华为云云采用框架

技术白皮书

文档版本 **01**

发布日期 6/28/2022

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目录

1 背景

数字技术新动能、数字经济新机遇、数字竞争新形势加速全球政企行业数字化转型及业务上云，但在战略落地中，政企行业往往面临什么能上什么不能上、先上什么后上什么、如何上、上云具体带来哪些价值、组织能力如何跟得上等一系列问题。

华为云云采用框架（Cloud Adoption Framework 简称 CAF）旨在帮助需要上云的客户从源头定义清楚上云的战略规划、策略方法、上云节奏，系统化做好上云准备和云上运行、云上治理，帮助客户架构师、运维、财务、安全等团队梳理清楚上云的方法和管理手段并构建所需能力，结合云服务产品能力，帮助各类角色实现业务目标，最终支撑政企数字化竞争力构建及商业成功。

华为云云采用框架以客户自身数字化转型战略为输入，结合全球政企行业项目实践及自身业务上云经验，整体分为四个阶段，云服务商提供相关服务支撑。

- **阶段一**：云规划， 在管理层明确上云动机，基于现状与差距分析，确定上云顶设蓝图、实施路径以及相应组织保障等关键举措，通过圈定范围、明确策略，为后续实施提供纲领性指引，保障方向正确。
- **阶段二**：上云准备， IT 团队负责 Landing Zone 建设和云上架构设计，做好上云准备。其中 Landing Zone 用于多业务单元“人财物权法”统一管控，云上架构用于满足业务及应用所需的 IaaS/PaaS/SaaS 云服务能力、云管理能力和高可用、可扩展、安全合规、高性价比、可运维等云架构能力。
- **阶段三**：云上运行， IT 团队和业务团队联合进行应用上云、数据上云及在云上开展业务创新，实现有序上云。
- **阶段四**：云上治理与运维，IT 团队负责通过成本管理、安全合规治理和云上运维，保证业务在云上经济、高效、安全、稳定的运行。

2 云规划

2.1 概述

云规划阶段旨在通过上云动机、IT 现状、关键差距的梳理分析及顶层设计规划，确定上云范围、上云战略、上云架构及上云节奏，确定关键能力构建目标，并将目标转化为可操作的行动计划。

云规划首要支撑预算授予、组织构建和人才培养，为后续上云实施提供“人财物权”保障；同时通过管理层汇报后应在相关组织进行基线发布，为后续上云实施提供“方向正确”保障。云规划一般会选取难度较低、价值较大的应用作为切入点进行项目试点，通过 Quick Win 在实战中构建组织级上云能力、消除问题风险。

云规划整体包括如下五大关键任务：

2.2 明确上云动机

8 个主要的行业上云动机：

✓ 解决软硬件生命周期等现实问题

一方面当有数据中心、服务器到生命周期，或者对多个 DC 进行整合，往往采用先进的云服务模式进行建设，而不是继续采用传统 DC；另一方面云服务模式能消除政企行业对 IT 硬件、中间件、技术平台等复杂的生命周期管理。

✓ 提升业务敏捷

云服务模式从三个层次提升业务敏捷：1）基础设施资源按需获取，避免硬件数周、数月到位周期影响新业务上市；2）应用、资源按需弹性伸缩，满足业务规模快速扩展需求；3）中间件、云原生、DevOps 等技术平台能力按需获取，降低新业务开发门槛、快速上市抢占先机。

✓ 降低 IT 成本

云服务模式可根据业务需求调整资源规模减少浪费性支出，降低基础设施和相关技术平台运维人员能力要求及运维成本，尤其采用公有云模式，无需管理运维本地数据中心、按需获取云资源及云服务能力，大幅降低 IT 成本，也大幅降低新业务创新的试错成本。

✓ 提升运维效率

云服务模式由云服务厂家数百、数千人专业运维团队提供专业运维服务，可以基于持续积累、全球经验显著提升运维质量和效率。

✓ 提升可靠和安全合规

云服务模式能基于丰富的行业最佳实践提供高可靠、高安全及行业合规所需的技术方案能力，协助完成策略制定、组织流程建设及标准认证。

✓ 支持全球化部署

云服务模式已部署的全球资源、全球网络和全球平台能帮助企业快速开展跨国新业务，并与集团形成业务、数据、管理的联动协同。

✓ 构建数据底座与数据资产

云服务模式从两个方面强化政企行业数据底座和数据资产建设：1）最先进的大数据、AI 智能、数据治理、数据安全等技术； 2）丰富的行业最佳实践，包括数据平台、性能优化、数据治理数据运营组织流程、数据智能场景应用等。

✓ 持续引入新技术加速业务创新和商业创新

云服务模式持续提供行业最新技术能力和实践经验，加速行业业务创新及商业创新，如云原生提升业务敏捷，AI 决策智能化、生产无人化/少人化，IoT 万物互联智能感知，区块链可信智能合约等。

不同政企行业、不同企业因为战略重点不同，所处的发展阶段不同，最核心的上云驱动力会有所不同，需要结合自身情况进行制定，可以从以下三个维度重点审视。

1. IT 现代化

➢ IT 系统现代化

当前 IT 系统往往面临三大困境：1）多业务单元、多部门多个数据中心，服务器和存储类型多种多样，应用绑定服务器，IT 资源效率低、成本高，维护及生命周期管理复杂；2）IT 系统灾备、安全、可扩展性、可维护性能力不足，不同程度影响业务稳定提供及按需扩容；3）受限于组织成员的能力与经验，在一些新技术领域如容器、云原生、区块链等引入困难，需要长时间摸索。迫切需要基于云上成熟的产品和丰富的经验快速构建自身所需的能力，实现 IT 系统现・代化升级，降本增效，构建面向未来行业竞争的 IT 支撑能力。

➢ IT 部门现代化

当前 IT 部门往往定位为支撑部门，被动支撑业务发展，但随着政企行业数字化转型的逐步深入，IT 及数字化能力渗透到规划、研发、生产、销售、服务、经营等全环节，直接影响业务结果及行业竞争力，迫切要求 IT 部门由被动支撑向主动服务转型，成为生产力的一部分，首要是意识、文化的转型，核心是云化服务化平台转型和数字化能力转型。

2. 数据智能与数据安全

数据已成为与土地、劳动力、资本、技术等传统要素并列的新型生产要素。如政府行业，数据驱动政务服务、政府治理跨部门联动协同，辅助政府管控、政策制定及管理决策，通过数据智能提升民众体验及政府效率，及时洞察社会、经济风向趋势并做出应对；如金融行业，数据智能辅助客户营销、信贷风控、产品设计等，同时支撑供应链金融、数字货币等重大业务扩展；如企业领域，数据智能实现设计测试仿真、智能原料配比、智能排产调动、供应链风险管理、经营可视等等，全环节提升企业效率质量、降低管控风险。

数据平台的能力要求越来越高，多样而庞大的数据量、波动的访问量、不断迭代的数据技术、不断涌现的场景需求，对数据平台高性能、高效率、高可靠、灵活扩展、快速演进提出了高要求，云服务模式成为必然选择，平台技术能力由云服务商提供，行业聚焦与自身数据相关的场景化能力。

数据安全逐步上升到关乎企业安全和国家安全的层面，云服务模式便于使用先进安全技术，统一管控数据安全，提供最大安全保障。

3. 业务及商业创新

数字化带动智能生产、智能服务、智能经营等业务创新，以及共享经济、产业链协同、能力外溢等商业创新，其中有两个特点：1）需要引入 AI、IoT、区块链、视频等新技术能力；2）需要快速推出和迭代，抢占先机并持续领先。云服务模式提供持续领先的 IaaS、PaaS、SaaS 能力，降低创新门槛和成本，加快创新落地。

2.3 现状与差距分析

制定上云策略前，应先梳理当前 IT 系统的底账、特殊需求和要解决的关键问题挑战，以及面向未来业务演进的可见新需求，进一步结合实际情况圈定上云关键目标。

完整的分析可参考如下云成熟度评估模型：

大类	战略与架构	敏捷开发与运营	业务应用云化服务化	云技术平台	云基础服务	云安全	云运营与运维	组织流程与能力
小类	云化战略 云化目标 云化战略规划 多云策略 云化蓝图架构牵引 云化路标和举措	DevOps流程 DevOps组织 DevOps运作机制 DevOps研发效能能力 DevOps平台化支撑	应用服务构建方法 应用服务拆分与构建 应用服务实现的技术 应用服务部署 应用服务注册发现 应用服务监控及健康检查 应用服务治理 应用服务生态与共享	应用使用PaaS服务水平 PaaS技术演进路标 容器化运行能力 基础中间件服务化能力 数据库服务化能力 创新服务平台能力 公共技术服务平台能力 集成能力 日志和监控服务能力	应用使用IaaS服务水平 多云架构规划 数据中心规划 全球可达网络能力 虚拟化资源池能力 自动化部署能力 弹性伸缩能力 高可靠能力 统一云管平台能力 容灾管理能力 容灾能力 数据备份能力	安全管理 网络安全能力 应用安全能力 主机安全能力 数据安全能力	运维流程 运维运营服务目录 服务化调用 一体化运维运营 自动化运维 智能化运营 在线配置管理 运维信息管理	云化组织 云化流程 实体化产品运作 DevOps敏捷团队 云化人才规划和获取 云化技能培养

重点完成的现状与差距分析包括：

- **基础设施分析：**

1) 基础资源和配置，如服务器、存储类型、基础配置、资源数量、资源使用率、生命周期、虚拟化、容器化和应用的分布等；

2) 特殊需求，如性能、安全、绑定关系和特殊的操作系统要求等；
3) 关键挑战，如可用性能力不足、难以维护等。

- **技术平台分析：**

1) 基础平台情况，如中间件、数据库、数仓、大数据、开发测试等平台数量、规模、使用情况；
2) 特殊需求及关键挑战，如中间件、大数据基于开源自研，性能和稳定性不足，缺乏对关键业务的容灾能力等；

- **关键应用分析：**

对关键应用进行分类，如包括渠道、业务系统、核心系统、数据四大类系统；渠道类要求性能弹性伸缩、功能快速迭代；业务系统要求系统可靠、容量按需扩展、业务灵活扩展；核心系统和数据要求系统绝对可靠稳定、大容量高并发。通过关键应用分类和分析，梳理明确关键需求，并为后续实施路径准备基础信息。

- **DFX（Design for X）能力分析：**

整体审视灾备、安全、性能、运维等能力存在的问题挑战；

- **面向未来演进的关键 GAP：**

比如 AI、区块链等新技术能力，基于容器、微服务、云原生的快速迭代能力，可拥抱公有云进行快速重构。

2.4 顶设蓝图

顶设蓝图明确上云战略、上云范围及关键能力构建目标，重点解决三大类问题：

1. 上云战略

首先是云模式选择，是商业敏捷和成本最优为首要目标，全面拥抱公有云；还是基于业务低时延、强安全监管等因素，采用混合云。其次就云服务商选择，是独家战略合作、联合构建领先能力，还是多云战略、选用各云服务商优势能力。

2. 顶层协同

垂直协同方面，包括如政府行业国家与州/省之间以及集团企业与分支公司之间的业务、数据、资源协同，以及云边协同；水平协同方面，包括混合云协同和地理容灾。

3. 上云架构和关键能力

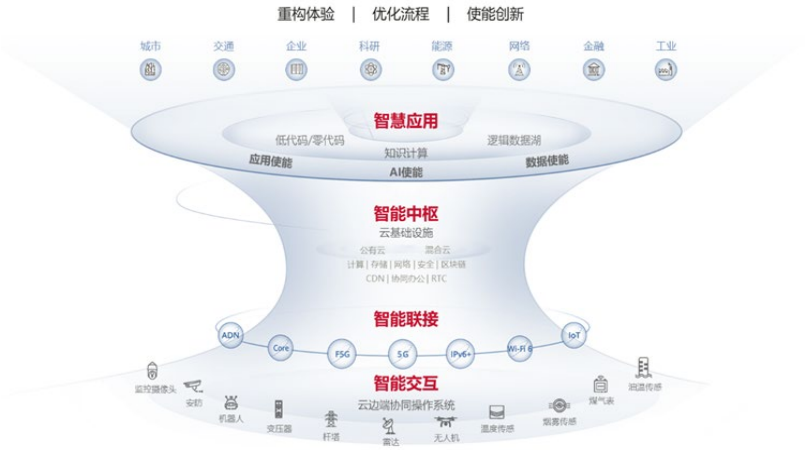
重点从 IaaS、PaaS、应用使能、应用/SaaS、云可靠、云安全、云运维、云运营分层次、分模块完成上云顶设蓝图。主要包括：

- 云基础设施：公有云/混合云、多云管理、多元算力、大数据存算、高性能计算…
- 数据湖：湖仓一体、灵活入湖、数据治理、数据安全、实时自助分析、数据智能应用…
- 使能平台：AI、视频、通信、IoT、区块链…
- 应用上云：上云范围、上云能力目标
- 应用创新（可选）：云原生应用、DevCloud、行业云…
- 云可靠：容灾、高可用 …

- 云安全：网络/主机/应用/数据安全体系、安全运营、安全生态、行业安全认证…
- 云运维：资源管理、云监控…
- 云运营：运营平台、组织、流程

具体顶设蓝图结合政企行业实际情况和惯用名称术语进行设计规划，以下为政府、企业通用参考架构示例。

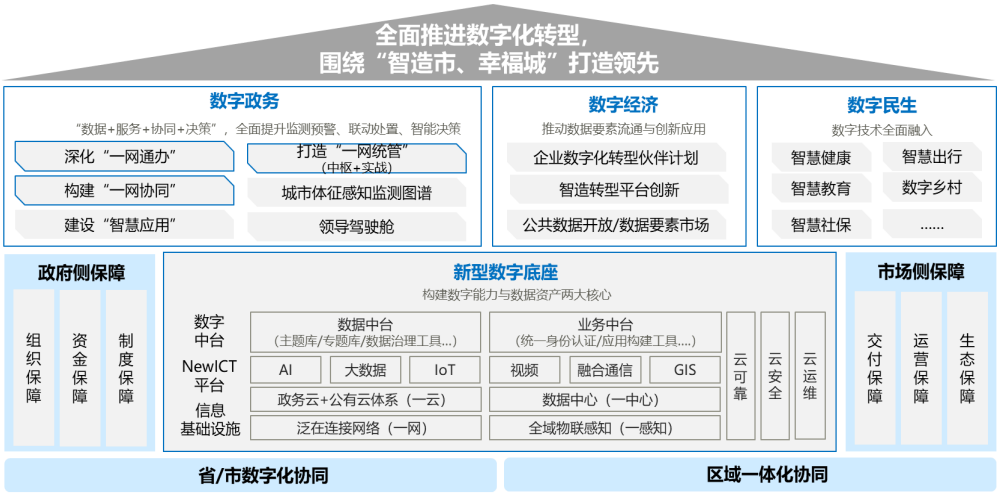
上云顶设蓝图重点是云应用、云基础设施、应用使能/AI 使能/数据使能平台能力，同时需要考虑与端侧/边侧智能感知交互的协同、云网协同，保障数据和应用的全面接入。



上云顶设参考架构 1

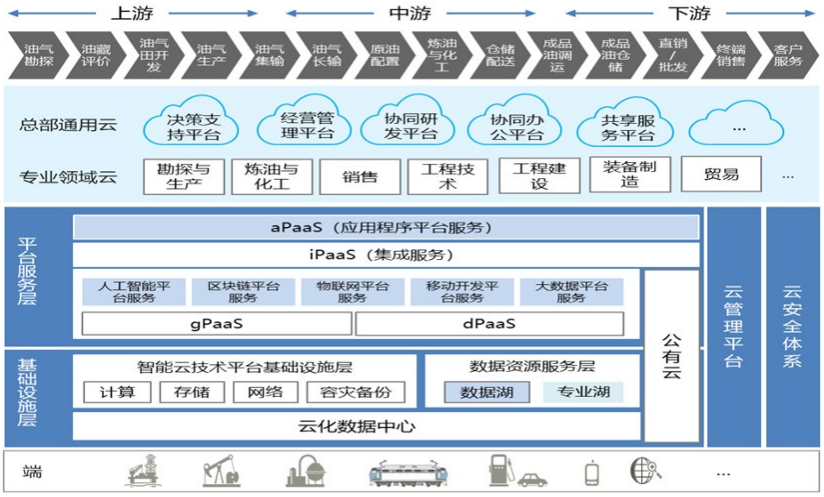
上云顶设参考架构 2

政府行业上云顶设的重点是打造一朵云、一张网、全感知，构建大数据、AI、视频、IoT 等新技术平台，加速政务、经济、民生类业务创新，除政府侧保障，同时引入国有运营公司实现交付、运营等保障。



数字政府上云顶设示例

能源企业上云顶设的重点是打造通用基础设施能力和平台服务能力，并在其基础上结合不同业务环节的场景化需求，打造专属能力。

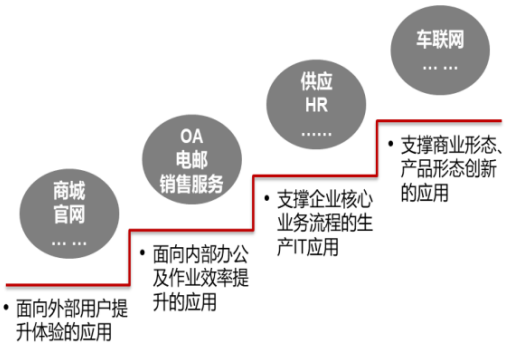


能源企业上云顶设示例

2.5 实施路径&上云计划

实施路径&上云计划基于“现网基础设施、技术平台、关键应用分析结果”和顶设蓝图明确的“上云范围、关键能力构建目标”，确定上云策略、上云节奏及试点项目。

- **上云分步参考：**

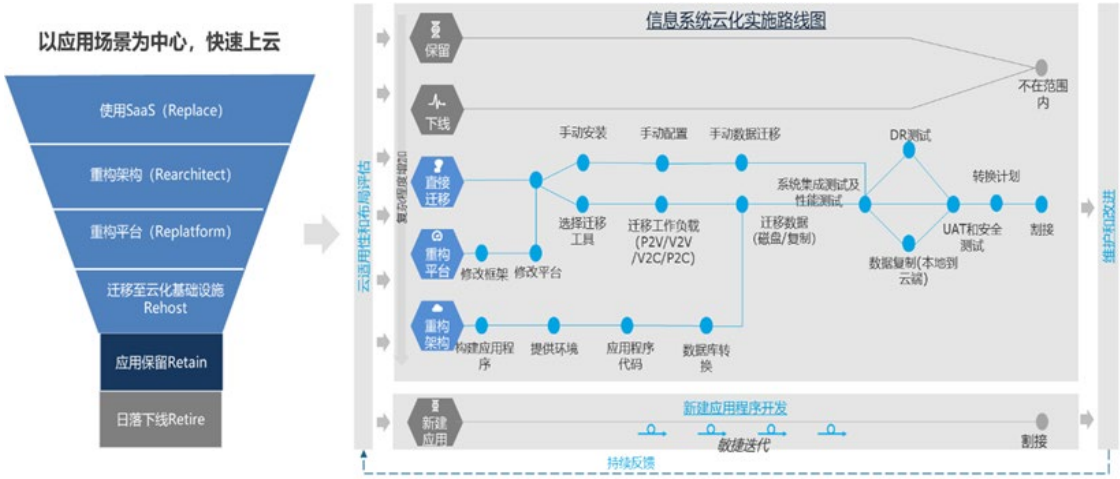


4S：基于华为 IT 应用上云实践形成的云化转型分步走方法：

- Step1：面向外部用户的应用；
- Step2：内部效率提升的应用；
- Step3：改变企业作业流程的核心业务系统；
- Step4：改变商业形态、产品形态。

➢ **上云策略：**

- Retire：即“日落下线”，对于企业中存在的已经没有使用价值、不再使用的部分应用系统，可以对其进行必要的归档备份后停用，减少对资源的浪费。
- Retain：即“应用保留”，是指在企业上云过程中基于资源成本、应用生命周期或企业业务策略等被识别为暂时不需要或者不适合上云的应用，策略上会采用保留的方式继续留在云下运行，但往往需要和云上其他应用进行访问互通和数据集成。
- Rehost：即 “直接迁移”或者“基础设施上云”，即对应用程序运行环境不做改变的情况下迁移上云， 一般的操作是 P2V（Physical to Virtual，物理机迁移至虚拟机）、V2V（Virtual to Virtual，虚拟机迁移至虚拟机），是应用进行云迁移时最常见的策略。
- Replatform：即 “重构平台”， 在不改变应用核心架构的基础上，对线下应用使用的中间件、数据库等基于云上的 PaaS 平台进行替换，以此来降低平台技术资源投入、降低管理成本，提升效率。
- Rearchitect：即“重构架构”，一般会改变应用的架构和开发模式，构建云原生能力，例如单体应用向微服务架构改造，这种策略一般在现有应用难以满足后续功能、性能、规模需求时采用，以支撑企业业务在云上的长远发展。
- Replace：即“新建应用”，指放弃原有应用，改为采购新的替代产品。典型的例子如新建 SaaS 应用或者购买第三方 SaaS 服务。



➢ **上云节奏：**

在确定上云节奏前，首先从上云价值&紧迫性、上云风险/业务影响、上云技术方案难度/业务复杂度三个维度对应用进行分级：

- 上云价值&紧迫性：如互联网类业务中对弹性扩缩容、敏捷性迭代要求高的应用，则上云价值高；如当前应用服务器面临生命周期问题，或需要基于云提供当前不具备的容灾能力，则上云紧迫性高；
- 上云风险/业务影响：如生产制造低时延类应用、金融核心系统，对性能、高可靠、数据安全管控等要求高，同时业务影响面大，上云影响较大；
- 上云技术方案难度/业务复杂度：如应用未做分层解耦而复杂度很高、周边依赖多，则上云技术方案难度较大。

为保障项目的顺利实施，结合华为云在“系统迁移、应用改造”类项目中总结的丰富经验，建议上云节奏遵循以下原则：

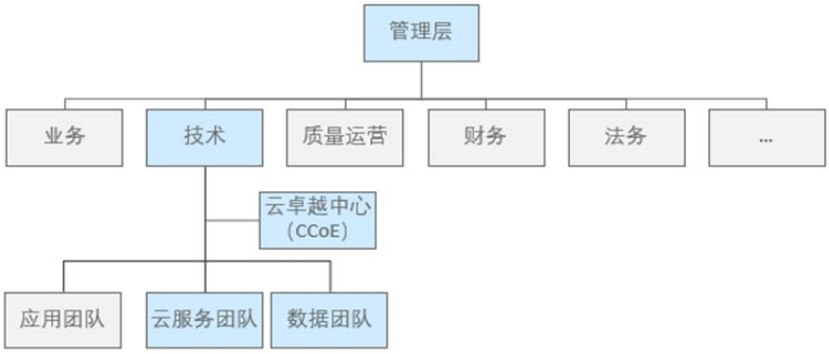
- 整体性原则：根据业务复杂度、业务定级确定迁移批次，优先迁移价值高、影响小、复杂度低的应用；
- 边缘到核心应用迁移原则：区分开发测试类业务、办公类业务、生产类业务、计费类业务等， 从支撑类应用到核心应用；
- 业务独立的应用优先迁移原则：对于周边关联关系少、业务复杂度低的应用优先迁移，对于业务复杂度高的应用后迁移；
- 应用迁移完整性原则：按照业务要求，保证实施范围、实施内容、实施流程的完整性，保证应用完整迁移，保障业务连续性；
- 最小影响原则：在实施过程中，充分考虑项目实施对目标系统的正常运行可能产生的不利影响，并采取必要的措施将风险降到最低。

➢ **试点项目：**

选取上云难度较低、驱动力强价值较大的部分应用进行项目试点，实现 Quick Win，实战中磨合组织、梳理流程、构建能力、消除风险。

2.6 组织和能力保障

确保云战略成功落地并且有生命力的持续演进，需要构建具有相应技能的组织来支撑，最有效的方法是建立一个集中式的治理团队。



➢ **管理层：**

业务上云涉及到治理体系的变化、组织架构的适配、云化文化和思维方式的塑造、项目实施管理、持续的运营运维优化等，是个系统性工程，也是一把手工程，需要最高管理层主导开展。核心包括：

- **明确战略**：战略层面确定上云动机、顶设蓝图及实施路径，对收益和风险有清晰的把控，并确保管理层及相关团队形成统一共识；
- **授予预算**：上云过程中，涉及采购资源、使用资源以及内部结算模式等变化，需要做好相应的财务预算及管控，以支持上云工作的顺利开展；
- **选择云服务商**：云服务商需具备强大的服务 2B 客户的基因，能够提供全流程服务、共享经验，同时能够保持长期投入，支持云平台技术的持续领先，才能够支撑客户聚焦业务的持续创新。选择合适的云服务商，是上云能够成功的基石；
- **优化组织**：成立拉通业务和 IT 部门的上云组织，明确职责分工和协同机制，制定决策及监督机制。

➢ **云卓越中心（CCoE：Cloud Center of Excellence）：**

云卓越中心（CCoE）支撑上云战略制定、承担架构职责，重点选择最佳解决方案、促进组织技能提升，具体包括定义云战略和策略、负责顶设蓝图、支撑云服务商选择、领导架构设计、指导云服务选择及运维治理等。CCoE 不承担日常业务职责，也不是项目管理组织。

CCoE 可以是一个虚拟团队，需要业务和技术职能之间的协作。CCoE 包括不限于以下角色。

- 云战略专家：负责云战略和战略分解；
- 云架构专家：负责云架构设计和迁移策略；
- 安全合规专家：负责安全云服务规划，构建、验证和部署安全策略；
- 业务、财务、法务、质量运营等相关专家。

➢ **云服务团队和数据团队：**

云服务团队负责具体的建云、上云、管云实施方案和方案交付，如包括：

- 建云阶段，按需构建云基础设施、PaaS、业务使能平台及灾备、安全等能力，除了云管自身功能，还需考虑将云管集成到企业整体运维管理体系中，进一步构建自助式资源管理、智能运维等能力。
- 上云阶段，联合应用团队，制定应用上云流程，负责具体上云方案制定与实施。
- 管云阶段，负责资源和权限管理、云上成本管控与优化、可靠性/安全/成本/性能等配置部署策略优化、云安全合规治理等。

数据团队负责具体的数据平台建设、数据管理、数据资产运营，如包括：

- 数据平台建设，基于云服务能力构建满足自身行业场景、性能、扩展性、成本、可靠性、安全等需求的数据平台。
- 数据管理，联合业务及云服务团队，负责数据集成、数据开发、数据治理、数据服务及数据安全，承接数据需求，保障数据质量，控制数据风险，对数据问题及争议进行处理及上升裁决。
- 数据资产运营，包括对内的数据共享交换、数据使用的规则流程制定、能力提供、流量监管，以及对外的数据资产变现运营，促进数据可信流通。

云服务团队和数据团队可以按照组织需要合设或分设，合设如政府行业，分设如部分企业。

➢ **人员培养计划：**

传统的 IT 工作如运维、安全等将发生重大变化。基础设施和技术平台由云服务商提供能力，政企 IT 工作更聚焦自身场景需求及能力构建，需要人员对云架构云技术有一定掌握，构建与自身场景结合的云方案、云迁移、云治理和数据管理运营能力，同时不断掌握新技术应用能力，满足政企使用云上最新 AI、IoT、区块链、微服务、DevSecOps 服务进行业务创新的需求。

人员培养计划需要通过原有人员培训转型和引入新兴人才两种渠道，构建与云服务模式匹配的新能力，支撑上云战略达成。

3 上云准备

3.1 概述

云上要构建高可靠、高可用的业务系统，需要有体系化的顶层设计框架和标准，从宏观层面统一规划，扫清后续上云的障碍。根据行业标准，结合华为云的自身实践，我们推出了适合华为云的 Landing Zone 体系架构理念，从“人财物权法”方面指导企业构建可靠的体系化能力；同时通过云上高可用架构能力建设，保障上云业务的高可用。

3.2 Landing Zone 建设

3.2.1 为什么需要 Landing Zone

公有云在安全稳定、服务质量、执行效率、成本效益等方面的优势逐渐被企业接受和认可，越来越多的企业逐步将全部应用系统往云上迁移，并优先采用云原生的方式开发面向未来的新应用系统。企业全面云化的时代已经来临，但在具体实践中经常会遇到以下各种挑战：

1. 如何做好业务单元（如事业部、部门、项目组等）的安全和故障隔离，确保业务单元之间的云资源、应用和数据的隔离？
2. 企业组织架构和业务架构经常调整，云上资源如何灵活应对？
3. 如何设计跨多个业务单元的网络架构、建立受控的网络连接通道？
4. 如何规划生产、开发和测试环境？
5. 公共资源如何在多个业务单元之间共享？
6. 如何统一管控各业务单元的预算和成本？如何优化云成本？
7. 如何避免各业务单元过度使用云资源？
8. 如何划分用户组？应该为用户组设置哪些权限？

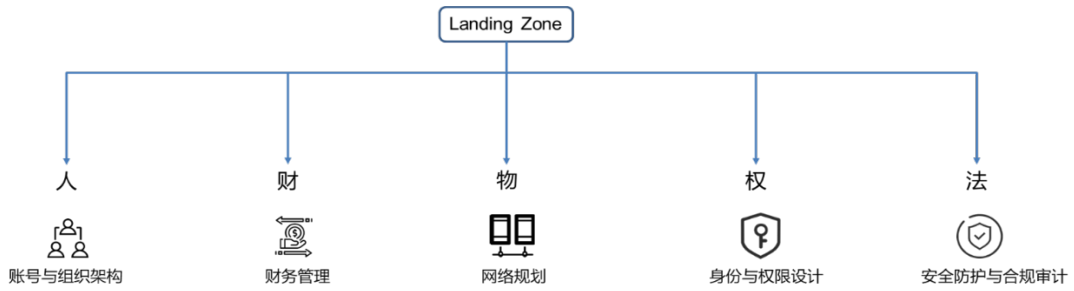
要应对上述挑战，需要设计一套全面的云上最佳实践，对业务单元、人员、权限、云资源、数据、应用、成本、安全等要素进行全面有效管理。华为云通过 Landing Zone 解决方案来全面应对这些云上的挑战。Landing Zone 本身是一个航空术语，指直升飞机等飞行器可以安全着陆的区域。云厂商都借用了这个航空术语，将企业业务系统安全平稳迁移到公有云的解决方案命名为 Landing Zone。华为云 Landing Zone 解决方案帮助企业在云上构建安全合规、可扩展的多账号运行环境，实现多账号的资源共享和“人财物权法”的统一管控。

1) 人的管理：多账号环境下对业务单元、账号、用户、用户组、角色等进行统一管理；
2) 财的管理：多账号环境下对资金、预算、成本、发票、折扣等进行统一管理；

3) 物的管理：多账号环境下对计算、存储、网络、数据、应用等云资源进行统一运维、监控和管理；
4) 权的管理：多账号环境下对云资源的访问权限进行统一管理，确保访问权限符合最小授权原则；
5) 法的管理：多账号环境下对安全合规进行统一管理，确保符合国家、行业和企业自身的安全合规要求。

3.2.2 Landing Zone 参考架构

以上提到的“人财物权法”分别对应的就是账号与组织架构、财务管理、网络规划、身份与权限设计、安全防护与合规审计。



以下分别对每个模块进行介绍。

3.2.2.1 账号与组织架构

Landing Zone 解决方案需要在云上构建安全合规、可扩展的多账号运行环境，首先要规划账号与组织架构。

华为云提供以下参考架构，建议按照业务架构、地理架构、IT 职能等维度设计组织层级和账号。

第一、按照业务架构在华为云上划分不同的组织层级和 Organization Unit(简称 OU)，每个业务 OU 下面可以按照业务系统创建独立的子账号。根据规模和隔离要求可创建独立或者共享的账号。

第二、按照地理架构在华为云上划分不同的组织层级和 OU，每个地理区域 OU 下面可以按照国家或地区创建独立的子账号，在上面可部署本地的客户关系管理系统、客户服务系统等。

第三、针对企业的中心 IT 部门，在华为云上创建对应的组织单元，并按照 IT 职能创建以下子账号，一方面实现 IT 管理领域的职责和权限隔离，另一方面对企业内多个子账号进行统一的 IT 管理。

账号名称	账号履行的 IT 职能	责任团队	资源或云服务
网络运营账号	集中部署和管理企业的网络资源，包括网络边界安全防护资源，实现多账号环境下的统一网络资源管理和多账号下 VPC 网络的互通，尤其需要集中管理面向互联网的出入口和面向线下 IDC 机房的网络出入口	网络管理团队，安全管理团队	NATG， EIP， VPC， 专线，云连接， VPN， CFW，WAF，Anti-DDoS
公共服务账号	集中部署和管理企业的公共资源、服务和应用系统，并共享给其他所有子账号使用	公共服务管理团队	NTP 服务器、AD 服务器、自建 DNS 服务器、OBS 桶、容器镜像库、协作办公系统等

安全运营账号	作为企业安全运营中心，统一管控整个企业的安全策略、安全规则和安全资源，为其他账号设置安全配置基线，对整个企业的信息安全负责	安全管理团队	统一部署具备跨账号安全管控的服务，如 DEW、SCM、VSS 等
运维监控账号	统一监控和运维各个子账号下的资源和应用，及时发现预警	运维团队	云堡垒机、Grafana，Prometheus 或第三方运维监控系统
日志账号	集中存储其他账号的运行日志、审计日志	日志分析团队，合规审计团队	日志服务 LTS、OBS 桶、SIEM 系统
数据平台账号	集中部署企业的大数据平台，将其他账号的业务数据统一采集到数据平台进行存储、处理和分析	数据处理团队，业务分析团队	数据湖、大数据分析平台、数据接入服务、数据治理平台
DevOps 账号	统一管理整个企业的 CI/CD 流水线，并进行跨账号部署	软件研发团队	DevCloud，或自建 DevOps 流水线
沙箱账号	用于进行各种云服务的功能测试、安全策略的测试等	测试团队	按需部署各种需要测试验证的资源和服务

除了上述子账号之外，中心 IT 部门可以根据自己的职责和权限隔离需求创建更多的子账号。比如独立的应用集成账号、协同办公账号等。

需要注意的是在组织的根下面会默认关联一个主账号，主账号下不建议部署任何云资源，主要是做好以下管理工作：

1) 统一组织和账号管理：创建和管理组织结构和组织单元，为组织单元创建子账号，或者邀请已有账号作为组织单元的子账号。
2) 统一财务管理：针对整个企业在华为云上的成本进行分析和统计；统一在华为云上充值、申请信用额度和激活代金券，再划拨给各个子账号，定期审视子账号的资金、信用额度和代金券的使用情况，及时进行回收。
3) 统一组织策略管理：为各个组织单元和子账号设置组织策略，强制限定子账号下用户（包括账号管理员）的权限上限，避免用户权限过大带来安全风险，创建组织策略时可以将其应用到某一个组织单元，该组织策略可以继承到关联的子账号和下层组织单元。

在每个子账号下面还可以通过企业项目（Enterprise Project， EP）或者标签对资源进行细粒度的逻辑分组，比如将一个应用系统的子系统、一个产品的子产品映射为华为云上的一个企业项目或者标签，并基于分组进行成本分摊、限定授权范围和资源筛选。

3.2.2.2 财务管理

3.2.2.2.1 概述

企业财务管理是华为云为有多账号的企业，提供账号管理、组织部门管理、资金、发票、账单、成本统一管理方案。

3.2.2.2.2 多账号财务管理

同一个企业下存在多个华为云账号时，可以建立企业主子账号关联关系，企业主账号可以根据自己的企业结构创建多层组织、新建子账号或关联子账号，并使其从属于主账号创建的组织部门，从而对这些子账号的财务进行管理。

1、主子账号关联

主账号可以通过创建一个华为云账号并与之关联，或者邀请一个华为云账号与之关联。同时主账号可以根据公司业务在企业中心创建组织部门信息，子账号可以从属于某个组织部门。

2、主子账号资金管理

主账号充值后，可以划拨现金、代金券给子账号用于资源的开通。子账号也可以通过自主充值后，进行资源的开通。

3、主子账号商务继承

主账号可以将其商务继承给子账号，继承后子账号的消费可以使用主账号的商务。避免同一家企业针对其不同账号需要签署多个商务的麻烦，增加了便利性。

4、主子账单查询

主子账号消费后，可分别登录华为云查看自己的消费数据。主账号可以申请查看子账号消费数据，申请成功后即可查看子账号的消费数据。

5、主子发票

主子账号消费后，各自独立向华为云申请开发票。主账号也可以代子账号开票。

3.2.2.3 网络规划

3.2.2.3.1 概述

合理规划云上网络架构是企业上云的基础，需对云下数据中心网络现状梳理，云上网络多账号设计、云上组网规划设计（包括 VPC 及子网、云上云下网络互通方案）等进行提前规划。

3.2.2.3.2 云下数据中心网络现状梳理

云下数据中心网络现状梳理，为了云上账号设计，云上组网规划设计做准备，主要内容包括：

1) 各数据中心的功能定位及业务承载梳理；

2) 云下各数据中心与云上 Region 和 AZ 的功能映射；

3) 数据中心内、数据中心间网络架构及网络分区梳理；

4) 应用系统分布及业务间数据流向梳理。

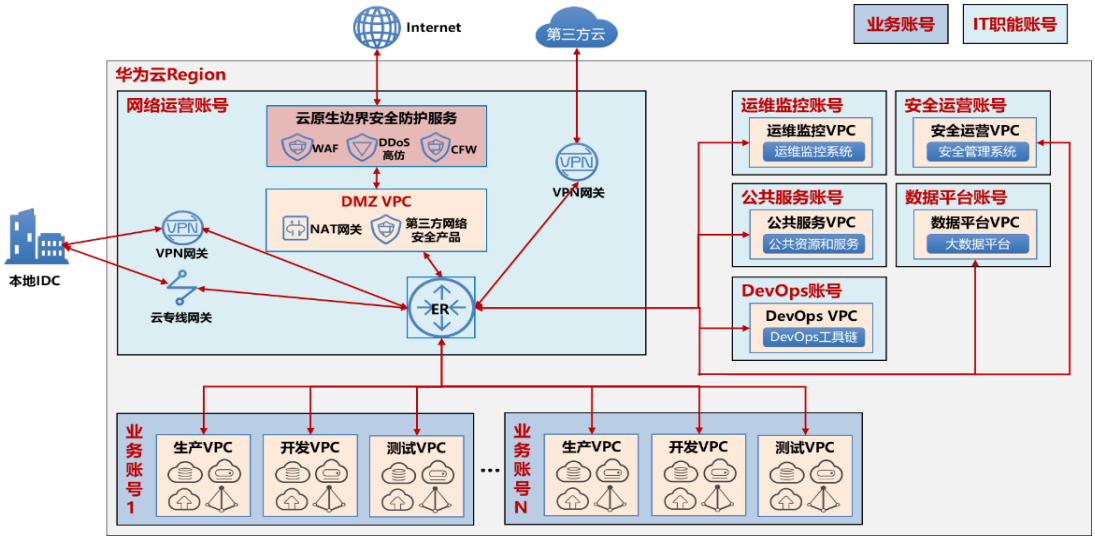
3.2.2.3.3 网络多账号设计

企业上云，在云上的账号需要与网络规划需要与云上账号有关联关系，以下分几个场景进行描述：

1) 单账号，单 VPC，账号管理简单(团队规划小)，安全要求低，统一在 1 个账号和 1 个 VPC 体系内，方便管理和运维；
2) 单账号，多 VPC，账号管理简单，安全要求中，使用多个 VPC 划分不同功能区和安全 域，统一在 1 个账号体系内，安全区域隔离，达到基本安全防护水平；
3) 多账号或者主子账号，多 VPC，账号管理要求高(团队规划大且多分支机构，分公司且业务复杂)，安全要求高。如果是同一 Region 内多账号多 VPC 通过企业路由器（Enterprise Router， ER）方式打通，如果是跨 Region 需要多账号多 VPC 通过云连接（Cloud Connect, CC）的方式打通。

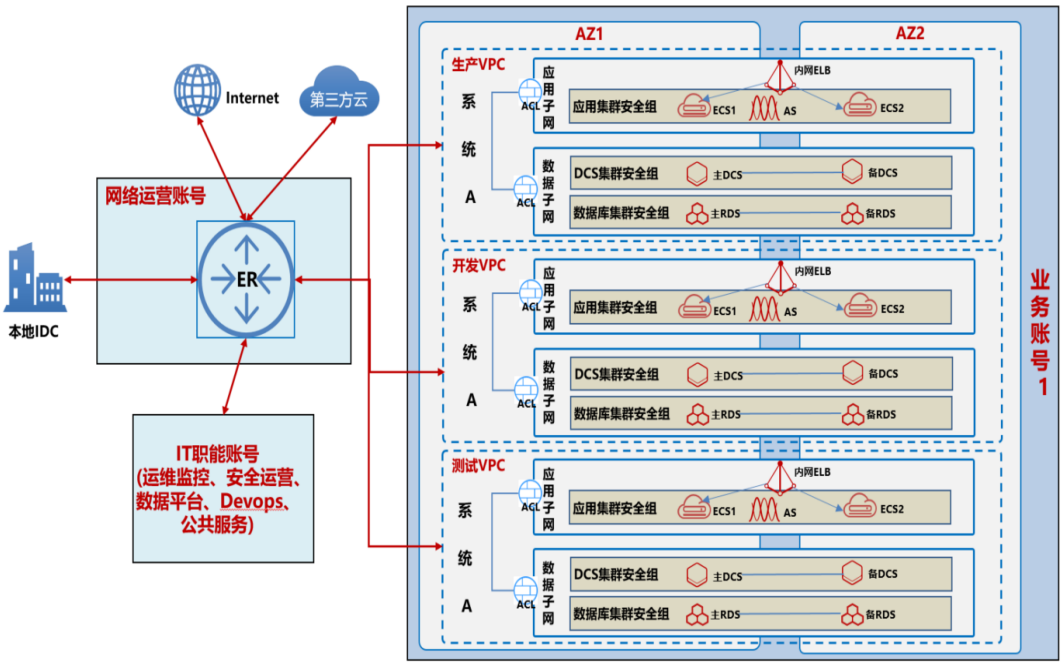
以上第一和第二种场景较为简单，主要是涉及 VPC 及子网的划分，请参考以下章节《云上组网规划设计》。以下重点讲讲多账号或者主子账号，多 VPC 的场景。

网络多账号多 VPC 架构设计如下图所示：

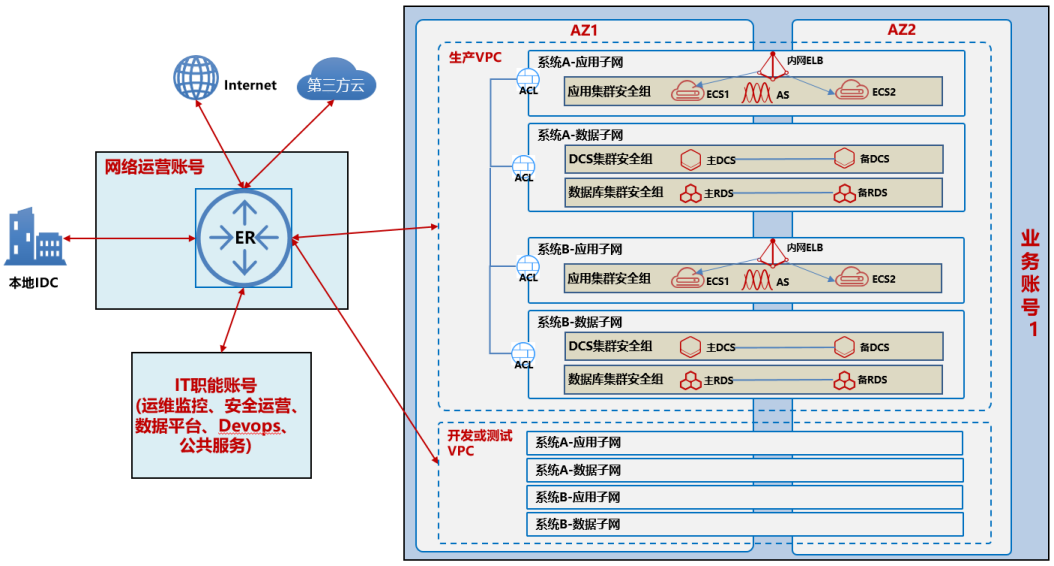


上述网络架构的核心是网络运营账号，作为连接其他账号的网络枢纽，其他账号之间的通信必须通过该账号的企业路由器（Enterprise Router， ER）进行。ER 可以通过设置路由规则决定哪些 VPC 之间的网络可以连通。

1. 针对一个大的业务系统，一般是对应一个独立的子账号，在该账号中我们建议为业务系统创建三个独立的 VPC：生产 VPC、开发 VPC、测试 VPC，VPC 之间彼此隔离。每个 VPC 至少部署二个子网：应用子网和数据子网，分别对应业务系统的应用层和数据层。子网之间使用网络 ACL 进行访问控制，还可以将云主机、DCS、RDS 等资源放入到安全组，通过安全组规则进行实例级别的访问控制。业务系统的应用主机集群可以跨可用区部署，实现应用层的高可用；再使用华为云跨可用区的主备数据库集群和缓存集群实现数据层的高可用。如下图所示：



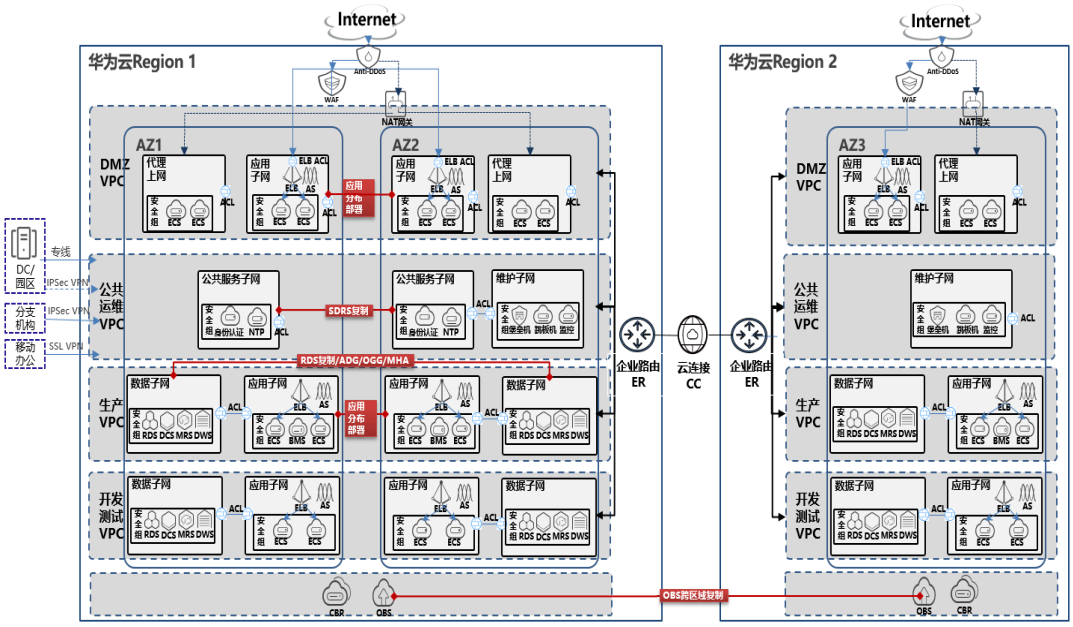
2. 针对多个没有严格安全隔离需求的小型业务系统，可以共用一个子账号，在该账号中同样建议创建三个独立的 VPC：生产 VPC、开发 VPC、测试 VPC，VPC 之间彼此隔离。这些小型业务系统共同部署在这几个 VPC 中，不同的业务系统通过子网隔离，每个业务系统也都有独立的应用子网和数据子网，为这些子网创建 ACL，以控制不同子网之间的内部网络流量。如下图所示：



注意:建议再为每个小型系统创建一个企业项目，将其生产、开发、测试环境的资源统一放置到该企业项目或者标签，并可以按照企业项目或者标签进行成本归集和细粒度授权。

3.2.2.3.4 云上组网规划设计

典型组网方案举例如下图所示，共分为以下几种场景，云上 VPC 及子网设计、云上 Internet 网络设计、 云上运维网络设计、云下到云上网络设计。

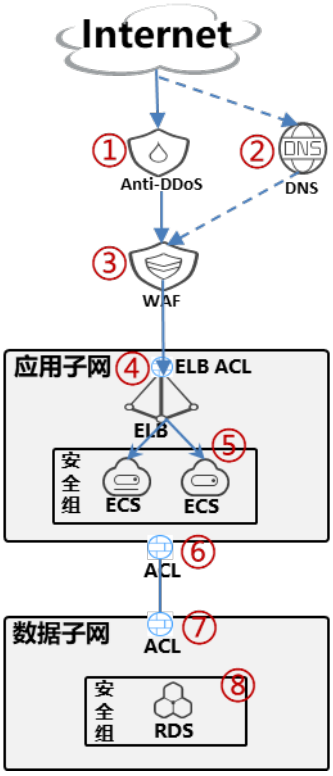


1、 云上 VPC 及子网设计

1) VPC 划分原则：
   a) 每个 VPC 可使用 IP 地址建议不超 5000 个；
   b) VPC 间默认隔离，可通过企业路由器（Enterprise Router， ER）实现点对点互通；
   c) VPC 划分为公共运维 VPC，DMZ VPC 和多个业务 VPC，不同 VPC 之间通过企业路由器（Enterprise Router， ER）方式打通；
   d) 业务 VPC 根据业务系统或部门划分：一个 VPC 对应一个相对独立的业务系统或部门，不需要互访的业务系统或部门应用分别部署在不同的 VPC；
   e) VPC 支持跨 AZ，跨 AZ 高可用部署的业务部署到同一个 VPC。
   f) 生产 VPC 和开发测试 VPC 默认不互通，不建立对等连接，数据传输建议通过 OBS 存储传输。
2) 子网划分原则：
   a) 企业应统一规划子网，避免 IP 地址段重叠；
   b) 同 VPC 内子网不可重叠，需要互通的 VPC 间子网不能重叠；
   c) 建议不同业务系统使用不同子网，可使用子网 ACL 控制按需访问；
   d) 建议应用和数据划分不同子网，默认数据子网只可被应用子网访问，应用子网按需对其他子网或者公网放通。
   e) 公共运维 VPC 对云下网络放通公共服务子网访问权限，按需放通维护子网访问权限。

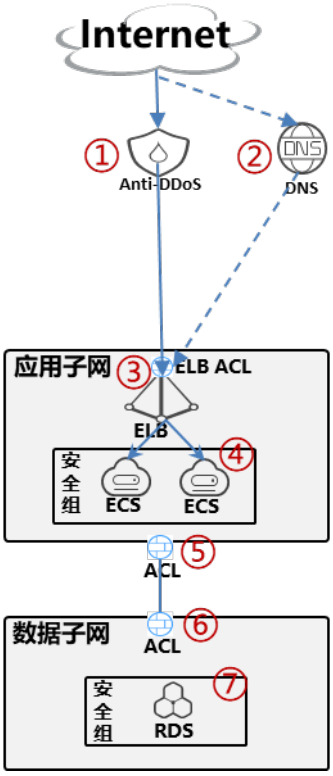
2、 云上 Internet 网络设计

方案 1：使用 WAF 进行 web 业务防护，如下图所示



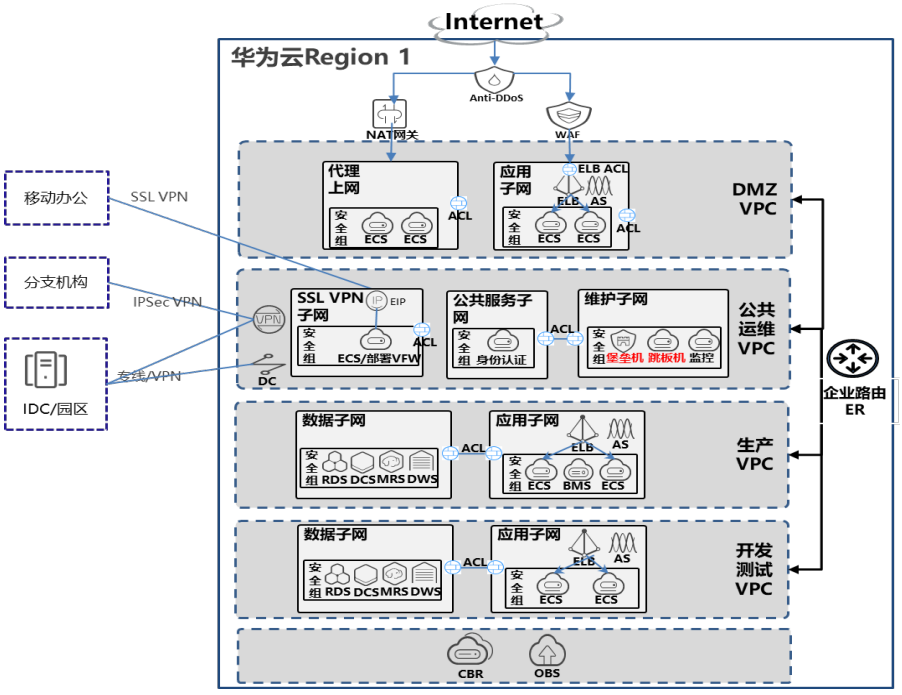
a) 针对公网 IP 开启 Anti-DDoS 服务，如果需要防护流量大需开启 DDoS 高防；
b) DNS 中配置 CNAME 将用户访问域名重定向到 WAF 进行 web 安全防控；
c) 使用 WAF 对域名进行 web 安全防护，将回源流量配置到 ELB；
d) ELB 通过白名单限制只有 WAF 回源 IP 地址池可访问；
e) 通过应用子网的业务虚机安全组限定可以访问主机的端口及 IP 地址段；
f) 应用子网 ACL 规则限定只与 WAF 回源地址及数据库子网互通；
g) 数据库子网 ACL 限定只有 web 所在应用子网可访问数据库 IP 及端口；
h) 数据库安全组限定数据库可访问端口及地址段；
i) 主机安全及数据库安全作为备选服务。

方案 2：未使用 WAF 进行 web 业务防护，如下图所示



a) 针对 EIP 公网 IP 开启 Anti-DDoS 服务，如果需要防护流量大需开启 DDoS 高防；
b) DNS 中配置域名解析到 ELB 公网 IP 地址；
c) ELB 通过黑白名单限制特定 IP 地址段可访问（可选）；
d) 通过应用子网的业务虚拟机安全组限定可以访问主机的端口及 IP 地址段；
e) 应用子网 ACL 规则限定只与数据库子网互通；
f) 数据库子网 ACL 限定只有 web 所在应用子网可访问数据库 IP 及端口；
g) 数据库安全组限定数据库可访问端口及地址段；
h) 主机安全及数据库安全作为备选服务。

3、 云上运维网络设计



a) 企业维护人员必须通过公共运维 VPC 接入企业内部网络后，才能通过云堡垒机维护云上资源；
b) 公共运维 VPC 和其它 VPC 之间通过企业路由器（Enterprise Router，ER）关联，通过子网 ACL 限制线下子网只能访问云上对外提供业务的子网，所有主机资源的维护只能通过维护子网进行；
c) 通过维护子网 ACL 及安全组，仅对线下具备维护权限的网段开通访问权限，限定访问维护子网的权限；
d) 各个 VPC 仅针对维护子网在网络 ACL 上放通远程连接端口；
e) 企业所有维护操作要求通过堡垒机进行操作，操作过程有记录，可审计。

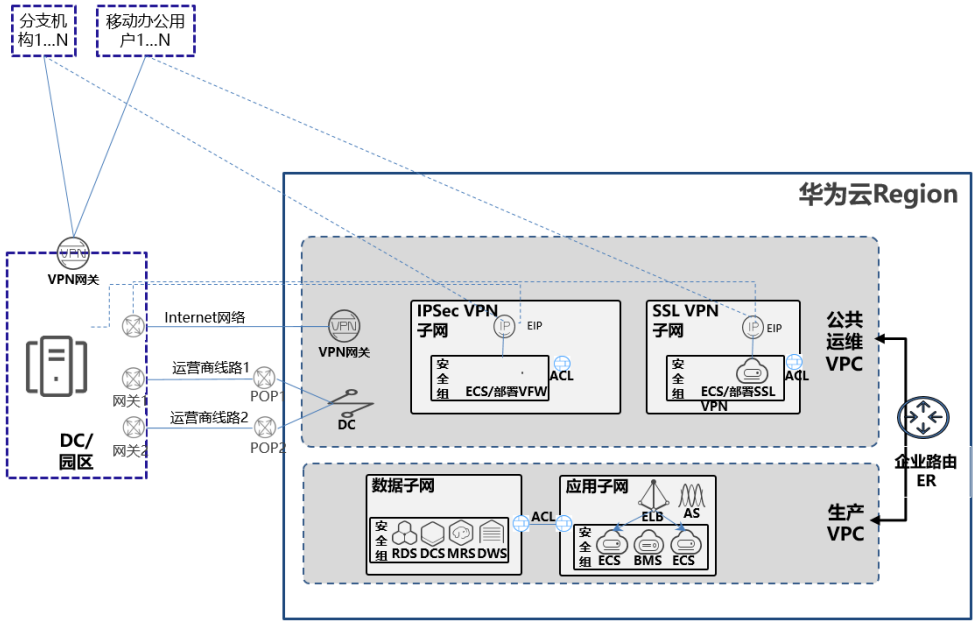
4、 云下到云上网络设计

云下和云上网络打通方案中，三种网络连接方式对比如下图，可根据场景需求进行选择。

对比项		专线上云	VPN 上云	SD-WAN 网络
架构	网络质量	高，SLA 保障	低，无 SLA 保障	中，Internet 就近接 入到 POP（主备），POP-云专线骨干段有保 障 双机可承诺 SLA（不包 括客户段 Internet）
	网络灵活度	低，按年付费，带 宽调整难	高，按需弹性计费，随时调整	中，按年付费，带宽调 整灵活
	硬件依赖	通用路由器	通用 VPN 设备	独采购配套的 SD-WAN 设备
	扩展服务	无	无	可提供安全，加速服务

成本	线路成本	高，10X	低，1X	中，3X
	时间成本	月	小时	天（含设备到货）
	维护成本	专业维护人员，管理分散	专业维护人员，管理分散	无需专业人员，云下轻配置，线上统一管理， 网络质量可视

1） **线下 DC/园区、分支机构、移动办公网络接入华为云：**



DC/园区接入场景：快速实现 DC/园区到公有云的安全可靠互联；复用云上 internet 出口降低成本；企业用户能够直接通过公司内网访问公有云服务。

方案 1：专线接入华为云公共运维 VPC（单链路/双链路）。

方案 2：IPSec VPN 接入华为云公共运维 VPC。

分支机构接入场景：企业有多个分支机构，将分支机构快速安全接入到云上网络，并对网络安全和时延有一定要求。

方案 1：IPSec VPN 接入华为云公共运维 VPC。

方案 2：分支机构通过 IPSec VPN 接入原 DC/园区网络，通过 DC/园区到公有云的专线/IPSec VPN 接入华为云公共运维 VPC。

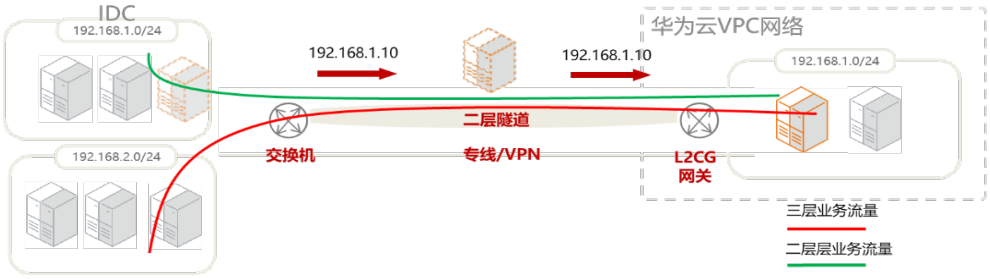
移动办公或门店接入场景：企业线下门店多或者分支机构多，多门店移动端 POS 等业务系统需要和云端的系统（如 ERP）保持实时交互，并对访问数据加密和网络时延有一定要求。通过公网公共安全性和稳定性得不到保障；通过专线链接成本过高。

方案 1：移动办公或门店通过 SSL VPN 接入华为云公共运维 VPC。

方案 2：移动办公或门店通过 SSL VPN 接入原 DC/园区网络，通过 DC/园区到公有云的专线/IPSec VPN 接入华为云公共运维 VPC。

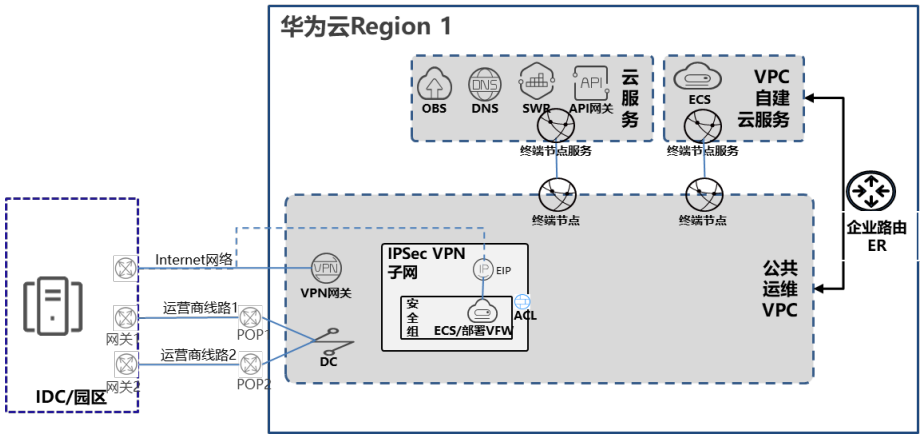
2) **IDC 主机 IP 地址不变迁移上云场景：**客户云下系统 IP 地址很多都固定，主机迁移到云上后不想换 IP，迁移过程不修改原有业务系统 IP 地址保证业务连续性。

方案：华为提供 L2CG 支持线上线下二层网络，极简网络规划，单个 IP 线上线下迁移，并且支持迁移过程线下线上业务不受影响。



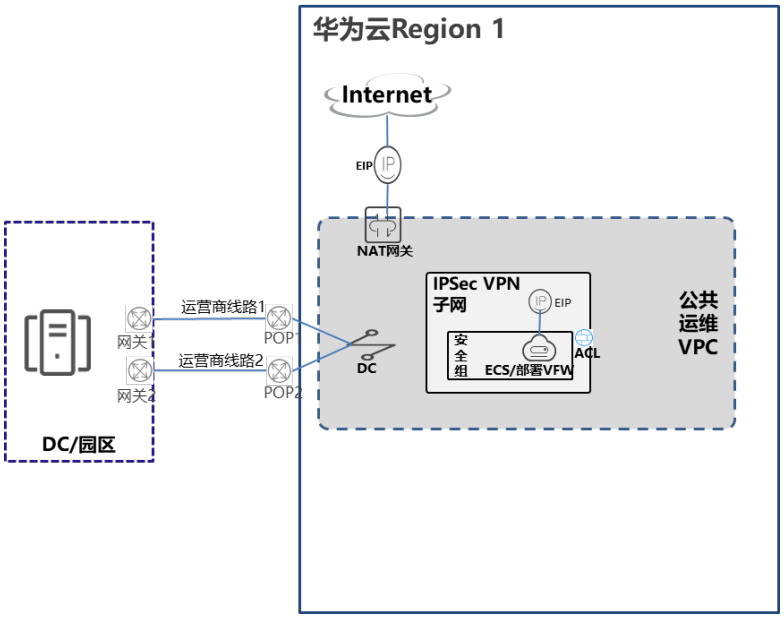
3) **IDC 通过内网访问云上服务场景：**企业用户通过内网直接访问云服务（OBS/SWR/API 网关），不需要通过 internet，如企业备份上云等。

方案：IDC 通过云专线/VPN 连接到华为云后，利用终端节点以内网方式访问华为云服务，安全高效，节约使用成本。

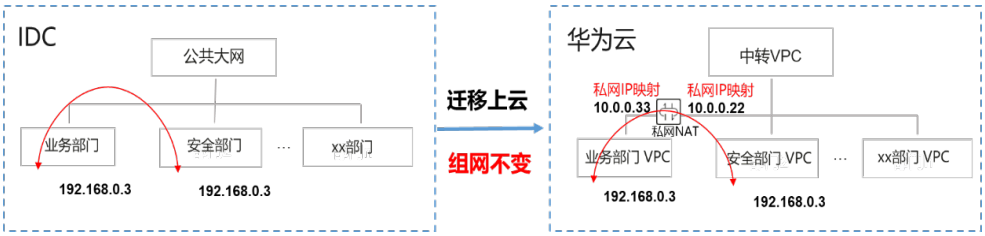


4) **IDC 复用云上 internet 出口场景：**企业 IDC 自有公共网线路质量差，价格昂贵，并且已经通过专线接入华为云，可以复用云上公网出口，节省成本，提高公网访问质量。

方案 1：专线+DNAT 线上线下共用公网出口。
方案 2：专线+SNAT 实现线下园区办公共享线上公网出口上网。

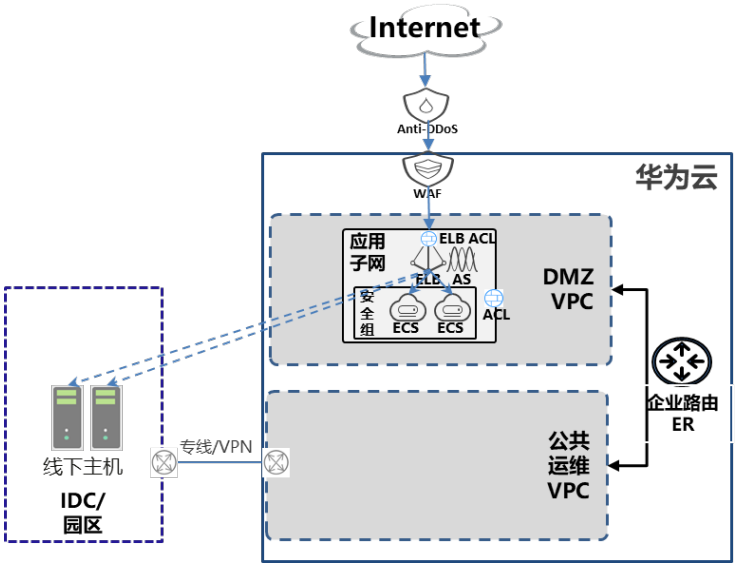


5) **企业私网 IP 重叠场景：**企业部门的网段独立规划，存在子网网段重叠的情况。客户希望保留原网段上云，且上云后仍能相互访问。
方案：华为云提供私网 NAT 网关，支持私网的 IP 地址映射。如下图，可以创建一个中转 VPC，然后使用私网 NAT 服务将业务部门的 192.168.0.3 转化为 10.0.0.33、将安全部门的 192.168.0.3 转化为 10.0.0.22，通过转化后的 IP 地址相互访问。



6) **ELB 云上云下负载均衡场景：**企业一部分业务仍然在 IDC 机房中，通过云上 ELB 对外提供服务，云端资源作为线下资源的弹性补充，应对流量高峰。

方案：通过云端 ELB 服务支持线下 IP 作为负载均衡主机组，解决云上云下业务融合，实现云上云下负载均衡。

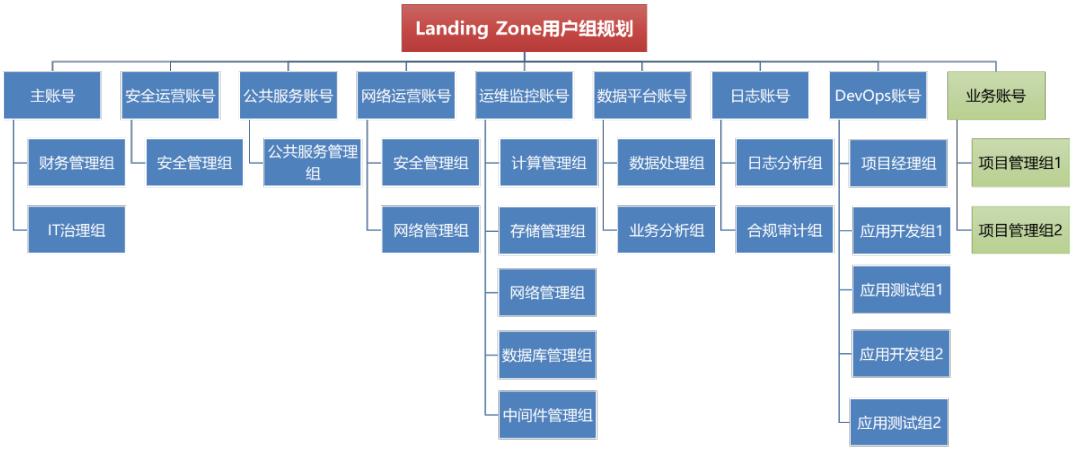


3.2.2.4 身份和权限设计

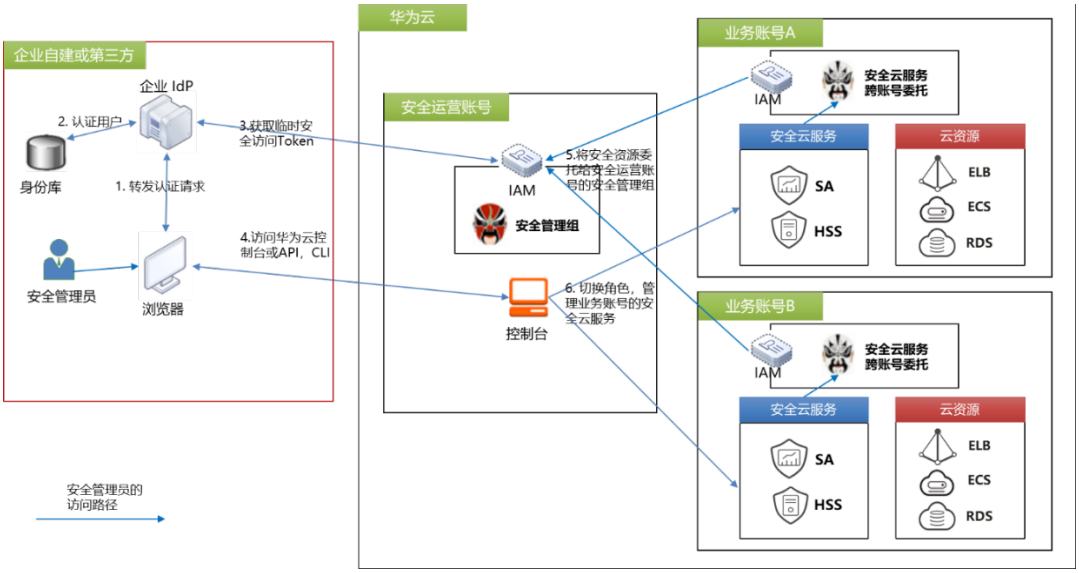
华为云基于大量成功交付的项目，总结提炼了以下用户和权限管理原则：

1) 建议使用企业自己的身份管理系统（如 AD 等）与华为云 IAM 进行联邦身份认证，前者的用户通过 SSO（Single Sign-on）登录到华为云控制台进行操作。企业自己的身份管理系统能更好更及时地匹配员工的入职、转岗和离职流程，避免转岗和离职人员继续拥有访问华为云的访问权限。
2) 不要把华为云 IAM 作为企业自己的用户管理系统，无需与华为云发生交互的企业员工，就不用在华为云 IAM 上创建相应的用户或用户组。
3) 不要将用户的密码共享给其他人，而是为每个管理或使用华为云资源的人创建一个单独的用户并分配相应的权限，这样每个自然人在华为云的操作都能被追踪审计。
4) 建议按照 IT 职能来划分用户组，将对应的员工加入与其职责匹配的用户组，如从资源运维和管理角度，需要遵守统一管理和运维的原则以提升效率。在运维监控账号内按照运维职责创建统一管理的用户组，包括计算管理组、存储管理组、网络管理组、数据库管理组等。
5) 遵守最小授权原则，只授予用户组完成职责所需的最小权限，如果用户组的职责产生变化，应该及时调整用户组的权限。授权时建议按照用户组而不是用户进行授权，简化授权操作。
6) IAM 账号管理员（与 IAM 账号同名）的权限很大，建议不要直接使用 IAM 账号管理员访问华为云，而是创建一个 IAM 用户，并按照最小授权原则授予相应的权限，以使用该 IAM 用户代替 IAM 账号管理员进行日常管理工作，保护 IAM 账号的安全。

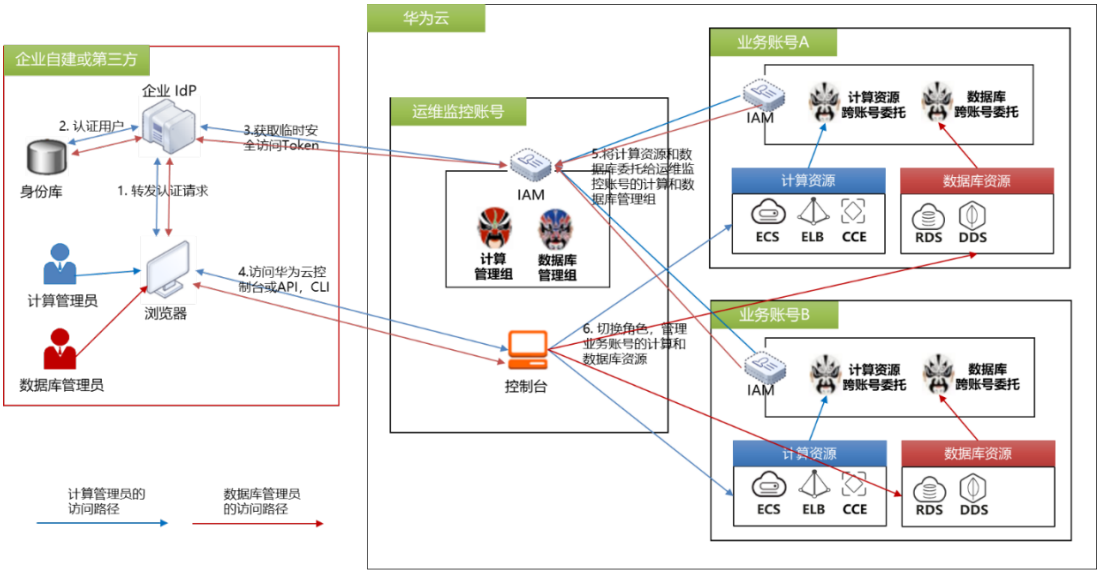
基于上述原则，针对 Landing Zone 的各类账号规划以下用户组，按照最小授权原则在华为云上为这些用户组配置对应的云服务访问权限。企业自己的身份管理系统的用户组逐一映射到华为云上的这些用户组，即可拥有对应的云服务访问权限。



Landing Zone 的各类 IT 职能账号为了实现统一管控的目标，需要通过委托的方式访问和管理其他账号下的云资源。举例来讲，Landing Zone 专门设计了一个安全运营账号，用于统一管理企业范围内多个账号的安全资源和服务，这就需要跨账号访问部署在其他业务账号下的安全服务（如 SA、HSS 等），通过以下联邦认证和跨账号委托的方式可以实现该目标。首先安全管理员通过 SSO 登录到安全运营账号的控制台，再通过切换角色到业务账号，然后访问和管理业务账号的安全云服务。



另一个类似的场景是运维监控账号需要统一监控和运维企业范围内多个账号的资源，这也要求运维监控账号能够跨账号访问其他账号下的资源，通过以下联邦认证和跨账号委托的方式可以实现该目标。



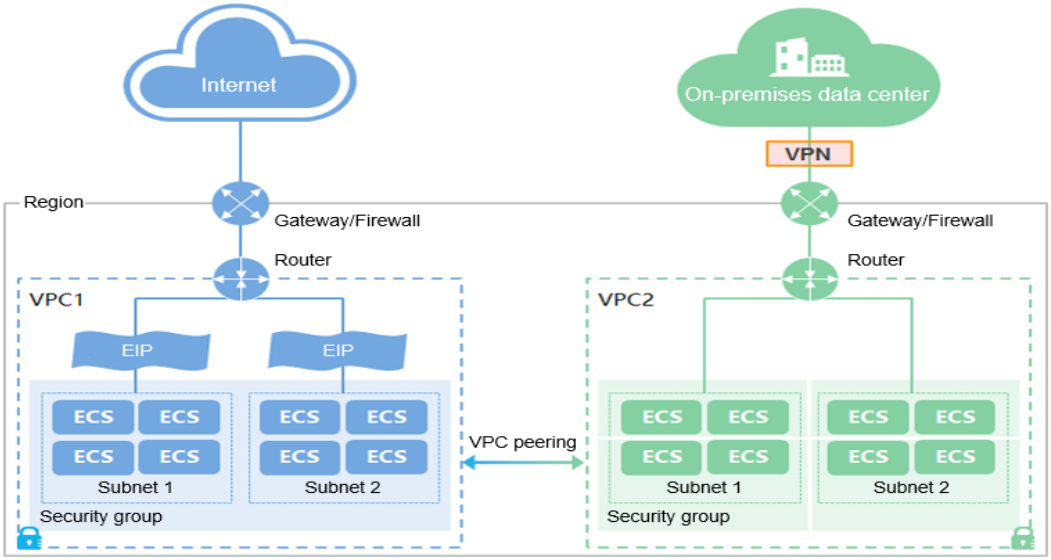
3.2.2.5 安全防护

Landing Zone 的安全防护主要包括：

- ✓ 虚拟网络安全
- ✓ 业务主机安全
- ✓ 业务应用安全
- ✓ 业务数据安全
- ✓ 业务安全管理

1. 虚拟网络安全

虚拟私有云服务(VPC)可以辅助租户为弹性云服务器构建隔离的、自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化业务系统的网络部署。

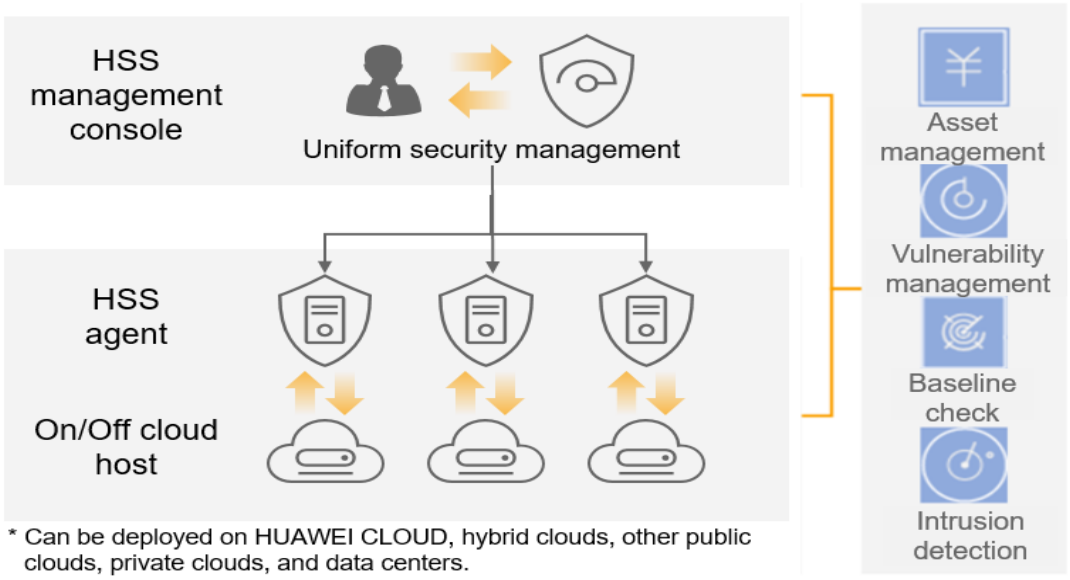


VPC 与业务网络安全强相关的网络功能：

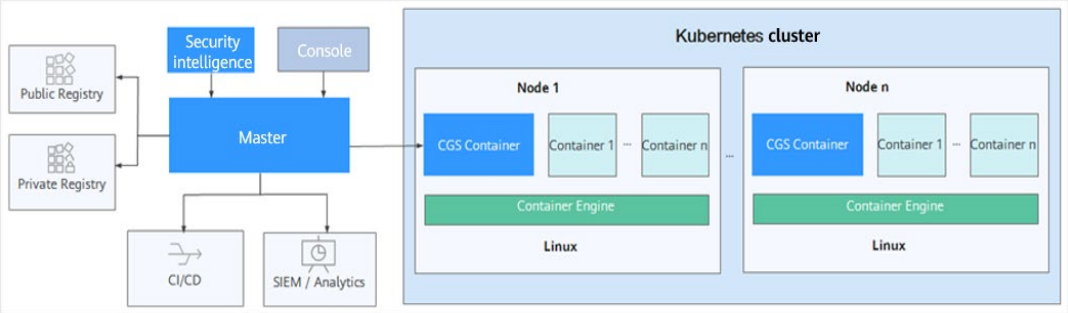
- 子网: 子网是用来管理弹性云服务器网络平面的一个网络，可提供 IP 地址管理、DNS 服务。同一个 VPC 的所有子网内的弹性云服务器默认均可以相互通信，处于不同 VPC 中的任意两台弹性云服务器默认禁止通信。
- 网络 ACL：网络 ACL 是对一个或多个子网的访问制定、维护并执行访问控制策略的系统，根据与子网关联的入站/出站规则，判断数据包是否被允许流入/流出关联子网。
- 安全组：在 VPC 中，安全组是一组对弹性云服务器的访问规则的集合，为同一个 VPC 内具有相同安全保护需求并且相互信任的弹性云服务器提供访问策略。用户可以自行创建并定义安全组内与组间弹性云服务器的访问规则，将 VPC 中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。
- VPN：VPN 用于远端用户和 VPC 之间建立一条安全加密的通信管道，使远端用户通过 VPN 直接使用 VPC 中的业务资源。默认情况下，在 VPC 中的弹性云服务器无法与用户自己的数据中心或私有网络进行通信，如需通信，租户可启用 VPN 功能，配置 VPN 相关参数。
- 云专线：云专线服务是在用户自营的内网本地数据中心与驻地云间建立连接的专线网络连接服务。用户可以利用云专线建立驻地云与用户自有数据中心、办公室或主机托管区域的专线连接，降低网络时延，获得比互联网线路更快速、更安全的网络体验

2. 业务主机安全

1）企业主机安全：企业云主机安全服务（HSS）是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营功能，可全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助用户构建服务器安全体系，降低当前服务器面临的主要安全风险。提供包括但不限于以下能力：入侵检测、文件完整性管理、异地登录监控、勒索病毒防护、统一资产管理、漏洞管理、基线检查、网页防篡改、自定义策略等。

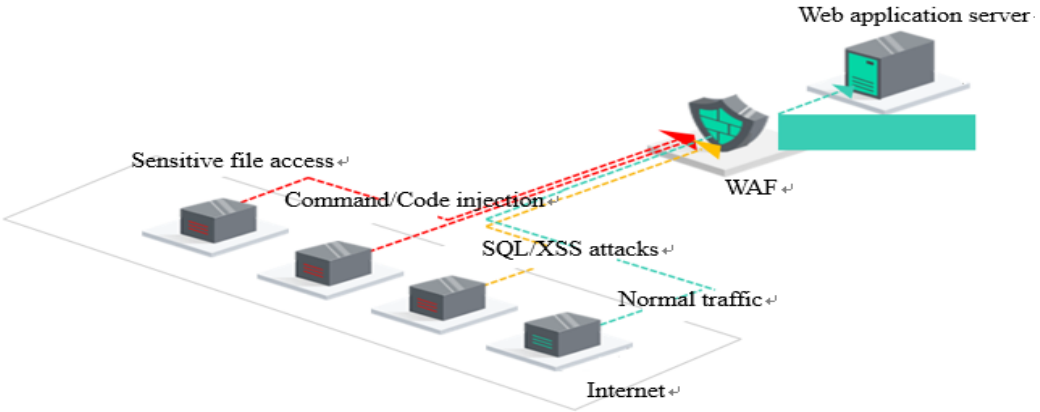


2）容器安全：容器安全服务（CGS）需能够扫描容器镜像中的漏洞，以及提供容器安全策略设置和防逃逸功能。容器安全具体应具备功能如下：漏洞管理、进程白名单、文件保护、运行监控等。



3. 业务应用安全

1） Web 应用防火墙：Web 应用防火墙可以帮助租户对网站业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御未知威胁，阻挡诸如 SQL 注入或跨站脚本等常见攻击，避免入侵攻击影响 Web 应用程序的可用性、安全性或消耗过度的资源，降低数据被篡改、失窃的风险。Web 应用防火墙包括但不限于以下能力：HTTPS 防护、IP 黑白名单设置、地理位置封禁、常见 Web 攻击拦截、攻击惩罚、精准访问自定义规则、CC 攻击缓解、0Day 漏洞虚拟补丁、动态防爬虫、告警通知等。



2）DDoS 高防服务：DDoS 高防是部署在云业务网络边界的，能够针对互联网服务器（包括非云上主机）在遭受大流量 DDoS 攻击后导致服务不可用的情况下推出的付费增值服务，用户可以通过配置高防 IP，将攻击流量引流到高防 IP 清洗，确保源站业务稳定可靠。DDoS 高防包含如下功能特性如下：网络型攻击防护、Web 应用攻击防护、支持地理位置过滤、支持流量转发负载均衡等。

4. 业务数据安全

1）数据加密服务：数据加密服务是一个综合的云上数据加密服务，公有云的数据加密服务已与多种云服务集成，如云硬盘服务、对象存储服务、文件存储服务等。用户也可以借此服务对外开放的 API 开发自己的加密应用。

数据加密的密钥分为数据加密密钥、用户主密钥和根密钥。依赖关系如下图所示：

数据加密密钥由用户主密钥加密保护，用户主密钥由根密钥保护。根密钥对用户和云服务提供商都不可见，由第三方硬件初始化时产生。根密钥的初始化由硬件 UKey 来进行。

数据加密服务应具有以下特点：

- 服务集成广泛：与对象存储、云硬盘、镜像服务、文件服务等服务集成，用户可以通过数据加密平台管理这些服务的密钥，线下用户还可以通过数据加密平台对外开放 API 完成本地数据的加密。
- 登录安全增强：用户可以通过管理控制台创建或者导入密钥对，在创建弹性云服务器时，选择通过密钥对方式登录，避免用户名密码方式口令可能被破解的隐患。

2）数据库安全服务：

通过对数据库安全服务进行安全防护配置操作，具体数据库安全审计的特性如下：SQL 注入攻击检测、风险操作管理、数据库审计等。

5. 业务安全管理

1）身份与访问管理：IAM 是可以按层次和细粒度授权，保证同一企业租户的不同用户在使用云资源上得到有效管控，避免单个用户误操作等原因导致整个云服务的不可用，确保租户业务的持续性。具备策略如：密码策略、登录策略、ACL、多因子认证（MFA）、权限管理等。

2）云堡垒机：云堡垒机提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。

3.2.2.6 合规审计

Landing Zone 要确保企业上云后的运行环境符合国家、行业和企业自身的安全合规要求，提供以下主要的安全合规措施：

1) SOD（Separation of Duty）：通过多账号架构实现 SOD，一个账号就是一个 SOD 单元，企业可以按照业务单元、地理单元、功能单元等维度划分账号，任何单一账号的崩溃不会影响全局系统，减少爆炸半径。
2) 操作审计：为每个账号开启操作审计，记录任何主体对资源访问的日志，也就是确保所有的操作都留下痕迹，同时将所有账号的审计日志进行集中存储和分析。
3) 配置变化跟踪：为每个账号开启资源配置记录功能，记录资源配置的变更日志，确保资源的所有变化都有迹可循，同时将变更日志进行集中存储和分析。
4) 安全护栏：安全护栏有两类，一类是安全红线，设定子账号不能做什么事情，相当于强制限定子账号的权限，避免子账号权限过大带来的安全风险，在设置安全红线时可以采用上文中的细粒度授权，安全红线也叫做预防性安全护栏；另一类是安全基线，要求子账号满足基本的安全合规要求，如根用户要启用 MFA，云硬盘要加密等，安全基线也叫做检测性安全护栏。完整的安全基线请参考华为云官网文档：
   中文：https://support.huaweicloud.com/usermanual-sa/sa_01_0021.html
   英文：https://support.huaweicloud.com/intl/en-us/usermanual-sa/sa_01_0021.html
5) 统一身份权限管理：统一管理多账号环境下的用户、用户组和权限，使得一个用户即可访问多个账号下的资源，统一身份权限管理可以减少权限管理的工作量，也有利于在企业范围内制定和实施统一的权限标准，避免权限设置不当造成的安全风险。
6) 统一安全管控：统一检测、处理和分析多账号环境下的安全事件、安全风险，并统一进行事件处理和响应，统一安全管控可以减少安全管控的工作量，也有利于在企业范围内制定和实施统一的安全规范。该功能的实现要求安全云服务具备多账号的统一安全管控能力。

3.3 云上架构设计

3.3.1 架构设计目的和原则

架构设计最重要的目的是能保证企业业务在发展过程中系统的持续可用，主要包括应用架构设计和技术架构设计；应用架构设计与行业特征、技术栈和企业发展阶段强相关，而技术架构设计更具备通用性，所以接下来我们将围绕云上技术架构中影响业务持续性最重要五个维度来展开介绍，包括高可用性、可扩展性、性能、安全和成本。

- 高可用性：单 AZ 可用性、跨 AZ 容灾和多活、异地灾备部署（两地三中心）等；
- 可扩展性：水平扩展、垂直扩展；
- 性能：性能规划方案、度量、检测和权衡等；
- 安全性：包括网络安全、数据安全、主机安全、应用安全等；
- 成本：成本设计、成本优化、成本管理等。

3.3.2 高可用架构设计

3.3.2.1 可用性定义

可用性(Availability)是产品/服务在规定的条件下和规定的时刻或时间区间内处于可执行规定功能状态的能力，是产品可靠性和可维护性的综合反映。服务可用性一般会用 SLA（Service-Level Agreement）来衡量，各类云服务都有承诺的 SLA 标准。不同 SLA 级别对应的停机时间如下表所示：

SLA	每周故障时间	每月故障时间	每年故障时间
99%	1.68 小时	7.2 小时	3.65 天
99.90%	10.1 分钟	43.2 分钟	8.76 小时
99.95%	5 分钟	21.6 分钟	4.38 小时
99.99%	1.01 分钟	4.32 分钟	52.56 分钟
100.00%	6 秒	25.9 秒	5.26 分钟

3.3.2.2 高可用方案

华为云上的绝大部分云服务都具备高可用性的方案，提供了从数据中心、硬件、数据、自助服务等多个层次的高可用性构建能力。华为云数据中心布局于全球，可以满足不同地域（Region）的资源需求，每个地域又分多个可用区（AZ），可用区之间的风火水电相互独立，可用区之间的故障相互隔离。企业可在此基础上构建如下场景的高可用体系：

- **单 AZ 高可用**：对于业务可用性要求不太高的业务，可以利用云服务主备、集群化部署模式来满足单个业务节点故障时快速恢复业务的需求，主要利用集群内节点故障自动探测和切换的方式来完成故障节点的恢复，消除业务单点，避免单点故障时业务受损。
- **双 AZ（同城）高可用**：对业务可用性要求比较高的业务，可以选择同城多机房的方式部署业务，这样可以避免单机房网络、物理设备、电力等故障时导致业务整体不可用；对应到华为云上用户可以采用服务跨多可用区（AZ）模式部署，各可用区之间相互隔离，当一个可用区故障时，可将业务切换到另一个可用区，快速恢复业务。云服务产品基本都具备相关的能力，用户只需在选购时选择对应的能力即可完成部署。
- **两地三中心高可用**：对于一些特大型或者安全要求很高的商业系统，对系统的高可用性提出了更高的要求，跨 AZ 的高可用方案并不能解决该地域级别的故障，如地震、洪水等。要满足此类业务场景可选择异地机房部署业务，华为云异地灾备方案在同城容灾的基础上，可再搭建异地灾备机房，满足此类业务需求。
- **跨云高可用**：为满足企业对多云高可用的部署需求，华为云同样支持多云容灾部署的能力，企业可以选择以华为云为主站点，其他的云厂商为备站点部署业务，借助多云来满足业务的可用性。

3.3.2.3 单 AZ 高可用方案设计

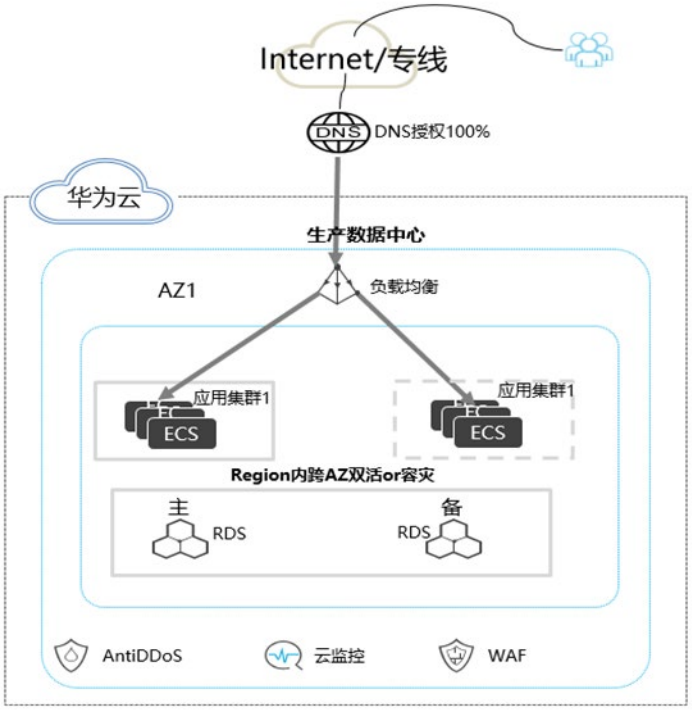
- 方案描述：
  - 业务分层部署：Web 接入层、业务层、数据层、管理区等；
  - 业务高可用：不存在单点，高可用部署（集群或主备）；
  - 云服务高可用：所选择的华为云服务为高可用部署。

从业务连续性和数据可用性的角度看，该方案实现了集群和主备级的高可用。与单节点部署相比，将应用集群或主备部署，会带来一定的成本，但可用性能力将明显得到提升。

- 高可用设计要点：

类别	高可用设计要点
业务高可用	可解耦部署：不同组件分别部署在不同的 ECS 上。 可高可用部署：全部节点高可用部署，若不能高可用(主备、集群）部署，有应急方案，如：云服务器备份 CSBS、应急环境。 可分层部署：比如：分成 Web 层、业务层、数据库层。 可弹性伸缩：结合 AS 服务自动调整弹性计算资源应对业务压力变化。

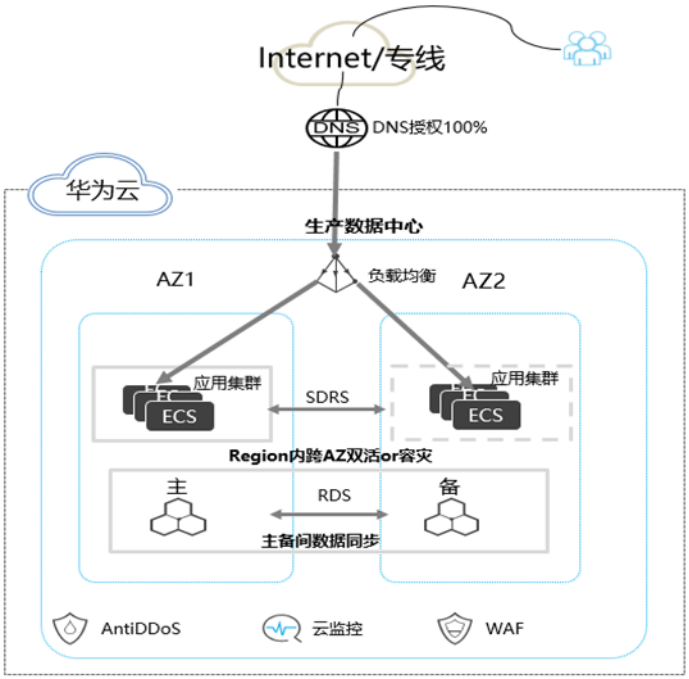
类别	高可用设计要点
云服务高可用	1、网络接入层： 1）专线：双活或者主备高可用。 2）VPN：专线主+VPN 备、VPN 主+VPN 备等热备方案。 3）ELB：后端运行多个 ECS 业务实例提供系统的可用性和可伸缩性，并开启健康检查；ELB 是系统中的潜在故障单点，需要在 CES 中重点监控。 4）NAT 网关：若有大量 ECS 需要访问外网，建议采用 SNAT 功能，避免将过多 ECS 暴露在外网。 2、云服务类型选择(RDS、DCS 等)： 至少生产业务需要采用主备或者集群部署模式，如 RDS 主备部署，Redis 集群化部署；在 ECS 上自建的服务也需要满足此要求，如选择 Redis 集群版。
数据可靠性	1、有数据可靠性备份恢复解决方案，如：采用 VBS、CSBS 备份 ECS 数据，开启 RDS 的备份策略，将关键数据备份到其他 Region or 线下 IDC 等。 2、定期验证数据备份恢复可靠性、应急演练方案等机制。



3.3.2.4 双 AZ 高可用方案设计

➢ 方案描述及设计要点：

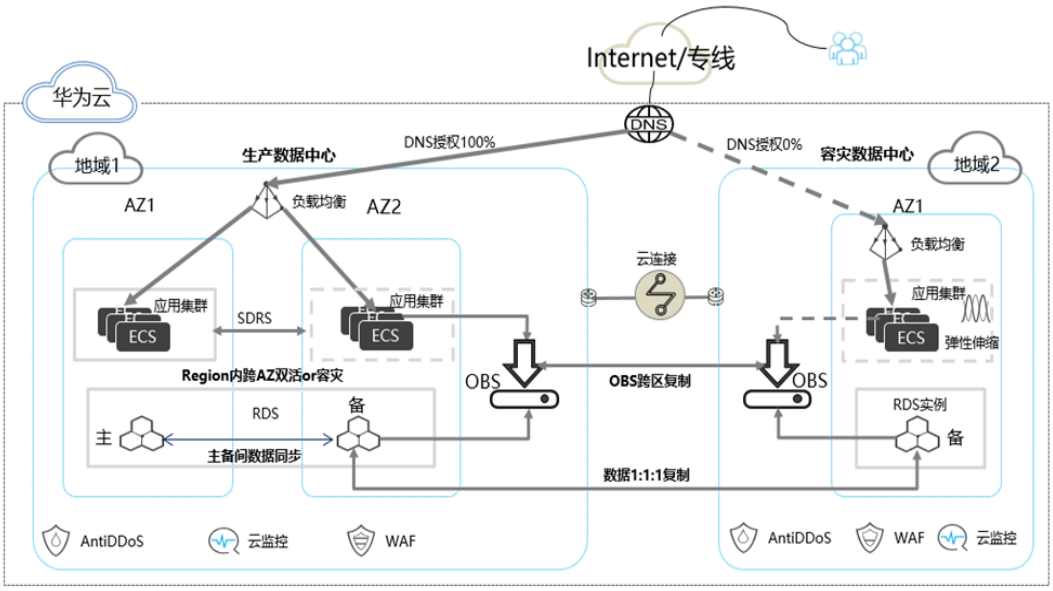
- 业务模块：集群部署的业务，资源分别部署到 2 个 AZ 内，并通过 ELB 实现双 AZ 的负载均衡；单点业务 ECS 可通过 SDRS 作 AZ 级容灾。
- 云服务高可用：主备节点分别双 AZ 部署。
- 数据库同步：云上使用 RDS 数据库服务，进行跨 AZ 主备部署，跨 AZ 间数据同步。
- 灾难恢复切换：当 AZ 发生故障时，RDS 数据库等自动切换至备库，应用层自动或者通过 SDRS 的一键容灾切换功能切换至其他 AZ。
- 容灾演练：通过应用切换或 SDRS 提供的容灾演练功能进行一键演练。



3.3.2.5 两地三中心跨 Region 高可用容灾架构设计

➢ 方案描述及设计要点：

- 生产数据中心和容灾中心分别部署在华为云 2 个不同 Region。
- 生产中心采用双 AZ 部署（双活、热备），容灾中心单 AZ。
- 在生产和容灾中心分别部署 RDS 数据库实例，数据库 1:1:1 主备复制。
- 生产和容灾中心产生的配置、日志、快照和备份等，通过 OBS 实现跨区复制。
- 生产站点某个 AZ 故障时，切换到另一个 AZ，数据库主备切换。
- 生产站点全体故障时，切换数据库的主备状态，然后将 DNS 授权修改为容灾站点（生产站点 0%，容灾站点为 100%）。
- 生产站点修复后，数据库切换回主库，DNS 切换回主站点（生产站点 100%，容灾站点为 0%）。
- 为提高容灾中心利用率，可将只读和数据分析业务放到容灾站点。



➢ 方案特点：

- 提供最高程度的业务连续性和数据可用性，在超大规模地域级自然灾害的时候都能保护数据和业务。
- RPO 时间取决于数据库复制间隔； 由于容灾站点一直运行，RTO 依赖容灾切换时间，通常取决于 DNS 缓存刷新时间，一般为分钟级，如果采用 GSLB 自动探测切换可进一步降低故障恢复时间。

高可用容灾能力构建是一个复杂的系统工程，涉及入口流量控制、业务层改造、中间件和数据库的控制，以及整体机制的协同，所以整个体系打造是存在一定门槛的；如果客户缺乏相关的经验，又期望快速构建高可用的容灾体系，可以考虑使用华为云提供的多云高可用服务（Multi-cloud high Availability Service 简称 MAS），它源自华为消费者业务多云应用高可用方案，提供从流量入口、应用层到数据层的端到端的业务故障切换及容灾演练能力，保障故障场景下的业务快速恢复，提升业务连续性。详见：MAS 介绍。

3.3.3 可扩展架构设计

3.3.3.1 云上可扩展性

云相较于传统 IDC 非常大的一个优势具备丰富的资源和强大的扩展能力；根据业务场景的不同需求，可以将扩展能力分成如下几类：

➢ 纵向（垂直）扩展：在单体应用、独立应用、有状态应用等场景下，随着业务不断发展和变化，需要快速升级硬件以应对业务变化。如在进行一些促销活动时，对资源的需求往往比正常要高出多倍，这时企业在云上就可以通过可视化界面或者 OpenAPI 快速升级资源的配置，将资源调整到更高规格的实例上（如更多的 CPU、内存、带宽、磁盘空间等），以应对活动的流量冲击；而在活动过后，又可以将规格收缩回原来的规格，达到降低成本的目的。

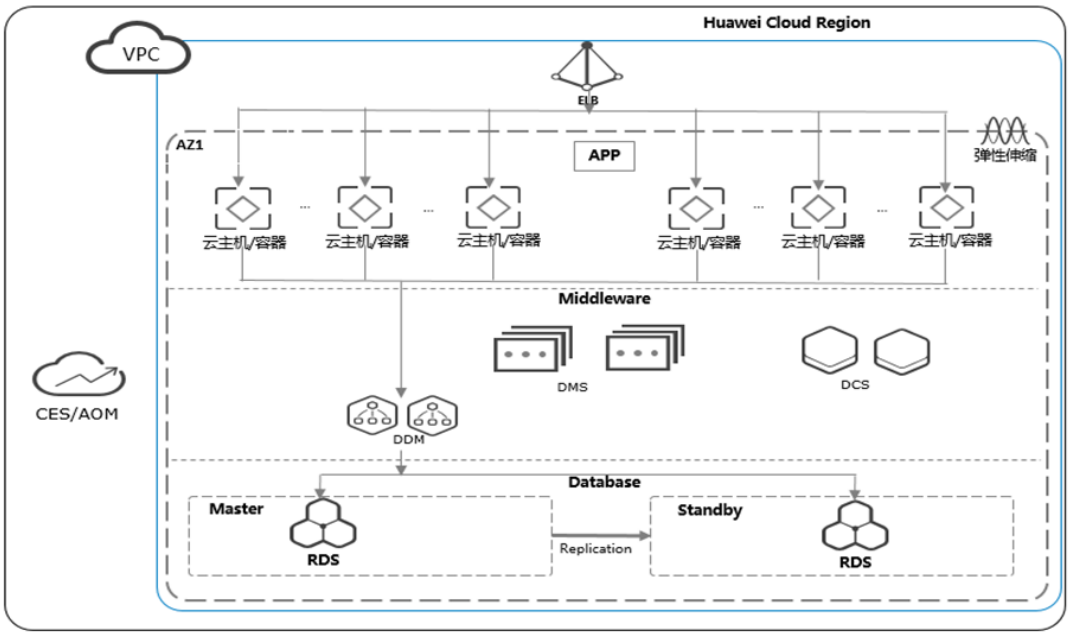
➢ 横向（水平）扩展：在分布式应用、无状态应用、快速变化的应用等场景下，固定数据的资源配比显然已经无法应对业务的快速变化，此时就可以依托于云上丰富的资源和快速的水平伸缩能力来应对。对于企业业务突增、活动促销的场景，用户可以快速通过伸缩策略来扩容和释放资源，同时在业务稳步增长的情形下，也可弹性调整以适配资源与业务。

- 极致弹性：某些业务场景可能会面临非预期的突发流量冲击，如明星绯闻事件，此时会要求系统短时间具备极致的扩容能力，如短时间扩容数千核的资源，这种对资源和系统极致的弹性场景云上是最好的选择。

云上扩缩容可支持如下策略：

- 定时模式：创建定时任务，在指定时间执行资源扩缩容。
- 指标模式：基于资源的性能指标（如 CPU 利用率、网络流量均值）创建报警任务，当指标数据满足指定的报警条件时，触发报警并执行资源扩缩容。
- 固定数量模式：设置最小/最大期望资源数量，当实例数量低于下限/超过上限时，系统会自动添加/移出资源，使得资源数量等于下限/上限。
- 手动模式：手动进行弹性伸缩，包括手动添加、移出或者删除已有的资源。

3.3.3.2 可扩展方案设计



可扩展能力可分层来设计，上图展示了华为云各层级的产品扩展能力全貌。下面来看下各层可扩展方案设计。

1) APP 层：若 APP 层实现了微服务架构，通过华为云 CCE 云容器引擎服务实现业务容器化部署，可通过 CCE 工作负载弹性伸缩能力实现 APP 业务的水平扩展，随着负载增加，APP 业务 POD 能自动扩展，随着负载的降低，APP 业务 POD 自动减容，支持配套应用性能监控（AOM）实现告警策略自动触发扩容或减容；若 APP 层使用 ECS 进行部署，则可通过华为云弹性伸缩服务 AS，设置对应的伸缩策略，随业务实现水平扩缩容。

2) 消息中间件层：华为云 DMS RabbitMQ 专享版底层是集群环境，随着消息处理量和负载的增加，可以平滑的扩大规格。

3) 缓存中间件层：华为云 DCS Redis 主备版随着热数据容量增加可无缝支撑缓存的平滑扩容节点规格。

4) 数据库中间件层：分布式数据库中间件采用华为云 DDM，DDM 本身集群部署，随着数据库业务增加，可平滑扩容 DDM 集群的规格，应对更大量的数据库处理。

5) 数据库层：华为云 RDS 数据库可平滑扩展只读数据库的实例，应对大量数据读的场景；配套 DDM 实现多套实例水平扩容，将大表的数据做水平拆分，均匀拆分到多个数据库实例中，从而提升数据库的容量和性能。此外华为云自研 GaussDB 数据库采用存算分离架构，支持分钟级的横向扩展能力，减少业务中断时间。

3.3.4 性能架构设计

作为软件系统非常重要的一项指标，性能不避免的成为架构设计中非常重要的一环。上一小节介绍了可扩展性设计，性能设计要考虑很重要的一点就是扩展性，可以说可扩展性是高性能的必要条件，除此之外，我们还要考虑以下几个方面的内容：方案的选择、性能度量、性能监测和性能权衡。

我们来了解一下影响云上应用性能的主要因素包括以下几个方面：

- 针对计算资源，延时是操作执行之间所花的等待时间，也是云计算性能的最直接表现；
- 针对网络资源，吞吐量是评价数据处理执行的速率；
- 在数据传输方面，用字节/秒或者比特/秒来表示，吞吐量的限制是性能瓶颈的一种重要表现形式；
- 针对存储资源，IOPS 是指每秒发生的输入/输出操作的次数，是数据传输的一个度量方法；
- 针对数据库资源，并发能力是指一个时间段中有几个程序都处于运行的能力。

➢ 方案选择
- 根据不同场景选择不同的解决方法，并且结合多种方法，这样可以更容易地找到一种与需求符合的方法；
- 不断迭代的方法，使用数据驱动来优化资源类型和配置选项的选择；

➢ 性能度量
- 设置性能度量和监控指标，以捕获关键的性能指标；
- 作为部署过程的一部分，在快速运行的测试成功通过后自动触发性能测试；
- 使用可视化技术，明确出现性能问题、热点、等到状态或者利用率低的地方；

➢ 性能监测
- 确定监控范围、度量和阈值；
- 从多个维度创建完整视图；

➢ 性能权衡
- 在架构中进行折衷以提高性能，例如使用压缩或者缓存技术等。

3.3.5 安全架构设计

云上客户的主要安全述求有三类：

- 业务连续不中断：防网络攻击、防黑客入侵、法律遵从合规等；
- 数据保密不扩散：防外部获取、非授权员工不可见、云服务商不可见等；
- 运维全程可管理：配置安全策略、风险识别处置、操作可审计可追溯等。

安全架构主要从区域边界，网络通信、计算环境和管理中心这四个角度进行构建。

➢ 区域边界
- 边界防护：受控连接、防私接、防非法外联、限制无线网络；
- 访问控制：网络访问控制策略的配置；
- 入侵防范：已知威胁防护、未知威胁防护、审计；

- 恶意代码防范：恶意代码检测、垃圾邮件过滤；
- 安全审计：用户行为审计、安全事件审计与分析。

➢ 网络通信

- 网络架构：性能冗余、链路冗余、设备冗余、分区隔离；
- 通信传输：采用密码技术保证传输过程中的数据保密性和完整性。

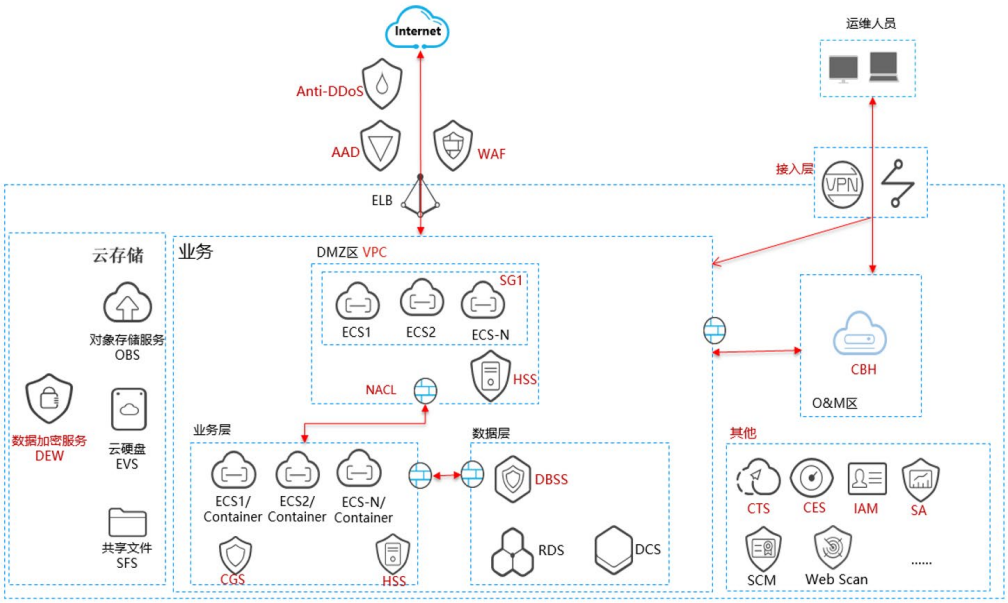
➢ 计算环境

- 身份鉴别：身份唯一性、鉴别信息复杂度；
- 访问控制：用户权限管理、冗余账号清除；
- 安全审计：用户行为审计及审计记录、审计进程的保护；
- 入侵防范：检测入侵行为、非使用端口关闭、漏扫检测；
- 恶意代码防范：恶意代码攻击识别与阻断；
- 镜像和快照保护：镜像完整性检测和快照保护；
- 数据完整性和保密性：保障重要数据在传输和存储过程中的完整性和保密性；
- 剩余信息保护：删除业务应用数据时，云存储中所有副本删除。

➢ 管理中心

- 系统管理：系统管理员的身份鉴别与系统配置；
- 审计管理：权限管理、操作审计；
- 安全管理：权限管理、操作审计；
- 集中管控：安全独立分区、网络监控、集中日志审计、安全事项感知等。

下图是云上安全架构全景图，详情可见 3.2.2.5 安全防护章节内容。



说明：

- AAD&Anti-DDoS：高防&流量清洗；
- WAF：应用防火墙；
- SG/NACL：安全组/网络防火墙；
- HSS/CGS：企业主机安全/容器安全服务；
- DBSS：数据库安全；
- DEW：数据加密服务；
- CBH：云堡垒机；
- CTS/CES/IAM/SA：云审计/云监控/统一身份认证/态势感知。

3.3.6 成本优化设计

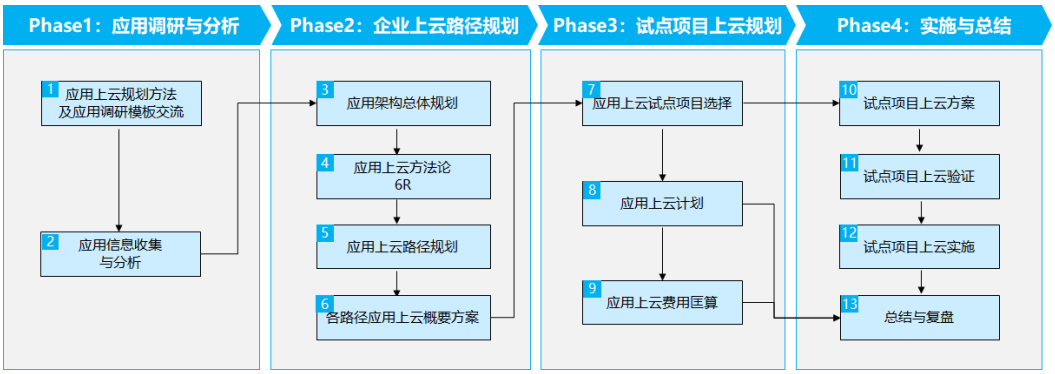
云上资源按需使用、按量计费、弹性伸缩，资源的合理使用决定了成本支出的大小，下图

是云上成本优化设计的大原则参考，详细设计内容参见 6.3 章节的成本管理。

4 云上运行

4.1 应用上云

华为云基于华为自身的成功实践和服务海量客户的经验，总结出来 4Phase 的应用上云步骤，以指导企业应用上云的规划与实施。4Phase 详细信息如下：



- Phase1：应用调研与分析。需要基于支持业务的各类应用开展调研工作，梳理清楚应用本身的功能、技术栈、部署形态、业务 SLA、应用与周边应用的集成关系、应用的来源、运维模式等等。

需要调研的内容包括但不限于如下内容：

- 应用架构调研；
- 包括应用包含的模块，以及模块与模块之间的依赖关系，应用与应用之间的外部依赖关系等；应用开发语言及框架；
- 主机信息调研；
- 包括主机配置规格、操作系统及版本、数据总量、网卡数量、高可用部署情况、容灾备份需求等；
- 数据库信息调研；
- 包括数据库类型、版本、数据量、性能以及高可用要求等；
- 中间件信息调研；
- 中间件类型（如消息中间件、缓存数据库）、版本、集群规模及容量。

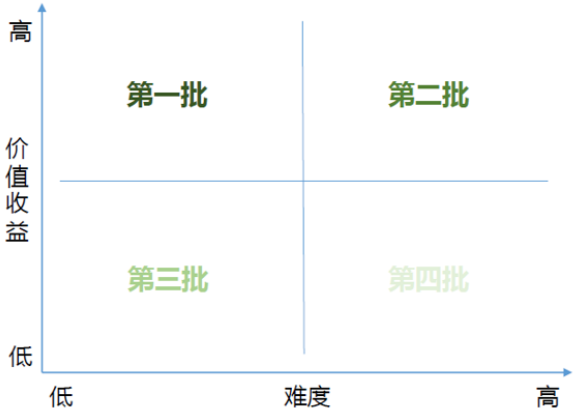
- Phase2：企业上云路径规划，在完成应用现状分析的基础上，基于 6R 方法论，结合应用上云的总体原则、应用上云难易程度与上云收益分析，对应用进行评估，给出应用上云的路径建议。

- 应用上云总体原则：

- ✓ 已通过采购第三方 SAAS 应用实现的业务，如果无显著痛点，保留当前 SAAS 应用不变；
- ✓ 对于基于主机部署的外购软件，采用 Rehost 或 Replatform 策略上云；
- ✓ 对于暂不具备上云条件业务，比如操作系统不兼容，外购件架构老旧且难以获取原厂支持，上云收益不明显的业务，保持 Retain 策略，不上云；
- ✓ 对于自研应用，根据客户技术栈需求可选用 Rehost、Replatform 或 Rearchitect 方式上云；
- ✓ 数据库、中间件一类组件，如果云上有匹配的云服务，建议采用 Replatform 方式上云，可实现资源按需获取，并降低运维技术难度与成本。

- 应用上云批次规划

根据应用上云带来的收益，以及应用上云的难易程度来评估应用上云的批次顺序。 上云难度低，而且收益高的应用优先上云；上云难度高，而收益低的应用可以考虑放在靠后批次上云，或者不上云。



对于价值收益的考量点包括但不限于：

- 对业务的提速、增效、降成本；
- 业务需求多变；
- 体验要求提升；
- 架构问题严重；
- 有资源弹性收缩需求；
- 审计合规。

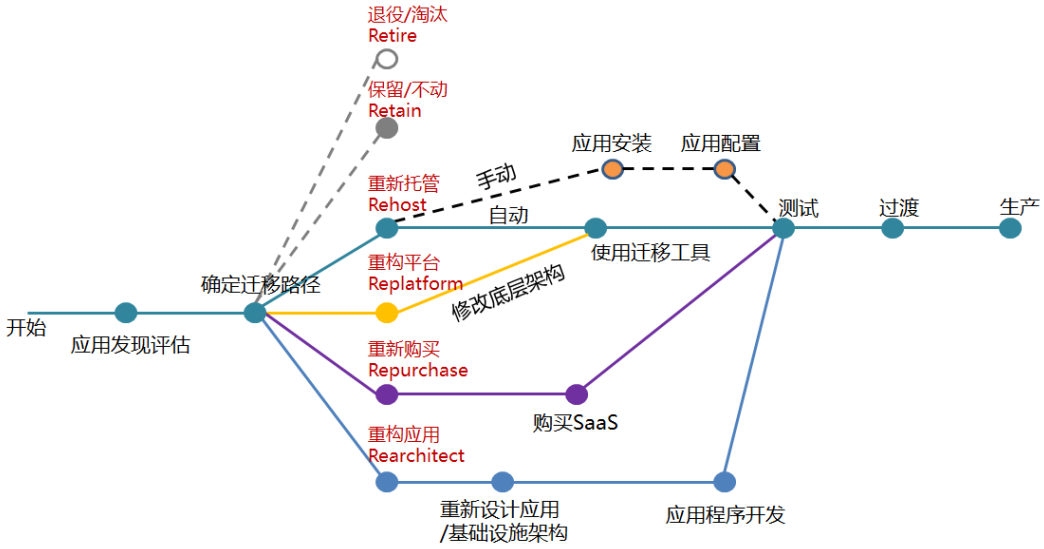
对于上云难度的考量点包括但不限于：

- 业务复杂度；
- 业务和 IT 设计的成熟度；
- 依赖关系；
- 组织和能力。

➢ Phase3：试点项目上云规划，在完成企业总体应用上云路径规划的基础上，选取试点项目，准备试点项目上云的实施计划，并预估试点项目上云所需的投入成本。已达成通过试点项目梳理云上应用架构，上云流程，并获得成功的上云经验，以支撑后续全面上云的目的。

➢ Phase4：实施与总结。在获得项目规划和预算的基础上，开展试点项目的上云工作，达到对上云过程中企业关注的技术、组织、流程、人才、成本等各方面的验证，该阶段的项目总结非常重要。通过不断的实践和总结才能获得与企业适配的成功经验，让企业在后续全面上云中获得更好的收益，提升企业上云的信心。

根据 6R 方法论，应用上云迁移有如下路径：



下面我们聚焦于 Rehost、Replatform、Rearchitect 场景的上云方案与上云迁移实施介绍。

4.1.1 Rehost 上云

Rehost 重新托管，也称为 “直接迁移”。这个是应用进行云迁移时最常见的策略，即对应用程序运行环境不做改变的情况下迁移上云， 一般的操作是 P2V（Physical to Virtual，物理机迁移至虚拟机）、V2V（Virtual to Virtual，虚拟机迁移至虚拟机）。在企业期望快速上云或单体类应用上云的场景中，这种策略比较合适。适用于企业的 SAP、ERP、CRM 等传统 IT 应用。

Rehost 上云有如下三种方案：

- **应用重新部署**

云上云主机环境（ECS/BMS），上传应用软件包的方式并重新安装部署应用。适用于无状态应用，无需数据的迁移。优点是云端主机操作系统可变（譬如操作系统过于老旧，OS 厂家已不提供技术支持，云上可切换为最新版本的操作系统），缺点是停机时间长。需要升级 OS 时，推荐采用此种方式。

- **镜像导入/导出**

线下环境导出操作系统镜像，云上通过制作私有镜像方式导入镜像。适用于数据量不大，但需要迁移线下主机数据的场景。迁移过程中云上和云下的操作系统版本保持一致（即无法替换或升级操作系统版本），停机时间长。

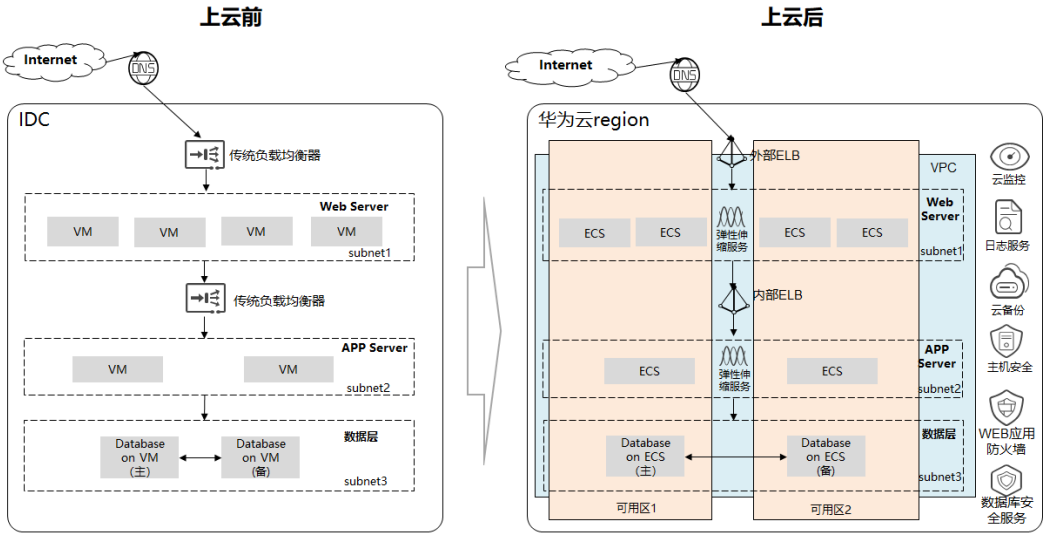
- **SMS 迁移工具迁移**

通过 SMS 工具迁移应用上云，可实现云下云上的数据同步，停机时间短。无法实现迁移过程中 OS 的升级。

主机	迁移方式	适用场景

虚拟机/物理机迁移	重新部署	OS 可变，停机时间长
	镜像导入/导出	OS 不变，版本一致，停机时间长
	SMS 工具	OS 不变，版本一致，停机时间短

以一个典型的 WEB/APP/数据库的三层架构应用为例，企业上云前与 Rehost 上云后的架构对比如下：



通过 Rehost 上云，企业获得收益如下：

- 云上应用架构与线下保持一致，技术栈一致，确保应用可平滑上云；
- 基于华为云弹性云主机（ECS）服务自建数据库，商用数据库场景可利旧数据库 license，节约成本；
- 应用跨可用区部署，支持数据中心级别高可用；
- 结合华为云弹性负载均衡（ELB）服务和弹性伸缩（AS）服务，支持业务按负载进行灵活弹性伸缩；
- 通过弹性负载均衡服务（ELB）替代线下传统硬件负载均衡设备，Network ACL 替代传统硬件防火墙，进一步降低硬件投资成本；
- 简化企业运维：结合华为云云监控服务（CES），提供云上基础设施的全方位运维监控，结合华为云日志服务（LTS），提供对应用日志快速采集与分析的能力。
- 提升应用可靠性：结合云备份服务（CBR），提供对云上主机和数据库服务器的备份。
- 加固企业应用：主机安全服务（HSS）提供对云上主机的保驾护航，WEB 应用防火墙（WAF）提供 WEB 应用流量的安全过滤，数据库安全服务（DBSS）对云上数据库进行安全加固。

4.1.2 Replatform 上云方案

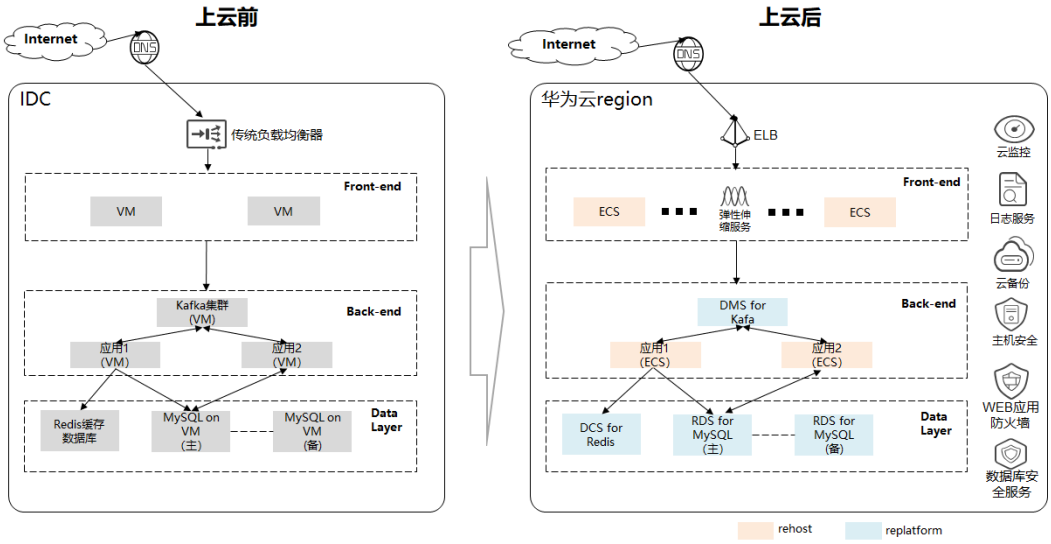
4.1.2.1 Replatform 上云方案介绍

Replatform 被称为“应用平台更换”，指在迁移上云时，在不改变应用核心架构的基础上，对应用使用到的平台组件（譬如数据库、中间件等）替换为华为云提供的托管式平台服务。例如将关系型数据库替换成华为云提供的云数据库服务，将自建消息中间件替换成华为云提供的消息队列服务，讲自建的缓存数据库替换为华为云提供的缓存数据库服务，以此来降低部分管理成本，提升效率，同时可以支持灵活的伸缩。

华为云支持企业自建或第三方云平台的数据库和中间件迁移上华为云，并提供相应的迁移方案如下：

迁移对象	对象类型	源平台	目标平台	迁移方式	适用场景
数据库	SQL SERVER	自建/DBaaS	华为云 RDS for SQL SERVER	华为云数据复制服务（DRS）	目标端是 RDS，停机时间~分钟级
	MySQL		华为云 RDS for MySQL	华为云数据复制服务（DRS）	目标端是 RDS，停机时间~分钟级
	PostgreSQL		华为云 RDS for PostgreSQL	华为云数据复制服务（DRS）	目标端是 RDS，停机时间~分钟级
	MongoDB		华为云文档数据库服务（DDS）	华为云数据复制服务（DRS）	目标端是 RDS，停机时间~分钟级
中间件	Redis	自建/云服务	华为云分布式缓存服务（DCS for Redis）	DCS-迁移	目标端是 DCS
		自建/云服务	华为云分布式缓存服务（DCS for Redis）	Redis-port	离线导出导入
	Kafka	自建	华为云分布式消息服务（DMS for kafka）	mirrorMaker	只能同步 Kafka 中的集群数据，无法同步消费组及消费进度

以如下典型架构场景为例，企业使用 Kafka 消息中间件实现前后端应用性能不一致屏蔽和应用间解耦，使用 Redis 缓存数据库实现热点数据缓存，使用 MySQL 数据库实现核心业务数据的存储。传统 IDC 线下部署场景，企业需自建中间件和数据库，自行实现中间件、数据库的高可用部署以及备份恢复方案，并对相应组件进行维护，面临着部署效率低，运维成本高，扩容难等问题。



通过业务上云，华为云可帮助企业实现中间件、数据库组件在公有云环境的 Replatform 部署，以云服务化的方式，帮助客户简化中间件、数据库的部署和运维：

- 分钟级的实例发放，按需获取中间件和数据库服务；
- 云服务方式提供高可用实例（如支持 MySQL 主备实例，kafka/redis 集群实例等），支持跨 AZ 部署，提供数据中心级别的高可用性；
- 云上多种中间件（消息中间件、缓存数据库）、数据库实例规格按需使用，支持云中间件服务和云数据库服务的一键式扩容，降低起步成本；
- 云中间件服务（消息中间件、缓存数据库）和云数据库服务免运维，降低运维难度和成本。

4.1.3 Rearchitect 上云方案

Rearchitect 被称为“应用重构”，指改变应用的架构和开发模式，进行云原生的应用服务实现。例如，单体应用向微服务架构改造，这种策略一般是在现有应用环境下难以满足日后功能、性能或规模上的需求时采用，该策略的迁移成本比较高，但是长远来看会更为满足未来的扩展需求。应用重构中的微服务拆分过程需要业务人员深度参与。

4.1.3.1 传统应用架构问题

传统单体应用架构常见问题包括但不限于：

➢ 资源使用率低，部署运维复杂
- 系统粒度粗，调度复杂，弹性能力差；
- 缺乏系统性的应用标准化措施，存在雪花服务器（因环境或组件升级导致的脆弱、难以被复制的服务器问题）；
- 缺乏统一、完善的应用状态监测和运维措施，运维需要负责底层基础设施的稳定性。

➢ 应用架构复杂
- 单体应用功能模块多，架构复杂；
- 应用状态内置，扩展复杂。

➢ 应用迭代周期长
- 开发复杂，开发者需要关注架构的所有细节（限流、熔断、降级等服务治理，数据访问及消息通信）；
- 使用命令式 API，开发需要关注执行过程细节；
- 没有自动化测试，无法快速发布应用；

- 单体应用复杂度高，应用迭代发布周期慢，无法支撑业务快速发展的需求。

4.1.3.2 云原生应用架构

CNCF（Cloud Native Computing Foundation 云原生计算基金会）对云原生的定义：云原生技术有利于各组织在公有云、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。云原生的代表技术包括容器、服务网格、微服务、不可变基础设施和声明式 API。

云原生应用架构建议：

➢ 微服务的架构系统

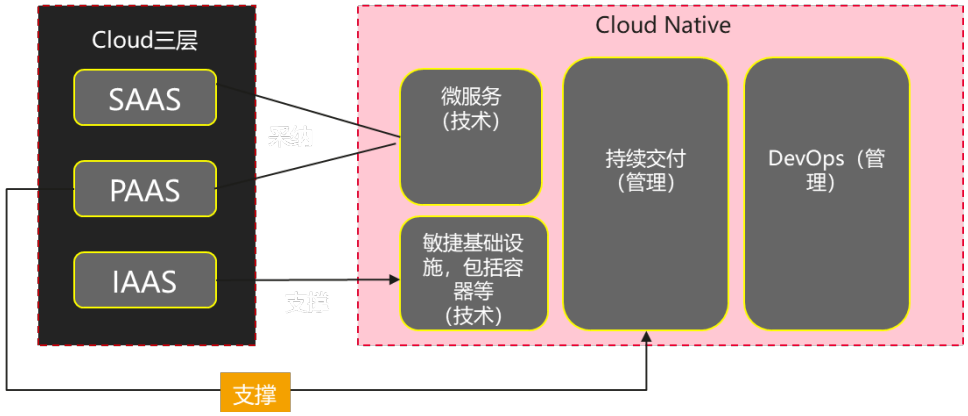
微服务是将应用作为小型服务集合进行开发的架构方法，助力解决“应用架构复杂”问题。

➢ 容器为代表的敏捷的基础设施

容器推动了微服务架构设计理念的落地，助力解决“资源使用率低”问题。

➢ DevOps 的实践模式

容器提升了软件开发和系统运维的效率，促进了 DevOps 体系的成熟与发展，助力解决“应用迭代周期长”和“部署运维复杂”问题。

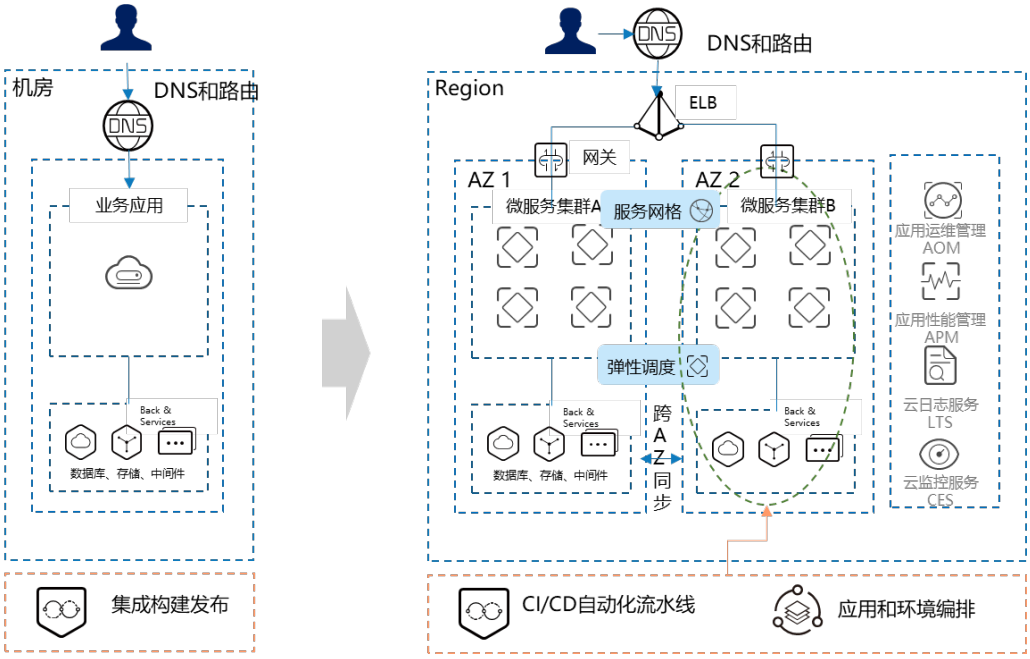


4.1.3.3 应用重构上云

应用重构上云主要包括如下三个方面：

➢ 应用微服务化改造：包括但不限于分析架构现状，要企业业务部门深度参与，根据业务能力要求划分微服务，再定义服务间接口，制定微服务改造的开发规范，进行微服务治理
➢ 应用容器化改造：包括但不限于确定容器化改造范围、分析应用依赖关系、制作容器镜像、容器编排和管理
➢ 应用 DevOps 改造：包括但不限于研发流程分析、研发工具分析、分析周边依赖、梳理差异点、云上敏捷试点、进行敏捷培训和推广

以如下典型架构场景为例，企业使用 VM 承载单体的业务应用，缺乏统一的服务治理工具和流水线平台，面临着资源使用率低、扩容难、研发效率低、上线慢、运维成本高等问题。



改造方案及客户收益如下：

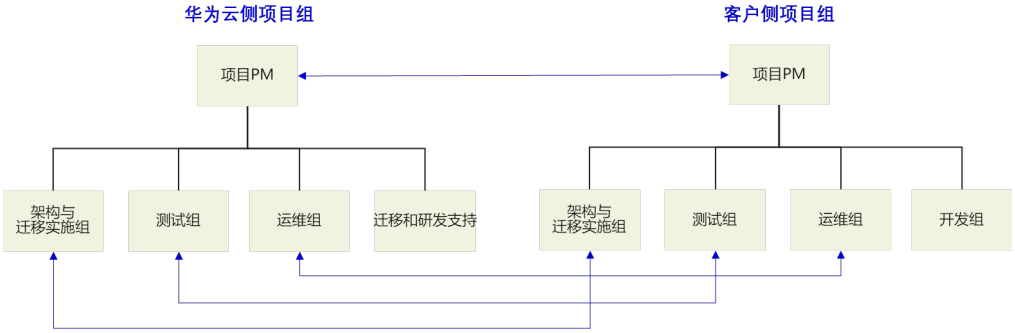
- 应用微服务化改造：单体应用根据 AKF 可扩展立方（Scalability Cube）模型、前后端分离、应用和状态分离等原则，拆分为小、独、轻、松的微服务集群，使用 Service Mesh 技术（如 Istio）进行跨编程语言的微服务治理；应用和数据库、中间件多 AZ 部署，通过弹性负载均衡分发流量，底层数据和状态保持同步，双活高可用对外提供服务；
- 应用容器化改造：应用使用容器化（Container）托管，解耦底层操作系统，快速而节约，基于 CCE（K8S）的弹性调度，不但能够自动化调度自愈，还能够根据使用情况弹性扩容缩容，确保应用资源节约，平稳行驶；
- 应用 DevOps 改造：通过自动化流水线和应用环境编排，达到秒级触发，小时级级环境就位；基于全链路技术的运维，加快日志、监控、告警等反馈效率，全方位明察秋毫；
- 自组织团队：小团队完成服务的分析、开发、测试、部署和运维，不断识别交付中的瓶颈，采用精益的方式快速验证和优化，小步快跑。

4.1.4 应用上云迁移实施

4.1.4.1 迁移团队组建

大型迁移项目往往规模大，周期短，需求多，产品多，并且涉及跨产品的复杂问题排障。因此大型迁移项目运作需要由目管理团队（PMO）来牵引，组织协调各方人员有序、高效的围绕项目目标开展相关工作。

根据华为云迁移项目经验，需要华为侧和客户侧组建项目团队，并且两个团队进行联合运作，建议迁移团队如下图所示：



- 项目 PM：组建联合项目 PMO 团队，负责项目进度、风险及问题管理，以及内部宣贯。
- 架构与迁移实施组：组建联合的架构与迁移实施组，负责上云迁移、割接等方案的设计，项目迁移实施管理和项目迁移实施，以及项目迁移实施过程中的技术风险把控。
- 测试组：组建联合的测试组，负责测试方案设计，以及项目迁移过程中的功能测试、性能测试、以及联调测试。
- 运维组：组建联合的运维组，负责云上资源的创建、管理、以及运维监控。
- 迁移和研发支持组（华为云侧）：支撑升级的技术问题。
- 开发组（客户侧）：负责应用开发、部署及应用迁移实施。

4.1.4.2 迁移实施保障机制

1) 项目开工会：启动正式的项目开工会，明确项目范围，目标，交付周期，责任分工等；
2) 项目沟通管理：建立与项目成员及项目干系人的定期沟通，暴露并解决潜在问题；
3) 项目进度管理：监控项目活动和关键任务执行，确保项目进度按照交付计划进行。当出现进度偏差，及时采取纠偏措施。并通过周报或日报的形式向项目成员及项目干系人通报。
4) 问题与风险管理：持续监控项目的假设和风险，量化风险和更新风险管理计划，确保风险应对措施执行。记录跟踪问题和风险，明确责任人和时间点。并通过周报或日报的形式向项目成员及项目干系人通报。
5) 交付矩阵：组织华为云侧和客户侧的联合项目交付矩阵。

4.1.4.3 测试与验证

在应用上云割接前，需要进行充分的功能测试和性能测试，验证应用在云上环境上运行的情况。

➢ 业务功能测试

根据应用在云上的资源清单，在华为云上开通相关资源，初始化环境配置并部署应用，最后将部分数据迁移过来进行功能联调测试。环境部署完成后客户可使用自己的测试用例对应用进行功能测试，确认业务功能运行正常。

➢ 性能测试

性能测试是一个总称，具体可细分为性能测试、负载测试、压力测试、稳定性测试。性能测试是一个不断对系统增加访问压力（在系统测试环境中，就是不断增加测试程序的并发请求数），以获得系统性能指标、最大负载能力、最大压力承受能力的过程。

性能测试可以选择华为云压测产品云性能测试服务 CPTS，支持 CPTS 测试工程和 JMeter 测试工程，或者采用第三方的压测工具。

使用 CPTS/JMeter（模拟用户流量）、tcpcopy/goreplay（录制或实时复制真实用户流量）对云上全链路应用进行压测，以验证功能和性能是否满足要求。

测试过程中结合监控系统的监控指标，例如华为云 CES、AOM、APM、和客户业务系统自有的监控系统的监控指标，以及应用日志，根据测试方案整理测试记录和输出测试报告。

压测完成后清空测试产生的脏数据，进行全量+增量的数据迁移，并择机进行业务流量割接。

4.1.4.4 业务割接与上线

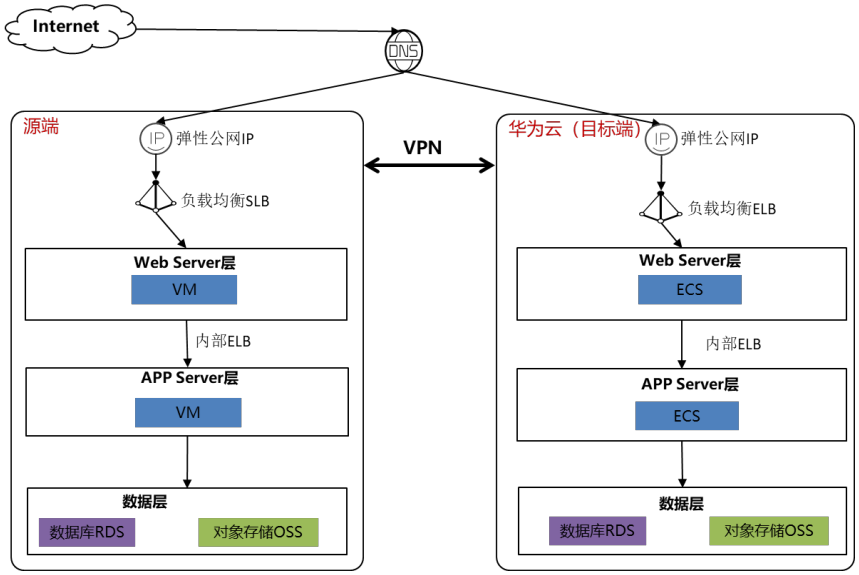
业务的割接上线是整个业务上云迁移实施的最关键环节，这一环节出问题，可能会造成重大故障。针对割接上线的重要性，需要在迁移方案中制定详细的割接前检查清单，保障业务割接的顺利执行。

在完成业务割接后，需要对割接上云的业务做好持续保障，对业务和数据做好监控，持续观察业务的运行状况，直到确认完全没有问题后，业务割接和上线工作才能结束。

正对业务割接的执行工作，华为云目标端完成数据同步、且目标端完成清除测试过程中的脏数据，即可在业务低峰期启动业务割接工作，业务割接一般分为两种方案：

- 一次性割接：针对较为简单，或者规模较小的系统，在业务充分验证的前提下一次性完成割接工作，割接工作耗时短，对客户业务影响也较小。

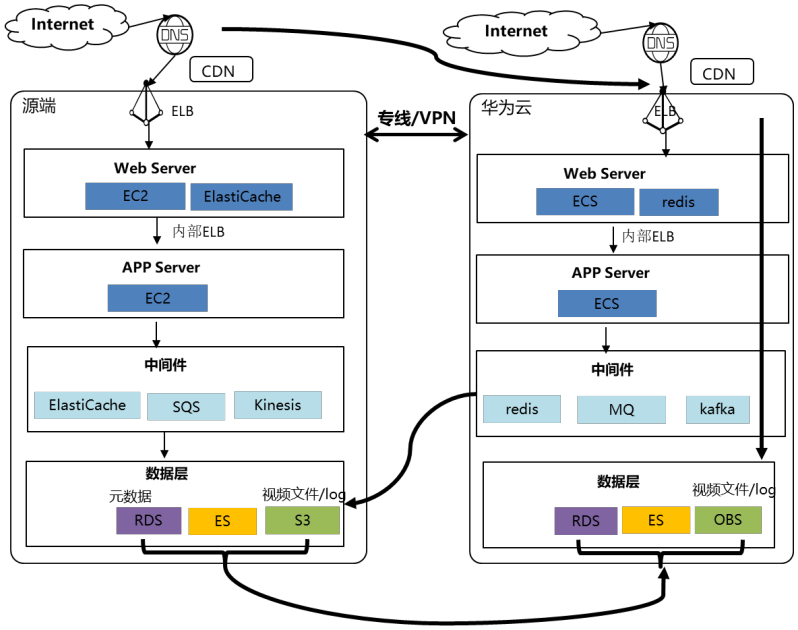
一次性割接流程如下：



1） 停止目标端测试，并且完成测试数据删除；
2） 停止源端业务（业务暂停）；
3） 完成数据增量同步；
4）（可选）配置反向数据同步，做好割接失败回退准备；
5） 修改 DNS 配置，切换 EIP，将流量切换到目标端（业务恢复）；
6） 观察目标端稳定性；
7） 持续保障。

- 分层割接：针对业务复杂，或者规模较大的系统，可以将业务分层解耦，分层割接。如果割接过程出现问题，可以分层回退，对整体服务影响小，割接风险较小。但是分层割接需要多次割接，耗时长，工作量较大。
  分层割接一般分为两步，第一步进行应用层割接，即先将应用层割接到华为云，数据库仍然读写源端。完成应用层割接后再通过数据迁移任务或应用双写将源端变化数据实时同步到华为云上数据库，完成数据增量迁移后再进行数据层割接。
  由于分层割接涉及到数据库的跨云访问，需要评估网络时延满足应用要求。

  分层割接流程如下：



  第一步：应用层割接步骤：

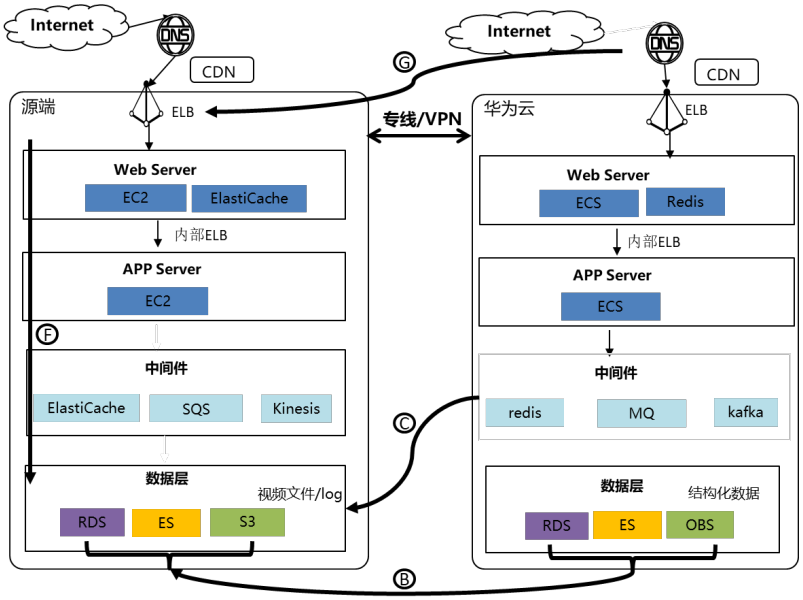
  1) 停止目标端测试，并且完成测试数据删除；
  2) 更改目标端中间件层配置，指向源端数据层（通过专线或者 VPN）；
  3) 修改 DNS 配置，切换 EIP，将流量切换到目标端；
  4) 观察目标端稳定性。

  第二步：数据库层割接步骤：

  1） 停止目标端业务（业务暂停）；
  2） 完成数据增量同步；
  3）（可选）配置反向数据同步，做好割接失败回退准备；
  4） 更改中间件层配置，指向华为云数据层；
  5） 启动目标端业务（业务恢复）；
  6） 观察目标端稳定性；
  7） 持续保障。

- 割接风险与业务回退

一次性割接场景回退方案比较简单，本章节以分层割接场景来介绍回退方案。



分层割接场景回退包含两个子场景：

- 尚未进行数据层割接：
  该阶段可以直接切换 DNS，将流量切换回源端系统。
- 已经完成数据层割接：
  1）将数据层进行回退，回退步骤如下：
    a) 停止目标端业务（业务暂停）；
    b) 完成数据反向同步；
    c) 更改目标端中间件层配置，将目标端中间件指向源端反向同步后新建的数据层；
    d) 恢复目标端业务（业务恢复）；
    e) 观察业务稳定性。
  2）要求进一步将应用层进行回退，回退步骤如下：
    a) 更改源端中间件层配置，指向源端反向同步后新建的数据层；
    b) 修改 DNS 配置，切换 EIP，将流量切换到源端；
    c) 恢复源端业务；
    d) 观察业务稳定性。

- 域名解析变更无缝割接保障方案

公网域名修改记录后，需要下发到全球各个 DNS 服务器，受限于全球基础网络，国内一般 2 小时内可以完全生效，海外一般 48 小时内完全生效。因此可能会存在部分用户访问域名会解析到原始 IP 地址，导致访问异常。

针对 DNS 解析未完全生效导致域名解析到原始 IP 的场景，可以通过在源端部署 nginx 或者 iptables，使用 nginx 的 http_proxy 或者 iptables 的 nat 功能实现流量转发，将域名记录未生效的流量转发到华为云，实现域名记录无缝切换。

以 nginx 的 http_proxy 为例，流量转发配置流程如下：

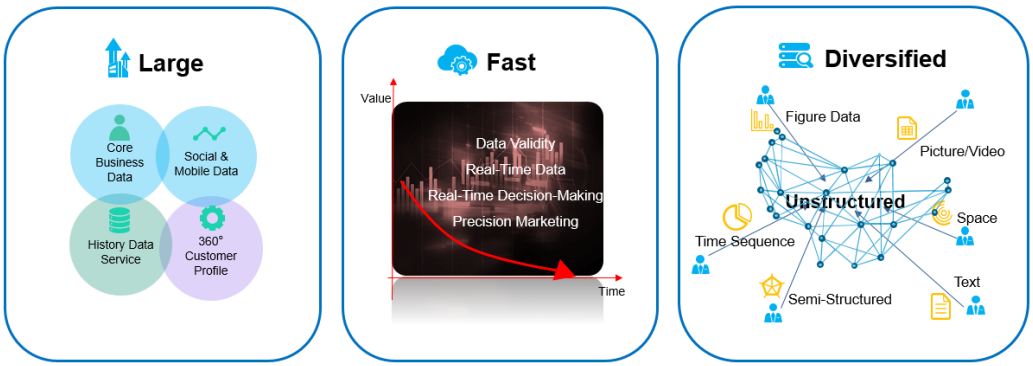
1) 割接前在客户源端部署 Nginx 反向代理集群，在负载均衡器后端部署 Nginx 转发服务器，负责将流量发送到华为云 ELB。
2) 域名切换后，迅速将源端域名 IP 绑定在负载均衡器上。

3) 负载均衡器将收到的请求转发给后端 Nginx 服务器，后端 Nginx 服务器通过公网将流量转发到华为云 ELB 公网 IP。
4) （可选）在源端 Nginx 服务器上部署流量监控软件（例如 ntop），同时查看 nginx 的 access 等日志，当网络监控显示无流量产生，access 日志无更新，说明 DNS 解析已经全部解析到华为云。
5) DNS 解析已经全部解析到华为云后，删除源端部署的负载均衡器和 Nginx 转发服务器。

4.2 数据上云

4.2.1 背景

随着移动互联网的兴起，数据出现爆炸式的增长，数据的形态（种类多样、体量巨大）和数据处理诉求（实时处理、融合分析）都发生深刻的变化。同时，企业在数字化转型过程中，烟囱式应用和数据孤岛是最大的阻碍。数据孤岛形成的原因主要来源于：1）部门之间不同的信息渠道产生的不同的数据存储格式。 2）部门通过自己业务来定义数据，数据没有形成规范理解和定义，同一份数据可能被赋予不同含义。这就使得我们在数据治理时遇到资源分散，数据不通，应用孤立等诸多挑战。



如何快速整合新增数据与历史数据，而避免信息孤岛；如何从种类繁多，不同价值密度的数据中，以更高性价比、更高效、更实时的方式，进行数据处理和分析，支撑不同业务的需求；如何将数据变成资产，甚至基于数据做创新，推动业务增长，这些都是企业最需要紧急解决的问题。

4.2.2 数据管理与分析平台的建设

4.2.2.1 业界数据湖

数据湖用来描述一种新类型的数据存储库，允许将所有结构化和非结构化数据存储在一个集中存储库中，不必首先结构化数据，并以任何规模存储。

第一代数据湖基于 Hadoop 分布式架构，其核心技术是基于开源 Apache Hadoop 生态系统，充分利用本地数据中心的通用硬件，分配和处理大量原始形式的数据。Hadoop 包含一个名为 HDFS 的文件系统，它使客户能够以其本机形式存储数据。第一代数据湖需要管理员持续关注容量规划、资源分配、性能优化等复杂任务。由于繁重的复杂度、缓慢的估价时间以及繁重的系统管理工作，许多本地数据湖项目未能实现数据湖计算的承诺。

新一代数据湖是基于云的对象存储之上而创建的。因为云提供了性能、可扩展性、可靠性、可用性、多样化的分析引擎集和巨大的规模经济，使得数据湖具有更高的性价比和扩展性。

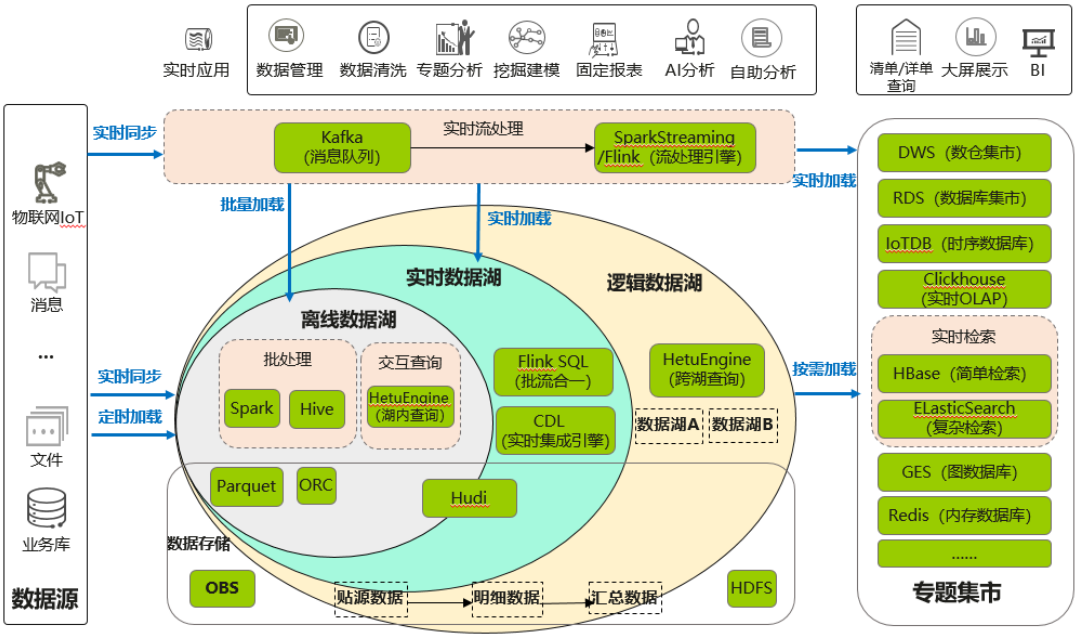
4.2.2.2 新一代数据湖建设

华为云新一代数据湖主要构建在 OBS 存储之上，而获得存算分离的优势， 计算资源和存储资源分离，单独扩缩容，避免单台节点计算、存储资源配比不均衡问题。

大数据湖小集市是企业构建数据湖的基本原则：一份数据支持多种分析，是数据湖最大的特点；数据湖是企业内多种格式数据源汇聚的大数据平台，通过严格的数据权限和资源管控，将数据和算力开放给各种使用者。

数据湖演进分三个阶段：

- 离线数据湖：数据从数据源产生后到进入到数据湖存储，无法做到实时，通常超过 15 分钟，为离线数据湖。
- 实时数据湖：数据从数据源产生后，可以实时进入到数据湖，通常 1 分钟以内，为实时，1 到 15 分钟之内，为准实时。
- 逻辑数据湖：数据无法在物理上汇聚到一个数据平台，而是若干个物理分开的数据平台形成一个虚拟数据湖，称为逻辑数据湖。



专题集市：企业内存储特定格式数据，提供给特定类型查询分析，针对特定业务场景的，为专题集市。客户对数据的分析是多种多样的，有的性能要求超高如实时 OLAP 和内存库，有的照顾存量应用如检索库，所以专题集市仍然是数据湖的重要补充。

有些场景，客户的数据只用来进行特定类型查询分析，因此专题集市可以单独存在，不依赖数据湖，此种场景过去较常见，现在已经越来越少见。专题集市方案通常会与数据湖方案配套使用。

数仓集市除具有数据仓库的基本特征以外，还具有以下特点：

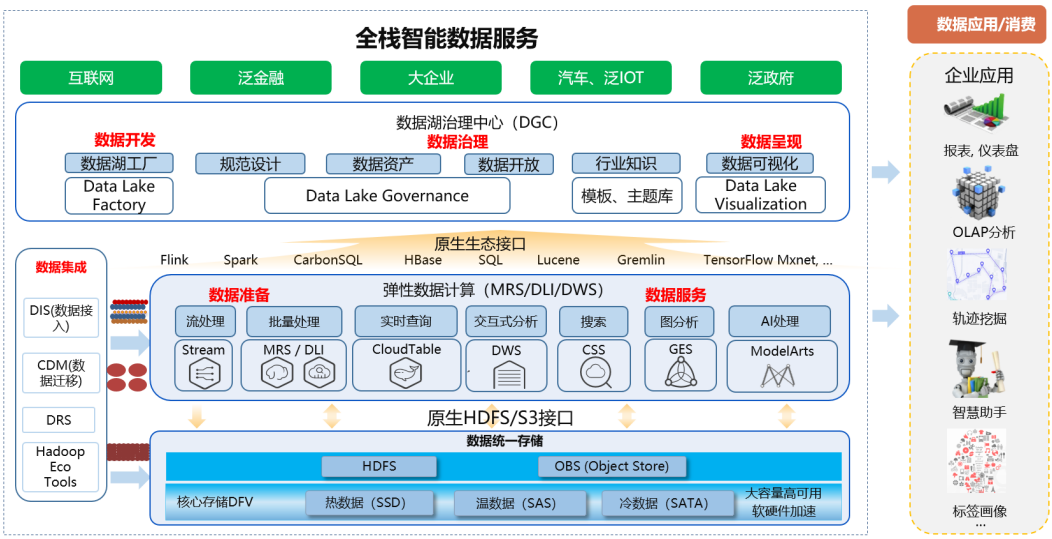
1) 规模较小，灵活，可以按照多种方式来组织，如按特定的应用、部门、地域。
2) 开发工作一般由业务部门主持定义、设计、实施、管理和维护。
3) 能够快速实现，代价较低，投资回收期短，风险小。
4) 工具集的紧密集成。

为了节省成本，建议把贴源数据和明细数据放在数据湖 OBS 里面，而把汇总数据放在数仓集市 DWS 里面。

专题集市按照使用场景也分为实时集市和离线集市。实时集市，需要数据实时加载进入集市，因此实时集市需要配合 Kafka + Flink 使用，较常见的有银行交易记录查询集市等。

4.2.2.3 华为云智能数据湖 FusionInsight Intelligent Data Lake

华为云数据管理和分析平台（FusionInsight），属于新一代数据湖，充分利用了云原生的优势，比如更快速的部署，自动弹性伸缩（Auto Scaling）， 几乎无限可扩展，高性价比存算分离，还有 Serverless 数据分析服务等等，旨在为企业提供一个高度可扩展、高可用的下一代先进的智能数据湖生态系统，帮助企业降低运维时间与成本，让企业有更多的时间和精力投入在数据分析与业务上面。



FusionInsight 提供最广泛的分析服务，适应企业所需的所有类型的数据分析场景，使各种规模和行业的组织都能用数据重塑业务。从数据采集、数据管理、数据存储、数据分析、日志分析、流分析和机器学习（ML）等全过程，华为云都提供具有最佳性价比、可扩展性的专用服务。

- 首先，是数据集成，用户想使用大数据平台做数据处理，离不开数据的接入，怎样把数据接到大数据平台呢？这里根据不同的场景提供了不同的工具，针对实时产生的数据，我们可以使用 DIS 数据接入服务，如水管一样实时引入数据；针对海量多样的离线数据，我们提供了 CDM 数据迁移服务，如同卡车一般将数据搬运到华为云；DRS 数据复制服务针对数据库的搬迁。

  DIS：数据接入服务（Data Ingestion Service，简称 DIS）可让您轻松收集、处理和分发实时流数据，以便您对新信息快速做出响应。DIS 对接多种第三方数据采集工具，提供丰富的云服务 Connector 及 Agent/SDK。适用于 IoT、互联网、媒体等行业的设备监控、实时推荐、日志分析等场景。
  https://www.huaweicloud.com/product/dis.html

CDM 和 DRS 介绍详见 4.2.4.4 大数据迁移工具章节的介绍。

- 其次，数据搬迁上云后，我们首先推荐将数据存入对象存储 OBS。如果是客户数据量不大，并且需要及时处理，客户也可以将数据存放在 HDFS。

  OBS：对象存储服务（Object Storage Service，OBS）是一个基于对象的存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力，使用时无需考虑容量限制，并且提供多种存储类型供选择，满足客户各类业务场景诉求。
  https://www.huaweicloud.com/product/obs.html

- 然后，就是核心的数据计算，根据不同场景我们提供了不同的组件，对于流处理场景，我们可以使用 Cloud stream 服务，离线批量处理可以使用 MRS 或 DLI，实时查询选择 CloudTable，交互式分析或 BI 分析时选择 DWS，搜索可以使用 CSS。

  MRS:（MapReduce Service）为客户提供 Hudi、ClickHouse、Spark、Flink、Kafka、HBase 等 Hadoop 生态的高性能大数据组件，支持数据湖、数据仓库、BI、AI 融合等能力。MRS 同时支持混合云和公有云两种形态：混合云版本，一个架构实现离线、实时、逻辑三种数据湖，以云原生架构助力客户智能升级；公有云版本，协助客户快速构建低成本、灵活开放、安全可靠的一站式大数据平台。
  https://www.huaweicloud.com/product/mrs.html

  GaussDB(DWS) 数据仓库服务（Data Warehouse Service，简称 DWS）是完全托管的企业级云上数据仓库服务，具备免运维、在线扩展、高效的多源数据加载能力，兼容 PostgreSQL 生态。助力企业经济高效地对海量数据进行在线分析，实现数据快速变现。 https://www.huaweicloud.com/product/dws.html

  DLI: 数据湖探索（Data Lake Insight，简称 DLI）是完全兼容 Apache Spark、Apache Flink、openLooKeng（基于 Presto）生态，提供一站式的流处理、批处理、交互式分析的 Serverless 融合处理分析服务。企业使用标准 SQL、Spark、Flink 程序就可轻松完成多数据源的联合计算分析，挖掘和探索数据价值.
  https://www.huaweicloud.com/product/dli.html

  CSS: 云搜索服务是一个基于 Elasticsearch 且完全托管的在线分布式搜索服务，为用户提供结构化、非结构化文本的多条件检索、统计、报表。完全兼容开源 Elasticsearch 软件原生接口。它可以帮助网站和 APP 搭建搜索框，提升用户寻找资料和视频的体验；还可以搭建日志分析平台，在运维上进行业务日志分析和监控，在运营上进行流量分析等等。https://www.huaweicloud.com/product/es.html

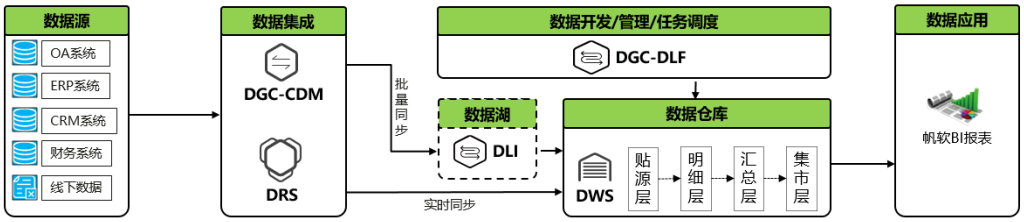
- 最后，我们会提供大数据应用开发和运营平台—数据湖治理中心 DGC，帮助用户轻松完成数据建模、脚本开发、作业调度、数据呈现、运维监控等多项任务，可以极大降低用户使用大数据的门槛，包括大数据作业开发调度和数据展现，帮助用户快速构建大数据处理中心。数据只有运营起来才能不断地给企业创造价值，增加收益。
  https://www.huaweicloud.com/product/dayu.html

我们也可以看到大数据的分析结果可以用于企业管理，包括报表分析、OLAP 分析、轨迹挖掘、用户标签等，帮助企业做更好的业务决策。

4.2.3 数据湖典型场景

4.2.3.1 数据仓库和报表分析

该场景为传统的数据仓库模式，也提供了实时数仓的能力。数据来源主要是数据库。要求数据仓库汇聚不同业务系统的数据（ERP、CRM、OA、财务、供应、线下数据等），并对数据进行汇聚、分层加工、治理、可视化，通过数据仓库的建设打通部门之间信息壁垒、连通数据孤岛，从而构建领导决策分析体系，为经营分析和决策提供数据支撑。



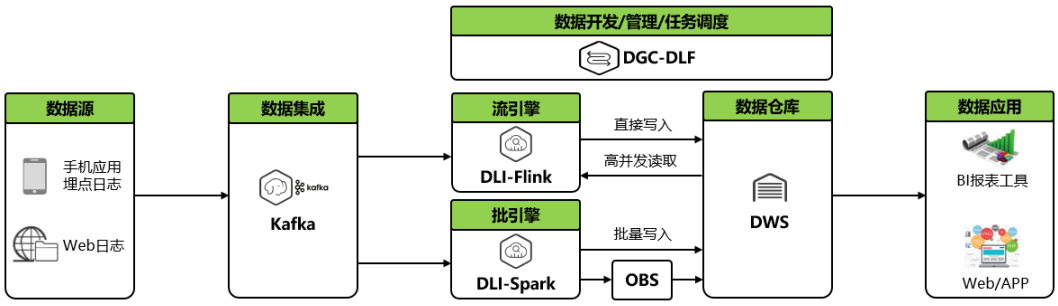
该方案以华为云数据仓库服务 DWS 为主要服务。价值主张：

- 一站式大数据 BI 平台：打通多个业务系统数据，提供全栈技术能力，为企业建立全面、精准、高效的一站式数据采集、分析和商业智能平台
- 高性价比数据分析底座：依靠华为云高性能 DWS 服务，以及配套的数据同步方案，满足海量数据分析的时效性要求，快速完成数据分析，释放数据价值。
- 高效开发、简易管理：通过 DGC 提供可视化的数据 ETL 任务开发、管理、调度能力，简单易用，灵活高效。
- 成熟、可靠的商业智能工具：与业界知名的 BI 厂商紧密合作，提供满足企业级要求的成熟可靠、灵活高效的可视化 BI 工具，大幅降低运营分析门槛，加快价值变现。

4.2.3.2 流、批、查询一体化解决方案

该场景主要应用于埋点日志处理，常用于用户行为分析、内容推荐、商品推荐等业务。埋点日志通过 Kafka 快速流入 Flink 做实时处理，而 Flink 需要的维度表存储在 DWS 中，DWS 为 Flink 实时处理提供百万 QPS 的查询能力，并且能够保存 Flink 分析后的结果数据，支撑上层业务对结果集的查询。

Spark 引擎作为批处理引擎，进行数据批量处理，加工后的报表数据存储到 DWS 中，或者 Spark 数据放在 OBS 上，DWS 以外表形式读取。



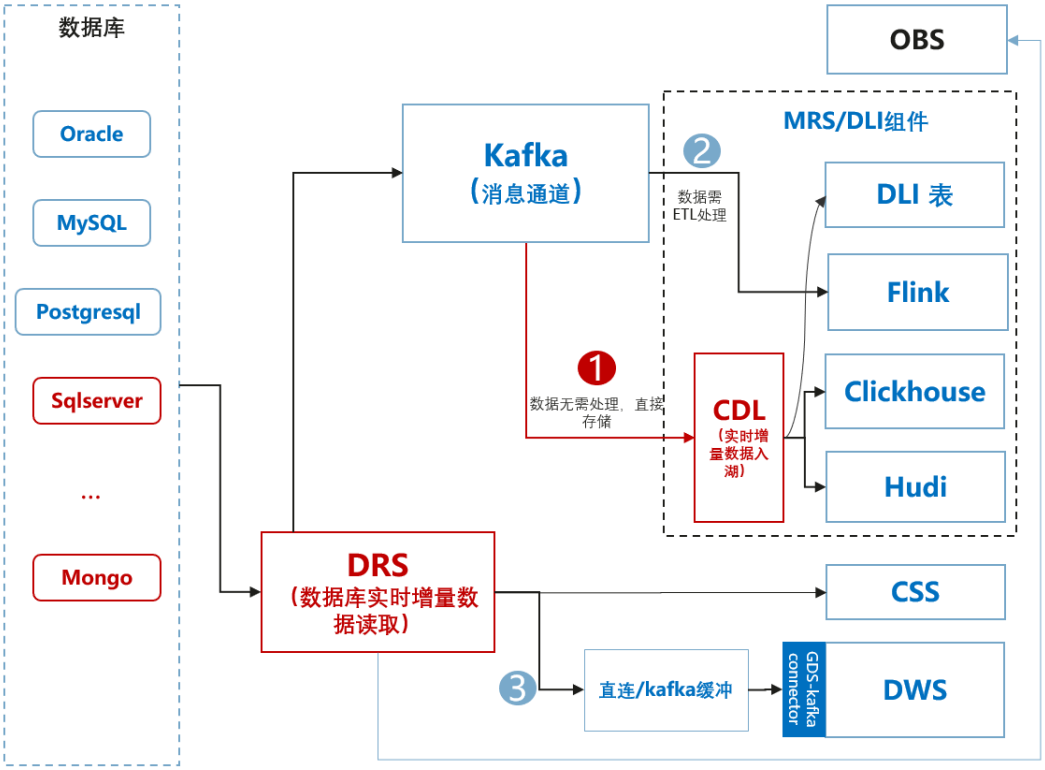
该方案以华为云 DWS 为主，其价值主张：

- DLI-Flink 支持流式处理，支持对埋点日志数据的高效处理；

- DWS 支持高效索引、聚簇等能力，为 Flink 的维表查询提供百万 QPS 毫秒级的点查询能力；
- DWS 可以读取 OBS 数据，使得 Spark 加工的数据可以直接以 DWS 外表方式对外提供查询服务，避免数据冗余存储；
- DWS 对外业务提供固定报表、自助分析等查询服务，为业务提供高性能、高并发、更灵活的报表查询能力。

4.2.3.3 数据库实时入湖场景

该场景为数据库源实时增量数据入湖。DRS：数据复制服务（Data Replication Service，简称为 DRS）提供 TP\HTAP 类数据库 CDC 能力，并支持将实时增量数据推送标准 Kafka 集群供入湖消费。

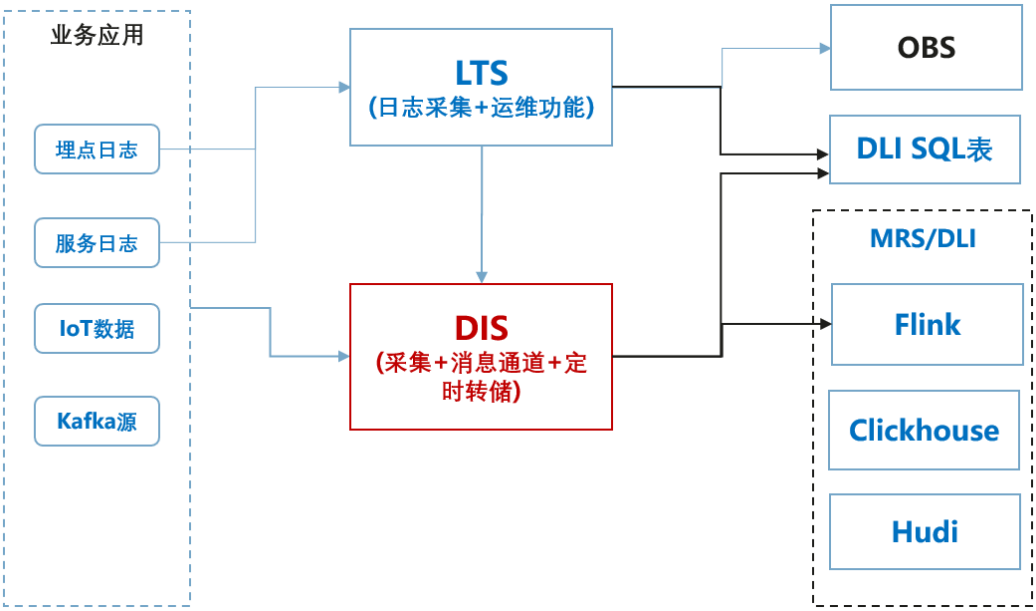


1) CDL 的内置 kafka 集群支持 DRS 直连对接，并支持实时写入 Hudi、Clickhouse、DLI 等。DRS 默认支持数据实时转储到 CSS、OBS（优先级低），供实时搜索场景消费和 AI 训练使用。CDL 构建到 DLI 链路，DLI 和 MRS 共用 CDL 入湖能力。
【CDL：Change Data Lake. 嵌入了 Spark 脚本， 不用客户写 SQL 脚本，直接消费，注入 Hudi 或者 ClickHouse】
2) 同时也可以间接入湖：CDC 实时 ETL 间接入湖（DRS+Kafka）
   - 可选用 DIS/DMS 提供标准 kafka 消息管道能力， 供 MRS、DLI 等大数据平台消费。DIS 需要支持标准 kafka 协议接口。
3) 数据库 CDC 实时入数仓 DWS(DRS+Kafka)
   - 直接入仓：适用于轻型业务场景（同步数据量<=3000 行/s），DRS 解析源数据库实时增量数据，直接写入 DWS。
   - 缓冲入仓：适用于重型业务场景（同步数据量>3000 行/s ），DRS 获取源数据库的实时增量数据并推送给后端 kafka 消息集群，DWS 内置的 GDS-kafka Connecor 负责消费 kafka 集群的实时增量数据并写入 DWS 表中。

4.2.3.4 消息、日志类数据实时入湖场景

由 DIS 构建 Serverless 化的消息集群能力，并提供数据采集、投递转储到 OBS、DLI 表、CloudTable 等能力。

LTS 提供应用日志采集、查询分析等应用运营运维能力，并且 LTS 支持将日志数据投递转储到 OBS、DIS、DLI 表等数据湖组件作进一步大数据分析。



消息类流式数据实时入湖场景：DIS

- DIS 是 serverless 化消息集群，提供消息管道能力， 供 MRS、DLI 等大数据平台消费。
- DIS 还支持数据采集和定时转储至 OBS、DLI、CloudTable 等大数据生态服务。

应用日志类流式数据入湖场景：LTS

- LTS 提供日志采集和运维功能，并支持投递至 DIS/DMS、OBS、DLI 等目标端，供进一步大数据分析。

4.2.4 大数据迁移

4.2.4.1 大数据迁移流程简述

大数据迁移是数据迁移的一部分，遵循整体上云迁移的理论与项目管理逻辑。大数据迁移，从项目管理的角度，分为业务调研、迁移方案设计、迁移实施与迁移验收四个阶段。

4.2.4.2 大数据迁移方案设计思路

在**业务调研阶段**，大数据迁移的关键工作就是调研梳理客户当前业务现状。其主导方是客户，云平台提供方为协助方，需要共同了解：

- 客户当前大数据平台，与大数据业务全景；
- 当前大数据平台物理部署和数据流全景；
- 大数据资产梳理，包括资源、数据、权限配置等。

在**迁移方案设计阶段**，需要详细设计整体迁移方案与落实迁移内容。其主导方是云平台提供方，客户为协助方：

- 迁移目标平台架构，有什么改造优化？如何平滑迁移？
- 整体迁移策略，是否分阶段迁移？每个阶段的目标？
- 平台迁移，涉及哪些云服务？
- 数据迁移 ，多少数据规模？如何迁移？专线？盒子？…
- 任务迁移，客户的任务调度系统是核心。
- 流量切换方案，涉及实时数据流，Nginx、ELB 等基础服务能力。
- 回滚方案，如何保证能够回退。

同时在**迁移方案设计阶段**，要对上云所需资源进行规划与评估。这部分主要包括：1）平台建设资源；2）迁移网络带宽评估等，跟整个上云的方案息息相关，涉及费用评估，也要对上云后的网络进行规划，包括网络流量如何打通，网络安全如何隔离防护等等。

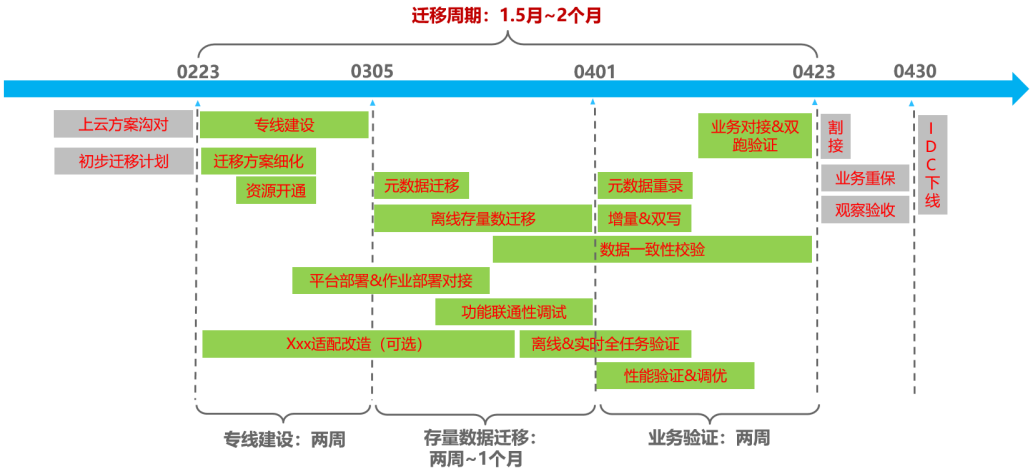
迁移实施阶段主要是具体的执行，其主导方是客户。包括，资源准备&部署，作业系统部署和流程验证，数据迁移和校验，增量数据迁移与再校验，双跑验证和性能调优等。

最后是**迁移验收阶段**，主要工作包括业务割接，业务验证和巡检，风险项识别和闭环，专项培训赋能，以及正式交接。

4.2.4.3 大数据迁移计划&周期示例

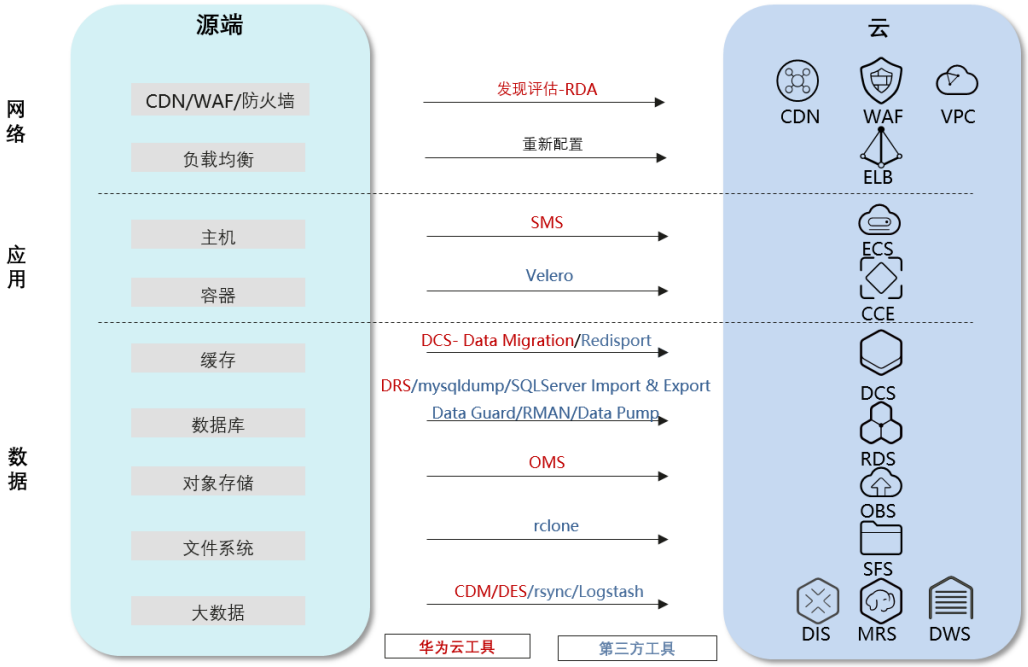
每个客户的数据量、任务量、使用组件、调度系统、专线带宽、数据可迁移时间段等都不一样，因此实际的迁移计划&周期都会不同。

以下是常见于中等规模客户（有效数据量 xPB，计算资源 x 千核）的迁移计划和周期。



4.2.4.4 大数据迁移工具

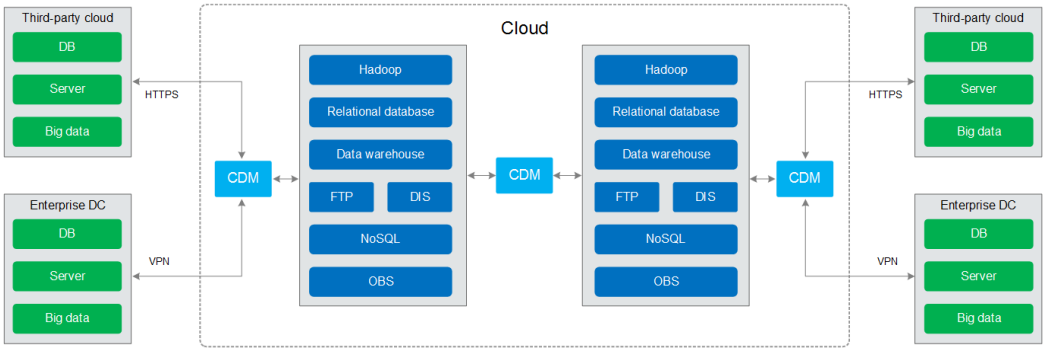
根据不同的场景，不同的数据源，数据量的大小，还有应用对数据的响应要求，客户可以选择不同的迁移工具。华为云提供了较为完整数据迁移工具，当然客户也可以选择开源的或者第三方工具。



华为云大数据核心迁移工具：

- CDM 云数据迁移（Cloud Data Migration）

CDM 是一个高效、易用的批量数据迁移服务。CDM 围绕大数据迁移上云和智能数据湖解决方案，提供了简单易用的迁移能力和多种数据源到数据湖的集成能力，降低了客户数据源迁移和集成的复杂性，有效地提高您数据迁移和集成的效率。详见：
https://support.huaweicloud.com/productdesc-cdm/cdm_01_0143.html



➢ Kafka MirrorMaker

目标端为 MRS-kafka，通过 Kafka MirrorMaker 实时转发，将流式数据实时接入华为云。消费者组对消息的顺序有严格要求，适用于消息有序场景。

注意点：一般在目标端开启 MirrorMaker 进程；源端 Kafka 和目标端 Kafka 的元数据需要保持一致，元数据需要手工配置。

➢ DRS：数据复制服务（Data Replication Service）

DRS 致力于提供数据库零停机的迁移上云体验，支持同构异构数据库、分布式数据库、分片式数据库之间的迁移，通过 DRS 也可以让数据库到数据库、数仓、大数据的数据集成与数据传输秒级可达，为企业数据贯穿和数字化转型打下坚实的第一步。
https://www.huaweicloud.com/product/drs.html

➢ OMS 对象存储迁移服务（Object Storage Migration Service）

OMS 是一种线上数据迁移服务，帮助您将其他云服务商对象存储服务中的数据在线迁移至华为云的对象存储服务（Object Storage Service，OBS）中。

对象存储迁移服务的典型应用场景有：

- 对象数据搬迁：将典型 Web 应用搬迁到华为云上时，把用户的对象存储数据搬迁到华为云中。
- 云上容灾：出于灾备，把用户对象存储数据复制到华为云中。
- 对象数据恢复：利用其他云服务提供商备份的数据，恢复用户在华为云丢失的对象存储数据。

详见：https://www.huaweicloud.com/product/oms.html

5 云上治理与运维

5.1 概述

为提升企业在华为云上业务的可用性，更好的节省成本以及保障业务安全可靠的运行，我们根据行业经验，结合华为自身的实践总结，打造了经验及服务的云上治理与运维环节，旨在为企业提供如下的价值：

- 专业体系：引导企业相关人员深入了解云上业务的成本管理、安全合规和运维治理体系，形成专业化的云上管理组织和能力；
- 成本优化：通过资源合理选型搭配，以及可视化的成本管理，优化云上成本；
- 安全合规：参考安全合规和治理方法论，全面标准化安全治理体系，确保业务安全运行；
- 稳定性提升：参考云上运维的分析和治理方法，全面分析业务存在的隐患、瓶颈和可用性问题，通过不断的优化提升系统的稳定性，减少业务损失。

5.2 成本管理

随着业务发展，如何做好云资源成本管理，合理利用云资源支持好业务发展，成为企业重点关注的领域。本章主要通过云资源选型和成本中心的数字化管理帮助企业实现成本的最优化控制。

5.2.1 云资源选型

1. 合理选择 ECS 实例类型和购买方式

基于应用场景和工作负载选择合适的实例类型和规格可以帮您节省 ECS 成本支出，同时，基于具体业务持续的周期，通过选择合适的购买方式可进一步帮您节省成本，具体实践有：

- 实例类型优化：针对不同应用场景，华为云提供多种类型的实例，如：通用性/内存优化型实例适合于网站、WEB 应用或中轻载企业应用等场景，高性能计算型/存储密集型/GPU 型则用于高性能计算、视频编码、3D 渲染等场景，可根据具体应用场景，选择合适实例优化成本。假如应用场景是电商网站运营，建议使用通用性或内存优化型实例，而非计算型实例，这样同样规格实例（如：8 核 16G），将节省 40%-50%的成本。
- 实例规格优化：针对不同工作负载，华为云提供了几十种实例规格，可基于业务工作负载，选择匹配的规格优化成本。假如电商网站访问量在 50 万 PV 以内且交易量在每天 3000 单以内，建议使用 4 核 8G 规格而非 8 核 16G，此种调整可节省 40%-50%成本。

- 购买方式优化：当前华为云提供按需、包月、包年 3 种购买方式，基于三种模式支出成本对比，针对业务的使用场景和持续周期，建议的最佳购买方式如下：

- 若应用持续周期小于 20 天，如：短期测试、电商节假日促销等场景，建议以按需方式购买；
- 若应用持续周期大于 20 天而小于 10 个月，如：游戏上线测试和运营等场景，建议以包月方式购 买；
- 若应用持续周期大于 10 个月，如：企业官网运营、政务民生信息查询运营等场景，建议以包年方式购买。

2. EVS 成本优化最佳实践

- EVS 类型优化：华为云提供 4 种类型 EVS，其中极速 SSD 型适用于大型 OLTP 数据库、NoSQL 数据库和流处理与日志处理等场景，超高 IO 型适用于高性能计算、数据仓库场景，通用 SSD 型适 用于企业应用和大中型开发测试场景，高 IO 型则适用于办公应用等场景。假如使用场景是电商网 站运营或企业官网运营，建议选用高 IO 型，而非超高 IO 型，这样同样容量 EVS，将节省 65%的成本。

- EVS 容量优化：基于 EVS 弹性扩容的能力，应根据当月的预测容量来购买量，在其利用率达到 80%或以上时，再进行实时扩容，以保证其利用率维持 80%左右，与按全年预测的最大容量购买相比（一般其利用率达不到 50%），EVS 的费用支出将减少 20%-30%。另外，也应定期检查账号，定期删除那些独立的、无用的 EVS 卷（随 ECS 创建而创建，ECS 删除时未删除的 EVS 卷），会进一步减少成本。

- 转换购买方式：若业务已在华为云上运行一段时间，针对已开通且后续长期使用 EVS 卷，建议从按需或包月方式购买转变为包年方式购买，这样做，同样容量的 EVS 卷，将至少节省 17%成本，另外将一些不经常使用非关键数据或归档数据转移到 OBS 存储会极大降低成本。

3. OBS 成本优化最佳实践

- OBS 类型优化：华为云提供 3 种不同可用性、持久性标准的 OBS 服务，其中标准存储适用于大数据、热点视频等需频繁访问数据的场景，低频访问存储适用于文件同步、企业备份等不频繁访问的场景，归档存储适用于数据归档、长期备份等很少访问的场景。基于不同业务需求，选择合适的对象存储类型，将极大节省成本开支。对于需要备份的企业数据，建议选择低频访问存储，同标准存储相比，可以节省 45%的成本，针对时间较久的备份数据，建议将其转移到归档存储，相比标准存储，可以减少 78%成本。

- 转换购买方式：针对标准存储，华为提供了多种容量规格和不同周期的存储容量包，针对已上传到标准存储且会将长期使用数据，可根据现有的数据容量，购买对应的包年容量包，同按需方式购买相比，采用包年容量包，将节省 25%成本。

4. EIP 成本优化：

- 带宽成本可能占到用户公有云使用成本的多达 30%，在进行云服务配置时需重点考虑。华为云提供静态 BGP 带宽和全动态 BGP 带宽两种选择，绝大部分情况下选择静态 BGP 带宽即可，如果是金融或游戏客户对带宽有极致体验诉求的可以选择全动态 BGP 带宽，静态 BGP 带宽价格比全动态 BGP 带宽低 20%。此外，5M 带宽以下时选择带宽包月往往比按流量更划算，5M 带宽以上时需要根据带宽大小和预估的带宽利用率按以上方法计算得出哪种方式更划算。如果是以按需(按小时)的方式购买带宽和按流量进行成本比较的话，结论为：如果是以按需方式购买 10M 静态 BGP 带宽，那么当带宽利用率大于 45%时选择按带宽计费更划算；如果是以按需方式购买 1M 静态 BGP 带宽，那么当带宽利用率大于 18%时选择按带宽计费更划算。

5. 利用 ELB 实现带宽集约减少带宽成本

- 以小型游戏云架构设计为例，如果将登陆和充值区、游戏一区、游戏二区分别部署在 1 台 ECS 上，每台 ECS 配置 10M 带宽，那么总共需要 30M 带宽。不过同一时间三个区的用户访问量有差异，会造成有的带宽利用率高有的带宽利用率低。因此可以在架构设计上部署 1 个 ELB 在 3 台 ECS 的上方做流量分发，ELB 只需配置 20M 左右的带宽即可，通过 ELB 实现带宽集中提升带宽利用率减少带宽本。

6. 合理使用 CDN 减少公网带宽使用量，降低 TCO

- 如果您正在通过 ECS 或 OBS 向互联网用户提供图片、视频、文件下载等静态内容，那么可以引入 CDN 服务降低流量成本，从下图价格表可以看出使用 CDN 能够降低流量成本达 50%~57%，并且 CDN 使用的流量越多单价越低节省成本越多。使用 CDN 除了能节省成本还能带给客户更好的体验。此外 OBS+CDN 的源站加速方案使用存储空间换公网带宽实现网络成本优化能达 20%+。

7. 当有大量数据需上传到公有云时，使用数据快递盒比使用专线传输数据大幅节省成本。

- 以一个有海量照片产生并存储需求的用户为例，每天新产生 35TB 图片数据需上传到 OBS。如果使用专线传输，需要购买 4G 带宽的专线才能满足每天传输 35TB 数据量的要求，4G 带宽的专线每个月费用在 32 万元左右。数据快递盒每次可运输 120TB 数据，可以使用数据快递盒每 3 天将新产生的图片数据运输一次，每个月作业 10 次的费用在 5 万元左右，相比使用专线传输数据可节省多达 80%的成本。

8. 华为云大数据的存算分离方案性价比业界领先

- 计算资源和存储资源分离，单独扩缩容，避免单台节点计算、存储资源配比不均衡问题。此外还支持使用鲲鹏算力，可以进一步节省算力成本。

5.2.2 成本中心

成本中心是华为云免费向客户提供的一项成本管理服务，可帮助您收集华为云成本和使用量的相关信息、探索和分析华为云成本使用情况、监控和跟踪华为云成本。

目前，关于成本中心包括以下内容：

5.2.2.1 成本计划

- **估算和预测成本**

云支出的可变性，导致云支出是很难预测的。

对于新产品发布或区域扩张，客户可使用华为云价格计算器在线自助估算各种产品，不同区域、不同规格、不同购买选项的成本。对于已使用产品，客户也可以使用华为云成本中心的成本分析来预测每日（最多未来 90 天）或每月（最多未来 12 个月）的云成本。该预测，主要基于客户历史成本和历史用量情况，应用机器算法进行估算。

- **创建预算以跟踪成本**

跟踪成本计划的有效工具是预算。

一旦完成成本的估算与预测，客户可以在华为云成本中心的预算管理创建精细粒度的预算来管理成本，并可以创建预算提醒，在实际或预测超过预算阈值时，自动通知利益相关人支出异常。客户还可以创建预算报告，每天/每周/每月，定期将指定预算进展通知给利益相关人。

5.2.2.2 成本分配

准确有效的成本分配，有利于企业内部的成本透明与问责。而透明的成本责任制是企业财务管理的基础。

- **确定成本组织方式**

企业进行财务管理之前，需要先确认云支出的组织方式，确保将企业在华为云上的支出能分摊到企业内部的组织层级结构上。

对于使用多账号的企业组织来说，可以使用关联账号来天然分摊企业在华为云的支出。同时，企业还可以使用标签将组织信息标记在资源上，资源标签会随资源使用添加到客户的成本数据上。客户可以使用标签识别不同环境（比如生产、测试）的成本、或使用标签识别不同的组织、产品、负责人。

华为云成本中心为客户提供成本标签功能，企业各成员账号（含主账号）在成本中心将资源标签激活为成本标签后，各账号就可以在成本中心基于成本标签进行成本分析、预算跟踪。成本标签只能影响激活后新产生的成本数据，因此我们建议客户尽早进行成本标签的规划和激活。

对于不能通过标签归集的成本（比如企业内部共用资源产生的成本，未及时标记标签产生的成本，或暂不支持标签管理的产品成本），建议客户在企业内部约定分配规则，将这类共同成本分配到企业内部。分配规则可以是平均分配、自定义比例，或者按照可归集成本的比例进行二次分配。

- **采用应计视角的摊销成本**

华为云成本中心为客户提供了不同的成本类型：

- 原始成本：反映了客户的原始使用和购买情况。该成本是基于云服务官网价，应用了商务折扣、促销折扣等优惠之后的金额。
- 摊销成本：反映了包年/包月产品的预付金额在订单有效期间内按日分摊后的有效成本。比如客户购买了有效期为一年的云服务共 365 元，则每天的摊销成本为 1 元。

从财务视角来看，摊销成本为应计成本，是按照权责发生制计算的成本，因此我们更建议客户使用摊销成本在企业内部分摊成本。

详细的成本摊销规则可参见：https://support.huaweicloud.com/usermanual-cost/costcenter_000002_01.html

5.2.2.3 成本分析

了解组织内的成本趋势和成本驱动因素，是企业进一步有效管理成本、控制和优化成本的关键。

- **分析成本及用量的趋势及分布**

华为云成本中心的成本分析支持使用汇总和过滤机制可视化最多 18 个月的原始成本或摊销成本，从而通过各种角度、粒度、范围深度分析成本和用量的趋势及驱动因素。企业主账号可以同时分析名下各子账号的成本和用量情况。

客户可以使用成本中心提供的预置分析报告对常见场景快速分析，预置报告包括：

报告名称	说明
按产品类型汇总的月度成本	了解过去 6 个月原始成本较高的产品类型。
按关联账号汇总的月度成本	了解过去 6 个月原始成本较高的关联账号。
每日成本	了解过去 3 个月的每日原始成本趋势，以及未来 1 个月的成本预测。
月度摊销成本	了解过去 6 个月摊销成本的月度趋势。

ECS 的月度按需成本和使用量	了解过去 6 个月云主机每月按需原始成本和按需使用量情况。

如果预置报告不能满足客户诉求，客户还可以**自定义分析**，通过调整时间粒度、周期、汇总条件、过滤条件以及成本类型，来洞察成本和用量的情况。对于客户经常关注的自定义分析，建议保存为**自定义报告**，便于再次查看相同条件下的分析数据。

无论是预置报告还是自定义分析报告，报告分析结果均支持导出 CSV 文件。同时，华为云成本中心还支持导出携带标签和关联账号的月度摊销成本明细，便于客户深入分析。

5.2.2.4 成本优化

云支出的主要影响因素，是费率和用量。因此企业在华为云上的成本优化也主要从这两方面着手考虑。

- **降低费率**

对于长期使用的按需产品，建议客户优先采用包年包月或资源包。

客户可使用华为云成本中心的按需转包年包月优化评估发现节省成本的机会。该评估基于客户 ECS、EVS、RDS 历史按需资源的使用情况进行分析，为客户提供按需转包年包月的可优化资源清单和优化前后的成本对比。

如果客户已购买资源包，客户还可以使用华为云成本中心的资源包使用率/覆盖率分析，分析已购买资源包的使用情况。对于使用率过低的资源包，判断是否购买过量；对于覆盖率过低的资源包，判断是否购买不足。客户根据分析结果优化下一周期的资源包购买。

- **减少用量**

客户可通过监控云服务的利用率，来识别空闲资源或利用率较低的资源。释放空闲资源或降配利用率低的资源，可以减少不必要的付费用量。需要注意的是，无论是释放资源还是降配资源，都需要和业务部门确认，以确保不影响业务使用。

客户可以基于业务技术方案的优化，比如存算分离、分时复用将资源充分利用起来，或使用性价比高的实例，来减少付费用量。

5.2.2.5 成本中心工具

总结下，目前成本中心提供的主要工具主要如下：

- 成本分析：以图表形式提供可视化的成本数据。您可以跨多个账期查看您的成本和使用量趋势，并按照产品类型、区域、关联账号、计费模式、成本标签等维度汇总和过滤图表。

- 成本与使用量预测：运用一定的科学方法，基于客户在华为云上的历史成本和历史用量情况，对未来的成本和用量进行预测。

- 预算管理：您可以设置预算来跟踪您的成本和使用量，并在成本或使用量超过您设置的提醒条件时收到提醒通知。

- 报告管理：您可以将成本分析结果保存为分析报告在账号内分享，我们在“分析报告”中还预置了常见的分析报告，您可以直接使用。您也可以创建“预算报告”来定期跟踪预算执行情况。

- 成本监控：可以监控您按需资源的成本情况，以检测异常成本，减少不必要的支出。

- 计费模式：

  - 成本优化建议：成本中心可以分析客户 ECS、EVS、RDS 按需资源的使用情况，通过“计费模式”下的“包年包月”为客户提供按需资源转包年包月的优化评估，帮助客户发现节省成本的机会。

- 资源包分析：您可以查看资源包分析数据，通过数据展示了解购买资源包是否被合理使用，以达节约成本的目的。

➢ 成本标签：您在使用标签标识和管理资源的同时，还可以将标签激活为成本标签来归集成本。成本标签可以应用在成本分析和预算管理中。

5.3 安全合规与治理

5.3.1 安全合规与治理方法论

随着全球监管环境的日益复杂，越来越严格的合规遵从先后颁布于生效。企业如果不能满足这些规定和要求，将会面临毁灭性的商业损失。因此，为了应对越来越严格的法规遵循要求，需要企业加强企业安全治理、风险和法规遵从等。

根据华为云 3CS（CLOUD SERVICE CYBERSECURITY & COMPLIANCE STANDARD）安全管理要求的治理体系的实践，安全合规及治理的思路如下：

1. **制定治理策略：**策略包括组织的安全治理的目标、安全治理角色和职责、最高管理层的承诺和保障、明确组织层面的安全治理工作重点以及核心评价指标、确保治理体系可有效地落地执行，并持续优化的方法。

2. **将安全控制要求融入管理流程：**组织应将安全合规控制要求融入到组织的各项管理流程中，使业务部门可根据日常需执行的业务流程来更好地理解并融入安全控制措施。

3. **采用合适的工具能力满足支撑安全合规和治理：**有一些安全合规的管控，传统手工方式几乎无法实现，例如岗位职责变化时应在 24 小时内完成帐号和权限变更，这类要求实际上在推动组织研究采用先进的技术工具，以匹配组织规模的发展，以及应对不断涌现的新型威胁。云服务商也可适时地向客户提供云安全服务产品和综合解决方案，例如华为云现已向客户提供 20+自研安全服务及 200+伙伴安全服务，协助客户快速实现先进的云安全管理技术能力。

4. **建设治理组织：**组织制定了网络安全与隐私保护的治理策略后，需要任命管理者，并建立一个组织架构来执行网络安全与隐私保护的管理工作。

5. **做好数据安全保护：**由于数据安全涉及的能力覆盖范围非常大，组织在进行数据安全能力建设时必须抓住重点，宜将注意力聚焦在与数据生命周期相关的主要风险上，避免将数据安全的概念泛化。

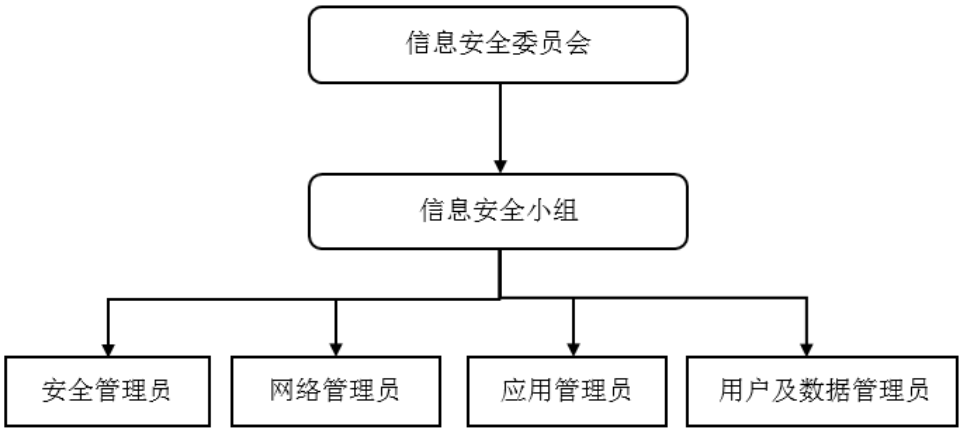
6. **执行信息安全度量：**组织的安全管理活动会产生大量的过程记录，通过对过程记录进行各种统计和分析，能得到许多数据。组织需要从中选择有管理意义的数据加工成度量指标。组织应先确定评估目标，再明确需要什么支持信息；选择指标的指导原则可归纳为：可量化、可重复、可获取、可比较、可牵引。

下文将安全合规和治理中的实践进行展开说明。

5.3.2 安全管理组织

为标准化信息安全管理流程，促进安全管理的组织建设，指导安全运营工作，落实数据安全保护管理责任，需要确定清楚组织与人员的角色与职责。

安全管理组织主要由信息安全委员会和信息安全小组组成，信息安全小组由安全管理员、网络管理员、应用管理员、用户及数据管理员等负责信息系统的具体管理工作。下图的组织架构供参考。



- **信息安全委员会工作职责：**

- 贯彻关于信息安全方面工作的方针政策，审定信息系统安全建设规划。
- 对信息系统安全工作的重大事项做出决策。
- 研究审定信息系统安全建设和管理工作中的制度、标准及相关政策，并协调相关部门监督制度、政策的实施情况。
- 组织、协调和指导信息安全的宣传、普及教育工作。

- **信息安全小组工作职责：**

- 负责贯彻落实政府关于信息系统安全工作的要求和规定。
- 负责各业务部门信息系统安全管理工作。
- 根据信息化建设的总体目标，负责信息系统的安全管理体系，包括：制度建设、技术保障和操作规范等各方面的逐步建成。
- 负责灾难备份系统及相关设施的完善及日常管理工作。制订并完善灾难备份系统评估标准，形成标准化管理模式。
- 监控灾难备份系统运行状况，定期或不定期组织演练，对灾难备份系统的运行状况进行审计和评估，并提出改进意见。
- 当信息系统运行发生重大问题时，协助相关部门正确判断原因，根据指令立即采取安全措施启动相关处理程序。
- 加强信息系统的安全教育，通过各种方式进行宣传和培训，提高全系统安全防范意识。
- 负责信息系统安全工作进行指导、检查并进行情况通报。
- 负责全系统的计算机恶意代码防治和网络安全的管理工作。
- 负责与外部安全机构的协调联系，在发生重大安全事件时以协调获取外部安全机构的支持。
- 负责制订信息系统安全规划，并在实施过程中逐步完善。
- 负责信息系统运行安全保障工作的管理、组织、实施和监督。

- 负责运行维护体系和技术支持平台的建设与运行管理。
- 组织制订和贯彻信息系统运行安全保障和维护工作制度。
- 组织实施对信息系统各类事故（故障）进行应急处理。
- 负责数据综合利用和查询展示的管理和实施。
- 负责容灾备份中心的运行管理。
- 负责落实信息安全委员会部署的各项工作。
- 负责信息系统安全制度、技术保障和操作规范的建立及其它相关信息安全管理工作。
- 负责对信息安全状况的定期检查；当出现安全事件时，对发生的安全事件及时上报，并配合相关的调查和纠正工作。
- 负责对内部人员进行信息系统安全的教育、培训，提高内部人员的信息系统安全意识。

➢ **安全管理员职责：**

- 负责信息系统的安全相关事务，协助监督安全制度的执行、修改等。
- 负责安全制度的贯彻执行。
- 负责制订信息系统安全规划，并在实施过程中逐步完善。
- 负责制定安全设备或系统的相关资产清单。内容包括资产管理的责任部门、信息分类和资产标识的方法和资产名称、重要程度、所处位置等。
- 负责规范安全设备或系统管理流程，建立管理台帐，明确资产所有者、使用者与维护者，对安全设备或系统进行标记，实现对机房资产购买、使用、变更、报废整个周期的安全管理。
- 负责制定安全设备或系统的文档化的操作和维护规程，使得相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。
- 负责对安全设备或系统运行维护管理，对安全设备或系统运转情况进行定期巡检、维护、故障处理和变更管理。负责组织实施安全设备或系统各类事故（故障）的应急处理。
- 负责协助领导安排安全培训，负责协助负责制定每年安全教育计划，加强信息系统的安全教育，通过各种方式进行宣传和培训，提高全系统安全防范意识。
- 负责制定安全检查计划，至少每季度检查一次。包括检查职责、检查周期、检查范围、检查内容、检查报告的编制、检查整改、检查通报等内容。对信息系统安全检查并进行情况通报。对记录进行收集、整理、归档。
- 当出现安全事件时，负责对发生的安全事件及时上报，并配合相关的调查和纠正工作。
- 当信息系统运行发生重大问题时，协助相关部门正确判断原因，根据指令立即采取安全措施启动相关处理程序。
- 负责与外部安全机构的协调联系，在发生重大安全事件时以协调获取外部安全机构的支持。
- 负责对各种记录文档、表单，半年一次进行汇总，并对制度开展情况向信息安全部领导进行汇报。

➢ **网络管理员职责：**

- 负责网络相关的运维、审批、变更事务，保存网络相关的文档、数据。
- 负责保障网络安全建设管理，对实施方责任、时间进度、任务要求、质量控制等进行监督管理。
- 规范网络管理流程，建立网络相关资产管理台帐，明确资产所有者、使用者与维护者，对所有信息资产进行标记，实现对信息资产购买、使用、变更、报废整个周期的安全管理。
- 采用技术和管理两方面的控制措施，加强对信息系统的安全控制，不断提高网络的安全性和稳定性，信息系统外网与互联网进行逻辑隔离。通过实施网络访问控制等技术防范措施，对接入进行严格审批并登记，加强使用安全管理，加强对系统使用的安全培训和教育，确保信息系统的安全。
- 对重要网络设备应有文档化的操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。
- 负责保障网络安全。协助安全管理员部署网络安全产品，确保网络安全。对网络设备设施运转情况进行定期巡检、维护、故障处理和变更管理。
- 在网络系统变更、重要操作、访问等的进行逐级审批，负责日常审批，重大变更上报到信息安全部。
- 负责组织实施网络各类事故（故障）的应急处理。

➢ **应用管理员职责：**

- 负责应用系统相关的运维、审批、变更事务，保存应用系统相关的文档、数据。
- 负责保障软件开发管理，对实施方责任、时间进度、任务要求、质量控制等进行监督管理。进一步重视软件开发安全。在系统立项和审批过程中，同步考虑信息安全需求和目标。需保证系统设计、开发过程的安全，重点加强对软件代码安全性的管理。属于外包软件开发的，需与服务提供商签署保密协议。系统开发完成后，并要求通过第三方安全机构对软件安全性的测评。
- 规范信息资产管理流程，建立信息资产管理台帐，明确资产所有者、使用者与维护者，对所有信息资产进行标记，实现对信息资产购买、使用、变更、报废整个周期的安全管理。
- 负责建立重要应用的文档化操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。
- 规范应用系统资产管理流程，建立应用系统资产管理台帐，明确资产所有者、使用者与维护者，对所有信息资产进行标记，实现对主机相关资产购买、使用、变更、报废整个周期的安全管理。
- 加强信息安全日常管理，包括应用系统口令管理、授权审批管理等，促使每位人员的日常工作符合信息系统安全策略和制度要求。
- 在应用系统变更、重要操作、访问等的进行逐级审批，负责日常审批，重大变更上报到信息安全部。
- 负责组织实施应用系统各类事故（故障）的应急处理。

➢ **用户及数据管理员职责：**

- 负责大型应用系统的后台技术支撑。根据数据监控及分析日常业务运营情况，善于捕捉业务运营的机会点与痛点。
- 对客户需求模型、数据进行深度分析挖掘，提供预警数值化指标。
- 对账户进行管理监控工作。

- 确保数据库的正常运行。
- 及时发现并解决后台问题与隐患。
- 进行系统性能调整和优化。
- 备份策略的规划与实施等。

5.3.3 人员安全管理

➢ **人员录用：**

- 应保证被录用人具备基本的专业技术水平和安全管理知识，在正式上岗前应对被录用人员进行基本的专业技术水平考核和安全管理知识考核。
- 应对被录用人的身份、背景、专业资格和资质等进行审查，并对相关审查资料进行留底和备案。
- 应对被录用人所具备的与岗位相关的技术技能进行考核。
- 应对被录用人说明其角色和职责，并进行针对性的岗位培训。
- 被录用人应签署保密协议，防止系统中的核心信息和相关重要信息的泄漏。

➢ **人员离岗：**

- 对于因各种原因即将离岗的员工，应立即终止其与系统相关的所有访问权限。
- 即将离职的系统管理员，应将管理设备的口令和密码上交，后续管理员应在第一时间进行口令和密码的修改工作。
- 离职员工应在人事部门办理严格的调离手续，并承诺调离后的保密义务后方可离开。

➢ **人员考核**

- 应定期对各个岗位的人员进行安全技能及安全认知的培训和考核，以确保系统各个方面的管理人员意识到信息安全威胁和隐患，并在正常工作时遵守信息安全方针，这种培训与考核有时候要扩大到有关的第三方管理人员和用户。
- 应对关键岗位的人员进行全面、严格的安全审查；对与系统各个方面的管理人员应该进行身份审查、岗位职责审查、权限和责任审查、保密审查等；对其他关键人员应该进行身份审查岗位职责审查等，以确保系统的安全运行和管理。
- 对违背安全策略和规定的人员进行惩戒；对违规的单位内部员工，情节较轻的，进行批评并要求其进行书面检讨，情节较重的，由相关部门追究其行政责任；对于违规的第三方管理人员，情节较轻的，责令其改正，并告知其项目负责人和该公司相关负责人，情节较重的，由相关部门追究其行政责任。

➢ **安全意识教育**

- 定期对各类人员进行环境安全、信息安全等方面的安全意识教育，要求员工持续学习网络安全知识，了解相关的政策和制度，知道哪些行为是可以接受，哪些是不能接受的，意识到即使主观上没有恶意，也要对自己的行为负责，并承诺按要求执行。
- 准确告知每个岗位上人员相关的安全责任和相关惩戒措施，对于较为关键和复杂的，应进行指导和相关培训工作。
- 宣传活动开展：面向全员开展形式多样的网络安全宣传活动，包括网络安全社区运营、网络安全典型案例宣传、网络安全活动周、网络安全动画宣传片等。
- 制定安全教育和培训计划，不定期对信息安全基础知识、岗位操作规程等进行培训。
- 对安全教育和培训的情况和结果进行详细记录，并归档保存。

- 签署信息安全承诺书，承诺遵守公司各项网络安全政策和制度要求。

➢ **安全能力培训**

可以参考业界优秀实践建立完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，确保员工有能力向客户交付安全、合规的产品、解决方案与服务。

- 网络安全基础培训：根据不同角色、岗位制定相应的安全基础能力培训计划。新员工转正前必须通过有关网络安全与隐私保护的上岗培训和考试；在岗员工需根据不同业务角色，选择相应课程进行学习与考试。管理者需参加网络安全必须的培训和研讨。
- 精准培训：通过大数据分析识别产品研发过程中的典型安全问题和问题关联责任人，并向其精准推送安全典型培训方案（包括案例、培训课程、练习题等），持续改进安全质量。
- 实战演练：引进业界优秀实践，开发网络安全实战演练平台，开展红蓝对抗，提供场景化的实战演练环境供员工练习和交流，提升员工的安全技能。
- 安全能力任职牵引：为了让员工更加自觉、有效地进行网络安全学习，将网络安全要求融入到任职资格标准中。员工在任职晋升过程中需要学习相应的网络安全课程，通过相应的网络安全技能考试，提升自身网络安全能力。

5.3.4 安全巡检

规范业务上云之后的各项安全服务或者系统的安全告警的监控处置工作，明确各层级安全防护系统的监控关键点、处置动作以及事件升级流程等工作。尽可能避免安全攻击行为导致的业务系统影响，快速发现风险消除威胁，保障业务安全稳定。

5.3.4.1 安全巡检检查点

➢ **网络安全巡检**

- 外网端口暴露：检测云服务 ELB、NAT 网关等配置策略，并确认护网相关业务不存在高危端口对外暴露，如：内部管理端口（如：22、3389 等）、高风险端口（TCP：135，139，445；UDP：137，138 等永恒之蓝以及勒索病毒常用端口）以及 EIP 直接绑定导致所有端口外露等情况；
- 内网网络互通：检查并确认护网相关的业务系统的网络 ACL、安全组等配置不存在内部网络规划不清晰、管理端口开放范围过大、主机端口任意访问等情况，力求做到业务之间网络护网互访关系明确、业务逻辑清晰；业务内部主机互访关系明确，相互只开放必须的业务端口。

➢ **系统安全巡检**

- 漏洞管理：针对护网相关业务系统的所有资产进行漏洞扫描，针对发现的安全漏洞进行限期修复，并对漏洞信息进行跟踪管理，形成漏洞全周期闭环管理；漏洞管理功能将检测 Linux 软件漏洞、Windows 系统漏洞和 Web-CMS 漏洞，帮助用户识别潜在风险；
- 基线配置：通过基线检查服务对护网相关业务资产进行基线扫描，主要包括：口令复杂度策略检测、经典弱口令检测、配置检测，并对风险项尽快完成整改；
- 资产管理：通过云安全服务对主机资产信息进行统一收集和管理，形成业务资产基线，主要包括：账号信息管理、主机开放端口检测、进程信息管理、Web 目录管理、软件信息管理、自启动项管理等；

- 入侵检测：通过云主机安全服务检测护网前业务主机是否存在恶意程序、异常进程、网站后门、异常 shell、风险账户以及 Rootkit 程序等风险，并拉通业务人员及时进行处置和消除。

➢ **应用安全巡检**

- 常规安全防护：检查并确认所有护网相关的业务系统均已配置 web 防火墙策略，能够有效监测并封堵大部分常规 web 应用层攻击，如：SQL 注入、XSS 跨站脚本、文件包含、目录遍历、敏感文件访问、命令/代码注入、网页木马上传、后门隔离保护等；
- 业务访问源控制：拉通业务人员确认业务应用访问源范围，并通过 WAF、VPN、堡垒机等手段尽可能减少业务对外开放范围，对可以确认的业务系统实行访问权限回收操作，如：VPN 权限回收、海外 IP 地址封堵、创建 IP 地址黑白名单等；
- 常规漏洞监测：护网前通过漏洞扫描服务对相关业务进行漏洞检测，及时协调业务人员对网站漏洞进行整改，至少保证护网前业务系统不存在高危漏洞对外暴露；
- 网页防篡改配置：根据业务梳理得到的信息，通过华为云主机安全服务对网站进行静态网页防篡改配置，对网站根目录进行全面保护，从根本上杜绝红队通过上传脚本的方式获取反弹 shell 权限；
- 渗透测试：通过人工方式进一步检测网站业务系统是否存在逻辑性漏洞，并组织业务人员及时修复，补充漏洞扫描的不足，规避绝大部分业务应用漏洞风险；
- 业务账号梳理：组织业务侧专家进行应用账号的梳理，对非业务必须类账号进行回收，尤其是 4A 等关键业务系统的账号权限；对护网相关业务网站进行登陆保护控制，如：部署多因子认证等，同时进一步清除僵尸账号和进行管理员账号权限回收。

➢ **数据安全巡检**

- 数据访问权限检查与控制：全面排查梳理数据库的访问账号和权限，删除测试账号，并以最小权限原则全面清理数据库的访问权限。
- 数据库安全防护：部署数据库审计设备和数据库防护设备，对数据库操作进行实时过滤、监控和审计。
- 运维接入面检查与整改：进行运维接入方式的安全排查与整改，防止红队通过运维账号渗透入内网，确认堡垒机、VPN 等运维接入系统用户均采用双因子认证方式且密码长度及复杂度符合安全要求，防止运维管理员的运维账号被窃取，导致大面积主机暴露的情况发生。
- 账号检查与整改：检查并确保密码长度及复杂度符合安全要求，不同账号权限均根据职位角色进行精确划分，确保不同管理员只能访问与自己业务相关的资源。
- 安全备份检查与整改：检查并确认护网相关的重要业务系统均已规划备份机制，如数据备份、主机备份、快照等，极端情况下可通过备份恢复保证业务正常。

5.3.4.2 安全巡检报告模板

分类	检查项	安全建议
账号口令	口令复杂度要求	密码长度最小 10 位；至少一个数字；至少一个大写字符；至少一个小写字符；至少一个特殊字符；不能和用户名重复或者用户名的倒序
	账户锁定策略	帐户锁定时间 （30 分钟）；帐户锁定阈值 （5 次无效登陆）；复位帐户锁定计数器 （30 分钟）

	口令修改策略	密码需定期更换，更换周期不得超过 90 天；在用户密码过期前通知用户 （7 天）
	不再使用的账号	删除
网络	网络 ACL	转维时提供配置清单，运维通过对比检查确认是否存在安全风险
	安全组	转维时提供配置清单，运维通过对比检查确认是否存在安全风险
	只保留业务必须的端口	转维时应提供必要端口列表，运维通过对比检查并关闭业务无关的端口
	网络流量	检查网络流量判断是否存在恶意流量，若有则深入分析，必要时让云服务商配合
操作系统	只保留业务必须的账号	清理/禁用与业务运行无关的账号
	系统账号	满足账号口令要求
	会话超时时间	一般设置为 15 分钟
	默认共享	禁止系统中默认共享的盘符、文件夹等
	只保留业务必须的进程	转维时应提供必要进程列表，运维通过对比检查非必要进程并关闭，如 alsasound、cups、fbset、nfs、postfix、rpcbind、smbfs、snmpd、splash、splash_early 等。
	系统漏洞	使用漏洞扫描工具进行扫描并修复
	系统日志	检查是否存在可能的异常/攻击，若有需进一步分析
	Messenger 服务	一般情况停止服务并禁用，业务确有需要时启用
	Remote Registry 服务	一般情况停止服务并禁用，业务确有需要时启用
	TCP/IP NetBIOS Helper 服务	一般情况停止服务并禁用，业务确有需要时启用
	Wireless Configuration 服务	一般情况停止服务并禁用，业务确有需要时启用
	Error Reporting Service 服务	一般情况停止服务并禁用，业务确有需要时启用
	Help And Support 服务	一般情况停止服务并禁用，业务确有需要时启用
	Telnet 服务	一般情况停止服务并禁用，业务确有需要时启用
	Print Spooler 服务	一般情况停止服务并禁用，业务确有需要时启用
	Computer Browser 服务	一般情况停止服务并禁用，业务确有需要时启用
	Themes 服务	一般情况停止服务并禁用，业务确有需要时启用
	Telephony 服务	一般情况停止服务并禁用，业务确有需要时启用

监控审计	系统日志备份	对系统日志进行备份以备审计
	业务监控信息	应提供系统/服务状态可监控能力，如系统监控项、数据库监控项、业务系统指标、网络等，运维能通过监控平台直观获取整个系统的总体监控信息
数据库	数据库账号	删除不使用的数据库默认账号，只保留业务必须的账号
	数据库口令	满足账号口令要求
	数据库文件访问权限	最小化文件/文件夹权限，只能被数据库进程运行账号及 DBA 账号读写
Web 服务	Web 漏洞	使用 Web 漏洞扫描工具检查漏洞并修复
	网站平台日志	检查是否存在异常/攻击情况，若有需进一步分析

5.3.5 账号安全管理

- **账号分类:**

- 堡垒机账号
- 操作系统账号
- 数据库账号
- 云管理平台账号
- 业务系统账号
- 云提供商提供的租户账号
- 其他与业务相关的账号

- **角色与职责:**

角色名称	职责
帐号申请人 （维护、开发、审计工程师）	根据工作相关原则为本人或者他人填写账号/权限相关申请；一般是帐号使用人
帐号使用人 （维护、开发、审计工程师）	指帐号/权限的使用人员。
帐号管理员 （系统管理员）	指帐号/权限管理的日常操作人员，如：负责处理审批后的开、销户申请单，进行口令保管、分发、回收，以及执行帐号使用人变更的操作等。
账号审批人 （运维负责人）	负责审批账号权限需求的必要性和合理性。 1、 负责依据工作相关原则，审核账号/权限相关申请内容的真实性、必要性和合理性； 2、 负责定期审视部门员工的账号/权限持有情况，对账号/权限持有不合理的情况，及时提交取消申请。 3、 对账号/权限的安全性负最终责任。

- **资质要求:**

- 只有确实因工作相关情况下才能申请接入现网生产环境的权限。
- 申请人必须为正式员工或已试用满 1 个月，同时未满试用期的，导师承担管理责任，否则不允许授予系统权限。

- 曾违反运维管理规范的，不得授予长期修改权限，只授予单次变更权限。

➢ **时长要求:**

- 不同角色具有不同时间期限，所有人员权限到期后需要重新申请。

申请时长	申请规则
1 年	从事长期现网运维工作，满足下列条件之一的： 运维人员 运维负责人 从事长期的运维工具开发、系统对接、上线的运维平台开发人员
三个月	适用进行服务交付期间的研发人员，服务转维后回收权限。
一周	有短暂需求的，如进行短期项目交付，验收、问题跟踪等工作。
一天	短暂访问，如事件/问题处理，升级变更等或安全探测等例外场景，可申请一天，到期后取消。

➢ **申请流程:**

- 申请人按照模板填写申请，发送账号审批人审批，同时抄送帐号管理员。
- 账号审批人对账号/权限申请进行必要性、合理性审核，给出审核意见。
- 账号审批通过完成后，由帐号管理员创建帐号后分发给账号使用人。
- 账号使用人在使用帐号之前修初始密码。

说明：变更需要账号权限的，需要提交审核通过的变更号或变更审批通过的邮件给账号管理员，账号管理直接开通账号权限，不需要账号审批人审批。

➢ **注销流程:**

- 账号申请人发送邮件或者填写电子流系统说明员工离职/转岗邮件/不再使用账号。
- 账号管理人实施销户，回收账号权限。
- 账号管理人实施注销后向申请人、账号责任人和使用人反馈注销结果，并进行归档记录。
- 账号管理人定期审视/核对账号期限，对过期帐号进行通报，与业务主管和当事人确认后清理账号。

说明：

- 对一周或一天期限的账号，不需要进行通报及确认，由系统自动注销账号权限。
- 对离职人员，须确保在人员正式离职前，完成权限清理。

➢ **使用注意事项:**

- 账号的密码设置规则：必须由数字、字符和特殊字符组成；密码长度不能少于 8 个字符；设置密码时应尽量避开有规律、易破译的数字或字符组合作为自己的密码。
- 本着“谁使用、谁负责”的原则，账号使用人不得将账号借给他人，杜绝账号共享。
- 对于 30 天没有登录使用的账号，邮件知会账号使用人后可直接进行回收处理。
- 若发现秘密有泄密迹象或被入侵，账号管理员需立即汇报给账号负责人，重置密码并通知账号使用人，处理完成后将详细情况以书面报告方式上报给账号负责人
- 账号的密码需定期更换，更换周期不得超过 90 天。

5.4 云上运维

5.4.1 背景

在业务上云的大趋势下，运维方式将从传统 IDC 模式转换到以云为主体的运维模式上。云平台上丰富的产品、海量的资源、灵活的弹性能力、端到端的安全保障、开放的 API 和多样的计费模式加速了业务的发展速度，降低了企业的成本，但众多的选择下如何合理的配合和维护却是一个不小的挑战。

云端的运维并非简单将 IDC 的能力平移到云上就完事了，据行业统计，上云的企业用户能充分利用云端服务能力的占比不超过 20%，如何用好云、维护好云上的业务、保障数据安全、做好变更和故障的应对等，是企业上云必修的课题。

5.4.2 趋势和挑战

5.4.2.1 运维发展趋势

随着云计算和 AI 的普及，云运维也在持续的发展。我们总结了当前云运维发展的核心趋势：

1) AIOps 是后续运维发展的必然趋势，随着数据量的增长和环境变得更复杂，如何利用 AI、大数据助力运维的持续发展一直是非常热门的研究主题；
2) 云原生、微服务、容器化和分布式技术的普及，依赖人的运维模式将难以承载，自动化运维体系必然要具备更强大的问题追踪和定位能力；
3) 私有云、公有云、多云是很多企业的必然选择，跨云的运维保障体系也是必须的能力；
4) 运维的职能的范围在不断扩大，不仅需要做系统维护，同时需要考虑整体规划、高可用能力、安全体系等的合理构建，赋能研发和产品。

5.4.2.2 云运维的挑战

云时代的运维相比于传统的运维，有很多差异，下面大致梳理了这些差异点：

- **模式转变**

• 传统运维，大部分能力都需要自建完成，直接管理的是物理的计算、网络、存储等硬件资源，责任自担，可控度高，但能力构建缓慢、负担重、难度大。

• 云端运维，云服务提供标准的基础能力，用户需要充分利用云服务相关的能力组合构建自己所需的架构和运维能力，通过软件暴露的接口或者 OpenAPI 来管理抽象的资源，责任共担，底层资源不透明，但能快速构建能力、灵活度高。

- **范围变化**

• 传统运维，主要聚焦在自身 IDC 机房范围的维护，环境相对固定，熟悉度高；

• 云端运维，因不同企业 IT 发展程度和行业要求不一样，可能有线下 IDC、私有云、公有云，甚至是多云的环境，运维的环境变得复杂，对运维的管控能力和人员技能要求变高。

- **统筹能力**

• 相较于传统 IDC 模式，云端提供了丰富的产品和功能选择，虽然运维人员不需要关注底层的维护，但是需要熟悉云端的各类产品，才能合理的做出选择，并高效的利用。

- **安全风险**

• 云端资源大多基于逻辑隔离的模式，相较于 IDC 的物理隔离模式，安全风险会增加，

需要有合理的安全规划，如企业对数据安全的要求，云端存储需采用加密保护；

• 云端架构方案的设计灵活，大多数管理都是基于 OpenAPI 的模式，一条命令就能放通访问，所以在设计对外访问时需要考虑更多的安全控制，同时对风险命令要有严格的审计机制，确保风险可控。

➢ **故障排查**

• 云端故障的排查和定位层级更深，尤其是微服务化之后服务间的关系更加复杂，在云端更需要合理利用好相关的运维工具支撑故障的定位；

• 部分较深的故障问题需要联合云服务支持团队共同定位，人员沟通范围变大，需与云服务支持团队密切配合。

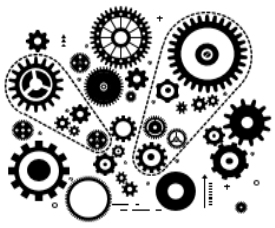
5.4.2.3 小结

综上，我们能看到云端运维能力越来越成为企业必然要具备的一种技能，云端运维人员的价值体现也会更加直观；企业上云后，如何持续深耕于云，充分利用云上的运维工具体系打造自身的运维能力将直接影响到业务的可用性和效率。

5.4.3 立体化运维

运维系统主要的目标是用来提供高质量的IT服务，从底层资源到上层应用，最终到用户体验，全方位监控系统的运行状态，并快速响应各类问题，保障业务长稳运行。云上运维随着业务形态、架构体系、资源模式和调用关系等的变化，对运维体系的管控规模和精细程度要求也越来越高。下面我们大致分析下这些方面的变化带来的典型运维述求。

1) 随着业务架构从单体、SOA到微服务化，服务数量呈指数级别的增长，更小粒度的服务带来了更快的迭代效率和原子化的精细管理能力，但庞大的微服务也给运维带来了管控规模和实效性的巨大挑战。

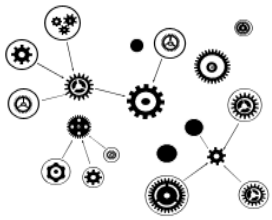


第一代：单体架构

- 紧耦合
- 系统复杂、错综交互，动一发而牵全身

第二代：SOA架构

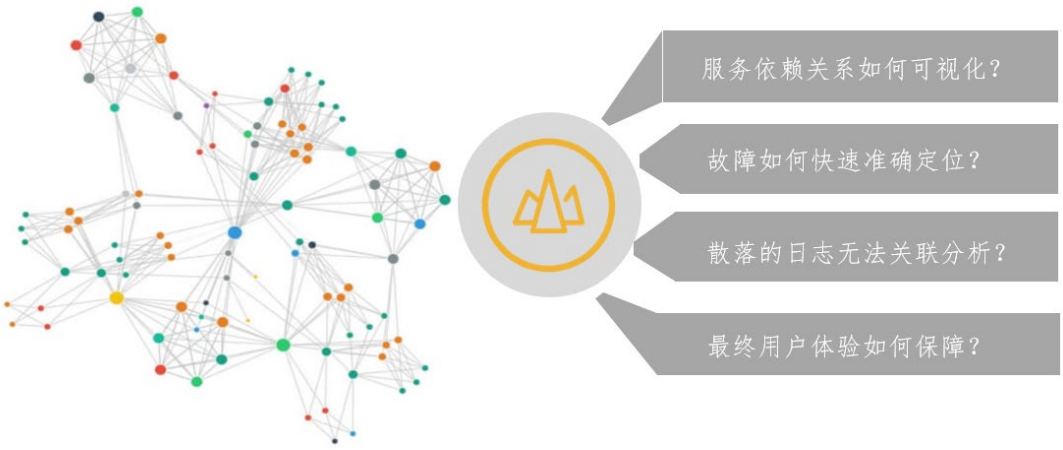
- 松耦合
- 在大型、超大型企业中仍然流行
- 通常通过ESB进行系统集成



第三代：微服务架构

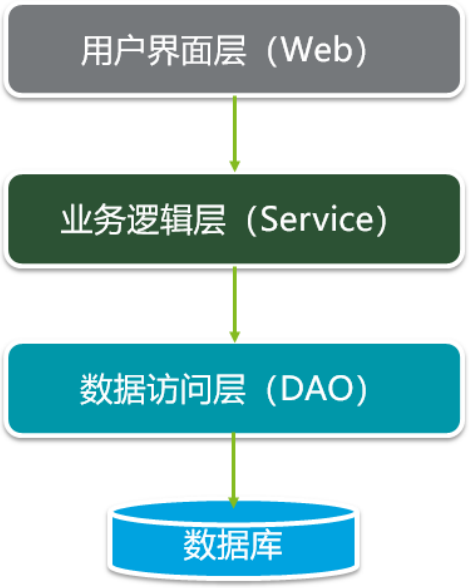
- 解耦
- TTM: 按天、周进行升级发布

2) 与此同时，云化大型的分布式的应用体系，让服务间的关系和调用层级也变得错综复杂，对各服务间的调用关系、调用质量、各环节的时延等信息需要有高效可视化的运维管控能力，能及时发现问题解决问题。



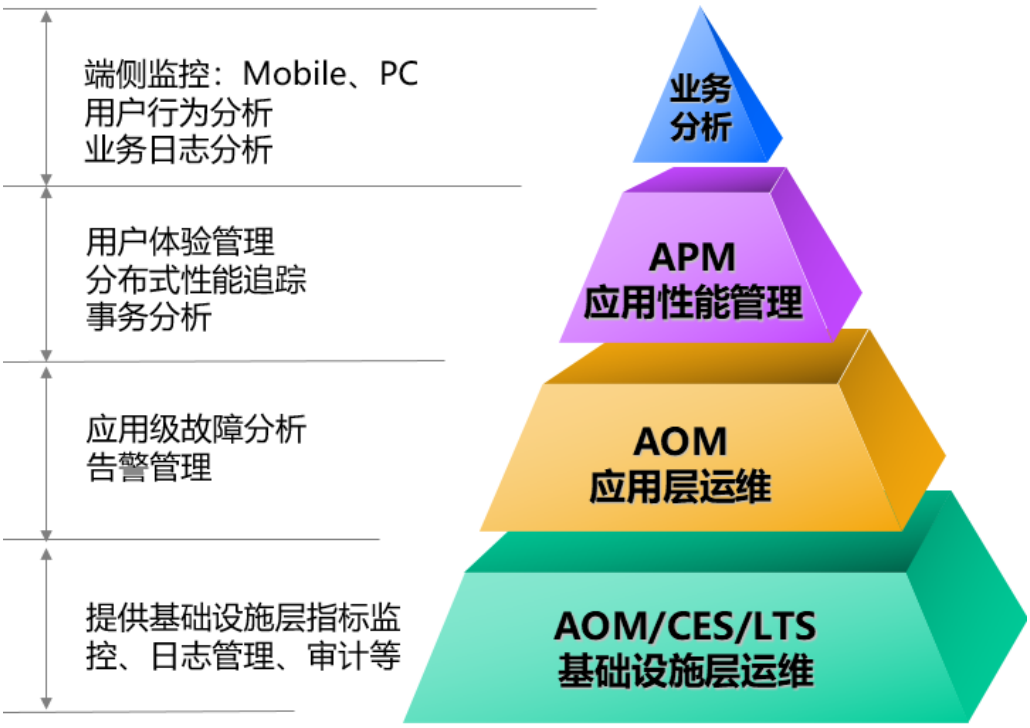
3) 应用微服务化之后，底层资源的载体也从物理机、虚拟机过度到了容器甚至Serverless的模式，服务的细化和规模大幅增长也带来了承载资源数量的指数级别增长，业务可能多种资源混合使用，这样导致运维需要管控的资源类型和资源规模环境也变得异常复杂，需要运维有精细化和规模化的管控能力，及时掌控资源的使用情况。

4) 当前应用架构都是分层架构，典型架构分为Web层、业务逻辑层、数据访问层和数据库层，一次访问往往需要跨越多个层级才能获取所需的数据，各层之间访问质量和串并行关系等需要有可视化的下钻上窜的链路质量监控能力，提升排障效率。



5) 最后，云上资源和服务纷繁复杂，账号和操作人员众多，各服务间的变更也会更加频繁，为保障系统整体的长稳运行，运维人员对云上的众多的资源必然要有强的管控和审计能力，在出现异常操作和预期外的变动时能及时发现和找到根因。

基于上述的运维述求，华为云构建了一套完整的面向云上应用的立体化运维系统，它融合了华为云的应用运维服务（AOM）、应用性能管理服务（APM）、日志采集和监控等能力，对虚机、存储、网络、数据库及应用等多维度实时监控，并通过应用与资源告警关联、日志分析、智能阈值、分布式调用追踪、手机 APP 异常分析等技术，实现分钟级问题快速诊断和修复，保障云上应用的长稳运行。



立体运维一站式完成基础设施层、应用层及用户体验层的监控，同时还具备完整的日志和

审计能力。

➢ **云监控（CES）**

云监控（Cloud Eye）服务为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。可全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

➢ **应用运维管理（AOM）**

应用运维管理（Application Operations Management）是云上应用的一站式立体化运维管理平台，实时监控应用及相关云资源，分析应用健康状态，提供灵活丰富的数据可视化功能，及时发现故障，全面掌握应用、资源及业务的实时运行状况。

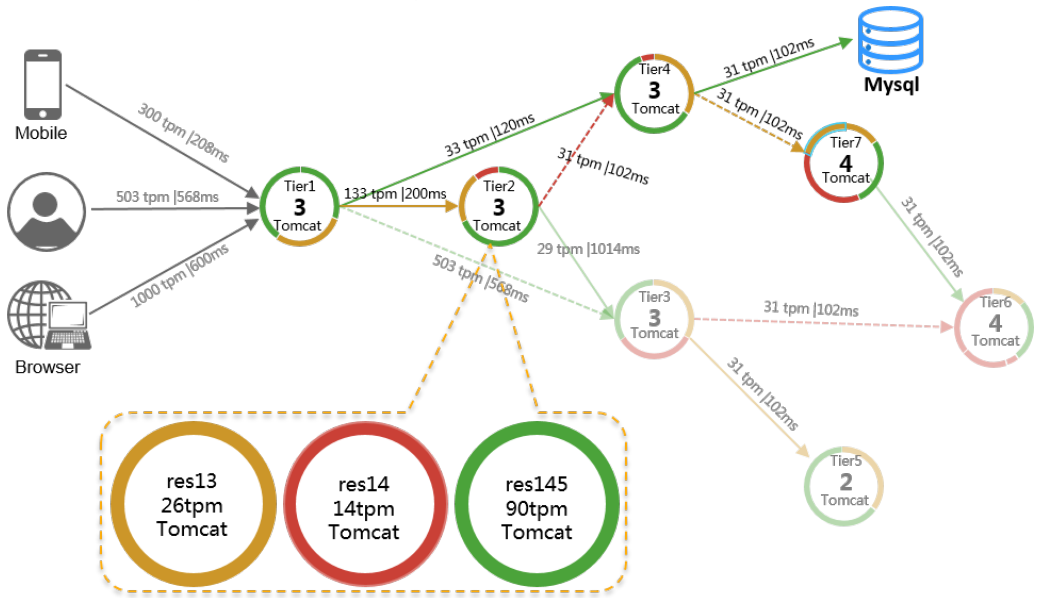
➢ **应用性能管理（APM）**

应用性能管理服务（Application Performance Management）包含应用监控和前端监控两大子产品，涵盖分布式应用、容器环境、浏览器、小程序、APP 等领域的性能管理，实现全栈式性能监控和端到端全链路追踪诊断，让应用管理轻松高效。

APM 可实现如下目标：

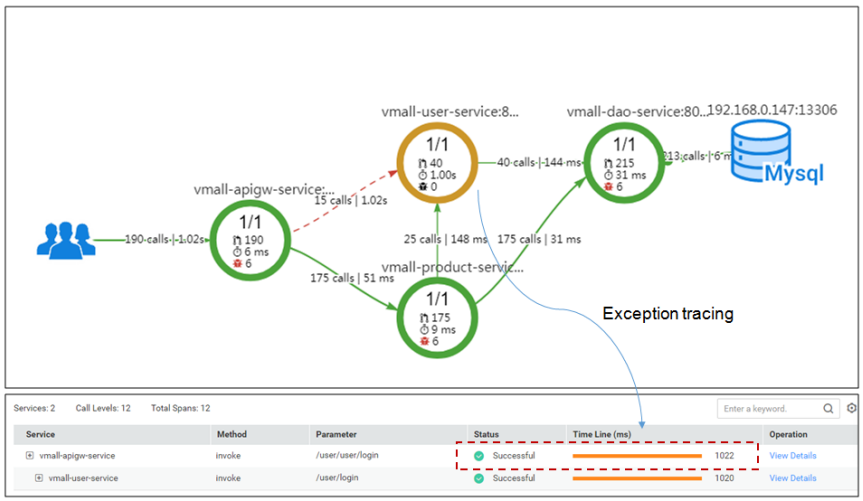
• **全链路拓扑：**调用关系与异常一目了然、故障下钻

全链路拓扑是对应用间调用关系和依赖关系的可视化展示，包括应用状态、时延、错误、负载、依赖关系等指标，支持数据库、缓存、消息中间件、NOSQL 等各类开源组件的情况。同时可以按照时间、服务、事务、Top 等维度进行筛选查看。在应用拓扑中，针对异常也可直接下钻查看调用关系，定位异常根因。



• **调用链追踪：**性能瓶颈与异常原因分钟识别

调用链跟踪、记录业务的调用过程，还原业务请求在分布式系统中的执行轨迹和状态，可以分钟识别异常原因。在业务方法被调用时，可自动捕获该方法的调用者、详细的堆栈以及各类参数，帮助开发人员快速锁定问题现场。



- **事务分析：**展示事务的吞吐率、错误率、时延等关键指标

APM 通过对服务端业务流实时分析，展示事务的吞吐率、错误率、时延等关键指标，使用健康指标 Apdex 对应用打分，直观体现用户对应用的满意度。当事务异常，则上报告警；对于用户体验差的事务，通过拓扑和调用链完成事务问题定位。如图 事务分析所示，以电商应用为例展示事务状况，健康指标异常的事务表示体验不佳。

事务URL	事务名称	吞吐率(次/分钟)	平均时延	健康指标	错误率	性能分析
hwid1.vmall.com/CAS/portal/login.html?validated=true	登录	52	323ms	正常	0%	调用链分析
hwid1.vmall.com/portal/search?id=34211223411	商品搜索	234	721ms	较慢	1%	调用链分析
hwid1.vmall.com/portal/buy?id=34211223411	购买	3	1.32s	正常	0%	调用链分析
hwid1.vmall.com/portal/pay?id=34211223411	支付	1	2.1s	异常	100%	调用链分析

➢ **云日志服务（LTS）**

云日志服务（Log Tank Service），用于收集来自主机和云服务的日志数据，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，为您提供实时、高效、安全的日志处理能力，可快速高效地进行实时决策分析、设备运维管理、用户业务趋势分析等。

下表我们列举了运维开源产品和华为云产品的对应关系。

大类	常用工具	华为云服务	功能
基础实施运维	Zabbix	CES	针对基础资源和实例进行监控、告警等。

	ELK	LTS	进行日志采集、分析、基于日志的告警和归档存储等。
应用层运维	Prometheus+Grafana	AOM	实时监控应用及相关云资源，分析应用健康状态，提供灵活丰富的数据可视化功能，帮助及时发现故障，全面掌握应用、资源及业务的实时运行状况。
应用性能管理	Zipkin/Pinpoint/Skywalking	APM	实时监控并管理应用性能和故障，提供分布式应用性能分析能力，帮助运维人员快速解决应用在分布式架构下的问题定位和性能瓶颈等难题。
业务监控	业务系统配套运维功能及业务日志	LTS	配套业务侧的监控、行为分析及业务日志分析等。

5.4.4 备份恢复

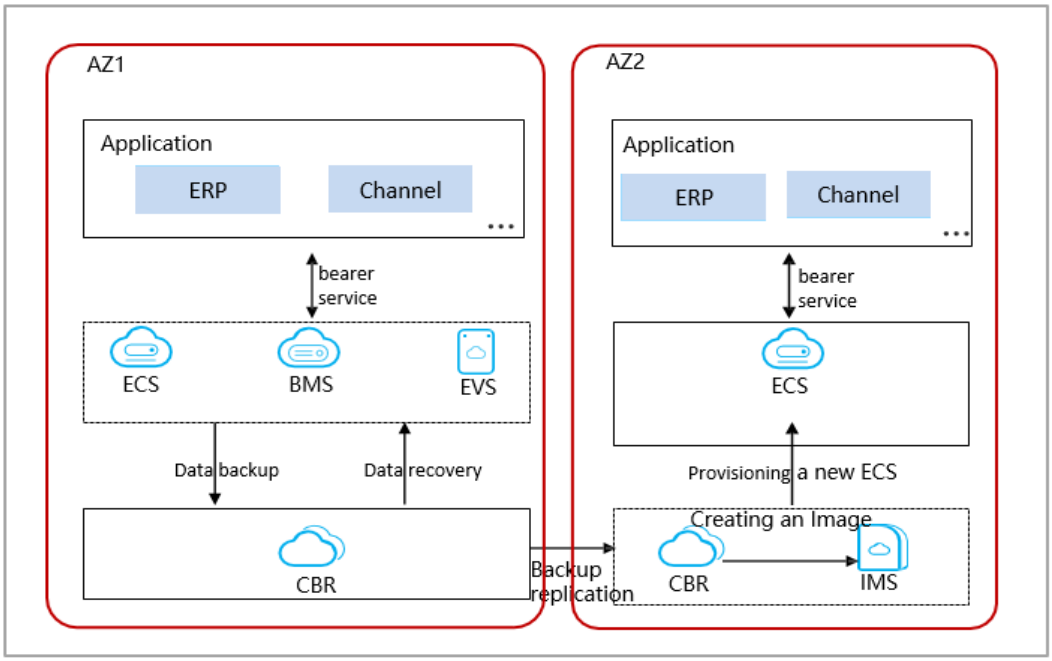
数据的安全是每个企业都非常关注的，业务上云后，云上的数据安全保障是不得不考虑的关键能力，华为云提供了全面的数据安全备份恢复保障体系。

- **概述**

对象	备份策略
云主机	使用云备份服务，基于快照技术，根据业务需求可以对云服务器进行整机备份，也可以针对系统盘和数据盘进行单独备份，备份策略可以根据时间点和周期进行配合使用。
数据库	• 针对云上数据库服务实例，**开启自动备份策略**后，会自动触发一次全量备份，之后会按照策略中的备份时间段和备份周期进行全量备份； • 实例在**执行备份**时，会将数据从实例上拷贝并压缩后上传到 OBS 备份空间，按照策略中的保留天数进行存放，备份时长和实例的数据量有关； • 自动备份策略开启后，实例每五分钟会自动进行一次**增量备份**，以保证数据的可靠性。
关键的业务数据（例如配置文件、关 键文档等）	关键业务数据可以**按文件的重要等级**以及**更改频率**进行备份周期和保留时长设置。建议将业务数据备份到 OBS 桶。

- **云主机备份和恢复**

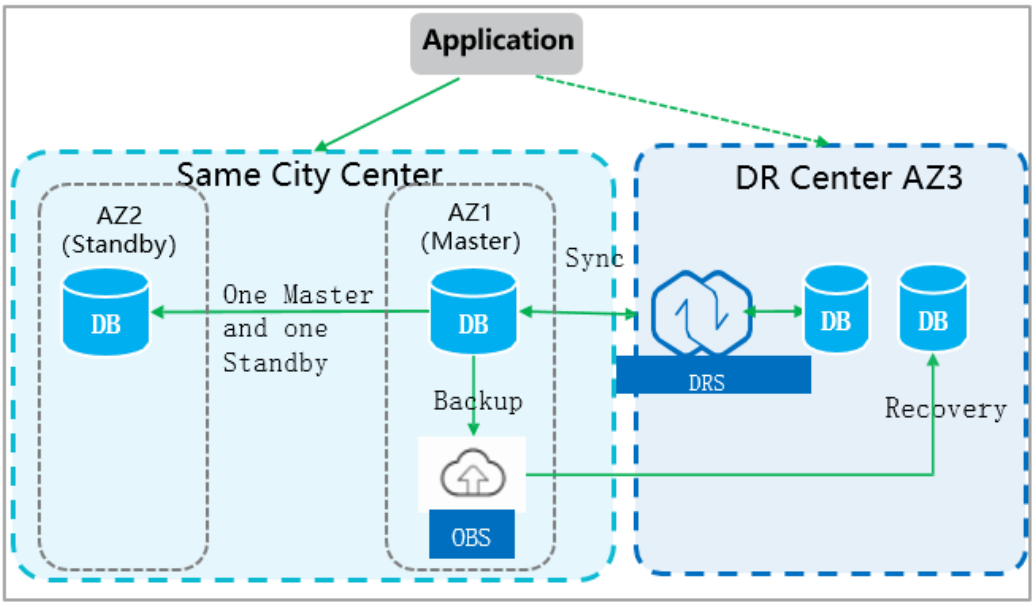
下图展示了华为云通过 CBR 来统一为 ECS、BMS、EVS 提供的备份支撑能力：



类别	用途	特性
备份（Backup）	云服务器备份	基于快照技术的备份，为云服务器包含的多个云硬盘的数据创建备份。
	裸金属服务器备份	基于快照技术的备份，将裸金属服务器包含的多个云硬盘的数据创建备份（仅支持 BMS 只使用 EVS 云硬盘的场景）。
	云硬盘备份	为单个云硬盘的数据创建备份。
恢复（Recovery）	备份数据恢复原云硬盘	将原云硬盘的数据恢复到指定备份点的状态。
	备份数据恢复原云服务器	将原云服务器的数据恢复到指定备份点的状态。
	备份数据创建新云硬盘	使用云硬盘备份数据创建新的云硬盘。
	备份数据创建镜像	使用云服务器备份数据创建镜像，再使用镜像发放新的云服务器。

- **数据库备份和恢复**

对于业务可用性要求比较高的场景，可通过同城双 AZ 主备，对象存储 OBS（冷备）或者数据传输服务 DRS（热备）构建异地灾备中心，实现两地三中心的数据安全保障机制。当 AZ1 和 AZ2 发生故障时，灾备中心依然可以保障数据的安全。



当数据库或表被恶意或误删除，备机数据库会被同步删除且无法还原，因此数据被删除后只能依赖于实例的备份机制保障数据安全：

- 自动备份：华为云数据库服务会在数据库实例的备份时段中创建数据库实例的自动备份，系统根据指定的备份保留期保存数据库实例的自动备份。
- 手动备份：根据指定的备份保留期保存数据库实例的手动备份，如果需要，可以将数据恢复到备份保留期中的任意时间点。
- 全量备份：对所有目标数据进行备份，全量备份总是备份所有选择的目标，即使从上次备份后数据没有变化。
- 增量备份：针对关系型数据库，系统每 5 分钟对上一次自动备份。

备份数据的恢复通过将 OBS 中保存的数据备份文件还原到数据库中实现，可以根据数据丢失情况结合全量和增量的备份文件，恢复数据到需要的时间点。此外，基于华为云 GaussDB 新的存算分离数据库架构体系（如 GaussDB For MySQL），可以提供快照技术的备份恢复能力，备份和恢复速度较传统逻辑备份和物理备份都有明显的提升（可参见官网说明），对客户的数据库做到 RPO 为零的保障。

云备份（Cloud Backup and Recovery 简称 CBR）为云内的云服务器、云硬盘、文件服务，云下文件、VMware 虚拟化环境，提供简单易用的备份服务，针对病毒入侵、人为误删除、软硬件故障等场景，可将数据恢复到任意备份点。详见：CBR 介绍。

5.4.5 变更管理

变更管理目的是规范生产环境变更管理活动（如申请、审核、调度、实施、验证等），明确申请、规范性审核和实施等变更活动的要求，确保变更活动充分准备，减少变更对业务的影响，保障变更成功，确保生产环境安全稳定地运行，并最大化的提升系统的可用性，满足所承诺的服务水平。

5.4.5.1 角色与职责

角色	职责定位
变更申请人 （维护工程师）	作为变更责任人： 负责按规范要求提交变更申请，确保变更信息正确。负责组织相关人员对变更结果进行验证、确认变更的执行结果。
变更经理 （运维负责人）	负责对变更申请进行规范性审核、分流、沟通和调度，督促变更实施责任人跟踪变更处理进展，关闭变更单。
变更评审组 （运维负责人、开发负责人）	负责对常规变更的方案和计划进行评审和决策。
变更实施人 （维护工程师）	负责按最终批准调度后的实施方案实施变更。

5.4.5.2 变更分类

- **紧急变更**

为了处理生产环境不可用或即将不可用而提出的计划外变更，来不及走正常流程进行评估审批的变更，如新暴露出来的版本缺陷导致用户使用过程中出现直接影响操作的问题。

- **重要变更**

针对业务系统的版本升级与操作维护，如在变更期间导致业务中断时长大于 30 分钟，变更前与受影响的用户沟通后执行。

- **一般变更**

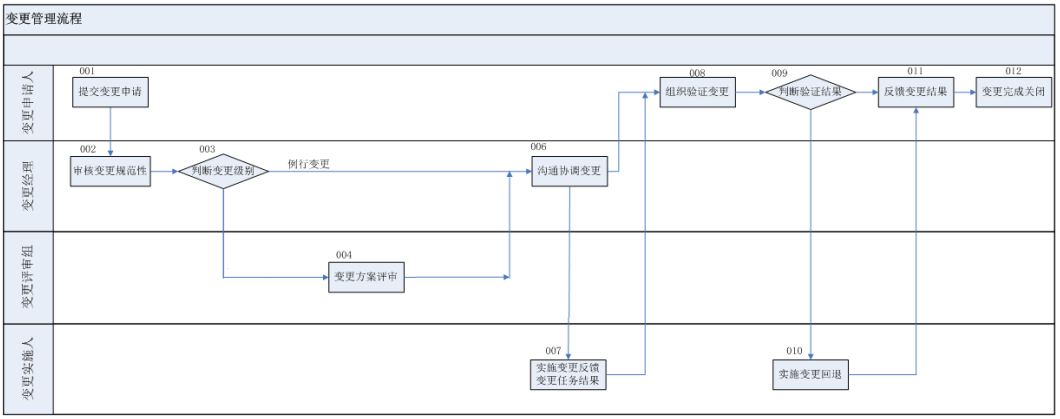
针对业务系统的版本升级与操作维护，如在变更期间导致业务中断时长小于 30 分钟，变更需同受影响用户沟通后执行。

- **例行变更**

指对于风险小、影响经运维部门与开发部门确认、操作步骤和实施角色固定、经多次（3 次以上）变更实施证明有效的生产环境变更，经过文档化和事先批准发布形成标准操作指导的低风险变更操作，不影响业务，升级过程中客户无感知的变更。

5.4.5.3 变更流程说明

➢ **流程示意图**



➢ **变更申请人提交变更申请**

变更前因素确定（不一定全部要有，如果没有，要能合理解释）：

- 原因和目的：变更的原因，表述实施变更的必要性；阐述变更的目的，必要时可简要说明概要方案，表述实施变更的可行性。
- 风险：描述实施变更可能带来的风险以及风险规避措施，同时不仅要考虑本系统、本领域的风险，还需要考虑对关联系统、关联领域的风险。
- 影响：描述实施变更具体带来确定性的影响，包括对客户、对其他领域的影响。
- 测试报告：变更前的测试过程，需要附上测试报告。

变更指导书明确表达如下几点：备份方案、实施方案、回退方案、验证方案。若变更对实施时间有特殊要求，需要变更申请人在提交变更时注明。

➢ **变更经理审核申请**

变更经理负责审核如下内容：变更时间窗、计划性、分类规范性审核。

- 变更申请时间是否满足计划性要求，如不满足，需要推迟变更以满足计划性要求，或者协助变更申请人走紧急变更审批流程处理。
- 变更类型分类选择是否合理，如紧急变更、重要变更、一般变更是否合理，变更的等级的准确性确认。
- 初步判断变更实施时间是否合理有效，并与变更申请人进行沟通、调整变更实施时间。

➢ **变更评审组评审变更方案**

- 变更原因和目的是否清楚。
- 变更风险是否描述清晰，应对这些变更风险的措施是否描述清楚。
- 变更影响是否描述清楚。包括在哪个时间段产生的对实际用户的影响和对生产环境的影响。
- 变更实施过程是否合适，操作步骤是否合理明确，是否能够达到正确的目的。

- 初步判断变更是否需要提供测试报告，是否已附上测试报告结果。
- 是否考虑了变更前临时备份、回退、验证方案。

➢ **变更经理调度变更**

- 主要关注多起变更之间是否有冲突（如时间冲突，变更内容冲突、组件关联等）、同时协助变更申请人关注变更与例行化操作、停机备份等运维操作是否有冲突。
- 对变更进行最终审批，给出最终是否允许变更实施的意见。

➢ **变更实施人实施变更**

- 任何变更必须经申请并得到最终批准调度后才能实施。
- 变更实施过程按照审批通过的方案进行实施。
- 变更实施过程中若发现不在变更方案计划内的服务下降或服务中断以及数据丢失，需要与变更经理联系，记录事件处理。
- 变更实施完成并验证后，变更实施人员按照实际情况反馈变更任务结果，包括变更实施结果和实际实施时间。

➢ **变更申请人验证变更**

- 由变更申请人按照变更方案中的验证方案进行验证，确认变更是否达到预期目的。若变更结果没有达到预期目的，需要反馈给变更实施人员。
- 变更验证人输出验证报告。
- 验证过程中若发现不在变更方案计划内的服务下降或服务中断以及数据丢失，需要与变更经理确认处理方法，记录事件处理。

➢ **变更实施人实施回退**

- 如变更结果未达到预期目的，变更实施人按照实施方案中的回退方案实施回退。如果在预定的时间窗内不能恢复系统服务，则按事件管理流程升级处理。
- 在变更时间窗内验证通过或变更时间窗内不能验证的变更，在变更结束后若发现需要回退需另外提交变更实施。

➢ **变更申请人反馈变更结果**

- 变更申请人必须在变更结束后及时反馈结果（如 2 个工作日内）。
- 若变更成功需要及时关闭工单。
- 若变更失败，需要反馈失败原因和改进措施，进行变更失败分析。

5.4.5.4 统计指标

➢ **变更成功率**

每月成功变更数与总变更数的比值，成功变更数指的是关闭变更时状态为成功的变更数。

计算公式：（成功变更数/总变更数）*100%。

➢ **变更导致服务意外中断次数**

每月变更导致业务意外中断的次数。

计算公式：每月累积所有变更导致服务意外中断的次数

➢ **中断业务变更率**

每月申请过中断业务变更占总变更数的百分比。

计算公式：（中断业务变更数/总变更数）*100%

➢ **紧急变更率**

每月申请过紧急变更的模块所申请的紧急变更次数，占总变更数的百分比。

计算公式：（紧急变更数/总变更数）*100%。

5.4.6 应急处置

规范各类事件的受理、处理、升级工作，确保客户问题高效处理，维持承诺的服务水平，明确相关领域对各类事件处理的职责，规范各类事件受理时限、通报工作。在不影响业务的情况下，尽可能快速的恢复服务，保障业务的稳定性，确保服务质量和可用性能够满足给客户的承诺。

➢ **角色与职责**

角色名称	职责
运维工程师（各维护工程师）	• 作为客户事件统一接口，受理客户通过热线电话、邮件等提交的事件； • 负责完整记录所有接收的事件信息，包括：记录事件报告人的详细联系方式、事件特征表现、描述、发生时间等； • 根据案例或相关操作指导书，对用户事件进行初步诊断、分析，提供解决方案。对于不能解决的事件，传递给对应的开发人员支持，不确定开发范围时可求助运维负责人； • 负责事件首问跟踪，跟催记录传递事件的处理进度，检查事件记录的处理进度，保持与用户的联系，根据客户需求通知事件处理进展； • 负责解决事件，对事件进行定位、定界，在指定时间内提供有效的解决方案；对于事件无法解决时，在规定的时间内，将事件传递给最合适的开发人员； • 对于提供解决方案的事件，负责与事件提出人沟通确认事件是否解决，并关闭事件； • 负责将重复发生、根因不明或已知缺陷的事件，转入问题管理流程； • 针对典型、共性事件，总结形成案例。
开发人员（各开发工程师）	• 对运维工程师传递的事件进行定位、分析，提供并实施解决方案； • 对于提供解决方案的事件，负责与跟踪人沟通，确认事件是否解决； • 负责解决生产环境的 BUG 类事件定位、给出彻底解决方案并实施。
事件经理（运维责任人）	• 负责对系统平台日常事件处理的整体协调和监控； • 负责对重大事件的解决协调资源，保障故障事件的最终排除； • 负责对重大事件的技术方案进行评审和决策； • 负责跟进重大事件的报告输出。

➢ **事件定级和响应要求**

1 级事件：对业务有严重的影响，如业务严重受损无法提供服务、丢失业务数据、业务数据或功能批量出错（导致大量客户投诉）、短期内反复出现的系统故障等。

2 级事件：对业务有较小的影响，如业务系统丧失了较少的服务功能（服务降级）、个别用户某些功能受到影响、个别数据出现不一致（未造成资金损失）、一般性系统故障等。

3 级事件：对业务没有影响，如数据查询或业务咨询、业务可正常使用但体验有影响等。

事件优先级对应的响应时限和解决时限（注：7x24 工作时间，从接收到事件开始计算时间）：

事件级别	响应时间	恢复时间	解决时间
1 级事件	10 分钟	2 小时	7 天
2 级事件	30 分钟	6 小时	20 天
3 级事件	60 分钟	24 小时	60 天

备注说明：

- 上表事件级别及应对时间要求只是示例，具体定义可根据企业实际情况调整。
- 运维工程师根据案例或操作指导对事件进行处理，规定时间内不能解决则进行传递。
- 响应时间：是指事件处理人从受理事件到着手处理事件所花费的最长时间。
- 恢复时间：是指事件发生到业务恢复之间的时间。
- 解决时间：是指运维工程师着手处理事件到事件被解决或传递出去的时间。

➢ **事件升级通报机制**

3 级事件不定义通报，1 级、2 级事件的通报机制如下：

关键点	通知方式	通知对象
首次通报（30 分钟）	短信和邮件	故障服务 Owner（邮件主送） 运维团队
	电话	开发负责人
进展通报（1 小时）	短信和邮件	故障服务 Owner（邮件主送） 运维团队
故障恢复	短信和邮件	故障服务 Owner（邮件主送） 运维团队
超期升级通报	短信和邮件	故障服务 Owner（邮件主送） 运维团队 开发负责人
	电话	开发负责人

根据运维事件的发展对业务造成的影响以及对用户和业务的影响，2 级事件可以升级为 1 级事件，升级后遵从 1 级事件标准跟踪处理。

➢ **事件管理注意事项**

- 现网处理的所有事件，必须进入统一的事件管理系统进行记录，以便分析。
- 严格在各级别事件规定的时间目标内响应事件、恢复事件。
- 每月对处理的事件进行汇总分析。

5.4.7 运维服务

5.4.7.1 服务介绍

企业上云后会面临哪些常见的维护问题？大致列举如下：

- 故障如何处理：使用云产品过程中的问题定位和故障排除需要协助；
- 云运维经验不足：缺少云运维人员和相关经验；
- 业务不稳定：系统频繁宕机、崩溃如何优化；
- 需要专项保障：重大活动期间需要保障业务的稳定和连续运行；
- 如何预知风险：需要周期性针对云资源进行健康检查，了解业务整体健康度。

基于此类述求，华为云运维服务在充分吸收华为云上优秀客户最佳实践的基础上，推出了四项运维服务，包括：健康检查服务、辅助运维服务、提升服务、云上保障护航服务。

- 健康检查服务：协助客户分析运行指标并评估系统的效率、健壮性和安全性；
- 辅助运维服务：遵循华为云最佳实践，为客户提供驻场运维服务支持，保障业务连续性；
- 提升服务：全链路分析业务现状并结合华为云最佳实践，提供优化建议，提升客户业务稳定性；
- 云上保障护航：在业务推广大促、重要节日、上线开服和云展会等活动期间，为客户业务保驾护航，稳定度过业务高峰。

具体服务流程包括：

- **服务申请**

- 客户提交服务申请；
- 交付经理评估客户需求；
- 交付经理对齐服务目标和服务范围；
- 客户下单。

- **服务实施**

- 交付人员按照服务内容交付；

- 交付人员向客户提供交付件。

➢ **客户验收**

- 客户验收并对服务进行评价。

5.4.7.2 客户案例

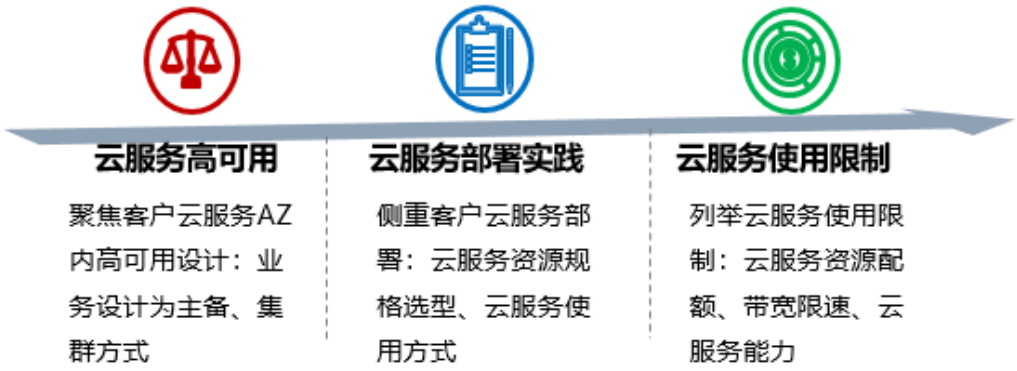
【案例 1】**健康检查**

J 客户是中国领先的应用软件产品和服务供应商，以”云服务为基础，多屏、内容为辅助，AI 赋能所有产品”的方式，为个人及企业提供办公业务。

客户 20 年 6 月份累计发生了 2 起故障，业务中断达 210 分钟，故客户对华为云稳定性产生强烈诉求，在此背景下，华为专家开始介入，帮助客户检查业务情况。

健康检查（覆盖 35 个云服务， 240 个检查项）聚焦如下几个方面，进行精细化管理：

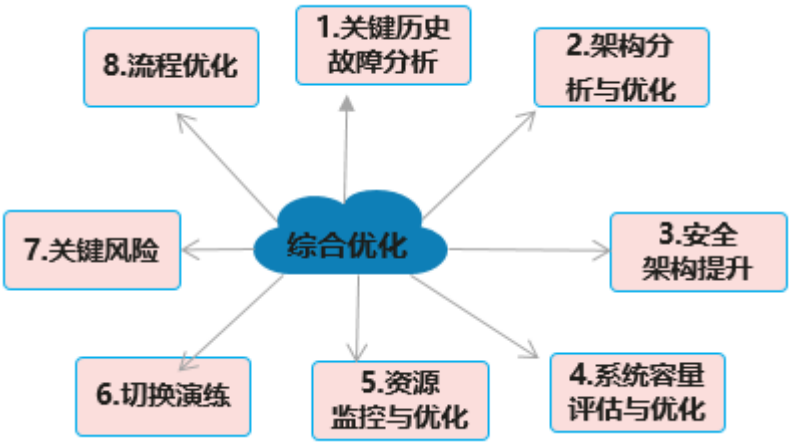
➢ 云服务使用限制
➢ 云服务部署实践
➢ 云服务高可用



健康检查服务共识别 N 个风险项，涉及 ECS、WAF、堡垒机等云产品，如系统核心业务未跨 AZ 部署，存在单 AZ 故障业务不可用的风险，建议后期新增资源按跨 AZ 部署，提升可靠性。客户按建议改进后，故障影响明显下降，稳定性得到大幅提升。

【案例 2】**提升服务**

MX 为首个上市公司全量业务搬迁到华为云平台的核心客户，该客户在全球拥有激活设备超过 18 亿台，月均活跃用户 2.X 亿，年云服务消费 XXXX 万元；随着客户业务全量搬迁上云后，一些潜在故障、访问异常等影响核心业务的问题逐步显现，其中含有部分客户业务中断事件，严重影响了客户业务的连续性与稳定性。



于是我们结合客户业务特点，从故障、架构、安全、容量、风险和流程等方面进行了全面的体检和能力提升改造，收益如下：

- 通过切换演练，验证了客户业务高可用能力，并通过切换演练建立客户侧逃生通道；
- 通过监控优化，覆盖业务关键告　警指标，快速发现并定位问题，减少业务中断风险；
- 保障期间按照客户诉求与日常负载分析，评估客户容量模型规划，并进行资源扩容，保障业务连续性；
- 圣诞节+元旦+春节保障期间业务稳定运行未出现重大故障，三节保障圆满完成，得到运维总监和 CTO 的一致好评。

【案例 3】**保障护航**

WAIC2021 由上海市政府与国家发展改革委、工信部、科技部、国家网信办、中科院、工程院、中国科协共同主办的全球化、专业化、综合性的世界级人工智能盛会。

华为云作为 WAIC2021 战略合作伙伴，秉承支撑客户上好云、用好云、管好云，确保云上业务 “零”中断、“零”故障、“零”投诉的目标，为本届大会提供全面的云技术支持和服务保障。

保障工作结束后，获得了客户如下评价：

- 客户 X 总在直播采访中，说到：“平台升级为三朵云（云会场、云展览、云直播）是初次尝试与磨合，其中云技术可靠性保障依赖华为云保障团队，他们在这个领域有着很强的技术实力，保障了三朵云会议期间的稳定性”；
- 通过现场+远程保障，在访问量 8000 万+、直播论坛 100 场+的高峰业务期间实现业务“零”中断、“零”故障、　“零”投诉，助力展会成功；
- 多资源云上服务化部署，风险转接减轻客户运维压力。

6 结束语

CAF 白皮书是基于华为云上众多客户的上云案例和自身的 IT 建设实践所总结的上云策略，分上云规划、云上建设、云上运行、云上治理和运维四个部分，为企业上云提供业务规划、准备、架构、组织、管理和运维运营等方面的全面引导，旨在为企业业务平稳上云、云上高效运行提供帮助，同时让上云和用云风险最小化，价值最大化。

如果您在查阅此白皮书过程中有任何的意见和建议，我们真诚的欢迎您将意见反馈到官网，我们将不断改进。

7 延伸阅读

有关更多信息，请参阅：

企业应用现代化白皮书
企业上云安全白皮书
云上 IT 治理最佳实践
DevOps 最佳实践
云容器引擎 CCE 最佳实践
主机迁移服务 SMS 最佳实践
数据复制服务 DRS 最佳实践
云数据迁移 CDM 最佳实践
对象存储服务 OBS 最佳实践
异构数据库迁移 UGO 最佳实践

