云采用框架

云采用框架与实践

文档版本	01
发布日期	2025-01-21

华为技术有限公司

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 云采用框架简介 1
1.1 概述 1
1.2 整体框架 1
1.3 目标读者 4
1.4 常用术语 4
1.5 缩略语 7
2 制定战略 11
2.1 概述 11
2.2 干系人利益分析 11
2.3 识别云化驱动力 15
2.3.1 云化驱动力简介 15
2.3.2 业务驱动力 15
2.3.3 技术驱动力 16
2.3.4 财务驱动力 18
2.3.5 多云战略的驱动力 20
2.3.6 如何识别驱动力 20
2.4 评估云化成熟度 22
2.4.1 评估云化成熟度的意义 22
2.4.2 云化成熟度评估模型 23
2.4.3 云化成熟度评估步骤 26
2.5 制定云化目标 27
2.6 分析云化收益 29
2.7 制定云化转型战略 32
2.8 战略制定的反模式 34
3 顶层规划 36
3.1 概述 36
3.2 云卓越中心 36
3.2.1 云卓越中心简介 37
3.2.2 指导委员会 38
3.2.3 应用团队 39
3.2.4 云架构团队 40
3.2.5 云实施团队 41

3.2.6 云运维团队 43
3.2.7 云安全团队 44
3.2.8 云治理团队 45
3.2.9 FinOps 团队 47
3.2.10 云项目经理 48
3.2.11 云卓越中心的演进 48
3.3 卓越架构设计 49
3.4 Landing Zone 设计 51
3.4.1 全面云化的 IT 治理挑战 51
3.4.2 为什么需要 Landing Zone 52
3.4.3 Landing Zone 设计原则 53
3.4.4 Landing Zone 参考架构 54
3.4.4.1 公司 IT 治理架构 54
3.4.4.2 组织和账号设计 56
3.4.4.3 整体架构设计 60
3.4.4.4 身份和权限设计 62
3.4.4.5 整体网络架构 65
3.4.4.6 公共服务管理 69
3.4.4.7 多账号统一管理 69
3.4.4.8 数据边界 73
3.5 安全架构设计 74
3.5.1 安全架构设计简介 74
3.5.2 安全责任共担 74
3.5.3 安全设计原则 76
3.5.4 安全参考框架 78
3.6 平台工程 79
3.6.1 什么是平台工程 79
3.6.2 如何构建平台工程 80
3.7 云运营模式 81
3.7.1 什么是云运营模式 81
3.7.2 去中心化运营模式 82
3.7.3 集中化运营模式 83
3.7.4 赋能和协同运营模式 85
3.8 应用生命周期管理 87
3.9 云项目管理 90
3.10 顶层规划的反模式 93
4 调研评估 95
4.1 概述 95
4.2 组建调研评估团队 96
4.3 基础设施调研 97
4.4 应用系统调研 97
4.4.1 调研应用全景图 98

4.4.2 调研应用部署架构 98
4.4.3 调研应用关联关系 101
4.4.4 调研应用上云需求 105
4.5 大数据调研 106
4.5.1 平台调研 106
4.5.2 数据调研 107
4.5.3 任务调研 108
4.6 调研方式 109
4.7 云服务选型 111
4.7.1 计算服务选型 111
4.7.2 存储服务选型 113
4.7.3 网络服务选型 117
4.8 调研评估的反模式 117
5 方案设计 119
5.1 概述 119
5.2 组建方案设计团队 120
5.3 基础环境设计 120
5.4 应用架构设计 121
5.4.1 应用部署架构概述 121
5.4.2 可用性设计 122
5.4.2.1 可用性定义 122
5.4.2.2 AZ 故障域说明 123
5.4.2.3 云上高可用方案 123
5.4.2.4 双 AZ 高可用设计 124
5.4.2.5 两地三中心高可用设计 125
5.4.2.6 跨 AZ 高可用设计示例 127
5.4.3 可扩展性设计 131
5.4.3.1 云上可扩展性 131
5.4.3.2 可扩展设计 132
5.4.4 性能设计 133
5.4.5 应用部署参考架构 133
5.4.5.1 应用部署架构示例 133
5.4.5.2 参考架构库 135
5.5 大数据架构设计 136
5.5.1 设计原则 136
5.5.2 大数据集群设计 137
5.5.3 大数据任务调度平台设计 137
5.5.4 大数据参考架构 138
5.5.5 华为云大数据组件 139
5.6 制定 6R 策略 140
5.7 设计标签方案 142
5.7.1 简介 142

5.7.2 标签最佳实践 143
5.7.3 典型使用场景 144
5.8 上云试点 145
5.8.1 为什么要上云试点 145
5.8.2 如何选择试点应用 146
5.8.3 上云试点执行与总结 147
5.9 批次规划 148
5.9.1 概述 148
5.9.2 迁移批次规划的方法 149
5.9.3 大数据迁移批次规划说明 151
5.10 成本预算计划 152
5.11 方案设计的反模式 153
6 采用实施 154
6.1 概述 154
6.2 组建实施团队 155
6.3 基础设施部署 156
6.4 应用迁移上云 156
6.4.1 应用迁移上云简介 157
6.4.2 设计迁移方案 159
6.4.2.1 迁移方案概述 159
6.4.2.2 接入层迁移方案 160
6.4.2.3 应用层迁移方案 161
6.4.2.4 中间件层迁移方案 162
6.4.2.5 数据层迁移方案 164
6.4.3 设计切换方案 166
6.4.3.1 如何选择停服不停服 166
6.4.3.2 停服切换方案 168
6.4.3.3 停写不停读切换方案 175
6.4.3.4 不停服切换方案 178
6.4.4 设计 Runbook 179
6.4.4.1 Runbook 设计原则 179
6.4.4.2 Runbook 角色设计 180
6.4.4.3 Runbook Checklist 设计 180
6.4.4.4 Runbook 操作步骤设计 181
6.4.4.5 Runbook 参考模板 182
6.4.5 部署 184
6.4.5.1 云资源开通及配置 184
6.4.5.2 迁移工具部署 186
6.4.6 迁移 186
6.4.6.1 接入层迁移实施 186
6.4.6.2 应用层迁移实施 187
6.4.6.3 中间件层迁移实施 190

6.4.6.4 数据层迁移实施 193
6.4.6.5 迁移实施常见问题 197
6.4.7 验证 197
6.4.7.1 数据验证 197
6.4.7.2 业务验证 199
6.4.8 切换 206
6.4.8.1 切换演练 206
6.4.8.2 正式切换 209
6.4.9 保障 214
6.5 大数据迁移 215
6.5.1 调研 215
6.5.2 设计 216
6.5.3 部署 220
6.5.4 迁移 221
6.5.5 验证 224
6.5.6 切换 224
6.5.7 保障 225
6.6 应用现代化 226
6.6.1 什么是应用现代化 226
6.6.2 基础设施现代化 227
6.6.3 应用架构现代化 228
6.6.4 开发与运维现代化 230
6.6.5 治理与运营现代化 231
6.7 云上创新 231
6.7.1 概述 232
6.7.2 人工智能 232
6.7.3 大数据 232
6.7.4 区块链 233
6.7.5 元宇宙 233
6.7.6 物联网 234
6.8 采用实施的反模式 234
7 运维治理 236
7.1 概述 236
7.2 精益化治理 236
7.2.1 概述 236
7.2.2 组织分级分域管理 237
7.2.3 精细化权限控制 238
7.2.4 集中化 IT 管理 239
7.2.5 全方位数据边界 240
7.2.6 精细化成本运营 242
7.3 确定性运维 242
7.4 安全运营 243

7.4.1 概述 243
7.4.2 安全运营框架 245
7.4.3 安全配置基线 246
7.4.4 软件工程安全 246
7.4.5 人员安全管理 248
7.4.6 云原生安全服务 249
7.5 FinOps 251
7.5.1 概述 251
7.5.2 FinOps 参考架构 253
7.5.3 成本计划 254
7.5.4 成本控制 255
7.5.5 成本分析 256
7.5.6 成本优化 257
7.6 持续优化 258

1 云采用框架简介

1.1 概述

云计算从根本上改变了IT基础设施和应用系统的建设、运维和管理方式。传统模式下，组织通常需要购买、安装和运维自己的硬件和软件，包括服务器设备、存储设备、网络设备、虚拟化软件、操作系统、数据库管理软件和中间件等IT基础设施，资源部署周期长，运维负担重，初始投资大。

云计算模式下，IT基础设施的建设和运维由云服务商负责，组织只需关注应用系统的开发和部署，可以从云服务商按需获取上述各种资源，资源可以快速部署、调整和扩展，运维负担轻，并大幅降低了初始投资。云计算提供了巨大的灵活性、可靠性和扩展性，但整个组织的云化转型是一项系统性工程，涉及组织、流程和技术的方方面面，您的组织需要一个成熟且一致的方法确保云化转型的成功，最大化业务收益。

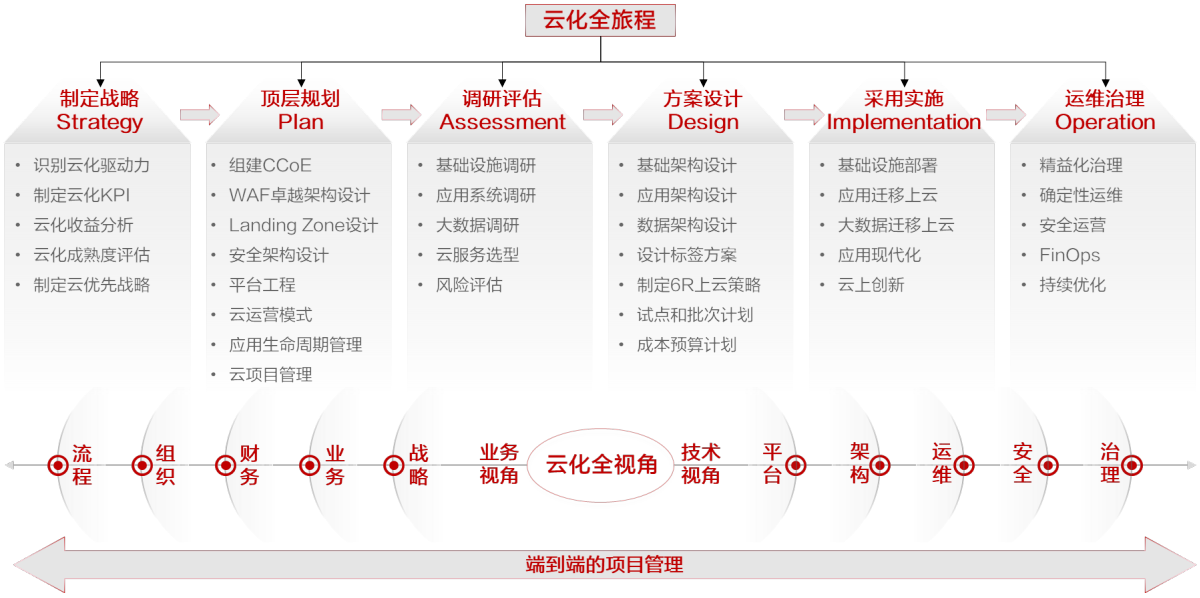
华为云云采用框架（Cloud Adoption Framework，简称CAF）是一个针对云化转型的端到端生命周期框架，涵盖云化旅程的所有阶段，包括制定战略、顶层规划、调研评估、方案设计、采用实施和运维治理。CAF提供了云化旅程各个阶段的方法论、最佳实践、工具和模版，可以帮助业务决策者、IT决策者、财务专家、运维专家和安全专家等干系人在云化旅程各个阶段做出正确决策，充分发挥云计算的价值。遵循CAF的最佳实践可让您的组织更好地对齐业务和技术战略，确保云化转型的成功。

CAF提供的方法、最佳实践、工具和模版来自于华为云、合作伙伴和客户上云、用云和管云的经验，华为云会持续基于不断积累的云化转型经验和认知升级对CAF进行迭代刷新，确保CAF提供的方法、最佳实践、工具和模版能够与时俱进。

1.2 整体框架

华为云CAF提供系统的和完整的云化转型方法论和最佳实践，CAF的完整性体现在两个方面，一要涵盖云化转型的全部旅程，二要涵盖云化转型所有干系人的视角。CAF的整体框架如下图所示。

图 1-1 CAF 整体框架



云化全旅程按照时间顺序包含以下六个阶段。

1. **制定战略**：制定云化转型的战略，这个战略要与组织的业务战略和技术战略保持对齐，确保云化转型能够实现组织的业务目标。在该阶段需要分析干系人利益、识别云化驱动力、评估云化成熟度、制定云化目标和分析云化收益，然后制定符合组织业务战略的云化转型战略。
2. **顶层规划**：云化转型是一项系统性工程，不是简单的将应用系统迁移到云上，需要基于组织的云化转型战略有针对性的设计云化转型的顶层框架，从组织、流程和技术方面整体考虑。在组织层面需要组建一个云卓越中心（Cloud Center of Excellence，简称CCoE）来领导、协调和推进整个云化转型项目。在技术层面需要基于卓越架构（Well-Architected Framework，简称WAF）设计Landing Zone、安全架构和平台工程。在流程层面需要根据组织的IT运营模式设计最佳的云运营模式，并基于云运营模式制定应用生命周期管理流程，最大化云计算带来的业务价值。
3. **调研评估**：针对组织的IT基础设施、应用系统和大数据平台进行现状调研，包括静态配置信息和动态运行信息的收集和分析，针对现状信息进行评估分析，选择正确的云服务，为后续详细方案设计提供有效输入。
4. **方案设计**：在云化转型的顶层设计框架内，基于调研评估结果，再结合组织的业务架构和WAF框架，详细设计云上技术架构、云上应用架构和云上数据架构，通过卓越的架构设计保障云基础设施和应用系统的安全性、可靠性和高性能。在该阶段需要根据应用系统的重要性制定POC试点和批次迁移计划，根据应用系统的特征选择合适的迁移策略，同时也需要制定云上的成本预算计划，最终整合输出详细设计方案。
5. **采用实施**：基于详细设计方案，首先要搭建Landing Zone，部署可扩展的网络基础设施，配置安全基线和运维基线；然后将各个应用系统和大数据平台迁移或直接部署到云上，或者基于云平台进行应用现代化改造，也可以基于云平台提供的各种创新技术直接在云上进行应用和业务创新。
6. **运维治理**：将应用系统迁移或部署到云上之后就进入了运维治理阶段，在该阶段需要针对云基础设施、应用系统和大数据平台进行持续的精益化治理、确定性运维、持续安全运营和成本运营，并基于WAF框架进行持续优化。

云化转型项目涉及组织内很多部门和干系人，这些干系人会参与云化转型项目的决策或影响云化旅程的各个阶段。如表1-1所示，不同的干系人有不同的视角和关注点，这些视角总体分为业务视角和技术视角。

华为云CAF会针对所有这些视角给出恰当的建议，您的组织可以将这些建议作为决策和行动的起点，结合组织的业务特点和偏好制定有针对性的行动方案。

表 1-1 云化全视角

分类	视角	关注点	干系人
业务	战略视角	• 基于云化转型项目支撑组织的业务战略和数字化战略，充分利用云计算的优势构建组织的核心竞争力。	CXO高级管理人员
业务	业务视角	• 提升业务连续性，支撑业务的持续发展； • 加速新业务上市速度，快速满足不断变化的市场需求； • 基于云上创新技术进行业务、产品或模式创新，为组织带来增量收益。	业务主管、CIO
业务	财务视角	• 云采用前后的TCO对比分析，降低IT的TCO； • 不断优化云资源的性能效率和成本效益； • 通过提升用户体验和业务创新带来新增收入。	CFO、财务专家
业务	组织视角	• 搭建云化转型的组织结构，定义云化转型人才的角色和职责； • 制定云化转型的绩效考核指标，云化转型人才的选、用、育、留。	CIO、HR专家
业务	流程视角	• 基于云平台和云服务的特点优化IT服务流程和运维流程，支撑上层应用系统的快速迭代和安全稳定运行。	CIO、IT主管
技术	平台视角	• 基于云平台和云服务构建企业级、高安全、高可靠、高性能和易扩展的IT基础设施或技术平台，对上层应用系统提供计算、存储、网络、安全、数据库、中间件等服务，帮助应用团队快速基于该平台进行应用系统的开发、测试、部署和高效运维，并支撑应用系统的安全稳定运行。	CIO、CTO、IT主管、IT运维专家、应用开发及测试专家、应用运维专家
技术	架构视角	• 基于云平台和云服务构建高安全、高可靠、高性能和易扩展的技术架构、应用架构和数据架构。	CTO、云架构师
技术	运维视角	• 基于云平台和云服务的特点构建完善的云上IT运维体系，针对IT基础设施和应用系统进行监控、告警、故障定位和故障修复，保障IT基础设施和应用系统的长期稳定运行。	CTO、IT运维专家、应用运维专家

分类	视角	关注点	干系人
技术	安全视角	● 基于云平台和云服务的特点构建云上全方位安全防护体系和持续安全运营机制，保障IT基础设施和应用系统的机密性、完整性和可用性。	CISO、安全专家
技术	治理视角	● 基于云平台和云服务的特点构建完善的云上IT治理体系，针对云上的“人财物权法”进行集中化和精益化的治理，有效控制云化转型的风险，最大化业务收益，保障业务的持续发展。	CIO、IT治理专家

云化旅程是一个长期和复杂的过程，涉及的人员庞大，要处理的任务非常繁多，企业要安排专门的项目经理对其进行端到端的项目管理，科学的项目管理方法和行动方案直接影响云化转型的效率和质量，最终将会影响云化转型战略目标的实现。

华为云CAF的目录结构按照云化全旅程的六个阶段展开，在相应的章节会展开介绍各个业务视角和技术视角的关注点和对应的实践建议。

1.3 目标读者

如整体框架所述，CAF的内容涵盖云化全旅程和云化全视角，涉及到了组织内不同部门的不同角色，以下角色能从CAF中找到跟自身职责相关的指导，这些角色可以将这些指导作为决策和行动的起点。

- CXO（包含CEO、CIO、CTO、COO、CFO等）
- 业务主管
- IT主管、技术主管
- 财务专家
- 人力资源主管
- 云架构师、应用架构师、数据架构师、网络架构师
- IT治理专家
- 运维主管、IT运维专家
- CISO、安全专家、合规审计专家
- 应用开发专家、应用测试专家
- 应用运维专家
- 迁移实施工程师
- 项目经理

1.4 常用术语

华为云CAF涉及到很多IT和云计算领域的术语，不同读者对术语字面上的理解可能不一样，为避免对术语的误解，特制定如下术语表。

表 1-2 术语列表

术语	解释
CAF	英文全称为Cloud Adoption Framework，是一个针对云化转型的端到端生命周期框架，涵盖云化旅程的所有阶段，包括制定战略、顶层规划、调研评估、方案设计、采用实施和运维治理，CAF提供了云化旅程各个阶段的方法论、最佳实践、工具和模版。
WAF	英文全称为Well-Architected Framework，是华为云的卓越架构技术框架，聚焦客户业务上云后的关键问题的设计指导和最佳实践。WAF以华为公司和业界最佳实践为基础，以韧性、安全性、性能效率、成本优化与卓越运营五个架构关注点为支柱，帮助客户在华为云上设计卓越的技术架构、应用架构。WAF也是 Web Application Firewall（Web应用防火墙）的缩写，读者需要结合上下文判断WAF的具体意思。
IT基础设施	是指一个平台化的IT支撑环境，用于支撑组织内所有应用系统的安全稳定运行。它向下抽象、管理和优化底层IT资源（例如数据中心、硬件、网络、虚拟化等），向上为应用系统提供必要的计算、存储、网络、数据库、中间件和其他IT服务，加快应用系统的开发、测试和部署速度，并为应用系统提供稳定、可靠、高效的运行环境。云计算可以极大加快您的组织建设和扩展IT基础设施的速度，也可以极大简化IT基础设施的运维管理工作，使您的组织能够聚焦在应用系统的开发和运维等高价值领域。IT基础设施有时候也叫做技术平台或技术中台。基于云计算构建的IT基础设施也称作云基础设施。
应用系统	是指为了完成特定任务或解决特定问题而设计的软件系统，以支撑组织内特定的业务流程和业务场景。它通常由一系列相互关联的应用程序、数据库、中间件、配置文件和文档等组成，并运行在IT基础设施之上。应用系统可以是独立的，也可以是更大应用系统的一部分。应用系统有时也称为业务系统、信息系统、业务应用系统、业务信息系统、工作负载等。
IT管理系统	为了支撑应用系统的长期安全稳定运行所建立的IT支撑和管理系统，如安全运营中心、IAM和监控运维系统等。
云服务	是指云服务商通过互联网或专有网络提供的各种IT服务，包括计算、存储、网络、安全、运维管理、数据库、中间件、大数据处理和AI等。用户可以按需访问这些服务，而无需自行购买和维护物理硬件和软件基础设施，只需为实际使用的资源付费。云服务的主要类型包括基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）。
IaaS	IaaS 将计算、存储、网络和其他基础设施资源以云服务的形式提供给用户，用户基于这些云服务可以部署和运行任意软件，其中可能包括操作系统、数据库、中间件和应用程序。用户不控制底层云基础设施，但可以控制操作系统、存储、部署的应用程序以及可能的有限的网络组件（例如主机防火墙）。
PaaS	PaaS 将DevOps工具链、中间件、数据库、微服务引擎、大数据等平台资源以云服务的形式提供给用户，用户基于这些云服务可以开发、测试、部署和运维应用程序。用户不管理或控制底层云基础设施和中间件、数据库、微服务引擎等平台资源，但可以控制已部署的应用程序及其相关的数据。

术语	解释
SaaS	SaaS 直接将应用程序以云服务的形式提供给用户，应用程序可以通过各种客户端设备访问，例如通过Web浏览器、手机App或API。用户不管理或控制底层云基础设施、平台资源和应用程序，但可以控制应用程序运行期间产生的属于用户的数据。
云资源	云资源是用户通过云服务创建出来的IT资源实例，包括计算、存储、网络、安全、运维管理、数据库、中间件、大数据处理和AI等，用户可以组合使用云资源快速搭建上层应用系统所需的IT基础设施。
云服务商	云服务商（Cloud Service Provider，简称CSP）是指提供云服务的公司。他们设计、建设和运维大规模的云数据中心，通过互联网或专有网络向客户提供按需访问的云服务。云服务商有时也叫做云服务提供商、云厂商。
Landing Zone	Landing Zone是一个航空术语，指直升飞机等飞行器安全着陆的区域。华为云和友商都借用了这个术语，将应用系统安全平稳迁移到和运行在公有云的解决方案命名为Landing Zone。通过Landing Zone搭建一套架构卓越、安全合规、易扩展的云上多账号运行环境，在此基础上构建精益IT治理体系，实现“人财物权法”的有序和集中管控，目的是系统性解决企业大规模使用云服务所带来的IT治理和安全合规的挑战。
账号	华为云账号是一个资源容器，用户可以在其中部署任意云资源和应用系统，不同的账号相当于不同的资源容器，账号之间是完全隔离的。因此在一个账号中的故障和安全风险不会影响和传播到其他账号。华为云账号也是安全管理边界，每个账号都有独立的身份和权限管理系统，一个账号内的用户只能访问和管理本账号的资源，未经允许，一个账号内的用户不能访问其他账号的资源、数据和应用。 从IT治理角度，账号分为管理账号和成员账号，管理账号用于创建和管理组织、成员账号和SCP策略。成员账号用于承载具体的应用系统（如ERP等）或IT管理职责。从财务治理角度，账号分为企业主账号和企业子账号，企业主账号和企业子账号之间可以形成财务托管和财务独立的财务管理模式。IT治理角度的管理账号和财务治理角度的企业主账号是同一个实体，成员账号和企业子账号也通常是一个实体。
云上组织结构	是组织云上资源的层级化结构，由多层级的组织单元和账号组成，一个组织单元下面可以包含多个下层组织单元和多个账号。按照**康威定律**，云上组织结构通常与企业的业务结构保持一致。
云卓越中心	云卓越中心（Cloud Center of Excellence，简称CCoE）是企业内部为云化转型专门成立的中心化团队，全程负责整个云化旅程，包括制定战略、顶层规划、调研评估、方案设计、采用实施和运维治理，其目标是通过提供最佳实践、指导和资源，帮助企业最大化云计算的价值，确保云化转型项目的成功实施。
云运营模式	云运营模式（Cloud Operating Model，简称COM）是企业内部使用、管理和运营云计算技术的流程和制度，目的是最大化云计算带来的业务价值。云运营模式要与组织内的业务运营模式对齐，明确CCoE和应用团队之间的协作关系和流程，通过有效的云运营模式，CCoE可以集中化运营整个云平台，提升管理效率和降低技术风险；应用团队也可以灵活地使用和管理所需要的云资源，加速应用创新的步伐。

术语	解释
数字化转型	数字化转型是指组织利用数字技术（如云计算、大数据、物联网、人工智能、区块链等）对其业务模式、运营流程、产品和服务进行全面的重塑和创新，以适应快速变化的市场环境和满足客户不断提升的需求。通过数字化转型，组织不仅可以提升效率和竞争力，还能创造新的价值和增长机会。
云化转型	云化转型（也叫云转型）是指将组织的IT基础设施、应用系统、业务流程等迁移到云计算平台，或者利用云计算技术对其业务模式和运营流程进行重构和优化的过程。它不仅仅是简单的“搬迁上云”，更是一个涉及战略、技术、组织和流程的全面转型。目标是利用云计算的优势，提升业务敏捷性和连续性，降低成本，并推动业务创新。云化转型是数字化转型的重要支撑，可以大幅加速组织数字化转型的进程。
业务单元	业务单元（Business Unit）是指企业内部根据产品、服务、市场、客户群体或功能领域等划分的独立运营和管理的组织单元。每个业务单元通常具有自己的战略目标、职责范围、资源配置和业绩指标，负责特定的业务活动和市场区域。业务单元的颗粒度可以是子公司、事业部、产品线、部门或项目组等。

1.5 缩略语

表 1-3 缩略语（按照字母顺序）

缩略语	英文全称	中文全称
AIOps	Artificial Intelligence for IT Operations	智能运维
AOM	Application Operations Management	应用运维管理服务
ALM	Application Lifecycle Management	应用生命周期管理
CAF	Cloud Adoption Framework	云采用框架
Capex	Capital expenditure	资本支出
CBH	Cloud Bastion Host	云堡垒机
CC	Cloud Connect	云连接
CCE	Cloud Container Engine	云容器引擎
CCI	Cloud Container Instance	云容器实例
CCM	Cloud Certificate Manager	云证书管理服务
CCoE	Cloud Center of Excellence	云卓越中心
CFW	Cloud Firewall	云防火墙
CMDB	Configuration Management Database	配置管理数据库

缩略语	英文全称	中文全称
CMM	Cloud Maturity Model	云化成熟度模型
CNCF	Cloud Native Computing Foundation	云原生计算基金会
COC	Cloud Operation Center	云运维中心
CSMS	Cloud Secret Management Service	云凭据管理服务
CSP	Cloud Service Provider	云服务提供商或云服务商
CSR	Corporate social responsibility	企业社会责任
DBSS	Database Security Service	数据库安全服务
DC	Direct Connect	云专线
DCMM	Data Management Capability Maturity Assessment Model	数据管理能力成熟度评估模型
DDoS	Distributed Denial of Service	分布式拒绝服务
DevOps	Development and Operations	开发与运维
DevSecOps	Development, Security, and Operations	开发、安全与运维
DEW	Data Encryption Workshop	数据库安全服务
DSC	Data Security Center	数据安全中心
ECS	Elastic Cloud Server	弹性云服务器
EIP	Elastic IP Address	弹性公网IP
ELB	Elastic Load Balancing	弹性负载均衡
ER	Enterprise Router	企业路由器
ESW	Enterprise Switch	企业交换机
EVS	Elastic Volume Service	弹性云硬盘
FinOps	Finance Operations	财务运营
GRC	Governance, Risk & Compliance	治理、风险和合规
HSM	Hardware Security Module	硬件安全模块
HSS	Host Security Service	主机安全服务
IaaS	Infrastructure as a service	基础设施即服务
IaC	Infrastructure as Code	基础设施即代码
IAM	Identity and Access Management	身份和权限管理
IDC	Internet Data Center	互联网数据中心
IDP	Internal Developer Platform	内部开发平台

缩略语	英文全称	中文全称
IoT	Internet of Things	物联网
ITSM	IT Service Management	信息技术服务管理
ITSS	Information Technology Service Standards	信息技术服务标准
KMS	Key Management Service	密钥管理服务
KPS	Key Pair Service	密钥对管理服务
LLM	Large Language Model	大语言模型
MFA	Multi-Factor Authentication	多因素鉴权
MSP	Managed Service Provider	托管服务提供商
MTBF	Mean Time Between Failure	平均无故障时间
MTTR	Mean Time To Repair	平均故障修复时间
NAT	Network Address Translation	网络地址转换
OACA	Open Alliance for Cloud Adoption	云采用开放联盟
OBS	Object Storage Service	对象存储服务
OLAP	Online Analytical Processing	在线分析处理
OLTP	Online Transaction Processing	在线事务处理
Opex	Operational expenditure	运营支出
PaC	Policy as Code	策略即代码
PaaS	Platform as a service	平台即服务
PUE	Power Usage Effectiveness	能源利用效率
QPS	Query Per Second	每秒查询数
ROI	Return of Investment	投资回报率
RPO	Recovery Point Objective	恢复点目标
RTO	Recovery Time Objective	恢复时间目标
SaaS	Software as a Service	软件即服务
SCIM	System for Cross-domain Identity Management	跨域身份管理
SCP	Service Control Policy	服务控制策略
SecMaster	Security Master	安全云脑
SFS	Scalable File Service	弹性文件服务
SLA	Service Level Agreement	服务水平协议

缩略语	英文全称	中文全称
SLO	Service Level Objective	服务水平目标
SNAT	Source Network Address Translation	源地址转换
SOC	Security Operation Center	安全运营中心
SRE	Site Reliability Engineering	站点可靠性工程
SSO	Single Sign-On	单点登录
TOGAF	The Open Group Architecture Framework	开放企业架构框架
TPS	Transactions Per Second	每秒事务处理量
VPC	Virtual Private Cloud	虚拟私有云
VPN	Virtual Private Network	虚拟专用网络
WAF	Well-Architected Framework	卓越架构技术框架
WAF	Web Application Firewall	Web应用防火墙

2 制定战略

2.1 概述

在全球化和技术迅速发展的新时代，企业所处的市场环境正经历着变化。消费者需求不断升级，市场竞争日益激烈，传统的商业模式面临巨大挑战。面对这些压力，数字化转型已成为企业实现业务创新和可持续发展的必由之路。

数字化转型是指组织利用数字技术（如IT基础设施、数据库、大数据、物联网、人工智能、区块链等）对其业务模式、运营流程、产品和服务进行全面的重塑和创新，以适应快速变化的市场环境和满足客户不断提升的需求。当前主流的云计算平台都已经内置集成了丰富的、高可用和高安全的数字技术，组织可以在全球范围内通过云服务的形式按需使用这些数字技术，云服务是组织获取数字技术最快和最高效的方式，云化转型是数字化转型的重要支撑，可以大幅加速组织数字化转型的进程，未来绝大部分的数字化业务将基于云服务构建。工业化时代的标志是“电”，用电量反映了社会的工业化发展水平；数字化时代的标志是“云”，用云量反映了社会的数字化发展水平。

云化转型（也叫云转型）是指将组织的IT基础设施、应用系统、业务流程等迁移到云计算平台，或者利用云计算技术对其业务模式和运营流程进行重构和优化的过程。它不仅仅是简单地将数据和应用程序迁移到云端，更是一个涉及战略、技术、组织和流程的全面转型。

云化转型的第一步是制定云化转型战略，这需要全面的规划和周密的准备。制定云化转型战略不仅涉及技术层面的考虑，还需要与组织的业务战略和数字化战略紧密对齐，并在公司范围内与高层领导和所有干系人对齐战略目标。通常在制定云化转型战略时需要分析干系人利益、识别云化驱动力、评估云化成熟度、制定云化目标、分析云化收益等，下面章节将详细阐述这些内容。

2.2 干系人利益分析

识别干系人是制定云化转型战略的起点，您需要识别组织内部所有参与云化转型战略决策的干系人，并仔细分析干系人的利益诉求，与其共同识别云化转型的驱动力、分析云化收益，最终制定组织的云化转型战略。以下是一些常见的干系人和利益诉求，以及他们参与云化转型战略决策和项目执行的方式。

表 2-1 云化转型干系人及利益诉求

干系人	主要利益诉求	参与方式
首席执行官（CEO）	• 推动企业战略目标的实现，提升业务敏捷性和市场竞争力。 • 促进收入增长和利润提升，确保企业的可持续发展。 • 降低运营风险，保障业务连续性。 • 加速业务创新，开拓新市场和新业务模式。 • 提升企业形象和社会责任，关注可持续发展。	• 全面领导云化转型战略的制定和实施，担任项目的最终决策者，确保云化转型战略与公司业务战略对齐。 • 协调各部门资源，确保跨部门合作。 • 定期审阅项目进展，提供战略指导和支持。 • 与高管团队一起识别和评估云化转型的驱动力和预期收益。
首席信息官（CIO）	• 提升IT部门的服务能力，支持业务需求的快速响应。 • 推动技术创新，提升技术架构的先进性和灵活性。 • 优化IT成本结构，提高资源利用效率。 • 加强信息安全，保障数据和应用系统的可靠性。	• 主导云化转型战略的技术规划和路线图制定，确保云化转型战略与公司业务战略对齐。 • 协调IT团队和其他业务部门的合作，确保技术方案符合业务需求。 • 管理云服务商的选择和合作关系。 • 监督云化转型项目的实施，确保项目按计划推进。
首席运营官（COO）	• 优化业务流程，提升运营效率和质量。 • 确保业务连续性，降低运营风险。 • 支持业务扩张和创新，满足市场需求。	• 参与云化转型战略的制定，提供运营层面的需求和建议。 • 协调运营部门的资源投入，支持项目的实施。 • 监督云化对业务运营的影响，确保平稳过渡。
首席技术官（CTO）	• 引入先进技术，提升企业的技术竞争力。 • 确保技术架构的可扩展性和灵活性，满足未来业务需求。 • 推广技术创新，支持新产品和服务的开发。	• 领导技术方案的设计和评估，确保云化转型的技术可行性。 • 指导技术团队的工作，确保技术实现与战略目标一致。 • 与CIO合作，制定技术标准和规范。
首席信息安全官（CISO）	• 保障信息安全，防范数据泄露和网络攻击。 • 确保符合行业和法律的合规要求。 • 维护企业声誉，避免安全事件带来的负面影响。	• 评估云化转型带来的安全风险，制定相应的安全策略。 • 指导安全团队实施安全控制措施，确保云环境的安全性。 • 与合规审计专家合作，确保安全和合规要求得到满足。

干系人	主要利益诉求	参与方式
首席财务官（CFO）	• 优化财务绩效，降低IT成本，提升投资回报率。 • 管理资本支出和运营支出，改善现金流。 • 评估云化转型的财务风险和收益，支持战略决策。 • 基于云服务进行产品和业务创新，带来收入增长。	• 参与云化转型的成本收益分析，提供财务建议。 • 审核和批准项目预算和支出，确保资金有效利用。 • 制定云化转型的财务KPI，监督财务目标的实现。
业务主管	• 提升业务部门的绩效，满足市场和客户需求。 • 加速产品和服务的创新，拓展新的业务机会。 • 确保业务系统的稳定性和可靠性，支持日常运营。	• 提供业务需求和期望，参与云化转型方案的制定。 • 配合IT团队，确保技术方案符合业务需求。 • 协调业务团队的资源，支持项目的实施和变革管理。
IT主管	• 提升资源利用率，实现IT系统的弹性扩展，支持业务的快速增长。 • 通过云化降低IT成本。 • 利用云服务商的高可用性架构和安全防护措施，提升IT系统的稳定性和安全性，减少故障和安全事件的发生。 • 通过云化转型提升IT部门的价值。	• 辅助CIO制定云化转型战略和具体的云化目标。 • 选择适合组织的云服务模式，评估不同云服务商的方案，制定技术规范。 • 建立专门的云化转型团队，培养和引进云计算人才。 • 担任云化项目的总负责人，推进云基础设施的建设和业务系统的云化。
人力资源主管	• 规划和管理人才需求，支持云化转型所需的技能提升。 • 推动组织变革和文化转型，促进员工适应新的工作方式。 • 设计激励机制，激励员工参与和支持云化转型。	• 制定培训和发展计划，提升员工的云计算技能。 • 参与组织结构调整，确保团队配置满足云化转型的需求。 • 参与制定云化转型团队的KPI，监督KPI达成情况。
运维主管	• 提高运维效率，减少故障和停机时间。 • 实现运维自动化，降低人力成本。 • 提升系统的可用性和可靠性，支持业务连续性。	• 基于云平台的特点制定云运维流程和标准。 • 推广云运维工具的使用，实现自动化和智能化。 • 培训运维团队，提升云运维技能。

干系人	主要利益诉求	参与方式
应用架构师	• 优化应用架构，提升系统性能、可扩展性和可靠性。 • 支持应用现代化，充分利用云服务的优势。 • 确保应用满足业务需求，具备敏捷性和灵活性。	• 设计应用的云化架构，指导开发团队的实现。 • 评估和选择云服务，确保与应用需求匹配。 • 解决云化过程中遇到的技术挑战，提供专业支持。
数据架构师	• 设计高效的数据架构，支持数据分析和业务决策。 • 确保数据的安全性和合规性。 • 实现数据的集成和共享，提升数据价值。	• 规划数据在云环境中的存储和管理方案。 • 选择合适的云数据库和大数据服务。 • 实施数据迁移和治理，维护数据质量，保障数据安全。
网络架构师	• 设计灵活可靠的网络架构，支持应用系统之间的连接需求。 • 确保网络安全和性能，满足数据传输要求。 • 实现网络的弹性和可扩展性，适应业务变化。	• 规划云网络架构，配置虚拟网络、子网、安全组等。 • 与安全团队合作，实施网络安全策略。 • 监控网络性能，优化网络配置。
合规审计专家	• 确保云化转型符合相关法律法规和行业标准。 • 降低合规风险，避免法律纠纷和罚款。 • 维护企业声誉，提升客户和合作伙伴信任。	• 识别云化转型中的合规要求，提供专业建议。 • 参与制定合规策略，确保云服务商符合要求。 • 定期审计和评估合规情况，提出改进措施。
IT治理专家	• 建立有效的IT治理框架，规范IT资源的使用和管理。 • 确保IT战略与企业战略的一致性，提升IT价值。 • 管控IT风险，提升决策透明度和责任明确性。	• 制定云化转型的治理策略和政策，明确职责和流程。 • 监控云化转型的进展和风险，提供治理报告。 • 协调各部门的沟通，确保信息共享和协同工作。
产品经理	• 加快产品开发和上市时间，满足市场需求。 • 引入新技术，提升产品竞争力。 • 收集客户反馈，持续改进产品。	• 制定产品需求，协同开发和运营团队。 • 利用云服务，快速验证和迭代产品。 • 分析产品数据，指导产品优化。

通过识别和分析这些干系人的利益诉求，可以更好地制定和执行云化转型战略，确保各方利益得到平衡和满足。

2.3 识别云化驱动力

2.3.1 云化驱动力简介

识别云化转型的驱动力是制定战略的前提，需要深入分析内部和外部因素，内部因素包括业务增长需求、成本优化需求、运营效率提升和业务创新需求等，外部因素包括市场竞争压力、客户需求变化、技术发展趋势和监管合规要求等。综合考虑这些内部和外部因素，总体上可以将云化驱动力分解为业务驱动力、技术驱动力和财务驱动力三种驱动力，分别对应CEO、CIO和CFO的视角。

2.3.2 业务驱动力

业务驱动力是推动CEO和业务主管拥抱云计算的核心原因，主要关注利用云计算的优势提升业务敏捷性、加速业务创新、保障业务连续性、进行市场扩张、保障合规遵从和提升可持续性，最终提升企业的核心竞争力和实现业务收益。

- **提升业务敏捷性**

  业务敏捷性是指企业迅速响应市场变化和客户需求的能力。在快速变化的市场环境中，企业需要具备敏捷的业务能力，以保持竞争优势。

  - **快速部署业务系统：**云平台提供了高度灵活和可扩展的基础设施，企业可以迅速部署业务系统和服务，缩短上市时间。
  - **快速弹性伸缩：**云计算的弹性特性使企业能够根据业务需求，动态调整资源配置，快速满足业务高峰期或突发性需求。
  - **敏捷开发与迭代：**云平台支持DevOps实践，加速软件开发周期，实现业务系统的快速迭代和更新。

- **加速业务创新**

  业务创新是企业获取新增长点，保持竞争力的关键。云计算为企业提供了创新的平台、技术和工具，大幅降低了创新门槛，加速产品和服务、商业模式、业务流程和运营模式的创新。

  - **获取先进技术：**云服务商提供了AI平台、大模型、大数据平台、物联网、数字人等先进技术，企业无需自行构建，即可快速利用这些技术进行创新。
  - **降低技术门槛：**云服务简化了复杂技术的应用过程，企业可以专注于业务创新，而无需担心底层技术的复杂性。
  - **全球化合作：**云服务商构建了全球生态伙伴网络，使得企业能够与全球的合作伙伴和开发者共同创新，拓展全球业务。

- **提升业务连续性**

  业务连续性是指企业在面对各类故障、外部攻击和突发事件时，仍能持续稳定地提供产品和服务的能力。云平台和云服务固有的高可用性和安全性可用确保业务系统的稳定运行，降低运营风险。

  - **高可用架构：**云服务商提供多地域、多可用区的部署模式，支持跨地域的容灾备份，提升业务系统的可靠性。
  - **自动故障转移：**云平台具备自动检测和故障转移机制，当发生硬件或软件故障时，能够迅速恢复业务运行，减少停机时间。
  - **安全防护能力：**云服务商在安全防护方面有很深的积淀，既有端到端的安全技术体系，也有完备的安全管理流程和规范，更有一支庞大的安全专家团队每时每刻在保障云平台的安全，因此公有云相比大多数组织的内部IT团队有更强大的信息安全保障能力。

- **市场扩张**

  将业务扩张到全球市场是企业收入增长的重要途径。借助云服务商的全球布局，可以有效支撑企业进入新市场、扩大业务版图和触达更多客户。

  - **全球化部署：**云服务商在全球范围内拥有云数据中心，企业可以快速在目标市场部署业务，降低进入新市场的技术和时间门槛。
  - **本地化服务：**云平台提供本地化语言支持，并且提供符合当地法规的服务，帮助企业快速适应当地市场需求。
  - **降低进入成本：**无需在当地建设数据中心或采购硬件设备，减轻了初始投资压力，降低了市场进入成本。
  - **提升客户体验：**通过就近部署和优化的网络架构，提供低延迟、高性能的服务，提升当地客户的满意度。

- **合规遵从**

  在当今瞬息万变的商业环境中，合规遵从已成为企业生存和发展的关键要素。随着全球各地法规和标准的日益严格和复杂化，企业需要确保其运营符合当地法律法规和行业标准，以避免法律风险、财务损失和声誉受损。借助云服务商提供的合规性支持服务，企业可以有效降低合规风险，专注于核心业务发展。

  - **全球化合规支持：**云服务商在全球范围内的数据中心和服务都符合当地法规和行业标准，例如 GDPR、HIPAA、PCI DSS 等。企业可以利用云平台的合规性认证和服务，快速满足不同市场的合规要求。
  - **本地化合规服务：**云平台提供本地化的合规服务，例如数据驻留、数据主权、数据加密等，帮助企业满足特定地区的合规要求。例如，一些国家要求数据必须存储在境内，云服务商可以提供符合要求的本地数据中心和服务。
  - **提升合规效率：**云平台提供自动化合规工具，例如安全审计、漏洞扫描、访问控制等，帮助企业进行自动化合规管理，提高效率并降低人为错误的风险。

- **提升可持续性**

  可持续性是企业履行社会责任，实现长期发展的重要方面。采用云计算可以减少能源消耗和碳排放，履行企业社会责任，实现绿色发展。

  - **降低能耗和碳排放：**云数据中心通常采用先进的能源管理和冷却技术，PUE能降到1.2以下，相比自建数据中心，能耗和碳排放显著降低。
  - **优化资源利用：**云计算通过虚拟化和资源池化，提高了服务器和存储设备的利用率，减少了物理设备的需求。
  - **支持绿色创新：**云平台支持开发基于数字技术的绿色解决方案，如智慧城市、智能交通、在线协作工具等，助力环保和节能减排。
  - **环境合规性：**云服务商通常遵守严格的环境标准和法规，企业利用云服务可以间接满足相关的环境合规要求。

云化转型的业务驱动力涵盖了敏捷性、创新性、连续性、市场拓展和可持续发展等关键业务领域的需求，深入理解云化转型的业务驱动力，能够帮助企业：

- 制定明确的云化转型战略目标，确保云化转型战略与业务战略紧密结合。
- 获得管理层和全体员工的支持，统一认识，共同推进云化转型。
- 实现业务价值最大化，提升企业的市场竞争力和可持续发展能力。

2.3.3 技术驱动力

在数字化时代，云计算已成为企业技术战略的核心。对于CIO、CTO和技术主管而言，云化转型不仅是业务发展的需求，更是技术创新和变革的必然选择。云计算提供的技

术优势，在资源弹性、系统韧性、扩展性、安全性和运维效率等方面实现飞跃。这些技术驱动力是业务驱动力和财务驱动力的底层技术支撑。

- **提升资源弹性**

  资源弹性是云计算的核心特性之一，是指云平台能够根据业务需求，按需对业务系统所需的计算、存储和网络等资源进行快速扩容和缩容。提升资源弹性可以有效提升业务敏捷性和业务连续性。

  - **动态资源调配：**云计算支持按需分配资源，企业可以在业务高峰期迅速扩展资源规模，以应对流量激增；在业务低谷期，则可以释放闲置资源，降低成本。
  - **自动化伸缩：**通过自动化的监控和调度机制，云平台能够根据预设的策略和实时的负载情况，自动进行资源的伸缩。
  - **快速部署和回收：**相较于传统的硬件采购和部署周期，云上资源的创建和销毁可以在几秒或几分钟内完成，大幅提高了资源的弹性速度。

- **提升系统韧性**

  系统韧性是指系统在面对各种外部灾难和内部软硬件故障时，仍然能够维持正常运行或快速恢复的能力。云平台和云服务能够大幅提升应用系统的韧性，从而有效提升业务连续性。

  - **高可用架构：**云服务商提供多地域、多可用区的部署模式，支持应用系统设计跨机房、跨地域的容灾和双活方案，甚至跨多个地域的多活方案，大幅提升应用系统的可用性和容灾能力。
  - **灾备和容灾：**云平台内置了数据备份、容灾切换等功能，帮助企业构建完善的灾难恢复方案，在突发事件中保障系统可用性。
  - **服务等级协议（SLA）**：云服务通常提供99.9%以上SLA，可以有效保障基于这些云服务构建的应用系统的可靠性SLO（Service Level Objective）。
  - **故障自动化处理：**云平台具备自动检测故障和自动恢复的能力，减少人为干预，缩短故障处理时间。

- **提升扩展性**

  扩展性指一个系统在面对不断增加的工作负载或请求时，在不改变系统架构或对现有系统进行最小修改的情况下，通过添加或调整资源（例如服务器、存储、带宽）而保持性能稳定、效率不降低的能力。云平台和云服务可以大幅提升应用系统的扩展性，平滑处理不断增加的用户、数据或事务量，而不会导致性能下降或系统崩溃。提升系统扩展性可以有效提升业务敏捷性和连续性。

  - **分布式架构**：云平台支持分布式系统架构设计，允许应用程序在多个服务器或节点上运行，分散负载，避免单点故障，提高系统的扩展性和可用性。
  - **自动弹性伸缩**：利用云平台的自动化伸缩功能，系统可以根据预设的策略自动增加资源实例，以应对流量高峰，保持性能稳定。
  - **微服务架构**：云平台天然适合微服务和容器化部署，支持应用拆分和独立扩展，提升灵活性和可维护性。
  - **无服务器计算**：云平台提供的无服务器计算服务（如 **FunctionGraph**）允许用户将代码部署到云端，而无需管理服务器。云平台会根据请求自动分配计算资源，并在请求处理完成后释放资源。这种模式极大地简化了扩展性管理。

- **提升安全性**

  安全性是指保护数据和应用系统免受未经授权的访问、使用、泄露、篡改、破坏或损失的能力。云服务商在信息安全领域投入巨大，为企业提供了多层次的安全保障。提升安全性可以有效提升业务连续性。

  - **云平台安全：**云服务商的云平台符合严格的安全标准和认证，如ISO 27001、CSA、SOC 1/2/3、安全等级保护、PCI-DSS、NIST CSF等。
  - **丰富的云原生安全服务：**云服务商提供主机安全、数据安全、应用安全、网络安全、身份安全和运维安全等丰富的云原生安全服务，帮助企业在云上为应用系统快速构建全方位的安全防线。

- **提升运维效率**

  运维效率是指IT运维团队以最少的资源投入（人力、时间、成本），管理尽可能多的IT资源，并保持高服务质量和稳定性的能力，它体现了资源利用率和人员生产力。企业采用云计算之后可以大幅提升运维效率，进而有效降低运维成本。

  - **无需管理IT基础设施：**云服务商负责云数据中心、硬件、网络、虚拟化等IT基础设施的运维，企业只需要聚焦应用系统的运维。
  - **智能监控系统**：云服务商提供全栈和智能监控系统，能够实时收集、分析云资源及应用性能指标，自动识别异常，预测潜在风险，并提供告警和可视化报表，帮助运维人员快速定位故障。
  - **自动化运维：**云服务商提供自动化部署、配置管理、监控告警和运维等工具，减轻运维人员的工作负担，提高运维效率。自动化运维还降低了人为错误的风险，从而减少了不必要的纠错工作。
  - **无服务器架构**：如果企业采用函数计算等Serverless服务，企业只需编写业务逻辑代码，无需管理任何服务器，将进一步减轻运维负担。

- **提升性能效率**

  提升性能效率的目标是用更少的IT资源处理更多的业务请求，最终体现在更高的吞吐量、响应时间或并发用户数等关键性能指标上。借助云服务商提供的云上卓越架构设计原则和性能检测和优化工具，企业可以有效提升系统的性能指标。

  - **选择合适的资源:** 根据业务实际需求选择最合适的计算、存储、中间件和数据库等资源的规格等，同时避免过度配置造成资源浪费。
  - **性能测试和规划：**基于云平台提供的性能测试工具评估应用系统当前的性能指标，再结合业务需求增长趋势提前进行容量规划。
  - **性能优化:** 挖掘现有资源的性能潜力，包括数据库查询优化、代码优化、使用缓存和CDN加速等，提升系统吞吐量和响应速度。
  - **架构优化:** 采用更有效率的架构模式。例如，使用异步处理和消息队列解耦系统组件，提高并发处理能力。

云化转型的技术驱动力为企业的IT战略和技术架构带来了深刻的变革。对于技术领导者而言，深入理解和利用这些技术驱动力将有助于：

- 制定前瞻性的技术战略，引领企业的数字化发展。
- 优化IT架构和资源配置，提升技术部门的价值贡献。
- 推动技术创新和业务融合，支持企业取得竞争优势。

2.3.4 财务驱动力

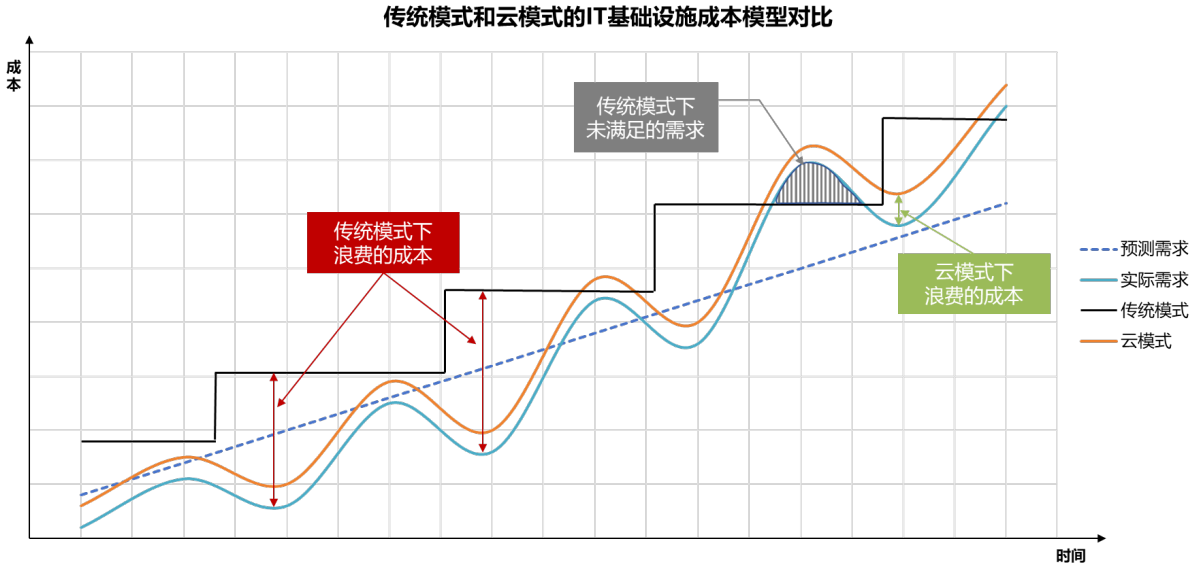
云化转型带来了大量的财务收益，包括按需付费，降低成本和新增收入等，对CFO和财务主管极具吸引力。

- **降低成本**

  传统模式（自建数据中心）下企业按照预测的业务峰值需求提前采购硬件和软件等IT资源，为了避免在高峰期出现性能瓶颈或服务中断，通常会过度采购资源。但实际业务负载具有波动性，大部分时间运行在平均水平或低于平均水平，结果是IT资源长期处于闲置或低利用率状态，造成成本的巨大浪费。

云模式下企业按照实际业务负载弹性提供所需的云资源，企业只需为实际使用的资源按需付费，无需预先购买大量硬件和软件。在业务高峰期，云平台能够迅速扩展云资源满足需求，而在在业务低谷期，能够释放多余云资源，这将大幅减少资源浪费、降低成本。传统模式和云模式的成本模型对比如下图所示。

图 2-1 传统模式和云模式的 IT 基础设施成本模型对比



总体上讲，云模式节省IT基础设施成本的主要原因有以下几点：

- **按需付费：** 云模式可以根据业务高峰期和低谷期自动调整云资源数量，企业只需为实际使用的云资源付费，而传统模式需要提前购买和维护大量的硬件和软件资源。这种按需付费的模式避免了资源闲置和浪费。
- **规模效应:** 云计算本质上是规模经济，云服务商建设和运营超大规模的数据中心，具备超大的计算能力和存储容量。由于规模庞大，云服务商可以通过批量采购硬件和软件、优化资源利用率、提升能源利用效率和自动化管理等方式大幅降低运营成本，以更低的成本对外提供IT资源。
- **降低运维成本:** 云服务商负责IT 基础设施的维护和管理，企业无需投入大量人力和资金进行IT基础设施的日常运维。而且云平台提供了智能监控系统和自动化运维系统可以大幅提升应用系统的运维效率，企业可以减少在应用系统运维领域的人力投入，进一步降低了运维人力成本。自动化运维也降低了人为错误的风险，从而减少纠错成本。

值得注意的是，云模式下也可能会产生成本浪费，上图中橙色曲线和蓝色曲线之间的部分就是云模式下的成本浪费，这种浪费是由很多原因造成的，比如在业务高峰期间申请的云资源没有及时释放掉，在后面的运维治理章节，我们将详细描述如何进行成本优化和持续成本运营。

- **新增收入**

  云计算不仅可以降低成本，还可以帮助企业创造新的收入来源：

  - **缩短产品上市时间:** 云平台可以快速部署和扩展应用，帮助企业更快地推出新产品和服务，抢占市场先机，从而获得更多的市场份额和收入。
  - **拓展新市场:** 云平台的全球覆盖能力，使得企业更容易进入新的市场，拓展业务范围，接触到更广泛的客户群体，从而增加收入。
  - **提升客户体验:** 云平台可以提供更稳定、可靠和高性能的服务，提升客户满意度和忠诚度，从而增加收入和客户留存率。

  - **业务创新:** 云平台的灵活性和集成的新技术，可以支持企业进行产品和服务创新、探索新的运营模式和商业模式，挖掘新的市场机会，创造新的收入来源。

- **资本支出转变为运营支出**

  传统模式（自建数据中心）下 IT 基础设施建设需要巨额资本支出（Capex），购买服务器、存储设备、网络设备等硬件，并承担维护和更新成本，这需要企业一次性投入大量资金。云服务则采用按需付费模式，将资本支出转化为运营支出（Opex）。企业只需根据实际使用的计算资源、存储空间和网络带宽付费，如同水电费一样。这种模式可以显著降低企业的初始投资门槛，提高资金利用效率，并根据业务需求灵活调整资源使用，避免资源闲置和浪费。这对于预算规划和现金流管理至关重要，也使得企业能够更灵活地应对市场变化。

总而言之，云化转型带来的财务优势是 CFO 和财务主管拥抱云计算的核心原因。通过降低成本、新增收入，并将资本支出转变为运营支出，云计算可以帮助企业提高财务绩效。

2.3.5 多云战略的驱动力

当前多云战略正在成为一种主流趋势，越来越多的组织选择将业务系统部署在多个云服务商的云平台上，而不是依赖单一的云服务商。这种趋势的背后是多种因素的驱动，以下是一些主要的驱动力：

- **避免单云故障：**将业务部署在单一云平台上存在单点故障风险。如果该云平台出现故障，例如大规模宕机或区域性灾难，企业的业务将受到严重影响。多云战略可以通过将业务系统部署在多个独立的云平台上，实现跨云容灾，避免单一云平台故障带来的业务中断。即使一个云平台出现问题，其他云平台上的业务仍然可以正常运行，保障业务连续性。
- **避免厂商锁定：**将所有业务都放在一个云服务商的云平台里会造成厂商锁定，使企业在未来的谈判中处于劣势，并且难以迁移到其他平台。多云战略可以避免这种情况，保持企业在选择云服务商方面的灵活性。
- **降本增效：**多云战略可以引入竞争机制，通过与多个云服务商合作，企业可以根据自身需求选择最合适的云服务，并利用云服务商之间的竞争来降低成本。此外，不同的云服务商在不同区域或服务上的定价策略可能存在差异，多云战略可以帮助企业优化资源配置，提高成本效益。
- **充分利用不同厂商的优势能力：**不同的云服务商在技术、服务和功能方面各有优势。例如，某个云服务商可能在人工智能和机器学习方面拥有更强的技术实力，而另一个云服务商可能在数据库服务方面更具优势。多云战略允许企业根据自身业务需求，选择最合适的云服务商及其优势服务，从而最大化地发挥云计算的价值。
- **合规遵从：**某些国家和地区有特定的数据存储和处理的法规要求，但每家云服务商的全球布局和合规遵从程度不一样。多云战略可以帮助企业选择最合适的云服务商来满足这些法规要求，例如将敏感数据存储在特定地区的云平台上。

多云战略的采用是为了提高业务连续性、成本效益和安全性。虽然多云战略也带来了管理复杂性等挑战，但随着云管理工具和技术的不断发展，这些挑战正在逐渐得到解决。

2.3.6 如何识别驱动力

识别驱动力是云化转型的前提，决定了组织是否有正当的理由开启云化转型。识别驱动力是一个比较复杂的过程，需要综合考虑企业的业务战略、业务需求、财务需求和技术需求，并要与高层和干系人达成一致。以下是推荐的步骤：

- **响应关键业务事件**

  企业高层的云化转型决策通常源于实际业务需求，而非凭空臆想。关键业务事件往往是促成云化转型的契机，因此，必须充分考虑企业当前和未来可能面临的关键业务事件。以下是一些常见的能够推动云化转型的关键业务事件。

  - **数字化转型：** 企业进行数字化转型，需要更先进的IT技术和平台支撑，云平台可以提供丰富的数字化工具和服务。
  - **数据中心退役：**现有数据中心即将到期或设备老化，需要进行更新换代，迁移上云成为一个具有吸引力的选择。
  - **合并和拆分：** 企业收购、合并或拆分会对IT基础设施产生重大影响，云服务的灵活性可以帮助企业快速调整IT资源，适应新的组织架构。
  - **现金流紧张：** 企业现金流比较紧张，希望降低资本支出，包括IT基础设施的投资，将Capex转化为Opex，云服务的按需付费模式可以满足这一需求。
  - **关键技术终止服务：** 现有关键技术的提供商即将停止支持服务，需要进行升级或迁移，上云可以提供更现代化、更可靠和更安全的技术方案。
  - **法规遵从变化：** 新的法规或合规性要求可能需要企业对IT系统进行调整，云平台通常能够更好地满足这些要求。
  - **关键业务系统中断：** 企业经历过关键业务系统的中断，收入和声誉受损，希望提高业务系统的可靠性，云平台可以提供更高的可靠性和容灾能力。
  - **碳排放未达标：** 企业希望降低能源消耗和碳排放，提升企业社会责任形象，云数据中心通常采用先进的能源管理和冷却技术，能源效率更高。
  - **市场快速变化：** 市场环境和客户需求快速变化，企业要加快产品上市速度，云平台提供更灵活和更弹性的IT基础设施，支持产品和新特性快速上市。
  - **遭遇安全攻击：** 企业近期遭遇了黑客攻击，希望提高业务系统和数据的安全性，抵御攻击和数据泄露，云平台可以提供更全面和更强大的安全防护措施。

- **将关键业务事件映射到驱动力**

  将第一步中识别出的关键业务事件与云化转型的驱动力关联起来，可以更清晰地理解云化转型如何应对这些关键业务事件带来的挑战。

  表 2-2 关键业务事件和驱动力的映射

关键业务事件	业务驱动力	技术驱动力	财务驱动力
数字化转型	提升业务敏捷性 加速业务创新 提升业务连续性 市场扩张	提升资源弹性 提升系统韧性 提升扩展性 提升安全性	新增收入
数据中心退役	-	提升资源弹性 提升系统韧性 提升扩展性 提升安全性 提升运维效率 提升性能效率	按需付费 降低成本

关键业务事件	业务驱动力	技术驱动力	财务驱动力
合并和拆分	提升业务敏捷性	提升资源弹性 提升扩展性	-
现金流紧张	-	提升资源弹性 提升运维效率 提升性能效率	按需付费 降低成本
关键技术终止服务	提升业务连续性	提升资源弹性 提升系统韧性 提升扩展性 提升安全性	-
法规遵从变化	合规遵从	提升安全性	-
关键业务系统中断	提升业务连续性	提升系统韧性 提升性能效率	-
碳排放未达标	提升可持续性	-	-
市场快速变化	提升业务敏捷性	提升资源弹性 提升扩展性	新增收入
遭遇安全攻击	提升业务连续性	提升安全性	-

- **确定驱动力的优先级**

  并非所有业务事件都具有相同的紧迫性和重要性，您需要根据企业的业务战略和业务现状，对已识别的驱动力进行优先级排序。例如，对于一家正在进行数字化转型的企业来说，“提升业务敏捷性”和“加速业务创新”的优先级更高。而对于一家面临现金流紧张的企业来说，“按需付费”和“降低成本”的优先级更高。这些优先级将决定未来进行方案设计时，应该优先考虑哪些方面。比如在韧性、安全和成本产生冲突时，对现金流紧张的企业来说，就要优先考虑成本低的设计方案，在安全、韧性方面可能就会有所妥协。

- **与高层和干系人对齐**

  在确定了云化转型驱动力和优先级之后， 将云化转型驱动力和优先级、预期收益清晰地记录下来，与企业高层和干系人进行沟通和对齐，听取他们的意见和建议，获取他们的理解和支持。

2.4 评估云化成熟度

2.4.1 评估云化成熟度的意义

评估云化成熟度的目的是全面了解组织在云化转型过程中的能力现状，识别差距，制定有针对性的能力提升计划，组织在制定云化目标时就能更加现实可行，避免过高或过低的期望。

2.4.2 云化成熟度评估模型

华为云参考了云采用开放联盟（OACA）的云化成熟度模型、CNCF云原生成熟度模型、中国信标委ITSS（IT服务标准）、DCMM等标准和评估模型，同时结合华为云大量政企客户深度云化的最佳实践设计了云化成熟度评估模型。在设计该模型的时候遵守以下五大原则。

- **业务驱动：**评估模型要以业务驱动力为中心，要求云化目标要与公司业务战略和业务目标对齐，云化转型最终要取得业务收益，而不仅是技术收益。
- **全要素：**评估模型要全面涵盖组织(People)、技术(Technology)和流程(Process)三个要素，而不仅仅是技术能力的评估。
- **全堆栈：**评估模型要涵盖全技术堆栈，包括卓越架构（Well-Architected Framework）、云基础设施、应用现代化、大数据与AI、运营运维、安全防护等技术领域。
- **全旅程：**评估模型要涵盖云化转型的端到端旅程，包括制定战略、顶层规划、方案设计、采用实施、运维治理等阶段。
- **一体化：**评估模型要考虑云上云下、多云之间、云内跨Region、云内多账号之间的一体化管理能力。

基于上述原则，华为云设计了以下10个评估维度。

图 2-2 云化成熟度评估模型的 10 个评估维度

- **云化业务收益**

  这个维度主要评估组织通过云化转型所能够实现的业务收益和财务收益，包括提升业务敏捷性、提升业务连续性、降低TCO、加速业务创新、提升可持续性等。这个维度放在首位是因为业务收益是最重要的维度，如果没有实现业务收益，其他维度做得再好也是徒劳。
- **战略与业务**

主要评估组织在云化转型中的战略规划能力，云化战略是否与整体业务战略和目标保持一致，是否识别了关键的业务驱动力，是否制定了清晰的云化战略、云化目标和迁移策略等。同时也评估组织在制定云化战略时的前瞻性、全面性和可行性，以及对行业趋势和云技术趋势的把握。

- **组织与流程**

  主要评估组织在云化转型过程中，组织结构、人员技能、工作流程等方面的适应性和变革能力，衡量组织是否具备支持云化转型的组织架构和人才队伍，是否建立了适合云环境的工作流程。

- **数智赋能**

  主要评估组织在大数据和人工智能领域的能力水平，是否能够利用云平台的数智化服务，实现数据驱动的业务创新和智能化转型，衡量组织的数据生命周期管理、数据治理能力，以及在人工智能技术（如AI开发、大模型等）方面的实践水平。

- **应用现代化**

  主要评估组织的应用系统是否采用了现代化的设计和开发模式，如微服务架构、事件驱动架构、容器化、Serverless、DevSecOps实践等，是否具备云原生应用的开发和部署能力。

- **云基础设施**

  主要评估组织对于云基础设施的设计、部署和管理能力，包括Landing Zone的设计和实施、网络和IAM的一体化管理、基于IaC的基础设施自动化部署、数据备份和弹性伸缩策略等。

- **云卓越架构**

  主要评估组织是否遵循**卓越架构技术框架（Well-Architected Framework）**的设计原则和最佳实践，包含韧性、安全性、性能效率、成本优化和卓越运营五个方面。

- **云运营与运维**

  主要评估组织在云环境下的运营和运维能力，包括可观测性、CMDB、自动化运维、混沌工程、ITSM和AIOps等。同时评估组织是否建立了最适合业务现状的云运营模式和运维流程，以支撑云上业务系统的敏捷交付和稳定运行。

- **云安全防护**

  主要评估组织在云环境中的安全防护措施和安全运营能力，包括身份安全、网络安全、数据安全、主机安全、应用安全、运维安全、安全管理规范和一体化安全运营等方面。

- **云财务管理**

  主要评估组织对云资源成本的管理和优化能力，包括成本预算、成本可视、成本优化、成本运营和一体化财务管理等方面。

  这些评估维度涵盖了组织、技术和流程三个要素，以及云化转型的全旅程和全技术堆栈，并考虑了一体化管理能力，总共有70+评估问题。针对每个评估问题分别设计了五个等级：起步(Initiating)、局部突破（Emerging）、全面开展（Performing）、竞争优势（Advancing）和领先（Leading）。

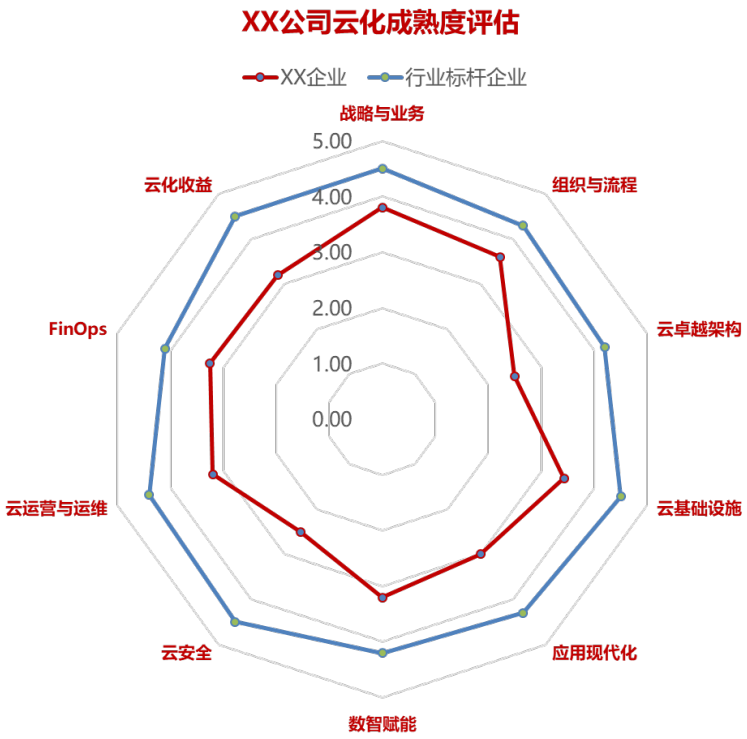
表 2-3 云化成熟度的 5 个等级

等级	分数	成熟度水平

起步	1分	• 对云计算的理解和应用处于初步探索阶段，对云原生技术和最佳实践的应用有限，存在安全和成本风险。 • 云化转型尚未真正开始，缺乏整体规划和战略，也缺乏支撑云化转型的组织和流程。
局部突破	2分	• 局部应用云计算技术，并取得了一些初步成果，但整体上仍然缺乏系统性和完整性。 • 开始关注云原生技术和最佳实践，但应用不够深入。自动化程度较低，安全和成本管理也需要进一步加强。 • 处于从传统IT模式向云原生模式转变的过渡阶段。
全面开展	3分	• 云化转型取得了成效，通过应用云计算技术建立了技术竞争力，但还未形成业务优势，业务收益不明显。 • 能够熟练运用各种云服务，并具备一定的自动化管理能力。 • 开始系统地应用云原生技术和最佳实践，例如 DevOps、微服务等。安全和成本管理也得到了一定的重视和落实。 • 具备完善的流程和完备的组织阵型，云化目标在IT部门内达成共识。
竞争优势	4分	• 云化转型取得了显著成效，通过应用云计算技术建立业务竞争优势，实现了显著的业务收益，如提升了业务敏捷性和连续性、增加收入等。 • 云计算已经成为驱动业务创新和提升竞争力的关键因素。 • 能够充分利用云原生技术和最佳实践，实现高度的敏捷性和可扩展性。 安全和成本管理体系成熟且高效。 • 流程得到有效的执行，云化目标在全公司范围内达成共识。
领先	5分	• 在云计算领域处于领先地位，能够引领技术和业务模式的创新。 • 充分发挥了云原生技术的优势，实现了高度自动化和智能化的运营。 • 安全和成本管理达到了业界领先水平。 • 云化转型不仅推动了自身业务的快速发展，也为行业树立了标杆。 • 紧跟业务需求和云计算技术的变化而不断迭代优化。

通过上述10个维度的详细评估分析，组织可以全面了解自身在云化转型过程中的能力现状，通过生成的雷达图可以很快找出与行业标杆企业之间的差距，从而制定有针对性的改进和提升计划。

图 2-3 云化成熟度雷达图



需要注意的是这个云化成熟度评估模型是一个相对高阶和粗颗粒度的评估，主要目的是为了快速识别组织的能力差距和制定云化目标，并不能代替调研评估阶段的详细现状调研，后者的目的主要是为了设计详细的技术实施方案。

2.4.3 云化成熟度评估步骤

上述云化成熟度评估模型相对比较完备，完成全部评估和分析需要1周左右的时间。以下是执行云化成熟度评估的具体步骤。

步骤1 定义评估范围

这是整个评估过程的基础。在这一阶段，您需要根据组织的现状和业务需求，确定需要评估的具体范围。由于云化转型涵盖多个评估维度和众多评估问题，您可能无法在一次评估中全部涵盖，您可以聚焦于组织当前发展阶段和业务目标最相关的方面，选择其中一部分关键维度进行评估。通过与相关业务部门、技术团队的沟通，明确当前最需要提升的领域，确保评估能够聚焦于对组织最有价值的方面。这一步骤的目标是制定一个清晰、可执行的评估范围，为后续评估工作的顺利展开奠定基础。

步骤2 识别和协调评估人

这对于评估的准确性和有效性至关重要。您需要确定内部最适合回答所选评估问题的人员，这些人员应当对各自负责的领域有深入的了解，能够提供客观、详实的答复。针对云化成熟度评估的10个维度，我们建议的评估人选如下：

表 2-4 推荐的云化成熟度评估人选

评估维度	推荐评估人选
战略与业务	CEO或者CIO

组织与流程	CIO或者人力资源主管
云卓越架构	CIO或者企业应用架构负责人
云基础设施	CIO或者IT主管
应用现代化	应用架构师
数智赋能	业务主管或者数据架构师
云安全	CISO
云运营与运维	运维主管
FinOps	云成本管理负责人
云化收益	业务主管或IT主管

您要协调好评估人的时间，尽量将评估活动集中在一个时间段内，有助于提高评估效率。此外，为了确保评估人对评估目的和要求有充分的理解，您可以在评估前进行统一的说明和培训，详细解释评估的目的、流程和要求。

步骤3 执行评估

这是整个过程的核心环节。评估人需要根据之前确定的评估范围和问题，逐一进行认真、客观的答复。在答复过程中，应当全面考虑组织在各个评估问题的实际情况，提供具体的数据和实例支持。如果评估人对某些评估问题存在疑问，应及时与评估专家联系，安排集中答疑，确保对问题的理解准确无误。执行评估时，应避免主观臆断，基于事实进行评价。此外，需要强调评估的客观性和保密性，鼓励评估人如实反映情况，不用担心负面影响。这一步的质量直接影响到评估结果的可靠性和后续改进措施的有效性，因此需要评估人给予足够的重视和投入。

步骤4 第四步、输出评估报告

评估专家在这一阶段需要汇总和分析所有评估人的答复，识别组织在云化成熟度方面的优势和差距。对于发现的能力差距项，评估专家应深入分析其原因和影响，并针对性地提出优化和提升的建议。这些建议应具体、可操作，包括改进措施的优先级、实施路径和预期效果。评估报告应逻辑清晰、条理分明，既能全面反映评估结果，又能为组织制定下一步行动计划提供有力支持。通过评估报告，组织管理层和各部门可以明确当前的能力水平，了解需要改进的领域，从而有针对性地制定和调整云化战略、云化目标和实施方案，推进云化转型的深入发展。一份高质量的评估报告能够为组织的云化转型提供重要的决策依据。

----结束

2.5 制定云化目标

云化目标一定要与组织的业务战略和业务目标对齐，而且云化目标要符合SMART原则，即目标应是具体的（Specific）、可衡量的（Measurable）、可实现的（Achievable）、相关的（Relevant）和有时限的（Time-bound）。例如，如果组织经常因为业务系统中断导致收入减少和品牌受损，可以制定一个具体的业务目标：“在未来一年，将业务系统的可用性从99%提升到99.9%”。在设定云化目标时，您还需要充分考虑组织的资源和能力现状，确保目标是可实现的。通过上述云化成熟度

评估，您正好能够掌握组织当前的能力现状和差距，可以有针对性地制定云化目标，避免设置过高或过低的目标。

为了制定可衡量的云化目标，需要针对云化驱动力设计合理的量化指标，方便组织的管理层进行跟踪和评估云化转型的实际效果。我们针对上述各种驱动力设计了以下量化指标。

表 2-5 云化驱动力的量化指标

类别	驱动力	量化指标
业务驱动力	提升业务敏捷性	● 新产品（新业务系统）的TTM，包含从设计、开发、测试到上市的端到端时间。 ● 已有产品（已有业务系统）的新版本或新特性的迭代周期，包含从设计、开发、测试到上市的端到端时间。
	加速业务创新	● 新产品、新服务和新商业模式等带来的新用户数。 ● 新产品、新服务和新商业模式等带来的新增收入。
	保障业务连续性	● 业务系统的可用性SLO。 ● 业务中断导致的经济损失。
	市场扩张	● 进入新市场带来的新用户数。 ● 进入新市场带来的新增收入。
	合规遵从	● 不合规造成的经济损失，包括赔偿和罚款。
	提升可持续性	● 碳排放减少量。
技术驱动力	提升资源弹性	● 资源利用率。 ● 资源扩容速度、资源部署时间。
	提升系统韧性	● RPO、RTO。 ● P1、P2、P3、P4事件数量。
	提升扩展性	● 系统扩容速度。
	提升安全性	● 安全事件数量。 ● 安全事件导致的经济损失，包括赔偿和罚款。
	提升运维效率	● 单位资源所需要的运维工时。 ● 每个运维工程师可运维的资源数量（如VM数和存储容量）。 ● MTTR（平均故障修复时间）。
	提升性能效率	● TPS、QPS等吞吐量指标。 ● 系统响应时间。 ● 并发用户数。 ● 资源利用率。

财务驱动力	按需付费	• IT基础设施资本支出。
	降低成本	• 业务单元成本，如每个订单的成本，每个用户的成本等。 • IT基础设施的TCO。
	新增收入	• 业务创新和市场扩张带来的新增收入。

上述量化指标比较多，跟踪、评估和管理这些指标的工作量比较大，所以不建议您的组织全部拿来评价云化转型的效果。考虑到有些指标之间存在包含关系，比如业务系统的可用性SLO隐含了RPO、RTO、MTTR等指标。另外，云化转型最终是为了取得业务收益，而不仅仅是技术收益。所以，我们建议您根据组织的业务目标和业务优先级将这些指标进行收敛，主要聚焦业务驱动力和财务驱动力所对应的指标，其次才是技术驱动力的相关量化指标。我们推荐以下指标来制定组织的云化目标。

表 2-6 云化目标示例

量化指标	云化目标示例
业务系统的可用性SLO	业务系统全年可用性SLO从99%提升到99.95%。
新产品或新版本的TTM	将新产品的TTM从6个月缩短至3个月，已有产品的迭代周期从3个月缩短至1个月。
不合规及安全事件造成的经济损失	将不合规及安全事件数量减少75%，经济损失减少75%。
IT基础设施的TCO	将 IT 基础设施的 TCO 降低 15%。
业务创新和市场扩张带来的新增收入	基于云进行业务创新和全球市场扩展，在未来三年带来X万活跃用户，实现新增收入 Y 亿元。
碳排放减少量	上云后减少碳排放量 50%。
每个运维工程师可运维的资源数量	将每个运维工程师可管理的服务器数量提升 2 倍，从100台提升至200台。

2.6 分析云化收益

基于前面制定的云化目标，您接下来还需要对其进行收益分析，将其转换为财务收益，以便进行项目ROI评估，为管理层的战略决策提供依据。下面根据前面推荐的7个云化目标分别进行财务收益的评估，汇总后就能得到整个云化转型项目的总收益。

- **提升业务系统的可用性SLO**

  通过提高业务系统的可用性SLO，减少系统的停机时间，进而减少因停机导致的收入损失，因此可以基于业务系统的每小时停机损失来计算该指标的财务收益。假设某业务系统每小时停机损失为10万元。云化转型前的SLO为99%，每年停机损失为 10万元/小时 * 87.6小时 = 876万元；云化转型后的SLO为99.95%，每年的停机损失为10万元/小时 * 4.38小时 = 43.8万元。那么的每年财务收益为832.2万元。

- **缩短新产品或新版本的TTM**

  云化转型后，企业借助云平台提供的DevOps工具链、应用现代化和弹性计算资源可以大幅加速新产品的TTM和已有产品的迭代周期。如果新产品的TTM从6个月缩短至3个月，假设新产品每个月带来200万元的收入，那么提前3个月上市将带来600万元的额外收入。对于已有产品，如果将其版本迭代周期从3个月缩短至1个月，假设新版本每个月能带来100万元收入，那么新版本提前2个月上市将带来200万元额外收入。

- **减少不合规及安全事件造成的经济损失**

  云化转型后，企业利用云服务商提供的全面安全防护措施、合规审计工具和自动化合规报告可以大幅提升安全性和合规性。如果安全事件和不合规事件的数量从原来的每年20起减少到5起，假设每起安全事件平均造成20万元的处理和损失费用，那么总共每年可以减少300万元的经济损失。

- **降低IT基础设施的TCO**

  传统模式（自建数据中心）下企业按照预测的业务峰值需求准备硬件和软件等IT资源，但实际业务负载长期处于平均水平，导致资源长期处于低利用率状态，造成巨大的成本浪费。而云模式下企业按照实际业务负载弹性提供所需云资源，企业只需为实际使用的资源付费，将大幅降低IT基础设施的成本。计算传统模式和云模式下的TCO涉及很多成本项目，两种模式下的成本项目不同，例如传统模式下需要考虑机房建设和维护成本，但云模式下没有这些成本项目，这些成本已经隐含在云服务的价格中。下表是传统模式的成本构成，包括资本支出和运营支出。

表 2-7 传统模式的成本构成

成本类别	成本项目	成本项目的具体含义
资本支出（Capex）	硬件成本	服务器、存储设备、网络设备（路由器、交换机、防火墙等）的采购成本。
	软件成本	操作系统、虚拟化、数据库、中间件等软件的许可证费用。
	机房成本	如果是自建机房，包括机房的建设和装修成本、安保系统（包含视频监控和门禁设备等）的建设成本、电力供应系统和冷却系统的建设成本。如果是租赁IDC机房，主要是机架租赁成本，这个属于运营支出。
	实施成本	一次性的系统集成、测试、部署等费用。
运营支出（Opex）	人力成本	机房运维、IT运维和安保所需的人力成本，包括人员的薪资、福利和培训等费用。
	硬件维护成本	硬件设备的维护、维修、更新换代费用。
	软件维护成本	软件更新、补丁、技术支持等费用。
	机房维护成本	除硬件和软件维护之外，针对安保系统、电力供应系统和冷却系统等为维持机房正常运转所必须的维护费用。
	能源成本	运行整个数据中心的能源和电力费用。

成本类别	成本项目	成本项目的具体含义
	机架租赁成本	租用IDC机架的费用。
	带宽成本	互联网接入带宽费用。

企业云化转型之后，主要包含运营支出，成本构成如下表所示：

表 2-8 云模式的成本构成

成本类型	成本项目	成本项目的具体含义
运营支出（Opex）	计算资源成本	虚拟机、容器、无服务器计算等服务的费用，通常按使用时间、CPU、内存等计费。
	存储资源成本	对象存储、块存储、文件存储等服务的费用，通常按存储空间、请求次数、数据传输量等计费。
	网络资源成本	互联网带宽、公网IP地址、NAT网关、负载均衡器、VPN等网络服务的费用。
	数据库成本	关系型数据库、NoSQL数据库等服务的费用，通常按实例规格、存储空间、请求次数等计费。
	安全运营成本	为保护云上数据和应用系统的安全而使用网络防火墙、应用防火墙、数据安全保护等安全服务的费用。
	其他服务成本	中间件、大数据、人工智能、物联网等其他云服务的费用。
	云管理成本	监控、日志、运维、审计、治理等云管理服务的费用。
	云迁移成本	一次性的迁移上云、资源部署和集成测试的费用。
	技术支持成本	根据选择的支持计划，需要支付的技术支持费用。
	人力成本	IT运维人员（主要是应用运维）的薪资、福利、培训等费用。

另外，传统模式下还需要考虑IT设备的折旧，通常3-5年就需要针对IT设备进行升级换代。所以对比两者的TCO时不应该按照一年期进行对比，而是应该按照企业的IT设备折旧周期，也就是对比3-5年的TCO。

计算上述传统模式和云模式的成本是一项复杂的工作。其一，IT设备和云服务的价格是动态变化的，比如云服务商经常调整云服务的价格，您计算云服务的成本时可以参考华为云提供的**价格计算器**和商务优惠。其二，同样的IT设备和云服务在每个国家和地区的价格也不一样，电力价格和人力薪资在不同的国家和地区差距比较大。其三，您还需要获取当前IT资源的数量和配置规格，然后将其逐一映

射到不同规格的云资源，这样才能相对准确地估算两者的TCO。华为云提供了一个计算TCO的Excel模版，可以帮助您快速分析和对比传统模式和云模式的TCO，可以联系您的销售人员获取这个模版。另外，您计算人力成本时，需要考虑提升IT运维效率所节省的IT运维成本，计算方式可以参考下面的第7点：提升IT运维效率。

按照分析报告和众多企业的上云实践，云化转型通常可以减少10%~30%的IT基础设施TCO，假设企业在传统模式下3年期的IT基础设施TCO为8000万，云化转型之后预计将减少800万元~2400万元。

- **业务创新和市场扩张带来的新增收入**

  云化转型后，企业借助云平台的先进技术进行产品、服务和商业模式创新，基于云服务商的全球布局快速进军海外市场。如果通过业务创新和进军新市场可以为企业带来50万活跃用户，假设每个用户每年平均贡献收入60元，总共每年为企业带来3000万元的新增收入。

- **减少碳排放量**

  由于大型云数据中心的规模效应和更高效的能源利用，以及云服务商大量使用了可再生能源，企业在云化转型后可以大幅降低能耗和碳排放量。计算碳排放量是一个复杂的过程，涉及很多因素，可以利用云服务商提供的碳排放计算器。如果云化转型后碳排放量减少50%，每年的碳排放量从10000吨减少到5000吨，假设碳交易价格为100元/吨，那么每年因减少碳排放量的收益为50万元。

- **提升IT运维效率**

  云化转型后，企业无需管理IT基础设施，再借助云服务商提供的智能监控系统和自动化运维工具可以大幅提升IT运维效率。如果每个运维工程师可管理的服务器数量提升 2 倍，从100台提升至200台，假设企业总共有2000台服务器，每个运维工程师的年薪是20万元，那么每年总共可以节省200万元运维成本。需要注意的是该项收益包含在降低IT基础设施的TCO所带来的收益中，可以将本项收益汇总到那里。

  以上收益均为估算，实际收益需根据企业具体情况进行调整。这些收益包括成本节约、损失减少和收入增加等直接收益，但不包含因提升业务系统可用性、提升安全性和合规性、减少碳排放量所带来的公司品牌价值提升等间接收益。将上述收益汇总后就得到了整个云化专项项目的总收益，结合云化转型的总投资可以计算出ROI，为管理层的战略决策提供有力支撑。

2.7 制定云化转型战略

在识别驱动力、评估云化成熟度、制定云化目标和分析云化收益之后，您需要正式制定云化转型战略。制定云化转型战略通常包含以下步骤：设计云化转型的愿景、明确具体的云化目标、与干系人对齐目标、邀请高层正式发布战略，以及在组织范围内进行战略宣贯。关键在于确保与所有干系人进行充分的沟通，以在组织内部达成一致意见。这个过程可能需要经过多轮的讨论、平衡和修正，才能最终形成一致的战略方向。

步骤1 设计云化转型的愿景

首先是设计云化转型的愿景。愿景是组织对未来的期望和蓝图，是全体员工共同努力的方向。在制定愿景时，需要结合组织的使命、价值观以及对行业发展的洞察。愿景应该具有前瞻性、鼓舞性和指导性。例如，一个有力的愿景可以是：“通过云化转型，我们将构建一个灵活、高效、安全的数字化平台，赋能业务创新，提升客户体验，最终成为行业领先的智能化企业。”这个愿景明确了云化转型的目标——构建数字化平台，强调了灵活性、高效性和安全性，突出了赋能业务创新和提升客户体验，最后指向成为行业领导者的愿景。这种清晰而有感染力的愿景能够激励员工，为他们

提供清晰的奋斗目标。在制定愿景的过程中，领导团队需要深入思考组织的核心竞争力，以及云化转型将如何增强这些竞争力。同时，还需要考虑行业趋势、技术发展和客户需求，确保愿景的现实性和可行性。

步骤2 明确具体的云化目标

接下来，明确具体的云化目标是将愿景转化为可执行行动的关键一步。云化目标应该符合SMART原则，并且与组织的业务战略保持一致。例如，可以制定如“在两年内，将IT基础设施运营成本降低15%”或“在一年内，实现业务系统的弹性扩展能力，提高资源利用率30%”等目标。这些目标都有明确的衡量标准，便于后续的跟踪和评估。详细内容参考**制定云化目标** 。

步骤3 与干系人对齐目标

云化转型需要得到高层领导和各个干系人的支持和认同，因此需要与他们进行深入的沟通，确保云化转型的目标与各个干系人的目标一致。在这一步，组织可以召开高层战略会议，邀请CEO、CIO、各业务部门负责人以及关键的干系人参与。在会议上，详细介绍云化转型的愿景和业务目标，讨论转型对各部门的影响和预期收益。例如，IT部门可能关心技术架构的变化，而业务部门则关注云化如何支持业务增长。通过这样的沟通，可以使各方了解云化转型的重要性，认同其价值，并提出他们的建议和意见。在这个过程中，组织需要倾听干系人的关切，及时回应他们的问题，调整策略以适应实际情况。这种对齐过程有助于减少转型阻力，确保各部门协同合作。

步骤4 邀请高层正式发布战略

在与干系人对齐目标之后，组织需要正式将云化转型战略公之于众。这一举措不仅可以展示高层对云化转型的重视程度，还能够提高全体员工对战略的理解和认同。组织可以策划一次全员大会或线上直播活动，由CEO或其他高层领导正式发布云化转型战略。在发布会上，高层领导可以阐述云化转型的愿景和业务目标，分享他们对未来的期待，并表达对员工的期望。例如，CEO可以说：“云化转型是我们迈向数字化未来的重要一步，它将赋能我们的业务创新，提升客户体验。我相信，在大家的共同努力下，我们一定能够实现这个目标。”这种正式的发布能够增强战略的权威性，激发员工的参与热情。

步骤5 战略宣贯

在组织范围内进行战略宣贯是确保云化转型战略深入人心的关键步骤。战略宣贯需要针对不同层级、不同部门的员工，采用多种方式进行。组织可以开展一系列宣讲会、培训课程，制作宣传手册、视频等，详细讲解云化转型的意义、目标和具体举措。例如，组织可以在内部网站开设云化转型专栏，定期发布相关信息和进展。同时，各部门负责人应当积极向团队成员传达战略内容，结合部门实际情况，解释云化转型将如何影响他们的工作，以及他们可以做出哪些贡献。通过这些努力，组织能够增强员工对战略的理解和认同，形成全员参与的良好氛围。

----结束

综上所述，制定组织的云化转型战略是一个系统性、全面性的过程。通过制定清晰鼓舞的愿景，明确具体的业务目标，与干系人对齐目标，邀请高层正式发布战略，并在组织范围内进行深入的战略宣贯，组织能够为云化转型奠定坚实的基础。面对数字化时代的机遇和挑战，组织需要以战略性的眼光，积极拥抱云计算技术，走在行业的前列。

2.8 战略制定的反模式

在云化战略的制定过程中，一些常见的反模式可能会阻碍云化转型的成功，甚至导致企业资源的浪费和业务的中断。识别并避免这些反模式，对于确保云化转型取得成功至关重要。以下是几种常见的反模式，以及对应的优化建议。

- **云化战略与业务战略没有对齐**

  这种反模式表现为云化转型缺乏与公司整体业务战略的紧密结合，成为IT部门的孤立行为。云化战略的目标与业务目标脱节，高层领导对云化转型的意义和价值缺乏认识，导致支持不足或参与度低。这将导致资源投入不足，转型方向偏离，最终难以实现预期的业务价值。例如，企业为了上云而上云，选择了最新的云技术，却没有考虑这项技术是否能真正解决业务痛点，提升业务效率，反而增加了成本和复杂性。

  针对这个反模式的优化建议如下：

  - **将云化转型战略与业务战略紧密结合：** 明确云化转型如何支持业务目标的实现，例如加速业务创新、降低成本、提升客户体验、开拓新市场等。用业务语言阐述云化转型的价值，避免使用纯粹的技术术语。
  - **获得高层领导的支持和参与：** 向高层领导汇报云化转型的价值和预期业务收益，争取他们的支持和资源投入。邀请高层领导参与到云化转型战略的制定和执行过程中，确保转型方向与公司整体战略一致。

- **云化战略只关注技术收益，忽略业务收益**

  这种反模式表现为过度关注技术指标的提升，例如资源弹性、数据存储容量或SLO等，而忽略了云化转型对业务的实际影响。虽然技术指标的提升很重要，但最终目的是要通过技术改进带来业务价值。如果只关注技术收益，可能会导致投资回报率低，甚至对业务造成负面影响。例如，企业上云后过度追求性能、弹性和可靠性等技术收益，但忽略了成本优化和运营，导致上云后成本增长过快。

  针对这个反模式的优化建议如下：

  - **以业务为中心制定云化目标：** 从业务需求出发，确定云化转型的目标和方向。将技术指标的提升与业务收益挂钩，例如通过提升系统韧性、扩展性、安全性来提升业务连续性，请参考章节**制定云化目标** 。
  - **量化业务收益：**基于前面制定的云化目标，对其进行收益分析，将其转换为财务收益，以便进行项目ROI评估，为管理层的战略决策提供依据，请参考章节**分析云化收益** 。
  - **持续跟踪和评估业务收益：** 定期评估云化转型的业务收益，并根据实际情况调整云化目标。

- **云化战略缺乏与干系人的对齐**

  云化转型涉及到公司内部的多个部门和团队，例如IT部门、业务部门、财务部门等，以及外部的合作伙伴和客户。如果缺乏与所有干系人的沟通和对齐，可能会导致转型过程中出现阻力，甚至失败。例如，IT部门在没有与业务部门充分沟通的情况下，就开始了业务系统的迁移上云工作，导致业务系统中断，影响了业务运营。

  针对这个反模式的优化建议如下：

  - **干系人利益分析：** 识别所有参与云化转型决策或受云化转型影响的部门、团队和个人。了解不同干系人的利益诉求，并制定相应的策略来满足他们的需求，减少潜在的阻力。请参考章节**干系人利益分析**。

- **积极开展沟通：** 制定详细的沟通计划，明确沟通的目标、内容、方式和时间表。采用多种沟通方式，例如会议、培训、邮件、内部网站等，确保所有干系人都能了解云化转型的进展和影响，以及需要干系人提供什么样的支持。
- **意见反馈机制：** 建立意见反馈机制，鼓励干系人提出意见和建议，并积极采纳合理的建议。

企业进行云化转型是一个复杂且充满挑战的过程。成功的云化转型需要仔细的规划、充分的沟通和持续的优化。通过识别和避免上述反模式，企业可以更好地管理云化转型风险，确保转型战略与业务战略对齐，最终实现预期的业务价值，并为企业未来的发展奠定坚实的基础。

3 顶层规划

3.1 概述

企业云化转型是一项复杂和系统的工程，涉及组织和流程、平台和架构、运维和管理等多个层面。如同建造摩天大楼，在挖地基之前就需要设计蓝图，企业在构建云基础设施和将业务系统上云之前，也需要进行全面而清晰的顶层规划。只有在充分的规划和准备下，才能最大程度地发挥云的优势，实现业务价值的最大化。

在组织和流程方面，首先需要设计云卓越中心CCoE（Cloud Center of Excellence）。CCoE作为推动企业云化转型的核心团队，负责制定云标准、最佳实践和治理框架，协调各业务单元之间的合作，确保云化转型的高效推进。此外，应用生命周期管理流程也需要进行变革，传统的开发和部署模式难以适应云环境的快速迭代需求，引入敏捷开发、DevOps等先进方法，可以提高开发效率，缩短交付周期，提高对市场变化的响应能力。

在平台和架构方面，Well-Architected Framework（WAF）提供了一套最佳实践和架构设计原则，帮助企业在云上构建高安全、高可用、高性能且成本优化的云基础设施和应用系统。Landing Zone 的规划和设计则为企业提供了安全合规、易扩展的云上多账号运行环境，可以加速应用部署并提高安全性。此外，平台工程的规划设计也很重要，它为开发团队提供标准化的工具、流程和基础设施支持，提高开发效率、减少复杂性，并加速软件交付。

在运维和项目管理方面，云运营模式的设计对于高效协同CCoE和应用团队至关重要。根据企业内部的协作方式和应用系统的特征建立最合适的云运营模式，可以有效保障应用系统的敏捷迭代和稳定运行。同时，制定详尽的云化转型项目管理计划，涵盖项目计划、项目任命、进度管理、风险管理等方面，能够确保各项工作按计划有序推进，提升项目的透明度和可控性，降低实施过程中的不确定性。

总而言之，企业要成功实现云化转型，必须在前期进行充分的顶层规划和设计。这包括构建卓越的组织结构、优化的流程、高效的平台和架构、完善的云运营模式和项目管理。缺乏这些关键的顶层设计，可能导致大量应用系统上云后的混乱无序和风险激增，事后整改不仅成本高昂，还可能对业务系统的稳定性造成严重冲击。因此，前期的顶层规划对于云化转型的顺利实施和长期成功至关重要。

3.2 云卓越中心

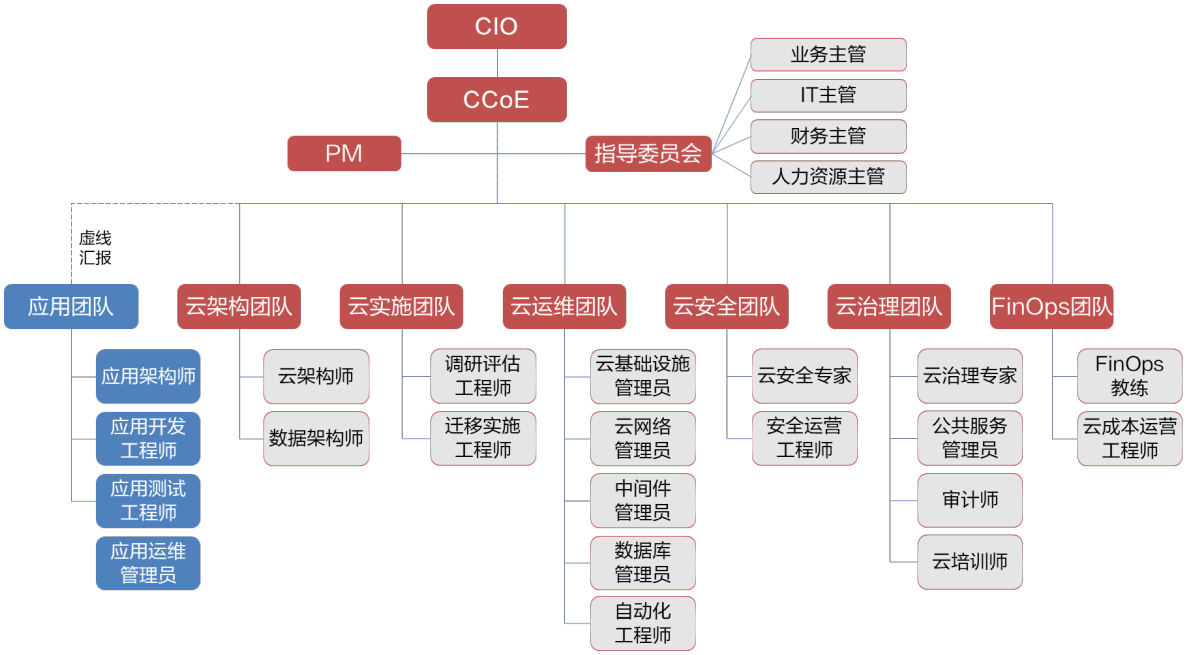
3.2.1 云卓越中心简介

如上述所，企业云化转型是一项复杂和系统的工程，需要组建一个云卓越中心（CCoE）来领导、协调和推进整个云化转型项目。CCoE是企业内部为云化转型专门成立的中心化团队，全程负责整个云化旅程，包括制定战略、顶层规划、调研评估、方案设计、采用实施和运维治理，其目标是通过提供最佳实践、指导和资源，帮助企业最大化云计算的价值，确保云化转型项目的成功实施。CCoE的主要责任如下：

- **制定云化战略：**负责制定符合企业业务目标的云化战略，评估云化成熟度，明确云化目标和预期收益，并规划具体的实施路线。
- **云化转型顶层规划：**负责云化转型项目的顶层规划和设计，包括应用云化流程优化、Landing Zone设计、平台工程设计、云运营模式设计等。
- **建立云治理框架：**负责制定云平台的治理框架、治理策略、安全标准、合规性要求等，确保云基础设施和应用系统的安全、稳定和合规。
- **提供云技术支持：** 为企业内部提供云技术方面的培训、咨询和支持，帮助各部门更好地理解和应用云技术。
- **管理云平台和资源：** 负责管理云平台的日常运营，包括资源分配、成本控制、性能监控等。
- **推动云最佳实践：** 负责推广云最佳实践，例如 云采用框架CAF和卓越架构技术框架WAF，帮助企业构建高效、可靠、安全的云基础设施和应用系统。
- **供应商管理：**评估和管理云服务商，根据自身业务需求，选择最合适的云服务商及其优势服务，最大化地发挥云计算的价值。
- **促进跨部门协作：** 作为跨部门的协调中心，促进业务部门、IT 部门和其他相关部门之间的沟通和协作，确保云化转型项目的顺利进行。
- **持续改进和优化：** 持续跟踪云化转型的进展，并根据实际情况进行调整和优化，确保云化转型目标的最终实现。

为了使CCoE发挥最大效能，必须协同企业范围内的干系人共同组建CCoE，包括业务部门、IT部门、财务部门、人力资源部门的专业人士等都应该加入到CCoE团队，形成一个跨职能的团队。这不仅能确保云化转型与业务目标紧密结合，还能在转型过程中有效解决各种问题。我们建议CCoE组织应该由CIO直接领导，这样可以有效提升云化转型过程中重要工作的汇报和决策效率。根据华为公司自身的云化转型成功经验和我们帮助大量客户云化转型所积累的成功经验，我们推荐如下CCoE组织结构及主要角色，您可以将其作为起点，基于您的IT组织的现状、员工技能水平和云化目标对其进行裁剪和完善，设计最适合您企业的CCoE组织结构。

图 3-1 云卓越中心组织结构



针对上面的CCoE组织结构中包含的团队和角色，下面详细描述对应的职责和技能要求，我们也提供了从哪里获取这些人力资源的建议。需要注意的是，这些角色并不需要由不同的员工承担，您可以根据企业的人力预算和员工的技能水平，让同一名员工承担多个角色。

3.2.2 指导委员会

指导委员会负责为云化转型项目提供建议、战略指导和决策支持，在云化转型中扮演着至关重要的作用。指导委员会的成员应该由云化转型的重要干系人（CEO、CIO、CTO、CFO、CISO、业务主管等）指定和委派，至少应该包含业务主管、IT主管、财务主管和人力资源主管。指导委员会按照内阁制进行集体决策，共同承担以下职责：

- **制定云化战略：**负责制定符合企业业务目标的云化战略，评估云化成熟度，明确云化目标和预期收益，并规划具体的实施路线。
- **筹备CCoE：**负责筹备和组建CCoE组织，明确CCoE组织内各个角色的职责和技能要求，协调相关部门快速获取CCoE所需要的各类人力资源。
- **云化转型顶层规划：**指导云架构团队、云运维团队、云安全团队和云治理团队等成员进行云化转型的顶层规划，包括应用云化流程优化、Landing Zone设计、平台工程设计、云运营模式设计等，对顶层设计的效果承担最终责任。
- **明确业务需求：**从业务角度出发，明确云化转型的具体需求和期望，例如提升业务连续性、业务敏捷性、增加收入等。
- **审批和监控预算：**负责审核和批准云化转型相关的预算，并监控预算执行情况，确保资金的合理使用和成本的有效控制。
- **人力资源管理：**负责CCoE成员的招聘、选拔、培养和留任，打造一支稳定和高绩效的CCoE组织。
- **跨部门协作：**促进业务部门、IT部门和其他相关部门之间的沟通和协作，确保云化转型方案得到各方的理解和支持，避免出现部门间的冲突和阻碍。
- **评估云化转型效果：**负责评估云化转型的效果和价值，例如成本节约、效率提升、业务创新等，并根据评估结果对转型策略进行调整和优化。

- **决策关键事项：**指导委员会是云化转型中的最高决策机构，负责对云化转型过程中的关键事项做出决策，例如云服务商的选择、技术方案的确定、实施计划的调整等。

3.2.3 应用团队

企业内部通常有多个业务部门，每个业务部门负责自身所需业务系统的投资、建设和运维，因此通常在业务部门会组建自己的应用团队。将这些业务系统云化需要应用团队的配合和协同，应用团队需要协同云实施团队进行业务系统的现状调研、迁移实施、应用现代化改造和测试验证，协同云架构团队基于云技术和云服务设计业务系统的云上应用架构，协同云运维团队确保业务系统在云上的长期安全稳定运行。应用团队的成员通常都来自于业务部门，因为不同的业务部门拥有独立的应用团队，所以应用团队可能是多个，这些应用团队虚线汇报给CCoE团队，应用团队通常包含应用架构师、应用开发工程师、应用测试工程师和应用运维管理员，其职责和技能要求如下表所示。

表 3-1 应用团队的角色和职责

角色	职责	技能要求	来源
应用架构师	• 明确业务系统云化的业务收益，如业务连续性、业务敏捷性等。 • 负责制定业务系统的迁移策略（Rehost、Replatform、Refactor等）和迁移顺序。 • 支撑云实施团队提供业务系统的现状进行调研，为其提供资源现状、应用架构、部署架构、依赖关系等信息。 • 负责设计和管理业务系统在云上的应用架构，包括应用的架构模式、技术选型、部署方式等，确保应用的性能、可扩展性、安全性和可靠性。 • 与数据架构师和云架构师紧密合作，确保应用架构与数据架构和云架构的兼容性。 • 指导开发团队进行应用开发和部署。	• 深入理解各种应用架构模式和设计模式，例如微服务架构、事件驱动架构等。 • 熟悉各种开发语言和框架。 • 熟悉DevOps实践和工具。 • 具备良好的代码设计和开发能力。 • 了解应用安全最佳实践。 • 具备良好的沟通和团队协作能力。	业务部门

角色	职责	技能要求	来源
应用开发工程师	• 将现有应用迁移到云平台，包括代码迁移、数据迁移、数据库迁移等。 • 负责应用现代化改造，如将单体应用拆分为微服务，或采用Serverless和事件驱动架构。 • 对现有代码进行重构，使其更具可维护性、可扩展性和可测试性，并针对云环境进行优化，例如利用云原生服务和API。	• 精通至少一门主流编程语言，例如 Java、Python、Go等 • 熟悉DevOps实践和工具。 • 具备良好的代码设计和开发能力。 • 熟悉主流的云平台及云服务。 • 能够与周边团队有效沟通和协作。	业务部门
应用测试工程师	• 针对云上业务系统设计测试用例并制定测试计划。测试用例包括功能测试、性能测试、安全测试和可靠性测试等用例 • 按照测试计划和测试用例，选择合适的测试工具对云上业务系统进行全方面的功能、性能、安全性和可靠性等测试。 • 编写和维护自动化测试脚本。 • 编写测试报告和文档。	• 有扎实的测试理论基础，熟悉软件测试理论、方法和流程等。 • 具备丰富的测试经验，熟悉各种测试类型，如功能测试、性能测试、安全测试和可靠性测试等。 • 熟悉主流的云平台及云服务。 • 熟练使用自动化测试工具，能够编写自动化测试脚本。 • 能够与周边团队有效沟通和协作。	业务部门
应用运维管理员	• 负责云上业务系统的部署、监控和维护，确保业务系统的安全稳定运行。 • 处理应用运行中的故障，优化应用性能。 • 配合开发团队进行应用的版本更新和发布。 • 监控应用日志，分析并解决潜在问题。	• 熟悉云平台的APM服务，具备应用性能监控和日志分析能力。 • 掌握CI/CD工具和容器编排工具。熟悉常见的应用部署方式（如容器化、微服务架构）。 • 熟悉常见中间件（如Nginx、Redis、Kafka）的运维管理。	业务部门

3.2.4 云架构团队

云架构团队在云化转型中发挥着关键作用，参照TOGAF框架和卓越架构技术框架架（Well-Architected Framework），全面负责设计云上的技术架构和数据架构，协同应用架构师基于云技术和云服务设计业务系统的云上应用架构，帮助企业在云上构建高安全、高可用、高性能且成本优化的云基础设施和应用系统。云架构团队通常包含云架构师和数据架构师，其职责和技能要求如下表所示。

表 3-2 云架构团队的角色和职责

角色	职责	技能要求	来源
云架构师	• 负责云平台和云基础设施的整体规划和架构设计，包括Landing Zone、平台工程、网络、存储、安全、灾备等方面，确保云基础设施的安全性、可靠性、性能和成本效益。 • 选择合适的云服务商和云服务类型。 • 制定和推广云上架构设计原则，赋能应用架构师和数据架构师在云上设计良好的技术架构。 • 领导和指导云实施团队，确保技术方案的落地。	• 深入理解云计算技术和架构，熟悉主流云平台。 • 具备丰富的Landing Zone、平台工程、网络、安全、存储、灾备等方面的知识和经验。 • 熟悉TOGAF和WAF等架构框架。 • 具备良好的沟通能力、团队合作精神和领导力。	企业架构师团队或者外聘
数据架构师	• 负责设计和管理企业在云上的数据架构，包括数据存储、数据处理、数据集成和数据治理。 • 选择合适的数据存储方案，例如关系型数据库、NoSQL数据库、数据仓库等。 • 确保数据的质量、安全性和合规性。 • 与应用架构师和云架构师紧密合作，确保数据架构与整体架构的兼容性。	• 深入理解数据建模、数据仓库、数据湖、数据治理等概念和技术。 • 熟悉各种数据库技术，包括关系型数据库和NoSQL数据库。 • 熟悉大数据技术，例如Hadoop、Spark、Flink等。 • 具备数据分析和数据挖掘能力。 • 熟悉数据安全和数据隐私相关的法规和标准。 • 具备良好的沟通和团队协作能力。	大数据部门或外聘

3.2.5 云实施团队

云实施团队负责将企业内各个业务系统迁移或者直接部署到云上，这要求对企业现有的IT基础设施和业务系统进行详细的调研和评估，设计并实施技术方案。技术方案的设计由云架构团队负责，交给云实施团队负责方案实施，云实施团队通常包含调研评估工程师、迁移实施工程师，职责和技能要求如下表所示。需要注意的是，这两个角色所负责的工作不是持续性的，业务系统全部上云之后也就不再需要了，所以这两个角色可以由IT部门内具备相关技能的工程师临时承担，或者外包给云迁移实施的专业服务提供商。

表 3-3 云实施团队的角色和职责

角色	职责	技能要求	来源
调研评估工程师	• 现状调研：对企业现有的IT基础设施、业务系统、应用架构、数据存储、安全策略等进行全面的调研和文档记录，包括硬件配置、软件版本、依赖关系、性能指标、安全漏洞等。 • 需求分析：业务部门沟通，了解其对云化转型的需求和期望，例如性能提升、成本优化、灾备恢复等，并将这些需求转化为具体的技术指标。 • 可行性评估： 评估将现有系统迁移到云平台的可行性，包括技术可行性、成本效益、风险评估等。 • 容量规划：根据业务需求和未来发展趋势，对云资源进行容量规划，例如计算资源、存储资源、网络带宽等。 • 成本估算：根据云服务商的定价模型，估算迁移到云平台的成本，并与传统IT架构的成本进行比较，为决策提供依据。	• 熟悉主流的云平台及云服务。 • 具备扎实的IT基础设施知识，包括服务器、网络、存储、数据库、中间件等。 • 熟悉各种操作系统和应用软件。 • 了解不同的迁移策略和方法。 • 具备一定的IT基础设施和业务系统的调研和评估经验。 • 具备良好的沟通和团队协作能力。	IT部门或者外包给云实施专业服务提供商
迁移实施工程师	• 迁移方案实施：根据架构师设计的技术方案和调研评估工程师提供的报告，具体实施业务系统的迁移和部署工作，包括环境搭建、数据迁移、应用部署、配置调整等。 • 测试和验证：对上云后的系统进行全面的测试和验证，确保系统功能正常、性能稳定和安全可靠。 • 故障排除：及时处理实施过程中出现的各种问题和故障，确保实施工作的顺利进行。	• 精通主流的云平台及云服务，并具备相关的认证资质。 • 熟悉各种迁移工具和技术，例如数据迁移工具、容器化技术、自动化部署工具等。 • 熟悉各种操作系统和应用软件。 • 具备扎实的脚本编写能力（例如Shell、Python等），能够实现自动化操作。 • 具备良好的沟通和团队协作能力。	IT部门或者外包给云实施专业服务提供商

3.2.6 云运维团队

云运维团队负责云基础设施的日常管理与维护，确保云基础设施的高可用性、高安全和高性能，协同应用运维管理员保障云上业务系统的长期安全稳定运行，并不断通过自动化和智能化技术提升运维效率。云运维团队通常包含云基础设施管理员、云网络管理员、数据库管理员和自动化工程师，职责和技能要求如下表所示。

表 3-4 云运维团队的角色和职责

角色	职责	技能要求	来源
云基础设施管理员	• 负责云平台上存储、虚拟机、操作系统等基础设施的日常运维管理。 • 监控和优化云资源的使用效率，确保资源分配合理。 • 处理虚拟机、存储和操作系统相关的故障，保障系统的高可用性。 • 定期进行系统补丁更新和安全加固。	• 熟悉主流云平台的虚拟机和云存储服务。 • 掌握Linux和Windows操作系统的管理与优化。 • 熟悉云原生的监控运维工具。 • 具备一定的脚本编写能力。 • 具备良好的故障排除和问题解决能力。	IT部门
云网络管理员	• 负责云平台网络架构的设计、配置和日常运维，保障网络稳定和安全。 • 管理VPN、专线、VPC、子网、网络ACL、路由、负载均衡、防火墙等网络组件。 • 监控网络性能，排查网络故障，优化网络延迟和带宽使用。 • 确保网络安全，防范DDoS攻击等网络威胁。	• 熟悉云平台的网络服务（如VPC、VPN、专线、负载均衡、防火墙等）及其配置。 • 熟悉TCP/IP、HTTP、DNS、TLS等网络协议。 • 具备网络故障排查能力。 • 熟悉网络安全技术（如防火墙规则配置、入侵检测等）。	IT部门
中间件管理员	• 负责消息队列 (例如 Kafka, RabbitMQ)，Web 服务器 (例如 Nginx, Apache)，应用服务器 (例如 Tomcat, JBoss)，缓存服务 (例如 Memcached, Redis) 等的安装、配置和维护。 • 监控中间件服务的性能指标，识别性能瓶颈，并进行调优以提高性能和效率。 • 快速诊断和解决中间件服务出现的故障和问题，确保业务的连续性。	• 熟练掌握常用的中间件技术，例如 Kafka, RabbitMQ, Nginx, Tomcat等。 • 熟悉主流云平台的中间件服务的部署和管理。 • 熟悉操作系统，例如 Linux, Windows Server 等。 • 了解 DevOps 理念和实践。 • 具备一定的脚本编写能力。 • 具备良好的故障排除和问题解决能力。	IT部门

角色	职责	技能要求	来源
数据库管理员	● 负责云上数据库的部署、配置、监控和维护。 ● 确保数据库的高可用性和数据安全，定期进行备份和恢复演练。 ● 优化数据库性能，解决查询慢、锁等待等问题。 ● 管理数据库的权限和访问控制，确保数据合规性。	● 熟悉云平台的数据库服务和数据库管理服务。 ● 熟悉主流数据库（如MySQL、PostgreSQL等）的管理。 ● 掌握数据库性能优化技术（如索引优化、分库分表）。 ● 具备数据库备份与恢复、主从同步、分布式架构的运维经验。 ● 熟悉数据库安全策略和数据加密技术。	IT部门
自动化工程师	● 开发和维护自动化运维工具，提升运维效率。 ● 实现云资源的自动化部署、监控和扩展。 ● 编写脚本或代码实现日常运维任务的自动化。 ● 推动智能化运维技术的应用，如AIOps。	● 熟悉自动化工具（如Ansible、Terraform、SaltStack等）。 ● 掌握脚本语言（如Python、Shell）和云平台API的使用。 ● 具备DevOps理念，熟悉CI/CD流程和工具。 ● 了解AIOps相关技术。	IT部门

3.2.7 云安全团队

云安全团队负责云基础设施和云上业务系统的安全保障工作，主要职责包括云平台安全方案设计、访问控制与权限管理、安全监控与威胁检测、漏洞扫描与修复、数据加密与隐私保护、合规性审查与风险评估，以及应急响应与安全事件处理，确保云上业务系统的安全性、合规性和稳定性。云安全团队通常包含云安全专家、安全运营工程师，职责和技能要求如下表所示。

表 3-5 云安全团队的角色和职责

角色	职责	技能要求	来源
云安全专家	• 负责云平台整体安全方案的设计与优化，制定安全策略和标准。 • 评估云基础设施和业务系统的安全风险，提出改进方案。 • 设计并实施身份安全、网络安全、数据安全、应用安全、主机安全和安全运维方案。 • 指导和审核安全运营工程师的工作，提供技术支持。 • 跟踪最新的安全技术，制定应对策略。	• 深入了解云平台的云安全服务和安全配置基线。 • 熟悉身份安全、网络安全、数据安全、应用安全、主机安全和安全运维等领域。 • 掌握安全评估工具和渗透测试技术。 • 具备安全合规（如等保2.0、ISO 27001等）的管理经验。 • 优秀的安全策略制定和技术指导能力。	IT部门
安全运营工程师	• 设计并实施持续安全运营方案。 • 负责云平台的日常安全监控与运维，及时发现并处理安全事件。 • 执行漏洞扫描、补丁管理和安全配置加固。 • 实施访问控制、权限管理和日志审计，确保系统合规性。 • 配合云安全专家完成安全技术方案的落地与优化。 • 编写安全运维脚本，提升安全运营效率。	• 熟练使用云平台的安全运营服务和各种安全监控工具。 • 掌握威胁检测技术、漏洞扫描工具和补丁管理流程。 • 熟悉日志分析工具和自动化脚本语言（如Python、Shell）。 • 了解云平台的安全配置（如安全组、防火墙规则）。 • 具备快速响应和处理安全事件的能力。	IT部门

3.2.8 云治理团队

云治理团队的职责是识别企业云化转型过程中的各种风险，并制定和实施有效的治理框架、策略和流程，目的是将企业云化转型的风险最小化，并最大化业务收益。云治理团队通常包含云治理专家、审计师和云培训师，职责和技能要求如下表所示。

表 3-6 云治理团队的角色和职责

角色	职责	技能要求	来源
云治理专家	• 识别和评估云化转型的各种风险，并制定相应的缓解措施。 • 制定和维护云治理框架，包括策略、标准、流程和指南，推动云治理最佳实践的落地和执行。 • 确保云治理策略与业务目标对齐。 • 持续优化云治理框架，以适应不断变化的业务需求和技术发展趋势。 • 监控云环境的合规性和安全性。	• 深入理解云架构、云安全、云成本优化等方面的知识。 • 熟悉主流云平台的云服务和最佳实践。 • 具备丰富的风险管理、合规性管理和IT治理经验。 • 优秀的跨部门沟通、协作和问题解决能力。	IT部门
公共服务管理员	• 识别各个业务单元所需要的公共IT服务和资源，比如NTP服务器、AD服务器、自建DNS服务器、OBS桶、容器镜像库等，也可以是CodeArts等PaaS服务。 • 负责集中部署和维护这些公共IT服务，并将其共享给公司内所有业务单元使用。 • 保障公共IT服务的安全稳定运行。	• 熟悉主流云平台的IaaS和PaaS服务，并能熟练部署这些服务。 • 熟悉云平台之上实现资源共享的技术方案，如基于网络的共享、基于资源权限策略的共享和华为云资源共享服务**RAM**。 • 具备良好的跨部门沟通、协作和问题解决能力。	IT部门
审计师	• 对云环境进行定期审计，评估其是否符合相关的法规、标准和最佳实践。 • 识别云环境中的安全漏洞和合规性风险。 • 撰写审计报告，并提出改进建议。 • 与云治理专家和相关团队合作，解决已识别的风险。 • 跟踪和监控改进措施的实施情况。	• 熟悉云安全、合规性审计和风险评估方法。 • 熟悉相关的法规和标准，例如等保2.0、ISO 27001等。 • 具备数据分析和报告撰写能力。 • 拥有良好的沟通和人际交往能力。 • 具备一定的云技术知识。	IT部门

角色	职责	技能要求	来源
云培训师	• 开发和交付云计算相关的培训课程，涵盖云基础设施、云架构设计、云运维、云安全等方面。 • 推广用云和管云的最佳实践，通过最佳实践减少云化风险。	• 扎实的云技术知识和实践经验。 • 优秀的教学能力和沟通技巧，能够将复杂的云技术概念清晰地传达给他人。 • 熟悉不同的培训方法和工具。	外包给云服务商

3.2.9 FinOps 团队

FinOps团队的主要职责是通过成本生命周期管理和持续成本运营，推动团队在预算内高效使用云资源，不断提升云资源的成本效益，实现业务价值最大化。FinOps团队通常包含FinOps教练、云成本运营工程师，职责和技能要求如下表所示。

表 3-7 FinOps 团队的角色和职责

角色	职责	技能要求	来源
FinOps教练	• 指导和培训团队成员理解和应用FinOps原则和最佳实践，不断学习云成本优化的新方法并进行推广。 • 协助制定和实施云成本管理策略，确保各部门在预算内高效使用云资源。 • 促进跨部门协作，推动成本优化和资源利用率提升。 • 在组织内部推广FinOps文化和理念。	• 深入了解FinOps框架和云成本管理最佳实践。 • 熟悉主流云平台的计费模式和成本管理工具。 • 熟悉常用的云成本优化方法。 • 具备项目管理能力，能够推动跨部门的协作和变革。	IT部门内部培养或者外聘
云成本运营工程师	• 监控和分析云资源的使用情况，识别成本节约机会。 • 生成详细的成本分析报告，为决策提供数据支持。 • 与云运维团队和应用团队合作，优化应用系统的成本效益。 • 实施成本优化策略，例如改变计费模式、购买资源包、关闭闲置资源等。	• 熟悉云平台的成本管理工具。 • 熟悉各种云服务的计费模式。 • 具备数据分析能力，能够从大量数据中提取有价值的见解。 • 具备良好的沟通能力，能够与技术和财务团队有效协作。	IT部门内部培养或者外聘

3.2.10 云项目经理

云项目经理在指导委员会的授权下，负责领导和管理整个云化转型项目，确保项目在预算内按时完成，并符合质量标准。其主要职责包括：

- **项目计划与目标设定:** 制定云化转型的整体计划，包括项目范围、目标、时间计划、预算和验收要求等。
- **项目执行与进度管理:** 监督项目的执行过程，确保各阶段任务按计划完成；跟踪项目进度，识别潜在问题并及时采取措施，确保项目按时交付。
- **预算与成本控制：** 监控云资源的使用和成本，确保项目在预算范围内运行；识别并实施成本优化措施，提升云化转型的经济效益。
- **质量管理：** 确保交付成果符合既定的质量标准和业务需求；组织质量评审，确保技术方案的稳定性、安全性和可扩展性。
- **沟通和协作:** 与利益相关者（包括业务部门、IT部门、财务部门、云服务商等）进行有效沟通，确保项目信息透明，并获得各方支持。
- **风险管理:** 识别、评估和管理项目风险，制定应急计划，并将风险最小化。
- **变更管理:** 管理项目变更，确保变更得到适当的评估和批准，并对项目的影响最小化。

云项目经理是一个综合管理角色，不仅需要有扎实的项目管理能力，还要求具备一定的云技术知识和业务理解能力，其技能要求如下：

- **项目管理技能:** 具备扎实的项目管理知识和经验，熟悉PMBOK项目管理方法论，能够熟练运用项目管理工具和技术。
- **云技术知识:** 深入理解云计算的概念、架构和服务，熟悉不同的云部署模型（公有云、私有云、混合云），了解主流云平台的特点和优势。
- **沟通和协调能力:** 优秀的沟通、协调和人际交往能力，能够有效地与不同团队和利益相关者沟通协作，具备跨部门沟通和协调能力。
- **问题解决能力:** 能够快速识别和解决项目中出现的问题和挑战，具备分析问题、制定解决方案和推动落地的能力。
- **领导力:** 能够领导和激励整个云化转型项目团队，确保团队高效协作，营造积极的团队氛围。
- **业务理解能力:** 能够理解业务需求，并将业务需求转化为技术方案，确保云化转型项目能够真正为业务带来价值。
- **成本管理能力:** 具备成本意识，能够有效地控制项目成本，并在项目生命周期中进行成本优化。

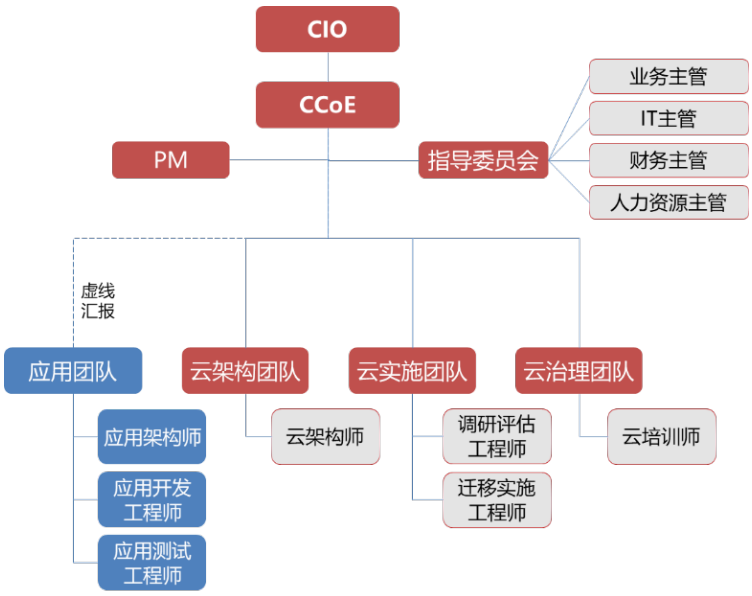
3.2.11 云卓越中心的演进

上述CCoE组织是针对企业大规模上云、用云和管云而建立的全功能团队，企业并不需要在云化转型早期就组建一个完整的CCoE组织。

云化转型早期主要是把第一批业务系统迁移或直接部署在云上，这个时候可以建立一个小型化CCoE组织，如下图所示，把必要的角色加入进来，足以支撑第一批业务系统的云化就可以。

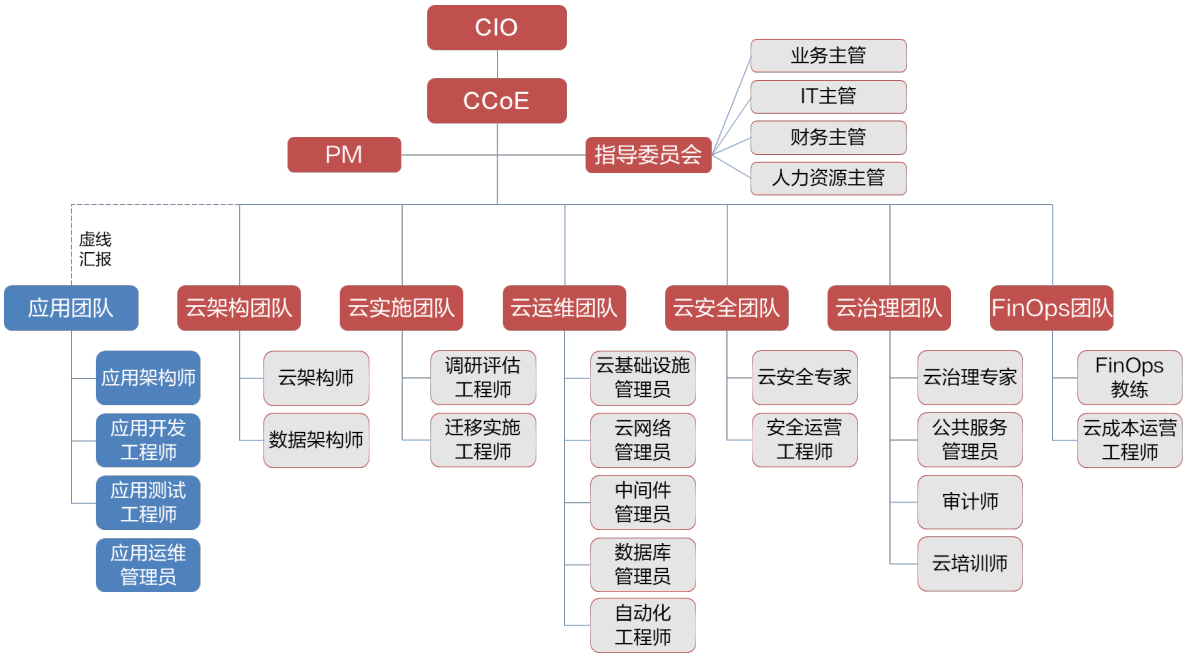
我们认为在早期的小规模CCoE组织中应该包含指导委员会、云项目经理、应用架构师、应用开发工程师、应用测试工程师、云架构师、调研评估工程师、迁移实施工程师等关键角色。通过这些角色的协同努力将第一批业务系统逐步云化，快速获取业务收益，从而推动企业将更多的业务系统逐步云化。

图 3-2 小型化 CCoE 组织架构



当企业云化转型的规模逐步变大，云化转型进入运维治理阶段的时候，可以将小型化的CCoE组织逐步扩大，增加更多的运维治理阶段所需的关键角色，如云基础设施管理员、云网络管理员、数据库管理员、应用运维管理员、云治理专家、安全运营工程师、云成本运营工程师等，逐步演进到如下全功能的CCoE组织。

图 3-3 全功能 CCoE 组织架构



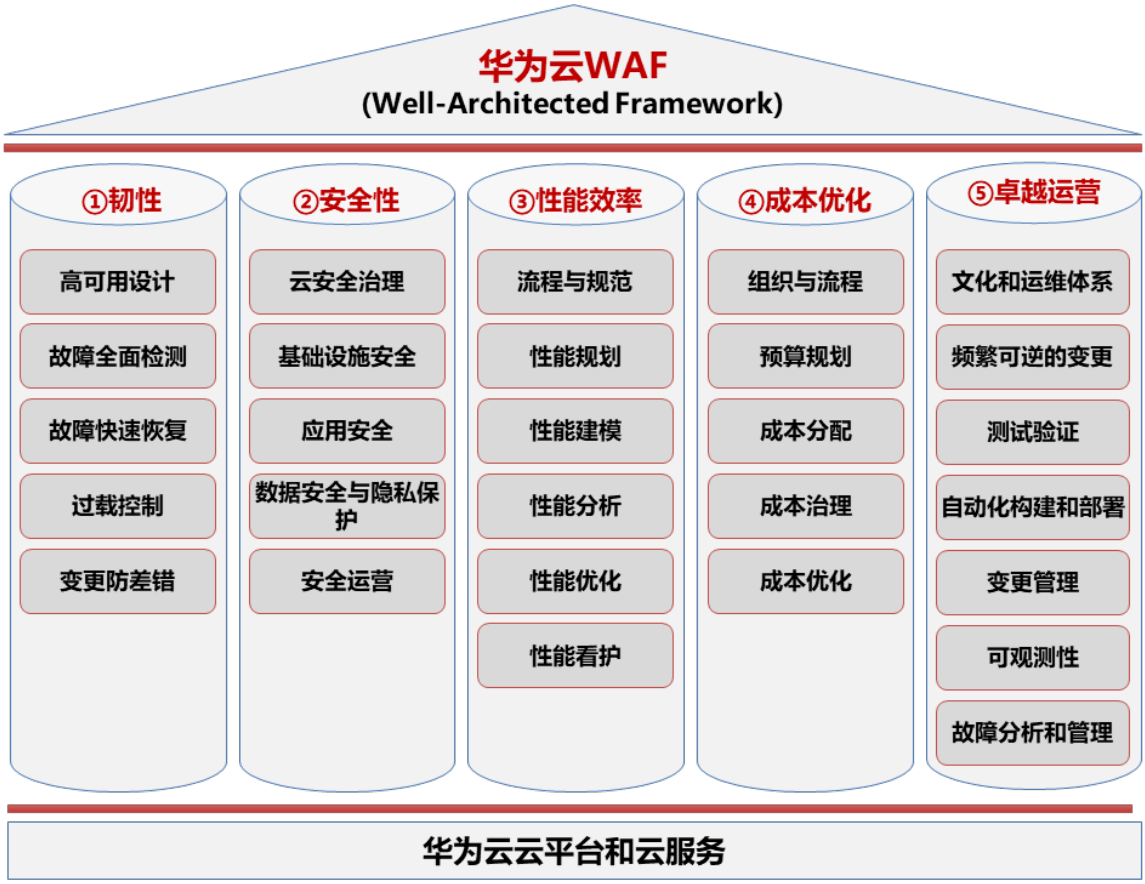
3.3 卓越架构设计

我们基于华为公司自身的云上架构设计经验和业界最佳实践整理了**卓越架构技术框架**（Well-Architected Framework，简称WAF），为架构师、软件工程师、运维工程师

等技术人员提供一套云上架构设计原则和最佳实践，其目的是帮助企业在云上设计、构建和运营高韧性、高安全、高性能且成本最优的应用系统。

WAF涵盖了五大支柱，如下图所示。

图 3-4 华为云卓越架构技术框架（Well-Architected Framework）



- **韧性支柱**

  韧性支柱关注系统在面对故障、压力和变化时的持续可用性和可靠性。它强调通过设计冗余组件、故障全面检测、过载控制和故障快速恢复等技术及流程，确保应用系统能够从各种故障中迅速恢复，即使在意外事件或高负载情况下也能持续提供服务。企业需要规划和实施故障转移策略、备份和恢复机制，以及定期进行灾难恢复演练，以验证应用系统的韧性。

- **安全性支柱**

  安全性支柱致力于保护信息、系统和资产的机密性、完整性和可用性。它涵盖了应用安全、数据安全与隐私保护、基础设施安全和安全运营等方面。企业应当建立强大的安全策略，包括使用身份验证和授权机制、加密数据传输和存储、实施网络安全措施，以及持续监控和审计系统活动，以及时发现和应对安全威胁。

- **性能效率支柱**

  性能效率支柱关注如何高效地使用云资源，满足系统性能需求并适应业务的变化。它强调通过性能规划、性能建模、性能分析、性能优化等手段确保系统能够在不同的负载条件下保持最佳性能。企业需要持续监控系统性能指标，优化应用程序和基础设施的配置，利用缓存等技术提高响应速度，并定期评估和调整架构设计。

- **成本优化支柱**

  成本优化支柱旨在提升云资源的成本效益，消除不必要的开销和资源浪费。它鼓励企业采用经济高效的资源配置，利用计费模式优化、资源优化和架构优化等手段持续提升成本效益。企业应该建立持续成本运营机制，持续分析和监控云成本，识别节约机会，避免过度配置或闲置资源，从而提高投资回报率和财务效率。

- **卓越运营支柱**

  卓越运营支柱关注高效地运营和监控系统，持续改进流程并交付业务价值。它强调实践DevOps、基础设施即代码、自动化部署、测试验证和自动化运维任务，建立全面的监控、日志记录和告警机制。通过精心设计的操作流程、变更管理和持续改进方法，企业能够快速响应变化，减少错误，提升团队协作效率，确保业务目标的实现。

关于华为云Well-Architected Framework的详细内容，请参考卓越架构技术框架**Well-Architected Framework**。

3.4 Landing Zone 设计

3.4.1 全面云化的 IT 治理挑战

大型企业的组织结构复杂，往往拥有数十上百个业务单元（如子公司、事业部、产品线、部门或项目组等），每个业务单元负责建设1到多个应用系统。这些应用系统的全面云化转型将导致在云上同时存在数百个业务系统和海量云资源，而且包括企业自有员工、外包员工及合作伙伴的员工在内的大量用户需要访问和操作这些云资源，量变导致质变，资源闲置、误操作、恶意操作、数据泄露和权限错配等风险将随着用云规模呈现指数级增长。大型企业必须构建精益化、集中化和结构化的IT治理体系才能有效控制这些风险，最大化业务收益。CIO和CTO需要在业务系统上云之前就开始着手设计云上IT治理体系。在具体实践中经常会遇到以下各种挑战。

- 如何做好业务单元的安全和故障隔离，确保业务单元之间的云资源、应用和数据的隔离？
- 如何减少单点故障的爆炸半径？
- 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？
- 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？
- 如何统一管控多个业务单元的边界网络出入口？
- 如何规划生产、开发和测试环境？
- 公共资源如何在多个业务单元之间共享？
- 如何统一监控、运维和管控多个业务单元的云资源？
- 如何统一管控各业务单元的预算和成本？如何优化云成本？
- 如何避免各业务单元过度使用云资源？
- 如何将用户进行分组？又应该为用户组设置哪些权限？
- 云资源、数据和应用如何满足国家、行业和企业自身的安全合规标准？
- 误操作、恶意操作和权限错配在所难免，如何规避由此产生的风险？
- 员工密码和密钥容易丢失或泄露，如何避免由此带来的数据泄露风险？
- 在尽量保留原有IT治理模式的前提下，如何将其迁移到公有云上？

要应对上述挑战，需要设计一套全面的云上IT治理方案和最佳实践，对业务单元、用户、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云上IT治理的挑战。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。是指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，目的是系统性解决企业大规模上云所带来的IT治理和安全合规的挑战。

3.4.2 为什么需要 Landing Zone

为了实现业务单元的安全和故障隔离，华为云的推荐做法是将不同业务单元的应用系统分别部署在不同的账号中。华为云账号具备以下三个属性。

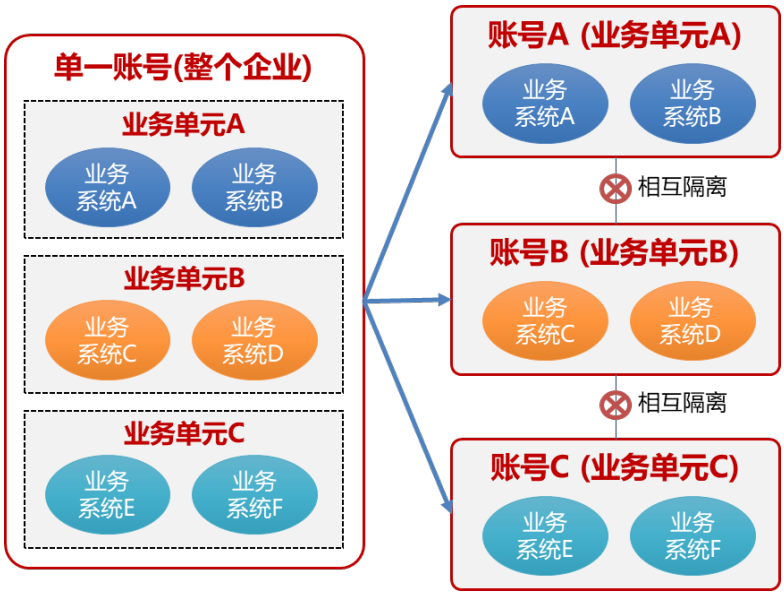
- 华为云账号是一个资源容器，用户可以在其中部署任意云资源和上层业务应用系统，不同的账号相当于不同的资源容器，账号之间是完全隔离的。因此在一个账号中的故障和安全风险不会影响和传播到其他账号。
- 华为云账号也是安全管理边界，每个账号都有独立的身份和权限管理系统，一个账号内的用户只能访问和管理本账号的资源，未经显式的授权，一个账号内的用户不能访问其他账号的资源、数据和应用。
- 华为云账号还可以作为独立的账单实体，每个账号可以单独在华为云上充值、消费云资源、结算和开票。

因此华为云账号可以针对业务单元进行有效的故障和安全隔离，还可以进一步进行管理和财务隔离。单一账号存在两个严重的问题：

- 单一账号的爆炸半径太大，如该账号崩溃将导致企业所有业务系统不可用。
- 云平台上账号的资源配额是有上限的，不能在一个账号内无限扩容云资源。

为了减少单点故障的爆炸半径，核心办法就是不要把所用业务系统及其云资源部署在单一账号，也就是不要“把鸡蛋放在一个篮子里”，而是应该按照不同的业务单元映射到不同的华为云账号，如下图所示。

图 3-5 多账号部署



因此当企业的全面云化转型需要采用多账号架构。按照**康威定律**，企业的多账号架构通常会与其组织架构或业务架构保持一致，即按照业务单元、地理单元、职能单元等

维度划分账号。采用多账号架构后可以实现职责分离，不同的账号负责不同的事情、承载不同的业务，每个账号的管理员可以对本账号内的资源进行自治管理。但从IT治理角度，不能让每个账号成为“信息孤岛”，必须在公司范围内进行统一IT管控，比如多账号的集中身份权限管理、集中运维管理、集中安全管控、集中网络管理、集中财务管理和公共资源管理等。针对这些核心诉求，华为云提出了Landing Zone解决方案来帮助企业在云上构建安全合规、易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。

- **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；
- **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；
- **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；
- **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；
- **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，集中构建全方位数据边界，避免敏感数据泄露。

企业成功实施了Landing Zone解决方案之后，可以有效规避大规模上云之后的管理失控、安全失控、成本失控的风险，全面应对各种IT治理挑战，帮助企业建立分统结合的IT治理体系和完善的安全合规体系。

- **分统结合的IT治理体系**：即在分权分域分级管理的基础上进行一定程度的统一管控，如集中运维管理、集中安全管控等；
- **完善的安全合规体系**：云上运行环境（包括云资源、数据、应用等）满足国家、行业和企业自身的安全合规标准。

3.4.3 Landing Zone 设计原则

华为云基于自身实践和大量Landing Zone项目的成功交付经验提炼了如下原则，您可以将其作为起点制定符合您企业所需的设计原则。

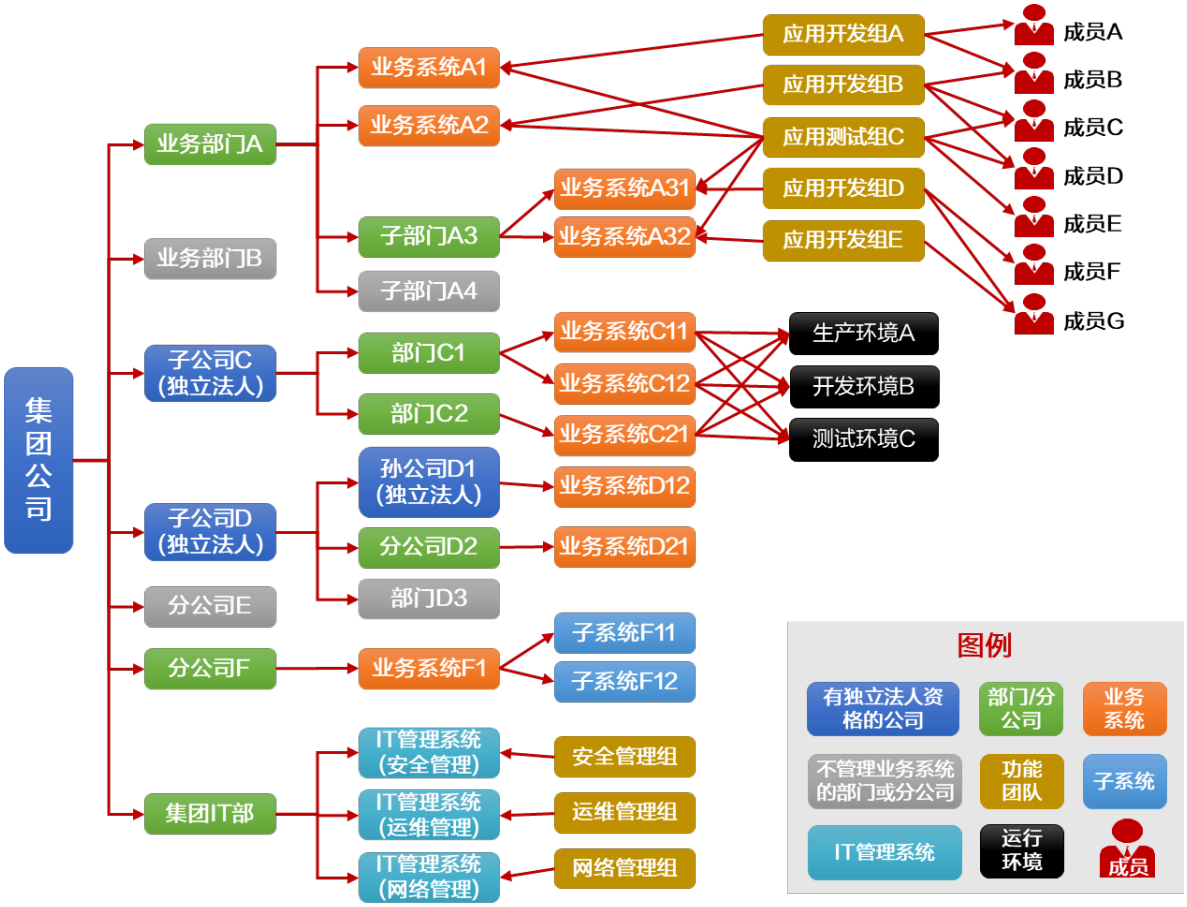
- **康威定律：**按照**康威定律**，系统的技术架构反映了所属组织的架构。Landing Zone的组织单元和账号架构应该与企业的组织架构和业务架构保持一致，推荐按照企业的业务架构、地理架构和IT职能规划Landing Zone的组织单元和账号体系。
- **相关性原则：**不需要把企业内部的完整组织架构映射到华为云上，只把那些负责管理IT系统的组织单元（如部门、分公司）和使用IT资源的用户映射到华为云上。如行政部门不管理、不查看、不操作任何云上IT资源，就不需要在华为云上创建一个对应行政部门的组织单元；如财务小张不负责IT系统的成本核算、分析和预算管理，就无需为小张在华为云上创建一个拥有财务管理权限的用户。
- **组织单元设计原则：**需要相同控制策略（包括**服务控制策略**和**标签策略**）的账号归属到同一个组织单元下，可以在该组织单元集中施加控制策略，该策略将继承到其下的每一个子账号和下层组织单元。
- **运行环境隔离原则：**生产环境要保持稳定、可靠和安全，而开发和测试环境更强调灵活性，所以生产环境与开发测试环境需要严格隔离。同时针对生产环境配置更严格的控制策略，针对开发测试环境配置更松的控制策略。
- **业务账号设计原则：**针对业务部门，建议按照企业当前所定义的业务单元（如子公司、事业部、产品线、部门或项目组等）创建对应的子账号。
- **IT管理账号设计原则：**针对IT部门，可以按照企业当前的IT职责划分不同的IT管理类子账号，如安全运营、运维监控、网络运营、数据平台等子账号。

3.4.4 Landing Zone 参考架构

3.4.4.1 公司 IT 治理架构

大企业的业务覆盖范围很广泛，分布在不同的产业和地理区域，为支持整个公司的长期稳定运行和有效管理，通常采用集团化和等级式管理模式。随着经营范围和规模的不断扩大，需要不断建立子公司、分公司，子公司再建立孙公司，大部门也逐步拆分成多个小部门，组织结构的层级也就越来越多。大企业的IT治理架构也会受到组织结构的影响，以下是一个典型的大企业IT治理架构示意图，由于图片空间有限，该示意图中没有穷举全部的层级和图元。本文所描述的Landing Zone参考架构以下图的IT治理架构为基础，将其全部映射到华为云上并有效运转起来。

图 3-6 大企业 IT 治理架构



在上述大企业IT治理架构中，各个层级的具体含义如下：

- **集团公司：**是指以资本为主要联结纽带，以母子公司为主体，以集团章程为共同行为规范的，由母公司、子公司及其他成员共同组成的企业法人联合体。
- **子公司：**是指一定比例以上的股份被另一公司（母公司）持有并受到该公司实际控制的公司。母公司对子公司的一切重大事项拥有实际上的决定权。但在法律上，子公司仍是具有法人地位的独立企业，并以自己的名义进行业务活动。子公司可以根据经营管理需求再成立自己的子公司或分公司。

- **分公司：**分公司是母公司管辖的分支机构，是指母公司在其住所以外设立的以自己的名义从事活动的机构，如在各个省市成立的销售分公司。分公司不具有企业法人资格，其民事责任由母公司承担。
- **部门：**母公司、子公司和分公司都可以基于自己的经营管理需求设立部门，如软件企业可以按照不同的软件产品线设立不同的部门，工业制造企业可以按照业务流程设立研发部、制造部、采购部、销售部、服务部等。大部门还可以再进一步拆分成小部门。
- **业务系统：**是指为了完成特定任务或解决特定问题而设计的软件系统，以支撑组织内特定的业务流程和业务场景，如ERP、CRM、营销管理系统等。业务系统的开发、测试和运行需要消耗一定的计算、存储、网络、安全、数据库、中间件、大数据、AI服务等资源。大型业务系统能够包含多个子系统。
- **IT管理系统：**为了支撑业务系统的长期安全稳定运行所建立的IT支撑和管理系统，如安全运营中心、IAM和监控运维系统等。
- **子系统：**大型业务系统或IT管理系统通常包含多个相互解耦且相互关联的子系统、功能模块或微服务，这些子系统相互协作，共同实现整体系统的功能。
- **功能小组：**参与业务系统或IT管理系统建设和运维的成员按照职责划分为不同的功能小组，如网络管理组、安全管理组、运维管理组和应用开发组等。
- **成员：**一个成员代表一个参与业务系统或IT管理系统建设和运维的人，1个成员可以加入多个功能小组，但成员一般不允许加入到多个部门。
- **运行环境：**业务系统或IT管理系统通常要部署到不同的运行环境，如生产环境、开发环境和测试环境等。

上述大企业IT治理架构中各个层级之间的关系如下图所示：

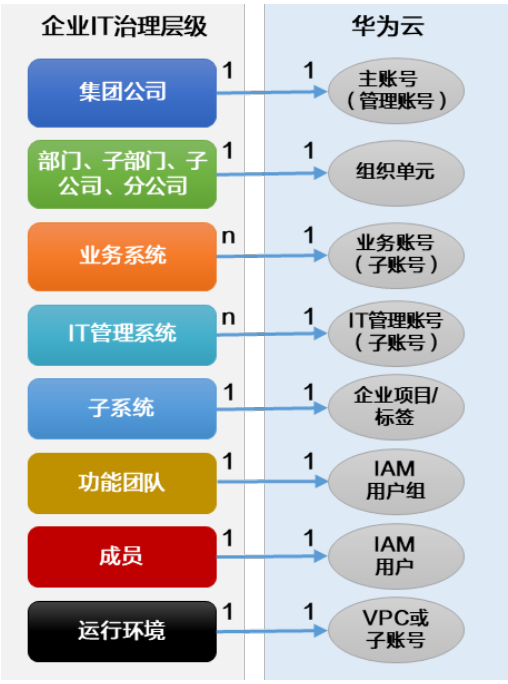
图 3-7 大企业 IT 治理架构的层级关系

层级关系	关系描述
公司(独立法人) 1 — n 部门/分公司	1个集团公司或者1个独立法人的子/孙公司包括多个部门和多个分公司(不具备法人资格，类似部门)
部门/分公司 1 — n 子部门	1个部门或者1个分公司可以管理多个子部门
集团公司 1 — n 子公司(独立法人)	1个集团公司可以控股多个子公司（子公司是独立的法人，拥有自己独立的公司名称、章程和组织结构）
部门/分公司 1 — n 业务系统/IT管理系统	1个部门或分公司可以管理多个业务系统或IT管理系统
业务系统/IT管理系统 1 — n 子系统	1个业务系统或IT管理系统可以包含多个子系统、功能模块或微服务
业务系统/IT管理系统 m — n 功能小组	1个业务系统或IT管理系统可以由多个功能小组（如应用开发组、应用测试组等）共同完成，1个功能小组（如应用测试组）也可以参与到多个业务系统或IT管理系统
功能小组 m — n 成员	1个功能小组可以由多个成员组成，1个成员可以同时加入多个功能小组
部门/分公司 1 — n 成员	1个部门或分公司包含了多个成员，成员一般不加入到多个部门或子公司。
IT系统 m — n 运行环境	1个IT系统需要多个运行环境（如生产环境、开发环境、测试环境），1个运行环境也可以承载多个IT系统。

上述IT治理架构中的各个层级需要逐一映射到华为云上，在华为云上创建相应的对象，华为云从精益治理的角度推荐如下图所示的映射关系。集团公司映射为华为云的主账号（或管理账号），下面的子公司、分公司和部门都可以映射为华为云的组织单元（Organization Unit, OU）。一至多个业务系统映射为一个业务账号（用于承载业

务系统的子账号），通常是将支撑一个业务单元所需的所有业务系统映射到一个业务账号。一至多个IT管理系统映射为一个IT管理账号（用于承载IT管理系统的子账号）。子系统则可以映射为华为云的**企业项目**或者标签。功能团队映射为华为云IAM的用户组，成员则可以映射到华为云IAM的用户。生产、开发和测试等运行环境可以映射到不同的VPC，有时候为了严格隔离生产、开发和测试等运行环境，也会将其映射为独立的子账号。需要注意的是，不负责建设和运维业务系统或IT管理系统的子公司、分公司或部门不用映射到华为云。

图 3-8 企业 IT 治理架构到华为云的映射



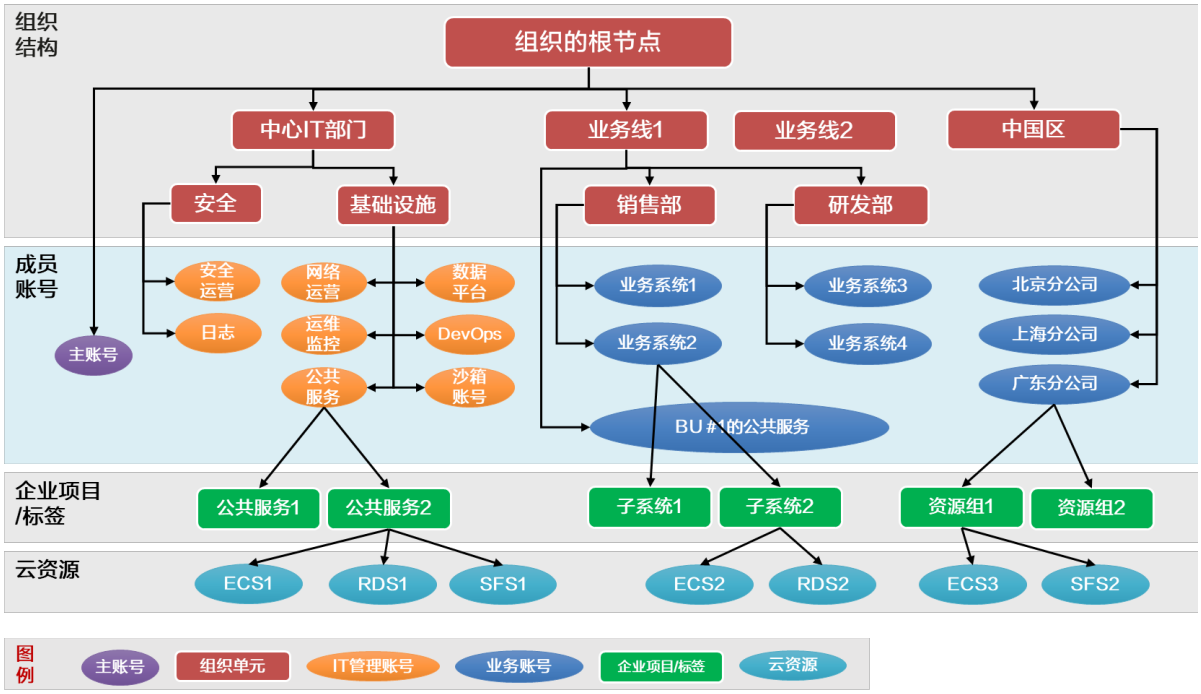
3.4.4.2 组织和账号设计

Landing Zone解决方案的目标是在云上构建安全合规、易扩展的多账号运行环境，首先要规划组织和账号架构。按照**康威定律**，企业在华为云上的账号结构要与企业的组织和业务架构总体保持一致，但也不用完全照搬复制。不需要把企业内部的完整组织结构映射到华为云上，只把那些负责建设和运维业务系统或IT管理系统的组织单元（如子公司、分公司、部门）和使用IT资源的用户映射到华为云上。

例如HR部门不管理、不查看、不操作任何云上IT资源，就不需要在华为云上创建一个对应HR部门的组织单元；财务小张不负责IT系统的成本核算、分析和预算管理，就无需为小张在华为云上创建一个拥有财务管理权限的用户。

华为云提供以下组织单元和账号的参考架构，建议按照业务架构、地理架构、IT职能等维度设计华为云上的组织单元的层级结构和账号群。

图 3-9 组织单元和账号参考架构

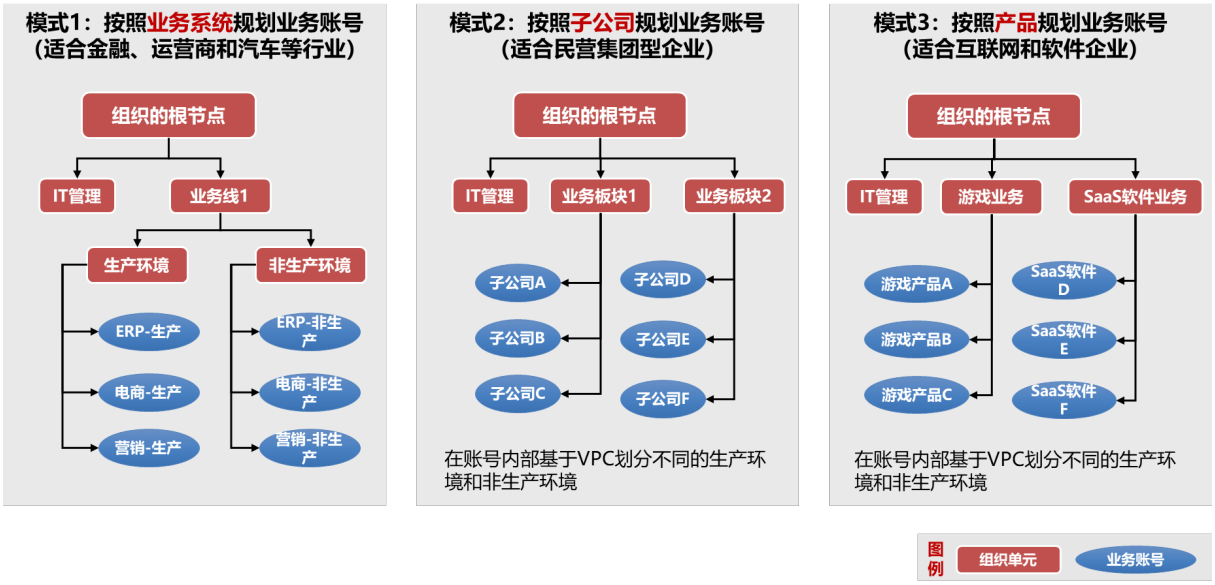


业务账号规划

按照业务架构在华为云上创建不同层级的组织单元OU，每个业务OU下面可以挂载多个业务账号，每个业务账号上可以承载一至多个业务系统。

原则上，业务账号的规划需要跟组织定义的业务单元（业务单元之间要求强隔离）保持一致，业务单元可以是子公司、事业部、产品线、部门、项目组或业务系统等。业务单元的粒度越细，组织对精益治理的诉求越强。根据华为云为大量企业和政府客户设计和实施Landing Zone方案的经验，总结了如下三种规划业务账号的模式。

图 3-10 规划业务账号的模式



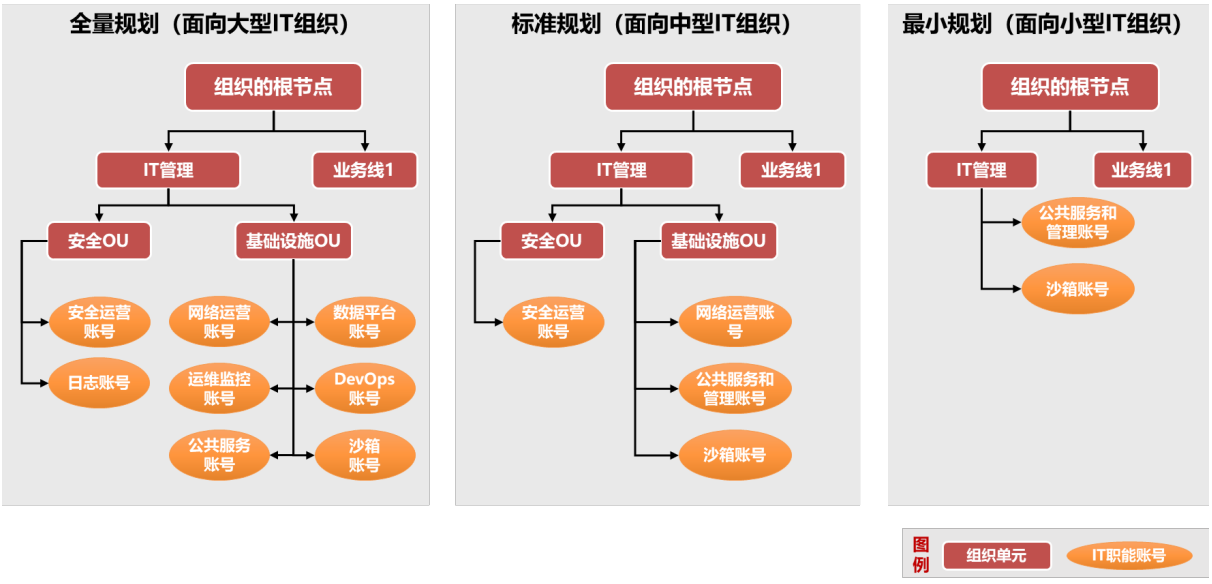
- 模式1是按照业务系统规划业务账号，相当于将业务单元细化到业务系统这个粒度，通过不同的子账号严格隔离不同的业务系统。同时按照生产环境和非生产环境规划不同的子账号，通过独立的子账号严格隔离生产环境和非生产环境，这种模式适合金融、运营商、汽车等管控严格的企业。
- 模式2是按照子公司规划业务账号，相当于将业务单元定义到子公司，也就是只需要在子公司层面进行严格的隔离。不同子公司的业务系统集中部署在子公司对应的子账号里面。在账号内部可以基于VPC为各个业务系统规划生产环境和非生产环境。这种模式适合很多民营企业集团，这些企业集团往往拥有数十上百个子公司，从公司治理角度要求子公司之间进行严格的业务隔离，但当前还不需要细化到在业务系统之间进行隔离。
- 模式3是按照产品规划业务账号，相当于将业务单元细化到产品粒度，这里面提到的产品是指企业面向它的外部客户提供服务的软件系统，如直播系统、网络游戏、SaaS软件等。不同的产品部署在不同的子账号中，产品之间保持严格隔离，在账号内部可以基于VPC为各个产品规划生产环境和非生产环境。这种模式特别适合互联网企业和SaaS软件企业。

IT 管理账号规划

针对企业的中心IT部门，在华为云上创建对应的组织单元，并在其下面创建安全和基础设施两个下级组织单元，分别容纳安全管理的子账号群和基础设施管理的子账号群。这些IT管理账号可以对企业范围内所有子账号进行统一的IT管理。

原则上，IT管理能账号的规划需要跟组织当前的IT组织规模和职责划分保持一致，避免打破当前利益平衡。根据华为云为大量企业和政府客户设计和实施Landing Zone方案的经验，总结了如下三种规划IT管理账号的模式。

图 3-11 规划 IT 管理账号的模式



- 模式1是全量规划，针对大型IT组织，这些IT组织通常有数十上百个IT管理人员，内部已经按照安全运营、日志审计、网络运营、运维监控、公共服务、数据平台、DevOps等职责划分了独立的IT职能小组。为了保障IT部门内部的职责隔离，将这些IT职能小组分别映射到独立的账号，这些账号行使独立的IT职责，所以称为IT管理账号或IT职能账号，如下表所示。

表 3-8 IT 管理账号

账号名称	账号履行的IT职能	责任团队	建议开通的云服务
主账号或管理账号	针对整个企业进行统一组织和账号管理、统一财务管理、统一控制策略管理和统一身份权限管理	CIO或IT主管	组织Organizations、资源治理中心RGC、成本中心、IAM身份中心
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	ER、DNS、NATG、EIP、VPC、DC、CC、VPN、CFW、WAF、AAD等
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，并共享给其他所有成员账号使用	公共服务管理团队	镜像服务IMS、容器镜像服务SWR、弹性文件服务SFS、对象存储服务OBS、自建NTP服务器、自建AD服务器等公共资源
安全运营账号	作为企业安全运营中心，统一管控整个企业内所有账号的安全策略、安全规则和安全资源，为成员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，如安全云脑SecMaster、企业主机安全HSS、数据安全中心DSC、数据加密服务DEW、云证书服务CCM、漏洞管理服务CodeArts Inspector
运维监控账号	统一监控和运维各个成员账号下的资源和应用，统一进行告警管理、事件处理和变更管理，并提供运维安全保障措施	运维团队	应用运维管理AOM、COC、云日志服务LTS、应用性能管理APM、云堡垒机CBH等
日志账号	集中存储和查看所有账号的审计日志和安全相关的日志（如VPC流日志和OBS访问日志等）	合规审计团队	云审计服务CTS、云日志服务LTS、、配置审计服务Config、对象存储服务OBS等
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	数据湖、大数据分析平台、数据接入服务、数据治理平台
沙箱账号	用于进行各种云服务的功能测试、控制策略的测试等	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等。

- 模式2是标准规划，针对中型IT组织，这些IT组织通常只有十几到二十几个IT管理人员，所以也不可能像大型IT组织那样将IT职责划分的那么细，但通常会划分独立的安全运营、网络运营、运维监控等IT职能小组。我们建议只需要创建独立的安全运营、网络运营、公共服务和运维管理等IT管理账号。跟模式1的全量规划相比，模式2的安全运营账号相当于合并了模式1中安全运营账号和日志账号的职能。模式2的公共服务和管理账号合并了模式1中运维监控账号、公共服务账号、数据平台账号和DevOps账号的职能。
- 模式3是最小规划，针对的小型IT组织，通常只有少数几个IT管理人员，这种情况下仅需创建一个公共服务和管理账号，将模式1的安全运营账号、日志账号、网络运营账号、运维监控账号、公共服务账号、数据平台账号和DevOps账号的职能全部合并。

地理区域账号规划

地理区域账号的规划比较简单，可以按照地理架构在华为云上划分不同层级的组织单元OU，每个OU下面可以按照国家或地区创建对应的子账号，在上面可部署本地的客户关系管理系统、客户服务系统和经营管理系统等。上述参考架构把中国区等区域组织映射为华为云的OU，为其下属的北京、上海等分公司创建独立的子账号以承载本地化的应用系统。

主账号规划

需要注意的是在组织的根下面会关联一个主账号（也叫管理账号），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**：针对整个企业的所有账号进行统一财务管理，包括统一预算管理、统一成本分析、统一账单管理、统一资金管理、统一申请代金券、统一成本结算和统一开票等。
3. **统一策略管理**：为各个组织单元和子账号设置（包括**服务控制策略**和**标签策略**），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，创建控制策略时可以将其应用到某一个组织单元，该策略可以继承到关联的子账号和下层组织单元。
4. **统一身份管理：**基于IAM身份中心，统一创建用户和用户群，或者统一配置与外部IdP（Identity Provider）的身份联邦，然后根据最小授权原则，为这些用户统一配置能够访问多个账号内云资源的权限。

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映射为华为云上的一个企业项目或标签，用户还可以按照企业项目或标签进行成本分摊和细粒度授权。

3.4.4.3 整体架构设计

华为云基于自身实践和大量Landing Zone项目的成功交付经验总结了如下图所示的Landing Zone解决方案整体参考架构，涵盖组织与账号管理、身份权限管理、集中网络管理、共享服务管理、统一安全管理、统一合规审计、统一运维管理、统一财务管理和数据边界总共9个领域。

图 3-12 Landing Zone 解决方案参考架构

这九大领域的实施需要在特定的账号内完成，比如组织与账号管理是在主账号（管理账号）中完成，而集中网络管理主要是在网络运营账号中完成。下表是九大领域对应的主要账号。

表 3-9 九大领域对应的主要账号

九大领域	对应的主要账号
组织与账号管理	主账号（管理账号）
身份与权限管理	主账号（管理账号）
集中网络管理	网络运营账号
共享服务管理	公共服务账号
统一安全管理	安全运营账号
统一合规审计	安全运营账号、日志账号
统一运维管理	运维监控账号
统一财务管理	主账号（管理账号）
数据边界	主账号（管理账号）、沙箱账号（用于测试各种控制策略）

组织与账号的设计方案在前面已经详细阐述了，后面将分别展开介绍其他8个领域的设计方案。

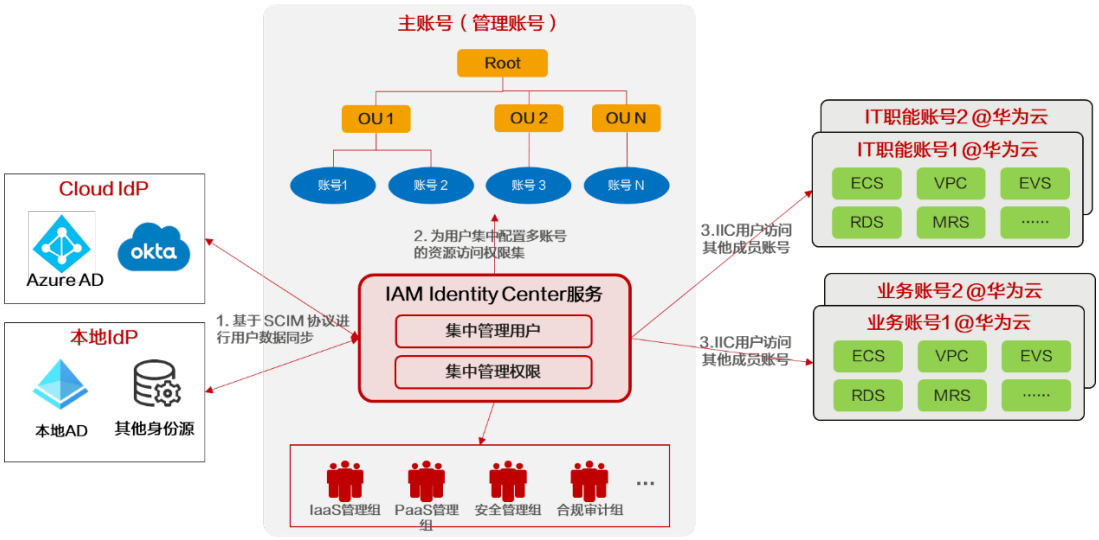
3.4.4.4 身份和权限设计

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的最佳实践。

集中身份和权限管理

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。建议您使用企业自己的身份管理系统与华为云IAM身份中心（IAM Identity Center）进行联邦身份认证，基于SCIM（System for Cross-domain Identity Management）协议将企业自己的身份管理系统中的用户同步复制到华为云的IAM身份中心。您还可以在IAM身份中心对这些用户集中配置访问多个账号内资源的权限。配置完成后，前者的用户可以通过SSO（Single Sign-on）登录到华为云控制台，可以看到该用户有权限访问的账号清单，点击“访问控制台”即可登录到该账号内部访问其中的云资源。

图 3-13 统一身份和权限管理



用户组和权限规划

您可以参照之前CCoE的角色划分来规划IAM身份中心的用户组，将对应的员工加入与其职责匹配的用户组，下表为推荐的用户组划分方式，基于这些用户组的职责，按照最小授权原则，下表也推荐了应该给这些用户组设置访问哪些账号的哪些权限，您可以将其作为起点，精细化规划符合企业要求的用户组和权限。

表 3-10 IAM 身份中心的用户组

用户组	用户组的职责	多账号访问权限的设置建议
财务管理组	统一管理成员账号的账单、成本、折扣、发票等财务元素	管理账号的BSS Administrator，BSS Finance等
IT治理组	创建和管理组织单元、成员账号和SCP策略	管理账号的Organizations FullAccess等

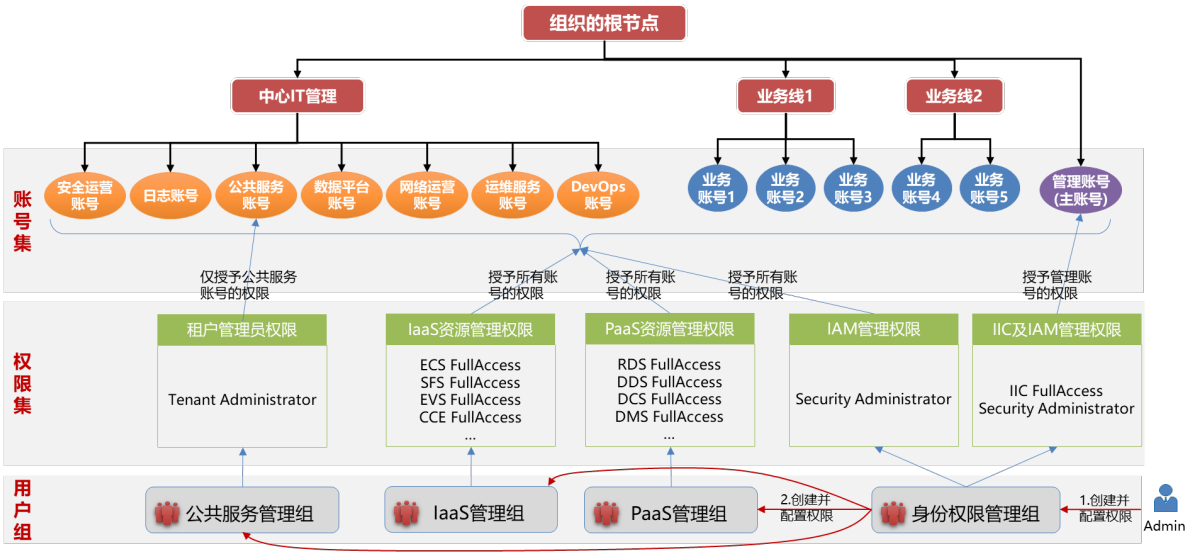
用户组	用户组的职责	多账号访问权限的设置建议
身份权限管理组	集中创建和管理用户、用户组，并集中配置权限、委托和SSO	• 管理账号的IdentityCenter FullAccess，Security Administrator权限 • 所有其他账号的Security Administrator权限
安全管理组	统一管控整个企业的安全策略、安全规则和安全资源，为其他账号设置安全配置基线，对整个企业的信息安全负责	所有账号下安全资源（安全云脑、HSS、DSC、DBSS等）的管理权限
合规审计组	统一查看所有账号的审计日志和安全相关的日志（如VPC流日志和OBS访问日志等）	• 日志账号的Tenant Administrator权限 • 所有其他账号下的Tenant Guest权限
网络管理组	集中部署和管理企业的网络连接资源，如ER、VPN、DC、NATG等，统一创建和管理各个账号的VPC、子网和NACL；集中部署和管理网络边界安全防护资源，如WAF，CFW等	• 网络运营账号的Tenant Administrator权限 • 所有其他账号下的VPC、子网和NACL等网络资源的管理权限 • 网络运营账号的网络安全资源（WAF、CFW等）的管理权限
IaaS管理组	也叫云基础设施管理员，统一管理各个账号下的IaaS资源	• 所有账号下IaaS资源的管理权限 • 所有其他账号下的运维监控服务（AOM，CES，APM等）的管理权限
PaaS管理组	也叫中间件管理员，统一管理各个账号下的中间件资源	• 所有账号下中间件资源的管理权限 • 所有其他账号下的运维监控服务（AOM，CES，APM等）的管理权限
自动化运维组	统一监控和运维各个账号下的资源	• 运维监控账号的Tenant Administrator权限 • 所有其他账号下的运维服务COC的管理权限
数据管理组	集中部署和管理企业数据平台，将其他成员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	数据平台账号的Tenant Administrator权限
公共服务管理组	集中部署和管理企业的公共资源、服务和应用系统，并共享给其他所有成员账号使用	公共服务账号的Tenant Administrator权限
应用开发组	负责应用的开发工作和开发环境的管理工作	• 开发账号的Tenant Administrator权限 • DevOps账号下的开发人员权限

用户组	用户组的职责	多账号访问权限的设置建议
应用测试组	负责应用的测试工作和测试环境的管理工作	• 测试账号的Tenant Administrator权限 • DevOps账号下的测试人员权限

权限设置

主账号的根用户或Admin用户属于超级管理员，拥有最大的权限，该用户的密码建议由企业的CIO或IT主管直接保管，日常管理和运维不要用Admin来执行，包括创建用户和配置权限也不应该由Admin来执行。我们建议先使用主账号的Admin在IAM身份中心创建出身份权限管理组和对应的用户，授予其完成职责所需要的权限，然后再由身份权限管理组的用户创建出其他的用户和用户组并授予权限。如下图所示。

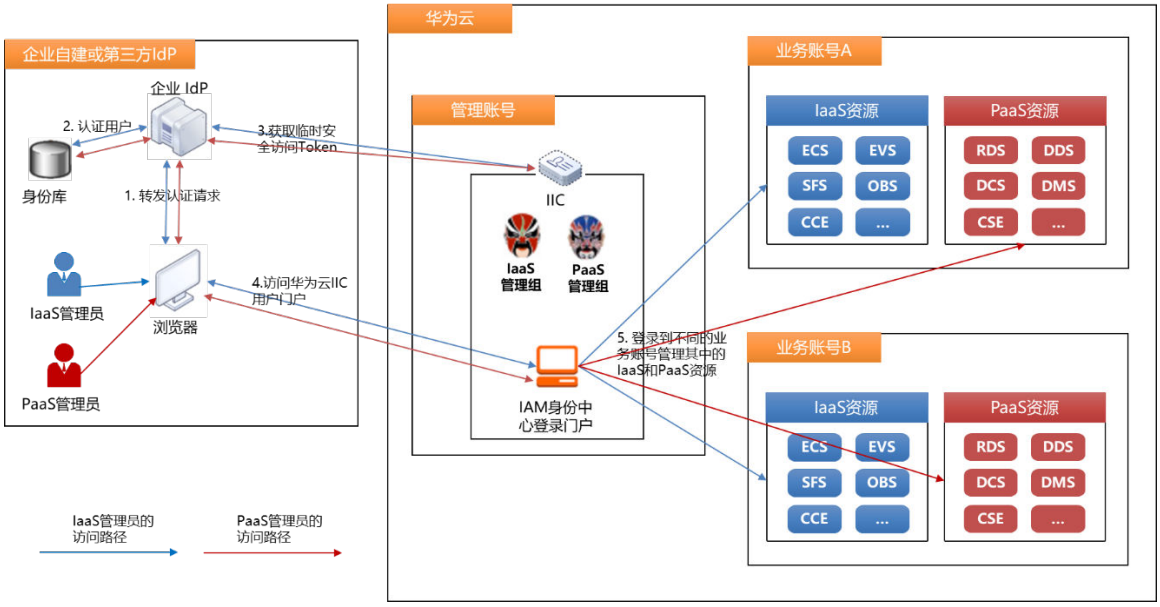
图 3-14 权限设置最佳实践



权限使用

Landing Zone为了实现统一管控的目标，IT管理人员需要通过IAM身份中心的多账号授权方式访问和管理其他账号下的云资源。例如，IaaS管理员和PaaS管理员需要统一管理企业范围内各个账号的IaaS资源和中间件资源，这就需要采用IAM身份中心提供的多账号授权方式访问部署在其他账号下的IaaS资源和中间件资源，如下图所示。

图 3-15 – IaaS 管理员和 PaaS 管理员统一管理多个账号的 IaaS 资源和中间件资源



其他身份和权限管理的最佳实践

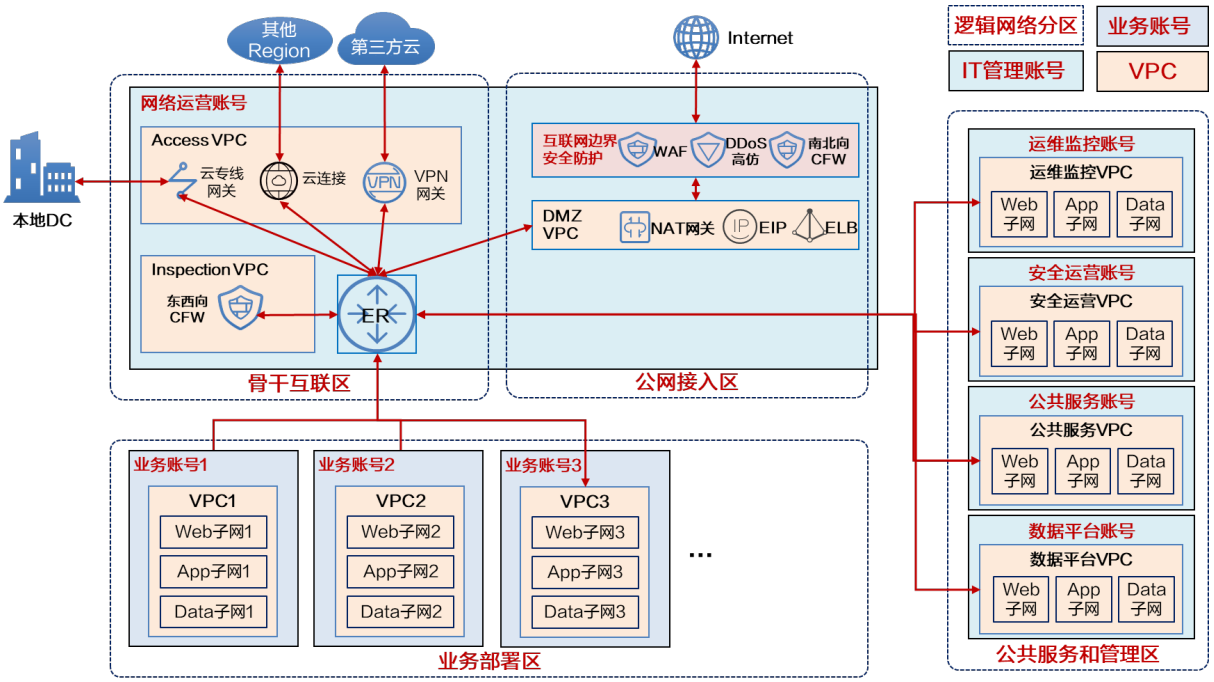
- 遵守最小授权原则，只授予完成职责所需的最小权限，如果用户组的职责产生变化，应该及时调整用户组的权限。
- 授权时建议按照用户组而不是用户进行授权，简化授权操作。
- 权限设置、权限使用和权限审计三权分立，由三个不同的人（自然人或者团队）分别承担职责，且这三个人不属于利益共同体。
- 敏感操作（删除和更新关键资源、大额资金使用等操作）要进行二次认证。
- 不要将用户密码共享给他人，而是为每个管理或使用华为云资源的人创建一个单独的用户并分配相应的权限，这样每个人在华为云的操作都能被追踪审计。
- 主账号根用户（与账号同名）的密码建议由企业的CTO或CIO保管，子账号根用户的密码建议由所属业务单元的负责人保管。
- 根用户（与账号同名）的权限很大，建议不要直接使用根用户访问华为云，而是创建一个或多个普通用户，并按照最小授权原则授予相应的权限，以使用这些普通用户代替根用户进行日常管理工作。
- 通过服务控制策略来约束子账号根用户的权限。

3.4.4.5 整体网络架构

Landing Zone的整体网络架构设计如下图所示。网络运营账号作为Landing Zone的网络枢纽，该账号集中管理多账号的边界网络出入口，并打通多账号下VPC之间的网络。在网络运营账号下集中部署企业路由器（Enterprise Router, ER），通过ER联通各账号下的VPC网络，从而实现多账号共享使用VPN和云专线与线下IDC互通，也能实现多账号共享使用公网NAT网关与互联网通信，还能共享使用云连接与其他Region进行互通。

在该账号下统一管理网络资源，一方面可以减少管理工作量，另外也有利于制定和实施统一的网络安全策略，例如统一部署面向互联网连接的DDoS高仿、云防火墙CFW、WAF等安全资源并统一配置具体的安全防护策略。

图 3-16 – 整体网络架构



Landing Zone的网络架构规划了四个逻辑网络分区：骨干互联区、公网接入区、业务部署区、公共服务和管理区。

骨干互联区主要功能

- 集中部署企业路由器（ER），为云上云下互联、云上多账号多VPC互联、云上跨Region互联构建网络枢纽。
- 集中部署VPN或专线与本地数据中心互联，打通云上云下互联的通道，所有账号都可以共享使用VPN或专线与本地数据中心通信。
- 集中部署云连接（Cloud Connect，CC）与华为云其他的Region进行网络互联，所有账号都可以共享使用CC与其他Region通信。
- 集中部署VPN与第三方云进行网络互联，所有账号都可以共享使用VPN与其第三方云通信。

公网接入区主要功能

- 集中设置DMZ区，部署和维护NATG、EIP、Proxy服务器和ELB等资源，为其他账号提供面向互联网的网络接入能力。
- 部署WAF、CFW、Anti-DDoS等安全服务集中保护互联网连接资源。
- 暴露明确的IP地址和端口，屏蔽其他端口，终结公网连接。

业务部署区主要功能

- 根据业务系统的需要创建VPC和子网，部署各种业务系统所需的云资源。
- 按照生产、开发和测试等运行环境划分不同的VPC。
- 按照应用架构分层划分Web、应用、数据等子网。

公共服务和管理区主要功能

- 根据公共服务和IT管理系统的需要创建VPC和子网，用于部署公共服务和IT管理系统所需的云资源。公共服务包括AD、DNS、文件系统、OBS桶、数据平台等；IT管理系统包括运维管理系统、安全管理系统等。
- 按照生产、开发和测试等运行环境划分不同的VPC。
- 按照应用架构分层划分Web、应用、数据等子网。

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，华为云基于以下假设并根据各个账号的职责梳理各个账号下VPC之间的连通性矩阵，据此则可以在ER上设置对应的路由规则。

- 运维监控账号需要运维第三方云和本地DC中的资源；
- 安全运营账号需要到公网获取系统补丁包；
- 数据平台需要获取第三方云和本地DC的数据；
- DevOps账号需要从Github下载代码，需要将软件制品部署到各个业务账号；
- 公共服务账号需要与本地IDC互联；
- 生产、开发、测试环境要求网络隔离。

图 3-17 各账号 VPC 网络的连通性矩阵

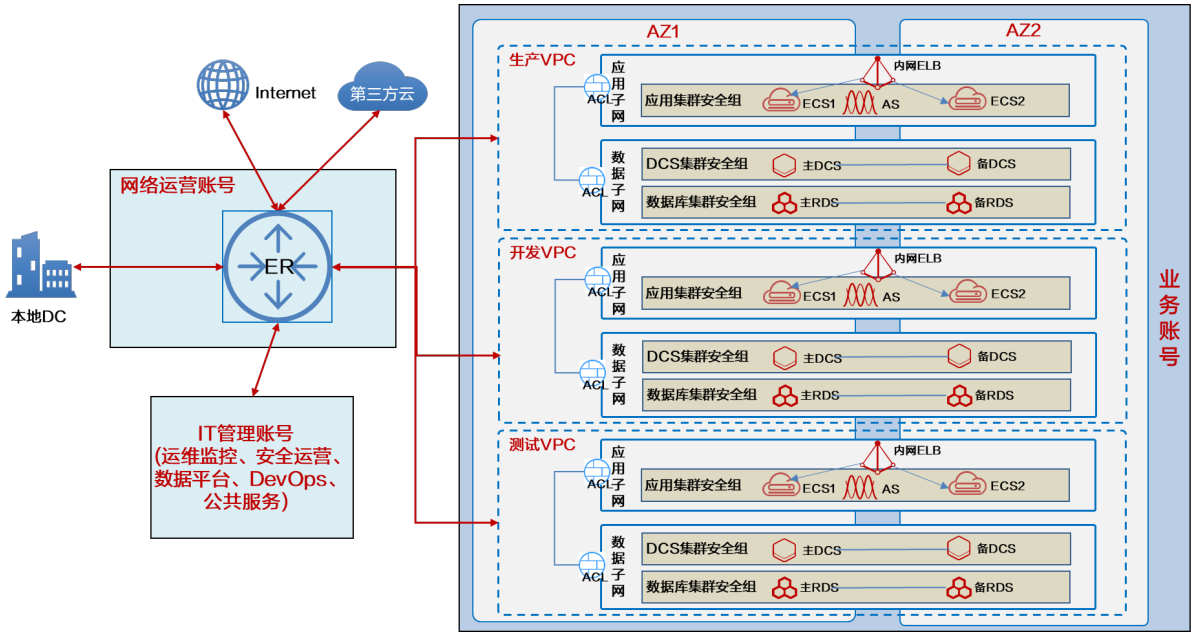
账号名称	网络运营账号(DMZ VPC)	网络运营账号(Access VPC)	公共服务账号VPC	安全运营账号VPC	运维监控账号VPC	数据平台账号VPC	DevOps账号VPC	业务账号A生产VPC	业务账号A开发VPC	业务账号A测试VPC	业务账号B生产VPC	业务账号B开发VPC	业务账号B测试VPC
网络运营账号(DMZ VPC)	N/A	X	X	X	✓	X	✓	按需	按需	按需	按需	按需	按需
网络运营账号(Access VPC)		N/A	✓	X	✓	✓	X	按需	按需	按需	按需	按需	按需
公共服务账号VPC			N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
安全运营账号VPC				N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓
运维监控账号VPC					N/A	✓	✓	✓	✓	✓	✓	✓	✓
数据平台账号VPC						N/A	X	✓	✓	✓	✓	✓	✓
DevOps账号VPC							N/A	✓	✓	✓	✓	✓	✓
业务账号A生产VPC								N/A	X	X	按需	X	X
业务账号A开发VPC									N/A	X	X	按需	X
业务账号A测试VPC										N/A	X	X	按需
业务账号B生产VPC											N/A	X	X
业务账号B开发VPC												N/A	X
业务账号B测试VPC													N/A

日志账号是集中存放审计日志和运行日志的地方，主要使用了华为云的CTS服务、LTS服务和OBS服务，该三个服务没有租户面IP地址，所以不需要考虑与其他账号的VPC进行互通。沙箱账号是一个允许客户任意测试华为云资源和控制策略的地方，包括VPC的功能测试以及与其他账号之间连通性测试，所以也不需要预先在ER中配置与其他账号的连通性。

前期规划业务账号时，如果是一个业务系统对应一个独立的账号，并且不需要严格隔离生产环境和非生产环境，那么我们建议在该账号为业务系统的不同运行环境创建独立的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、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。业务系统的应用服务器集群可以跨可用区部署，实现应用

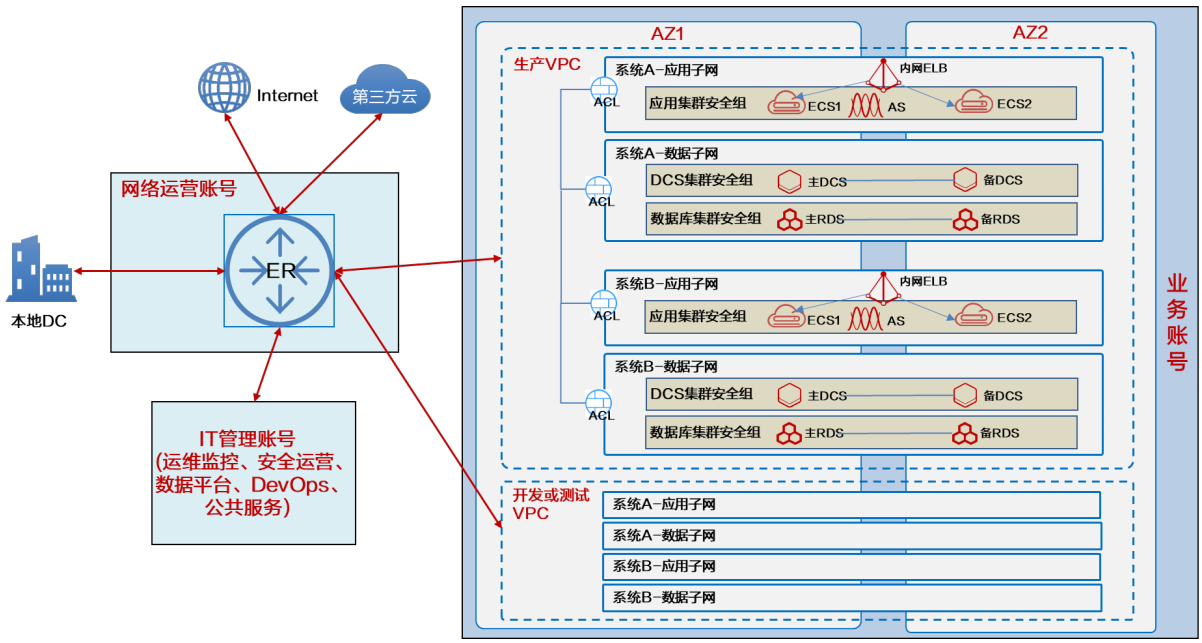
层的高可用；再使用华为云跨可用区的主备数据库集群和缓存集群实现数据层的高可用。如下图所示：

图 3-18 业务账号内的网络规划：一个业务系统对应一个子账号



针对多个业务系统共用一个子账号的场景，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：

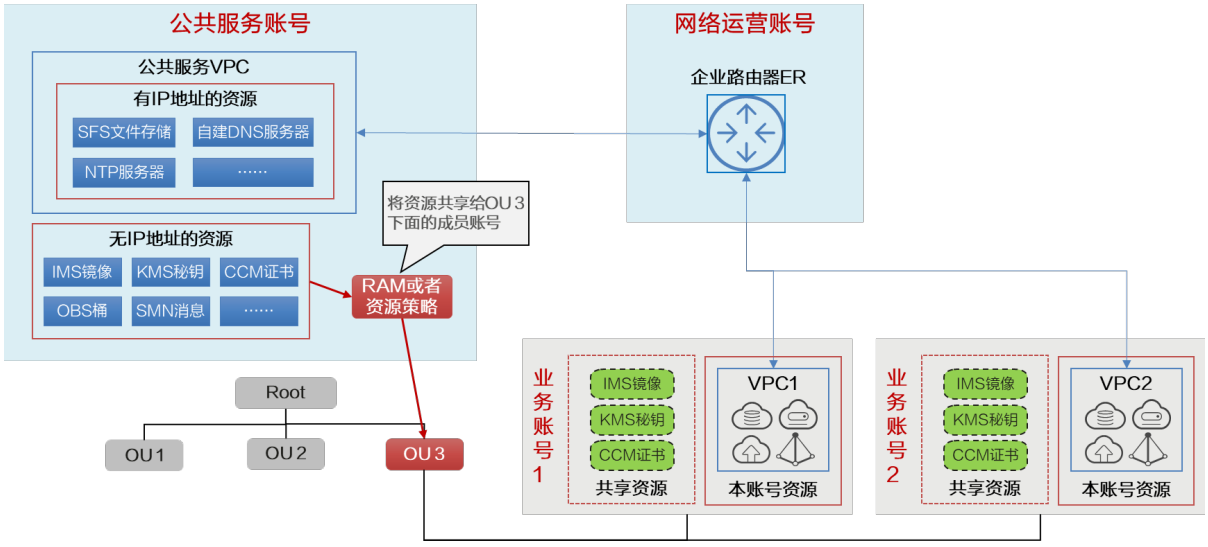
图 3-19 业务账号内的网络规划：多个业务系统共用一个子账号



3.4.4.6 公共服务管理

首先您要识别出各个业务单元所需要的公共IT服务和资源，比如NTP服务器、SFS文件存储、自建DNS服务器、OBS桶、虚拟机镜像、证书等，也可以是CodeArts等PaaS服务。然后集中部署和维护这些公共IT服务，将其共享给公司内所有业务单元。华为云提供了三种资源共享的方式。

图 3-20 资源共享方案



- **基于网络的共享**：通过ER或VPC Peering将账号之间的网络打通，在此基础上进行资源共享，该方式仅限于拥有租户可见IP地址的资源，如NTP服务器、自建DNS服务器或者SFS文件存储等。
- **基于RAM的共享：**通过华为云**RAM**服务设置资源共享，授权其他组织单元和账号使用该共享资源的权限，该共享方式更加安全。目前支持通过RAM进行跨账号共享的资源清单请参考**官网文档**。
- **基于资源策略的共享：**通过资源策略授予其他账号访问资源的权限，如OBS服务的桶策略、IMS服务的**共享镜像**和CBR的**共享备份**等。

3.4.4.7 多账号统一管理

多账号的统一管理包含统一安全管理、统一合规审计、统一运维管理和统一财务管理。通过以上各个方面的统一管理，企业可以显著提高管理效率和一致性，同时降低管理成本。账号数量越多，通过统一管理获得的收益越大。

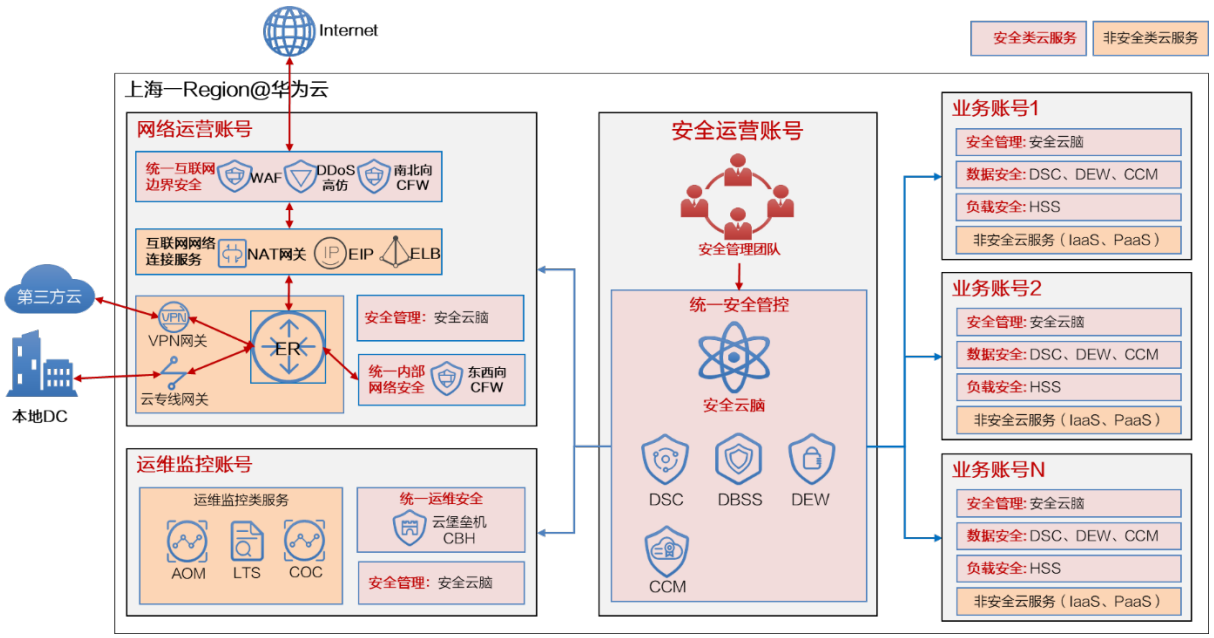
统一安全管理

以安全运营账号为中心，在这里集中部署安全云脑（SecMaster）、数据安全中心（Data Security Center，DSC）、数据库安全服务（Database Security Service，DBSS）、数据加密服务（Data Encryption Workshop, DEW）、云证书管理服务（Cloud Certificate Manager，CCM）和主机安全服务（Host Security Service，HSS）等，针对其他子账号进行统一的安全管理，如下图所示。

安全运营账号中的SecMaster服务可以与部署在其他账号下的安全云脑和HSS服务进行协同，无需登录到其他账号，在安全运营账号中就可以对其他账号进行统一的安全运营，包括统一云上资产管理、统一的安全态势管理、统一安全信息和事件管理、统一的安全编排与响应等活动。安全运营账号的DSC服务可以对所有成员账号进行统一的

数据安全防护，包括针对所有成员账号的统一数据安全风险识别和统一数据保护（数据水印、数据脱敏）。安全运营账号的DBSS服务可以基于Agent采集模式，在网络可达的前提下，实现跨账号的数据库审计和统一信息展现。安全运营账号的CCM服务可以集中申请SSL证书，然后通过RAM服务共享给其他账号使用。安全运营账号的DEW服务可以集中创建KMS秘钥，然后通过RAM服务共享给其他账号使用。

图 3-21 多账号的统一安全管理



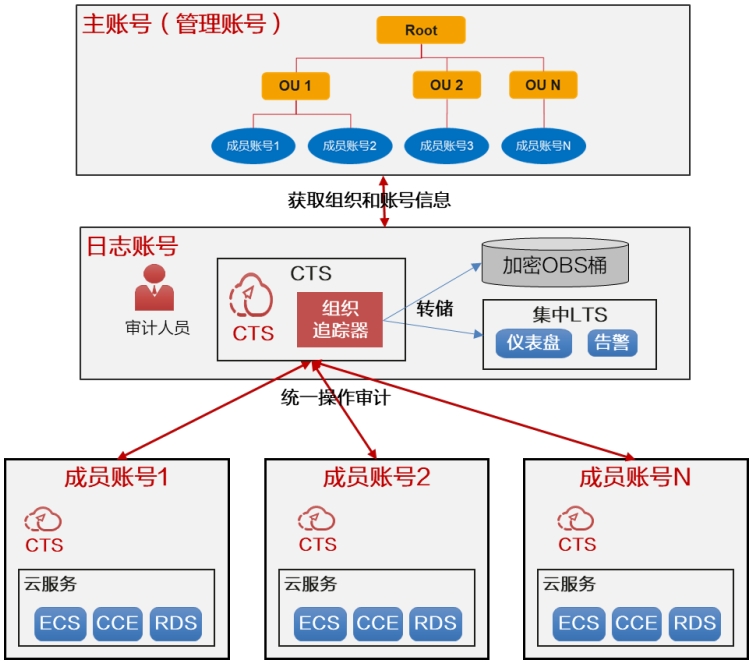
网络安全防护相关的服务，如WAF、Anti-DDoS和网络防火墙等服务，按照就近部署原则集中部署在网络运营账号，以保护网络运营账号中的NAT网关和弹性公网IP等网络连接资源。

统一合规审计

审计人员以日志账号为中心对所有成员账号进行统一的操作审计，而无需逐个登录到成员账号，如下图所示。统一的操作审计包括对所有成员账号统一配置追踪器和关键操作通知。

- 在日志账号的CTS中统一创建组织追踪器，汇聚各个成员账号中CTS收集的审计日志，配置将组织追踪器的审计记录转储到日志账号的LTS中。
- 在上述LTS中可以集中查看所有成员账号的审计记录。
- 在LTS中还可以针对关键操作（如创建、删除资源）配置告警通知。

图 3-22 多账号的统一操作审计



审计人员还可以基于Config服务提供的**组织合规规则**和**组织合规规则包**对成员账号进行统一的资源配置审计，统一呈现所有成员账号中不合规的资源配置。

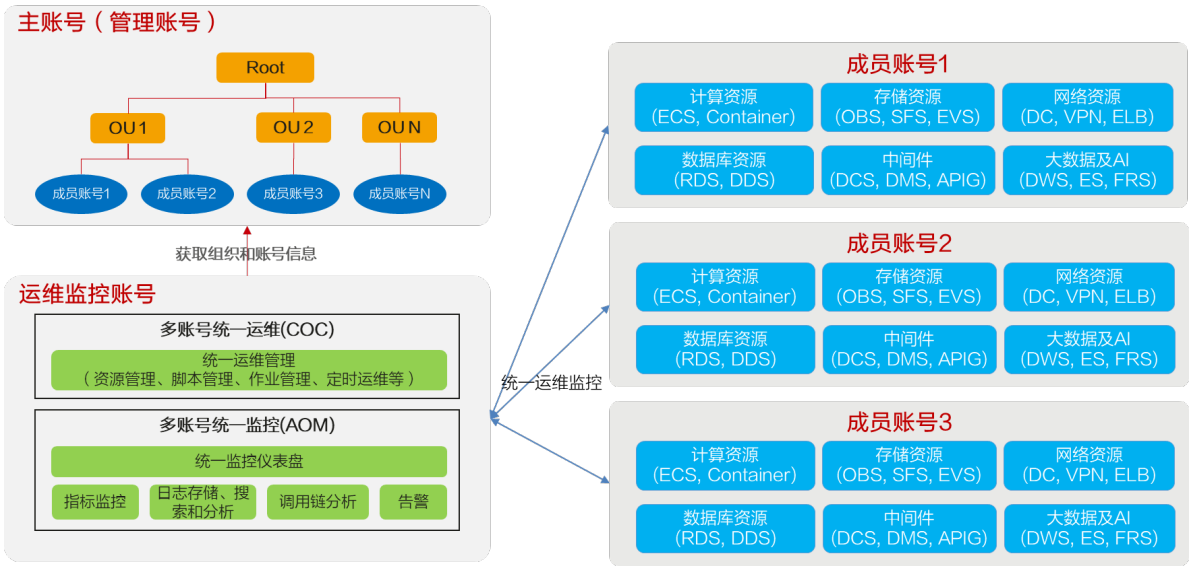
统一运维管理

以运维监控账号为中心，在这里集中部署云运维中心（Cloud Operation Center，COC）和应用运维管理服务（Application Operations Management，AOM），针对其他子账号进行统一的监控和运维管理，如下图所示。

运维监控账号中的AOM服务与其他账号下的AOM服务进行协同，可以统一接入其他账号下的各个云服务的监控指标数据，并在运维监控账号中统一查看这些指标数据，在此基础上进一步统一配置告警规则。具体实施步骤请参考**通过多账号聚合Prometheus实例实现指标数据统一监控**。

运维监控账号中的COC服务当前可以统一纳管其他账号下的云资源进行统一的资源管理，也可以将运维指令下发给其他账号执行。

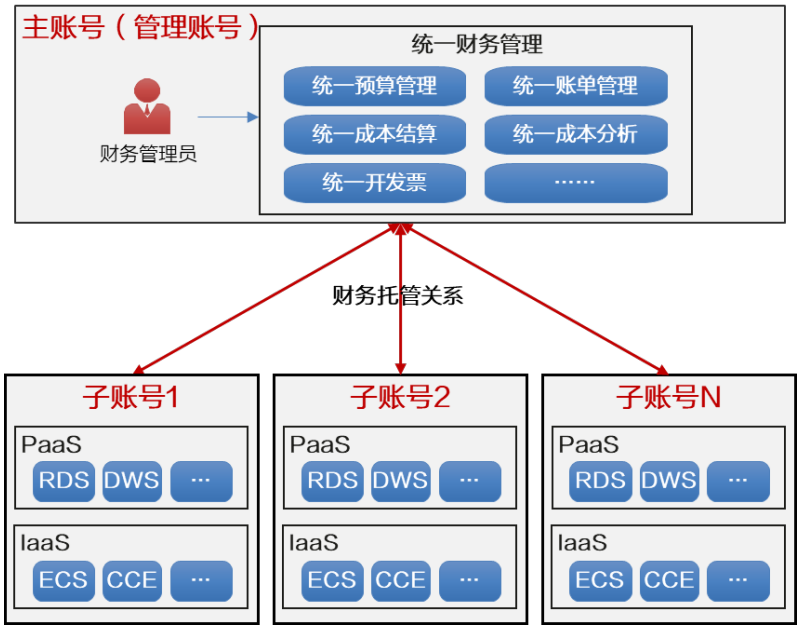
图 3-23 多账号的统一运维管理



统一财务管理

我们建议您在企业中心创建子账号时，选择财务托管模式。建立财务托管关系之后，财务管理员可以在主账号中统一管理子账号的资金、账单及发票，子账号的云资源消费统一由主账号支付。华为云统一开票给主账号，华为云的交易主体是主账号。如下图所示。

图 3-24 多账号的统一财务管理



财务托管模式下，主账号可以针对子账号执行以下统一财务管理。

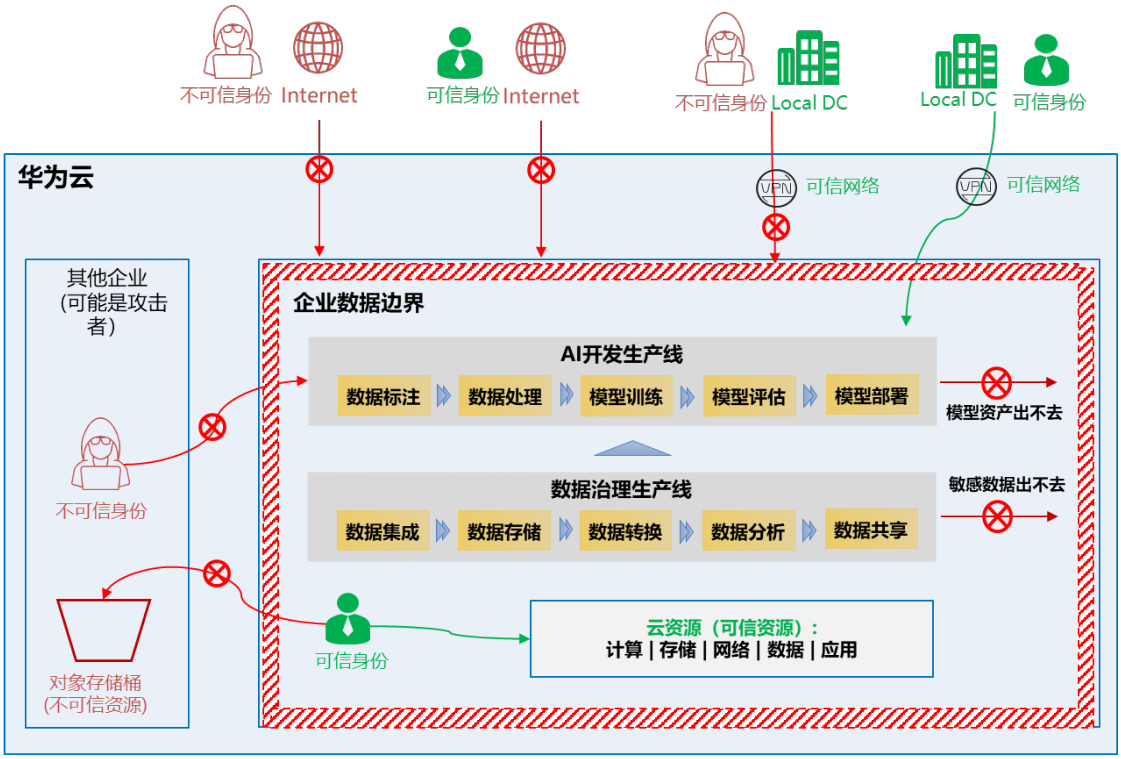
- **共享商务：**主子账号间商务实现默认共享，避免客户重复申请子账号商务，大大降低客户成本。
- **统一支付：**子账号无须通过主账号手工划拨现金、信用和代金券的方式进行消费，子账号消费统一由主账号支付，大幅降低财务操作负担。

- **一站式账单管理：**主账号可以查询所有子账号的账单，也可以将多个子账号的账单合并至一个账单。
- **统一发票：**主账号可针对单个子账号的消费开票，也可以将所有子账号的费用合并开票。
- **统一成本管理：**主账号统一管理所有子账号的成本，包括统一预算管理、统一成本预测、统一成本分析、统一成本监控和统一成本优化等，大幅提升集团企业客户的成本管理效率。

3.4.4.8 数据边界

华为云提供了全方位数据边界保护您的敏感数据，全方位数据边界基于身份控制策略、网络控制策略和资源控制策略构筑起一道坚固的数据安全屏障。确保只有经过严格验证的可信身份，在符合安全标准的可信网络环境中，方能获得对特定资源的访问权限，从而保障数据安全。如下图所示，可信身份从互联网（不可信网络）访问云资源的请求会被拒绝，不可信身份通过本地数据中心网络（可信网络）访问云资源的请求也会被拒绝，可信身份访问其他企业的对象存储桶（不可信资源）的请求还会被拒绝，只有可信身份通过本地数据中心网络（可信网络）访问本企业的云资源的请求是允许的。

图 3-25 全方位数据边界



通过全方位的数据边界提供的保护措施，您可以实现如下数据保护能力：

- 禁止业务账号直接接入互联网。只允许通过网络运营账号的DMZ网络提供互联网服务或访问互联网。
- 禁止公网访问华为云管理控制台，用户只能从内网访问控制台，确保敏感数据不经过互联网。
- 限制用户可以使用的Region，限制数据在不同Region间的转移，满足GDPR等合规要求。

3.5 安全架构设计

3.5.1 安全架构设计简介

云安全和传统IT安全虽然目标都是保护数据和系统安全，但在基础架构、安全责任、安全管理、合规与审计等方面存在显著差异。

- **在基础架构方面**，传统IT安全主要针对企业自建的物理硬件和网络设施，安全措施集中于物理环境和内部网络的防护，包括部署防火墙、入侵检测系统和防病毒软件等。云安全则基于虚拟化技术和云服务商的基础设施，安全防护需要考虑虚拟化层、多租户环境下的数据隔离、API接口安全等新挑战。
- **在安全责任方面**，传统IT环境中，企业对所有的安全层面负全责，涵盖物理硬件、网络、操作系统、应用程序和数据等。而在云环境下，采用的是安全责任共担模型。云服务商负责基础设施层面的安全，包括数据中心的物理安全、网络和虚拟化平台的安全；企业作为云服务的租户，则需要负责其在云上部署的操作系统、应用程序和数据的安全配置和管理。
- **在安全管理与技术实现方面**，传统IT安全更多地依赖于硬件设备，安全策略的实施和更新通常需要手动完成，周期较长。云安全则借助于云服务商提供的丰富安全工具和服务，如身份与访问管理（IAM）、虚拟防火墙、安全组、加密服务等，支持自动化和可编程的安全管理，能够快速响应和调整安全策略，提高了安全管理的效率。
- **在合规与审计方面**，传统IT需要企业自行确保满足相关的安全合规性，需投入大量资源进行审计和认证。云服务商通常已经通过了多项国际安全认证，企业可以借助云服务商的合规基础，但仍需对自身的应用和数据进行合规管理。

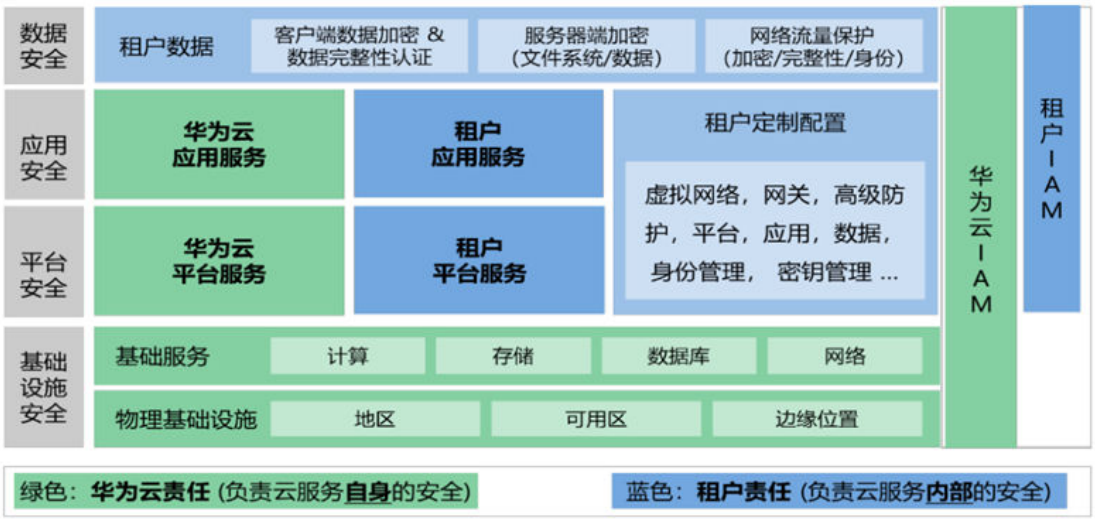
华为云对云安全整体设计和实践更侧重于为您提供完善的、多维度的、按需定制和组合的各种安全和隐私保护功能和配置，涵盖基础设施、平台、应用及数据安全等各个层面。同时，不同的云安全服务又进一步为您提供了各类可自主配置的高级安全选项。这些云安全服务需要通过深度嵌入各层云服务的安全特性、安全配置和安全管控来实现，并通过可整合多点汇总分析的、日趋自动化的云安全运营能力来支撑。

综上所述，云安全与传统IT安全的关注点和实现方式存在显著的区别。企业在云化转型的过程中，需要重新审视和调整原有的安全策略和安全架构，充分利用云服务商提供的云原生安全能力，适应云环境下的安全管理模式，保障业务和数据的安全。

3.5.2 安全责任共担

华为云把安全合规作为首要任务，安全是华为云和客户的共同责任。在云服务模式下，华为云与客户共同承担云环境的安全保护责任，为明确双方的责任，确定责任边界，华为云制定了如下图所示的责任共担模型。

图 3-26 安全责任共担模型



华为云的安全责任在于保障云平台和云服务自身的安全，涵盖华为云数据中心的物理环境和运行其上的基础服务、平台服务、应用服务等。这不但包括华为云基础设施和各项云服务的安全功能和性能，也包括对这些云基础设施和各项云服务进行安全运维和运营，以及保障华为云平台和云服务遵从相关的合规性要求。

- 华为云一方面确保各项云技术的安全开发、配置和部署；另一方面，华为云负责所提供云服务的运维运营安全，例如，对安全事件实现快速发现、快速隔离、快速响应，确保云服务的快速恢复。同时采用适合云服务的漏洞管理机制，对云服务安全漏洞及时应急响应，保证适合 CSP 运维周期的快速发布和不影响租户服务的持续部署，包括不断优化云服务的默认安全配置、补丁装载前置于研发阶段和简化安全补丁部署周期等措施。另外，华为云的安全责任还表现在开发有强大市场竞争力、简单易用的云原生安全服务。
- 华为云将其基础设施的安全与隐私保护视为运维运营安全的重中之重。基础设施主要包括支撑云服务的物理环境，华为自研的软硬件，以及运维运营包括计算、存储、网络、数据库、平台、应用、身份管理和高级安全服务等各项云服务的系统设施。同时，华为云深度集成第三方安全技术或服务，并负责对其进行安全运维。
- 华为云还负责其支撑的各项云服务的自身安全配置和版本维护。
- 华为云对租户数据提供机密性、完整性、可用性、持久性、认证、授权、以及不可否认性等方面的全面数据保护功能，并对相关功能的安全性负责。但是，华为云只是租户数据托管者，租户对其数据拥有所有权和控制权。华为云绝不允许运维运营人员在未经授权的情况下访问租户数据。华为云关注内外部合规要求的变化，负责遵从华为云服务所必需的安全法律法规，开展所服务行业的安全标准评估，并且向租户分享我们的合规实践，保持应有的透明度。
- 华为云携手云安全商业合作伙伴向租户提供咨询服务，例如协助租户对虚拟网络、虚拟机（包括虚拟主机和访客虚拟机）进行安全配置；对系统和数据库进行安全补丁管理；对虚拟网络防火墙、API 网关（API GW）和高级安全服务进行定制配置；以及协助租户进行DoS/DDoS 攻击防范演练、租户安全事件的应急响应及灾难恢复演练。

租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类各项云服务内部的安全配置进行有效管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

- 租户的安全责任细节由最终所使用的云服务来决定，具体到租户负责执行什么默认和定制的安全配置。对于华为云的各项云服务，华为云只提供租户执行特定安全任务所需的资源、功能和性能，而租户需负责各项租户可控资源的安全配置工作。
- 租户负责部署配置：（1）其虚拟网络的防火墙，网关和高级安全服务等的策略配置；（2）租户的虚拟网络、虚拟主机和访客虚拟机和容器等云服务所必需的安全配置和管理任务（包括更新和安全补丁）、容器安全管理（包括容器集群、节点和容器的安全配置、访问控制安全配置等）、大数据分析等平台服务的租户配置；（3）其他各项租户租用的云服务内部的安全配置等；（4）其自行部署在华为云的任何应用程序软件或实用程序进行安全管理。
- 在配置云服务时，租户负责各项安全配置，在部署到生产环境前应做好充分测试，以免对其应用和业务造成负面影响。对大多数云服务的安全性而言，租户只需配置账户对资源的访问控制并妥当保管账户凭证。少数云服务需要执行其他任务，才能达到应有的安全性。各项监控管理服务和高级安全服务具有较多安全配置选项，租户可寻求华为云和其合作伙伴的技术支持，以确保安全性。
- 以华为云MapReduce服务（MRS）为例，租户应负责：（1）管理其购买的MRS大数据集群的弹性IP、虚拟网络防火墙等策略配置；（2）配置访问控制策略，如弹性IP绑定的端口仅对信任的网络或主机开放，避免大数据集群直接暴露在互联网；（3）负责大数据集群的用户管理、大数据组件的安全配置，并且妥当保管相关的账户凭证；（4）以及对其部署在大数据集群上的应用进行安全管理。
- 再以数据库服务为例，租户应负责：数据库引擎的生命周期管理及数据库安全管理，包括（1）缺省使用最新的实例版本、及时根据官网提示和漏洞通告升级版本等；（2）梳理资产分类及制定数据库实例防护策略，如数据库主备及集群设计、数据灾备及恢复策略、VPC及安全组配置、互联网访问配置、访问通道加密配置、数据库认证和鉴权配置、数据库审计配置以及其他安全配置。
- 无论使用哪一项华为云服务，租户始终是其数据的所有者和控制者。租户负责各项具体的数据安全配置，对其保密性、完整性、可用性以及数据访问的身份验证和鉴权进行有效保障。在使用统一身份认证服务（IAM）和数据加密服务（DEW）时，租户负责妥善保管其自行配置的服务登录账户、密码和密钥，并负责执行密码密钥设定、更新和重设规则的业界优秀实践。租户负责设置个人账户和多因子验证 (MFA)，规范使用安全传输协议与华为云资源通信，并且设置用户活动日志记录用于监测和审计。
- 租户负责对其自行部署于华为云上、不属于华为云提供的各项应用和服务所必需的合规遵从，并自行开展所服务行业的安全标准评估。华为云提供**安全基线配置指南**，供租户配置参考。

需要注意的是，云计算的服务类型（IaaS、PaaS和SaaS）、云计算的服务模式（云服务交付、云软件交付等）、安全厂商的引入，都会影响各自的安全责任范围，为此华为云与中国信通院在2024年联合发布了《云安全责任共担模型》，该份白皮书详细介绍了云安全责任共担2.0体系，同时提供了云安全责任共担机制的实施参考。

3.5.3 安全设计原则

华为云根据自身安全实践和成功交付大量项目的经验，提炼了如下十大安全设计原则，你可以在此基础上设计企业在云上的整体安全方案。

- **零信任原则（Zero Trust Principle）**

  遵循“永不信任，始终验证”的安全理念，假设任何人或程序都不可信，无论是内部用户、外部用户还是网络设备。系统内的组件进行任何通信之前都将通过显式的验证，减少系统信任带来的攻击面。零信任把现有的基于实体鉴别和默认授权的静态信任模型（非黑即白），变成基于持续风险评估和逐次授权的动态信任

模型。零信任不根据网络空间位置决定可信度，其重心在于保护资源，而不是网段。与传统安全理念对比，它将网络防御的重心从静态的、基于网络的边界转移到了用户、设备和资源上。所有的资源（如人/物/终端/应用/网络/数据/供应链）都需要进行持续身份验证和信任评估，从全局视角执行动态安全策略。零信任通过动态、持续性的实体风险评估，缩小受攻击面，保证系统安全。

- **最小授权原则（Principle of Least Privilege）**

  基于华为云的细粒度授权机制，只授予用户或应用程序完成任务所需的最小权限，限制访问权限可以减少攻击面，即使用户密码或应用程序被攻破，攻击者也难以获得更广泛的访问权限。如果用户或应用程序的任务产生变化，也应该及时调整权限确保任务能够顺利完成。

- **纵深防御（Defense in Depth）**

  不要依赖单一的安全机制，而是采用多层安全措施，即使一层防御失效，其他层也能提供保护。这就像城堡的护城河、城墙、城门等多重防御体系。需要企业建立覆盖涵盖全技术堆栈的纵深防御机制，将多种类型的安全控制应用于所有技术堆栈，包括网络边缘、VPC、云存储、ECS实例、操作系统、应用程序配置和代码等。

- **安全和成本平衡（Balance between Security and Cost）**

  尽管安全领域强调纵深防护，但越全面的安全防护方案的成本也更高。企业应基于业务系统的合规要求（如信息安全等级保护）和敏感数据的分类分级设计成本可接受的安全防护方案，不应盲目针对所有的业务系统和数据都采用全方位和高级别的安全防护方案。

- **云原生安全防护（Cloud Native Security）**

  云服务商提供了丰富的云原生安全服务（比如WAF、Anti-DDoS、云防火墙、秘钥管理等）。这些云原生安全云服务与云平台深度集成，在性能、弹性、便利性上有较好的优势，同时，云服务商的安全运营经验也会持续推动云原生安全服务的能力提升，因此建议企业优先选择云原生安全服务。华为云提供的云原生安全服务清单，请参考章节**云原生安全服务**-。

- **攻击者视角（Attacker Perspective）**

  企业应当从攻击者视角评估业务系统的安全性，识别安全风险，据此加固安全方案，以降低系统被攻击的可能性、提升攻击成功的难度，让攻击者发起攻击的成本超过其获得的利益。

- **持续安全运营（Continuous security operation）**

  安全防护三分在于技术，七分在于运营。只有不断优化安全管理流程、持续安全运营、持续监控和评估云环境的合规性，才能保障业务系统的长期安全稳定运行。

- **木桶原则（Barrel Principle）**

  安全是一项系统工程，适用木桶原则，任何一项安全短板都会降低整体安全性，因此要避免安全短板的出现。

- **人和数据分离（Separation of people and data）**

  利用工具和管理机制减少人员直接访问和处理数据的必要性，减少处理敏感数据时出现人为错误和人为删改的风险。

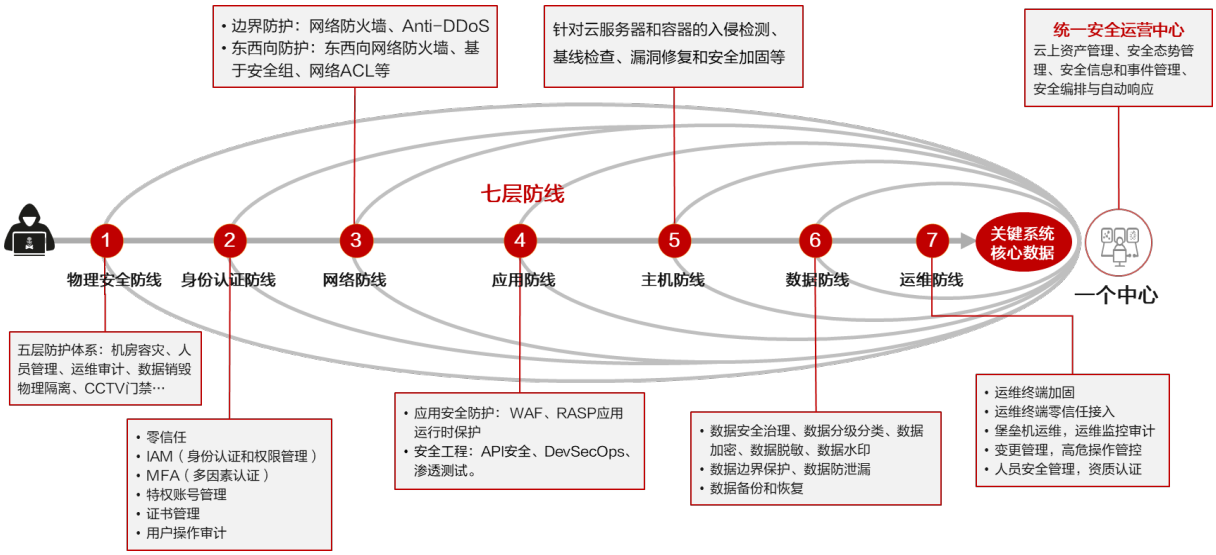
- **DevSecOps**

  将安全性纳入到整个软件开发生命周期中，从需求分析、设计、开发、测试、部署、运维、运营的每个阶段都考虑安全性，以确保系统的安全性和稳定性。通过将安全检测手段与DevOps的自动化流程相结合，DevSecOps可更快地检测和修复安全漏洞，并提高软件开发的效率和质量。

3.5.4 安全参考框架

基于上述安全设计原则，华为云推荐采用“一个中心 + 七层防线”的安全参考框架和华为云提供的云原生安全服务来构筑企业的云上安全防护体系，如下图所示。该安全框架完全遵守了纵深防御原则，将各种安全防护措施有机组合起来，针对保护对象（企业的关键业务系统和核心数据），因地制宜的部署合适的安全措施，形成多层安全防线，各层安全防线能够相互支持和补救，避免攻击者突破单层防线后畅通无阻，层层阻击，为防御方检测响应赢得时间。

图 3-27 一个中心和七层防线



- **物理安全防线**

  华为云建设和运营的数据中心都严格实施了五层安全防护，包括机房容灾、人员管理、运维审计、数据销毁和物理隔离、CCTV和门禁等防护措施，华为云的租户无需关注数据中心的物理安全。但对于部署在企业自建机房的专属云，企业需要自己做好物理安全防护。

- **身份认证防线**

  需要基于零信任理念做好身份认证和权限管理，授权要遵从最小授权的原则，用户认证默认要启用多因素认证，管理好特权账号，对用户在云平台上的任何操作进行记录和审计。建议参考官网提供的**IAM最佳实践**。

- **网络防线**

  核心是要做好网络边界防护和内网东西向的访问控制。

  - **网络边界防护：**网络边界主要指的是企业内部网络与外部网络的边界，典型的场景如互联网接入、VPN、专线接入。客户可以基于华为云提供的云防火墙（Cloud Firewall，CFW）、VPC的安全组和ACL实施网络边界访问控制。CFW内置了网络入侵检测、入侵防御的功能。网络边界的策略应该严格按照白名单开通，应该禁止对外开放高危端口和协议。
  - **东西向网络防护：**应该对不同的业务按密级实施分层分级管理，如将不同密级的业务部署在不同的VPC中，通过VPC实施大的网络安全域隔离，通过CFW实施东西向VPC网络之间访问控制，并通过VPC的安全组和ACL在VPC内进一步实施网络微分段隔离。

- **应用防线**

面向互联网发布的应用应该默认部署WAF防护。应用的安全是设计出来的，要重视在软件安全工程上的投入，提高应用的内生安全能力。从安全风险的角度，应优先关注面向外部网络暴露的应用，同时要识别内部核心关键应用，对这些应用优先实施针对性的安全加固。

- **主机防线**

  在主机层面进行入侵检测往往是最有效的，主机上要全面覆盖主机安全产品，主机安全产品可以帮助做好主机的漏洞管理，安全配置管理等基础性工作。

- **数据防线**

  要做好数据资产的主动发现和分类分级，围绕数据全生命周期开展数据安全治理工作，对重要数据使用过程中考虑脱敏、加密、审计等措施，对重要数据做好备份。基于身份控制策略、网络控制策略和资源控制策略构筑坚固的数据安全边界，保障敏感数据不泄露。

- **运维防线**

  要限制只能从安全的网络环境发起运维活动，并为运维人员建立专门的运维访问通道，如让运维人员使用专门的运维服务、堡垒机接入运维，尽量减少黑屏运维操作，降低运维活动过程中的不确定性，确保运维的活动可审计可追溯。

- **一个中心**

  安全防护三分在于技术，七分在于运营，只有各层防线的安全产品得到正确的配置和良好的维护，才能有效的发挥出安全防护的效果。通过一个统一的安全运营平台，将各种安全产品能力有机的整合起来，将安全防护的效果最大化。

纵深防御体系的建设往往需要经历一个漫长的过程，很难一蹴而就，在建设的过程中需要考虑安全、效率、成本和体验方面的平衡。企业应该例行开展安全风险评估，针对TOP安全风险实施针对性的安全加固，持续提升安全防护的能力，并通过红蓝对抗等机制来检验安全防护体系的有效性。

3.6 平台工程

3.6.1 什么是平台工程

平台工程（Platform Engineering）是一种通过构建和运营自助式内部开发平台（IDP，Internal Developer Platform）来优化软件交付和生命周期管理的工程学科。其目标是通过标准化和自动化的方式，减少开发人员与底层基础设施之间的复杂交互，从而提高开发效率和交付速度。Gartner在2023年和2024年连续将其列为十大重要战略技术趋势，并预测到2026年将有80%的大型软件工程组织将建立平台团队为开发者提供可重用的服务、组件和工具。平台工程对企业带来的价值如下：

- **提升开发者体验:** 平台工程提供自助服务功能，简化了基础设施配置、应用部署和管理等流程，让开发者更专注于业务逻辑的开发，而不是底层基础设施的管理。
- **加速软件交付:** 通过提供预先配置好的环境、自动化流程和可重用的组件，平台工程可以显著缩短软件交付周期，更快地将产品推向市场。
- **提高运营效率:** 平台工程通过自动化和标准化，减少了手动操作和人为错误，提高了运营效率，并降低了运营成本。
- **增强安全性合规性:** 平台工程可以内置安全策略和合规性检查，确保应用和基础设施符合安全标准和法规要求。
- **促进创新:** 平台工程为开发者提供了更灵活、更便捷的开发环境，鼓励他们尝试新技术和新方法，从而促进创新。

3.6.2 如何构建平台工程

在云平台上构建平台工程，可以充分利用云平台提供的丰富服务和工具，降低构建和维护成本，并提高IDP的可靠性和可扩展性。以下是一些关键步骤。

明确平台工程的目标和需求

平台工程的核心目标是通过构建自助式内部开发平台（IDP），优化软件交付和生命周期管理，提高开发效率和交付速度。为此，您需要详细分析企业当前的开发流程和痛点，确定哪些环节需要优化。例如，可能存在环境配置复杂、部署流程繁琐、资源获取周期长等问题。通过与各个团队的沟通，收集需求，明确需要哪些服务、工具和功能来支持开发人员的工作。通过需求分析，制定平台工程的目标，包括但不限于：

- 提供统一的应用开发、测试和部署平台。
- 实现自动化的持续集成和持续交付（CI/CD）流水线。
- 沉淀和复用企业内的公共组件和服务。
- 建立完善的监控和运维机制。
- 确保平台的安全性和合规性。

基于华为云搭建 IDP

华为云提供了丰富的云服务可以帮助您快速构建企业的内部开发平台。

1. **应用平台（AppStage）**是基于平台工程理念打造的下一代应用全生命周期管理和AI原生应用生命周期管理平台，帮助客户快速高效地实现传统应用及AI原生应用全生命周期管理，为应用构建、运维和运营等生命周期管理活动提供自助式服务能力，目标是通过标准化和自动化的服务来提升用户体验 ，促使客户可以专注于交付应用逻辑和云上业务创新。
2. **软件开发生产线（CodeArts）**是面向开发者提供的一站式云端平台，即开即用，随时随地在云端交付软件全生命周期，覆盖需求下发、代码提交、代码检查、代码编译、验证、部署、发布，打通软件交付的完整路径，提供软件研发流程的端到端支持。
3. **应用管理与运维平台（ServiceStage）**是面向企业的应用管理与运维平台，提供应用发布、部署、监控与运维等一站式解决方案。支持Java、Php、Python、Node.js、Docker、Tomcat技术栈。支持Apache ServiceComb Java Chassis（Java Chassis）、Spring Cloud等微服务应用。
4. **微服务引擎**（Cloud Service Engine，CSE），是用于微服务应用的云中间件，支持华为云贡献到Apache社区的注册配置中心Servicecomb引擎、开源增强的注册配置中心Nacos引擎和应用网关。您可结合其他云服务，快速构建云原生微服务体系，实现微服务应用的快速开发和高可用运维。
5. **云应用引擎**（Cloud Application Engine，CAE）是一个面向WEB、微服务应用的Serverless托管服务，提供极速部署、极低成本、极简运维的一站式应用托管方案。支持从源码、软件包、镜像包快速发布应用，秒级弹性伸缩、按量付费。可做到基础设施免运维，根据可观测的运行指标对应用进行生命周期管理。

沉淀公共服务

您需要对企业内部的公共组件和服务进行梳理和沉淀，这是提升平台工程价值的关键。首先，您需要识别企业内部被多个应用系统共用的软件组件，例如认证组件、日志组件、消息组件等，对这些组件进行标准化，确定接口定义、数据格式和错误处理机制，确保组件的一致性和可复用性。然后，将这些公共组件封装成独立的微服务，

部署在CSE之上。通过CSE的服务注册中心，实现微服务的自动注册和发现，其他应用系统可以通过调用这些微服务来使用这些公共组件，避免重复开发，提高开发效率，并保证代码质量的一致性。利用CSE的服务治理功能，您还可以进一步提升公共组件的可靠性和性能。您需要编写详细的组件使用文档和API说明，方便开发者查阅和使用。并且需要建立组件的版本管理机制，规范组件的升级和维护流程，确保组件的持续优化和迭代。

建立完善的监控和运维机制

为了保障平台和应用的稳定运行，需要建立覆盖基础设施、平台服务和应用层面的监控和运维机制。您可以利用**应用运维管理服务（AOM）**，集中监控微服务的性能指标，如响应时间、错误率和调用次数等，帮助快速定位和解决问题。您可以采用**日志服务（LTS）**收集和分析系统日志和应用日志，支持日志检索、告警和报表功能，方便故障排查和性能分析。此外，您还可以使用**应用性能管理（APM）**，监控应用的调用链路，分析性能瓶颈，定位异常请求，提升应用性能。

持续迭代和优化

平台工程的建设是一个持续优化的过程，需要根据使用情况和技术发展，不断地改进和完善。定期与开发、测试、运维等团队进行沟通，收集他们对平台的建议和意见。利用监控数据分析平台的性能指标，识别性能瓶颈，优化资源配置。

同时，关注云原生、容器化、微服务和Serverless等新技术的发展，评估其在平台中的应用价值。选择适合的项目进行新技术试点，验证效果后逐步推广。完善平台的使用手册、API文档和最佳实践等，方便新成员快速上手。定期组织培训，提升团队对平台的理解和使用水平。

3.7 云运营模式

3.7.1 什么是云运营模式

在云计算技术出现之前，企业已经建立了IT运营模式用来定义IT如何支撑业务发展。狭义上的IT运营模式是指企业管理和运营其IT资源、服务和基础设施的方式，它涉及到如何有效地配置、管理和优化IT资源，旨在提升性能和效率、降低成本、增强灵活性，以支持企业的业务目标和战略。广义上的IT运营模式还包括组织结构、运营流程、角色和职责等要素。简单来讲，IT运营模式是指IT部门如何运作的方式。传统的IT运营模式侧重于部署在自建数据中心或IDC机房的IT基础设施，包括IT硬件和虚拟化等基础软件，企业通常需要一次性购买IT硬件和基础软件资产，支撑业务系统的安全稳定运行。IT硬件的性能会逐步下降甚至损坏，技术人员需要花费大量时间管理、维护和更新IT硬件。

当云计算技术出现之后，企业基于云平台和云服务搭建IT基础设施，并逐步把大量业务系统迁移或者直接部署在公有云上，IT运营模式进入云计算时代。基于云平台的IT运营模式（简称云运营模式）将企业的关注点从IT基础设施上移到应用程序和数据资产，您需要有效配置、管理和优化云资源，以支持业务系统在云上的安全稳定运行。简单来讲，云运营模式是指企业如何利用云技术和云服务支撑业务发展的方式。云运营模式和传统IT运营模式的目标是一致的，都是通过技术支撑企业达成业务目标，最大化业务价值。两者的差异如下表所示。

表 3-11 传统 IT 运营模式和云运营模式的区别

比较项	传统IT运营模式	云运营模式
成本模式	• 依赖于资本支出（Capex），需要提前规划和购买硬件设备，周期较长。	• 采用按需付费的运营支出（Opex）模式，企业可以根据实际使用情况灵活调整成本，减少了前期投入。
管理重点	• 企业的管理重点在于IT基础设施的维护、服务器的正常运行时间以及数据中心的物理安全。	• 企业的管理重点转向更高层次的操作，如应用程序的性能优化、数据管理和云安全。
敏捷性	• 硬件采购和部署周期较长，资源扩展需要经过复杂的审批和采购流程，响应速度较慢。 • 创新和变更受到硬件资源的限制，难以快速适应业务需求的变化。	• 云资源可以按需动态扩展或缩减，企业可以快速响应业务需求的变化。 • 部署新应用或功能的速度显著提高，支持敏捷开发和持续交付。 • 创新不再受硬件采购周期的限制，企业可以更快地试验和推出新产品或服务。
安全性	• 企业承担所有的安全保护职责。 • 安全性主要依赖于数据中心的物理边界和内部网络的防护。	• 采用共享安全责任模型，云服务商负责云平台和云服务本身的安全，企业负责上层应用和数据的安全。 • 云服务商也会提供云原生安全服务和云安全最佳实践帮助企业保护上层应用和数据的安全。
人员技能	• 技术人员主要管理和维护IT基础设施，需要大量时间处理硬件故障、性能优化和系统更新等工作 • 需要具备硬件维护、网络管理、虚拟化技术等技能。	• 技术人员需要掌握云平台的使用、云资源的配置与优化、自动化运维工具以及云安全管理等技能。 • 需要具备更加高层次的技能，如应用程序性能优化、数据管理。

云运营模式在灵活性、敏捷性和成本效益方面具有显著优势，但也对企业的人员技能和安全管理提出了更高的要求。企业需要根据自身业务需求和发展战略，逐步从传统IT运营模式向云运营模式转型。

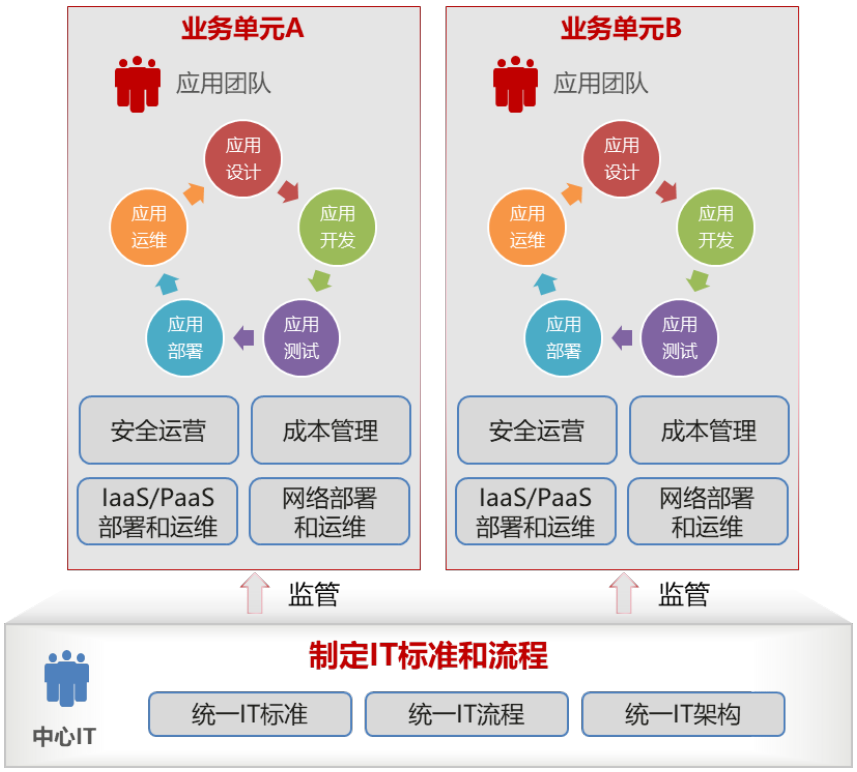
云运营模式并不是企业云化转型的结果，并不是把业务系统都迁移到云上就自然拥有了一个能够有效支撑业务目标的云运营模式。制定一个良好的云运营模式是确保企业云化转型成功的前提。企业需要根据当前的IT运营模式和业务系统的特点设计最佳的云运营模式，以最大化云计算带来的业务价值。云运营模式需要明确CCoE团队和应用团队之间的责任界面和协作机制。华为云基于大量企业的云化转型经验，总结了以下三种云运营模式。

3.7.2 去中心化运营模式

去中心化运营模式是常见运营模式中最简单的一种，如下图所示。在这种运营模式中，所有业务系统都由专门的应用团队独立运营，应用团队不仅负责应用的设计、开

发、测试、部署和运维工作，还需要负责业务系统所需IaaS和PaaS资源的部署和运维，同时要确保业务系统的安全性和云资源的成本管理。中心IT团队仅负责制定统一IT标准和IT流程，通过发文的方式让各个业务系统采纳，并监管业务系统的执行情况，但没有办法强制业务系统执行这些标准和流程。在这个运营模式下，基本上不需要专门成立CCoE团队。

图 3-28 去中心化运营模式



去中心化运营模式的优点如下：

- **敏捷性高：**各业务单元根据自身需求快速部署和扩展资源，加快创新速度。
- **贴近业务：**应用团队更了解业务需求，可以更好地定制云解决方案。
- **责任明确：**各业务单元对自己的云环境负责，更容易追溯问题和优化性能。

去中心化运营模式的缺点如下：

- **缺乏一致性：**各业务单元独立部署和运维所需的云环境，缺乏统一的IT标准和安全策略，可能导致标准不统一，安全策略不一致，增加管理难度。
- **成本增加：**缺乏中央协调，容易导致重复建设和资源浪费，进而增加云成本。
- **缺乏整体视图：**难以获得企业整体的云资源使用情况，阻碍战略决策和优化。

基于上述优缺点分析，去中心化运营模式适合那些需要完全控制云资源创建和运维的创新业务系统，这些创新业务系统需要紧贴业务需求进行快速创新和迭代。

3.7.3 集中化运营模式

去中心化模式更强调的是快速创新而不是集中控制，集中化运营模式正好相反，强调的是集中控制而不是快速创新。如下图所示，在集中化运营模式中，CCoE团队负责集中建设和维护Landing Zone，包含云上的骨干网、IAM和合规审计系统等，同时对企

业范围内的云环境进行集中化的IT治理。业务系统所需的云资源也由CCoE团队负责集中部署和运维，所以CCoE团队更容易识别出各个业务系统所需要的公共资源，进而集中部署和管理这些公共资源，同时也需要通过集中化的手段统一管理所有业务单元下的云资源，并进行集中的安全运营和成本管理。应用团队完全不用关心基础设施和云资源的部署和管理，可以将主要精力放在应用的设计、开发、测试、部署和运维工作上。

图 3-29 集中化运营模式

集中化运营模式的优点如下：

- **集中化管理：**集中化管理确保一致的安全策略、合规性和标准化流程，降低风险，相比分散管理，集中化管理还可以降低运营复杂度，提高效率。
- **成本优化：**通过统一搭建公共资源、集中采购和资源整合，提升资源利用率，降低总体成本。
- **全局视图：**CCoE团队集中监控和分析整个企业的云资源使用情况，可以进一步优化资源配置。

集中化运营模式的缺点如下：

- **缺乏敏捷性：** 所有云资源请求都需要经过CCoE团队，可能导致响应速度慢，影响业务的敏捷性。
- **瓶颈风险：** CCoE团队的工作负荷过重，无法及时满足各业务单元的需求，影响效率。
- **缺乏业务理解：**CCoE团队可能不理解具体业务场景，导致资源配置不匹配业务需求。

- **难以满足多样化需求：**统一的标准可能难以满足不同业务单元的特定需求。

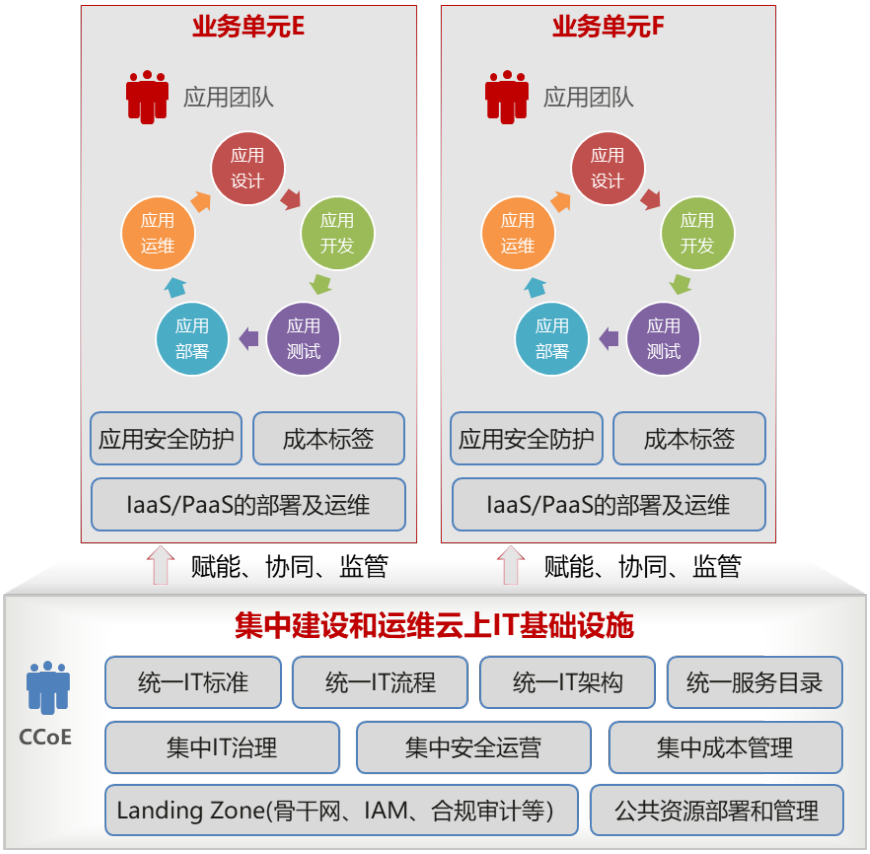
基于上述优缺点分析，集中化运营模式适合稳态的业务系统，这些业务系统的更新频率比较低，例如企业采购的SAP等商业软件，或者企业自研的进入成熟期的业务系统。集中化运营模式也适合那些由IT部门统一建设和运维的业务系统。

3.7.4 赋能和协同运营模式

赋能和协同运营模式综合了上述两种云运营模式的优点，既允许一定程度的集中化管理，也确保业务系统的敏捷性。如下图所示，在赋能和协同运营模式中，CCoE团队负责集中建设和维护Landing Zone，包含云上的骨干网、IAM和合规审计系统等，同时负责制定统一的IT标准、IT流程和IT架构，以及对企业范围内的云环境进行集中化的IT治理。CCoE团队赋能应用团队全权负责业务系统所需云资源的部署和运维，这样既可以减轻CCoE团队的负担，又可以提升应用团队的自主性，进一步提升应用系统的敏捷性。为避免各业务单元独立部署和运维云资源带来的标准不统一问题，CCoE团队需要制定相应的IT治理策略强制各个业务单元遵守相应的IT标准，CCoE团队还可以制定统一的服务目录，应用团队只能使用经过CCoE团队授权的云服务来开发和部署业务系统。

CCoE团队和应用团队要紧密协同，共同保障业务系统在云上的安全稳定运行并实现最优的成本效益。在运维方面，CCoE团队负责云上IT基础设施（包括骨干网、IAM和合规审计系统等）的日常运维，各个业务单元的应用团队负责应用及所需云资源的日常运维，业务系统出现故障后两边协同进行故障定位和修复。在安全运营方面，CCoE团队负责平台层面的安全防护和集中安全运营，各业务单元的应用团队需要关注应用层的安全防护，如防止SQL注入等；在成本管理方面，CCoE团队负责集中化的成本管理，包括集中化的成本计划、成本监控、成本分析和成本优化等，各业务单元的应用团队需要负责针对云资源打上成本标签。

图 3-30 赋能和协同运营模式



赋能和协同运营模式兼具上述两种运营模式的优点：

- **平衡集中控制和敏捷性：**既能保持集中化管理和控制，又能赋予业务单元一定的自主权，提升业务敏捷性。
- **紧密协同：**CCoE团队与业务单元的应用团队紧密协同工作，避免出现问题时的互相推诿，提升整体运营效率。
- **成本优化：**通过统一搭建公共资源、集中采购和资源整合，提升资源利用率，降低总体成本。
- **全局视图：**CCoE团队集中监控和分析整个企业的云资源使用情况，可以进一步优化资源配置。

赋能和协同运营模式的缺点如下：

- **实施复杂度高：**需要制定复杂的IT治理措施，强制各个业务单元执行统一的IT标准，另外还需要额外定义和管理统一的服务目录。
- **能力要求高：** 成功实施需要组织具备成熟的管理能力和丰富的IT 治理实践，同时对CCoE团队成员的技能要求更高，需要承担布道师角色，赋能和推动应用团队按照最佳实践去部署和运维云资源。

基于上述优缺点分析，赋能和协同运营模式更适合敏态的业务系统，这些业务需要快速迭代发布新功能，以满足快速变化的市场需求，如自研的数字化营销系统。另外，如果稳态业务系统拥有IT能力较强的独立应用团队，也可以采用这种运营模式。

需要注意的是，上述三种云运营模式适合不同的业务系统和组织特征，而在一个大型企业里面，很有可能同时存在这些业务系统，所以需要混合使用这几种云运营模式来支撑这些业务系统的敏捷迭代和安全稳定运行。

云运营模式将深刻影响应用生命周期管理流程，下一个章节将会展开介绍。

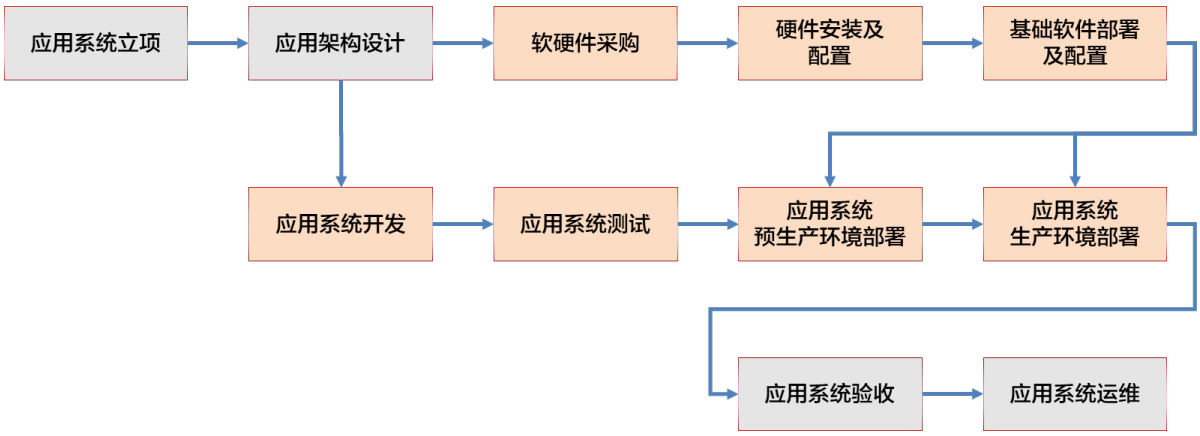
3.8 应用生命周期管理

企业云化转型最核心的工作就是将支撑企业生产和运营的各种应用系统云化。首先，最基本的要求是保障应用系统可以在云平台上长期安全稳定运行；其次，要让应用系统可以充分利用云计算的优势提升应用系统的质量，如提升应用系统的韧性、敏捷性、安全性和性能等，最后，应用系统生于云、长于云，可以基于云平台提供的新技术快速进行产品、服务甚至商业模式的创新，孵化新功能、提高业务运营效率、提升用户体验，并带来增量收入。

然而应用系统云化是一项复杂的系统性工作，需要从应用生命周期管理（Application Lifecycle Management，简称ALM）角度考虑如何进行云化，确保应用生命周期的各个阶段都能够充分利用云计算的优势。

基于传统IT的应用生命周期管理流程如下图所示。应用系统的部署依赖硬件资源，但硬件采购和发货周期比较长，所以在应用系统立项之后就需要开始着手硬件设备和基础软件的采购，硬件到货后再将这些硬件部署到自建数据中心或者租赁的IDC机房，然后在这些硬件设备上再安装和配置操作系统和虚拟化软件等基础软件，基于这些硬件搭建应用系统所需的预生产环境和生产环境。等应用系统完成开发和测试后，就可以直接在预生产环境和生产环境上部署运行。一种常见的场景是企业购买的是现成的商业软件（如ERP、CRM），基本上不涉及应用程序的代码开发工作，或者只需要很少的跟周边系统的集成开发工作，这种场景的应用上线时间很容易被硬件的采购和发货周期阻塞和延迟。

图 3-31 基于传统 IT 的应用生命周期



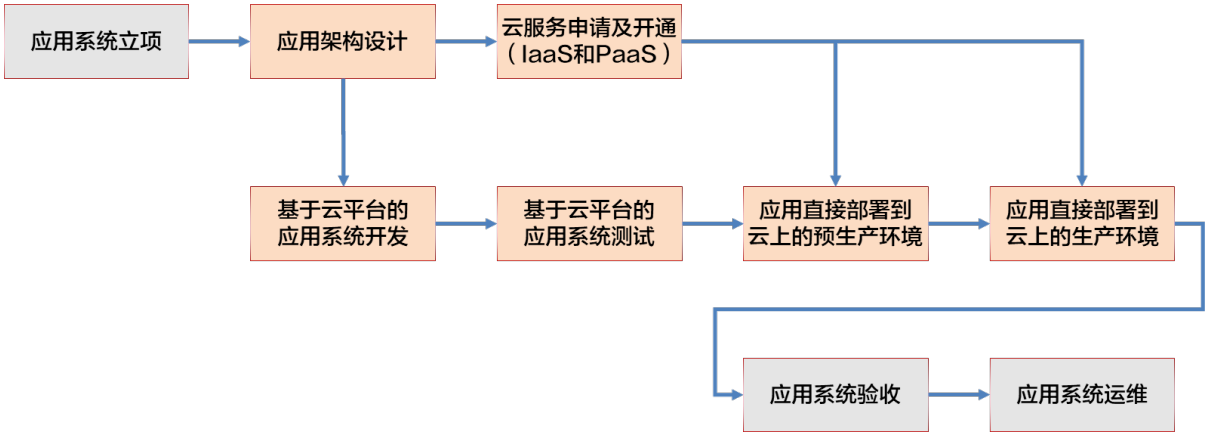
基于云计算的应用系统建设的基本流程没有变化，但要求应用生命周期的某些阶段（上图中浅黄色标示的阶段）需要进行调整以适配云计算的特点，进而充分发挥出云计算的价值。

首先，由于云平台已经搭建了统一的资源池，并提供了应用系统所需要的IaaS和PaaS云服务，所以应用系统的建设过程中不再需要独立采购硬件设备和基础软件（操作系统、虚拟化软件等），您只需要按需购买和开通云平台提供的IaaS和PaaS云服务就可以即时搭建出来应用系统所需的测试环境、预生产环境和生产环境，不再需要等待企业的采购周期和厂商的发货周期。上图中的“软硬件采购”、“硬件安装及配置”和“基础软件部署及配置”三个环节在云计算模式下都可以归一到“云服务申请及开通”环节。

其次，由于云平台提供了云原生的DevOps开发工具链，如华为云提供的CodeArts,而且华为云提供的云服务都对外开放了很多API，您完全可以基于这些云原生的工具链和

API进行应用系统的开发及测试，并通过流水线将应用系统直接部署在云平台上的预生产环境和生产环境。这样的应用系统从开发、测试、部署到运行都是在云平台之上进行，也就是我们常说的云原生应用，通过这种方式可以更加充分发挥云计算的价值。下图是基于云计算的应用生命周期。

图 3-32 基于云计算的应用生命周期



基于云计算的应用生命周期管理需要与前面介绍的云运营模式匹配，不同的云运营模式下，CCoE（或中心IT）与应用团队之间的责任边界和协作关系是不一样的，所以应用生命周期管理流程也会发生变化。

去中心化运营模式

在该模式下的应用生命周期管理流程如下图所示。应用团队全权负责应用的整个生命周期管理。中心IT团队仅负责制定统一IT标准，在应用系统的架构设计环节，中心IT团队对其提出架构、运维和安全等方面的IT标准建议，并监管应用系统的执行情况，但没有办法强制应用系统执行这些标准。

图 3-33 去中心化运营模式的 ALM

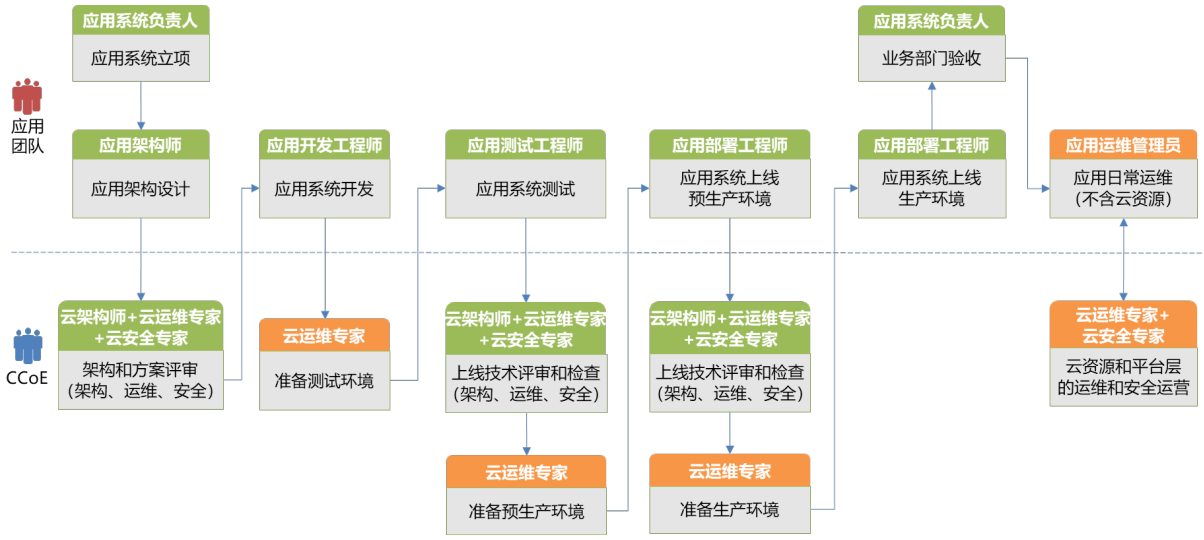
集中化运营模式

在该模式下的应用生命周期管理流程如下图所示。应用系统所需的云资源由CCoE团队负责集中部署和运维，应用团队完全不用关心基础设施和云资源的部署和管理，可以将主要精力放在应用系统的设计、开发、测试、部署和运维工作上。CCoE团队的云架构师、云运维专家和云安全专家需要在应用架构设计阶段深入参与进来对应用团队的

设计方案进行架构、运维和安全评审，确保方案符合云技术的设计原则和最佳实践，以充分发挥云计算的价值。为了避免设计阶段遵守但开发阶段不遵守最佳实践的情况，云架构师、云运维专家和云安全专家还需要在应用系统上线预生产环境和生产环境前对应用系统进行上线技术评审和检查，确保设计方案和最终实现的方案是一致的。通过一前一后的评审，CCoE团队将能够帮助应用团队大幅提升应用系统在云平台之上的韧性、安全性和性能等指标。

在应用运维阶段，CCoE团队负责云资源和平台层的日常运维和安全运营，应用团队需要负责应用软件本身的日常运维以及应用层的安全运营，如防止SQL注入等。

图 3-34 集中化运营模式的 ALM



赋能和协同运营模式

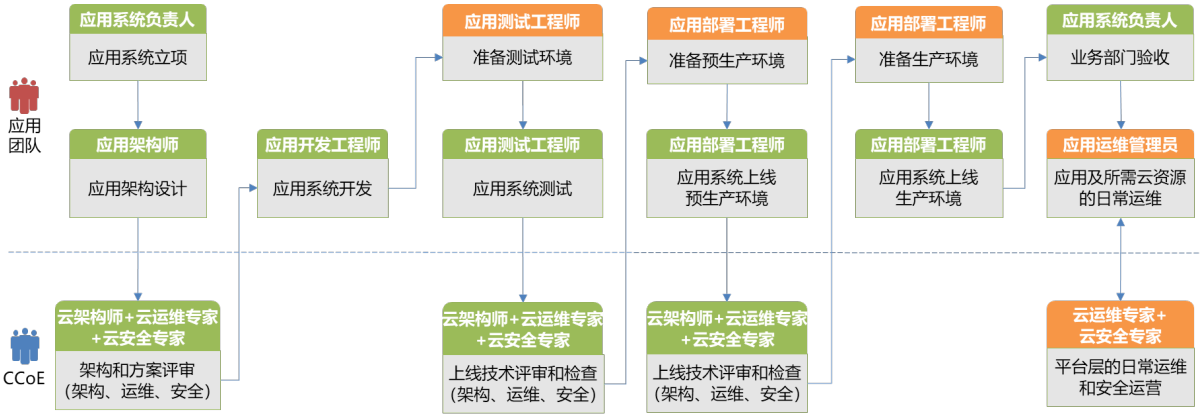
该模式下的应用生命周期管理流程与集中化运营模式基本相同，所有的环节都有，但某些环节的责任主体和工作范围发生了变化，下图中黄色标示的环节是有变化的环节。

在该模式下，CCoE团队赋能应用团队全权负责应用系统所需云资源的部署和运维，这样既可以减轻CCoE团队的负担，又可以提升应用团队的自主性，进一步提升应用系统的敏捷性。为避免各个应用团队独立部署和运维云资源带来的标准不统一问题，CCoE团队需要制定相应的IT标准并强制各个应用团队遵守。

CCoE团队和应用团队要紧密协同，共同保障业务系统在云上的安全稳定运行。在运维方面，CCoE团队负责云平台或云上IT基础设施的日常运维，应用团队负责应用及所需云资源的日常运维，业务系统出现故障后两边协同进行故障定位和修复。在安全运营方面，CCoE团队负责平台层面的安全防护和集中安全运营，各个应用团队需要负责应用系统及所需云资源的安全防护和安全运营，如防止SQL注入等。

与集中化运营模式相同，CCoE团队的云架构师、云运维专家和云安全专家需要在应用架构设计阶段深入参与应用设计方案的评审，在应用系统上线到预生产环境或生产环境前再对其进行上线技术评审和检查。

图 3-35 赋能和协同运营模式的 ALM



3.9 云项目管理

企业的云化转型对目标、范围、进度、成本和质量要有清晰的定义，需要作为一个标准的项目进行运作，然而，企业的云化转型是一项系统性工程，涉及组织、流程和技术的方方面面，它是一个持续时间长达数年的复杂项目，科学的项目管理方法和行动方案直接影响云化转型的效率和质量，最终将会影响云化目标的实现。

云化转型项目的管理通常涵盖可行性评估、项目准备、项目启动、项目过程管理、业务上线管理和业务保障。基于华为云项目管理和交付经验，通常会采用如下图的方法来管控整个企业云化转型的过程。接下来，本文将围绕该流程针对每一部分进行概要说明。

图 3-36 云化转型项目管理流程

可行性评估

一个企业在上云之初，企业决策层通常想了解上云最终能给企业带来什么价值，以及这些价值是否是企业当前以及未来业务发展所迫切需要的。为了解这些信息，通常决策层会让IT部门评估上云的价值和收益，而IT部门通常具备传统IT运营理念和IDC技术栈，缺乏对云深入的了解以及实践。这时，就需要引入云化转型专家协助信息化团队完成价值评估，这个阶段称之为可行性评估和蓝图规划阶段。在这个阶段，通常是由云化转型专家主导、IT部门辅助，共同完成当前业务、组织、运营、平台、安全、运维等多个维度的现状评估，根据评估结论和差距分析，估算云化转型能带来的价值和收益，并给出云化后整体蓝图规划设计。通过这一系列行动论证云化可以满足当前和未来业务发展的迫切需要，并让决策层看到云化后的业务连续性和业务敏捷性的提升以及业务创新能力的增强，加速决策层做出科学、合理的决策。

项目准备

决策层做出云化决策后，项目进入启动前的准备阶段。准备阶段主要目的是为项目启动提供完整的项目目标、项目范围、项目计划、项目管理机制、项目验收标准，并组建项目团队。为实现这一目的，需要在该阶段与客户确认云化工作的范围和边界，明确云化要实现的目标，并根据云化转型项目影响到的组织范围，构建联合项目团队，并提前和相关组织做好预沟通工作（如项目计划排程、责任分工、参与的阶段与角色，主要工作内容等）。项目计划需要在启动会前完成设计，并和业务部门等周边相关部门确认好时间计划、人员投入和资源就绪情况等。项目管理机制是项目顺利开展的关键环节，包含项目例会管理、项目风险管理、项目变更管理以及项目汇报机制，通过一系列机制保障项目在复杂场景下有序、平滑地开展。项目验收方案需要提前明确，基于项目目标以及业务诉求明确验收用例、验收指标、验收标准，确保业务系统上云后的功能和性能指标满足要求，这一步通常需要提前拉通业务部门和用户进行核心业务流程、关键指标的确认，并由业务部门负责最终输出业务验收指标。任何项目的执行都离不开人，所以准备阶段必须组建一个项目团队，也就是前面提到的CCoE团队，具体如何筹备和组建CCoE团队，请查看章节 **云卓越中心** 的内容。

在完成上述项目准备工作之后，需要举行正式的项目启动会。项目启动会的目的是将云化转型项目正式定义为一个真正意义上的工作任务，是一个有目标、有计划、有组织、有任命、有监督和考核的正式任务，确保项目成员按照责任界面和项目计划各司其职以达成项目目标。项目启动会参与者是CCoE的全体成员以及云服务商的项目团。

项目启动会中一个重要且关键的环节就是组织任命和授权。通过对项目团队的正式任命和授权将云化转型项目作为一个正式任务和KPI下发到每个组织成员头上。一方面确保组织成员的工作是正当、明确且可衡量的，同时也保证项目成员的稳定性，并激发团队成员完成目标的热情。

在项目启动会中，除了项目团队的任命和授权，还需要明确项目汇报监督机制。项目有个多个实施阶段，每个阶段的执行结果是否能达到预期？是否存在卡点和问题？项目团队是否具备处理这些问题的资源和能力？这些都是项目团队在执行过程中所面临的问题，如何快速高效处理问题，通常取决于对问题的理解和项目团队对资源的掌控能力，但仅仅依靠项目团队很难解决所有问题，因此，定期会议、高层汇报至关重要。通常在项目交付中，我们建议采用敏捷项目管理模式，即每日站会+周会的形式来快速识别阶段卡点和问题，快速找到应对机制来快速闭环，将问题解决周期尽可能缩短。站会和周会的机制可以让项目卡点快速通达决策层，依靠决策层的能力快速拉通资源来闭环问题，这就是上述我们提到的质量监督机制。通过这种机制，集合企业最高层的能力来确保项目成功，这也是项目高效、高质量交付结果的精髓所在。

除了组织任命和授权、汇报监督机制，项目启动会还需要定义项目日常运作管理机制（日报、周报、问题上升机制等）、风险变更机制（人员变更、周期变更、环境变更等）以及跨团队间的分工协作机制，这些通常可以参考常规的项目管理方法进行管理和运作。

项目过程管理

该阶段主要包含项目进度管理、汇报管理、风险管理、以及变更管理等部分。在前面我们已经提到进度管理、汇报管理的关键环节，如通过敏捷管理（站会、周会等）持续对齐目标和周期，确保项目进度在预期可控范围内；通过拉通高层周期性汇报机制快来监督项目进展和风险，以达到快速闭环问题和卡点的目的。云化转型项目实施和管理过程中风险通常包括项目周期风险、人员变更风险、技术可行性风险、操作风险、安全风险等。接下来主要针对风险管理（包括变更管理）以及敏捷管理方法做概要介绍。

项目进度风险通常是云化转型项目因各种超出预期的事件或问题导致项目周期延后，如新业务发布上线、关键业务数据库故障、病毒感染等事件，都会对项目实施周期带

来影响，因此项目团队应充分考虑可能遇到的问题或风险来制定项目周期。应对项目周期风险的策略通常是综合评估各个阶段可能存在的风险，并预留适度的项目周期，并针对某些极端风险制定逃生方案，尽可能确保项目在规定的时间内完成。

对于人员变更风险，是云化转型项目管理过程中经常碰到的风险场景，项目开始前必要的角色备份非常必要。针对某些单人单岗的关键角色，尤其需要考虑变更带来的风险，如一个公司一个DBA等情况，项目经理需要针对这一问题在项目开始前就要做备份计划，特定情况可以跨部门人员备份或提前进行人员储备，这一风险不仅仅云化转型项目管理中的问题，更是企业核心业务是否能可持续运营的风险问题。

技术风险的应对机制相对来说更为可控，项目团队通常可以采用POC验证的方式验证技术的可行性，这包括功能是否满足当前业务运行需求，以及非功能性部分是否可以满足业务运行的性能、延迟、吞吐量等指标等。同时针对迁移过程中的技术风险，项目团队可以通过迁移割接演练来模拟迁移实施过程，从中发现潜在的风险和问题，并形成Runbook来应对和规避相应风险。

云化转型项目实施过程中的操作风险与传统项目操作风险处理方式存在差异，原因在于传统IT项目实施基于硬件平台和系统实施操作，关键操作常常是多人共同参与，一个人操作，多人监督，确保操作和预期的一致。而云化转型项目的操作实施基于网络进行，业务和平台高度集成，一个操作失败可能影响多个组件或服务。因此，云上操作风险处理通常建议采用自动化的方式进行，尤其在业务系统割接上线的环节，尽可能减少人为带来的误操作风险。简而言之，能脚本化、自动化的就不手工操作，能工具化的就不用脚本操作，全面消除人为操作风险。

云化转型的项目管理对安全要求较高，如针对业务系统上云环节，要秉持“上云不带病、带病不上云”的基本原则，因此上云前项目团队通常要进行必要的问题巡检和安全扫描，这些工作涉及硬件、系统、中间件以及应用的状态、日志、事件、告警信息等部分，以及采用安全扫描工具进行系统的安全扫描，确保现有的系统运行是健康且没有潜在运行风险的。

相较于传统IT项目，云化转型项目虽然没有集成各个不同硬件厂商、不同ISV的复杂性和漫长的交付执行周期，但交付执行过程涉及面广、平台集成度高，问题处理过程复杂，致使云化转型项目的管理过程往往容易形成集中式卡点和风险，一个功能点不足都可能拖延整个项目周期。因此传统瀑布式项目管理模式往往无法适应云化转型项目的管理，敏捷项目管理模式则更有成效。

前面章节已经概要说明了项目问题处理的方法，如每日站会、每周例会等，实现项目卡点的快速审视、拉通和闭环，从根本上说这些方法和策略都是敏捷项目管理的一种形式。归根结底，敏捷项目管理模式也是一种逆向工作法思路，也即在项目开展过程的各个阶段，分别设定阶段交付的目标，通过在执行过程中不断审视当前进展、卡点或问题，并通过与阶段性目标对齐，寻求最快、最短的解决路径。作为一个云化转型的项目经理，应充分明确各个阶段的目标，在每个阶段执行过程中（如卡点、问题处理、风险应对举措等）持续与本阶段目标对齐，从实现目标的角度出发来解决当前问题，可以快速发现更加合适的方法和策略。

敏捷项目管理需要基于敏捷管理工具实现，将敏捷管理流程和工具结合形成快速闭环的过程管理能力。常用的敏捷管理工具包括Jira，也可以使用华为云提供的云原生项目管理工具**CodeArts Req**。CodeArts Req和华为云的云原生DevOps工具链CodeArts的其他工具无缝打通，可以有效提升端到端项目管理和应用交付的效率。

业务系统上线管理

业务系统上线管理的目的是保障业务系统上线过程中业务依然能够平稳运行，将对业务的影响和风险降低或消除。业务系统上线管理涵盖环境准备、组织宣贯、风险应急和割接上线实施等环节。

业务系统割接上线前云环境准备通常包含业务环境部署，数据同步（如迁移场景）、周边业务系统协同配置、内外部连通性确认等等，通过这些前提准备提前完成业务系统正常运行的基础平台环境的搭建，确保业务系统上线所需的基础环境处于就绪状态。

组织宣贯在割接上线前是一个关键环节，尤其是在传统企业初始上云的场景下。通过组织宣贯让所有项目成员和相关人员各司其职，通力配合完成业务系统上线工作（如上线影响说明、角色分工、配合实施内容、配合时间点、问题反馈机制等等），确保业务系统上线的每个流程、指标都可以得到验证并成功上线。另一方面，企业高层可以通过组织宣贯向公司内部传达一个关键信息：企业上云是公司未来的战略，每个组织、个人都应积极转换思想、意识，来积极主动拥抱云、拥抱企业数字化未来。

风险应急准备是每个业务系统上线前必要的环节，需要提前识别上线可能遇到的风险和问题并制定解决方案。风险识别不限于在技术实施过程中遇到的各类风险，还包括组织、流程、安全以及平台的系统性风险。如常年运行的系统可能存在硬件损坏无法修复的风险、业务系统运行环境潜藏破坏性病毒、业务系统上线环节上遗漏关键角色等等，每个风险都可能成给业务系统上线带来破坏性影响，提前识别、提前制定预案并进行必要环节的演练，尽可能将风险影响降低或消除。

割接上线实施是业务系统上线前最后一个环节，也是最关键的环节，但通常前期准备和风险应急工作充分、验证过程完善，割接过程基本都会比较顺利。在这个环节，主要做的工作就是按照前期演练完善的手册进行系统化验证，根据指标确定割接是否成功。一个关键的要点是本阶段是一个人员密集型工作阶段，组织宣贯阶段所有人员均需按照宣贯要求在不同的执行环节参与进来，并按标准要求执行相关动作和验证相关过程和结果，并为结果负责（通常需要签字验收指标通过）。基于所有反馈结果来最终判断割接是否成功。

业务保障

业务系统上线后，进入业务系统的上线保障期，上线保障期的工作内容涵盖保障期问题处理和闭环以及知识转移等事项。保障期通常是上线后一周，这个周期内通常是上云后问题高发期，是云化转型项目团队要重点关注和保障的阶段，通常云服务商会有专门保障团队和企业形成联合项目团队共同保障业务平稳运行。在这个阶段，基于业务部门提出的问题按照业务关键性等级和问题等级区分出轻重缓急，基于不同的紧急重要程度快速响应和闭环。知识转移则是在业务系统上线后，需要为业务部门的应用运维团队进行云技术的赋能，保证应用运维团队具备在云平台上对业务系统进行必要的日常运维管理和事件处理的能力。

3.10 顶层规划的反模式

在顶层规划阶段，一些常见的反模式可能会阻碍云化转型的成功。识别并避免这些反模式，对于确保云化转型取得成功至关重要。以下是几种常见的反模式，以及对应的优化建议。

CCoE 团队成员不够完善

CCoE是企业内部为云化转型专门成立的中心化团队，全程负责整个云化旅程，其目标是通过提供最佳实践、指导和资源，帮助企业最大化云计算的价值，确保云化转型项目的成功实施。CCoE就像云化转型的引擎，如果CCoE团队成员不够完善，就像引擎缺少关键零件，无法高效运转，甚至可能导致转型失败。这种反模式的具体例子如下：

- **缺乏云架构师:** 缺失专业的云架构师会导致云化转型如同无舵之舟。架构设计缺乏整体规划，系统扩展性差，难以维护，容易形成“拼凑式”的云环境，资源利用率低。技术选型不当则可能导致性能问题、成本超支和安全风险。此外，现有系

统与云平台的整合也将面临挑战，难以充分利用云原生特性。最终，企业将难以发挥云平台的优势，甚至面临安全和性能瓶颈。

- **应用团队参与不足:** 应用团队是云平台的最终用户，如果他们没有充分参与到CCoE的工作中，将会导致云平台与实际业务需求脱节。由于缺乏来自业务一线的实际输入，云化技术方案的设计可能无法满足业务场景，迁移过程也会因缺乏应用团队的配合而变得困难重重。更重要的是，应用团队的缺席会阻碍DevOps和自动化的推进，限制创新，最终导致云化转型无法带来预期的业务价值。
- **缺乏云治理专家：** 云治理专家如同云环境的“管家”，他们的缺失会导致云资源的使用缺乏管控，成本失控，安全风险增加。由于缺乏专业的治理策略和措施，企业难以满足合规性要求，面临法律风险。此外，缺乏有效的监控和管理机制，无法及时发现和解决问题，影响业务稳定性。

关于如何建立一个功能完整的CCoE团队，请参考章节 **云卓越中心** 。

没有搭建 Landing Zone 就开始启动迁移

Landing Zone是指在云平台上搭建的一套架构卓越、安全合规、易扩展的多账号运行环境，它包含了云骨干网络、IAM、合规审计、资源组织和治理策略等。未建立Landing Zone就开始进行业务系统的迁移，意味着企业在没有统一的云基础架构和治理框架的情况下，将应用和数据直接迁移到云上，好比没有打好地基就盖房子，是一种常见的反模式。它会导致一系列问题，最终延误项目进度，增加成本，甚至危及安全性。请在迁移任何业务系统之前就应该完成Landing Zone的规划和部署，关于如何规划Landing Zone，请参考章节**Landing Zone设计** 。

选择了不适合的云运营模式

在企业云化转型过程中，选择了不合适的云运营模式是一种常见的反模式。云运营模式直接影响企业在云环境中的资源管理、运营效率、安全合规和成本控制等方面。如果企业在未充分了解自身业务需求、组织结构、技术能力和战略目标的情况下，选择了不适合的云运营模式，可能会导致运营效率低下、安全合规风险加大、成本失控、管理复杂度增加等一系列问题，最终阻碍企业获取云化的业务价值。这种反模式的具体例子如下：

- **集中化运营模式用于快速变化的业务：** 如果企业业务需要快速响应市场变化，但采用了集中化运营模式，所有资源申请和变更都需要CCoE团队审批，就会导致流程缓慢，错失商机。
- **去中心化运营模式用于需要高度合规性的业务：** 如果企业的业务系统相对成熟稳定，对安全性和合规性要求很高（例如金融行业），但该企业采用了去中心化运营模式，各个部门各自为政，就难以保证整体的安全策略一致性，增加合规风险。
- **赋能和协同运营模式用于资源和预算有限的小型企业：** 赋能和协同运营模式需要投入较多的资源来构建和维护复杂的IT基础设施和IT治理策略，对于资源和预算有限的小型企业来说，可能过于复杂和昂贵。

4 调研评估

4.1 概述

上云调研不是一次完成的，而是持续整个上云过程，需要进行多次调研，持续迭代，每个阶段调研的信息都不同。本章主要介绍调研分析的思路和方法，在上云的每个阶段都可以参考此方法进行调研。如果上云工作不是企业自己主导，企业也可以基于此调研思路更好地配合第三方进行高效调研。但注意，同一阶段，能合并调研的要尽量合并调研，减少调研次数，尤其是访谈次数。

- **基础环境的调研：**是在云上架构设计之前进行的，包括整体IT技术架构以及IT治理现状和需求。
- **应用的调研：**持续整个上云过程，在评估规划阶段只需要调研业务全景图，而在迁移试点和大规模上云阶段，则需要打开到每个应用系统的详细技术架构，收集每个应用系统的技术组件的详细信息，如组件版本信息，组件相关配置参数等。
- **大数据调研：**先调研大数据的整体技术架构，然后逐步打开调研详细的信息。

每次的调研工作按照以下6步执行：

1. 根据上云阶段，确定调研目的，梳理需要调研的信息。
2. 对齐已有信息，避免重复调研。
3. 对准调研目标，识别还缺哪些信息，为什么要调研这些信息，以及这些信息的获取方式。
4. 基于企业组织架构和分工，判断能提供这些信息的干系人。
5. 制定调研访谈提纲和调研模板，制定沟通策略和计划。
6. 依照干系人认可的授权方式获得需要的信息，并进行信息的整理，完成调研。

图 4-1 调研方法

调研的总体思路是先易后难，先粗后细，持续迭代，具体含义如下：

- **先易后难（调研的方式）：**是指调研方法的难易，调研有多种方法，我们要优先选择简单快速的调研方式。
- **先粗后细（调研的内容）：**是指调研到的信息详细程度，评估规划阶段获取的信息比较粗，实施阶段获取的信息最为详细。
- **持续迭代（调研的过程）：**是指调研不是一次完成的，需要持续迭代，尤其在大规模迁移阶段，详细信息的调研可按迁移批次有序执行。

4.2 组建调研评估团队

在企业上云过程中，组建一支高效的调研评估团队是至关重要的。该团队将负责开展详尽的调研工作，评估企业现有的IT基础设施、业务需求和上云的收益，确保上云策略的有效性和可行性。调研评估团队由来自不同部门的成员组成，企业可以参考前述的CCoE组织架构和角色职责，组建出一个全面且专业的上云调研评估团队，以下为必要的团队成员。

- **调研评估工程师：**由IT主管指派，来自IT部门，对企业现有的IT基础设施、业务系统、应用架构、数据存储、安全策略等进行全面调研和评估，包括硬件配置、网络架构、软件版本、依赖关系等；分析这些设施与云服务的兼容性和迁移难度，评估将现有系统迁移到云平台的可行性。调研评估工作属于一次性工作，经常会外包给云服务商或者云实施专业服务提供商。
- **业务专家：**由业务主管指派，来自业务部门，收集和分析业务需求，与利益相关者访谈，了解不同部门的需求和期望，提供业务价值分析，为团队提供业务层面的指导和建议，帮助量化上云收益。
- **应用架构师：**由业务主管指派，来自业务部门应用团队，支撑云实施团队提供业务系统的现状进行调研，为调研评估团队提供资源现状、应用架构、部署架构、依赖关系等信息。

- **财务专家：**由财务主管指派，来自财务部门，对上云项目的成本进行核算和分析，包括云服务费用、迁移费用、运维费用等；评估上云项目的经济效益和ROI（投资回报率）。为上云决策提供财务支持和建议。
- **云安全专家：**由IT主管指派，来自IT部门安全团队，评估云服务的安全性、合规性以及数据保护能力，识别和应对潜在**的**安全风险，确保上云过程符合相关法律法规和行业标准。
- **项目经理：**来自项目管理办公室（PMO），管理调研项目进度，确保各项任务按时完成，协调各部门之间的沟通与协作，促进信息流通，及时解决项目中的问题。
- **云架构师：**来自IT部门或云厂商，作为云技术的专家，为团队提供上云技术支持和指导，包括上云方法论，调研的最佳实践等。

调研评估团队的组建又分为两种场景，对于企业主导上云的场景，调研工作由企业内部的这些角色主导，云厂商配合，提供必要的技术支持；对于企业购买第三方专业服务，由第三方主导上云的场景，上云调研工作由第三方厂商主导，企业内部团队配合，提供相关的业务和技术信息。

4.3 基础设施调研

基础环境调研的主要是企业当前的IT基础架构的现状和上云需求，包括资源信息、组网信息、安全架构、运维架构、访问权限管控、资源计量计费等。调研的方式主要是从IT系统导出（如CMDB、CMP、虚拟化管理软件），并结合问卷访谈。基础环境的调研主要是找企业的运维团队。调研人员会与企业的运维团队合作，收集与基础环境相关的数据和信息。

一种常见的调研方式是通过企业内部的IT系统导出信息，例如配置管理数据库（CMDB）、云管理平台（CMP）、虚拟化管理软件等。这些系统可以提供有关硬件设备、网络拓扑、操作系统、应用程序以及相关配置和版本的信息，帮助调研人员了解企业的IT基础架构。

此外，问卷调查和访谈也是常用的调研方法。调研人员可以设计问卷，收集关于资源使用情况、组网配置、安全架构、运维流程以及访问权限管控等方面的信息。他们还可以与运维团队进行面对面的访谈，深入了解企业的实际情况、挑战和需求。

在调研过程中，调研人员应与运维团队充分沟通，确保准确获取和理解企业的IT基础环境信息。他们需要考虑敏感性和机密性的问题，并遵循企业的安全和保密要求。

基于调研结果，企业可以更好地了解自身的IT基础架构现状和上云需求，有针对性地进行规划和决策。通过评估资源使用情况、组网配置、安全架构等方面的数据，企业可以制定合适的云迁移策略，优化资源配置，提高运维效率，并确保访问权限的管控和资源计量计费的准确性。

总而言之，基础环境调研是为了深入了解企业的IT基础架构现状和上云需求，通过与运维团队合作，结合从IT系统导出和问卷访谈等方式，收集相关数据和信息。这样的调研工作可以为企业未来的IT规划和迁移决策提供有价值的参考。

4.4 应用系统调研

4.4.1 调研应用全景图

应用迁移的调研信息是由粗到细、逐步迭代的，持续整个上云周期，在前期主要是调研应用的全景图，在迁移阶段，要打开每个应用，调研详细的部署架构和组件信息。应用的调研需要找各业务域的应用架构师和应用运维管理员。

应用全景图的调研是在评估规划阶段进行的，一般按照业务域->业务系统->应用模块逐层打开，如下图：

图 4-2 应用全景图示例

应用全景的调研方法由易到难分别是：

- **知识库：**有些企业的知识库做的比较好，有现成的文档记录应用的全景图信息，此种场景可以直接获取，但需要注意，知识库中的文档信息可能会比较旧，需要与业务负责人进行信息对齐和确认。
- **CMDB：**有些企业的CMDB系统有所有应用的信息，我们可以先从CMDB导出应用的信息，然后按照业务域和业务系统进行归类，并与业务负责人进行信息对齐和确认。
- **可观测平台：**有些企业有构建应用可观测平台，比如Datadog、华为云APM等，通过可观测平台可以发现应用间的调用关系，也可以用于输出应用全景图。
- **调研访谈：**与每个业务域的负责人进行访谈，并记录该业务域的系统和应用信息。每个业务域都调研完以后，再绘制全景图。

4.4.2 调研应用部署架构

应用部署架构的调研是在试点迁移或大规模迁移阶段进行的，应用部署架构是基于单个应用进行调研的，主要调研应用的四层部署架构，即接入层、应用层、中间件层和数据层，同时还要调研每一层技术组件的详细信息，比如规格、版本、容量等。具体的调研内容如下：

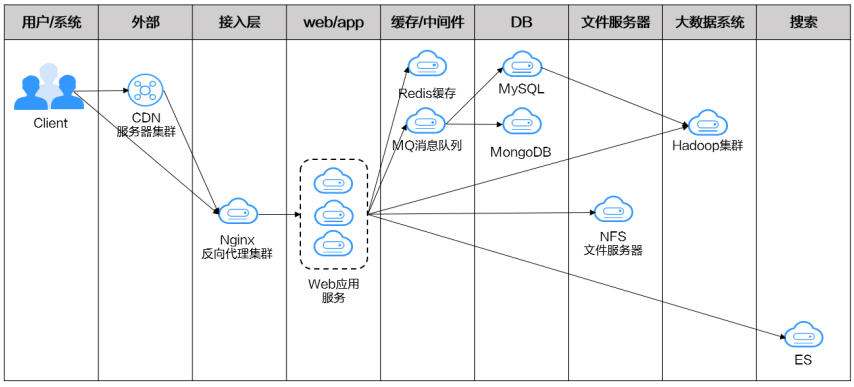
调研应用的四层部署架构

收集接入层、应用层、中间件层和数据层的详细信息，收集三种关联关系（共享数据、共享服务器、应用间通信依赖），可以参考下表收集应用的详细部署架构：

表 4-1 应用调研表

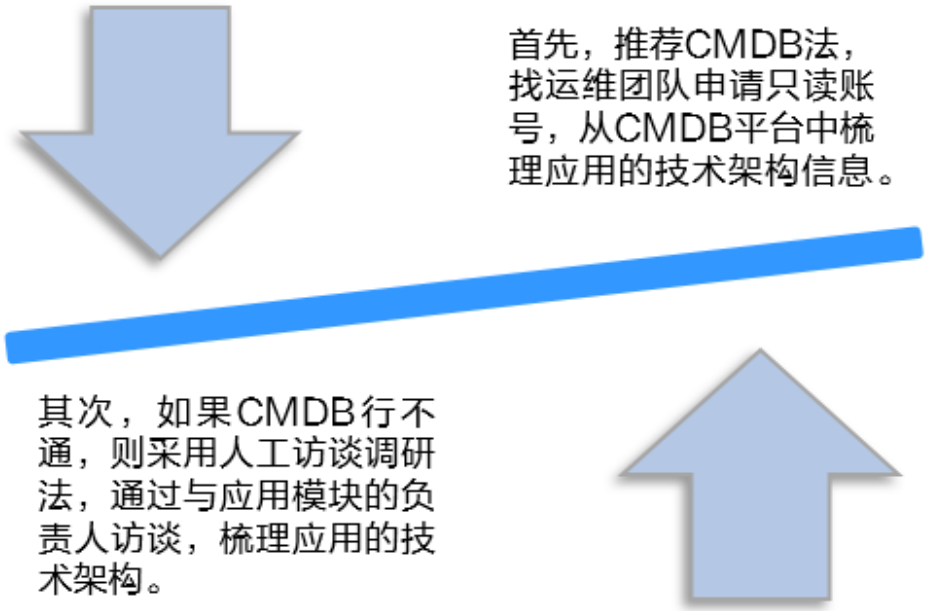
应用类型	接入层		应用层		中间件层			数据层		接入域名		备注
应用名称	NAT	NGINX	主机数量	IP地址	Redis	Kafka	MQ	MySQL	Mongo	内部/外部域名	WAF	备注

也可参考下图绘制应用的部署架构图：



调研方式如下图所示：

图 4-3 调研方式



调研技术组件的详细信息

调研单个应用的部署架构所涉及的各个技术组件（包括主机、数据库和中间件等）的详细信息，包括资源规格、版本、容量、配置等，如下表格所示。

表 4-2 主机信息调研表示例

主机名	主机类型(ECS/物理机)	规格	CPU（core）	内存（GB）	操作系统版本	系统盘类型	系统盘大小（G）	数据盘类型	数据盘大小（G）	私网IP	公网IP
此处仅给出表头信息作为参考。 表格具体内容请按业务实际情况进行补充。											

表 4-3 数据库信息调研表

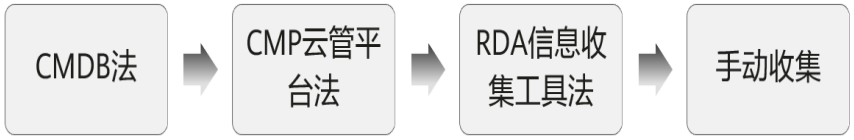
应用名称	区域	实例名称	架构类型	IP地址：端口	版本	实例规格	CPU	内存	存储类型	磁盘容量
此处仅给出表头信息作为参考。 表格具体内容请按业务实际情况进行补充。										

表 4-4 中间件信息调研表

应用名称	区域	名称	版本	连接地址	规格	Topic数量	Partition数量
此处仅给出表头信息作为参考。 表格具体内容请按业务实际情况进行补充。							

调研方式如下所示。

图 4-4 调研方式图



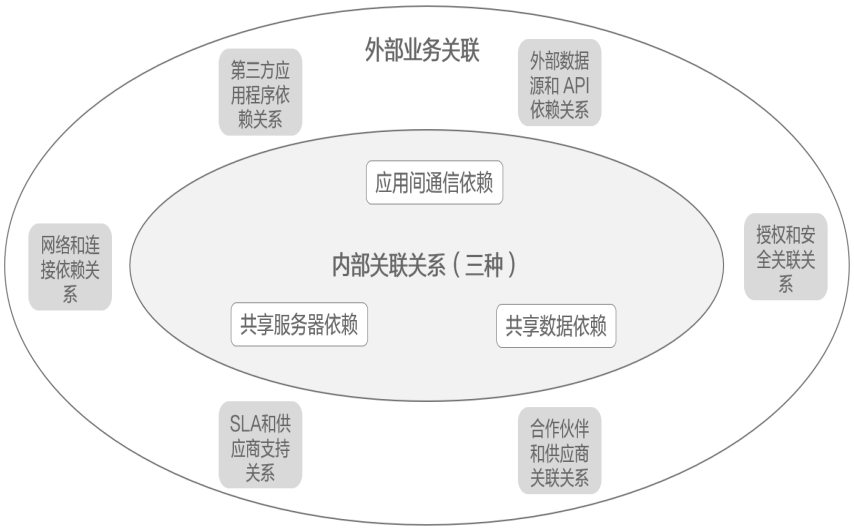
1. 首选CMDB法；
2. 如果CMDB无法获取，次选CMP云管平台法，从现网云管平台或虚拟化管理软件获取；

3. 如果CMDB和CMP都行不通，可以安装信息收集工具（比如华为云RDA）进行采集；
4. 如果以上方法都不可行，则采用人工访谈的方式调研信息。

4.4.3 调研应用关联关系

在应用迁移上云时，除了调研企业内部的业务关联关系，还需要考虑外部关联关系。内部关联关系主要用于迁移批次规划和制定切换方案，外部关联关系主要用于评估业务影响，选择合适的停机窗口和制定切换方案。

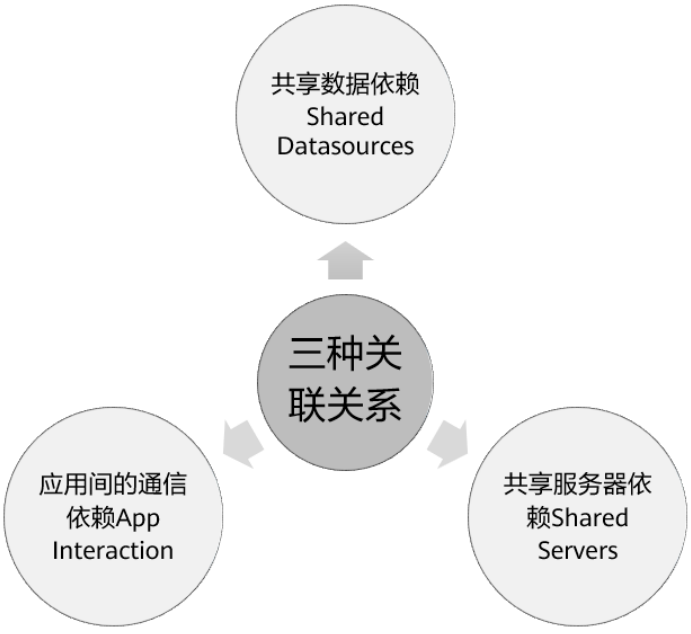
图 4-5 关联关系调研图



调研内部关联关系

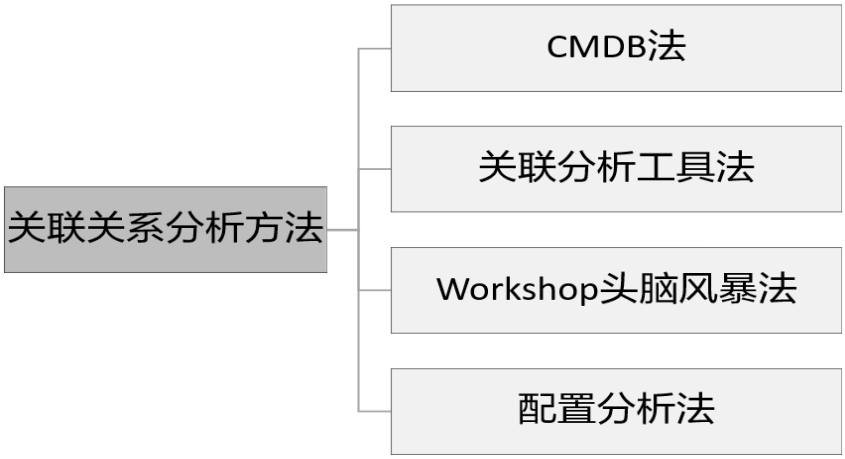
关联关系分析是批次规划和切换方案的重要输入，也是上云迁移的难点，影响上云迁移的关联关系主要有三种，如下图：

图 4-6 三种关联关系



关联分析有如下4种方法，上云迁移过程中，企业可以根据自身的实际情况选择合适的分析方法：

图 4-7 关联关系分析法



- **CMDB法**：适用于客户有CMDB系统，CMDB系统中通常有应用间的通信依赖，应用与数据库的依赖，应用与中间件的依赖等，可直接通过CMDB获取依赖关系。

图 4-8 CMDB 法

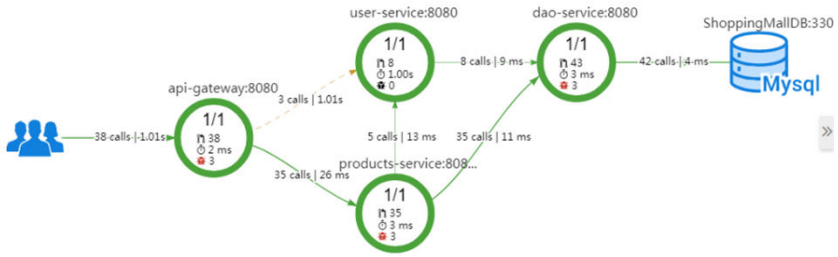
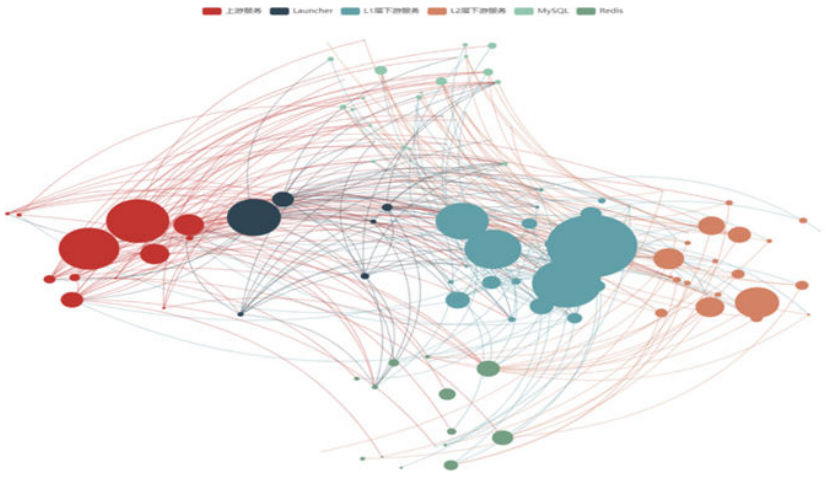


图 4-9 CMDB 法示例



- **关联分析工具法**：可以通过专门的关联分析工具进行关联分析，比如华为云的MgC工具，也可以采用业界的一些关联分析工具。

表 4-5 关联分析工具表

软件名称	是否商用	说明
Dynatrace	商用	Dynatrace平台包括出色的应用程序性能管理工具，能够提供自动的应用程序依赖关系映射。它可以发现和监控微服务和应用程序，甚至是那些在容器内运行的微服务和应用程序。它收集性能数据和通信时间数据，并突出显示性能不佳的服务和应用程序。
网络空间测绘	商用	网络空间测绘是一个应用和服务器发现工具。支持无代理自动发现，广泛支持MS和LINUX/Unix、云供应商、管理程序，硬件、虚拟和应用层；可用于多数据中心的远程收集。
Device42	商用	Device42是一个发现和映射工具，用于收集和组织整个IT环境上的数据。它包括设备发现和资产管理，以及专用的应用程序映射和管理功能。 它还可以检测网络设备，如交换机和负载均衡设备，以及电源和环境设备，包括PDU、UPS和CRAC设备。
艾联科iSRG动态智能系统	商用	艾联科iSRG动态智能系统资源图谱软件，提供传统网络/云/微服务/容器/虚拟系统的资源动态管理能力。包含资源的发现与采集，模板管理、资源管理、视图编辑等功能。
ManageEngine Applications Manager	商用	ManageEngine是一个应用程序管理器的工具。这是一个通用服务器和应用程序监控工具，它支持对服务器和数据库、虚拟机、应用程序、Web服务和其他组件的监控。
Datadog	商用	Datadog是一款具有应用程序监控和映射功能的性能监控工具。它可以在整个基础架构中收集信息，包括匹配特定客户、端点或错误代码的跟踪，它自动映射数据流，并可以按依赖关系组织服务。
Pinpoint	开源	Pinpoint可以跟踪分布式应用程序之间的事务，以检查整体结构和运行状况。Pinpoint可以实时监控应用程序，并清晰快速地了解应用程序拓扑。

- **Workshop头脑风暴法**：可以通过组织专题会议，引导熟悉业务系统的骨干人员梳理关联关系。

图 4-10 WorkShop 法

- **配置分析法**：配置分析法是一种通过分析应用系统的配置文件来探索关联关系的方法，它可以帮助我们了解应用之间的相互调用关系、应用与数据库之间的连接以及其它关联关系。以下是配置分析法的基本步骤：
  - **收集配置文件：**首先需要收集和获取与目标应用系统相关的配置文件。这可能包括DNS配置、ELB配置、NAT配置以及Nginx.conf等。
  - **解析配置文件：**对于每个配置文件，需要编写脚本或使用现有工具来解析其内容，脚本可以根据文件格式和语法规则，提取出关键信息并进行处理。
  - **提取关联信息：**在解析配置文件时，需要识别出与其他组件或资源相关的信息，例如，可以查找应用之间的相互调用关系，比如从一个应用到另一个应用的URL或API调用；还可以查找应用与数据库之间的连接信息，如数据库地址、用户名和密码等。
  - **构建关联图谱：**将提取到的关联信息组织成图谱或关系模型，这可以是有向图、无向图或其他合适的数据结构，用于表示应用间的关系和依赖。
  - **分析关联关系：**对于构建的关联图谱，可以使用图论算法或其他分析方法来探索关联关系，这可以帮助我们发现隐藏的依赖。

通过配置分析法，我们可以深入了解应用系统内部的关联关系，从而更好地理解整体架构和运行方式，这对系统迁移等方面具有重要的价值，然而，需要注意的是，配置文件可能会受到变更和更新的影响，因此在进行关联分析时需要及时更新和验证配置信息的准确性。

调研外部关联关系

以下一些常见的外部关联关系，需要在应用迁移前进行调研和评估。确保全面理解应用的外部依赖，并采取适当的措施，以确保迁移后外部业务正常运行，不受影响。

- **第三方应用程序依赖关系**

  调研与目标应用有关的第三方应用或服务，包括其版本和集成方式。确定是否需要对这些依赖项进行调整或重新配置。

- **外部数据源和 API 依赖关系**

  分析和记录目标应用所依赖的外部数据源和 API，例如外部数据库、文件系统、消息队列或第三方服务。确保这些依赖关系在迁移后能够正确访问和使用。

- **授权和安全关联关系**

  确定与目标应用有关的授权和安全关联关系。包括涉及身份验证、访问控制、令牌管理、IP白名单等方面的外部服务和机制。

- **合作伙伴和供应商关联关系**

  如果目标应用涉及与合作伙伴或供应商的集成，需要调研这些关系，并确保在迁移后能够继续正常工作。

- **SLA（Service Level Agreement）和供应商支持关系**

  检查既有的 SLA 和供应商支持协议，并评估迁移到云平台后对这些关系的影响。确保在云环境中依然能够满足业务需要并获得期望的支持和服务。

- **网络和连接依赖关系**

  调研目标应用所需的网络连接和传输协议。确定上云后是否需要进行网络配置和访问控制，以确保应用程序可以与相关的外部系统正常通信。

  外部关联关系主要靠如下方式去做调研，可以多种方式结合，以提高调研效率和结果完整度：

- **文档和现存资料**

  阅读现有的文档和技术资料，包括应用程序的架构图、部署说明和运维手册等。这些资料可以识别出应用程序的关键依赖和集成点。

- **与开发团队和运维团队沟通**

  与应用程序的开发团队和运维团队进行沟通，了解他们对系统依赖关系的认识和理解。他们可能提供有关应用程序的详细信息、依赖关系的描述以及与其他系统的集成情况。

- **代码分析**

  仔细检查应用程序的源代码，特别是配置文件和代码中涉及的外部依赖关系。因为有些依赖关系可能由代码直接指定。

- **系统扫描和监控**

  借助系统监控工具和网络扫描工具，扫描整个系统并识别出与应用程序相关的依赖关系。

- **与相关团队交流**

  与其他部门或团队进行交流，了解应用程序与其他公司、供应商或合作伙伴之间的集成关系。这些关系可能包括数据共享、接口调用、权限控制等。

- **服务提供商和文档**

  如果应用程序依赖于外部服务提供商，查阅其提供的文档、API 参考和支持资源，以获取关于依赖关系的详细信息。

4.4.4 调研应用上云需求

调研内容包括当前应用上云的需求和约束条件：

- 迁移时间窗
- 切换时间窗
- 目标架构的要求（功能、性能、可用性、安全、成本、可扩展性、可运维性）
- 回退要求

- 业务的关联关系确认。

调研方式包括人工访谈或Workshop头脑风暴，可以与前面2项调研内容合并调研，减少调研次数。

4.5 大数据调研

4.5.1 平台调研

大数据调研简介

大数据迁移是指将大数据集群、大数据任务调度平台和大数据应用从一个运行环境迁移到另一个运行环境的过程。

图 4-11 大数据调研的对象

大数据迁移需要调研4部分信息：

- 大数据平台调研，包括大数据集群、任务调度平台、数据流向。
- 数据调研，包括待迁移的数据类型、数据量、元数据、数据权限、数据更新频率等。
- 任务调研，包括待迁移的任务类型、任务数量、更新周期等。

本节重点介绍大数据平台、数据和任务的调研。

平台调研

大数据平台调研主要调研大数据集群、大数据任务调度平台和数据流向。

- **调研大数据集群**

  需要调研大数据集群的数量和功能划分，各个集群或组件负责的业务和处理的数据类型，处理实时/离线数据的组件及详细版本信息，数据格式类型和压缩算法，数据安全性和权限控制，高可用性和容错机制，扩展性和弹性等。

  调研大数据集群数量和功能划分：例如Hadoop集群、Spark集群、Hive集群等，并根据业务需求划分它们的功能，如存储集群、计算集群、查询集群等。

  调研各个集群或组件负责的业务范围，以及它们处理的数据类型和数据流转的方式。

  调研用于处理实时数据和离线数据的组件，例如实时数据可能使用Apache Kafka、Apache Flink等，离线数据可能使用Hadoop、Spark等。

调研数据格式类型和压缩算法：

调研平台对数据的安全性和权限控制机制，例如数据加密、用户访问权限管理等。

了解大数据集群的高可用性和容错机制，包括故障恢复、备份策略、容灾方案等。

- **调研大数据任务调度平台**

  需要调研大数据任务调度平台的类型、版本、支持的大数据框架和技术，调度任务类型，可视化和管理界面，扩展性和集成性，容错和故障恢复，安全性和权限控制以及社区支持和文档资料等方面的信息。用于后续大数据调度平台的选型和方案设计。

  调研现有的大数据任务调度平台的类型，例如Azkaban等，了解它们的特点和适用场景。

  调研现有大数据任务调度平台的版本，并了解最新版本的功能更新和改进。

  确认任务调度平台是否支持当前使用的大数据框架和技术，例如Hadoop、Spark、Hive、Pig、Flink等。

  调研任务调度平台支持的任务类型，包括Jar类任务、SQL类任务、脚本类任务（Python、Shell）等。

  调研任务调度平台是否提供可视化和管理界面，以方便任务调度的配置、监控和管理。

  了解任务调度平台的容错机制，包括任务失败后的重试机制、故障恢复策略等。

- **调研数据流：**

  调研大数据平台及业务的架构图及数据流图，如下图：

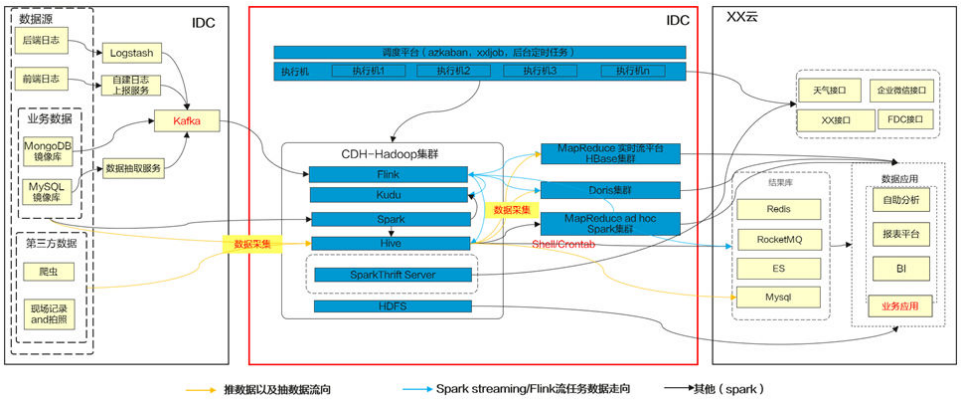
  大数据平台及业务的架构图和数据流图。

  平台数据接入源。

  数据流入方式（如：实时数据上报、批量数据抽取）。

  分析大数据平台数据流向，数据在平台内各个组件间的流向，例如：数据采集组件类型、采集组件下一层、存储数据组件，数据处理过程中的工作流等。

图 4-12 数据流示例



4.5.2 数据调研

数据调研主要包括如下方面：

表 4-6 数据调研方法表

调研内容	调研目的	举例
数据类型	根据数据类型选择合适的迁移工具	HDFS、HBase、MySQL等
数据量	历史数据量，用于评估历史数据迁移周期； 日增量数据，用于评估每日增量数据同步周期。	历史数据X PB 日增量Y TB
数据分层	调研数据分层主要用于迁移优先级和数据校验标准。	数据接入层、中间层、结果层
数据权限	根据源端数据权限控制组件的不同，选择不同的权限数据迁移方式	Sentry、Ranger等
数据重要性	调研数据重要性的目的是区分核心数据和非核心数据，用于迁移优先级和数据校验标准。	交易类是核心数据，日志类是非核心数据
数据更新频率	针对不同的刷新周期，制定数据的迁移计划和校验计划。	日刷新/周刷新/月刷新/实时更新
任务执行区间	让数据迁移、数据校验和业务高峰期错开。	离线任务上班前和下班后执行

调研的方法主要是通过当前大数据平台获取，并辅助一些调研访谈进行补充和确认。

4.5.3 任务调研

任务调研主要包括如下方面：

表 4-7 任务调研方法表

调研内容	描述
任务调度	如Azkaban、DolphinScheduler，Hera、Crontab等。
任务类型	基于编程语言分类： ● Jar类：常用于MRS、Flink、Spark等 ● SQL类： 常用于Hive、Spark、UDF等 ● Python类：常用于Spark、算法场景等 ● 其他类：如Shell、Scala等，多用于脚本调用
任务数量	调研各类任务的总数量，用于评估任务迁移周期及改造工作量。如：XX调度平台下，Jar任务XX个。
任务更新周期	识别出不同调度平台，不同任务类型的任务更新周期。如：XX调度平台XX类任务月度更新；XX平台XX类型任务每日XX点更新。

调研内容	描述
任务详细信息	识别出所有任务的详细信息，包括任务ID、名称、责任部门、责任人、执行时间、更新周期等。用于后续任务改造和迁移时，和关键人员及时沟通。
任务依赖关系	识别关键任务，识别任务间依赖关系。

调研的方法主要是通过当前大数据平台获取，并辅助一些调研访谈进行补充和确认。

4.6 调研方式

调研方法有很多，企业要结合自身的实际情况，从调研的效率、调研获取信息的完整度和真实度三个方面评估，选择最合适的调研方式。通常情况下，优先推荐CMDB调研法，CMDB中缺少的信息再通过云管平台或调研访谈的方式补齐。

如下是常见的调研方式，建议企业遵循由易到难的调研思路进行调研。有些服务商可能会提供大量的调研表格让企业反馈，这是低效的、易错的，若企业有类似CMDB等信息化系统，建议优先通过CMDB等信息化系统支持调研。为了安全起见，企业可以提供只读账号让调研人员自行登录CMDB获取信息或者企业直接导出相关信息给调研人员。

表 4-8 不同调研方式的适用场景

序号	调用方式	适用场景	优势	不足
1	现网CMDB平台	客户有CMDB平台，且包含应用调用模块	所见即可得，高效，可直接获取详细资源清单、数据层-数据层、数据层-应用层关联关系	1.有些传统的CMDB系统信息更新不及时
2	现网云管平台	客户有CMP或虚拟化管理平台	能够获取准确的资源详情	无法获取应用架构、关联关系等信息
3	现有文档	客户有比较完整的设备档案，包括设计文档，实施方案等。	可快速获取现网信息	文档的及时性和完整性无法保证
4	安装工具（RDA\第三方）	客户同意安装工具agent	可较快获取详细资源清单	1.需要客户现网环境安装agent，较敏感； 2.针对数据库、中间件等获取信息较少，且无法获取应用调用关系。

序号	调用方式	适用场景	优势	不足
5	调研访谈	客户人力和时间充足，且愿意配合	客户业务团队对资源清单及应用调用关系负责	1.调研周期不可控； 2.调研信息准确性及完整性不可控

不同的调研方式获取信息的效率、完整度和真实度是有区别的，总体来说，CMDB法是最高效的调研方式。

表 4-9 不同调研方式的综合对比

调研渠道	应用架构调研					技术架构调研					方法评估		
	业务全景	业务域	业务系统	应用系统模块	应用关联关系	技术架构（整体）	技术架构（按业务域打开）	技术架构（按业务系统打开）	技术架构（按应用系统模块打开）	技术架构（技术组件详情）	效率	完整度	真实度
现网CMDB	√ 需整理	√ 需整理	√	√	√	√ 需整理	√ 需整理	√ 需整理	√	√	高	高	中高或高
现网云管平台	-	-	-	-	-	-	-	-	-	√	高	低	高
现有知识库	√ 可能有	√ 可能有	√ 可能有	√ 可能有	√ 可能有	√ 可能有	√ 可能有	√ 可能有	√ 可能有	√ 可能有	高	低中高都有可能	低中高都有可能
RDA工具收集	-	-	-	-	-	-	-	-	-	√	中	低	高

调研&访谈	√	√	√	√	√	√	√	√	√	√	低	高	中高

4.7 云服务选型

4.7.1 计算服务选型

华为云提供的计算服务主要是ECS（Elastic Cloud Server）服务和CCE（Cloud Container Engine）服务，华为云提供了很多ECS的实例类型，如下表所示，以满足多样化的计算场景需求。关于上述ECS实例类型的详细信息，请查看**实例类型**。

表 4-10 ECS 实例类型

架构	实例类型	CPU	实例系列	系列说明	适用场景
x86	通用计算增强型	Intel	c	计算、存储、网络各方面性能均衡，CPU独享、性能稳定	适合大部分应用场景
		AMD	ac	与c系列相比，CPU不同、同规格分配的网络带宽更小，保持稳定性能的同时成本更低	
	高性能计算型	Intel	h	与c系列相比，CPU主频更高、计算性能高20%左右	HPC/游戏/科学计算
	内存优化型	Intel	m	与c系列相比，提供1:8的CPU/内存配比，内存性能更强	内存密集型，数据库/内存数据库
		AMD	am	与ac系列相比，提供1:8的CPU/内存配比，内存性能更强	
	超大内存型	Intel	e	与c系列相比，提供1:20的CPU/内存配比，内存性能更强	
	磁盘增强型	Intel	d	与c系列相比，提供大容量、低成本的SATA本地盘	大数据/缓存数据库
	超高I/O型	Intel	i	与c系列相比，提供高IOPS、低时延的大容量NVMe本地盘	
			ir	与c系列相比，提供高IOPS、低时延的小容量NVMe本地盘	
	通用计算型	Intel	s	与c系列相比，采用非绑定CPU共享调度模式，主机负载较轻时可提供基本与c系列一致的计算性能，成本更低、性价比更高，但无法保证实例计算性能的稳定，适合对性能抖动容忍度较高的场景	一般Web/开发环境/小型数据库

架构	实例类型	CPU	实例系列	系列说明	适用场景
	通用入门型	Intel	t	成本最低的实例，具备突发性能能力，突发时长受CPU积分影响，低价格	个人使用/维护终端等
	GPU加速型	Intel	g	搭载T4卡，图像加速	3D动画渲染、CAD
			p	搭载V100卡，计算加速	AI深度学习、科学计算
			pi	搭载T4卡，推理加速	实时推理+轻量级训练
	AI加速型	Intel	ai	搭载昇腾310芯片，计算加速或推理加速	深度学习、科学计算、CAE
ARM	鲲鹏通用计算增强型	鲲鹏	kc	与c系列相比，采用鲲鹏处理器，价格更低	已适配ARM的大部分应用场景
	鲲鹏内存优化型	鲲鹏	km	与m系列相比，采用鲲鹏处理器，价格更低	数据库/内存数据库
	鲲鹏超高I/O型	鲲鹏	ki	与i系列相比，采用鲲鹏处理器，价格更低	大数据/缓存数据库
	鲲鹏AI推理加速型	鲲鹏	kai	与ai系列相比，采用鲲鹏处理器，价格更低	深度学习、科学计算、CAE

以下是ECS服务的选型原则：

- **业务适用：**满足业务需求是选型的第一原则，除CPU、内存外，要特别重点关注带宽需求，通常同一系列的实例规格越大支持的带宽越大。
- **性价比：**在能够满足业务需求的情况下，需要考虑低成本的选型方案。例如：同规格情况下，s系列/ac系列价格低于c系列，运维终端等无强性能需求时选择t系列更划算。对于业务量波动较大的业务，建议通过多节点集群负荷分担+AS弹性伸缩配合，此场景不建议使用大规格实例节点，否则弹性缩容到最小节点数时会存在较多的性能浪费。
- **可靠性：**资源选型需要考虑如何降低故障率、避免单点故障，因此建议优先选择新系列（规格中代系数字更大的），且跨双可用区均衡部署。资源选型优化降本

不能以牺牲业务的可靠性为代价，集群组网中单个节点故障不应造成剩余节点超负荷。

- **一致性：**为保证基于镜像的快速扩容、快速恢复、弹性伸缩，承载同一类服务的主机，要求选型规格保持一致，无特殊需求的情况下同一业务系统中避免使用过多的实例类型/规格。
- **资源满足度：**考虑业务发展和扩容诉求，资源选型时一般建议选择主力型号，避免选择老旧、冷门的规格，且尽量选择在主力可用区（如北京四的可用区1和7、上海一的可用区1和4）。

除AI等特殊场景需要使用BMS外，通用算力一般使用ECS即可，几个典型场景的选型建议如下：

表 4-11 典型场景的 ECS 服务选型

位置	典型应用		选型建议
接入层	负载均衡/应用代理	Nginx	c/m系列
	运维终端	跳板机	t系列
应用层	普通应用	Web服务	ac/am系列
	高性能计算服务	转码服务	c/m系列
中间件层	自建中间件	自建Redis/RocketMQ	c/m系列
数据层	自建数据库	自建MySQL/Oracle	c/m系列

4.7.2 存储服务选型

华为云提供的存储服务主要是OBS（Object Storage Service，对象存储服务）、EVS（Elastic Volume Service，弹性云硬盘）、SFS（Scalable File Service，弹性文件服务）等，这三类存储服务的对比表如下所示。

表 4-12 三类存储服务的对比

对比维度	EVS	SFS	OBS
特点	高可靠、高IOPS、弹性扩展（等同于硬盘）	高带宽、按需扩展、共享访问（等同于NAS）	高可靠、低成本、海量可扩展性、支持任意类型和大小的对象
使用场景	高性能计算、企业核心集群应用、企业应用系统和开发测试等	高性能计算、媒体处理、文件共享和内容管理和Web服务等	大数据分析、静态网站托管、在线视频点播、基因测序和智能视频监控等
存储逻辑	存放的是二进制数据，无法直接存放文件，如果需存放要先格式化文件系统	存放的是文件，会以文件和文件夹的层次结构来整理和呈现	存放的是对象，可以直接存放文件，文件会自动产生对应的系统元数据，用户也可以自定义文件的元数据

对比维度	EVS	SFS	OBS
访问方式	只能在ECS/BMS中挂载使用，不能被操作系统应用直接访问，需要格式化成文件系统（OS层，不涉及应用改造）	在ECS/BMS/CCE中通过网络协议挂载使用，支持NFS/CIFS（通用文件系统不支持CIFS），需要指定网络地址访问，也可以将网络地址映射为本地目录后访问（OS层，不涉及应用改造）	可以通过互联网或专线指定桶地址使用HTTP或HTTPS访问（应用层，需要应用集成SDK或调用API接口，涉及应用改造）
数据共享	支持，需通过ECS/BMS中安装的集群管理软件控制，不能跨可用区共享	支持，直接NFS V3协议访问即可（SFS Turbo还支持CIFS），支持跨可用区共享	支持，直接HTTP/HTTPS访问即可，可无限制共享
远程访问	不支持	支持	支持
单独使用	不支持	支持	支持
容量	TiB级	PiB级（SFS Trubo）/EiB级（通用文件系统）	EiB级
时延	最小	中	最大
吞吐带宽	MiB/s级	GiB/s级	TiB/s级
数据冗余	单可用区	单可用区（SFS Turbo）/单或多可用区（通用文件系统）	单可用区/多可用区
数据可靠性	9个9	10个9	单AZ：11个9；多AZ：12个9
存储计费方式	按容量计费	SFS Turbo按容量计费/SFS通用文件系统按使用量计费	按使用量计费

以下是存储服务的选型原则：

业务适用原则

首先要根据业务场景选择适用的存储类型，重点考虑如下几个方面：

1. **可用的访问方式：**EVS盘或SFS文件系统挂载到主机后，体现为操作系统中的一个文件系统路径，上层应用可以直接访问，而OBS需要业务应用调用专用的SDK或API接口访问，需要了解业务可接受的访问方式。对于数据库类需要直接裸盘映射的应用，只能使用块存储（EVS）。

2. **是否需要共享：**EVS支持共享操作，需要在购买时勾选共享特性，并通过专用集群软件管理共享磁盘。而SFS和OBS天然支持共享，因此需要结合业务场景分析要存储的内容是否有多节点共享的诉求。
3. **存储容量：**不同的存储类型可以支持的容量不同，需要基于当前业务量和未来发展预估所需的容量级别，以便选择合适的存储类型：

表 4-13 存储服务的最小和最大容量

存储类型		最小容量	最大容量
EVS		10GB	32TB
SFS Turbo	20MB/s/TiB	3.6TB	1PB
	其他	1.2TB	1PB
SFS通用容量型		0	无限制
OBS		0	无限制

性能匹配

存储服务的性能指标包括传输带宽、IOPS和时延等，如下表所示，您需要根据业务系统的性能要求和特点选择最合适的存储服务及对应的规格。

另外，EVS和OBS对所存储对象的大小无限制，SFS通用容量型不适合1MB以下的海量小文件应用，SFS Turbo和后续的SFS通用性能型可支撑海量小文件应用。

表 4-14 存储服务的性能指标

存储类型		带宽上限（GB/s）	IOPS上限	平均时延级别
EVS	高IO-SAS	0.15	5K	1~3ms
	通用型SSD-GPSSD	0.25	20K	1ms
	超高IO-SSD	0.35	50K	1ms
	通用型SSD V2-GPSSD2	1	128K	1ms
	极速型SSD-ESSD	1	128K	亚毫秒级
	极速型SSD V2-ESSD2	4	256K	亚毫秒级
SFS Turbo	20MB/s/TiB	20	250K	2~5ms
	40MB/s/TiB	20	250K	2~5ms
	125MB/s/TiB	100	百万级	1~3ms
	250MB/s/TiB	100	百万级	1~3ms
	500MB/s/TiB	200	百万级	1~3ms
	1000MB/s/TiB	200	百万级	1~3ms

SFS通用型	容量型	50	100K	7ms
	性能型	200	2000K	5ms
OBS		TB级	千万级	10ms+

成本优化

存储类型的选择还需考虑成本因素，在满足业务性能要求的情况下降低存储成本。

1. 满足业务性能要求的情况下，优先选择存储单价低的存储服务。
2. 按规格计费的存储（EVS及SFS Turbo）做好业务增量预测和容量监控告警，建议预留15%~20%作为扩容阈值即可，避免初始购买的容量规格过大造成资源浪费。
3. 按量计费的存储（SFS通用型及OBS）做好使用量规划，适当购买资源包抵扣使用量，可以进一步降低成本。
4. 支持生命周期管理的存储（SFS通用型及OBS）做好生命周期策略规则，及时将冷数据转入低频存储，可以进一步降低成本。
5. 对于存储容量需求较大、数据保存周期较长的业务，通过业务应用层的改造，根据不同类型存储的特点组合使用（例如组合EVS/SFS Turbo和OBS），可以在保证业务性能要求的情况下优化成本。

可靠性保障

EVS、SFS Turbo、SFS通用型、OBS均是三副本存储，数据持久性可满足业务的要求，但可靠性方面存在一定的差异：

- EVS、SFS Turbo的三副本均在同一个可用区，若可用区出口或机房出现故障时，会导致业务不可用。
- SFS通用型、OBS支持单可用区或多可用区（当前SFS通用型还只有单可用区可选，后续逐步上线多可用区产品），对连续性要求高的业务，可选择多可用区的实例。
- EVS支持通过镜像、快照、云备份功能进行数据的快速备份和恢复，SFS Turbo支持通过云备份功能进行备份和恢复，SFS通用型、OBS一般用于超大容量业务场景、暂未规划备份能力。

基于以上选型原则，以下是一些典型场景的选型建议：

- 除非自建数据库双机/集群等场景，否则通常不建议使用共享盘，而是改用SFS服务来实现多主机的文件共享（共享盘不支持跨AZ被挂载到多个ECS，而SFS支持）。
- 对于需要频繁读写大量日志、且需要对日志做汇总分析的应用，建议优选SFS作为多节点共享的日志统一存储（具体类型根据性能需要选择）。
- 异步交互/对时延不敏感的业务，优选OBS存储，节省成本；若业务难以适配改造，则可以考虑SFS通用容量型替代。
- AI场景综合考虑性能和成本，通常建议组合SFS Turbo+OBS使用。

4.7.3 网络服务选型

华为云提供的网络服务有虚拟私有云VPC、企业路由器ER、企业交换机ESW、云专线DC、虚拟专用网络VPN、全球加速GA、弹性负载均衡ELB、NAT网关、弹性公网IP等。以下是这些网络服务的选型建议：

- 云内同区域少量VPC互通用对等连接，跨区域VPC互通用云连接CC，云上云下互通用云专线DC或VPN，需要简化VPC之间、云上云下之间的互通连接和路由管理用企业路由器ER。
- 云上云下子网网段重叠、IP分开，需要二层互连打通用企业交换机ESW
- 云上云下子网网段重叠或因管理原因不允许直接打通两端子网段的路由，但业务需要互访，用私网NAT网关。
- 需要在云上自建高可用双机系统，建议两台ECS位于同一子网、跨可用区部署，绑定虚拟IP结合keep-alive实现。
- 跨境业务需要提升指定区域用户范围跨境资源的体验时，选择云连接CC搭配全球加速GA，使流量通过华为云骨干网实现降低时延的效果。
- 低并发、大流量基础四/七层负载分发场景建议选择共享型ELB并开启性能保障模式（支持5万并发），购买两个实例、通过域名解析分流可获得更大的并发支持。
- 超过10万并发、要求全链路HTTPS或高级转发策略支持的场景，建议选择独享型ELB。
- ECS需要访问公网时，不建议直接绑定EIP，建议增加公网NAT网关统一走SNAT，便于更灵活的管控。
- 需要面向公网提供服务时，不建议将公网IP直接绑定到ECS，而是建议绑定到ELB或NAT网关，以便灵活扩展和管控调整。
- 无特殊情况，EIP的链路类型建议使用缺省的“全动态BGP”。

4.8 调研评估的反模式

在进行上云调研评估时，可能会遇到一些反模式，这些模式如果不加以识别和避免，可能会影响调研评估的效率，也可能会导致调研评估结果不准确，无法支撑有效决策和后续的上云方案设计。以下是一些在上云调研评估中常见的反模式。

- **没有选择正确的调研方法**

  调研开始阶段，直接发各种复杂的调研表格给企业，进行信息收集，容易造成信息提供方抵触，从而影响调研的效率和结果的完整性及准确性。

  优化建议：应采用科学的调研方法，遵循先易后难、先粗后细、持续迭代的调研思路，比如，先从CMDB收集信息，并结合现有的文档资料，梳理出需要调研的Gap信息，然后再精简调研表格，去做高效的调研和补充。

- **业务调研不足**

  仅关注技术层面的调研评估，而忽略了业务需求和用户场景。

  优化建议：深入业务调研，分析用户场景，确保上云能够满足业务需求，提升用户体验。

- **评估不全面**

  仅关注某个单一指标（如成本、性能等），而忽略了其他同样重要的因素。

  优化建议：建立全面的评估指标体系，综合考虑成本、性能、安全性、可扩展性、可运维性等多个方面。

- **低估迁移复杂性**

  认为上云只是一个简单的技术迁移，而忽视了应用程序架构、数据依赖关系及其对业务流程的影响，导致迁移后出现各种问题。

  优化建议：要充分进行内、外部各种关联关系分析，识别强弱关联，并评估风险和影响，作为后续批次规划和切换方案的输入，将问题和影响降到最低。

通过识别并避免这些反模式，可以更加高效准确地进行上云调研评估，为企业的上云决策和方案设计提供有力支持。

5 方案设计

5.1 概述

云上架构设计包括基础环境设计、应用部署架构设计、大数据架构设计三部分，如下图所示：

图 5-1 云上架构设计总图

1. **基础环境设计：**企业上云首先要准备好基础环境，基础环境构建好以后，上云工作才能正式开始。基础环境在业界也叫做LandingZone（着陆区），基础环境设计包括6个方面，即账号和权限设计、整体网络设计、整体安全设计、资源治理设计、运维监控设计、财务管理设计。
2. **应用部署架构设计：**应用部署架构是应用在云上的技术架构，应用部署架构要从接入层、应用层、中间件层和数据层来设计，包括每一层的云服务技术选型，同时还要考虑架构设计的6要素（即：可用性、性能、可扩展性、安全、成本、可运维性），其中重点考虑可用性、可扩展性和性能，安全、成本和可运维性遵循基础环境的设计进行适配即可。
3. **大数据架构设计：**大数据的部署架构设计包括大数据集群部署架构设计、大数据任务调度平台部署架构设计和大数据应用部署架构设计，其中大数据应用的部署

架构可以参考应用部署架构的设计方法。大数据架构设计同样要考虑架构设计的6要素。

在做云上架构设计时，企业可以参考TOGAF的架构设计方法论，可以关注其架构开发方法（ADM）、四个架构设计领域、最佳实践和工具，有助于设计出更加高效、灵活和可扩展的上云架构。

5.2 组建方案设计团队

在企业推进上云方案设计的过程中，构建一个高效且专业的方案设计团队是确保项目成功的关键。该团队将负责设计全面的上云方案，涵盖上云技术架构、业务架构优化、成本效益分析、安全合规等多个维度，以保障上云方案的可行性。企业可以参考前述的CCoE组织架构和角色职责，组建出一个全面且专业的上云方案设计团队，以下为必要的团队成员。

1. **云架构师：**来自IT架构部门或具备深厚云技术背景的专家，负责设计云上技术架构，包括选择合适的云服务（IaaS、PaaS、SaaS），基于四架构六要素设计云上目标架构，确保技术选型合理、资源配置最优，并为各项技术决策提供咨询。
2. **数据架构师：**由IT主管指派，来自IT部门的大数据团队，负责设计企业在云上的数据架构，包括数据存储、数据处理、数据集成和数据治理。
3. **应用架构师：**由业务主管指派，来自业务部门的应用团队，负责设计和管理业务系统在云上的应用架构，包括应用的架构模式、技术选型、部署方式等，确保应用的性能、可扩展性、安全性和可靠性。
4. **业务专家：**由业务主管指派，来自业务部门，深入了解当前业务流程，确保方案设计能满足实际业务需求，推动业务价值的实现，提升运营效率和用户体验。
5. **财务专家：**由财务主管指派，来自财务部门或具备财务分析能力的专业人士，负责全面评估上云方案的成本结构，包括初期投资、运营成本、潜在节省及长期收益预测。通过量化分析，为决策提供成本效益比、ROI（投资回报率）等关键财务指标。
6. **云安全专家：**来自信息安全部门或具有安全合规认证的专业人士，负责评估云服务商的安全合规性，设计数据保护策略，确保上云方案符合行业安全标准、法律法规要求，有效防范安全风险。
7. **项目经理：**来自项目管理办公室（PMO）或具备丰富项目管理经验的个人，负责整个上云方案设计项目的规划、执行、监控和收尾工作。确保项目按时、按质、按预算完成，协调跨部门资源，促进团队协作与沟通。
8. **云服务商顾问：**来自选定的云服务商或专业服务公司，提供基于最佳实践的上云方案建议，协助企业量身定制上云方案，包括技术实施细节、最佳实践分享等。

方案设计团队的组建模式同样分为两种场景，在企业自主主导上云方案设计的场景下，上述角色主要由企业内部人员担任，云服务商提供咨询和技术支持；若企业选择购买第三方专业服务进行上云方案设计，则由第三方团队主导，企业提供必要的业务需求和技术信息，企业团队需与第三方紧密合作，确保方案设计符合企业的业务需求，双方紧密合作，共同推进方案设计。

5.3 基础环境设计

企业在云上的基础环境主要就是Landing Zone，企业在将任何业务系统云化之前，都需要提前规划和设计一个架构卓越、稳定可靠、易扩展和安全合规的云上运行环境。

具体内容请参考章节 **Landing Zone设计**。

企业需要针对云环境的安全防护设计全面的安全防护方案，请参考章节**安全架构设计**。

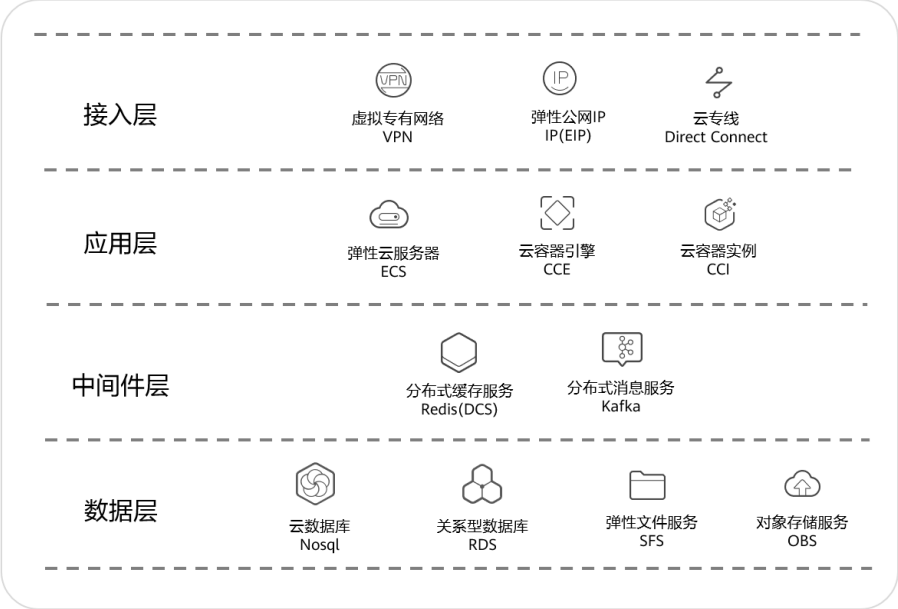
5.4 应用架构设计

5.4.1 应用部署架构概述

应用部署架构设计的方法论来源于华为云架构师在各个领域的实战经验，基于这些实战案例，我们总结了一套方法论来指导企业进行云上应用部署架构的设计，帮助企业上好云、用好云。

应用部署架构按照各个组件的功能，一般可以抽象出四个层级：接入层、应用层、中间件层、数据层。

图 5-2 应用的四层部署架构设计



- **接入层：**为外部访问提供了访问入口，云上业务部署在VPC私有网络中，与外部网络是隔离的，当外部需要访问VPC业务时，通常可以通过如下两种方式：
  - **专线：**云专线是搭建用户本地数据中心/其他云厂商与云上虚拟私有云（Virtual Private Cloud，VPC）之间高速、低时延、稳定安全的专属连接通道。可以让用户通过内网地址访问云上弹性云服务器、负载均衡等资源，也可以使云上云下进行业务互通、数据传输等。
  - **EIP：**即弹性公网IP（Elastic IP），包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑，提供访问公网和被公网访问能力。
  - **VPN：**虚拟专用网络（Virtual Private Network）用于搭建用户本地数据中心与华为云VPC之间便捷、灵活，即开即用的IPsec加密连接通道，实现灵活一体，可伸缩的混合云计算环境。
- **应用层：**负责工作流控制，实现业务逻辑。上承接入层，处理接入层的请求，返回请求结果；下接中间件层或数据层，实现对数据的增删查改。在云上，应用承载的资源主要有：

  - **虚拟机：**在云上，虚拟机又叫做弹性云服务器（Elastic Cloud Server，ECS），是由CPU、内存、操作系统、云硬盘组成的基础的计算组件。弹性云服务器创建成功后，可以像使用自己的本地PC或物理服务器一样，在云上使用弹性云服务器。
  - **容器：**容器虚拟化技术已经成为广泛认可的容器技术服务器资源共享方式，容器技术可以在按需构建容器技术操作系统实例的过程当中为系统管理员提供极大的灵活性。
- **中间件层：**负责应用软件在不同的技术之间共享资源，管理计算资源和网络通信，主要解决分布式环境下的数据传输，数据访问，应用调度，流程管理等。在云上，常用的业务中间件有：
  - **缓存：**华为云提供的缓存中间件主要为分布式缓存服务（Distributed Cache Service，简称DCS），包含Redis、Memcached等。
  - **消息中间件：**华为云提供的分布式消息中间件主要包含：Kafka、RabbitMQ、RocketMQ等。
- **数据层：**负责系统业务数据的持久化，为上层业务逻辑的实现提供数据支持，一般是各类数据库、文件系统等。

应用部署架构设计的目的是保证企业应用的性能体验、可用性和安全性，同时还要兼顾可扩展性、成本和可运维性，因此设计应用部署架构需要考虑6个要素，包括可用性、可扩展性、性能、安全、成本和可运维性，原因如下：

- **可用性：**可用性设计的目的是确保应用系统在云上的可用性和可靠性，保证系统在面临各种异常情况下仍能保持稳定运行，保障业务连续性。
- **可扩展性：**可扩展性设计的目的是确保应用程序能够在不同的负载下保持可用性和性能，能够基于负载进行扩展以满足这些需求，而不会导致系统崩溃或者性能下降，保障用户体验。
- **性能：**性能设计的目的是为了确保应用在云上的部署架构能够满足用户的性能需求，包括响应时间、吞吐量、并发数等。
- **安全性：**安全性设计的目的是确保应用程序和数据在云环境中得到充分的保护，防止恶意攻击和数据泄露等安全问题发生。
- **成本：**成本设计的目的是为了在保证应用性能、可用性、安全性的前提下，尽可能地降低部署和运维的成本。
- **可运维性：**可运维性设计的目的是提高系统的可维护性（包括自动化部署、监控告警、日志分析、容量规划、故障排查等），保障系统在运行时的状态可视化，故障时的快速恢复。

其中安全性、成本和可运维性这三个设计要素是全局的，在基础环境中进行统一设计，应用部署架构设计时可以直接适配使用。因此，应用部署架构设计需要重点关注的是可用性、可扩展性和性能这三个要素，下面重点介绍这三个要素的设计：

5.4.2 可用性设计

5.4.2.1 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：

表 5-1 SLA 级别表

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

5.4.2.2 AZ 故障域说明

AZ (Availability Zone) 是公有云的一个独立的故障域，一个AZ是由物理上互相隔离的数据中心组成，每个AZ都具有独立的电力供应、网络连接和硬件设施，公有云厂商通常会将不同的AZ部署在不同的地理位置，以提高系统的可用性和故障容错能力，AZ故障域的优点包括：

- 高可用性：将应用程序和数据部署在多个AZ上，确保即使一个AZ发生故障，其他AZ仍可提供服务，保证应用程序持续可用。
- 故障容错：在一个AZ发生故障时，可以快速地将应用程序和数据切换到其它正常的AZ上，以确保服务不中断。
- 地理冗余：将不同的AZ部署在不同的地理位置，可以防止地区范围的故障，例如自然灾害或电力中断对整个系统的影响。

企业可以基于AZ故障域进行应用的高可用性署设计，设计时可以考虑如下方面：

- 跨AZ部署：将应用程序的不同组件部署在多个AZ中，以确保即使一个AZ不可用，其他AZ中部署的组件仍能正常运行，企业可以使用云服务提供商的工具或容器编排工具来简化多AZ部署的管理。
- 负载均衡：使用负载均衡将流量分发到不同AZ中的应用程序实例，可以设置合适的转发策略，避免单个AZ过载，以确保即使一个AZ受到高负载或故障影响，其他AZ也能接受并处理流量。
- 数据冗余和备份：在不同的AZ中实施数据冗余和备份策略，确保数据的可用性和可恢复性，即使一个AZ的数据丢失或不可用，仍能从其他AZ中的冗余数据进行恢复，确保数据的可用性和完整性。
- 自动故障恢复：设置自动化故障转移机制，在一个AZ发生故障时，自动将应用程序切换到其他可用的AZ上，以快速恢复服务，企业可以利用容器编排工具、自动化脚本或云服务提供商提供的故障转移功能来实现自动故障恢复。
- 监控和警报：设置监控和报警机制，实时监测每个AZ中的应用程序和基础设施的健康状态，在发生故障时，及时触发告警，并通知有关人员进行故障排查和处理，以减少服务中断时间。

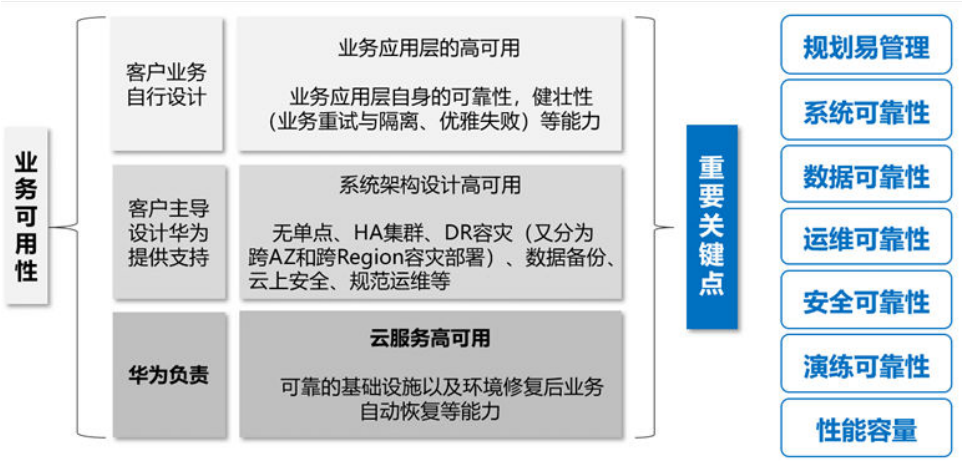
通过基于AZ故障域的高可用部署设计，企业可以提高业务系统的可用性和故障容错能力，最大限度地减少服务中断和数据丢失的风险，并确保业务的连续性。

5.4.2.3 云上高可用方案

公有云上业务的可用性，由应用层的可用性，架构设计的可用性、云服务的可用性共同决定。业务可用性目标的达成是一项系统工程，公有云模式下，业务的可靠性取决

于客户对整体业务架构的可用性设计、运维规范管理（如：备份机制、日常演练、人员操作规范等）。

图 5-3 业务可用性方案



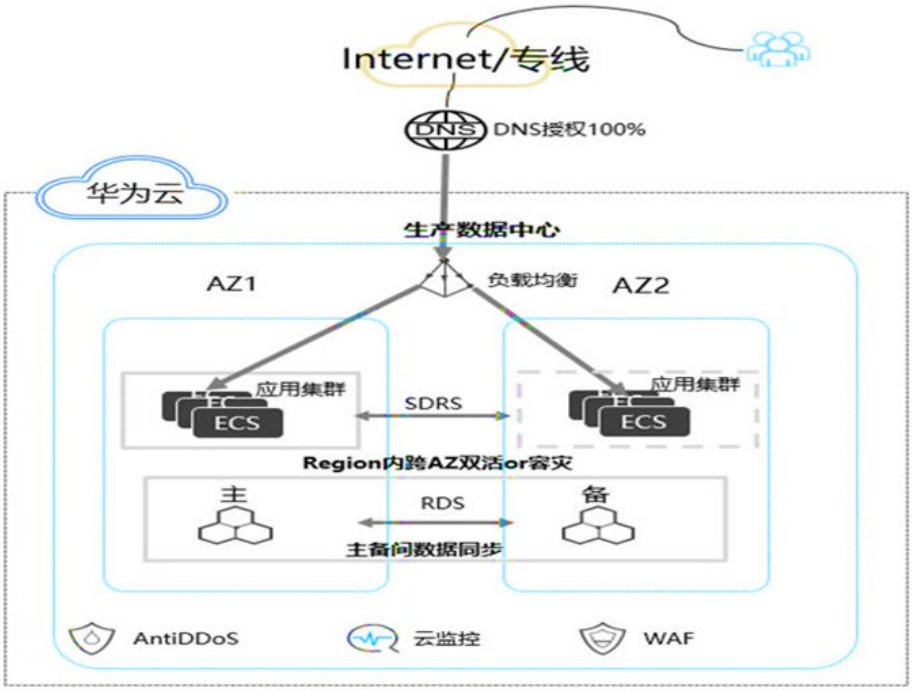
华为云上的绝大部分云服务都具备高可用性的方案，提供了从数据中心、硬件、数据、自助服务等多个层次的高可用性构建能力。华为云数据中心布局于全球，可以满足不同地域（Region）的资源需求，每个地域又分多个可用区（AZ），可用区之间的风火水电相互独立，可用区之间的故障相互隔离。企业可在此基础上构建如下场景的高可用体系：

- **单AZ部署：**通常情况云上不建议单AZ部署，除非是对时延特别敏感的业务，无法接受同Region的AZ间时延，这种情况可以考虑单AZ部署，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。

5.4.2.4 双 AZ 高可用设计

公有云最常用的就是双AZ高可用方案，应用的四层架构（接入层、应用层、中间件、数据层）建议实现端到端的双AZ部署，如下图所示。

图 5-4 双 AZ 高可用设计



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。

说明

进行双AZ高可用设计时，如果业务对时延特别敏感（比如电信业务的NFV网元上云），则需要进行充分的验证和评估，并采取适当的优化措施，以确保业务能够在公有云双AZ环境中获得满意的性能和用户体验，

- **选择合适的AZ**

  云服务提供商通常会提供各个AZ的大致物理位置和网络延迟信息，不同AZ间可能在物理位置上相隔较远，导致网络延迟增加，实施跨AZ高可用方案要优先选择距离较近的AZ，可以降低网络延迟并提高应用的响应速度。

- **延迟验证**

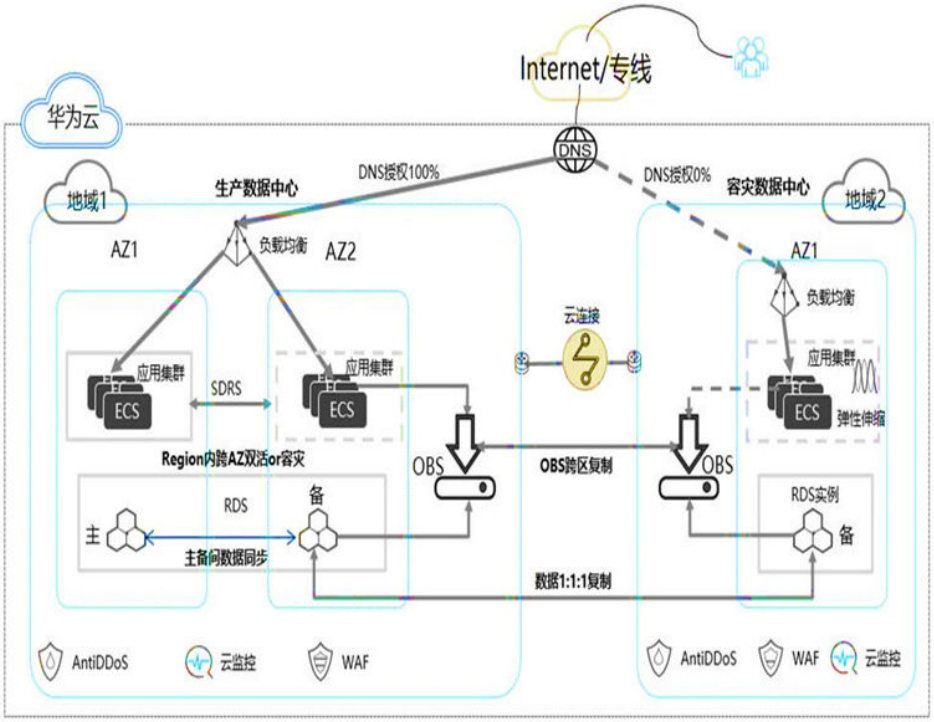
  在正式实施双AZ高可用方案前，需要充分的测试和验证来评估应用程序在不同AZ之间的延迟情况。通过模拟真实负载的压力测试，来记录不同AZ之间的应用调用延迟，用于评估是否满足业务的需求，并做出相应的决策。

5.4.2.5 两地三中心高可用设计

对于业务连续性要求较高的业务，可以考虑两地三中心的高可用性方案，如下图所示。

- 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。

图 5-5 三 AZ 高可用设计



设计要点：

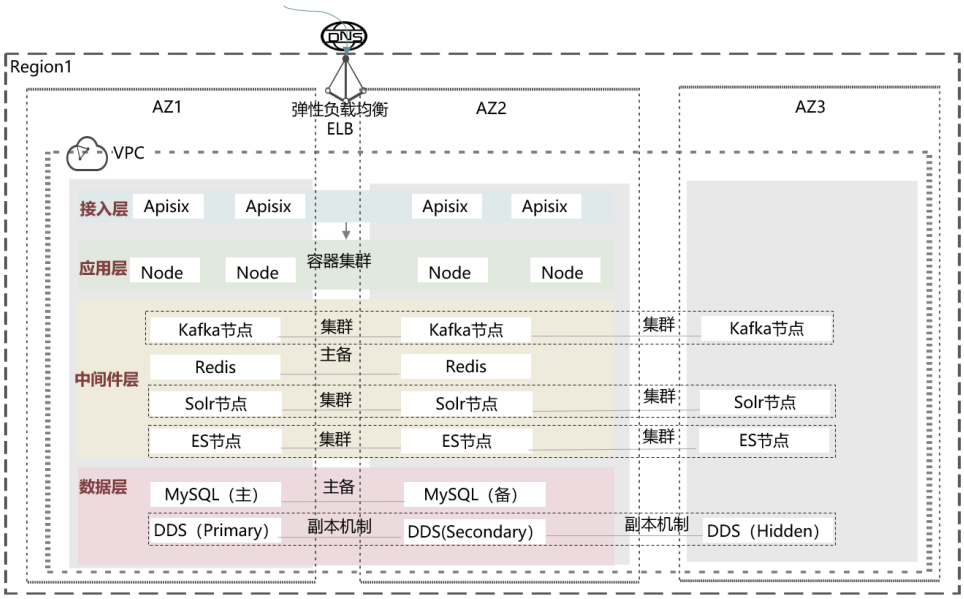
- 生产数据中心和容灾中心分别部署在华为云 2 个不同 Region。
- 生产中心采用双AZ部署（双活、热备），容灾中心单AZ。
- 在生产和容灾中心分别部署RDS数据库实例，数据库 1:1:1 主备复制。
- 生产和容灾中心产生的配置、日志、快照和备份等，通过 OBS 实现跨区复制。
- 生产站点某个AZ故障时，切换到另一个AZ，数据库主备切换。
- 生产站点全体故障时，切换数据库的主备状态，然后将 DNS 授权修改为容灾站点（生产站点 0%，容灾站点为 100%）。
- 生产站点修复后，数据库切换回主库，DNS 切换回主站点（生产站点 100%，容灾站点为 0%）。
- 为提高容灾中心利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

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**华为云MAS高可用服务。**

5.4.2.6 跨 AZ 高可用设计示例

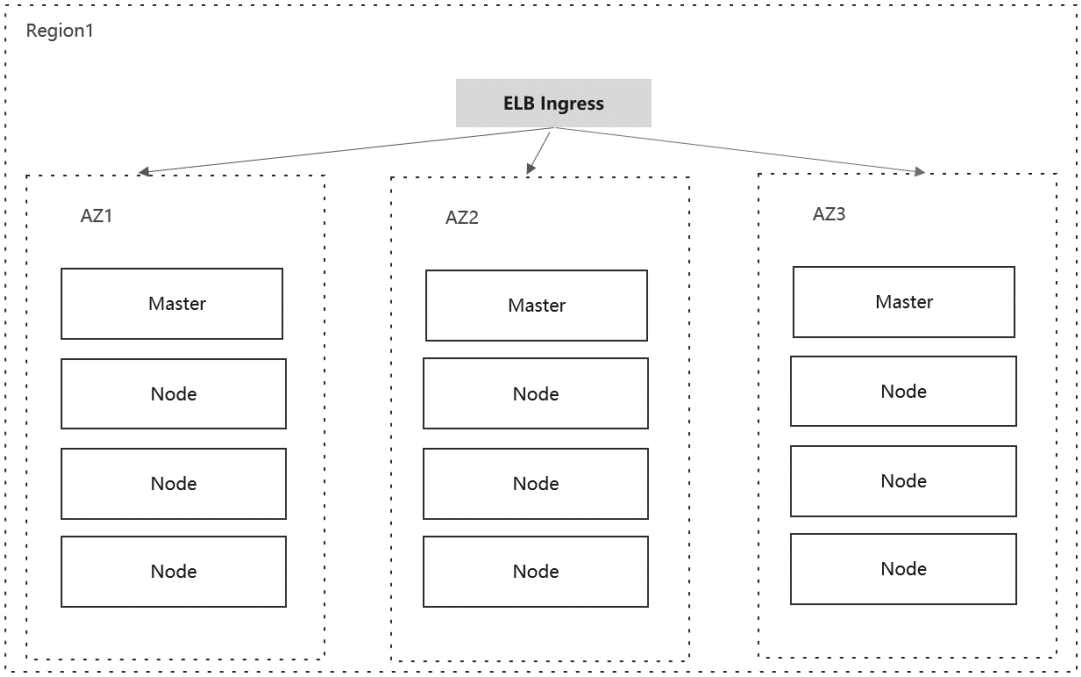
跨AZ高可用是IDC上云最主要的价值之一。企业上云后最适合做跨AZ高可用，不仅成本低，而且很便利。下面以某大型零售电商平台为例，介绍上云后的跨AZ高可用设计方法。下图是总体架构图：

图 5-6 高可用设计示例



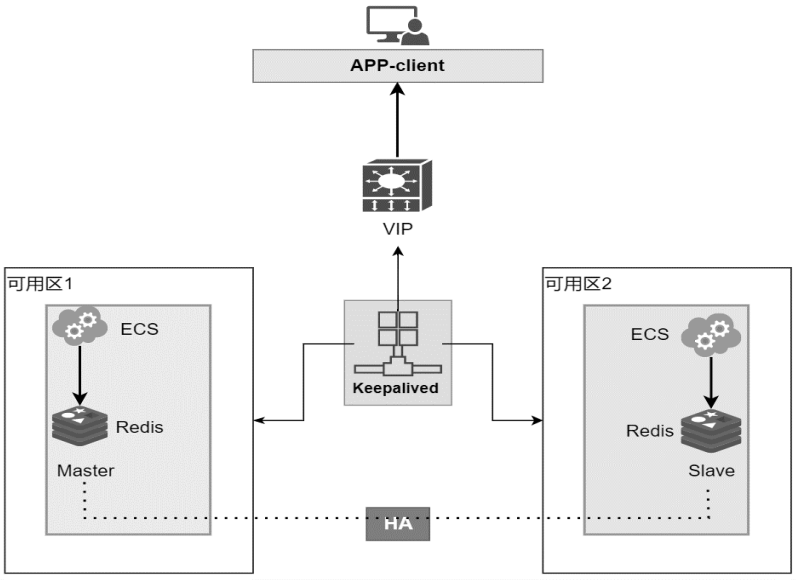
- **接入层：**Apisix双AZ均衡分布，当某个AZ出现故障时，ELB健康检查机制仍可将流量转发到正常AZ的Apisix实例处理。
- **应用层：**容器化部署，业务节点跨AZ分布。即使某AZ异常，Apisix可以将流量转发到正常应用后端。
- **中间件层：**Kafka、Solr和ES采用3AZ集群部署，任意一个AZ故障，服务仍然可用；Redis采用双AZ主备节点部署。
- **数据层：**MySQL数据库采用双AZ主备部署实现HA；MongoDB使用副本集或Cluster集群，3AZ分布，某AZ故障，其他AZ正常提供服务。
- **应用层-容器集群高可用**
  - Master高可用：容器集群Master 节点3AZ分布， 3节点（1+1+1）。
  - Ingress网关高可用：ELB实例开启多可用区，ELB Ingress即支持跨可用区高可用。
  - 应用高可用：K8S本身就支持应用高可用，可通过配置TopologyKey实现pod跨AZ分布。

图 5-7 应用层高可用设计示例



- **中间件层-Redis高可用**
  - 主备实例配置了数据持久化，数据不仅会持久化到主节点磁盘，还会实时同步到备节点，同时备节点也会持久化一份数据。
  - 主备实例部署在不同的可用区内，不同可用区的电力、网络相互隔离，当主节点所在的机房因为电力或者网络出现故障，备节点将接管服务，客户端与备节点正常建立连接以及读写数据。
  - Redis集群搭配Keepalived生成VIP，提升业务可用性。

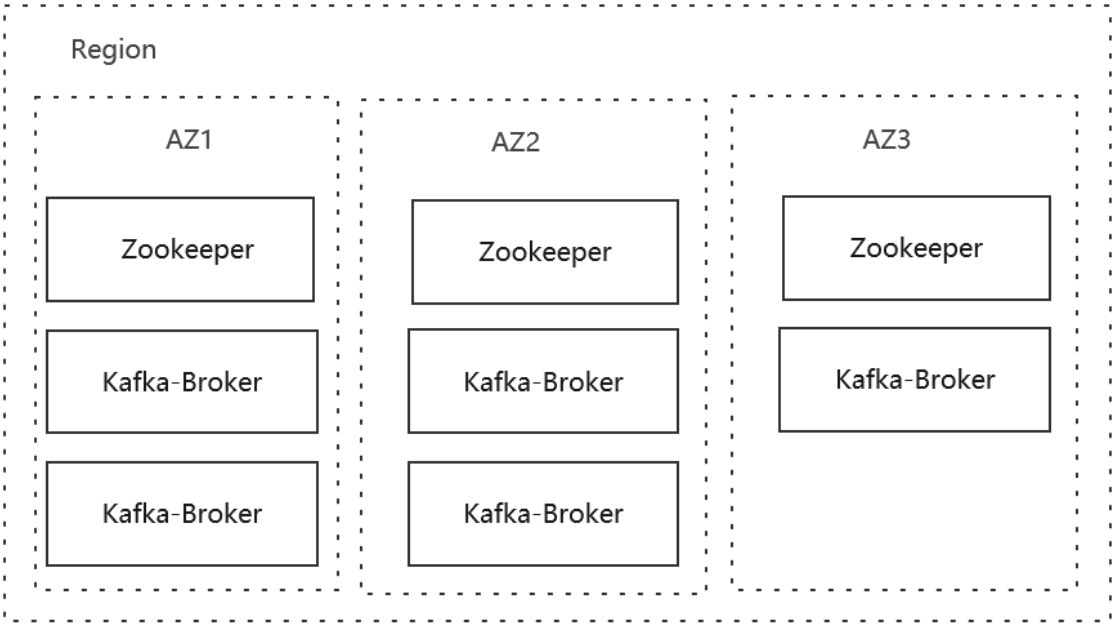
  图 5-8 中间件层 Redis 高可用设计示例



- **中间件层-Kafka高可用**

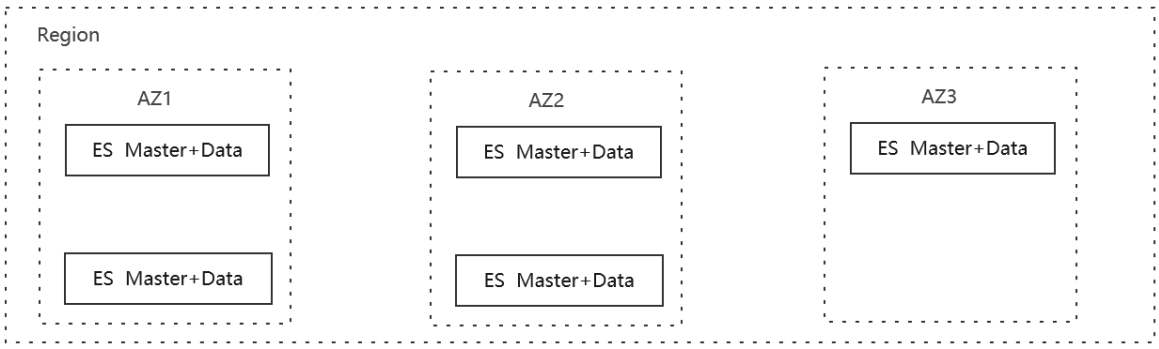
- Zookeeper高可用：Zookeeper节点3AZ分布， 3节点（1+1+1）或5节点（2+2+1）。当某个AZ不可用时，集群依旧有超过半数的法定主节点选举个数，保证ZK leader的正常选主。
- Kafka-Broker数据节点高可用：Kafka-Broker节点3AZ分布(2+2+1)。Topic副本至少设置3副本，设置unclean.leader.election.enable参数为true，在3AZ其中任意一个AZ整体宕机情况，确保集群始终最少有一份副本。

图 5-9 中间件层 Kafka 高可用设计示例



- **中间件层- Elasticsearch高可用**
  - Master高可用：ES Master节点3AZ分布（2+2+1）。在任意一个可用区不可用时，集群依旧有超过半数的法定主节点选举个数，保证Master的正常选主。
  - 数据节点：ES Data节点3AZ分布（2+2+1）。索引shard分片至少设置2副本，加上主分片副本有3副本。假如3AZ中任意一个AZ整体宕机，集群始终都有1份完整的副本，确保数据节点高可用。

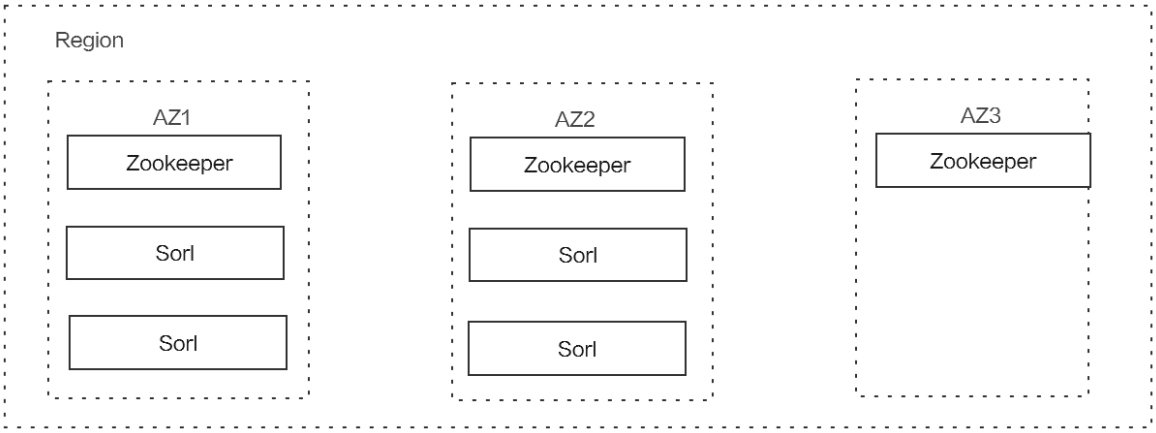
图 5-10 中间件层 ES 高可用设计示例



- **中间件层- Solr高可用**
  - Zookeeper高可用：Zookeeper节点3AZ分布，3节点（1+1+1）或5节点（2+2+1）。当某个AZ不可用时，集群依旧有超过半数的法定主节点选举个数，保证ZK leader的正常选主。

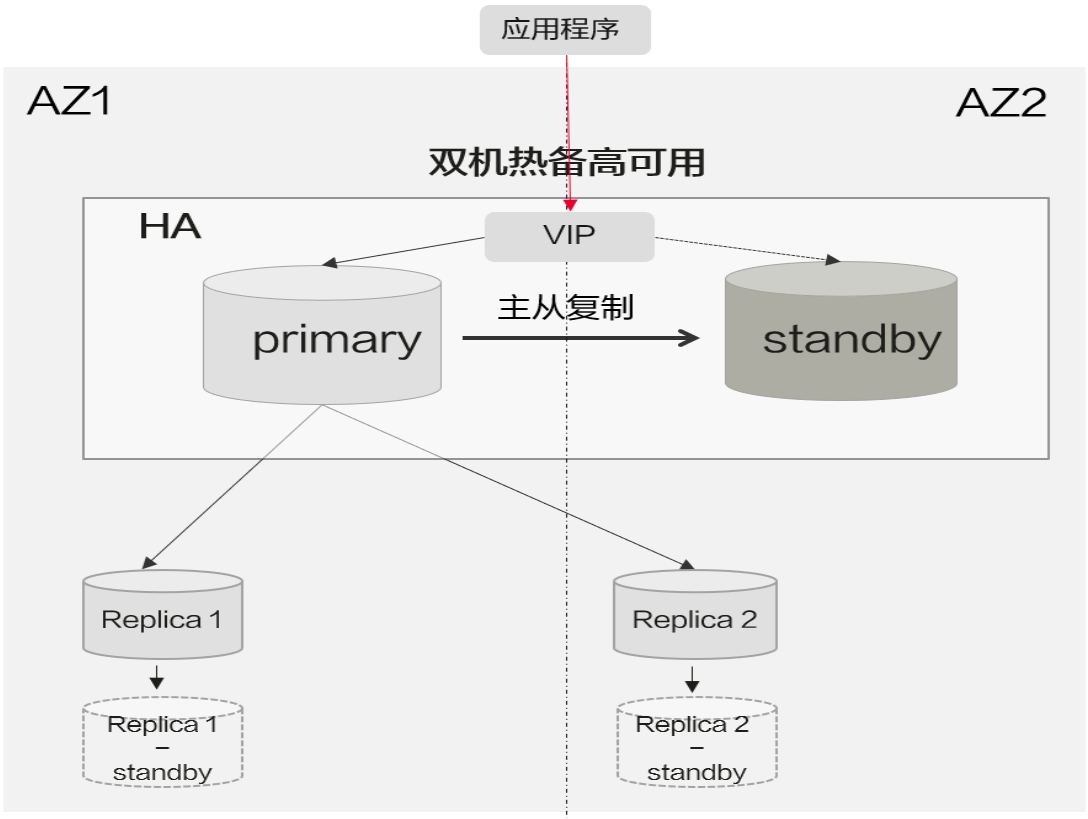
- Sorl数据节点：Sorl Data节点2AZ平均分布。索引分片至少设置（N/2）+1副本，在2AZ其中任意一个AZ整体宕机情况，确保集群始终有一份完整的副本确保数据高可用。

图 5-11 中间件层 Sorl 高可用设计示例



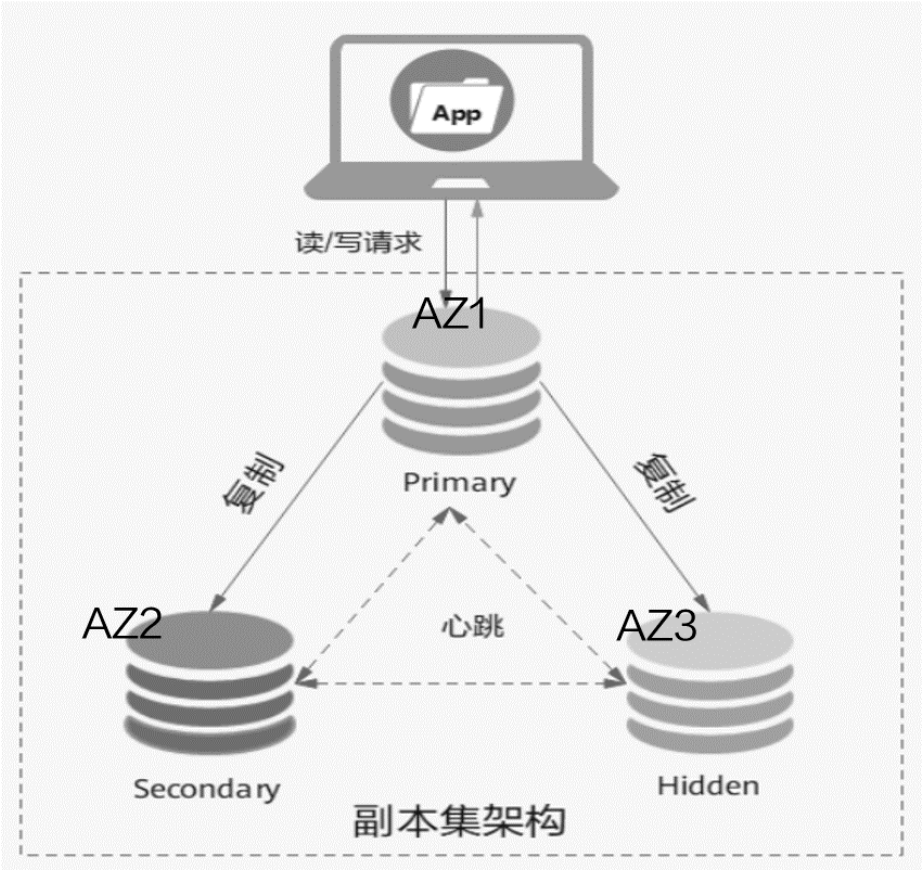
- **数据层- MySQL高可用**
- 主备实例跨AZ部署，借助原生MySQL主从复制同步能力实现主备间数据同步。
- 主备实例以VIP对外提供服务，自身IP不对租户开放。
- 主备秒级切换，主备切换时VIP漂移至新的主节点，应用感知小（只在切换瞬间有秒级中断）。
- 支持挂载只读节点，只读节点亦可跨AZ部署

图 5-12 MySQL 高可用设计示例



- **数据层- MongoDB高可用**
  - DDS副本集支持跨三AZ部署、三个节点（默认为三节点、最多可支持七节点）分别部署在三个AZ，利用Mongo原生的复制能力进行数据同步。
  - Mongo Client原生支持配置多个Server地址，并支持探活。
  - 单AZ故障时，若Primary节点所在AZ故障，利用原生的Mongo选主机制选新主，当备节点不可用时，隐藏节点接管服务，保证高可用，当前支持三副本、五副本、七副本。

图 5-13 MongoDB 高可用设计示例



5.4.3 可扩展性设计

5.4.3.1 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3类：

- **纵向（垂直）扩展：**适用于单体应用、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：**适用于分布式应用、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。

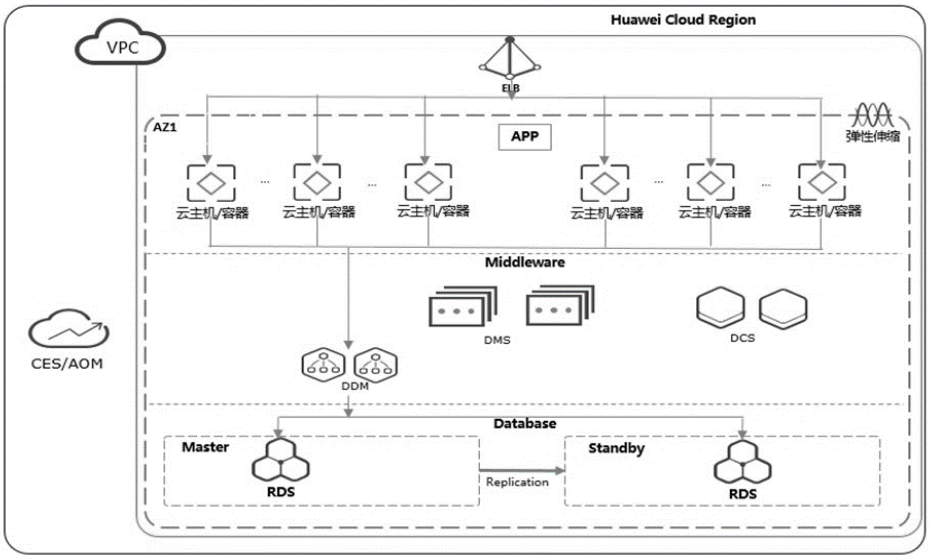
云上扩缩容可支持如下策略：

- 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。

5.4.3.2 可扩展设计

可扩展能力可分层来设计，下图展示了华为云各层级的产品扩展能力全貌。

图 5-14 可扩展性设计示例



应用上云目标架构的各层可扩展方案设计要点如下：

- **应用层可扩展设计要点**
  - 若应用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；
  - 若应用层使用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。
- **中间件层可扩展设计要点**
  - 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。
  - 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。

- **数据层可扩展设计要点**
  - 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。
  - 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。

5.4.4 性能设计

性能是目标架构设计中需要考虑的非常重要的一个方面。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， 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。

除此之外，我们还要考虑以下几个方面的内容：方案选择、性能度量、性能监测和性能权衡。

- **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；

  使用可视化技术呈现性指标和性能问题（如：异常状态、低利用率等）；
- **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**

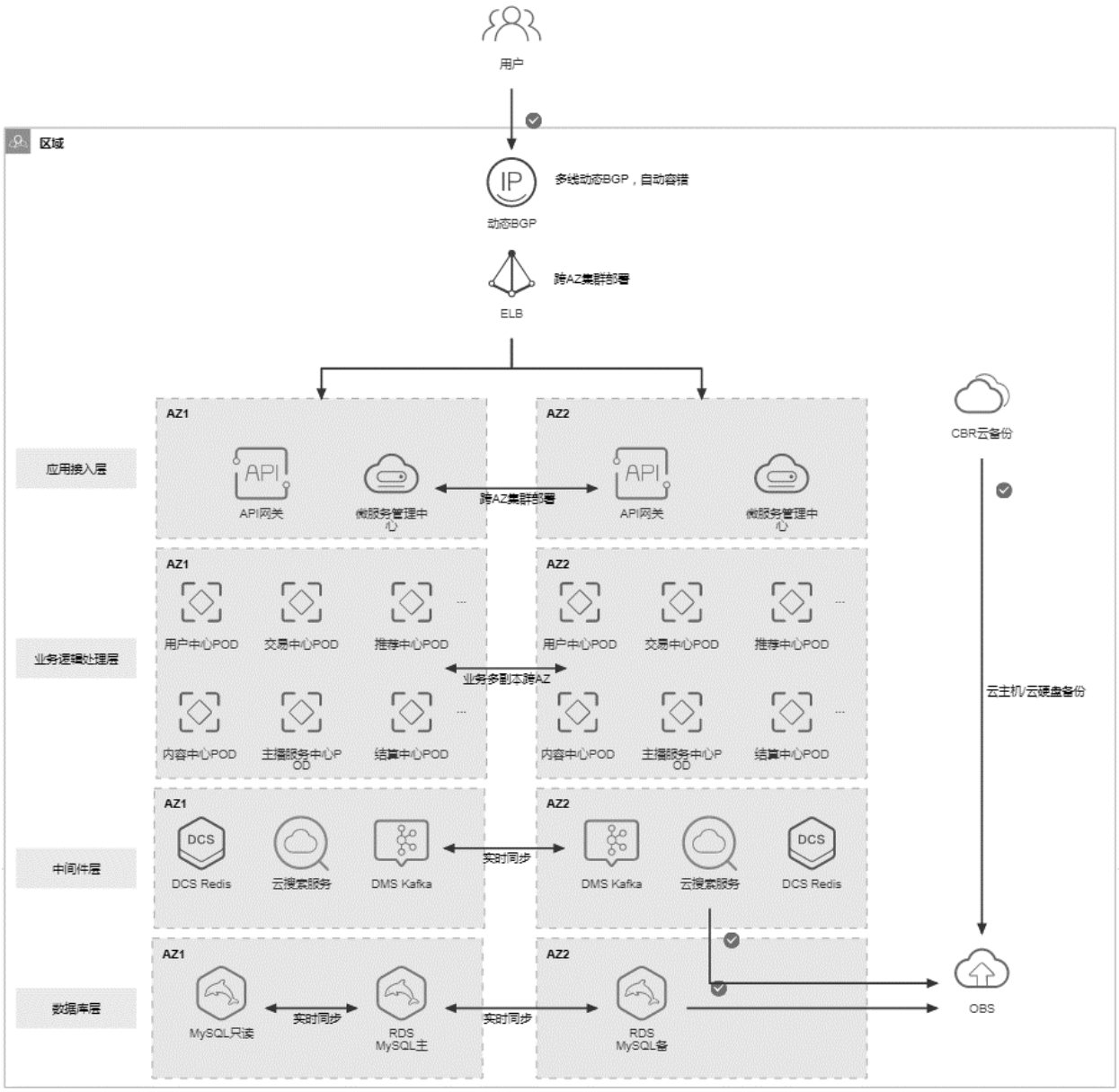
  在架构中进行折中以提高性能，例如使用压缩或者缓存技术等。

5.4.5 应用部署参考架构

5.4.5.1 应用部署架构示例

下图是音频类应用的云上部署设计参考架构：

图 5-15 应用部署架构设计示例



设计要点：

- 用户接入采用多线路动态BGP，实现公网访问线路的自动容错，可靠性高；
- 华为云ELB采用集群跨可用区高可靠部署，单数据中心机房故障对业务无影响；
- 应用接入层采用跨可用区集群部署，单可用区的故障不会影响到全局业务；
- 业务容器POD多副本均衡的跨AZ部署，通过华为云CCE容器引擎的调度策略实现，从而确保业务负载跨数据中心高可靠；
- DCS Redis跨AZ主备部署，确保跨可用区的高可靠；DMS Kafka构建跨双可用区或三可用区集群，确保消息的高可靠；CSS云搜索引擎服务可以跨AZ集群部署，单AZ的故障不影响业务运行；
- RDS for MySQL采用主备部署方式，主备实例之间的数据实时同步，如果主实例出现故障，备实例可以快速升为主实例；

- Redis、Kafka、CSS云搜索、RDS for MySQL都支持把数据备份到OBS桶，应对数据误操作之后的风险；
- 云主机/云硬盘可通过CBR云备份服务实现整个云主机或者云硬盘的备份。

5.4.5.2 参考架构库

Haydn是华为云面向合作伙伴和客户的数字化平台，当前Haydn已经积累了700+各类参考架构，企业可以根据业务场景搜索并引用华为云的应用部署参考架构，基于Haydn做架构设计，企业可以对参考架构做定制化修改，以更符合企业业务。

- **架构模板查找**

  登录华为云官网，在上方导航栏选择“解决方案>通用解决方案>Haydn解决方案数字化平台”进入**Haydn解决方案数字化平台**首页，在页面右下角点击“解决方案加速场>架构模板”可进入架构模板页面。

  a. 支持输入架构模板名称、适用行业、适用场景等关键字对架构模板进行查找；

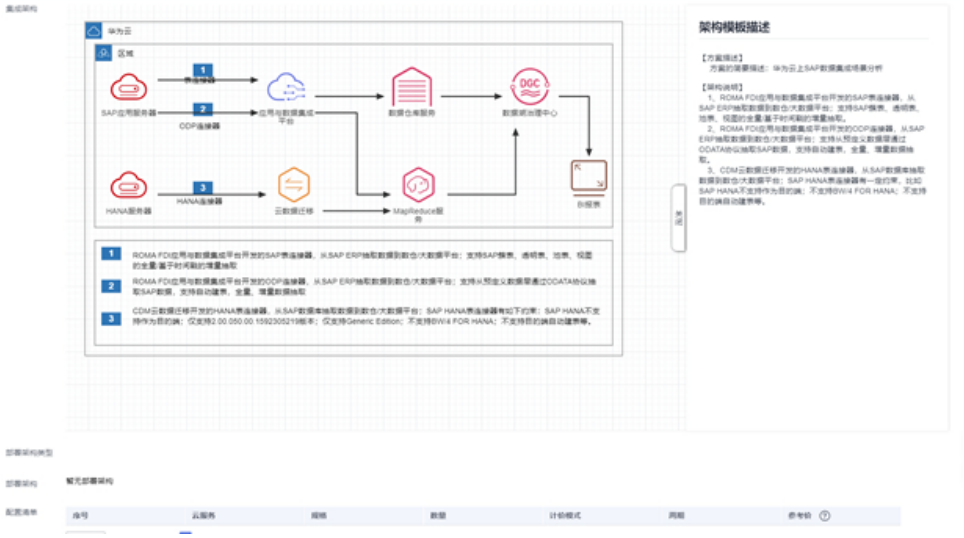
  b. 支持按照模板类型、部署环境、适用行业、适用场景对架构模板进行过滤筛选，您也可以在适用行业和适用场景右侧下拉选择更多行业和场景；

  c. 支持按照默认综合排序、最新发布、最多引用、我的关注对架构模板进行排序。

  图 5-16 Haydn 平台架构设计模板

- **架构模板详情**

图 5-17 Haydn 平台模板详情



- **架构模板引用**

  在详情页面右上方，点击“引用到设计中心”，可将该架构模板引用到指定的解决方案下。

5.5 大数据架构设计

5.5.1 设计原则

大数据的部署架构设计包括大数据集群、大数据任务调度平台和大数据应用，其中大数据应用的部署架构请参考**应用架构设计**。

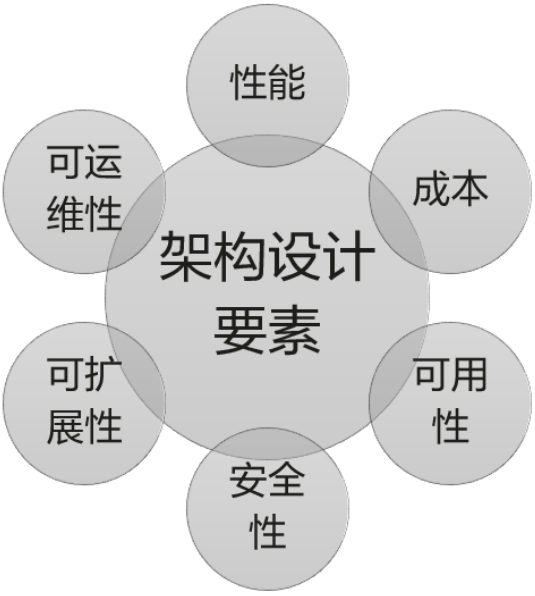
图 5-18 大数据架构设计分类

大数据架构设计同样要考虑架构设计的6要素:

- 成本
- 可用性
- 安全性
- 可扩展性
- 可运维性

- 性能

图 5-19 架构设计 6 要素



5.5.2 大数据集群设计

设计云上的大数据集群部署架构时，建议参考原则如下：

- **优先用大数据云服务：**如果源端是自建的大数据集群，在目标云平台上有对应的云服务，且功能、性能、兼容性都满足，经评估改造工作量很小，建议设计大数据集群部署架构时，优先采用大数据云服务。如果目标云平台上没有对应的大数据集群组件，部署架构设计时，可以考虑继续采用自建的方案。如果目标云平台上有对应的大数据集群组件，但兼容性较差，经评估可能需要较大的改造工作量，部署架构设计时，可以考虑继续采用自建的方案。
- **最小改造原则：**如无特别的业务驱动，要尽量避免进行大规模改造。大数据集群的组件要1：1对标设计，版本尽量一致，有版本升级需求的需要评估适配改造工作量。
- **弹性扩展和自动伸缩：**设计云上的大数据集群时，应考虑集群的弹性扩展和自动伸缩能力。这意味着集群可以根据工作负载的需求自动增加或减少计算和存储资源，以提高性能、效率并节约成本。
- **容错和高可用性：**云上部署的大数据集群应具备容错和高可用性，以保障系统的可靠性和稳定性。这可以通过使用多个副本、冗余节点和故障转移机制来实现，以确保在硬件或软件故障情况下的数据和任务的持久性。
- **数据安全和合规性：**在云上部署的大数据集群需要有严格的数据安全和合规性保障。采用适当的数据加密、身份验证、访问控制和数据隔离措施，以保护敏感数据免受潜在的安全威胁。
- **成本效益：**在云上部署大数据集群时，需要考虑成本效益。云服务提供商可以提供弹性的计算和存储资源，避免了对物理硬件的直接投资和维护成本。同时，通过根据需求进行资源的优化和调整，可以最小化成本，提高资源利用率。

5.5.3 大数据任务调度平台设计

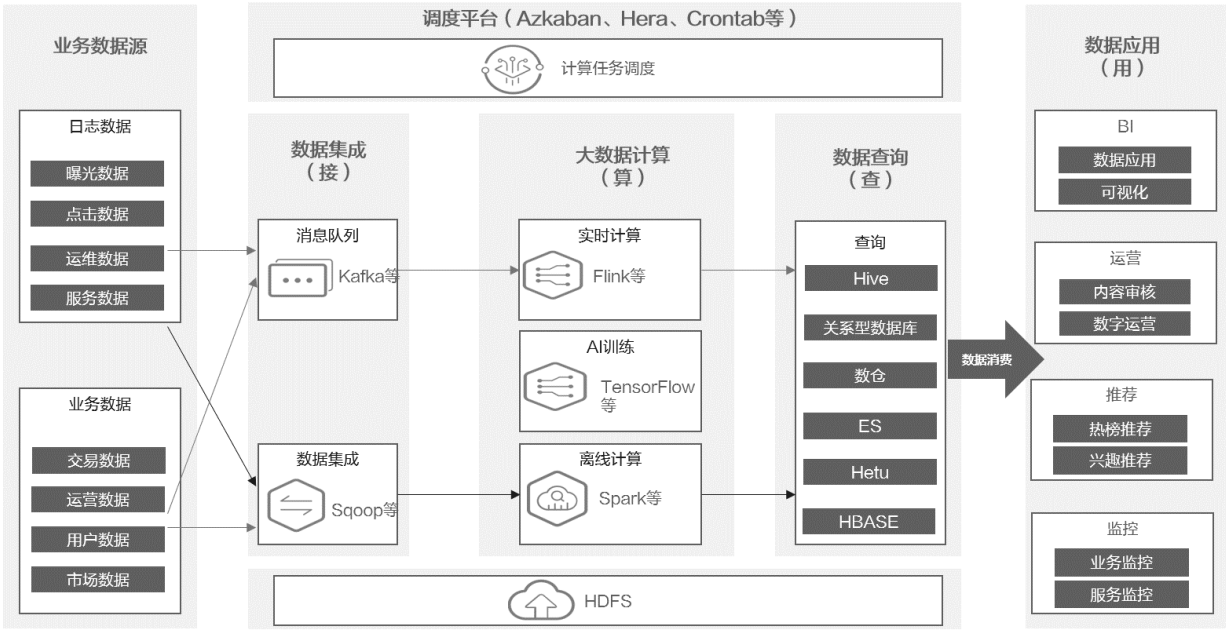
设计云上的大数据任务调度平台部署架构时，建议参考原则如下：

- **优先用大数据云服务：**如果源端是自建的大数据任务调度平台和组件，在目标云平台上有对应的云服务，且功能、性能、兼容性都满足，经评估改造工作量很小，建议部署架构设计时，优先采用大数据云服务。如果目标云平台上没有对应的大数据任务调度组件，部署架构设计时，可以考虑继续采用自建的方案。如果目标云平台上有对应的大数据任务调度组件，但兼容性较差，经评估可能需要较大的改造工作量，部署架构设计时，可以考虑继续采用自建的方案。
- **最小改造原则：**如无特别的业务驱动，要尽量避免进行大规模改造。大数据任务调度平台的组件要1：1对标设计，版本尽量不变更，有版本升级需求的需要评估适配改造工作量。
- **弹性和可扩展性：**在云上部署大数据任务调度平台时，应考虑平台的弹性和可扩展性。云环境提供了弹性计算和存储资源，可以根据工作负载的需求自动调整容量。确保任务调度平台能够快速处理增加的任务负载，并支持水平扩展以满足业务需求。
- **高可用性和容错性：**确保在云上部署的任务调度平台具备高可用性和容错性。采用冗余设计和自动故障恢复机制，以确保系统的持续可用性。例如，使用多个调度节点和备份策略来防止单点故障，并确保任务不会因节点故障而中断。
- **安全性和数据保护：**云上部署的任务调度平台需要具备安全性和数据保护机制。确保对敏感数据和系统组件进行适当的访问控制和加密，以防止未经授权的访问和数据泄露。
- **性能优化：**在云上部署任务调度平台时，需要考虑性能优化。优化资源配置、任务调度算法和数据分发策略，以提高任务执行的效率和速度。还可以利用云平台提供的服务和功能，如缓存、预取数据等，来优化任务执行的性能。

5.5.4 大数据参考架构

下图是典型的大数据架构，从数据集成、存储、计算、调度、查询和应用，构成了一个完整的数据流。

图 5-20 大数据参考架构



大数据架构通常包括以下几个核心组件和流程，企业可以根据实际需要选择云服务或自建大数据组件：

- **业务数据源：**

  业务数据源是大数据平台的数据输入来源，可以是传感器、网站日志、移动应用、社交媒体等各种数据源。通过数据采集和提取，将原始数据收集到大数据平台进行后续处理和分析。

- **数据集成：**

  数据集成是将来自不同数据源的数据进行整合和转换的过程。这包括数据清洗、数据预处理、数据格式转换、数据合并等操作，以确保数据的一致性和准确性。

- **数据存储：**

  大数据平台需要具备高效的数据存储能力，以承载海量的数据。常见的数据存储技术包括分布式文件系统（如HDFS）、列式数据库（如HBase）等。这些存储系统提供高可靠性、可扩展性和容错性，以支持大规模数据的存储和访问需求。

- **大数据计算：**

  大数据计算是对海量数据进行分布式、并行和实时处理的关键环节。主要的计算框架包括Hadoop、Spark、Flink等，它们支持分布式计算模型和任务调度。通过这些计算框架，可以进行数据处理、特征提取、机器学习、数据挖掘等复杂的计算和分析任务。

- **数据查询和分析：**

  对于大量的存储在大数据平台中的数据，需要提供灵活且高性能的查询和分析能力。这可以通过使用SQL查询引擎（如Hive）或分布式数据库（如Elasticsearch）等实现。这些工具和系统支持在海量数据集上进行查询、聚合和可视化，以提供数据洞见和决策支持。

- **任务调度：**

  大数据平台通常需要处理复杂的数据作业。任务调度系统（如Azkaban等）用于管理和调度各种数据处理作业，可以设置作业的依赖关系、调度频率、重试策略等，以确保作业的顺利执行和任务的准时完成。

- **数据应用：**

  大数据平台的最终目的是为业务提供有价值的数据应用。数据应用可以是基于大数据分析的实时报表、可视化仪表盘、智能推荐系统、欺诈检测系统等。通过将大数据的分析结果与业务流程集成，可以实现数据驱动的业务决策和创新。

5.5.5 华为云大数据组件

常用的华为云大数据服务组件如下，设计大数据部署架构时可参考：

- **MapReduce服务（MapReduce Service，简称MRS）**

  MRS是一个在华为云上部署和管理Hadoop系统的服务，一键即可部署Hadoop集群，完全兼容开源接口，轻松运行Hadoop、Spark、HBase、Kafka、Storm等大数据组件，并具备在后续根据业务需要进行定制开发的能力，帮助企业快速构建海量数据信息处理系统。详细信息请参考官网文档。

- **数据湖探索（Data Lake Insight，简称DLI）**

  完全兼容Apache Spark、Apache Flink、Trino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，支持标准SQL/Spark SQL/Flink SQL，支持多种接入方式，并兼容主流数据格式。数据无需复杂的抽取、转换、加载，使用SQL或程序就可以对云上CloudTable、RDS、DWS、CSS、OBS、ECS自建数据库以及线下数据库的异构数据进行探索。详细信息请参考官网文档。

- **云搜索服务（Cloud Search Service，简称CSS）**

  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、以及基于AI向量的多条件检索、统计、报表。Elasticsearch是一个搜索

引擎，可以实现单机和集群部署，并提供托管的分布式搜索引擎服务。在ELK整个生态中，Elasticsearch集群支持结构化、非结构化文本的多条件检索、统计、报表。详细信息请参考官网文档。

数据仓库GaussDB（DWS）

GaussDB(DWS)是基于华为融合数据仓库GaussDB产品的云原生服务，兼容标准ANSI SQL 99和SQL 2003，同时兼容PostgreSQL/Oracle数据库生态。DWS提供标准数仓、IoT数仓和实时数仓三种产品形态。详细信息请参考官网文档。

- **数据治理中心（DataArts Studio）**

  DataArts Studio支持对接所有华为云的数据湖与数据库云服务作为数据湖底座，例如MRS Hive、数据仓库服务DWS等，也支持对接企业传统数据仓库，例如Oracle、MySQL等。详细信息请参考官网文档。

- **数据接入服务（Data Ingestion Service,简称DIS）**

  处理或分析流数据的自定义应用程序构建数据流管道，主要解决云服务外的数据实时传输到云服务内的问题。数据接入服务每小时可从数十万种数据源（如IoT数据采集、日志和定位追踪事件、网站点击流、社交媒体源等）中连续捕获、传送和存储数TB数据。详细信息请参考官网文档。

- **云数据迁移（Cloud Data Migration，简称CDM）**

  云数据迁移（Cloud Data Migration, 简称CDM），是一种高效、易用的数据集成服务。 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，有效的提高您数据迁移和集成的效率。详细信息请参考官网文档。

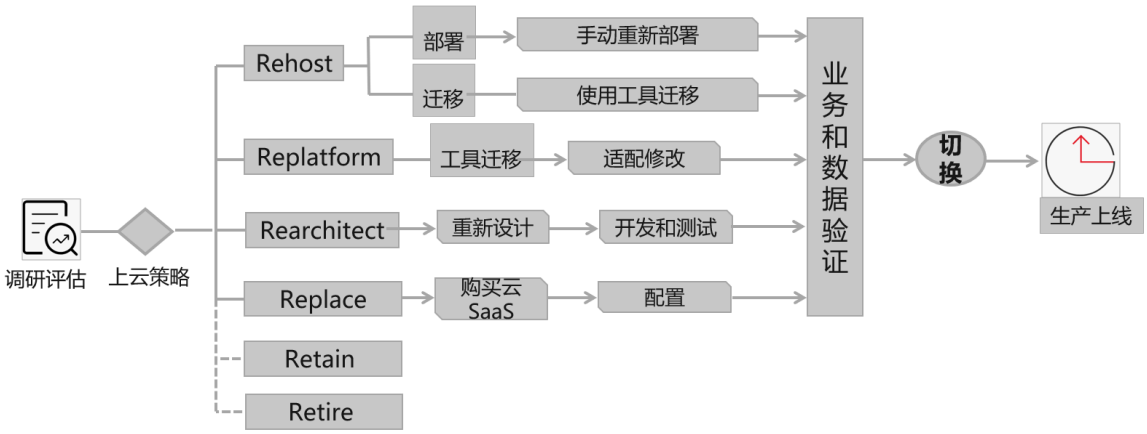
- **数据快递服务（Data Express Service，简称DES）**

  DES是面向TB到数百TB级数据上云的传输服务，目前支持Teleport和磁盘两种数据传输方式。磁盘方式适用于30TB以下的数据量迁移，Teleport方式适用于30TB~500TB的数据量迁移，500TB以上的数据量建议通过专线迁移。详细信息请参考官网文档。

5.6 制定 6R 策略

6R策略是指将现有的应用程序和数据迁移到云端的六种不同方式，如下图所示。

图 5-21 6R 策略



以下是6R策略的含义和适用场景。

表 5-2 6R 策略的含义和适用场景

策略	含义	适用场景
Retire	停止使用应用程序或其组件，因为它不再需要或有更合适的替代方案。这并非严格意义上的“迁移”，而是对现有应用的淘汰。	• 应用程序不再被业务使用。 • 应用程序的功能已被其他系统取代。 • 维护应用程序的成本过高，且其业务价值低。 • 应用程序的技术过时，难以维护和升级。
Retain	将应用程序保持在当前状态，不进行迁移。这通常是针对短期策略或正在进行更广泛的IT战略规划时的临时措施。	• 应用程序依赖于特定硬件或软件，无法轻松迁移。 • 应用程序迁移的风险过高，且短期内没有迫切的迁移需求。
Rehost	也称为“直接迁移”或“Lift and Shift”，将应用程序原封不动地从本地数据中心迁移到云平台。通常使用工具将虚拟机或物理服务器转换为云中的虚拟机。	• 快速迁移到云平台，以降低成本或提高可用性。 • 需要快速完成迁移，时间紧迫。 • 缺乏应用程序的深入了解或修改代码的资源。
Replatform	在迁移过程中对应用程序进行少量修改，以适应云平台。例如，将应用程序从使用本地数据库迁移到使用云数据库服务。这通常不涉及修改核心应用程序代码。	• 希望利用云平台的PaaS服务，例如数据库、消息队列等，以减轻自建数据库和消息队列的运维压力。 • 需要提高应用程序的性能或可扩展性。 • 不需要进行大规模代码修改，但希望优化应用程序在云平台上的运行。
Rearchitect	对应用程序代码进行重写或重构，以更好地适应云原生架构。例如，将单体应用程序重构为微服务架构，或者采用Serverless和事件驱动架构。	• 需要显著提高应用程序的性能、可扩展性和可维护性。 • 希望充分利用云原生技术，例如容器化、无服务器计算等。 • 应用程序架构过时，难以维护和扩展。
Replace	使用全新的应用程序或服务替换现有的应用程序。这通常涉及购买 SaaS 产品或其他新应用软件。	• 现有的应用程序无法满足业务需求。 • 维护现有应用程序的成本过高，且有更合适的替代方案。 • 市面上有成熟的 SaaS 产品可以满足业务需求。 • 希望快速部署新的功能和服务。

在6R策略中，真正涉及迁移到云的策略只有Rehost、Replatform和Rearchitect，这三种策略的对比情况如下表所示，企业可以根据业务需求和实际的应用场景，并综合比较每种策略的迁移风险、周期、成本、难度和业务收益选择最合适的迁移策略。

表 5-3 迁移策略对比

迁移策略	迁移风险	迁移周期	迁移成本	迁移难度	业务收益
Rehost	低	短	低	小	低
Replatform	中	中	中	中	中
Rearchitect	高	长	高	大	高

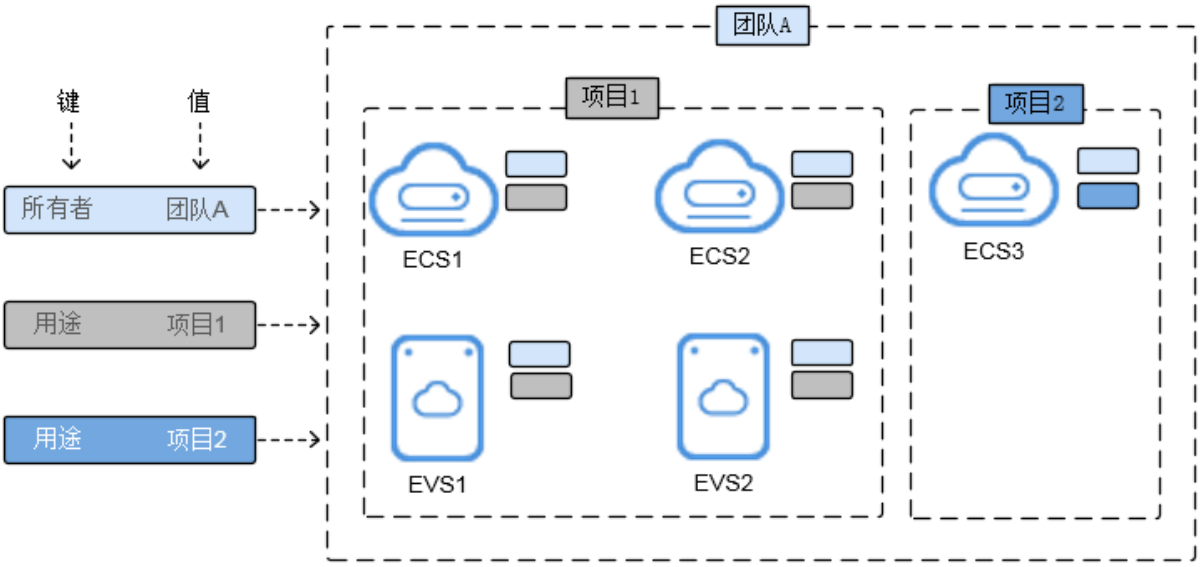
5.7 设计标签方案

5.7.1 简介

标签是用于标识和分类云资源，通常由键（Key）和值（Value）组成。当用户拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境等）对云资源进行标识和分类，然后基于标签进行资源筛选、成本归类和细粒度权限设置等，从而简化资源管理和优化成本。

如下图所示，用户为每个云资源分配了两个标签，每个标签都包含自定义的一个“键”和一个“值”，一个标签使用键为“所有者”，另一个使用键为“用途”，每个标签都拥有相关的值。

图 5-22 资源标签示例



华为云提供的标签管理服务（Tag Management Service，简称TMS）是一种快速便捷将标签集中管理的可视化服务，提供跨区域、跨服务的集中标签管理和资源分类功

能，为客户提供统一的控制台与API接口，并最终实现用户对资源的使用权限、计费与管理高效结合。关于TMS的具体功能和使用说明请参考**官网文档**。

5.7.2 标签最佳实践

标签设计原则

为华为云资源设计标签时，我们提供以下建议：

1. 请勿在标签中存储用户身份信息或其他敏感信息。
2. 对标签区分大小写格式，并跨所有资源类型一致地应用该格式。
3. 虽然标签有长度规格上限，但尽量不要每个标签都达到标签规格上限，标签长度能标明含义即可。
4. 提前识别标签的应用场景，比如成本管理、运维和自动化、细粒度权限控制、数据分类、安全运营等，并据此制定标签键值规范，下面会介绍。

标签键值规范

根据标签设计原则制定企业范围内的标签键值规范，所有用户在给云资源打标签时需要严格遵守这些键值规范，标签键值规范的典型示例如下表所示。

表 5-4 标签键值规范示例

应用场景	标签键	允许的标签值
成本管理	Department	Marketing, Engineering, Sales，Service，Research等
成本管理	Application	CRM，ERP，HRM，财务管理系统等
成本管理	CostCenter	123, 456, 789等
权限控制	Environment	Development, Test, Stage, Product等
权限控制	Layer	DB, App, Web等
数据分类	DataClass	Public, Private, Confidential等
安全运营	Compliance	PCI-DSS, HIPPA等
运维和自动化	Status	Active, Inactive, Deprecated等

使用标签策略

制定了标签键值规范之后，需要强制所有用户严格按照这个规范对云资源打标签，否则很容易造成资源标签的混乱，影响标签的使用效果。华为云提供的**标签策略**可帮助您在华为云账号中对云资源添加的标签进行规范化管理。

例如，标签策略规定为某资源添加的标签A需要遵循标签策略中定义的大小写规则和标签键值规范。若标签A使用的大小写、标签键值不符合标签策略的要求，则资源将会被标记为不合规。

标签策略当前的应用方式为事前拦截，即标签策略开启强制执行后，则会阻止在指定的资源类型上完成不合规的标记操作。

标签策略可以绑定到组织的根、OU和账号。当绑定到根和OU时，所有子OU和子账号都继承该标签策略。账号继承的所有标签策略和直接绑定到账号上的所有标签策略，根据继承运算符最终聚合为有效标签策略。

标签命名限制和要求

1. 每个资源最多可以有20个用户创建的标签。注意：以 _sys_开头的系统创建标签将保留供华为云系统使用，并且不计入此限制
2. 对于每个资源，每个标签键都必须是唯一的，每个标签键只能有一个值
3. 标签键必须包含1到128个Unicode字符，并且以UTF-8格式表示
4. 标签值必须包含0到255个Unicode 字符，并且以UTF-8格式表示
5. 标签键和值区分大小写，建议利用标签策略在所有资源类型中一致地实施该策略。例如，决定是使用 HuaweiCloud、huaweicloud 还是 Huaweicloud，应保持相同的规则。

5.7.3 典型使用场景

成本管理

通过为每个云资源设置标签，可以实现精细化的成本追踪和管理，有效控制云成本，提高企业财务管理的有效性和便捷性。标签也是财务部门实施精细化管理的重要工具。可以让财务人员以更好地理解、管理和优化公司的IT投资。这包括且不限于以下几个方面：

1. **更精确的成本控制：**合理且标准的标签，可以使财务人员更准确地追踪每一个资源的实际使用成本。这有助于识别和优化高成本的资源使用，从而实现成本节约。
2. **更有效的预算管理：**财务人员将云支出分配到具体的预算类别中，使得制定和调整预算更加科学合理。同时，也可以更容易地监控实际支出
3. **更透明的费用分配：**对于多部门或多项目的公司，标签使得将成本直接关联到相应的部门或项目，确保了费用分配的公正性和透明度。这不仅有助于内部成本核算，也有利于向客户或其他利益相关者报告时提供清晰的成本构成。
4. **更简化的账单管理和分析：**使用标签可以大大简化账单解析工作，让财务人员能够快速理解和审核账单内容。此外，还可以利用标签进行详细的费用分析，找出节省成本的机会点。
5. **更准确的决策：**准确的标签信息为管理层提供了基于事实的数据基础，帮助他们做出更明智的投资决策。

CCoE团队在通过标签进行成本管理和财务管理时，可以配备一位具有财务相关知识的人员，共同制定资源标签的相关策略。

使用标签进行成本管理的主要流程

- **制定标签规则**

  CCoE团队联合企业财务人员，共同制定标准化标签命名规范。例如以子公司、运行环境、部门、业务单元、应用系统为维度，基于标签设计原则制定用于成本管理的标签的键和值。

- **设置资源标签**

按照上面设计的标签命名规范，为每个云资源创建相应的标签。为避免云资源的实际操作人员乱打标签，您可以通过华为云提供的标签策略强制执行标签命名规范。

- **激活成本标签**

  使用标签按各种维度（例如用途、环境、部门等）对云资源进行成本分类之前，需要先进行成本标签激活，具体步骤请参考**官网文档**。

- **成本分析和优化**

  激活成本标签之后，进入“成本分析”页面，通过成本标签进行成本数据汇总和过滤。CCoE团队可以查看哪些标签下的资源被闲置，哪些标签下的资源负载过高，从而进行成本优化。

运维管理

标签是云运维实践的重要组成部分，它不仅提高了工作效率，帮助云运维团队更好地掌控复杂的IT环境。标签对于云运维具有多方面的重要意义，主要体现在以下几个方面：

- **简化资源管理：**标签允许运维人员以更灵活的方式管理和组织云资源。例如，可以按项目、环境（如开发、测试、生产）、所有者或成本中心等维度对资源进行分类，从而提高资源的可见性和可管理性。
- **管理生命周期：**标记资源的生命周期信息，以便于规划资源的启动和删除，辅助运维人员进行资源管理。
- **合规性和安全性：**安全运营人员可以根据应用数据的敏感度对资源配置标签，确保应用和数据遵循相应的安全和隐私法规，或内部/外部的审计需求。
- **协助故障排除：**运维人员可以利用标签快速定位受影响的资源，加速问题的诊断和解决过程。
- **协助自动化运维：**运维人员可以根据标准化的标签来编写脚本或配置规则，实现自动化任务。比如，自动启动或停止带有特定标签的实例，或者定期释放带“删除”标签的资源，这大大减少了人工干预的需求，降低了人为错误的风险。
- **协助性能优化：**运维人员可以将记录的关键指标（如CPU利用率内存利用率等）标注在标签内，以提示相关人员采取行动，进行性能优化。
- **协助安全加固：**运维人员可以基于标签，进行安全策略实施权限分配，确保只有特定授权用户能够访问或操作某些敏感资源。
- **协助灾备恢复：**为灾备时需要快速恢复的应用建立标签，以确保灾难发生后这些应用能够第一时间被重启。

5.8 上云试点

5.8.1 为什么要上云试点

上云迁移试点是企业在进行大规模上云迁移之前的重要步骤，它能够帮助企业在大规模迁移之前充分了解和评估各种因素，通过试点上云迁移流程与相关配置，企业可以提前识别出相关风险，为后续大规模上云迁移提供经验。

- **风险控制：**上云迁移是一个复杂的过程，涉及到不同的系统和业务。通过进行迁移试点，企业可以在小范围内验证整个迁移流程的可行性，发现潜在问题并及时解决，确保后续的大规模迁移顺利进行。同时试点还可以帮助企业识别潜在的风

险和挑战，例如，某些业务可能无法适应云环境，通过试点，可以在较小的范围内暴露这些问题，并及时采取纠正措施，从而降低全面迁移时的风险。

- **验证可行性：**上云迁移试点可以验证企业的应用和数据是否适合迁移到云端。通过选择一小部分应用或业务进行试点，企业可以评估业务在云环境中的兼容性、性能、安全性、可靠性等方面是否满足需求。如果发现某些应用不适合迁移到云端，企业可以根据评估结果重新规划迁移策略或寻找替代方案，避免将不适合或难以迁移的应用直接投入生产环境。
- **掌握经验：**上云迁移试点可以让企业的技术团队和业务人员获得实践经验。在试点过程中，他们可以学习并熟悉云平台的特点、功能和最佳实践，了解迁移的工具和流程，并积累相关知识和技能，为后续的全面迁移做好准备。
- **确定优先级：**通过试点迁移，企业可以评估不同应用或业务的迁移优先级。根据试点结果，企业可以确定哪些应用或业务对于上云迁移的影响较小，可以先行迁移，进而有序地推进整个迁移过程。
- **性能优化：**迁移试点还可以帮助企业识别并解决潜在的性能问题，通过在小规模环境中进行试点，企业可以验证应用在云环境下的性能指标，如延迟、吞吐量和响应时间等，了解应用在云环境中的实际表现，这样可以及早发现瓶颈并做出相应的优化和调整，确保在正式迁移之前获得良好的性能和用户体验。
- **成本控制：**迁移试点提供了一个机会，让企业更准确地评估上云迁移的成本，通过试点阶段的实际操作，企业可以更好地理解云服务的费用结构、资源消耗情况以及可能的隐藏成本，这有助于避免意外的成本增加并优化资源利用，以实现成本控制的目标。
- **团队磨合：**上云迁移的成功离不开各参与方的高效协同（运维团队、开发团队、测试团队，云服务供应商、第三方系统供应商等），上云迁移试点为不同团队提供了一个合作的机会，通过试点可以识别团队间的合作问题和风险，并针对性制定相关应对措施，保证大规模上云期间合作顺畅。

5.8.2 如何选择试点应用

试点应用的选择应该站在整体角度综合考虑是否满足优先试点的条件，选择试点应用时可以考虑如下因素：

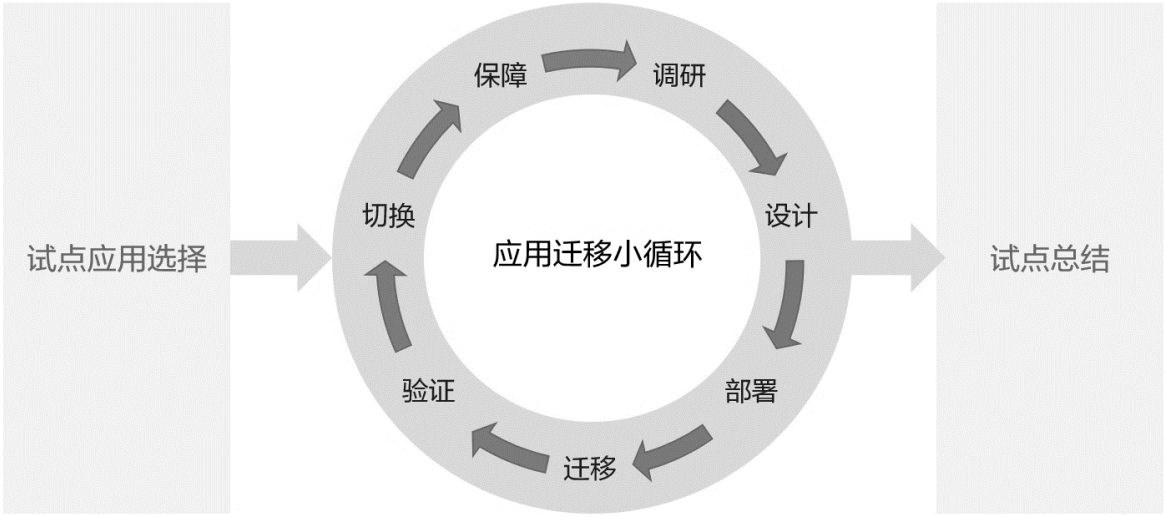
- **上云意愿：**企业推行全面上云时，不同业务部门的上云意愿是不一样的，可以优先考虑意愿度高、有充足的人力和时间、投入积极的业务。
- **业务重要性：**根据企业现有的应用和业务，选择重要性较高，但又不影响正常运营的应用作为试点。
- **上云价值：**选择上云的价值可量化、容易量化的应用，如降低成本、提升可用性、实现业务快速部署等，通过试点应用证明上云的价值。
- **实施难度：**根据企业的IT部门的实施能力，选择一些实施难度较低的应用作为试点。
- **业务影响：**考虑上云后对其它业务流程及数据流向的影响，尽量避免影响其它业务的正常运行。
- **安全性：**考虑上云后对数据安全性及相关法律法规要求，尽量避免存在安全风险或者违反相关法律法规情况。
- **可测试性：**企业上云要通过试点迁移尽量验证方案并识别可能存在的问题，并不断测试和优化方法来保证上云成功，因此，要选择可测试性强的应用，能够充分验证方案，为后续规模上云铺路。

5.8.3 上云试点执行与总结

上云试点执行

试点应用选择好以后，上云迁移试点按照应用迁移小循环流程执行即可，最后输出试点总结：

图 5-23 迁移小循环流程



上云试点总结

上云迁移试点总结旨在总结试点项目的成果、经验和教训，并为后续的大规模迁移提供指导和改进方向。这对于企业切实评估上云的收益、风险和挑战，以及制定有效的迁移策略至关重要。上云迁移试点一般从如下方面总结：

1. **目标和范围：**总结上云迁移试点的目标和范围，明确试点迁移的期望结果，描述试点涉及的应用程序、系统或业务流程，以及试点的时间、地点、参与人员等信息。
2. **迁移方法和策略：**总结采用的迁移方法和策略，描述采用的技术、工具和流程，以及与迁移相关的关键决策。
3. **成果评估：**评估上云迁移试点的效果，包括成功迁移的应用程序数量、迁移过程中的问题和挑战，以及解决方案和改进措施等，总结迁移试点对企业的业务影响和收益。
4. **技术和性能评估：**评估试点迁移后的系统和应用程序的性能和稳定性，考虑应用程序的可伸缩性、响应时间、数据传输速度等因素，总结试点迁移对系统性能和用户体验的影响。
5. **成本效益分析：**分析上云迁移试点对企业成本的影响，包括成本节约、资源利用优化、维护和支持成本的变化等方面的评估。
6. **安全和合规性评估：**评估上云迁移试点的安全性和合规性，考虑迁移后的数据安全性、访问控制、合规法规要求等方面，总结试点迁移的合规性水平和安全风险控制程度。
7. **学习和经验教训：**总结上云迁移试点过程中的学习和经验教训，包括成功因素、失败原因以及识别到的最佳实践，记录技术和管理方面的发现，以帮助后续大规模迁移更好地规划和执行。

8. **建议和改进措施：**根据试点迁移的结果，提供进一步的建议和改进措施，以指导未来大规模迁移的计划，包括优化迁移流程、加强培训和沟通等方面的建议，以及在安全和合规性方面采取的进一步措施。
9. **后续计划和风险管理：**提供针对试点迁移后续步骤的计划，包括大规模迁移计划、资源调配计划、风险和问题解决计划等，总结试点迁移对后续迁移计划的指导和影响，并提供风险管理和应对措施。

5.9 批次规划

5.9.1 概述

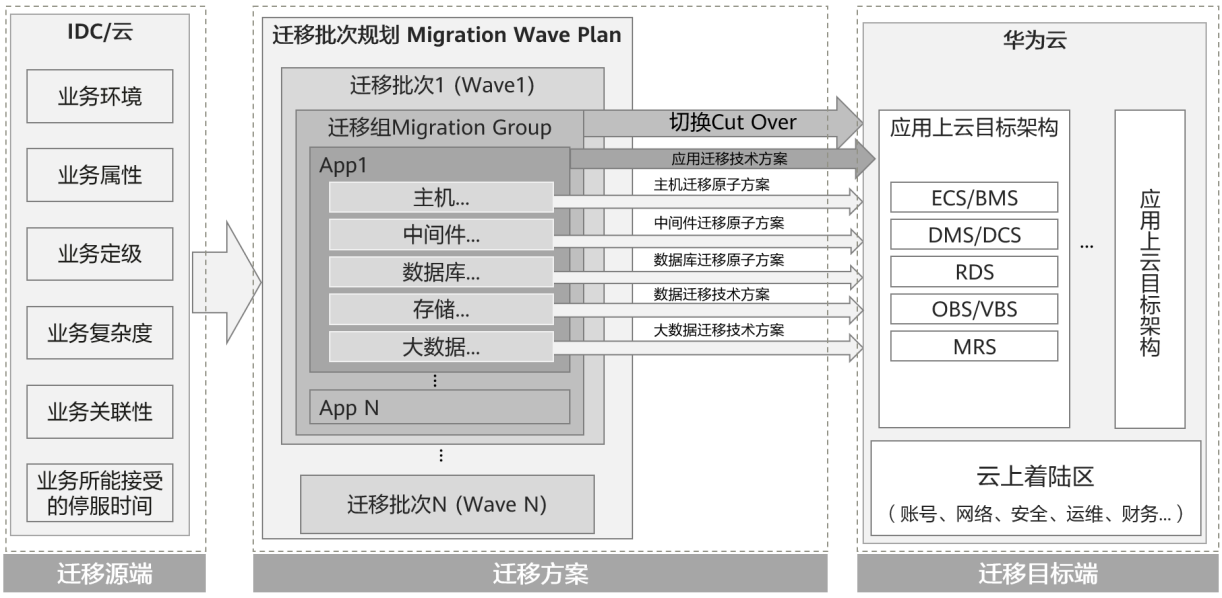
为什么要做批次规划

上云迁移批次规划是为了把上云迁移分成几个阶段，以便更加有效地迁移企业应用到云端。批次规划的目的是为了将上云迁移的复杂性减少到最低，以便更有效地安排上云迁移的时间，统筹资源，并分析各个迁移阶段的风险，让企业在最短的时间内完成上云迁移。

批次规划是企业上云迁移很重要的一项工作，在批次规划之前我们先要了解几个概念：迁移组、迁移批次、迁移优先级、迁移批次规划。

1. **迁移组：**是一组具有依赖关系（含环境依赖）的应用程序和基础架构的集合，包括APP、主机、存储、数据库、中间件。
2. **迁移批次：**是指一组具有相同的预期开始日期和结束日期的一个或多个迁移组的组合，一个迁移批次可能含有多个迁移组。
3. **迁移优先级：**是指应用程序的迁移顺序。
4. **迁移批次规划：**包括迁移分组、分批的信息和迁移优先级的信息，给出了各个批次的迁移对象和实施时间顺序。

图 5-24 迁移概览图



5.9.2 迁移批次规划的方法

迁移批次规划既是科学也是艺术，有些规划依据数据，有些规划只能依赖专家经验，批次规划需要做好三件事情：迁移分组、迁移分批、迁移优先级。

图 5-25 批次规划

一、迁移分组

迁移分组主要是基于依赖关系将迁移对象进行分组，我们将一组具有强依赖关系的应用程序和基础架构的集合（包括APP、主机、存储、数据库、中间件等）放进一个迁移分组，迁移的时候要放同一批次，切换的时候要一起切。

依赖关系主要包括三种：共享数据依赖、共享服务器依赖、应用间的通信依赖。

依赖关系还有强弱之分：以共享数据依赖举例：应用程序A、B 和 C 都连接到db01，A和B 每秒都会进行许多读写操作，但是C每晚在非高峰时间运行批处理作业，因此A、B和db01是紧耦合，C与db01是松耦合，A和B必须与db01一起迁移，放到同一个迁移分组，C可以单独移动，如果需要可以放到另一个迁移分组。

二、迁移分批

企业上云过程往往是分批进行的，1个分批可以包含1个或多个迁移分组，每个分批都是上云过程的一个里程碑，迁移分批一般参考以下原则：

- **依据关联性分析结果，强关联的应用要放在一个分批**

  关联性强的要放在一个批次一起迁移，避免云上云下互访延时对业务的影响

- **一个分批跨度4~8周最合适**

  将批次划分到合适的大小，以确保有足够的人力和技术资源来执行迁移过程，并将风险降至最低，业界最佳实践一个批次跨度

  4~8周最合适，时间指的是（部署、迁移、切换），不包含准备阶段。

- **一个分批不能太大，太大增加迁移风险**

  根据业界最佳实践，一个批次不应超过20个应用程序、150 个服务器和30个数据库，超过这个大小挑战和风险都很大，增加失败挑战和回退风险，建议严格检查此规则的任何例外情况。

如果一个分批很大，首先要将关联关系打开，识别出强关联和弱关联，将弱关联断开，拆分成较小的分批迁移，降低风险。

- **同一供应商的系统安排在同一批或相邻的批次上云**

  同一供应商的多个系统之间耦合度较高，将这些系统的上云时间安排在一起，更有利于供应商在一段较短的时间内集中人力资源，确保各项目组之间的协同，有利于上云迁移实施的顺利开展。

- **不同的迁移环境放到不同的分批**

  将生产环境与测试环境放在不同的分批中，先迁移测试环境，可以大大降低生产环境的迁移风险。

三、迁移优先级

影响上云迁移优先级的影响因素有如下：

表 5-5 迁移优先级影响因子

影响因素	影响结果
业务上云意愿	上云意愿度高的先上，意愿度低的后上
业务环境	测试环境优先，生产环境最后
业务重要性	一般业务先上，核心业务后上
业务关联度	关联关系简单的业务先上，复杂的业务后上
基础架构复杂度	底层基础架构简单、实例数少的先上，复杂的后上
允许停服时间	停服时间长的先上，不停服的最后上
迁移策略	平迁的先上，要改造的后上

其中，业务部门的上云意愿是第一优先级，先基于上云意愿排序，然后再按其余因素进行排序。如果做的更科学一点，可以基于每个影响因子打分，按照打分结果确定优先级。

表 5-6 迁移优先级参考评分表

分类	影响因素	分数参考
业务环境	开发	5
	测试	3
	生产	1
业务重要性	一般	5
	重要	3
	核心	1
关联性	简单（0-3）	5

分类	影响因素	分数参考
	复杂(4-6)	3
	非常复杂(7~)	1
基础架构复杂度	简单（实例数1~3）	5
	复杂（实例数4~10）	3
	很复杂（实例数11~）	1
允许停服时长	120分钟以上	5
	60~120分钟	3
	<60分钟	1
迁移策略	Rehost	5
	Replatform	3
	Re-architect	1

应用迁移批次规划样例

表 5-7 批次规划样表

应用名称	上云策略	上云批次	第一批次上云	第二批次上云	第三批次上云	第四批次上云
-	-	-	2025.01.01~2025.03.31	2025.04.01~2025.06.30	2025.07.01~2025.09.30	2025.10.01~2025.12.31
此处仅给出表头信息作为参考。 表格具体内容请按业务实际情况进行补充。						

5.9.3 大数据迁移批次规划说明

大数据迁移上云时，是选择整体迁移还是分批迁移，原则如下：

- **整体迁移的场景：**
  - 规模小：大数据平台数据量少（TB级），计算任务数量不多，可以采用整体迁移的方法，先在云上部署大数据平台，然后全量迁移元数据、数据和任务。
  - 关联关系复杂：大数据任务之间的关联关系很复杂，很难拆分，此时也可以选择整体迁移。
- **分批迁移的场景：**大数据规模很大，但关联关系比较清晰。

  大数据平台数据量大（PB级甚至EB级），计算任务数量多。虽然规模很大，但任务之间关联关系很清晰，比如可以按照业务域进行清晰的梳理，此时我们可以对

大数据按业务域进行拆分，将有关联的数据、任务、应用划分到一个批次进行迁移。分批次迁移可以有效的减少大数据迁移的风险，降低迁移方案复杂度，提高迁移效率。

大数据迁移通常按照主题域进行分批。主题域通常是按照业务功能划分，将有相似业务逻辑的关联数据集合到一起，比如销售主题域、供应链主题域、日志处理主题域等。每个主题域有专门的数据处理流程、分析模型和相关业务逻辑，以支持特定的业务需求和分析目标。大数据迁移批次规划的参考原则如下：

- **按主题域进行分批：** 按主题域分批需要考虑2个相关性，数据相关性和任务相关性。数据相关性是指将具有相似业务逻辑、相互依赖或紧密相关的数据放在同一批次中，以确保一致性和完整性。任务相关性是指将具有依赖关系的任务和数据集中放在同一批次中。这样可以保证任务在正确的数据上运行，并确保任务之间的顺序和一致性。基于这2个相关性，将主题域划分为多个迁移批次，将相关的任务和数据流集中在同一批次中，提高迁移效率和降低风险。
- **尽量减少批次数量：**大数据迁移过程中会对数据进行抽取、转换、加载等操作，每个操作步骤都会增加复杂度和风险，影响数据的一致性，因此，应尽量减少批次的数量。
- **批次间相互独立：**批次划分时，确保不同批次间尽量是相互独立的、松耦合的，很少有相互依赖的任务和数据流。独立的批次划分，有助于降低迁移中对其它业务域的影响。
- **批次内紧耦合：**批次划分时，确保每个批次包含相关性较高的主题域和相互依赖的任务和数据流，包括数据共享场景。
- **保证业务的连续性：**迁移过程中应避免业务中断的情况发生，因此，在迁移批次划分时，需要考虑将与主题域关联性强的大数据应用系统也放在同一批次，以减少业务中断的风险。
- **迁移优先级排序：**根据业务优先级、迁移复杂度、数据量等因素，对主题域进行优先级排序。通常，先迁移数据量较小或相对简单的主题域，后迁移复杂的主题域。

5.10 成本预算计划

企业上云过程中，可以利用华为云的成本中心进行成本预算计划和管理。通过华为云的成本中心，企业可以实现对云开支的全面预算管理和监控，提高资源利用率，降低不必要的支出。合理的预算计划和持续的成本优化将有助于企业在云环境中获得更高的投资回报，实现业务的数字化转型目标。

制定预算计划时，可以参考以下内容：

- 基于历史成本数据进行预测：使用成本中心的成本分析功能，根据历史支出预测未来时间范围的成本。
- 基于业务驱动因素进行预测：基于未来的业务需求（如扩容、大促、新业务上线等），进行未来成本的变动估算。
- 基于历史数据和未来业务需求，制定出最终的预算计划。

华为云成本中心为您提供了预算模板，简化您的预算创建流程，您可快速创建成本预算，同时用户可以为预算任务创建预算报告，华为云会在报告日为您发送预算情况报告。详情请参考华为云**成本中心帮助文档**。

5.11 方案设计的反模式

在做上云方案设计时，可能会遇到一些反模式，这些模式如果不加以识别和避免，可能会降低系统的性能和安全性、造成不必要的成本浪费、增加维护难度，甚至导致项目的失败。以下是一些常见的上云方案设计时的反模式。

- **资源配置不合理**

  目标架构设计时，未根据业务负载需求合理配置资源，导致资源过度分配或不足，从而增加成本或影响性能。

  优化建议：根据业务需求和应用特点，选择合适的云资源规格，可以采用自动扩展策略，合理设置包周期和按需资源的比例，定期监控资源使用情况，持续优化调整。

- **设计存在单点故障**

  架构设计时未考虑高可用性，导致关键组件成为单点故障，一旦发生故障，整个系统将无法正常工作。

  优化建议：实现冗余设计，采用负载均衡策略，确保应用的关键服务在多节点上运行，提升系统的可靠性和可用性。

- **架构设计未考虑业务的地理分布**

  设计云上部署架构时，未考虑业务的地理分布，导致用户访问延迟高，体验不好。

  优化建议：根据业务的用户分布特点，选择合适的Region与AZ部署，确保用户能够就近访问应用实例。

  将当前的传统架构直接迁移到云上，而没有进行必要的适配和优化，可能会出现稳定性、体验差等问题。

  优化建议：对当前的应用架构进行评估，并进行相应的适配改造，以适应云上环境，并充分应用云原生的能力，提升架构的可用性、可扩展性和性能。

- **未考虑合规性和法律要求**

  在设计云上部署架构时，未考虑数据存储和访问的合规性要求，可能导致法律风险和数据泄露问题。

  优化建议：在设计上云方案时，确保了解相关的法律法规和合规要求，建立数据治理和安全策略，确保数据的存储、访问和处理符合当地法规。

通过识别和避免这些反模式，并参考行业最佳实践和成功案例，可以更加科学地设计上云方案，从而更好地利用云端优势，凸显上云的价值。

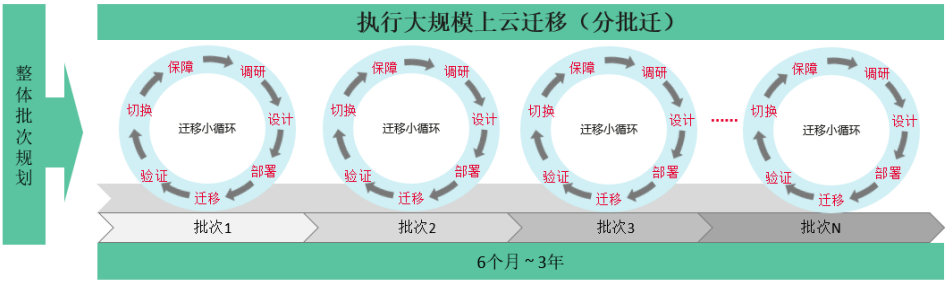
6 采用实施

6.1 概述

企业上云通常先进行试点，试点完以后才进入大规模的上云迁移阶段。大规模上云阶段有两种上云形态：

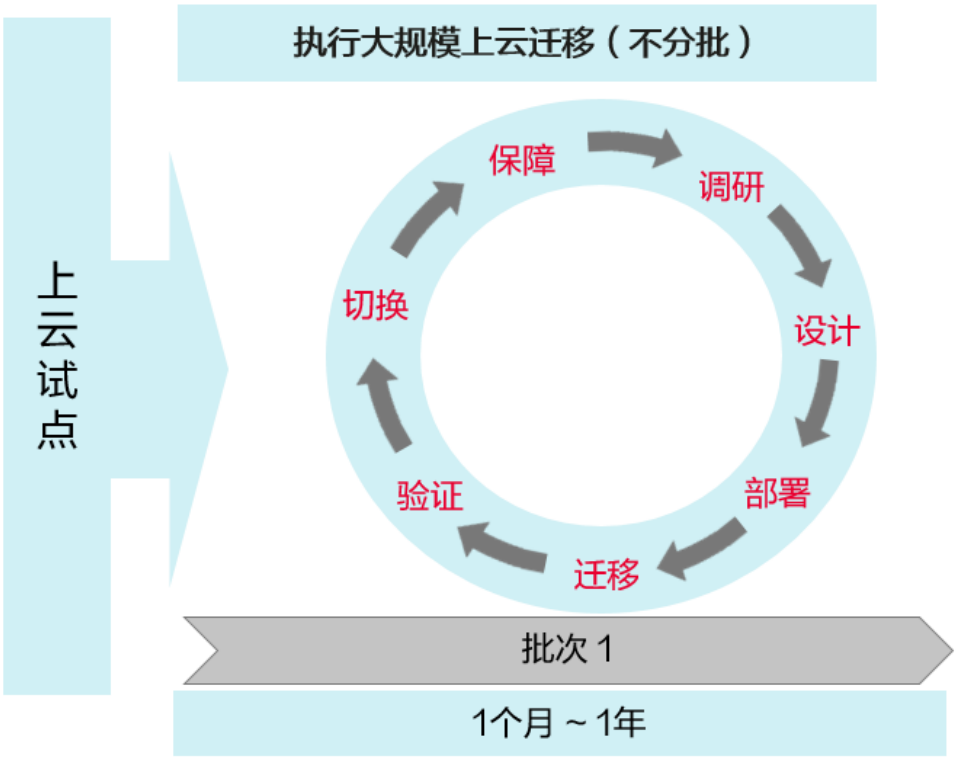
- **分批迁移：**对于能分批迁移的，企业通常会将大规模迁移划分为多个批次进行。大规模迁移的执行主要是按照批次规划逐批次进行迁移，如下图：

  图 6-1 分批迁移

- **整体迁移：**对于不能分批的，应用的关联关系往往非常复杂，只能选择所有业务系统整体一个批次迁移，如下图：

图 6-2 整体迁移



6.2 组建实施团队

在企业上云的实施阶段，组建一支高效且专业的实施团队是确保项目成功的关键。该团队将负责执行上云计划和具体的上云实施工作，保障各项上云任务的顺利进行。上云实施团队应由来自不同领域的专业人员组成，企业可以参考前述的CCoE组织架构和角色职责，组建出一个全面且专业的上云实施团队，以下为必要的团队成员。

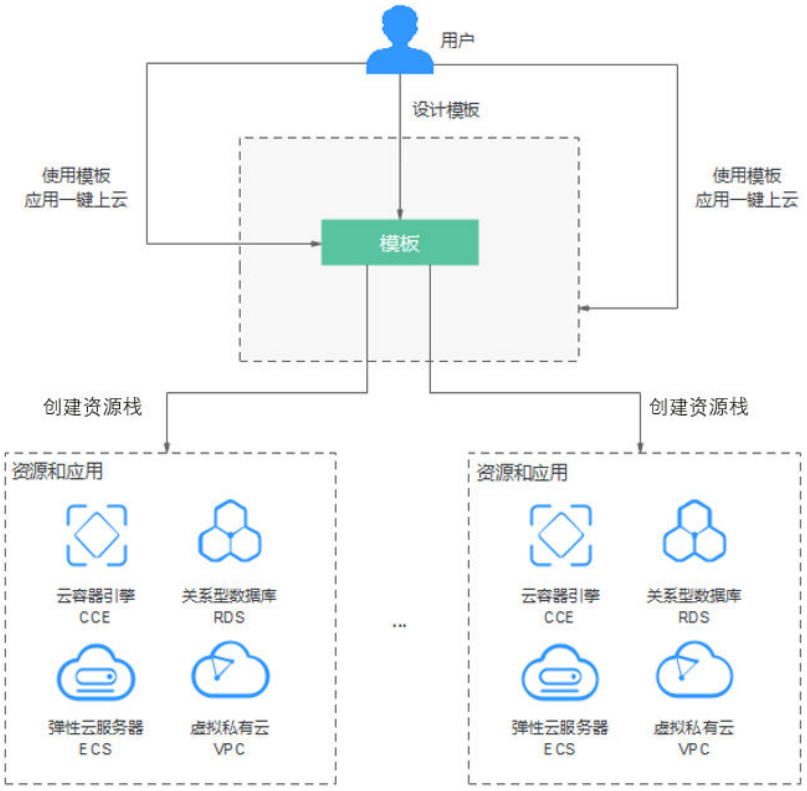
- **项目经理：**来自项目管理办公室（PMO）或具备丰富项目管理经验的IT部门成员，负责整个上云实施的项目管理，确保项目实施按计划进行，同时协调资源解决实施过程中的问题。
- **迁移实施工程师：**来自IT部门或具备云迁移经验的IT专业人员，负责具体的迁移实施工作，包括数据迁移、应用迁移、系统配置、业务割接等，确保迁移过程的数据一致性、安全性和性能。迁移实施工作属于一次性工作，经常会外包给云服务商或者云实施专业服务提供商。
- **云架构师：**来自IT架构部门或具备深厚云技术背景的专家，负责云上架构的部署和优化，为实施团队提供技术支持和指导。
- **云基础设施管理员**：来自IT部门的运维团队，负责管理云基础设施，建立和实施云运维流程，以支持云环境的管理、监控和优化。
- **云安全专家：**来自信息安全部门或具有安全合规认证的专业人士，专注于云安全和合规，确保上云过程中遵循行业规范、法律法规和企业内部管理要求，同时制定和实施安全策略，识别潜在风险并提出相应的解决方案。
- **应用开发工程师**：来自业务部门的应用团队，负责业务上云的适配改造和应用现代化改造，确保应用能够在云环境中高效、稳定、安全运行。
- **应用测试工程师：**来自测试团队，负责业务的功能、性能、可用性、可扩展性测试，配合迁移切换演练和正式的上云切换操作。

6.3 基础设施部署

基础设施部署主要是部署Landing Zone，有三种部署Landing Zone的方式。

- 由实施人员手动在华为云上部署Landing Zone，这种方式非常灵活，不受自动化工具的功能限制，但部署周期比较长。
- 基于**资源治理中心**完成自动化部署Landing Zone，具体步骤请参考**官网文档**。但资源治理中心部署的是最小化Landing Zone，不一定符合企业的实际需求，还需要在此基础上通过手工或自动化的方式进一步设置Landing Zone。
- 使用华为云提供的资源编排服务RFS或第三方自动化工具（如Terraform等）实现Landing Zone的自动化部署和管理。华为云资源编排服务（Resource Formation Service，简称RFS）是完全支持业界事实标准Terraform（HCL + Provider）的新一代云服务资源终态编排引擎。基于业界开放生态HCL语法模板，实现云服务资源的自动化批量构建，帮助用户高效、安全、一致创建、管理和升级云服务资源，能有效提升资源管理效率，并降低资源管理变更带来的安全风险。具体请参考华为云**官网文档**。

图 6-3 华为云 RFS 编排示例



6.4 应用迁移上云

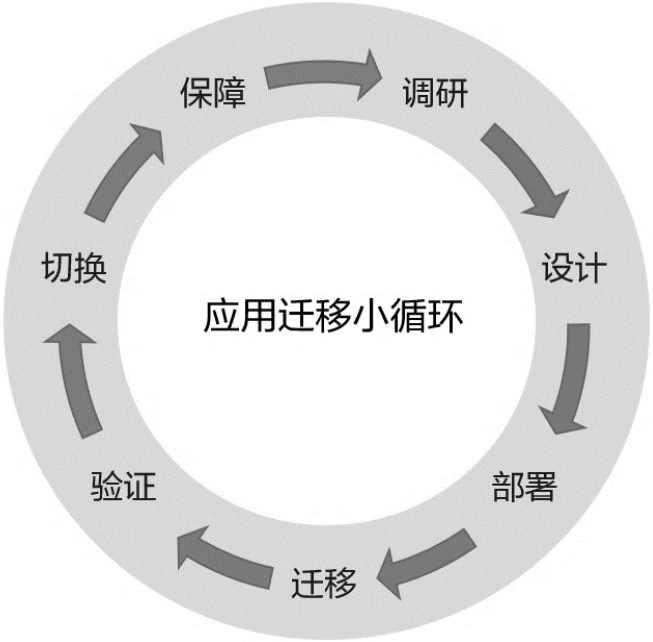
6.4.1 应用迁移上云简介

应用迁移上云简介

应用上云迁移是指将应用的接入层、应用层、中间件层和数据层迁移到云端的过程，迁移策略采用Rehost或Replatform，不含Refactor（应用改造），数据层包含对象存储、块存储、文件存储、关系型数据库、非关系型数据库。

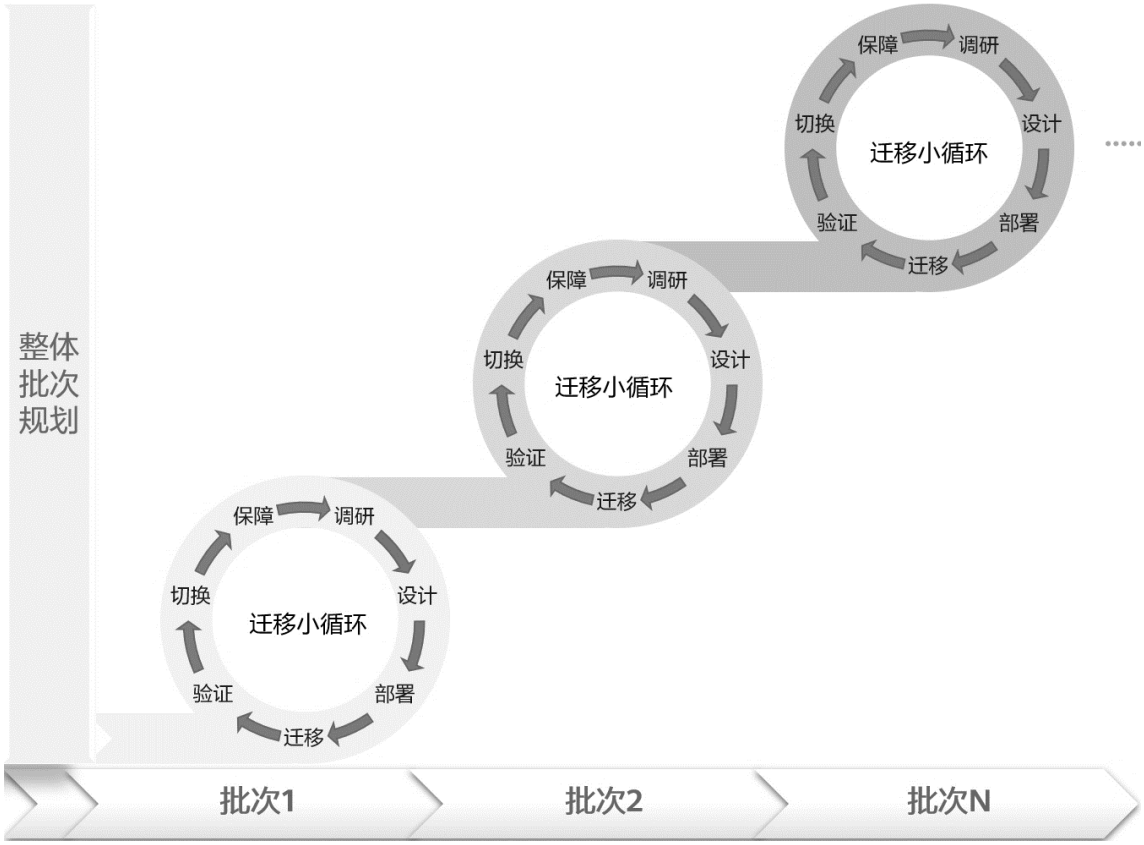
应用上云迁移遵循如下的流程：

图 6-4 应用迁移小循环



上述流程的执行对象是应用迁移分组，一个迁移批次通常包含一个或多个应用迁移分组，需要重复执行上述流程，才能将一个迁移批次的所有应用迁移到云端，如下图：

图 6-5 分批迁移流程



用小循环的每个阶段概述如下：

- **调研：**对应用的技术架构进行详细的调研，详细到具体的技术组件和版本信息。
- **设计：**深度调研结果，给出云上的技术架构和规格选型，输出详细的迁移方案和切换方案。
- **部署：**创建云上资源，上云适配改造（如涉及），并做目标环境测试。
- **迁移：**将源端应用和数据迁移到云上目标环境。
- **验证：**进行数据和业务验证。
- **切换：**进行切换演练，刷新Runbook，实施正式切换。
- **保障：**业务切换后进行一段时间的实时监控和特别运维保障。

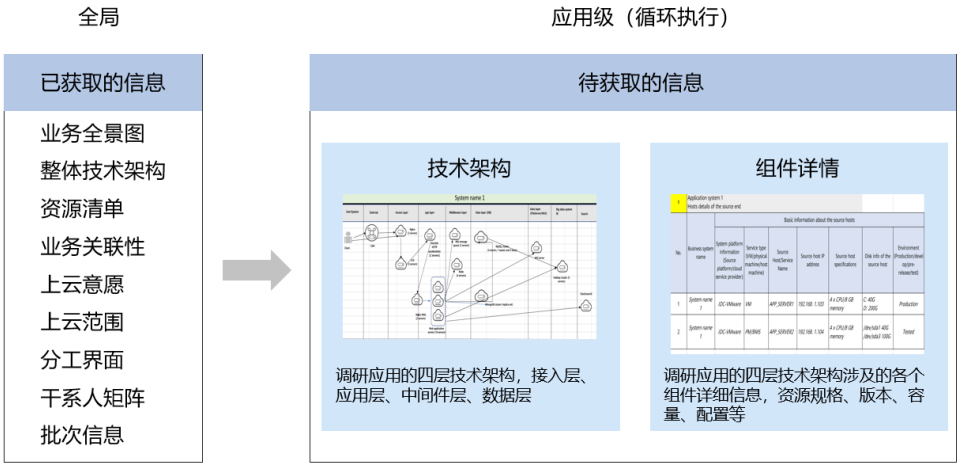
调研

应用迁移小循环需要调研的信息主要集中在单个应用级别，前面阶段获取的调研信息可以复用。

本阶段主要是“由粗到细”打开到能够指导迁移实施的详细程度。

调研方法请参考**应用系统调研**的内容，需要调研的内容包括应用的技术架构、详细的组件信息。

图 6-6 应用调研



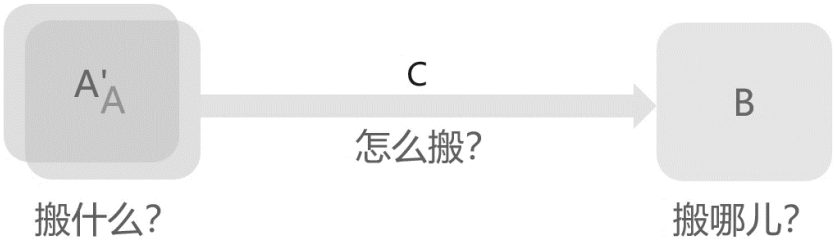
6.4.2 设计迁移方案

6.4.2.1 迁移方案概述

迁移方案概述

应用上云迁移就像一次“搬家”，是围绕迁移源、迁移目标、迁移过程三要素而开展的一系列活动。

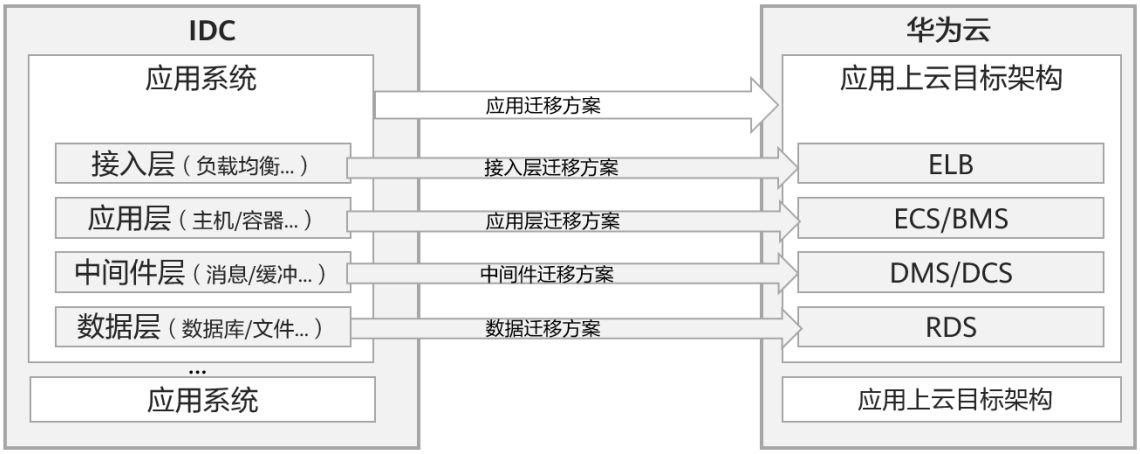
图 6-7 应用上云迁移示意图



在进行迁移方案设计之前，先要参考第5章完成该应用的云上目标架构设计（B），然后设计从A->B的迁移方案（C）。

应用迁移方案要基于应用的四层架构来设计，分别设计每一层的迁移方案，如下图：

图 6-8 应用迁移过程



- **接入层：**通常是负载均衡、网关代理等组件，一般通过重新配置的方式实现迁移。
- **应用层：**通常部署在主机或容器上，部署在主机上的应用一般通过华为云主机迁移工具SMS来迁，部署在容器上的应用，一般通过企业的CICD系统重新发布。
- **中间件层：**通常是缓存中间件和消息中间件。缓存中间件一般通过华为云DCS迁移工具来迁移，消息中间件，一般不迁移，待消费者服务消费完通道内的消息后，整个消息中间件直接切换到华为云。
- **数据层：**包括数据库、对象存储、文件系统，数据库一般通过华为云的数据迁移工具DRS做迁移，对象存储一般通过华为云对象存储迁移工具OMS做迁移，文件系统一般通过Rsync等迁移工具来迁移。

迁移工具兼容性

迁移工具的兼容性以各个迁移工具官网文档发布的最新结果为准：

- **SMS兼容的操作系统清单**
- **DRS兼容的数据库清单**
- **OMS兼容的源端对象存储清单**
- **CDM兼容的数据源清单**

6.4.2.2 接入层迁移方案

接入层为应用的外部访问提供了访问入口，常见的接入层技术4种，分别是Nginx/Openresty、硬件或软件负载均衡器，微服务网关Kong/Zuul、DNS。通常采用重新配置的方式进行迁移，具体如下：

表 6-1 接入层迁移方式

技术组件	功能说明	迁移方式

nginx/ openresty	使用nginx或openresty做流量转发	方案1：使用SMS主机迁移工具将nginx或openresty服务运行的服务器迁移到华为云，并修改对应的转发策略。 方案2：在华为云ECS服务上重新部署nginx或openresty，然后拷贝源端配置文件到目的端，并修改配置文件的转发策略。
负载均衡器	提供4层或7层流量转发	将源端的负载均衡策略重新配置到华为ELB
Kong/Zuul网关等	微服务网关	方案1：使用SMS主机迁移工具将Kong/Zuul网关服务运行的服务器迁移到华为云。 方案2：在华为云ECS重新部署Kong/Zuul网关，然后拷贝源端配置文件到华为云ECS，并修改转发策略
DNS域名解析	解析应用的内外部域名	方案1：使用华为云平台的DNS服务替代源端的DNS，并重新配置DNS解析地址。 方案2：在华为云的ECS上部署DNS服务，并重新配置DNS解析地址。 方案3：使用SMS工具将源端DNS服务器迁移到华为云并修改DNS配置。

6.4.2.3 应用层迁移方案

应用层通常部署在物理机、虚拟机或容器内，应用的类型包括有状态和无状态两种。应用的部署方式和应用状态是应用层迁移方案设计时需要考虑的因素，不同的部署方式和应用状态适用的迁移方案不同。

- **平迁部署在主机上的应用**

  传统架构的应用，通常部署在物理机或虚拟机，建议优先通过华为云SMS主机迁移工具进行迁移；如果无法使用华为云SMS进行迁移的，可以采用应用重新部署的方式；对于可停机迁移的应用，也可以考虑采用镜像导出导入的方式进行迁移，详细方案见下表：

  表 6-2 主机平迁方案

迁移方案	迁移方式	特点	适用场景
使用华为云SMS主机迁移工具迁移（推荐）	全量+增量	1.停机时间短，可持续进行增量同步 2.依赖网络传输，且要求源端操作系统版本在华为云支持列表内	适用于所有源端为x86架构的物理机或虚拟机迁移，有增量数据
华为云ECS重新部署	NA	1.不依赖网络传输 2.相比工具迁移工作量较大	所有

镜像导出导入	全量	1.不依赖网络传输 2.停机时间较长，需要源端物理机或虚拟机停机后，制作完整镜像	停机窗口较长的场景 （停机窗口至少4小时以上才建议考虑此方案）

- **平迁部署在容器中应用**

  部署在容器中应用一般是云原生的应用，通常是微服务架构的应用，可以通过镜像迁移或重新发布两种方式做迁移。

  企业云原生应用系统以微服务架构为主，通常部署在容器中，这种场景，多数企业也同时会拥有自己的开发流水线CI/CD系统，所以，这种场景的应用上云可以使用容器镜像迁移的方式迁移，或者使用CI/CD流水线重新发布的方式迁移。

  表 6-3 容器迁移方案

1. 迁移方案	1. 特点	1. 适用场景
1. CI/CD重新发布（推荐）	1. 操作简单，配置可控	1. 源端具备CI/CD流水线
1. 容器镜像迁移	1. 人工操作，工作量大	1. 所有
1. 容器迁移工具（Velero或E-Backup）	1. 操作简单，可快速还原源端配置	1. 所有

- **主机上的应用容器化上云**

  对于部署在主机上的传统应用，如果要迁移到容器，就需要将传统应用进行容器化改造，将主机上的应用改造成容器镜像，部署到K8S或华为云CCE集群。容器化改造上云，属于应用现代化，具体请参考**应用现代化**。

6.4.2.4 中间件层迁移方案

当前企业业务中使用比较多的中间件类型为缓存中间件和消息中间件。中间件作为数据存储的临时场所，数据一般不用迁移，但在切换时，为了确保源端和目的端数据的一致性，需要等中间件消息队列中的消息完成消费后再切换。如果中间件缓存数据是持久化的，即作为数据库使用，此场景需要进行数据的迁移。所以中间件的迁移方案需结合业务使用情况进行具体分析，下面将详细介绍各类中间件的迁移方案。

- **Redis迁移方案**
- **确定Redis使用场景**

  Redis使用场景主要有2种，将Redis用作缓存或者将Redis用作数据库。不同使用场景的Redis迁移方案不同，详见下表所示。

  表 6-4 Redis 迁移场景

Redis使用场景	**迁移方式**

Redis实例中的数据用作缓存	业务切换时，为防止Redis后端的数据库被击穿，可基于数据库性能判断使用哪种迁移方案： 方案1：不迁移，将Redis缓冲数据提前预热 方案2：使用Redis迁移方案迁移缓冲数据
Redis实例中的数据是持久化的，作为数据库使用	使用Redis迁移方案迁移持久化数据

- **Redis迁移方案**

表 6-5 Redis 迁移方案

迁移方案	迁移方式	特点	适用场景
DCS迁移工具（推荐）	全量+增量迁移	源端业务停机时间短、操作简单、支持在线实时同步增量	适用于源端是自建Redis或其他云厂家Redis实例迁移至华为DCS的场景
RDB/AOF文件备份恢复	全量迁移	离线迁移，操作复杂，源端业务停机时间长，需要源端业务停机后制作RDB/AOF文件，不支持增量同步数据	所有

- **消息中间件迁移方案**
- **确定消息中间件的切换场景**

表 6-6 消息中间件切换场景

适用产品	切换窗口	迁移方式
Kafka RabbitMQ RocketMQ ActiveMQ	切换时间窗充足	切换时间充足，业务评估在切换时间窗口内可以完成消息消费，此时，消息中间件中的数据不需要迁移，等待消费者将消息消费完成即可
	切换时间窗有限	切换时间有限，业务评估在切换时间窗口内无法完成消息消费，请参考消息中间件迁移方案进行消息迁移

- **消息中间件迁移方案**

表 6-7 消息中间件迁移方案

迁移方案	迁移方式	特点	适用场景

开源工具MirrorMaker 2.0	全量+增量	1.部署复杂，操作繁琐 2.支持消费队列offset偏移量的同步	所有
华为云SmratConnect工具	全量+增量	1.工具界面化，操作简单 2.支持消费队列offset偏移量的同步	适用于自建kafka或云服务迁移到华为云kafka

6.4.2.5 数据层迁移方案

数据层主要负责业务数据的持久化，为上层业务逻辑的实现提供数据支持，数据层包括两类数据，结构化数据和非结构化数据。结构化数据包含各类数据库，例如MySQL数据库、MongoDB数据库等，非结构化数据包含对象存储、各类文件存储等。

- **结构化数据迁移方案**

  结构化数据，主要为业务提供即时数据支撑，包含数据查询、计算、分析、修改等操作。业务连续性高的业务，很依赖数据库迁移工具的实时同步能力。在做结构化数据迁移方案时，需要结合业务连续性、迁移网络、业务架构等因素，选择合适的结构化数据迁移方案，做到数据迁移复杂度、数据迁移实时性，业务连续性的平衡。

- **MySQL迁移方案**

  表 6-8 MySQL 迁移方案

迁移方式	迁移方式	特点	适用场景
华为云DRS数据复制服务（推荐）	全量+增量迁移	配置简单，一键迁移，支持实时同步增量数据	1.适用于自建或云服务MySQL实例迁移华为云服务MySQL实例 2.适用于自建或云服务MySQL实例迁移至华为云自建MySQL实例（需先迁到云服务再迁移到自建）
mysqldump导出导入	全量迁移	不依赖网络，操作较为复杂，只能全量迁移，不支持增量数据同步	停服时间窗较长场景
主从复制replication	全量+增量迁移	操作复杂	仅适用于源端和目标端均为自建MySQL数据库，由于源端和目的端版本不兼容等问题无法使用华为云DRS数据复制服务的场景

- **SQLserver迁移方案**

表 6-9 MySQL 迁移方案

迁移方式	迁移方式	特点	适用场景
华为云DRS数据复制服务（推荐）	全量+增量备份导入	工具界面化，操作简单	适用于自建SQLserver实例或云服务SQLserver实例迁移至华为云云服务SQLserver实例
备份与恢复	全量+增量备份导入	操作繁琐	适用于自建SQLserver实例或云服务SQLserver实例迁移至华为云RDS for SQL Server

- **PostgreSQL迁移方案**

表 6-10 PostgreSQL 迁移方案

迁移方式	迁移方式	特点	适用场景
华为云DRS数据复制服务（推荐）	全量+增量迁移	配置简单，一键迁移，支持实时同步增量数据	适用于自建PostgreSQL实例或云服务PostgreSQL实例迁移至华为云自建PostgreSQL实例或RDS for PostgreSQL
pg_dump导出导入	全量迁移	优点：不依赖网络 缺点：操作较为复杂，只能全量迁移，不支持增量数据同步	适用于无法使用华为云DRS数据服务的场景

- **MongoDB迁移方案**

表 6-11 MongoDB 迁移方案

迁移方式	迁移方式	特点	适用场景
华为云DRS数据复制服务（推荐）	全量+增量迁移	配置简单，一键迁移，支持实时同步增量数据	适用于自建MongoDB实例或云服务MongoDB实例迁移至华为云自建MongoDB实例或云服务MongoDB实例
导出导入	全量迁移	不依赖网络，操作较为复杂，只能全量迁移，不支持增量数据同步	适用于无法使用华为云DRS数据服务的场景

- **非结构化数据迁移方案**

  非结构化数据是数据结构不规则或不完整，没有预定义的数据模型，不方便用数据库二维逻辑表来表现的数据。包括所有格式的办公文档、文本、图片、XML、HTML、各类报表、图像和音频/视频信息等等。当前企业业务中承载非结构化数据的存储方式主要为文件存储和对象存储。

- **NAS迁移方案**

  表 6-12 NAS 迁移方案

迁移方案	迁移方式	特点	适用场景
华为云CDM服务 （海量数据迁移推荐）	全量+增量	操作简单，支持增量迁移。对海量数据支持更好	适用于将源端对象存储、网络文件存储，大数据存储迁移至华为云OBS对象存储、华为云SFS弹性文件存储、华为云大数据存储中的海量数据迁移。
开源工具rclone/rsync	全量	rclone配置复杂；rsync迁移效率低	适用于华为云FMS工具和华为云CDM服务无法使用时的迁移场景。

- **对象存储迁移方案**

  表 6-13 对象存储迁移方案

迁移方案	迁移方式	特点	适用场景
华为云OMS服务（推荐）	全量+增量	操作简单，高并发，支持数据校验、可视化报告	适用于将源端对象存储迁移至华为云OBS对象存储。
开源工具rclone/rsync	全量	rclone配置复杂；rsync迁移效率低	适用于华为云OMS服务无法使用时的迁移场景。

6.4.3 设计切换方案

6.4.3.1 如何选择停服不停服

业务切换是整个上云迁移的关键环节，出问题会直接影响企业业务，不同业务对停服的要求是不一样的，比如，有些业务在切换期间是不允许停服的，停服会造成较大的业务损失；有些业务在切换期间是允许停服的，比如办公OA系统，夜间非工作期间可以停服；有些业务系统，为了更好的客户体验，希望切换期间部分浏览类的业务继续提供服务，只是涉及写操作的业务受到影响。设计切换方案时，对于不同的业务场景和停服要求，会面临多种方案的选择，下面详细介绍如何合适的切换方案。

业务系统从源端切换到目的端，切换方案可以分为3类，即停服切换、停写不停读切换和不停服切换。每类切换方案优缺点具体如下表：

表 6-14 切换方案比较

切换类型	方案说明	数据一致性风险	业务改造投入	停服时长（小时）	
				读	写
停服切换	最常用的切换方式，停止服务切换能重复保证数据一致性	低	低	0.5~3.5	
停写不停读切换	较少用的切换方式，需要业务整改来实现停写不挺读，停止写服务切换能充分保证数据一致性	低	中	不停	0.5~3.5
不停服切换	很少用的切换方式，需要业务整改来实现双写或者双向同步，不停服切换需要业务改造来保证数据一致性，复杂度和难度较高	高	高	不停	不停

所以3种切换方案各有优缺点，不存在风险小、投入少、中断时间短的完美方案，企业需根据业务场景、停服要求和投入产出选择合适的方案。关于如何选择停服不停服，您可以从以下几个方面考虑：

1. **根据行业选择**

不同行业有各自的行业标准和要求，例如部分电商零售行业，在凌晨后，交易数量大幅度减少，甚至没有交易，停服后也不会造成重大社会影响，可以在凌晨后使用停服切换方案。而部分交通出行行业，全天24小时有业务，并没有明显的业务低峰期，停服会造成较大的业务损失，可能需要选择不停服切换方案。

1. **根据业务重要程度选择**

有些业务，例如游戏业务、金融业务，重要程度高，属于核心业务，又需要24小时提供服务，所以要选择不停服切换方案。其他业务，例如OA、运营等非核心业务，停服造成的业务损失可接受，就可以选择停服切换方案。

1. **根据项目周期选择**

业务不允许停服，如果上云周期较长，时间充足，且企业具备不停服的改造能力，可以选择进行双写改造，实现不停服切换。如果上云周期紧张或企业没有太多人力投入上云工作，建议选择改造量少、人力投入少的停服切换方案。

1. **根据投入产出选择**

不停服切换方案通常需要研发额外投入进行大量的应用改造才可以实现，停服切换方案则通常无需大量改造，研发投入工作量小。因此，投入产出也是切换方案选择的决策依据之一，企业可以在业务影响所造成的损失跟研发改造所产生的成本之间找到一个合理的平衡。

6.4.3.2 停服切换方案

停服时长评估

基于华为云的迁移经验，切换期间大部分应用停服时长在0.5小时~3.5小时，下面停服时长可供参考：

表 6-15 停服时长分析

上云迁移停服时长评估								
总停服时长（36~211分钟）								
源端停机（12~75分钟）			增量数据同步及校验（6~40分钟）			目的端拉起（18~96分钟）		
目的端拉起（18~96分钟）	时长（分钟）	缩短时长的方法	增量数据复制	时长（分钟）	缩短时长的方法	目的算业务拉起	时长（分钟）	缩短时长的方法
接入层流量入口关闭（网关/ELB）	1~5	1、通过API接口调用或脚本批量操作，减少操作时间	最后一次增量同步	1~10	1、在业务低峰进行切换，减少增量数据	数据库开启写	1	1、脚本开启
应用层停服（关停应用）	1~30	1、提前关停非核心业务，减少操作量 2、统一运维批量关停，减少操作时间 3、统一日志平台，减少应用日志检查时间	数据校验	5~30	1、开启工具的动态校验功能，减少校验时间	应用启动	1~30	1、统一运维平台，批量关停，减少操作时间 2、统一日志平台，减少应用日志检查时间

上云迁移停服时长评估								
中间件层停服（消息消费完）	5~30	1、提前关停非核心业务，减少消息量 2、统一监控平台，减少检查时间	-	-	-	应用测试	15~60	1、测试用例自动化 2、只测试核心测试用例
数据层停服（停写检查）	5~10	1、统一监控平台，减少检查时间	-	-	-	流量切换	1~5	1、通过API接口调用或脚本批量操作，减少操作时间

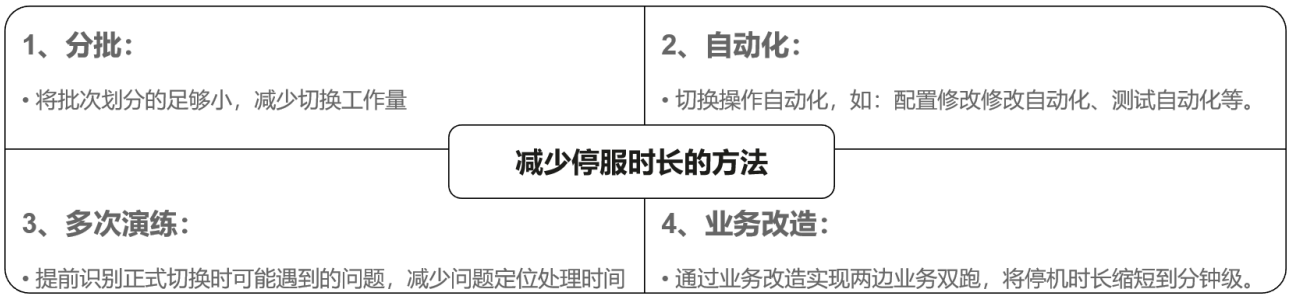
停服时长例外情况

1. **停服时长小于30分钟：**若停服时长要求小于30分钟，可以通过分批迁移，划分较小的批次或者采用分层切换（比如先切应用层再切数据层）的方式，且所有操作都脚本化/工具化，停服时长也有可能小于30分钟。
2. **停服时长大于3.5小时：**迁移规模和数据量大、业务关联关系复杂无法分批、切换Runbook操作复杂且自动化程度不高，停服时长可能大于3.5小时，有的甚至8~10小时。比如某大型企业600+微服务，100+个中间件，80+数据库，1000+个批处理任务，4000+个测试用例，停服时长约8个小时。

减少停服时长的方法（分钟级）

停服时长与多个因素有关，企业可以通过分批+自动化+多次演练+业务适配改造，来减少停服时长。下图是四种减少停服时长的方法：

图 6-9 减少停服时长的方法



四种停服切换方式

表 6-16 四种停服切换方式

切换方式	适用场景	停服时长	停服次数	影响范围
一把切（应用层和数据层整体停机后切换）	适用于停机窗口较长、无法清晰梳理应用之间和应用与数据层之间关联关系的业务	长	1	全部业务
分3~4次切换，应用层先灰度切流（1%，30%，…100%），然后停机，数据层整体切换，再将内外部域名切换到目的端	适用于停机窗口较小，业务可接受短时间的跨云访问，跨云带宽和时延评估可以满足业务需求。	中	1	全部业务
分5~10次切换，应用灰度切流（1%，30%，…100%），然后数据层分批次切换（比如：第一批缓存+数据库，第二批缓存+数据库，第三批中间件消息队列等）	适用于停机窗口较小，业务可接收短时间的跨云访问，跨云带宽和时延评估可以满足业务需求，且切换多次对内外部影响可控。	短	多次	部分业务
按照业务域分批切	适用于业务域相对独立，关联关系简单，可独立拆分上云。	短	多次	部分业务

一把切（应用层和数据层整体停机后切换）

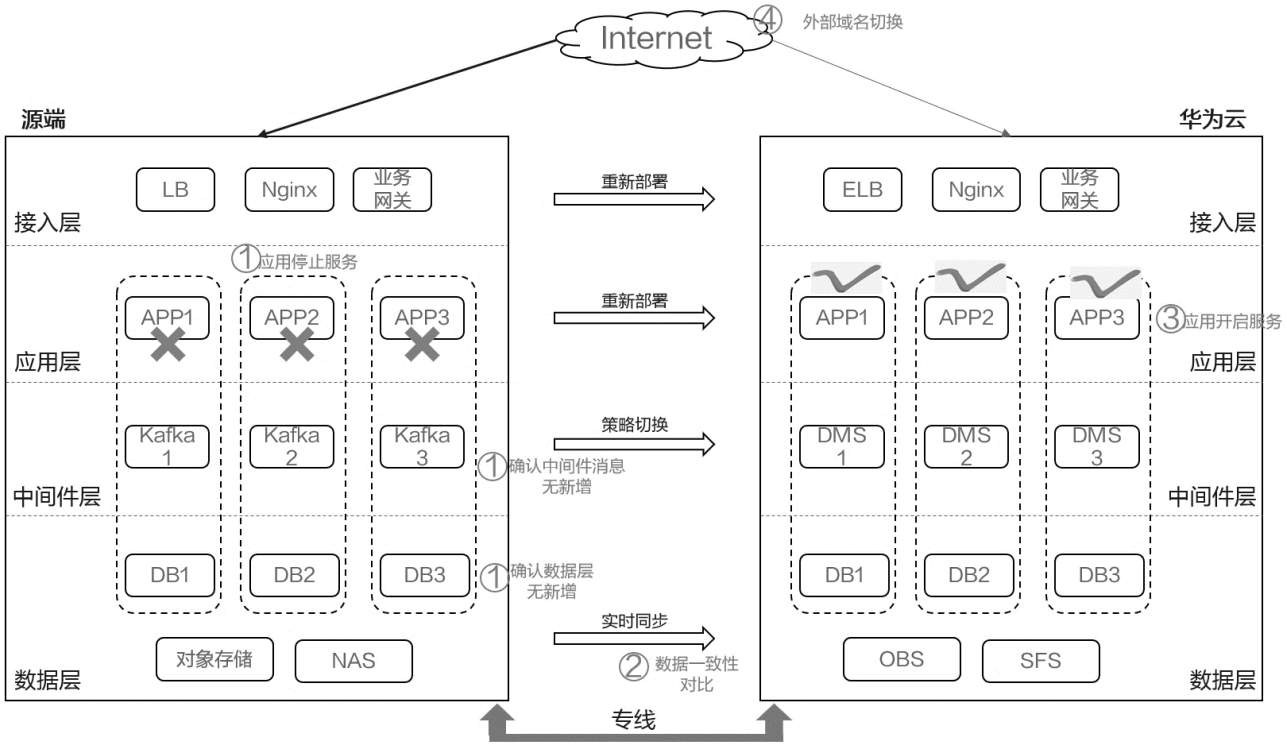
准备工作：

1. 源端应用和数据已迁移到华为云；
2. 华为云应用层和数据层已完成业务功能和性能验证，可正常使用；

业务切换：

1. 停止源端应用层和批处理任务，使源端不再产生新增数据，检查中间件消息无新增，检查数据层无新增；
2. 源端数据层和华为云数据层增量同步完成，并完成数据一致性对比，断开同步链路；
3. 华为云上的应用层和数据层内部域名等配置修改，重启华为云上的应用服务；
4. 外部DNS域名解析，将解析地址从源端接入层切换到华为云接入层，使外部流量进入华为云；

图 6-10 一把切方案



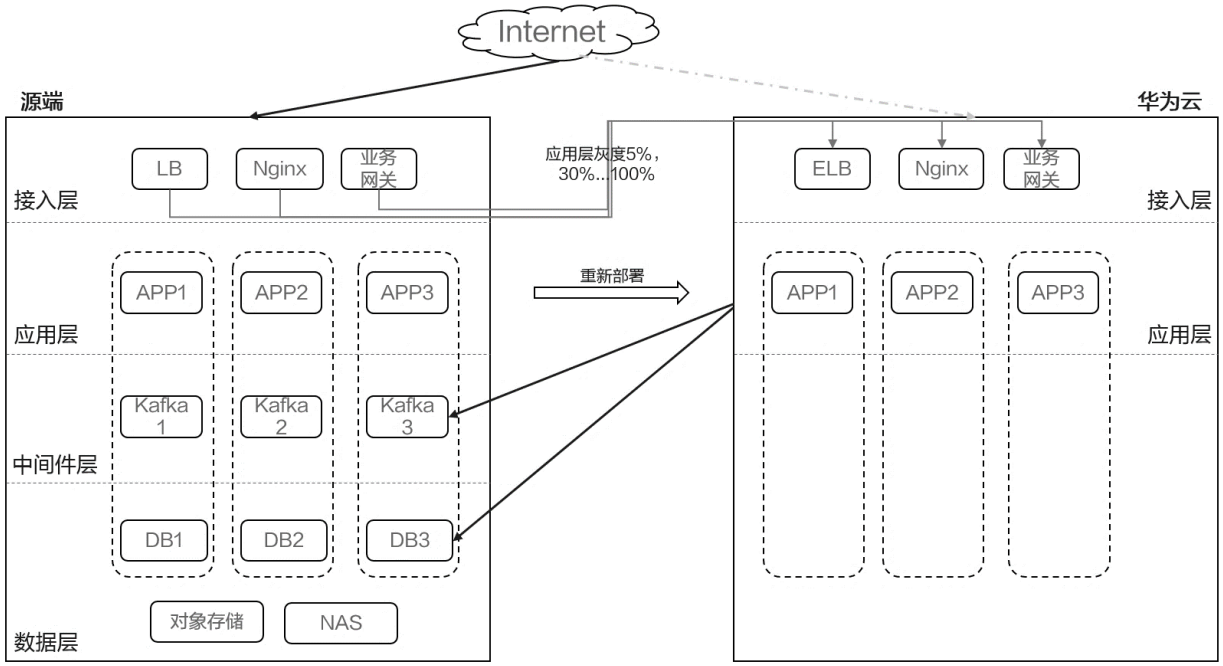
应用层灰度切流，数据层整体切换

应用层灰度切流前做好如下准备工作：

1. 源端应用层已迁移或部署到华为云；
2. 华为云应用层跨云访问源端数据库，已完成业务功能和性能验证，可正常使用。

准备工作完成过后，从源端接入层引流，按照1%~30%，…100%逐步加大流量的方式，流量逐步灰度切换到华为云接入层。

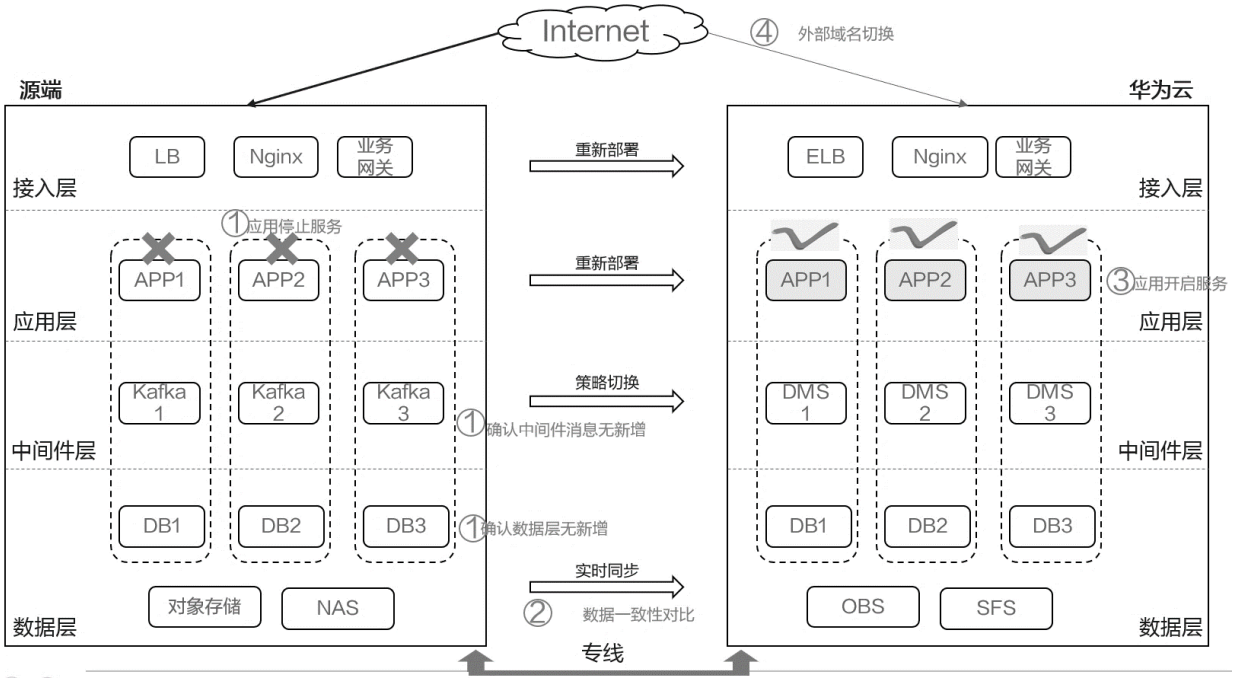
图 6-11 应用层灰度切流



接下来进行数据层整体切换，步骤如下：

1. 源端和目标端的应用层和批处理任务停止服务，防止新数据写入，此时业务无法使用；
2. 等中间件消息队列中的消息消费完成，数据层增量同步到华为云，对比源端和目标端数据层数据一致性；
3. 修改配置，将华为云应用层指向华为云数据层，启动应用服务；
4. 外部DNS域名解析，解析地址从源端切换到华为云，流量进入华为云。

图 6-12 数据层整体切换



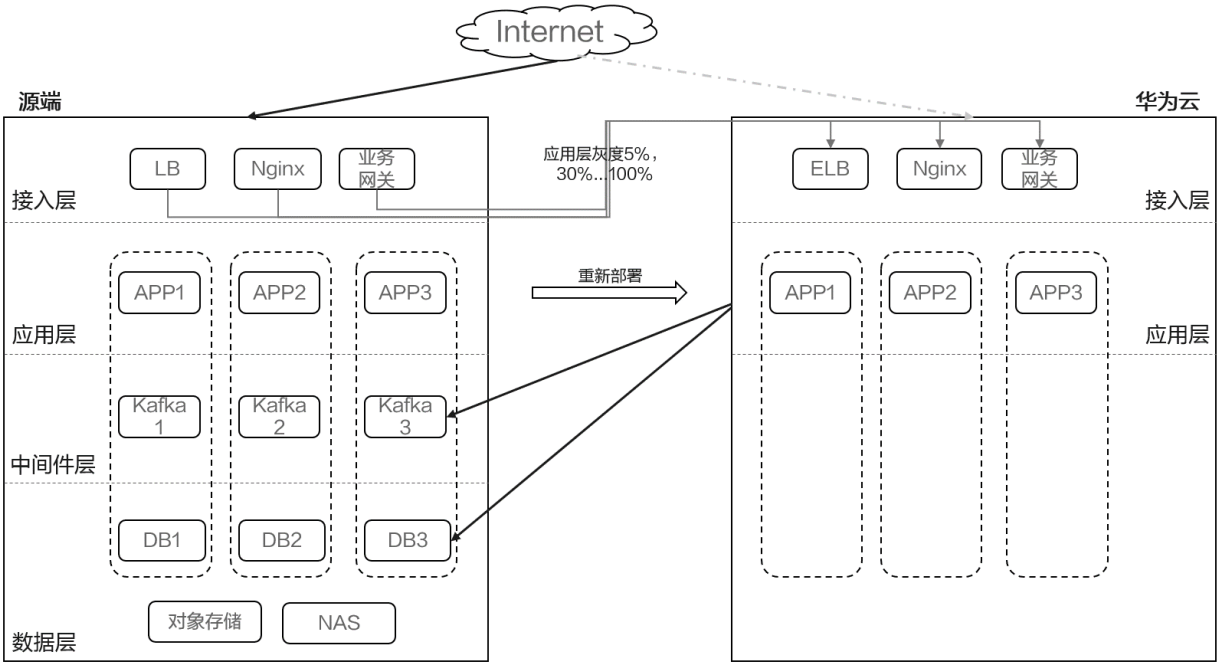
应用层灰度切流，数据层分批切换

应用层灰度切流前做好如下准备工作：

1. 源端应用层已迁移或部署到华为云；
2. 华为云应用层跨云访问源端数据库，已完成业务功能和性能验证，可正常使用。

准备工作完成过后，从源端接入层引流，按照1%~30%，…100%逐步加大流量的方式，流量逐步灰度切换到华为云接入层。

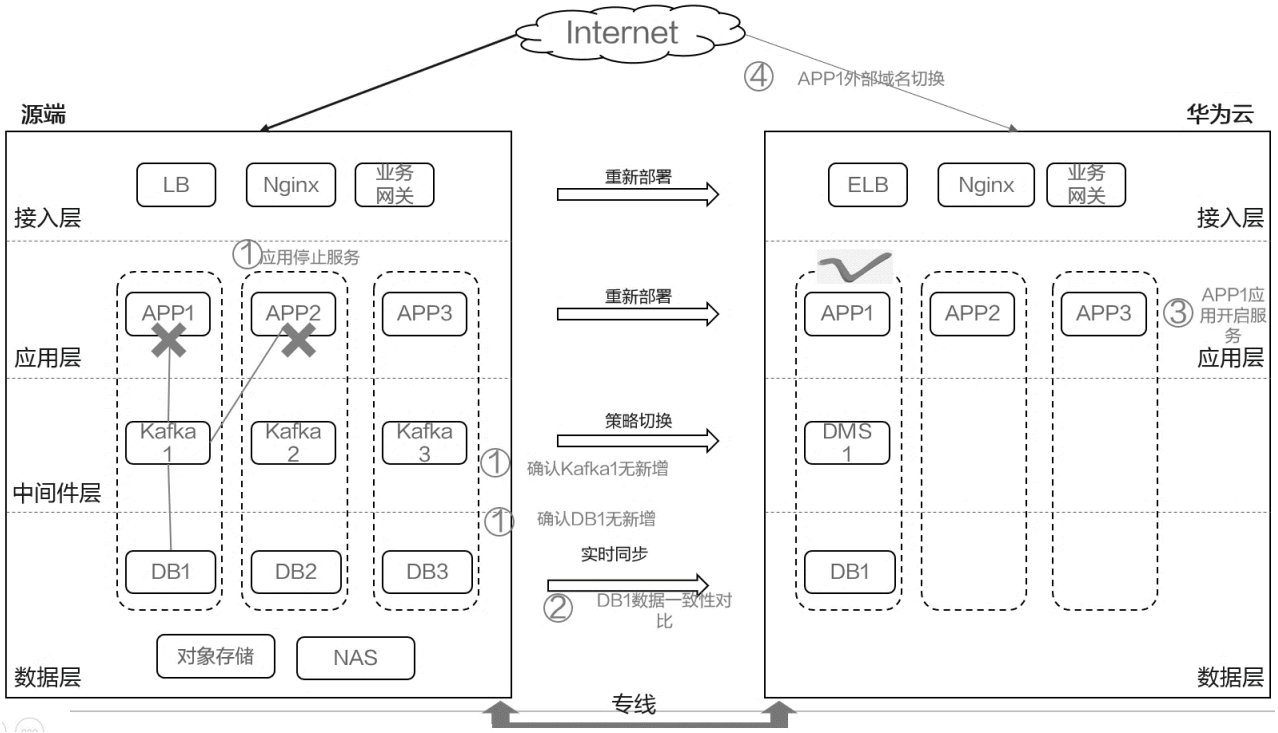
图 6-13 应用层灰度切流



接下来进行数据层分批切换，某批次数据层切换步骤如下：

1. 停止本批次数据层相关的应用和批处理任务。本批次的数据层静止（中间件消息队列中的消息消费完成，数据库无新增数据）；
2. 数据对比一致后，切换数据层；
3. 修改相关的配置，启动和本批次数据层相关的应用和批处理任务。进行功能验证及保障，确保业务正常；
4. 某批次应用（如APP1）的外部DNS域名解析，解析地址从源端切换到华为云，流量进入华为云。

图 6-14 数据层分批切换



该方案的优点如下：

1. 应用切换阶段操作简单，引流阶段只调整网关流量权重和负载均衡流量权重即可；
2. 网关、负载均衡灰度引流，一旦有问题，随时可以把流量切换回原环境；
3. 应用切换阶段，应用不需要停止，可正常访问；数据层切换阶段，仅需要部分应用停止写入，但可以读；
4. 数据层单次只切换部分节点，操作较少。只需要部分业务停机，其他业务可以正常使用。

   该方案的缺点如下：

5. 需要应用层和数据层梳理，需要花费大量人力和时间；
6. 跨云后，数据层回退难度较大；
7. 跨云阶段依赖专线、如果有大量数据需要跨云访问，可能会造成业务延迟。

按照业务域分批切换

准备工作：

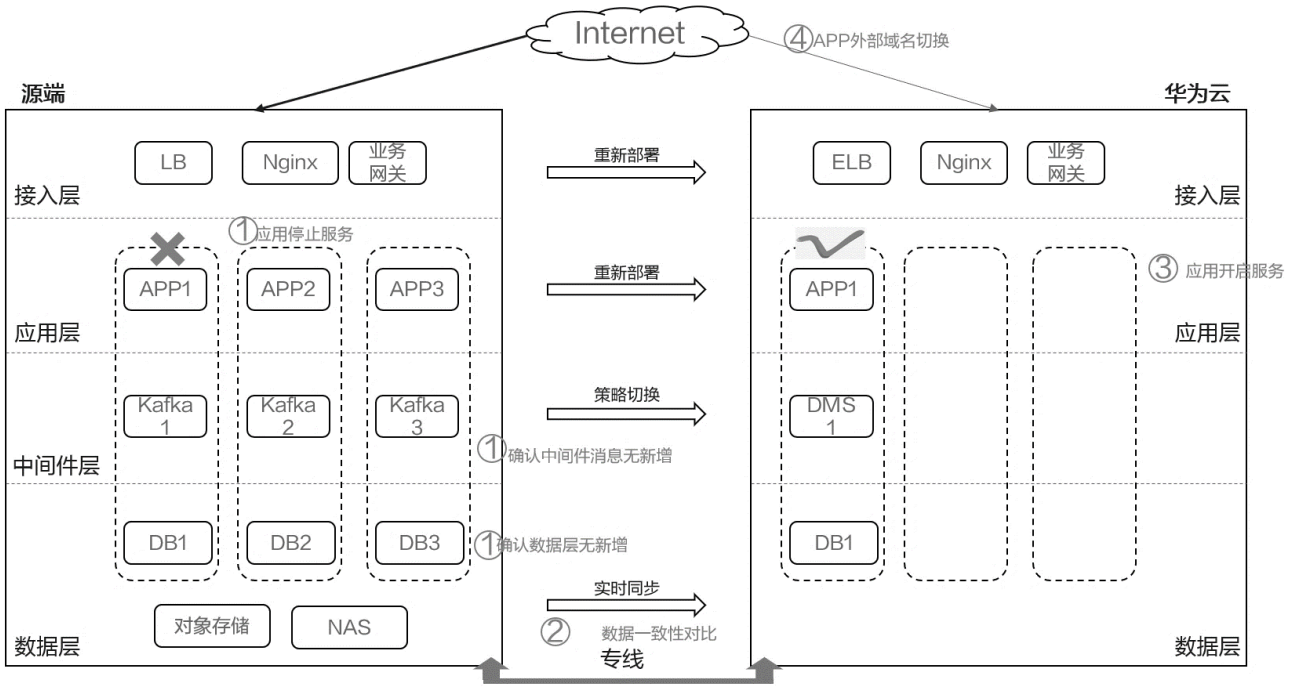
1. 本批次要切换的业务域如X业务已完成部署及迁移；
2. 本批次要切换的业务域已内部通过功能和性能验证，可正常使用。

本批次业务域切换步骤：

1. 停止源端业务域1对应的应用层和批处理任务等，使其不再产生新增数据；停止和本业务域共用中间件和数据库的应用和批处理任务等，使其不再产生新增数据；
2. 检查本批次要切换的中间件和数据层无新增数据，数据对比一致后断开同步链路；

3. 修改目的端的相关配置；启动目标端业务域1对应的应用服务和批处理任务；启动源端和其共用中间件和数据库的应用服务和批处理任务；
4. 域名切换到华为云，进行功能和性能验证，确保业务正常。

图 6-15 按业务域分批切



6.4.3.3 停写不停读切换方案

停写不停读，主要指切换期间，为了追求较好的用户体验，保持一部分读的服务不停服，保持在线可使用状态；为了保持数据一致性，写的服务仍然采用停服方式进行切换。从业务对外体验上，多数用户感知不到停服的影响，比如某购物平台，用户仍然可以浏览商品，但是不能下单，下单时可友好的提示：系统正在升级中，预计凌晨4点恢复，请您稍后重试下单等。

1. **四种停写不停读切换方案对比**

停写不停读切换有4种方案可以选择：

表 6-17 四种停写不停读切换方式

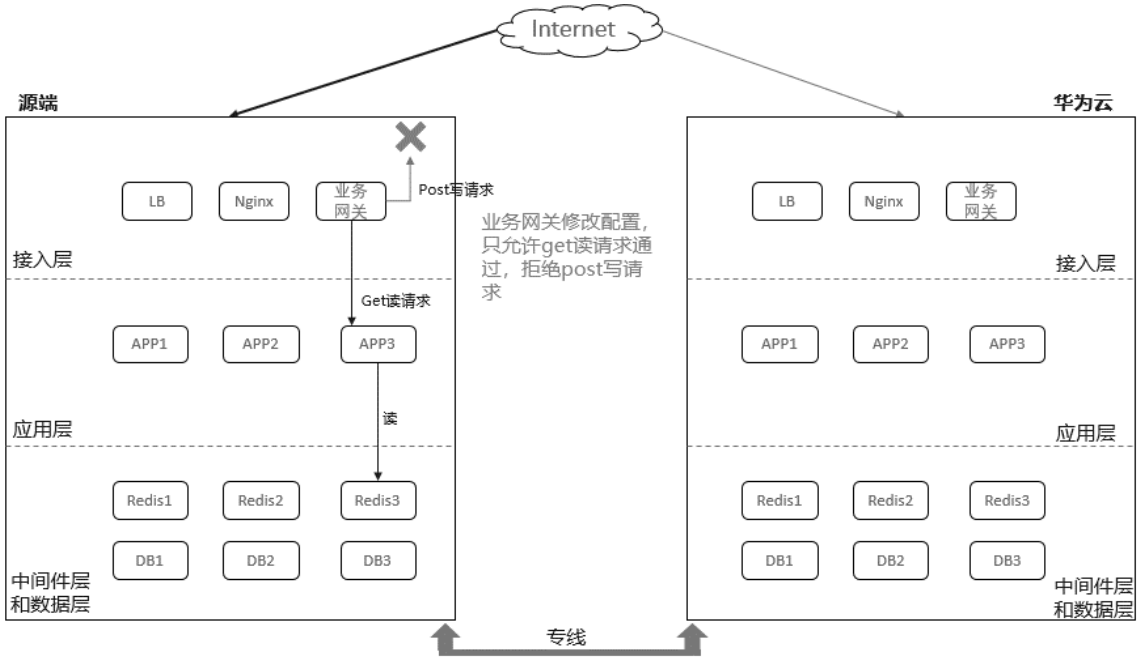
方案	操作方式	适用场景	操作复杂程度	改造工作量
网关拦截	接入层，服务网关拦截写请求，放通读请求	入口统一，有统一网关，网关具有拦截能力，并对拦截的接口能配置友好的提示。	简单	无需改造
停止写服务，读服务不停	写服务或对应接口shutdown，读服务或对应接口保持alive	应用层服务已做读写分离场景，每个服务只进行单独的读操作或写操作，没有同时进行读写的服务	简单	无需改造

方案	操作方式	适用场景	操作复杂程度	改造工作量
应用层先做读写分离改造，然后停止写服务，读不停	应用层修改代码，拆分读写服务	应用层服务没有读写分离的场景	复杂	大
中间件层/数据层直接回收写权限	中间件层/数据层设置业务账号只读，收回写权限	直接回收写权限，业务系统会报错，需要做相关轻微改造处理这些报错	简单	轻微改造

- **网关拦截**

  服务网关（Gatekeeper、Zuul、Kong等），拦截写请求，放通读请求；例如Gatekeeper网关可以拦截POST请求，只放通GET请求。这可以通过在Gatekeeper网关上配置规则来实现。可以设置一个规则，只允许GET请求通过，拒绝POST请求。

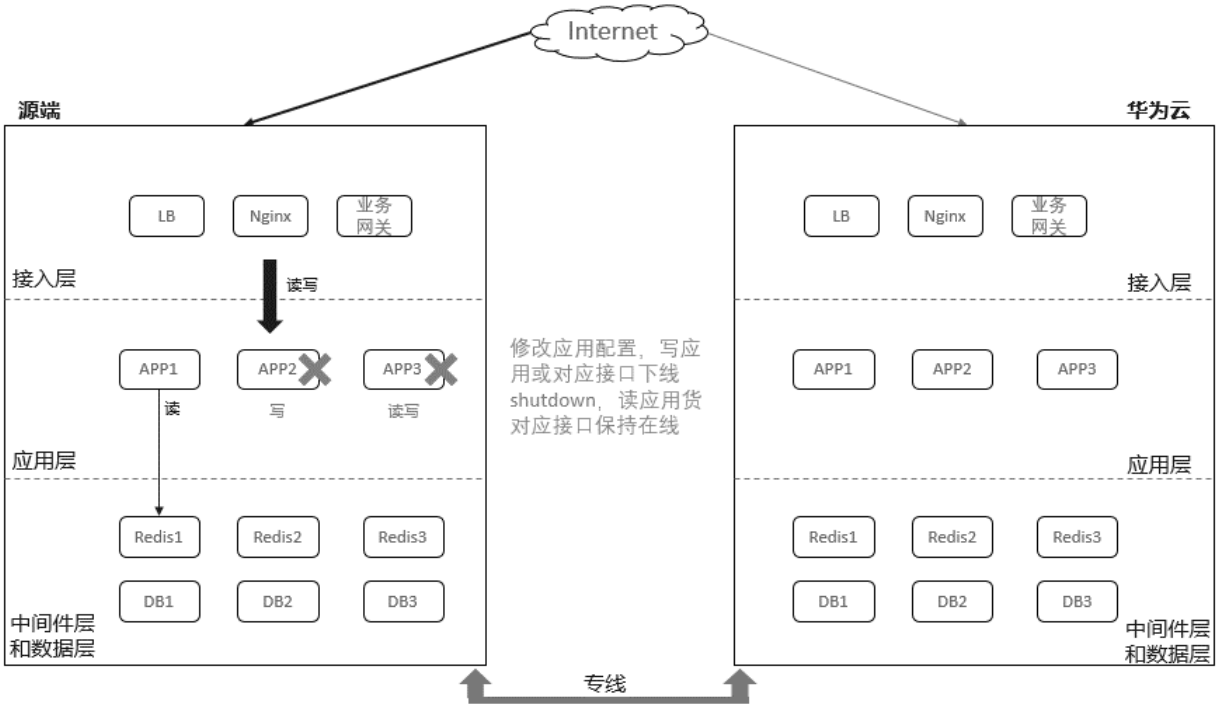
图 6-16 网关拦截方案



- **写服务关停**

  应用层服务已做读写分离的场景，直接关停写服务或对应接口下线shutdown，读服务或对应接口保持在线，从而达到业务只读不写的效果。

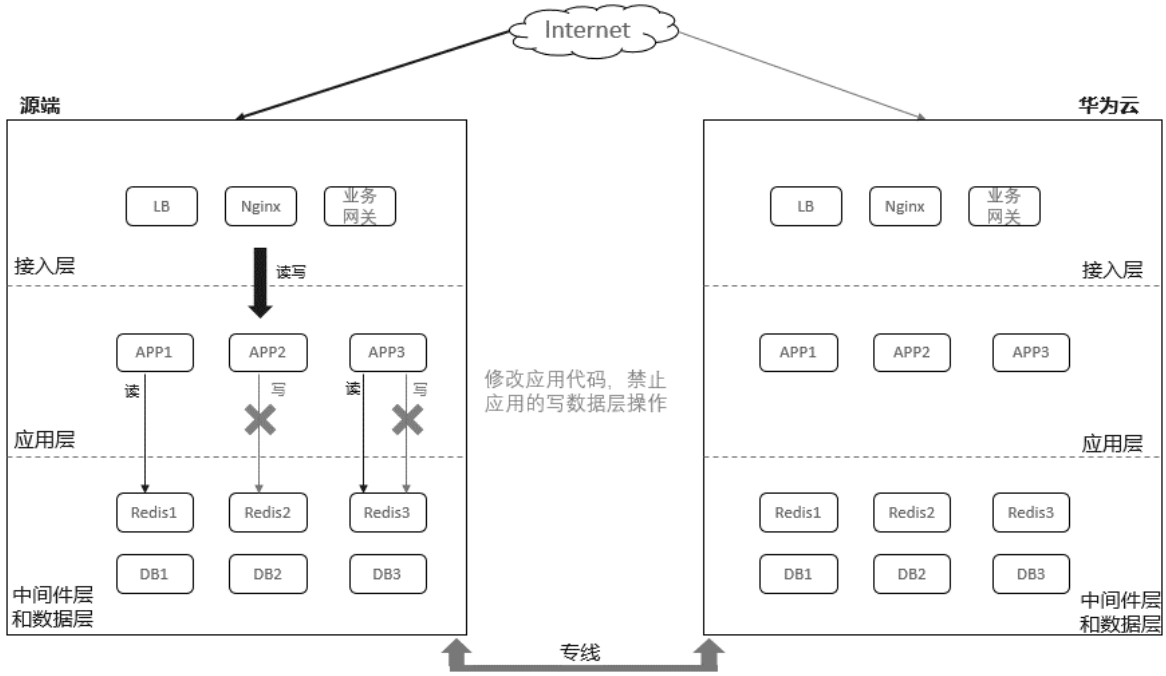
图 6-17 写服务关停方案



- **应用改造**

  应用代码进行读写分离改造，改造后再按照8.4.3.3写服务关停方案实施，实现只读不写的效果。

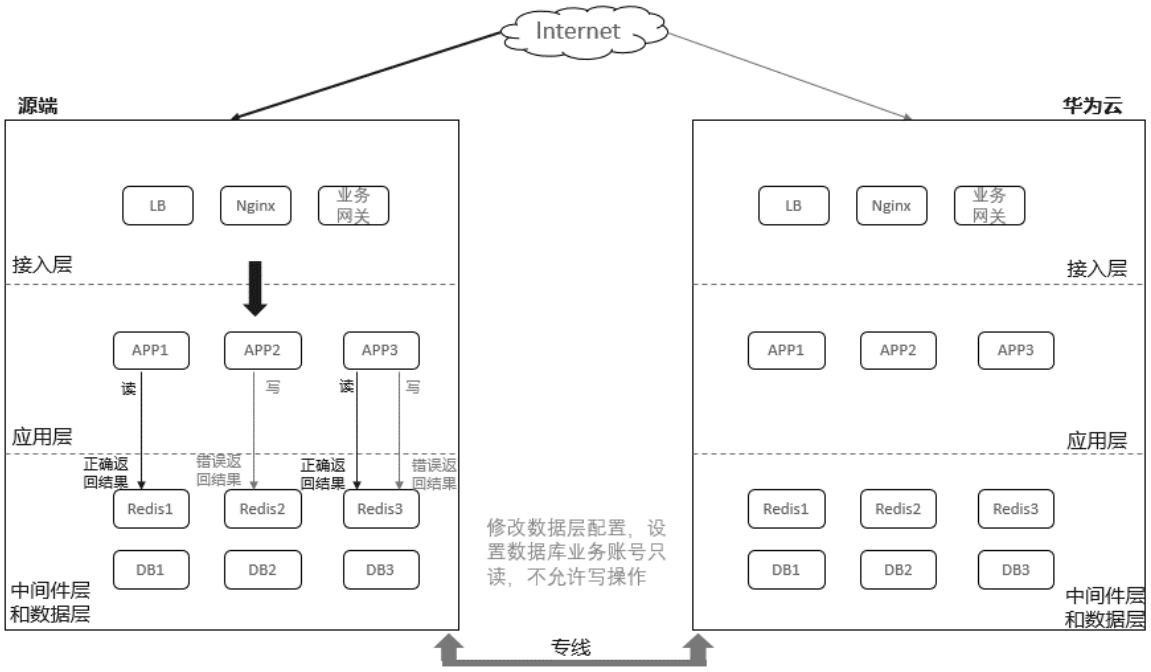
图 6-18 应用改造方案



- **中间件层/数据层配置只读**

  中间件层和数据层收回业务账号写权限，不允许服务写中间件层/数据层的操作。

图 6-19 中间件和数据只读方案



6.4.3.4 不停服切换方案

- **应用层切换不停服方案**

  若只涉及到应用层的切换，可参考章节 **停服切换方案** 中提到的应用灰度切流方案，切换期间不停服。

- **数据层或应用整体切换不停服方案**

  准备工作：

  a. 华为云应用层和数据层已完成迁移；

  b. 华为云应用层和数据层已完成业务验证，可正常使用。

  业务切换：

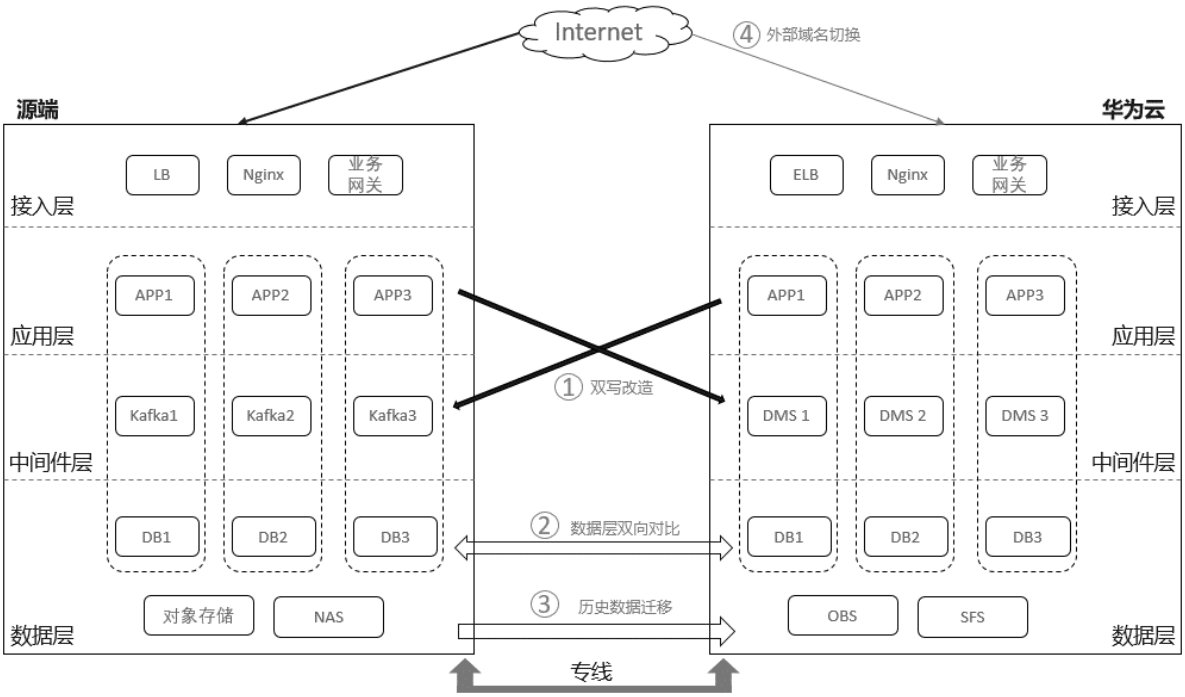
  a. 修改两边的配置，使源端应用层指向源端和目标端的中间件层/数据层，目标端的应用层指向源端和目标端的中间件层/数据层，实现双写。注意：双写的数据一致性由应用逻辑保障；

  b. 实时对比源端和目标端数据一致性；

  c. 历史数据迁移至华为云数据层；

  d. 修改外部DNS域名解析地址，将外部流量从源端切换到华为云。

图 6-20 不停服切换方案



6.4.4 设计 Runbook

6.4.4.1 Runbook 设计原则

Runbook是上云迁移过程中一个非常重要的文档，用于指导切换当天多人协同进行切换操作，规定了业务切换的流程和详细步骤。Runbook主要包括两部分，Runbook checklist和Runbook操作步骤，下面将从几个方面详细介绍如何设计切换Runbook。

Runbook设计原则如下：

- 一个Runbook对应一次切换操作。
- Runbook要详细描述切换步骤、操作人、确认人，并预估开始时间、结束时间、执行时长。
- Runbook执行步骤要尽量细化，确保每个执行步骤对应1个操作人和1个确认人，尽量避免发生1个步骤多个人确认的场景。
- Runbook要细化到每个执行命令，尽量脚本化或工具化，操作人直接执行即可，不需要现场临时定制，避免出现人为事故。
- Runbook步骤中有并行操作和串行操作，要标记好串并行顺序，避免人为操作不当影响切换时长和切换结果。
- Runbook的每个切换操作都可能会执行失败，要提前分析每个步骤发生执行失败时的决策项，细分失败场景，决策是回退还是继续进行，防止切换当天决策组讨论时间较长，无法决策的情况发生。

回退决策点设计原则如下：

- 每个切换阶段设计最晚的执行完时间，超时需要决策是否进行回退。
- 核心表数据比对结果不一致，需要决策是否回退。

- 核心的P0测试用不通过，需要决策是否回退。
- 性能验证不达预期，需要决策是否回退。

6.4.4.2 Runbook 角色设计

Runbook通常涉及如下角色，职责如下：

表 6-18 Runbook 角色与职责

角色	职责
操作人	按Runbook执行相应的操作步骤，并负责操作异常问题处理
确认人	确认操作人的操作步骤是否正常执行完成，并向引导人反馈执行结果，如遇异常，需要按Runbook约定要求，定期向引导人员同步处理进展。
引导人	引导Runbook的执行，通报问题处理进展
记录人	刷新Runbook的执行状态，记录Runbook中各个步骤的完成时间，记录问题处理时长
决策组	由决策组负责人牵头对“决策点”进行决策
会务组	负责维护现场秩序，提供切换期间的会务保障。

说明

- 每一行执行步骤都对应一个操作人和一个确认人（如涉及多人确认的情况，可以通过共享文档由多个分项确认人在线刷新确认进展）。
- 引导人通常是1~2个，是整个切换的总指挥（对于大规模切换，参与人员多，操作时间长的场景，也可以设计2~3名引导人，互为备份），引导人需要对整个Runbook非常熟悉，尤其对于每个步骤执行时序，多个步骤的并行情况要熟悉。

6.4.4.3 Runbook Checklist 设计

Runbook Checklist记录了正式切换前需要准备和执行的操作，通常包括如下几个方面：

- **人员和场地准备**
  a. 核对参与切换人员，并通知，包括内部人员和第三方配合人员通知和时间核对。
  b. 建立切换保障群，切换期间在保障群里进行切换相关公告和通知。
  c. 确定切换的具体日期、入场签到时间、操作开始时间。
  d. 切换场地的准备，如预约会议室，准备相关的物料（电脑、插排、投屏等）。
  e. 工具、终端和登陆平台准备，切换涉及的人员需提前检查使用的工具、平台是否可用，如堡垒机账号权限是否正常，测试终端（测试手机、电脑）是否可用等。
  f. 提前通知相关人员发布官网公告，若涉及到第三方的官网公告，需要提醒第三方进行官网公告发布。

- **应用清单核对和操作脚本刷新**

  a. 上云迁移期间，企业的软件版本开发、迭代发布通常还在正常进行，所以在切换前需要进行一次环境详细清单的核对，包括应用清单和JOB任务等。

  b. 清单核对完成，通知版本封版，避免正式切换时环境和准备时的不一致情况。

  c. 根据最新的应用清单和JOB任务清单，刷新Runbook中相关的切换操作脚本。

- **环境检查**

  切换前需确保源端、目的端、迁移任务状态正常，执行脚本准备就绪。

  a. 源端检查：首先，检查是云专线同步带宽是否有超带宽的告警，评估是否需要进行带宽的扩容，其次，对源端应用和数据库进行告警监控等的观测，确保源端告警清理，状态均正常。

  b. 目的端检查：通知云厂家进行资源日常状态的巡检和高可用性检查。另外目的端切换后就是正式生产环境，要确保告警、监控、日志、安全策略均已完成配置并做最后一次检查和确认。

  c. 正向迁移任务的状态检查：系统切换前通常迁移任务已经创建完成，并在增量同步状态中，确保迁移任务的增量同步状态正常，无异常报错或告警。

  d. 反向迁移任务的状态检查：数据层或中间件通常要考虑回退的链路，切换之前同时要检查反向迁移同步任务的状态，确保无异常报错或告警。

  e. 参数一致性检查：核对源端参数和目的端云服务参数的一致性，如数据库的字符集一致性，数据库的用户名等一致性等。

6.4.4.4 Runbook 操作步骤设计

Runbook中的每一步操作，都有明确的操作步骤、操作命令/脚本、串/并行标记、操作人、确认人、预估开始时间、结束时间、预估执行时长。切换方案不同，对应的Runbook的操作步骤也不同。切换方案可以分停服切换和不停服切换。不停服切换方案对应用架构的要求比较高，通常需要对应用架构进行大规模改造，所以业界普遍采用的切换方案是停服切换。下面以停服切换为例，介绍Runbook设计的注意事项。

- **设计正向操作步骤**

  依据切换方案，将正向切换步骤细化到文档中，需要考虑到以下几个方面：

  a. 停服之前需挂停服公告，充分考虑用户感知。

  b. 停服操作需考虑系统的可用性机制，部分系统检测到应用停止会有自动拉起功能，所以需先关闭可用性机制，防止出现应用一直无法停止的风险。

  c. 数据库切换时需要考虑数据一致性问题，要想切换前后数据一致，必须源端的数据先静止，然后断开增量同步任务，数据一致性对比方案需详细规划，是做行数对比还是做内容对比，不同对比方式对比时长不同，需根据表的重要性和切换时长综合考虑来确定数据一致性对比方案。

  d. 源端数据静止，除了停止应用外，还要考虑批处理任务和消息队列中的消息消费情况等。

  e. 应用和定时任务的启停经常有顺序，需梳理应用和批处理任务的启停顺序，避免启动顺序不当造成业务影响。

  f. 由于公网DNS的域名解析有缓存功能，所以通常会出现虽然系统已切换到目的端，但是仍然有访问流量转发到源端的场景。所以Runbook步骤需要考虑公网DNS缓存问题，建议保留一段时间源端到目的端的转发路径，并持续观测一段时间后，再切断此转发路径。

- **设计回退操作步骤**

  在切换过程中，出现严重问题无法短时间解决的必须进行回退，以恢复到切换之前的状态，避免对业务造成不可逆的影响。以下是设计业务回退步骤的关键点：

  a. 正向操作的每个步骤操作失败都可能导致回退，所以回退的可能场景会比较多，每个可能的回退场景均需考虑。

  b. 回退操作从整体上可以分为有损回退和无损回退。在目的端产生新数据之前的回退都可以是无损的，数据可恢复到切换前的状态。若目的端产生新数据，又无法将目的端的新数据反向同步到源端，则就是有损的回退，此时回退会造成一定的数据丢失。要想在目的端已产生新数据场景下采用无损回退，必须建立目的端到源端方向的数据同步任务。

  c. 对于较大规模场景的业务应用，回退还会涉及到全量回退还是部分回退。采用全量回退还是部分回退，需结合业务影响进行判断和决策。比如当天同时切换了10个应用系统和10套数据库，若某一套数据库切换失败是全量回退还是只回退这1套数据库，判断依据需要业务部门评估应用跨云访问数据库和应用之间跨云访问时延是否满足要求等。

总之，在设计切换Runbook时，要充分考虑回退操作，制定合理的回退方案和步骤，明确操作人员，并在执行过程中严格按照规定的流程和步骤进行操作，以确保切换过程出现异常仍然可以按照既定的步骤进行回退，避免业务受到更大的影响。

6.4.4.5 Runbook 参考模板

- Runbook Checklist参考

表 6-19 Runbook Checklist 参考样例

大类	前置工作项	责任部门	活动	是否涉及	是否完成	计划完成时间	责任人
组织和保障准备	-	项目经理	-	是	-	-	-
	-	项目经理	-	是	-	-	-
第三方/业态	-	业务相关	-	是	-	-	-
环境清单核对	应用清单检查并刷新启停	研发相关	-	是	-	-	-
	-	研发相关	-	是	-	-	-
环境（源端、目的端、迁移任务、执行脚本）检查	云服务基础检查项	运维相关	-	是	-	-	-
	数据库检查项	运维相关	-	是	-	-	-

大类	前置工作项	责任部门	活动	是否涉及	是否完成	计划完成时间	责任人
		运维相关	-	是	-	-	-
	大数据检查项	大数据相关	-	是	-	-	-
		大数据相关	-	是	-	-	-
	应用检查	运维相关	-	是	-	-	-
	执行脚本检查	运维相关	-	是	-	-	-
		运维相关	-	是	-	-	-
	日志系统检查	运维相关	-	是	-	-	-

- Runbook操作步骤参考

  此外，还可能包含的项，例如：实际开始时间、实际结束时间、实际耗时等条目。

  表6-20设置样例，具体表格内容请参考实际业务情况后填写。

表 6-20 Runbook 操作步骤参考样例

序号	任务	步骤顺序	子任务	步骤	详细操作指导	决策	详细清单	操作人	确认人	计划开始时间	计划结束时间
1	XXX	1.1	-	-	-	必须解决	-	-	-	-	-
2		1.1	-	-	-	必须解决	-	-	-	-	-
3		1.2	-	-	-	必须解决	-	-	-	-	-
4		1.3	-	-	-	必须解决	-	-	-	-	-
5		1.3	-	-	-	必须解决	-	-	-	-	-
6		1.3	-	-	-	必须解决	-	-	-	-	-

序号	任务	步骤顺序	子任务	步骤	详细操作指导	决策	详细清单	操作人	确认人	计划开始时间	计划结束时间
7	XXX	1.4	-	-	-	非阻塞	-	-	-	-	-
8		1.4	-	-	-	非阻塞	-	-	-	-	-
9	回退决策1：时间点XX前完成上述步骤，否则决策是否回退。					-	回退-决策点1			-	-
10	XXX	21.1	-	-	-	阻塞执行	-	-	-	-	-
11		21.2	-	-	-	阻塞执行	-	-	-	-	-

6.4.5 部署

6.4.5.1 云资源开通及配置

部署主要是进行云上目标环境的资源开通和配置，并做好上云前的各项检查和测试，并进行迁移环境的准备。

要按照应用部署架构设计方案进行云上资源的开通和配置，云上资源开通主要有如下3种方式：

- 在云平台Console控制台手动创建云资源。
- 编写脚本或通过自动化平台对接，调用云平台的API接口，批量发放云资源，每个云服务都有对应的API接口，可以进行资源的生命周期管理。详情请见对应服务的帮助文档。例如，利用API创建云服务器，请参考**这个链接**。
- 使用华为云提供的应用编排服务RFS，对资源进行编排和批量发放，具体操作方法，请参考**RFS的官网文档**。

上述三种资源开通方式的对比如**表6-21**。具体使用哪种方式进行资源的发放和配置，需要根据实际情况和需求综合考虑。

表 6-21 三种资源开通方式对比

开通方式	场景	优点	缺点
Console控制台手动开通	适用于比较少的资源发放场。	技术门槛低	资源量大的情况下，人力投入较大。

开通方式	场景	优点	缺点
脚本调用API开通	• 量比较大的场景。 • 业务定制需求，程序运行按需调用，实现资源的自动创建与删除。	• 自动化操作：减少资源管理，减少人力投入 • 灵活性：快速创建、配置、启停云上资源，方便根据业务灵活部署 • 可编程性：API提供丰富的功能和参数，可以利用编程语言二次开发，满足特定的业务需求 • 速度快：避免手动操作的繁琐 • 可重复性：保障资源部署的一致性，降低人工操作出错的风险	• 学习成本：需要学习使用API接口，及相应的编程语言和工具，需要学习成本 • 维护复杂性：随业务扩大，脚本的结构和逻辑会复杂，管理和维护更加困难 • 安全风险：若没有正确的安全措施和权限控制，可能会泄漏敏感数据或资源被滥用等
AOS资源编排	适用于资源量比较大的场景。	• 自动化：可以自动化部署和管理云上资源，省去手动管理的繁琐步骤，提高效率 • 可视化：通过资源编排模板，可以清晰了解云上资源的依赖关系和配置信息减少出错率，提高管理效率 • 可重用性：编排模板可以反复使用和修改，节约时间和精力，提高开发和管理效率 • 可追踪性：带有审计功能，方便故障的追踪和回溯 • 一致性：保证资源配置的一致性，减少人工出错导致的不一致问题	• 学习成本高，需掌握编排模板语言和云服务相关知识。 • 调试复杂，因涉及多个云资源之间的依赖关系，如果其中某个环节出错，需耗时排查问题 • 安全风险，需妥善保管资源编排过程中使用的敏感的认证信息和密钥 • 风险管理，模板执行过程中出错或缺陷，可能导致资源的不可用 • 不适用于特殊场景，例如需要复杂的交互和手动干预的场景 • 可能存在的依赖问题，资源编排中的某些资源可能依赖其它资源的创建和配置，如果依赖的资源不存在或配置不正确，可能会导致资源编排失败 • 限制，可能存在的限制，如无法直接控制操作系统，不支持所有类型的资源等

6.4.5.2 迁移工具部署

华为云提供的迁移工具有：迁移中心（Migration Center, MgC）、资源发现与评估工具（RDA）、主机迁移工具（SMS）、数据复制工具（DRS）、Redis数据迁移工具、云数据迁移工具（CDM）、对象存储迁移工具（OMS）等。

- **迁移中心（MgC）**：是一站式迁移平台，集成了华为云的各个迁移工具，内置了由最佳实践总结而来的迁移工作流模板，您可以根据不同迁移场景，选择合适的迁移模板构建迁移工作流。具体功能及使用方法请查看**MgC帮助文档**。
- **资源发现与评估工具（RDA）**：是一个部署在Windows主机上的工具，用于评估上云驱动力和准备度，发现应用基础设施(例如虚拟机规格信息，CPU，内存利用率性能数据，网络拓扑数据等)，并提供其迁移到华为云的推荐配置以及主机的一站式迁移能力。
- **主机迁移服务（SMS）**：是一种P2V/V2V迁移服务，可以把X86物理服务器或者私有云、公有云平台上的虚拟机迁移到华为云弹性云服务器云主机上，具体使用方法请查看**SMS帮助文档**。
- **数据复制服务（DRS）**：用于数据库实时迁移和数据库实时同步的云服务。提供了实时迁移、备份迁移、实时同步、数据订阅和实时灾备等多种功能。具体功能及使用方法请查看**DRS帮助文档**。
- **Redis数据迁移服务**：用于自建Redis或其它云Redis服务（要求源端Redis已放通SYNC和PSYNC命令）向华为云上Redis（DCS服务或自建Redis）数据迁移，具体使用方法请查看**DCS数据迁移帮助文档**。
- **云数据迁移服务（CDM）**：支持近20种常用数据源，满足数据在云上和云下的不同迁移场景。具体使用方法请查看**CDM帮助文档。**
- **对象存储迁移服务（OMS）**：可以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对象存储服务（OBS），具体使用方法请查看**OMS帮助文档**。

资源发现与评估工具（RDA）需要部署在华为云VPC内的ECS云服务器（Windows操作系统）上；对象存储迁移工具（OMS）为公共服务，不占用VPC内网IP资源，如果通过专线迁移数据，则需要部署离线OMS工具在华为云VPC内的ECS云服务器上；其它工具均会暂时占用VPC内网IP资源。

6.4.6 迁移

6.4.6.1 接入层迁移实施

- **EIP**

  EIP不涉及到迁移，EIP通常需要在目标端华为云环境中重新购买，如果EIP需要对华为云以外的地方提供服务，那么该EIP需要在当地信管局进行服务域名和对应EIP的备案，备案通过后，方可对外提供服务。EIP购买和使用方法，请参照**华为云弹性公网IP服务**。

  备案是中国大陆的一项法规，使用大陆节点服务器提供互联网信息服务的用户，需要在服务器提供商处提交备案申请。不同备案类型的备案流程略有区别。具体备案流程，请参照**华为云备案服务**。

- **负载均衡**

  迁移到华为云ELB：源端的负载均衡可能是硬件负载均衡器或者是负载均衡软件，都可以使用华为云的ELB云服务替代，在目标端开通ELB服务，然后参考源端策略配置目标端ELB负载均衡策略，具体部署流程，请参照**华为云弹性负载服务ELB**。

  迁移到ECS上部署的软件负载均衡：如果源端是服务器上自建的负载均衡，迁移到华为云上仍然采用ECS自建负载均衡的场景，也可以使用SMS工具迁移。

- **VPN**

  VPN需要在目标端华为云重新部署，具体部署流程请参照**华为云虚拟专用网络VPN**。

6.4.6.2 应用层迁移实施

- **主机迁移**

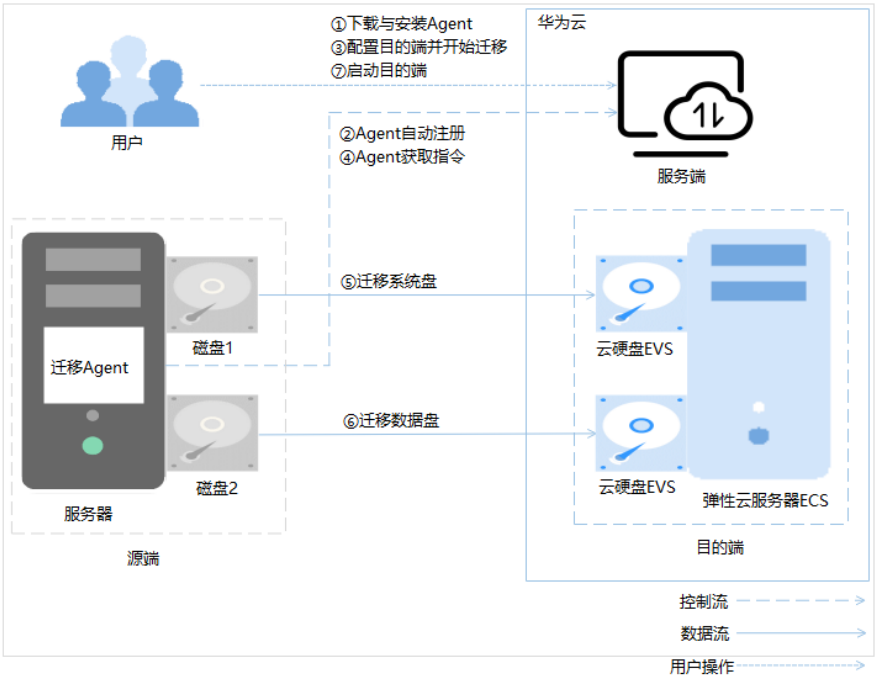
  主机迁移是典型的Rehost迁移方式，虽然主机（服务器）上可以承载各种系统应用如Nginx代理、数据库、容器、中间件、大数据等，但由于数据库/中间件/大数据等应用是以数据为核心，对于这类数据层面的迁移我们通常会采用独立的数据迁移方式而非主机迁移，这里讲的主机迁移对应的迁移层级为应用和操作系统。主机迁移的方式主要有以下三种：

  表 6-22 三种主机迁移方式说明

主机	迁移方式	适用场景	备注
虚拟机/物理机迁移	重新部署	OS可变，停机时间长	-
	SMS工具迁移（免费）	OS不变，版本一致，停机时间短	优先推荐，华为云有技术支持
	镜像导入/导出	OS不变，版本一致，停机时间长	-

- **重新部署：**针对公有云的平迁方式的应用上云场景，我们建议使用CI/CD流水线构建自动化平台，然后在云上重新部署应用。
- **SMS工具迁移：**是一种P2V/V2V迁移服务，可以帮您把X86物理服务器或者私有云、公有云平台上的虚拟机迁移到华为云弹性云服务器上，从而帮助您轻松地把服务器上的应用和数据迁移到华为云，主机迁移服务工作原理如下图所示：

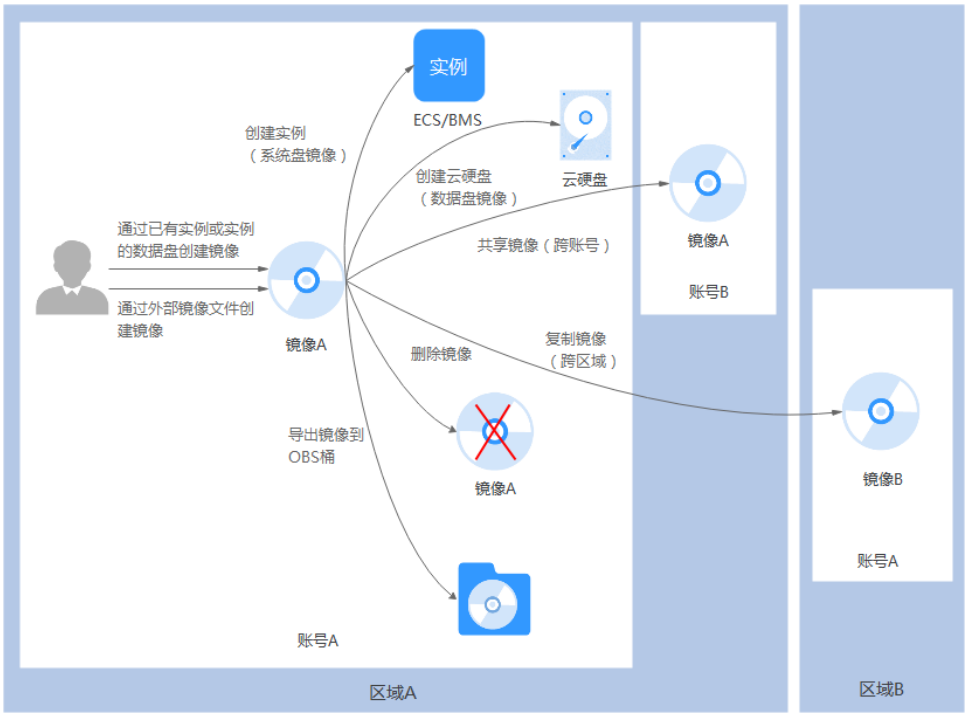
图 6-21 SMS 迁移过程



主机迁移服务的安全传输原理指的是：源端服务器中的迁移Agent从主机迁移服务获取到迁移指令后，会动态生成安全证书和密钥并且通过华为云OpenStack 元数据管理服务传输给目的端服务器，此后，源端服务器和目的端服务器会重启并使用新生成的动态安全证书建立安全的SSL通道。SMS主机迁移过程中，无需中断或者停止业务，只需在”持续同步”状态时，启动目的端前停止业务，大大减少业务中断时间。关于主机迁移服务的更多详细信息，请参考**SMS主机迁移服务**。

- **镜像导入/导出：**主机迁移也可利用华为云自主研发的镜像服务（Image Management Service，IMS）的导入功能，通过已有的云服务器或使用外部镜像文件创建私有镜像，将已有的业务云镜像导入到云平台，方便企业业务迁移与业务的批量部署，实现业务上云或云上迁移。

图 6-22 镜像导出导入方案



在源端与目标端无法通过网络使用SMS主机迁移服务进行整机迁移时，可以使用IMS镜像服务进行整机迁移。将源端服务器的系统盘和数据盘分别制作私有镜像，上传至华为云OBS对象存储服务中，在IMS镜像服务中，使用上传的外部镜像文件制作成私有镜像，最后使用私有镜像发放云服务器，完成整机迁移。迁移后的主机操作系统、系统配置，数据文件与源端服务器完全一致。关于主机迁移服务的更多详细信息，请参考**IMS帮助文档**。

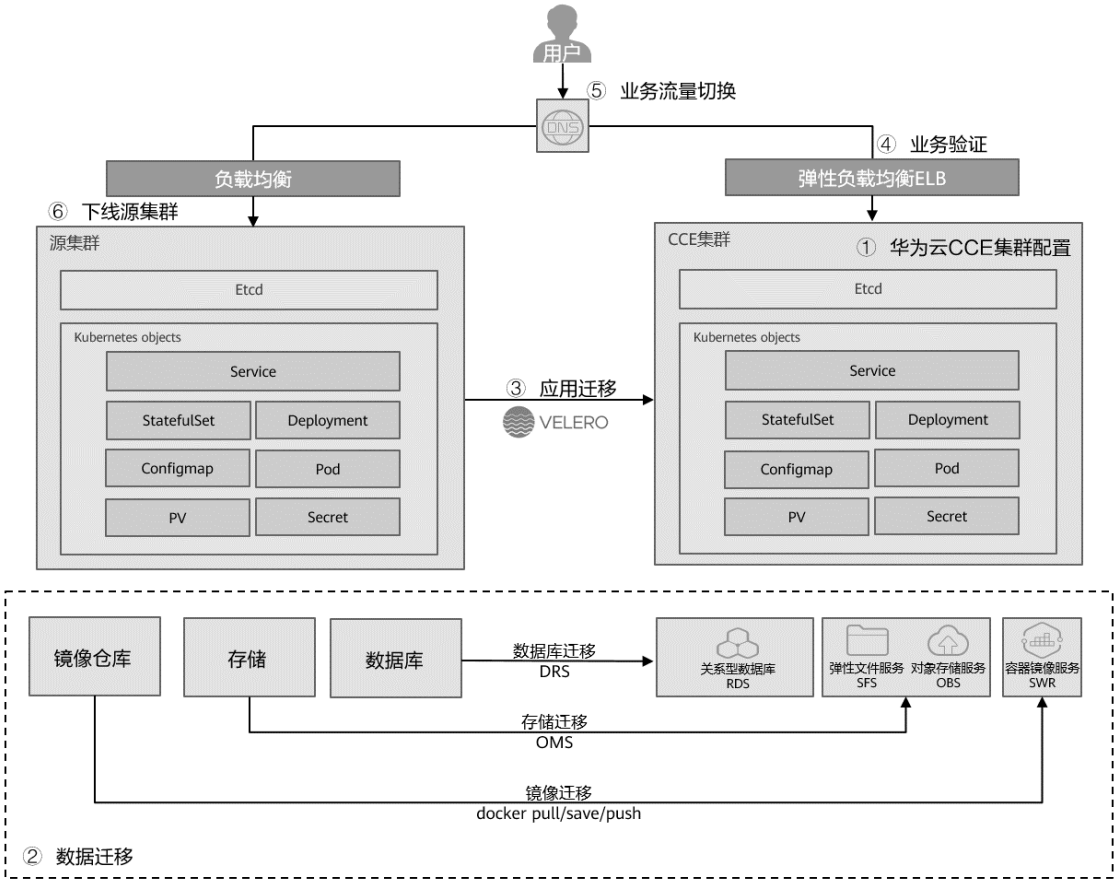
- **容器迁移**

  容器是操作系统内核自带能力，是基于Linux内核实现的轻量级高性能资源隔离机制。Kubernetes是一个开源的容器编排部署管理平台，用于管理云平台中多个主机上的容器化应用。Kubernetes的目标是让部署容器化的应用简单并且高效，Kubernetes提供了应用部署、规划、更新、维护的一种机制。对应用开发者而言，可以把Kubernetes看成一个集群操作系统。Kubernetes提供服务发现、伸缩、负载均衡、自愈甚至选举等功能，让开发者从基础设施相关配置等解脱出来。

  华为云容器引擎（Cloud Container Engine，CCE）提供高度可扩展的、高性能的企业级Kubernetes集群，支持运行Docker容器。借助云容器引擎，您可以在华为云上轻松部署、管理和扩展容器化应用程序。CCE是基于开源Kubernetes的企业级容器服务，提供高可靠高性能的企业级容器应用管理服务，支持Kubernetes社区原生应用和工具，简化云上自动化容器运行环境搭建。您可以通过CCE控制台、Kubectl命令行、Kubernetes API使用**华为云容器引擎**所提供的Kubernetes托管服务。

  这里的容器迁移指的是将其它云上的容器集群应用迁移至华为云CCE为例来讲解。总体迁移方案如下图所示。

图 6-23 容器迁移方案



整体的容器镜像迁移步骤：

a. 导出第三方集群上使用的容器镜像。

b. 按照第三方容器镜像服务上的操作指南拉取镜像到客户端机器。

c. 将导出的容器镜像文件上传到华为云SWR。

d. 使用docker pull命令将镜像上传到华为云，具体操作方法请查看**推送镜像到镜像仓库像**。

6.4.6.3 中间件层迁移实施

- **Redis迁移**

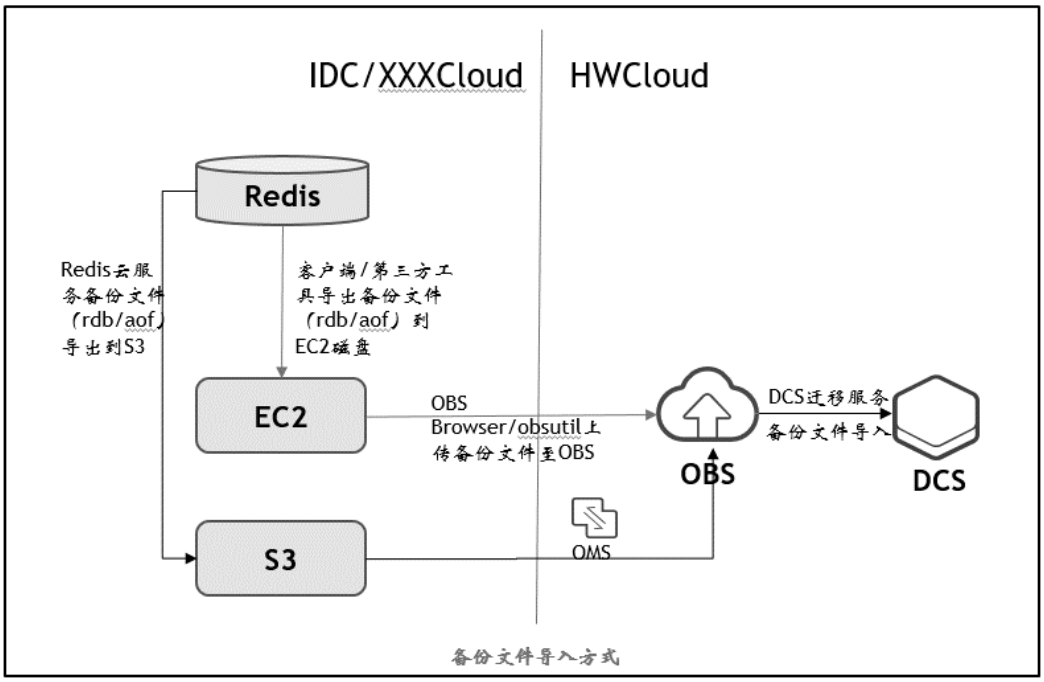
  Redis服务一般分为两种大的场景：缓存和数据库存储。在缓存时，一般不用进行迁移数据，大多数场景都是重新在华为云SQL数据库中重新缓存。一般迁移数据都是针对的Redis作为数据库存储使用的场景，其中在web场景下的缓存session时，也可以不用迁移，当客户端重新登录时会在华为云DCS中再一次存储。

- **离线备份导入**

  备份文件导入方式当前支持迁移到Redis3.0、Redis4.0和Redis5.0；暂时不支持导入自建Redis5.0生成的rdb备份文件。无论是IDC自建Redis，还是第三方云Redis服务，只要能进行导出备份文件（AOF或RDB），就可以使用DCS迁移服务的备份文件导入方式进行迁移。此种迁移方式属于全量迁移方式，在迁移过程中产生的新增数据无法进行迁移。

  源端容量大于10G的情况下，该迁移方式的迁移效率会大大折扣，故当源端内存使用量大于10G的情况下，不建议使用该迁移方案。

图 6-24 Redis 离线迁移方案



- 迁移过程如下：

  a. 源Redis数据备份导出：

     - IDC：使用第三方工具或配置策略将备份数据落盘（方法见Redis-cli或Redis-port）；
     - 使用备份功能将rdb文件输出到S3中。

  b. 备份数据上传至OBS：

     - EC2：使用OBS Browser/obsutil工具将备份文件（aof/rdb）上传至DCS所在的Region的OBS。
     - S3：创建OMS任务，将S3中的rdb备份文件迁移传输到DCS所在的Region的OBS。

  c. 创建DCS迁移任务：

     - 在DCS服务中的数据迁移模块创建迁移任务，选择备份文件导入方式，并选择OBS中源端的aof/rdb备份文件，填写其余选项，启动迁移任务。

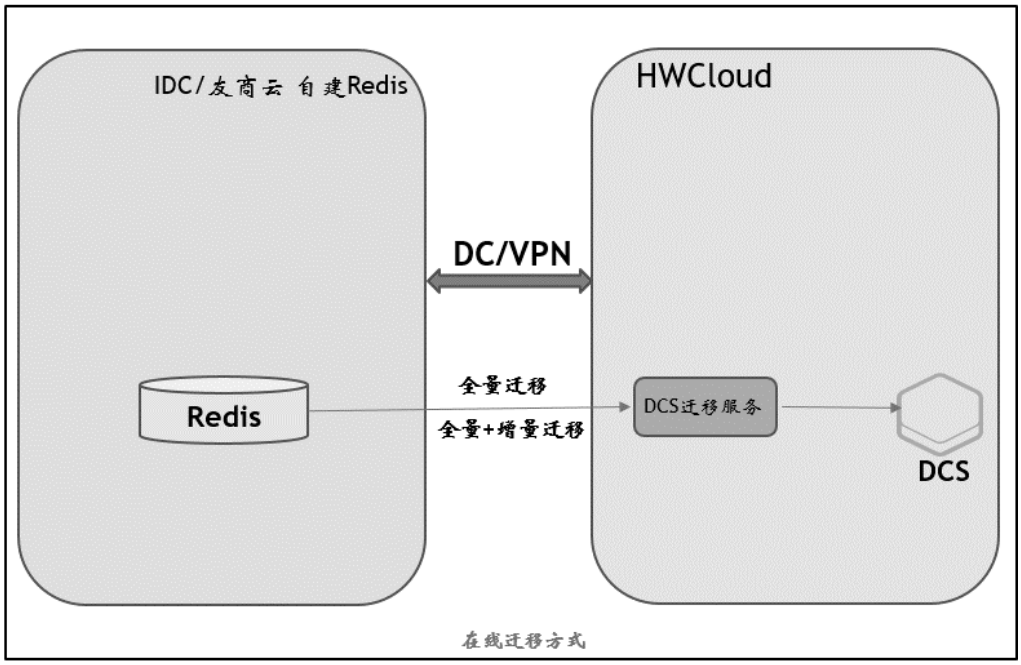
  d. DCS数据查询对比两端数据

     - 使用redis查询命令：info keyspace

- **在线迁移**

  在线迁移不光可以迁移全量数据，还可以实时同步迁移过程中的增量数据，但是这种迁移方法，需要源端与华为云目标端之间内网互通，而且源端Redis未禁用SYNC和PSYNC命令。

图 6-25 Redis 在线迁移方案



迁移过程如下：

a. 创建DCS迁移任务：

在DCS服务中的数据迁移模块创建迁移任务，选择在线迁移方式，根据需要选择去全量迁移或全量迁移+增量迁移方法，填写其余选项，启动迁移任务。

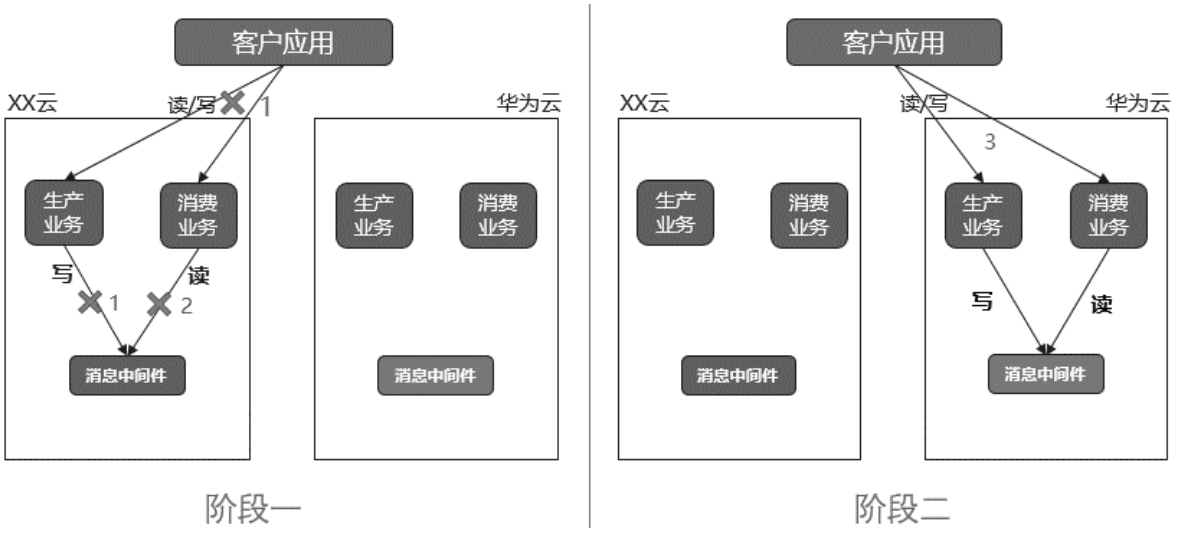
a. DCS数据查询对比两端数据

迁移任务完成后，使用redis查询命令：info keyspace

- **消息中间件迁移**

  消息中间件，包含Kafka、RabbitMQ、RocketMQ、IBMMQ等，消息中间件在迁移项目中，通常使用策略切换的方案来进行迁移。

图 6-26 消息中间件迁移方案



迁移步骤如下：

a. 中断企业应用和生产消息的相关业务，直到消费组中的消息消费完毕
b. 待消息消费完毕，停止消费相关业务
c. 启动华为云的生产消息和消费消息的业务，接入客户流量，观察业务是否正常

6.4.6.4 数据层迁移实施

1. **对象存储迁移**

对象存储适用于存储非结构化的数据，我们日常生活中见到的文档、文本、图片、XML、HTML、各类报表、音视频信息等等都是非结构化数据。不同的量级对应了不同的迁移方式，如下图所示：

图 6-27 对象存储迁移方案

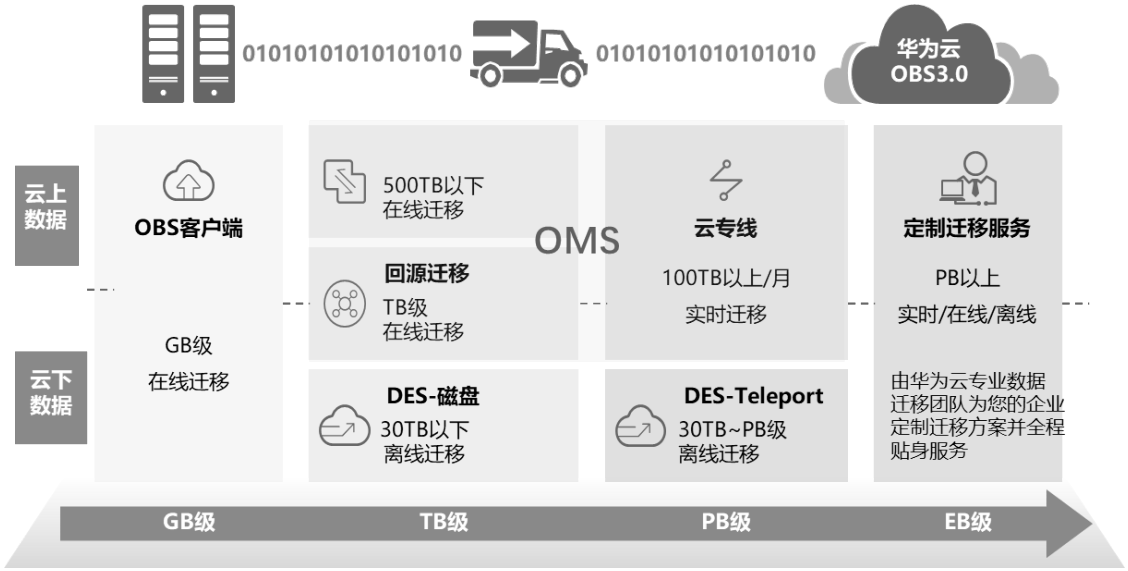


表 6-23 三种对象存储迁移方式说明

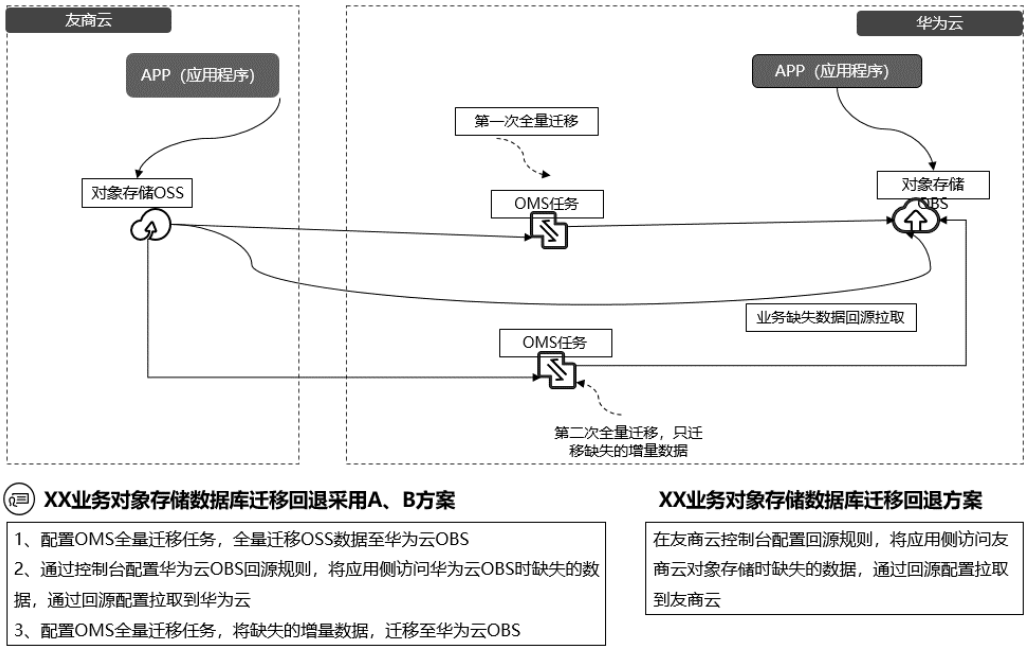
对象存储	迁移方式	适用场景	备注
对象存储迁移	OBS客户端拷贝	数据量较少，GB级数据	-
	OMS工具迁移+回源	数据量大，TB级及PB级数据，且有较大增量数据	优先推荐，华为云有技术支持
	线下DES磁盘拷贝	数据量较大，增量少的TB级数据	-

- **OMS工具+回源迁移：**对象存储迁移服务OMS作为易用、高效的线上数据迁移服务，通过调用源端对象存储的SDK，可快速传输数据并对数据进行加密存储，将数据复制到华为云OBS，可以帮助把对象存储数据从其他云服务商对象存储服务中的数据轻松、平滑地迁移到华为云。通过第一次全量任务，将源端对象存储全量数据迁移至华为云OBS，业务切换时，在华为云配置回源规则，将部分增量数据，通过回源的方式迁移至华为云OBS，在业务切换后，再进行一次全量迁移，

本次全量迁移，将自动跳过已经迁移的对象，将剩余增量数据迁移至华为云OBS。

在对象存储迁移服务中，可以查看迁移任务、管理迁移任务，创建迁移任务组，评估桶内数据，查看审计日志等，具体内容请查看**OMS帮助文档**。

图 6-28 对象存储迁移服务



- **线下DES磁盘拷贝：**

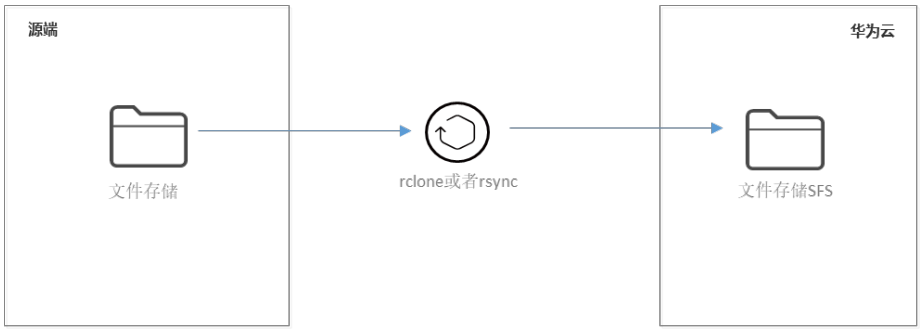
  云下数据也提供了数据快递服务（DES）来迁移数据，DES 是面向TB或PB级数据上云的传输服务，它使用物理存储介质（USB、eSATA接口的磁盘等）、或Teleport向华为云传输大量数据，解决了上云带宽昂贵、传输时间长的难题。详细信息请查看**DES帮助文档**。

  同时，对于储存数据的迁移华为云也提供了定制迁移服务，专业数据迁移团队可以为企业定制迁移方案并全程贴身服务，协助客户实施全量与增量数据迁移，协助客户验证全量与增量数据迁移的效果，完成云下存储数据到云上存储数据的迁移。详细信息请查看**上云迁移服务**。

- **文件存储迁移**

  NAS文件存储是一种可共享访问、弹性扩展、高可靠以及高性能的分布式文件系统。华为云的**弹性文件服务**SFS提供按需扩展的高性能文件存储（NAS），可为云上多个弹性云服务器（Elastic Cloud Server，ECS）、容器（CCE&CCI）和裸金属服务器（BMS）提供共享访问。NAS文件储存迁移时，在网络互通的情况下，可以进行多平台挂载使用，通过Rclone工具或者Rsync工具的复制文件的能力，在中转主机上将源挂载目录文件复制到SFS或者SFS Turbo文件系统上。

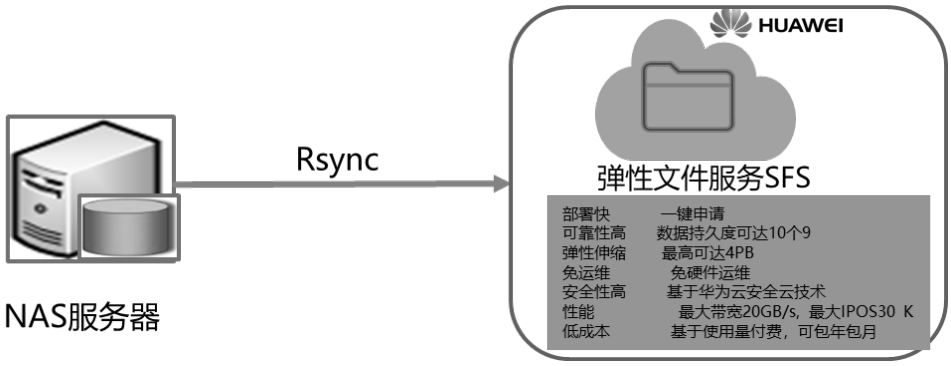
图 6-29 文件迁移方案



Rclone 是一款命令行工具，支持在不同对象存储、网盘间同步、上传、下载数据，Rclone工具支持自定义多线程多并发迁移任务，大大提高迁移效率，缩短迁移周期。具备数据同步、检查能力，能够将源端文件系统中的数据拷贝到目的端，完成NAS文件的迁移。

Rsync（Remote synchronize）是一种基于RCP协议（Remote Copy Protocol）的，使用其Rsync算法的远程文件同步工具。

图 6-30 Rsync 迁移



通过在各业务平台开启Rsync服务，在文件服务器中配置Rsync客户端脚本，通过FileServer系统的定时任务，如：Linux的Crontab，定时将业务服务器的文件以文件增量的方式（第一次是全量）同步到磁阵中。优势：

a. 文件增量同步，速度快，效率高，占用资源少。

b. 通过SSH，RSH等模式可对第三方平台跨网络开放。

c. 服务端不想共享时，只需停止Rsync服务，不影响其它业务。

d. 支持镜像方式数据拷贝，适合于互联网模式下的静态文件分布式部署，可扩充性好。

- **数据库迁移**

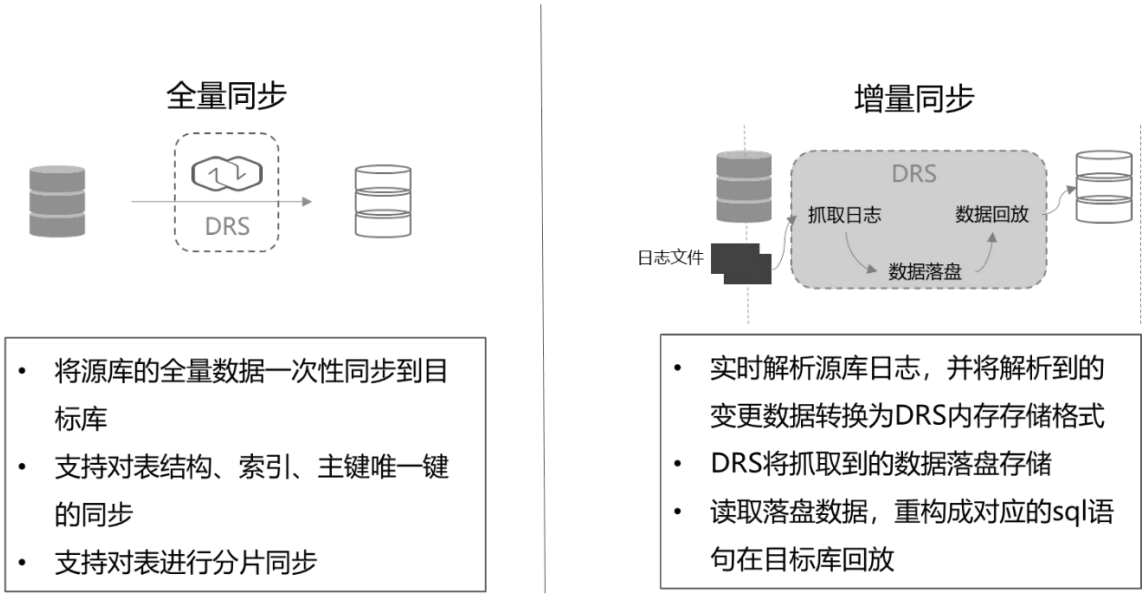
  数据库主要分为关系型数据库与非关系型数据库两大类，能保持数据一致性是关系型数据的最大优势，从IDC或者云上将数据库迁移到华为云，有以下三种方法：

  a. 利用SMS主机迁移。如果源端是在ECS上自建数据库，需要将自建ECS数据库服务器迁移到华为云弹性主机ECS上，SMS可以帮助轻松实现，但是此时会中断数据库业务，需要注意。但是当对停机时间有较高要求，您也可以使用数据库的备份恢复功能或者数据库同步复制技术进行迁移。

b. 使用备份恢复进行迁移。备份恢复迁移数据库的备份还原方案是指的保存源系统的数据，停止源系统数据库业务，在源系统进行数据库全备份，确保必要的日志也保留，并在目的系统进行还原。

c. 使用数据库复制服务（Data Replication Service，DRS）进行迁移，实现跨云平台数据库迁移、云下数据库迁移上云或云上跨Region的数据库迁移等多种场景，用于数据库在线迁移和数据库实时同步的云服务。DRS服务是一种易用、稳定、高效，用于数据库平滑迁移和数据库持续同步的云服务。DRS围绕云数据库，降低了数据库之间数据流通的复杂性，有效的减少数据传输的成本。数据复制服务支持多种数据源之间的数据流通，实时迁移、备份迁移、实时同步、数据订阅和实时灾备对不同数据库的支持不同，详细情况请查看**DRS帮助文档**。

图 6-31 DRS 迁移



以下是常见的数据库迁移最佳实践。更多最佳实践可以查看**DRS最佳实践汇总**。

表 6-24 数据库迁移最佳实践

源数据库类型	目标数据库	最佳实践在线文档
其他云MySQL数据库	华为云RDS for MySQL	**其他云MySQL迁移到云数据库 RDS for MySQL**
	华为云GaussDB(for MySQL)	**其他云MySQL迁移到GaussDB(for MySQL)**
其他云MongoDB	华为云DDS	**其他云MongoDB迁移到DDS**
自建MySQL	华为云RDS for MySQL	**自建MySQL迁移到RDS for MySQL**

源数据库类型	目标数据库	最佳实践在线文档
ECS自建MySQL	华为云GaussDB(for MySQL)	ECS自建MySQL迁移到GaussDB(for MySQL)
ECS自建MongoDB	华为云DDS	ECS自建MongoDB迁移DDS
本地自建MySQL	华为云RDS for MySQL	本地MySQL迁移到RDS for MySQL
本地自建MongoDB	华为云DDS	本地MongoDB迁移到DDS
华为云RDS for MySQL	分布式数据库中间件DDM	RDS for MySQL迁移到DDM
MySQL分库分表	分布式数据库中间件DDM	MySQL分库分表迁移到DDM
本地Microsoft SQL Server	华为云RDS for SQL Server	本地Microsoft SQL Server备份迁移至本云RDS for SQL Server实例

6.4.6.5 迁移实施常见问题

关于迁移实施过程中的常见问题及答案，请查看如下链接。

1. 主机迁移服务SMS的常见问题。
2. Redis数据迁移常见问题。
3. 对象存储迁移服务OMS的常见问题。
4. 数据库迁移的常见问题。

6.4.7 验证

6.4.7.1 数据验证

- **数据验证标准**

  迁移完成后，需要对源端和目的端数据做一致性比对，对于数据一致性比对的精度，不同的场景有不同的要求。一般来说，核心业务的数据库表要求源端和目的端100%一致；对于大数据类业务中的部分场景，例如用户画像计算等，可以约定原始数据90%一致。如下是一个参考标准，可根据实际情况调整：

表 6-25 数据校验标准参考

分类	数据一致性要求	业务举例
核心业务	100%	电商系统的核心会员数据、交易数据、支付数据等，数据是用户最核心的资产，涉及到真实的财产金额等。所以这部分核心业务对于数据一致性要求是100%。建议进行数据的行数对比和对象对比，抽样内容对比。
非核心业务	99.9%	电商系统的用户购物车商品数据、客服沟通消息数据等，作为非核心业务的数据，如果有微量损失，并不会影响客户的业务使用和体验。建议若切换时间有限，可以只进行数据的行数对比。
边缘业务	90%	电商系统的首页推荐数据、用户浏览数据、用户画像数据等，如果有一部分损失，并不会影响客户的业务使用可体验。建议进行表级的的行数对比，抽样内容对比。

- **数据验证方法**

  数据分为数据库数据、中间件数据和文件数据，这三种数据的一致性验证方法和工具不同：

  - 数据库数据一致性验证的方法如下表所示。

    表 6-26 数据库一致性对比方式

对比项	工具	描述
库和表级内容对比	DRS工具	查询对比数据库表的每一条数据，确保每一条的每一个字段都与源端数据库表一致。相较于行对比，内容对比较慢。
	python脚本	根据DRS任务的ID，调用接口批量执行对比任务，对比结果输出到xlsx文件中。相比于工具可批量执行，执行效率较高。
库和表级对象对比	DRS工具	对数据库、索引、表、视图、存储过程和函数、表的排序规则等对象进行对比。
	python脚本	根据DRS任务的ID，调用接口批量执行对比任务，对比结果输出到xlsx文件中。相比于工具，可批量执行，执行效率较高。
库和表级行数对比	DRS工具	对比表的行数是否一致，只查询表的行数，对比速度较快
	python脚本	批量脚本，创建N个并发任务线程，遍历所有表进行逐一COUNT，输出对比结果到xlsx文件中，相比于工具可批量执行，执行效率较高。

- 中间件数据一致性验证的方法如下表所示：

表 6-27 中间件一致性对比方式

对比项	工具	描述
Keys数量对比	redis-cli	通过redis-cli命令info keyspace查看keys参数和expires参数的值，对比源Redis和目标Redis的keys参数分别减去expires参数的差值。如果差值一致，则表示Keys数量一致，迁移正常。
Key-value内容对比	开源Redis-Full-Check工具	通过全量对比源端和目的端redis中的数据内容的方式来进行数据校验，其工具实现方式会多次抓取源和目的端的数据进行差异化比较，记录不一致的数据进入下轮对比。然后通过多轮比较不断收敛。最后sqlite中存在的数据就是最终的差异结果，无内容则表示数据内容完整，迁移正常。

- 文件类数据一致性验证的方法如下表所示：

表 6-28 文件数据一致性对比方式

类型	对比项	工具	描述
对象存储	对象数量	OMS	OMS迁移工具，通过MD5校验文件完整性和比对两边桶对象数据量是否一致。
文件存储	文件数量	rclone	Rclone迁移工具，使用MD5哈希值来验证文件的完整性。同步后会再对比源端和目的端文件数量。
		rsync	rsync迁移工具，使用MD5哈希值来验证文件的完整性，如果校验和不匹配，则rsync会重新传输该文件，以确保数据一致性。同步后会再对比源端和目的端文件数量。
	文件大小	python脚本	迁移完成后，通过对比源端和目的端总文件大小判断是否一致。
	文件内容	python脚本	迁移完成后，通过计算源端和目的端文件的哈希值，比较两个文件的哈希值是否一致。

6.4.7.2 业务验证

业务验证对上云迁移非常重要。业务验证主要包括功能验证和性能验证等。在上云迁移过程中，有两个阶段需要进行业务验证。首先，业务部署完成后，在切换前需要进行功能和性能验证，其次，业务切换时，当业务流量切换到目的端，切换后也需要进行功能和性能验证。

功能验证

- **功能测试内容**

  功能测试确保应用系统在上线前能够正常运行，以下是功能测试的内容：

  表 6-29 功能测试内容列表

测试内容分类	说明
本应用功能测试	测试的内容强依赖应用系统的功能，比如某电商系统，核心的功能测试用例至少包括线上线下的浏览、购物、下单支付（各种支付途径支付、用券支付）、打印账单、开发票、活动促销、库存同步、新会员注册，老会员退会、订单退款、订单返券等核心功能。
周边系统集成功能测试	测试的内容强依赖应用系统的集成功能，比如某大型零售电商平台，和某团购平台、某外卖平台、某到家平台、某小视频平台等都有业务合作，集成的用例至少包括在这些集成平台的下单、用券、通知发货，评论等各种功能的验证。

- **功能测试目的**
  - 验证应用系统迁移到目标端华为云后，更换了技术组件后的应用功能是否正常
  - 验证应用更换到目标端后，应用和周边的系统的集成是否正常，识别需要周边系统配合修改的内容都已修改正常。
- **功能测试方法**
  - 冒烟测试：冒烟测试是一种简单的功能测试，通过执行少量的核心测试用例来验证系统是否可用。在目标端部署完成后，可以首先执行冒烟测试来确认系统的基本功能是否正常。
  - 全业务功能测试：全面的业务功能测试可以验证系统的所有功能是否正常，通过执行针对各种业务流程的测试用例，确保所有功能模块正常。
  - 日志分析：在目的端业务部署完成后，需要对系统的日志进行分析，检查是否存在异常情况的错误信息。通过日志分析可以发现一些潜在的问题和隐患，及时进行修复和优化。
  - DNS劫持测试：因云上部署的业务一般按照生产环境的域名进行配置，在使用手机App或浏览器测试业务功能时，需要配合使用DNS劫持的方式进行测试，可以使用内网WIFI及运维改造的APISIX，配合WiFi上的DNS解析，劫持流量指向测试环境，进行的内网测试。
- **功能测试流程**

图 6-32 功能测试流程

a. **确定测试目标和重点关注点**：明确需要测试的应用功能和场景，以及测试的重点和关注点。

i. 系统功能：如促销活动，用券支付、退货反券等

ii. 批处理JOB功能：若本次搬迁的应用同时涉及多个批处理JOB，在功能测试时，需要重点关注批处理JOB的执行情况，比如库存推数。

iii. 第三方业务集成功能：如某团购平台、某外卖平台、某到家平台、某小视频平台的集成功能验证，以及门店POS支付等功能验证。

b. **确认测试环境：**确认使用哪个环境用作测试，不要对生产业务造成影响。注意，如果有请求第三方接口的业务，需要注意外网隔离，防止测试污染生产数据，可以通过内网搭建特殊WIFI，让内部测试人员登录模拟进行三方功能的测试。

表 6-30 测试环境的对比分析

场景	测试环境选择建议	优点	缺点
目标端华为云生产环境是否已上线部分应用	方案1：在目标端华为云生产环境用作测试	1.测试后直接转生产上线，节省工作量 2.各项参数在测试期间已调为最优	需做好网络隔离，有对现网影响的风险。
	方案2：在目标端华为云新建一套测试环境用作测试	对现网无影响	1.新搭建一套环境有一定的成本费用 2.在测试环境调测好的配置参数需要1：1配置到生产环境，有一定工作量
目标端华为云生产环境是全新环境	目标端华为云生产环境用作测试	1.测试后直接转生产上线，节省工作量 2.各项参数在测试期间已调为最优	无

c. **设计测试用例**：根据测试目标，设计和准备测试用例。切换之前的测试用例要尽可能的全覆盖，切换期间，由于测试时间有限，建议将测试用例划分P0、P1、P2三个优先级。

i. P0定义：最核心的功能用例，此用例通过，可以决策不再考虑回退。

ii. P1定义：重要功能用例，此用例通过表示基本功能全部可用，此用例通过后，即可宣布当晚切换成功，可取消外部维护公告。

iii. P2定义：其他补充用例，如切换时间窗足够，可切换当晚测试，如果切换时间窗不够，可第二天测试。

表 6-31 测试用例执行说明

阶段	测试用例	覆盖率
切换前测试	所有	包括所有的应用功能和第三方集成功能测试。特殊无法测试场景需单独讨论模拟测试方案。

阶段	测试用例	覆盖率
切换期间测试	分P0、P1、P2三个级别。 在切换时间窗内至少完成P0和P1级用例测试。	根据切换时间窗口，时间窗口充足，完成所有的用例，时间窗口不足，至少完成P0和P1级用例。

对于测试环境的测试用例选择，企业需要根据应用场景分析是否具备测试条件，比如第三方库存同步的用例，第三方只有生产环境对接本企业生产环境，无法对接测试环境情况下，此用例就无法测试。所以需识别无法测试的用例，评估测试用例的覆盖率，对于无法覆盖的用例单独讨论模拟测试方法，参考如下：

场景	是否具备测试条件	特殊场景应对措施
第三系统下单	第三方系统由于和测试环境无法打通，所以在测试环境无法测试	针对无法测试的场景，讨论应对方案如直接调用库存同步接口模拟测试
库存同步	第三方库存由于和测试环境的库存系统无法打通，所以在测试环境无法进行测试	针对无法测试的场景，讨论应对方案如直接调用库存同步接口模拟测试
支付	线上支付具备测试条件 线下POS支付由于和测试环境无法打通网络，不具备测试条件	针对无法测试的场景，讨论应对方案如：直接调用接口模拟测试等
…	…	…

d. **预置测试数据：**为了确保测试的真实性和有效性，需提前预置测试数据。可以使用源端测试环境数据，也可以使用脱敏后的生产数据。

e. **执行测试用例：**部分企业测试自动化起步较晚，大量用例仍需要人工执行，手工执行用例，在测试过程中需执行人详细记录测试时间、测试人员、用例执行结果等相关信息。部分企业已有自动化测试能力，上云过程中只需要将新增的用例增加到自动化平台自动执行。

f. **输出测试报告：**全部测试用例测试完成后，输出测试报告。 总的来说，功能测试需要确保测试环境和生产环境尽可能的一致，测试用例覆盖率100%，以保证应用上云后的功能正常。

性能验证

- **性能验证**

  应用系统迁移到云上后，底层技术组件更换了，云上的技术组件默认参数可能与源端默认参数不同，或者源端和目的端的技术组件实现机制不同，可能会导致上云发生性能问题，需要进行性能测试，性能测试内容包括如下三类。

表 6-32 性能测试内容

测试内容	说明
云服务性能测试	针对某个云服务进行性能测试，比如数据库，Hbase、存储的IOPS等。
应用接口性能测试	接口性能是系统性能评估的一个方面，针对某几个接口进行针对性接口压测。
应用整体性能测试	根据应用的使用场景，比如大促期间，上千人同时浏览一个产品并抢购的场景下，整体的性能测试。

这三类性能测试的目的如下表所示。

表 6-33 性能测试目的说明

测试内容	目的
云服务性能测试	评估云服务的规格是否满足应用高并发下的性能，参数是否是最优配置。
应用接口性能测试	针对某几个接口评估接口的极限负载能力
应用整体性能测试	1. 确定云上业务系统的极限负载能力：通过高并发、高负载的测试，确定云上业务系统可以承载的最大负载，以及达到极限负载时系统的表现和响应时间。在压力逐步上升的过程中，观察云上业务系统在承载和源端压力相当时的性能表现，并对比收集到的指标，确定是否存在问题。 2. 验证系统的稳定性和可靠性：通过长时间、高负载的测试，验证云上业务系统在各种情况下的稳定性和可靠性，包括系统资源的管理、数据传输、异常处理等。 3. 评估系统的可扩展性：在系统压力逐步增大的过程中，测试云上业务系统的可扩展性，可以确定系统是否可以扩展到更大的规模，并支持更多的用户和业务需求 4. 识别系统的性能瓶颈：通过对云上业务系统的压力测试，可以识别系统的瓶颈，确定迁移过程中业务环境的改变带来的系统性能问题，从而优化系统性能。

上述三类性能测试的具体方法如下。

1. **云服务性能测试（以数据库为例）**

   对于大多数应用系统来说，整个系统的瓶颈往往在数据库。因为应用的其他组件，例如网络带宽、负载均衡、应用服务器、中间件等比较容易实现水平扩展，但对于数据库，由于数据一致性要求高，多数业务系统仍然采用数据库主备方式实现，未实现数据库的分布式架构。

   常用的数据库相关指标有：

   - **TPS/QPS：**每秒处理事务数和每秒查询数，用于衡量数据库的吞吐量。

- **响应时间：**包括平均响应时间、最小响应时间、最大响应时间、时间百分比等，其中时间百分比参考意义较大，如前95%的请求的最大响应时间。
- **并发量：**同时处理的查询请求的数量。
- **成功率：**指请求在一定时间内成功返回结果的比例。

华为云RDS提供了数据库的TPS/QPS等标准性能基线，企业也可以基于自己的业务数据重新进行压力测试。常用的数据库压测工具是Sysbench，支持多线程，支持多种数据库。主要包括以下几种测试：

- CPU性能
- 磁盘IO性能
- 调度程序性能
- 内存分配及传输速度
- POSIX线程性能
- 数据库性能(OLTP基准测试)

2. **应用接口性能压测**

   你可以使用以下两种方式针对应用接口进行性能测试，一种是采用华为云提供的云原生性能测试工具CodeArts PerfTest，另一种是使用Goreplay。两种方式的优缺点如下表所示。

表 6-34 接口性能压测方式对比

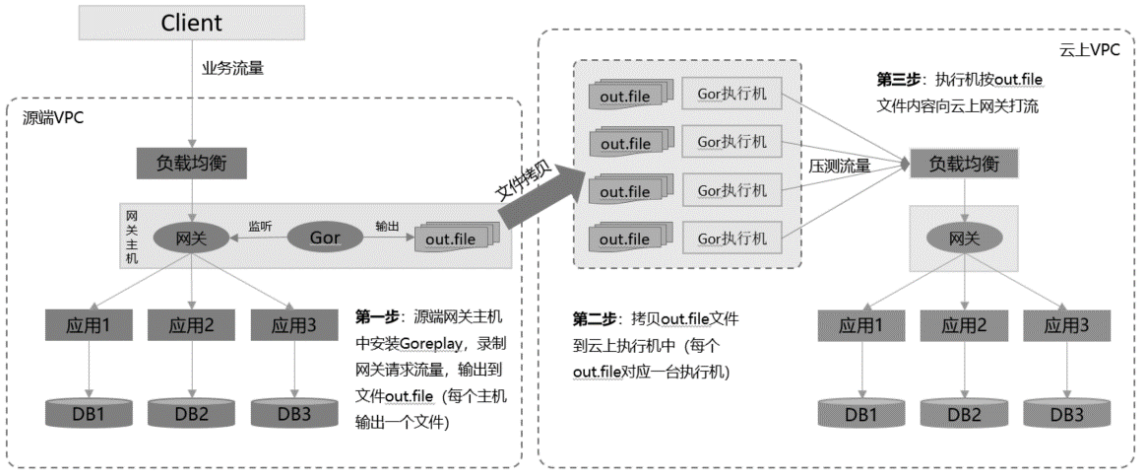
测试工具	压测方式	优点	缺点
CodeArts PerfTest	基于华为云性能测试工具完成接口压测。	• 支持多协议、高并发、复杂场景的测试 • 专业性能测试报告，应用性能表现一目了然 • 与生产环境核心业务不产生交互，不会对现网产生影响 • 接口测试对其他业务依赖较少，可以基于单业务系统进行。	• 执行成本高，前期业务梳理和脚本编写耗时较久。 • 对测试人员技术要求较高，需要熟悉测试工具的使用和相关测试知识，否则测试效果可能不够理想。

测试工具	压测方式	优点	缺点
GoReplay	在业务网关部署GoReplay工具，复制现网流量，在目的端进行回放。	• 低成本、效率高：无需梳理各个系统的接口和业务逻辑，可以直接基于实际流量进行测试 • 一方面线上大量真实流量确保覆盖率，另一方面支持中间过程的验证，例如发送消息的内容、中间计算过程等等的全对象的对比验证，传统手工编写验证点很难实现。	• 需要在生产环境流量入口网关上安装插件，会占用一定的cpu和存储空间。 • 对于分批割接的场景，由于流量录制是基于所有业务请求进行录制，如果目标端有部分业务没有部署，会导致有接口404的报错，需要人工进行定位，定位工作量大。 • 只支持HTTP协议，对于HTTPS、TCP、UDP等无法录制

关于如何使用CodeArts PerfTest进行性能压测，请**参考官网文档**。以下介绍如何通过GoReplay流量复制进行性能压测。

GoReplay是一个用于复制、重放和操作HTTP流量的开源工具。它可以捕获实时流量，并将其发送到一个或多个目标服务器，从而实现流量的复制和重放。通过GoReplay，可以将实际的HTTP请求和响应流量复制到测试、开发或生产环境中，以便在这些环境中进行测试、监控和分析。在上云迁移过程中，我们可以使用GoReplay工具，从源端现网业务网关流量入口复制请求数据，在目的端云上执行机上回放业务请求，实现对云上相关业务接口的压力测试，详细方案如下图所示：

图 6-33 GoReplay 流量复制压测方案



使用GoReplay做性能压测时要注意以下事项：

- 在源端网关使用GoReplay录制请求流量时，要注意对主机性能的影响，需实时观察主机相关指标，如CPU使用率，内测使用率等。同时，GoReplay输出

的out.file文件，会占用大量的磁盘空间，注意磁盘使用率，防止因磁盘写满导致网关应用不可用，最好使用网络存储来存放输出文件。

- 在进行流量回放时，目的端业务如果有访问第三方接口的需求，可能会对生产业务产生影响，注意做好网络隔离。

3. **应用整体性能压测**

   应用整体性能压测是指对业务系统的所有业务流程和功能进行综合性的压力测试，以评估系统在真实生产环境下的稳定性和性能表现。在压测过程中，模拟真实用户的行为，并生成高负载情景，以评估系统在高负荷下的性能和稳定性，确认业务系统能够满足用户的实际需求。

   以下是几个常见的全业务整体性能压测场景：

   a. 正常业务负载：模拟系统在正常使用情况下的业务负载，包括用户请求的数量、频率和类型等。通过验证系统在正常负载下的性能表现，确保系统能够满足用户需求。

   b. 峰值负载：模拟系统面临最高负载的情况，通常是在特定时间段内用户请求达到峰值。这种场景用于确定系统的扩展能力是否能够处理高峰期的请求，并确保系统不会出现性能瓶颈或崩溃。

   c. 突发负载：模拟系统面临的异常情况，如突然增加的用户请求或大规模数据处理等。这种场景用于评估系统在压力突增时的稳定性和容错能力，确保系统能够优雅地处理异常负载而不受影响。

   d. 长时间负载：模拟系统长时间运行的情况，一般持续数小时甚至更长时间。这种场景用于测试系统在长时间运行后是否会出现内存泄漏、资源耗尽等问题，以确保系统的稳定性和可靠性。

   e. 异常场景：模拟系统面临的各种异常情况，如网络故障、服务器宕机、数据库连接中断等。这种场景用于测试系统在异常情况下的容错能力和恢复能力，确保系统能够正确处理异常并保持可用性。

6.4.8 切换

6.4.8.1 切换演练

在功能测试和性能测试完成之后，如果云端应用程序和服务运行稳定，就可以开始进行业务切换了。

业务切换是将业务从源端旧系统切换到云上新系统的过程，需要仔细规划和协调，以确保切换过程中不会影响数据的完整以及业务运行。

一般情况下，业务切换需要进行一定的时间，逐步切换流量，同时关闭旧的业务系统。通过这个过程，可以实现从旧系统向新系统的平稳过渡，并最终将业务成功迁移上云。在正式切换前通常会进行切换演练，然后才是正式切换。

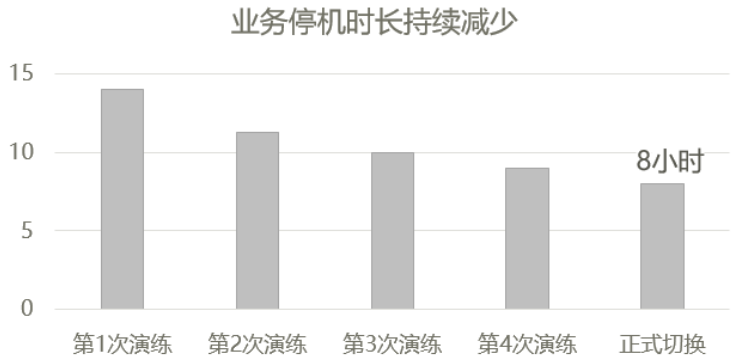
为什么要演练

切换演练在上云迁移过程中扮演着至关重要的作用，通过一次或多次演练为正式切换提供信心和保障。它的主要意义在于可以最大程度地识别问题和风险，提高大家操作熟练度，减少中断时长，确保切换过程的顺利进行。

1. **预防问题：**演练可以帮助发现可能存在的问题，比如切换过程中的应用和批处理任务启停顺序问题、网络配置问题、数据一致性对比等问题，从而提前进行预防和解决。
2. **团队配合：**演练可以让团队成员熟悉切换的全流程和切换步骤，从而更好地协同工作，提高团队配合效率。

3. **优化Runbook：**演练过程中可以识别出切换步骤的问题，比如整体串并行顺序问题以及某个步骤执行时间过长等问题，可以通过演练复盘优化Runbook步骤和时长，提高正式切换步骤的正确性和合理性，提高切换效率。
4. **预估正式切换时长：**通过演练，记录每个执行步骤的开始时间、结束时间和执行时长，可以更加准确地预估正式切换的时长，从而合理规划对外停机公告时间，协调周边团队的配合时间。
5. **减少正式切换的中断时间：**通常一个大型系统的切换要200多个步骤，中间有并行操作和串行操作交叉进行，涉及角色和人员也较多，可以通过一次或多次演练，提高切换操作的熟悉度和各方的配合默契度以及问题处理的效率，对于一些操作时长比较长的步骤，还可以通过自动化脚本代替人工操作或者持续优化脚本提高执行效率，从而减少正式切换的中断时长。以某大型零售平台上云为例，采用所有业务系统一把切的方案，通过4次演练，正式切换的时间比预期缩短了40%。

图 6-34 演练效果展示

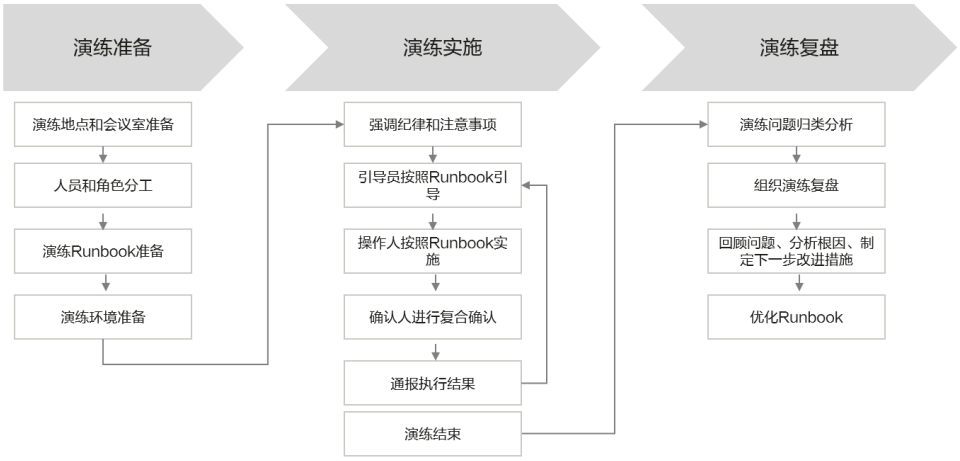


6. **识别未知问题：**演练环境可以帮助发现一些未识别到的问题，比如某系统在切换过程中，涉及的应用都已关停，但是仍然有session在连接数据库，导致数据一直无法静止，定位发现某第三方店铺在店铺关停后仍然在做一些操作等。企业可以根据识别的未知问题，有针对性的调整和优化切换方案，提高切换上线的成功率。

演练流程

建议正式切换前做2~3次演练，切换演练的流程如下：

图 6-35 演练流程



1. **演练准备**

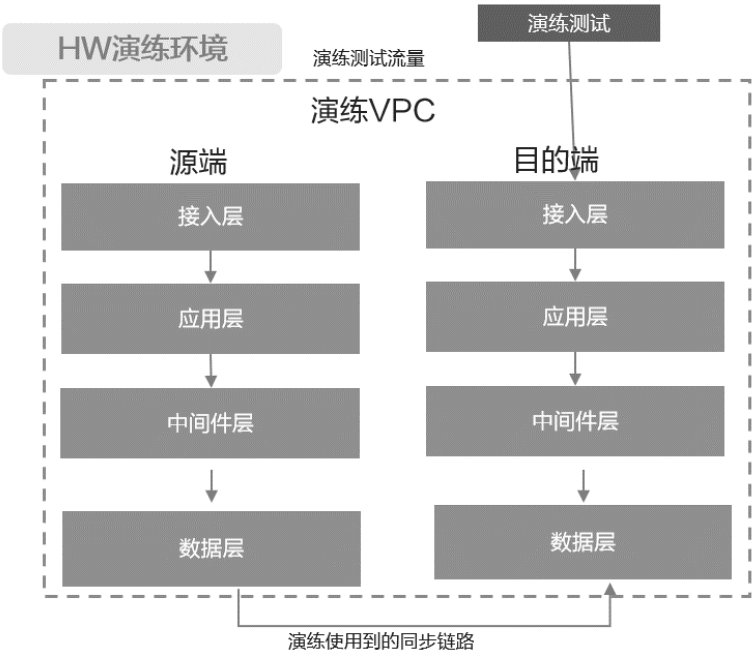
   演练的准备内容主要包括如下几个方面：

2. **演练地点或会议室的准备：**提前确定演练的地点（几楼）和哪个会议室，提前进行会议室的预定。
3. **人员准备和角色分工：**明确参与演练的各方人员及其责任分工，演练人员和最终切换操作人员尽量保持一致。演练角色可以参考**设计Runbook**的Runbook角色设计。
4. **演练Runbook准备：**按照演练环境细化演练Runbook，并组织多轮评审，最终定稿。
5. **演练环境准备：**演练需要有演练的源端和演练的目的端。演练环境的源端需要能真正的模拟生产环境，数据尽量和生产保持一致。提前进行数据的预置，环境的检查等。

   演练环境的准备有2种方案，企业可以结合实际情况，选择合适的方案：

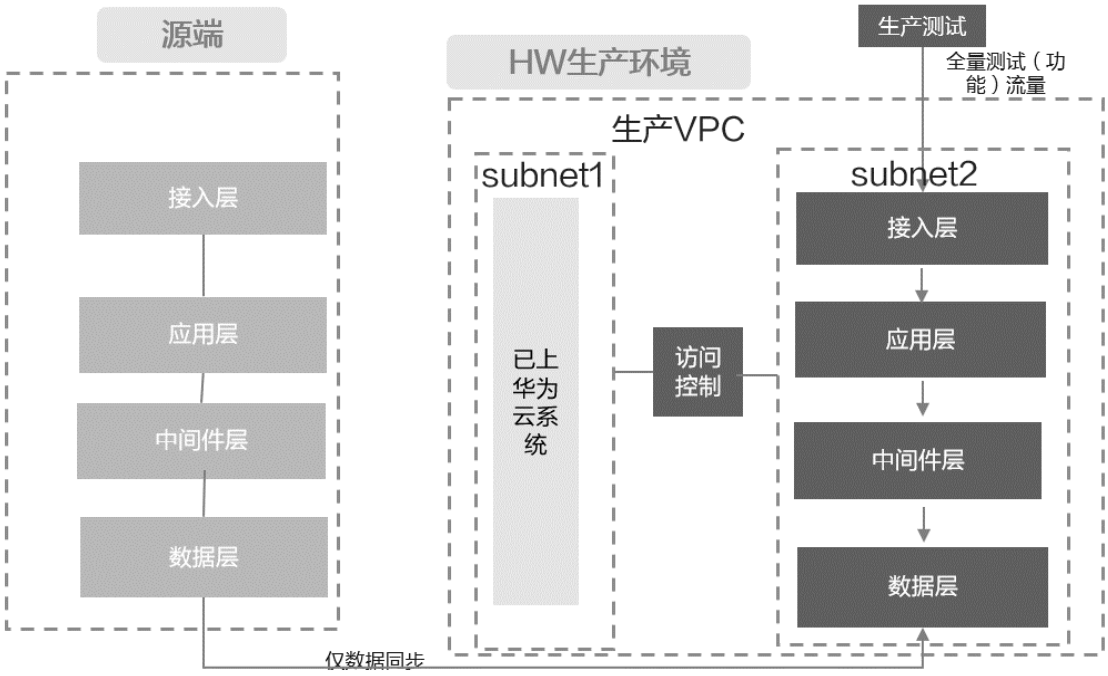
   a. 若企业没有能真正模拟生产的测试环境做演练，则需要在华为云搭建一个完整的源端、目的端环境，用于模拟演练源端到目的端的切换步骤。

   图 6-36 演练环境



   b. 若企业源端有测试或预生产环境可以用作演练的源端，则只需在华为云搭建一套目的端即可。演练的目的端也可以复用华为云的生产环境，但是需要注意和生产环境要做好隔离，否则可能演练过程影响生产，造成重大事故。

图 6-37 演练环境



6. **演练实施和复盘**

- **演练实施通常按照如下步骤进行：**
  a. 引导员宣读演练纪律和注意事项
  b. 引导员按照Runbook步骤宣读操作任务、操作人、确认人（注意：可能涉及多任务并行执行）。
  c. 操作人按照Runbook执行此步骤
  d. 确认人进行复合确认
  e. 确认人复核确认后，及时通报给引导员（注意：若一个步骤涉及多个确认人，为了方便引导员实时查看执行进展，确认人确认完毕后，将自己的完成状态登记在在线共享文档中）
  f. 如此循环，直到在引导员的引导下完成所有步骤的执行
  g. 演练结束后，操作人和确认人要及时记录操作过程中的问题，为演练复盘做准备。
- **演练复盘通常按照如下步骤进行：**
  a. 把演练记录的问题进行归类整理，包括技术问题和演练组织方面的其他问题
  b. 组织演练复盘，回顾每一个问题的事件、分析根因、讨论下一步改进措施
  c. 具体改进措施落实到人，更新到下次的演练Runbook或正式Runbook中

6.4.8.2 正式切换

正式切换的组织、准备和角色分工同切换演练基本一致，这里不再重复介绍。切换实施时，按照正式切换Runbook执行。不同业务系统的切换方案不同，对应的切换Runbook步骤也会不同，下面Runbook切换步骤仅供参考：

步骤1 切换前准备和检查

正式切换前，先要按照Runbook Check List做切换前准备和检查，不同业务系统的切换Runbook准备和检查步骤会有所不同，下面步骤仅供参考：

表 6-35 切换前准备和检查项

大类	前置工作项	责任部门	活动	是否涉及	是否完成
组织和保障准备	确定停机切换窗口	企业项目经理	确定停机切换窗口为：X月X日X时X分开始	是	是
	确认停机公告图片和话术	企业项目经理	确认停机公告图片和话术已更新为最新版本	是	是
	通知相关人员发布官网公告	企业项目经理	邮件发送通知相关人员进行官网公告发布	是	是
	预约会议作战室	企业项目经理	会议室布置安排	是	是
	切换相关人员通知和核对	企业项目经理	确认切换参与人员是否可以出席	是	否
		企业项目经理	第三方配合切换当晚参与人员和联系方式确定	是	是
		企业项目经理	停服切换期间，运营中心值班人员就位	是	是
	企业内部发送内部微信群通知	企业项目经理	切换微信群名：XX项目切换群	是	是
	云厂家建立后端保障团队	云厂家项目经理	云厂家建立和客户的联合切换保障团队 云厂家单独拉通后端运维和研发组建保障welink群	是	是
第三方/业态影响沟通和提醒	第三方/业态提前通知项	企业项目经理	分别与业态沟通停机影响和应对方案	是	否
		运维团队	对于第三方调用固定IP地址的情况，确认配置修改详细步骤	是	否
环境清单核对	确定发版暂停的截至日期	研发团队	确定发版暂停的截至日期	是	否
	应用清单检查并刷新启停脚本	研发团队	研发人员Check上云应用清单	是	否
	JOB清单检查并刷新脚本	研发团队	Check最新的job清单	是	否
		研发团队	检查脚本中的清单是否是最新的	是	否

大类	前置工作项	责任部门	活动	是否涉及	是否完成
环境（源端、目的端、迁移任务、执行脚本）检查	云服务基础检查项	运维团队	确认运维提供的测试wifi是否已准备就绪	是	否
		运维团队	检查华为云专线同步带宽使用是否有超带宽的告警	是	否
		运维团队	云厂家后端保障人员进行日常状态检查	是	否
		运维团队	云服务高可性检查，确认目标端云资源是否存在单AZ或单点故障问题	是	否
	数据库检查项	数据库相关	检查华为云数据库端口是否和生产保持一致	是	否
		数据库相关	检查NTP时钟设置是否一致	是	否
		数据库相关	检查中间件Reids数据迁移任务状态正常，无异常报错或告警（包含回退任务）	是	否
		数据库相关	检查DRS-mysql数据迁移任务状态‘增量迁移中’，无异常报错或告警（包含回退任务），数据动态比对任务配置完成	是	否
		数据库相关	检查DRS-mongodb数据迁移任务状态‘增量迁移中’，无异常报错或告警（包含回退任务）	是	否
		数据库相关	检查MySQL数据库源和目的端字符集是否一致	是	是
		数据库相关	数据库确认源端和目的端库用户一致	是	是
	周边系统配合检查项	大数据相关	修改大数据抽数的数据库地址为IDC备库地址	是	否
	执行脚本检查	运维团队	应用服务启动脚本放在执行机	是	否
		运维团队	应用心跳检查脚本放在执行机	是	否
	日志系统检查	运维团队	检查ELK日志平台，是否能承受大量应用启动时产生的大量日志	是	否

大类	前置工作项	责任部门	活动	是否涉及	是否完成
	告警监控系统检查	运维团队	监控系统是否正常	是	是
	磁盘无用信息清理	运维团队	生产环境检查磁盘使用情况，提前执行脚本批量清理磁盘	是	是
操作指导书、工具、终端和登陆平台准备	通知全员更新到最新的Runbook	项目经理	同步最新生产Runbook地址给切换全员（包含业态人员）	是	否
	相关人员准备	项目经理	人员最后一次熟悉整体切换流程以及各自操作指导	是	否
	相关人员操作权限检查	ALL	人员登录操作环境检查操作权限（登录系统，OS，操作界面等）	是	否
		测试团队	ITSM是否可以正常登录?是否可以正常记录上云项目的问题?	是	否
		ALL	登录批处理任务平台后检查当天操作人员是否有操作执行器的权限	是	否
	操作终端检查	ALL	具体到人，割接、演练前一晚必须确保笔记本，环境等无异常（DBA单独一根网线，提前准备好大交换机）	是	否
	测试客户端检查	测试团队	测试人员清理客户端以及浏览器缓存	是	否

----结束

步骤1 Runbook切换操作

完成切换前准备和检查后，企业就可以按照Runbook中的计划和步骤进行正式切换了，每个任务都要严格按照Runbook中的操作命令进行操作，不同业务系统对应的切换Runbook步骤会有不同，下面步骤仅供参考，注意步骤顺序标号一致的表示是并行执行。

如果批处理任务较多，切换时间窗有限，可根据优先级分批次进行启动。

表 6-36 切换操作步骤样例

任务	步骤顺序	子任务

源端业务流量转发至维护公告页面	1.1	变更CMDB业务状态为维护中
	1.2	外部访问流量转发至维护公告页面
停止源端定时任务	2.1	停止源端的定时任务
	2.1	停止源端的数据库定时任务
停止源端应用服务及配置中心	3.1	停止源端应用服务（xxx个）
	3.1	停止源端配置中心
消息队列数据迁移	4.1	消息队列MQ数据迁移
	4.2	等待&确认kafka消费完成
确认源端的数据层数据静止	5.1	确认源端的redis数据静止
	5.1	确认源端的MySQL数据静止
	5.1	确认源端的MongoDB数据静止
数据一致性对比	6.1	redis数据一致性对比、停止同步任务
	6.1	MongoDB数据一致性对比、停止同步任务
	6.1	MySQL 数据一致性对比、停止同步任务
修改数据层的DNS内网域名解析	7.1	修改应用间访问的内部域名-》华为云上应用实例
	7.1	修改目的端redis的内网域名-》华为云实例IP
	7.1	修改目的端的MySQL的内网域名-》华为云实例IP
	7.1	修改目的端MongoDB的内网域名-》华为云实例IP
	7.1	修改目的端消息队列MQ的内网域名-》华为云实例IP
	7.1	修改目的端Kafka的内网域名-》华为云实例IP
启动配置中心、定时任务调度服务、JOB注册、开启kafka消费开关	8.1	启动配置中心
	8.2	启动定时任务调度服务
	8.3	批量发布配置中心配置（执行JOB注册）
	8.3	批量发布配置中心配置（开启kafka的消费开关）
	8.4	检查阿配置中心和定时任务调度服务的开关是否正确
内网停机公告撤销&启动目的端应用&检查	9.1	启动目标端消息队列MQ
	9.2	启动目的端应用服务（xxx个服务）

	9.3	心跳检查
	9.4	基础业务检查
	9.5	取消内网转发至维护公告页面
启动目的端的数据库定时任务和优先级最高的定时任务）	10.1	启动数据库定时任务
	10.1	启动目的端第一批批处理任务
主流程测试（P0用例）	11.1	主流程测试（P0用例） ● 进行验证测试，确保应用程序在目标云环境中正常运行。 ● 验证核心功能和关键业务流程，确保与迁移前一致。 ● 监测日志和指标，确保系统运行情况正常。
外网停机公告撤销	12.1	取消外网转发至维护公告页面
启动目的端第二批批处理任务	13.1	启动目的端第二批批处理任务
	13.2	
P1业务验证 （启动JOB后，P1用例验证）	14.1	验证目的端业务功能
启动目的端第三批批处理任务	15.1	启动目的端第三批批处理任务
启动目的端第二批批处理任务	13.1	启动目的端第二批批处理任务

----结束

6.4.9 保障

在上云迁移的保障阶段，需要执行以下任务来确保顺利过渡到新的云环境：

- **云平台监控：**确保建立有效的监控系统，跟踪云平台的性能、可用性和安全性。设置警报机制，及时发现并解决潜在的问题。
- **系统监控和运维：**设置系统监控和告警，确保及时发现和解决潜在的问题。配置基础设施监控工具，监测服务器、存储、网络等关键指标，并确保日志记录和错误报警机制正常运行。
- **安全检查和漏洞修复：**进行安全检查，查找可能存在的漏洞或弱点，并采取适当的补救措施来加强安全性。更新和修补系统和软件，确保使用的组件和版本都是最新的，并及时应用安全补丁。
- **备份和灾难恢复策略：**评估和设置新的备份和灾难恢复策略，确保数据的安全性和可恢复性。执行定期备份，并进行灾难恢复演练来验证备份的可用性和恢复过程。

- **优化和调整：**根据实际运行情况，进行系统和应用程序的优化和调整。监测性能指标，识别瓶颈和性能问题，并针对性地进行调整和优化，以提升系统的稳定性和响应能力。
- **培训和支持：**提供必要的培训和支持给运维团队，确保熟悉新的云环境和工具。
- **文档输出：**记录并维护文档，以供将来参考和备案。

6.5 大数据迁移

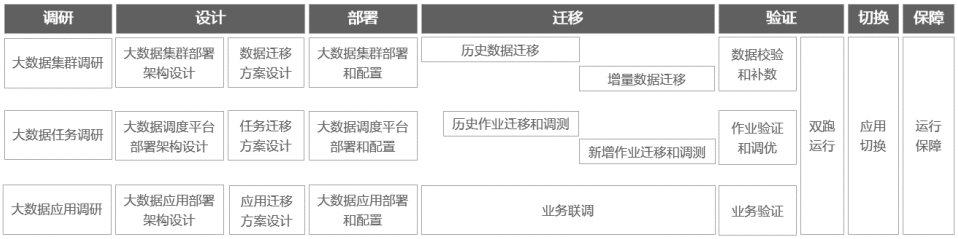
6.5.1 调研

大数据迁移是指将大数据集群、大数据任务调度平台和大数据应用从一个运行环境迁移到另一个运行环境的过程。它包含如下三个模块，本节重点介绍的是大数据集群和大数据任务调度平台的迁移，大数据应用的迁移方法请参考**应用迁移上云**，本节只介绍差异部分。

- **大数据集群迁移：**将大数据集群（包括存储、计算和管理组件）迁移到新的运行环境，包括集群的重新配置和数据迁移。集群迁移需要考虑数据的迁移方式、网络传输速度、兼容性和数据一致性等因素。
- **大数据任务调度迁移：**是将现有的大数据任务调度系统、工作流和调度策略迁移到新的运行环境，包括梳理任务依赖关系、任务适配和改造、任务调优、部署、测试和验证。
- **大数据应用迁移：**是将基于大数据应用从一个运行环境迁移到另一个运行环境。

大数据迁移遵循如下的流程：

图 6-38 大数据迁移流程



其中大数据应用的迁移请参考**应用迁移上云**，本章只对大数据应用迁移的特殊注意点进行描述。

大数据迁移流程每个阶段概述如下：

1. **调研：**调研大数据平台的版本和配置信息、数量类型和数据量、任务类型和任务量。
2. **设计：**设计大数据的部署架构、数据迁移方案、任务迁移方案和数据校验方案。
3. **部署：**部署大数据平台，包括集群部署和任务调度平台部署。
4. **迁移：**实施数据迁移和任务迁移。
5. **验证：**进行数据校验和任务验证。
6. **切换：**配合大数据应用进行切换。
7. **保障：**业务切换后进行一段时间的实时监控和特别运维保障。

请参考**大数据调研**的调研方法，调研大数据集群、大数据任务调度平台和大数据应用的现状信息。

6.5.2 设计

大数据在云上的部署架构设计请参考**大数据架构设计**，本节不再赘述。这里重点介绍数据迁移方案和任务迁移方案的设计。

设计数据迁移方案

大数据的数据迁移涉及到3类数据，如下表：

表 6-37 大数据迁移的三类数据

分类	说明
元数据	Hive元数据或外置元数据
存量数据	历史数据，短期内不会变化
增量数据	数据定期更新

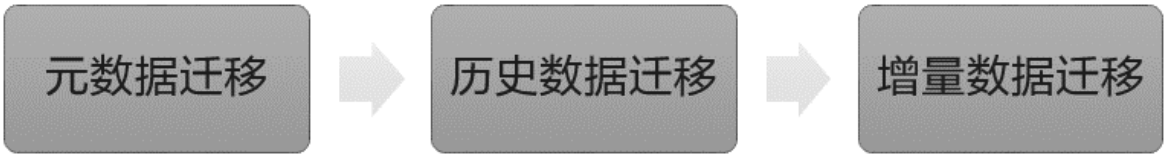
这3类数据的迁移方法如下：

表 6-38 大数据三类数据的迁移方式

数据分类		迁移方法
元数据	HIVE元数据	导出源端HIVE元数据，导入华为云MRS-Hive
	外置元数据MySQL	使用华为云DRS服务同步MySQL中的元数据到云上RDS
存量数据	Hive历史数据存放在HDFS	使用华为云CDM工具迁移所有历史数据到华为云MRS服务或华为云OBS存储（存算分离场景）
	Hbase历史数据	1. 使用华为云CDM工具迁移所有历史数据到华为云MRS服务 2. 使用Hbase快照方式，迁移Hbase数据到华为云MRS服务
增量数据	Hive增量数据	根据源端元数据查询每日变化数据，识别出需要迁移的数据目录，使用华为云CDM工具迁移增量数据上云
	Hbase增量数据	使用华为云CDM工具迁移所有增量数据(根据时间戳)到华为云MRS服务

企业可以根据不同的数据类型选择合适的迁移方案，CDM是数据迁移阶段主要使用的工具。大数据的数据迁移通常按照如下顺序执行：

图 6-39 大数据的数据迁移顺序



- **元数据迁移**

  首先，进行元数据的迁移。元数据是描述数据的数据，包括数据结构、数据定义、数据关系等信息。在元数据迁移阶段，需要将原始数据的元数据信息导出，并在目标系统中重新建立或导入元数据，以确保目标系统能够正确理解和解析数据。

- **历史数据迁移**

  在元数据迁移完成之后，进行历史数据的迁移。历史数据是指在过去某个时间段内生成的数据，它们需要被迁移到目标系统中进行后续的分析和处理。历史数据迁移可能涉及将数据从原始存储位置导出，并按照预定的规则和格式加载到目标系统中。

- **增量数据迁移**

  当历史数据迁移完成后，进行增量数据的迁移。增量数据是在历史数据迁移之后生成的新数据，需要实时或定期迁移到目标系统中。增量数据迁移通常通过数据同步或数据传输的方式进行，确保新数据能够及时和准确地被目标系统所使用。

设计数据校验标准

在大数据迁移过程中，并不是所有数据类型都要求100%的数据一致，需要根据业务需求和数据的重要性来确定数据一致性的要求，并采取相应的数据迁移策略和技术手段来保证数据的正确性和完整性。

1. **从数据类型来看：**对于包含事务性数据（例如银行交易记录），通常需要确保迁移过程中的数据一致性。这意味着在迁移完成后，源数据和目标数据需要精确匹配，以避免数据不一致引发的问题。而对于非事务性数据，一些微小的数据差异可能是可以接受的。
2. **从数据重要性来看：**关键业务数据对于迁移过程中的数据一致性要求更高，这些数据可能包含了企业核心业务的重要信息，因此在迁移过程中需要确保数据的准确性和完整性。而对于非关键性业务数据，一些小的数据差异可能可以被容忍。

因此在数据迁移实施前，企业需要确定不同数据的校验标准，可以参考如下模板：

表 6-39 数据类型和校验标准

数据类型	校验标准	详细表名
X类数据	100%一致	A表、B表、C表…
Y类数据	误差小于0.01%	D表、E表、F表…
…	自定义标准	…

设计任务迁移方案

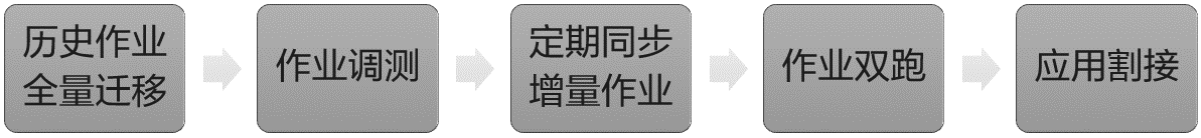
大数据的任务包括三类：Jar类任务、SQL类任务、脚本类任务（Python、Shell），可以根据不同的任务类型选择合适的迁移方案。

表 6-40 任务类型和迁移方案

任务类型	迁移方案
JAR类任务	• 所有Jar类任务都需要根据云上集群版本重新编译jar包，适配云上环境
SQL类任务	• 同版本： Hive大版本相同，可平迁SQL类任务 • 不同版本：Hive大版本不同，先平迁SQL类任务，然后根据版本语法变动，微调SQL语句以适配云上版本语法
脚本类任务（Python、Shell）	• 同调度平台：平迁脚本类任务 • 不同调度平台：平迁脚本类任务，根据云上调度平台，对脚本进行适配改造，以适应新的调度平台运行环境

大数据任务迁移通常按照如下顺序执行：

图 6-40 大数据的任务迁移顺序



1. **历史作业全量迁移**

   首先，将历史作业的数据和相关代码迁移至新的大数据平台。这包括将数据从原来的存储系统导出，并重新加载到新的存储系统。同时，将原有的作业脚本和相关配置文件进行调整和迁移，以适应新的计算环境。

2. **作业调测**

   在全量迁移完成后，对已迁移的历史作业进行调测和验证。这包括运行作业并检查输出结果是否符合预期，以及验证作业执行过程中的性能和稳定性。如果发现问题或异常，需要进行适当的调整和修复。

3. **定期同步增量作业**

   在历史作业成功迁移并通过调测后，开始进行增量作业的迁移和同步。增量作业是指在迁移过程中新增的、需要定期运行的作业。

4. **作业双跑**

   在增量作业迁移和同步成功后，进行作业双跑。作业双跑是指在新的大数据平台上同时运行原有系统和新系统的作业，以验证新系统的结果和原有系统的一致性。这可以通过比较作业输出、日志和指标等来判断两个系统的结果是否一致。

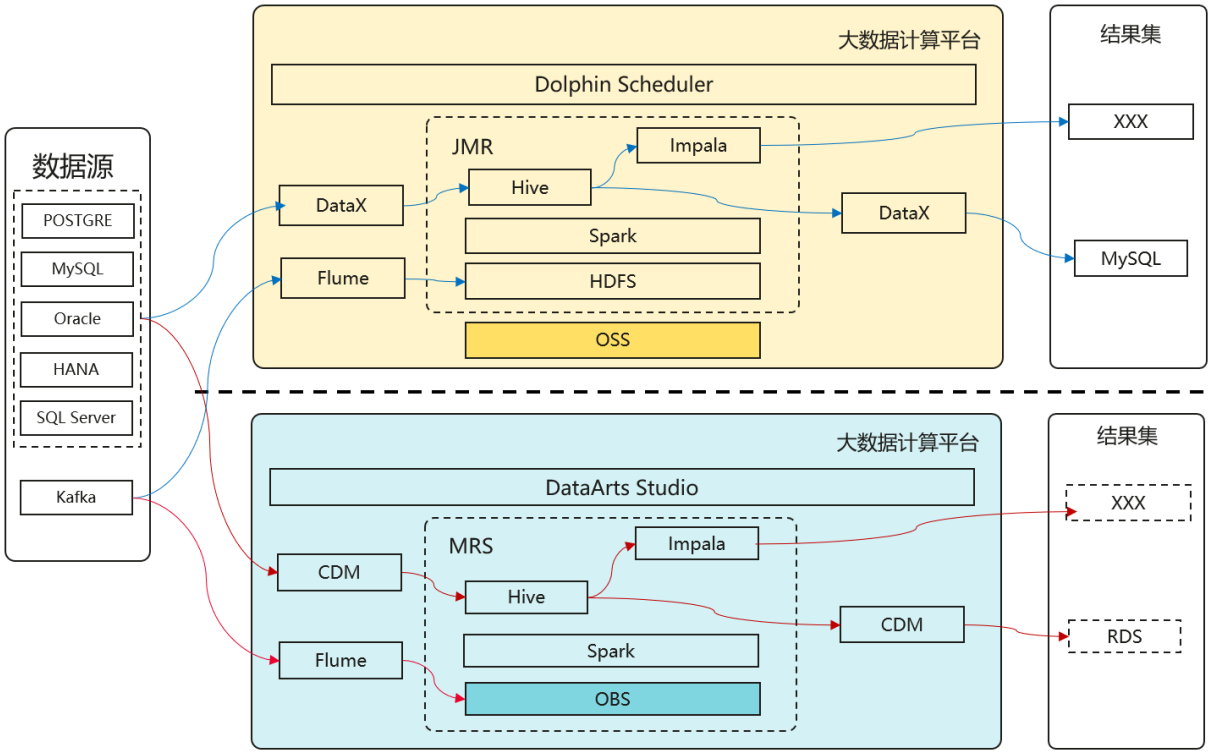
5. **应用割接**

   最后，作业双跑一段时间没有问题后，就可以进行大数据应用割接，业务全部切换到新大数据平台。

6. **设计大数据双跑方案**

   双跑方案是一种常见的大数据迁移策略，通过双平台同时运行，持续验证数据和任务，双跑运行一段时间稳定以后，再将业务切换到新的大数据平台。如下图：

图 6-41 大数据双跑方案



双跑方案的设计思路如下：

a. **数据和任务迁移**

在数据源接入前，先进行数据和任务的迁移，包括将历史数据从原平台迁移到新的大数据平台，并迁移相关的作业代码、脚本和配置文件等。迁移工具和方法根据具体需求选择，例如使用离线数据传输工具、大数据迁移工具CDM等。

a. **数据源接入**

将目标大数据集群接入与原大数据集群相同的数据源。这确保了源数据的一致性。可以使用数据同步工具、ETL工具或自定义脚本等方式实现数据源的连接和数据同步。离线计算任务的数据源可以使用数据同步工具CDM、ETL工具或自定义脚本实现数据接入；对于实时计算任务的数据源，可以使用Kafka MirrorMaker、Nginx流量镜像配置等方式，将实时数据上报到双跑的两个平台。

a. **双平台同时运行**

目标大数据集群、任务调度平台与原大数据集群、任务调度平台同时运行一段时间。在这段时间内，两个平台会并行处理任务，并产生相应的结果。

a. **运行稳定性验证**

在双平台同时运行期间，需要对目标大数据平台任务执行的稳定性、数据一致性进行持续的观察和验证。这包括监测任务的执行情况、检查任务日志和结果的一致性等。如果发现任何问题或异常情况，需要及时处理和修复。

a. **业务正式切换**

在确认目标大数据集群和任务调度平台的运行稳定性以及数据和任务迁移的完整性和准确性后，可以进行业务的正式切换，这包括将业务流量和作业任务切换到目标大数据平台上，并停止原大数据集群和任务调度平台。

6.5.3 部署

大数据平台部署

大数据平台的部署可以参考如下方法：

- **大数据集群部署**

  基于架构设计的原则，云上大数据集群一般采用云服务。华为云MRS是一个在华为云上部署和管理Hadoop系统的服务，一键即可部署Hadoop集群。MRS提供租户完全可控的企业级大数据集群云服务，轻松运行Hadoop、Spark、HBase、Kafka等大数据组件。具体部署方法可参考**MRS官网文档**。

- **大数据任务调度平台部署**

  如果目标架构是采用华为云的任务调度平台DataArts Studio，可以参考如下**官网文档**进行部署和配置。

  如果目标架构是采用自建的大数据任务调度平台，有2种方法部署，可以基于华为云ECS重新部署大数据任务调度软件，或者是使用华为云SMS工具将源端调度平台迁移到华为云ECS。

- **大数据应用部署**

  大数据应用的部署有2种方法，可以基于华为云ECS重新部署大数据应用，或者是使用华为云SMS工具将大数据应用迁移到华为云ECS。

平台权限配置

- **平台权限配置**

  在部署好目标大数据平台后，为了确保正确的权限设置，可以参考源端平台的权限设置，并按照以下步骤进行设置：

- **审查源端权限设置**

  仔细审查源端平台的权限设置，包括用户、角色、组织结构和权限级别等信息。了解每个用户的权限范围和访问权限，以便在目标平台上进行对应的设置。

- **创建用户和角色**

  根据源端平台的权限设置，创建相应的用户和角色。确保在目标平台上设置与源端平台一致的用户身份和角色分配。

- **调整权限级别和范围**

  在目标平台上，根据源端平台的权限设置，调整权限级别和范围。确保目标平台上的权限设置与源端平台一致，并确保用户只能访问其应有的资源。

- **权限分配和继承**

  在目标平台上，根据源端平台的权限设置，对用户进行权限分配和继承。确保用户在目标平台上具有与源端平台相同的权限，并能够继承相应的角色和权限设置。

- **审查和调整访问控制**

  审查目标平台上的访问控制机制，并根据源端平台的权限设置进行调整。确保访问控制能够限制用户的访问范围，并遵循源端平台的权限规则。

- **安全审计和监测**

  设置安全审计和监测机制，确保目标平台上的权限设置得到有效的审计和监测。这可以帮助发现和防止未经授权的访问，并及时采取相应的措施。

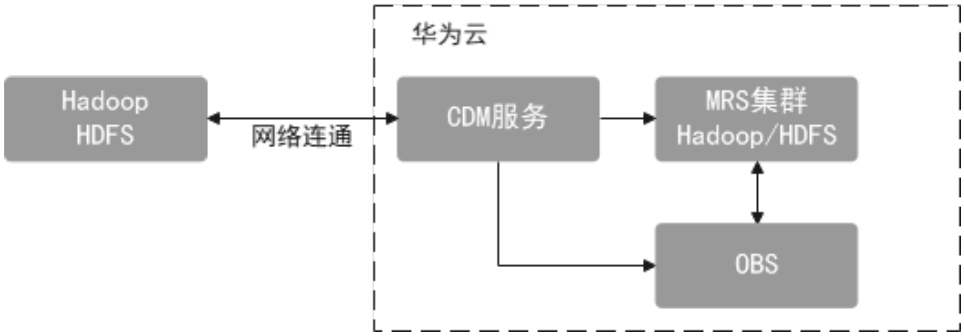
6.5.4 迁移

数据迁移

1. **Hadoop数据迁移到华为云MRS服务**

   如图所示，将IDC机房或者其他公有云的Hadoop集群中的数据迁移到华为云MRS服务。详细操作指导请参考**官网文档**。

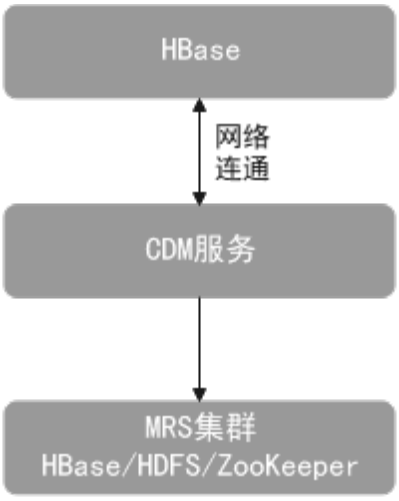
   图 6-42 Hadoop 数据迁移



2. **HBase数据迁移到华为云MRS服务**

   将IDC机房或其他公有云的HBase集群中的数据迁移到华为云MRS服务。HBase会把数据存储在HDFS上，主要包括HFile文件和WAL文件，由配置项“hbase.rootdir”指定在HDFS上的路径，华为云MRS的默认存储位置是“/hbase”文件夹下。HBase自带的一些机制和工具命令也可以实现数据搬迁，例如：通过导出Snapshots快照、Export/Import、CopyTable方式等，可以参考Apache官网相关内容。也可以使用华为云CDM云迁移服务进行HBase数据搬迁，详细操作指导请参考**官网文档**。

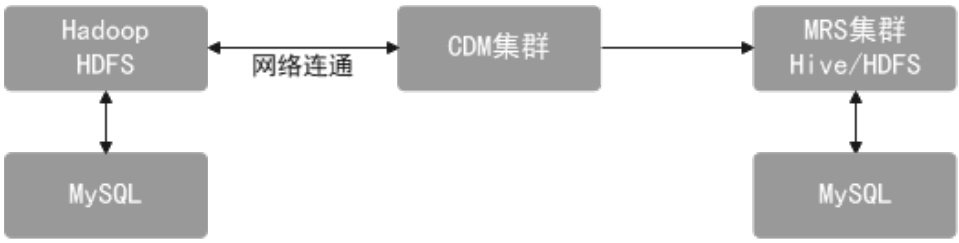
   图 6-43 HBase 数据迁移



3. **Hive数据迁移到华为云MRS服务**

   使用华为云CDM服务可以很方便将IDC机房或者其他公有云Hive集群中的数据迁移到华为云MRS服务，详细操作指导请参考**官网文档**。

图 6-44 Hive 元数据迁移



4. **使用BulkLoad向HBase中批量导入数据**

   企业经常面临向HBase中导入大量数据的情景，向HBase中批量加载数据的方式有很多种，最直接方式是调用HBase的API使用put方法插入数据；另外一种是用MapReduce的方式从HDFS上加载数据。但是这两种方式效率都不是很高，因为HBase频繁进行flush、compact、split操作需要消耗较大的CPU和网络资源，并且RegionServer压力也比较大。使用华为云MRS服务时，推荐的方法是使用BulkLoad方式向HBase中批量导入本地数据，在首次数据加载时，能极大的提高写入效率，并降低对Region Server节点的写入压力。详细操作指导请参考**官网文档**。

5. **MySQL数据迁移到MRS集群Hive分区表**

   Hive的分区使用HDFS的子目录功能实现，每一个子目录包含了分区对应的列名和每一列的值。当分区很多时，会有很多HDFS子目录，如果不依赖工具，将外部数据加载到Hive表各分区不是一件容易的事情。云数据迁移服务（CDM）可以轻松将外部数据源（关系数据库、对象存储服务、文件系统服务等）加载到Hive分区表。详细操作指导请参考**官网文档**。

6. **MRS HDFS数据迁移到OBS**

   CDM支持将MRS HDFS的数据迁移到OBS，详细操作指导请参考**官网文档**。

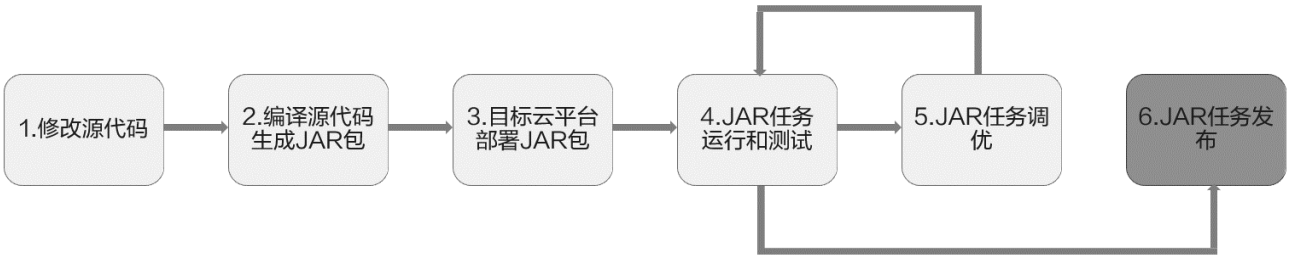
7. **任务迁移**

   大数据任务迁移是指将大数据任务从一个调度平台迁移到另一个调度平台的过程，主要涉及Jar类任务、SQL类任务、脚本类任务，以下简要介绍这三类任务的迁移实施方法。

8. **Jar类任务迁移**

   迁移Jar类任务需要深入了解源端任务的源代码和依赖库，重新编译代码以生成适用于云环境的可执行Jar文件，并进行充分的验证和调优。可以参考以下步骤进行：

图 6-45 Jar 类任务迁移流程



前提：Jar类任务调试依赖的数据已完成迁移，迁移方法请参考前面的数据迁移部分的内容。

a. 根据云上大数据资源配置，修改源代码，例如版本、依赖库、数据库连接串，以及本地开发环境的库依赖配置等。

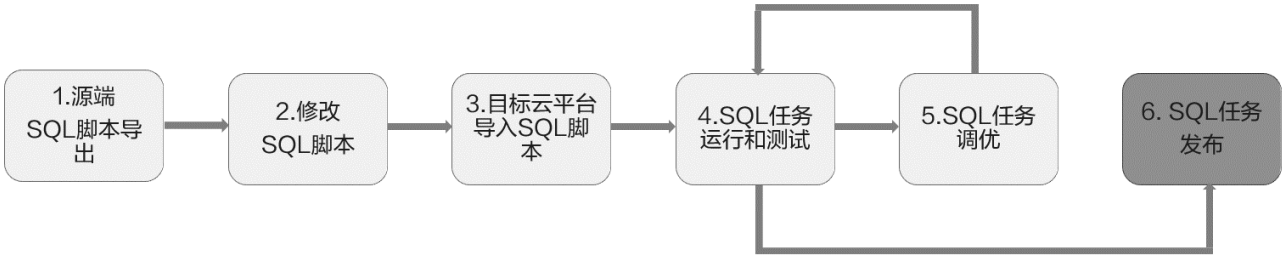
b. 编译源代码，生成云上环境可执行的Jar包。
c. 上传Jar包，并在任务调度平台部署和配置Jar包。
d. 执行调度任务，并根据日志检查任务执行状态和结果。
e. 如果任务执行不符合预期，例如执行时间过长，需要查找根因并进行优化和验证。
f. 按业务需要的时间配置调度任务。

您如果使用华为云的**DataArts Studio**作为大数据任务调度平台，可以参考**官网文档**进行Jar作业的配置。

9. **SQL类任务迁移**

迁移SQL类任务时，主要工作是对SQL脚本进行适配改造，可参考如下步骤：

图 6-46 SQL 类任务迁移流程



前提：SQL类任务调试依赖的数据已完成迁移，迁移方法请参考前面的数据迁移部分的内容。

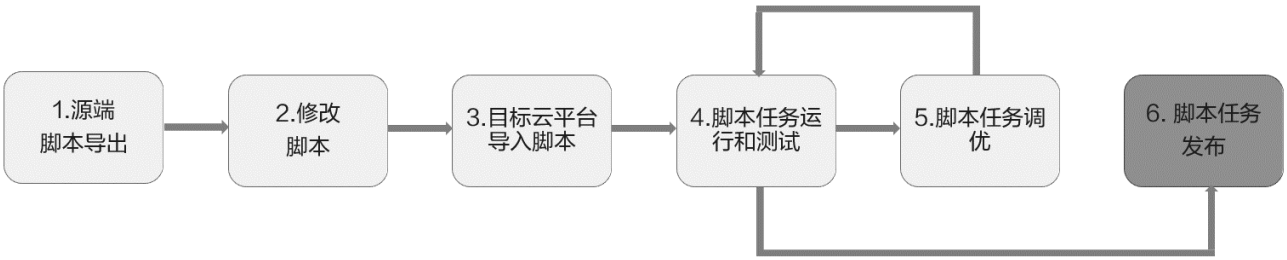
a. 源端SQL脚本导出：从源端任务调度平台导出SQL脚本。
b. 修改SQL脚本：根据云上调度平台的语法及资源配置修改SQL脚本。
c. 目标云平台导入SQL脚本：在云上任务调度平台配置SQL类任务，导入SQL脚本。
d. SQL任务运行和测试：执行SQL调度任务，通过日志和运行结果检查任务运行情况。
e. SQL任务调优：如果任务执行不符合预期，例如执行时间过长，需要查找根因并进行优化和验证。
f. SQL任务发布：按业务需要的时间配置调度任务，配置正确的任务依赖关系。

您如果使用华为云的**DataArts Studio**作为大数据任务调度平台，可以参考**官网文档**进行SQL作业的开发和配置。

10. **脚本类任务（Python、Shell等）迁移**

迁移脚本类任务时，同样面临云上环境适配问题，可以参考如下步骤进行：

图 6-47 脚本类任务迁移流程



前提：脚本类任务调试依赖的数据已完成迁移，迁移方法请参考前面的数据迁移部分的内容。

a. 源端脚本导出：从源端调度平台拷贝调度任务的可执行脚本。
b. 修改脚本：根据云上环境配置，修改脚本，例如数据库连接串，资源配置，输出目录等。
c. 目标云平台导入脚本：上传脚本到云上调度平台，并配置脚本类调度任务。
d. 脚本任务运行和测试：执行调度任务，并根据日志和执行结果检查脚本运行情况。
e. 脚本任务调优：如果任务执行不符合预期，例如执行时间过长，需要查找根因并进行优化和验证。
f. 脚本任务发布：按业务需要的时间配置调度任务，配置正确的任务依赖关系。

您如果使用华为云的**DataArts Studio**作为大数据任务调度平台，可以参考**官网文档**进行Shell脚本和Python脚本的开发和配置。

6.5.5 验证

- **数据校验**

  数据库的对比方法有数据库内容对比、对象对比、行数对比，文件的对比方法有文件数量对比，大小对比，内容对比。具体的数据对比的方法请参考章节**数据验证**的内容。

- **任务验证**

  大数据任务迁移后，要确保作业能够正常运行、产生准确的结果，并且满足性能要求。一般从如下三方面验证：

- **验证作业执行的成功率**

  在任务迁移完成后，对迁移后的大数据任务进行验证。这包括运行作业并检查作业的执行成功率。验证过程中，需要关注作业的状态、日志以及错误和异常情况。对于执行异常的任务，需要仔细检查和调试，找出问题并进行修复。

- **验证作业执行结果的一致性**

  验证大数据任务执行结果的一致性，对比新旧大数据平台的作业输出结果数据是否一致。可以使用对比工具、数据校验脚本或手动检查的方式进行验证。如果发现数据不一致的情况，可能需要考虑迁移过程中的数据转换、数据格式或数据处理逻辑的问题，并进行相应的修复和调整。

- **作业执行的性能验证**

  在迁移后，验证作业的执行性能，包括运行时间、资源利用率、并发性等。通过监测作业的执行指标和性能指标，可以评估迁移后的作业性能是否符合预期。如果作业的性能有问题，可能需要调整作业的配置参数、优化作业代码或考虑资源调配的问题。

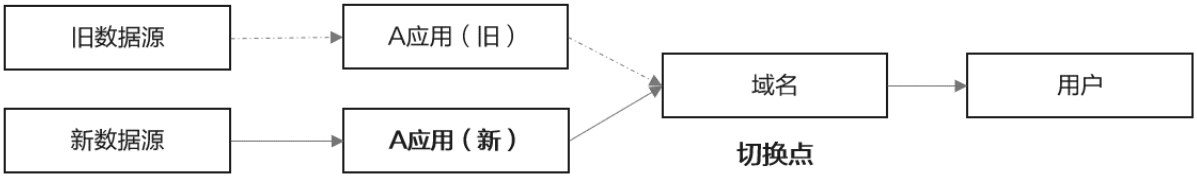
在作业验证过程中，可以使用监控工具、日志分析和数据校验等手段，确保迁移后的大数据任务的可靠性和稳定性。

6.5.6 切换

大数据的切换主要是指大数据应用的切换，其切换演练和正式切换的步骤请参考章节**切换**。本节重点介绍大数据应用切换的3个切换点，以便更好的指导大数据应用的切换。

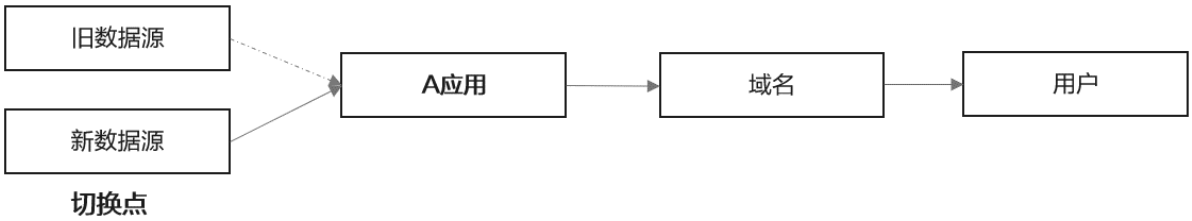
- **双跑场景：**大数据应用分别在源环境和目标环境各部署一套，实现双跑，切换点在域名，业务切换时只需要进行域名的切换，将业务流量切换到新应用。

图 6-48 双跑场景



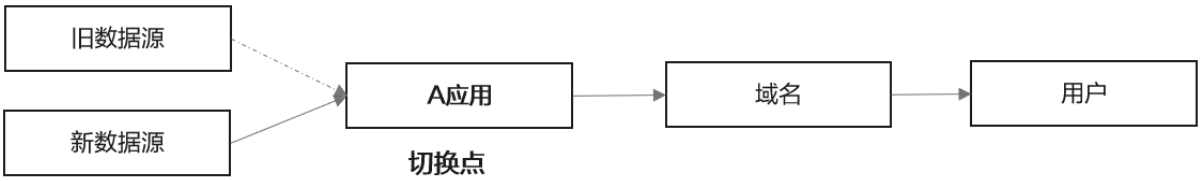
- **推数场景：**适用于数据源主动向应用推数的场景，切换点在数据源，需要停止旧数据源推数，配置并启动新数据源向应用推数，将应用的数据源从旧数据源切换到新数据源。

图 6-49 推数场景



- **抽数场景：**适用于应用向数据源抽数的场景，切换点在应用，需要先停止应用向旧数据源抽数，然后配置并启动应用从新数据源抽数，将应用的数据源从旧数据源切换到新数据源。

图 6-50 抽数场景



6.5.7 保障

在大数据迁移的保障阶段，需要执行以下任务来确保顺利过渡到新的云环境：

- **监控和警报设置：**建立实时监控系统，监测集群、任务调度平台和应用程序的运行状态。设置警报，以便及时发现潜在的问题并采取措施。
- **优化集群性能：**对大数据集群进行性能评估和调优。监视资源使用情况，优化配置参数、调整集群大小和资源分配，以提高整体性能。
- **数据安全和权限管理：**审查和加强数据的访问控制和权限管理机制。确保只有经授权的人员可以访问敏感数据，并采取适当的加密和脱敏措施保护数据安全。
- **自动化任务调度：**确保大数据任务调度平台的运行和调度正常。优化调度策略，确保任务按时准确完成，并处理可能的故障或异常情况。
- **异常处理和故障恢复**：建立故障处理和恢复计划，包括对集群、任务和应用程序可能出现的问题进行分类并定义相应的响应和恢复步骤。
- **团队培训和知识共享**：培训团队成员以适应新的环境和技术栈。建立知识分享机制，促进团队内部的交流和经验分享。

6.6 应用现代化

6.6.1 什么是应用现代化

把应用和数据搬“上云”并不是终点，上云只是数字化转型的开始，我们还需要持续进行巩固和优化，通过“应用现代化”来应对新的IT和业务的需求，支撑云上业务发展，“上云”只是做了搬运工和架构师的事，“云上”我们要做体验官，通过使用云的新技术来不断优化业务体验，支撑业务创新。

近年来各大云服务商都提出了应用现代化的愿景。数字化时代，企业能快速应对变化并实现敏捷创新，将成为未来企业构筑自身持续竞争力的决定性因素，应用现代化已经成为很多企业开展数字化转型过程的必然选择。传统应用要向现代化应用演进，应用现代化要结合应用实现和云平台能力综合考虑。云平台支持应用现代化进行分层解耦，应用聚焦业务逻辑，尽可能将DFx（Design for X）及治理等公共能力建立在云平台上。

图 6-51 现代化应用发展趋势

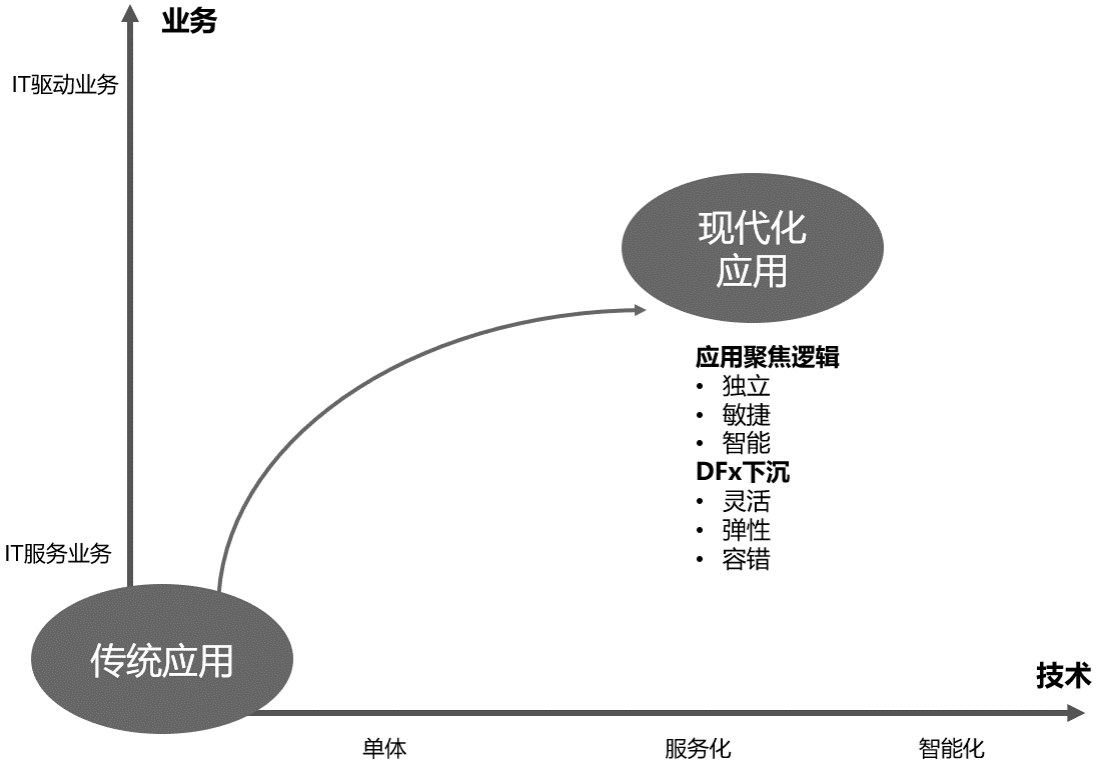


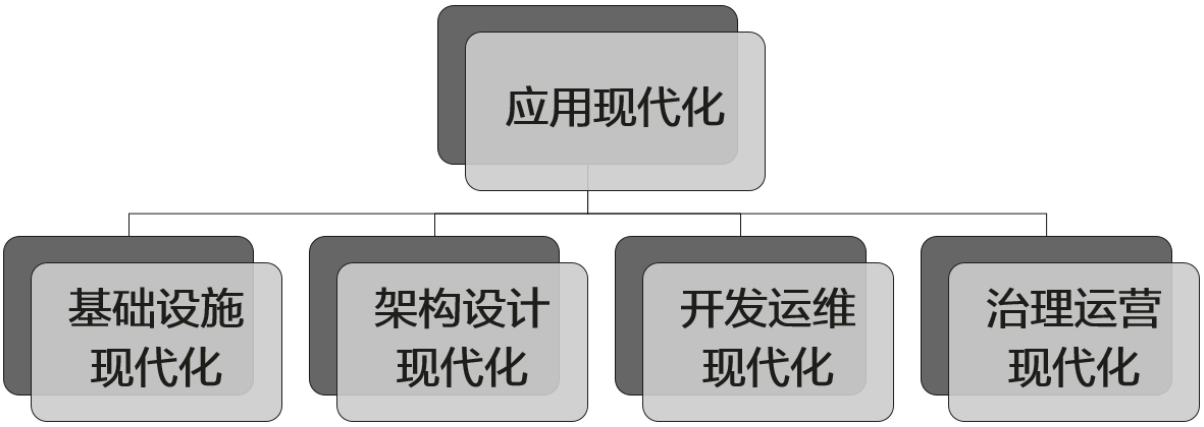
表 6-41 传统应用和现代化应用比较

传统应用	现代化应用
单体架构，模块间耦合度高	微服务化架构，应用间充分解耦，快速组合
应用入口多，影响用户体验	以用户为中心，一站式个性化体验
无法快速响应新业务变化	面对新业务可快速组合和按需定制

传统应用	现代化应用
新功能需求绑定大版本上线，需求交付周期长（年/月级）	快速迭代上线，交付周期缩短（周/天级）
团队规模大，传统开发模式	团队拆小，DevSecOps敏捷运作
物理服务器	容器化部署、全面上云

应用现代化不只是采用云原生技术（如容器、微服务、DevOps、API网关等），还包括新技术（如AI、数字人、IoT、区块链等）的应用，使业务能够跟上时代的潮流，提升用户体验和创新能力。应用现代化包括如下4个方面：

图 6-52 应用现代化的四个方面



- **基础设施现代化**，节约成本减轻用户使用的心智负担。通过传统设施的云原生化改造，实现基础设施的高可用与弹性，降低运维成本，把开发运维人员从重复繁琐的资源调配中解放出来，投入到有益于业务发展的工作。
- **架构设计现代化**，解耦可复用功能与业务逻辑。通过改造应用架构，使用微服务架构、Serverless（无服务器）架构等技术，将应用拆分为能独立快速发布的不同模块，使开发运维人员能聚焦于应用和创新工作。
- **开发运维现代化**，提升运维过程的自动化与安全性。通过建设以DevSecOps 为代表的开发运维安全一体化能力，让发布跟上开发的速度，让安全内置在开发运维中。
- **治理运营现代化**，整合全域新老资产推动架构可演进。通过全域融合集成、应用资产统一治理运营等技术实现应用的治理运营现代化，构建可平滑演进的应用架构，实现新老资产的价值最大化。

6.6.2 基础设施现代化

容器化改造是将传统应用程序或服务迁移至容器化环境的过程，以下是进行容器化改造的一般步骤：

- **评估和规划：**首先，评估应用程序或服务的特性、依赖关系和架构。确定哪些部分适合容器化，并制定一个改造计划。
- **容器化平台选择：**选择一个适合你的需求的容器化平台。最常见的容器化平台是Docker，但也有其他选择，如Kubernetes等。

- **容器化应用程序：**将应用程序拆分为较小的模块或微服务，并将每个模块打包为独立的容器镜像。使用Dockerfile定义容器镜像的构建过程，包括依赖安装、配置和启动命令。
- **容器编排与管理：**如果需要管理多个容器实例、自动扩展和负载均衡等功能，可以使用容器编排工具，如Kubernetes。通过编写配置文件或使用命令行工具，定义容器的部署和运行方式。
- **网络和存储配置：**配置容器之间的网络通信和访问外部资源的方式。确保容器可以与其他容器、数据库、消息队列等进行交互，并确保数据持久性和可靠性。
- **安全性和监控：**确保容器化环境的安全性，例如限制容器的权限、使用安全的镜像源、进行漏洞扫描等。同时设置监控系统，以便实时监测容器的性能和运行状态。
- **测试和部署：**在容器化改造完成后，进行全面的测试，包括单元测试、集成测试和性能测试。确保应用程序在容器环境中正常运行。然后，使用自动化工具或脚本将容器部署到生产环境中。
- **持续集成与交付：**建立持续集成与交付（CI/CD）流程，以便能够快速、可靠地构建、测试和部署新版本的容器化应用程序。

容器化改造是一个复杂的过程，需要仔细规划和评估。在开始之前，建议深入了解容器化技术和所选平台，并根据具体情况选择合适的工具和方法。

6.6.3 应用架构现代化

微服务改造上云

将传统的单体应用进行微服务改造并迁移到云环境是一个复杂的过程。下面是关于如何进行微服务改造和上云的一些基本步骤和考虑事项。

1. **评估现有应用和目标：**

   首先，对传统单体应用进行全面评估，了解其架构、功能和性能特点。同时，明确希望在云环境中实现的目标，例如可伸缩性、高可用性和灵活性等方面的要求。这个评估阶段可以帮助您确定是否适合将应用进行微服务改造和迁移到云上。

2. **拆分单体应用：**

   在微服务改造之前，您需要将单体应用拆分为更小的、独立的功能模块。这个过程通常被称为"分解单体"。通过仔细分析应用的业务逻辑和功能，识别出可以独立运行的模块，并将其划分为不同的微服务。每个微服务负责特定的业务功能，且应该是松耦合的，相互之间尽可能地独立。

   在拆分过程中，可以采用不同的策略，例如按照业务领域进行拆分（领域驱动设计）、按照功能模块进行拆分等。确保每个微服务具有清晰的职责，并通过清晰的接口定义它们之间的交互方式。

3. **定义服务边界和接口：**

   拆分后，您需要定义每个微服务的边界和接口。确定每个微服务暴露的外部接口以及它们之间的通信方式（例如使用RESTful API或消息队列）。在定义接口时，确保它们是清晰、一致且易于使用的。这样可以促进团队间的协作，并支持未来的扩展和变更。

   另外，考虑采用开放标准和协议，如OpenAPI规范（前身为Swagger）来定义接口。这将使得各个微服务之间的集成更加简单，同时也方便文档生成和代码生成。

4. **设计和实施服务治理：**

   在微服务架构中，服务治理变得至关重要。您需要考虑如何发现、注册、配置和监控您的微服务。选择适合您的需求的服务注册与发现工具（如Consul、Eureka等），并确保在整个服务生命周期中能够有效地管理、监控和维护微服务。服务注册与发现工具可以帮助您自动化服务的注册和发现过程，并提供服务的健康状态检查和负载均衡等功能。

   此外，还应该考虑负载均衡、故障恢复和服务安全等方面的问题。使用负载均衡机制来平衡请求的分发，确保每个微服务能够处理适量的负载。实施故障恢复机制（如断路器模式）来处理故障情况，防止级联故障。同时，通过合适的授权和认证机制来保护微服务的安全性，限制对敏感数据和功能的访问。

5. **引入容器化技术：**

   微服务架构通常使用容器化技术进行部署和管理，最常见的是使用Docker容器。将每个微服务打包到独立的容器中，以便更好地隔离和部署。使用容器编排工具（如Kubernetes）来自动化容器的部署、扩展和管理，提高系统的可伸缩性和弹性。通过容器化，可以更加灵活地部署和管理微服务。容器化还有助于解决开发环境与生产环境之间的一致性问题。开发团队可以在本地使用相同的容器运行微服务，并确保其在开发和测试阶段的正常运行。然后，将这些容器化的微服务镜像上传到云平台，以供部署和生产使用。

6. **数据管理和持久化：**

   在单体应用转换为微服务时，您需要考虑数据管理和持久化的问题。每个微服务可能需要有自己的数据库，或者共享同一个数据库。选择适合您的需求的数据库解决方案，并确保数据的一致性和可靠性。在云环境中，您可以考虑使用托管的数据库服务，如华为云RDS、GaussDB等。另外，还需要考虑如何处理跨多个微服务的数据事务和数据一致性问题。一种常见的方法是使用分布式事务管理器（如Saga模式），以保证微服务之间的数据操作具有一致性和原子性。

7. **实施监控和日志记录：**

   对于微服务架构，实施全面的监控和日志记录是非常重要的。使用适当的监控工具和日志系统，收集和分析每个微服务的指标和日志，以及整体系统的性能和故障信息。这将帮助您快速发现和解决潜在的问题，并保证系统的可用性和稳定性。您可以利用云提供商所提供的监控和日志服务，如华为云监控、LTS等，来集中管理和分析监控数据和日志。同时，采用可视化和告警机制，使得团队可以实时监控系统的运行状态，并在出现异常情况时能够及时采取措施。

8. **自动化部署和持续集成/持续交付：**

   微服务架构通常需要频繁地进行部署和更新。为了简化和加快部署过程，可以引入自动化部署和持续集成/持续交付（CI/CD）流程。使用适当的工具和技术，例如Jenkins、GitLab CI/CD等，来实现自动化的构建、测试和部署流程。在自动化部署和CI/CD流程中，可以包括编译代码、运行单元测试和集成测试、构建和推送容器镜像、部署到云环境等一系列步骤。这样可以加快交付速度，减少人为错误，并提供可靠的部署管道。

9. **安全性和权限管理：**

   在微服务架构中，安全性是一个重要的考虑因素。确保每个微服务都有适当的访问控制和权限管理机制，以防止未授权的访问和数据泄露。可以使用身份验证和授权技术（如OAuth、JWT）来验证请求的合法性，并在微服务之间进行身份传递。同时，采用适当的网络安全措施，如防火墙、SSL/TLS加密等，保护微服务之间的通信。此外，定期进行安全审查和漏洞扫描，确保系统的安全性和可靠性。

10. **渐进式迁移：**

    将传统单体应用进行微服务改造并迁移到云上是一个复杂的过程，并且可能需要一定的时间和资源。为了降低风险和减少中断，您可以采用渐进式迁移的方法。

首先，选择一个较小且相对独立的模块来进行微服务改造和云迁移。通过这个实验项目，您可以验证架构设计、技术选型和流程的可行性，并获得宝贵的经验教训。在成功迁移第一个模块后，逐步将其他模块进行类似的改造和迁移。渐进式迁移还可以帮助您逐步培养团队的能力和熟悉新的架构和工具。同时，您可以在此过程中收集反馈并不断进行调整和优化，以确保整个改造过程的顺利进行。

总结起来，微服务改造和上云是一个复杂而关键的过程。它需要综合考虑架构设计、拆分、接口定义、服务治理、容器化、数据管理、监控日志、自动化部署、安全性等多个方面。通过详细评估现有应用和目标，拆分单体应用为独立的微服务，引入适当的技术和工具，并采取渐进式迁移的方法，您可以成功地将传统的单体应用改造成高度可伸缩、弹性和可靠的微服务架构，并将其迁移到云环境中。

微服务架构优化

我们经常看到一些互联网企业的业务发展非常快，不同业务单元的软件工程师不断增加新的微服务或重复开发实现同样业务功能的微服务，导致微服务架构非常混乱，像毛线团一样，严重影响了TTM，也导致问题定位非常耗时，面对混乱的微服务架构，可以采取以下一些优化策略来改善情况，加速TTM（Time to Market）并提高问题定位效率：

1. **进行现有架构评估：**首先，对当前的微服务架构进行全面评估。了解整体架构、服务之间的依赖关系、通信协议和数据流。这将帮助你理清架构的复杂性，并确定需要改进的关键领域。
2. **进行重构和拆分：**根据评估结果，考虑对现有的微服务进行重构和拆分。识别那些过于庞大、职责不清晰或高度耦合的服务，将它们拆分成更小、更专注的单元。这样做可以简化系统结构并提高可维护性。
3. **引入服务治理：**采用适当的服务治理机制来管理微服务架构。使用服务注册与发现、负载均衡、熔断器等技术来增强服务的可见性、弹性和稳定性。这有助于减少故障和延迟，并提高问题定位的效率。
4. **实施自动化测试：**建立全面的自动化测试策略和工具链。通过单元测试、集成测试和端到端测试等各个层面的自动化测试，可以快速捕捉和解决问题，确保修改一个服务不会对其他服务造成意外影响。
5. **强调文档和标准：**建立明确的文档和标准，包括架构设计规范、接口规范和开发规范等。这有助于团队成员理解整体架构，并在开发过程中遵循一致的实践。文档和标准也可以帮助新加入团队的成员更快地适应和贡献。
6. **实时监控和日志记录：**引入实时监控和日志记录系统，以收集和分析微服务的运行情况和性能指标。这样可以及时发现潜在的问题或异常，并迅速进行定位和解决。同时，合适的报警机制可以帮助你快速响应故障和异常情况。
7. **采用持续交付和部署：**使用持续集成/持续交付（CI/CD）工具和流程来自动化构建、测试和部署微服务。这将缩短发布周期，降低发布风险，并加快新功能和修复的上线速度，从而提高TTM。
8. **建立跨团队协作：**鼓励不同团队之间的合作和沟通，特别是在微服务架构中。促进知识共享、问题协作和经验交流，可以加速问题定位和解决，并避免重复工作。

通过这些优化策略，可以逐步改善混乱的微服务架构，提高TTM并加强问题定位的效率。微服务架构的优化是一个持续的过程，需要不断地评估、调整和改进。

6.6.4 开发与运维现代化

通过DevOps实践，可以实现开发与运维的现代化。下面是一些步骤和实施建议：

- **文化转变：**首先，要实现开发与运维的现代化，需要在组织中建立一个强调合作与共享的文化。开发团队和运维团队应该互相信任、合作，并且共同追求系统稳定性和持续交付。
- **自动化：**自动化是DevOps的核心原则之一。通过自动化工具和流程，可以减少手动操作、降低错误风险，并提高效率。例如，使用持续集成和持续交付（CI/CD）工具来自动构建、测试和部署应用程序。
- **基础设施即代码（IaC）：**采用基础设施即代码的方法可以将基础设施配置和管理纳入代码库中。这样可以确保基础设施的可重复性、版本控制和自动化部署，从而提高整个环境的稳定性和可靠性。
- **集中日志和监控：**通过集中管理日志和监控数据，可以实时了解系统运行状况，并及时发现和解决问题。选择适当的日志管理和监控工具，并定义关键指标（KPIs）和警报规则，以确保系统的可用性和性能。
- **容器化和微服务架构：**采用容器化技术（例如Docker）和微服务架构可以实现应用程序的解耦和扩展。这样可以使开发团队更加灵活地部署、更新和维护应用程序，同时提高可伸缩性和弹性。
- **持续学习和改进：**DevOps是一个持续演进的过程，团队应该不断学习和改进工作流程。通过持续反馈、迭代和改进，可以逐步优化开发与运维的协作方式，提高交付速度和质量。

这些是实现开发与运维现代化的一些关键实践。但请注意，具体的实施方式可能因组织的需求和现状而有所不同。建议根据实际情况进行评估，并逐步引入和调整相应的实践。

6.6.5 治理与运营现代化

企业上云时，并不是所有应用都进行了现代化改造，新旧应用会有一段共存期，华为云的Roma Connect可以帮助企业实现新旧应用的集成，使其能够在云上共存而不破坏现有的应用环境。以下是一些步骤和建议，供参考：

- **了解新旧应用：**首先，您需要对现有的旧应用和要集成的新应用进行全面的了解。这包括了解它们的功能、数据结构、接口和通信方式等。这将有助于确定集成策略和技术选择。
- **选择合适的集成方式：**根据您的需求和应用特点，选择合适的集成方式。华为云的Roma Connect提供了多种集成方式，如API集成、消息队列、事件触发器等。根据应用之间的依赖关系和通信方式，选择最合适的集成方式。
- **设计集成方案：**基于对应用的分析和选定的集成方式，设计一个详细的集成方案。这包括定义接口规范、数据映射、消息传递机制等。确保设计方案兼容旧应用和新应用之间的交互，并且不会中断现有的业务流程。
- **实施集成：**根据集成方案，开始实施集成。使用Roma Connect提供的工具和平台，配置和设置必要的集成组件和连接器。确保正确地配置数据映射、消息路由和安全认证等关键参数。
- **测试和验证：**在将集成应用投入生产之前，进行全面的测试和验证。确保新旧应用之间的数据传递和功能调用正常工作，并且没有任何破坏或冲突发生。
- **监控和维护：**一旦集成应用上线，建立监控机制来跟踪集成环境的运行情况。监控包括应用性能、接口可用性和数据一致性等方面。及时处理任何异常情况，并定期进行维护和优化。

6.7 云上创新

6.7.1 概述

基于云平台的新技术正驱动着产品和服务创新浪潮。

- 人工智能与大模型结合，赋予产品更智能的交互和更精准的个性化服务，例如AI客服、智能推荐系统等。
- 区块链技术则增强了产品和服务的安全性和可信度，可应用于供应链管理、数字身份认证等场景，构建透明可追溯的体系。
- 数字人技术打造虚拟形象，应用于虚拟主播、在线教育等领域，提供更具沉浸感的用户体验。
- 大数据分析则帮助企业深入了解用户需求，优化产品和服务，实现精准营销和精细化运营。
- 物联网技术将设备连接上云，实现数据实时采集和远程控制，催生了智能家居、智慧城市等创新应用。

华为云使得这些新技术唾手可得，企业随时随地都能利用这些新技术进行快速创新和快速试错，大幅加速了创新的步伐，通过这些创新可以帮助企业开发创新的产品和服务、改进业务流程、增强决策能力、提升用户体验，并开创新的商业模式和市场机会。

6.7.2 人工智能

人工智能是模拟人类智能的技术和方法，在各个领域都发挥着重要作用。以下是AI如何使能业务创新、与业务结合并推动业务现代化的几个方面：

- **自动化和智能决策：**AI技术可以通过自动化和智能决策来提升业务效率和准确性。例如，利用机器学习算法，企业可以自动处理大量的数据，识别模式和趋势，进行预测分析和决策支持。这有助于加快业务流程，减少人力资源消耗，并提高决策的准确性和效果。
- **个性化和客户体验：**AI技术可以通过个性化推荐、智能客服和虚拟助手等方式改善客户体验。通过分析用户行为和偏好，AI可以向客户提供定制化的产品推荐和服务。此外，通过自然语言处理和情感分析等技术，AI可以实现更智能、人性化的客户服务，提高客户满意度。
- **智能生产和供应链管理：**AI技术在生产和供应链管理方面的应用可以提高生产效率和供应链的可视化与规划。例如，利用机器学习和物联网，可以实现智能制造和预测性维护，提高生产线的运行效率和设备的可靠性。同时，AI还可以优化供应链中的库存管理、运输计划和交付路线，减少成本并提升响应能力。
- **创新商业模式：**AI技术为企业创造了许多新的商业模式和市场机会。例如，云计算和AI结合可以实现弹性计算和按需服务，推动软件即服务（SaaS）模式的发展。另外，AI与物联网的结合也可以支持智能家居、智能城市和智慧医疗等领域的创新商业模式。

6.7.3 大数据

大数据是指规模庞大且复杂的数据集合，对于企业来说，如何收集、存储和分析大数据具有重要意义。以下是大数据如何使能业务创新、与业务结合并推动业务现代化的几个方面：

- **数据驱动决策：**大数据分析可以帮助企业从海量数据中提取有价值的信息和洞察力，为决策提供支持。通过对历史数据和实时数据的分析，企业可以发现市场趋势、需求变化以及潜在风险。这有助于做出准确的决策，提高业务的竞争力。

- **个性化营销和客户关系管理：**大数据技术可以帮助企业更好地了解客户，实现个性化的营销和客户关系管理。通过对客户行为、兴趣和偏好的分析，企业可以精确地进行定制化的产品推荐和营销活动，提高销售转化率和客户满意度。
- **预测分析和供应链优化：**大数据分析可以帮助企业进行预测分析，以便更好地规划生产和供应链。通过对历史销售数据、市场趋势和供应链数据的分析，企业可以进行需求预测、库存优化和交付计划，减少库存成本、提高运营效率并提升供应链的响应能力。
- **创新产品与服务：**大数据可以为企业的产品和服务创新提供有力支持。通过分析大数据，企业可以发现市场上的空白点和机会，掌握用户需求，并基于这些洞察力开发出更具竞争力和创新性的产品和服务。例如，一些公司利用大数据分析医疗记录和基因组数据，提供个性化的医疗解决方案。

6.7.4 区块链

区块链是一种去中心化、分布式的账本技术，可以确保数据的安全性和可信度。以下是区块链如何使能业务创新、与业务结合并推动业务现代化的几个方面：

- **透明度和可信度：**区块链技术通过去中心化的特点，确保所有交易和数据记录被公开透明地存储，并且无法篡改。这为企业创造了更高的数据可信度和透明度，消除了传统中介机构的需求，降低了操作风险。
- **智能合约和自动化执行：**区块链上的智能合约是一种自动化的合约机制，能够根据预先设定的条件和规则自动执行。这在供应链管理、金融服务等领域具有广泛的应用。智能合约可以提高交易的效率，减少人工干预，降低成本，并防止欺诈和纠纷。
- **去中介和减少摩擦：**区块链技术消除了许多中介机构的需求，使得交易过程更直接、高效，并降低了交易成本和摩擦。例如，利用区块链技术，企业可以实现快速的跨境支付和资金清算，减少中间银行或支付机构的介入。
- **去中心化的应用和社区经济：**区块链技术为去中心化的应用提供了基础。企业可以通过区块链构建去中心化的应用平台，实现用户之间的直接交易和价值转移。这种社区经济模式可以鼓励用户参与、共享价值，并促进创新和合作。

6.7.5 元宇宙

元宇宙是一个虚拟的数字世界，通过增强现实（AR）、虚拟现实（VR）等技术与现实世界互动。以下是元宇宙如何使能业务创新、与业务结合并推动业务现代化的几个方面：

- **交互与协作：**元宇宙技术可以提供更加沉浸式和互动性的体验，使得用户能够在虚拟环境中进行交互和协作。企业可以利用元宇宙创建虚拟会议、培训和团队合作等场景，实现远程工作和远程协作的效果。这将带来更高效的工作流程和全球范围内的合作机会。
- **虚拟商店和数字资产：**元宇宙为企业提供了创造虚拟商店和销售数字资产的机会。通过元宇宙平台，企业可以展示和销售虚拟产品、数字艺术品和虚拟房地产等。这种数字化的商业模式可以创造新的收入来源，并且具有全球触达的潜力。
- **虚拟旅游和娱乐：**元宇宙可以为旅游和娱乐产业带来革命性的改变。通过虚拟现实技术，用户可以身临其境地参观名胜古迹、参加虚拟音乐会或观看虚拟体育赛事。这将为旅游业和娱乐业带来更广阔的市场和创新的商业模式。
- **数据收集和个性化体验：**元宇宙技术可以收集用户在虚拟环境中的行为数据，从而为企业提供更深入的用户洞察和个性化体验。通过分析用户在虚拟空间中的行为、兴趣和偏好，企业可以更好地定制产品和服务，提高用户满意度和忠诚度。

6.7.6 物联网

物联网是指将各种物理设备和传感器与互联网连接起来，实现设备之间的通信和数据交换。以下是物联网如何使能业务创新、与业务结合并推动业务现代化的几个方面：

- **智能家居和智慧城市：**物联网技术可以将家居设备、城市基础设施和公共服务连接起来，实现智能化管理和优化资源利用。通过物联网，人们可以通过手机或其他终端设备控制家居设备，实现智能家居的概念。同时，物联网还可以应用于智慧城市领域，优化城市交通、能源管理和公共安全等方面。
- **工业自动化和智能制造：**物联网技术在工业领域的应用可以实现工业自动化和智能制造。通过将设备和机器连接到物联网，企业可以实现设备之间的协同工作、远程监控和预测性维护。这将提高生产效率、降低故障率并优化供应链管理。
- **数据采集和分析：**物联网设备可以收集大量的传感器数据，包括温度、湿度、压力等各种环境参数。通过对这些数据进行分析，企业可以获得有价值的洞察，用于改进产品质量、优化运营流程和预测需求变化。
- **客户体验和增值服务：**物联网设备可以与客户的手机或其他终端设备连接起来，为用户提供个性化的服务和增值体验。例如，智能家居设备可以根据用户的行为习惯自动调节室温、照明和安全系统，提供更舒适、便捷和安全的居住环境。此外，物联网还可以为企业提供机会推出定制化的产品和服务，满足用户个性化需求。
- **资产追踪和供应链管理：**物联网技术可以实现对资产和物品的追踪和管理。通过将传感器和标签应用于物品上，企业可以实时监控物品的位置、状态和运输情况，提高物流和供应链的效率，并减少丢失或损坏的风险。
- **健康监测和医疗保健：**物联网技术在医疗领域具有广泛应用。通过将传感器嵌入到医疗设备、可穿戴设备和健康监测器上，可以实时监测患者的健康数据，并进行远程监护和诊断。这有助于提高医疗保健的效率、减少医疗资源的浪费，并改善患者的生活质量。

6.8 采用实施的反模式

在云采用实施阶段，可能会遇到一些反模式，这些模式如果不加以识别和避免，可能会影响上云迁移效率、导致业务中断、造成不必要的成本浪费和增加维护难度。以下是一些常见的云采用实施阶段的反模式：

- **未采用自动化部署模式**

  该反模式是指企业依赖手动进行代码、云资源的配置和部署，效率低，人为错误高。

  优化建议：采用自动化的配置和部署工具，如Terraform、CI/CD等，以提高云资源部署的效率和准确性。

- **未进行切换演练**

  该反模式是企业未进行充分的切换演练，导致在正式业务切换时出现问题。

  优化建议：在正式切换前进行全面的切换演练，模拟真实环境中的不同场景，及时发现并解决问题，确保系统在切换后能正常运行。

- **测试不充分**

  该反模式是指业务系统切换前测试不充分，导致潜在问题未能及时发现和解决，上线后出现各种功能、性能、安全性等问题，影响用户体验。

  优化建议：业务切换前，要进行全面的测试，包括功能测试、性能测试、可用性测试、安全测试等，确保每个功能模块在云环境中能正常稳定运行。

- **资源未打标签**

  该反模式是指云资源未正确打标签，导致资源管理困难，增加了查找、监控和管理的复杂性。

  优化建议：所有创建的云资源都要打好标签，方便后续的运维管理和成本优化。

通过识别和避免这些反模式，并参考行业最佳实践和成功案例，可以更加科学实施上云方案，提高上云和用云的效率，更好地利用云平台的优势，发挥云技术的价值。

7 运维治理

7.1 概述

应用系统迁移或部署到云上后，云化转型正式进入了运维治理阶段。这一阶段至关重要，因为它直接影响着云上IT基础设施和业务系统的性能、可靠性、安全性和成本效益。通过持续和有效的运维治理，企业能够确保云资源的高效利用，保障业务的连续性和稳定性，实现对云环境的全面掌控，最大化云化转型的收益。

运维治理阶段需要针对云上IT基础设施、应用系统和大数据平台进行精益化治理、确定性运维、全方位安全运营和精细化FinOps，并基于WAF框架进行持续优化。首先，精益化治理贯穿始终，它提供了一套标准化治理框架和最佳治理实践，确保云资源得到高效利用，并符合安全合规要求，最小化云化转型的风险。其次，确定性运维旨在构建可防、可控、可治的运维管理体系，把数字化转型和业务快速发展带来的“不确定性”通过运维变成“确定性”，保障应用系统的长期稳定运行，减少故障和停机时间。

全方位安全运营则涵盖了数据安全、网络安全、访问控制等各个方面，构建全面的安全防护体系，保护企业核心数据和应用系统。最后，精细化FinOps 通过成本分析、优化和预算管理，帮助企业控制云支出，最大化云转型的投资回报。所有这些活动都应该基于Well-Architected Framework进行持续优化，确保云环境始终保持最佳状态，并能够根据业务需求灵活调整。

组建运维治理团队

开展任何工作之前必须确保有具备相应技能水平的人高效完成这些工作，运维治理阶段主要的工作包括精益化治理、确定性运维、安全运营和FinOps。请参考**云卓越中心**所描述的角色职责和技能要求，结合企业的实际情况组建运维治理阶段需要的团队，包括云治理团队、云运维团队、云安全团队和FinOps团队。

7.2 精益化治理

7.2.1 概述

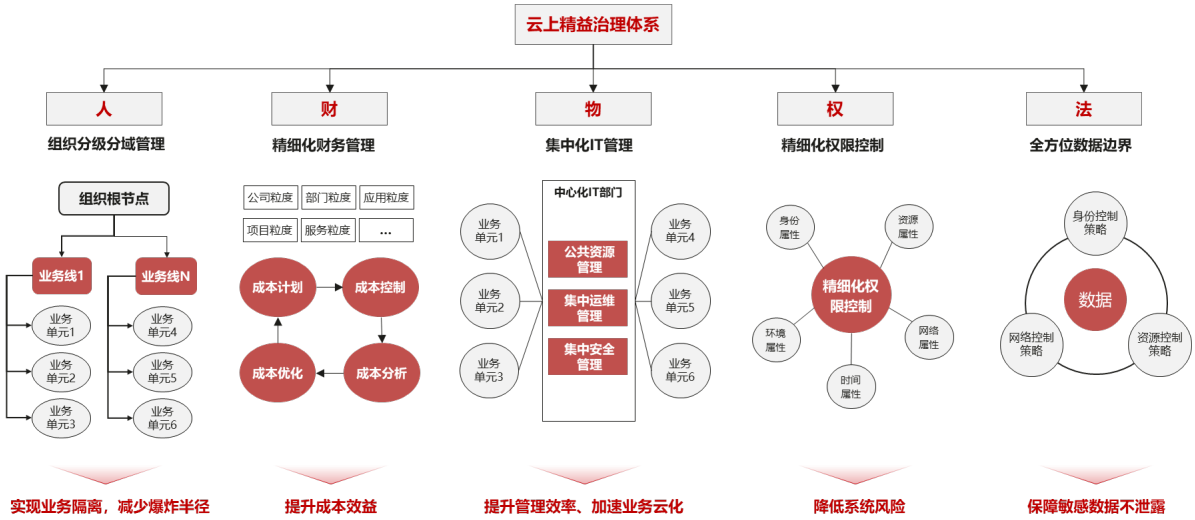
当企业上云规模逐渐变大，在云上有数十上百个应用系统和海量云资源，包括企业自有员工、外包员工及合作伙伴的员工在内的大量用户需要访问和操作这些云资源，量

变导致质变，资源闲置、误操作、恶意操作、数据泄露和权限错配等风险将随着用云规模呈现指数级增长。

您需要开始着手构建精益化、集中化和结构化的IT治理体系才能有效控制这些风险，最大化业务收益，保障业务的持续增长。

华为云基于自身的IT治理实践经验和帮助大量客户实施IT治理的经验，总结了如下图所示的云上精益治理体系，对企业在云上的“人才物权法”等要素进行集中化和精益化治理。下图中的组织分级分域管理、集中化IT管理、全方位数据边界、精细化权限控制是华为云Landing Zone解决方案的组成部分，精细化成本运营则属于华为云FinOps解决方案。

图 7-1 云上精益治理体系



7.2.2 组织分级分域管理

组织分级分域管理是一种在现代企业治理中至关重要的方法，特别是在云计算环境下，随着业务的扩展和多样性的发展，这种管理方式变得越来越重要。您可以按照业务架构的不同层次和领域，基于华为云Organizations服务构建一个清晰、有序、易于管理的云上组织架构，然后将企业的不同业务单元（如子公司、业务系统、产品线、部门、项目等）部署在各自独立的云账号中。这种方式不仅能够与公司现有的治理架构完美匹配，还能够实现高效的故障和安全隔离，将单个业务单元的故障和风险限制在其自身的范围内，减少“减少爆炸半径”。

首先，分级分域管理可以很好地反映和匹配公司的治理架构。企业往往由多个业务单元组成，每个业务单元都有其特定的目标、团队和运营模式。通过将这些业务单元分配到不同的云账号中，企业可以在云环境中重现其组织结构。这不仅有助于清晰地界定各个业务单元的责任和权限，还方便了资源的分配和管理。例如，某家公司可能有多个子公司，每个子公司都有自己的产品线和项目团队。通过将每个子公司的资源部署在独立的云账号中，可以确保每个子公司拥有自主的管理权限，同时又可以按照公司的整体策略进行统一的监管。

其次，分级分域管理在故障和安全隔离方面具有显著的优势。在云环境中，共享资源虽然带来了便利和效率，但也可能增加了风险。如果所有的业务单元都在同一个云账号中运行，那么一个业务单元的故障或安全问题可能会影响到其他业务单元，甚至整个系统。而通过将不同的业务单元部署在独立的云账号中，企业可以有效地隔离故障和风险，防止问题的扩散。举个例子，如果某个业务系统遭遇了安全攻击，攻击者可

能只能够接触到该业务系统所在的云账号中的资源，无法进一步影响到其他业务单元。这种隔离机制大大提高了整个企业的安全性和稳定性。

此外，各个业务单元只能查看和管理自己的云账号内的资源、数据和应用，这种权限管理方式可以确保业务数据的安全性和保密性。业务单元之间的数据隔离，可以防止因人为错误或恶意行为导致的数据泄露和篡改。同时，这也有助于各个业务团队专注于自己的业务发展，减少不必要的干扰和冲突。

公司IT部门可以对各个业务单元进行一定程度的集中管理，实现分统结合的管理模式。在这种模式下，虽然业务单元在各自的云账号中独立运行，但IT部门可以通过统一的策略和工具，对全公司的云资源进行监控、监管和优化。例如，IT部门可以制定统一的安全策略，确保所有的云账号都符合公司的安全标准；可以通过自动化工具，对各个云账号的资源使用情况进行监控，及时发现和解决潜在的问题。这种分统结合的管理方式，在业务灵活性和中央管控之间达成了平衡。业务单元拥有足够的自主权，可以根据自身的需求灵活调整资源和策略，快速响应市场变化。而IT部门则可以从全局角度出发，确保公司的整体安全性、合规性和资源利用效率。

最后，组织分级分域管理还有助于成本的精细化控制。通过对各个云账号的独立计费，企业可以清晰地了解每个业务单元的资源消耗和成本支出。这为成本优化和预算管理提供了有力的支持。业务单元可以根据自身的预算，合理规划和调整资源的使用，而公司层面也可以根据整体的财务目标，制定和调整各业务单元的预算和成本策略。

7.2.3 精细化权限控制

在安全合规要求日趋严格的情况下，企业需要采用精细化权限控制手段授予用户足够履行其职责的最小权限。企业利用这些细粒度授权方法可以精确设置访问控制的5 个要素：Who、What、How、Where、When。Who 表示谁可以访问云资源，What 表示可以访问哪些云资源，How 表示有权执行该资源的哪些操作，Where 表示允许用户从哪里访问，When 则表示允许访问的时间段。细粒度授权体现在以下三个方面：

- **细粒度资源：**授权时可以指定特定的资源组甚至单个资源，而不是把租户内所有的资源都授权出去，这个可以通过企业项目、标签等方式来限定授权的资源范围。如果需要授权特定资源，可以先把这些资源归集到一个企业项目或者打上一个标签，然后按照企业项目或标签来设置权限。
- **细粒度操作：**将云资源的读、写、列表等操作进一步细化，对其细化操作进行鉴权，并将这些细化操作变成可供用户配置的权限操作。以云主机为例，将其读操作细化为读取规格、读取标签、读取服务器详情、读取挂载的磁盘、读取网卡等细粒度操作，这些细粒度操作在用户配置权限的时候是可以自由选择的，这样就可以将权限控制到用户所需的最小操作集合。
- **细粒度属性：**ABAC（Attribute-based Access Control）相比 RBAC（Role-Based Access Control）更加灵活和精细，您可以在权限设置的时候附加各种基于属性的条件，在权限判定的时候检查当前的访问请求是否满足这些属性所对应的条件，满足条件时才允许访问。这些属性通常包含五大类：一是身份属性，比如用户姓名、是否启用 MFA 、是否根用户等；二是网络属性，比如源IP地址、源VPC ID等；三是资源的属性，比如资源的标签、资源名称等；四是时间属性，比如访问时间、Token的签发时间等；五是环境属性，比如访问请求来自哪个账号，目标资源位于哪个账号等。您可以在**这个链接**查看华为云当前支持的全局级条件键和服务级条件键。通过 ABAC 可以更细粒度地设置访问控制的权限，例如运维人员张三只有启用了 MFA 认证后并且只能在晚上 12 点后、凌晨 4 点之前对指定的ECS实例进行关机和重启操作。

7.2.4 集中化 IT 管理

集中化IT 管理是指将企业内分散的IT 资源、服务和管理职能集中到中心IT 部门进行统一管理和协调，中心IT 部门可以针对众多业务单元进行集中网络管理、集中运维管理、集中安全管理、集中合规审计、集中身份权限管理和公共资源管理等。通过集中化的方式提高IT 管理的效率和一致性，降低运营成本。各个业务单元无需为基础设施的部署和运维操心，可以加速业务云化进程。

集中化IT管理是指将企业内原本分散在各个业务单元的IT资源、服务和管理职能，集中到一个中心化的IT部门进行统一的管理和协调。这种管理模式在当今信息技术高速发展的时代，显得尤为重要。通过将分散的IT职能集中起来，企业可以在多个层面上获得显著的优势，既能提高IT管理的效率和一致性，又能有效降低运营成本。在集中化IT管理模式下，中心IT部门（或者CCoE）可以针对众多业务单元实施多方面的集中管理：

- **集中网络管理：**中心IT部门统一规划、部署和维护企业在云上的网络基础设施，包括专线、企业路由器、VPN、云连接、NAT网关、VPC等。这样可以确保整个企业的网络架构统一、稳定、安全，避免各业务单元自行管理网络所带来的不一致性和潜在的安全漏洞。同时，统一的网络管理还能提高数据传输的效率，保障各部门之间的信息交流畅通无阻。
- **集中运维管理：**借助**AOM**和**COC**等服务所提供的多账号统一监控和运维管理功能，所有业务单元的云资源的运维工作可以交给中心IT部门负责。通过建立标准化的运维流程和规范，对云资源的性能监测、故障处理、升级更新等进行统一管理。这种方式可以有效实施统一的运维管理标准，提升运维效率，减少运维成本。
- **集中安全管理：**网络安全是企业运营的重中之重。借助安全云脑等服务提供的多账号统一安全管控功能，中心IT部门可以针对所有业务单元进行统一的安全运营，包括云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等。集中化的安全管理可以确保安全策略的一致性，有效防范网络攻击和数据泄露，保护企业的核心资产。
- **集中合规审计：**随着各类信息安全法规和行业标准的出台，合规性成为企业必须关注的重点。借助**CTS**和**Config**等服务提供的多账号统一合规审计的功能，中心IT部门统一负责企业的合规管理和审计工作，确保各业务单元的云资源符合国家、行业和企业自身的合规标准。这样，可以降低合规风险，避免因不合规而导致的法律责任和声誉损失。
- **集中身份权限管理：**通过**IAM身份中心**提供的多账号统一身份管理与访问控制的功能，中心IT部门可以统一管理企业中使用华为云的用户，一次性配置企业的身份管理系统与华为云的单点登录，以及所有用户对组织下账号的访问权限。管理员集中创建用户，分配登录密码，并对其进行分组管理。集中权限管理加强了对用户权限的控制，防止未经授权的访问，保障系统的安全性。
- **公共资源管理：**企业内部的公共IT资源，如DNS服务器、容器镜像库、CA证书机构、云盘等由中心IT部门统一部署和管理。集中管理可以避免资源的重复建设和闲置浪费，提高资源利用率，降低采购和维护成本。

通过以上各个方面的集中管理，企业可以显著提高IT管理的效率和一致性。首先，集中管理催生了标准化的管理流程和规范，使得各项IT工作更加有序和透明，减少了因管理松散导致的错误和安全漏洞。其次，专业的中心IT团队具备更强的技术能力和经验，能够及时引入先进的技术和最佳实践，为企业提供高水平的IT支持。

集中化IT管理还有效降低了运营成本。通过统一的资源规划和采购规模化，企业可以获得更优惠的价格，减少不必要的开支。集中化的运维和管理，优化了人力资源配置，避免了各业务单元各自为政带来的人力资源浪费。整体而言，企业可以在不增加投入的情况下，获得更高效、更可靠的IT服务。

集中化IT管理还能缩短各业务单元的IT项目交付周期。由于中心IT部门已经建立了完善的基础设施和服务框架，业务单元在需要新系统或应用时，可以快速集成和部署，避免了重复的建设和调试过程。业务单元可以将更多的精力和资源投入到自身的核心业务发展上。这种专业分工，使得业务单元能够更快地响应市场需求，加速产品和服务的创新，提升市场竞争力。

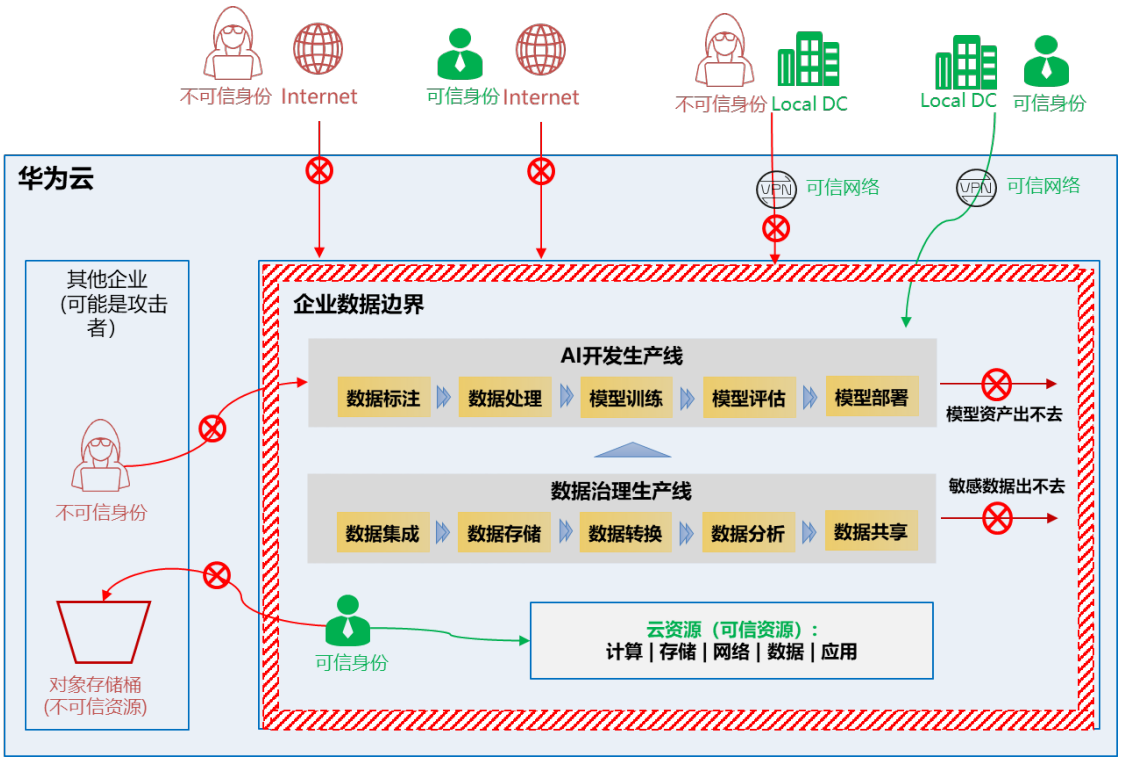
然而，实施集中化IT管理也需要企业在组织架构、管理模式和文化上进行一定的调整。首先，企业需要建立明确的管理机制和流程，明确中心IT部门和业务单元的职责分工，确保双方的沟通顺畅。其次，中心IT部门需要具备服务意识和灵活性，能够根据业务单元的需求，提供个性化的支持和解决方案。最后，企业的高层领导需要对集中化IT管理予以足够的重视和支持，为其推行扫清障碍。

总之，集中化IT管理是一种符合现代企业发展需求的管理模式。通过将分散的IT资源、服务和管理职能集中到中心IT部门，企业能够提高IT管理的效率和一致性，降低运营成本，提升整体竞争力。各个业务单元在这种模式下，可以专注于自身的核心业务，无需为基础设施的部署和运维操心，从而加速业务云化进程，实现业务的快速发展和创新。在推行集中化IT管理的过程中，企业需要统筹规划，协调各方利益，充分发挥集中化管理的优势，为企业的长期健康发展奠定坚实的基础。

7.2.5 全方位数据边界

全方位数据边界基于身份控制策略、网络控制策略和资源控制策略构筑起一道坚固的数据安全屏障。确保只有经过严格验证的可信身份，在符合安全标准的可信网络环境中，方能获得对特定资源的访问权限，从而保障数据安全。如下图所示，可信身份从互联网（不可信网络）访问云资源的请求会被拒绝，不可信身份通过本地数据中心网络（可信网络）访问云资源的请求也会被拒绝，可信身份访问其他企业的对象存储桶（不可信资源）的请求还会被拒绝，只有可信身份通过本地数据中心网络（可信网络）访问本企业的云资源的请求是允许的。

图 7-2 全方位数据边界



身份控制策略

身份控制策略是数据边界的第一道防线。它确保只有经过严格验证的可信身份才能够访问企业的云资源。身份控制策略主要通过SCP（Service Control Policy，服务控制策略）和IAM策略来实现。

SCP是一种基于组织的访问控制策略。组织管理账号可以使用SCP指定组织中成员账号的权限边界，限制账号内用户的操作。SCP可以关联到组织、OU和成员账号。当SCP关联到组织或OU时，该组织或OU下所有账号均受该策略影响。关于SCP的详细介绍，请查看**这个链接**。需要注意的是，SCP的影响范围比较大，在生产环境实施SCP之前，强烈建议您先在测试环境下开展充分的测试验证，避免对生产环境中云资源的使用产生不必要的影响。

IAM策略用于精细化地控制用户、用户组和委托对华为云资源的访问权限。通过IAM策略，企业可以基于最小权限原则，为用户分配恰到好处的权限，确保他们只能访问与其工作相关的资源和操作。这不仅提高了安全性，还减少了权限滥用的风险。关于IAM策略的详细介绍，请查看**这个链接**。

在华为云中，身份控制策略主要通过SCP和IAM策略来实现。如果同时设置了SCP和IAM策略，对用户来讲实际有效的权限范围是两者的交集。

网络控制策略

网络控制策略是数据边界的第二道防线，主要是通过VPCEP（Virtual Private Cloud Endpoint，VPC终端节点）策略来实现。

VPCEP是一种用于在VPC中建立私有连接的网络服务。通过VPCEP，用户可以在不使用公网IP地址的情况下，安全地将VPC连接到华为云的服务和资源。这意味着数据在传输过程中不会经过互联网，降低了被截获和攻击的风险。VPCEP策略附加到VPC终端节点上面，允许您控制哪些主体（或身份）可以使用该VPC终端节点访问云资源，通过配置VPCEP策略，企业可以构建一个封闭、安全的网络环境，不仅可以确保数据在内部网络中安全传输，还可以保障只有可信的身份才可以访问云资源及敏感数据。例如，企业可以将关键业务系统部署在VPC内，通过VPCEP访问华为云的RDS实例，而不必暴露在公网中，同时可以限定只有数据库管理员张三可以通过该VPCEP访问RDS实例，进一步保证了敏感数据的安全性。关于如何管理VPCEP策略，请查看**这个链接**。

资源控制策略

资源控制策略是数据边界的第三道防线。这主要由云服务提供的访问控制策略来实现，如OBS（Object Storage Service，对象存储服务）的桶策略。

桶策略是一种基于资源的访问控制策略，允许桶的所有者指定对桶和对象的权限控制。通过桶策略，企业可以定义允许或拒绝哪些用户可以对桶执行哪些操作。例如，可以允许某个用户对特定的桶进行读取操作，但禁止写入或删除。桶策略支持基于条件的访问控制，可以根据请求者的IP地址、请求时间等条件，灵活地控制访问权限。例如，企业可以设置桶策略，仅允许来自公司内部网络的请求访问桶，或者限制特定时间段的访问。关于如何创建桶策略，请查看**这个链接**。

桶策略和VPCEP策略可以结合起来使用，达到“双端固定”的效果，一方面，设置VPCEP策略可以限制VPC中的服务器（ECS/CCE/BMS）只能访问OBS中的特定资源；另一方面，设置桶策略可以限定OBS中的桶只能被特定VPC中的服务器访问，从而在请求来源和被访问资源两个角度保障了安全性。关于如何配置双端固定，请查看**这个链接**。

全方位数据边界的构建，是一个系统性和综合性的工程，需要企业在身份、网络和资源三个层面都实施严格的控制策略。只有三者相互配合，才能真正构筑起坚不可摧的数据安全屏障。

7.2.6 精细化成本运营

精细化成本运营基于FinOps 理念，将财务管理与云资源运营相结合，旨在帮助企业优化云资源的使用和成本管理。

通过基于FinOps 的成本全生命管理体系，企业可以在云环境中实现精细化的成本控制和资源分配。这种管理体系允许企业按照不同的粒度进行成本分析和管理，包括子公司、业务系统、产品线、部门、项目，甚至是微服务级别。这种细粒度的管理使得企业能够准确识别各个业务单元的成本消耗情况，从而做出更明智的决策。通过实施FinOps，企业可以提升资源使用效率，避免资源浪费，并在不影响业务性能的前提下降低成本。关于FinOps的详细实践，请查看本章后面的内容。

总之，企业通过精益化治理可以实现数据边界可守护、复杂组织可治理、人员权限可管控和资源成本可优化，有效控制大规模用云的各种风险，最大化业务收益。

7.3 确定性运维

确定性运维是华为云基于自身多年的云服务运维经验沉淀的一套运维理念、方法论和最佳实践，可以帮助企业在云上高效运维自建和采购的业务系统，确保这些业务系统在云上能够持续高效稳定运行。

确定性运维旨在构建可防、可控、可治的运维管理体系。通过高质量的产品开发，严谨的运维流程和制度来降低故障的概率，要挑战零故障。同时也要有技术手段对可能发生的故障进行管理，将故障间隔、故障影响范围及故障恢复时间做到可防、可控、可治。总而言之，要把数字化转型和业务快速发展带来的“不确定性”通过运维变成“确定性”。

在确定性运维的推动下，企业可以实现资源的高效利用。通过合理的资源规划、分配和调度，企业能够避免资源的浪费和闲置，提高资源的利用率。此外，确定性运维还能够通过自动化、智能化的手段，降低运维成本，提高运维效率，为企业节省大量的人力和物力。

构建确定性运维体系是一个系统性和综合性的工程，需要从质量文化、高可用架构、动态风险治理以及智能运维工具这四个方面全方位入手，如下图所示。

图 7-3 确定性运维框架

- **质量文化是基础**

质量文化是确定性运维的基石。一个注重质量的文化能够激发团队成员对运维工作的责任感和使命感，从而确保工作的精细化和标准化。以下是一些构建高质量文化的最佳实践：

- 自上而下，从最高层面强调和践行质量的重要性，并将其纳入核心价值观。
- 构筑开发与运维团队共同的质量目标和方法。
- 在运维团队开展组织变革，不断提升组织能力，牵引用软件工程的方法解决问题，从“消防员”向“建构师”转型。

- **高可用架构是前提**

  高可用架构是确定性的前提，通过设计合理的架构，可以降低系统故障的风险，缩短故障恢复的时长，并且控制故障的影响范围，高可用架构的设计与落地需要关注如下三点：

  - 瞄准SLO 的目标，运用科学的方法进行架构的设计，对可用性架构的选择以及落地时间进行管理。
  - 在产品规划设计、上线运行阶段，给运维团队授予相应的责权利，对开发和商用计划有所制约，确保可用性需求落地。
  - 在产品运行维护期间，有计划地对高可用设计进行验证，以确保系统符合设计要求。

- **动态风险治理是保障**

  动态风险治理是应对不确定性和突发事件的重要保障手段。其本质也是对变更、故障模式、业务运行数据的识别开展全生命周期的主动运维和能力构建：

  - 针对变更作业的风险，开展全面的能力建设，包括版本发布架构体系建设、账号权限管理、自动化变更能力建设等。
  - 针对已知和未知的故障风险，通过科学的方法梳理故障模式库（树），并目的地进行快恢能力建设，一方面制定应急预案和响应机制，确保在突发事件发生时能够迅速响应和处理，另一方面定期组织演练和复盘，验证可用性架构运行情况以及团队应急响应能力。
  - 业务运行态数据的智能运营，是指导团队开展工作持续改进的核心基础能力，需要构建一套实时的采集以及数据运营系统，以支撑业务决策。

- **智能运维是未来**

  智能运维工具能够提高运维工作的效率和质量，降低人力成本。尤其是AI 时代，通过引入自动化、智能化等技术手段，团队可以更加高效地管理和维护系统，有几个原则：

  - 选择合适的工具和技术，确保其与业务需求和技术栈相匹配，如自动化部署、故障预测、智能定界定位等。
  - 将工具与现有系统进行整合，根据实际需求进行定制和优化，以满足特定的运维需求。
  - 关注新兴技术和发展趋势，不断更新和升级智能运维工具，提升运维水平。

  关于确定性运维的详细实践指南，请参考华为云发布的**《确定性运维白皮书--稳定可靠篇2.0》**。

7.4 安全运营

7.4.1 概述

安全防护三分在于技术，七分在于运营。安全运营是指在云计算环境中，通过持续监控、检测、响应和改进，确保云资源、数据和应用的安全性。这种方法强调安全防护

是一个持续的过程，而不是一次性的任务。只有通过持续的、有效的安全运营才能将多道安全防线有效协同起来，共同保障业务系统的安全稳定运行、保障关键数据的安全。然而，安全运营面临着很多挑战。

- **安全体系越来越复杂**

  随着数字化转型的深入，企业的ICT环境变得日益复杂。云计算、网络管道、终端设备、边缘计算、操作系统、数据库、应用程序等多个层面交织在一起，形成了一个庞大而复杂的生态系统。每个环节都有可能成为安全漏洞的切入点，增加了整体安全管理的难度。此外，安全产业的碎片化现象加剧了这种复杂性。市场上安全厂商众多，各自提供不同的产品和解决方案，产生了大量格式各异的日志和数据，缺乏统一的标准。这使得安全信息的整合和分析变得困难，无法形成全局性的安全态势感知。

  同时，合规要求的提高也给企业带来了新的挑战。国内外的法律法规，如中国的网络安全法、数据安全法和个人信息保护法，欧盟的GDPR，金融行业的PCI-DSS，医疗行业的HIPPA等，对数据隐私和网络安全提出了严格的要求。企业需要投入大量的资源来满足不同地区和行业的合规标准，增加了管理负担。

  更为严峻的是，攻击手段日益复杂化。攻击者利用人工智能和机器学习技术，加速了攻击工具和方法的迭代，手法新颖多变。例如，APT攻击（高级持续性威胁）是指隐蔽而持久的网络攻击，攻击者通常是拥有强大资源的组织或犯罪集团，他们目标明确，长期潜伏，利用各种高级技术手段窃取敏感数据或破坏目标系统。APT攻击难以检测和防御，危害极大。

  综上所述，安全体系的复杂性源于技术环境的多元化、安全产业的碎片化、合规要求的严苛化以及攻击手段的复杂化。企业需要建立统一的安全管理平台，整合各类安全信息，提升全局防护能力，才能应对当前的安全挑战。

- **安全专家稀缺**

  安全专家的稀缺已成为制约企业安全运营的一大瓶颈。首先，受投资有限的影响，许多企业无法组建庞大的安全团队，专业的安全人才不足。安全领域高度专业化，培养一名合格的安全专家需要经过长期的实战锻炼，积累丰富的经验和技能，成长周期漫长。此外，安全专家的经验和知识往往难以体系化地沉淀下来，缺乏有效的知识传承机制。一旦专家离职，宝贵的经验也随之流失，给企业带来不可估量的损失。

  由于安全事件频发，专家的工作负荷巨大，他们的精力常常被日常重复性的运作所消耗。例如，处理大量的安全告警、分析日志、进行常规的安全检查等。这些工作虽然重要，但重复性高，耗时费力，导致专家无法专注于更具价值的工作，如安全战略规划、复杂威胁分析和安全体系优化等。

  此外，随着攻击技术的不断演进，安全专家也需要持续学习和更新知识，以保持专业水平。这进一步增加了他们的压力和负担。在人才市场竞争激烈的情况下，留住安全专家也是一大挑战。

  为解决安全专家稀缺的问题，企业需要加大对安全人才的培养和投入，建立完善的培训和晋升机制。同时，利用自动化和智能化工具，减轻专家的重复劳动，让他们专注于核心安全事务。建立知识管理体系，沉淀专家的经验，实现知识共享，降低因人才流失带来的风险。

- **安全运营效率低**

  安全运营效率低下是当前企业面临的普遍问题。首先，风险告警数量过多，安全设备每天产生海量的告警信息，其中包含大量的误报和冗余信息。安全人员难以在短时间内对所有告警进行有效的筛选和处理，真正的威胁可能被淹没在海量数据中而被忽视。

  其次，威胁识别速度慢。面对复杂的安全事件，缺乏智能化的分析工具，安全团队需要耗费大量时间进行手动分析，无法及时判断威胁的性质和严重程度。这种被动的响应方式，可能错过最佳的处理时机，导致安全事件的进一步扩大。

再次，事件响应和处理缓慢。从发现问题到采取行动，通常涉及多个部门和人员，流程繁琐，协调困难。手动操作的过程容易出现疏漏和错误，影响处理效果。

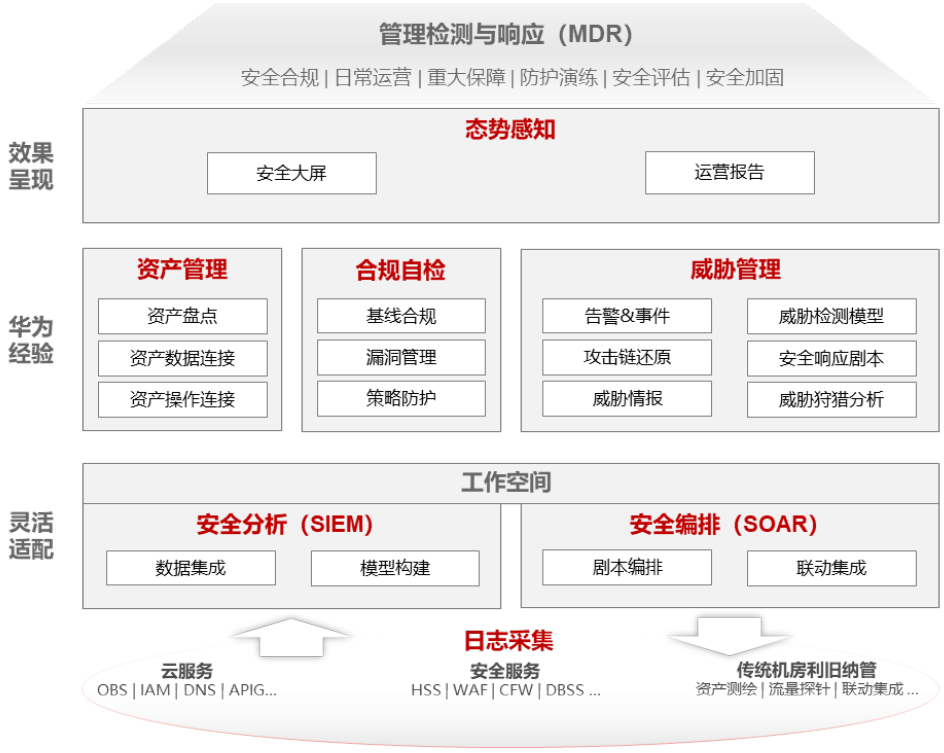
这些问题的根源在于缺乏高效的安全运营机制和工具支持。传统的安全运营模式已无法适应当前快速变化的安全环境。为提升安全运营效率，企业需要引入先进的安全运营中心（SOC），利用大数据分析、机器学习等技术，实现告警的自动关联和优先级排序。通过自动化响应工具，加快事件处理速度。建立标准化的流程和协同机制，提高跨部门的响应效率。同时，加强对安全人员的培训，提高其分析和决策能力。

总之，提高安全运营效率，需要技术和管理的双重提升。只有构建高效、敏捷的安全运营体系，才能及时应对各种威胁，保障企业核心业务系统和数据的安全。

7.4.2 安全运营框架

华为云基于自身多年的安全运营实践经验和帮助大量客户持续安全运营的经验，基于华为云提供的**安全云脑服务**总结了如下安全运营框架和流程，您的企业可以将其作为起点设计符合企业要求的安全运营框架及流程。

图 7-4 安全运营框架



- **划分安全运营职责**

  首先，根据企业设计的云运营模式，明确业务部门的应用团队与CCoE团队之间的责任边界，如企业采用了赋能与协同运营模式，CCoE团队负责平台层面的安全防护和集中安全运营，应用团队则需要负责应用系统及所需云资源的安全运营。然后在安全云脑中为CCoE团队和各个应用团队分配安全运营的工作空间，在保证各应用团队的安全职责清晰划分的同时，可以向CCoE团队提供统一的安全运营管理视图，最后将业务系统运行环境的安全数据、资产，纳管对接到统一的安全运营平台中，安全云脑可以纳管华为云和IDC的运行环境，还可以跨Region、跨账号纳管运行环境。

- **资产盘点，识别并清理资产风险**

  使用安全云脑自动盘点华为云上各类资产（主机、IP、网站、数据库等），并使用第三方生态软件将云下的资产信息，自动对接到安全云脑中。

  开通HSS对资产上Linux操作系统、Windows操作系统、Web应用漏洞进行自动扫描，并将结果自动对接至安全云脑，进行全生命周期管理。您可以在安全云脑中，对OS漏洞进行一键修复。

  您需要按照法律法规和行业标准，识别资产中的安全风险，在安全云脑中，您可以按照10多个安全合规遵从包（如：等保、PCI-DSS、ISO27001等）以及最佳安全配置实践对各类云资产的安全配置进行自动检查，生成风险项、加固建议、遵从报告，基于安全云脑提供详细加固指导进行风险闭环管理。您可以进一步使用安全云脑全面清点各类资产的防护覆盖情况，统一管理各层防线的安全策略。

- **数据集成及安全分析**

  首先，将安全数据统一对接到安全云脑中，云服务日志一键接入，同时构建云上云下数据统一集成方案，接入第三方生态软件的日志。

  其次，基于安全数据构建安全威胁检测模型并找到安全威胁，分析全攻击链环节、各层防线行为特点，纵深布控，基于大数据技术，训练智能分析算法，海量数据中精准冒泡异常行为，结合用户和实体行为分析（UEBA），还原攻击链，自动更新描绘用户画像、资产指纹、情报画像。

  然后，关联威胁情报辅助判断，从日常运营数据、日志、告警中描绘行为实体，生成新的威胁情报，还可以共享使用华为云平台安全运营自用情报。

- **安全事件处置**

  您需要对告警、事件进行响应、调查、处置；关联实体、资产、情报、历史信息，辅助调查还原告警、事件攻击链；并提供处置预案。您还可以利用安全云脑提供的自动化编排能力，编排自动响应剧本和流程，以快速响应和处置安全威胁。

以上过程是持续不断进行的，在持续不断发现新的安全威胁和处置新安全威胁的循环中，业务系统的安全性得到不断加强，安全运营团队的能力也在不断提升。

7.4.3 安全配置基线

安全配置是信息系统的最小安全保障，云安全配置是云环境最基本的安全保证，是开展安全防护和安全运营的基础。

如果云服务没有达到安全配置基线要求，云上业务及资产将面临巨大安全风险。为了帮助客户提高云环境的安全防护能力，华为云为客户提供了**华为云安全配置基线指南**。该指南包括身份与访问管理、日志与监控、虚拟机与容器、网络、存储、数据库、企业智能等方面的安全配置，但并不是所有可能的安全配置的详尽列表。建议您将该指南作为一个起点，并根据实际需要在此基础上进行补充或裁剪。

按照**华为云安全配置基线指南**，您可以手工检查当前的云服务的安全配置是否满足基线要求，如果不满足，进一步按照指南提供的修复方法进行修复。您也可以使用华为云安全云脑提供的**基线检查**功能完成自动化检查。

7.4.4 软件工程安全

软件工程安全是指在软件开发的整个生命周期中，应用一系列安全原则、实践和技术，以减少软件漏洞，提高软件抵御恶意攻击的能力，最终保障软件的机密性、完整性和可用性。它涵盖了从需求分析、设计、编码、测试到部署和维护的各个阶段。

- **安全设计**

企业需要遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析。威胁分析使用的引导分析威胁库、消减库、安全设计方案库来源于企业自身的安全工程经验积累和业界优秀实践。当识别出威胁后，应用架构师根据消减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，最终保障业务系统的的安全性。

- **安全编码与测试**

  企业需要制定安全编码规范，要求应用系统的开发和测试人员在上岗前均需通过了对应规范的学习和考试。其次，企业需要引入了静态代码扫描工具进行每日检查，其结果数据将导入持续集成和持续部署（Continuous Integration，Continuous Deployment）工具链，通过质量门限进行控制，以评估应用系统的安全性。最后，所有应用系统在发布前均需完成静态代码扫描的告警清零，确保上线时不存在编码相关的安全问题。

  为了确保应用系统的安全性，所有云服务在发布前首先将由应用测试人员执行多轮安全测试，包括但不限于认证、鉴权、API安全、数据库安全等专项安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。对于无法通过安全测试的应用系统，将禁止上线运营。

- **第三方软件安全管理**

  企业对引入的开源及第三方软件需要制定明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件退出等环节，均实施严格的管控。例如在选型分析环节，增加开源软件选型阶段的网络安全评估要求，严管选型。在使用中，须将第三方软件作为应用系统的一部分开展相应活动，并重点评估开源及第三方软件和自研软件的结合点，或使用独立的第三方软件是否引入新的安全问题。

  在社区发布开源软和第三方软件的漏洞时，第一时间发现漏洞并修复，将开源及第三方软件作为应用系统的一部分开展测试，验证开源及第三方软件已知漏洞是否修复，并在应用系统的Release Notes里体现开源及第三方软件的漏洞修复列表。

- **配置与变更管理**

  配置和变更管理对保障应用系统的安全起着重要作用。企业需要对所有应用系统进行配置管理，包括提取配置模型(配置项类型、各类配置项属性、配置项间的关系等)，记录配置信息等。并通过专业的CMDB工具对配置项、配置项的属性和配置项之间的关系进行管理。

  应用系统的各项变更都是影响应用系统安全稳定运行的因素。生产环境中的操作系统、数据库、中间件和应用程序等的变更，包括软件更新、配置改变等，都需要通过有序的活动进行变更管理。所有的变更申请生成后，由变更经理进行变更级别判断后提交给变更委员会，通过评审后方可按计划实施变更。所有的变更在申请前，都需通过类生产坏境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响。

- **上线安全审批**

  为确保应用系统满足法律法规及企业自身的安全规范，最大程度的降低应用系统的网络安全与隐私保护合规风险，CCoE团队的云安全专家需要参与到应用系统的上线活动中，与应用团队合作，共同分析、判断其相关版本或服务是否符合所服务区域的安全隐私合规要求。

  其中，为了确保中低安全与合规风险的应用系统可以快速上线，云安全专家需要发布安全与隐私合规的自检清单，该清单包含企业需要满足的的合规要求，应用团队在开发、部署、上线过程中需利用该清单进行自检。对于中低风险的应用系

统，自检通过后即可上线，自检结果也同步提交给云安全专家执行审计。对高风险的应用系统，通过更多的投入、在短时间内执行更严格的上线检测和审批，确保应用系统安全性的同时，也让应用系统及时上线。

7.4.5 人员安全管理

企业需要对IT部门内的员工以会接触到企业敏感数据的员工进行人员安全管理，主要包括安全意识教育、安全能力培训、重点岗位管理和安全违规问责等。

- **安全意识教育**

  为了提升全员的信息安全意识，规避信息安全违规风险，保证业务的正常运营，企业可以从意识教育普及、宣传活动开展、承诺书签署三个方面开展安全意识教育

  - **意识教育普及：**定期开展信息安全意识教育学习，要求员工持续学习信息安全知识，了解相关政策和制度，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。
  - **宣传活动开展：**面向全员开展形式多样的信息安全宣传活动，包括信息安全社区运营、信息安全典型案例宣传、信息安全活动周、信息安全动画宣传片等。
  - **承诺书签署：**将信息安全纳入《员工商业行为准则》，通过公司统一开展的年度例行学习、考试和签署活动来传递公司对全员在信息安全领域的要求，提高员工信息安全意识。签署信息安全承诺书，承诺遵守公司各项信息安全政策和制度要求。

- **安全能力培训**

  参考业界优秀实践，建立完备的信息安全培训体系。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。

  - **信息安全基础培训：**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信息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。管理者需参加信息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，开发信息安全实战演练平台，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和安全响应能力。
  - **安全能力任职牵引：**为了让员工更加自觉、有效地进行信息安全学习，将信息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信息安全课程，通过相应的信息安全技能考试，提升自身信息安全能力。

- **重点岗位管理**

  为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，建议您对运维工程师等重点岗位实施专项管理。具体如下：

  - **上岗安全审查：**针对新上岗人员，开展上岗人员安全审查，确保上岗人员背景和资历符合企业的信息安全要求。
  - **在岗安全培训赋能：**围绕信息安全意识、客户网络服务的业务规范、用户数据及隐私保护要求进行信息安全学习和考试，并根据业务变化定期刷新学习和考试大纲。

  - **上岗资格管理：**重点岗位员工必须通过信息安全上岗证的考试，并取得证书。通过证书管理平台对已通过安全上岗证考试的员工发放有效期不超过两年的电子证书，证书到期前提醒员工重新参加考试。
  - **离岗安全审查：**按照调动、离职安全审查清单，对内部调离、离职人员进行离岗安全审查，包括离岗权限账号的清理或修改等。

- **安全违规问责**

  企业需要建立严密的安全责任体系，贯彻违规问责机制。要求每个员工都对自己工作中的行为和结果负责，不仅要对技术和服务负责，也要承担法律的责任。安全问题一旦发生，可能会对企业带来极大影响。因此不管故意还是无意，要以行为和结果为主要依据对员工进行问责。根据安全违规的性质，以及造成的后果确定问责处理等级，分级处理。对触犯法律法规的，移送司法机关处理。直接管理者和间接管理者存在管理不力或知情不作为的，须承担管理责任。违规事件处理根据违规个人态度与调查配合情况予以加重或减轻处理。

7.4.6 云原生安全服务

华为云提供了丰富的云原生安全服务，这些云原生安全云服务与华为的云平台深度集成，在性能、弹性、便利性上有较好的优势，同时，云服务商的安全运营经验也会持续推动云原生安全服务的能力提升，建议企业优先选择云原生安全服务。

- **数据加密服务**

  数据加密服务（Data Encryption Workshop, DEW）是一款综合的云上数据加密服务。它可以提供专属加密、密钥管理、凭据管理、密钥对管理等服务，安全可靠的为您解决了数据安全、密钥安全、密钥管理复杂等问题。其密钥由硬件安全模块（Hardware Security Module，HSM）保护，并与多个华为云服务集成。用户也可以借此服务开发自己的加密应用。关于DEW服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **主机安全**

  主机安全服务（Host Security Service，HSS）是以工作负载为中心的安全产品，HSS通过对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。HSS不受地理位置影响，为主机、容器等提供统一的可视化和控制能力。关于HSS服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **Web应用防火墙服务**

  Web应用防火墙（Web Application Firewall，WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。在WAF管理控制台将网站添加并接入WAF，即可启用WAF。启用之后，您网站所有的公网流量都会先经过WAF，恶意攻击流量在WAF上被检测过滤，而正常流量返回给源站IP，从而确保源站IP安全、稳定、可用。关于WAF服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **数据库安全**

  数据库安全服务（Database Security Service，DBSS），是一个智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库的安全。包括用户行为发现审计、多维度分析、实时告警、提供精细化报表、敏感数据保护、审计日志备功能。数据库安全审计提供的旁路模式数据库审计功能，可以对风险行为进行实时审计和告警。同时，通过生成满足数据安全标准的合规报告，可以对数据库的内部违规和不正当操作进行审计及定位追责。关于DBSS服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **云防火墙**

  云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，支持按需弹性扩容，是为用户业务上云提供网络安全防护的基础服务。其安全功能包括VPC间边界防护、访问控制策略、入侵防御策略、病毒防御、流量分析、系统管理、等功能特性。关于CFW服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **数据安全中心**

  数据安全中心服务（Data Security Center，DSC）是新一代的云化数据安全平台，提 供数据分级分类、数据安全风险识别、数据水印溯源和数据静态脱敏等基础数据安全能力。DSC通过数据安全总览整合数据安全生命周期各阶段状态，对外呈现整体云上数据安全态势，帮助用户实现数据安全全生命周期管理。关于DSC服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **安全云脑**

  安全云脑（Security Master，SecMaster）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理。关于SecMaster服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **DDoS防护**

  DDoS防护（Advanced Anti-DDoS，AAD）在企业重要业务连续性方面提供了有力保障。当用户的服务器遭受大流量DDoS攻击时，DDoS防护可以保护用户业务持续可用。DDoS防护通过高防IP代理源站IP对外提供服务，将恶意攻击流量引流到高防IP进行清洗，确保重要业务不被攻击中断。DDoS防护服务于华为云、非华为云及IDC的互联网主机。关于DDoS防护服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **云证书管理服务**

  云证书管理服务（Cloud Certificate Manager，CCM）是一个为云上海量证书颁发和全生命周期管理的服务。目前，它提供有SSL证书管理（SSL Certificate Manager，SCM）和私有证书管理（Private Certificate Authority，PCA）服务。关于云证书管理服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **漏洞管理服务**

  漏洞管理服务（CodeArts Inspector）是针对网站、主机、移动应用、软件包/固件进行漏洞扫描的一种安全检测服务，目前提供通用漏洞检测、漏洞生命周期管理、自定义扫描多项服务。扫描成功后，提供扫描报告详情，用于查看漏洞明细、修复建议等信息。关于漏洞管理服务的详细功能和详细使用方法，请参考**官网帮助文档**。

- **云堡垒机**

  云堡垒机（Cloud Bastion Host，CBH）是华为云的一款4A统一安全管控平台，为企业提供集中的帐号（Account）、授权（Authorization）、认证（Authentication）和审计（Audit）管理服务。CBH服务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。关于CBH服务的详细功能和详细使用方法，请参考**官网帮助文档**。

7.5 FinOps

7.5.1 概述

根据Flexera在2024年发布的《State of the Cloud Report》报告显示，管理云成本成为企业用云的头号挑战，企业的的云成本平均超过预算15%，平均有27%的公有云成本是浪费的，51%的企业已经成立了专门的FinOps团队，另外有20%的企业计划在未来一年成立FinOps团队。

越来越多的企业在利用云的敏捷高效、创新、弹性扩展优势时，遇到云成本管理方面的一系列难题，主要有如下四个难点：

- **成本可变导致成本规划困难：**传统IT采购后成本固定，上云后这一规则被打破。云资源 按需弹性使用，云成本随着业务动态变化，如高峰流量时云资源占用多、升级 扩容时动态开通新资源等。云成本可变导致静态规划的预算和业务实际产生的 成本偏差大。
- **去中心化采购导致成本控制难：**传统IT采购由采购部门集中采购，可管可控。而上云 后云资源消费贯穿用云整个过程，采购责任也从集中采购变为去中心化采购， 即工程师直接购买资源而非传统的采购人员购买。工程师在消费云资源时成本 意识薄弱，且消费云资源的工程师部门多人数多，使得云成本控制困难。
- **云服务丰富导致成本优化难：**云服务商通常都提供数百个云服务和多样化的计费量纲，各服务也没有统一的调优方案。而且云厂商持续发布新服务、新实例类型和新的优惠。面对云上如此丰富的供应和选择，企业难以开展成本优化工作。
- **灵活开通导致精细化管控难：**云的灵活扩展和支出限制少，有利于业务发展和创新，但也容易产生资源浪费。如为了追求性能和质量，业务团队配置的资源大 于运行工作负载实际需要，产生过度配置；部分项目新建环境或者扩容实例 后，最后忘记关闭形成闲置等；

  企业面对这些问题时，发现难以精细化管理云成本，也难以选择最优的成本优化路径，且优化后的效果难以持续，因此FinOps必须被提上日程。

  FinOps是“Finance”和 “DevOps”的结合，推崇业务团队和工程团队（IT团队）之间的沟通和协作，目的是解决企业管理云成本难题。按照**FinOps基金会的定义**，FinOps是一个运营框架和文化实践，它最大限度地发挥云的业务价值，支持及时的数据驱动决策，并通过工程（IT）、财务和业务团队之间的协作来建立财务问责制。

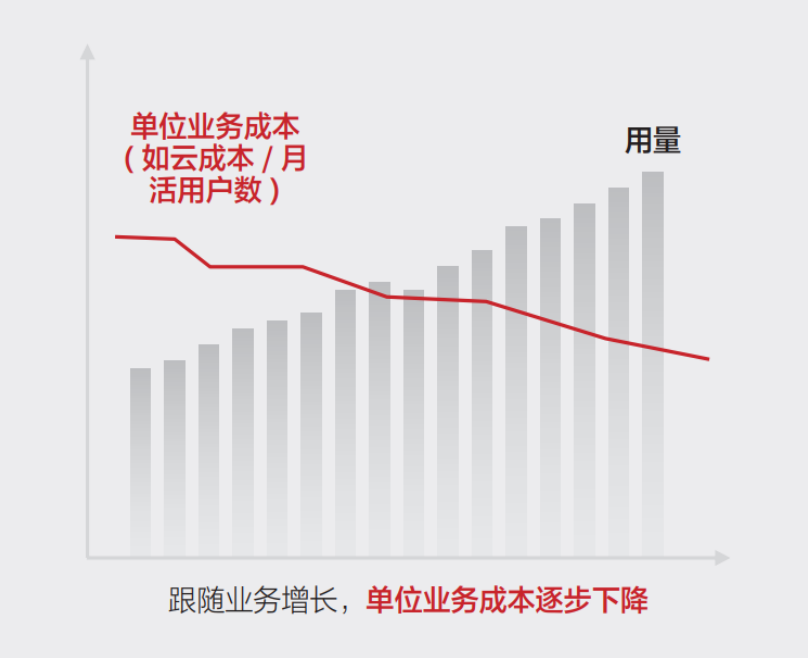
  企业云资源消费贯穿云化转型的整个过程，管理云成本也需要持续迭代优化。FinOps基金会梳理的**FinOps框架**包含三阶段：成本可视、成本优化和持续成本运营，指导企业对成本进行持续优化，如下图所示。需要注意的是，在成本优化时要做好成本、质量与效率的平衡，避免企业为了极低成本导致业务效率和稳定性受到影响。

图 7-5 FinOps 的三个阶段

FinOps框架指导企业从组织、文化、流程等多方面建设成本运营体系，通过多团队协作和基于数据决策，精细化管理云成本：各业务团队成本可视，主动控制不超支不浪费；企业基于数据决策云投资，保障企业核心业务和战略业务方向的支出。企业应用FinOps后，可以持续降低**单位业务成本**。

需要了解更多关于FinOps的信息等，请直接参考**FinOps基金会的网站**。

图 7-6 单位业务成本逐步下降



7.5.2 FinOps 参考架构

华为云结合FinOps基金会的FinOps框架和华为自身的FinOps实践总结提炼的一套FinOps参考架构，如下图所示，总体上包含成本计划、成本控制、成本分析和成本优化四个阶段。

图 7-7 华为云 FinOps 参考框架

华为云还提供的丰富的成本管理工具，提升成本管理的效率，帮助企业在华为云上开展FinOps实践，持续提升云的成本效益。

表 7-1 华为云的云成本管理工具列表

分类	工具	适用场景
成本规划与计划	价格计算器	自主搭配产品估算新业务上云支出
	成本与使用量预测	预测存量业务的未来支出
	企业多账号	大型企业、集团公司，通过账号隔离资源和成本
	企业项目	中小型企业及单账号下的组织映射
	成本标签	更多维度、更细粒度、更灵活的组织映射
	预算管理（含预算报告）	计划跟踪所需粒度的云支出，及时获取超预算提醒，或定期周知最新进展
管理账单与控制成本	资金管理	监控可用额度，跟踪支出异常
	资源包管理	监控资源包是否即将用尽
	账单管理	了解各帐期的实际消费与支出，多维对账
	成本监控	监控云支出的异常增长，减少异常账单

分类	工具	适用场景
成本分配与可视化	成本分析（含分析报告）	了解成本趋势与分布，洞察成本变化的驱动因素
	成本单元	将成本按照业务语义分配到有意义的分组，拆分公共成本
	成本明细	获取成本分配明细（下载和OBS订阅）
	账单数据存储	订阅详细的账单明细到OBS桶
	云智能看板（CXO看板）	面向CXO、高管以及组织管理者提供的仪表盘集合。
成本节省与优化	按需转包年包月优化评估	获取按需转包年包月商品的成本优化机会
	资源包使用率/覆盖率分析	了解已购买资源包的使用效率
	资源包建议	获取资源包购买建议以节省成本
	资源优化建议	识别空闲资源以节省成本
	优化顾问	识别使用率低或闲置的云资源以节省成本

7.5.3 成本计划

- **匹配企业管理模型，确保未来成本可追溯**

  云财务管理的基础是树立成本责任制，让各部门、各业务团队、各负责人参与进来，为各自消耗云服务产生的成本负责。

  华为云为客户提供了多种工具，以帮助客户合理规划组织，确保成本可追溯。

  大型企业或集团公司可以使用企业组织+多账号的方式，通过账号隔离资源和成本，方便业务快速拓展。

  中小型企业以及单账号客户，建议优先使用人财物权管理相对完善的企业项目来映射组织。如果存在更多维度、更细粒度规划的诉求，可以使用标签作为组织规划的补充。比如用标签来区分资源归属的产品团队和负责人

  综上所述，无论是采用哪种方式，您都需要尽早完成组织规划，并确保规划的规则能始终如一的执行下去。

- **通过智能预测和估算，预估未来成本**

  随着企业深度上云，企业云上支出持续高速增长，如何预估未来云成本对企业的规划至关重要。企业未来用云成本通常包含两类，一是已经上云的业务持续产生的云成本，另外一类是因为新规划业务产生的云成本，如新上云业务或者出海等在其他区域提供服务产生的云成本。由于云支出是可变的，没有一种预测方法可以适用所有场景， 结合基于趋势（已上云业务的历史支出作为输入）的预测和基于业务驱动因素（例如新业务上云或区域扩张）的预 测，可以有效改进并提升企业的财务预测准确率。

  使用成本中心的成本分析，可以根据客户的历史支出预测未来时间范围的成本。成本分析的成本和使用量预测，会参考不同的计费模式特征，结合机器学习和基于规则的模型来分别预测所有消费模式的成本和使用量。

使用成本分析确定基于趋势的预测之后，您还可以利用华为云的**价格计算器**，根据新业务上云或区域扩展所需的产品和使用量，自主搭配产品进行未来成本的估算。

- **通过预算管理，跟踪未来资源用量和费用执行**

  预算超支是管理云成本核心难题之一。完成组织和成本的规划后，企业可以为各业务团队制定预算，并跟踪各业务团队预算执行情况。通过预算跟踪，确保各业务团队及时看到预算执行情况，并根据实际成本和预算的差异及时控制，避免预算超支。

  华为云提供了通用的**预算管理**工具，您可以根据企业实际规划的预算，用预算管理工具跟踪起来，并可以设置细粒度的过滤条件，精细化跟踪具体产品、团队、项目的成本。

  除了在成本中心查看预算进展外，您还可以为指定预算设置预算提醒，当实际使用或预测使用达到提醒阈值时，及时接收系统发出的短信或邮件预警，从而及时采取下一步措施。

  您还可以设置**预算报告**，定期将指定预算的执行情况以日报、周报、月报的形式周知给企业内部相关角色，比如业务部门、财务、CTO，达到成本透明的目的。

7.5.4 成本控制

- **通过预算管理，跟踪未来资源用量和费用执行**

  云资源按需灵活扩展，云成本在用云过程中不再固定不变。为了避免意外账单，需要在用云过程中精细化控制，对风险事项建立监控预警机制和应对机制，一旦产生预警则及时应对，避免产生异常高成本。在发生异常时，分析根因也至关重要。如发现异常成本时，需要确认是业务发展导致，还是资源过度配置或资源闲置导致，并根据根因进行扩大预算或者优化资源使用。

  使用成本中心的**成本监控**，您可以及时识别成本的异常增长。

  成本监控引入机器学习，对客户历史消费数据进行建模，对于不符合历史数据模型的成本增长，识别为异常成本记录，同时提供异常增长的Top潜在原因。

  客户可设置监控提醒，定期获取影响成本高的异常记录提醒，并根据系统提供的潜在原因，结合成本分析和业务情况进行深入分析，进而快速做出反应，维持预期的成本支出。

- **通过账单核对支出，个性化对账提高对账效率**

  多样化的费用图表可以帮助您快速了解账单情况，完成账单的多维度对账。

  华为云为客户提供多种维度的**账单介绍**，您可以重点关注总体的消费走势、Top产品类型、Top企业项目、Top区域、Top计费模式，从而快速评估月度消费是否符合预期。您还可以获取流水账单和明细账单，按月度查看资金流水和资源扣费的详细信息。消费总计、付款情况、账单的明细数据等。

  客户可以将华为云导出的账单和公司自己财务生成的账单进行**多维度对账**，以确认资源的购买、使用和账户的实际支出是否一致。

- **资金监控和资源包预警**

  华为云分别从账户资金余额和资源包剩余使用量的角度跟踪是否有异常支出，避免产生额外消费。

  开启可用额度预警，您可以及时接收系统发出的可用额度不足预警，从资金账户的角度跟踪支出是否存在异常

  如果您购买了资源包，可使用费用中心的**资源包管理**功能，及时了解已购买资源包的剩余用量情况；并开启资源包的剩余使用量预警，在资源包用尽前及时接收预警，从而通过限制按需使用或补充购买新资源包的方式，避免意外按需消费的产生。

7.5.5 成本分析

成本分配驱动业务方承担财务责任

成本分配支撑企业将成本分配到各业务团队中，使得各业务团队的成本清晰可见。根据清晰的成本，业务部门可准确定价，并平衡成本、稳定性和性能，经济高效的提供领先方案。企业管理者基于数据决策各业务的云开支， 保障核心业务和战略业务方向的支出，不超支，不浪费。 典型的成本分配场景包括：

- 分配成本到项目：呈现不同项目团队成本情况，如创新项目、拓展项目等。
- 分配成本到部门：呈现各个部门的成本情况，如研发部门成本、测试部门成本。
- 分配成本到品牌：呈现各个品牌的成本情况，如研发、制造、门店销售过程中用云成本等。
- 分配成本到各系统：呈现服务内部的IT系统成本，如多业务使用的中台成本。

华为云提供多种成本分配能力支撑企业分配成本：

- **直接成本分配：**企业可以通过按照资源产生成本时归属的关联账号、企业项目或成本标签进行成本分配。
- **权益商品成本分摊：**包年包月、资源包等权益商品成本，按照实际使用情况**摊销**到企业项目、标签和资源。
- **流量型资源的公共成本按用量拆分**：使用成本中心的**共同成本分拆能力**，可将CDN、Live等团队共享使用的云资源成本，按照实际用量分摊到域名或IP。
- **容器集群成本拆分**：华为云提供**CCE成本洞察**，开通后可将CCE集群相关的CCE集群管理费、CCE集群关联的ECS和EVS资源费用拆分到集群、命名空间和工作负载。
- **多维度分类和汇总**：使用**成本单元**，综合多种条件（产品类型、账单类型、关联账号、企业项目、成本标签）对成本进行分类和汇总，如品牌维度、子系统维度等。
- **公共成本分配**：使用**成本单元**的公共成本拆分能力，将公共成本（例如共享资源&平台服务等公共成本、未及时 标记的成本）按比例在组织内进行再分配，满足各团队或业务部门公平分配公共成本的需求。

多维度成本分析探索成本和用量

企业针对云成本做精细化分析，看清成本结构和趋势，常用的成本分析场景包括：

- 成本增长趋势是否和业务一致，增长趋势是否平稳；
- 哪些云服务开支最大，哪些云服务开支增长最快；
- 资费模式是否合理，是否使用了性价比最高的新规格资源；
- 资源布局是否合理？是否使用了低成本的Region资源；
- 哪些原因导致成本波动？

华为云提供**成本分析**，为您提供多维度的汇总和过滤机制，从而通过各种角度、范围分析成本和用量的趋势及驱动因素。针对客户常用的成本数据筛选条件，成本中心提供如下预置报告，帮助客户快速分析：

表 7-2 成本中心的预置报告

预置报告名称	说明
按多维度汇总的当月至今成本	了解当月至今按多维度汇总的原始成本数据，查看成本的分布和流向。
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。
月度摊销成本	了解过去6个月摊销成本的月度趋势。
每日成本	了解过去3个月+未来一个月的每日原始成本趋势。
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的月度成本数据。
按企业项目汇总的月度成本	了解过去6个月各企业项目的原始成本月度数据。
按区域汇总的月度成本	了解过去6个月按照区域汇总的原始成本月度数据。
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。
容器成本洞察	了解CCE集群、命名空间、工作负载粒度的成本分布和趋势。

7.5.6 成本优化

- **选择合适的计费模式**

  华为云为客户提供了按需、包年包月、资源包、竞价实例等多种计费模式，不同的计费模式有着不同的适用场景。企业合理利用云资源的不同计费模式，来适配不同的业务形态，可以有效降低费率，实现成本节省。

  按需计费：适用于临时、突发的业务场景。

  包年包月：通过预付一定周期的资源使用费用，来获取优惠的计费模式。一般适用于资源长期使用，业务较稳定的场景。

  资源包：一种特殊的包年包月，可通过预付一定周期下某种资源使用量的费用，来获取优惠的计费模式。资源包可以抵扣多个资源的用量，适用于长期使用且用量比较稳定的场景。

  竞价计费：适应于业务稳定性不高，中断也不影响业务的场景，目前仅ECS支持。

- **优化计费模式与节省成本**

  华为云提供计费模式的优化建议，帮助企业在不改变资源性能的情况下，通过调整计费模式来节省成本。

  按需转包年包月成本优化评估：自动识别客户长期按需使用的资源（比如云主机、云硬盘、RDS数据库），按需转包周期的转换建议和节省评估。客户可重点关注高节省低风险的节省建议（“预计月度节省”高且“盈亏平衡时间”短）。

  资源包购买建议：根据您资源包覆盖产品（比如OBS、SFS）的按需资源消费情况，提供相应的**资源包购买建议**。

您还可以通过**资源包的使用率/覆盖率分析**，了解已购资源包的使用情况，识别资源包购买过多（使用率低），还是过少（覆盖率低），从而优化下一阶段的购买。

- **识别空闲和低利用资源**

  华为云提供**资源优化建议**，通过监控客户的历史消费情况和资源利用率，帮助您识别空闲资源（比如云主机）。您可参考系统给出的利用率信息、预估月度节省，结合业务团队意见，采取资源优化行动。

  华为云**优化顾问**，提供成本维度的巡检，可以帮助您快速准确地识别出当前存在的风险点，并给出优化建议。

- **架构优化与持续运营**

  FinOps专业服务结合企业业务场景，可针对业务布局、资源规划、数据存储各层次进行架构优化，如在离线业务混合部署提升资源利用率、存算分离使计算和存储各自按需使用避免绑定浪费、冷热分离降低冷数据存储成本等。

7.6 持续优化

运维治理阶段是一个持续改进的循环，您需要基于**Well-Architected Framework（简称WAF）**定期审查和评估云环境，根据业务需求和 WAF 的最佳实践进行调整和优化。您也需要持续学习和应用新的华为云服务和功能，不断提升云环境的成熟度。

通过将 WAF 的五大支柱与精益化治理、确定性运维、全方位安全运营和精细化FinOps相结合，可以构建一个持续优化、安全可靠、高性能、经济高效的云上环境，从而更好地支撑业务发展。

相关链接

Well-Architected Framework（简称WAF）

