领域，从Docker这种通用场景的容器技术逐渐演进出安全容器、边缘容器、Serverless容器、裸金属容器等多种技术形态。技术实践选型结合业务进行大量比较选择，存在选型障碍。

3 现有业务系统未必兼容云原生架构，改造实践难度大

作为IT架构新成员的云原生平台涉及多级系统的对接。云原生平台作为全新的技术实践，需要融入到现有的软件工程及数据运维的管理体系中，可能会涉及全行业级CMP云管平台及企业ITSM系统的对接。

企业的云原生化改造，涉及容器化平台技术，提供高资源利用率、弹性伸缩、自动化秒级扩展的平台基础架构；微服务框架设计，支持灵活、敏捷的业务快速迭代模式；多集群管理功能，支持异地多中心部署方式，可在异地间实现服务负载的分流、故障切换和统一管理； 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；企业级PaaS云计算平台构建方案，提供分布式高可靠、覆盖从开发到测试和部署运行全链条的DevOps环境，提供日志、监控、告警分析的智能化运维手段。

面对各行各业不同的业务需求和行业特点，原系统数字化改造程度也各不相同，进行云原生化的过程中将面临巨大的实践挑战。

4 云原生化改造技术难度大，技术团队建设难以满足

目前大多数的架构都是成长于云时代之前，学习的经典架构模式知识也都来自于那个旧时代。对于开发人员，云原生的技术及理念都需要在实践中逐渐学习，传统基础设施及开发流程会成为引入新技术及理念的很大阻力，在迁移过程中开发人员处于新旧并存混合环境中。这就需要既懂技术又懂业务的专业人才，既要懂得传统信息系统又

要懂得云原生技术还要能设计改造架构。专业人才的稀缺同样是制约企业云原生化的严重问题，要保证企业完成云原生化改造，并在上云后有效运转，企业就一定要有自己的技术与管理人才。对于非互联网的传统企业，IT部门的人才梯队往往不能够满足云原生化改造的技术和能力需求，除了一些新兴的科技型企业之外，大部分企业都存在信息技术人员水平不高或人员不够的现状，尤其是既精通业务又懂云原生技术的跨界融合人才少之又少。

面对这一现状，应该大力发展公共云业务，鼓励企业在公共云上开展云原生化实践，将云原生应用到生产环节，用户可以直接上传托管容器镜像、Helm Chart 等云原生资产。也可以通过构建功能自动从源代码智能构建成容器镜像。同时为了解决流程化、自动化、更安全的方式交付云原生应用这一需求，容器镜像服务企业版引入了云原生应用交付链功能。云原生应用交付链以云原生应用托管为始，以云原生应用分发为终，全链路可观测、可追踪、可自主设置。可以实现一次应用变更，全球化多场景自动交付，从流程层面极大地提升了云原生应用万节点分发的效率及安全性。有效提升企业云原生化效率，将企业从技术细节中解放出来，更多地将精力投入到业务领域。

4 敏捷基础设施的构建与风险防控

1 敏捷基础设施的关键构建环节

IT架构敏捷化转型建设并非一蹴而就，需要科学规划循序渐进的推进，既要解决存量应用的兼容部署问题，也需要充分考虑增量业务的扩展性，核心构建环节包括如下几个：

应用微服务化改造。对于企业/组织而言，将应用系统进行微服务拆分设计改造，需要充分考虑业务驱动因素是否充足，进行微服务改造的可行性分析，不适时或不适度的微服务架构同样会增加企业/组织的技术和运维成本。一般而言，微服务架构更适合于业务需求迭代快、系统模块复杂度高或用户需求持续增加的应用服务。因此建议，满足以下几类业务应用系统可以考虑应用微服务架构：

a）互联网业务应用服务：该类服务通常具有业务需求快速开发迭代的需求。

b）业务系统过于庞大应用服务：该类服务由于长期积累的问题，导致系统模块关系复杂，耦合度高，单次上线更新无法快速完成。

在确立应用微服务化改造的切分领域后，需要将微服务技术根植服务中，包括高性能分布式服务框架、微服务治理中心、Service Mesh等，以实现应用的高可伸缩性和高容错性，满足大规模部署下的性能要求。

部署载体容器化改造。在容器化改造的准备阶段需要对应用部署做清晰规划（如强依赖关系的应用共同部署等），定位环境变量为复用容器镜像铺垫基础，选定数据持久化存储方案。通过云原生应用PaaS平台和容器技术，将大规模运维能力与渐进式的云原生架构转型方案融合，基于云原生技术实现大规模容器编排，支持云原生应用的部署和运行，提供镜像管理和集群管理能力，支持多租户，提升研发效率和自动化水平，降低成本和业务技术风险。

研运流程DevOps化改造。构建云原生化的敏捷架构，打通研发和运维团队的隔阂来更加快速高效地构建和部署应用是重要的一环。综合考虑企业研运的流程，借助DevOps工具链实现研运过程的高度自动化、标准化，使研发、运维、质量管理和安全团队的相关人员密切合作，优化研运流程。通过云原生DevOps相关技术，以可视化的方式，对云上云下业务负载等进行灵活流程编排，有效解决业务运维服务的自动化、定制化及灵活的流程调度编排需求，以持续交付实践不断提高研发效率。

2 云原生架构的技术与管理风险分析

1、云原生架构安全需在构建、运营过程重点关注

云原生架构促使IT架构从稳态转向敏捷。IT架构的变换也使得基于边界的传统安全模型不在适用，新架构下的

安全风险值得关注。

隔离和组件交互方面存在新挑战

以容器和编排为核心基础的云原生技术架构，将容器取代虚拟机成为资源承载调度的最小单元。部署模式的改变带来全新安全问题：**在隔离性方面**，不同于虚拟机的独立操作系统，容器技术共享宿主机操作系统，这种进程级别的“软”隔离，增加了逃逸风险；**在数据共享方面**，紧密联系的多个容器通常共享某些数据，这些容器中的某一个被攻破都会导致数据泄露，使得攻击面大大增加；**在组件交互方面**，容器及其编排系统的组件高度解耦、分散部署，协同交互的组件链条增长，中间态的攻击风险增加。同时新技术的不熟悉也导致因部署不合规而被攻击的现象频发。

容器镜像全链路追踪管控成为难题

容器镜像是云原生技术架构中软件交付流转的主要形态，贯穿应用研发、测试、预生产和生产运营的全生命周期，流转链路长、涉及人员机构复杂，安全管控难度较高。**基础镜像来源复杂，源头管控难**，除官方镜像仓库外，还存在大量第三方镜像仓库，镜像来源难以统一把控，同时包括官方镜像在内的大量基础镜像均存在一定程度的安全漏洞，也为镜像安全的源头控制增加了难度。**传输过程中间人攻击篡改难校验**，现阶段容器签名技术尚未被企业、用户大范围采用，若用户采用非加密方式在镜像仓库下载传输容器镜像，传输过程中被中间人篡改而难以发现。**全链路交互人员复杂，链路监测追踪难实现。**容器镜像的完整生命周期涉及跨部门的多团队协作，开发、测试和运维人员会根据不同需求操作容器镜像，任何一个环节的改动都会增加镜像的安全风险。实现容器镜像全生命周期的流转监测、更改、部署和反向追踪难度较大。

应用微服务化增加攻击风险，存在连锁攻破可能

容器技术保证了运行环境的强一致性，为应用服务的拆分解耦提供了前提，应用微服务化进程加速，同时也带来新的安全隐患：**单体应用拆分导致端口数量暴增，攻击面大幅增加。**微服务将单体架构的传统应用拆分成众多个

服务，应用间交互的端口成指数级增长，相较于单体应用架构集中在一道口防护的简单易行，微服务化应用在端口防护、访问权限、授权机制等方面的难度陡增。**强关联微服务间连锁攻破风险高。**尽管微服务提倡隔离、轻量、独立开发部署、业务松耦合，但现实情况中很多场景下的多个服务间是紧密联系的，这些强关联的微服务间是点对点的形式进行沟通连接，随着连接点的增多，整个连接体系中的单一服务因漏洞被攻破会增加整个系统的破解风险。

2、平台管理能力亟需云化提升

企业IT云化管理需求凸显

企业数字化转型的经济效率更高，业务产品上线周期缩短，业务运营更加快速，为了匹配业务产品的上线速度，企业数字基础设施资源和能力的交付需要从被动支撑向更敏捷、更主动的交付转型。首先需要结合云计算技术实现对底层基础软硬件资源的统一管理，其中虚拟化实现资源的快速交付，容器实现应用的快速部署，微服务架构实现应用开发的拆分；其次需要资源和共性组件的模块化、PaaS平台化，低成本定制开发适配多种业务场景和职能部门需求的IT工具产品，从而实现IT工具服务的敏捷交付和自服务式使用。

以客户为中心的IT服务运营

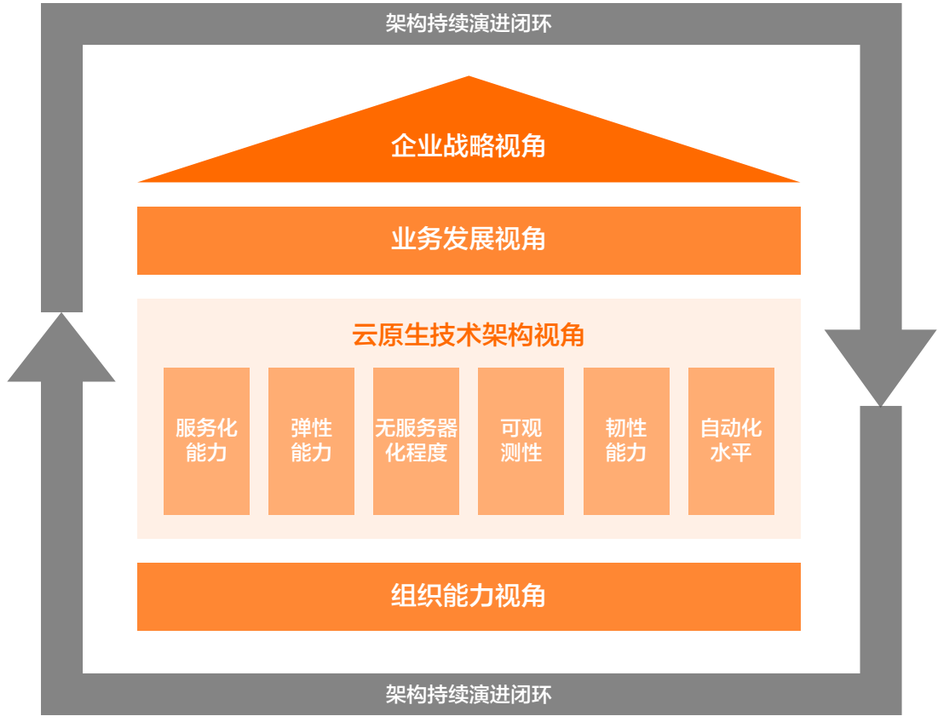
云原生架构下，IT管理转型的关键是管理者以客户为中心的服务运营思路。一是IT管理者更加关注用户体验和客户满意度，从战略管理上将服务运营理念运用到IT管理过程中，打破部门间壁垒，重组资源配置、业务流程和生产方式，促进企业各方面IT管理更加精准有效，发挥企业整体效能；二是通过合理规划组织架构、人才、资源与技术的配比，使组织架构与IT服务产品能力和服务运营体系相匹配，以最小的成本投入输出高质量的IT服务和产品，促进IT服务能力最大化，持续提升客户满意度，最大化带来价值，实现IT部门从成本中心到价值中心的转型升级。

5 阿里巴巴云原生架构设计

1 ACNA（Alibaba Cloud Native Architecting）架构设计方法

阿里巴巴为大量各行各业的企业客户提供基于阿里云服务的解决方案和最佳实践，帮助企业基于阿里云特别是云原生技术完成数字化转型，并积累了大量的方案和经验教训。阿里巴巴将企业的核心关注点、企业组织与 IT 文化、工程实施能力等方面与架构技术等进行结合，形成了阿里巴巴独有的云原生架构设计方法——ACNA（Alibaba Cloud Native Architecting）。

ACNA 是一个「4+1」的架构设计流程，「4」代表架构设计的关键视角，包括企业战略视角、业务发展视角、组织能力视角和云原生技术架构视角；「1」表示云原生架构的架构持续演进闭环。4 个架构视角和一个闭环的关系如下图所示：



ACNA 架构图设计方法

ACNA 除了是一个架构设计方法，也包含了对云原生架构的评估体系、成熟度衡量体系、行业应用最佳实践、技术和产品体系、架构原则、实施指导等。

2 企业战略视角

任何架构都必须服务于企业战略，云原生架构也不例外。云原生架构和以往的架构升级不同，云原生架构不仅是一个技术升级，更是一个对企业核心业务生产流程（即通过软件开发和运营构建数字化业务）的重构，如果打一个比方的话，就像工业时代用更自动化的流水线替换手工作坊一样深刻。

企业必须规划清楚战略中业务战略与 IT 战略之间的关系，即 IT 战略只是服务好业务战略进行必要的技术支撑呢，还是 IT 战略本身也是业务战略的一部分。通常高科技公司本身会对云计算有更高的需求，比如通过大量使用云厂商提供的 AI 技术为用户提供智能化的用户体验，也会使用 IoT 和音视频技术为用户建立更广泛和生动的连接。实际上我们发现，在数字化转型的今天，越来越多的企业认为 IT 战略应该在企业战略中扮演技术赋能业务创新的重要角色，CTO（Chief Technology Officer）、CIO（Chief Information Officer）、CDO（Chief Data Officer）、CISO（Chief Information Security Officer）等岗位的设计也从一个层面表明了这些技术在企业战略中的位置。

3 业务发展视角

阿里巴巴在为企业提供云服务和咨询的过程中，发现数字化业务对技术架构的主要诉求是业务连续性、业务快速上线、成本以及科技赋能业务创新。业务连续性诉求主要包括了数字化业务必须能够持续为用户提供服务，不能因为软硬件故障或者 bug 导致业务不可用，也能够抵御黑客攻击、数据中心不可用、自然灾害等意外事故。此外，当业务规模快速增长时，不能因为软硬件资源来不及购买或者部署而导致不能拓展新用户。

市场瞬息万变，数字化业务由于比传统实体业务更灵活可变而被要求更快的推向市场能力，包括新业务快速构建的能力、现有业务快速更新的能力。这些能力诉求被云原生架构深刻理解并在产品、工具、流程等层面得到不同程度的处理，需要注意的是这个诉求同时对组织结构带来了新的要求，也可能要求应用进行彻底的重构（比如微服务化）。

云计算作为新的技术必须为企业释放成本红利，帮助企业从原来的 CAPEX 模式转变为 OPEX 模式， 不用事先购买大批软硬件资源，而是用多少付多少；同时大量采用云原生架构也会降低企业开发和运维成本，有数据展示通过采用容器平台技术就降低了 30% 以上的运维支出。

传统模式下如果要使用高科技技术赋能业务，有一个冗长的选型、POC、试点和推广的过程，而大量使用云厂商和三方的云服务，由于这些云服务具备更快的连接和试错成本，且在不同技术的集成上具备统一平台和统一技术依赖的优势，从而可以让业务更快速的应用新技术进行创新。

4 组织能力视角

云原生架构涉及到的架构升级对企业中的开发、测试、运维等人员都带来了巨大的影响，技术架构的升级和实现需要企业中相关的组织匹配，特别是架构持续演进需要有类似“架构治理委员会”这样的组织， 不断评估、检查架构设计与执行之间的偏差。

此外前面提到云原生服务中重要的架构原则就是服务化（包括微服务、小服务等），这个领域典型的一个原则就是“康威定律”，要求企业中让技术架构与企业沟通架构保持一致，否则会出现畸形的服务化架构实现。

5 云原生技术架构视角

服务化能力

用微服务或者小服务构建业务，分离大块业务中具备不同业务迭代周期的模块，并让业务以标准化 API 等方式进行集成和编排；服务间采用事件驱动的方式集成，减小相互依赖；通过可度量建设不断提升服务的 SLA 能力；

弹性能力

通过资源池化确保弹性可用；自动根据业务峰值、资源负载扩充或者收缩系统的规模；

无服务器化程度

在业务中尽量使用云服务而不是自己持有三方服务，特别是自己运维开源软件的情况；并让应用的设计尽量变成无状态的模式，把有状态部分保存到云服务中；尽量采用 FaaS、容器/ 应用无服务器的云服务；

可观测性

IT 设施需要被持续治理，任何 IT 设施中的软硬件发生错误后能够被快速修复，从而不会让这样的错误对业务带来影响，这就需要系统有全面的可观测性，从传统的日志方式、监控、APM 到链路跟踪、服务 QoS 度量；

韧性能力

除了包括服务化中常用的熔断、限流、降级、自动重试、反压等特性外，还包括高可用、容灾、异步化的特性；

自动化水平

关注整个开发、测试和运维三个过程的敏捷，推荐使用容器技术自动化软件构建过程、使用 OAM（Open Application Model）标准化软件交付过程、使用 IaC（Infrastructure as Code）/GitOps 等自动化 CI/CD 流水线和运维过程；

安全能力

关注业务的数字化安全，在利用云服务加固业务运行环境的同时，完善安全软件开发生命周期，使应用符合 ISO27001、PCIDSS、等级保护等安全要求。

6 架构持续演进闭环

云原生架构演进是一个不断迭代的过程，每一次迭代都是从企业战略、业务诉求到架构设计与实施的一个完整闭环，整体关系如下图：

架构持续演进闭环

其中，

关键输入：企业战略视角、业务发展视角；

关键过程：识别业务痛点和架构债务、确定架构迭代目标、评估架构风险、选取云原生技术、制定迭代计划、架构评审和设计评审、架构风险控制、迭代验收和复盘。

7 云原生架构成熟度模型

由于云原生架构包含了 6 个关键架构维度（ 简写为 SESORA，Service + Elasticity + Serverless + Observability + Resilience + Automation ），因此我们先定义关键维度的成熟度级别：

指标维度	ACNA-1（0分）	ACNA-2（1分）	ACNA-3（2分）	ACNA-4（3分）
服务化能力（Service）	无（单体应用）	部分服务化&缺乏治理（自持技术，初步服务化）	全部服务化&有治理体系（自持技术，具备治理能力）	Mesh化的服务体系（云技术，治理最佳实践）
弹性能力（Elasticity）	全人工扩缩容（固定容量）	半闭环（监控+人工扩缩容）	非全云方式闭环（监控+代码伸缩，百节点规模）	基于云全闭环（基于流量等多策略，万节点规模）
无服务器化程度（Serverless）	未采用BaaS	无状态计算委托给云（计算、网络、大数据等）	有状态存储委托给云（数据库、文件、对象存储等）	全无服务器方式运行（Serverless/FaaS运行全部代码）
可观测性（Observability）	无	性能优化&错误处理（日志分析、应用级监控、APM）	360度SLA度量（链路级Tracing、Metrics度量）	用户体验持续优化（用观测大数据提升业务体验）
韧性能力（Resilience）	无	韧性能力（Resilience）	分钟级切流（熔断、限流、降级、多活容灾等）	秒级切流、业务无感（Serverless、Service Mesh等）
自动化能力（Automation）	无	自动化能力（Automation）	具备自描述能力的自动化（提升软件交付自动化）	基于AI的自动化（自动化软件交付和运维）

云原生架构成熟度	零级	基础级	发展级	成熟级
级别和定义	完全传统架构（未使用云计算或者云的技术能力）	小于等于10分	大于10且小于16分 且无ACNA-1级	大于等于16分 且无ACNA-2级

第一步
根据SESORA对6个未读分别评分并汇总

→

第二步
根据分值分段获得评级结果

6 各个行业面临的挑战及解决方案

随着云计算的普及与云原生的广泛应用，越来越多的从业者、决策者清晰地认识到「云原生化将成为企业技术创新的关键要素，也是完成企业数字化转型的最短路径」。因此，具有前瞻思维的互联网企业从应用诞生之初就扎根于云端，谨慎稳重的新零售、政府、金融、医疗等领域的企业与机构也逐渐将业务应用迁移上云，深度使用云原生技术与云原生架构。面对架构设计、开发方式到部署运维等不同业务场景，基于云原生架构的应用通常针对云的技术特性进行技术生命周期设计，最大限度利用云平台的弹性、分布式、自助、按需等产品优势。借助以下几个典型实践案例，我们来看看企业如何使用云原生架构解决交付周期长、资源利用率低等实际业务问题。

1 案例一：申通快递核心业务系统云原生化上云案例

1、背景和挑战

作为发展最为迅猛的物流企业之一，申通快递一直积极探索技术创新赋能商业增长之路，以期达到降本提效目的。目前，申通快递日订单处理量已达千万量级，亿级别物流轨迹处理量，每天产生数据已达到 TB 级别，使用

1300+ 个计算节点来实时处理业务。

过往申通快递的核心业务应用运行在 IDC 机房，原有 IDC 系统帮助申通安稳度过早期业务快速发展期。但伴随着业务体量指数级增长，业务形式愈发多元化。原有系统暴露出不少问题，传统 IOE 架构、各系统架构的不规范、稳定性、研发效率都限制了业务高速发展的可能。软件交付周期过长，大促保障对资源的特殊要求难实现、系统稳定性难以保障等业务问题逐渐暴露。

在与阿里云进行多次需求沟通与技术验证后，申通最终确定阿里云为唯一合作伙伴，采用云原生技术和架构实现核心业务搬迁上阿里云。2019 年开始将业务逐步从 IDC 迁移至阿里云。目前，核心业务系统已经在阿里云上完成流量承接，为申通提供稳定而高效的计算能力。

2、云原生解决方案

申通核心业务系统原架构基于 Vmware+Oracle 数据库进行搭建。随着搬迁上阿里云，架构全面转型为基于 Kubernetes 的云原生架构体系。其中，引入云原生数据库并完成应用基于容器的微服务改造是整个应用服务架构重构的关键点。

引入云原生数据库

通过引入 OLTP 跟 OLAP 型数据库，将在线数据与离线分析逻辑拆分到两种数据库中，改变此前完全依赖 Oracle 数据库的现状。满足在处理历史数据查询场景下 Oracle 数据库所无法支持的实际业务需求。

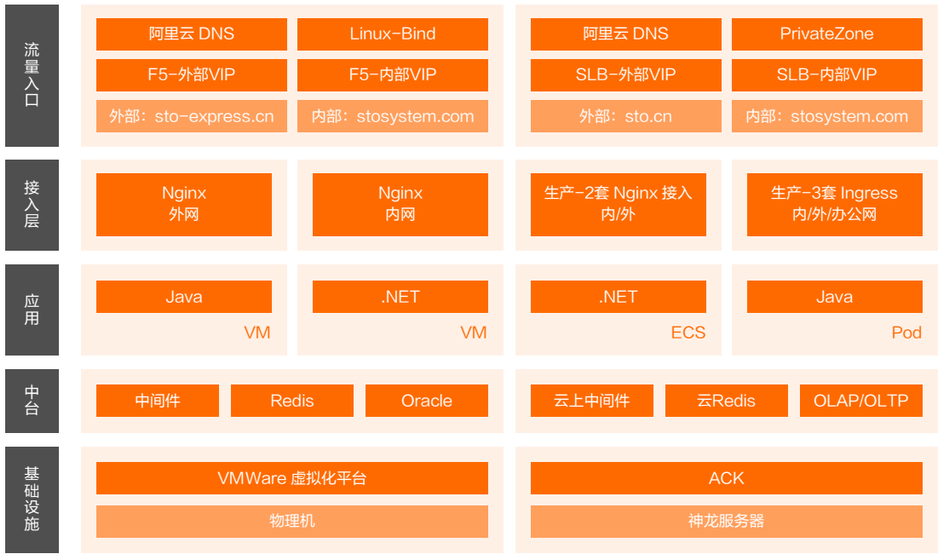
应用容器化

伴随着容器化技术的引进，通过应用容器化有效解决了环境不一致的问题，确保应用在开发、测试、生产环境的一致性。与虚拟机相比，容器化提供了效率与速度的双重提升，让应用更适合微服务场景，有效提升产研效率。

微服务改造

由于过往很多业务是基于 Oracle 的存储过程及触发器完成的，系统间的服务依赖也需要 Oracle 数据库 OGG 同步完成。这样带来的问题就是系统维护难度高且稳定性差。通过引入 Kubernetes 的服务发现，组建微服务解决方案，将业务按业务域进行拆分，让整个系统更易于维护。

综合考虑申通实际业务需求与技术特征，最终选择了「阿里云 ACK+ 神龙 + 云数据库」的云原生解决方案，从而实现核心应用迁移上阿里云。



上云混合态架构

申通核心业务上云架构示意图

2.1 架构阐述

基础设施，全部计算资源取自阿里云的神龙裸金属服务器。相较于一般云服务器（ECS），Kubernetes 搭配神龙服务器能够获得更优性能及更合理的资源利用率。且云上资源按需取量，对于拥有大促活动等短期大流量业务场景的申通而言极为重要。相较于线下自建机房、常备机器，云上资源随取随用。在大促活动结束后，云上资源使用完毕后即可释放，管理与采购成本更低，相应效率。

流量接入，阿里云提供两套流量接入，一套是面向公网请求，另外一套是服务内部调用。域名解析采用云 DNS 及 PrivateZone。借助 Kubernetes 的 Ingress 能力实现统一的域名转发，以节省公网 SLB 的数量，提高运维管理效率。

2.2 平台层

基于 Kubernetes 打造的云原生 PaaS 平台优势明显突出。

打通 DevOps 闭环，统一测试，集成，预发、生产环境； 天生资源隔离，机器资源利用率高；

流量接入可实现精细化管理；

集成了日志、链路诊断、Metrics 平台；

统一 ApiServer 接口和扩展，天生支持多云跟混合云部署。

2.3 应用服务层

每个应用都在 Kubernetes 上面创建单独的一个 Namespace，应用跟应用之间实现资源隔离。通过定义各个应用的配置 Yaml 模板，当应用在部署时直接编辑其中的镜像版本即可快速完成版本升级，当需要回滚时直接在本地启动历史版本的镜像快速回滚。

2.4 运维管理

线上 Kubernetes 集群采用阿里云托管版容器服务，免去了运维 Master 节点的工作，只需要制定 Worker 节点上线及下线流程即可。同时业务系统均通过阿里云的PaaS 平台完成业务日志搜索，按照业务需求投交扩容任务， 系统自动完成扩容操作，降低了直接操作 Kubernetes 集群带来的业务风险。

应用效益

成本方面：使用公共云作为计算平台，可以让企业不必因为业务突发增长需求，而一次性投入大量资金成本用于采购服务器及扩充机柜。在公共云上可以做到随用随付，对于一些创新业务想做技术调研十分便捷。用完即释放， 按量付费。另外云产品都免运维自行托管在云端，有效节省人工运维成本，让企业更专注于核心业务。

稳定性方面：首先，云上产品提供至少 5 个 9 以上的 SLA 服务确保系统稳定，而自建系统稳定性相去甚远。其次，部分开源软件可能存在功能 bug，造成故障隐患。最后，在数据安全方面云上数据可以轻松实现异地备份，阿里云数据存储体系下的归档存储产品具备高可靠、低成本、安全性、存储无限等特点，让企业数据更安全。

效率方面：借助与云产品深度集成，研发人员可以完成一站式研发、运维工作。从业务需求立项到拉取分支开发， 再到测试环境功能回归验证，最终部署到预发验证及上线，整个持续集成流程耗时可缩短至分钟级。排查问题方面， 研发人员直接选择所负责的应用，并通过集成的 SLS 日志控制台快速检索程序的异常日志进行问题定位，免去了登录机器查日志的麻烦。

赋能业务：阿里云提供超过 300 余种的云上组件，组件涵盖计算、AI、大数据、IOT 等等诸多领域。研发人员开箱即用，有效节省业务创新带来的技术成本。

② 案例二： 特步业务中台案例（零售、公共云）

1、背景和挑战

成立于 2001 年的特步，作为中国领先的体育用品企业之一，门店数 6230 家。2016 年，特步启动集团第三次战略升级，打造以消费者体验为核心的“3+”（ 互联网 +、体育 + 和产品 +）的战略目标，积极拥抱云计算、大数据等新技术，实现业务引领和技术创新，支撑企业战略变革的稳步推进。在集团战略的促使下，阿里云中间件团队受邀对特步 IT 信息化进行了深度调研，挖掘阻碍特步战略落地的些许挑战：

商业套件导致无法满足特步业务多元化发展要求，例如多品牌拆分重组所涉及的相关业务流程以及组织调整。对特步而言，传统应用系统都是紧耦合，业务的拆分重组意味着必须重新实施部署相关系统。

IT 历史包袱严重，内部烟囱系统林立。通过调研，阿里云发现特步烟囱系统多达六十三套，仅 IT 供应商就有三十余家。面对线上线下业务整合涉及到的销售、物流、生产、采购、订货会、设计等不同环节及场景，想要实现全渠道整合，需要将几十套系统全部打通。

高库存、高缺货问题一直是服装行业的死结，特步同样被这些问题困扰着。系统割裂导致数据无法实时在线，并受限于传统单体 SQLServer 数据库并发限制，6000 多家门店数据只能采用 T+1 方式回传给总部，直接影响库存高效协同周转。

IT 建设成本浪费比较严重，传统商业套件带来了“烟囱式”系统的弊端，导致很多功能重复建设、重复数据模型以及不必要的重复维护工作。

2、云原生解决方案

阿里云根据特步业务转型战略需求，为之量身打造了基于云原生架构的全渠道业务中台解决方案，将不同渠道通用功能在云端合并、标准化、共享，衍生出全局共享的商品中心、渠道中心、库存中心、订单中心、营销中心、用户中心、结算中心。无论哪个业务线、哪个渠道、哪个新产品诞生或调整，IT 组织都能根据业务需求，基于共享服务中心现有模块快速响应，打破低效的“烟囱式”应用建设方式。全渠道业务中台遵循互联网架构原则，规划线上线下松耦合云平台架构，不仅彻底摆脱传统 IT 拖业务后腿的顽疾并实现灵活支撑业务快速创新，将全渠道数据融通整合在共享服务中心平台上，为数据化决策、精准营销、统一用户体验奠定了良好的产品与数据基础，让特步真正走上了“互联网 +”的快车道。

2017 年 1 月特步与阿里云启动全渠道中台建设，耗时 6 个月完成包括需求调研、中台设计、研发实施、测试验证等在内的交付部署，历经 4 个月实现全国 42 家分公司、6000+ 门店全部上线成功。以下是特步全渠道业务中台总体规划示意图：

下面是基于云原生中间件的技术架构示意图

架构关键点：

应用侧：新技术架构全面承载面向不同业务部门的相关应用，包括门店 POS、电商 OMS、分销商管理供销存 DRP、会员客户管理 CRM。此外，在全渠道管理方面也会有一些智能分析应用，比如库存平衡，同时可以通过全渠道运营平台来简化全渠道的一些配置管理。所有涉及企业通用业务能力比如商品、订单等，可以直接调用共享中心的能力，让应用“更轻薄”。

共享中心：全渠道管理涉及到参与商品品类、订单寻源、共享库存、结算规则等业务场景，也涉及与全渠道相关的会员信息与营销活动等。这些通用业务能力全部沉淀到共享中心，向不同业务部门输出实时 / 在线 / 统一 / 复用的能力。直接将特步所有订单 / 商品 / 会员等信息融合、沉淀到一起，从根本上消除数据孤岛。

技术层：为了满足弹性、高可用、高性能等需求，通过 Kubernetes/EDAS/MQ/ARMS/PTS 等云原生中间件产品，目前特步核心交易链路并发可支撑 10w/tps 且支持无线扩容提升并发能力。采用阿里历经多年双 11考验的技术平台，稳定性/ 效率都得到了高规格保障，让开发人员能够更加专注在业务逻辑实现，再无后顾之忧。

基础设施：底层的计算、存储、网络等 IaaS 层资源。

后台系统：客户内部的后台系统，比如 SAP、生产系统、HR/OA 等。

应用收益

全渠道业务中台为特步核心战略升级带来了明显的变化，逐步实现了 IT 驱动业务创新。

经过中台改造后，POS 系统从离线升级为在线化。包括收银、库存、会员、营销在内的 POS 系统核心业务全部由业务中台统一提供服务，从弱管控转变为集团强管控，集团与消费者之间真正建立起连接，为消费者精细化管理奠定了坚实的基础。

中台的出现，实现了前端渠道的全局库存共享，库存业务由库存中心实时处理。借助全局库存可视化，交易订单状态信息在全渠道实时流转，总部可直接根据实时经营数据对线下店铺进行销售指导，实现快速跨店商品挑拨。中台上线后，售罄率提升 8%，缺货率降低 12%，周转率提升 20%，做到赋能一线业务。

IT 信息化驱动业务创新，通过共享服务中心将不同渠道类似功能在云端合并共享，打破低效的“烟囱式”应用建设方式，吸收互联网 DDD (Domain Driven Design) 领域驱动设计原则，设计线上线下松耦合云平台架构，不仅彻底摆脱了传统 IT 拖业务后腿的顽疾并灵活支撑业务快速创新。全渠道数据融通整合在共享服务中心平台上，沉淀和打造出特步的核心数据资产，培养出企业中最稀缺的“精通业务，懂技术”创新人才，使之在企业业务创新、市场竞争中发挥核心作用。截止2019 年初，业务部门对 IT 部门认可度持续上升，目前全渠道业务支撑系统几乎全部自主搭建，80% 前台应用已经全部运行在中台之上，真正实现技术驱动企业业务创新。

INFORMATION

指导委员：
刘湘雯 / 刘松 / 任庚 / 霍嘉 / 何宝宏 / 刘俊龙

编写组长：
宿宸 / 李冰 / 陈立 / 刘旭 / 陈屹力

主笔成员：
阿里云 - 崔昊 / 王昕 / 彭智超
德勤中国 - 张志钢 / 蔡铁柱 / 杜军君 / 何江 / 罗以谨
中国信通院云计算与大数据研究所 - 刘如明

设计服务：
阿里云设计中心

致谢

本白皮书撰写期间，亦得到德勤中国云服务团队宋小娜、任姝，阿里云智能团队何登成、李力、何登攀、陈彦博、白明、赵而星、赵杰、吴伟波、付睿、赵秋杰、石阳、邱经忠、郭晶璠 对白皮书内容的贡献和支持。

特此致谢！

THANKS

阿里云研究中心简介

作为整个阿里云智能的研究机构，成立于2016年的阿里云研究中心，一直致力于用科技探索“新商业”边界。

研究领域主要包括两个方向：一方面涵盖云计算、人工智能、区块链、大数据、物联网、量子计算等前沿科技的演变趋势及产业应用；同时，更进一步积极探索在前沿科技的推动下，零售、数字政务和智慧城市、金融、制造、能源等产业的数智化转型路径及商业实践。

过去三年，阿里云研究中心一共产出了上百个数字化转型行业灯塔案例、数十份行业前瞻分析报告、几十门的在线课程，还通过首席增长官CXO平台、微咨询等产品和服务形态，为上百家政企机构提供了数字化转型的战略陪伴服务。

除了与阿里巴巴集团整个生态的研究力量紧密合作，阿里云研究中心还依托扎实的研究成果，与几十家国内外顶尖商学院、咨询公司、智库机构，和130多家行业协会、生态合作伙伴展开深入立体的交流合作，共同探讨产业数字化转型的方法论，为走在转型路上的企业高管带来思考和启发。

联系我们

宿宸
阿里云研究与战略咨询部总经理
suchen.cs@alibaba-inc.com

刘松
阿里巴巴集团副总裁
song.ls@alibaba-inc.com

钉钉请扫码

微信请扫码

欢迎扫码关注阿里云研究中心，查看更多数字化转型研究成果