

序 言

百联集团在建设成为面向未来的数字化商业体的战略目标指引下，通过与华为的紧密合作，迈出了全面数字化转型的第一步——打造云底座。“道阻且长，行则将至。行而不辍，未来可期”，我们也希望借此报告发布，分享我们的实践经验总结，助力中国企业坚定转型升级信心，明晰创新发展路径，践行科学发展精神。

孙伟 百联集团副总裁

华为云持续践行“一切皆服务”，通过全栈创新加速企业数字化转型升级。华为与百联的合作旨在共同推动数字化商业体的转型与发展，此次合作也使我们有机会共享彼此的知识 and 经验，将我们的理论框架、知识体系和落地实践分享出来，形成大型零售电商平台云转型白皮书，旨在为中国零售行业提供一份高质量的指南，为他们的转型升级之路指引方向。

石冀琳 华为云副总裁、全球 Marketing 与销售服务部总裁

编制委员会

主要参编单位和人员：

百联：王善良（主编）、张国炜、李祥宝、郭君、汪正、蒋帅、袁伟、徐松、王远、谢俊民

华为：贾小江（主编）、郭喜平、何凯、李伟、董洪均、史章斌、黄灵杰、张博文、杨帆、

马新刚

编委会名单：

百联：孙伟、王晓琰、华磊、张栋艺、杨峰

华为：石冀琳、张修征、郭奕昱、徐敬滨、刘正宝、张英梗、王斌、张东生、张明煌、钱

琪、曹照连、方磊、胡迪辉、刘江江、齐舟、陈琦隼、徐殿军

致 谢：白皮书撰写期间，亦得到百联厉波、王佳露，华为刘宗辉、林华鼎、黄勤来、王有龙、刘丽丽、苏战、张顺、张雷、时涓涓、周练、刘科、张文强、李康、周纪、孙慧、刘思圆、沈梦霞的帮助和建议。

由于时间仓促，书中可能存在不完善和疏漏之处，非常欢迎读者朋友们提出宝贵的意见和建议，以便不断改进和完善本白皮书。非常感谢您的理解和支持！

使用说明

本白皮书适用于企业上云场景，白皮书站在企业的视角详细介绍了上云迁移的全过程，包括企业上云的驱动力和价值评估、上云准备、云上架构设计、小范围试点、可执行的批次规划、实施大规模上云迁移、云上运维和治理。白皮书提供了一套经过实践验证的标准化的上云流程和方法，对于企业上云，特别是大企业全量上云，具有参考和借鉴意义。

目标读者：本白皮书的目标读者是企业的 CTO、运维总监、云架构师、业务架构师以及其他与上云相关的人员。建议架构师可重点阅读第 5 章（云上架构设计）；迁移实施相关的人员可重点阅读第 8 章（应用上云迁移小循环）、第 9 章（大数据迁移上云）和第 11 章（大规模上云阶段经验）。

目标企业：由于不同企业的研发能力、IT 运维能力和治理能力存在有差异，导致他们选择的上云方式也有所不同。对于业务系统主要是自研的企业来说，通常有自己的运维团队，企业 IT 能力也比较强，可以主导上云工作，建议精读此白皮书，对企业主导上云工作有借鉴意义。对于业务系统主要是外部采购或由供应商定制开发的企业来说，企业 IT 能力通常比较弱，系统主要依赖第三方厂商代维，企业无法主导上云工作，上云迁移主要依赖于第三方供应商，为了企业能更好地监控并配合供应商完成上云任务，相关负责人也需要大致了解白皮书的内容，熟悉上云迁移的整体流程。

目 录

序 言.....	1
编制委员会.....	2
使用说明.....	3
目 录.....	4
1 云迁移框架概述.....	13
1.1 企业上云趋势.....	13
1.2 企业上云的挑战.....	14
1.3 企业典型的 IT 架构.....	16
1.4 云迁移框架介绍.....	16
2 上云调研分析.....	20
2.1 调研方式.....	20
2.2 调研内容.....	21
2.2.1 基础环境调研.....	21
2.2.2 应用迁移调研.....	22
2.2.2.1 调研应用全景图.....	22
2.2.2.2 调研应用部署架构.....	23
2.2.2.3 调研应用关联关系.....	25
2.2.2.4 调研应用上云需求.....	29
2.2.3 大数据迁移调研.....	29
2.2.3.1 平台调研.....	29
2.2.3.2 数据调研.....	31
2.2.3.3 任务调研.....	31
2.3 调研过程.....	32
3 上云评估规划.....	34
3.1 企业上云的驱动力评估.....	34
3.1.1 常见的上云驱动力.....	34
3.1.2 识别企业上云动机.....	35
3.2 云成熟度评估.....	36

3.2.1 评估方法	36
3.2.2 评估维度说明	36
3.3 上云可行性评估	38
3.4 上云策略规划	38
3.5 高阶方案规划	39
3.5.1 方案范围	39
3.5.2 高阶方案示例	40
3.5.2.1 基础环境规划示例	40
3.5.2.2 应用部署架构示例	43
3.5.2.3 迁移方案示例	44
3.6 企业上云的收益评估	45
3.6.1 降低 TCO	45
3.6.1.1 降低资源配置成本	45
3.6.1.2 降低灾备建设成本	45
3.6.1.3 降低运维人力成本	47
3.6.2 提升系统可用性	47
3.6.3 加快业务创新	47
3.6.4 增强安全能力	48
3.6.5 增强运维便利性	49
4 企业上云准备	50
4.1 干系人识别	50
4.1.1 内部干系人	50
4.1.2 外部干系人	51
4.2 组建 CCoE 团队	52
4.2.1 什么是 CCoE	52
4.2.2 为什么要构建 CCoE	53
4.2.3 如何构建 CCoE	54
4.3 技能准备	55
4.3.1 做哪些技能准备	55
4.3.2 如何做技能准备	56
4.4 运维平台准备	56
4.5 项目管理准备	57
4.5.1 概述	57

4.5.2 目标制定	58
4.5.3 过程管理	59
4.5.4 有效沟通	60
4.6 上云动员会	61
5 云上架构设计	63
5.1 架构设计概述	63
5.2 基础环境设计	64
5.2.1 基础环境介绍	64
5.2.2 统一账号权限	65
5.2.2.1 组织映射	65
5.2.2.2 账号规划	66
5.2.2.3 权限设计	67
5.2.2.4 合规使用	68
5.2.3 统一网络管理	69
5.2.3.1 云上网络设计	69
5.2.3.2 网络互联建议	70
5.2.3.3 迁移网络设计	71
5.2.3.4 迁移带宽评估	72
5.2.3.5 迁移专线建议	72
5.2.4 统一安全管控	73
5.2.4.1 整体安全设计	73
5.2.4.2 应用安全设计	75
5.2.5 统一资源治理	77
5.2.5.1 资源治理原则	77
5.2.5.2 资源共享	78
5.2.5.3 资源合规	78
5.2.5.4 资源分组	78
5.2.5.5 资源标签	80
5.2.5.6 资源命名	81
5.2.5.7 资源配额	82
5.2.5.8 资源控制	83
5.2.6 统一运维监控	84
5.2.6.1 统一监控及告警	84

5.2.6.2 统一日志存储	85
5.2.6.3 统一补丁更新	86
5.2.7 统一财务管理	87
5.2.7.1 成本计划	87
5.2.7.2 成本分配	88
5.2.7.3 成本分析	90
5.2.7.4 成本优化	91
5.3 应用部署架构设计	94
5.3.1 应用部署架构概述	95
5.3.2 可用性设计	96
5.3.2.1 可用性定义	96
5.3.2.2 AZ 故障域说明	97
5.3.2.3 云上高可用方案	97
5.3.2.4 双 AZ 高可用设计	98
5.3.2.5 两地三中心高可用设计	99
5.3.3 跨 AZ 高可用设计示例	101
5.3.4 可扩展性设计	105
5.3.4.1 云上可扩展性	105
5.3.4.2 可扩展设计	106
5.3.5 性能设计	107
5.3.6 应用部署参考架构	108
5.3.6.1 应用部署架构示例	108
5.3.6.2 参考架构库	109
5.4 大数据架构设计	112
5.4.1 范围说明	112
5.4.2 设计原则	112
5.4.2.1 大数据集群设计	113
5.4.2.2 大数据任务调度平台设计	113
5.4.3 参考架构	114
5.4.4 华为云大数据组件	115
6 上云迁移试点	118
6.1 为什么要上云试点	118
6.2 如何选择试点应用	119

6.3 上云试点执行	119
6.4 上云试点总结	120
7 上云批次规划	121
7.1 相关术语说明	121
7.2 为什么要做批次规划	121
7.3 迁移批次规划的方法	122
7.3.1 迁移分组	122
7.3.2 迁移分批	122
7.3.3 迁移优先级	123
7.4 应用迁移批次规划样例	124
7.5 大数据迁移批次规划说明	124
8 应用上云迁移（小循环）	126
8.1 概述	126
8.2 调研	127
8.3 设计（迁移方案）	128
8.3.1 迁移方案概述	128
8.3.2 接入层迁移方案	129
8.3.3 应用层迁移方案	130
8.3.3.1 平迁部署在主机上的应用	130
8.3.3.2 平迁部署在容器中应用	130
8.3.3.3 主机上的应用容器化上云	131
8.3.4 中间件层迁移方案	131
8.3.4.1 Redis 迁移方案	131
8.3.4.2 消息中间件迁移方案	132
8.3.5 数据层迁移方案	133
8.3.5.1 结构化数据迁移方案	133
8.3.5.2 非结构化数据迁移方案	134
8.3.6 迁移工具兼容性查询	135
8.4 设计（切换方案）	135
8.4.1 如何选择停服不停服	135
8.4.2 停服切换方案	137
8.4.2.1 停服时长评估	137
8.4.2.2 减少停服时长的方法（分钟级）	137

8.4.2.3 四种停服切换方式.....	138
8.4.2.4 一把切（应用层和数据层整体停机后切换）.....	138
8.4.2.5 应用层灰度切流，数据层整体切换.....	139
8.4.2.6 应用层灰度切流，数据层分批切换.....	141
8.4.2.7 按照业务域分批切换.....	143
8.4.3 停写不停读切换方案.....	144
8.4.3.1 四种停写不停读切换方案对比.....	144
8.4.3.2 网关拦截.....	145
8.4.3.3 写服务关停.....	146
8.4.3.4 应用改造.....	146
8.4.3.5 中间件层/数据层配置只读.....	147
8.4.4 不停服切换方案.....	147
8.4.4.1 应用层切换不停服方案.....	147
8.4.4.2 数据层或应用整体切换不停服方案.....	148
8.4.5 设计 Runbook.....	148
8.4.5.1 Runbook 设计原则.....	148
8.4.5.2 Runbook 角色设计.....	149
8.4.5.3 Runbook CheckList 设计.....	150
8.4.5.4 Runbook 操作步骤设计.....	151
8.4.5.5 Runbook 参考模板.....	152
8.5 部署（目标环境和迁移环境）.....	152
8.5.1 云资源开通及配置.....	152
8.5.2 迁移工具部署.....	153
8.6 迁移.....	154
8.6.1 接入层迁移实施.....	154
8.6.2 应用层迁移实施.....	155
8.6.2.1 主机迁移.....	155
8.6.2.2 容器迁移.....	157
8.6.3 中间件层迁移实施.....	158
8.6.3.1 Redis 迁移.....	158
8.6.3.2 消息中间件迁移.....	160
8.6.4 数据层迁移实施.....	161
8.6.4.1 对象存储迁移.....	161

8.6.4.2 文件存储迁移	163
8.6.4.3 数据库迁移.....	164
8.6.5 迁移实施常见问题及应对.....	168
8.7 验证.....	168
8.7.1 数据验证	168
8.7.1.1 数据验证标准	168
8.7.1.2 数据验证方法	169
8.7.2 业务验证	170
8.7.2.1 功能验证	170
8.7.2.2 性能验证	174
8.8 切换.....	177
8.8.1 切换演练	177
8.8.1.1 为什么要演练.....	177
8.8.1.2 演练流程	178
8.8.1.3 演练准备	179
8.8.1.4 演练实施和复盘	180
8.8.2 正式切换	181
8.8.2.1 切换前准备和检查.....	181
8.8.2.2 Runbook 切换操作	184
8.9 保障.....	185
9 大数据迁移上云.....	186
9.1 概述.....	186
9.2 调研.....	187
9.3 设计.....	187
9.3.1 设计数据迁移方案.....	187
9.3.2 设计数据校验标准.....	188
9.3.3 设计任务迁移方案.....	189
9.3.4 设计大数据双跑方案	190
9.4 部署.....	191
9.4.1 平台部署	191
9.4.2 平台权限配置.....	192
9.5 迁移.....	192
9.5.1 数据迁移	192

9.5.2 任务迁移	195
9.6 验证.....	197
9.6.1 数据校验	197
9.6.2 任务验证	197
9.7 切换.....	197
9.8 保障.....	198
10 应用现代化上云.....	199
10.1 什么是应用现代化.....	199
10.2 基础设施现代化	201
10.2.1 容器化改造上云	201
10.3 应用架构现代化（微服务改造/优化）	201
10.3.1 微服务改造上云（单体->微服务）	201
10.3.2 微服务架构优化	203
10.4 开发与运维现代化.....	204
10.5 治理与运营现代化.....	205
10.6 新技术使能业务现代化	205
11 大规模上云阶段经验.....	209
11.1 大规模上云阶段概述.....	209
11.2 大规模上云阶段经验总览.....	210
11.3 如提前拉通专线	210
11.4 如何做技术评估	211
11.4.1 研发侧技术评估	211
11.4.2 运维侧技术评估	213
11.5 如何做上云适配改造	214
11.6 如何分析业务影响.....	215
11.6.1 线下业务影响分析.....	215
11.6.2 线上业务影响分析.....	216
11.6.3 业务降级演练.....	217
11.7 如何选择停机窗口.....	217
11.8 如何解决应用跨云时延	219
11.9 如何制定测试策略.....	220
11.10 如何组织切换演练.....	221
11.10.1 会场布置	221

11.10.2 全员宣讲	222
11.10.3 明确纪律	223
11.10.4 确定分工	224
11.10.5 过程管理	225
11.10.6 优化 runbook	226
11.11 如何做风险管理	226
11.12 如何做复盘分析	230
12 云上运维及治理.....	233
12.1 云运维概述.....	233
12.2 云运维组织.....	235
12.3 云运维流程.....	236
12.4 云运维平台.....	237
12.4.1 ITSM.....	238
12.4.2 CMDB	238
12.4.3 ITOM	239
12.4.4 运维平台选择.....	239
12.4.5 运维平台集成.....	241
13 附录.....	244
13.1 缩略语列表.....	244

1 云迁移框架概述

1.1 企业上云趋势

当今世界正经历百年未有之大变局，过去三年全球经济形势发生了深刻的变化，越来越多的企业将传统的线下业务转移到线上，借助科技手段来应对这种变化。在当前形势下，企业数字化转型已从一个选择性的优势项，变成了企业生存发展的必需项。企业数字化转型往往以“上云”作为起手式，先业务上云，再云上创新，乘云启航，逐步实现企业数智化转型战略。企业上云的现状可以概括为“从被动到主动，然后成为一种新常态”。企业上云的趋势可以概括为如下六点：

1. **企业上云已经从潮流变为标配。**原先很多企业还在观望和犹豫，而现在上云已成为大部分企业的共识。云服务的用户也从开始的小型 and 中型企业逐渐扩展到大型企业，且涵盖了各个行业，包括制造业、零售、医疗健康、教育、媒体和娱乐等，云服务提供商的业务量也大幅增长。根据 Gartner 的最新预测，到 2023 年，全球最终用户在公有云服务上的支出预计将增长 21.7%，达到 5973 亿美元。企业越来越多的业务计划或者已经迁移到云端。
2. **从基础设施迁移到深度用云。**上云不再仅限于简单的基础设施迁移，企业使用的云服务逐渐由单一的基础设施即服务（IaaS）发展到平台即服务（PaaS）和软件即服务（SaaS），越来越多的企业应用逐步深入使用云上中间件、大数据、容器、微服务、人工智能和其它高阶服务。另外，从技术角度看，无论是 IaaS、PaaS 还是 SaaS，云计算技术都已经非常成熟，同时各云服务提供商都提供了专业的迁移工具和支持服务，大幅度降低了上云迁移的难度和风险。
3. **从边缘业务到核心业务上云。**随着数字化转型的推进，核心业务系统的灵活性、可扩展性和创新能力变得越来越重要。越来越多的企业开始意识到将核心业务上云所带来的好处。随着企业对云计算的信任度不断增加，企业上云的趋势正在逐渐从边缘业务扩展到核心业务。这些核心业务可能涵盖企业的关键流程，如客户关系管理、供应链管理、财务和人力资源等领域。云平台提供了大数据分析、人工智能、机器学习等先进技术和工具，使企业能够更好地利用数据和智能化技术来推动业务增长和创新，使企业能够更好地应对市场变化。
4. **云的新技术成为推动企业上云的重要力量。**首先，云原生技术，如容器、微服务、持续集成/持续部署（CI/CD）、基础设施即代码（IaC）等，将使企业更好地利用云环境，提高效率，降低成本。其次，人工智能技术（AI）的发展推动了云计算向更高层次发展，加速了各行各业的数智化进程，助力企业更好地理解 and 利用数据，提高决策效率和准确性。最后，随着 5G 和物联网（IoT）的发展，边缘计算将成为未来云计算的重要趋势，通过将数据存储在更靠近的数据源，边缘计算可以大大提高服务质量，降低延迟。
5. **云相关的法规政策更加明朗化。**随着云计算的普及和发展，各国政府和监管机构对云相关的法规政策逐渐完善和明朗化。这些政策旨在确保数据安全、隐私保护和业务运营的合规性，为企业上云提供清晰的指导。比如，许多国家都制定了数据保护法和隐私法规，以规范云服务提供商在处理个人

数据时的责任和义务，例如欧盟的 GDPR；还有一些国家或行业对存储和处理敏感数据设置了数据本地化要求，要求企业将数据存储在不同的地理区域内，例如，中国实施了《中华人民共和国网络安全法》，对关键信息基础设施的数据本地化提出了要求；还有云安全认证标准，比如 ISO 27001、CSA STAR 等。具体的法规政策因国家和地区而异，因时而异，法规也在不断演变，企业上云时应了解并遵守适用的法规政策，确保合规性和数据安全。

6. **企业上云是渐进式的。**企业上云并不是一蹴而就的，而是一个渐进式的、持续深化的上云过程。企业通常先进行试点上云，然后逐步将更多核心业务、甚至业务创新环节，都迁移到云端，释放出更多的业务价值。

总的来说，企业上云已成为新常态，不断发展的云计算技术将引领企业进入新的商业时代。而企业则需要更深入的理解云计算，学习上云和用云的方法，将业务搬迁上云，更好地利用云的技术，实现业务的快速发展和持续创新。

1.2 企业上云的挑战

企业上云是指将企业的应用、数据甚至大数据平台搬迁到云上的过程。虽然云具有很多优势，但是上云却不是一件容易的事，企业在上云过程中会面临着许多痛点和挑战。

1. 上云适配改造

企业从传统的本地数据中心架构转向云架构，或者从一个厂家的云架构转向另外一个厂家的云架构，这个过程可能会面临一些上云适配改造工作，比如版本不一致导致的版本升级改造，SDK 接口不一致导致的兼容性的适配改造、异构数据库搬迁导致的数据格式的转换等。

2. 人员技能和组织变革

上云需要企业内部人员具备云相关的知识和技能，由于云与传统 IT 存在差异，不同云厂家的云也存在差异，员工需要学习云相关技术，适应云上新的工具和流程。培训和人员准备是一个重要的挑战，企业需要制定相应的培训计划和知识共享机制，鼓励员工接受新的工作方式和新技术。同时，上云也可能涉及到组织和文化的变革，包括 CCoE 跨部门的合作，敏捷开发和 DevOps 文化的引入等。

3. 数据安全和合规

数据安全和合规对企业非常重要。企业上云后，数据会存储在云服务提供商的基础设施中，企业需要评估云服务提供商的数据保护机制，并与合规团队密切合作，制定企业的安全和合规措施。不同行业和地区可能有特定的监管要求和法律法规，企业可能面临数据隐私保护、数据存储地点限制、数据监管审核等方面的挑战，企业需要确保数据上云符合相关的合规要求。

4. 成本控制

虽然云计算提供了弹性和按需付费的优势，但是企业仍然需要管理云资源的使用，并持续优化企业用云成本。云费用控制、资源优化和合理的预算是成本控制的一个挑战，企业需要合理估算云成本、控制资源的使用和选择适合的定价模型。另外，上云过程中的成本管理也是一大挑战，包括数据传输费用、应用重构或改造费用、员工培训费用、上云迁移演练和测试环境费用、外部供应商费用等。举一个例子，如果企业的业务系统是独家采购自第三方供应商，则第三方供应商可能会收取较高的上云服务费用。

5. 数据的一致性

在数据迁移过程中保持数据的完整性和一致性是企业上云的一个重要挑战。迁移现有数据到云平台，可能会面临数据格式转换、兼容性和一致性的问题，企业需要制定合适的迁移方案，选择正确的数据迁移工具和校验工具，并进行充分的测试和验证。

6. 关联分析和批次规划

关联分析和批次规划是企业上云的一大难点，对于大规模全量搬迁上云的企业来说，为了降低迁移风险，通常需要将迁移划分为多个批次进行，而批次规划首先依赖的就是应用的关联分析结果。在上云迁移过程中，企业需要正确的梳理各种关联关系，包括应用与数据层的依赖、应用与中间件的依赖，系统内部应用间的通信依赖，本系统与第三方系统或第三方终端的集成依赖等，这些关联关系通常非常复杂，并且很多企业都缺乏全面和准确的文档记录，这使关联分析变得非常困难。

7. 云服务商选择

企业选择的云服务提供商可能会对企业产生长期影响，一旦企业将核心应用和数据迁移到某云上，后续再想切换云服务商可能会很困难，其切换过程可能和首次上云同等复杂和困难。因此，选择合适的云服务提供商，并建立良好的合作关系是上云的关键。不同云服务提供商之间可能存在差异，如定价、功能、性能和技术支持等。企业需要充分评估不同云厂家之间的区别，并制定合适的合作和管理策略。

8. 业务连续性

上云过程中，企业需要确保业务的连续性和高可用性，并管理潜在的风险，降低业务中断时长和影响。企业需要采取适当的风险管理措施，包括进行业务影响分析并制定应对措施，同时业务上云后的高可用方案、应用的故障恢复机制等也是需要考虑的。

9. 云运维监控

业务上云后的运维和监控是一个挑战。企业需要建立完整的云运维监控体系，确保云资源的性能可实时监控、安全可实时观测、告警可实时通知，日志可实时查看等。云服务提供商通常会提供基础的监控能力，如资源层面的 CPU、内存、IOPS、网络带宽等监控，但企业可能仍然需要借助额外的工具和技术来保障应用层面的告警、监控和日志能力。

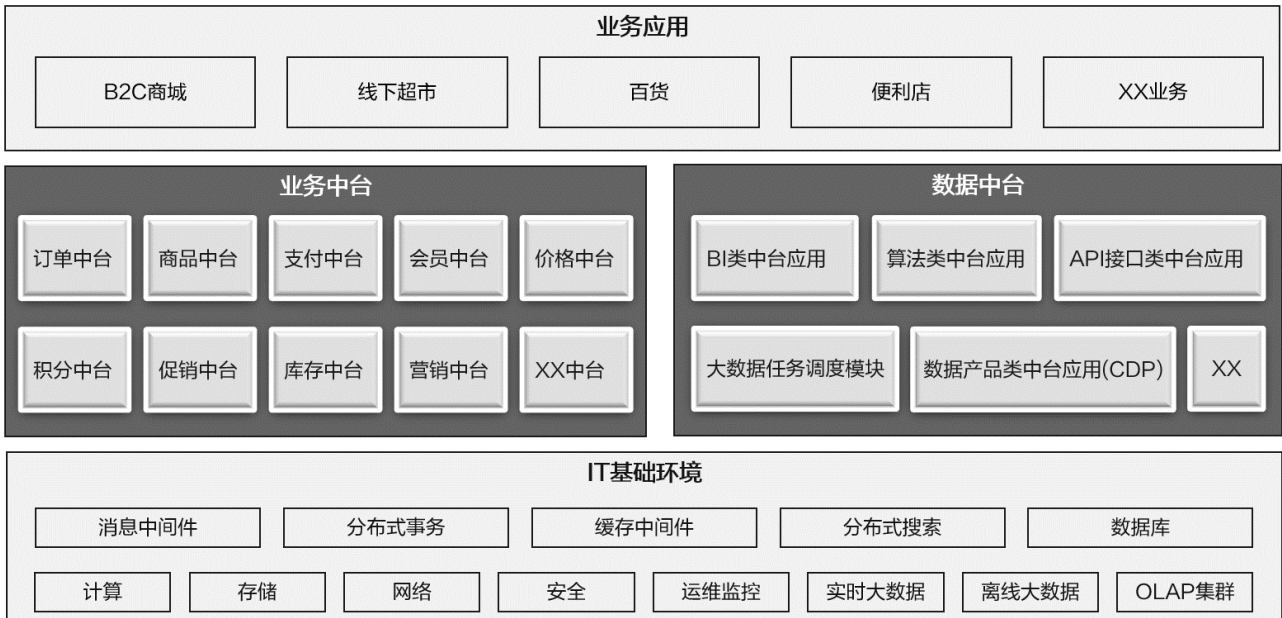
10. 项目管理

上云迁移是一项复杂的工作，从架构设计到应用迁移、从安全性到合规性、从管理到监控，企业需要综合考虑各种影响因素，并建立一个全面的上云规划和执行框架，确保上云迁移顺利进行。在上云过程中，企业需要投入一定的资源，大规模上云通常需要一个专职的项目经理，负责周边部门协调，管理上云规划、架构设计、迁移实施、测试验证、演练切换等一系列上云活动。同时，企业还需要挑选骨干人员进行新技术的学习和储备。所以上云迁移是一个系统性工程，不仅仅是搞定技术迁移方案，也需要系统性的进行项目运作，获得企业领导层的支持和投入，协调周边部门或第三方相关资源配合。

总体来说，企业在上云过程中面临着许多痛点和挑战，涵盖了技术、人员、安全、成本、数据管理、供应商管理、业务连续性等方面。企业需对以上的多个痛点和挑战有足够的认识与准备，才能确保上云项目的顺利进行和成功实施，必要时可以引入专业的上云顾问，并与云服务提供商紧密合作才可以克服这些挑战，并获得上云所带来的各种优势和收益。

1.3 企业典型的 IT 架构

企业的 IT 架构通常包括 4 大模块，即 IT 基础环境、业务中台、数据中台和业务应用。以某大型零售企业为例，其 IT 架构如下：



1. IT 基础环境：IT 基础环境包括基础硬件（如服务器、存储、网络等）和基础软件（如操作系统、虚拟化平台、数据库、中间件等）。它为企业的 IT 系统提供基本的运行环境。
2. 业务中台：业务中台是指企业的核心业务组件和服务平台。它提供了共享的业务功能和服务，为各个业务应用提供支持，促进业务协同和效率提升。业务中台可以包括企业资源规划（ERP）、客户关系管理（CRM）、供应链管理（SCM）等关键业务系统。
3. 数据中台：数据中台是指企业的的核心数据管理和数据服务平台。它集中管理和整合企业各类数据资源，提供数据存储、处理、分析和服务的核心能力。数据中台包括数据采集、数据存储、数据湖、数据治理、数据分析等组件，用于支持企业的核心数据驱动决策和业务需求。
4. 业务应用：业务应用是指企业特定领域的核心应用软件，用于支持和执行特定的业务功能和流程。这些应用可以是内部开发的定制化软件，也可以是第三方提供的行业解决方案。业务应用通常建立在业务中台和数据中台的基础上，以满足具体业务需求。

企业上云需要分别考虑这 4 个模块的上云方案，包括云上部署架构以及迁移方案。

1.4 云迁移框架介绍

企业上云对于中型或大型企业来说绝非易事，上云不仅是一个技术问题，同时也是一场变革，涉及到企业 IT 治理体系的变化、组织架构的适配、技能的转型、文化和思维方式的塑造、持续的运营运维优化等。这些方面对企业上云提出了很大的挑战，企业迫切需要一套方法论进行指导，确保上云之路更加顺畅。为此，我们编写了华为云上云迁移框架白皮书，为企业上云提供总体建议和方法指导。

云迁移框架（Cloud Migration Framework，以下简称 CMF）是站在客户视角的上云迁移方法论，它来源于华为云的经验及百联等大型企业上云的优秀实践，为企业上云提供完整的上云指导。企业上云的整体思路是，先整体规划，然后小范围试点，最后再大规模上云。按照这个思路，我们把企业上云的生命周期分为 8 个阶段，分别是调研分析、评估规划、上云准备、云上架构设计、上云迁移试点、整体批次规划、大规模上云迁移、云上运维与治理，其中调研分析贯穿整个上云周期，整体框架如下：



其中有 5 个阶段是全局任务，即项目级的任务，包括评估规划、上云准备、云上架构设计、整体批次规划、云上运维与治理。有 2 个阶段是应用级的任务，即每个应用迁移都要执行一个小循环。小循环内按调研、设计、部署、迁移、验证、切换、保障 7 个步骤有序运转，上图中的上云迁移试点和大规模上云迁移都是循环执行小循环迁移流程。

（一）企业上云的过程包含如下 8 个阶段：

1. 调研分析

调研工作持续整个上云周期，整体调研思路是由粗到细持续迭代，比如评估规划阶段只需要调研到全景（打开到业务域），在迁移实施阶段要打开到每个业务系统和应用系统模块，并调研详细的信息。

2. 评估规划

评估规划，首先要识别企业上云的动机，上云后想要实现的业务收益，然后结合企业的云成熟度现状，制定合适的上云策略，并规划整体上云的蓝图。

3. 上云准备

上云准备是企业正式上云之前要做的相关准备工作。首先是组织准备，企业首先要构建自己的云转型团队 CCoE，负责整个上云工作和云的能力建设。其次，组织一个正式的动员会，上云是一把手工程，需要中高层参与，召集云厂商和各集成商做到三个对齐“组织对齐”、“目标对齐”“责任对齐”。

4. 云上架构设计

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。

- 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。应用部署架构要从应用的四层技术架构来设计，即接入层、应用层、中间件层和数据层。需要设计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、安全性、成本和可运维性。其中，安全性、成本和可运维性这 3 个要素可以参考基础环境的设计，应用部署架构设计时可重点关注可用性、性能和可扩展性这 3 个要素。
- 3) 大数据架构设计：大数据架构设计的范围包括大数据集群、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可以参考应用部署架构的设计方法。要根据具体业务需求和技术要求，选择合适的大数据云服务或自建大数据组件。大数据部署架构的设计同样要考虑架构设计的 6 要素。

5. 上云迁移试点

在正式上云之前先要进行小范围试点，为大规模上云奠定基础，上云试点主要是做好团队磨合、方案磨合、技能磨合，并验证企业上云的价值，通过试点增强各业务部门上云的信心。试点一般选 1~3 个合适的应用上云，执行上云迁移的小循环（调研、设计、部署、迁移、验证、切换、保障）。

6. 整体批次规划

整体批次规划是指将企业的应用程序和数据分阶段地迁移到云平台的计划和安排。批次规划将复杂的迁移过程分解为更小的可管理的步骤，使企业能够更好地管理和控制上云过程，降低了上云的风险。批次规划既是科学又是艺术，企业可以先基于关联关系进行分组，然后参考优先级和分批的原则，并结合上云试点的结果，输出可执行的整体批次规划。

7. 大规模上云迁移

大规模上云迁移是按照整体批次规划，滚动执行上云迁移小循环的过程，每个小循环都包括 7 个阶段：调研、设计、部署、迁移、验证、切换、保障。

大规模上云有 3 种方式：

- 1) 应用迁移上云：是指将应用的运行环境迁移到云上，迁移的对象包括接入层、应用层、中间件层和数据层，采用的上云策略是 Re-host 或 Re-platform，主要是平迁，包含少量上云适配改造，遵循应用迁移小循环流程。
- 2) 大数据迁移上云：是指将大数据的运行环境迁移到云上，包括数据迁移和任务迁移，采用的上云策略是 Re-platform，包含大数据任务的适配改造，遵循大数据迁移流程。
- 3) 应用现代化上云：是指将传统应用进行云原生改造上云，采用的上云策略 Re-architect，包括数据库改造、容器化改造、微服务改造等，遵循云原生的框架和方法。应用现代化改造通常需要较长的周期，企业可以结合上云的里程碑、改造工作量和开发人力综合决定是先改造再上云，还是先平迁上云再现代化改造。对于新型业务，企业也可以直接使用公有云的新技术（AI、区块链、元宇宙等）快速开展业务创新，使能应用现代化。

8. 云上运维与治理

聚焦上云后的治理和持续运维，包括成本管理、安全基线、可观测性运维、运维治理的自动化。

(二) 学习和复盘

在整个上云迁移过程中要不断学习和复盘，尤其是大规模迁移，通过持续学习和复盘，企业可以不断改进上云方案，推动上云迁移项目成功，提高云化转型的质量和效果。

1. 学习内容包括云计算基础，云产品知识，云服务的日常使用，架构设计方法，迁移方案和切换方案的最佳实践等。
2. 复盘包括上云试点复盘、切换演练复盘、每一批应用迁移结束后的复盘、项目管理复盘等。

(三) 上云项目管理

对于大规模的上云迁移，需要指定专职的项目经理。项目经理在企业大规模上云迁移中扮演着关键的角色，有效的规划、协调、管理和控制迁移过程是项目顺利、高效地完成的保证。项目经理的专业经验和技能对于成功推动大规模上云迁移与实现预期的上云转型目标至关重要。

(四) 企业上云的三转

当企业决定进行云化转型时，除了技术层面的考虑外，还需要关注以下三个方面的转变，即转意识、转组织和转能力，整个上云迁移的过程都在落地和践行“三转”。

1. **转意识 (Transition of Mindset)**：企业需要理解并接受云计算的概念、优势和价值，并意识到云化转型对整个组织和业务的深远影响。这包括培养对云计算的认知和理解，打破传统的 IT 思维方式，鼓励创新思维和敏捷方法，并推动全员参与和支持云化转型的意识。
2. **转组织 (Transition of Organization)**：企业需要重新评估和调整组织结构，以适应云化转型的需求。这可能包括建立专门的云团队或中心，负责云化项目的规划、实施和管理。同时，需要修改相关流程和职责，定义清晰的角色和职责，以确保云化转型的有效推进和持续运营。
3. **转能力 (Transition of Capability)**：企业需要培养和发展与云计算相关的技术能力，包括云架构设计、云平台管理、自动化运维、安全与合规等方面的知识和技能。同时，企业还需要进行员工培训和知识共享，以提高整体团队的云计算能力和素质。

通过“三转”的综合推进，企业可以更好地适应和应对云化转型带来的挑战和机遇。转意识帮助企业建立正确的云计算思维方式，转组织确保组织结构和流程适应云化转型，转能力提升企业人员的技术和能力水平，从而成功的实现企业上云转型。

2 上云调研分析

上云的调研工作不是一把完成的，而是持续整个上云过程。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。

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：

1. **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
2. **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。
3. **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。

2.1 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。

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。
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



易
↓
难

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，如下图：

	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
1	现网CMDB	√ 需整理	√ 需整理	√	√	√	√ 需整理	√ 需整理	√ 需整理	√	√	高	高	中高或高
2	现网云管平台									√		高	低	高
3	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
4	RDA工具收集									√		中	低	高
5	调研&访谈	√	√	√	√	√	√	√	√	√	√	低	高	中高

2.2 调研内容

2.2.1 基础环境调研

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。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。

2.2.2 应用迁移调研

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开发团队架构师和运维人员。

2.2.2.1 调研应用全景图

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：



应用全景的调研方法由易到难分别是：

1. 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。

2. 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。
3. 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。

2.2.2.2 调研应用部署架构

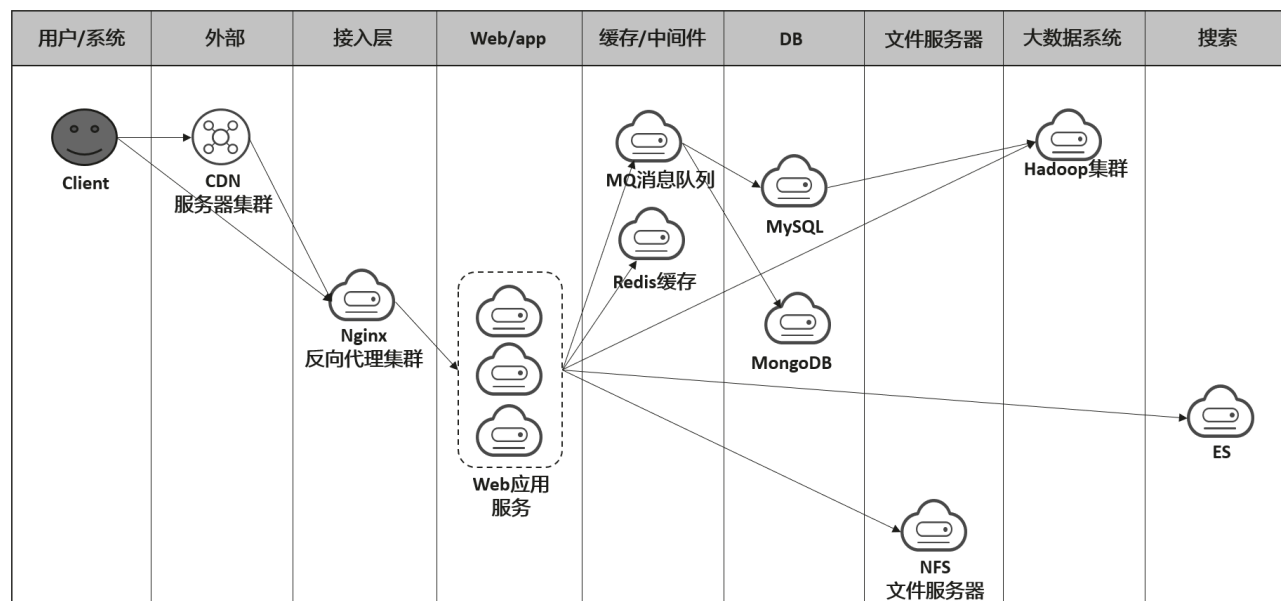
应用部署架构的调研是在试点迁移或大规模迁移阶段进行的, 应用部署架构是基于单个应用进行调研的, 主要调研应用的四层部署架构, 即接入层、应用层、中间件层和数据层, 同时还要调研每一层技术组件的详细信息, 比如规格、版本、容量等。具体的调研内容如下:

(一) 调研应用的四层部署架构

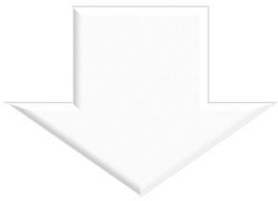
收集接入层、应用层、中间件层和数据层的详细信息, 收集三种关联关系 (共享数据、共享服务器、应用间通信依赖), 可以参考下表收集应用的详细部署架构:

				接入层ELB			应用层		中间件层			数据层			接入层域名				
接口组	应用名称	应用别名	应用别名	NAT	SLB	NGINX	主机数量	IP地址	Redis	Kafka	MQ	Oracle	MySQL	Mongo	内部域名	外部域名	CDN	WAF	备注

也可参考下图绘制应用的部署架构图:



调研方式:



首先，推荐CMDB法，找运维团队申请只读账号，从CMDB系统中梳理应用的技术架构信息。

其次，如CMDB行不通，则采用调研访谈法，通过与该应用模块的负责人访谈，梳理应用的技术架构。



(二) 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项技术组件的详细信息（包括资源规格、版本、容量、配置…）

主机详情信息

信息项	平台信息	企业项目 (IDC不必须)	应用名称	环境	区域 (IDC填写: 机房位置; 友商云填写: 机房位置)	实例名称	主机名称 (ECS/物理机)	规格 (IDC不填写)	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)	私有IP
举例	阿里云ECS	XX	XX	生产	北京	online-other-game-02	ecs	ecs.c4.large	2	8	centos 7.4.64	SSD云盘	200	通用SSD	500	10.20.30.179
1																
2																
3																
4																
5																
6																
7																
8																

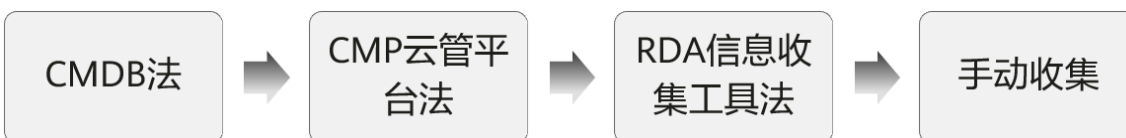
数据库详情信息

信息项	企业项目 (IDC机房不必须)	应用名称	环境	区域 (IDC填写: 机房位置; 友商云填写: 机房位置)	实例名称	架构类型	IP地址	端口	是否有只读实例	只读实例名称	版本	实例规格	CPU	内存	存储类型	磁盘容量	CPU利用率 (可选)	内存利用率 (可选)	磁盘利用率 (可选)	备注
举例	XX	XX缓存	生产	北京	fenxi-udb02	主备	10.11.12.1	3306	是	读可用	MySQL 5.7	mysql.r2.medium.2	8	32	SSD云盘	500GB	1.5% 70% 均值	0.66	0.79	
1																				

中间件详情信息

信息项	企业项目 (IDC机房不必须)	应用名称	环境	区域 (IDC填写: 机房位置; 友商云填写: 机房位置)	名称	版本	连接地址	源规格 (IDC机房自建与虚拟机规格)	是否需要超高IO	Topic数量	Partition数量
举例	XX	XX缓存	生产	北京	ashupu-mq	2X	10.10.176.98	alibaba.hw.2xlarge	是	50	30
1											
2											

调研方式：

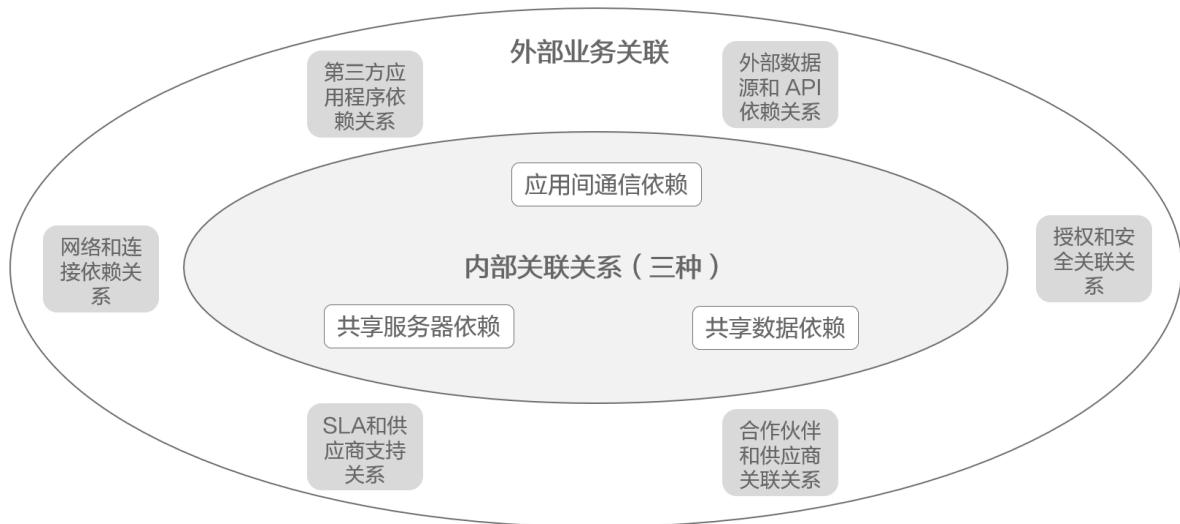


1. 首选 CMDB 法；
2. 如果 CMDB 无法获取，次选 CMP 云管平台法，从现网云管平台或虚拟化管理软件获取；
3. 如果 CMDB 和 CMP 都行不通，可以安装信息收集工具（比如华为云 RDA）进行采集；

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。

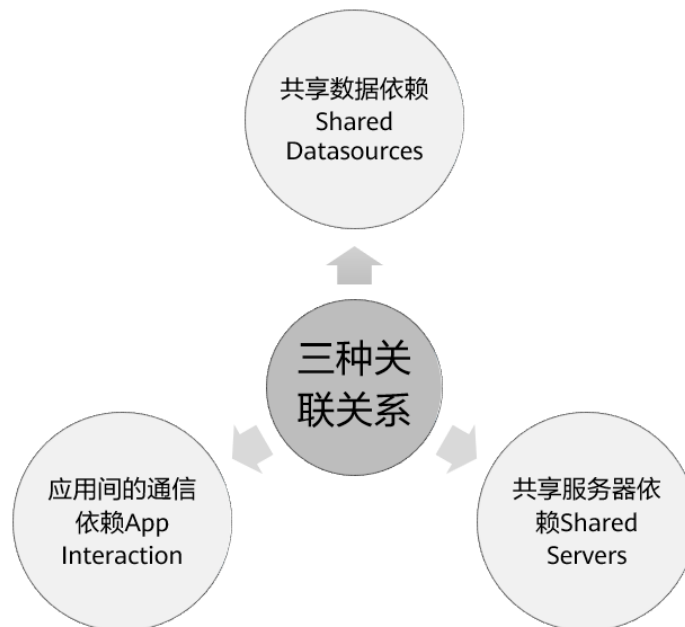
2.2.2.3 调研应用关联关系

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。

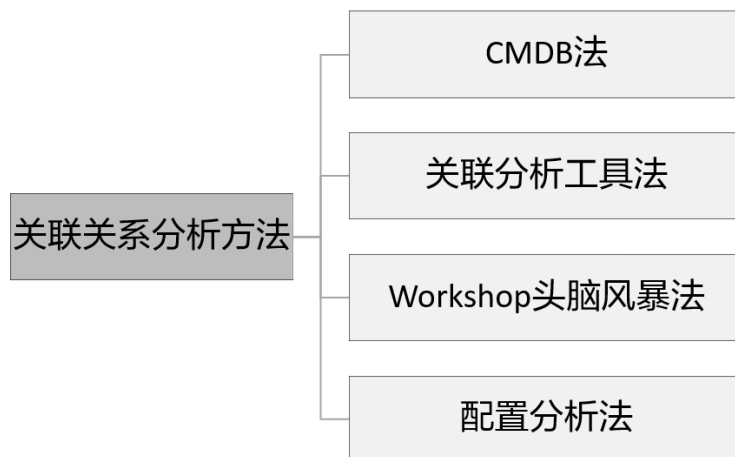


(一) 调研内部关联关系

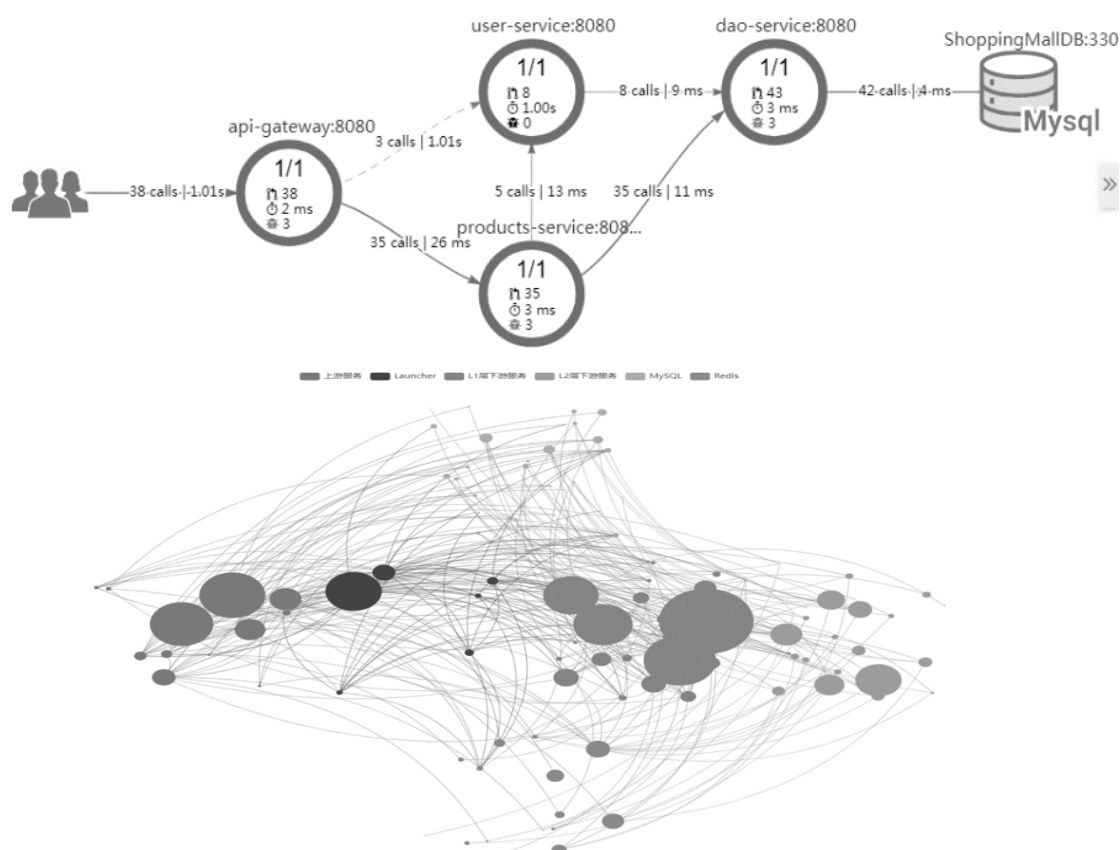
关联关系分析是批次规划和切换方案的重要输入，也是上云迁移的难点，影响上云迁移的关联关系主要有三种，如下图：



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：



1. 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，如下图所示。



2. 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，如下表：

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。

3. 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。



4. 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：

- 1) **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。
- 2) **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。
- 3) **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。
- 4) **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。
- 5) **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。

(二) 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。

1. 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。

2. 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。

3. 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。

4. 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。

5. 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。

6. 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：

1. 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。

2. 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。

3. 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。

4. 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。

5. 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。

6. 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。

2.2.2.4 调研应用上云需求

调研内容：当前应用上云的需求和约束条件，比如迁移时间窗、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：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。

2.2.3 大数据迁移调研

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。

大数据应用（BI类、算法类、API类）

大数据任务调度平台（Azkaban、Hera等）

大数据集群（在线、离线、OLAP）

大数据迁移需要调研 4 部分信息：

1. 大数据平台调研，包括大数据集群、任务调度平台、数据流向。
2. 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。
3. 任务调研，包括待迁移的任务类型、任务数量、更新周期等。
4. 大数据应用调研，请参考 2.2.2，本节不再赘述。

本节重点介绍大数据平台、数据和任务的调研。

2.2.3.1 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。

1. 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。

- 1) 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。

- 2) 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。
- 3) 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。
- 4) 调研数据格式类型和压缩算法：
- 5) 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。
- 6) 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。

2. 调研大数据任务调度平台：

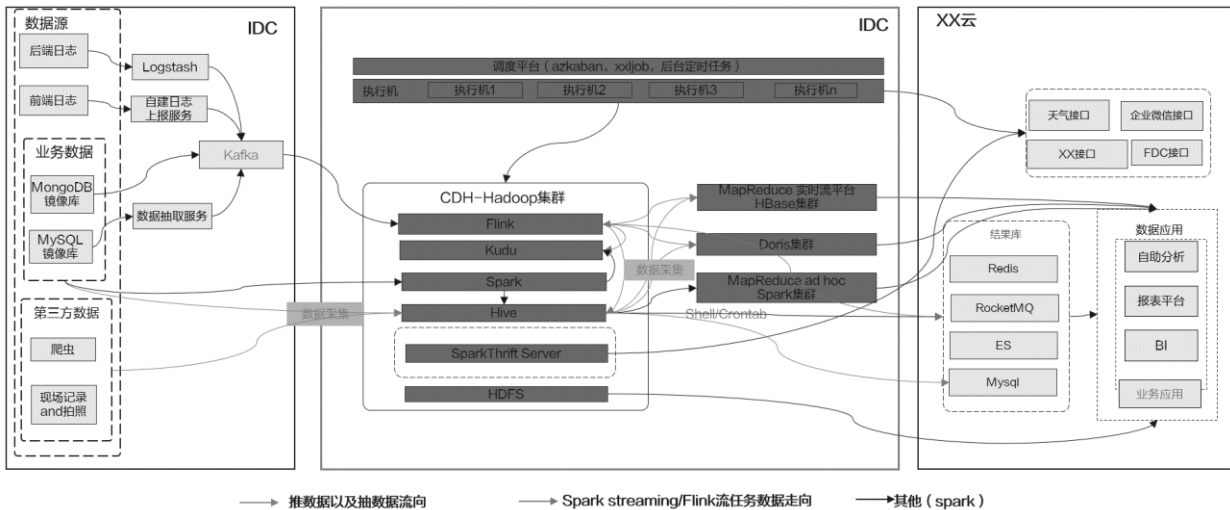
需要调研大数据任务调度平台的类型、版本、支持的大数据框架和技术，调度任务类型，可视化和
管理界面，扩展性和集成性，容错和故障恢复，安全性和权限控制以及社区支持和文档资料等方面的
信息。用于后续大数据调度平台的选型和方案设计。

- 1) 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。
- 2) 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。
- 3) 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。
- 4) 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。
- 5) 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。
- 6) 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。

3. 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：

- 1) 大数据平台及业务的架构图和数据流图。
- 2) 平台数据接入源。
- 3) 数据流入方式（如：实时数据上报、批量数据抽取）。
- 4) 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。



2.2.3.2 数据调研

数据调研主要包括如下方面：

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。

2.2.3.3 任务调研

任务调研主要包括如下方面：

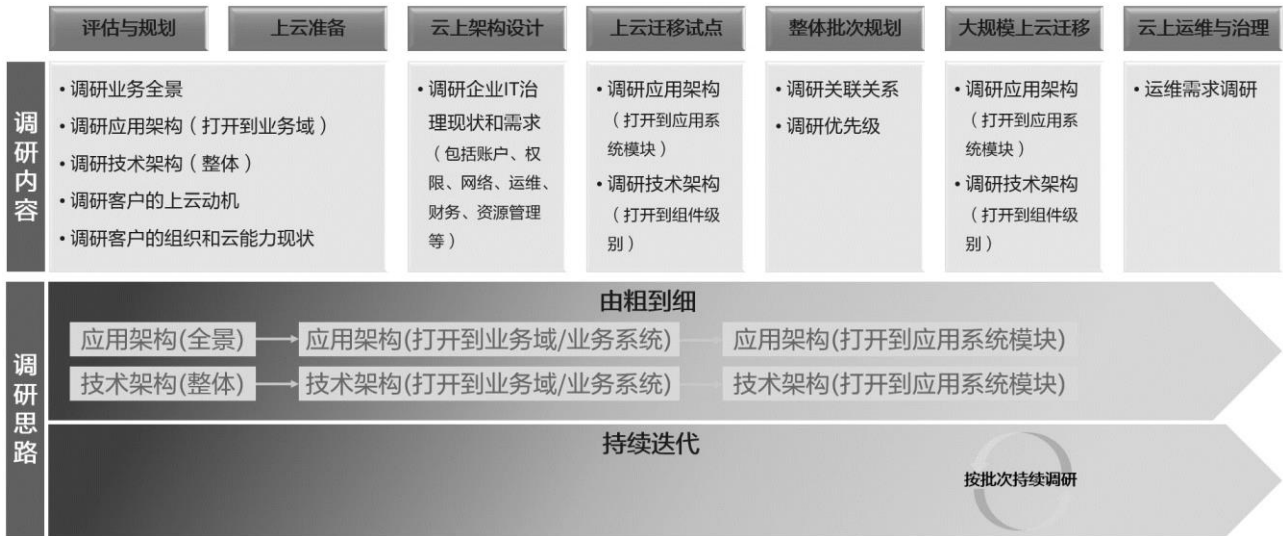
调研内容	描述
任务调度	如 Azkaban、DolphinScheduler, Hera、Crontab 等。
任务类型	基于编程语言分类： <ul style="list-style-type: none"> ● JAR 类：常用于 MRS、Flink、Spark 等 ● SQL 类：常用于 Hive、Spark、UDF 等 ● Python 类：常用于 Spark、算法场景等 ● 其他类：如 Shell、Scala 等，多用于脚本调用
任务数量	调研各类任务的总数量，用于评估任务迁移周期及改造工作量。如：XX 调度平台下，JAR 任务 XX 个。
任务更新周期	识别出不同调度平台，不同任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。
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。

2.3 调研过程

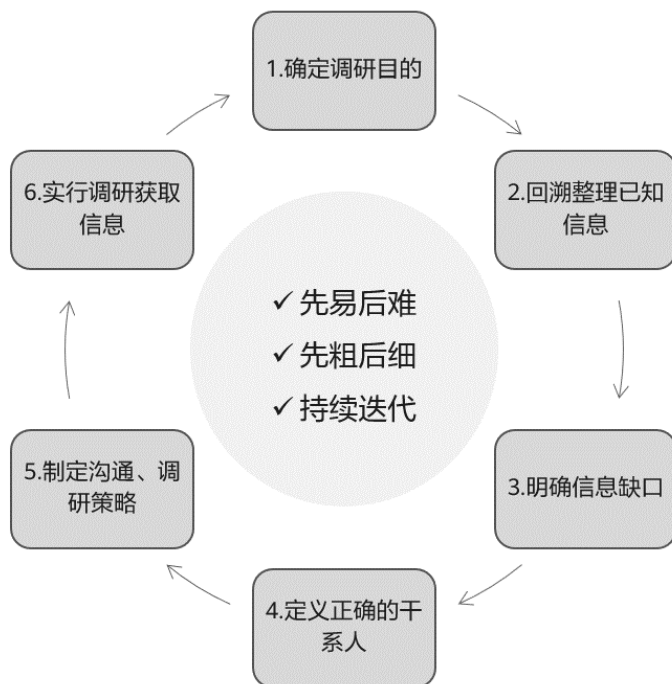
上云调研不是一次完成的，而是持续整个上云过程，需要进行多次调研，持续迭代，每个阶段调研的信息都不同。但注意，同一阶段，能合并调研的要尽量合并调研，减少调研次数，尤其是访谈次数。

1. 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。
2. 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。
3. 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。



每次的调研工作可以通过如下 6 步法进行：

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。



3 上云评估规划

识别企业上云的主要动机，评估企业的用云现状和上云可行性，制定上云策略和高阶方案，用于指导企业的后续上云实施工作。

3.1 企业上云的驱动力评估

在企业上云之前，首先要明确企业上云的动机，基于企业上云的初心来规划整体上云策略和蓝图，制定企业上云的业务目标，重点关注上云为业务创新带来的价值，从而在公司层面确定企业上云的总体战略、蓝图规划、上云节奏。

3.1.1 常见的上云驱动力

三年疫情导致全球经济形式变差，很多企业开始重视固定资产的投资和管理，减少当期固定资产投资，更多的机会转向公有云服务。

驱动企业上云的动机一般有：关键事件驱动、优化驱动、创新驱动。

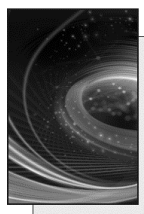
1. **关键事件驱动**：关键事件驱动指的是特定事件或情况促使企业采取上云行动。



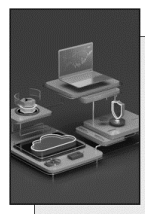
关闭IDC：运营和维护IDC需要大量的投资和人力资源，当企业面临成本压力时，可能会选择关闭企业自己的数据中心（IDC），上云可以减少当期固定资产投资。



业务扩张：当企业面临业务扩张，需要快速扩展其计算和存储资源时，上云可以提供弹性和灵活性，以满足业务扩张需求。



合规要求：某些法规和合规要求可能要求企业处理和存储敏感数据的方式发生变化。上云可以提供更高的数据安全性和合规性，帮助企业符合相关的监管要求。



应急和灾备：面对自然灾害、硬件故障或其他紧急情况时，上云可以提供强大的备份和恢复能力，帮助企业迅速恢复业务，减少中断时间和数据损失。

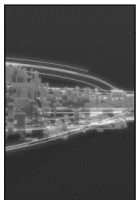
2. **优化驱动**：优化驱动的目标是通过上云来提高效率、优化架构、降低成本。



优化资源成本：上云后，企业可以根据实际需求动态分配和调整资源，避免资源的浪费，提高资源利用率，从而降低成本。



提升资源利用率：通过上云，企业可以更好地利用其计算和存储资源，降低资源的闲置率，提高整体资源利用率。

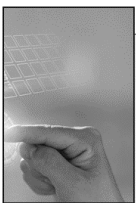


提升业务可用性：云平台提供高可用性和容灾功能，企业可以通过优化架构保障业务的连续性，减少服务中断的风险。

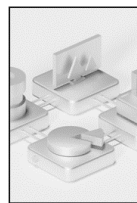


简化运维管理：上云可以将基础设施运维交给云服务商，减轻了企业的管理负担，使其专注于核心业务。

3. 创新驱动：创新驱动的目标是借助云计算技术推动业务的创新和发展。



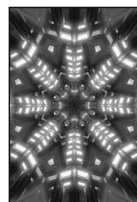
加快TTM (Time to Market)：即缩短产品或服务从开发到上市的时间，云计算提供了快速构建和部署应用程序的能力，企业可以更迅速地将新产品或服务推向市场。



数据驱动决策：上云可以提供强大的数据分析和挖掘能力，帮助企业从海量数据中获取有价值的洞察，支持数据驱动的决策和创新。



业务灵活部署：上云使企业能够快速调整资源，灵活部署新服务和功能，推动业务的快速创新和扩展。



新技术推动创新：云平台不断推出新的服务和功能，可以促使企业从技术创新的角度重新设计和开发应用程序，实现更高的效率和业务效果。

关键事件驱动、优化驱动和创新驱动有时是相互重叠的，一个因素可能同时属于多个驱动力。企业在决策上云时，应综合考虑多个驱动因素，并根据自身需求和目标做出权衡和决策。

3.1.2 识别企业上云动机

要识别企业上云的动机，首先应该了解企业的业务情况，了解其业务的特点，以及其当前的 IT 环境。然后，根据企业的业务情况和 IT 环境，分析企业上云的动机。企业的上云动机会决定后续的上云策略，识别企业的上云驱动力，可以参考以下方法：

- 分析业务需求：**了解企业的当前业务需求和未来发展计划。是否有关键事件（例如扩张、合规要求、灾备需求等）需要满足？是否需要优化资源利用率或降低成本？是否有意愿推进创新和数字化转型？这些需求将提供线索来确定企业的上云驱动力。
- 考察现有 IT 基础设施：**评估企业所持有的 IT 基础设施（例如服务器、数据中心、网络等）的状况和成本效益。如果企业正在面临硬件老化、高成本维护或扩容困难等问题，它们可能成为优化驱动和关键事件驱动上云的因素。

3. **研究市场趋势：**了解业界对于云计算的发展态势和趋势，包括其他类似企业是否已经或正在上云，相关行业采用云计算的程度等。这可以提供洞察力，判断是否需要跟随市场潮流上云。
4. **与企业决策者沟通：**与企业的决策者、IT 团队或其他相关部门进行对话，了解他们对于上云的看法和目标。询问他们对于关键事件驱动、优化驱动和创新驱动的认知，并尝试理解他们对云计算的期望和期限。
5. **考虑组织文化和领导力：**企业的组织文化和领导力对于上云决策至关重要。如果企业强调创新和敏捷性，有强大的数字化转型战略或实践，那么创新驱动可能更为重要。如果企业注重成本控制、效率和稳定性，那么优化驱动可能更为突出。

综合考虑以上因素，可以帮助识别企业的上云驱动力。重要的是要了解企业的特定情况和目标，并根据其独特的需求和优先事项来评估驱动力，以便制定适合的上云策略和计划。

3.2 云成熟度评估

很多企业在全量上云之前，可能已经做过一些上云尝试，部分业务可能已经部署在私有云或公有云上，企业可能已经具备一定的云计算能力。云成熟度评估是对企业当前用云的程度和能力进行评估，帮助企业了解其用云水平，识别潜在的改进点，后续可以针对性的制定云转型策略和上云规划。

3.2.1 评估方法

云成熟度评估可以参考如下方法进行：

1. **确定评估的范围和目标：**首先需要明确评估的目标和评估的范围。例如，可以选择评估整个企业的云能力，或者仅评估某个部门或某个业务线的云能力。
2. **确定评估维度和指标：**云成熟度模型通常包括多个维度和指标，例如云战略、云技术、云安全、云治理等，企业需要根据实际情况选择适合的指标。
3. **收集数据：**收集与评估指标相关的数据，可以通过问卷调查、访谈、会议、查阅文献资料等方式进行收集。
4. **评估结果：**对收集到的数据进行分析，了解企业在各个评估指标上的得分情况，找出企业在云方面的短板和改进方向，评估结果可以用图表等形式呈现，以便于理解和分析。
5. **改进建议：**根据评估结果，提出改进建议，这些建议可以包括技术、组织、流程等方面的改进措施，以及这些改进措施的优先级。

通过云成熟度评估，可以全面了解企业在云计算方面的现状和发展需求，有针对性地提出改进措施，从而更好地利用云计算技术带来的优势，推动企业的数字化转型和创新发展。

3.2.2 评估维度说明

云成熟度模型包括多个维度和指标，通常从如下几个维度进行评估：

1. **云战略评估：**评估企业在云战略方面的成熟度，包括是否制定了云战略、蓝图和目标，并且将其纳入到企业整体战略中。

2. **云技术能力评估**: 评估企业在云技术架构方面的成熟度, 包括基础设施即服务 (IaaS)、平台即服务 (PaaS)、软件即服务 (SaaS) 等不同层次的技术能力。
3. **云业务应用评估**: 评估企业在云原生应用方面的成熟度, 包括业务的云原生化程度, 以及企业在云原生应用开发、容器化、微服务、DevOps 和 CI/CD 等领域的实践能力。
4. **云安全能力评估**: 评估企业在云原生安全方面的成熟度, 包括网络安全、数据安全、应用安全等方面的实践情况, 以及企业在安全合规、风险管理和安全文化等方面的表现。
5. **组织管理能力评估**: 评估企业在组织管理方面的成熟度, 包括云原生团队建设、云流程规范等方面的实践情况, 以及企业在云原生文化、领导力和创新力等方面的表现。
6. **云运维治理能力**: 评估企业在云运维和治理方面的成熟度, 包括: 资源管理、成本管理、应用部署、自动化测试、监控、故障排除等。

下表是评估维度和指标的一个样例, 企业可以根据实际情况进行调整, 以更符合企业的现状和需求。可以基于指标进行逐项评估, 起步是 1 分, 行业领先是 5 分。

- 1 分 - (起步)Initiating
- 2 分 - (局部突破)Emerging
- 3 分 - (全面开展)Performing
- 4 分 - (成为竞争优势)Advancing
- 5 分 - (行业领先)Leading

分类	指标	得分	总分
云战略	云战略		
	云蓝图		
	云目标		
	...		
云技术	IAAS 使用能力		
	PAAS 使用能力		
	SAAS 使用能力		
	...		
云业务	云原生程度		
	容器应用能力		
	微服务应用能力		
	DevOps 能力		
	...		
云安全	数据安全能力		
	网络安全能力		
	应用安全能力		
	安全管理能力		
	...		
组织管理	云化组织		
	云化流程		

	...		
云运维治理	资源管理		
	成本管理		
	监报告警		
	自动化		
	...		

这些方面的评估可以帮助企业了解云能力的现状和短板，帮助企业制定相应的云转型战略，进一步提高企业的云能力水平。

3.3 上云可行性评估

企业上云的可行性评估，可从以下几个维度进行：

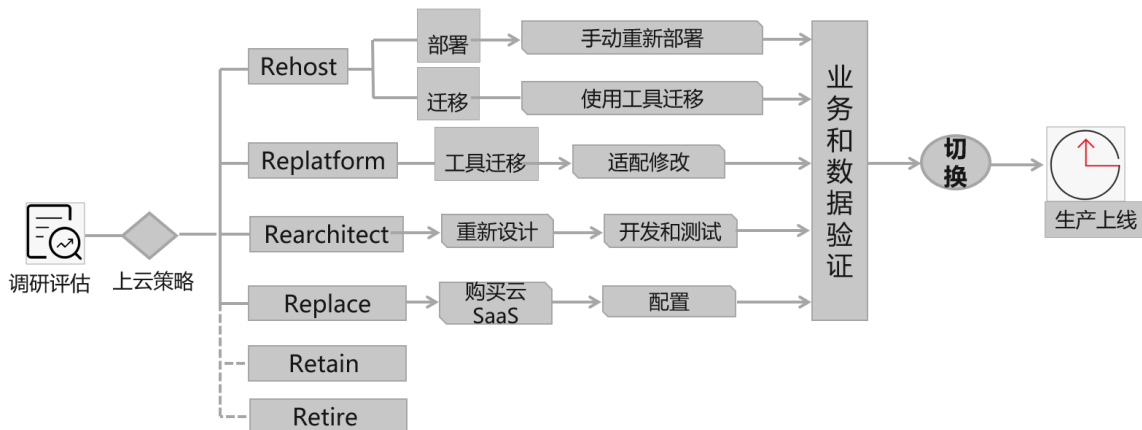
1. **业务成本：**在企业上云之前，需要评估企业从 IDC 迁移到云的转换成本。评估成本时，需要考虑企业的业务规模、经营业务、技术水平、客户需求等情况，以及各云服务提供商的价格，并结合企业的业务情况，选择合适的上云方案，计算出上云的成本。如下是常见的上云成本考虑因素：



2. **业务收益：**在企业上云之前，需要评估企业上云后跟之前相比，将获得哪些业务收益，包括成本、效率、可用性、安全性、可运维性、敏捷性等。
3. **信息安全：**企业上云之前，需要评估上云后的数据安全能否满足相关安全合规政策和标准。
4. **技术评估：**企业上云之前，需要评估云服务能否满足当前的技术要求，比如兼容性（小型机、第三方数据库、硬件加密机）、性能等。如果涉及到业务适配改造，需要评估改造成本与投入。

3.4 上云策略规划

上云迁移 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：



企业的上云动机是迁移 6R 策略选择的第一驱动力，在规划 6R 策略前，首先要清晰定义企业的业务上云驱动，常见的企业上云动机和推荐的上云策略如下：

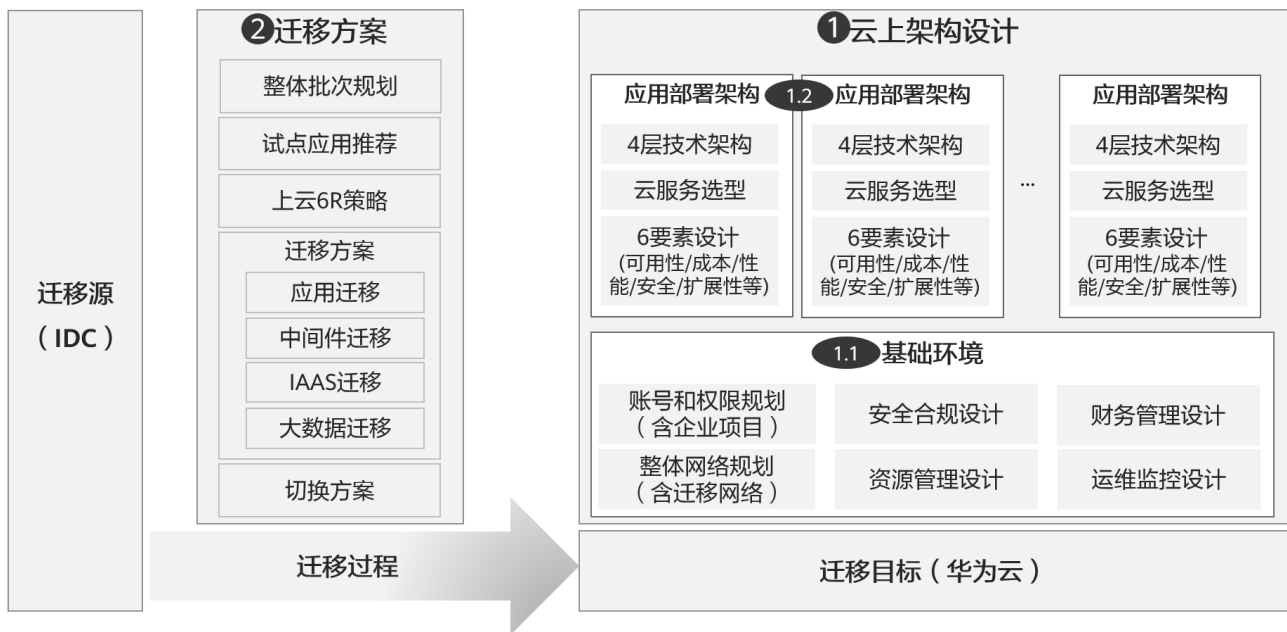
上云驱动 举例	上云收益	6R策略建议	性价比说明				
			迁移风险	业务收益	迁移周期	迁移成本	迁移难度
加快TTM (创新驱动)	版本的迭代频率更快，新功能的发布速度更快，从月缩短到周或天	通过ReArchitect重构应用程序为微服务架构，提高新功能上市的速度	高	高	长	高	大
降低成本 (优化驱动)	基础设施成本降低，运维成本降低，云上实现同城高可用成本大幅降低	1.Rehost适当优化规格 2.Retire利用率低或闲置的服务器	低	低	短	低	小
提升可用性 (优化驱动)	系统可用性提升，SLA提升，意外宕机事件和宕机时间减少	RePlatform迁移到云端PAAS服务，关键应用实施高可用性	中	中	中	中	中

另外上云策略是否可行，还受到很多其它因素的制约，比如技术满足度、开发预算、上云周期等，需企业综合评估后进行合理规划。

3.5 高阶方案规划

3.5.1 方案范围

如果把上云迁移比作搬家的话，上云就是把业务系统从迁移源端（比如 IDC）搬到目标端（比如华为云），因此业务上云方案包括两部分，即云上架构设计和迁移方案设计，其中云上架构设计又包括基础环境设计和应用部署架构设计，如下图：



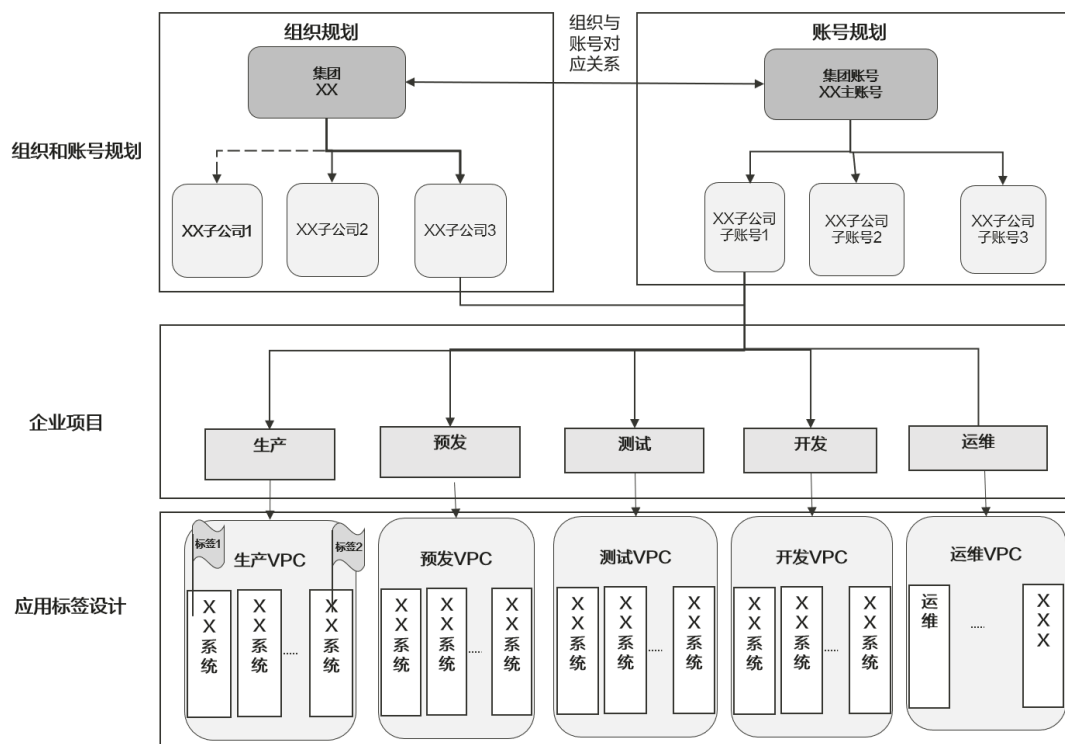
1. **云上架构设计**: 包括基础环境设计和应用部署架构设计，其中基础环境是整个云上目标架构的底座。企业上云时，先要做好基础环境设计，然后才是设计每个业务在云上的应用部署架构。
2. **迁移方案设计**: 包括上云策略、批次规划、试点应用推荐、迁移方案和切换方案。

3.5.2 高阶方案示例

3.5.2.1 基础环境规划示例

(一) 账号与权限规划示例

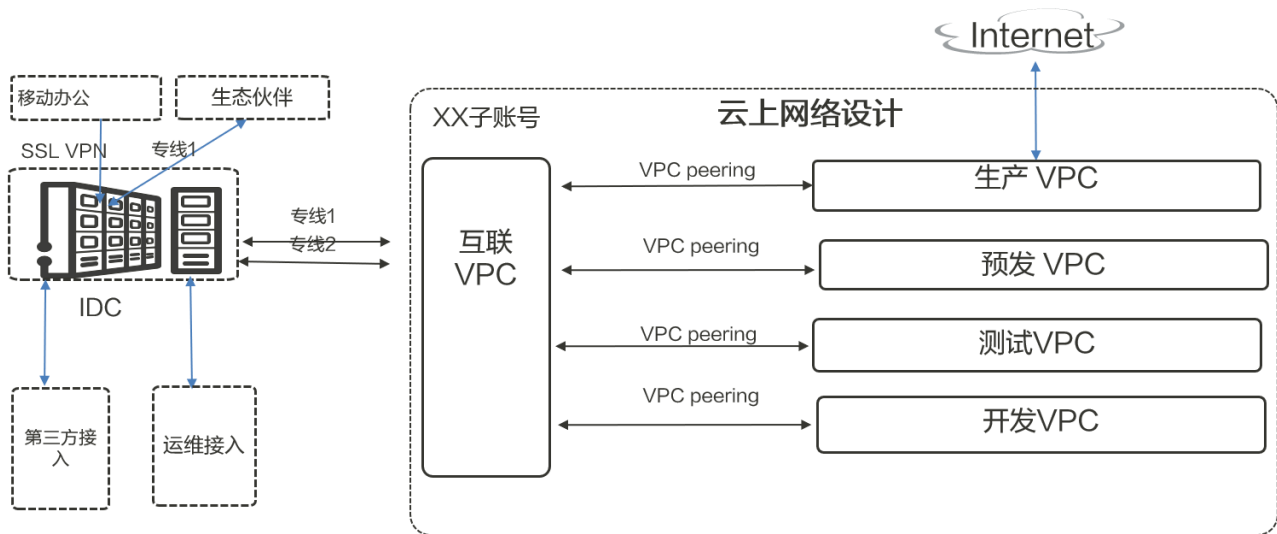
1. **集团对应主账号**，可以创建和管理企业的组织结构、子账号，统一对子账号进行财务管理，并为子账号设置组织策略限定其权限范围，一个组织单元可以包含多个子账号。
2. **子账号**，可以作为账单实体，按照业务单元、产品、运行环境、成本中心等规划账号。
3. **企业项目**，对资源进行逻辑分组和标签，基于分组进行成本分摊、限定授权范围和资源筛选，一个账号可以包含多个企业项目。



按照最小授权原则，对各账号进行权限设置：

账号	分类	用户组名称	用户组履行的IT职责	用户组归属团队	管理的资源或云服务	用户组内IAM账号
XX子账号	系统	系统运维admin组	除IAM外，拥有云上所有资源的所有权限，包括费用中心、资源中心、帐号中心的权限，可以购买资源，管理续费，查看账单等。	运维leader团队	ALL	员工1, 员工2
	网络	网络admin组	云上网络管理员，拥有云上VPC、EIP、专线、VPN等云上网络资源所有权限。	网络运维团队	NAT、EIP、VPC、专线、云连接、VPN	员工3
		网络普通组	云上网络资源只读权限	网络运维团队		员工4, 员工5
	应用	应用admin组	云上应用管理员，拥有ECS、云盘、中间件的所有权限。	应用运维团队	ECS、EVS、CCE、OBS、kafka、日志等	员工6, 员工7
		应用普通组	云上应用资源只读权限	应用运维团队		员工8, 员工9
	数据库	数据库admin组	云上数据库管理员，拥有云上IAAS和数据库（如RDS、DDS等）的所有权限	数据库运维团队	RDS、DDS、DCS等数据库	员工10
		数据库普通组	云上数据资源只读权限	数据库运维团队		员工11
	安全	安全admin组	云上数据安全管理员，拥有云上安全产品，如Anti-DDoS、DDoS高防、WAF、云防火墙、加密服务等安全产品的所有权限	安全管理团队	WAF, Anti-DDoS, CFW	员工12
安全普通组		云上安全产品只读权限	安全管理团队		员工13	

(二) 整体网络规划示例



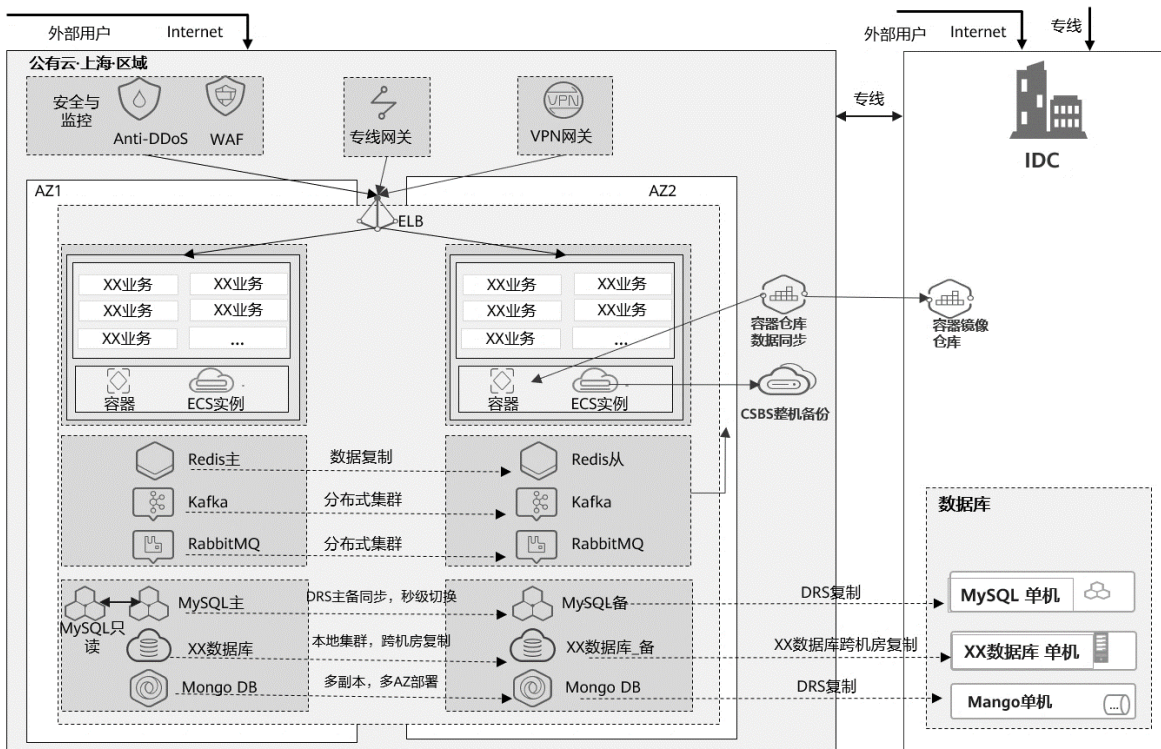
VPC 划分原则

1. 根据环境进行 VPC 规划，不同环境的规划不同的 VPC。
2. 规划一个运维 VPC，承担与线下 IDC 或办公区网络的互联中转作用，可减少专线数量。
3. 强隔离业务可单独规划一个 VPC。

VPC 规划

1. 网络互联 VPC：云上和线下互联，IDC 通过专线接入网络互联 VPC，网络互联 VPC 再通过 VPC Peering 实现和其它业务 VPC 的互联。
2. 生产 VPC：部署各业务域生产系统，通过 VPC peering 按需打通和其它 VPC 的连接，VPC 内可规划不同的子网，通过网络 ACL 和安全组实现隔离。
3. 开发 VPC、测试 VPC、预发 VPC：开发、测试和预生产各自独立规划一个 VPC，部署对应的开发、测试和预生产系统，3 个环境相互隔离。

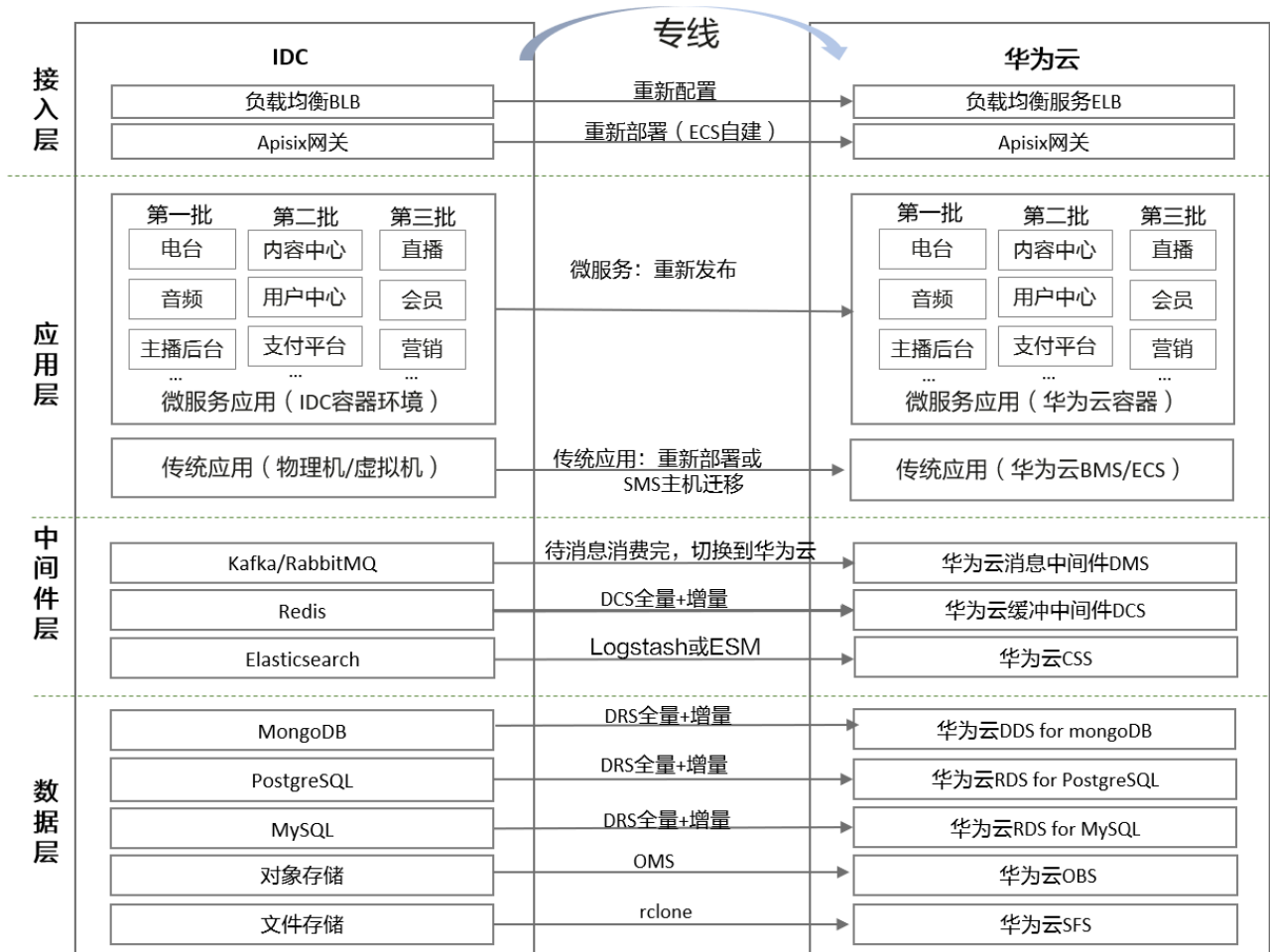
3.5.2.2 应用部署架构示例



方案说明:

1. IDC 和公有云之间通过专线连接。
2. 前端通过负载均衡服务 ELB 在双 AZ 分发流量，ELB 结合 AS 支持弹性伸缩，灵活配置自动伸缩策略，可支撑亿级用户并发。
3. 业务系统以集群方式跨 AZ 部署。
4. Kafka、RabbitMQ、Redis、数据库中间件跨 AZ 高可用部署。
5. MySQL 推荐使用 RDS for MySQL 云数据库,支持一主多读部署模式，替换 MHA 中间件；跨 AZ 部署高可用，秒级主备切换。
6. MongoDB 推荐使用公有云 DDS-MongoDB 数据库，跨三个可用区部署，支持弹性扩容。
7. IDC 机房作为灾备中心，将容器镜像、数据库数据同步到线下 IDC。

3.5.2.3 迁移方案示例



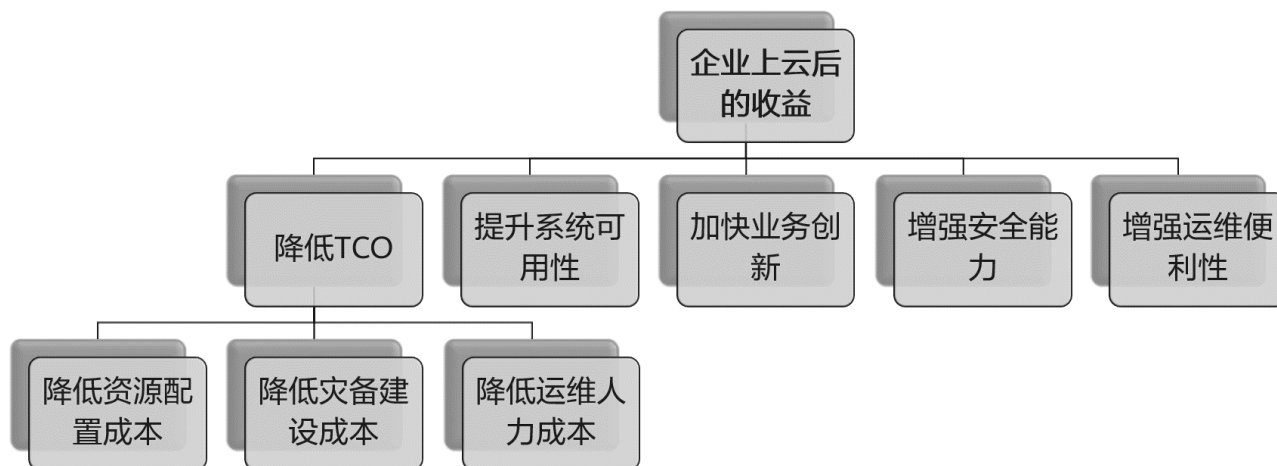
迁移方案说明:

- 接入层:** 全局服务, 涉及 BLB 和 APISIX 网关, 提前在华为云上完成部署、配置和验证
- 应用层:** 通过自动化部署工具 (提前完成华为云 CCE Turbo、内网 DNS 等服务对接) 实现容器化应用的重新发布到华为云
- 中间件层:**
 - Redis: 缓冲中间件, 通过 DCS 工具完成全量+增量迁移
 - Kafka/ RabbitMQ: 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
 - Elasticsearch: 搜索引擎, 使用开源工具 Logstash/ESM 迁移索引数据, 支持全量+增量数据迁移
- 数据层:**
 - PostgreSQL、MySQL、MongoDB: 通过 DRS 工具完成全量+增量迁移

- 2) 对象存储：通过 OMS 工具完成对象存储数据全量+增量迁移
- 3) 文件存储：通过 rclone 等工具完成文件数据全量+增量迁移

3.6 企业上云的收益评估

重度用云的时代已经来临，企业上云前要制定可衡量的业务目标，不仅要关注成本节约、效率提升方面的目标，更要关注云为业务创新创造价值的目标，企业上云后的收益可以从如下维度评估：



3.6.1 降低 TCO

3.6.1.1 降低资源配置成本

通过“IDC 按峰值配置->云上按需配置”的转变，优化资源配置方式，减少资源配置浪费。

企业上云前，通常是在 IDC 自建 IT 系统，而这个 IT 系统必须按照企业最大的业务需求来设计，因为企业需要应对业务高峰，IT 资源通常是参考业务峰值配备的，大部分时候这些资源可能是不需要的，而 IDC 物理资源共享起来又比较困难，因此造成一定的浪费，IT 资源成本很高。

企业上云后，IT 成本从 Capax 模式转变为 Opex 模式，IT 资源可以按需付费，资源可以实现弹性伸缩，按实际资源的使用量来收费，因此上云后可以降低这部分成本，使企业在不过度配置 IT 资源的情况下，动态满足业务对 IT 资源的诉求。

具体上云后能降多少 IT 成本，跟企业的业务峰值特点、IDC 的资源现状、上云后的弹性伸缩策略都有关系。因此，需要充分进行业务调研，按照业务需求设计云上目标架构，选择合适的云服务规格，选择合适的包年包月和按需资源的比例，并且设置合适的弹性伸缩策略，做好 FinOps 才能实现降成本目的。

3.6.1.2 降低灾备建设成本

企业上云后，业务连续性方案的构建成本，比如本地备份、同城容灾、两地三中心，云上相比 IDC 将大幅降低。云上构建灾备方案的成本比 IDC 降低大约 30%~50%左右，云上灾备方案相对于 IDC 灾备方案在节约成本的同时，还具有安全性和便利性方面的优势，具体体现在：

(一) 本地备份:

企业需要在 IDC 购置大量硬件设备, 而且需要提前购置, 即使当前还用不到那么大备份存储容量, 同时供电成本高, 并且需要专人负责这些设备的维护和更新, 将来扩容也很慢, 需要走一系列软硬件采购和安装流程; 而采用云备份, 企业不需要关注底层资源的容量问题, 使用云服务, 按需计费, 不会浪费, 也不要关注设备的维护问题, 省钱又便捷。

(二) 同城容灾:

IDC 构建同城双活需要购买设备、租用机房、配置线路等一系列硬件和软件资产的投入, 而云上构建同城双活的方案则是通过云计算平台将资源虚拟化后进行配置, 不需要像 IDC 一样购买设备、租用机房和配置线路等硬件资源。

1. **基础设施成本降低:** 不需自建或租用容灾机房, 不会造成计算资源浪费, 比如, 如果是主备容灾, IDC 的容灾资源通常是空闲的, 造成资源浪费。而公有云可以按需使用计算和存储资源, 可以策略性地选择将容灾站点的 ECS 关闭以降低成本, 或者容灾节点先用小规格的 ECS, 后续按需变更规格。
2. **无专线费用:** IDC 自建同城容灾, 需要在两个数据中心之间拉通专线, 成本高; 而云上构建同城容灾, 同一 Region 的不同 AZ 机房之间默认是打通的, 且是高速内网, 不收费。
3. **降低容灾配置成本:** IDC 构建同城容灾方案, 通常需要对应用的 4 层架构进行复杂的配置, 需要分别考虑接入层、应用层、中间件层和数据层的灾备方案, 并且需要购买相应的灾备硬件和软件, 成本较高。而公有云原生具备同城容灾的特性, 数据层的 RDS 可以直接选择购买跨 AZ 的主备部署实例, 不需要任何额外配置; 中间件 DCS 也可以选择跨 AZ 主备部署实例; 应用层可以选择跨 AZ 部署, 是同一个内网; 接入层 ELB 也是部署在多个可用区, 多活模式且互为备份。
4. **降低容灾管理和运维成本:** 公有云原生具备同城灾备特性, 不需要用户进行底层配置、管理和运维。相比 IDC, 公有云的同城灾备管理和运维更加简单, 不需要考虑专线运维、不需要考虑数据库、中间件的容灾管理和运维, 不需要考虑负载均衡器的设备管理和运维。

(三) 两地三中心:

公有云上构建两地三中心方案时, 两地的方案优势可以参考同城容灾的描述, 差异点主要在于异地专线部分, 云上的两地专线费用会更低一点。云服务商都会提供 Region 间的高速专线连接, 比如华为云的 CC 服务, 会提供不同种类和规格的网络高速专线, 用户可以根据自己的需求选择合适的服务。相比较而言, 用户自己在两地拉专线的费用可能较高, 涉及到专线设备的采购、维护和升级等方面的费用。此外, 用户自己在两地拉专线还需要考虑跨地域的政策和规定, 可能需要申请相关的审批手续。如果是采用公有云服务, 则这些都不需要考虑, 只需按需使用。具体成本会降低多少, 跟服务提供商、专线带宽、使用时间、地理位置等因素而有所不同。但云上构建两地三中心的便利性是一大优势。

总体来说, 公有云上构建灾备方案相对于 IDC 构建灾备方案, 基础资源的利用率更高, 不浪费, 成本有一定降低, 容灾网络成本更低, 管理和运维成本低, 同时扩展性好、更便捷。具体成本降低的幅度, 还需要根据企业的实际情况和选择的云服务来进行评估。

3.6.1.3 降低运维人力成本

云上运维服务相对于传统的 IDC 运维服务，可以降低运维服务的投入，提高服务质量和效率。云运维相比传统运维可以降低一定的成本，但具体降低多少成本取决于企业的具体情况和实际需求。

1. **运维范围变小：**传统运维需要管理机房，运维物理设备，包括服务器、网络、存储、安全设备等。企业业务全量上云后，基础设施的管理和运维交给了云服务商，企业将不再需要做底层基础设施的运维。
2. **运维效率提升：**
 - 1) **扩展效率更高：**云运维可以弹性扩展资源，可以根据实际业务需求快速扩展计算和存储资源，而传统运维则需要预先规划、购买和部署硬件资源。
 - 2) **运维自动化：**云运维更加注重自动化管理，服务提供商通常会提供自动化的运维工具和服务，实现自动化部署、监控、备份等操作，而传统运维需要手动进行这些工作。

3.6.2 提升系统可用性

企业上云后，应用的可用性将大幅度提升，计划外的停机时间将大幅度减少，具体可用性可以提升多少，与企业 IDC 的现状和上云后的云服务选择有关。企业应用上云以后，天生就具备同城容灾特性，以很少的成本，实现从 IDC 本地高可用，扩展到云上的同城高可用。

1. **数据层可用性提升：**企业上云后，数据层可以实现从 IDC 本地高可用到同城两地/三地高可用，比如可以创建跨 AZ 的 RDS 数据库主备实例，并且还可以额外创建只读副本，大幅提升可用性；OBS 存储支持跨 AZ 多副本存储，即使一个数据中心损坏也不影响数据的访问，比如华为云 OBS 的数据持久性高达 99.9999999999%，业务连续性高达 99.995%，远高于传统架构。
2. **中间件层可用性提升：**中间件层可以创建跨 AZ 的主备或集群部署的缓冲中间件或消息中间件云服务，比本地部署，可用性有大幅度提升。一个数据中心故障，不会影响业务访问。
3. **应用层高可用提升：**应用层可以跨 AZ 部署，云服务商提供了负载均衡服务，可以自动分发流量到不同数据中心的服务器上，确保服务的可用性和性能。此外，负载均衡还可以实现自动故障转移和容错功能，比本地可用性有大幅度提升。
4. **接入层可用性提升：**云服务的负载均衡支持同时部署在多个可用区，多活模式且互为备份，相比 IDC 的本地负载均衡，提供更高的可用性。

总之，上云之后，业务系统的接入层、应用层、中间件层和数据层的可用性都提升到了同城多数据中心高可用级别，相比 IDC 的本地部署，可用性有大幅度提升。上云之后，业务可以非常方便的实现同城高可用，可以理解为，上云之后，原生就具备同城高可用特性，同时两地三中心的实现也比线下要快捷、方便、省钱的多。

3.6.3 加快业务创新

云通过提供基于互联网的灵活、可扩展、安全的计算资源和服务来支持业务创新和快速上线。以下是云实现业务更快创新和加快上线时间的几个方面：

1. 首先，云提供了快速部署和弹性扩展的能力。云服务可以根据客户需要快速部署新的资源，同时可以根据需求进行弹性扩展，从而满足不断变化的业务需求。这使得客户可以更快地推出新产品和服务，以满足市场需求。
2. 其次，云提供了丰富的开发工具和服务，如 API、SDK 等，可以帮助客户更快的开发和部署应用程序。云还提供了多种不同的服务模型，如 SaaS、PaaS 和 IaaS，以满足不同客户的需求，从而加速了应用程序的开发和部署，尤其是大数据、AI、区块链等服务，企业可以直接调用，以使能新业务的开发、测试和商用。
3. 同时，云还提供了全球范围内的网络和基础设施，企业可以在全球范围内部署和管理应用程序，可以根据业务需求选择不同区域的数据中心，从而将应用程序部署到离用户更近的地方，提供更快的响应时间和更好的用户体验。
4. 最后，云还提供了强大的安全和合规功能，如身份验证、访问控制、加密等，可以保护企业的数据和应用程序的安全性和合规性。这使得企业可以更加自信的开发和部署新的应用程序，从而更快地推出新产品和服务。

综上所述，云通过提供灵活、可扩展、安全的计算资源和服务来支持创新和快速上市，帮助企业更快的推出新产品和服务，满足不断变化的市场需求。

3.6.4 增强安全能力

企业上云后，相比 IDC，安全能力有以下几个方面的增强：

1. **更强的防护能力：**云提供了多层安全防护，包括物理安全、网络安全、主机安全、数据安全等方面。云服务提供商会为客户提供多重安全措施来保护客户数据的安全，如防火墙、入侵检测、DDoS 防护等。相比在 IDC 自建安全方案，云的能力更强、更容易获得。
2. **安全合规性更高：**云平台通常具备更加严格的安全合规性要求，包括数据加密、身份验证和访问控制等。这些要求可以确保企业数据的安全性和隐私性。云服务提供商通常会获得多种安全合规认证，如 PCI DSS、ISO 27001、CSA STAR 等。这些认证证明了云服务提供商在安全和合规性方面的能力和质量，客户可以放心地将数据和应用程序放在云计算平台上运行。
3. **严格的访问控制和身份验证：**云计算提供了多种访问控制和身份验证的方式，如账号密码、多重身份验证、访问控制列表等。客户可以根据需要对用户进行身份验证、授权和权限管理，从而确保只有授权的用户才能访问和使用应用程序和数据。
4. **实时安全监控和告警：**云提供了实时监控和告警功能，可以帮助客户实时了解应用程序和数据的状态，及时发现和处理安全问题。云服务提供商还可以提供安全事件的警报和通知，帮助客户快速响应和处理安全事件。
5. **专业安全团队：**云平台通常拥有专业的安全团队，能够提供更加专业的安全服务和支持，及时解决安全问题，帮助企业构建更加安全可靠的云计算环境。

总之，相比 IDC，企业上云后可以获得更多的安全防护、访问控制、安全合规性认证以及实时监控和告警等功能，从而增强了企业的安全能力。

3.6.5 增强运维便利性

企业上云后，不需要做基础设施运维，相比 IDC 运维更加便利：

1. 基础设施免运维：云平台提供了服务化的管理方式，客户可以使用云服务提供商提供的服务来管理和部署应用程序和基础设施，如 RDS、DCS 等，客户只需关注应用程序的业务逻辑，无需关注基础设施的管理和维护。
2. 可视化运维：云提供了可视化的管理界面，客户可以通过云服务提供商提供的控制台来管理和监控应用程序和基础设施。控制台提供了丰富的功能和工具，如监控、日志、诊断、自动扩展等，可以帮助客户快速发现和解决问题。
3. 自动化运维：云平台提供了自动化运维的功能，客户可以通过 API、脚本等方式进行运维自动化。客户可以使用云平台提供的自动化工具和服务，如华为云 AOS 等来快速创建、部署和管理基础设施和应用程序。
4. 弹性扩展更便捷：云计算平台提供了弹性扩展的能力，客户可以根据业务需求自动扩展应用程序和基础设施，从而提高响应能力和可用性。客户无需考虑底层基础设施的管理和维护，可以专注于开发和部署应用程序。
5. 运维支持服务：云服务提供商提供了丰富的常见问题解决方案，客户可以通过查看文档、FAQ、论坛等方式快速解决问题，云服务提供商还提供了技术支持服务，客户可以通过电话、邮件等方式获得技术支持。同时，云服务商还会提供更高级别的支持服务，比如华为云的企业级支持计划，购买了企业级支持计划的企业将获得更多的支持服务，比如专属的 TAM 等。

综上所述，企业上云后可以通过自动化运维、可视化管理、弹性扩展、服务化管理和常见问题解决方案等方式增强运维便利性，降低运维技术门槛。

4 企业上云准备

企业决定全面上云后，在正式开始之前，需要进行一系列准备工作，以确保云转型工作能够顺利进行。首先，需要识别干系人并组建上云团队，负责统筹和领导企业的云转型工作。其次，做好技能准备，企业需要评估现有团队的技术能力，并通过培训、认证等方式提高员工的云计算知识和技能，同时还要熟悉云服务商的技术特性和上云实践。最后，组织上云动员，向企业内部员工和关键利益相关者传达上云的重要性、目标和收益，做好“三个对齐”，增强团队的合作意愿和参与度。

4.1 干系人识别

企业上云，尤其是大规模全量上云工作，会涉及到许多内部和外部干系人，这些干系人在不同的阶段和层面上会发挥重要作用，对企业上云的成败有决定性影响，因此在组建上云团队前，我们需要先识别干系人，这些干系人，是企业组建自己的上云团队 CCoE 的重要来源。

4.1.1 内部干系人

企业上云涉及许多内部干系人，每个干系人在不同阶段扮演着重要的角色。以下是一些常见的内部干系人和他们在上云过程中的职责：

1. **高层管理人员：** 高管层是企业上云的决策者和推动者，确定上云战略和目标，提供资源和支持。
2. **运维团队：** 运维团队负责现有基础设施和系统的管理和维护，在上云时，他们的职责包括评估现有环境的可迁移性，规划和执行上云策略，设计上云架构，搭建和维护云基础设施，确保其高可用性、安全性和性能，保障平稳迁移，并提供上云后的日常运维和技术支持。
3. **开发团队：** 开发团队负责应用程序的开发和部署，在上云时，他们负责将企业的应用程序迁移到云平台，对应用程序进行上云适配改造或重构，确保应用程序能够适应云环境，并利用云平台提供的服务和功能。
4. **测试团队：** 测试团队负责验证和确保上云后应用程序的功能、性能和可靠性，制定测试计划、设计测试用例和执行策略，确保应用程序在云环境下正常运行，并符合预期的质量标准。
5. **财务部门：** 财务部门负责预算规划、成本控制和效益评估，在上云时，他们需要参与预算的编制和审批、评估上云的成本效益、跟踪和管理云资源费用使用情况，并与供应商进行合同谈判和管理。
6. **子公司：** 对于大型的集团型企业而言，子公司也是重要干系人，他们需要匹配集团的上云战略，并参与到上云的规划和执行中。

4.1.2 外部干系人

企业上云涉及到许多外部干系人，他们在上云过程中发挥着重要作用，企业需要与这些外部干系人建立紧密的合作关系，并在整个上云过程中保持密切的沟通和协调，确保上云计划的成功实施。以下是一些常见的外部干系人及其在企业上云过程中的职责：

- 1. 云服务提供商：**云服务提供商是企业上云的关键合作伙伴，他们负责提供云基础设施和相关服务，包括计算、存储、网络等资源，他们的职责包括：
 - 提供稳定、可靠的云基础设施和服务
 - 协助企业进行上云架构的规划和设计
 - 提供上云迁移的技术指导和实践
- 2. 咨询公司：**企业可能会聘请第三方咨询公司来提供企业上云的咨询，他们的职责包括：
 - 分析企业现有的业务架构、技术架构，评估上云的可行性
 - 分析企业需求，制定上云战略和蓝图规划
 - 设计上云的高阶方案
- 3. 应用系统开发商/供应商：**如果企业的业务系统是第三方定制开发的或者采购自第三方供应商，那么应用系统开发商/供应商在上云过程中也会扮演重要角色，他们的职责包括：
 - 数据迁移和集成服务，将现有系统和数据迁移到云平台
 - 应用程序开发和定制，根据企业的上云需求开发和定制云应用程序
 - 应用程序的集成和测试，并提供技术支持和维护
- 4. 监管机构：**某些行业可能受到特定监管要求的约束，企业上云时需与监管机构合作，确保合规性。他们的职责包括：
 - 提供相关的法规和合规指导
 - 审查企业的上云计划和实施情况
 - 监督数据隐私和安全合规性
- 5. 外部组织：**某些企业在上云期间需要评估对外部业务的影响，比如对于零售企业来说，可能会涉及第三方销售渠道（比如某团购平台），上云切换时需要评估对第三方销售渠道的业务影响，并制定应对措施。

请注意，具体的外部干系人和其职责可能因企业的规模、行业和上云策略而有所不同。因此，在实际情况中，企业需要根据自身需求和情况确定相关的外部干系人，并明确他们的职责和合作方式。

4.2 组建 CCoE 团队

企业上云首先要组建一支专业的上云队伍，识别出干系人以后，可以结合业界最佳实践，组建上云的 CCoE 团队，来负责推动企业云转型战略的落地。

4.2.1 什么是 CCoE

CCoE 是 Cloud Center of Excellence 的缩写，即云卓越中心，不同企业可能会根据其具体需求和组织结构来命名这个团队，比如有些企业也命名它为云中心团队、云中心运营团队、云治理团队、云办公室、云创新中心或云能力中心等，虽然叫法不同，但他们都是负责制定和推进企业云转型策略、规范上云和用云过程、提供云运维和治理的最佳实践等。CCoE 是企业上云旅程的起点，它是一个跨部门的团队，它的成员来自我们前面识别的干系人部门。CCoE 主要包括如下职责：

1. 云战略和规划 (Cloud Strategy and Planning) :

- 制定云战略、目标和愿景
- 制定上云迁移的路线图
- 进行业务和技术可行性研究
- 确定适合企业需求的云服务模型和提供商
- 监测和评估市场上的新兴云技术和趋势

2. 云架构和设计 (Cloud Architecture and Design) :

- 针对不同类型的工作负载，制定云架构和设计原则
- 选择合适的云服务和工具，以支持架构需求
- 设计弹性和可伸缩的云架构，以满足业务需求
- 提供云基础设施和平台的架构设计指导
- 对云应用程序进行架构评估和优化

3. 云运营和管理 (Cloud Operations and Management) :

- 选择和实施合适的云管理工具
- 定义服务级别协议 (SLA) 和监控机制
- 制定云运营管理策略和最佳实践
- 监控云环境的性能、可用性和安全性
- 实施自动化和编排工具，提升效率和可靠性

4. 云安全和合规性 (Cloud Security and Compliance) :

- 制定和实施云安全策略和控制措施

- 管理云环境的身份验证、访问控制和数据保护
- 进行风险评估和漏洞管理，以降低安全风险
- 确保云服务符合合规性要求和相关法规
- 建立安全监控和事件响应机制

5. 云培训和技能发展 (Cloud Education and Skill Development) :

- 提供云计算相关的培训和认证计划
- 建立云技能发展计划，培养组织内部的云专家
- 组织内部的云社区和知识共享活动
- 建立云知识库和文档中心
- 推广云计算最佳实践和经验分享

以上 5 个方面构成了 CCoE 的总体框架，具体的落地方案可能因不同企业的需求和实践而有所不同，实际执行时可以根据企业的需求和实际情况进行调整和定制，做出符合企业特点的方案，帮助企业顺利进行云转型。

4.2.2 为什么要构建 CCoE

构建 CCoE 可以帮助企业更好地规划和管理云转型过程，提高上云效率和降低 IT 治理成本，加强安全和合规，促进创新和竞争力的提升，它是企业实现云战略和数字化转型的关键组成部分。为确保企业上云转型成功，企业需要构建 CCoE 团队。

CCoE 团队可以为企业上云提供战略引导、技术专业支持、资源整合和管理，以及安全合规保障。这个团队的存在可以加速上云过程，降低风险，并确保企业能够充分发挥云计算的优势和潜力，实现成功的云转型和数字化转型。CCoE 可以给企业带来如下好处：

1. **统一的云战略和路线图：**构建 CCoE 可以帮助企业制定统一的云战略和路线图，明确组织对云的愿景和目标。它能够帮助企业更好地规划和管理云转型过程，减少云迁移过程中的风险和不确定性。
2. **上云期间更好的协作：**CCoE 通过建立一个跨部门的协作平台，促进不同部门之间的沟通和协作。它能够帮助企业建立云决策机制，对云相关项目进行协调和管理，确保整个组织在云转型过程中的一致性和协同性。
3. **提高效率和降低成本：**CCoE 可以通过推广和应用最佳实践，提供云相关的培训和咨询，帮助企业高效地采用云技术，并降低云转型过程中的成本和风险。它能够帮助企业实现规模经济效益，提高资源利用效率。
4. **强化安全和合规：**构建 CCoE 有助于企业建立和实施统一的安全和合规策略。它可以提供安全咨询和培训，确保企业在云环境中能够满足法规和标准的要求，保障数据和系统的安全。

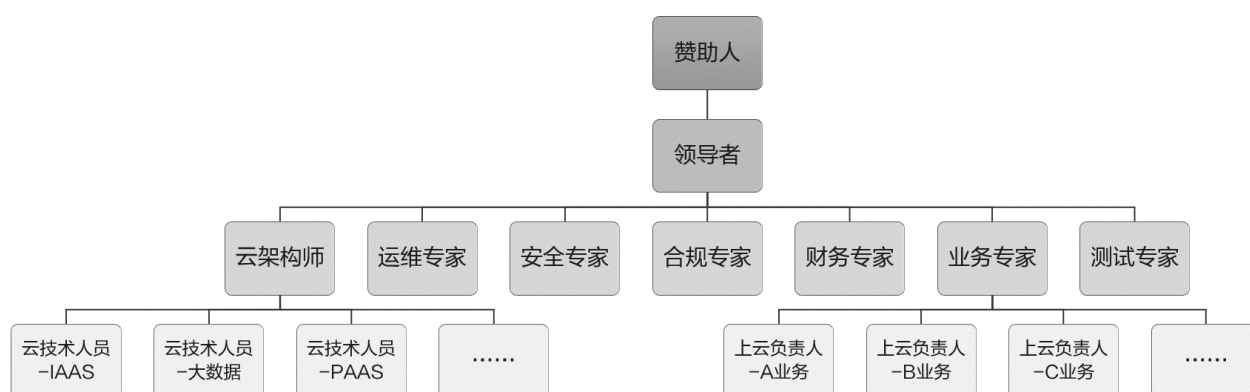
- 5. **提升创新能力**：CCoE 可以帮助企业更好地应用和推广云的创新技术和最佳实践，促进新业务模式的创新和实验。它能够帮助企业快速响应市场需求，加速产品和服务的上市时间，提升企业的竞争力。

4.2.3 如何构建 CCoE

CCoE 构建的前提是企业已经制定了云转型战略，并且获得企业高层支持。企业上云的规模决定了 CCoE 团队的大小，参与上云的业务模块越多，CCoE 团队就越大。CCoE 一般包括如下角色：

- **赞助人**：来自企业高层，是企业数字化和云化转型的高层赞助人。
- **领导者**：企业云转型的领导者，是云战略专家，了解云的先进技术，并对业务有深刻理解。
- **云架构师**：具备云的专业知识，确定上云的技术路线，提供云的最佳实践和模板，负责上云架构设计和上云迁移工作。
- **运维专家**：提供上云之后的运维模型和最佳实践，建立企业云上运维体系，搭建运维平台，以及通过自动化运维的方式，对云上环境进行持续治理和管理，包括架构优化、平台建设、资产管理、权限管理、云自动化等，比如根据业务需求分配云资源和所需权限，并对资源进行初始化配置。
- **安全专家**：负责上云的安全标准、规范和准则的制定，确保云上运营运维安全。
- **合规专家**：确保企业上云后满足相关法规、行业标准和内部合规要求，以最大程度地降低风险并保护企业利益。
- **财务专家**：负责制定上云成本分摊原则，进行成本优化和控制治理。
- **业务专家**：多名来自各业务团队的上云代表，是各业务团队的上云负责人，负责上云工作在本业务部门的落地和执行。
- **测试专家**：企业上云时，对业务进行全方位的功能、性能、可用性测试。

CCoE 团队的参考架构如下：



CCoE 是一个跨部门的虚拟团队，成员并不一定都来自企业内部，前期可以通过咨询公司或云厂商承担部分职责，运作成熟后再逐步自主承担，CCoE 是一个持续存在的组织，不止负责上云工作，还负责上云后的持续运营、运维和治理，以及新技术的更新迭代和持续优化。

4.3 技能准备

企业上云时，团队成员需要具备一定的云技能和知识，以便更好地支持企业的上云过程，因此，在企业上云之前，建议对团队成员进行培训，做好相关技能准备，以确保他们具备必要的云技能来支持企业的云转型。

4.3.1 做哪些技能准备

企业上云对不同团队成员的技能的要求会有所差异，以下是各个部门在上云过程中可能需要具备的一些云相关技能和知识，仅供参考，实际情况可能会因不同企业的具体需求而有所变化。

- 1. 企业高层：**负责决策和资源支持，他们需要掌握以下技能。
 - 了解云的基本概念和优势，理解云转型对企业的战略意义
 - 了解云的商业模式和运营方式，能够进行战略决策
- 2. 开发团队：**开发团队需要在云上进行应用程序开发和部署，他们需要掌握以下技能。
 - 了解云的基本概念和架构，理解云服务模型（如 IaaS、PaaS、SaaS）以及其应用场景
 - 熟悉使用云平台提供的工具、API 和 SDK，能够与云进行集成和交互，能够使用云平台进行云原生应用的开发和部署
 - 掌握云原生开发的能力，包括容器化、微服务架构、CI/CD 等
 - 了解云网络和云安全的基础知识，以确保应用程序的高可用性和安全性
- 3. 测试团队：**测试团队需要在云环境中对应用程序进行测试和验证，他们需要具备以下技能。
 - 能够在云上搭建和管理测试环境，包括虚拟机、容器等资源的使用和配置
 - 掌握云平台的监控和日志分析工具，能够进行性能测试和故障排查
 - 了解云环境下的测试流程，能够进行云上应用程序的功能测试、性能测试和安全测试
 - 掌握云平台提供的自动化测试工具和服务，能够在云上进行自动化测试的编写和执行
- 4. 运维团队：**运维团队需要监控和维护云环境中的应用程序和基础设施，他们需要具备以下技能。
 - 掌握云平台的基础设施管理，包括虚拟机、存储、网络等资源的配置和监控
 - 掌握云平台的自动化运维工具和技术，能够进行自动化部署、调优和故障处理
 - 掌握云平台提供的自动弹性伸缩和负载均衡功能，能够进行资源的调度和优化
 - 了解云平台的安全策略和权限管理，能够进行合理的访问控制和安全配置
- 5. 财务部门：**财务部门需要负责上云的预算和成本管理，他们需要具备以下技能。
 - 了解云计算的成本模型和计费方式，能够进行云服务的成本估算和预算规划
 - 掌握云平台提供的费用计量和消费分析工具，能够进行资源利用率和成本优化分析

4.3.2 如何做技能准备

企业可以制定详细的上云培训计划，可以包括多种形式，包括集中授课、实验账号演练、在线文档学习，专家经验分享，并且最好通过云厂商相应级别的认证考试，支撑好企业全业务上云，培训资源可以通过如下方式获取：

1. 云计算基础知识自学：企业员工可以通过阅读相关书籍、文档、博客等方式进行学习，自学云计算的基本概念、架构。
2. 参加云计算培训课程：企业可以参加各种云计算培训课程，包括免费公开课、购买云厂商的认证培训等，学习云计算的具体技术和实践，如华为云的解决方案认证培训 HCIA/HCIP/HCIE。
3. 进行实践和练习：企业可以通过搭建云计算环境、部署应用程序、维护和管理云环境等方式来进行实践和练习。可以选择一些云服务提供商提供的试用版本，进行免费试用，也可以购买一些云服务，进行实际的应用开发和测试。
4. 邀请专家讲座：企业可以邀请上云方面经验丰富的云计算架构师来培训员工，了解上云的流程、风险、注意事项及最佳实践。
5. 参加社区活动：企业可以参加云计算社区的活动，如技术交流、讨论、分享等，与其他云计算从业者进行交流和學習。
6. 获得相关认证：企业可以获得相关的云计算认证，如华为云 HCIP/HCIE 认证等，证明自己掌握了云计算的相关技能和知识。

4.4 运维平台准备

在企业上云前，需要提前做好企业现有的运维平台与公有云的对接集成，实现快速自动化部署和集中运维管理，一方面可以提高上云时的部署和迁移效率，另一方面迁移期间的问题处理更加高效。建议做好以下运维系统与公有云的对接：

1. 统一日志平台对接公有云

- **对接方式：**通过配置日志收集代理或使用公有云提供的 API 将公有云的日志数据传输到统一日志系统中。
- **作用和价值：**实现公有云日志的统一汇总和管理，提供集中化的日志分析、搜索和监控功能。这样可以方便运维人员对云上应用进行故障排查、性能优化和安全分析。

2. 统一告警平台对接公有云

- **对接方式：**通过配置告警通知规则或使用公有云提供的 API 将公有云的告警信息发送到统一告警系统中。
- **作用和价值：**实现公有云告警的集中管理和处理，将云上的各种异常情况和事件与企业现有的告警平台进行整合，方便及时发现和响应问题，提高故障处理效率和系统可靠性。

3. 自动化部署平台对接公有云

- **对接方式：**利用云平台提供的 API 或命令行工具与自动化部署系统进行集成，并配置相应的资源编排模板或脚本（如通过 Terraform 批量开通云资源和配置参数，一切配置代码化，结合 Jenkins 创建自动化的基础设施部署流水线），实现在上云期间通过自动化平台发放云资源并自动化部署微服务应用。
- **作用和价值：**在上云迁移期间，可以实现在上云迁移期间的自动化资源管理和应用部署，减少手动操作和人工干预，提高上云灵活性及效率，同时降低了上云过程中的误操作风险。

4. CMDB 对接公有云

- **对接方式：**将企业现有的配置管理数据库（CMDB）与云平台进行对接，通过集成 API 或其他方式，将云上资产的信息同步到 CMDB 中，实现云上资产的统一管理。
- **作用和价值：**通过对接 CMDB 和云平台，可以实现对云上资源的统一管理和跟踪，包括资源配置、关联关系、变更记录等。这样可以提高对云上资源的可视化管理，并支持后续的容量规划、资源优化和安全管理。

5. ITSM 对接公有云

- **对接方式：**将企业现有的 ITSM 系统与云平台进行集成，例如通过插件、API 等方式实现工单、变更管理的联动。
- **作用和价值：**ITSM 工具用于管理和跟踪 IT 服务请求和问题，通过与 ITSM 系统的集成，可以将云上资源的变更、故障等事件与企业现有的问题管理、变更管理流程进行关联，提高运维的响应速度和问题解决效率。比如 JIRA 可以实现上云期间业务测试问题的统一记录和管理，提供全面的事务视图和报告，促进跨团队的协作和问题解决，加快上云工作的进展。

总之，提前准备好运维平台，实现公有云与企业现有运维体系的无缝衔接，可以提高上云迁移的可控性、稳定性和效率，同时减少迁移期间的风险和工作量。

4.5 项目管理准备

4.5.1 概述

对于大规模的上云迁移项目，在项目启动前，需要根据项目实际情况，制定出切实可行的管理制度，这些制度在项目中要始终如一的执行，比如项目启动制度、项目动员会、每日报告制度、周例会制度、里程碑会议制度、每月例会制度、问题管理制度、变更管理制度、文档管理制度、项目结束制度、人员进出制度、权限管理制度、信息安全制度等。项目经理（PM）在项目管理中扮演着关键的角色，以下是一些经验和建议，可以帮助 PM 有效的管理大规模上云迁移项目：

1. **充分了解业务需求和迁移目标：**PM 应该与业务部门和利益相关者紧密合作，全面了解业务需求，并明确迁移目标。这将有助于确定项目的范围、优先级和关键成功指标，并确保迁移与业务目标的契合。

2. **制定详细的项目计划和时间表：**根据项目目标和复杂性，制定一个详细的项目计划，包括迁移的阶段、任务和关键里程碑。建立合理的时间表，并与团队成员共享，以确保每个人都了解任务和期限，并能够做好时间管理和资源分配。
3. **组建高效的项目团队：**PM 需要组建一个高效的项目团队，包括具有相关技能和经验的成员。确保团队成员之间的角色和职责明确，并能够有效协作和沟通。PM 还应提供必要的培训和支持，确保团队具备所需的知识和技能。
4. **有效的项目沟通：**建立良好的沟通机制和渠道，确保在项目团队内部和与利益相关者之间进行及时、清晰和准确的沟通。定期召开项目会议，共享项目进展、问题和决策，以促进团队合作和项目的透明度。
5. **风险管理和问题解决：**PM 应该制定风险管理计划，识别和评估潜在风险，并制定相应的风险应对策略。同时，PM 需要建立问题解决机制，跟踪和解决项目中出现的问题。及早发现和解决问题，以避免其对项目进展和成果的不良影响。
6. **资源管理和优化：**PM 需要合理规划和管理项目所需的资源，包括人员、预算、技术设备和云服务等。确保资源的合理利用和优化，以满足项目的需求，并最大程度地提高效率和成果。
7. **持续改进和学习：**上云迁移是一个持续演进的过程。PM 应积极推动团队的持续改进和学习，包括识别和应用最佳实践、评估项目绩效并提供改进建议。利用经验教训和项目的反馈，不断优化项目管理方法和流程。
8. **监控和报告项目进展：**PM 需要定期监控项目的进展和状态，并及时报告给利益相关者。利用适当的项目管理工具和技术，跟踪项目里程碑的达成情况，及时识别时间和质量偏差，并采取相应的纠正措施。
9. **管理变更和期望：**上云迁移项目可能面临变更请求和需求的变化。PM 应制定变更管理计划，评估和管理变更的影响，确保变更得到适当的评估、批准和跟踪。同时，积极管理并与利益相关者共同管理期望，确保对项目范围和资源的合理管理。
10. **建立良好的团队文化：**PM 需要营造一种积极、协作和开放的团队文化。鼓励团队成员分享经验和知识，提供支持和反馈，激励团队达到共同的目标。建立团队的认同感和归属感，定期组织团建活动，以增强团队的凝聚力和项目的成功。

通过应用上述项目管理经验，PM 能够有效地管理并成功交付大规模上云迁移项目，提高项目的效率和成果，同时降低风险和问题的影响。

4.5.2 目标制定

项目经理需要理解上云迁移的定位和价值，做到知其然也知其所以然。项目经理需要与企业的中高层对齐项目目标和里程碑，明确项目需要的资源和需要配合的周边部门，明确项目在企业中的重要性，以便在项目遇到瓶颈时求助中高层以获得协助和指导。明确企业内部对项目结果的预期，是全量系统上云还是部分系统上云，是以应用平迁为主还是需要辅以应用升级改造，并确定验收标准。

4.5.3 过程管理

(一) 制定可衡量的任务

迁移项目的过程管理，需要时刻保持任务跟进，针对一个长期跟进的任务，需要可量化、可追踪，明确操作步骤和责任人以及完成时间，举例如下：

任务名称	量化标准
输出《迁移方案》	输出《迁移方案》的文档
扩容或新建专线	专线扩容至XXXMb，新建XXX条XXXMb的专线
完成上云代码改造项	需要改造XXX项
第三方进行上云相关修改	需要XXX个第三方配合改造XXX项
梳理测试用例（功能、性能、自动化）	功能用例XXX个，性能用例XXX个，自动化用例XXX个
上云前小规模测试（部署类、连通类、兼容类）	得出明确的结论：XXX应用可以使用云服务，XXX应用需要做修改等
部署演练环境	部署XXX个应用或微服务、XXX套数据库、XXX套中间件
部署生产环境	部署XXX个应用或微服务、XXX套数据库、XXX套中间件
测试（切换前，功能、性能、自动化）	生产环境的用例必须通过XX%，演练环境的用例必须通过XX%
输出runbook	runbook必须要细化到命令
切换演练	明确可以演练的步骤，通过演练优化时间
灰度切流	灰度引流生产环境流量
切换100%流量	切换100%流量

(二) 识别、跟进闭环风险和问题

在上云迁移过程中，需要特别关注相关的风险识别及跟进闭环，主要可以从以下几个方面开展：

1. **识别和评估风险：**在项目开始之前，与团队成员一起识别潜在的风险，并对其进行评估，确定风险发生的可能性和影响，并为每个风险制定适当的应对计划和应对责任部门及责任人。

2. **监控和控制风险：**通过监控风险指标和进行风险评估，及时识别新的风险和变化的风险，在风险发生时，采取适当的措施来控制 and 降低风险的影响。
3. **设定问题解决机制：**建立一个有效的问题解决机制，确保项目团队能够及时处理和解决出现的问题。这可能包括设立问题反馈通道、制定问题解决流程、明确问题负责人等。
4. **跟踪问题解决状态：**记录和跟踪所有的问题，包括问题状态、解决方案、解决进展。使用问题跟踪工具或项目管理软件，确保问题得到适当的处理，并在解决之前及时进行跟进。
5. **定期沟通和报告：**定期与团队成员和利益相关者沟通，并向他们报告项目的风险和问题情况。提供透明的信息和及时的更新，确保所有相关方都了解项目的风险和问题，并参与解决。
6. **学习和持续改进：**在项目执行过程中，通过回顾风险和问题的处理方式，总结经验教训，并在未来项目中吸取这些经验教训。持续改进过程管理方法和流程，提高项目的执行效率和质量。

(三) 有效开会

1. 会前准备会议材料

- 根据会议主题准备会议材料
- 设置会议提醒，避免与会者遗忘
- 材料提前发送，提醒与会者，会前阅读材料，会上直接讨论

2. 会中控制会场节奏

紧扣主题，遇到弱相关问题或与主题无关问题，及时制止，另行安排专题会议讨论。议题接近结束时间时，及时提醒与会者。

3. 会后输出纪要并跟踪闭环

纪要包含议题、与会者、结论、遗留事项。遗留事项必须责任到人，明确完成时间并跟踪闭环。

(四) 紧密跟踪任务

针对计划，每日跟踪完成进展，且发送日报。针对会议遗留任务，明确责任人和完成时间点，跟踪完成情况。针对风险和问题，跟踪处理进展。

4.5.4 有效沟通

企业上云由于涉及的组织和人员较多，要做好沟通管理，制定沟通计划，明确沟通的机制，使相关干系人对上云目标、进度、风险等有清晰的理解和认识，为共同目标达成而协同努力。建议设置专职的 PM 负责例行管理，并针对各个事项安排到人，沟通协作贯穿全过程，在沟通的过程中，需明确以下几点：

1. **清晰明确的沟通目标：**确保所有沟通都有明确的目标和目的，明确沟通的内容。
2. **制定不同层级的沟通会：**
 - 1) 项目组通过周例会审视进度、问题和风险，支撑上云目标达成
 - 2) 管理层通过月度例会进行整体审视、关键事项决策、问题推动
 - 3) 通过专题会议，审视核心交付物，如上云架构、切换方案、实施标准等

3. **定期沟通：**制定详细的沟通计划，包括固定的沟通时间和频率，以确保与项目团队、利益相关者之间的沟通顺畅和及时。如：项目前期可开展周例会，项目冲刺阶段开展日站会等。
4. **选择适当的沟通方式：**根据需求和情况选择合适的沟通方式，包括会议、电子邮件、在线协作工具、通讯工具等。有些信息可能需要面对面会议来达成共识，而其他信息则可以通过电子邮件或在线协作工具进行，同时需保持信息沟通过程中的透明性及时效性。针对不同场合及目的选取不同的沟通方式。如：各部门正式沟通采取会议方式，并留存会议纪要，日常沟通统一通讯工具（微信、飞书等），紧急事项及时电话沟通等。
5. **及时提供反馈和更新：**定期向项目团队和利益相关者提供项目的进展和更新。及时提供重要的信息和决策，以便所有人都能了解项目的状态。

4.6 上云动员会

1. Why: 为什么要组织上云动员会

组织上云动员会的目的是统一思想、建立信心，公司从上到下达成共识。通过上云动员会，将上云过程中的利益相关者聚集在一起，让大家对上云迁移要达成的目标、整体里程碑、项目运作规范、上云迁移的流程和高阶方案有个统一的认识。

- 1) **统一认知和目标：**上云涉及到不同部门和员工的参与，而他们对云的理解和认识程度可能不一致。通过上云动员会，企业可以统一员工对于上云的认知，确保所有人理解上云的目的、上云策略和计划。动员会可以激发员工的信心和动力，提高员工支持和积极参与上云的意愿。
- 2) **加强沟通和协作：**上云涉及到不同部门和团队的合作，动员会提供了一个共同交流的机会，促进了各个部门之间的沟通和协作，有助于上云期间跨部门的高效协同和配合。
- 3) **确定责任与任务：**通过上云动员会明确每个部门和个人在上云过程中的职责和任务，确保所有相关方都明确自己的角色，并协调好资源和人力分配。
- 4) **说明项目规范：**向项目人员说明项目的运作规范，以便项目经理有效地对项目实施管理。
- 5) **了解上云迁移流程和高阶方案：**让全员了解上云迁移流程和高阶方案，这样在项目运作过程中，项目组成员才能有效的配合，对每个阶段该做什么、为什么这么做、该如何做就非常清楚。

2. What: 动员会做什么

动员会 = 3 对齐（组织对齐 + 目标对齐+ 责任对齐）+ 仪式感。

- 1) **组织对齐：**成立联合项目组，针对关键岗位形成“一对一互锁”。
- 2) **目标对齐：**明确上云的里程碑，颗粒度细化到每周。
- 3) **责任对齐：**明确联合项目组中的运维、研发、测试、项目管理团队责任分工。
- 4) **仪式感：**需要从人员、场地、道具和时间等方面来营造仪式感，让联合项目成员知道上云的重要性和时间感。

3. How: 怎么开好动员会

需要从以下几个方面进行强准备：会议材料、地点、道具、时间、时长。

- 1) 会议材料：需要包含项目里程碑、项目组组织架构、分工矩阵、当前进展和下一步工作。
- 2) 地点：选择在大型且装修最好的会议室。
- 3) 道具：印有上云迁移等字样的横幅。注意，根据企业要求，如果企业没有拉横幅的习惯则取消。准备 PPT 作为最后合影的背景墙。其他物料：名牌、矿泉水等。
- 4) 时间：选择上午时间，让大家知道项目的重要性，上午是人们精神最充沛的时间。
- 5) 时长：控制在 1 个小时，时间短说不清楚，时间长人们无法集中注意力。

4. Who: 哪些人参加动员会

建议企业高层（董事长、CEO、CTO）之一参加、各级中层主管（运维总监、研发总监、测试总监、PMO 总监等）尽量参加、各级业务骨干（由中层主管确定）必须参加、其他人员选择性参加（推荐全部参加）。

5. When: 什么时候开动员会

当企业确定上云，各项调研、评估规划、上云准备就绪后，召开动员会，以对整个项目组进行动员和统一思想。

5 云上架构设计

5.1 架构设计概述

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：



- 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。
- 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。
- 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。

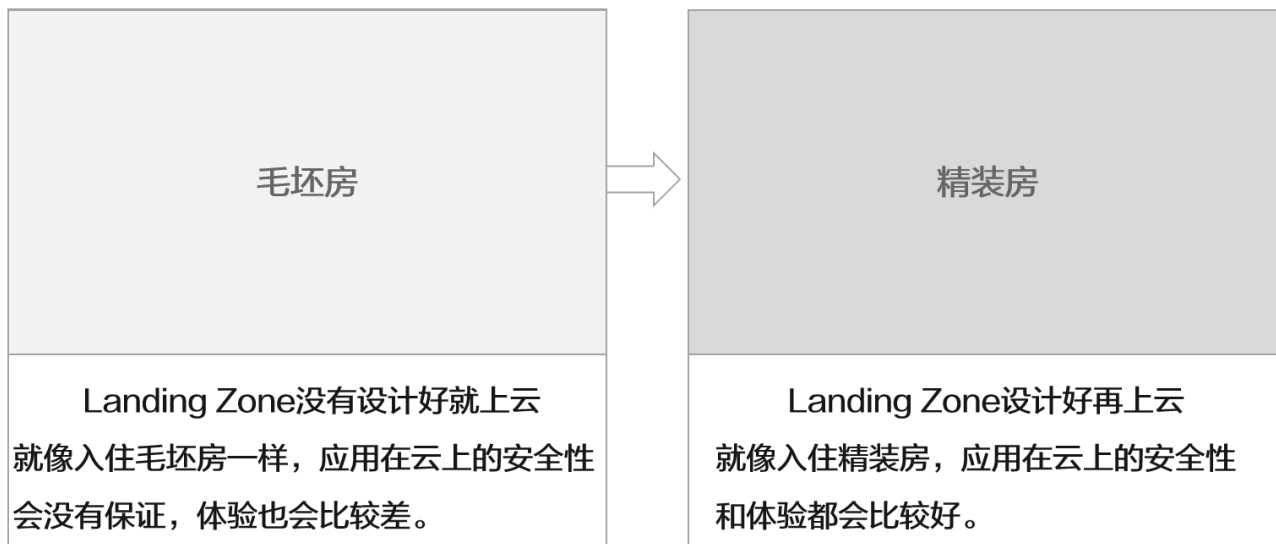
5.2 基础环境设计

5.2.1 基础环境介绍

基础环境在业界也叫做“着陆区（Landing Zone）”，它是一个航空术语，本意是指飞机可以安全着陆的区域。引申到企业上云场景，企业上云同样需要有一个云上的安全着陆环境（Landing Zone），来保障上云的安全、合规、高效，如下图：



基础环境(Landing Zone)的设计对企业上云至关重要，它是企业业务在云上的地基，基础环境没设计好就上云，就像没有经过装修直接入住毛坯房一样，会导致很多风险，参考下图类比：



基础环境的设计包括如下 6 个方面：

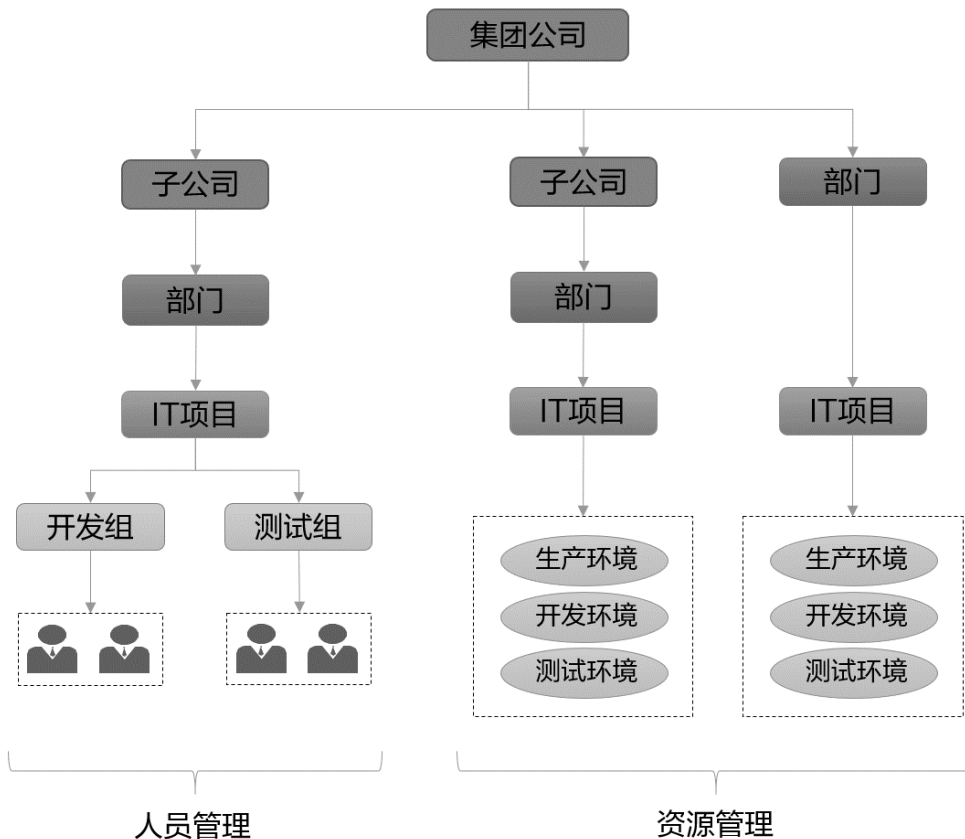


5.2.2 统一账号权限

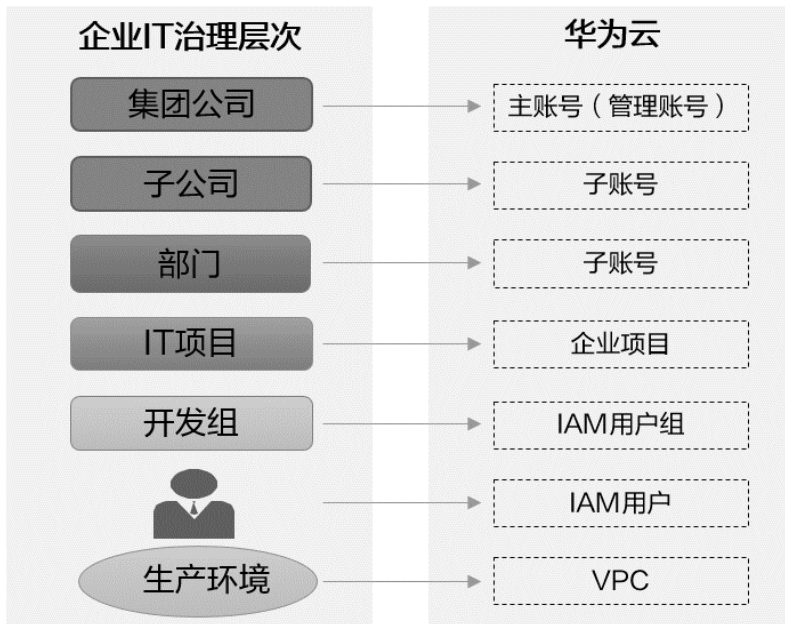
在企业上云之初，首先设计和落地的是身份管理和访问控制方案，然后才能创建云资源。

5.2.2.1 组织映射

企业的 IT 治理架构会受到组织结构的影响，需要将企业的 IT 治理架构映射到云上，下图是一个典型的企业 IT 治理架构：



需要将企业 IT 治理架构中的各个层级逐一映射到华为云上，在华为云上创建相应的对象，推荐的映射关系如下表所示：



只把那些负责管理 IT 项目的组织单元（如部门、分公司等）和管理 IT 资源的用户映射到云上，云上组织映射建议不超过两层，避免 IT 治理的碎片化。不管理 IT 项目的部门或分公司不需要映射到华为云。

5.2.2.2 账号规划

1. 组织

主账号可以创建和管理企业的组织结构、子账号、统一对子账号进行财务管理，并为子账号设置组织策略限定其权限范围。一个组织单元可以包含多个子账号。

2. 账号

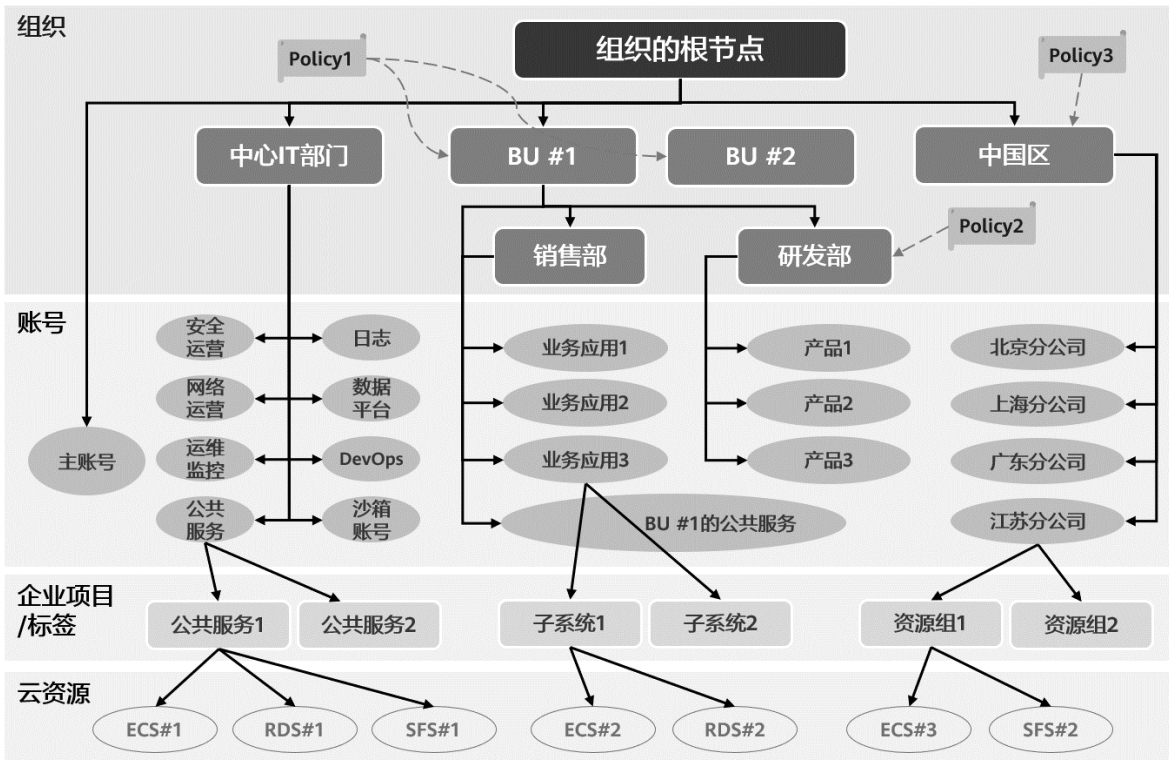
账号是一种资源容器和安全管理边界，也可以作为账单实体。可以按照业务单元、产品、运行环境、成本中心等规划账号。一个账号可以包含多个企业项目。

3. 组织策略

组织策略可以限制子账号的权限上限，相当于安全红线，子 OU 自动继承父 OU 的组织策略，也可以为子 OU 设置额外的组织策略，OU 上的策略针对 OU 下面所有的子账号都生效。

4. 企业项目/标签

企业项目和标签可以对资源进行逻辑分组，并基于分组进行成本分摊、限定授权范围和资源筛选。



中心 IT 部门负责主要的云上治理职能，如果企业规模很大，可以设计不同的 IT 职能账号，参考如下：

账号名称	账号履行的IT职能	责任团队	资源或云服务
网络运营账号	集中部署和管理企业的网络资源，包括网络边界安全防护资源，实现多账号环境下的统一网络资源管理和多账号下VPC网络的互通，尤其需要集中管理面向互联网的出入口和面向线下IDC机房的网络出入口	网络管理团队，安全管理团队	NAT, EIP, VPC, 专线, 云连接, VPN, CFW, WAF, DDoS高防
公共服务账号	集中部署和管理企业的公共资源、服务和应用系统，并共享给其他所有子账号使用	公共服务管理团队	NTP服务器、AD服务器、自建DNS服务器、OBS桶、容器镜像库、协作办公系统等
安全运营账号	作为企业安全运营中心，统一管控整个企业的安全策略、安全规则和安全资源，为其他账号设置安全配置基线，对整个企业的信息安全负责	安全管理团队	统一部署具备跨账号安全管控的服务，如DEW、SCM、VSS等
运维监控账号	统一监控和运维各个子账号下的资源和应用，及时发现预警	运维团队	云堡垒机、Grafana, Prometheus或第三方运维监控系统
日志账号	集中存储其他账号的运行日志、审计日志	日志分析团队，合规审计团队	日志服务LTS、OBS桶、SIEM系统
数据平台账号	集中部署企业的大数据平台，将其他账号的业务数据统一采集到数据平台进行存储、处理和分析	数据处理团队，业务分析团队	数据湖、大数据分析平台、数据接入服务、数据治理平台
DevOps账号	统一管理整个企业的CI/CD流水线，并进行跨账号部署	软件研发团队	DevCloud, 或自建DevOps流水线
沙箱账号	用于进行各种云服务的功能测试、安全策略的测试等	测试团队	按需部署各种需要测试验证的资源和服务

5.2.2.3 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权限管理原则，企业可以参考：

- 相关性原则：**不要把华为云 IAM 作为企业自己的用户管理系统，无需与华为云发生交互的企业员工，就不用在华为云 IAM 上创建相应的用户或用户组。
- 最小化使用根用户原则：**IAM 账号管理员（也叫根用户，与 IAM 账号同名）的权限很大，建议不要直接使用 IAM 账号管理员访问华为云。而是用账号管理员创建一个系统管理组和对应的 IAM 用

户，授予系统管理组必要的管理权限，后面尽量使用系统管理组中的 IAM 用户替代华为云 IAM 账号管理员进行日常管理工作，保护 IAM 账号的安全。

3. **用户组授权原则：**授权时建议按照用户组而不是用户进行授权，用户组的数量和用户的数量相差几个数量级，按照用户组授权可以极大简化授权操作。
4. **最小授权原则：**只授予用户组完成职责所需的最小权限，如果用户组的职责产生变化，应该及时调整用户组的权限。按照最小授权原则，优先在企业项目中对用户组进行授权，如果确实需要针对账号内所有区域或特定区域的所有资源进行统一授权，则可以使用 IAM 项目进行授权，避免在各个企业项目中逐一授权，简化授权操作。
5. **SSO 集成原则：**建议使用企业自有的身份管理系统（如 Azure AD 等）与华为云 IAM 进行联邦身份认证，前者的用户通过 SSO（Single Sign-on）登录到华为云控制台进行操作。企业自有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。主账号和 IT 职能账号需要与企业自己的身份管理系统进行 SSO 集成，业务账号中除了作为逃生通道的系统管理员，没有其他 IAM 用户，所以业务账号通常不需要与 SSO 集成。
6. **运行环境权限管理原则：**生产环境要求安全稳定，其下资源由 IT 管理员进行统一管理；开发测试环境要求灵活，其下资源可由开发测试人员全权管理。

5.2.2.4 合规使用

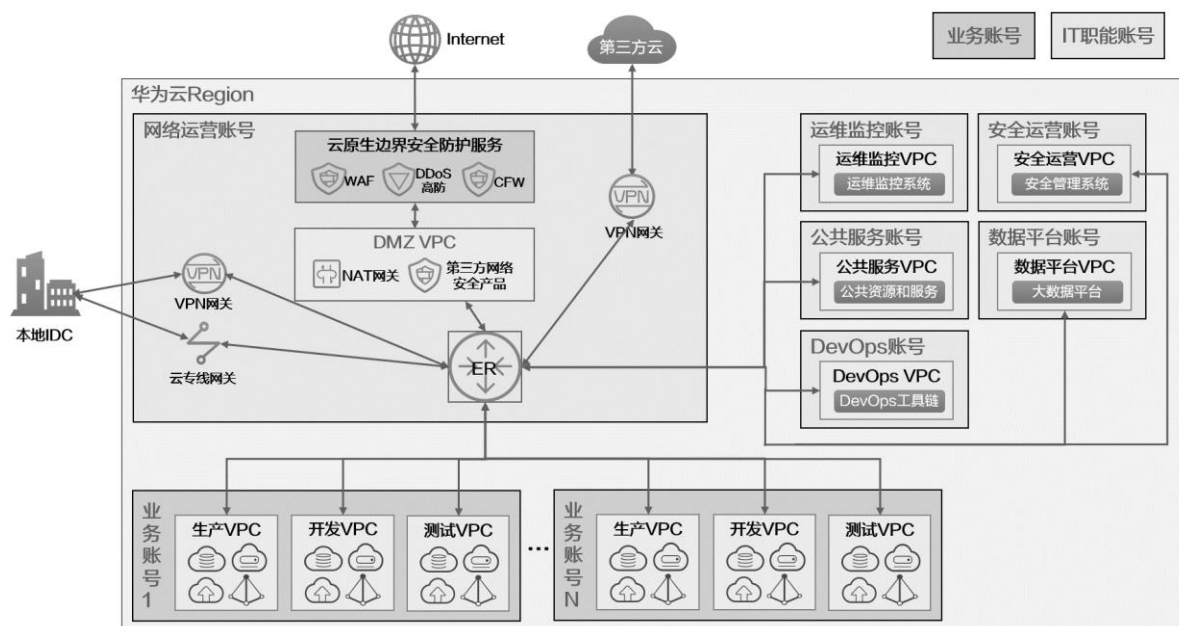
账号和权限的使用要合规，建议企业上云遵循如下原则：

1. **操作日志审计：**开通云审计服务，记录用户对各种云资源的操作，并将这些操作记录进行集中存储、查询，用于支撑安全分析、合规审计和问题定位。在云审计服务 中开启关键操作通知，实时感知高危敏感操作；
2. **资源合规检查：**在云上创建资源合规检查规则，对账号下面的各种云资源进行合规审计，及时处理不合规的情况；
3. **谨慎启用访问密钥：**访问密钥用于 CLI、API 和 SDK 调用，非必须具备，但容易通过代码和配置文件泄露。为了提高安全性，仅对需要进行 CLI、API 和 SDK 访问的用户创建访问密钥，并对这些用户授予最小权限；
4. **不要将密码嵌入代码：**当使用 CLI、API、SDK 访问云服务时，请勿直接将访问密钥嵌入到代码中，而是写到一个本地配置文件中，以避免源代码版本控制系统将访问密钥泄露出去；
5. **高权限用户开启多因素认证：**建议给 IAM 账号以及账号中具备较高权限的 IAM 用户开启 MFA（多因素认证）功能，在用户名和密码之外再额外增加一层保护（MFA 设备的验证码）；
6. **设置强密码策略：**为 IAM 账号及用户设置强密码策略，例如密码最小长度、包含不同类型的字符、密码中同一字符连续出现的最大次数、密码不能与历史密码相同；
7. **开启敏感操作保护：**当用户进行敏感操作时，例如删除资源、生成访问密钥等，需要输入密码和验证码进行验证，避免误操作带来的风险和损失；
8. **定期修改密码：**如果不知道密码或访问密钥已经泄露，定期进行修改可以将不小心泄露的风险降至最低；
9. **清理僵尸用户：**通过用户的“最近一次登录时间”识别长期未登录的用户，及时修改他们的身份凭证，包括修改密码和删除访问密钥；另外建议设置“帐号停用策略”来控制长期未使用的用户到期自动停用。
10. **密码不共享原则：**不要将用户的密码共享给其他人，而是为每个管理或使用华为云资源的人创建一个单独的用户并分配相应的权限。

5.2.3 统一网络管理

5.2.3.1 云上网络设计

云上网络设计是基础环境构建很重要的组成部分，目标是构建稳定可靠、可扩展的网络基础设施，统一管理各类网络资源和相关的网络安全防护资源，确保业务访问安全可靠。整体网络设计通常分为 4 个逻辑分区，即公网接入区、网络互联区、业务部署区、公共和运维管理区。



(一) 公网接入区

在该区主要部署互联网访问相关的网络资源和边界安全防护资源，功能如下：

1. 通过对互联网访问流量进行实时监控，及时发现和清洗 DDoS 攻击流量
2. 提供南北向防火墙功能，包括访问控制、入侵防御、流量分析和日志审计等
3. 防护 Web 应用遭受来自互联网的 SQL 注入、XSS 等应用层攻击
4. 在 DMZ VPC 集中部署和管理面向互联网连接的 NAT-GW、EIP 和 ELB
5. DMZ VPC 统一管理互联网的出入口，作为互联网连接的终结点

(二) 网络互联区

在该区提供云上 VPC 之间、云上云下、云间互联等网络互联服务，功能如下：

1. 云上 VPC 互联，将业务账号和 IT 职能账号的 VPC 网络进行互联
2. 云上云下互联，将本地数据中心和办公区接入到华为云
3. 云间互联，将华为云与第三方云进行网络互联

4. 多 Region 互联，将部署在华为云多个 Region 的业务系统进行互联
5. 提供东西向防火墙功能，集中控制东西向网络的安全访问策略

(三) 业务部署区

该区主要部署各种业务系统，功能如下：

1. 为各个业务系统提供 IaaS 资源、PaaS 资源或自建中间件
2. 在业务账号内为不同的业务系统提供隔离的 VPC
3. 按照应用架构分层在每个 VPC 下面再划分应用、数据等子网

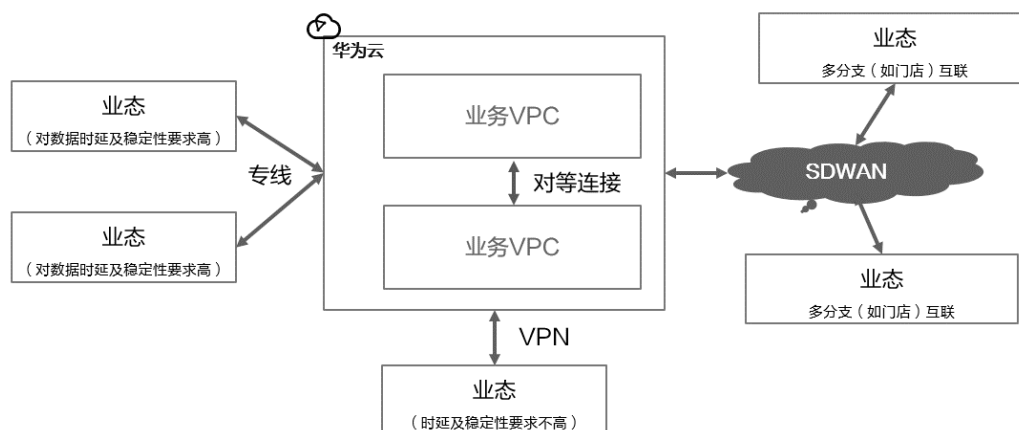
(四) 公共和运维管理区

该区主要部署公共服务和 IT 管理系统，功能如下：

1. 公共服务，如 DNS 转发器、虚拟机镜像库、容器镜像库等
2. 集中的安全运营管理系统
3. 集中的运维监控系统，补丁更新服务器，堡垒机等
4. 集中的数据管理和分析平台
5. 集中的 DevOps 流水线

5.2.3.2 网络互联建议

当企业业务从 IDC 迁移到云上后，之前与 IDC 互联的其他业务或第三方的网络也需要变更，需要设计新的网络互联方案，确保其他业务或第三方与企业的云上业务互联正常。以某大型零售电商平台上云为例，其与其他业态或第三方网络互联方式有三种，如下图：



1. 专线连接：对数据时延及稳定性要求高的业态，通过专线直接与云上网络互通。
2. VPN 连接：对延迟和带宽要求不高的业务，通过 VPN 实现与云上网络互通。
3. SD-WAN 连接：对于多分支互联场景，通过 SD-WAN 实现与云上网络互通。

在进行网络互联规划时，需要根据具体的业务需求和预算限制，选择适合的云上互联方案，通常需要考虑以下因素：

1. 业务需求和性能要求：根据业务需求评估对互联网络的性能要求，包括带宽、延迟、可靠性等。不同业务场景可能对这些性能指标有不同的要求。
2. 安全性需求：确保网络互联的安全性，包括数据加密、访问控制、防火墙策略和身份验证等。根据业务需求和合规要求，选择合适的安全措施和技术。
3. 可扩展性和弹性：考虑未来业务发展的需求，选择具备良好扩展性和弹性的互联方案。例如，是否能够轻松增加带宽，支持多地点的互连需求等。
4. 成本效益：评估不同互联方案的成本效益，包括建设成本、运营成本、网络租用费用等。根据企业预算和长期投资计划，选择适合的方案。
5. 管理和监控：考虑互联方案的管理和监控需求，包括对连接状态、性能和故障的实时监控。确保能够及时诊断和解决网络问题，提供可靠的服务。

5.2.3.3 迁移网络设计

在整体网络设计时，我们还要统一考虑迁移网络选择，我们要基于应用的上云需求，从如下几个维度，综合考虑并选择最合适的迁移网络，这些维度包括：

- 1) 网络费用
- 2) 迁移带宽
- 3) 数据安全性
- 4) 网络时延
- 5) 网络稳定性
- 6) 网络灵活性

以下是常见的迁移网络类型的优缺点，供迁移网络选择时参考：

迁移网络类型	优点	缺点
专线	1、性能稳定：时延低至毫秒级 2、带宽选择范围可达几十 Gbit/s 3、数据传输安全性高	1、成本高：一般是包年包月 2、源端和目的端私网 IP 地址不能重叠 3、开通时间长：一般需提前 1 个月申请
VPN	1、组网灵活，随时搭建 2、稳定性较好，安全性较好 3、成本适中：公网费用+VPN 费用	1、时延较高 2、源端和目的端私网 IP 地址不能重叠

公网 IP	1、支持源端和目的端私网 IP 一致的情况下实施迁移 2、带宽任意选择 (Mbit/s ~ Gbit/s) 3、即买即用, 快速绑定 4、成本低	1、稳定性差: 带宽可能无法全部利用, 迁移速率相对较慢 2、公网传输数据有泄漏风险
线下 (数据快递 DES)	1、容量大 (单次 50~120TB) 2、成本最低	1、迁移方式不够灵活, 一般用于历史数据的迁移, 增量迁移局限性较大

5.2.3.4 迁移带宽评估

迁移带宽主要跟如下三个因素有关:

1. 迁移的数据总量
2. 迁移的总周期
3. 应用是否有跨云访问, 以及跨云访问的带宽预测

可以基于这三个维度进行迁移带宽的评估, 比如:

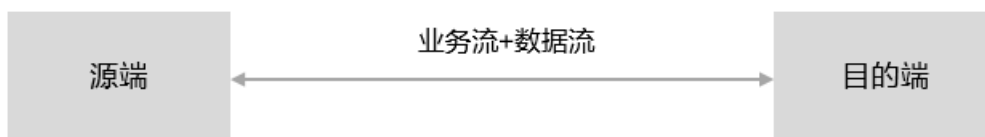
上云迁移带宽评估工具				
	输入项	输入子项	输入值	备注
输入	源端数据量	应用层主机数据 (GB)	138000	
		中间件层数据 (GB)	500	
		数据库数据量 (GB)	1000	
		对象存储数据量 (GB)	1000	
		文件存储数据量 (GB)	0	
		大数据数据量 (GB)	0	
	迁移周期	期望多久迁移完 (天)	90	指整个迁移周期 (从调研开始到全部切换完成)
带宽利用率	带宽利用率 (专线或互联网)	80%	专线带宽利用率默认80%, 可以不改	
应用跨云访问带宽	应用跨专线访问应用/中间件/数据库的最大带宽 (Mb/s)	0	如果选择先切应用层后切数据层的切换方案, 或者分批切换后应用有跨云访问的需求, 则本项要填写应用实际跨云访问的带宽 (需要与客户一起评估), 否则填写0	
输出	迁移带宽 (专线/互联网) 评估 (Mb/s)		1000	

5.2.3.5 迁移专线建议

迁移专线的选择跟成本、数据量、业务类型、业务重要性都有关系, 可以根据企业的实际情况选择最合适的专线方案, 上云迁移期间常见的专线部署方案有如下四种, 请参考:

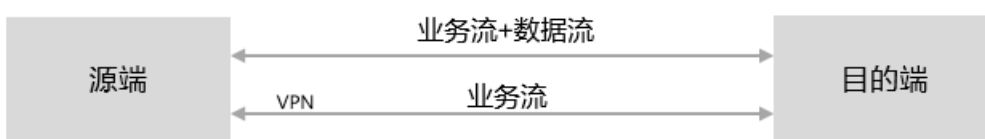
1. 方案一、单根专线

- 受成本限制，源端和目的端只拉通一根专线
- 业务流和数据流(应用数据和大数据)共用一根专线



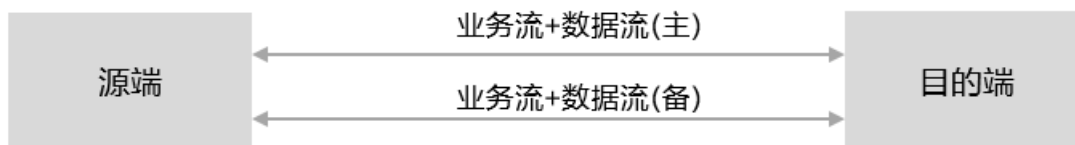
2. 方案二、单根专线+VPN

- 源端和目的端只拉通一根专线，业务流和数据流共同使用
- VPN 作为备用，专线中断时候只作为业务交互使用



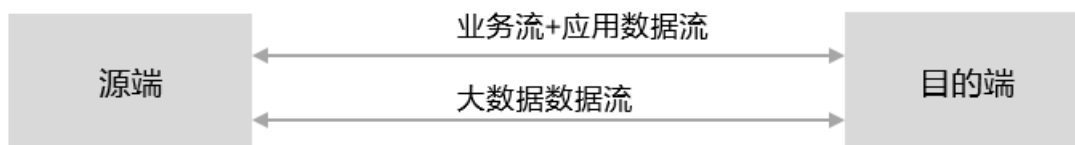
3. 方案三、两根主备专线

- 数据流和业务流(应用跨专线调用)共用一根专线
- 源端和目的端拉通 2 根相同规格的专线作为主备，防止专线意外中断导致业务和迁移受阻



4. 方案四、一根迁移业务专线，一根迁移大数据专线

- 源端有大数据，且数据量巨大，切换前需要长时间从源端抽数据双跑，单独占一根专线
- 业务和业务数据迁移使用另一根专线



5.2.4 统一安全管控

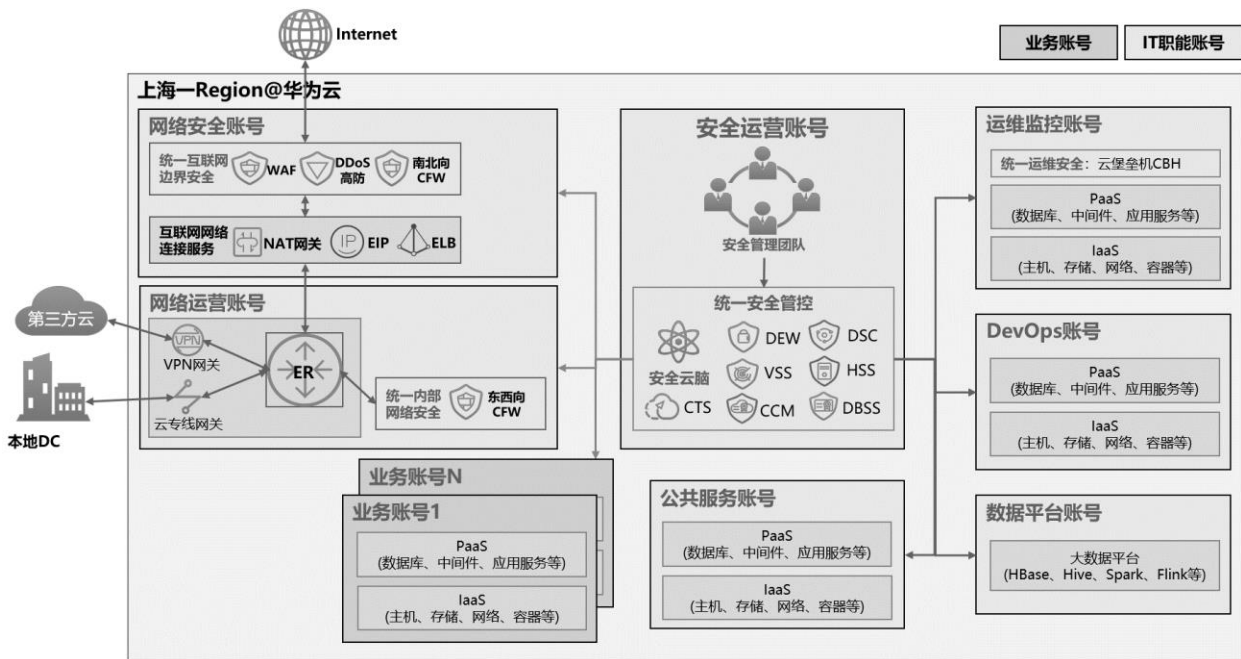
5.2.4.1 整体安全设计

华为云根据自身安全实践和成功交付数百个项目的经验，提炼如下安全设计原则：

1. **基于合规要求确定安全方案：**安全是一项系统工程，从建设成本和方案上看有较大的弹性空间。企业应基于业务的合规要求（如安全等级保护级别）确定安全方案。

2. **基于风险识别加固安全方案：**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。
3. **建立纵深防御机制：**建立覆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、负载均衡、云存储、ECS 实例、操作系统、应用程序配置和代码等。
4. **数据传输和存储安全：**基于敏感级别进行数据分类，针对敏感数据的传输使用 TLS 等方式进行保护，敏感数据存储时要进行加密并设置访问控制权限。
5. **人和数据隔离：**利用工具和管理机制减少人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。
6. **最小化授权：**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职责所需的最小权限，如果职责产生变化，应该及时调整权限。
7. **确保操作的可追溯性：**完整记录所有用户和应用程序对云上资源、数据和应用的操作访问日志，出现安全问题时可以基于日志进行追溯。
8. **云原生安全防护：**云服务商提供了丰富的云原生安全服务（比如 WAF、DDoS 高防、云防火墙、密钥管理等）。这些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。
9. **木桶原则：**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。

基于如上设计原则，我们建议华为云上的整体安全架构参考如下：



企业可以按需购买并部署对应的安全云服务以保障业务的安全，通过安全云脑服务实现安全资源的跨账号统一管理。安全云脑服务能实现安全资源、日志、策略的统一管理，同时支持用户自定义的安全编排、自动化和响应（Security Orchestration, Automation and Response, SOAR）。客户只需要在安全云脑服务上进行配置，即可以建立和其他账号的关联关系，管理其他账号的合规安全、数据安全、负载安全和应用安全。

5.2.4.2 应用安全设计

部署在云上的应用系统的安全诉求主要有三类：

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

应用的安全性主要从区域边界、网络通信、计算环境和管理中心这四个角度进行考虑：

1. 区域边界

- 边界防护：未经授权的访问、恶意攻击、数据泄露；
- 访问控制：内部外部的网络访问控制策略的配置；
- 入侵防范：防范已知及未知的病毒、恶意软件及外部黑客的威胁；
- 安全审计：记录系统及用户的网络活动和安全事件。

2. 网络通信

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

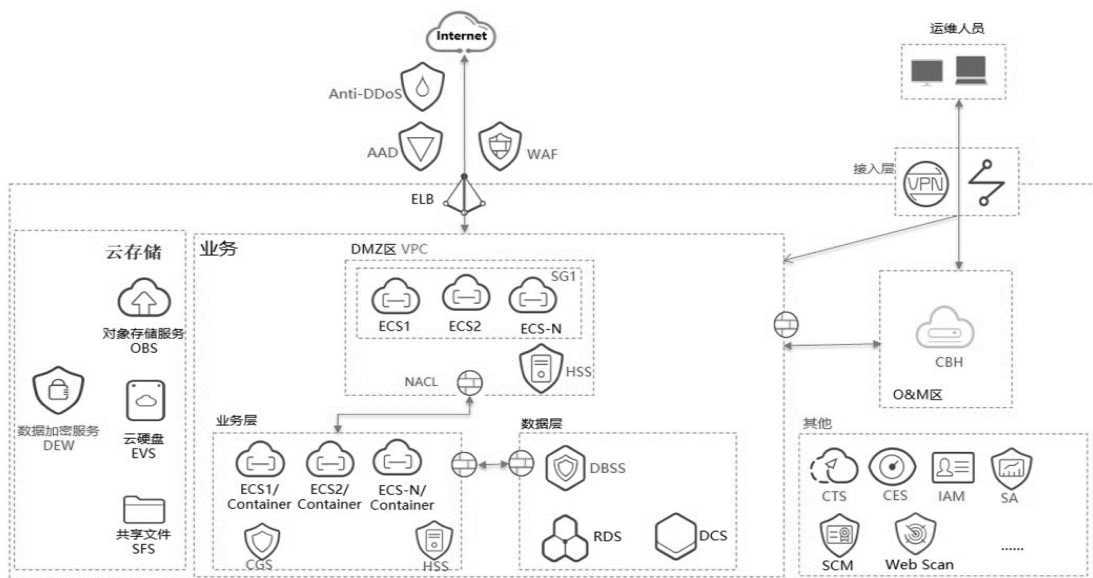
3. 计算环境

- 身份鉴别：密码复杂性及定期修改、MFA、SSO；
- 访问控制：用户权限管理、最小化权限、冗余账号清除；
- 安全审计：用户行为审计及审计记录、审计进程的保护；
- 入侵防范：检测非授权访问、创建非授权端口及漏洞利用；
- 恶意代码防范：恶意代码攻击识别与防范及最新的情报获取；
- 镜像和容器安全：镜像及容器安全配置，确保容器之间的隔离和安全运行，防止容器逃逸等攻击；
- 数据加密和数据隔离：对敏感数据进行加密，确保数据在传输和存储过程中得到保护。实施数据隔离策略，限制数据的访问范围；
- 剩余信息保护：删除业务应用数据时，云存储中所有副本删除。

4. 管理中心

- 资产管理：数据资产、网络设备、主机系统等，确保各个部分资产的保护情况；
- 权限管理：严格的权限控制机制，只有经授权才能进行相关操作，限制未经授权的访问；
- 自动化与集成：自动化的运维和集成，方便与其他安全设备和系统集成，形成更加完善的安全防护体系；
- 合规性与标准检测：管理中心应符合相关的法规和标准要求，对系统进行整体的安全评估和检测；
- 集中管控：统一管理界面，能进行集中式的配置、监控和管理，减少管理复杂性。

应用安全要基于整体的安全架构进行适配，下图是应用在云上的安全架构参考：



应用可能面临的三大安全风险：

1. 如果业务系统无备份，则数据有丢失风险
2. 无主机安全，存在主机遭受挖矿、攻击等风险
3. 无监控，存在业务节点异常无法及时感知的风险

如果服务器承载以下类型业务，建议尽量开通使用 ECS 三大护盾（云服务器备份 CSBS、云监控 CES、企业主机安全 HSS）增值服务：

1. 承载“关键业务场景”的云服务器：直接影响企业经营生产，对中断容忍度低。
2. 承载“核心数据库”的云服务器：业务持续运转依赖于对数据的连续读取。
3. 存储“关键企业数据”的云服务器：硬盘数据包含是企业关键经营数据，对数据安全诉求高。
4. 存储“高保密数据”的云服务器：机密性数据需要额外提供安全防控保障。

5.2.5 统一资源治理

资源治理包含资源共享、资源标签、资源命名规范、资源管理、配额管理、镜像管理和服务控制策略等。

5.2.5.1 资源治理原则

华为云基于大量成功交付的项目，总结提炼了以下资源治理原则：

1. **公共资源集中部署**：公共资源、共享资源集中部署在公共服务账号中，由管理员统一规划、配置和管理，按需共享给其他 IT 职能账号和业务账号使用，不在各个子账号中分别部署和管理。
2. **网络资源集中部署**：网络连接资源（如 VPN、DC、CC、ER）集中部署在网络运营账号中，互联网边界安全防护的资源（如 WAF、DDoS 高防、南北向防火墙）集中部署在网络安全账号中，这些资源由相应的管理员实行专业化管理。
3. **业务和管理资源分开**：运维监控、安全合规等管理类服务，部署在独立的 IT 职能账号中，由相应的管理员实行专业化管理，该类账号内不要承载业务系统，通常不需要部署 IaaS 和 PaaS 资源，除非需要用来部署第三方运维监控系统或安全管理系统。
4. **资源分组管理**：在单个账号内，使用企业项目而不是 IAM 项目进行资源的分组和管理，企业项目可以跨区域管理资源，支持资源的迁入迁出、项目级授权管理、资源的成本核算，比 IAM 项目更能满足企业的项目管理需求。
5. **资源标签管理**：对账号内的资源，建议可以从分类搜索筛选、成本分析、自动化操作、分类监控等维度，提前规划好标签分类、键和值。标签非常灵活，可以对不同资源做一个或多个标记，可以极大提升资源管理的效率。
6. **资源利用率分析**：定期（月度、季度、年度）统计分析各个账号的资源利用率，及时发现资源空转、资源利用率低的情况，并及时删除空转资源、进行资源整合。
7. **资源配额监控**：持续监控各个子账号的资源配额使用情况，如果发现当前资源数量接近配额上限，需要尽快提交扩容配额的工单。
8. **关键应用反亲和部署**：对于重要应用，AZ 内要进行跨主机组或跨机柜的反亲和部署，通过物理节点的反亲和来保证 AZ 内的高可用。

5.2.5.2 资源共享

对一个企业来讲，网络连接、镜像等基础和公共资源应该统一规划和配置，由网络管理员或公共服务管理员集中控制和管理，并根据各个子账号的需求，分配或共享给这些子账号使用。资源的跨账号共享为企业带来以下好处：

1. **提升资源安全性：**对共享资源设置一致的策略和权限，确保企业范围内遵守相同的安全规则。
2. **提升管理效率：**通过集中配置和管理共享资源，可以大幅提升资源管理效率。
3. **减少资源消耗：**通过共享资源，各账号就不用独立创建同类资源。

共享资源根据管理权归属的不同部署在不同的账号中，由相应的管理员统一管控。通常情况下，网络连接类基础资源部署在网络运营账号中，互联网边界安全防护资源部署在网络安全账号中，其他如镜像等公共资源在公共服务账号中统一管理。

注意：在跨账号共享资源时，需要确保遵守适用的法规和合规要求，并进行相应的合规性评估，避免可能带来的数据隐私和安全审计方面的风险。

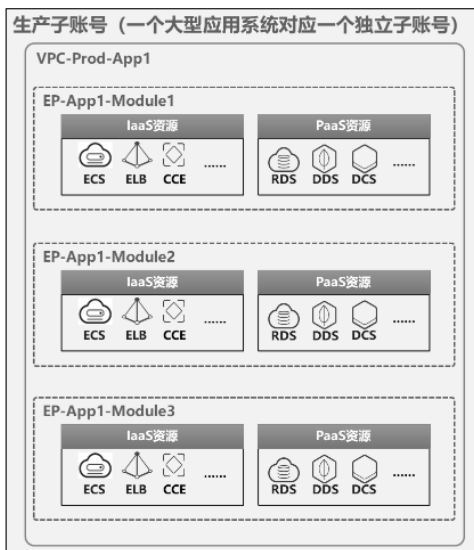
5.2.5.3 资源合规

华为云建议从如下两个维度进行云上资源的合规管理。

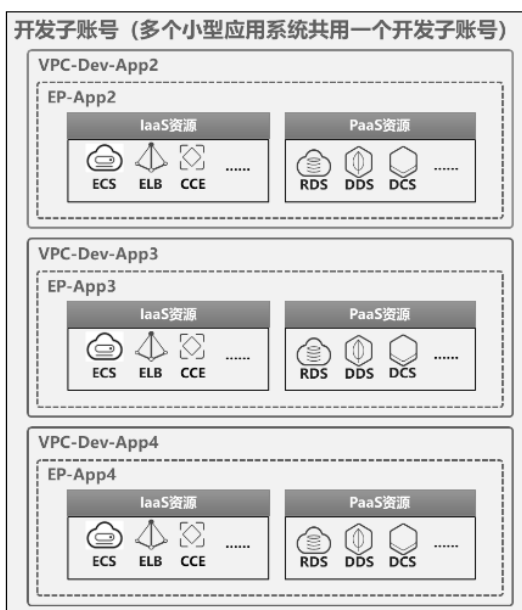
1. **资源配置合规检查：**云资源分布在多个 IT 职能账号和大量业务账号中，需要对这些账号的资源合规检查规则进行统一配置，保证合规检测的一致性和及时性，确保云资源满足企业、行业或者国家的安全要求。华为云的 RMS (Resource Management Service) 服务提供资源合规检查功能，帮助用户快速创建一组合规规则，用于评估资源是否满足合规要求。
2. **资源变更记录检查：**企业需要对各账号的资源使用情况进行定期的查看和审计。各账号的资源快照需要集中存储，便于企业审计人员定期查看及工具化分析。RMS 服务还提供资源记录器的功能，启用该功能后，RMS 会定期（每隔 24 小时）对资源配置进行快照并存储。通过该功能，企业可以针对各账号的当前及历史资源使用情况进行定期审计和分析，确保各个账号对资源的使用符合企业要求，并可根据资源变更记录进行问题排查。

5.2.5.4 资源分组

企业项目 (Enterprise Project, 缩写为 EP) 提供了账号内逻辑资源分组的能力，为账号内归属不同企业项目的资源进行权限控制、成本归集等能力。客户可以按照业务系统或者子系统映射到企业项目，不同的业务系统或子系统的资源归属到不同的企业项目。需要注意的是一个资源只能归属一个企业项目。针对一个大型应用独占的业务账号，我们推荐将这个大型应用的每个子系统、微服务或者功能模块的资源归集到一个企业项目，如下图所示：



针对多个小型应用共享的业务账号，为了做好业务系统的隔离，我们推荐将每个业务系统部署到不同的VPC，并将其资源归集到一个独立的企业项目，如下图所示：



利用企业项目对业务账号内的资源按照业务系统或子系统进行逻辑分组之后，客户可以进一步基于企业项目进行细粒度授权和成本归集。

1. **基于企业项目的权限控制：**当多个业务系统共享一个开发或者测试子账号时，需要将某个业务系统的资源委托给 DevOps 账号的应用开发组或应用测试组进行全权管理，在该子账号中设置委托权限时，就可以将授权范围限定到对应的业务系统所在的企业项目，如上图中的 EP-App2、EP-App3、EP-App4。
2. **基于企业项目的成本归集：**财务管理员可以在成本中心按照企业项目统计和查看每个业务账号下生产环境、开发环境和测试环境所消耗的成本。针对多个小型应用共享的业务账号，还可以分别统计每个运行环境的每个应用所消耗的成本。

5.2.5.5 资源标签

华为云的标签是由用户定义的键和值组成，标签可以更灵活地帮助用户管理资源，包括识别资源、搜索资源和基于标签进行成本分类等。

在为华为云资源创建标签策略时，华为云有以下建议：

1. 请勿在标签中存储用户身份信息或其他机密或敏感信息
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. 需要提前规划用于多种用途的标签准则，如管理资源访问控制、成本跟踪、自动化和归属组织

(一) 标签命名限制和要求

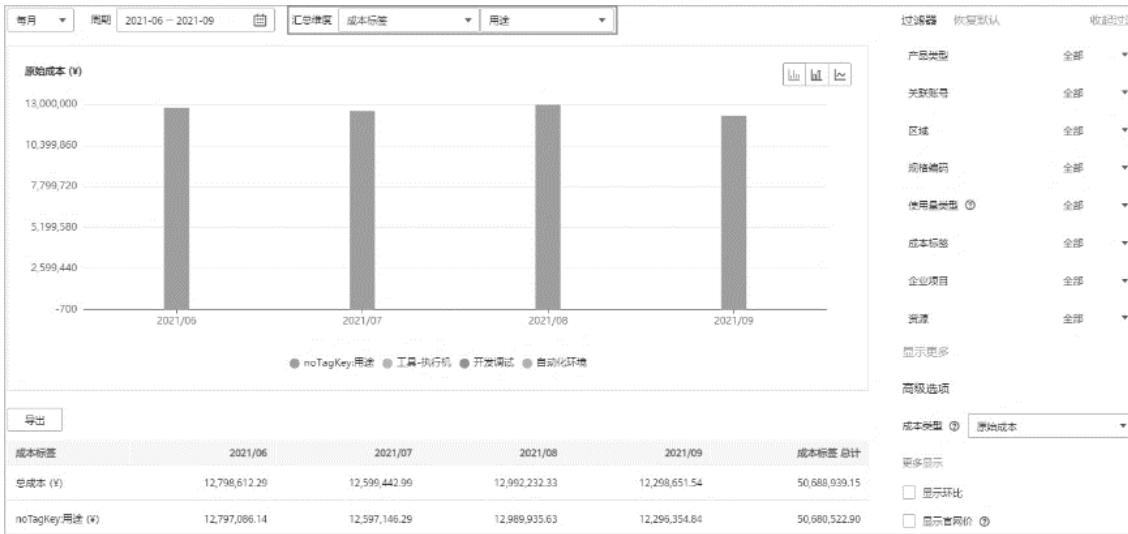
1. 每个资源最多可以有 20 个用户创建的标签。注意：以 `_sys_` 开头的系统创建标签将保留供华为云系统使用，并且不计入此限制
2. 对于每个资源，每个标签键都必须是唯一的，每个标签键只能有一个值
3. 标签键必须包含 1 到 128 个 Unicode 字符，并且以 UTF-8 格式表示
4. 标签值必须包含 0 到 255 个 Unicode 字符，并且以 UTF-8 格式表示
5. 标签键和值区分大小写，建议利用标签策略在所有资源类型中一致地实施该策略。例如，决定是使用 `HuaweiCloud`、`huaweicloud` 还是 `Huaweicloud`，应保持相同的规则。

(二) 常见的标签策略

1. **资源治理标签：**用户可以配置标签来与资源一起显示，并且可以按标签进行搜索和筛选。使用 TMS 服务，用户可以按资源类型和 Region 过滤资源，给多个资源批量打标签。
2. **成本标签：**华为云的成本中心可让用户在使用标签标识和管理资源的同时，还可以将标签激活为成本标签来归集成本。成本标签可以应用在成本分析和预算管理。
3. **自动化标签：**该类标签通常用于在自动化任务时做资源过滤筛选。自动化标签用于选择加入或退出自动化任务，或识别要存档、更新或删除的资源的特定版本。例如，用户需要在非工作时间关闭一些云资源以降低成本，这时候可以给这些云资源打上标签标明需要被定时关闭。

(三) 通过标签分析成本

企业可以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。在此之前，需要先进行成本标签激活，具体步骤请参考 https://support.huaweicloud.com/usermanual-cost/costcenter_000005_02.html，然后进入“成本分析”，通过成本标签进行成本数据汇总和过滤，如下所示。



5.2.5.6 资源命名

命名规范对高效管理云资源非常重要，制定标准和一致的命名规范，能使客户在云上资源的成本分析、自动化、安全控制等方面的管理更加清晰和便捷。命名原则如下：

1. 命名规则是可扩展的
2. 确保在一定范围内的命名是唯一的
3. 通过资源命名便于分类，譬如为监控、安全控制等提供可见性
4. 命名字段定义如下：
 - **Logical area:** access (公网接入区)、connection (骨干互联区)、business (业务应用部署区)、manage(公共和管理服务部署区)
 - **appname:** newbie、NBMS、CCM、DCC、PULS 等
 - **env:** dev、uat、stage、prod、dmz、inspection 等
 - **usage:** app、CCE、web、db、uplink 等

(一) 计算资源命名规范：

华为云资源	资源命名规范	示例
ECS instance	ecs-{logical area}-{appname}-{env}-{region}	ecs-business-adv-dev-shanghai1
IMS image	img-{logical area}-{appname}-{env}-{usage}-{region}	img-business-adv-dev-db-shanghai1
EVS volume	disk-{logical area}-{appname}-{env}-{usage}-{region}	disk-business-adv-dev-k8s-shanghai1

华为云资源	资源命名规范	示例
EVS snapshot	ss-{logical area}-{appname}-{env}-{usage}-{region}	ss-business-adv-dev-db-shanghai1
AutoScaling	as-{appname}-{env}-{usage}-{region}	as-adv-dev-web-shanghai1

(二) 存储资源命名规范:

华为云资源	资源命名规范	示例
OBS bucket	obs-{logical area}-{appname}-{env}-{region}	obs-business-adv-dev-shanghai1

(三) 网络资源命名规范:

华为云资源	资源命名规范	示例
VPC	vpc-{logical area}-{appname}-{env}-{region}	vpc-business-adv-dev-shanghai1
Subnet	sn-{logical area}-{appname}-{env}-{usage}-{region}	sn-business-adv-dev-db-shanghai1
ACL	acl-{logical area}-{appname}-{env}-{usage}-{region}	acl-business-adv-dev-k8s-shanghai1
安全组	sg-{logical area}-{appname}-{env}-{usage}-{region}	sg-business-adv-dev-db-shanghai1
ELB	elb-{appname}-{env}-{usage}-{region}	elb-adv-dev-web-shanghai1
EIP	eip-{appname}-{env}-{usage}-{region}	eip-adv-dev-web-shanghai1
NAT	nat-{appname}-{env}-{usage}-{region}	nat-adv-dev-web-shanghai1

5.2.5.7 资源配额

每个账号中的每种服务资源都有配额，当账号内开通的资源数量达到配额后，将无法开通新的资源实例。企业要继续监控账号的资源配额使用情况，提前识别容量风险，如果发现当前资源数量接近配额上限，需要尽快提交扩容配额的工单。资源治理人员可以通过优化顾问服务中提供的服务配额检查功能，做定期的配额情况巡检，查看账号内每个服务的配额以及使用情况。

1. 查看资源配额：登录管理控制台，在页面右上角，选择“资源 > 我的配额”。系统进入“服务配额”页面。



2. 可以在“服务配额”页面，查看各项资源的总配额及使用情况。

服务	资源类型	已用配额	总配额
弹性云服务器 ECS	实例数	3	200
	核心数	17	800
	RAM容量 (MB)	33,792	1,638,400
镜像服务 IMS	镜像	1	50
	镜像数量	0	400
函数工作流 FunctionGraph	代码存储(MB)	0	10,240
	工作流数	0	512
	弹性伸缩 AS	伸缩组	0
	伸缩配置	0	100
	m5	0	5

3. 如果当前配额不能满足业务要求，可以点击“申请扩大配额”，就会进入到申请工单界面，通过问题描述，提交工单，让华为云后台管理员更改配额。



5.2.5.8 资源控制

企业需要根据各种安全管理要求对各账号的行为做管控，确保各账号无法执行违反要求的行为。为此华为云提供了组织策略，也叫服务控制策略，可以对整个组织进行权限管控。服务控制策略是可继承的，附加在一个组织单元上的策略，将对其所有下层组织单元及关联账号生效。

在多账号场景下，企业可以在主账号中对整个组织，或指定的业务单元做集中的策略控制。强烈建议用户不要在没有彻底测试服务控制策略对账户影响的情况下将服务控制策略附加到整个组织。用户可以先创建一个测试组织，将服务控制策略附加到该测试组织上进行充分测试验证，然后再把对应账号逐个或小批量移入该组织，确保该策略不会对业务运行产生重大影响。以下是几个典型的服务控制策略。

1. 网络变更控制

禁止成员账号进行网络变更，包括 VPC、网络、子网、带宽、IP、ACL、安全组的创建、变更、删除等操作。成员账号不能修改已有的网络配置，无法在成员账号中创建公网 NAT 网关和弹性公网 IP 等。在完成所有网络配置后，建议应用该策略。

2. 监控配置控制

禁止成员账号用户删除运维配置，包括监控面板、告警等操作。在运维管理员完成系统的运维配置后，建议应用该策略。

3. RMS 配置控制

禁止成员账号修改 RMS 的配置，包括合规规则，资源记录器等操作。成员账号不能修改合规规则，无法关闭资源记录器。在完成所有 RMS 配置后，建议应用该策略。

4. MTD 配置控制

禁止成员账号进行 MTD 相关操作。在完成所有 MTD 检测配置后，建议应用该策略。

5. 禁止删除日志

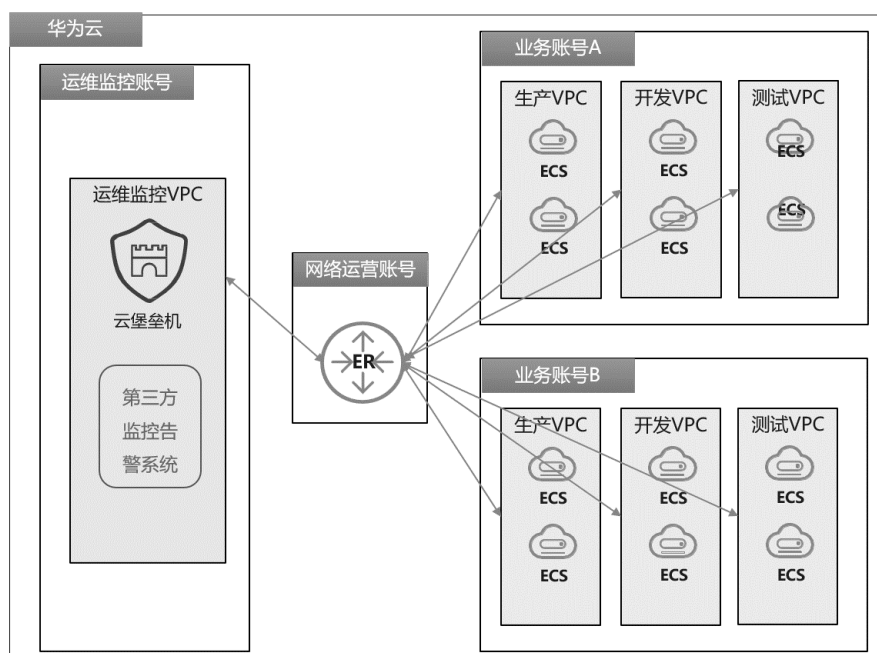
禁止成员账号删除日志，包括 CTS、LTS、VPC 流日志等。在完成所有日志配置后，建议在整个组织应用该策略。

5.2.6 统一运维监控

5.2.6.1 统一监控及告警

云平台提供了许多自带的运维工具，可以提供资源的监控能力，对计算、存储、网络、数据库等云服务进行监控，运维人员可以配置相应的告警阈值和告警通知。

除了云平台自带的工具外，企业还可以使用第三方工具进行云上的统一运维。比如，如果企业有自己的运维监控平台，可以通过 API 方式与云平台对接。企业可以在运维监控账号内集中部署企业自己的或第三方的运维监控系统，对所有业务成员账号下的资源进行集中监控和统一告警管理。

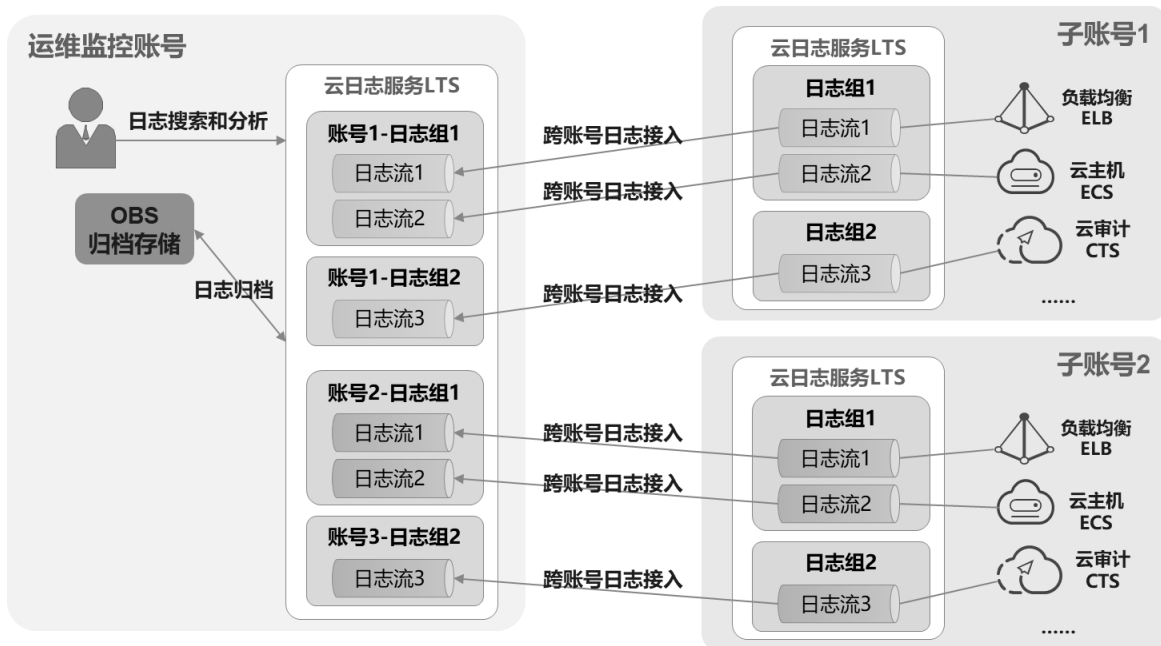


5.2.6.2 统一日志存储

华为云日志服务 LTS 可以将不同账号下的云服务日志、用户应用程序日志统一收集到运维监控账号中。

(一) 统一日志收集

企业可以在每个子账号中收集应用程序和云服务的日志，然后通过华为云提供的“跨账号接入-日志流映射”功能，将子账号中的所有日志接入到运维监控账号的 LTS 服务中进行集中存储、搜索和分析。在运维监控账号 LTS 存储了一段时间的日志数据也可以归档存储到更低成本的 OBS 中。

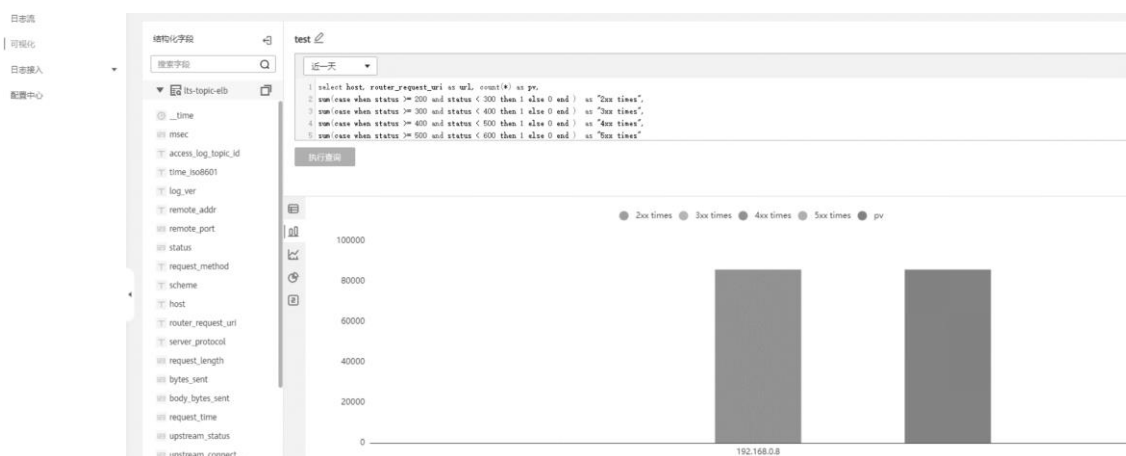


各子账号中收集日志后，需要将子账号中的日志集中到运维监控账号。为了实现这一点，需要在子账号的 IAM 服务中创建委托，被委托方是运维监控账号，并授予日志账号“LTS FullAccess”权限。创建委托后，在运维监控账号中就可以配置“跨账号接入-日志流映射”，将子账号中的日志流接入到运维监控账号中。在一个账号下日志组和日志流的数量是有限制的，建议**运维监控账号的日志组名称和子账号中相同，日志流名称添加“子账号名_”前缀**，这样可以快速明确运维监控账号日志流和子账号日志流的对应关系。

1. **日志组织方式：**可以将同一大类的云服务的日志放到同一个日志组中，例如安全相关服务的日志都放在 security 日志组中，网络相关服务的日志都放在 network 日志组中。同一大类下不同的云服务可以放到独立的日志流中，例如可以在 security 日志组中创建 WAF 日志流用来存放 WAF 服务的日志，在 network 日志组中创建 ELB 日志流用来存放 ELB 服务的日志。
2. **日志存储时间：**子账号中的日志存储时间可以设置为 90 天，这样方便每个子账号的用户搜索日志，用于各种业务场景下的运维运营工作。运维监控账号中的日志存储时间可以设置为 180 天，进行日志的集中审计，这样符合中国三级安全等保的合规性要求。
3. **日志转储到 OBS：**每个账号能创建的 OBS 桶的数量有限，企业可以根据自己的业务需要创建一个或多个桶。在运维监控账号中，设置日志流转储到 OBS，自定义转储路径建议设置为“/日志组名

称/日志流名称/%Y/%m/%d/%H/%m”，转储周期 30 分钟。转储到 OBS 中的好处是可以将日志归档，实现长期存储并节省成本。

- 应用日志采集：**对于应用日志，华为云建议使用 ICAgent 收集，应用日志一般包括应用程序日志、客户自建网关日志、操作系统日志、容器日志等，这些日志会写入本地系统磁盘，可以通过 ICAgent 将这些日志从所在主机发送到华为云日志服务。对于华为云上的 CCE 容器应用，在控制台打开日志采集开关即可收集日志到 LTS 服务。对于自建 K8S 集群，可以使用 LTS 服务提供的 CRD 方式采集原生 K8S 容器日志，具体步骤请参考 https://support.huaweicloud.com/usermanual-lts/lts_04_1110.html
- 日志分析：**日志统一收集到日志服务后，企业的日志分析团队就可以使用关键词来搜索过滤日志，可以使用 SQL 语法来分析日志，并生成可视化图表（表格、柱状图、饼图、折线图等）。企业可以将图表组合到仪表盘中，为业务团队提供运营分析。支持提取仪表盘为模板，为不同的日志流提供开箱即用的分析能力。日志分析团队还可以基于关键词或者是 SQL 语句创建告警规则，用来监控系统的运行情况，可以通过短信、邮件、企业微信、钉钉等多种方式发送告警。

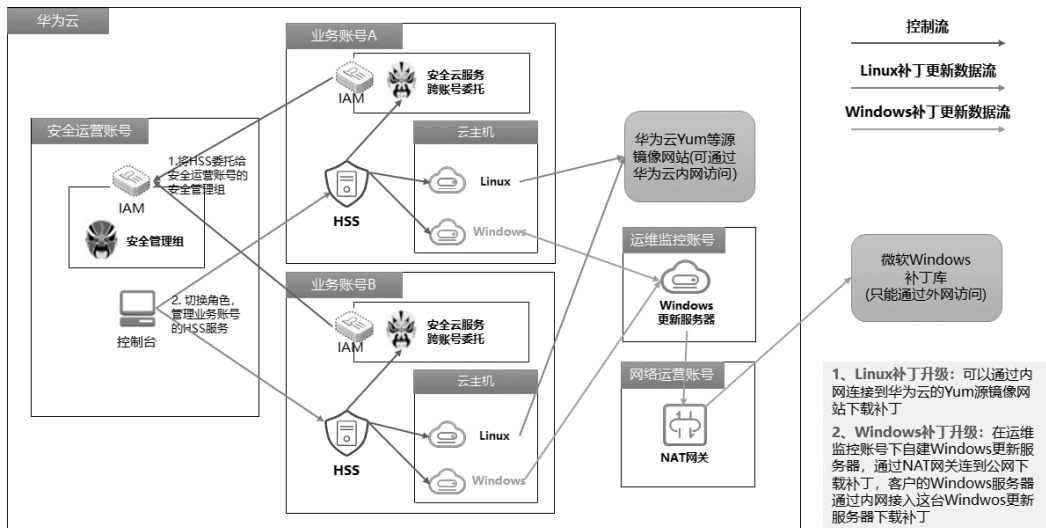


6. 集成到第三方 SIEM 系统

如果企业采用了统一的 SIEM（安全信息和事件管理）系统，可以将运维监控账号中集中存储的 LTS 日志发送到外部 SIEM 系统进行集中的安全事件和风险分析。

5.2.6.3 统一补丁更新

华为云使用企业主机安全服务（Host Security Service，HSS）实现操作系统（Linux，Windows）的漏洞检查和补丁更新。漏洞检查分为定时扫描和手工扫描。扫描出漏洞需要在 HSS Console 上手工操作修复。运维人员先登录到华为云安全运营账号下，再通过账号委托方式切换到各个业务账号，到 HSS 下做操作系统统一补丁更新。



5.2.7 统一财务管理

企业的主账号要对其下关联的子账号进行统一财务管理，包括：

1. **主子账号关联：**主账号可以通过创建一个华为云账号并与之关联，或者邀请一个现有的华为云账号与之关联。同时主账号可以根据公司业务架构在企业中心创建层级式的组织单元，子账号可以从属与某个组织单元，也可以从一个组织单元变更到另一个组织单元。

2. **账号资金管理：**主/子账号的资金管理有以下两种方式：

第一种：主账号充值后，可以划拨现金、代金券给子账号用于资源的开通。子账号也可以通过自主充值后，进行资源的开通。

第二种：主账号是后付费用户，有华为云授信，此时可以给子账号划拨信用进行消费，此时子账号通过信用产生的消费由主账号统一结算。划拨信用的子账号与主账号必须是实名信息一致或者是主账号对应公司的分公司。

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

2. **账单查询：**主/子账号消费后，可分别登录华为云查看自己的消费数据。主账号可以申请查看子账号消费数据，申请成功后即可查看子账号的消费数据。

3. **开票：**主/子账号消费后，各自独立向华为云申请开发票。主账号也可以代子账号开票。

5.2.7.1 成本计划

1. 估算和预测成本

云服务的价格取决于规格、所在区域、计费模式等因素。对于还未使用的云服务，客户可使用华为云价格计算器在线自助估算这些云服务的成本。对于已使用的云服务，客户也可以使用华为云成本中心的成本分析来预测每日（最多未来 90 天）或每月（最多未来 12 个月）的云成本。该预测，主要基于客户历史成本和历史用量情况，应用机器算法进行估算。然而由于企业的业务活动是动态变化的，云服务的消费支出也会随之动态变化，导致云支出很难准确预测。

2. 创建预算以跟踪成本

跟踪成本计划的有效工具是预算。一旦完成成本的估算与预测，客户可以在华为云成本中心的预算管理创建精细粒度的预算来管理成本，并可以创建预算提醒，在实际或预测超过预算阈值时，自动通知利益相关人。客户还可以创建预算报告，定期（每天/每周/每月）将指定预算进展通知利益相关人。

5.2.7.2 成本分配

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

(一) 确定成本的组织方式

企业进行财务管理之前，需要先确认云支出的组织方式，确保将企业在华为云上的支出能分摊到企业内部的组织层级结构上。比如：对于企业来说，可以使用各个子账号（IT 职能账号和业务账号）来分摊在华为云的支出，同时，还可以使用标签将组织信息标记在资源上，资源标签会随资源使用添加到成本（账单）数据上，企业可以使用标签识别不同环境（比如生产、测试）的成本，或使用标签识别不同的组织、产品、负责人。

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

(二) 确定成本分摊方式

华为云成本中心为客户提供了两种不同的成本类型：

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

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

https://support.huaweicloud.com/usermanual-cost/costcenter_000002_01.html

(三) 确认公共成本的分摊方式

不是所有成本都可以通过标签直接归集的，比如企业内部共享带宽、套餐包产生的成本，未及时标记标签产生的成本，或暂不支持标签管理的云服务产生的成本。这类共同成本如果不能适当分配，企业内部各组织就无法全面了解各自的实际成本。

成本中心为客户提供一种组织成本的工具—成本单元。客户可以创建成本单元，定义规则，根据标签、企业项目、产品类型、账单类型等条件，将符合条件的成本归集到有意义的分类上，识别共同成本并定义拆分规则，将共同成本分摊到企业内部。

比如，客户需要将成本在部门 A、B、C 之间分配。其中，大部分成本可以通过客户标记在资源上的标签（KEY=部门）来标识归属的部门；另外，A 部门还单独使用了人脸识别服务（人脸识别服务不支持标签管理），所有部门共用了共享带宽。



此时客户可以创建一个名为“部门”的成本单元，并创建如下几个自定义规则：

1. 规则一：沿用成本标签=部门的取值进行成本归集
2. 规则二：产品类型=人脸识别的成本，归集部门 A
3. 规则三：产品类型=共享带宽的成本，归集到共同成本
4. 最后将不满足上述规则的成本，也归集到共同成本

经过上述处理之后，客户可以获取以下四个数据：

部门	月度摊销成本净值
部门A	¥10000.00
部门B	¥20000.00
部门C	¥5000.00
共同成本	¥1500.00

接下来，客户可以创建共同成本拆分规则，将共同成本分摊到部门 A、B、C。成本单元支持三种拆分规则：

1. 平均分配

$$\text{每个目标被分摊金额} = \frac{1}{N} \times \text{源成本} \quad (N \text{ 为目标数量})$$

2. 按比例分摊

$$\text{每个目标被分摊金额} = \frac{\text{每个目标的实际成本}}{\text{所有目标实际成本之和}} \times \text{源成本}$$

3. 自定义比例

$$\text{每个目标被分摊金额} = \text{自定义比例} \times \text{源成本} \quad (\text{每个目标自定义比例之和} = 100\%)$$

还是上面的例子，客户选择按比例拆分共同成本，则最终拆分结果如下：

部门	月度摊销成本净值	拆分百分比	拆分到的成本	最终分配成本
部门A	¥10000.00	28.57%	¥428.55	¥10428.55
部门B	¥20000.00	57.14%	¥857.1	¥20857.1
部门C	¥5000.00	14.29%	¥214.35	¥5214.35
共同成本	¥1500.00	-100%	-¥1500.00	--

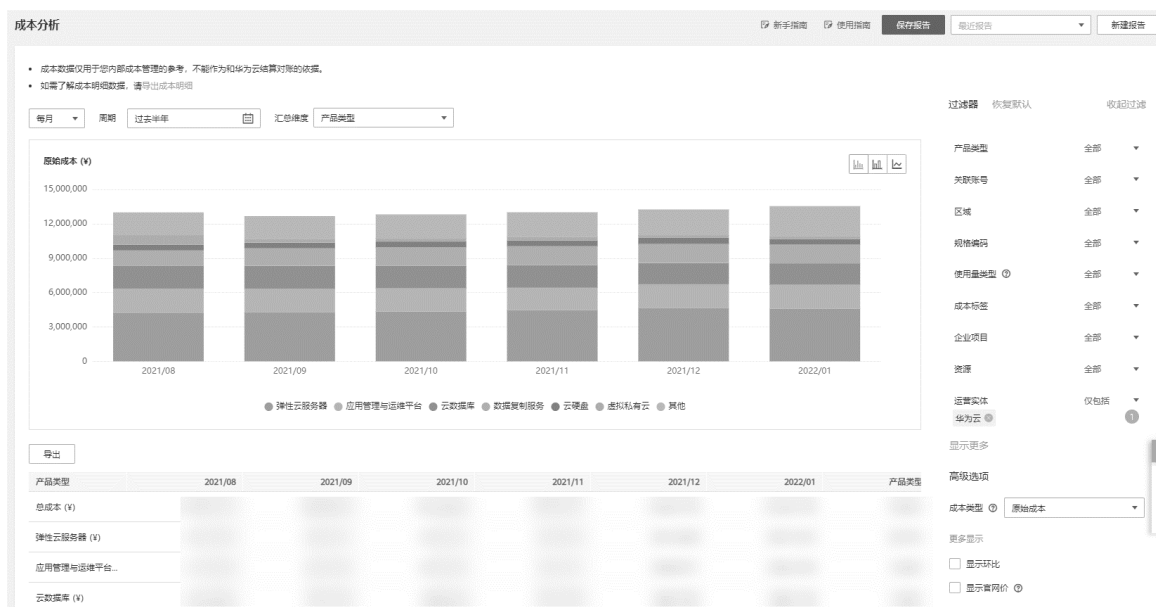
成本单元创建后还可以应用于成本分析、预算跟踪。

5.2.7.3 成本分析

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

1. 分析成本及用量的趋势及分布

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



企业可以使用成本中心提供的**预置分析报告**（见下表）对常见场景快速分析。

报告名称	说明
按产品类型汇总的月度成本	了解过去6个月原始成本较高的产品类型。

按关联账号汇总的月度成本	了解过去6个月原始成本较高的关联账号。
每日成本	了解过去3个月的每日原始成本趋势，以及未来1个月的成本预测。
月度摊销成本	了解过去6个月摊销成本的月度趋势。
ECS的月度按需成本和使用量	了解过去6个月云主机每月按需原始成本和按需使用量情况。

如果预置报告不能满足客户诉求，客户还可以**自定义分析**，通过调整时间粒度、周期、汇总条件、过滤条件以及成本类型，来洞察成本和用量的情况。对于客户经常关注的自定义分析，建议保存为**自定义报告**，便于再次查看相同条件下的分析数据。无论是预置报告还是自定义分析报告，**报告分析结果均支持导出 CSV 文件**。同时，华为云还提供携带标签信息的按月/按日成本明细数据，便于客户深入分析。

明细说明	提供方	提供方式	参考说明
携带标签和关联账号的摊销成本明细（月度明细）	成本中心	导出csv、API	导出csv： https://support.huaweicloud.com/usermanual-cost/costcenter_000002_03.html API： https://support.huaweicloud.com/api-occe/mbc_00010.html
携带标签和关联账号的账单明细（按日）	费用中心	OBS订阅-csv	https://support.huaweicloud.com/usermanual-billing/bills-topic_50000004.html

5.2.7.4 成本优化

云支出的主要影响因素是费率、资源用量、产品选型和方案设计。因此企业在华为云上的成本优化也主要从这几个方面着手考虑。

1. 优化资源费率

对于长期使用的按需产品，建议客户优先采用包年包月或资源包。客户可使用华为云成本中心的**按需转包年包月优化评估**发现节省成本的机会。该评估基于客户 ECS、EVS、RDS 历史按需资源的使用情况进行分析，为客户提供按需转包年包月的可优化资源清单和优化前后的成本对比。

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

2. 优化资源用量

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

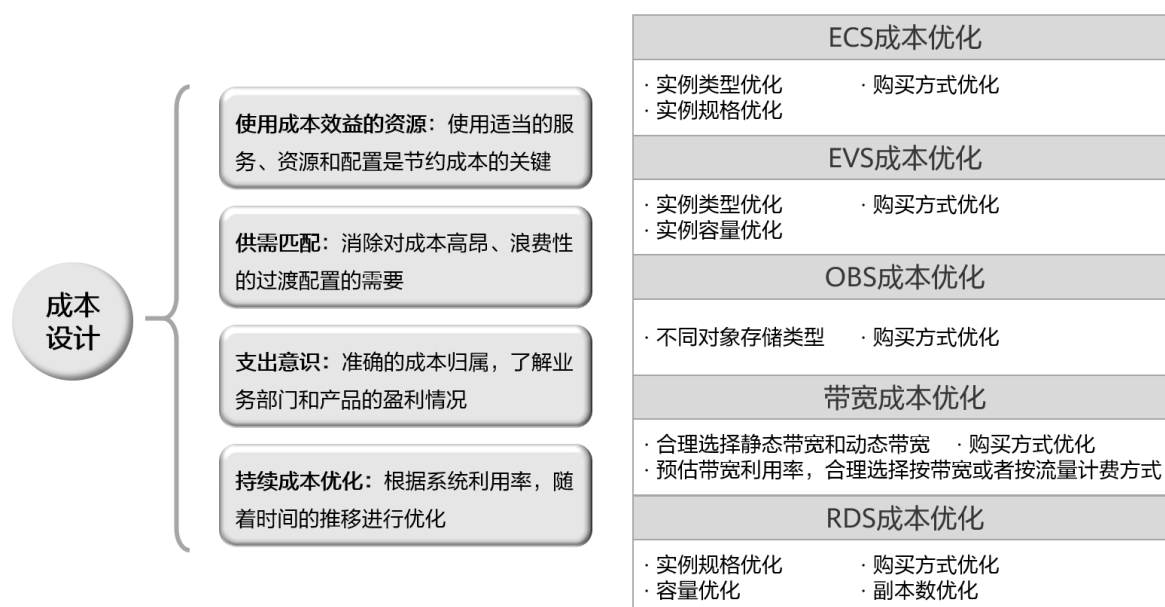
3. 优化产品选型

在满足业务目标的前提下选用低成本的云资源，如允许中断且对及时性要求不高的业务可以选用竞价实例降低成本，冷数据和归档数据可以选用对象存储降低成本。

4. 优化方案设计

客户可以在设计技术方案时充分考虑成本因素，在满足客户业务诉求的基础上，尽量选择成本更加合理的技术方案，比如设计大数据方案时选择存算分离的架构可以有效节省大数据方案的整体成本；使用 OBS 托管静态网站可以有效节省购买 ECS 的成本。

云上资源按需使用、按量计费、弹性伸缩，资源的合理使用决定了成本支出的大小。结合资源的售卖特性，可以优化资源使用成本。如下图：



1. 华为云 ECS 成本优化建议

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

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

- 3) **购买方式优化:** 当前华为云提供按需、包月、包年 3 种购买方式, 基于三种模式支出成本对比, 针对业务的使用场景和持续周期, 建议的购买方式如下:
 - 若应用持续周期小于 20 天, 如: 短期测试、电商节假日促销等场景, 建议以按需方式购买;
 - 若应用持续周期大于 20 天而小于 10 个月, 如: 游戏上线测试和运营等场景, 建议以包月方式购买;
 - 若应用持续周期大于 10 个月, 如: 企业官网运营、政务民生信息查询运营等场景, 建议以包年方式购买。

2. 华为云 EVS 成本优化建议

- 1) **EVS 类型优化:** 华为云提供 4 种类型 EVS, 其中极速 SSD 型适用于大型 OLTP 数据库、NoSQL 数据库和流处理与日志处理等场景, 超高 IO 型适用于高性能计算、数据仓库场景, 通用 SSD 型适用于企业应用和大中型开发测试场景, 高 IO 型则适用于办公应用等场景。假如使用场景是电商网站运营或企业官网运营, 建议选用高 IO 型, 而非超高 IO 型, 这样同样容量 EVS, 更节省成本。
- 2) **EVS 容量优化:** 基于 EVS 弹性扩容的能力, 应根据当月的预测容量来购买量, 在其利用率达到 80%或以上时, 再进行实时扩容, 以保证其利用率维持 80%左右, 与按全年预测的最大容量购买相比 (一般其利用率达不到 50%), EVS 的费用支出将明显减少。另外, 也应定期检查账号, 定期删除那些独立的、无用的 EVS 卷 (随 ECS 创建而创建, ECS 删除时未删除的 EVS 卷), 会进一步减少成本。
- 3) **转换购买方式:** 若业务已在华为云上运行一段时间, 针对已开通且后续长期使用 EVS 卷, 建议从按需或包月方式购买转变为包年方式购买, 将明显节省成本, 另外将一些不经常使用的非关键数据或归档数据转移到 OBS 存储会大幅度降低成本。

3. 华为云 OBS 成本优化建议

- 1) **OBS 类型优化:** 华为云提供 3 种不同可用性、持久性标准的 OBS 服务, 其中标准存储适用于大数据、热点视频等需频繁访问数据的场景, 低频访问存储适用于文件同步、企业备份等不频繁访问的场景, 归档存储适用于数据归档、长期备份等很少访问的场景。基于不同业务需求, 选择合适的对象存储类型, 将极大节省成本开支。对于需要备份的企业数据, 建议选择低频访问存储; 针对时间较久的备份数据, 建议将其转移到归档存储, 成本可以明显降低。
- 2) **转换购买方式:** 针对标准存储, 华为提供了多种容量规格和不同周期的存储容量包, 针对已上传到标准存储且会将长期使用数据, 可根据现有的数据容量, 购买对应的包年容量包, 成本明显降低。

4. 华为云带宽优化建议

带宽成本是公有云使用成本很重要的一部分, 在进行云服务配置时需重点考虑。

- 1) 华为云提供静态 BGP 带宽和全动态 BGP 带宽两种选择, 绝大部分情况下选择静态 BGP 带宽即可, 如果是金融或游戏客户对带宽有极致体验诉求的可以选择全动态 BGP 带宽, 静态 BGP 带宽价格比全动态 BGP 带宽价格低很多。
- 2) 5M 带宽以下时选择带宽包月往往比按流量更划算, 5M 带宽以上时需要根据带宽大小和预估的带宽利用率按以上方法计算得出哪种方式更划算。

- 3) 利用 ELB 实现带宽集约，以减少带宽成本。以小型游戏云架构设计为例，如果将登陆和充值区、游戏一区、游戏二区分别部署在 1 台 ECS 上，每台 ECS 配置 10M 带宽，那么总共需要 30M 带宽。不过同一时间三个区的用户访问量有差异，会造成有的带宽利用率高有的带宽利用率低。因此可以在架构设计上部署 1 个 ELB 在 3 台 ECS 的上方做流量分发，ELB 只需配置 20M 左右的带宽即可，通过 ELB 实现带宽集中提升带宽利用率减少带宽成本。
- 4) 合理使用 CDN 减少公网带宽使用量，降低 TCO，如果您正在通过 ECS 或 OBS 向互联网用户提供图片、视频、文件下载等静态内容，那么可以引入 CDN 服务降低流量成本。使用 CDN 除了能节省成本还能带给客户更好的体验。
- 5) 当有大量数据需上传到公有云时，使用数据快递比使用专线传输数据大幅节省成本。

5. 弹性伸缩和定期资源优化建议

企业上云后，通过配置合适的弹性伸缩策略和定期优化资源可以帮助降低成本，参考如下：

- 1) **基于负载自动扩缩容：**根据系统负载情况自动增加或减少资源。当负载较高时，增加实例数量以满足需求；当负载较低时，减少实例数量以节省成本。
- 2) **基于时间表自动扩缩容：**如果业务在某个时间段内会有更高的负载，例如每天的特定时间段或周末，可以预先设定一个计划来在这些时间段自动扩展资源，并在负载较低时恢复到正常水平。
- 3) **基于指标的自动扩缩容：**监控关键指标（如 CPU 使用率、网络流量等），当这些指标超过或低于阈值时，自动扩展或收缩资源。例如，当 CPU 使用率持续高于 70% 时，自动增加实例数量来分担负载。
- 4) **弹性伸缩组使用一定的包周期实例：**可以通过购买一定数量的包周期实例来降低成本，而不是完全依赖按需实例。弹性伸缩组可以同时使用包周期实例和按需实例，并根据需求设置自动缩放规则，确保系统自动调整实例数量以适应负载变化，既可以提供足够的计算能力，又可以获得较低的成本。注意，由于业务负载可能会随时间变化，这项工作需要定期进行评估和优化，以最大程度地降低成本。
- 5) **定期优化资源：**定期评估资源使用情况，识别空闲或低负载资源，并及时释放或调整它们的规格，这有助于避免浪费和不必要的成本。
- 6) **使用云服务提供商的成本优化工具：**许多云服务提供商都提供了专门的成本优化工具，可帮助企业分析和优化资源使用情况。这些工具可以提供建议和推荐，帮助企业制定更合理的弹性伸缩策略。

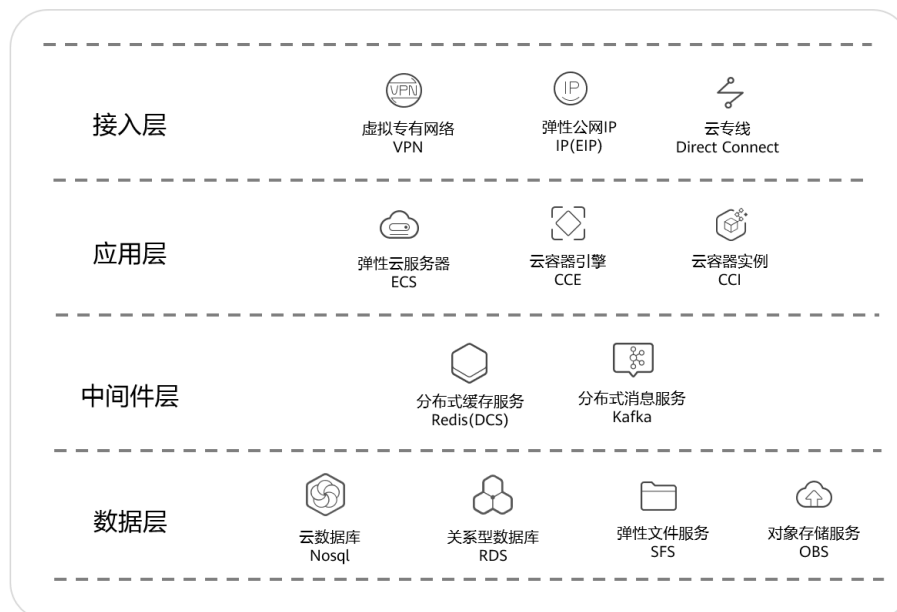
通过基于负载、时间表、指标的自动化弹性伸缩策略，以及购买预留实例和定期优化资源等方法，可以有效地降低企业上云后的成本，同时，需要密切关注云服务提供商的新功能和工具，以获取最新的成本优化建议。

5.3 应用部署架构设计

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。

5.3.1 应用部署架构概述

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。



- 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 workflow 控制，实现业务逻辑。上承接接入层，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：

- 1) **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。
 - 2) **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。
4. **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：

1. **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。
2. **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。
3. **性能**：性能设计的目的是为了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。
4. **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。
5. **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。
6. **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：

5.3.2 可用性设计

5.3.2.1 可用性定义

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

SLA	每周故障时间	每月故障时间	每年故障时间
99%	1.68 小时	7.2 小时	3.65 天
99.90%	10.1 分钟	43.2 分钟	8.76 小时
99.95%	5 分钟	21.6 分钟	4.38 小时

99.99%	1.01 分钟	4.32 分钟	52.56 分钟
--------	---------	---------	----------

5.3.2.2 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：

1. 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。
2. 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。
3. 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。

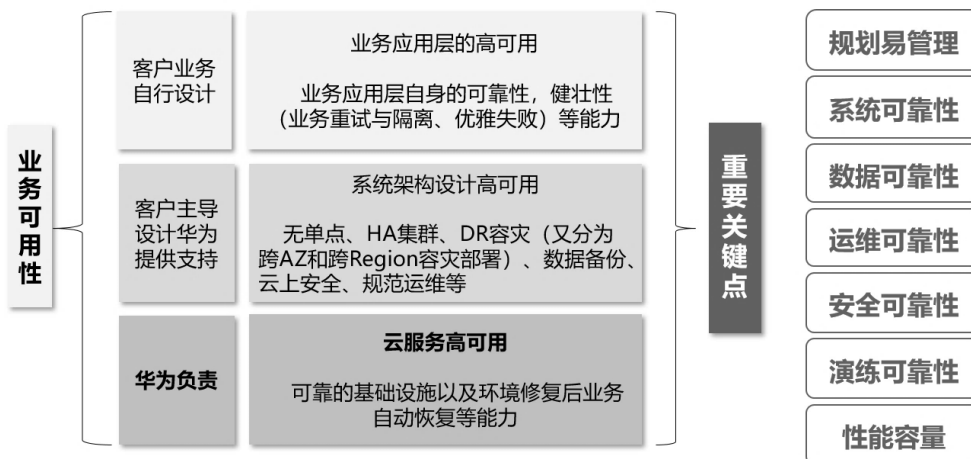
企业可以基于 AZ 故障域进行应用的高可用性设计，设计时可以考虑如下方面：

1. 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。
2. 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。
3. 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。
4. 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。
5. 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。

5.3.2.3 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）。

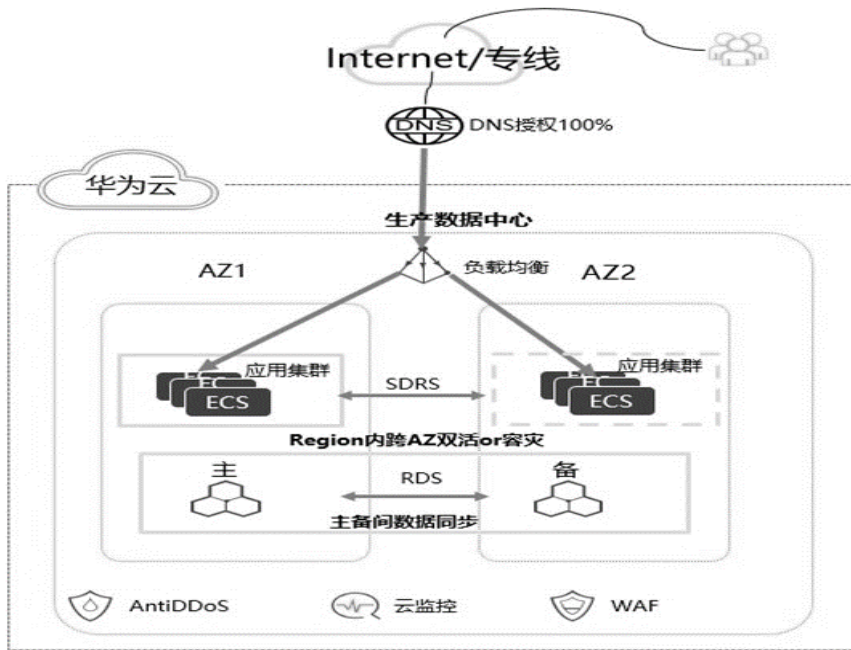


华为云上的绝大部分云服务都具备高可用性的方案，提供了从数据中心、硬件、数据、自助服务等多个层次的高可用性构建能力。华为云数据中心布局于全球，可以满足不同地域（Region）的资源需求，每个地域又分多个可用区（AZ），可用区之间的风火水电相互独立，可用区之间的故障相互隔离。企业可在此基础上构建如下场景的高可用体系：

1. 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。
2. 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。
3. 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。
4. 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。

5.3.2.4 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。



设计要点:

1. 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。
2. 云服务高可用：主备节点分别双 AZ 部署。
3. 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。
4. 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。
5. 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。

注意：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，建议如下：

1. 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。

2. 延迟验证

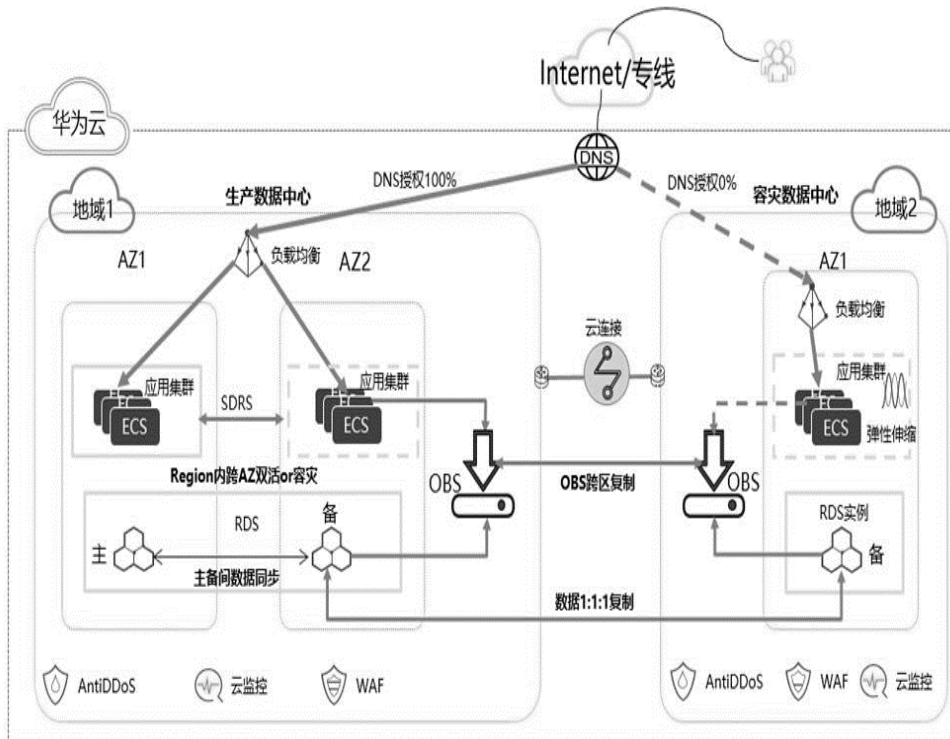
在正式实施双 AZ 高可用方案前，需要充分的测试和验证来评估应用程序在不同 AZ 之间的延迟情况。通过模拟真实负载的压力测试，来记录不同 AZ 之间的应用调用延迟，用于评估是否满足业务的需求，并做出相应的决策。

5.3.2.5 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。

1. 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。

2. 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。



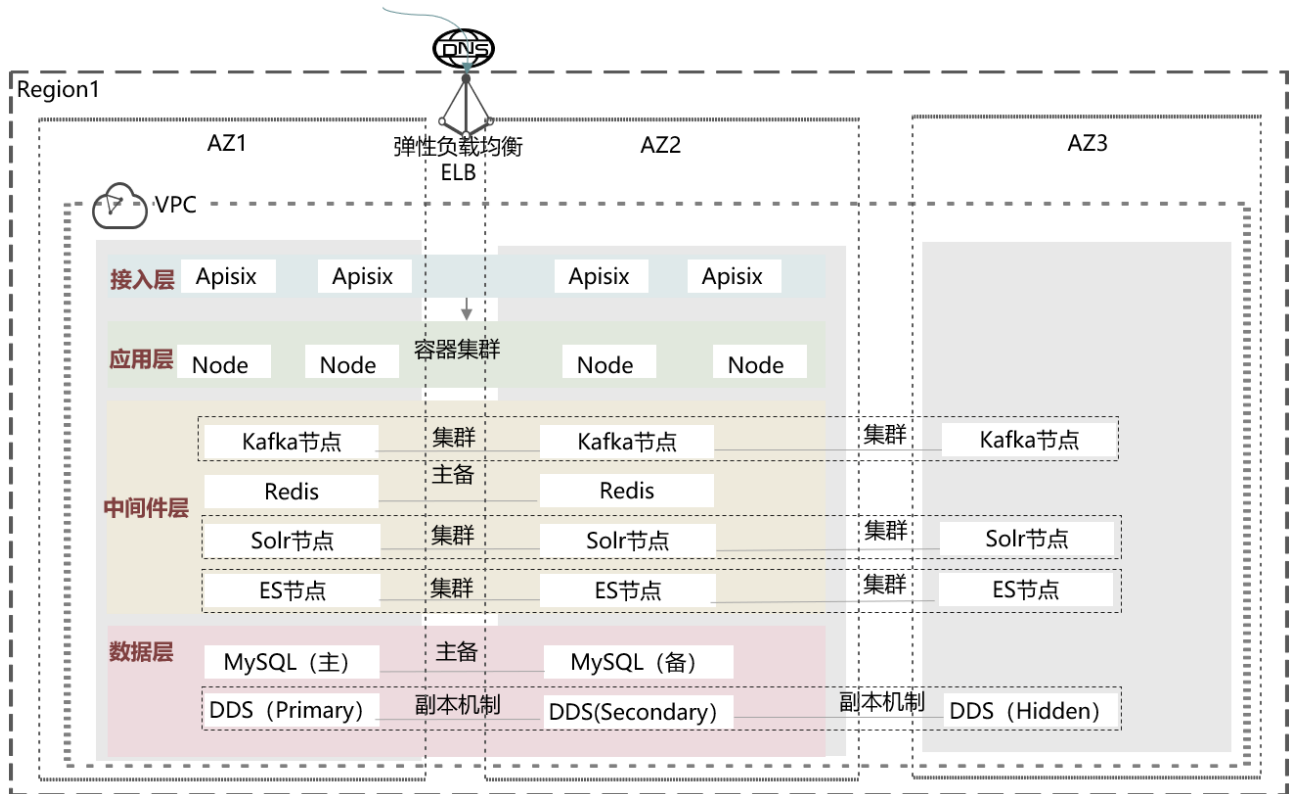
设计要点：

1. 生产数据中心和容灾中心分别部署在华为云 2 个不同 Region。
2. 生产中心采用双 AZ 部署（双活、热备），容灾中心单 AZ。
3. 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。
4. 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。
5. 生产站点某个 AZ 故障时，切换到另一个 AZ，数据库主备切换。
6. 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%）。
7. 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%）。
8. 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（https://support.huaweicloud.com/mas/index.html）](https://support.huaweicloud.com/mas/index.html)。

5.3.3 跨 AZ 高可用设计示例

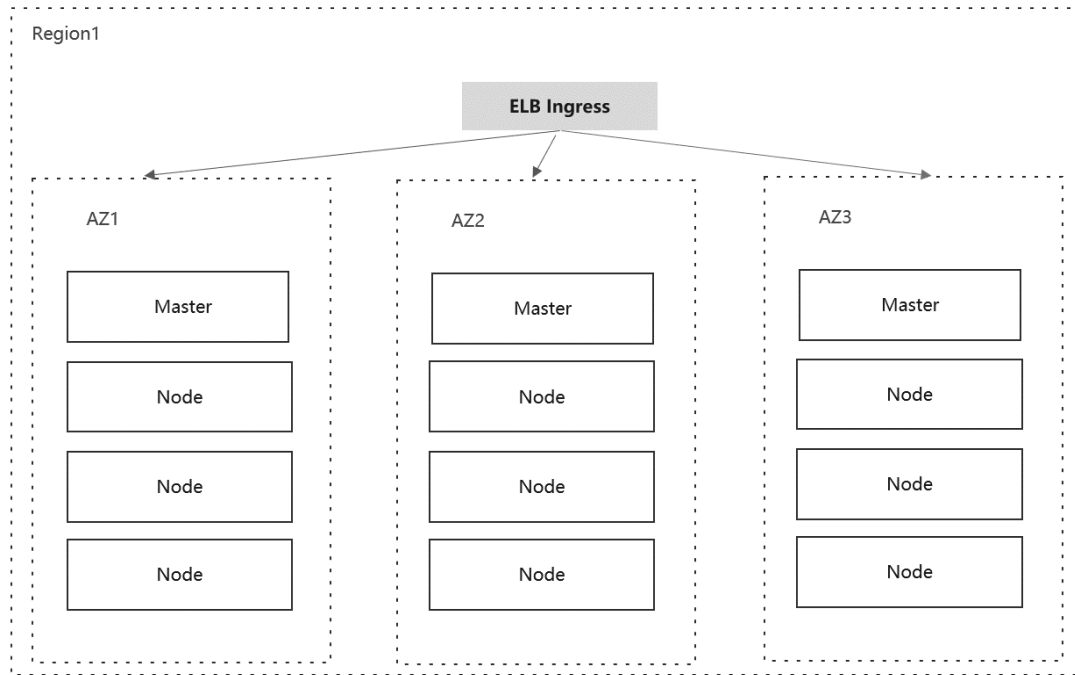
跨 AZ 高可用是 IDC 上云最主要的价值之一。企业上云后最适合做跨 AZ 高可用，不仅成本低，而且很便利。下面以某大型零售电商平台为例，介绍上云后的跨 AZ 高可用设计方法。下图是总体架构图：



1. **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。
2. **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。
3. **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。
4. **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。

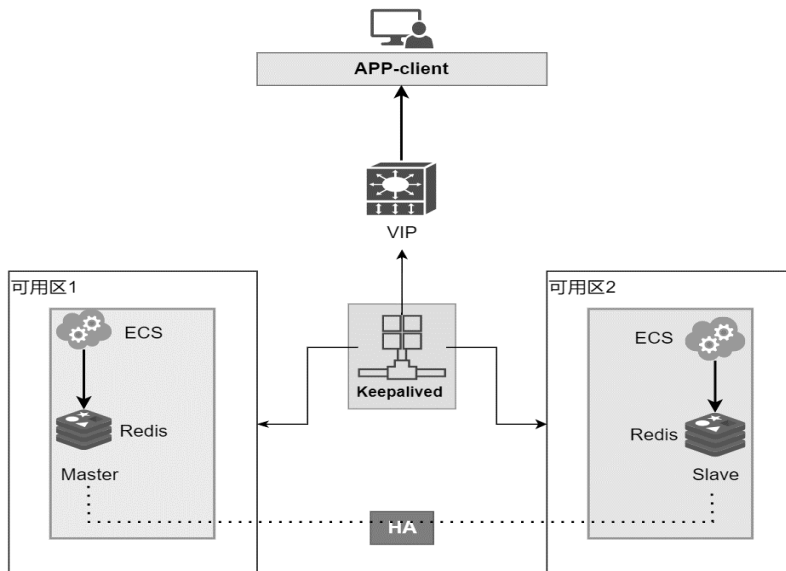
(一) 应用层-容器集群高可用

1. Master 高可用：容器集群 Master 节点 3AZ 分布，3 节点 (1+1+1)。
2. 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。
3. 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。



(二) 中间件层-Redis 高可用

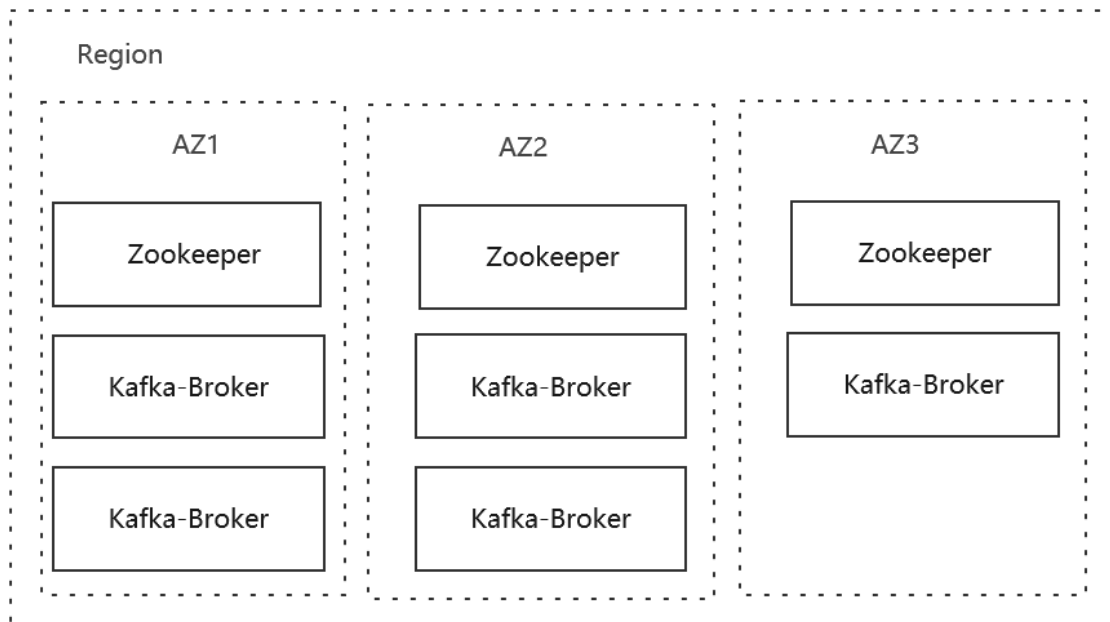
1. 主备实例配置了数据持久化，数据不仅会持久化到主节点磁盘，还会实时同步到备节点，同时备节点也会持久化一份数据。
2. 主备实例部署在不同的可用区内，不同可用区的电力、网络相互隔离，当主节点所在的机房因为电力或者网络出现故障，备节点将接管服务，客户端与备节点正常建立连接以及读写数据。
3. Redis 集群搭配 Keepalived 生成 VIP，提升业务可用性。



(三) 中间件层-Kafka 高可用

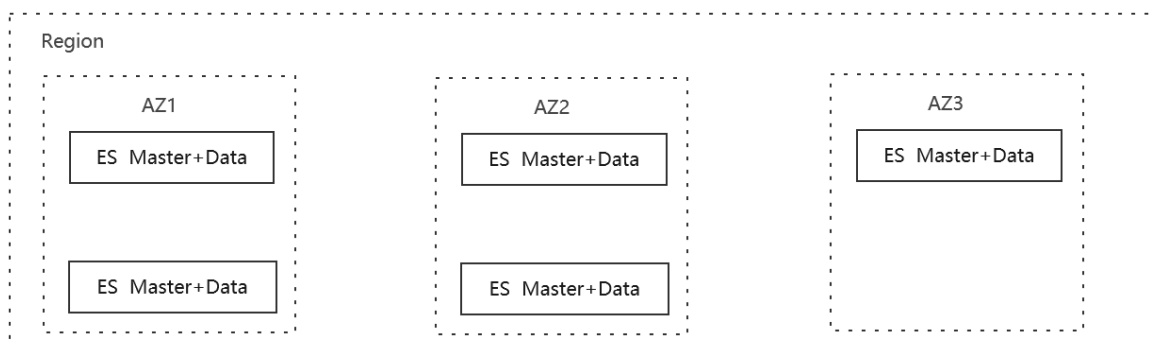
1. Zookeeper 高可用: Zookeeper 节点 3AZ 分布，3 节点 (1+1+1) 或 5 节点 (2+2+1)。当某个 AZ 不可用时，集群依旧有超过半数的法定主节点选举个数，保证 ZK leader 的正常选主。

2. 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。



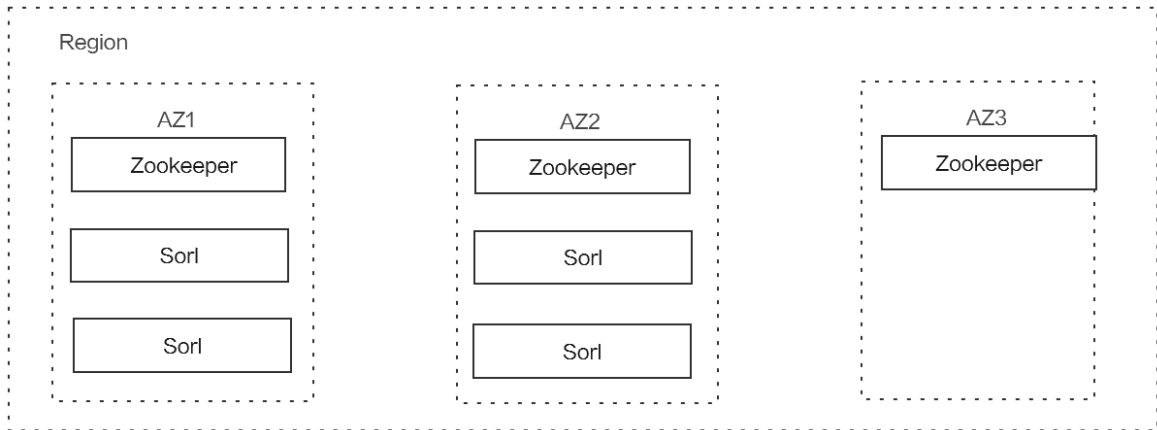
(四) 中间件层- Elasticsearch 高可用

1. 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。
2. 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。



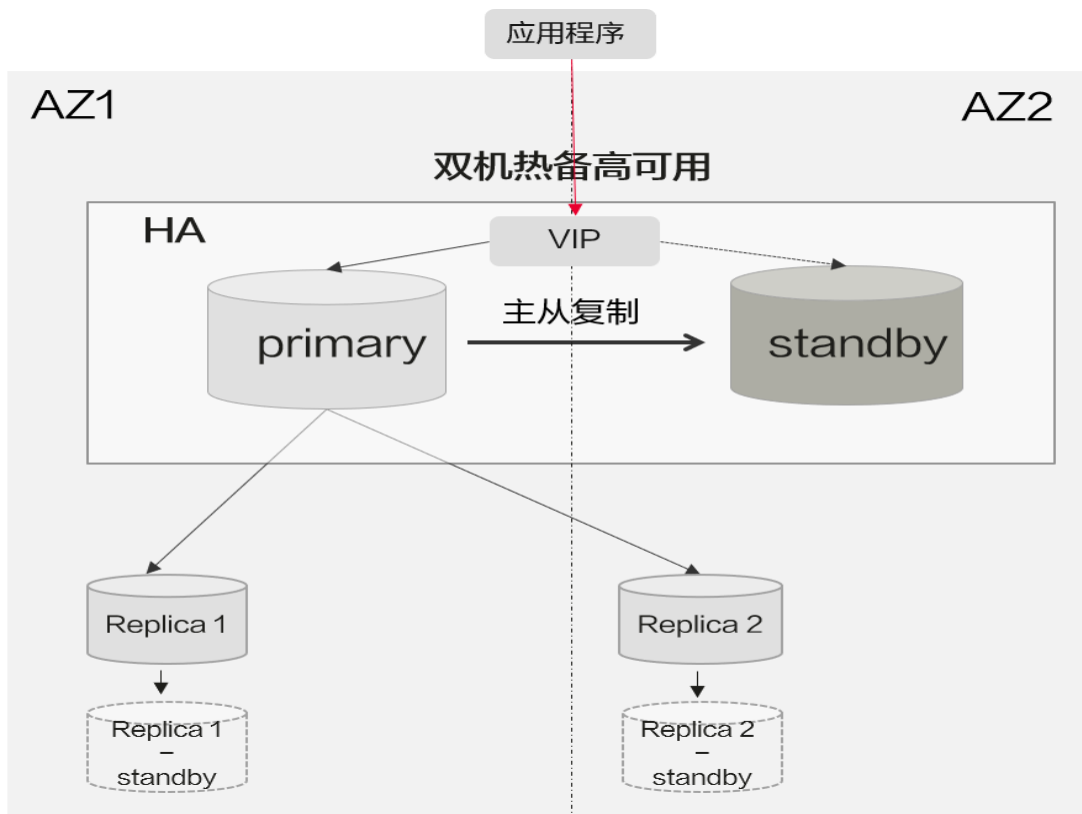
(五) 中间件层- Solr 高可用

1. 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。
2. Solr 数据节点: Solr 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。



(六) 数据层- MySQL 高可用

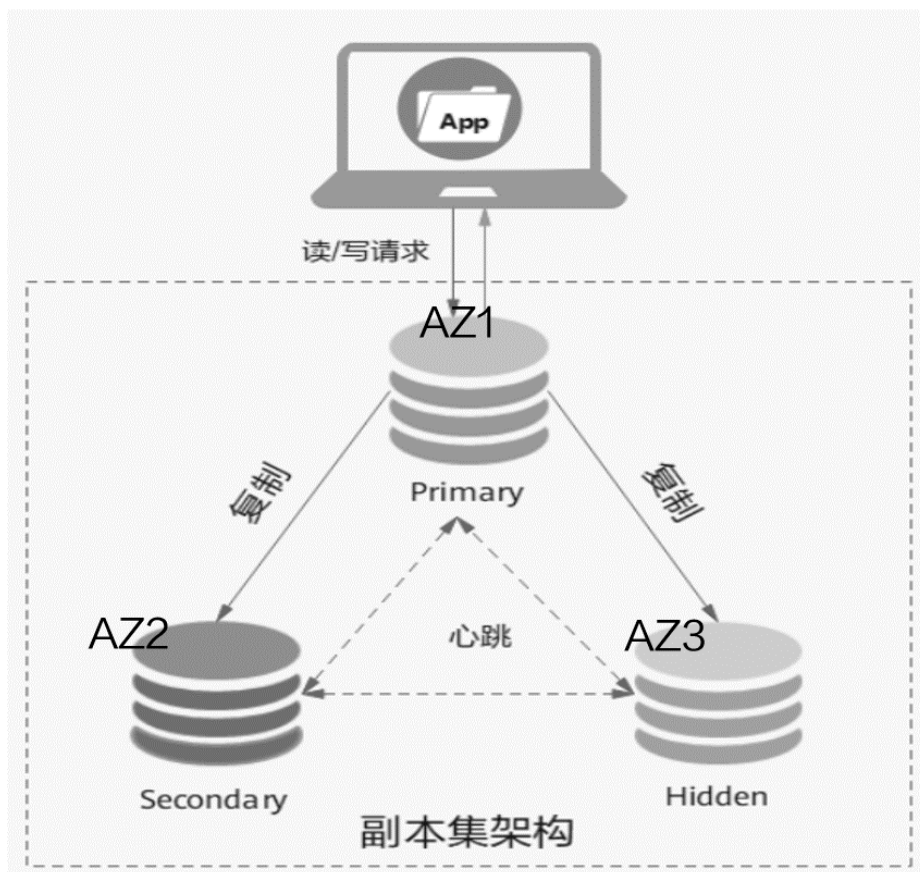
1. 主备实例跨 AZ 部署，借助原生 MySQL 主从复制同步能力实现主备间数据同步。
2. 主备实例以 VIP 对外提供服务，自身 IP 不对租户开放。
3. 主备秒级切换，主备切换时 VIP 漂移至新的主节点，应用感知小（只在切换瞬间有秒级中断）。
4. 支持挂载只读节点，只读节点亦可跨 AZ 部署



(七) 数据层- MongoDB 高可用

1. 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。

2. Mongo Client 原生支持配置多个 Server 地址，并支持探活。
3. 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。



5.3.4 可扩展性设计

5.3.4.1 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：

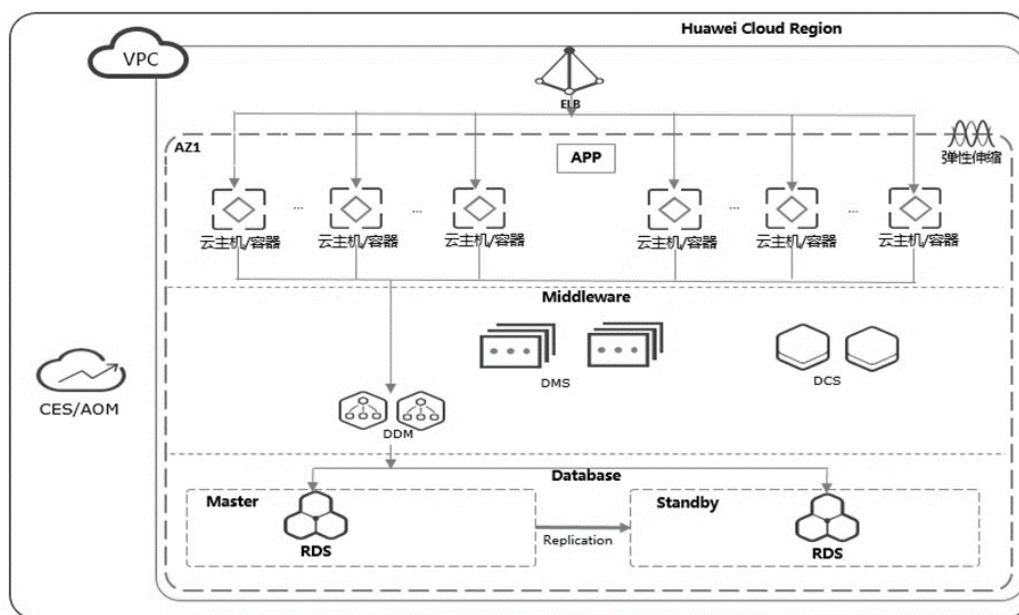
1. **纵向（垂直）扩展：**适用于单体应用、独立应用、有状态应用等场景下，随着业务不断发展和变化，需要快速升级硬件以应对业务变化。如在进行一些促销活动时，对资源的需求往往比正常要高出多倍，这时企业在云上就可以通过可视化界面或者 OpenAPI 快速升级资源的配置，将资源调整到更高规格的实例上（如更多的 CPU、内存、带宽、磁盘空间等），以应对活动的流量冲击；而在活动过后，又可以将规格收缩回原来的规格，达到降低成本的目的。
2. **横向（水平）扩展：**适用于分布式应用、无状态应用、快速变化的应用等场景下，固定数据的资源配比显然已经无法应对业务的快速变化，此时就可以依托于云上丰富的资源和快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：

1. 定时模式：创建定时任务，在指定时间执行资源扩缩容。
2. 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。
3. 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。
4. 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。

5.3.4.2 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。



应用上云目标架构的各层可扩展方案设计要点如下：

(一) 应用层可扩展设计要点：

1. 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；
2. 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。

(二) 中间件层可扩展设计要点：

1. 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。
2. 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。

(三) 数据层可扩展设计要点:

1. 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。
2. 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。

5.3.5 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:

1. 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;
2. 针对网络资源, 吞吐量是评价数据处理执行的速率;
3. 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;
4. 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;
5. 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: 方案的选择、性能度量、性能监测和性能权衡。

1. 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;

2. 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);

3. 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;

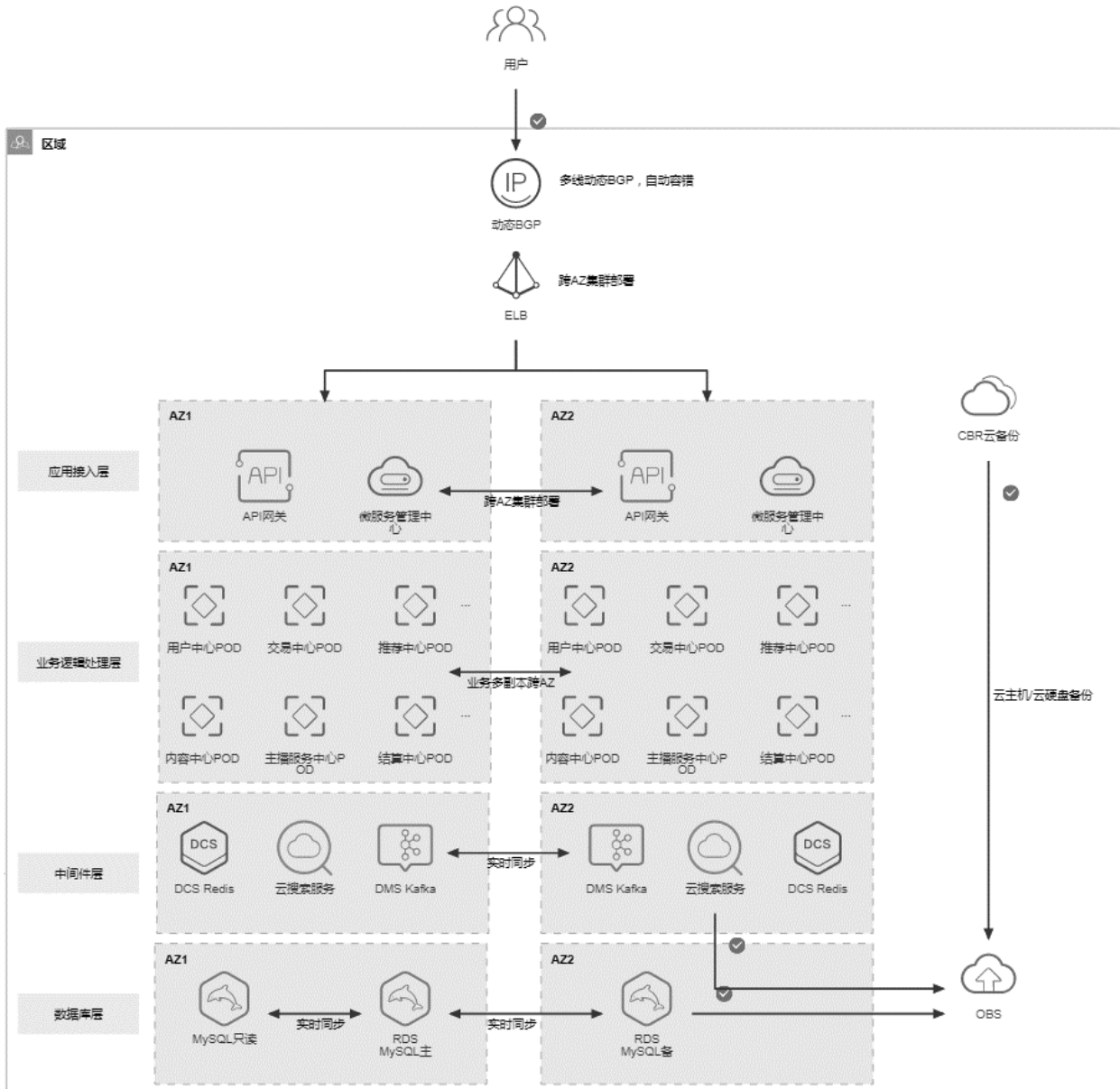
4. 性能权衡

- 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。

5.3.6 应用部署参考架构

5.3.6.1 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：



设计要点：

1. 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；
2. 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；
3. 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；

4. 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；
5. 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；
6. 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；
7. 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；
8. 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。

5.3.6.2 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。

1. 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。

- 1) 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；
- 2) 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；
- 3) 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。



模板类型: **全部** 完整架构模板 子场景架构模板

部署环境: **全部** 华为公有云 华为云Stack 华为云Stack Online 智能边缘小站

适用行业: **全部** 通用行业 零售 互联网 制造 金融 教育 数字政府 电网 游戏 物流 交通 医疗卫生 信息技术服务业 建筑地产 基因 服务业
 建材 大数据 化工 保险

适用场景: **全部** 企业上云 数据集成 智慧园区 数据迁移 AI 容灾 数据分析 灾备 SAP 网络加速 迁移上云 HANA 数据使能 云边协同 数字化营销
 企业安全 大数据 数据治理 零售 数据灾备

更多行业

更多场景

综合排序 最新发布 最多引用 我的关注

新 SAP云上数据集成方案架构 b711884ea5644951a8c3837713f6af18

【方案描述】方案的简要描述: 华为云上SAP数据集成场景方案 【架构说明】 1、ROMA FDI应用与数据集成平台开发的SAP集成连接器, 从SAP ERP抽取数据到数仓/大数据平台; 支持SAP报表、透明表、池表、视图的全量/基于时间戳的增量抽取。 2、ROMA FDI应用与数据集成平台开发的ODP连接器, 从SAP ERP抽取数据到数仓/大数据平台; 支持从预定义...

模板类型: 完整架构模板 企业名称: 深圳华为云计算技术有限公司 作者: ***** 发布时间: 2022/11/30

适用行业: 通用行业

适用场景: SAP数据集成 ROMA FDI集成SAP SAP数据抽取 HANA数据集成 HANA数据抽取

部署环境: 华为公有云

8.1k 31 4 5

综合排序 最新发布 最多引用 我的关注

华为云上SAP备份方案架构 f80cee1994b54c7bb80295dccb8bdeca

【方案描述】方案的简要描述: 华为云上SAP应用和数据库备份参考架构 【方案优势和价值】 1、通过SAP认证的HANA备份解决方案 2、无备份软件license费用, 可直接从OBS存储 备份还原 【架构说明】 1、操作系统备份: CBR云备份服务提供ECS备份的备份, 可以提供SAP应用和HANA数据库操作系统的备份。 2、SAP应用数据备份: CBR云备份服务同时提供单个磁盘的备份, SAP应用服务器的数据文件系统 Ausrisaptrans和sapmnt 可通过CBR云备份服务执行备份流程。 3、HANA数据库的...

模板类型: 完整架构模板 企业名称: 深圳华为云计算技术有限公司 作者: ***** 发布时间: 2022/11/30

适用行业: 通用行业

适用场景: 华为backint SAP上云 HANA云上备份 SAP备份

部署环境: 华为公有云 华为云Stack Online

29 8 0 0

云上SAP Scale-out集成架构参考 96cc8cab47c34a3789b0efcb9635f2b3

【方案描述】方案的简要描述: 华为云上SAP HANA scale-out集成架构参考 【架构说明】 1、通过反亲和性将HANA集群中每个节点部署在不同的物理服务器上, 有效避免了单一服务器故障导致整个集群宕机。 2、Log&Data分发与共享: 一个HANA集群中的每个HANA工作节点将所有的Log&Data都Abaonch上, 但是只在一个节点上Mount和使用。 3、使用EVS共享存储PVSCSI制, 实现自动的故障接管

模板类型: 完整架构模板 企业名称: 深圳华为云计算技术有限公司 作者: ***** 发布时间: 2022/09/24

适用行业: 通用行业

适用场景: SAP HANA Scale-out SAP集群 SAP高可用 SAP BW BW Scale-out

部署环境: 华为公有云 华为云Stack

35 8 0 0

疾控平台解决方案系统架构参考 83ee09471c64ae79f96898d3dd02a05

【业务场景&挑战】防疫系统自身产生的防疫相关的业务数据, 如流调数据、重点管控人员、高风险人员等; 同时业务系统数据通过数据交换平台的大数据主题、专题库、知识图谱、法人库、轮数信息、电子病历信息、位置信息等。由于数据存在于多个系统, 导致数据标准不一致, 数据量比较大, 不同业务场景需要不同来源的数据, 且处理逻辑强依赖于业务 【架构说明】 1、外部系统的数据先进入HDFS, 经过清洗处理, 再进入下一步的业务处理 2、业务主题数据存储在MR3D ClickHouse 3...

模板类型: 完整架构模板 企业名称: 深圳华为云计算技术有限公司 作者: ***** | 医疗行业SE 发布时间: 2023/02/01

适用行业: 通用行业 卫健部

适用场景: 医疗 防疫 数据交换 数据处理

部署环境: 华为公有云

32 6 0 0

SAP华为云上网络和安全架构 05be616f9454d0f879d0c4b0059f08

SAP华为云上网络和安全架构 【方案描述】 根据SAP业务特点, 结合华为云上SAP实践, 提供华为云上SAP安全架构参考 【架构说明】 1、根据SAP业务特点, 参考企业安全实践, 将云上网络划分为不同安全级别的多个子区域: DMZ区、生产应用、非生产HANA、非生产HANA、管理区。 2、DMZ区: 直接和Internet互联, 承载公网用户以及SAP支持人员对业务系统的访问; 安全级别最低, 安全风险最高。 3、SAP应用区: 部署SAP应用, 包括生产应用和非生产应用两个...

模板类型: 完整架构模板 企业名称: 深圳华为云计算技术有限公司 作者: ***** 发布时间: 2022/11/30

适用行业: 通用行业

适用场景: SAP上云 SAP HANA上云 SAP云上安全 SAP云上容灾

部署环境: 华为公有云 华为云Stack Online

83 4 0 2

2. 架构模板详情

架构模板 / 架构模板详情

基本信息 引用到设计中心

架构模板名称: [SAP云上数据集成方案架构](#) b711884e5644951a9c38377139faf18

模板类型: 完整架构模板

架构模板描述: **【方案描述】**
方案的简要描述: 华为云上SAP数据集成场景分析

【架构说明】

1. ROMA FDI应用与数据集成平台开发的SAP表连接器, 从SAP ERP抽取数据到数仓/大数据平台; 支持SAP数表、透明表、池表、视图的全量/基于时间戳的增量抽取。
2. ROMA FDI应用与数据集成平台开发的ODP连接器, 从SAP ERP抽取数据到数仓/大数据平台; 支持从预定义数据层通过ODATA协议抽取SAP数据, 支持自动建表, 全量、增量数据抽取。
3. CDM云数据迁移开发的HANA表连接器, 从SAP数据库抽取数据到数仓/大数据平台; SAP HANA表连接器有一定约束, 比如SAP HANA不支持作为目的端; 不支持BW4 FOR HANA; 不支持目的端自动建表等。

通用行业: [通用行业](#)

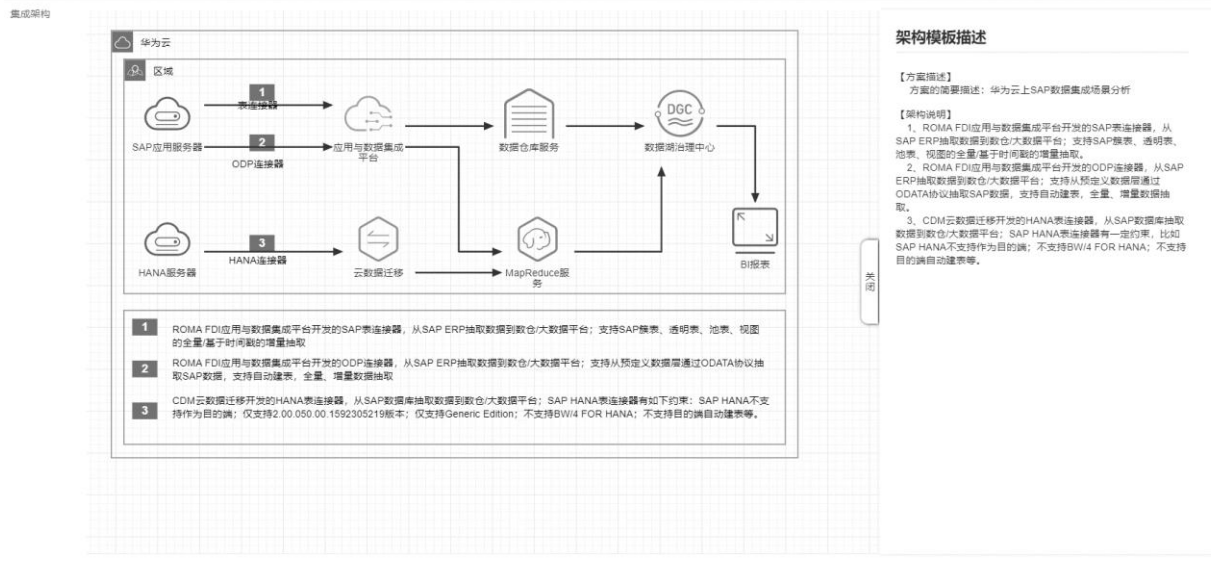
适用场景: [SAP数据集成](#) [ROMA FDI集成SAP](#) [SAP数据抽取](#) [HANA数据集成](#) [HANA数据抽取](#)

部署环境: [华为公有云](#)

发布时间: 2022/11/30 16:28:26 GMT+08:00

模板附件: 暂无附件

119 18 2 2



部署架构类型: 暂无部署架构

部署架构: 暂无部署架构

配置清单

序号	云服务	规格	数量	计价模式	周期	参考价

3. **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。



5.4 大数据架构设计

5.4.1 范围说明

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 5.3。

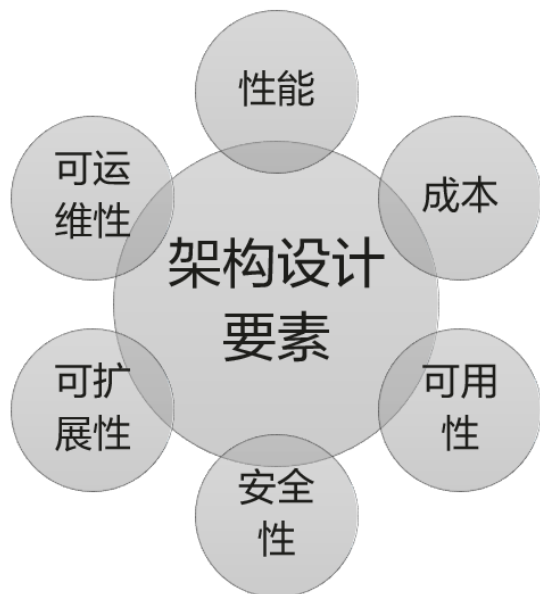
大数据应用（BI类、算法类、API类）

大数据任务调度平台（Azkaban、Hera等）

大数据集群（在线、离线、OLAP）

5.4.2 设计原则

大数据架构设计同样要考虑架构设计的 6 要素，如下：



5.4.2.1 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：

1. **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方案。如果目标云平台上对应的组件，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方案。
2. **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。
3. **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。
4. **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。
5. **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。
6. **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。

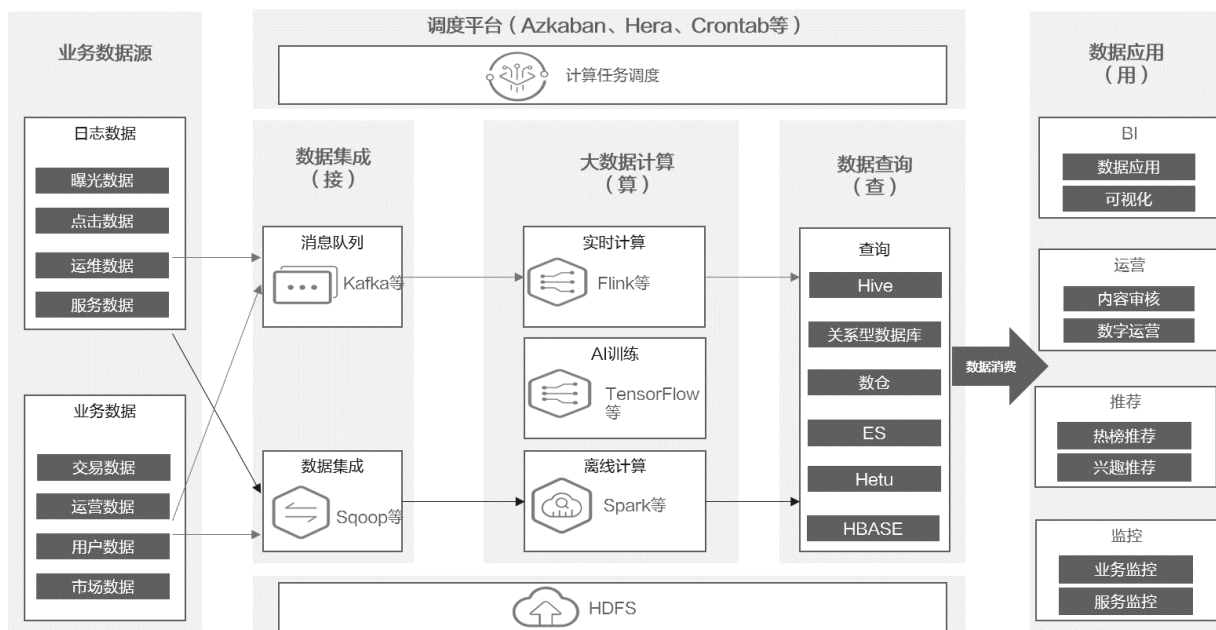
5.4.2.2 大数据任务调度平台设计

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：

1. **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。如果目标平台上对应的组件，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。
2. **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。
3. **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。
4. **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。
5. **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。
6. **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。

5.4.3 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。



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：

1. 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。

2. 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。

3. 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。

4. 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。

5. 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。

6. 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。

7. 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。

5.4.4 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：

1. 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。详细信息请参考链接：

<https://support.huaweicloud.com/function-mrs/index.html>

2. 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。详细信息请参考链接：

https://support.huaweicloud.com/productdesc-dli/dli_01_0378.html

3. 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。详细信息请参考链接：

https://support.huaweicloud.com/productdesc-css/css_04_0001.html

4. 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。详细信息请参考链接：

https://support.huaweicloud.com/productdesc-dws/dws_01_0002.html

5. 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。详细信息请参考链接：

https://support.huaweicloud.com/productdesc-dataartsstudio/dataartsstudio_07_001.html

6. 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。详细信息请参考链接：

https://support.huaweicloud.com/productdesc-dis/dis_07_0001.html

7. 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。详细信息请参考链接：

https://support.huaweicloud.com/productdesc-cdm/cdm_01_0143.html

8. 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。详细信息请参考链接：

https://support.huaweicloud.com/productdesc-des/zh-cn_topic_0047663842.html

6

上云迁移试点

6.1 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。

1. **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。
2. **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。
3. **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。
4. **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。
5. **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。
6. **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。
7. **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。

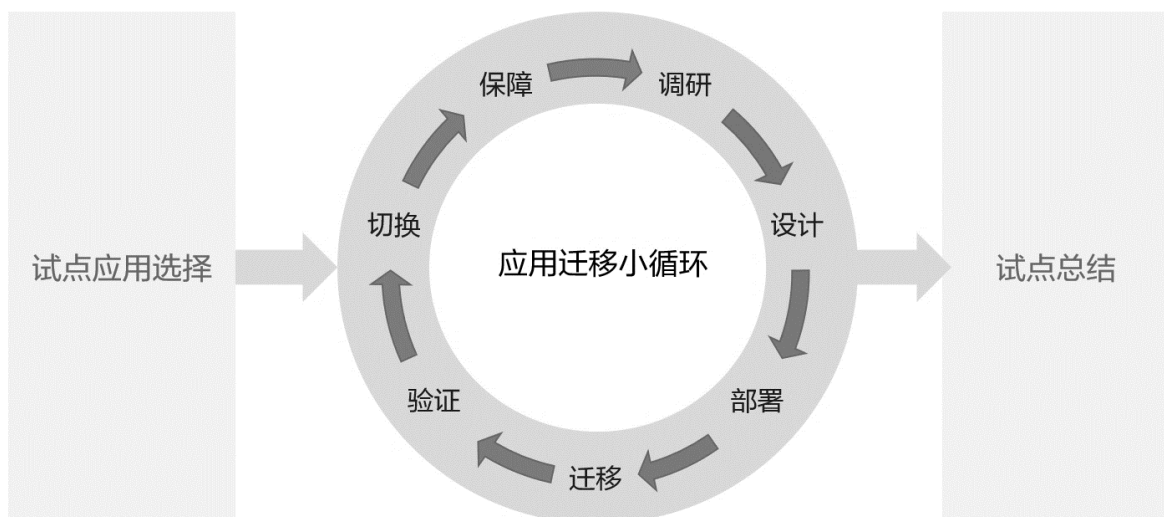
6.2 如何选择试点应用

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：

1. **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。
2. **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。
3. **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。
4. **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。
5. **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。
6. **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。
7. **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。

6.3 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：



6.4 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：

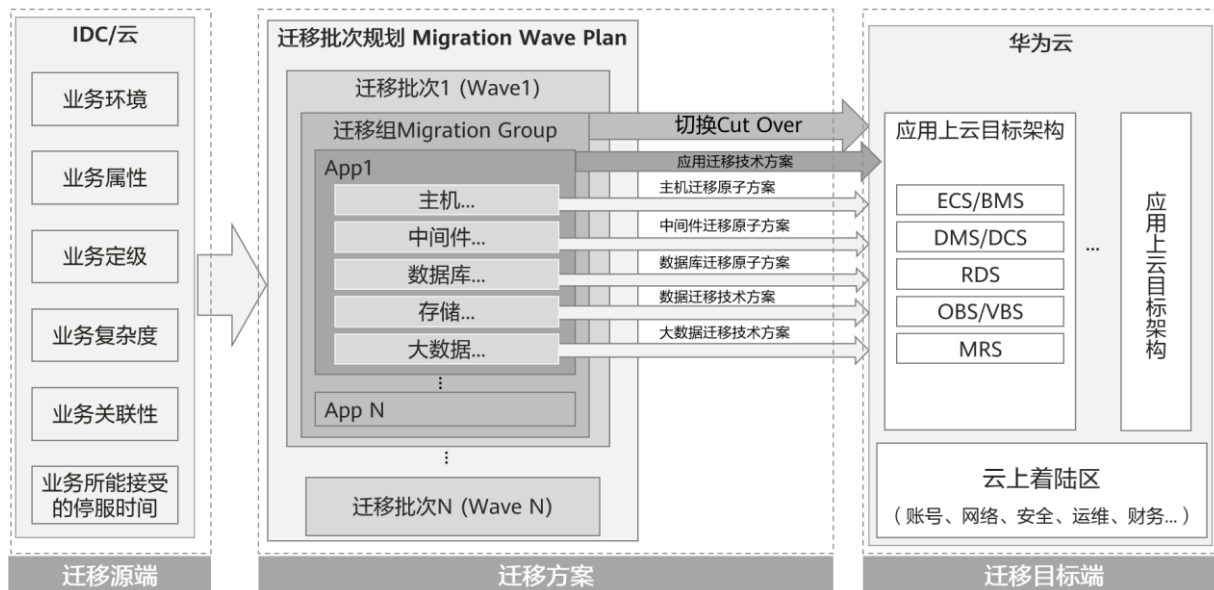
1. **目标和范围：**总结上云迁移试点的目标和范围，明确试点迁移的期望结果，描述试点涉及的应用程序、系统或业务流程，以及试点的时间、地点、参与人员等信息。
2. **迁移方法和策略：**总结采用的迁移方法和策略，描述采用的技术、工具和流程，以及与迁移相关的关键决策。
3. **成果评估：**评估上云迁移试点的效果，包括成功迁移的应用程序数量、迁移过程中的问题和挑战，以及解决方案和改进措施等，总结迁移试点对企业的业务影响和收益。
4. **技术和性能评估：**评估试点迁移后的系统和应用程序的性能和稳定性，考虑应用程序的可伸缩性、响应时间、数据传输速度等因素，总结试点迁移对系统性能和用户体验的影响。
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。

7 上云批次规划

7.1 相关术语说明

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。



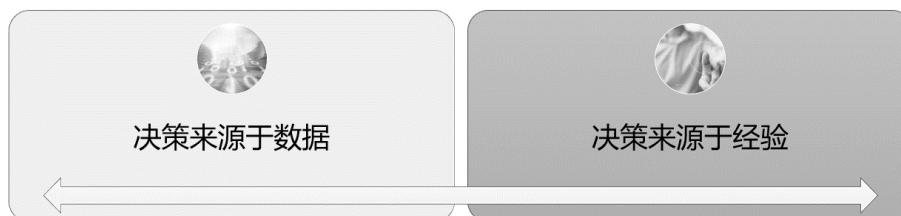
7.2 为什么要做批次规划

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。

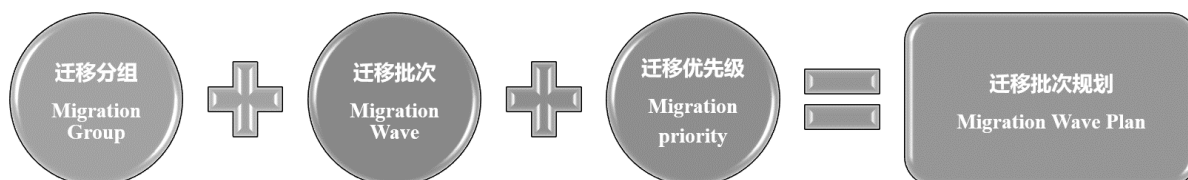
7.3 迁移批次规划的方法

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：分组、分批、优先级。

迁移批次规划既是科学也是艺术



迁移批次规划需要做3件事



7.3.1 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。

7.3.2 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：

迁移分批
参考原则

- 1 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

- 2 一个分批跨度1~2月最合适
 - 华为云的最佳实践表明，每个迁移批次的跨度应该在1~2个月，时间从部署到迁移和切换（不含准备），以确保有充足的资源来执行迁移过程，并将风险和影响降到最低。

- 3 一个分批不能太大，太大增加迁移风险
 - 根据华为云的最佳实践，建议一个分批不要迁移超过150台服务器，不要超过20个数据库，否则会增加项目管理和协同的复杂度，并增加问题定位的难度，大幅增加迁移风险。

- 3.1 分批太大的拆分原则
 - 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。

- 4 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。

- 5 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

7.3.3 迁移优先级

影响上云迁移优先级的影响因素有如下：

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
允许停机时间	停机时间长的先上，不停机的最后上
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。

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
	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

7.4 应用迁移批次规划样例

应用名称	上云策略	上云批次	第一批上云			第二批上云			第三批上云			第四批上云		
			2023.06.01-2023.06.30			2023.07.01-2023.07.30			2023.08.01-2023.08.30			2023.09.01-2023.09.30		

7.5 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：

1、整体迁移的场景：

- 1) 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。

2) 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。

2、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：

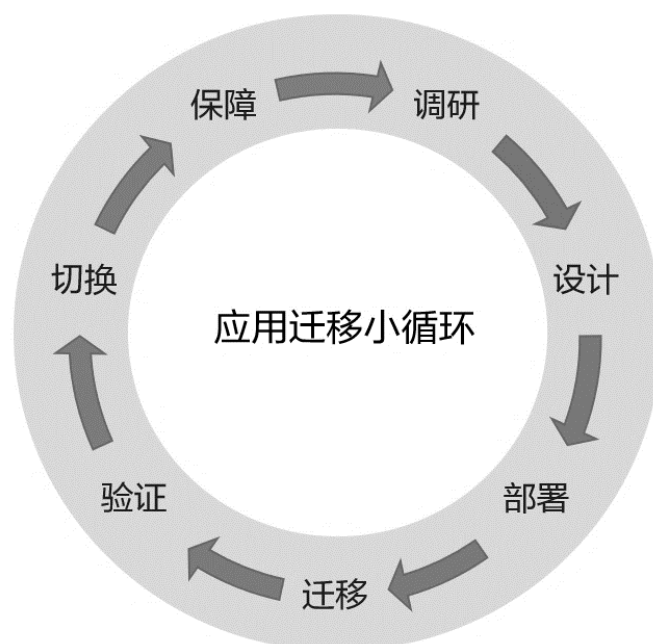
1. **按主题域进行分批：**按主题域分批需要考虑2个相关性，数据相关性和任务相关性。数据相关性是指将具有相似业务逻辑、相互依赖或紧密相关的数据放在同一批次中，以确保一致性和完整性。任务相关性是指将具有依赖关系的任务和数据集中放在同一批次中。这样可以保证任务在正确的数据上运行，并确保任务之间的顺序和一致性。基于这2个相关性，将主题域划分为多个迁移批次，将相关的任务和数据流集中在同一批次中，提高迁移效率和降低风险。
2. **尽量减少批次数量：**大数据迁移过程中会对数据进行抽取、转换、加载等操作，每个操作步骤都会增加复杂度和风险，影响数据的一致性，因此，应尽量减少批次的数量。
3. **批次间相互独立：**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。
4. **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。
5. **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。
6. **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。

8 应用上云迁移（小循环）

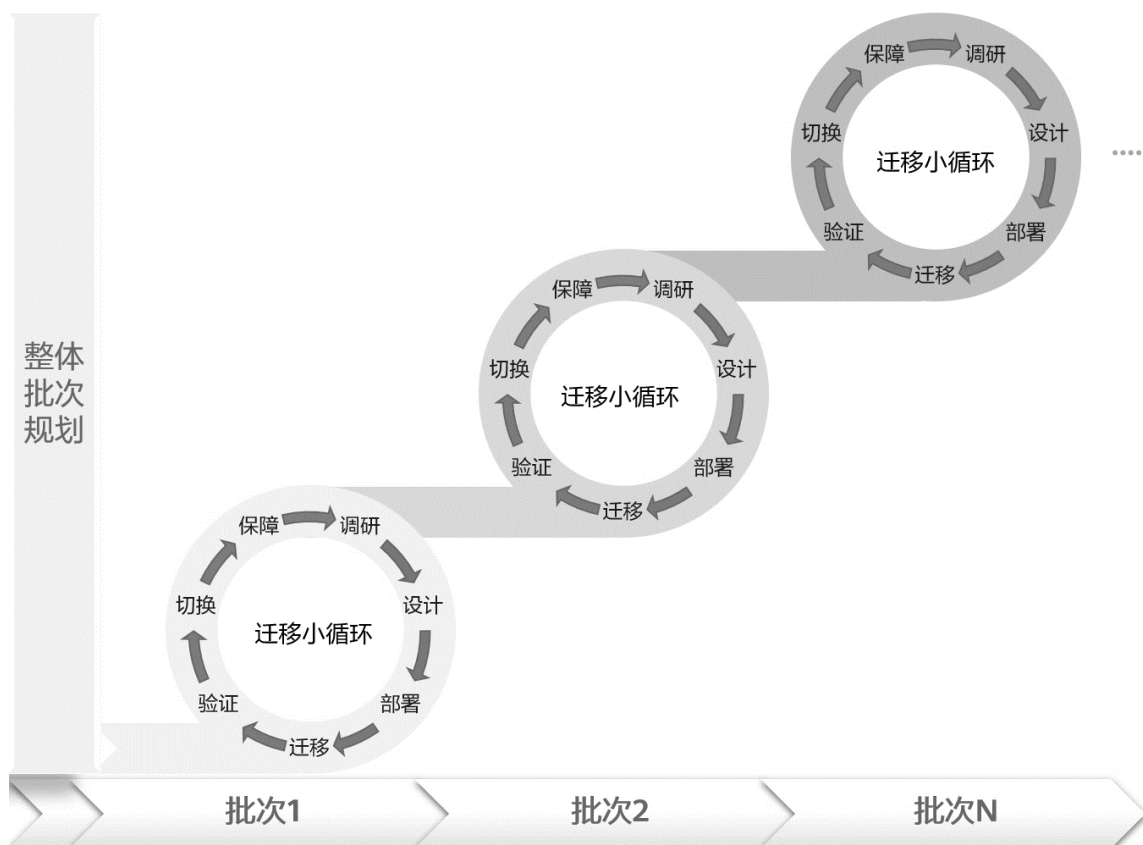
8.1 概述

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 Re-host 或 Re-platform，不含 Re-Factor（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：



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：

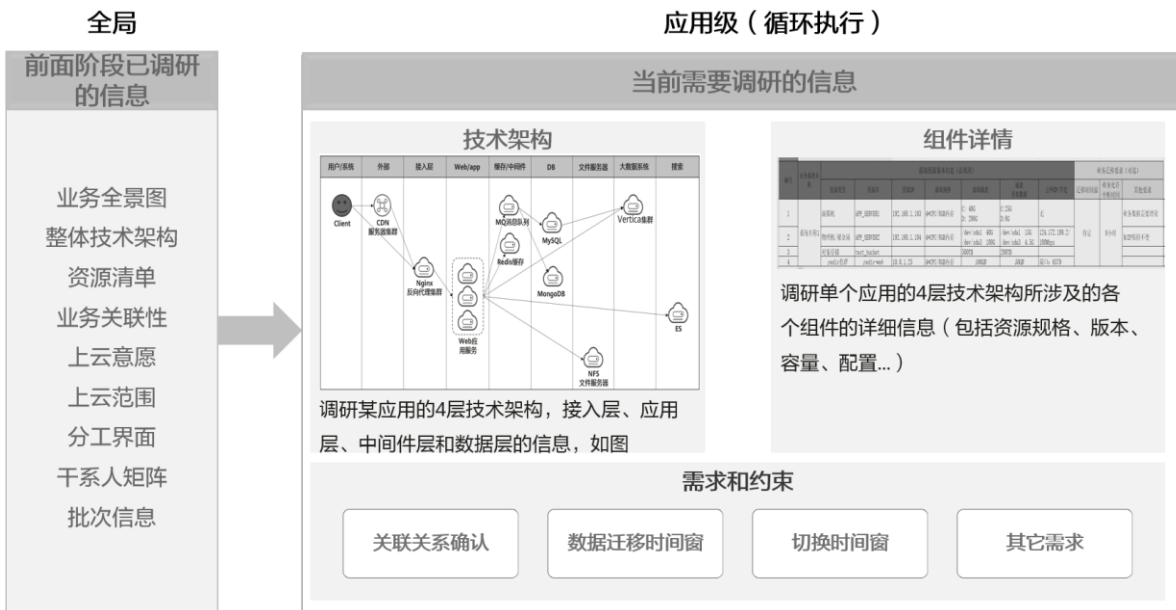


用小循环的每个阶段概述如下：

1. **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。
2. **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。
3. **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。
4. **迁移**：将源端应用和数据迁移到云上目标环境。
5. **验证**：进行数据和业务验证。
6. **切换**：进行切换演练，刷新 Runbook，实施正式切换。
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。

8.2 调研

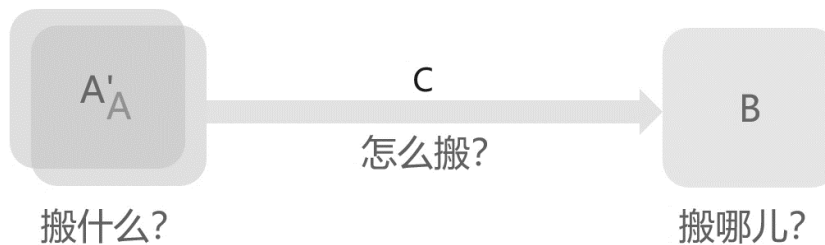
应用迁移小循环需要调研的信息主要集中在单个应用级别，前面阶段获取的调研信息可以复用，本阶段主要是“由粗到细”打开到很详细能够指导迁移实施的程度，调研方法论请参考第二章，需要调研的内容包括应用的技术架构、详细的组件信息。



8.3 设计（迁移方案）

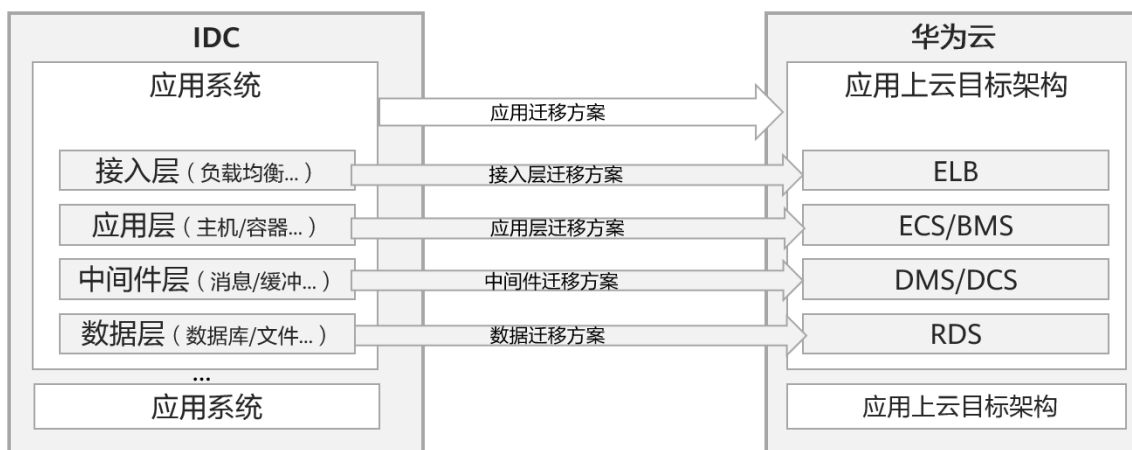
8.3.1 迁移方案概述

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。



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：



1. **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。
2. **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。
3. **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。
4. **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。

8.3.2 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：

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	解析应用的内外部分域名	<p>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。</p> <p>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。</p> <p>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。</p>

8.3.3 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。

8.3.3.1 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：

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）

8.3.3.2 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。

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

8.3.3.3 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，具体请参考基础设施现代化章节。

8.3.4 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。

8.3.4.1 Redis 迁移方案

1. 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。

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
-------------------------------	----------------------

2. 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

8.3.4.2 消息中间件迁移方案

1. 确定消息中间件的切换场景

适用产品	切换窗口	迁移方式
Kafka RabbitMQ RocketMQ ActiveMQ	切换时间窗口充足	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
	切换时间窗口有限	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

2. 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

8.3.5 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。

8.3.5.1 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。

1. 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	停机时间窗较长场景
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

2. SQLserver 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

3. 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	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

(推荐)			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

4. 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

8.3.5.2 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。

1. 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。

2. 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。

8.3.6 迁移工具兼容性查询

工具的兼容性以华为云官网发布的最新结果为准：

工具	兼容性查询地址
SMS	https://support.huaweicloud.com/productdesc-sms/sms_01_0013.html
DRS	https://support.huaweicloud.com/productdesc-drs/drs_01_0307.html
OMS	https://support.huaweicloud.com/productdesc-oms/oms_01_0038.html
CDM	https://support.huaweicloud.com/productdesc-cdm/cdm_01_0095.html
DCS	https://support.huaweicloud.com/migration-dcs/dcs-migration-090626002.html

8.4 设计（切换方案）

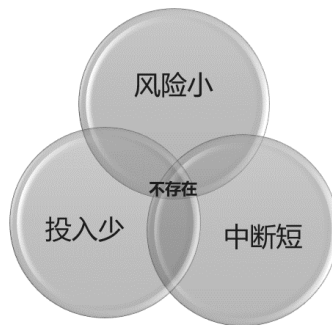
业务切换是整个上云迁移的关键环节，出问题会直接影响企业业务，不同业务对停服的要求是不一样的，比如，有些业务在切换期间是不允许停服的，停服会造成较大的业务损失；有些业务在切换期间是允许停服的，比如办公 OA 系统，夜间非工作期间可以停服；有些业务系统，为了更好的客户体验，希望切换期间部分浏览类的业务继续提供服务，只是涉及写操作的业务受到影响。设计切换方案时，对于不同的业务场景和停服要求，会面临多种方案的选择，下面详细介绍如何合适的切换方案。

8.4.1 如何选择停服不停服

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：

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，停止服务切换能充分保证数据一致性	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停读，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。



如何选择停服不停服：

1. 根据行业选择

不同行业有各自的行业标准和需求，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。

2. 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。

3. 根据项目周期选择

业务不允许停机，如果上云周期较长，时间充足，且企业具备不停机的改造能力，可以选择进行双写改造，实现不停机切换。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、人力投入少的停机切换方案。

4. 根据投入产出选择

不停机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，停机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。

8.4.2 停机切换方案

8.4.2.1 停机时长评估

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

上云迁移停机时长评估								
总停机时长 (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)			目标端拉起 (18~96分钟)		
源端业务停机	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	目标端业务拉起	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
应用层停机 (关停应用)	1~30	1、提前关停非核心业务，减少操作量 2、统一运维平台批量关停，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
中间件层停机 (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，减少检查的时间				应用测试	15~60	1、测试用例自动化 2、只测试核心测试用例
数据层停机 (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

停机时长例外情况：

- 1. 停机时长小于 30 分钟：**若停机时长要求小于 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，停机时长也有可能小于 30 分钟。
- 2. 停机时长大于 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，停机时长可能大于 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，停机时长约 8 个小时。

8.4.2.2 减少停机时长的方法（分钟级）

停机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，来减少停机时长。下图是四种减少停机时长的方法：

1、分批： • 将批次划分的足够小，减少切换工作量	2、自动化： • 切换操作自动化，如：配置修改修改自动化、测试自动化等。
减少停服时长的方法	
3、多次演练： • 提前识别正式切换时可能遇到的问题，减少问题定位处理时间	4、业务改造： • 通过业务改造实现两边业务双跑，将停机时长缩短到分钟级。

8.4.2.3 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

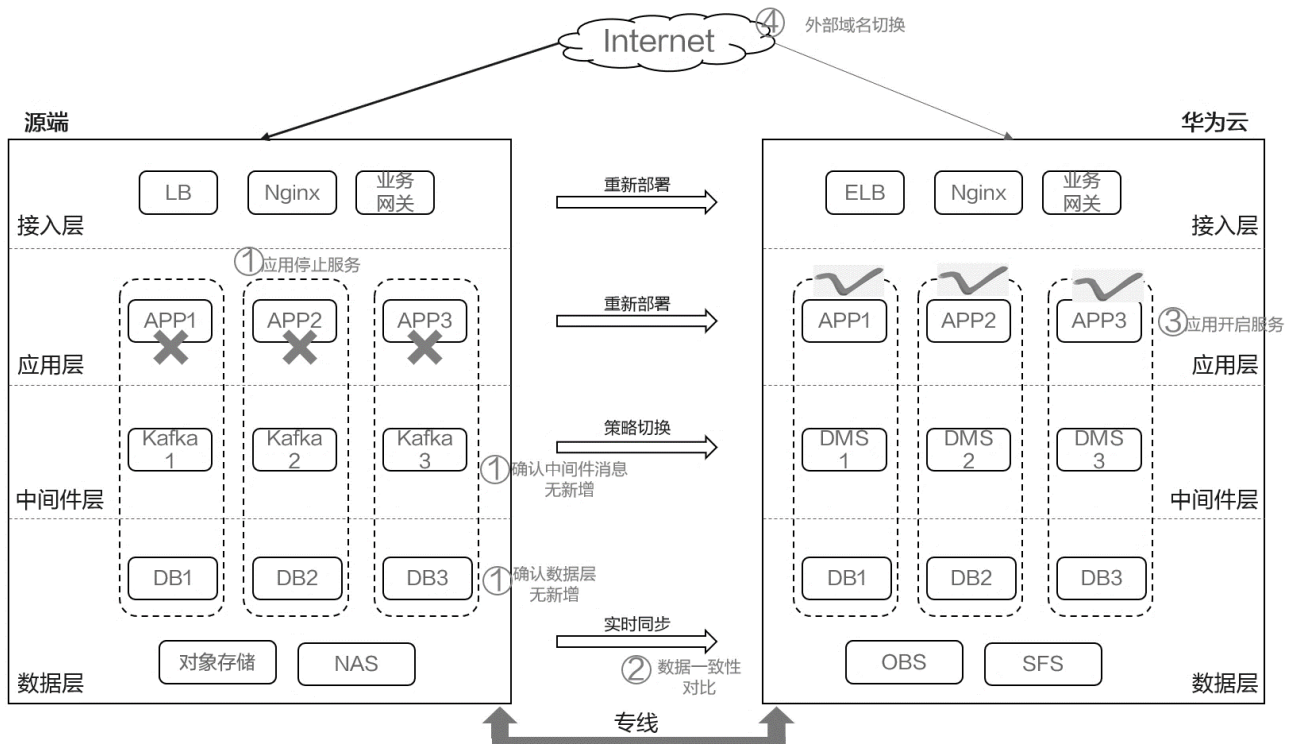
8.4.2.4 一把切（应用层和数据层整体停机后切换）

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；



8.4.2.5 应用层灰度切流，数据层整体切换

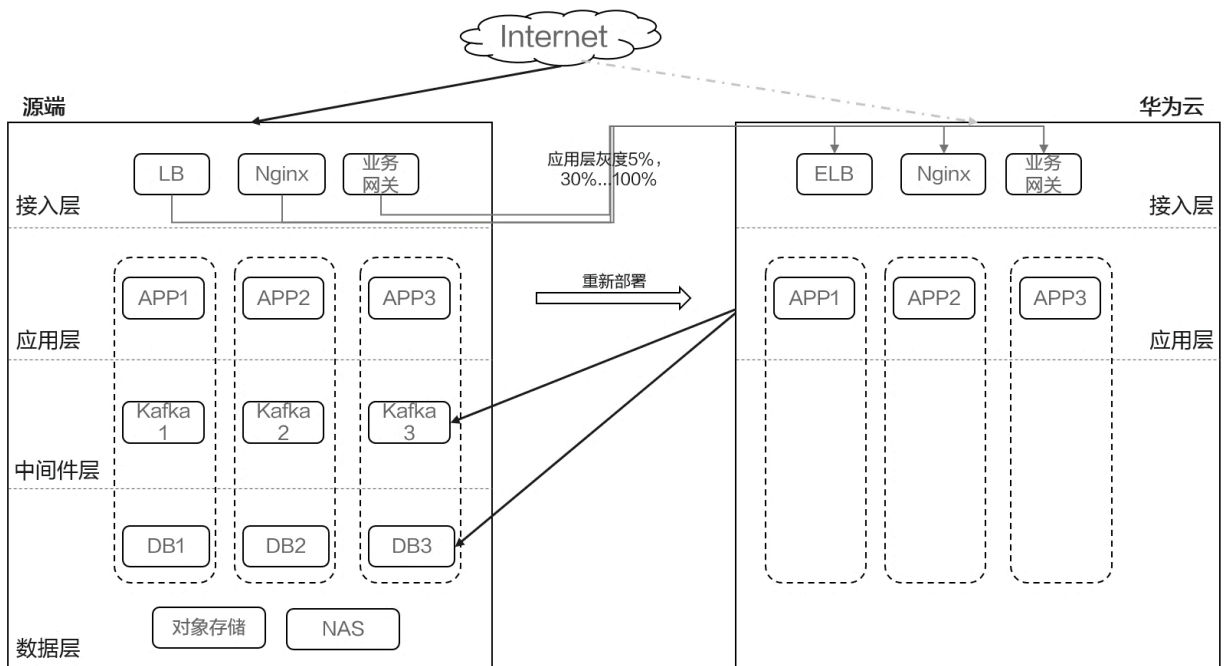
(一) 应用层灰度切流

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。

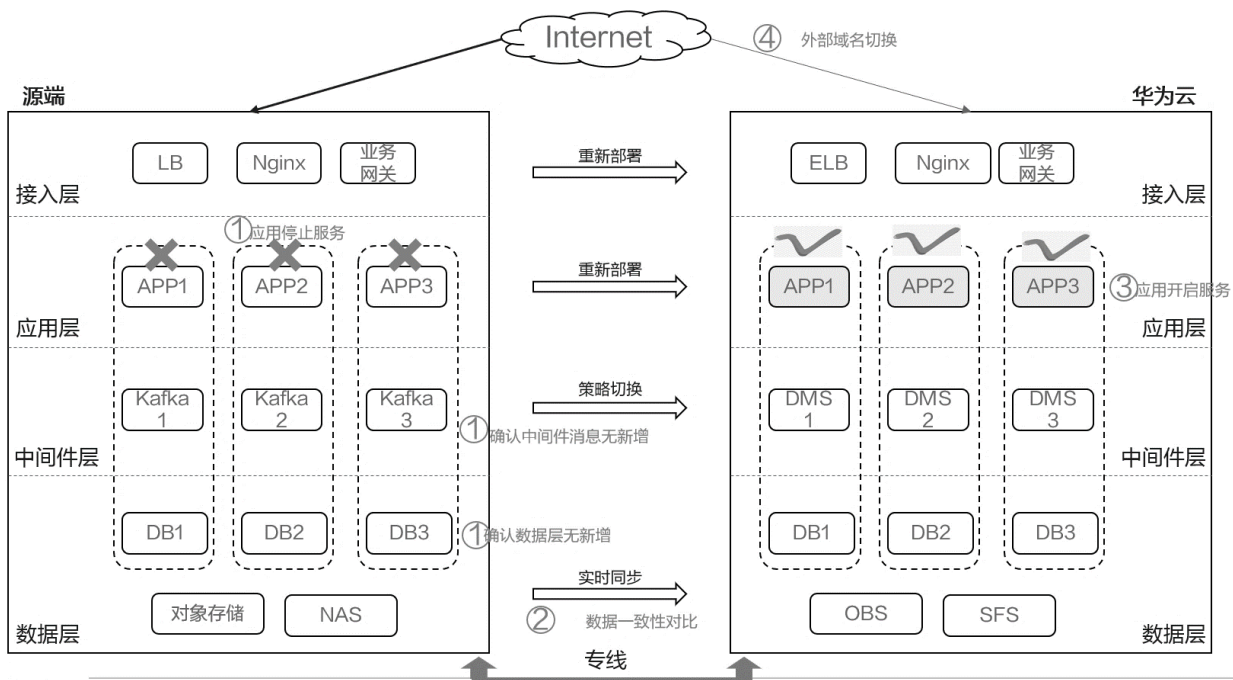
应用层灰度切流：

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。



(二) 数据层整体切换

- 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。



8.4.2.6 应用层灰度切流，数据层分批切换

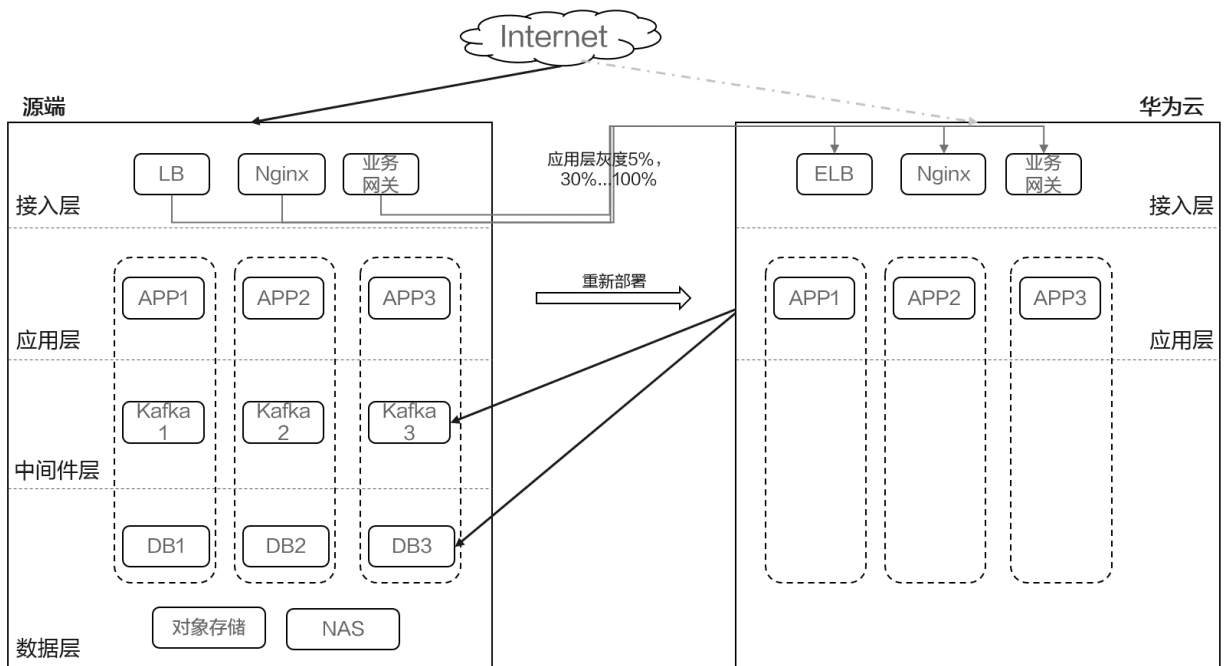
(一) 应用层灰度切流

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。

应用层灰度切流：

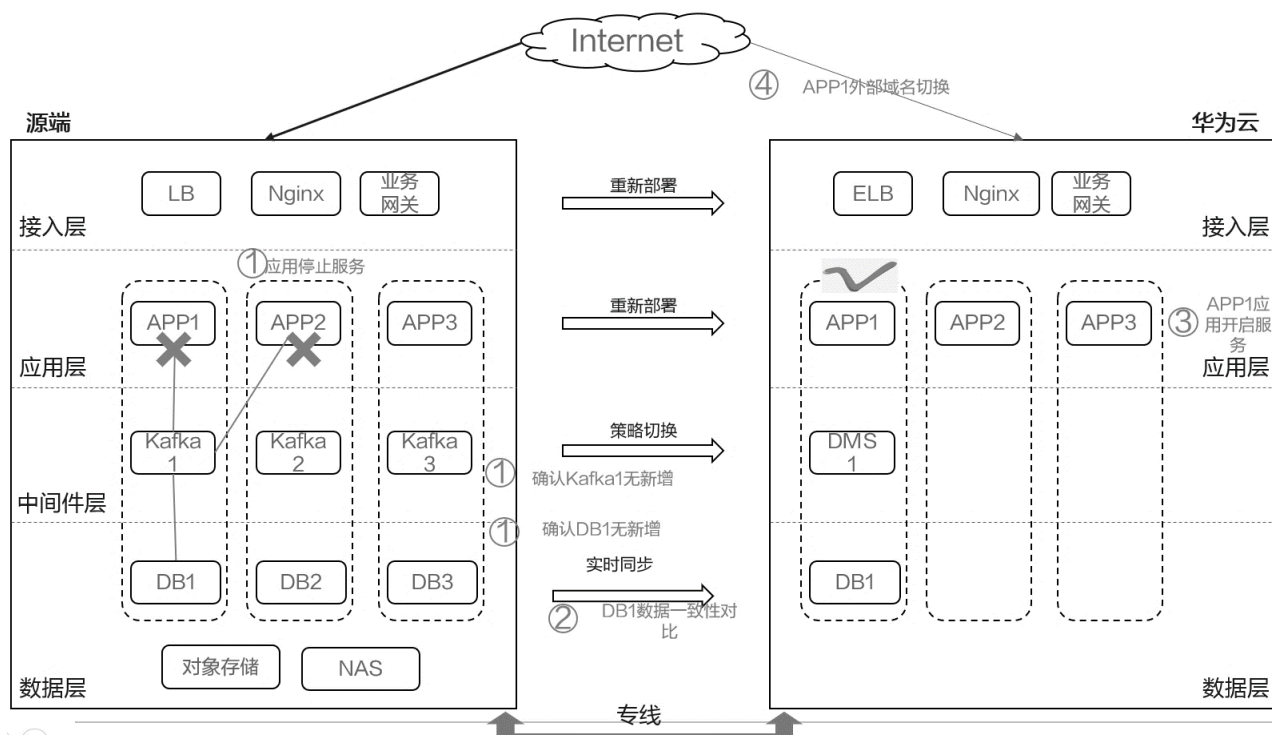
从源端接入层引流，按照 1%~30%，...100%逐步加大流量的方式，流量逐步灰度切换到华为云接入层。



(二) 数据层分批切换

某批次数据层切换过程：

- 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。



(一) 方案优缺点

优点:

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。

缺点:

1. 需要应用层和数据层梳理，需要花费大量人力和时间；
2. 跨云后，数据层回退难度较大；
3. 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。

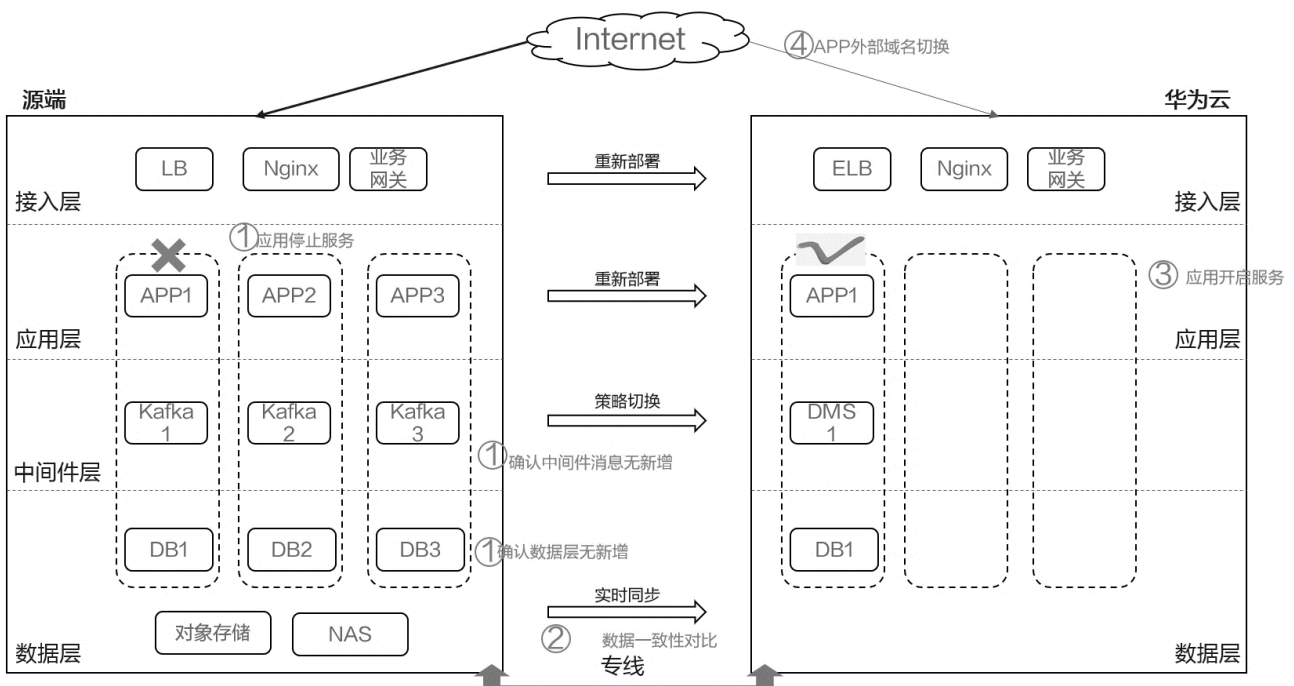
8.4.2.7 按照业务域分批切换

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。



8.4.3 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。

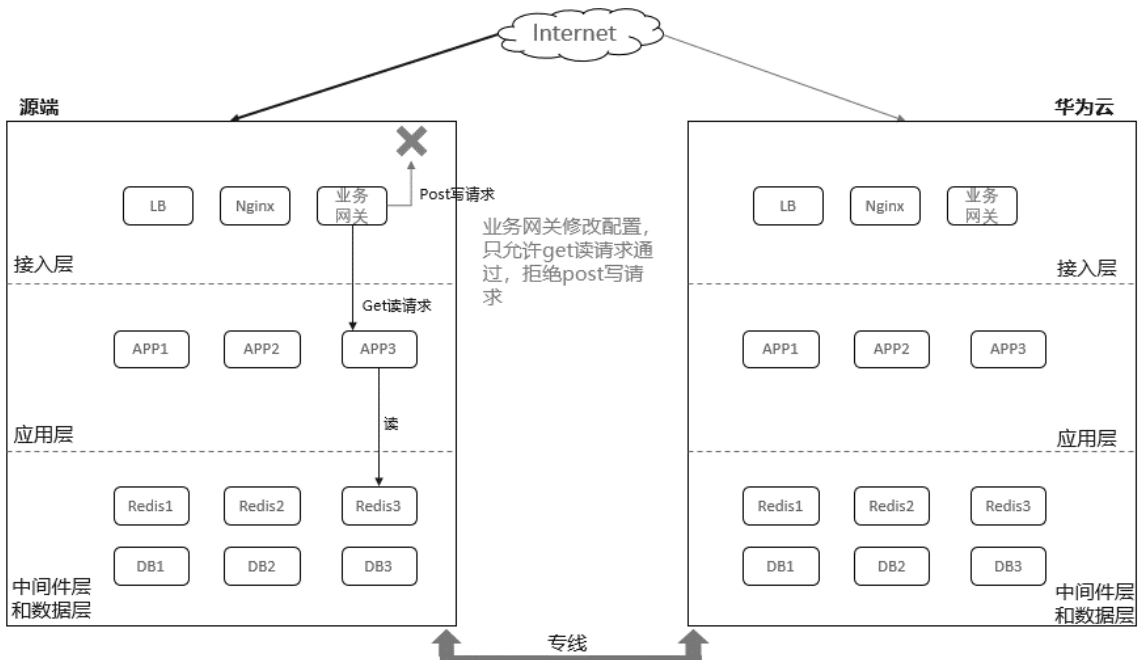
8.4.3.1 四种停写不停读切换方案对比

停写不停读切换有4种方案可以选择：

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
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

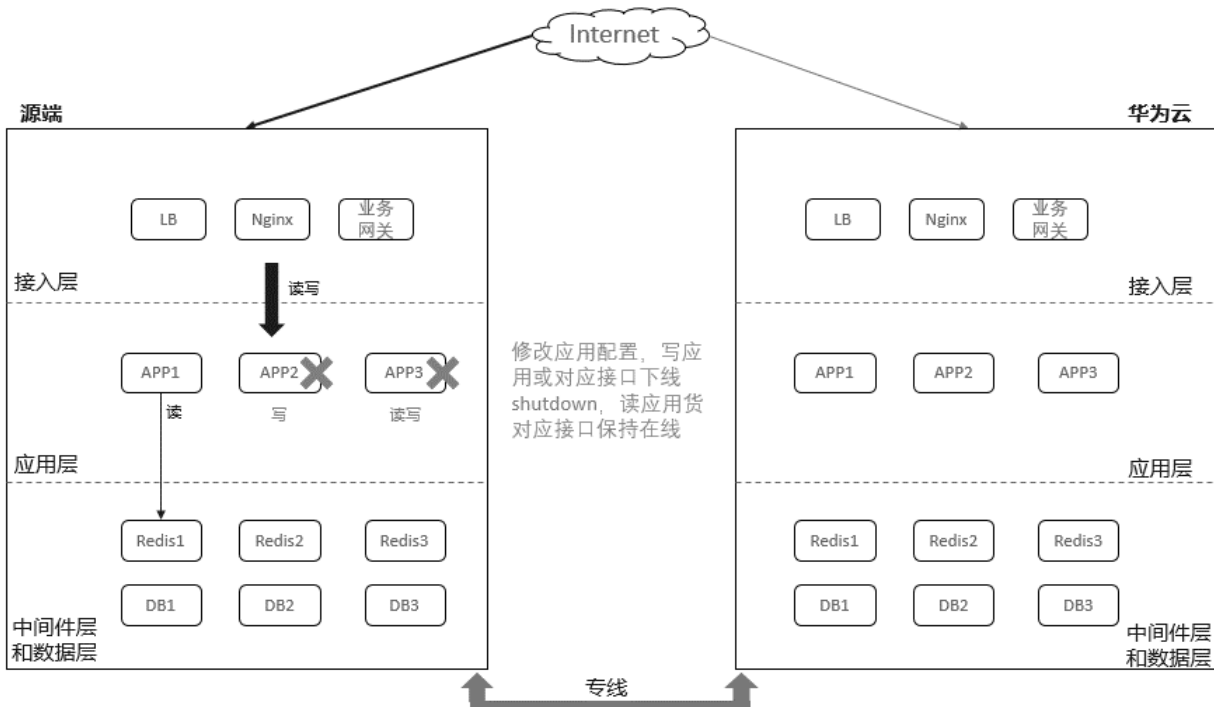
8.4.3.2 网关拦截

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。



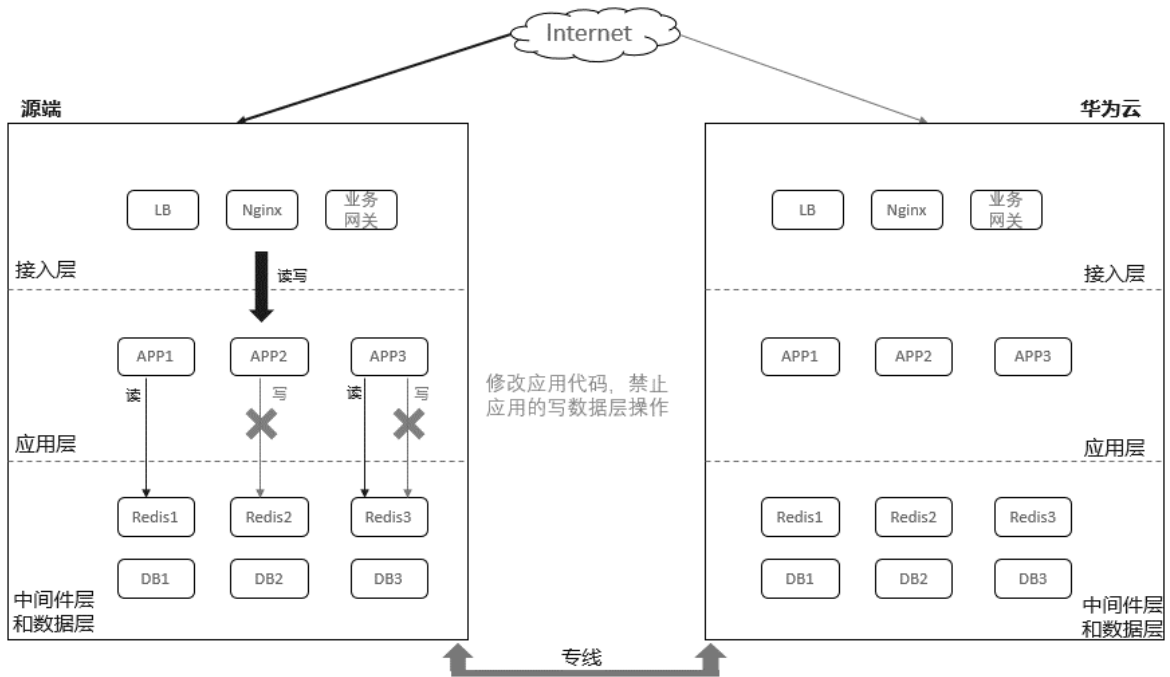
8.4.3.3 写服务关停

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。



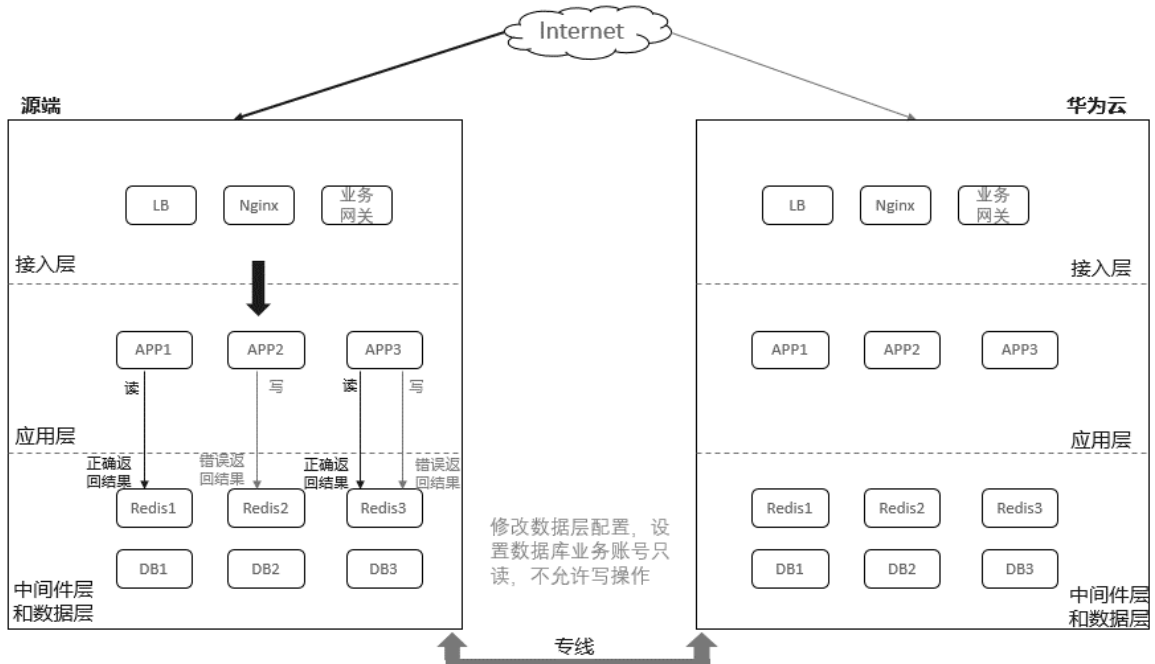
8.4.3.4 应用改造

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。



8.4.3.5 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。



8.4.4 不停服切换方案

8.4.4.1 应用层切换不停服方案

若只涉及到应用层的切换，可参考 8.4.2.5 应用灰度切流方案，切换期间不停服。

8.4.4.2 数据层或应用整体切换不停服方案

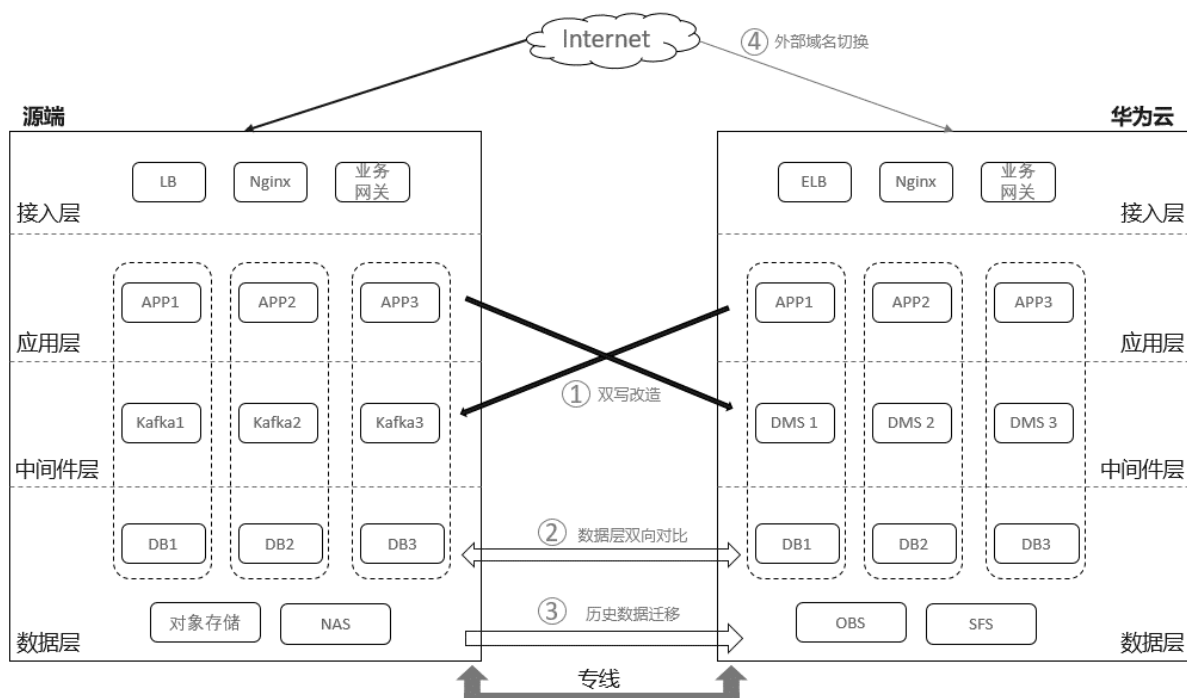
(一) 切换步骤

准备工作：

1. 华为云应用层和数据层已完成迁移；
2. 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：

1. 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；
2. 实时对比源端和目标端数据一致性；
3. 历史数据迁移至华为云数据层；
4. 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。



8.4.5 设计 Runbook

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。

8.4.5.1 Runbook 设计原则

Runbook 设计原则：

1. 一个 runbook 对应一次切换操作。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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：

1. 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。
2. 核心表数据比对结果不一致，需要决策是否回退。
3. 核心的 P0 测试用不通过，需要决策是否回退。
4. 性能验证不达预期，需要决策是否回退。

8.4.5.2 Runbook 角色设计

Runbook 通常涉及如下角色，职责如下：

序号	角色	职责
1	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
2	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。
3	引导人	引导 runbook 的执行，通报问题处理进展
4	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
5	决策组	由决策组负责人牵头对“决策点”进行决策
6	会务组	负责维护现场秩序，提供切换期间的会务保障。

说明：

1. 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）。

2. 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。

8.4.5.3 Runbook CheckList 设计

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

1. 人员和场地准备：

- 1) 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。
- 2) 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。
- 3) 确定切换的具体日期、入场签到时间、操作开始时间。
- 4) 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）。
- 5) 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。
- 6) 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。

2. 应用清单核对和操作脚本刷新

- 1) 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。
- 2) 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。
- 3) 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

3. 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。

- 1) 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。
- 2) 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。
- 3) 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。
- 4) 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。

- 5) 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。

8.4.5.4 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。

1、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：

- 1) 停服之前需挂停服公告，充分考虑用户感知。
- 2) 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。
- 3) 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。
- 4) 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。
- 5) 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。
- 6) 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。

2、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：

- 1) 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。
- 2) 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。
- 3) 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。

8.4.5.5 Runbook 参考模板

1. Runbook CheckList 参考

编号	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	
1	组织和保障准备		项目经理		是	<input checked="" type="checkbox"/>			
2			项目经理		是	<input checked="" type="checkbox"/>			
4	第三方/业态影		业务相关		是	<input type="checkbox"/>			
9	环境清单核对	应用清单检查并刷新启停	研发相关		是	<input type="checkbox"/>			
10			研发相关		是	<input type="checkbox"/>			
11		云服务基础检查项	运维相关		是	<input type="checkbox"/>			
12			运维相关		是	<input type="checkbox"/>			
13		数据库检查项	运维相关		是	<input type="checkbox"/>			
14			大数据相关		是	<input type="checkbox"/>			
15			大数据相关		是	<input type="checkbox"/>			
16			应用检查	运维相关		是	<input type="checkbox"/>		
17			执行脚本检查	运维相关		是	<input type="checkbox"/>		
18			运维相关		是	<input type="checkbox"/>			
19		日志系统检查	运维相关		是	<input type="checkbox"/>			

2. Runbook 操作步骤参考

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	计划预估耗时(分钟)	实际开始时间	实际结束时间	实际耗时	
1	XXX	1.1	XXX			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	-									
7	XXX	1.4	XXX			非阻塞	-									
8		1.4				非阻塞	-									
9	回退决策1:时间点XX之前完成上述步骤, 否则决策是否回退。							回退-决策点1								
10		21.1				阻塞执行										
11		21.2				阻塞执行										

8.5 部署 (目标环境和迁移环境)

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。

8.5.1 云资源开通及配置

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:

1. 在云平台 console 控制台手动创建云资源。
2. 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: ECS 资源创建 API 调用示例: https://support.huaweicloud.com/api-ecs/ecs_02_0101.html

3. 使用华为云提供的应用编排服务 AOS, 对资源进行编排和批量发放, 具体操作方法:

<https://support.huaweicloud.com/aos/index.html>

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。
脚本调用 API 开通	1、适用资源量比较大的场景。 2、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。	1、自动化操作：减少资源管理，减少人力投入 2、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 3、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 4、速度快：避免手动操作的繁琐 5、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	1、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 2、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 3、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。	1、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 2、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 3、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 4、可追踪性：带有审计功能，方便故障的追踪和回溯 5、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	1、学习成本高，需掌握编排模板语言和云服务相关知识 2、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 3、安全风险，需妥善保管资源编排过程中使用的敏感认证信息和密钥 4、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 5、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 6、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 7、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

总之，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。

8.5.2 迁移工具部署

华为云提供的迁移工具有：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、大数据迁移工具（CDM）、对象存储迁移工具（OMS）等

1. **资源发现与评估工具（RDA）**：资源发现与评估，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。

2. **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：
<https://support.huaweicloud.com/sms/index.html>
3. **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：
<https://support.huaweicloud.com/drs/index.html>
4. **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：
<https://support.huaweicloud.com/migration-dcs/dcs-migration-0713001.html>
5. **大数据迁移服务 (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：<https://support.huaweicloud.com/cdm/index.html>
6. **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：<https://support.huaweicloud.com/oms/index.html>

其中：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，需要部署在华为云 VPC 内的 ECS 云服务器上，具体配置方法见 RDA 页面文档；其它工具均会暂时占用 VPC 内网 IP 资源。

8.6 迁移

8.6.1 接入层迁移实施

(一) 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 \(https://support.huaweicloud.com/eip/index.html\)](https://support.huaweicloud.com/eip/index.html)。

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 \(https://beian.huaweicloud.com/\)](https://beian.huaweicloud.com/)。

(二) 负载均衡

1、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 \(https://support.huaweicloud.com/elb/index.html\)](https://support.huaweicloud.com/elb/index.html)。

2、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。

(三) 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 \(https://support.huaweicloud.com/vpn/index.html\)](https://support.huaweicloud.com/vpn/index.html)。

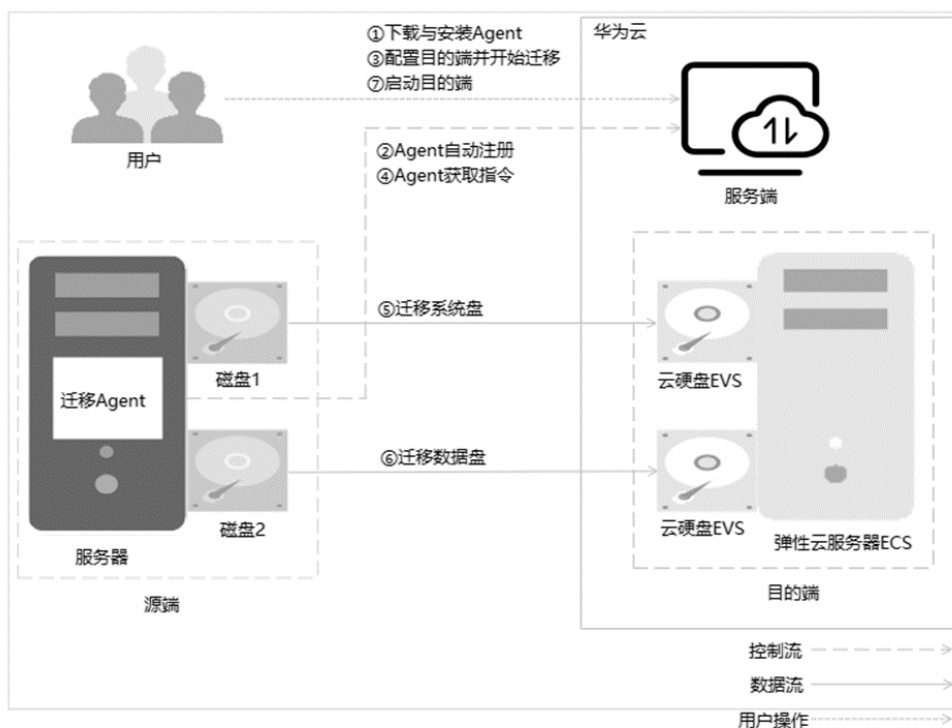
8.6.2 应用层迁移实施

8.6.2.1 主机迁移

主机迁移是典型的 Re-host 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：

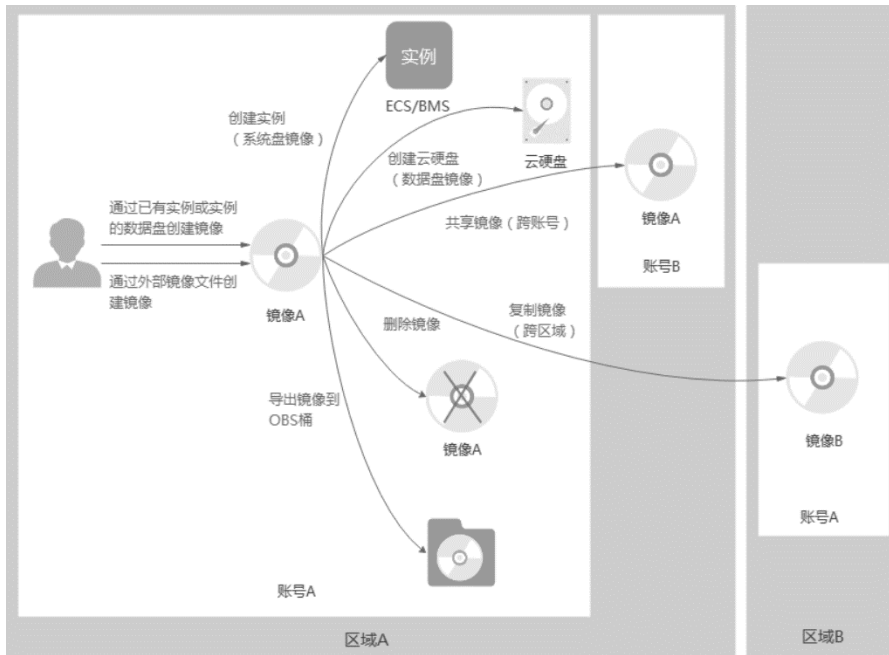
主机	迁移方式	适用场景	备注
虚拟机/物理机迁移	重新部署	OS 可变，停机时间长	
	SMS 工具迁移（免费）	OS 不变，版本一致，停机时间短	优先推荐，华为云有技术支持
	镜像导入/导出	OS 不变，版本一致，停机时间长	

- 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：**主机迁移服务(Server Migration Service, SMS)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：



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](https://support.huaweicloud.com/sms/index.html) (<https://support.huaweicloud.com/sms/index.html>)。

3. **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。



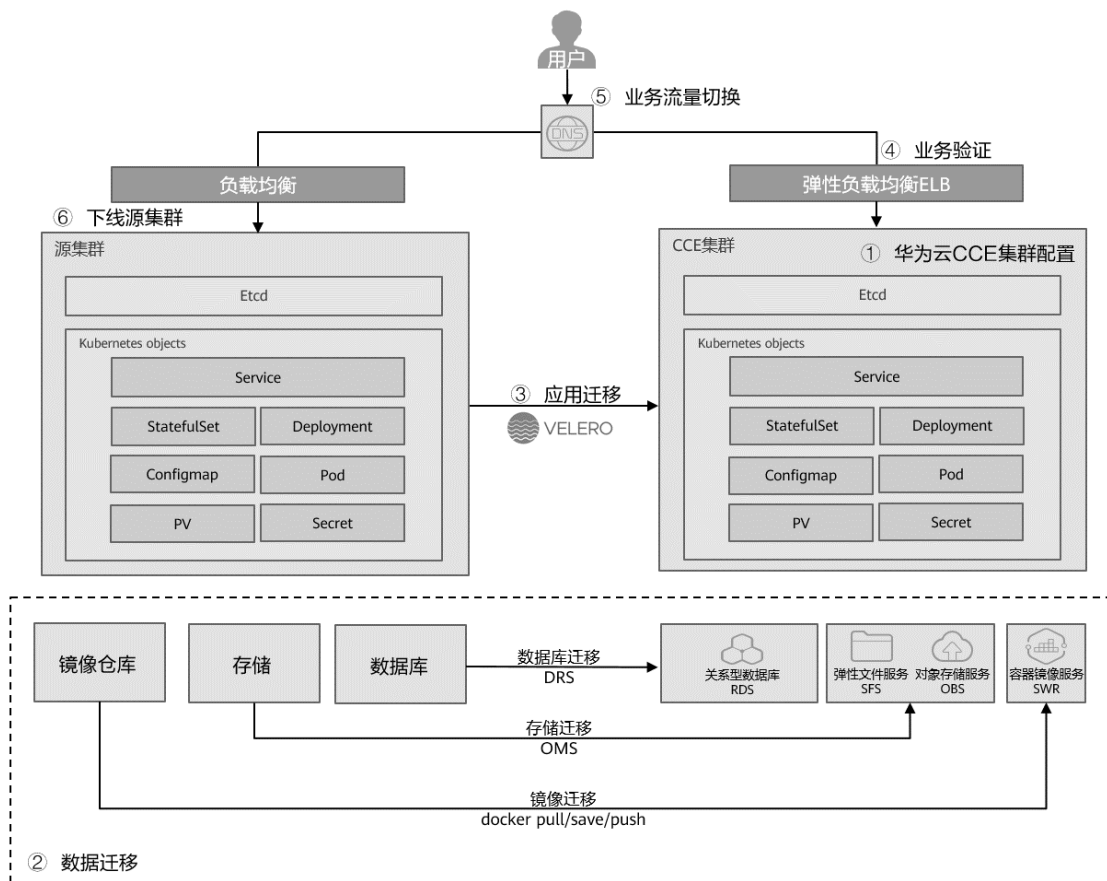
在源端与目标端无法通过网络使用 SMS 主机迁移服务进行整机迁移时，可以使用 IMS 镜像服务进行整机迁移。将源端服务器的系统盘和数据盘分别制作私有镜像，上传至华为云 OBS 对象存储服务中，在 IMS 镜像服务中，使用上传的外部镜像文件制作成私有镜像，最后使用私有镜像发放云服务器，完成整机迁移。迁移后的主机操作系统、系统配置，数据文件与源端服务器完全一致。关于主机迁移服务的更多详细信息，请参考 [IMS 镜像服务 \(https://support.huaweicloud.com/ims/index.html\)](https://support.huaweicloud.com/ims/index.html)。

8.6.2.2 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。



整体的容器镜像迁移步骤：

1. 导出第三方集群上使用的容器镜像。
2. 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。
3. 将导出的容器镜像文件上传到华为云 SWR。
4. 使用 docker pull 命令将镜像上传到华为云，具体操作方法请参见[客户端上传镜像 \(https://support.huaweicloud.com/usermanual-swr/swr_01_0011.html \)](https://support.huaweicloud.com/usermanual-swr/swr_01_0011.html)。

8.6.3 中间件层迁移实施

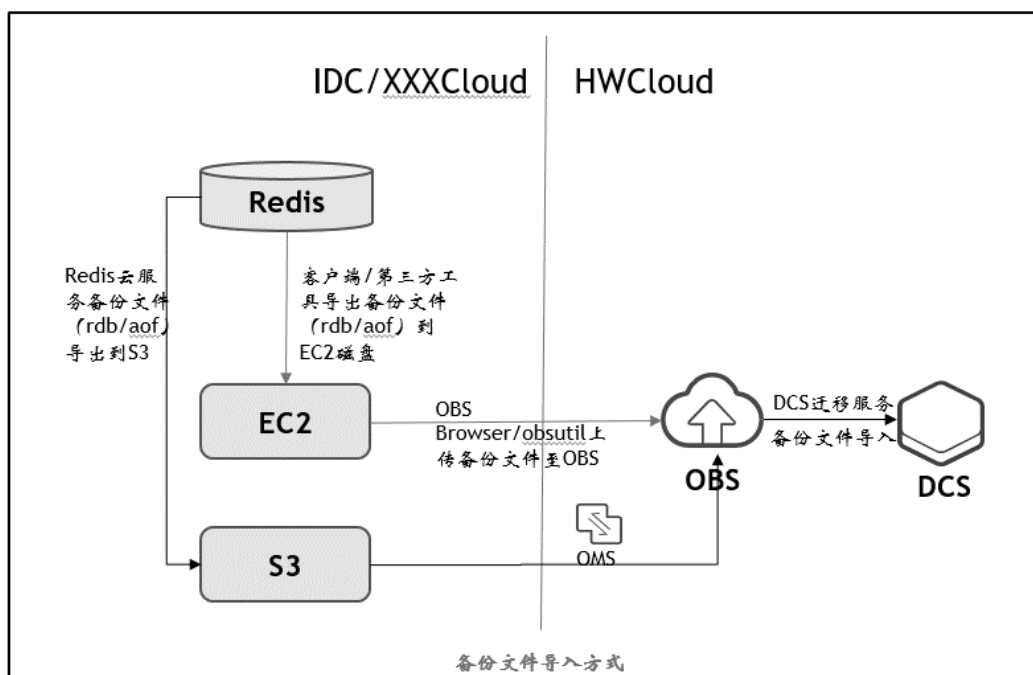
8.6.3.1 Redis 迁移

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。

1. 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。



迁移过程：

1. 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）；

AWS：使用备份功能将 rdb 文件输出到 S3 中。

2. 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。

3. 创建 DCS 迁移任务：

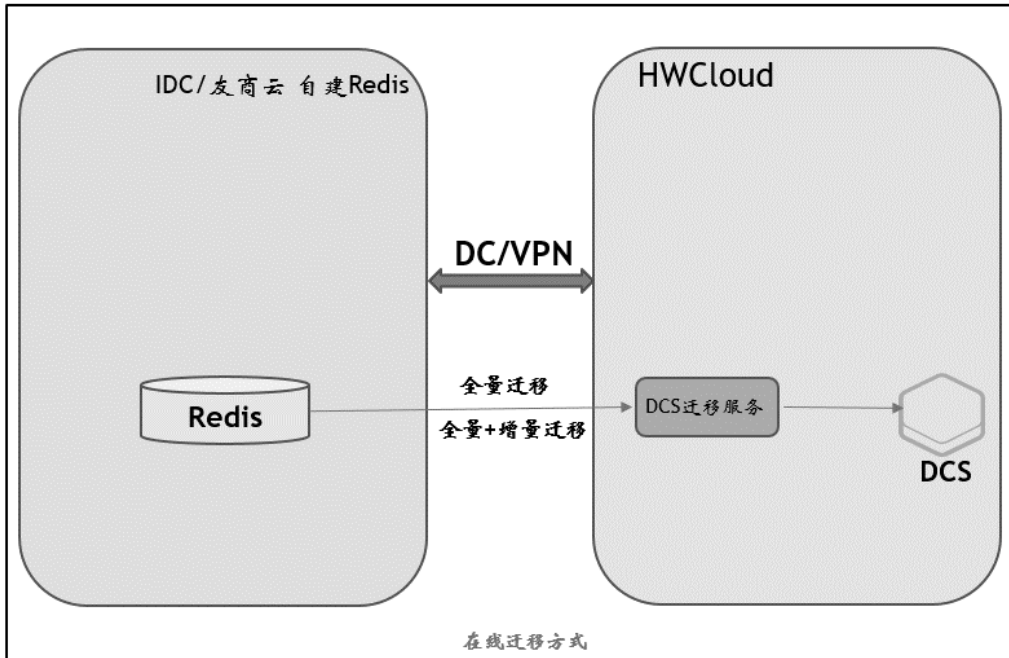
在 DCS 服务中的数据迁移模块创建迁移任务，选择备份文件导入方式，并选择 OBS 中源端的 aof/rdb 备份文件，填写其余选项，启动迁移任务。

4. DCS 数据查询对比两端数据

使用 redis 查询命令：info keypace

2. 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。



迁移过程：

1. 创建 DCS 迁移任务：

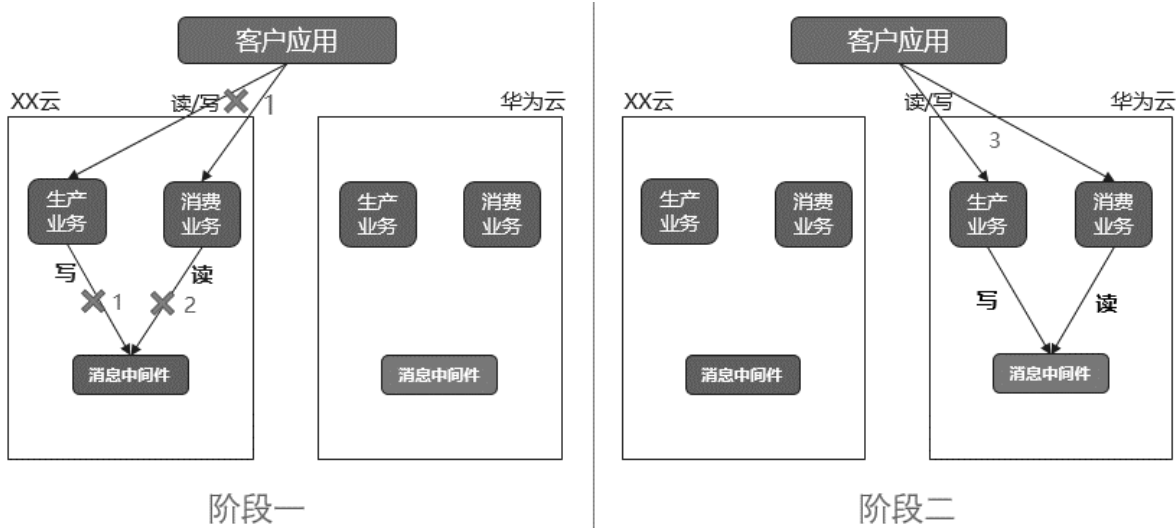
在 DCS 服务中的数据迁移模块创建迁移任务，选择在线迁移方式，根据需要选择去全量迁移或全量迁移+增量迁移方法，填写其余选项，启动迁移任务。

2. 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 keypace

8.6.3.2 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。



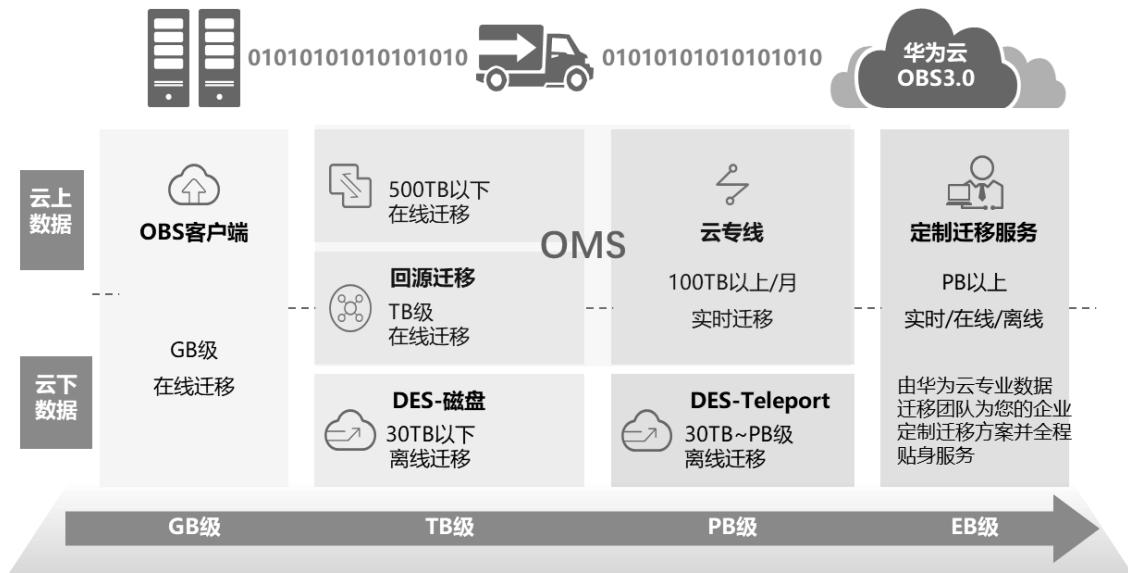
迁移步骤：

1. 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
2. 待消息消费完毕，停止消费相关业务
3. 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

8.6.4 数据层迁移实施

8.6.4.1 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：

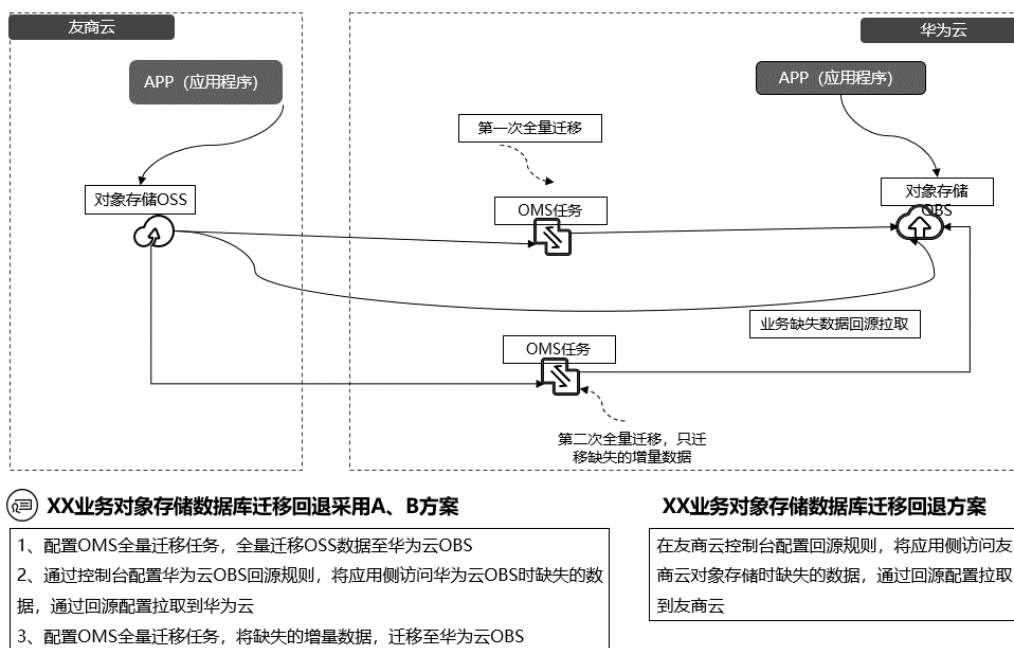


对象存储	迁移方式	适用场景	备注
------	------	------	----

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（Object Storage Migration Service, OMS）工具作为易用、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，具体内容请参考[对象存储迁移服务](https://support.huaweicloud.com/oms/index.html)（<https://support.huaweicloud.com/oms/index.html>）。

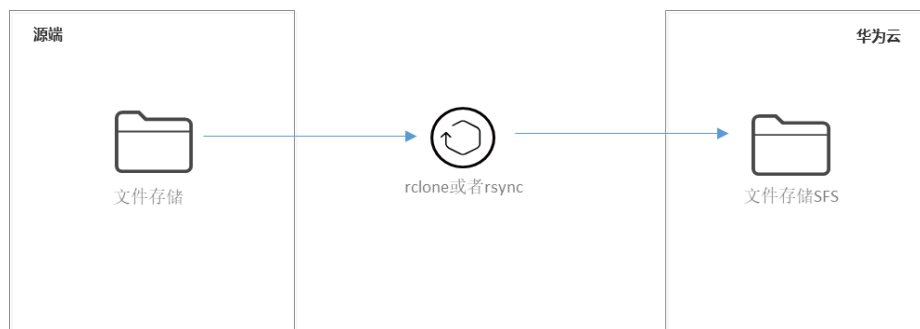


线下 DES 磁盘拷贝：云下数据也提供了数据快递服务（DES）来迁移数据，DES 是面向 TB 或 PB 级数据上云的传输服务，它使用物理存储介质（USB、eSATA 接口的磁盘等）、或 Teleport 向华为云传输大量数据，解决了上云带宽昂贵、传输时间长的难题。详细信息见[数据快递服务](https://support.huaweicloud.com/des/index.html)（<https://support.huaweicloud.com/des/index.html>）。

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。详细信息请见[上云迁移服务](https://www.huaweicloud.com/service/migration.html)（<https://www.huaweicloud.com/service/migration.html>）。

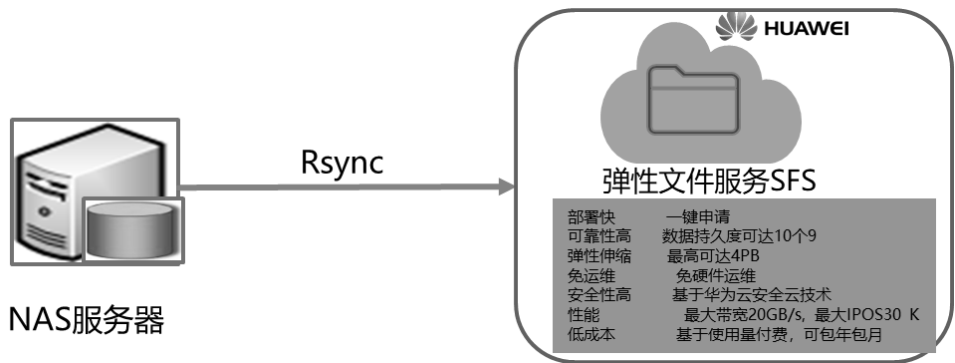
8.6.4.2 文件存储迁移

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**（Scalable File Service, 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），裸金属服务器（BMS）提供共享访问。NAS 文件存储迁移时，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。



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。



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：

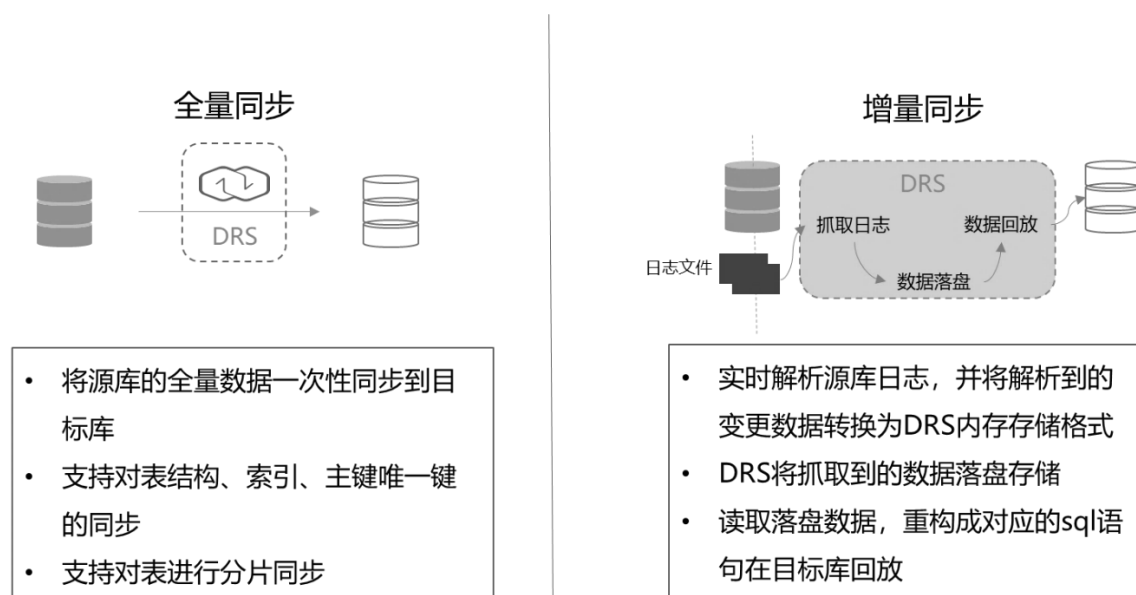
1. 文件增量同步，速度快，效率高，占用资源少。
2. 通过 SSH, RSH 等模式可对第三方平台跨网络开放。
3. 服务端不想共享时，只需停止 Rsync 服务，不影响其它业务。
4. 支持镜像方式数据拷贝，适合于互联网模式下的静态文件分布式部署，可扩充性好。

8.6.4.3 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：

1. 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。
2. 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。
3. 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。

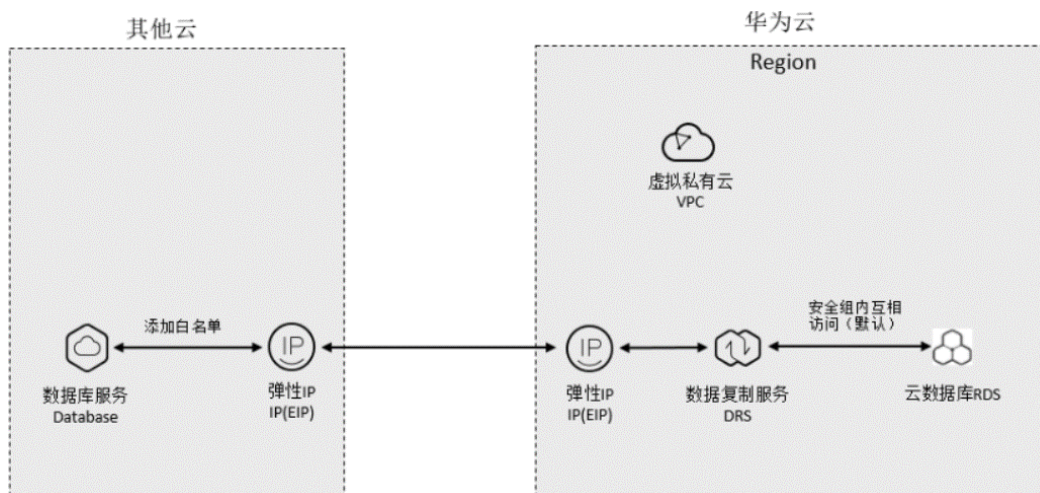
华为云针对于数据库的迁移提供了数据复制服务（Data Replication Service，DRS），DRS 服务是一种易用、稳定、高效，用于数据库平滑迁移和数据库持续同步的云服务。DRS 围绕云数据库，降低了数据库之间数据流通的复杂性，有效的减少数据传输的成本。数据复制服务支持多种数据源之间的数据流通，实时迁移、备份迁移、实时同步、数据订阅和实时灾备对不同数据库的支持不同，详细情况参考 [DRS 服务（https://support.huaweicloud.com/productdesc-drs/drs_01_0307.html）](https://support.huaweicloud.com/productdesc-drs/drs_01_0307.html)。



数据库的迁移方案以 DRS 迁移为主，逻辑导出导入辅助数据库的迁移。了解更多的数据库迁移，请查看 [华为云数据库迁移上云指南（https://www.huaweicloud.com/special/zijiantords.html）](https://www.huaweicloud.com/special/zijiantords.html)。

(一) MySQL 迁移到华为云 RDS for MySQL

1. 部署架构

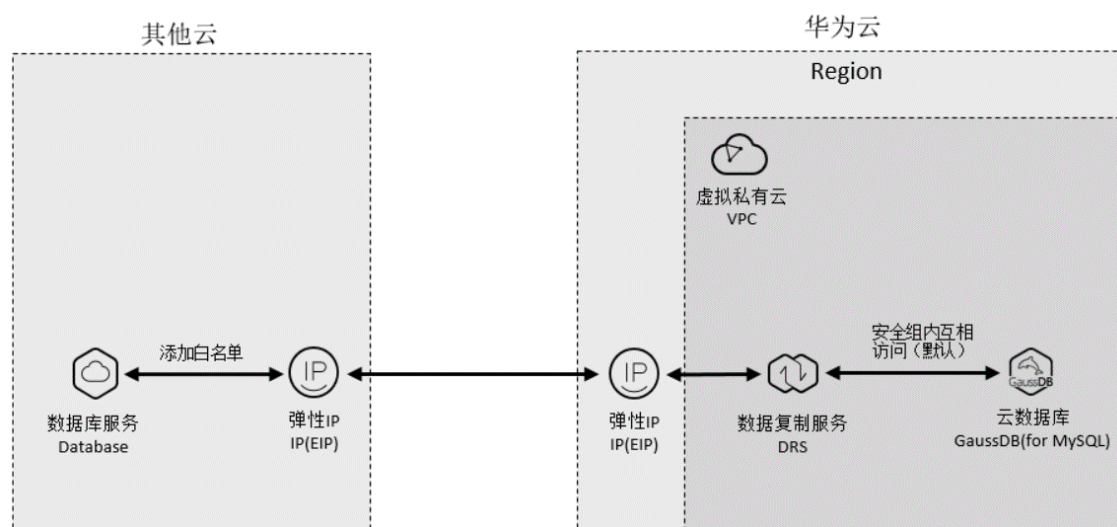


2. 操作步骤

具体操作步骤请参照华为云 DRS 文档《其他云 MySQL 迁移到云数据库 RDS for MySQL》
https://support.huaweicloud.com/bestpractice-drs/drs_02_0009.html

(二) MySQL 迁移到 GaussDB(for MySQL)

1. 部署架构

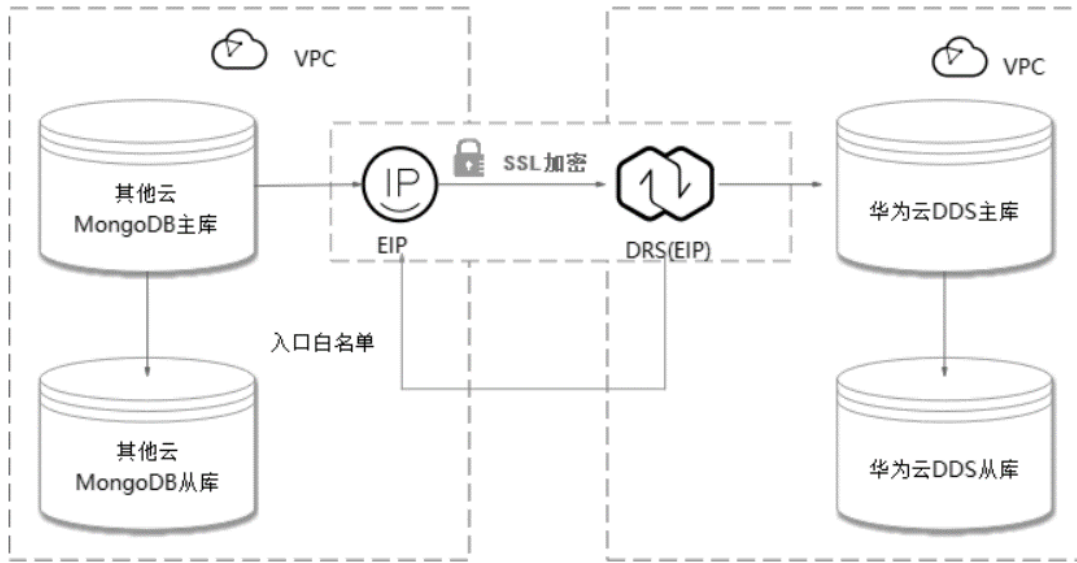


2. 操作步骤

具体操作步骤请参照华为云 DRS 文档《其他云 MySQL 迁移到 GaussDB(for MySQL)》
https://support.huaweicloud.com/bestpractice-drs/drs_06_0018.html

(三) MongoDB 迁移到 DDS

1. 部署架构



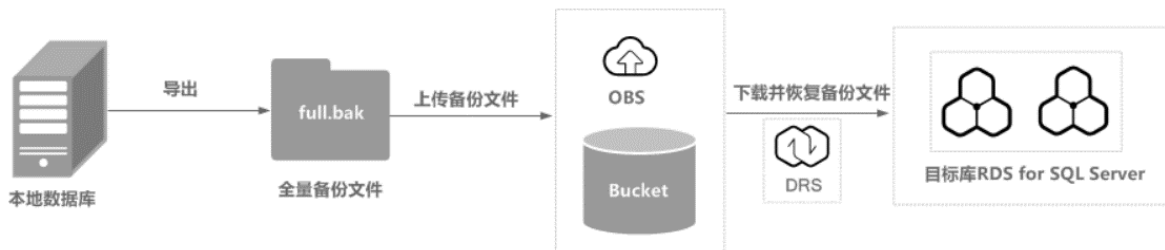
2. 操作步骤

具体操作步骤请参照华为云 DRS 文档《[其他云 MongoDB 迁移到 DDS](#)》

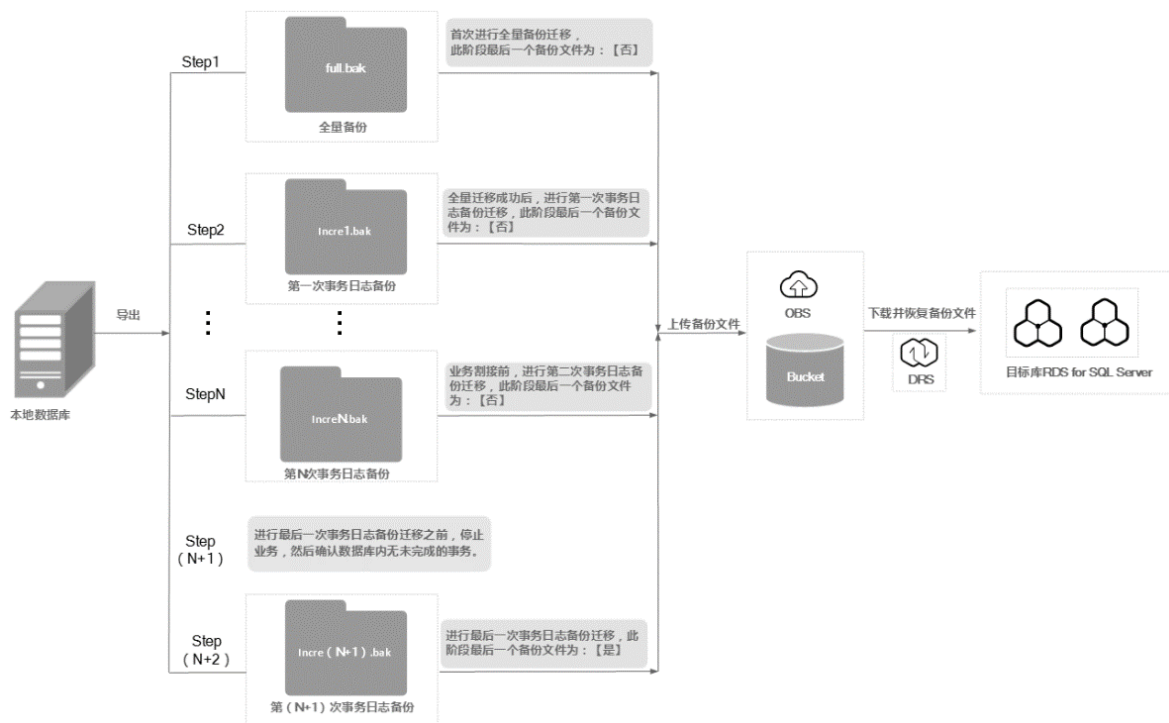
https://support.huaweicloud.com/bestpractice-drs/drs_01_0005.html

(四) 本地 Microsoft SQL Server 备份迁移华为云 RDS for SQL Server 实例

1. 部署架构（全量迁移）



2. 部署架构（全量+增量）



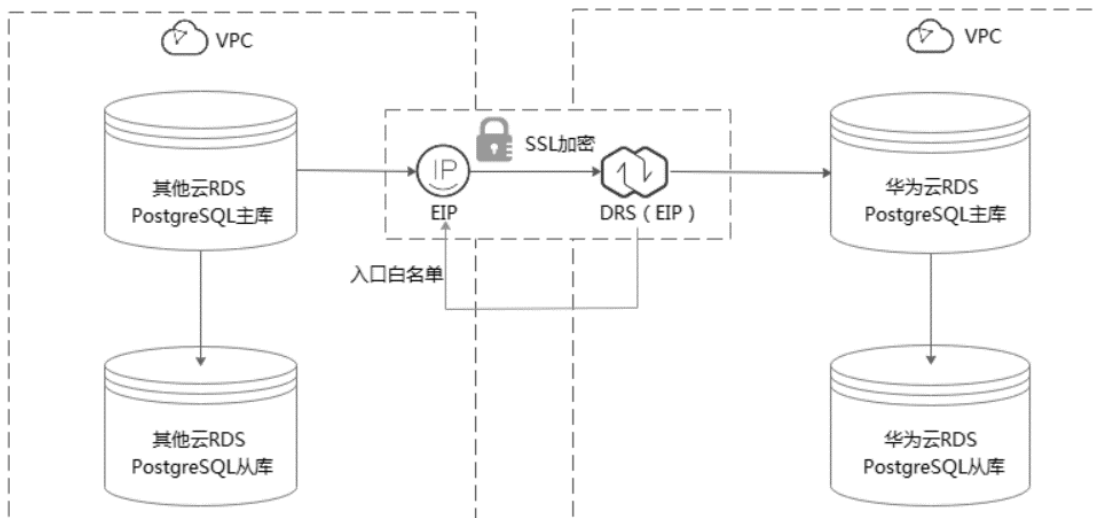
3. 操作步骤

具体操作步骤请参照华为云 DRS 文档 《本地 Microsoft SQL Server 备份迁移至本云 RDS for SQL Server 实例》

https://support.huaweicloud.com/bestpractice-drs/drs_04_0003.html

(五) PostgreSQL 同步到 RDS for PostgreSQL

1. 部署架构 (全量迁移)



2. 操作步骤

具体操作步骤请参照华为云 DRS 文档 《其他云 PostgreSQL 同步到 RDS for PostgreSQL》

https://support.huaweicloud.com/bestpractice-drs/drs_01_0004.html

8.6.5 迁移实施常见问题及应对

1. 主机迁移常见问题处理。

参考：https://support.huaweicloud.com/sms_faq/sms_faq_0060.html

2. Redis 数据迁移常见问题处理。

参考：https://support.huaweicloud.com/dcs_faq/dcs-faq-0713007.html

3. 对象存储数据迁移常见问题处理。

参考：https://support.huaweicloud.com/oms_faq/oms_faq_gaopin.html

4. 数据库迁移常见问题。

参考：https://support.huaweicloud.com/drs_faq/drs_04_0025.html

8.7 验证

8.7.1 数据验证

8.7.1.1 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：

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，数据为用户最核心的资产，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。
--	--	---------------------

8.7.1.2 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：

1. 数据库数据一致性验证的方法：

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。

2. 中间件数据一致性验证的方法：

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。
--	--	---------

3. 文件类数据一致性验证的方法：

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。

8.7.2 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测试和性能测试等。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测试，

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。

8.7.2.1 功能验证

(一) 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：

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。

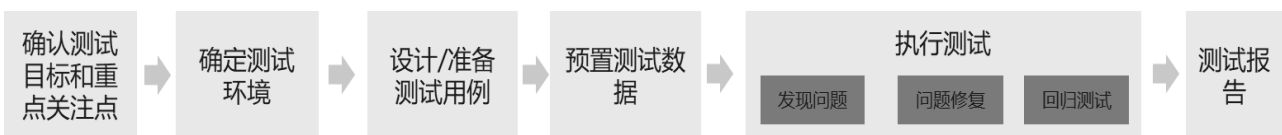
(二) 功能测试的目的

1. 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
2. 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。

(三) 功能测试的方法

1. 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。
2. 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。
3. 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。
4. 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。

(四) 功能测试的流程



1. **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。
 - 1) 系统功能：如促销活动，用券支付、退货反券等
 - 2) 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。

3) 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。

2. **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。

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

3. **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。

1) 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。

2) 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。

3) 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。

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。
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。

评估测试用例覆盖率: 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
...

- 4. 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。
- 5. 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。
- 6. 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。

8.7.2.2 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，需要进行测试验证：

(一) 性能测试内容包括如下三类：

测试内容	说明
云服务的性能测试	针对某个云服务进行性能测试，比如数据库，Hbase、存储的 IOPS 等。
应用的接口性能测试	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。
应用整体的性能测试	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。

(二) 这三类性能测试的目的如下：

测试内容	目的
云服务的性能测试	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。
应用的接口性能测试	针对某几个接口评估接口的极限负载能力
应用整体的性能测试	<ol style="list-style-type: none"> 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。

(三) 性能测试方法

1. 云服务的性能测试（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：

- 1) **TPS/QPS**：衡量吞吐量。
- 2) **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。
- 3) **并发量**：同时处理的查询请求的数量。
- 4) **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。



CPU/内存	建议连接数	TPS/QPS	IPv6
<input type="radio"/> 2 vCPUs 4 GB	1,500	334 6,673	不支持
<input checked="" type="radio"/> 2 vCPUs 8 GB	2,500	552 11,039	不支持
<input type="radio"/> 4 vCPUs 8 GB	2,500	756 15,122	不支持
<input type="radio"/> 4 vCPUs 16 GB	5,000	1,062 21,249	不支持
<input type="radio"/> 8 vCPUs 16 GB	5,000	1,338 26,756	不支持
<input type="radio"/> 8 vCPUs 32 GB	10,000	2,117 42,335	不支持

当前选择实例：通用型 | 2 vCPUs | 8 GB, 建议连接数: 2500, TPS/QPS: 552 | 11039

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：

- 1) cpu 性能
- 2) 磁盘 io 性能
- 3) 调度程序性能
- 4) 内存分配及传输速度
- 5) POSIX 线程性能
- 6) 数据库性能(OLTP 基准测试)

2. 应用接口压测

方法	工具	压测方式	优点	缺点
方法一	CPTS	基于华为云 CPTS 工具	1、支持多协议、高并发、复杂场景的测试 2、专业性能测试报告，应用性	1、执行成本高，前期业务梳理和脚本编写耗时较长。 2、对测试人员技术要求较

		完成接口压测。	能表现一目了然 3、与生产环境核心业务不产生交互，不会对现网产生影响 4、接口测试对其他业务依赖较少，可以基于单业务系统进行。	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。
方法二	Goreplay 流量复制	在业务网关部署 Goreplay 工具，复制现网流量，在目的端进行回放。	1、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 2、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。	1、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。 2、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。 3、只支持http协议，对于https、tcp、udp等无法录制

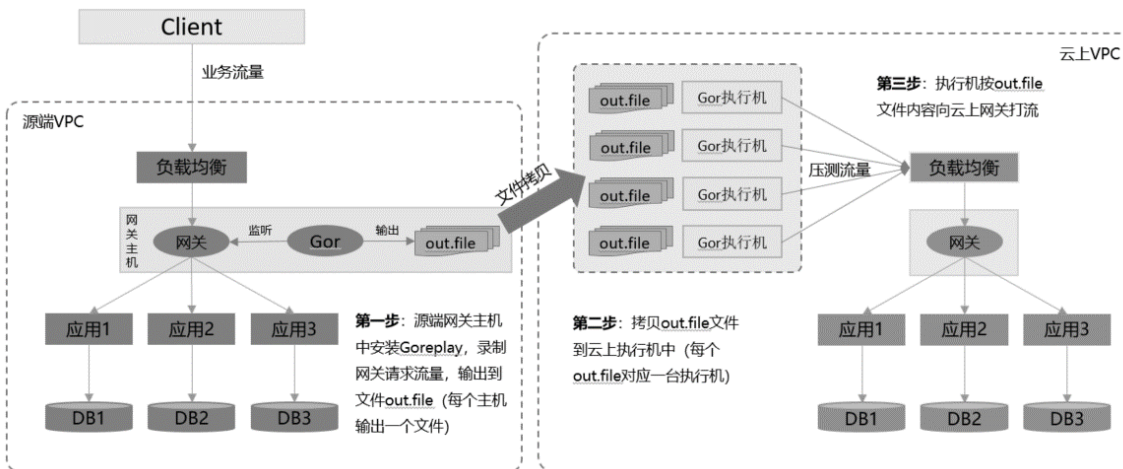
1) 华为云 CPTS 做压测

参考官网说明：<https://support.huaweicloud.com/cpts/index.html>

2) 通过 Goreplay 流量复制做压测

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：



注意事项：

1. 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，Gor 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。
2. 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. 应用整体压测

应用整体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，以评估系统在高负载下的性能和稳定性，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压测场景：

- 1) 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。
- 2) 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。
- 3) 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。
- 4) 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。
- 5) 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。

8.8 切换

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。

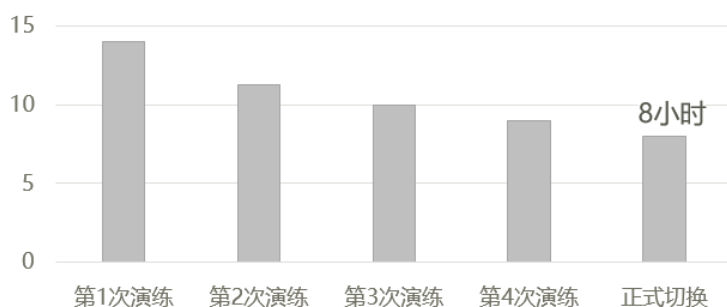
8.8.1 切换演练

8.8.1.1 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%。

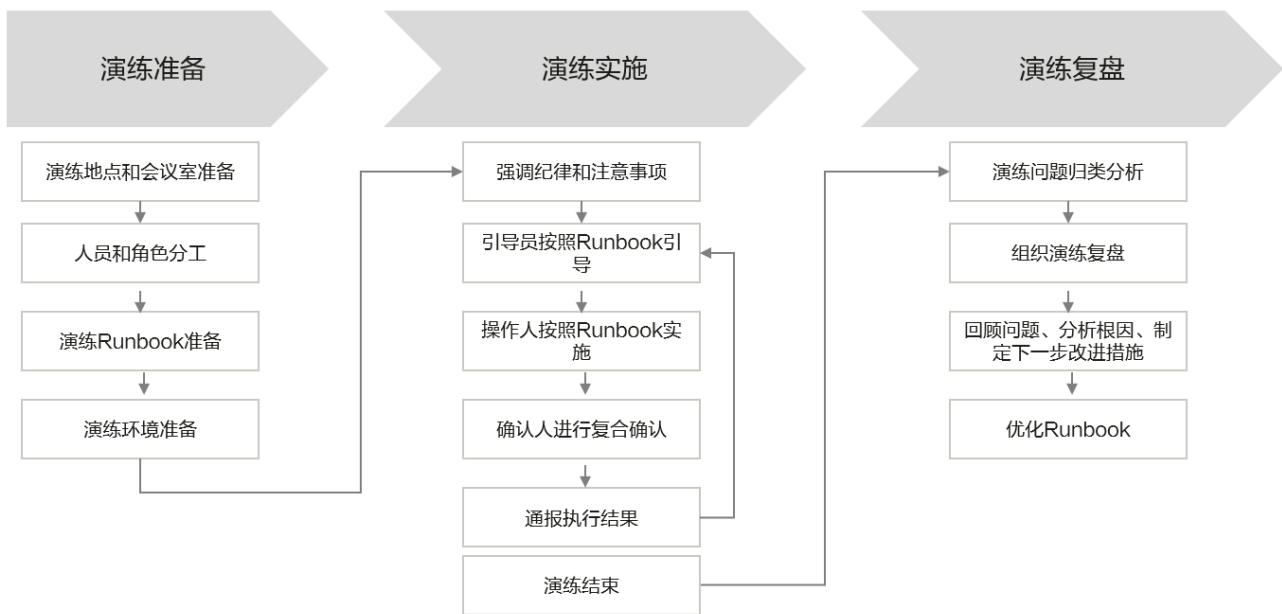
业务停机时长持续减少



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。

8.8.1.2 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：



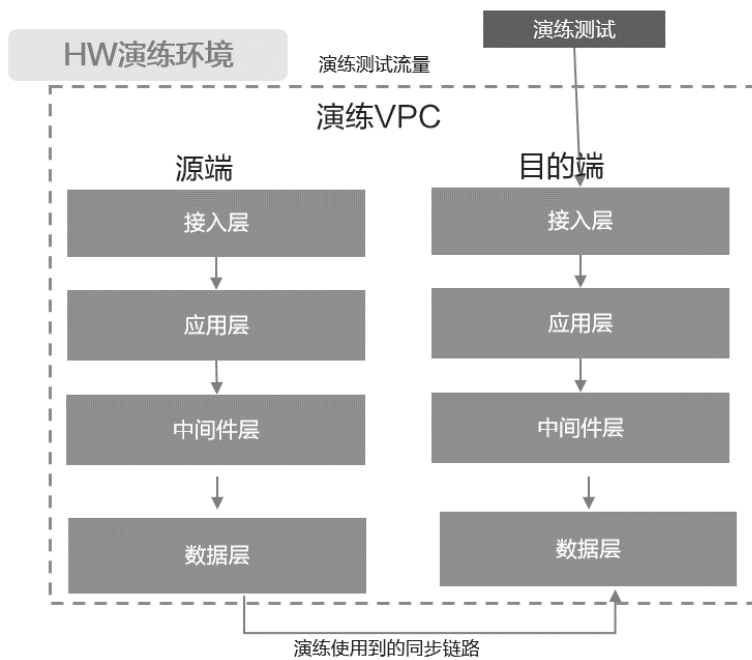
8.8.1.3 演练准备

演练的准备内容主要包括如下几个方面：

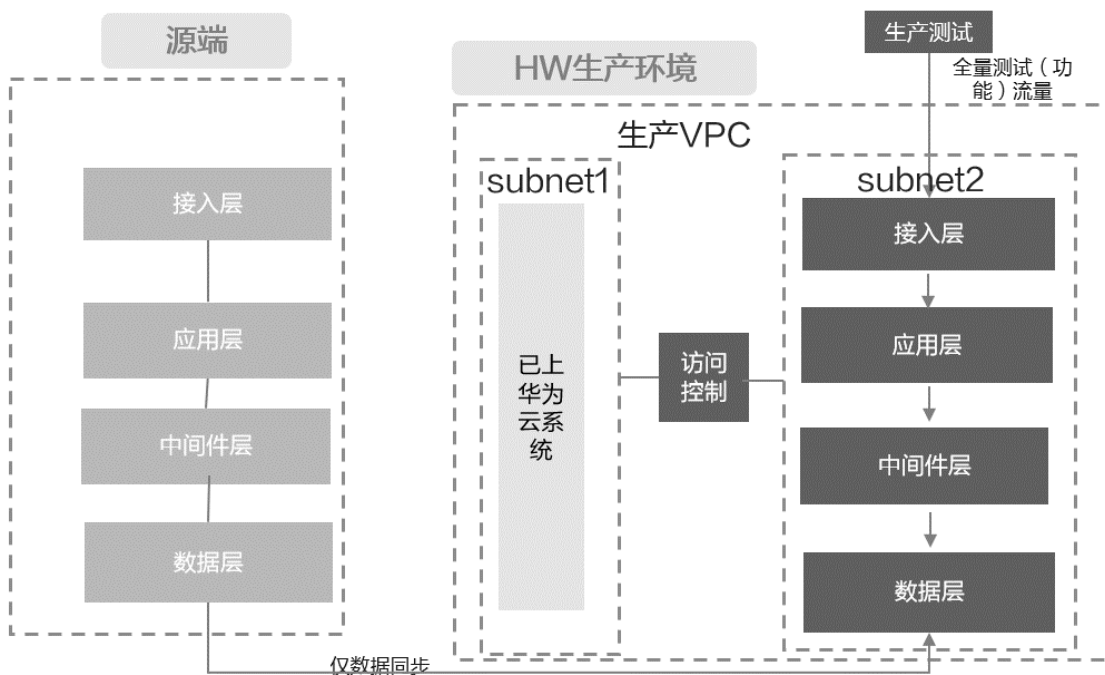
1. **演练地点或会议室的准备：**提前确定演练的地点（几楼）和哪个会议室，提前进行会议室的预定。
2. **人员准备和角色分工：**明确参与演练的各方人员及其责任分工，演练人员和最终切换操作人员尽量保持一致。演练角色分工可以参考 8.4.5 切换 Runbook 角色设计。
3. **演练 Runbook 准备：**按照演练环境细化演练 Runbook，并组织多轮评审，最终定稿。
4. **演练环境准备：**演练需要有演练的源端和演练的目的端。演练环境的源端需要能真正的模拟生产环境，数据尽量和生产保持一致。提前进行数据的预置，环境的检查等。

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：

1. 若企业没有能真正模拟生产的测试环境做演练，则需要和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。



2. 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。



8.8.1.4 演练实施和复盘

1. 演练实施通常按照如下步骤进行：

- 1) 引导员宣读演练纪律和注意事项

- 2) 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）。
- 3) 操作人按照 Runbook 执行此步骤
- 4) 确认人进行复合确认
- 5) 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）
- 6) 如此循环，直到在引导员的引导下完成所有步骤的执行
- 7) 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。

2. 演练复盘通常按照如下步骤进行：

- 1) 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
- 2) 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
- 3) 具体改进措施落实到人，更新到下次的演练 Runbook 或正式 Runbook 中
- 4) 关于如何组织好复盘，请参考“大规模上云迁移经验”这一章的“如何做复盘分析”

8.8.2 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：

8.8.2.1 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：

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	<input checked="" type="checkbox"/>
	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	<input checked="" type="checkbox"/>
	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	<input checked="" type="checkbox"/>
	预约会议作战室	企业项目经理	会议室布置安排	是	<input checked="" type="checkbox"/>
	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	<input type="checkbox"/>

		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	<input checked="" type="checkbox"/>
		企业项目经理	停机切换期间，运营中心值班人员就位	是	<input checked="" type="checkbox"/>
	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	<input checked="" type="checkbox"/>
	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	<input checked="" type="checkbox"/>
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	<input type="checkbox"/>
		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	<input type="checkbox"/>
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	<input type="checkbox"/>
	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	<input type="checkbox"/>
	JOB 清单检查并刷新脚本	研发团队	Check 最新的 job 清单	是	<input type="checkbox"/>
研发团队		检查脚本中的清单是否是最新的	是	<input type="checkbox"/>	
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	<input type="checkbox"/>
		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	<input type="checkbox"/>
		运维团队	云厂家后端保障人员进行日常状态检查	是	<input type="checkbox"/>
		运维团队	云服务高可用性检查，确认目标端云资源是否存在单 AZ 或单点故障问题	是	<input type="checkbox"/>
	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	<input type="checkbox"/>
		数据库相关	检查 NTP 时钟设置是否一致	是	<input type="checkbox"/>
		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	<input type="checkbox"/>
		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	<input type="checkbox"/>

	数据库相关	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	<input type="checkbox"/>
		数据库相关	检查 mysql 数据库源和目的端字符集是否一致	是	<input checked="" type="checkbox"/>
		数据库相关	数据库确认源端和目的端库用户一致	是	<input checked="" type="checkbox"/>
	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	<input type="checkbox"/>
	执行脚本检查	运维团队	应用服务启动脚本放在执行机	是	<input type="checkbox"/>
		运维团队	应用心跳检查脚本放在执行机	是	<input type="checkbox"/>
	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	<input type="checkbox"/>
	告警监控系统检查	运维团队	监控系统是否正常	是	<input checked="" type="checkbox"/>
	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	<input checked="" type="checkbox"/>
	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
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	<input type="checkbox"/>
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	<input type="checkbox"/>
		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	<input checked="" type="checkbox"/>
		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	<input type="checkbox"/>
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	<input type="checkbox"/>
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	<input type="checkbox"/>

8.8.2.2 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。

任务	步骤顺序	子任务
1.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
2.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
3.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
4.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
5.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
6.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
7.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
8.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
9.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
10.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
11.主流程测试（P0 用例）	11.1	主流程测试（P0 用例）

		<ul style="list-style-type: none"> ● 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。
12.外网停机公告撤销	12.1	取消外网转发至维护公告页面
13、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	
14. 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
15.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
13、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

注意：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。

8.9 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：

1. **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。
2. **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。
3. **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。
4. **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。
5. **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。
6. **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。
7. **文档输出**：记录并维护文档，以供将来参考和备案。

9 大数据迁移上云

9.1 概述

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，本章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第 8 章，本章只介绍差异部分。



- 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：

调研	设计		部署	迁移		验证	切换	保障	
大数据集群调研	大数据集群部署架构设计	数据迁移方案设计	大数据集群部署和配置	历史数据迁移	增量数据迁移	数据校验和补数	双跑运行	应用切换	运行保障
大数据任务调研	大数据调度平台部署架构设计	任务迁移方案设计	大数据调度平台部署和配置	历史作业迁移和调测	新增作业迁移和调测	作业验证和调优			
大数据应用调研	大数据应用部署架构设计	应用迁移方案设计	大数据应用部署和配置	业务联调		业务验证			

其中大数据应用的迁移请参考第 8 章应用迁移的方法，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。

9.2 调研

请参考第 2 章的方法，调研大数据集群、大数据任务调度平台和大数据应用的信息。

9.3 设计

大数据在云上的部署架构设计请参考第 5 章的大数据架构设计方法，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。

9.3.1 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：

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

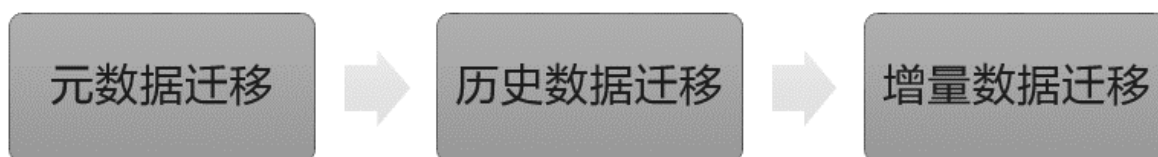
这 3 类数据的迁移方法如下：

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：



1. 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。

2. 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。

3. 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。

9.3.2 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。

- 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。
- 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：

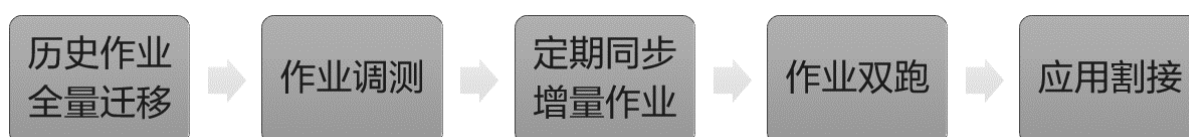
数据类型	校验标准	详细表名
X 类数据	100%一致	A 表、B 表、C 表…
Y 类数据	误差小于 0.01%	D 表、E 表、F 表…
…	自定义标准	…

9.3.3 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。

任务类型	迁移方案
JAR 类任务	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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)	<ul style="list-style-type: none"> ● 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：



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：

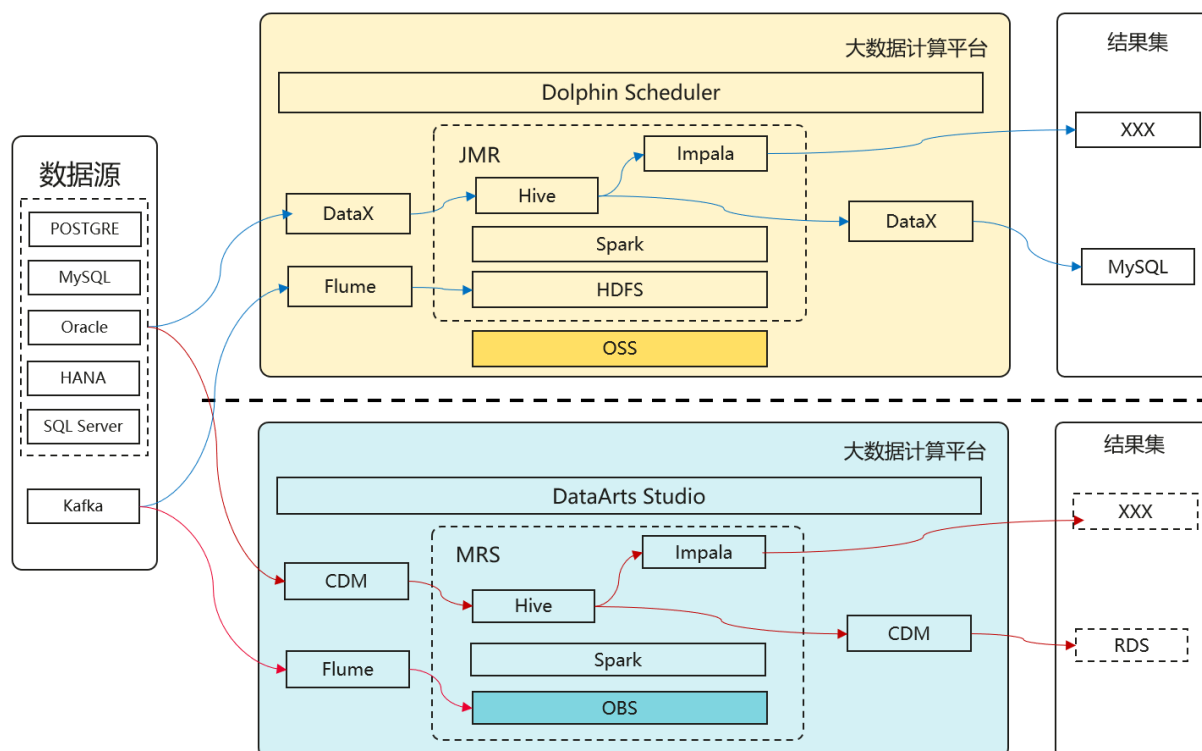
在增量作业迁移和同步成功后，进行作业双跑。作业双跑是指在新的大数据平台上同时运行原有系统和新系统的作业，以验证新系统的结果和原有系统的一致性。这可以通过比较作业输出、日志和指标等来判断两个系统的结果是否一致。

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。

9.3.4 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：



双跑方案的设计思路如下：

1. 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。

2. 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。

3. 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。

4. 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。如果发现任何问题或异常情况，需要及时处理和修复。

5. 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。

9.4 部署

9.4.1 平台部署

平台的部署可以参考如下方法：

1. 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官网指导：

https://support.huaweicloud.com/qs-mrs/mrs_09_0010.html

2. 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，可以参考如下官网文档进行部署和配置：

https://support.huaweicloud.com/prepare-dataartsstudio/dataartsstudio_01_0115.html

如果目标架构是采用自建的调度平台，有 2 种方法部署，可以基于华为云 ECS 重新部署任务调度软件，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。详细操作指导请参考 SMS 主机迁移服务官网指导：

<https://support.huaweicloud.com/sms/index.html>。

3. 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。详细操作指导请参考 SMS 主机迁移服务官网指导：

<https://support.huaweicloud.com/sms/index.html>。

9.4.2 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：

1. 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。

2. 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。

3. 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。

4. 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。

5. 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。

6. 安全审计和监测：

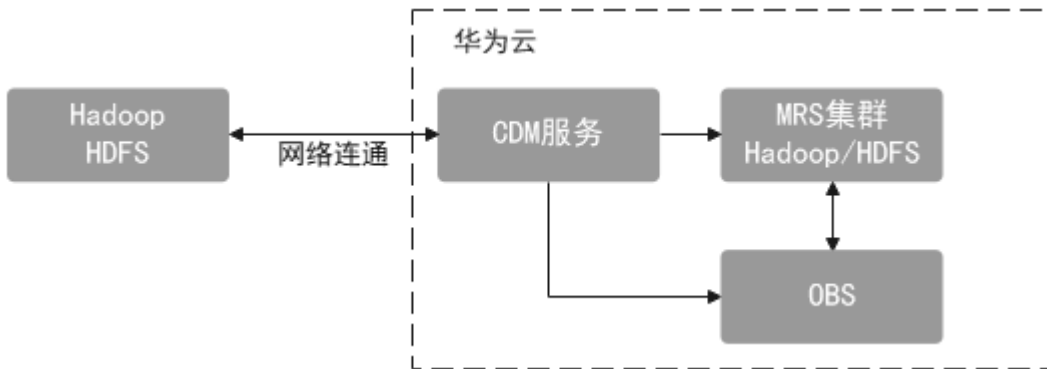
设置安全审计和监测机制，确保目标平台上的权限设置得到有效的审计和监测。这可以帮助发现和防止未经授权的访问，并及时采取相应的措施。

9.5 迁移

9.5.1 数据迁移

1. Hadoop 数据迁移到华为云 MRS 服务

将线下 IDC 机房或者公有云 Hadoop 集群中的数据迁移到华为云 MRS 服务。

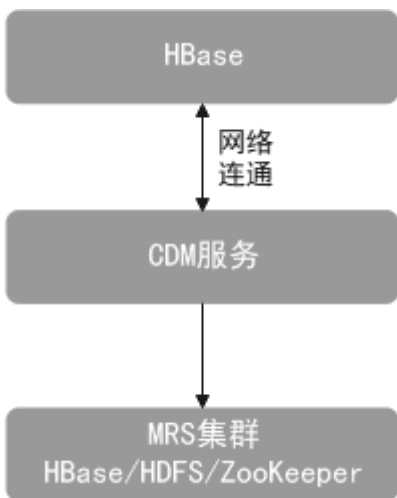


详细操作指导请参考官方文档：

https://support.huaweicloud.com/bestpractice-mrs/mrs_05_0029.html

2. HBase 数据迁移到华为云 MRS 服务

将线下 IDC 机房或者公有云 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。



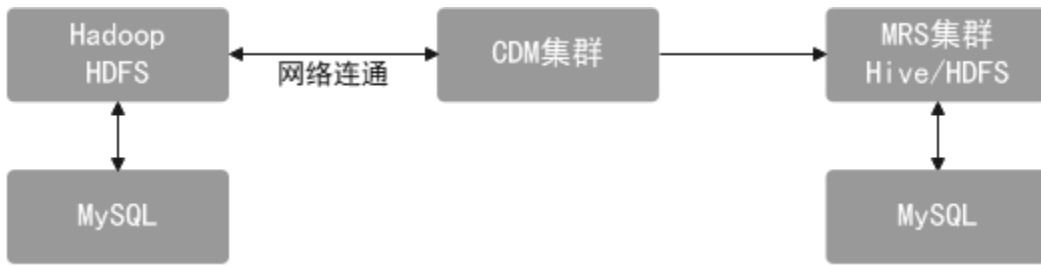
也可以使用华为云 CDM 云迁移服务进行 HBase 数据搬迁，详细操作指导请参考官方文档：

https://support.huaweicloud.com/bestpractice-mrs/mrs_05_0030.html

3. Hive 数据迁移到华为云 MRS 服务

将线下 IDC 机房或者公有云 Hive 集群中的数据迁移到华为云 MRS 服务。Hive 数据迁移分两部分内容：

1. Hive 的元数据信息，存储在 mysql 等数据库中。MRS Hive 集群的元数据会默认存储到 MRS DBService（华为的 Gaussdb 数据库），也可以选择 RDS（mysql）作为外置元数据库。
2. Hive 的业务数据，存储在 HDFS 文件系统或 OBS 对象存储中。



使用华为云 CDM 服务“场景迁移功能”可以一键式便捷地完成 Hive 数据的迁移，详细操作指导请参考官方文档：

https://support.huaweicloud.com/bestpractice-mrs/mrs_05_0031.html

4. 使用 BulkLoad 向 HBase 中批量导入数据

我们经常面临向 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 MapReduce 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方文档：

https://support.huaweicloud.com/bestpractice-mrs/mrs_05_0033.html

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方文档：

https://support.huaweicloud.com/bestpractice-mrs/mrs_05_0047.html

6. MRS HDFS 数据迁移到 OBS

CDM 支持 MRS HDFS-->OBS 的迁移，详细操作指导请参考官方文档：

https://support.huaweicloud.com/bestpractice-mrs/mrs_05_0048.html

7. Hive/Kafka/Elasticsearch/RDS/DWS 迁移到华为云 DLI

华为云数据迁移服务 CDM 支持将其他云服务或者业务平台的数据迁移至 DLI，包含 Hive、Kafka、Elasticsearch、RDS、DWS 的迁移。详细操作指导请参考官方文档：

https://support.huaweicloud.com/bestpractice-dli/dli_05_0042.html

8. 文件/关系数据库/Hbase/MongoDB 增量迁移

CDM 支持文件、关系数据库、Hbase、MongoDB 的增量数据迁移。详细操作指导请参考官方文档：

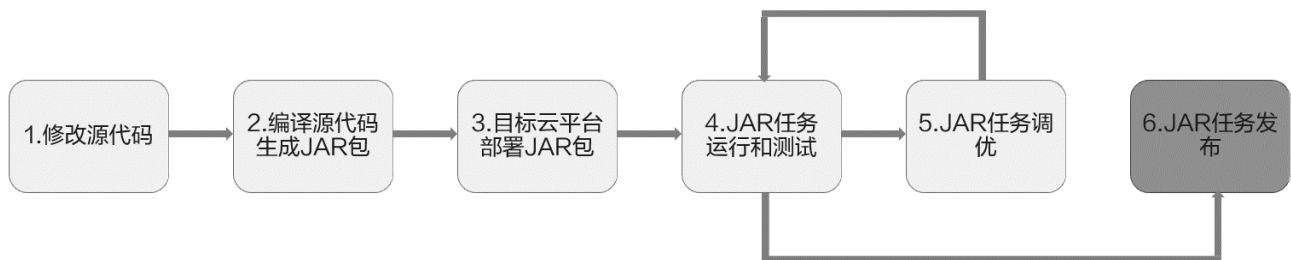
https://support.huaweicloud.com/bestpractice-dataartsstudio/dataartsstudio_05_0004.html

9.5.2 任务迁移

大数据任务迁移是指将大数据的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，以下就这三类任务的迁移实施方法做简单描述。

(一) 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：



前提：JAR 类任务调试依赖的数据已完成迁移，迁移步骤参考 9.5.1 节。

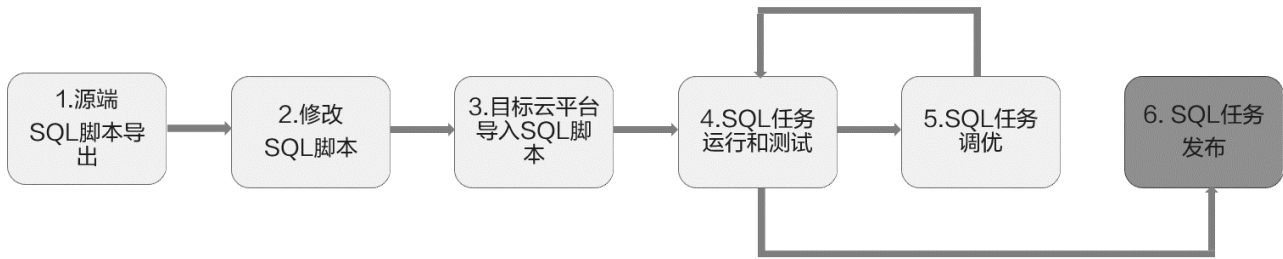
1. 修改源代码：根据云上大数据资源配置，修改源代码，例如版本、依赖库、数据库连接串，以及本地开发环境的库依赖配置等。
2. 编译源代码，生成 JAR 包：开发环境生成云上环境可执行的 JAR 包。
3. 目标云平台部署和配置 JAR 包：上传 JAR 包，并在任务调度平台配置调度任务。
4. JAR 任务运行和测试：执行调度任务，并根据日志检查任务执行状态和结果。
5. JAR 任务调优：如果任务执行不符合预期，例如执行时间过长，需要查找根因并进行优化和验证。
6. JAR 任务发布：按业务需要的时间配置调度任务。

华为云 DataArts Studio 数据治理中心服务的 JAR 类任务配置可以参考：

https://support.huaweicloud.com/usermanual-dataartsstudio/dataartsstudio_01_1824.html

(二) SQL 类任务迁移

迁移 SQL 类任务时，主要工作在于 SQL 脚本的云上适配改造，可以参考如下步骤进行：



前提：SQL 类任务调试依赖的数据已完成迁移，迁移步骤参考 9.5.1 节。

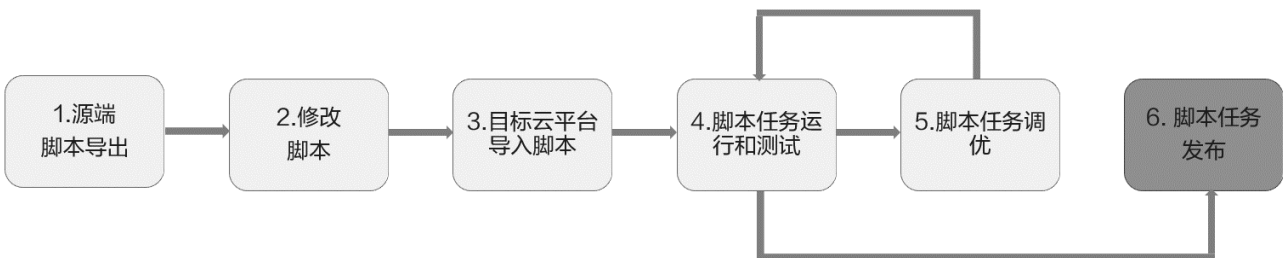
1. 源端 SQL 脚本导出：从源端任务调度平台导出 SQL 脚本。
2. 修改 SQL 脚本：根据云上调度平台的语法及资源配置修改 SQL 脚本。
3. 目标云平台导入 SQL 脚本：在云上任务调度平台配置 SQL 类任务，导入 SQL 脚本。
4. SQL 任务运行和测试：执行 SQL 调度任务，通过日志和运行结果检查任务运行情况。
5. SQL 任务调优：如果任务执行不符合预期，例如执行时间过长，需要查找根因并进行优化和验证。
6. SQL 任务发布：按业务需要的时间配置调度任务，配置正确的任务依赖关系。

如果使用华为云 DataArts Studio 数据治理中心进行 SQL 类任务调度，可以参考：

https://support.huaweicloud.com/usermanual-dataartsstudio/dataartsstudio_01_0424.html

(三) 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：



前提：脚本类任务调试依赖的数据已完成迁移，迁移步骤参考 9.5.1 节。

1. 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。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。

如果使用华为云 DataArts Studio 数据治理中心进行脚本类任务调度，可参考如下链接：

Shell 脚本任务：

https://support.huaweicloud.com/usermanual-dataartsstudio/dataartsstudio_01_0425.html

Python 脚本任务：

https://support.huaweicloud.com/usermanual-dataartsstudio/dataartsstudio_01_4503.html

9.6 验证

9.6.1 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第 8 章“数据验证方法”这一节。

9.6.2 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：

1. 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。

2. 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。

3. 作业执行的性能验证

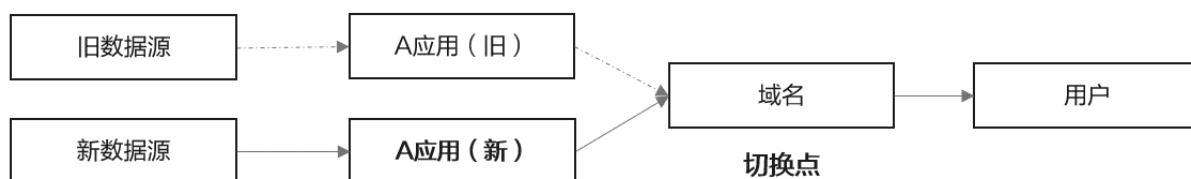
在迁移后，验证作业的执行性能，包括运行时间、资源利用率、并发性等。通过监测作业的执行指标和性能指标，可以评估迁移后的作业性能是否符合预期。如果作业的性能有问题，可能需要调整作业的配置参数、优化作业代码或考虑资源调配的问题。

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。

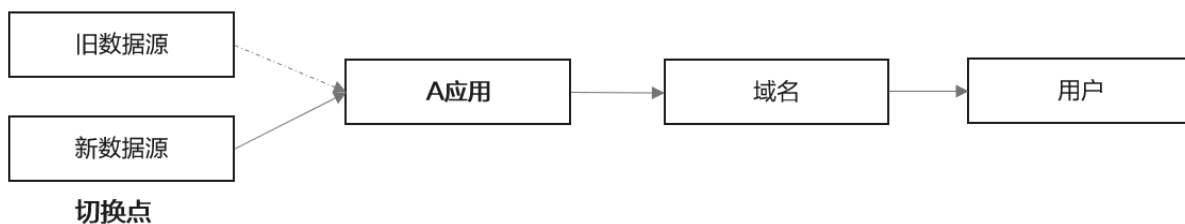
9.7 切换

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第 8 章应用迁移的切换章节。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。

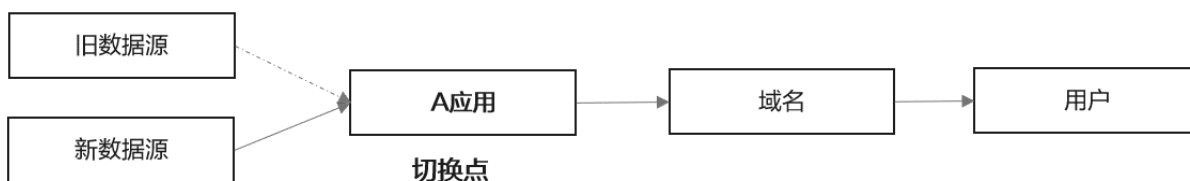
1. **双跑场景**：大数据应用分别在源环境和目标环境各部署一套，实现双跑，切换点在域名，业务切换时只需要进行域名的切换，将业务流量切换到新应用。



2. **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。



3. **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。



9.8 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：

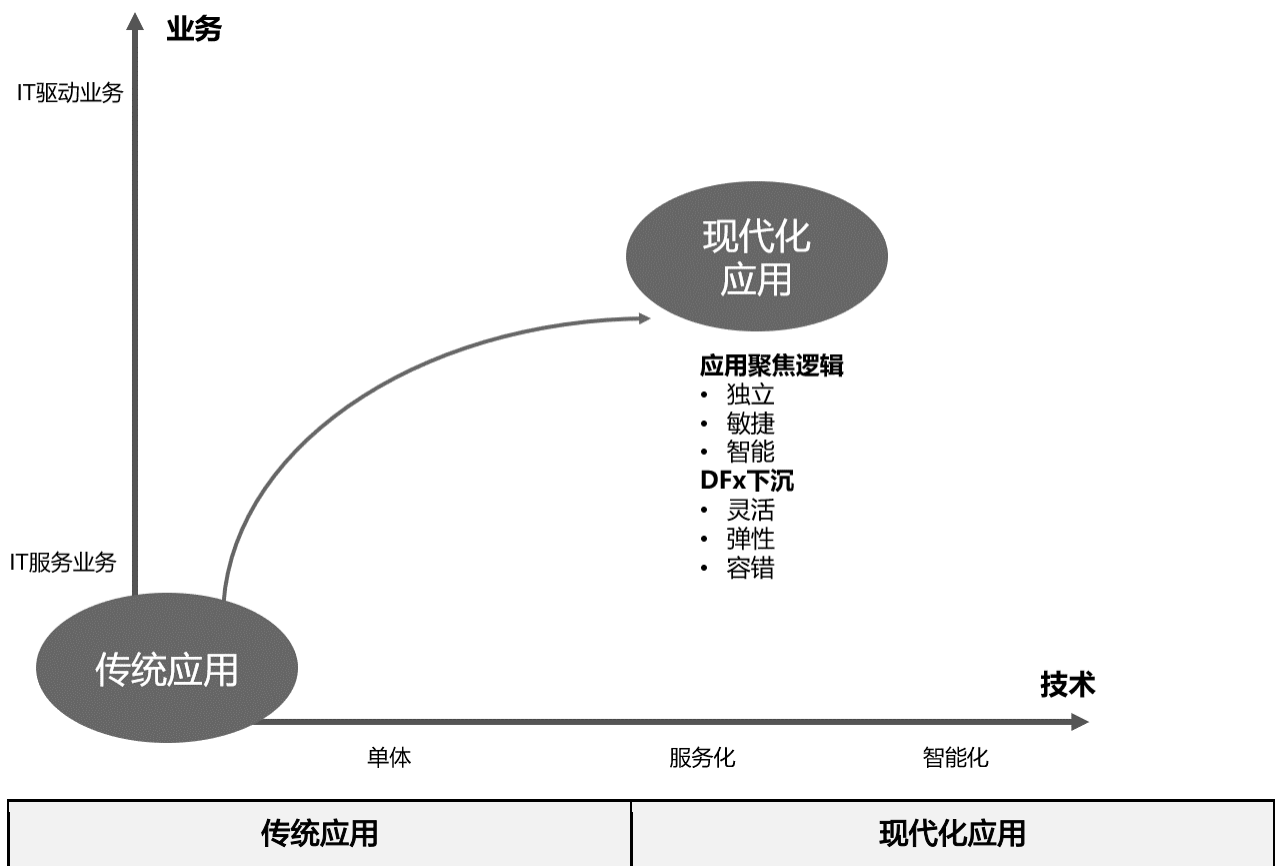
1. **监控和警报设置**：建立实时监控系统，监测集群、任务调度平台和应用程序的运行状态。设置警报，以便及时发现潜在的问题并采取措施。
2. **优化集群性能**：对大数据集群进行性能评估和调优。监视资源使用情况，优化配置参数、调整集群大小和资源分配，以提高整体性能。
3. **数据安全和权限管理**：审查和加强数据的访问控制和权限管理机制。确保只有经授权的人员可以访问敏感数据，并采取适当的加密和脱敏措施保护数据安全。
4. **自动化任务调度**：确保大数据任务调度平台的运行和调度正常。优化调度策略，确保任务按时准确完成，并处理可能的故障或异常情况。
5. **异常处理和故障恢复**：建立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。
6. **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。

10 应用现代化上云

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。

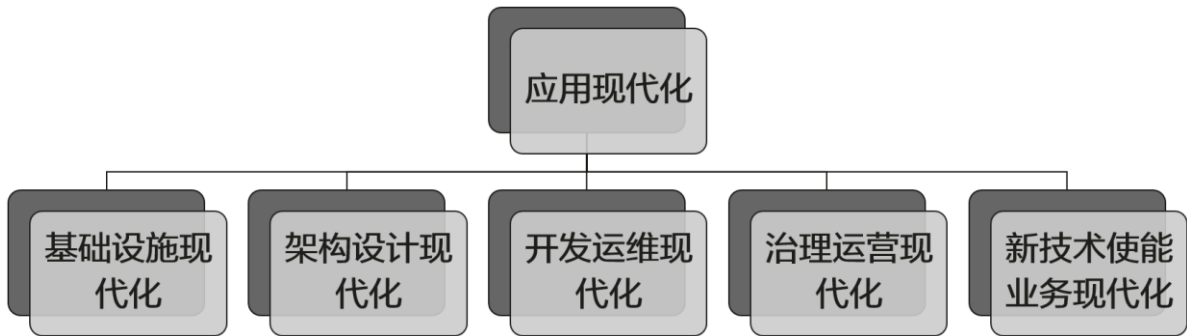
10.1 什么是应用现代化

近年来各大云厂商都提出了“应用现代化”的愿景和价值主张。数字时代，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。“未来 IT”要向“应用现代化”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 及治理等公共能力建立在云平台上。



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
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 5 个方面：



1. **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。
2. **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。
3. **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。
4. **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。
5. **新技术使能业务现代化**：通过使用云的新技术，如人工智能、数字人等，将传统应用转型为适应当前业务需求和技术趋势的现代化应用，提升用户体验和创造新的商业价值。

10.2 基础设施现代化

10.2.1 容器化改造上云

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：

1. **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。
2. **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。
3. **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。
4. **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。
5. **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。
6. **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。
7. **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。
8. **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。

10.3 应用架构现代化（微服务改造/优化）

10.3.1 微服务改造上云（单体→微服务）

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。

10.3.2 微服务架构优化

一些互联网企业野蛮生长，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。

10.4 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：

1. **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。
2. **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。
3. **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。
4. **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。

5. **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。
6. **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。

10.5 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：

1. **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。
2. **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。
3. **设计集成方案：**基于对应用的分析 and 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。
4. **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。
5. **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。
6. **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。

10.6 新技术使能业务现代化

云的新技术，包括人工智能、大数据、区块链、元宇宙和物联网等，在业务创新和现代化方面提供了广泛的机会和潜力。这些技术可以帮助企业改进业务流程、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。

一、人工智能（AI）：

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：

1. **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。
2. **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。
3. **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。
4. **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。

二、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：

1. **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。
2. **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。
3. **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。
4. **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。

三、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：

1. **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。

2. **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。
3. **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。
4. **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。

四、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：

1. **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。
2. **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。
3. **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。
4. **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。

五、物联网（IoT）：

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：

1. **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。
2. **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。

3. **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。
4. **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有机会推出定制化的产品和服务，满足用户个性化需求。
5. **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。
6. **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。

总而言之，大数据、区块链、元宇宙和物联网等新兴技术在不同领域都具有巨大的潜力，可以推动业务创新和现代化。企业可以根据自身的需求和业务模式，结合这些技术来实施创新和改进，提高竞争力并满足用户的需求。

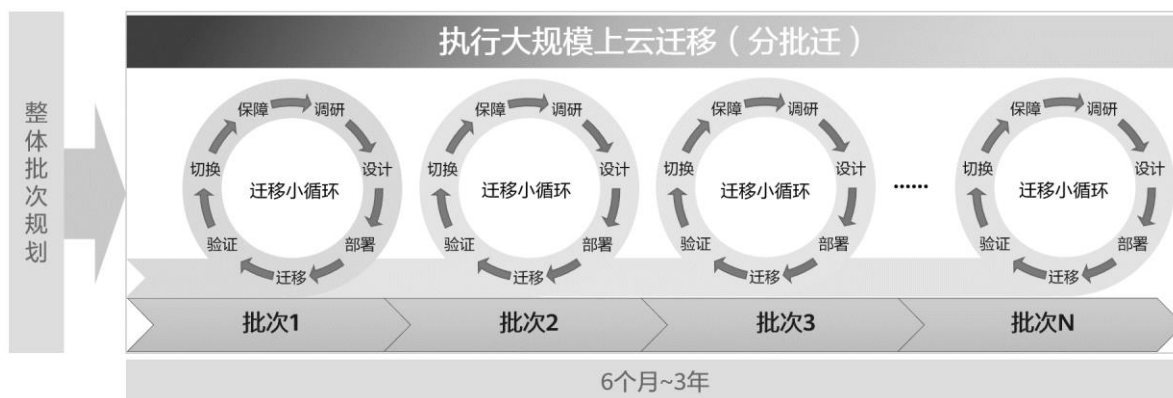
11

大规模上云阶段经验

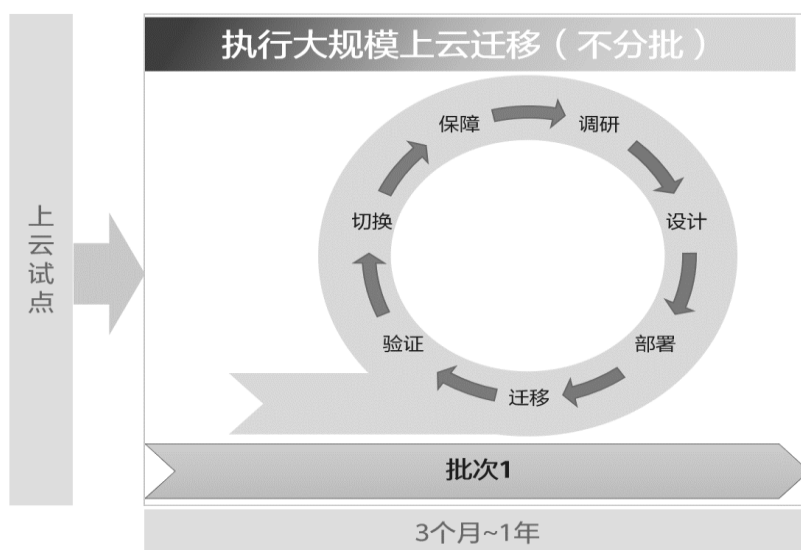
11.1 大规模上云阶段概述

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：

1. **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：



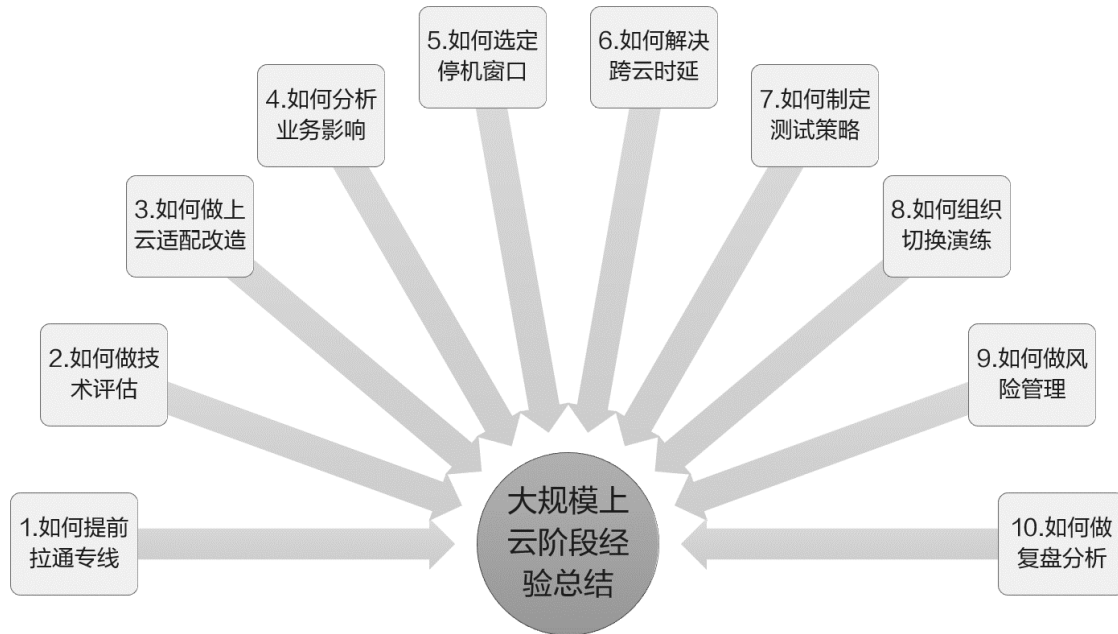
2. **整体迁移**：对于不能分批的，应用的关联关系往往非常复杂，只能选择所有业务系统整体一个批次迁移，如下图：



本章对大规模上云阶段会遇到的常见问题进行了总结，对大规模上云具有一定的参考和借鉴意义。

11.2 大规模上云阶段经验总览

大规模上云阶段经常会遇到的问题包括提前拉通专线、技术评估、上云适配改造、业务影响分析、选定停机窗口、解决跨云时延、制定测试策略、组织切换演练、风险管理和复盘分析等。本章将介绍解决这些问题的详细流程和实践经验。



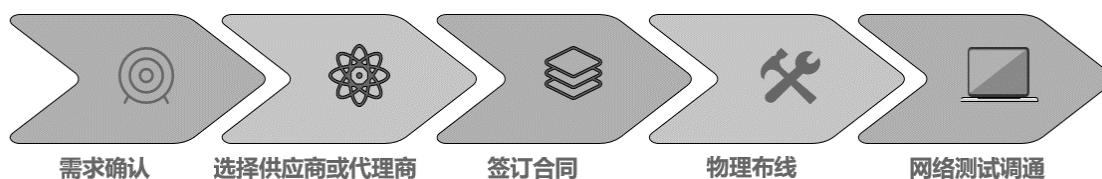
11.3 如提前拉通专线

IDC 机房大规模搬迁华为云，建议拉通专线。因为专线有更低的延迟、更高的稳定性、更优的数据传输效率、更大的带宽、以及更高的安全性。专线能够在上云迁移过程中，提供更多的迁移和切换方案选择。

- 更低的延迟：**专线通常具有更高的服务质量保障，例如更高的可靠性、更低的丢包率等，可以保证数据传输的稳定性和可靠性，从而减少延迟。同城专线一般延迟在 5ms 左右，而公网则在 50ms 左右。
- 更高的稳定性：**专线通常是由两个物理网络节点之间直接连接的，不会受到其他用户的影响，因此网络拥塞的可能性更小，数据传输更加稳定。
- 更优的数据传输效率：**专线连接的通信双方之间不存在其它节点，而公网上通信双方的数据需要经过多个路由器和交换机等设备转发，因此专线的物理路径更短，数据传输的时间更短，传输效率更高。专线的带宽使用率，通常可以维持在 90% 以上，即 100MB/s 的专线，可以达到接近 90MB 每秒以上的传输速率。而在公网，带宽利用率通常只能达到 70% 左右，且通信质量受公网稳定性的影响。

4. **更大的带宽**：运营商提供的专线带宽上限，远远超过公网可以达到的带宽。通常情况下，专线的带宽上限可以达到 30Gbps，即 3GB/s 以上。大带宽可以为迁移提供更高的传输效率和更短的迁移窗口。
5. **更高的安全性**：专线是一种点对点的连接方式，只有两个端点之间才能进行通信。且专线通常采用物理隔离的方式，通过专用线路或光缆等物理设备将两个端点隔离开来，从而避免了公网上的安全威胁，如黑客攻击、病毒感染等。

专线拉通基本流程：



1. **需求确认**：根据业务和迁移需求，确定这条专线的带宽需求、专线类型、接入点、SLA 要求、安全要求、费用预算等
2. **选择供应商或代理商**：选择合适的骨干网供应商或专线代理商，对接客服人员，提供需求清单。
3. **签订合同**：对专线服务提供商的接客服人员并提供需求清单。根据需求清单，与供应商或服务商进行报价、谈判、签订合同。
4. **物理布线**：根据合同内容，专线供应商施工人员在对接点附近进行施工，连通骨干网专线设备与接入点的物理线路。接入点也应做好机房内部网络跳线并调通内部设备工作。
5. **网络测试调通**：供应商工程师和机房工程师共同对专线两端的设备进行 ping 通测试、网络延迟和稳定性测试。

专线拉通周期较长，与骨干网运营商或专线代理商确定专线方案到专线调通过程通常需要一个月左右的时间。为保障业务搬迁上云的按期进行，建议客户提前一个月与骨干网运营商或专线代理商进行专线拉通相关事项的开展。

11.4 如何做技术评估

11.4.1 研发侧技术评估

大规模上云期间研发侧主要关注如下事宜：

1. **保障数据一致性**：梳理中间件、JOB 等调用情况，停服迁移过程中，保证数据的一致性。
2. **减少跨云业务影响**：对于跨云延迟问题，研发要从批量任务、应用间多次调用、应用和数据层多次调用等方面评估相关影响。

3. 选择合适的云服务：要注意云服务版本、规格及配置要和源端环境保持一致。

为了保证大规模迁移的顺利进行，研发侧的评估项和建议如下：

序号	评估项	场景	影响评估和建议	可选/必选
1	云服务适配性评估	云服务与现有技术架构存在差异，需要评估上云后涉及哪些改造项，	需要评估现有技术架构迁移到云上时有哪些适配改造，并评估改造难度、时间和成本，比如企业当前在 IDC 使用的是 CEPH 存储，迁移到华为云使用 OBS 对象存储，则相关应用需要进行 OBS 对接改造。	必选
2	IP 地址修改为域名评估	IP 地址固化在配置文件中	对于配置文件中固化了 IP 地址的情况，迁移到云上后 IP 地址会发生变更。企业上云时需要提前识别此类场景，建议提前将配置文件中的 IP 地址修改为域名，正式切换时只需要修改域名 IP 即可，减少了切换时的操作风险，同时也方便后续的运维管理。	可选
		IP 地址固化在软件代码中	对于程序代码中固化了 IP 地址的情况，迁移到云上后 IP 地址会发生变更，需要提前修改软件代码并重新编译。企业上云时需要提前识别此类场景，并评估改造的可行性，建议上云后统一将 IP 地址修改为域名，以方便后续的运维管理。	必选
3	流量入口治理评估	业务系统使用存在多个流量入口（多套流量网关）	在流量切换的过程中，需要进行大量配置修改，可能会发生部分配置修改遗漏的风险，致使切换失败。建议对流量入口进行评估和治理，统一入口流量及转发。	可选
4	定时任务评估	业务系统中有大量定时任务参与业务处理	需要评估定时任务的启动的顺序和依赖性。 定时任务启停顺序：定时任务启动和停止是否有顺序，即后一个定时任务的执行，依赖前一个定时任务的执行过程或执行结果。如果有启停有顺序，需要评估并梳理，在切换时按照顺序停止和启动。 定时任务依赖性：定时任务的执行，依赖某个数据库或 Redis 中的数据状态，需要评估被依赖的数据源是否迁移同步至目标端。	必选

5	消息中间件评估	消息中间件迁移保障数据一致性	消息中间件迁移过程中，生产者和消费者对应用启停顺序可能导致消费的消息丢失，较复杂的系统很难梳理出应用系统的启停顺序。可采用改造生产者和消费者的组件，可以在迁移期间，暂停对消息生产和消费，当所有系统成功启动验证无误后，方可打开开关。	必选
6	共用中间件拆分评估	多个业务系统共用一个中间件集群，迁移期间存在业务跨云调用中间件的情况	云上业务在读写中间件时会有延迟，建议评估时延造成的业务影响是否能够接受，如果不能接受，需要评估中间件的共用情况，将多业务共用的中间件进行拆分，云上和云下分开。	可选
7	共用数据库拆分评估	多个业务系统共用一个数据库，迁移期间存在业务跨云调用数据库的情况	云上业务在读写数据库时会有延迟，建议评估时延造成的业务影响是否能够接受，如果不能接受，需要评估数据库的共用情况，将多业务共用的数据库进行拆分，云上和云下分开。	可选

11.4.2 运维侧技术评估

大规模上云期间，运维侧主要关注运维自动化平台为适应迁移所必须做的改造点及相关改造工作，为了保证大规模迁移的顺利进行，运维侧的技术评估项和建议如下：

序号	评估项	场景	影响评估和建议	
1	自动化平台对接评估	上云期间通过自动化平台实现资源的批量发放	需要评估现有自动化平台与云平台的对接开发项，评估云平台有哪些 API，评估对接难度、时长、工作量和风险。	建议对接
2	运维监控平台对接评估	上云期间通过统一的运维监控平台实现对云上资源和应用的统一监控	需要评估现有的运维监控平台与云平台运维监控功能的对接项，评估云平台有哪些 API，评估对接难度、时长、工作量和风险。	建议对接
3	统一日志平台对接评估	上云期间通过统一的运维监控平台实现对云上资源和应用的统一日志管理	需要评估现有的日志平台与云平台日志功能的对接项，评估云平台有哪些 API，评估对接难度、时长、工作量和风险。	建议对接
4	运维通道评估	上云期间如何对云上、云下环境统一运维	需要评估业务迁移到华为云后，开发及运维人员如何连接管理云上资源和业务，需要评估云平台的相关功能能否满足要求	建议对接

		(比如云堡垒机、VPN、专线等), 如何与现有环境适配。	
--	--	------------------------------	--

11.5 如何做上云适配改造

在大规模上云时, 企业需要提前制定改造策略并做好整体规划, 按照计划完成应用上云迁移的适配改造工作, 避免影响大规模迁移的进程。适配改造的策略和原则参考如下:

(一) 改造原则

1. 业务驱动改造, 不要影响上云迁移里程碑, 上云前后改造均可。

比如: 预估 2~4 年后网站的用户会增加 1 倍, 数据库会因为用户量增加、负载压力过高而成为网站的瓶颈, 为了满足业务性能的需要, 企业需要对数据库进行读写分离改造。该改造是由业务驱动的改造, 改造时间在上云前后均可。建议企业根据上云节奏合理安排改造时间。

2. 对于时延敏感的业务, 企业应优先考虑整体迁移和切换, 因为分批或分层迁移会由于时延问题导致改造工作量。
3. 对于搬迁导致的临时改造, 比如迁移中间态的时延问题, 优先考虑改造实现简单, 工作量小的方案, 避免对企业开发人员造成较大的负担。

(二) 接入层改造

1. **统一流量入口改造:** 企业不同的业务系统可能会使用不同的流量入口和网关, 造成运维难度大、搬迁复杂。这种情况, 建议企业根据业务流量类型, 将多个不同的流量入口或网关, 统一为少数几个流量入口或网关, 以降低运维难度, 减少迁移切换的复杂度。
2. **IP 地址硬编码改造:** 硬编码方式就是 IP 地址直接写在软件代码中或配置文件中, 业务系统从源端迁移到华为云后, 通常 IP 地址会变更, 因此需要排查 IP 地址硬编码的场景, 在业务切换前完成改造。

(三) 应用层改造

1. **容器化改造:** 如果源端应用是部署在虚拟机上, 上云后需要部署在华为云 CCE 上, 那么应用需要提前完成容器化改造。
2. **云服务组件版本升级适配改造:** 如果源端用的是 MongoDB 3.6 版本, 上云后需要使用华为云 MongoDB 4.0 版本, 那么应用需要提前完成版本升级适配改造。
3. **接口适配改造:** 如果源端应用调用了 CEPH 存储的 API 接口, 迁移到华为云后需要使用 OBS 对象存储的 API 接口, 那么应用需要提前完成 OBS 适配改造。
4. **跨云循环调用改造:** 如果采用分批切换方案, 应用、数据库、中间件的跨云 For 循环调用可能会导致严重的时延问题, 导致业务体验很差, 因此需要提前排查 For 循环调用情况, 在上云前完成应用改造, 避免跨云来回调用的高延时影响业务运行和用户体验。

5. **服务慢接口改造**：慢接口是指在业务系统中响应时间较长的接口。通常一个服务接口在被调用时，响应时间应该在几十到几百毫秒以内。如果一个服务接口的响应时间超过了一定的阈值，就可以被认为是慢接口。慢接口可能会导致业务系统单个业务或整体业务性能下降，影响用户体验，甚至可能引起业务系统崩溃。建议上云前进行慢接口的排查，并完成改造，避免上云后存在同样的问题，也避免在测试期间无法定位是云引起的性能问题还是应用慢接口引起的性能问题。
6. **消息中间件消费开关改造**：对消息中间件消费的公共组件进行升级改造，增加生产和消费开关的控制，保障在上云过程中，重要消息不丢失。
7. **IBMMQ 的改造**：对于跨云调用 IBMMQ 采用短链时，每次请求耗时较高，对于性能要求比较高的系统，建议改造成长链接来解决此性能问题。
8. **JOB 消费及开关改造**：对 Job 的各个维度进行梳理，特别对靠时间先后顺序依赖关系的 Job 进行改造，对三方平台超时未收到 Job 推送任务会有处罚相关的也进行梳理，并从各层面制定相应的应对方案。由于跨云延迟问题，对 Job 调度的公共组件进行升级改造，保障能通过配置保障云上或云下的调度情况。
9. **心跳改造**：为了保障上云期间应用启动后各中间件连接正常，采用了 Springboot 的 HealthCheck，保障了启动后通过心跳检测，能快速发现应用和各中间件的连通性是否正常。

(四) 中间件层和数据层的改造

1. **中间件层和数据层的架构优化改造**：业务上云是一次架构优化的机会，企业可以结合业务实际情况和上云周期，决定是否在上云的同时进行中间件和数据库的架构优化改造，比如共用中间件拆分改造、共用数据库拆分改造、数据库读写分离改造等。

11.6 如何分析业务影响

业务影响分析是上云迁移中很重要的一项工作，大规模上云迁移时，业务影响分析会很复杂，以零售业为例，传统零售业务系统通常分线上和线下业务，多数企业是先有线下业务系统，线下由传统的分销渠道进货，线下实体店出货的模式来实现盈利。近些年受线上交易和高成本的冲击，传统零售逐步将业务扩大到线上。所以通常传统零售行业的业务系统是线上线下并存。所以业务影响的分析可以从线上和线下 2 个维度去分析。

11.6.1 线下业务影响分析

以零售行业为例，零售行业的线下业务主要是通过实体店面销售商品，如超市、百货商店、药店、附加业务如停车场、餐馆饭店等。

1. **停车场业务影响**：停车场管理系统的功能是对停车场车辆出入和收费进行管理。切换期间若系统停服，就会出现停车系统无法使用，继而导致车辆无法出入的情况。具体的业务影响和停车场的运营模式及停机窗口有关。对于非 24 小时营业的停车场，若错开营业时间，系统服务中断是无影响的。若存在 24 小时停车场或选定的停机时间在停车场营业时间窗内，就会导致车辆无法出入。

应对措施：要先梳理停车场的营业时间，营业时间在停服窗口内的，企业上云团队要和业务团队沟通，安排对应的业务人员以人工抬杆和收费的方式去处理。另外，考虑到车主的体验，企业应提前给待出停车场的车主发送短信通知。

2. **超市、百货商店、药店业务影响：**切换期间若系统停服，主要影响会员，收银支付，订单拣货，配送和优惠券的使用等。

应对措施：切换时间窗要尽量避开超市和百货商店的营业时间。若实在无法避开的，可以根据业务影响的范围和结果，采取其它适当的措施，比如对于业务影响小的小店，可以预先通知客户进行提前关店；对于业务影响大的商超，可以考虑采用降级措施，比如支付降级，在降级期间不能使用企业自有的支付功能，但可以调用第三方支付完成交易，通过降级将影响降到最低。

3. **库存影响：**零售行业如超市、百货商店、药店等每天的营业信息，如小票、库存等都会同步到线上中心库。这样中心库才能根据各家门店库存情况进行及时配货，根据小票信息汇总进行每日营业分析等。若切换期间系统停服，会出现小票、库存等无法同步的问题。小票与库存数据量一般较大，通常在夜间进行，同步时间会较长，所以切换时间很难避开这个时间窗。

应对措施：等切换完成，比如预估凌晨 XX 点切换完成，需提前和第三方沟通，安排好支撑人员，配合业务切换完成后再进行重新推送数据。并且要提前预估重新推送数据的时间，确保在第二天营业开始之前完成数据推送。

4. **餐馆饭店影响：**饭卡系统实现了信息化，切换期间若系统停服，主要影响刷卡系统的使用。

应对措施：切换时间窗要尽量避开餐馆饭店的营业时间。若实在无法避开的，同样要采取告知运营人员并进行人工收取现金等应急措施。

11.6.2 线上业务影响分析

1. **线上下单、线下送货的影响：**零售行业如超市、百货商店、药店等，存在线上下单线下送货的商业模式，比如药店可以在某团购平台线上接收顾客订单，选择立即送货或选择按照指定日期送货。若切换期间与第三方销售渠道对接的系统停服，会导致第三方销售渠道下单后无法进行拣货送货的问题。

应对措施：尽量避开第三方销售渠道营业时间，若实在无法避开的，就要协调第三方销售渠道入口关停，避免不及时送货等造成平台惩罚。

另外部分第三方销售渠道具备指定日期送货功能，若在停服之前下单，指定的送货日期在切换窗口内，就会出现无法拣货送货问题，所以也需要和第三方销售渠道沟通，取消指定日期-第二天配送功能，避免无法及时送货造成平台惩罚。

1. **线上促销影响：**超市、百货门店和药店的线上 app 系统，称之为线上业务。线上业务也经常搞一些促销活动，通常由运营人员提前配置活动规则、开始时间和结束时间，系统根据运营人员的配置开启线上促销活动。然而，如果运营人员配置的活动开始时间或结束时间在系统停服切换的时间窗口内，则会对促销业务产生影响。

应对措施：与运营人员做好充分沟通，在切换期间不要配置促销活动。

11.6.3 业务降级演练

业务降级是指在面对业务全量搬迁或异常情况时，为了保护系统的稳定性和可用性，暂时降低业务功能或服务质量。通过对部分业务功能进行降级处理，可以加快业务搬迁节奏或减少系统负载。此外，降级的业务还能避免因搬迁造成的数据错乱或因异常情况而导致的连锁错误。业务降级是临时的，一旦搬迁完成或异常情况得到解决，应尽快恢复正常的业务功能和服务质量。

业务降级可以分为两种类型：强依赖降级和弱依赖降级。

强依赖降级是指在发生业务搬迁或业务系统异常情况时，为了保证核心功能的可用性，暂时关闭一些非核心功能或者拒绝部分请求，以保证系统的稳定性和数据一致性。

弱依赖降级是指在发生异常流量或错误调用时，通过降低服务质量或关闭部分功能来保护系统稳定性和可用性。

业务降级的方式

1. 流量限流：通过限制请求的数量或关闭外部流量来控制业务系统的外部流量，降低接入用户数量。
2. 功能降级：当业务系统处于搬迁过程时，将该业务功能进行降级处理，例如关闭一些非核心功能，使其处于数据静止状态，加快业务搬迁节奏。
3. 异步处理：将一些耗时较长且实时性要求不高的操作转化为异步处理，使数据进行堆积，等业务搬迁完成后再进行统一处理。
4. 超时控制：设置合理的超时时间，当请求超过预设的时间仍未得到响应时，可以选择重试、返回默认值或者进行其他处理。

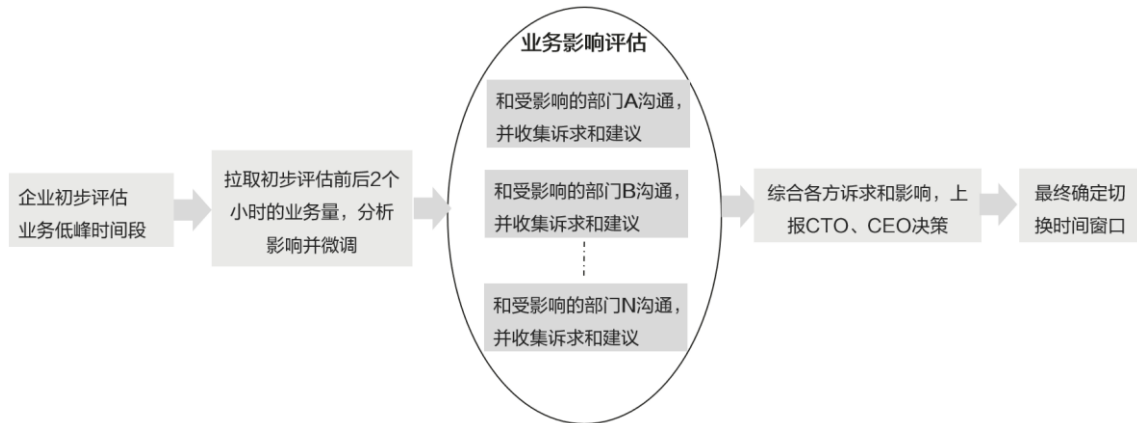
业务降级演练的主要目的是为了验证系统在业务全量搬迁或发生异常情况时的稳定性和可用性，并为系统运维人员和开发人员提供实践经验和应对策略。业务降级演练有以下几个用途：

1. 测试整个业务的持续运行能力：通过迁移演练或异常情况下的部分业务降级，可以测试业务系统在迁移过程中，当部分业务系统不可用时，其它业务系统是否能依然正常使用，维持业务基本运行。
2. 熟悉应急操作流程：通过演练，运维人员和开发人员可以熟悉业务降级操作流程，包括切换到备用服务、关闭部分功能等操作，以提高运维人员和开发人员在紧急情况下的反应速度和准确性。
3. 发现潜在问题和风险：演练过程中可能会暴露出一些之前未发现或未考虑到的问题和风险，企业可以及时进行修复和改进。

通过业务降级演练，可以有效提升系统的稳定性、可用性和可维护性，确保系统在面对异常情况时能够正常运行并提供基本的服务。

11.7 如何选择停机窗口

在大规模迁移项目中，停机窗口的分析和选定是一个关键的决策过程，下图是某大型零售电商的停机窗口决策过程，供参考：



确定停机窗口时，需要综合考虑各种因素，下面建议供参考：

1. **初步评估业务低峰时间段：**和开发、运营、运维等部门沟通，大致评估一个业务低峰时间段。
2. **拉取低峰段的业务量数据：**拉取低峰时间段前后 X 小时各业态的业务量。拉取业务量的模板参考：

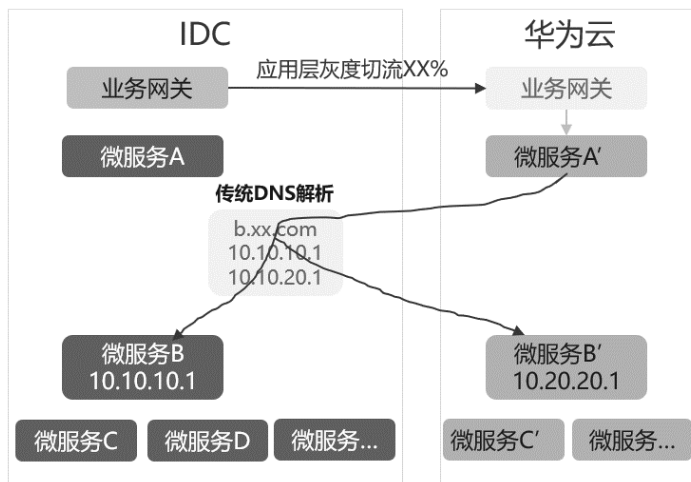
	19: 30 ~20: 30	20: 30 ~21: 30	21: 30 ~22: 30	22: 30 ~23: 30	23: 30 ~24: 30
业态 1: 非大促期间新建会员数	244	346	558	200	100
业态 2: 非大促期间新建会员数	109	270	690	100	86
业态 2: 非大促期间线下券使用数量	160	199	200	181	90
业态 2: 非大促期间线下券使用数量	40	60	70	153	190
业态 1: 本系统支付情况	200	300	600	700	200
业态 2: 本系统支付情况	100	200	300	400	500
业态 1: 非大促期间使用本系统自动停车的数量(平日)	50	80	60	300	800

业态 2: 非大促期间使用本系统自动停车的数量(周末)	160	70	300	900	1500
-----------------------------	-----	----	-----	-----	------

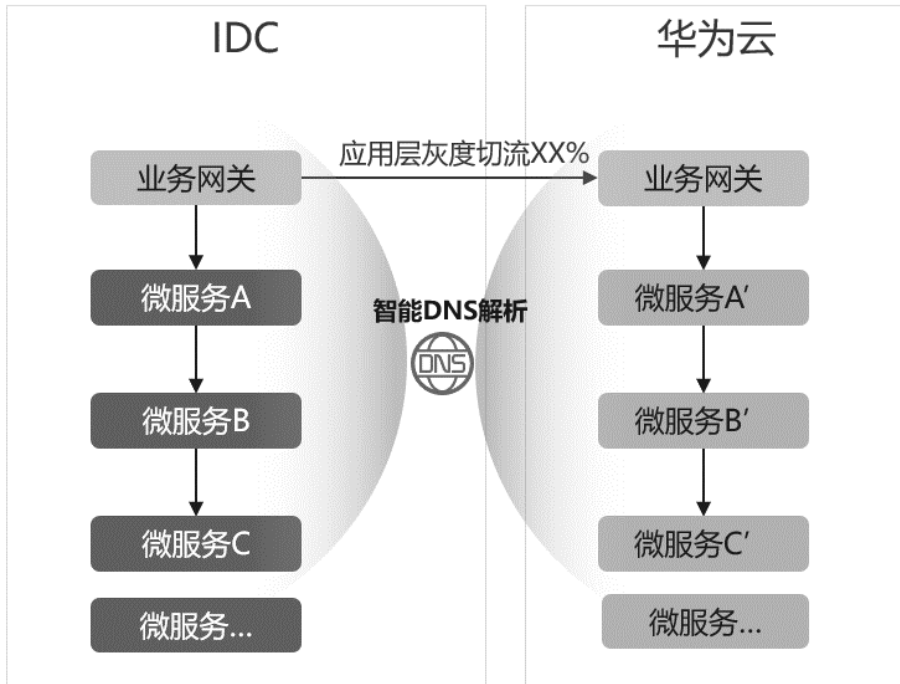
3. **定量分析并微调时间段:** 根据拉取的各业态业务量, 分析各个时间段的业务影响, 并对初步评估的切换时间窗进行微调。
4. **和受切换影响的相关方初步沟通:** 跟受切换影响的业态和第三方初步沟通, 收集各方诉求和建议。如果各方对切换时间窗异议较大, 无法达成一致, 需要上升 CTO、CEO 决策。
5. **综合各方诉求和影响, 上报 CTO 和 CEO 决策:** 根据拉取的业务单量、各业态和第三方的诉求, 上报 CTO、CEO 决策。
6. **最终确定切换时间窗口:** 根据 CTO、CEO 决策结果, 最终确定切换时间窗口。
7. **通知第三方或业态切换时间窗口:** 通知各业态和第三方最终切换的时间窗, 若有争议, 邀请相关领导沟通和协调。

11.8 如何解决应用跨云时延

应用双跑场景, 在灰度切流阶段, 线上和线下共用传统 DNS 解析, 微服务域名会随机解析到云上或 IDC, 当应用层灰度切流时, 会出现微服务间频繁跨云调用, 应用的访问时延会成倍增加, 影响业务体验, 如下图:



IDC 部署智能 DNS, 配置解析规则, 基于请求源的物理位置自动解析出最近的服务地址, 使访问请求分别在 IDC 和 华为云 内部自闭环, 避免跨云影响业务, 保证上云切流成功。



11.9 如何制定测试策略

大规模迁移往往涉及到成千上万条测试用例，全量测试必将导致切换时间很长，影响业务的正常开展。因此，制定合适的测试策略是非常重要的，建议如下：

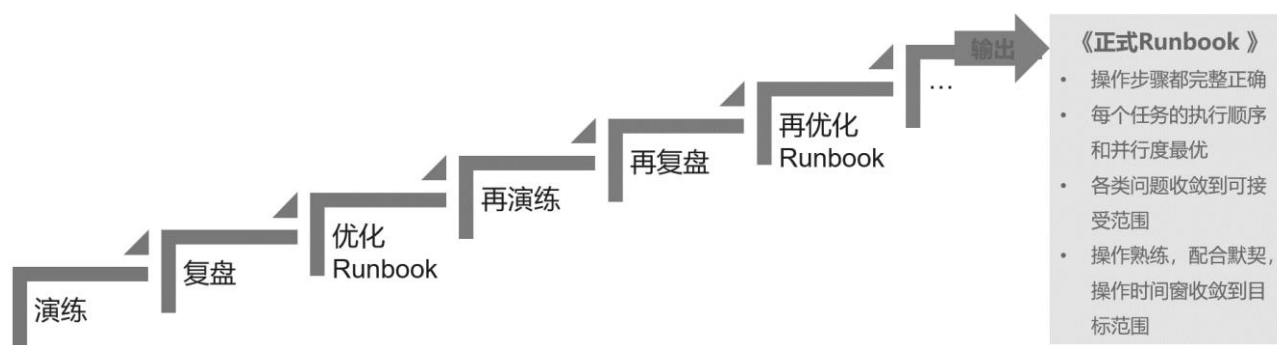
1. **风险导向的测试：**根据迁移的复杂性和关键性，确定测试的重点和优先级。优先完成对业务功能和数据完整性等关键方面有重大影响的测试用例验证，以最大限度地减少迁移过程中的风险。比如，可以先测试影响业务主流程的 P0 用例。
2. **自动化测试：**利用自动化测试工具和框架，减少测试的人工劳动。自动化测试能够加快测试执行速度，减少测试人员的负担，并提高测试的一致性和准确性。对于重复性高的测试用例，特别是针对系统基本功能的测试，自动化测试是非常合适的选择。
3. **并行执行：**将测试用例分成多个组，并在多台机器上并行执行。这样可以大大缩短整个测试执行的时间。通过并行执行，可以同时运行多个测试用例，提高测试效率。
4. **阶段性测试：**将测试分为多个阶段进行，每个阶段关注不同的测试目标。例如，优先验证核心功能（即应用的运行、系统与系统间的连通性、中间层的运行），然后渐进式的进行其他功能和场景的测试。
5. **集成测试：**在测试验证阶段，重点关注各个子系统之间的集成，特别是数据和功能流的正确性。确保不同子系统之间的数据传输和处理是正常的，并进行端到端的集成测试。
6. **回归测试：**对于已通过测试的部分，建议进行回归测试，以确保新迁移的部分没有对现有功能产生不良影响。同时，监测系统的性能和稳定性，确保迁移后整体系统的正常运行。

7. **预留足够的时间**：为测试阶段预留足够的时间，以确保充分的测试覆盖和错误修复。如果测试时间紧迫，可能会导致遗漏一些重要的测试场景和问题。

通过以上策略，可以逐步缩短测试时间，并在保证测试质量的同时，有效地完成大规模迁移的测试验证。

11.10 如何组织切换演练

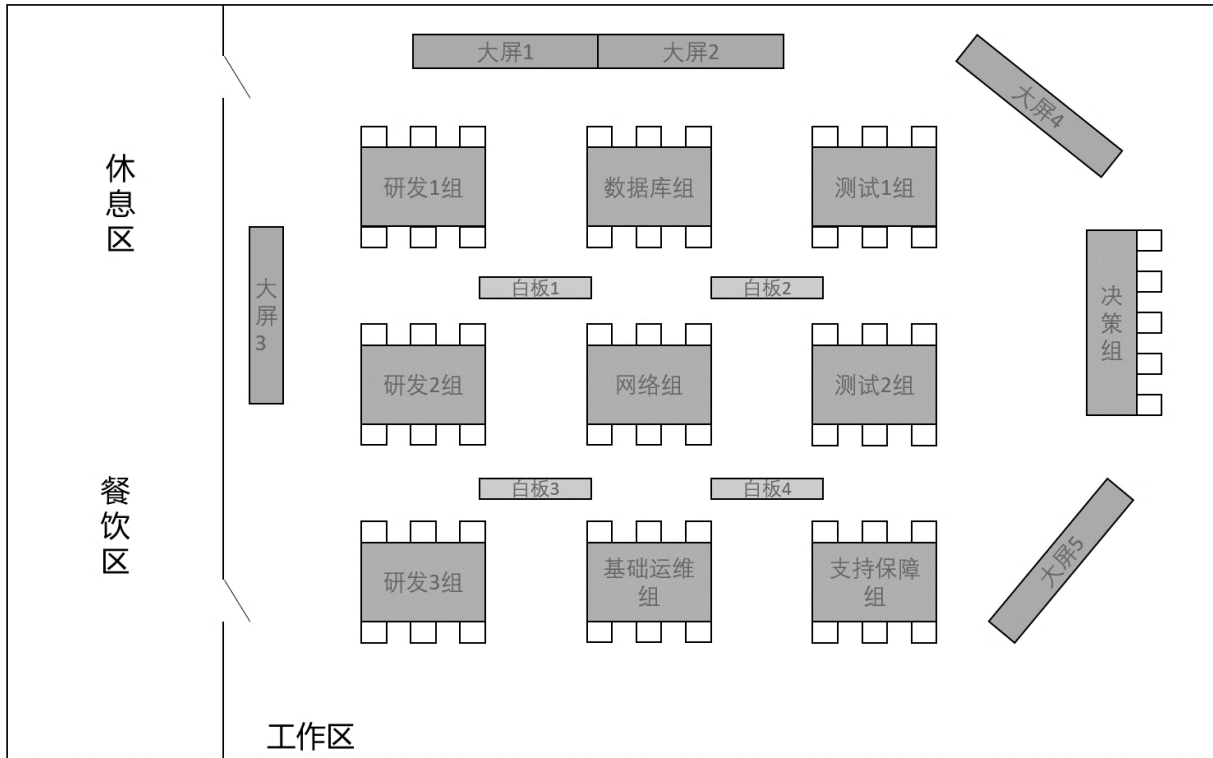
大规模迁移前一般要进行多次演练以降低正式切换的风险，演练要尽量模拟正式切换的环境和场景，通过演练->复盘->优化（Runbook）->再演练->再复盘->再优化（Runbook）->...，直至Runbook 中的步骤和各角色配合都比较完美，然后才形成最后正式的切换 Runbook。



11.10.1 会场布置

大型的演练/切换需要有一个专门的会场，以下是一些会场准备和布置座位的建议：

1. **选择合适的场地**：选择一个宽敞的场地，足够容纳所有参与者和设备，提供足够的桌子和椅子，以便参与者能够有良好的工作空间。同时，确保会场内部通风良好，并提供充足的电源、插座和网络接入等设施。
2. **分组座位**：根据团队或角色将人员分组，每个小组要坐到一起，方便高效沟通和协作
3. **跨团队沟通**：将相互依赖的小组坐在相邻的区域，方便不同团队之间的交流，促进跨团队的沟通和合作。
4. **核心团队的座位**：将引导员、记录员和关键决策者安排在会场的中央位置，以便他们能够更好地监督整个演练过程，及时进行沟通 and 决策。
5. **提供白板和显示屏**：确保会场有足够的白板和显示屏，方便展示和讨论。
6. **提供休息区**：为参与者设置休息区域，提供舒适的座椅、饮料和小吃，以便他们在演练繁忙之余可以得到适当的休息和放松。



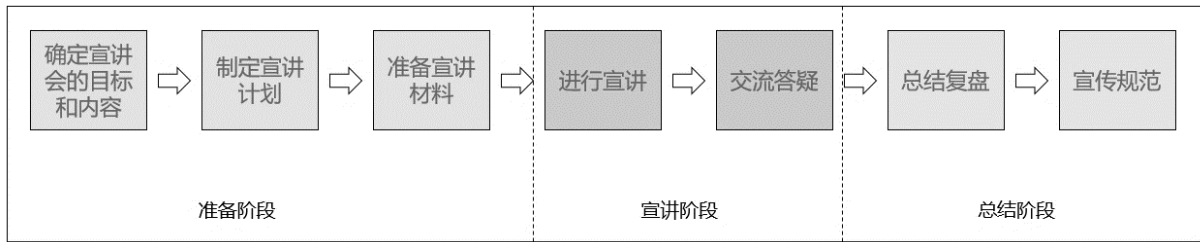
要提前准备好会场相关物料，示例如下：

序号	类别	事项	配合部门
1	场地	根据演练参与人数选择合适大小的会议室，检查座椅、桌子数量等	XX
2	物料	检查电源插板、投影、交换机、名牌等	XXX
3	住宿	安排参加切换人员，在就近的酒店住宿等	XXX
4	餐饮	食品、饮料、就餐区设置等	XXX

11.10.2 全员宣讲

大规模迁移通常涉及几十到数百人的协同，在大规模切换演练前都需要进行全员宣讲。全员宣讲的目的是为了向组织内的所有成员传达本项目的目的、规划、迁移方案、切换方案、改造方案、注意事项等，以确保所有成员都能够理解项目组的目标。通过全员宣讲，项目组可以确保所有成员都充分理解迁移和切换方案，避免信息传递不畅、误解和不一致的情况发生。

全员宣讲会建议按照以下流程进行：



1. 确定宣讲会的目标和内容：宣讲会的目的是为了向全员介绍项目的背景、目标、重要性和计划等内容。确定好要宣讲的具体内容，包括项目的目标、进展情况、关键节点和里程碑等。
2. 制定宣讲计划：确定全员宣讲会的时间、地点和参与人员。全员宣讲会应包含 IT 运维人员、IT 开发人员、业务人员及周边相关人员。确保所有相关人员都能参加，并提前通知他们。
3. 准备宣讲材料：根据确定的内容，准备好宣讲所需的材料，包括 PPT、文档等。确保材料简洁明了，重点突出，能够清晰地传达项目信息。
4. 进行宣讲：在宣讲会上，首先介绍项目的目标，然后详细介绍项目计划、进展情况和关键节点等内容。
5. 交流答疑：在宣讲会的过程中，应预留答疑时间，集中解答项目组成员的疑问。
6. 总结复盘：宣讲会结束后，及时总结会议内容，并将反馈和建议整理记录下来。根据反馈和建议进行项目调整和优化，并在后续工作中持续跟进。
7. 宣传规范：宣讲会结束后，可以通过各种方式进行宣传，如内部通知、邮件、企业 wiki 平台等。并将项目流程、规范等制定成文档或手册，确保所有相关人员都能了解并按照规范进行工作。

11.10.3 明确纪律

对于大规模的演练场景，需要有明确的纪律，保证切换期间的高效协同，纪律条令建议如下：

1. 只向 1 个人通报进展

切换过程中，操作人员只向引导员汇报进展和问题，不回答其他人员的问题。其他人员不得向操作人员询问进展。

2. 遇到问题及时上报，其他领域人员不要询问进展

切换过程中如遇到问题（无法解决/异常报错等影响切换进度）操作人员及时向引导人通报（可以举手示意）。操作人员接受引导员的安排（如：引导员告诉操作员，此问题立刻联系支付的 AA 和会员的 BB 一起定位）。

3. 提前 60 分钟到场

参与切换的人员需提早 60 分钟到达现场进行准备，并按照预定的座位落座，不得迟到早退影响切换操作时间。

4. 调节手机铃声适中

参与切换的人员需将手机提前设置为铃声（适中音量）或震动模式，接打电话请移步至就餐区或者阳台，切换现场不要有太大的异常响动。

5. 操作完在座位上保持安静

切换的操作人员完成操作后在现场保持安静，不询问其他人员的情况，不玩手机（游戏、视频等）。

6. 按照 runbook 通报进展

引导人按照切换步骤通过麦克风通报切换进展，记录人根据引导人的通报实施刷新 runbook 状态。

7. 切换场地禁止随意走动

除决策组人员、引导人，其余人员不要在现场来回走动，不能围观其他人操作。

8. 切换场所不能吃东西

确保所有行为均与切换演练有关，如需就餐请移步至食堂，不得在切换现场饮食。

9. 有序离开

切换完成后全体人员有序离场，将随身物品带离现场。

11.10.4 确定分工

大规模迁移通常会涉及几十到上百人的协同，如何协同好，需要有明确的角色和分工，参考如下：

序号	角色	职责	需要遵守的原则
1	操作人	<ul style="list-style-type: none"> ➢ 按照 runbook 步骤进行相应的操作 ➢ 定位问题并处理 ➢ 问题上升与上报 	问题无法定位或短期内无法解决需第一时间上报；
2	确认人	<ul style="list-style-type: none"> ➢ 验证切换操作是否完成 ➢ 协助定位问题 ➢ 问题上升与上报 ➢ 向引导人员同步操作进展和结果 	问题无法定位或短期内无法解决需第一时间上报；
3	引导人	<ul style="list-style-type: none"> ➢ 引导 runbook 的执行 ➢ 通报问题处理进展 	<ul style="list-style-type: none"> ➢ 引导 runbook 的执行步骤 ➢ 通报进展
4	记录人	<ul style="list-style-type: none"> ➢ 刷新 runbook ➢ 记录 runbook 中各个步骤的完成时间 ➢ 记录问题处理时长 	<ul style="list-style-type: none"> ➢ 刷新 runbook 的操作时间，记录问题处理时间，记录问题情况
5	决策人	<ul style="list-style-type: none"> ➢ 牵头对“决策点”进行决策 	<ul style="list-style-type: none"> ➢ 实时关注 runbook 的执行情况，根据业务影响决策是否回退。

6	现场管理	依据《切换记录条令》维护现场秩序，提醒现场人员遵守纪律；	<ul style="list-style-type: none"> ➤ 只维持场内秩序 ➤ 不参与问题处理，不参与问题记录
---	------	------------------------------	--

11.10.5 过程管理

运作方式：

1. 操作人员提前 60 分钟到现场，引导员宣布规则和注意事项。
2. 将 runbook 投影在大屏中，显示切换 runbook 关键步骤。
3. 引导员宣布切换开始，并宣布当前要执行的任务、操作人、确认人。
4. 操作人员按照 runbook 的详细步骤和指导执行操作，确认人检查和确认，通过外置显示器共享操作过程，操作人员执行完 runbook 条目后，经确认人确认，知会记录员在 runbook 中刷新进展，引导员通报进展，并宣布下一步要执行的任务、操作人和确认人。
5. 操作人员遇到问题，应及时通报给引导员，引导员安排技术人员进行讨论。
6. 遇到决策点，引导员召集管理团队按照应用级别进行决策是否回滚。

过程记录：



已执行完的任务可以标绿，正在执行的任务标黄，并投屏展示，方便大家看到进展：

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
5、停止 源端应用 服务	5.1	停止源端应用服务	停止源端应用服务	XXXX	阻塞解决，实在不行关掉服务器	XX	XX	XX
	5.2	XXX数据迁移	停止源端XXX服务	XXXX		非阻塞，在第9步骤之前完成	XX	xx
	5.2		停止源端的XXX服务	XXXX	xx			xx
	5.3		XXX增量文件迁移	XXXX	xx			xx
	5.3		XXX增量文件迁移	XXXX	xx			xx
	5.2	停止源端XXX服务	停止源端Apollo服务	XXXX	阻塞执行		xx	xx

11.10.6 优化 runbook

进行大规模上云迁移时，Runbook 操作步骤会很多，涉及到多方配合，可以通过演练可以不断优化 runbook，下面是一些建议：

1. **输出 runbook 初稿：** 在开始演练之前，根据迁移计划和目标，制定一个初始的 runbook。该 runbook 应包含详细的操作步骤、操作命令、操作人、确认人、预期操作时间。
2. **第 1 次演练：** 首先，使用初始的 runbook 进行演练，在一个模拟环境中，按照 runbook 的步骤进行切换操作，记录每个步骤的执行情况和遇到的问题。
3. **第 1 次演练复盘：** 在完成第 1 次演练后，团队应对演练过程进行复盘分析。在复盘会前，大家应汇总演练中发现的问题，并给出初步的解决措施和 runbook 优化建议。然后开正式的复盘会，runbook 优化建议进行讨论和决策，达成一致。
4. **第 1 次优化 runbook：** 根据第 1 次演练复盘的结论，对 runbook 进行优化。这可能包括增加细节步骤、提供更准确的操作指南、更新文档或修正错误等。
5. **第 2 次~第 N 次迭代演练：** 使用优化后的 runbook 进行一轮新的演练。记录每个步骤的执行情况，分析和解决遇到的问题，并继续收集反馈和意见。每轮演练后，团队应进行总结和反馈，进一步改进 runbook 的内容和流程。
6. **正式切换 Runbook：** 持续通过多轮演练不断迭代和优化 runbook，形成最终切换的 runbook。

通过不断演练和优化 runbook，团队可以逐步改进迁移过程的可靠性和效率，减少潜在的风险和问题。在这个过程中，要鼓励团队成员提供反馈和建议，保持开放的沟通，以共同完成优化 runbook 的目标。

11.11 如何做风险管理

大规模上云迁移是一项非常复杂的工作，企业将会面临很多管理和技术上的挑战，做好上云期间的风险管理是大规模迁移成功的保障，大规模迁移期间常见的风险如下：



下文将详细阐述上述各种风险，并提供应对策略，以帮助企业在大规模上云时，能更好地规避风险。

(一) 数据安全风险

对于任何企业来说，数据安全都是最为关键的问题。在迁移至云端过程中，如果没有有效的安全措施，数据可能会遭受泄露、篡改或丢失，带来重大损失。

应对策略：

1. 云安全评估：进行全面的云安全评估，了解云服务提供商的安全措施、数据隔离机制、合规性和审计能力。
2. 数据梳理和分类：将敏感和重要数据与普通数据分开，并为不同级别的数据应用不同的安全措施，对关键和敏感数据进行特别的保护，可以采取加密、脱敏等方式。
3. 身份验证和访问控制：实施严格的身份验证和访问控制机制和细粒度的访问控制策略，确保只有授权人员可以访问特定数据。
4. 数据加密：在数据存储、传输和处理过程中使用加密措施，保护数据免受未经授权的访问。
5. 备份和恢复：实施定期的数据备份和灾难恢复计划，以应对数据丢失、损坏或勒索软件等情况，对数据备份的可用性和完整性进行校验。
6. 定期漏洞扫描和安全审计：对云环境进行定期的漏洞扫描，及时发现并修复潜在的漏洞和弱点；对云操作进行安全审计，以防止非授权及无意的泄露行为。
7. 制定应急响应计划：制定和测试应急响应计划，以应对安全事件和数据泄露等紧急情况，确保应急响应计划的有效性。

8. 持续改进：不断审查和改进现有安全防护策略，以保障在技术和威胁持续改变的情况下，安全措施的有效性。

(二) 业务中断风险

迁移过程中，可能会发生服务中断或无法访问的情况，导致业务无法正常进行。

应对策略：

1. 制定详细的迁移计划和时间表，并在非业务高峰期执行迁移；
2. 进行充分的测试和验证，包括功能测试、性能测试；
3. 实施灵活的回滚策略，以便在必要时能够快速回滚到原始环境；
4. 建立有效的通信渠道，及时通知用户和相关团队迁移计划以及可能的影响；
5. 对于不可中断的业务，提前做好降级演练，切换期间进行业务降级。

(三) 运行性能风险

大规模上云迁移可能会因为网络延迟、应用程序与云服务之间的兼容性问题等，造成运行性能下降。

应对策略

1. 在选择云服务供应商时，应特别关注其服务的可靠性和稳定性，同时注意网络带宽和延迟，确保能达到业务需求；
2. 在迁移之前进行充分的性能测试，并优化应用程序和基础架构配置；
3. 对运行在云环境中的应用进行优化，提高性能和响应速度；
4. 使用自动化工具来监测和管理系统性能，并及时采取措施解决潜在问题；
5. 采用逐步迁移的策略，先迁移少量的关键应用程序和数据，进行测试和验证，确保正常运行后再进行下一步迁移；
6. 建立全面的监控和故障排除机制，及时发现和解决系统不稳定的问题，确保系统可靠性和性能。

(四) 批次规划风险

大规模上云迁移往往涉及到复杂的系统架构和大量的应用程序迁移，如果业务系统之间存在高度耦合，迁移过程中可能面临很难分批迁移，切换操作复杂的风险。为了应对这种风险，可以考虑以下措施：

应对策略

1. 深入了解业务系统之间的依赖关系，进行风险评估和合理规划，以降低对业务连续性的影响。
2. 根据业务依赖关系和优先级，将迁移划分为阶段，逐步迁移，减少对整个业务的冲击。先迁移少量的应用程序或服务，并进行测试和验证，然后再逐步扩大规模。
3. 制定详细的迁移计划，并确保包含了必要的资源和时间预算。
4. 预留足够的时间和资源来解决可能出现的问题和挑战。

(五) 迁移成本风险

大规模上云迁移的初期，可能会面临高昂的迁移成本，包括应用程序重构、数据迁移、员工培训等费用，而在运营期间，还有可能产生不可预期的附加费用。

应对策略

1. 提前做全面的迁移成本评估，包括直接和间接成本。
2. 尽可能选择能降低迁移复杂性的云服务供应商，例如支持一键迁移、兼容多种硬件和软件环境等。
3. 尽可能通过自动化方式进行迁移，降低人力成本。
4. 在迁移前进行详细的成本分析和规划，包括计算、存储、网络和支持等方面的成本。
5. 对于大型应用程序，可以先进行小规模试点迁移，评估迁移过程中的成本和风险，并做出调整。
6. 定期监控和优化云资源的使用，优化资源利用率，以避免资源浪费和不必要的费用支出。
7. 定期审查和优化云服务的使用情况，以减少不必要的费用。
8. 定期审查和优化云服务供应商的合同和定价模型，以确保最合适的成本效益。

(六) 人员技能风险

组织内部缺乏云计算和相关技术的专业知识和经验积累，可能影响迁移的进度和质量。

应对策略：

1. 培训和教育现有员工，提高他们在云计算领域的技能和知识水平。
2. 考虑雇佣具有云计算经验的专业人员或与外部顾问合作，以填补技能缺口。
3. 建立一个跨职能的团队，包括开发人员、运维人员和安全专家，共同推动迁移项目。

(七) 业务适配风险

上云迁移可能需要调整现有的业务流程，应用程序也可能会出现与现有系统不兼容的问题。为了应对这个风险，需要进行充分的测试和验证，确保新环境与现有系统的兼容性，应用程序可能也需要适配改造。

应对策略：

1. 进行详细的业务和应用程序分析，评估现有流程和应用程序与云环境的适配性。
2. 识别需要改变的方面并制定相应计划，比如必要的上云适配改造。
3. 与关键利益相关者和业务用户进行合作，确保他们对变化有清晰的了解并参与到迁移过程中。

(八) 合规风险

企业的数据库、应用一旦迁移到云端，就需要符合目标国家或地区的法律法规，例如关于数据隐私保护、数据存储、数据迁移等方面的规定。

应对策略

1. 提前了解和学习目标国家或地区的法律法规，并确保自身业务和操作符合相关规定。
2. 选择符合所在地域和行业合规要求的云服务提供商，例如一些国家或地区可能要求数据中心必须在本地。
3. 尽可能明确在合同中规定数据的所有权和责任归属，以及在服务终止后的数据处理方式。

(九) 运维和治理风险

大规模上云后，企业的运维和治理活动将与 IDC 有很大不同，费用控制、权限控制、服务管理、运维监控等方面。迁移到云环境需要新的技能和知识，团队可能缺乏云运维和治理相关的经验。

应对策略

1. 建立合适的云团队，进行专业的云技术和管理方面的培训，确保团队有处理各种云问题的能力。
2. 提供培训和培养计划，使团队成员掌握所需的技能和知识。与云服务供应商和第三方培训机构合作，组织培训课程和认证计划。培养内部的云中心或专家团队，以支持和管理云环境。
3. 建立合理且完善的运维和治理流程，利用自动化工具日常活动，提高运维效率。
4. 监控服务质量和费用，定期评估云服务供应商的服务质量和成本效益。

总的来说，虽然大规模上云迁移存在风险，但只要企业做好充分的准备和应对，就能够充分享受云计算带来的便利和效率。在迁移过程中，通常需要对软硬件架构进行大幅改造，因此关键在于找准平衡点，找到最符合企业业务需求和风险承受能力的上云迁移策略。

11.12 如何做复盘分析

在每个批次的切换活动后，应及时进行复盘总结，对切换活动中的收获和问题进行复盘和总结，对做的好的地方进行延续，对做的不好的地方进行改进。上云迁移的复盘分析是非常重要的，它可以给后续的迁移批次提供宝贵的经验，并不断改进迁移过程。

(一) 复盘的价值

上云迁移中的复盘分析对于后续的迁移批次具有重要价值，以下是一些相关的价值参考：

1. **发现潜在问题：**复盘分析会帮助团队发现在先前的迁移中可能出现的问题和挑战。通过仔细审查迁移过程、检查关键环节和步骤，团队可以识别并提前解决潜在问题，从而降低后续迁移批次的风险和难度。
2. **总结经验教训：**复盘分析允许团队回顾和总结迁移过程中的经验教训。通过分享成功实践和面对的困难，团队成员可以相互学习和借鉴，让后续迁移批次更高效且更有针对性。
3. **改进迁移策略：**通过复盘分析，团队可以评估并调整迁移策略。根据实际经验和教训，团队有机会优化迁移计划、改进迁移流程、提高资源利用效率，从而在后续的迁移批次中取得更好的效果。

4. **提高效率和质量：**通过复盘分析，团队可以识别并解决迁移过程中的瓶颈和问题。这有助于提高迁移的效率，减少重复工作，同时确保数据的完整性和安全性。
5. **促进团队合作和沟通：**复盘分析过程是一个团队成员共同参与的机会。在这个过程中，团队成员可以分享彼此的观点、思维方式和工作方式，促进团队合作和协作，并加强团队的沟通能力。
6. **持续改进：**复盘分析帮助团队建立一个持续改进的文化。通过不断复盘和反思，团队将获得更多的见解，并能够在后续迁移批次中应用新的改进措施，进一步提升迁移过程的效率和成功率。

综上所述，复盘分析对于后续的迁移批次具有重要价值。它不仅可以帮助团队发现问题、总结经验教训，还能优化迁移策略、提高效率和质量，促进团队协作和沟通，并推动持续改进。这将使后续的迁移批次更加顺利和成功。

(二) 复盘的过程

迁移复盘有助于发现问题、总结经验，并提供改进迁移过程的方向，复盘的方法可以参考如下：

1. **召集团队：**邀请所有与上云迁移相关的团队成员参与复盘会议。这包括项目经理、开发、测试、运维、产品经理、决策团队、云厂商、集成商等。确保团队成员的代表足够全面，能够提供关键的见解和反馈。
2. **回顾迁移目标：**首先，回顾本批次迁移的目标和里程碑，确保团队对整个迁移过程的目标有清晰的理解。参考并比较实际达成的目标与最初设定的目标，以及其中的差异和原因。
3. **分享成功和挑战：**团队成员可以分享与迁移过程相关的成功案例和值得称赞的成就，以及遇到的挑战和困难。确保每个人都有机会分享经验和观点，倾听他们的见解。
4. **识别问题和障碍：**团队共同审查迁移过程中出现的问题和障碍。记录具体的问题和障碍，并对其进行分类和分析。确定问题的根本原因，以避免类似问题在后续的迁移批次中再次出现。
5. **分析影响和教训：**评估问题和障碍对迁移过程和业务的影响。分析其严重程度以及衍生出的教训和经验，找出可以改进的方面和潜在的解决方案。
6. **制定改进措施：**基于复盘分析的结果，制定具体的改进措施和行动计划。确保所提出的改进建议是具体、可执行，并能够直接应用于后续的迁移批次。
7. **追踪和复盘反馈：**跟踪和记录已经实施的改进措施的效果，并定期进行复盘分析的反馈会议，确保改进计划得到适时的评估和调整。

这些步骤可以根据团队和项目的特定需求进行调整和定制。重要的是确保复盘会议是一个开放和包容的环境，鼓励团队成员分享经验和提出建议，从而形成一个持续学习和改进的文化。通过持续的复盘分析，团队可以不断优化和提升上云迁移的效率和质量。

(三) 复盘注意事项

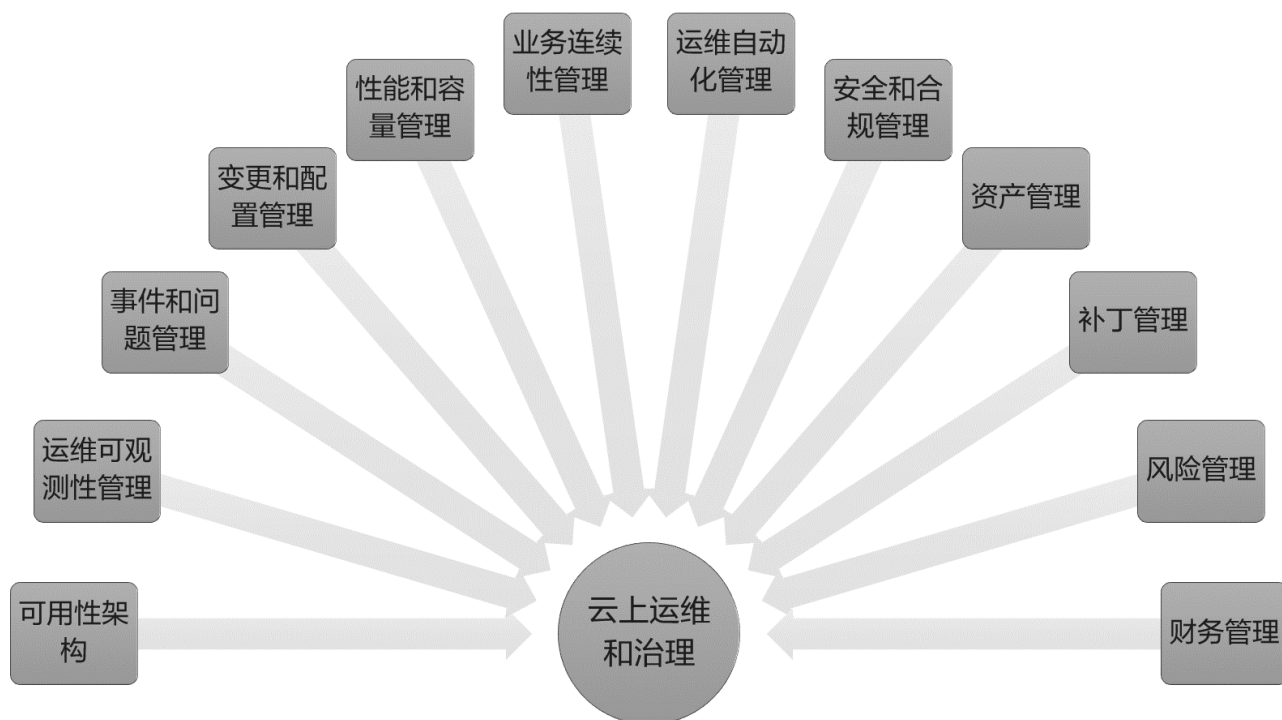
在复盘总结过程中，应注意以下方面：

1. 为提升复盘效率，在复盘会前，与会人要提前做好相关准备工作，带着思考和建议来参加复盘
2. 提前明确需要复盘的事件或问题。确定复盘的目标和范围，提高复盘会的效率，避免思维发散。

3. 提前收集与复盘事件相关的数据、日志、报告等信息，并输出复盘思维导图或材料，以便全面了解待复盘事件的全貌。
4. 复盘问题时，着重关注问题本身而不是个人责任，避免指责和埋怨，着重于问题的原因和解决方案。
5. 鼓励所有参与人员积极参与讨论，分享意见和经验。
6. 根据复盘分析的结果，制定具体的改进措施。确保改进措施切实可行，并建立有效的跟踪机制，确保改进措施得到有效执行，并及时调整和反馈。
7. 将复盘总结的过程、结果以及提出的改进措施记录成会议纪要或文档形式。为后续批次的切换提供参考，并有助于知识沉淀和分享。

12 云上运维及治理

在基础架构准备阶段，我们已经做过一些初步的运维和治理工作，但上云后，IT 环境会随着业务的变化而变化，因此云上运维和治理是一个持续的过程，随着业务发展，不断进行配置优化，使业务收益最大化，业务风险最小化。云上运维和治理主要涉及如下几个方面：



本章只做初步描述，更多专业内容请参考《华为云确定性运维白皮书》。

12.1 云运维概述

随着云计算技术的不断成熟和普及，越来越多的企业选择将自己的业务迁移到云平台上。在这个过程中，运维扮演着重要的角色，负责保证云平台的正常运行，以及对业务进行监控、调整和优化。企业上云后，运维的工作将会发生很大的变化。传统的运维模式已经无法满足云计算时代的需求，因此，运维需要进行全面的转型和升级，包括运维组织、运维流程、运维技术平台、运维人员和技能等。

1. 运维组织

企业上云后，运维组织需要进行调整。传统的运维组织结构通常是分层次的，由运维经理、运维工程师、运维管理员等组成。但是，在云计算时代，这种组织结构已经无法满足需求。因此，运维组织需要进行扁平化，强调团队协作和快速响应能力。

在云计算时代，运维团队需要具备更高的敏捷性和灵活性。因此，运维团队需要采用敏捷开发的方法，强调快速迭代和持续交付。在运维团队的组织结构上，可以参照 DevOps 模式，将开发和运维团队进行融合，构建跨职能团队，实现快速迭代和持续交付。此外，运维团队还需要具备更高的**自动化能力**，以便更好地支持云计算环境。

2. 运维流程

企业上云后，运维流程也需要进行调整。传统的运维流程通常是基于 ITIL 框架的，包括问题管理、变更管理、配置管理等。但是，在云计算时代，这种流程已经无法满足需求。因此，运维流程需要更加灵活和自动化。

在云计算时代，运维流程需要更加注重**自动化和持续交付**。运维团队需要采用 DevOps 的方法，将开发和运维融合在一起，实现持续集成、持续交付和持续部署。运维流程还需要更加注重安全性和可靠性，以确保云计算环境的稳定性和安全性。由于云计算环境具有高度自动化的特点，因此在运维流程中可以增加**自动化测试、自动化部署、自动化监控**等环节，提高运维效率。同时，在服务质量保证方面，可以引入基于 SLA 的服务管理机制，确保服务的可用性和稳定性。

3. 运维技术平台

企业上云后，运维技术平台也需要进行调整。传统的运维技术平台通常是基于物理服务器的，包括服务器、存储、网络等。但是，在云计算时代，这种技术平台已经无法满足需求。因此，运维技术平台需要更加注重虚拟化和云化。

在云计算环境下，运维技术平台也需要进行相应的升级和优化。运维技术平台需要更加注重容器化和微服务化，以便更好地支持 DevOps 的方法，可以考虑使用容器化技术，将应用程序打包成容器，实现快速部署和扩展。同时，在监控和日志管理方面，可以使用 ELK、Prometheus 等开源工具，实现全链路的监控和可视化。

4. 运维人员和技能

企业上云后，运维人员和技能也需要进行调整。传统的运维人员通常是基于物理服务器的，包括服务器、存储、网络等。但是，在云计算时代，这种人员已经无法满足需求。因此，运维人员需要具备更高的技能和能力。

在云计算时代，运维人员需要具备更高的技能和能力。运维团队需要具备更高的自动化能力和编程能力，以便更好地支持 DevOps 的方法。此外，运维人员还需要具备更高的安全意识和安全技能，以确保云计算环境的安全性。

总之，企业上云后，运维需要进行全面的转型和升级。运维组织需要进行扁平化，强调团队协作和快速响应能力。运维流程需要更加灵活和自动化，采用 DevOps 的方法，实现持续集成、持续交付和持续部署。运维技术平台需要更加注重虚拟化和云化，采用容器化和微服务化的方法。运维人员需要具备更高的技能和能力，包括自动化能力、编程能力和安全技能。

12.2 云运维组织

企业上云后，运维组织的调整和优化是至关重要的。在传统的 IT 运维中，通常会有专门的服务器、网络、存储等职能部门，各自负责不同的硬件设备和系统服务。但是，在云计算环境下，这种分工模式已经不再适用，因为云平台提供了一系列统一的服务和接口，使得硬件和软件之间的边界变得模糊和不可见。因此，企业需要通过重新组织运维团队，来适应云计算的特点和需求。

1. 建立云运维团队

首先，企业需要成立一个专门的云运维团队，负责云平台的日常运营和维护。这个团队应该由具有云计算知识和经验的专业人员组成，包括云架构师、开发工程师、运维工程师等。他们需要具备深入了解云平台技术特性和使用场景的能力，以便能够有效地管理和维护云服务。

2. 重构职能和责任

在云计算环境下，传统的硬件设备和系统服务已经被虚拟化和抽象化，因此原来的职能和责任也需要重新定义和分配。企业需要结合云平台的特点，制定新的职能和责任，以保证整个运维团队能够协同工作和高效运转。

3. 引入 DevOps 运维组织

传统运维模式通常采用分层管理方式，将开发、测试、运维等不同职能部门分开管理。在这种模式下，各个部门之间通常存在着对立和矛盾，协作效率低下，往往难以满足快速迭代和持续交付的需求。

为了解决传统运维模式的缺陷，可以采用 DevOps 运维模式，即将开发和运维进行融合，构建跨职能团队，实现快速迭代和持续交付。DevOps 团队由开发人员、运维人员和质量保证人员组成，他们共同负责软件的开发、测试、部署、监控和维护等工作。在 DevOps 模式中，强调自动化和监控整个软件开发过程，并在测试、部署、运行等阶段实现快速反馈和持续改进。

采用 DevOps 模式的运维团队可以获得以下优势：

1) 提高效率

DevOps 模式强调自动化和监控整个软件开发过程，可以大幅提高软件开发和运维效率，缩短上线时间。

2) 保证质量

通过自动化测试、自动化部署、自动化监控等手段，可以保证产品的质量和稳定性。

3) 提高协作效率

DevOps 团队采用跨职能团队的方式进行工作，协作效率更高，各个部门之间通常不存在对立和矛盾。

4) 加强安全性

DevOps 团队可以通过持续监控和快速反应来加强安全性，及时发现和解决安全问题。

12.3 云运维流程

一旦企业上云，就需要面对新的运维挑战，在云上进行运维需要掌握新的技术和方法，以确保云服务的高可用性和稳定性。在进行云上运维之前，企业需要进行一些准备工作。

首先，需要确保云基础设施的可靠性和安全性。这包括确保云平台的稳定性、备份策略的制定、灾备方案的设计、安全性补丁的及时更新等等。

其次，需要对云上的应用程序和数据进行分类和管理，以便更好地保护其安全性。

最后，需要确定云上的监控策略和流程，并确保所有必要的监控工具和服务都已准备就绪。

企业在进行云上运维之前，需要制定完善的运维策略。运维策略应该包括监控策略、自动化策略、容错和可用性策略、安全策略、性能优化策略等等。运维策略需要根据企业的业务需求和应用程序特点进行制定。

1. 监控和警报

监控是云上运维中最重要的一环之一。监控可以帮助企业及时发现和处理云服务的问题，并避免潜在的灾难。监控内容包括服务器的基本状态、应用程序的运行状态、网络带宽等等。监控可以通过云平台的自带监控服务，也可以通过第三方监控工具来实现。监控服务需要设置警报规则，以便在出现问题时及时通知相关人员。

2. 自动化

自动化是云上运维的另一个重要环节。自动化可以帮助企业快速响应和解决问题，并减少人工干预的误差。自动化内容包括自动化部署、自动化测试、自动化备份、自动化修复等等。企业可以使用云平台自带的自动化工具，也可以使用第三方自动化工具来实现。

3. 可用性和容错

可用性和容错是云上运维的核心。云服务的可用性和容错能力决定了企业的业务连续性和稳定性。可用性和容错需要从多个层面进行保障，包括网络、存储、计算、应用程序等等。云平台提供了许多容错和可用性解决方案，例如负载均衡、自动扩展、容器化等等。企业需要根据自身的业务需求和应用程序特点，选择最适合的容错和可用性解决方案。

4. 安全性

安全性是云上运维的另一个重要环节。云服务的安全性需要从多个维度进行保障，包括网络安全、身份认证、访问控制、数据加密等等。企业需要制定完善的安全策略，包括数据分类管理、网络安全策略、访问控制策略等等。此外，企业还需要定期进行安全漏洞扫描和修复，并建立完善的安全监控和警报机制。

5. 性能优化

性能优化是云上运维的最后一个环节。性能优化可以帮助企业提高业务效率和用户体验。性能优化需要从多个层面进行，包括应用程序优化、数据库优化、网络优化等等。企业可以使用云平台提供的性能优化工具，也可以使用第三方性能优化工具来进行优化。

6. 定期备份和恢复测试

备份和恢复测试是云上运维中必不可少的环节。企业需要定期备份云上的数据和应用程序，并进行恢复测试，以确保备份和恢复的可靠性和准确性。备份和恢复测试需要定期进行，以确保备份的及时性和准确性。

7. 不断优化和改进

云上运维流程是一个不断优化和改进的过程。企业需要不断地评估云上运维的效果，并根据评估结果进行优化和改进。优化和改进的内容包括监控策略、自动化策略、容错和可用性策略、安全策略、性能优化策略等等。企业需要保持敏锐的洞察力和创新精神，不断探索新的云上运维方法和技术。

总之，企业上云后，运维流程是一项非常重要的工作。运维流程需要从多个层面进行保障，包括监控和警报、自动化、可用性和容错、安全性、性能优化等等。企业需要制定完善的运维策略，并使用云平台自带的工具和服务，也可以使用第三方工具和服务来进行云上运维。备份和恢复测试是云上运维中必不可少的环节，企业需要不断优化和改进云上运维流程，以确保云服务的高可用性和稳定性。

12.4 云运维平台

如何管理和监控运行在云上的应用程序和服务，以确保它们始终处于正常运行状态，是一个非常值得考虑的问题。因此，在企业将业务迁移到云端之前，需要对运维技术平台进行规划和优化。运维管理分为体验、自动化和效能三类，企业可以结合自己的业务特点，构建适合自身的云上运维平台。常见的运维平台和工具如下：

运维体验管理		运维交付自动化		运维效能分析
ITSM		CICD 自动化		AIOps 平台
CMDB		DevOps 平台		应用性能监控 APM
资产管理		IT 流程自动化		动态容量管理平台
IT 服务管理		服务生命周期自动化		三维数字监控平台
学习与知识管理		IT 配置自动化		网络故障性能监控平台
服务请求管理		补丁管理自动化		统一通信监控平台

对于中大型企业，云下往往已经形成了较完整的运维管理体系，企业需要了解云上运维的目标和需求，分析企业现状，包括 CMDB、监控、自动化、ITSM 等，清晰定义云平台与运维体系间的关系，定义合适的运维体系架构：

1. 如果企业考虑建设统一的云管平台（Cloud Management Platform），则需要将 CMP 放到运维管理体系中统筹考虑，明确 CMP 在运维系统中的位置，以及与 ITOM 中其他运维领域如何交互
2. 打通企业 CMDB、监控、自动化运维平台、ITSM 流程管理，实现资源的全生命周期管理
3. 构建统一的运维数据平台，将监控运维数据集中入湖处理，进行数据清洗、AI 分析处理，对外提供服务及可视化能力，做到运维的智能化、更好的服务于业务，支撑运营决策与成本优化。

云计算有丰富的计费模式，结合公有云弹性和按需模式，云上运维意味着转变成成本优化的思维，运维需要帮助企业达成 IT 的灵活性与低成本之间的平衡。

12.4.1 ITSM

ITSM（IT Service Management）是指管理 IT 服务的过程和方法，旨在实现 IT 服务的高质量、高效率和 high 可靠性。ITSM 平台通常由以下模块组成：

1. 服务台：用于解决用户的问题和请求，并为用户提供各种支持。
2. 变更管理：用于记录和跟踪所有变更请求，包括硬件、软件、网络、安全等方面的变更。
3. 事件管理：用于监控和报告与 IT 服务相关的事件，例如故障、警报、监控数据等等。
4. 配置管理：用于记录 IT 资源的配置信息，例如服务器、网络设备、存储设备等等。

在云上部署应用程序时，ITSM 平台的一个重要作用是确保应用程序始终处于正常运行状态。如果应用程序出现故障或异常，服务台可以及时响应并解决问题。变更管理可以跟踪所有对应用程序进行的变更，并通过审批流程确保变更的安全性和质量性。事件管理可以监控应用程序的健康状况，并在发生故障或异常时及时报告给相关团队。配置管理可以记录应用程序所依赖的硬件和软件资源，以及它们之间的关联关系，帮助运维团队更好地了解和管理整个系统的架构和拓扑结构。

12.4.2 CMDB

CMDB（Configuration Management Database）是指一种用于记录 IT 资源配置信息的数据库。CMDB 通常包含以下信息：

1. 资源属性：记录 IT 资源的各项属性信息，例如 IP 地址、MAC 地址、操作系统版本、CPU 型号、内存大小等等。
2. 资源关系：记录 IT 资源之间的关联关系，例如服务器与存储设备之间的关系、虚拟机与物理主机之间的关系等等。
3. 变更历史：记录 IT 资源的变更历史，包括创建时间、修改时间、删除时间等等。

在云上部署应用程序时，CMDB 的一个重要作用是帮助运维团队更好地了解和管理整个系统的架构和拓扑结构。通过记录应用程序所依赖的硬件和软件资源，以及它们之间的关联关系，CMDB 可以帮助运维团队更好地了解整个系统的逻辑架构和物理拓扑结构，从而更好地进行故障排除和问题解决。

另外，CMDB 还可以提供实时的资源状态信息和监控数据，帮助运维团队更好地了解系统的运行情况和性能状况，并在需要时快速响应和解决问题。

12.4.3 ITOM

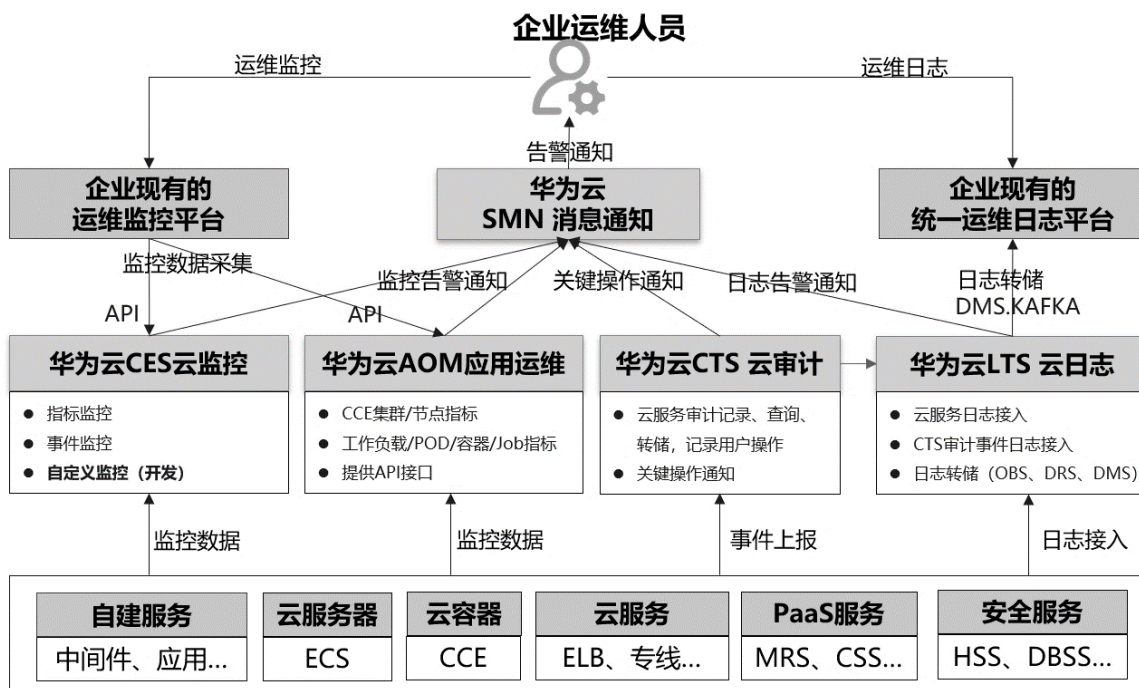
当企业上云后，运维团队需要重新调整其工作方式和实践，在云环境中，运维的重点将从传统的硬件设备和基础架构管理转移到更多的服务管理和自动化，运维团队需要采用适应云环境的 ITOM 平台来管理和监控云基础设施、优化资源利用率、提供高效的服务管理、确保安全性和可用性，并实现自动化和持续交付，这将帮助企业充分发挥云计算的优势。ITOM（IT Operations Management）提供了一套综合的解决方案来管理企业的 IT 基础设施和服务，包括：

1. 自动化管理：云环境具有弹性和可扩展性，因此自动化管理对于提高效率和降低成本至关重要。ITOM 平台应该能够提供自动化工具和功能，以简化常规任务的执行，例如自动配置、监控、修复和扩展。
2. 资源管理：在云环境中，资源管理变得更加复杂。ITOM 平台应该提供一个集中化的资源管理系统，用于跟踪和优化云资源的使用情况。这包括监控虚拟机、存储空间、网络带宽等，并提供自动化报告和警报机制。
3. 监控和故障排除：ITOM 平台应该具备全面的监控功能，实时跟踪云环境中各个组件的性能和可用性。它应该能够提供即时警报和通知，并自动执行故障排除流程来快速解决问题。
4. 安全管理：上云后，安全变得尤为重要。ITOM 平台应该具备强大的安全管理功能，包括访问控制、身份验证、日志记录和事件响应等。它应该能够监测潜在的安全漏洞，并提供实施安全策略和合规性控制的能力。
5. 服务管理：云环境中，运维团队需要转变为提供服务的角色。ITOM 平台应该支持服务目录、请求管理、变更管理和问题管理等功能，以确保及时响应用户需求，并跟踪和解决服务相关的问题。
6. 可视化和报告：ITOM 平台应该提供直观的界面和报告功能，用于监控和分析云环境的性能、资源利用率和服务水平。这些报告可以帮助运维团队进行容量规划、优化资源配置和评估服务质量。
7. 弹性伸缩：云环境的一个主要特点是其弹性和可扩展性。ITOM 平台应该能够与云服务提供商的自动伸缩功能集成，以根据需求自动调整资源规模，并确保高可用性和性能。
8. 持续交付：在云环境中，持续交付变得更加重要。ITOM 平台应该支持自动化部署、配置管理和版本控制，以便快速部署和更新应用程序，并确保一致性和可靠性。

12.4.4 运维平台选择

1. 使用云平台自带的工具和服务

云平台提供了许多自带的工具和服务，可以帮助企业更好地进行云上运维。企业可以使用云平台自带的监控服务、自动化工具、容错解决方案、安全解决方案等等。这些自带的工具和服务通常比第三方工具更加集成和稳定。



2. 使用第三方工具和服务

除了云平台自带的工具和服务之外，企业还可以使用第三方工具和服务来进行云上运维。例如，企业可以使用第三方监控工具、自动化工具、容错解决方案、安全解决方案等等。使用第三方工具需要注意选择有信誉和可靠的供应商。华为云 Market Place 提供了很多联营商品供客户选择。

服务名称	价格
智能业务运维平台	¥980,000.00 /次
云管理运维服务	¥388.00 /月
SAP系统迁移实施运维服务	¥3,500.00 /次
赛意迁移实施及运维服务	¥6,000.00 /次
智能业务运维平台配套服务	-
沃趣QFusion数据库运维...	-
IStorM DR容灾运维管理...	-
沃趣QFusion数据库运维...	-

3. 引入自动化和智能化技术

在云计算环境下，运维工作量和复杂度都会大幅增加，因此需要借助自动化和智能化技术来提高运维效率和质量。企业可以引入自动化运维工具和平台，如 Puppet、Chef、Ansible 等，来实现自动化部

署、配置、监控和维护。同时，还可以利用人工智能和机器学习等技术，对运维数据和日志进行分析和挖掘，以便更好地诊断和解决问题。

12.4.5 运维平台集成

企业上云后，与云平台自带的工具和服务进行集成是关键的一步，它可以提高运维效率、降低管理成本，并实现更好的资源利用和监控。下面将需要集成的方面以及相应的集成方法进行阐述。

1. ITSM (Information Technology Service Management) 集成:

ITSM 是指为管理和交付 IT 服务而采用的一系列实践和方法。在企业上云后，需要将原有的 ITSM 系统与云平台自带的工具进行集成，以确保云服务的管理和交付。

集成目标:

- 1) 自动化云资源的请求、审批和分配流程。
- 2) 在 ITSM 系统中展示云资源的相关信息，例如实例状态、使用情况等。
- 3) 整合事件管理，将云平台产生的事件与 ITSM 系统进行关联和处理。
- 4) 提供用户自助服务，使其能够通过 ITSM 系统访问和管理云资源。

集成方法:

- 1) 使用云平台提供的 API 或 SDK，与 ITSM 系统进行对接。通过调用云平台的接口，实现云资源的创建、删除和配置等操作。
- 2) 建立自动化工作流，将云资源的申请、审批和发布过程纳入 ITSM 系统的服务目录和流程中。
- 3) 通过事件集成，将云平台产生的事件发送给 ITSM 系统，以便进行统一的事件管理和处理。
- 4) 在 ITSM 系统中嵌入云平台的用户界面，提供自助服务和资源管理功能。

2. ITOM (IT Operations Management) 集成:

ITOM 涉及监控、自动化和管理 IT 基础设施和操作。在企业上云后，需要将原有的 ITOM 系统与云平台自带的工具进行集成，实现对云资源的全面监控和管理。

集成目标:

- 1) 自动发现和注册云资源，并将其纳入到 ITOM 系统的配置管理数据库 (CMDB) 中。
- 2) 监控云资源的性能和可用性，及时发现和解决问题。
- 3) 实现自动化运维，通过 ITOM 系统对云资源进行批量操作和管理。
- 4) 提供报告和分析功能，帮助优化云资源的使用和规划。

集成方法:

- 1) 使用云平台提供的 API 或 SDK，实现与 ITOM 系统的数据交换。通过调用云平台的接口，获取云资源的指标数据、日志和状态信息等。

- 2) 建立监控策略和告警规则，将云平台的监控数据与 ITOM 系统进行对接，实现全面的监控和告警功能。
- 3) 利用 ITOM 系统的自动化工具，对云资源进行批量操作和管理。例如，自动调整云资源的容量、配置和位置等。
- 4) 在 ITOM 系统中集成云平台的报告和分析功能，提供针对云资源的性能、使用情况和优化建议等的报告。

3. CMDB (Configuration Management Database) 集成:

CMDB 是存储和管理 IT 基础设施配置信息的数据库。在企业上云后，需要将云平台自带的配置管理工具与原有的 CMDB 进行集成，实现对云资源的统一管理和控制。

集成目标:

- 1) 将云资源的配置信息纳入到 CMDB 中，实现全面的配置管理和跟踪。
- 2) 提供云资源的关系和依赖性视图，帮助理解和分析云环境。
- 3) 实现变更管理，将云资源的变更记录和审批过程纳入到 CMDB 中。
- 4) 支持自动发现和注册云资源，保持 CMDB 的准确性和完整性。

集成方法:

- 1) 使用云平台提供的 API 或 SDK，实现与 CMDB 的数据交换。通过调用云平台的接口，将云资源的配置信息同步到 CMDB 中，包括实例、网络、存储等相关信息。
- 2) 建立关系映射，将云资源与 CMDB 中的其他配置项进行关联，形成资源的关系和依赖性视图。
- 3) 利用 CMDB 系统的变更管理功能，记录和追踪云资源的变更历史，包括配置的修改、扩容、缩容等操作。
- 4) 配置自动发现工具，定期扫描云环境，自动更新 CMDB 中的云资源信息，确保 CMDB 的准确性和完整性。

4. 其他集成:

除了上述提到的 ITSM、ITOM 和 CMDB 集成外，还有一些其他方面需要考虑进行集成。

- 1) 身份和访问管理 (IAM) 集成: 将企业原有的身份和访问管理系统与云平台的 IAM 服务进行集成，实现用户权限的统一管理和控制，确保安全合规性。
- 2) 日志和审计集成: 将云平台产生的日志数据与企业原有的日志管理和审计系统进行集成，提供全面的日志记录、分析和报告功能，以满足合规要求和安全需求。
- 3) 自动化工具集成: 将企业原有的自动化工具与云平台的自动化服务进行集成，实现对云资源的自动化部署、配置和管理，提高运维效率和灵活性。
- 4) 服务目录和自助服务集成: 将云平台提供的服务纳入到企业原有的服务目录中，并通过自助服务门户实现用户对云资源的自助申请、管理和报告。

- 5) 安全审计和合规集成：将云平台的安全审计和合规性工具与企业原有的安全审计和合规系统进行集成，实现对云环境的安全监控、漏洞扫描和合规性检查等。
- 6) 数据备份和恢复集成：将企业原有的数据备份和恢复系统与云平台的备份和恢复服务进行集成，确保云资源数据的可靠性和可恢复性。

集成方法：

- 1) 利用云平台提供的 API 或 SDK，与原有系统进行对接和数据交换。
- 2) 借助中间件或集成平台，实现不同系统之间的集成和数据传输。
- 3) 使用标准化的消息队列或事件总线，实现异步集成和实时数据传递。
- 4) 配置和定制适配器或连接器，使系统间的数据能够流畅地传递和转换。
- 5) 实施 ETL (Extract, Transform, Load) 过程，将数据从一个系统提取出来，经过转换后加载到另一个系统中。

集成的具体步骤如下：

- 1) 需求分析：明确集成的目标、范围和要求。了解原有系统和云平台的功能和特点，确定需要集成的模块和数据类型。
- 2) 系统对接：根据集成需求，调研并选择合适的集成方法和工具。根据云平台 and 原有系统的文档，配置相关连接和认证信息。
- 3) 数据映射与转换：分析云平台 and 原有系统之间的数据差异，设计数据映射规则和转换逻辑。确保数据在不同系统之间的格式和结构能够正确匹配和转换。
- 4) 接口开发：根据云平台 and 原有系统的 API 文档，开发需要集成的接口。这可能涉及编写代码、配置中间件或使用集成平台进行可视化拖拽式开发。
- 5) 测试与调试：编写集成测试用例，验证集成的正确性和稳定性。进行逐步调试，确保数据能够准确地在系统之间传递和同步。
- 6) 部署与监控：将集成完成的系统部署到生产环境，并设置监控和告警机制，以便及时发现和解决集成过程中可能出现的问题。
- 7) 维护与优化：持续监控集成的性能和稳定性。根据实际运行情况，优化集成方案，修复漏洞和改善性能。

总体来说，企业上云后，与云平台自带的工具和服务进行集成是一项复杂而又关键的任务。通过合理的规划和分析，选择合适的集成方法和工具，可以实现企业原有运维平台与云平台的无缝对接，提高运维效率、降低管理成本，并实现更好的资源利用和监控。

13 附录

13.1 缩略语列表

简写	全称	中文
CMF	Cloud Migration Framework	云迁移框架
SMS	Server Migration Service	主机迁移服务
DRS	Data Replication Service	数据复制服务
OMS	Object Storage Migration Service	对象存储迁移服务
CDM	Cloud Data Migration	云数据迁移
CCoE	Cloud Center of Excellence	云卓越中心
FinOps	Financial Operations	财务运营
ITSM	IT Service Management	IT 服务管理
ITOM	IT operations management	IT 运维管理
CMDB	Configuration Management Database	配置管理数据库
CMP	Cloud Managemen Platform	云管理平台
MFA	Multi-factor Authentication	多重身份验证
TCO	Total Cost of Ownership	总体拥有成本
CTO	Chief Technology Officer	首席技术官

简写	全称	中文
OBS	Object Storage Service	对象存储服务
SSO	Single Sign-on	单点登录
VPC	Virtual Private Cloud	虚拟私有云
WAF	Web Application Firewall	Web 应用防火墙
VPN	Virtual Private Network	虚拟专用网络
DC	Direct Connect	云专线
IDC	Integrated Data Center	集成数据中心
CC	Cloud Connect	云连接
ER	Enterprise Router	企业路由器
RMS	Resource Management Service	资源管理服务
EP	Enterprise Project	企业项目
LTS	Log Tank Service	云日志服务
DDM	Distributed Database Middleware	分布式数据库中间件
ELB	Elastic Load Balance	弹性负载均衡
CICD	Continuous Integration/Continuous Deployment	持续集成/持续交付
DCS	Distributed Cache Service	分布式缓存服务
IaC	Infrastructure as Code	基础设施即代码
TAM	Technical Account Manager	大客户技术服务经理
AOS	Application Orchestration Service	应用编排服务

简写	全称	中文
VSS	Vulnerability Scan Service	漏洞扫描服务
HSS	Host Security Service	主机安全服务
DBSS	Database Security Service	数据库安全服务
CSP	Cloud Service Provider	云服务提供商
MSP	Managed Service Provider	管理服务提供商

无担保声明：本资料内容仅供参考，华为云计算技术有限公司及或百联集团有限公司不对本资料所有内容提供任何明示或暗示的保证，包括但不限于适销性或者使用与某一特定目的的保证，在法律允许的范围内，华为云计算技术有限公司及或百联集团有限公司在任何情况下都不对使用本资料任何内容而产生的任何特殊的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉或预期节约的损失进行赔偿。（内部发行，免费赠阅）

版权声明：版权归华为云计算技术有限公司和百联集团有限公司共同所有，保留一切权利。