企业云管理与治理

许毅 / 埃森哲启云科技

极客时间App — 数字人才的专属学习空间

Geekbang.

极客时间

- 极客时间是**数字人才**的专属学习空间，有近**200+**体系课和**1400+**技术视频。为学员提供系统化、场景化、工具化和游戏化的学习服务
- 极客时间课程涵盖：前端/移动、计算机基础、后端/架构、AI/大数据、运维/测试等**十多门**技术学习版块
- 在极客时间可以学习各**大厂CTO**及阿里**P8**级以上技术大牛**独家技术修炼心法**，更有技术大牛直播，面对面帮你解决技术难题

更多精品好课

下载免费领取7天学习卡

17 条学习路径，补足能力短板

由浅到深，由易到难，从垂直深耕到触类旁通

后端工程师 20+ 门课程 43.4w 人已学习	架构师 20+ 门课程 41.5w 人已学习	前端工程师 15+ 门课程 25.6w 人已学习
运维工程师 15+ 门课程 21.6w 人已学习	计算机基础知识 10+ 门课程 21.5w 人已学习	Go 工程师 15+ 门课程 18.6w 人已学习
测试工程师 15+ 门课程 22.9w 人已学习	Java 工程师 20+ 门课程 31.2w 人已学习	Python 工程师 15+ 门课程 23.9w 人已学习

名师出高徒

1000+ 大牛独家心法，站在巨人的肩膀上不走弯路

李运华
前阿里资深技术专家（P9），《从 0 开始学架构》专栏作者

> 《从 0 开始学架构》我写了 3 年，很荣幸能成为 5.8 万程序员的架构入门选择，今年又重新梳理了一遍，把我认为旧的内容替换掉，新的思考写成加餐。之后会继续花时间完善内容和回复评论区疑问，每个观点都是我当下的认知，期待你和我同频。

云创新数字服务实现企业全栈上云、智能管云、极致用云

全栈上云、智能管云、极致用云

以业务应用为中心，帮助企业客户构建开发平台和云基础设施，形成完整的数字化转型支撑

- 尝试数字化建设
- 尝试组件化高效上云
- 部分板块可运营
- 零散客户支持

- **战略：**运用丰富行业经验与领先技术实践，提供LandingZone作为上云前指导，以业务与技术双轮驱动，为客户匹配云产品解决方案
- **交付：**将建云交付能力优化分装，使得云产品能以统一的接入方式无缝地接入，完成高效上云

- 改进数字化战略，帮助创新提升业绩
- 端到端多元化交付
- 具有高效数字化运营模型及平台型运维

- **运维：**建立统一的混合云管理平台，保证统一的云管理入口、统一的数据打通、统一的运维管理等
- 实现精准、高效、智能的混合云和多云的统一管理，实现高效运维，保障云业务持续稳定、可靠

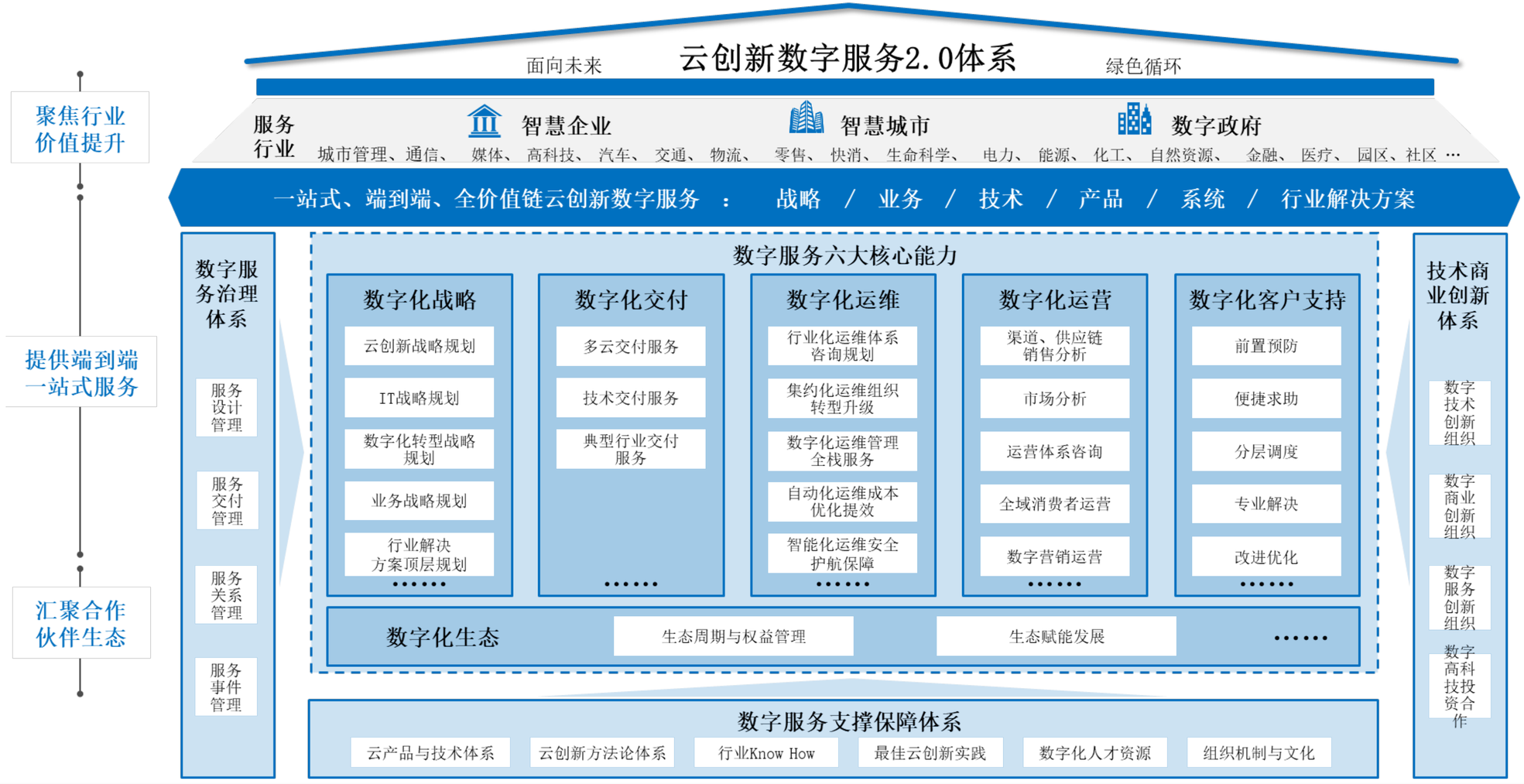
- 柔性服务
- 智能服务
- 绿色服务
- 全价值链服务

- **运营&客户支持：**借助积累的研发实践更便捷更高效地使用云，例如供应链运营、数字营销运营等
- 同时将客户支持能力进行有机的封装和集成，降低用户使用新技术的门槛，提升云研发能力
- 帮助客户快捷地和公共云进行实时的应用开发和数据同步

云创新数字服务依托于六大核心能力、三大支撑体系

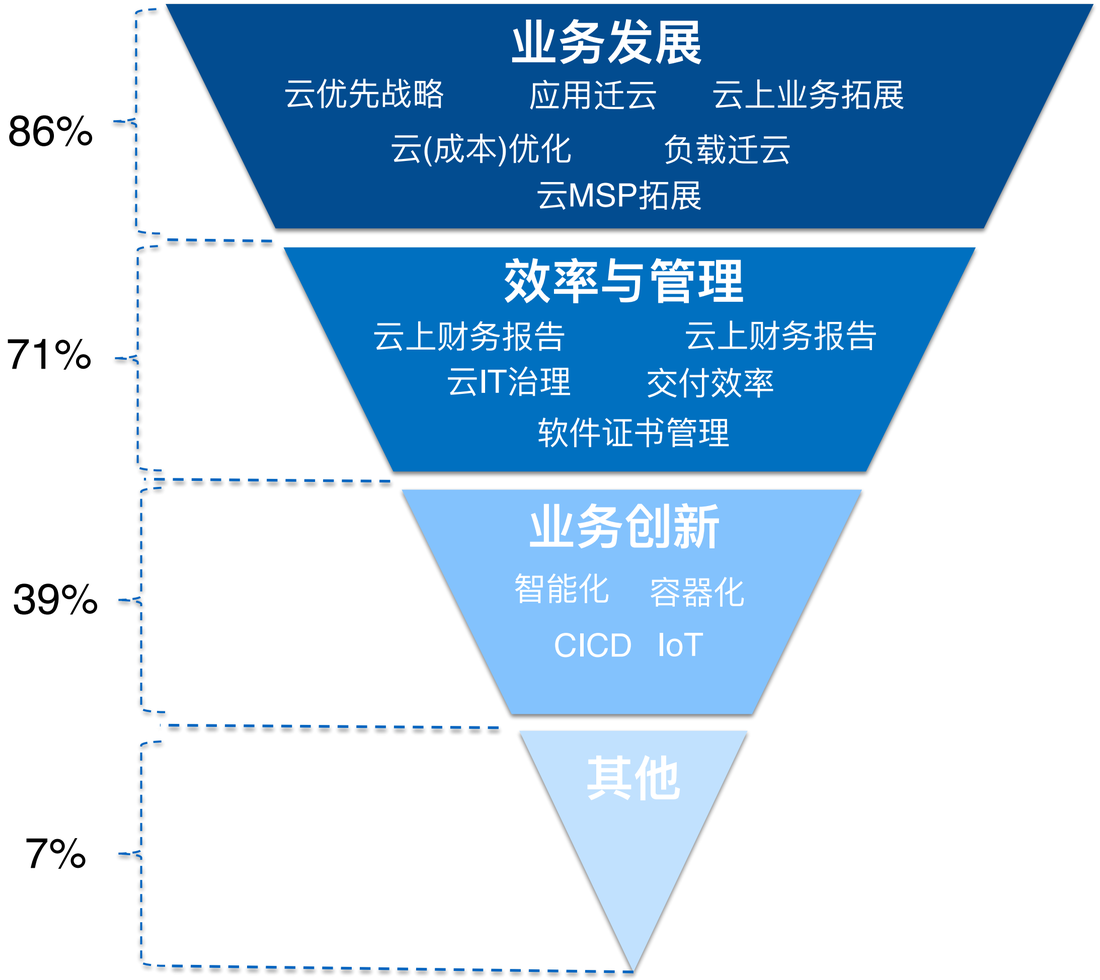
围绕各行业价值链构建端到端、跨领域、多场景的云上数字化转型服务，建立以服务支撑保障、服务治理及技术商业创新三大体系为支撑，

构建战略、交付、运维、运营、客户支持、生态六大核心能力，赋能各行业全量业务云化与全域数字化转型

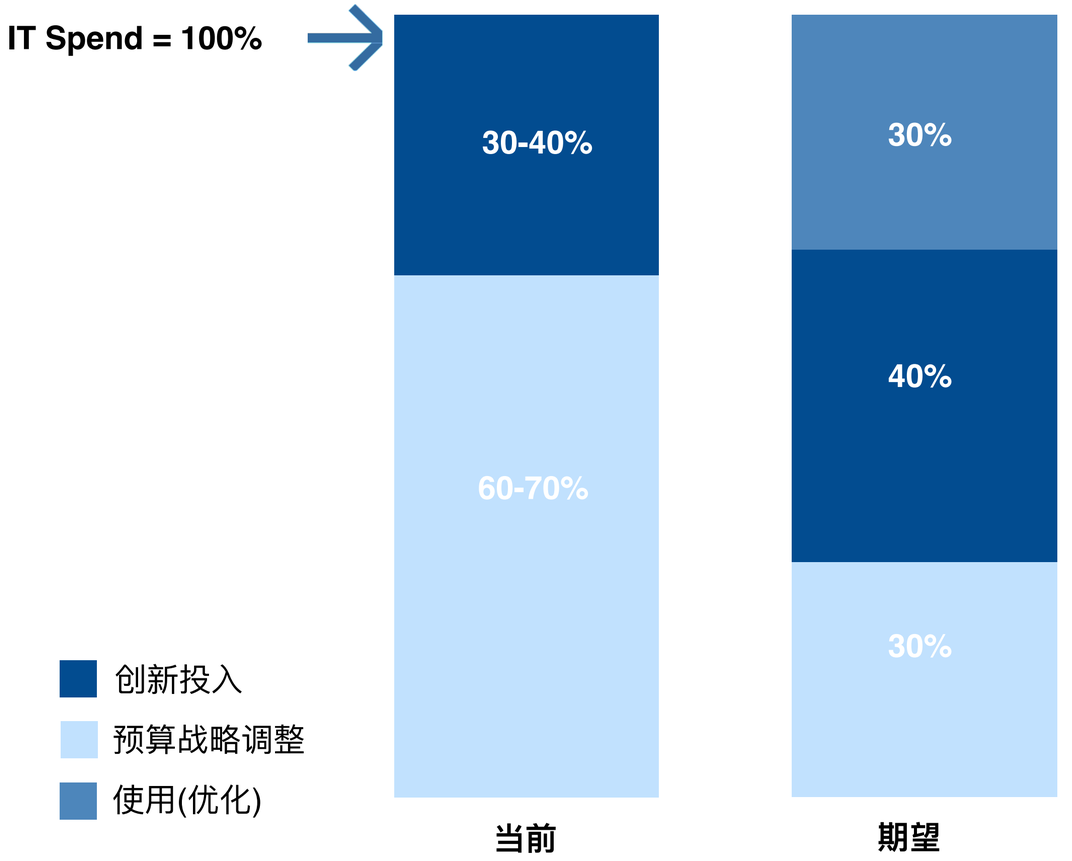


上云过程中问题发现

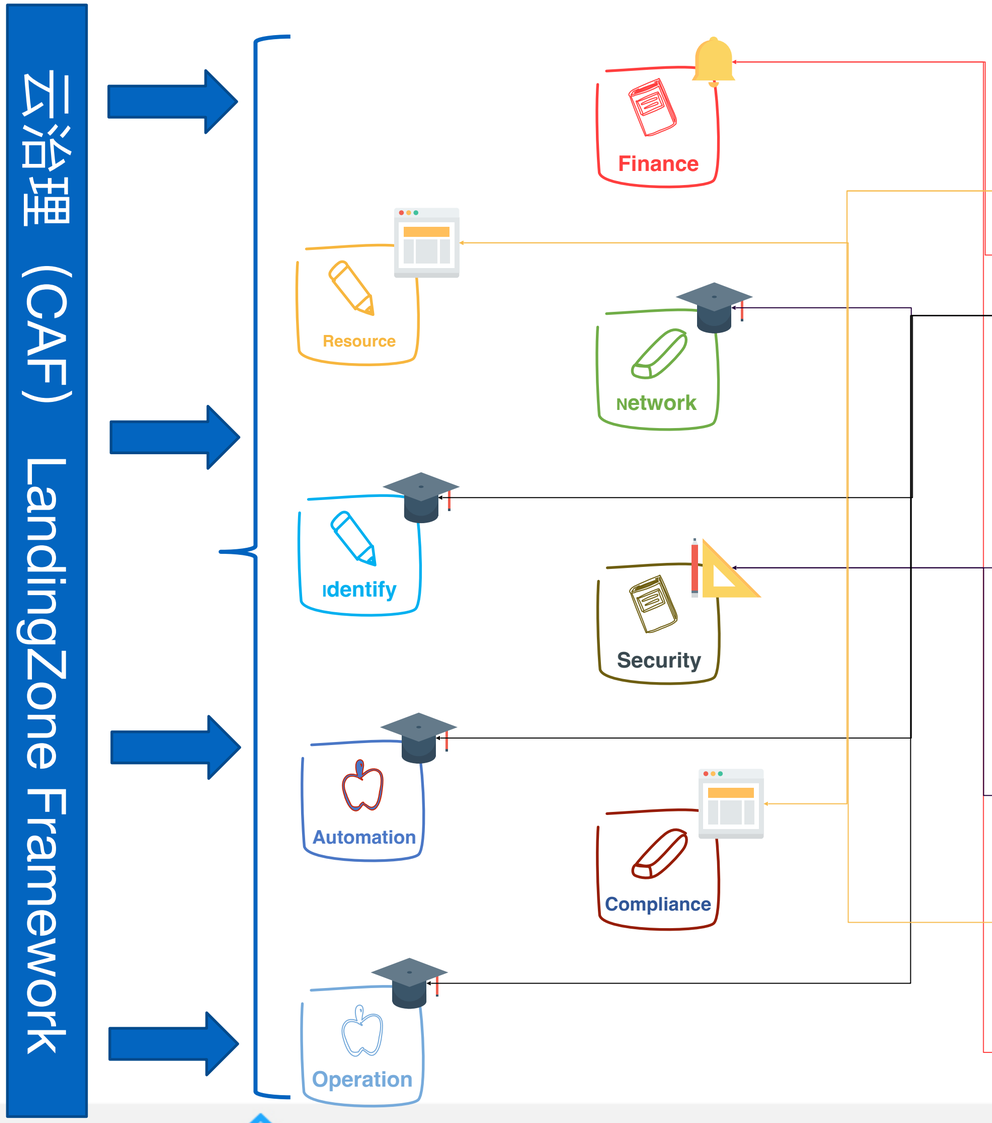
2022年企业上云动机分析



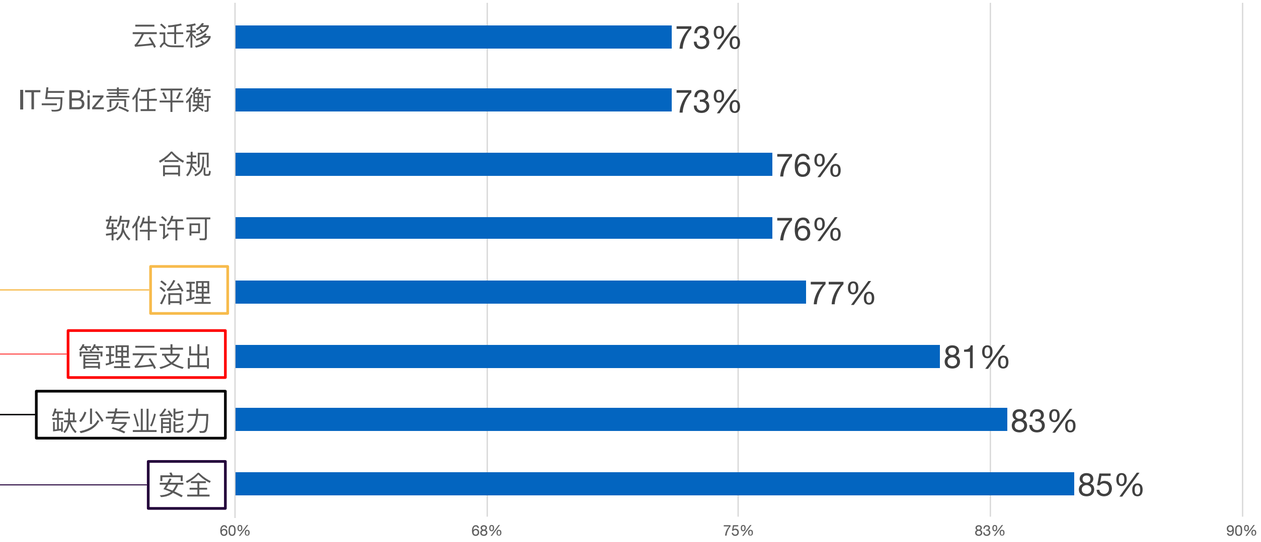
有效优化云上架构和规划云资源成为云战略首要问题



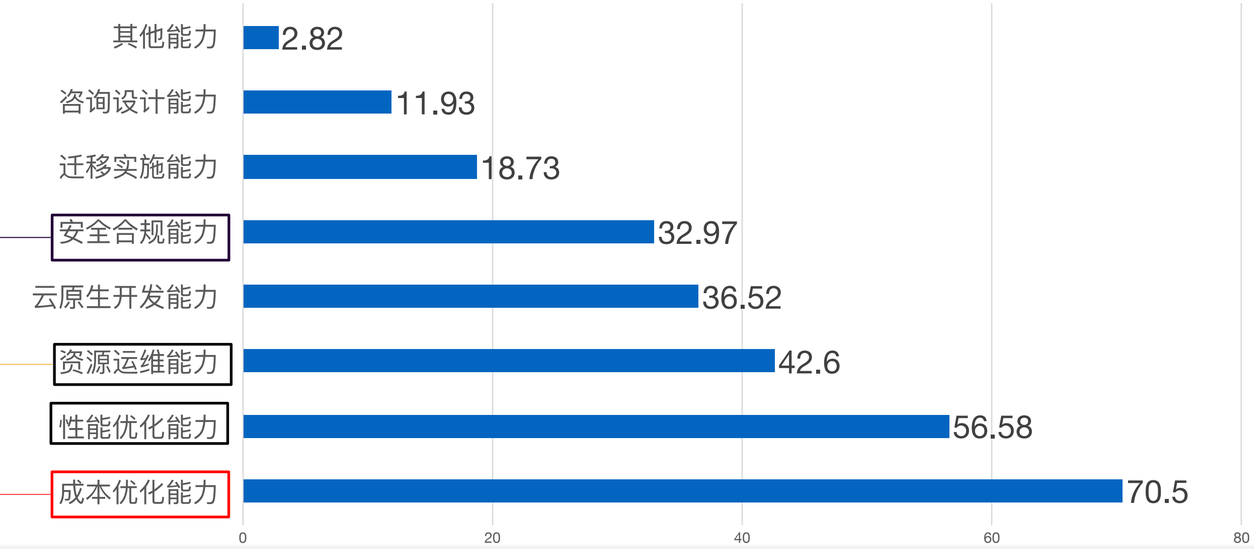
云发展趋势痛点映射分析



来源：Flexera，2022年（单位:%）



来源：中国信息通信研究院，云计算白皮书，2021年6月（单位:%）



云服务市场供给侧与需求侧彼此成就、携手共进

全价值链专业服务

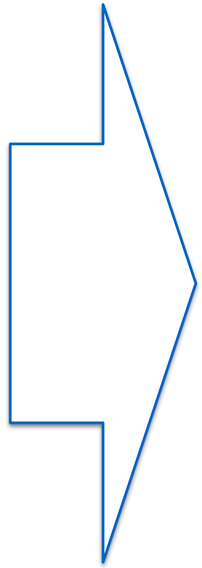
- 业务经营相关的数字化战略咨询、业务云化、业务重构、云运营及可持续经营等全价值链服务
- 关注内部业务数据传递或交互，配套相应的数字化运维管理体系来支撑日常作业及管理工作的“云化”

现代化云服务

- 现代化云采用**LandingZone**框架，为用户全方面实现架构稳定性、健壮性、安全性等基础设施
- 原生业务架构改造/新建，为全面数字化业务夯实业务提供原生化业务底座
- 高效响应、事件高效处理、预判问题并快速定位解决， 最终达到整体大幅提升运维和治理能力。

传统云服务

- 系统或应用的稳定性
- 对底层云资源进行精细化运营
- 降低总IT成本



- 提升业务连续性
- 赋能创新发展
- 实现持续商业价值
- 提升行业竞争力

埃森哲基于Landing Zone的咨询及交付模型

咨询

1、对IT系统现状进行评估

- ❑ 访谈/会议纪要
- ❑ Landing Zone需求跟踪矩阵

2、阿里云Landing Zone企业方案设计

- ❑ Landing Zone高阶解决方案设计
- ❑ Landing Zone网络连接方案设计
- ❑ Landing Zone实施路线图和发布计划

3、 交付成果评审及客户汇报

- ❑ 最终发布报告

交付

1、 构建并验证Landing Zone云环境

- ❑ Landing Zone基础设施环境
- ❑ Landing Zone网络连接实现
- ❑ 基础架构即代码（IaC）工具、模板和部署

2、客户验收，知识转移与交接

- ❑ 操作手册和运维手册等文档
- ❑ 支持团队的交接计划

下面，有请阿里云Landing Zone技术总监程超，为大家详细展开

THANKS

Landing Zone

阿里云 / 程超

目录

01、企业上云的问题和挑战

02、阿里云Landing Zone介绍

03、Landing Zone框架最佳实践

WHY → HOW

企业上云面临的问题

基础架构

- 业务账号没有隔离
- 网络地址没有规划
- 安全策略不清晰

财务

- 成本分不清楚
- 资源闲置没发现
- 预算管理困难

身份权限

- 离职员工权限回收难
- AK泄漏到GitHub
- 权限粒度过大无法收敛

合规

- 法律法规带来的挑战
- 内部合规部门挑战
- 人肉审计费时费力

什么是Landing Zone?

一个帮助企业快速搭建安全、合规、可扩展的云环境的框架

阿里云企业上云框架Landing Zone

8大版块

资源规划
- 账号架构
- 资源标识
- 账号基线
- 账号打标

财务管理
- 统一付款
- 费用预警
- 成本分摊
- 成本优化

身份权限
- 身份管理
- 授权管理
- 访问安全
- AK管理

合规审计
- 事前预防
- 事中发现
- 事后审计

安全防护
- 主机安全
- 网络安全
- 应用安全
- 数据安全

网络规划
- 云上组网
- 网络互联
- 公网出入
- 混合云/多云架构

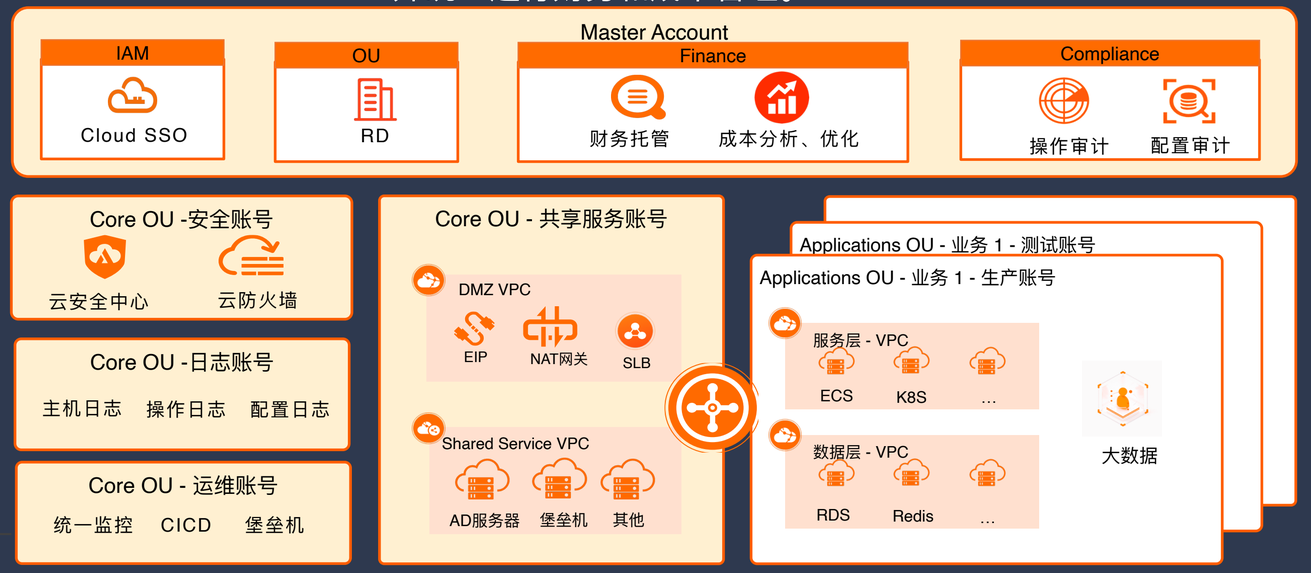
运维管理
- 配置管理
- 监控管理
- 日志管理
- 服务目录

自动化
- 部署自动化
- 管理自动化
- 治理自动化

构建安全、合规、可扩展的云基础环境

1 统一多账号管理和财务管理

基于组织的多账号管理，实现业务的隔离；
并统一进行财务和成本管理。



2 简化身份管理

通过打通企业IdP与阿里云的单点登录，统一和简化员工身份、权限管理，规避访问风险。

3 企业级网络架构

统一规划云上网络，线上线下互连，实现公网出口管控、网络隔离和网络安全。

4 全面安全防护

体系化的安全防护方案，涵盖访问安全、网络安全、主机安全和数据安全，确保安全可控。

5 内置合规管理

通过事先、事中和事后的审计，满足企业对于在地法规和内审需求。

6 可扩展的框架

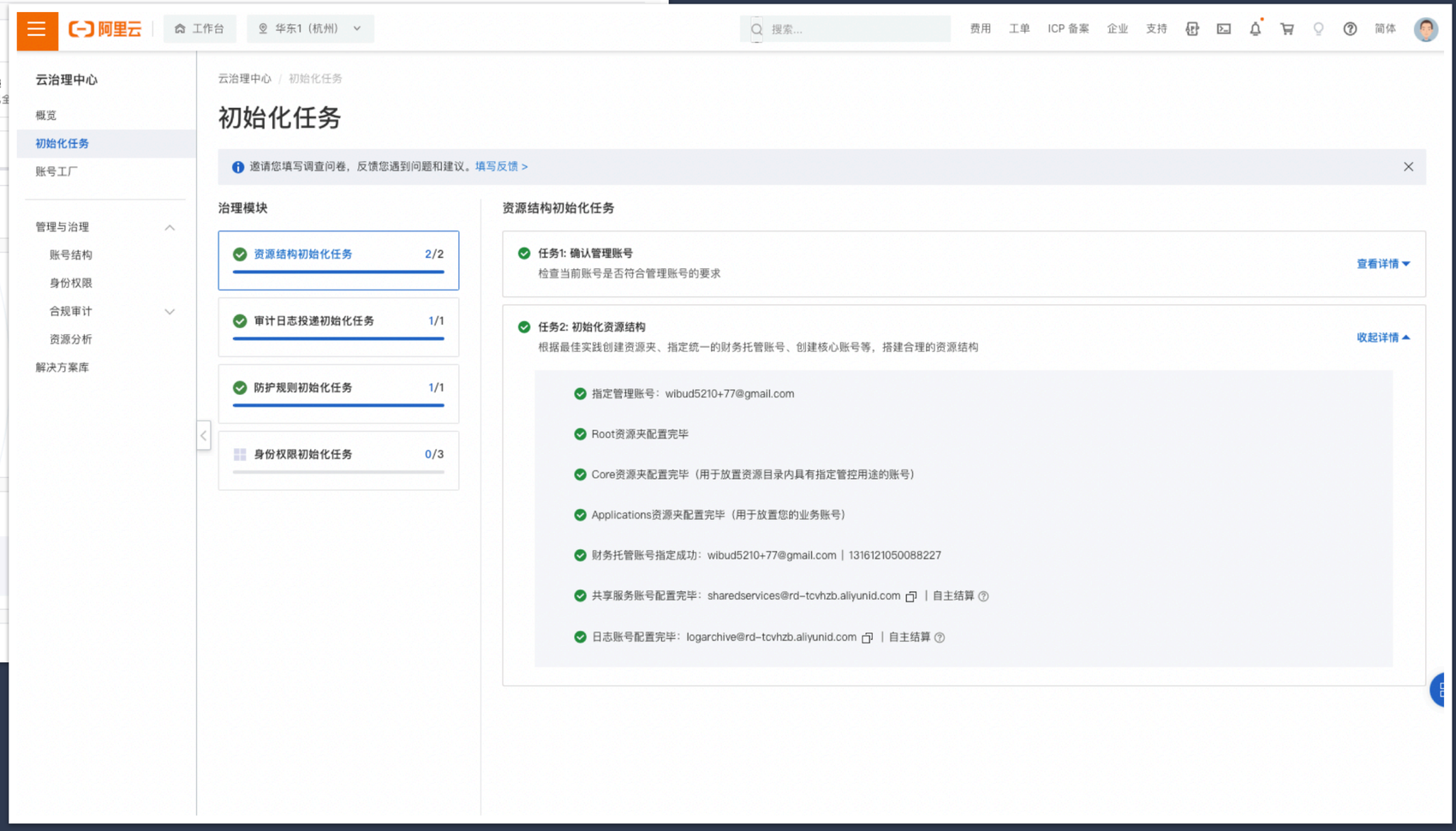
在整体管控体系之下，满足企业业务发展需求，扩展云上环境。

7 快速搭建

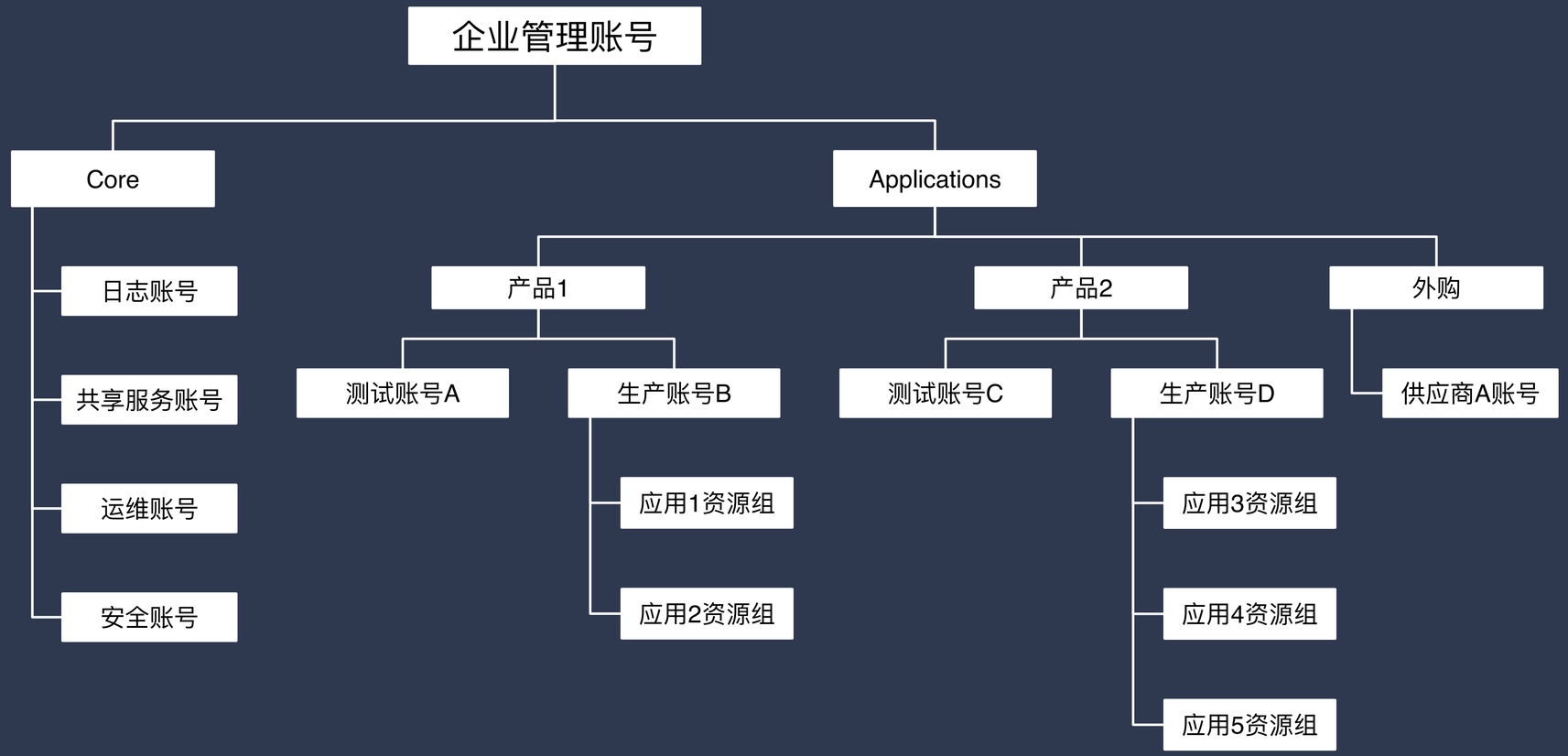
借助云治理中心 & Terraform 可以快速搭建符合规范的可扩展的基础环境。

Alibaba Cloud | LANDING ZONE

云治理中心



基于组织的多账号架构



业务隔离

- 支持不同BU或团队间的隔离
- 不同用途的环境隔离：生产环境、测试环境和研发环境

集团管控

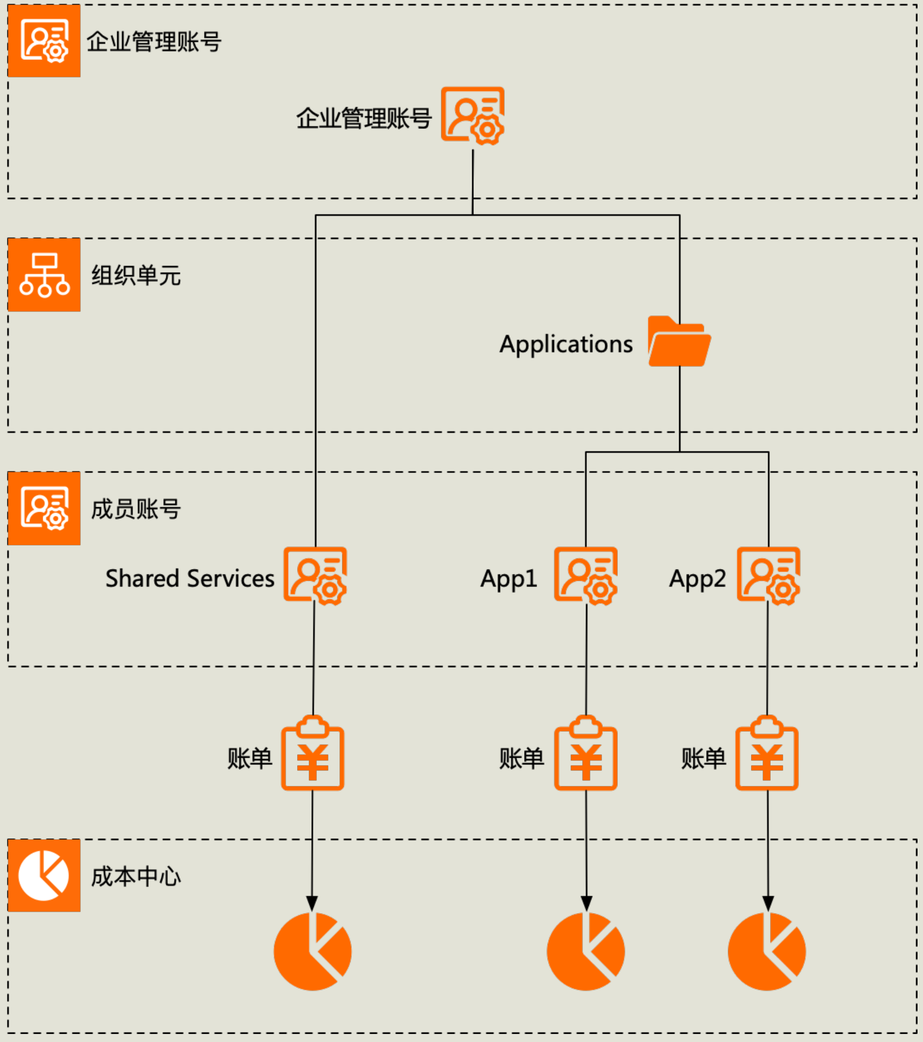
- 企业管理账号统一管控
- IT团队负责统一的安全、合规审计和运维管理

扩展性强

- 可以按租户的级别进行横向扩展
- 支持组织调整或者外部收购业务的统一纳管

多账号企业云上分账方案

财务管理



客户痛点

- ✓ 企业无法讲清楚IT成本构成，无法进行成本优化。
- ✓ 各种业务资源混在一块，成本无法分摊到各个业务。
- ✓ 人肉分账，分不清楚的账完全靠拍脑袋，无法将成本与业务关联起来。

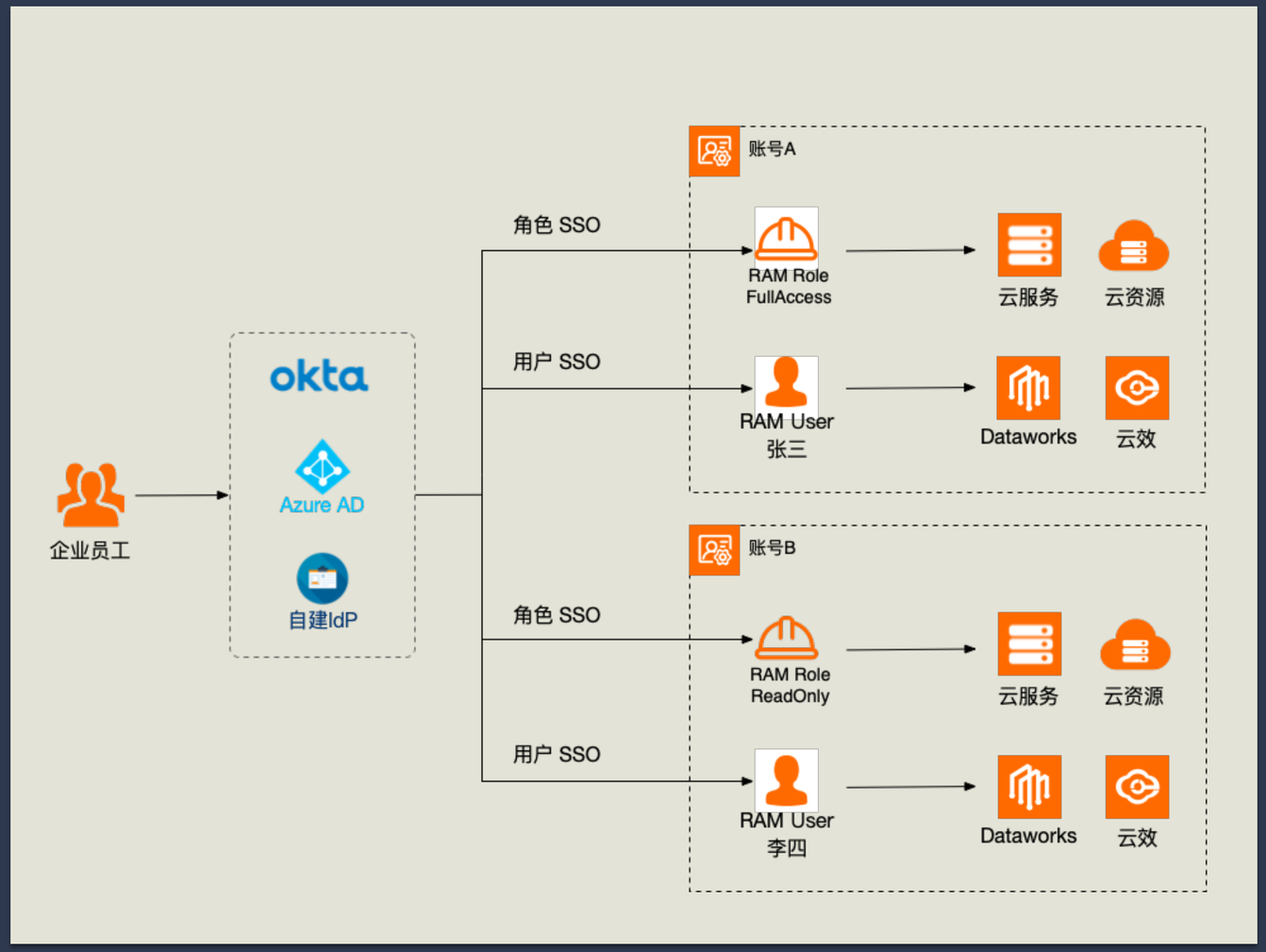
解决方案

- ✓ 多账号多级财务分账：站在企业管理视角，在不同的组织单元维度，来归集各成员账号产生的账单费用。
- ✓ 单账号多级财务分账：通过在单个账号内，对资源进行多维度打标，或创建多级财务单元来实现。
- ✓ 单账号一级财务分账：通过在单个账号里，对资源打标或财务单元来实现。

客户价值

- ✓ 解决CIO/CTO最关心的云上IT治理，IT成本核算等问题。
- ✓ 解决财务分账问题，清楚企业内部各部门成本及云上IT成本结构。
- ✓ 解决资源管理，财务分账问题，让CIO/CTO准确地掌握云上资源成本情况，清楚业务与成本的关系。
- ✓ 解决资源打标，财务分账问题，让客户采购/运维轻松搞定每月的IT成本汇报。

企业IdP集成阿里云SSO



客户痛点

- ✓ 使用RAM用户登录阿里云，用户转岗、离职时员工未及时清理，带来数据安全风险
- ✓ 大量的新用户管理工作，需要维护多份员工数据
- ✓ 员工也需要保存多份账号密码，容易导致账号泄漏风险

解决方案

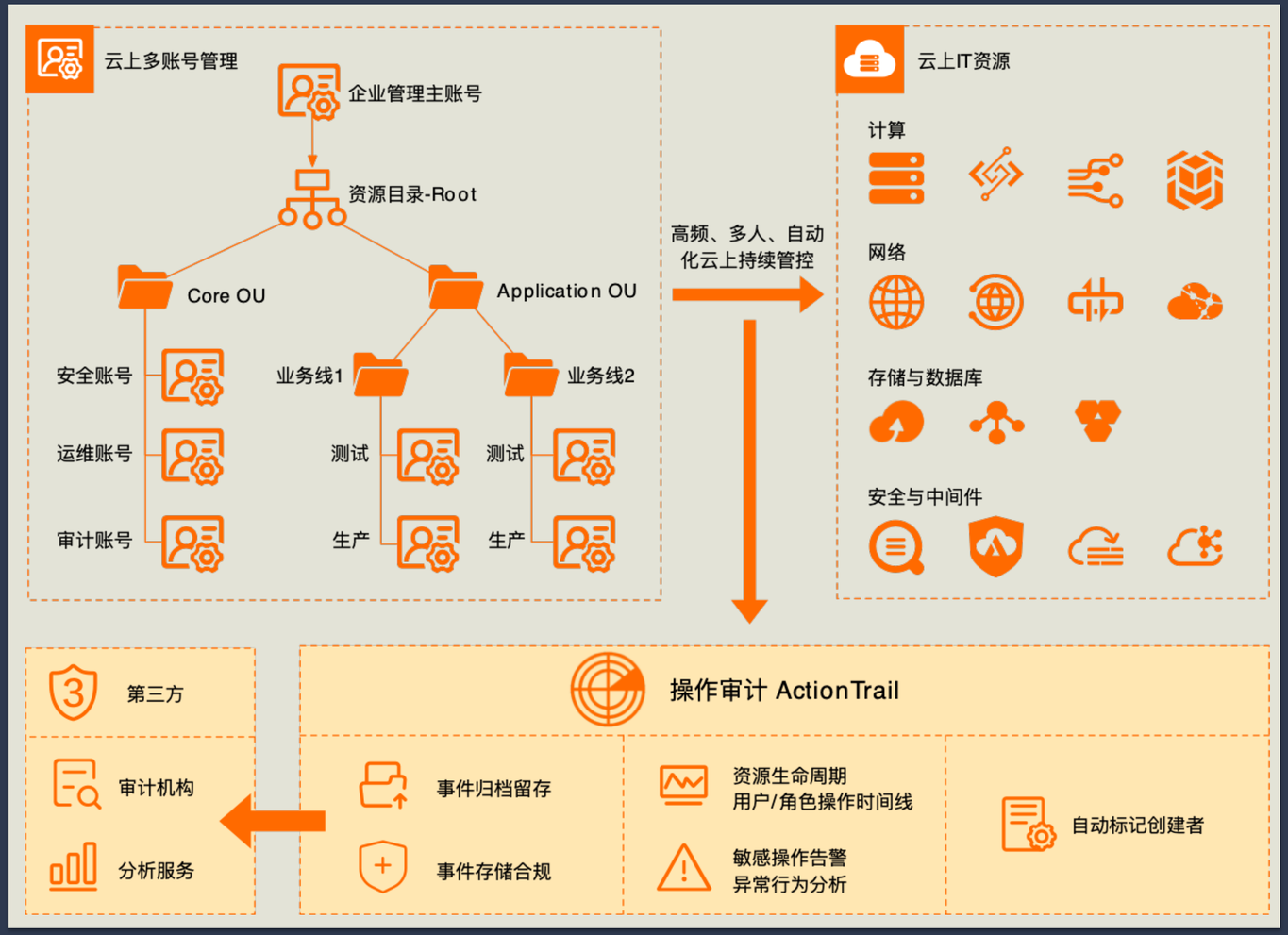
- ✓ 基于客户现状，使用角色SSO或者用户SSO的方式，跟阿里云集成SSO
- ✓ 统一在IDP侧维护员工身份和权限

客户价值

- ✓ 使用企业账号登录阿里云，在用户转岗、离职时可以做到有效阻断，避免发生数据安全风险
- ✓ 减少新用户管理工作量，提高管理效率
- ✓ 员工只需要维护企业IDP一份账号密码即可完成云控制台的登录

多账号操作日志统一归集与审计

合规审计



客户痛点

- ✓ 根据中国网安法和等保2.0要求，企业必须留存180天及以上的IT系统运维访问日志
- ✓ 企业日常故障排查、自动运维、运维监控及安全洞察都必须依赖完整可靠的审计日志

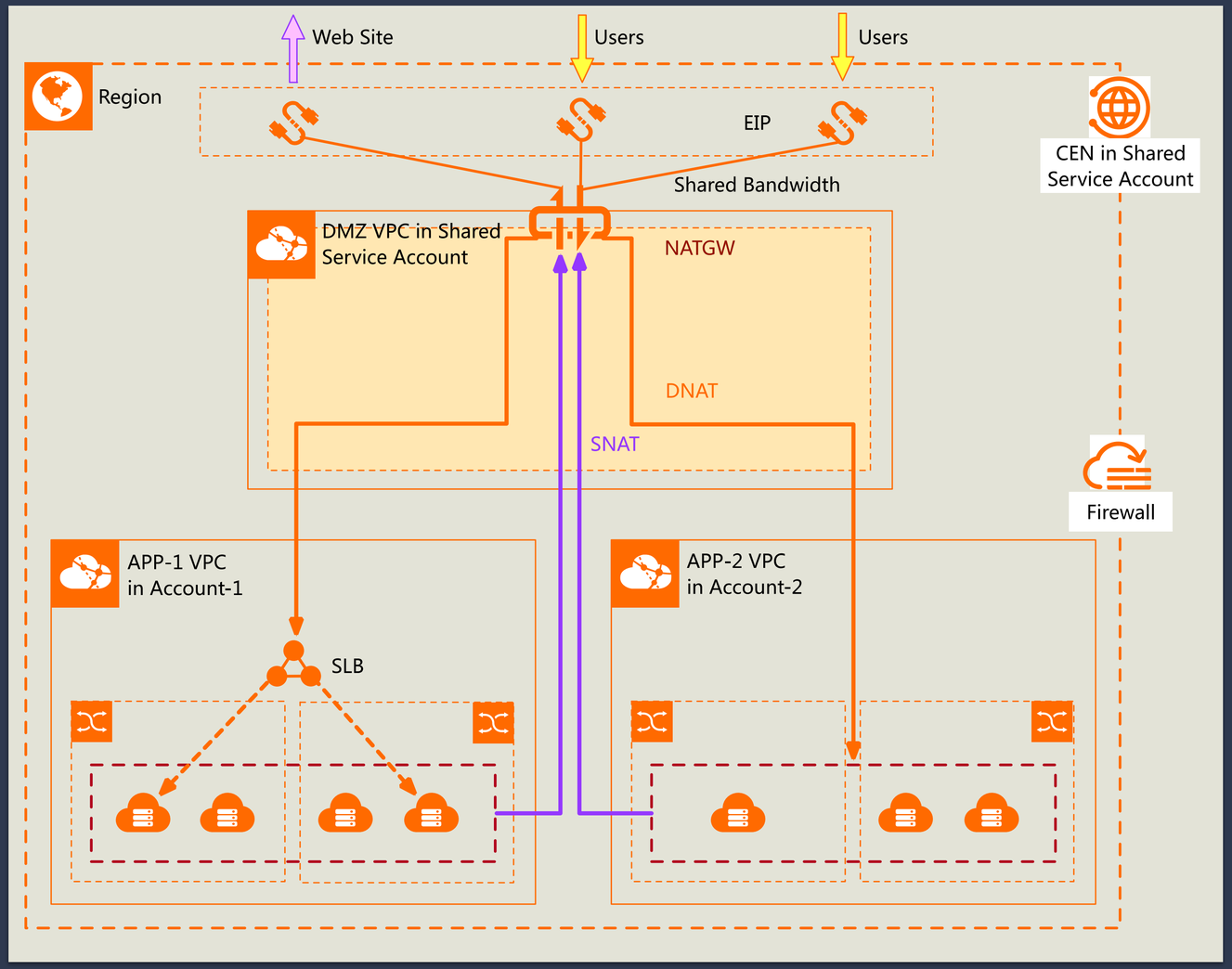
解决方案

- ✓ 企业管理主账号创建审计跟踪和历史事件投递任务，将日志全量归集到审计账号并设置长期留存，未来可支持外审及分析
- ✓ 企业管理主账号通过管控策略限制跟踪不能被停止和删除，限制审计账号不能被移出资源目录，限制日志存储空间不能被删除
- ✓ 基于审计日志实现日常分析，持续监控告警和专项安全分析

客户价值

- ✓ 基于资源目录和操作审计，实现多账号中心化归集并留存审计日志，应对企业外部审计及内部监管要求
- ✓ 基于管控策略，确保审计数据的收集和存储始终运转正常
- ✓ 基于操作事件及时洞察可能存在的高危操作、非法操作意图等潜在风险，并支持日常故障排查

企业级公网统一出口



客户痛点

- ✓ 传统企业：上云之后因基础架构需求，云上DMZ VPC和云下互联网出口实现设计对标，需要统一公网出口
- ✓ 集团型企业：集团IT部门为统一监管、统一安全审计，需要构建统一公网出口，为集团各子公司及部门提供公网访问服务

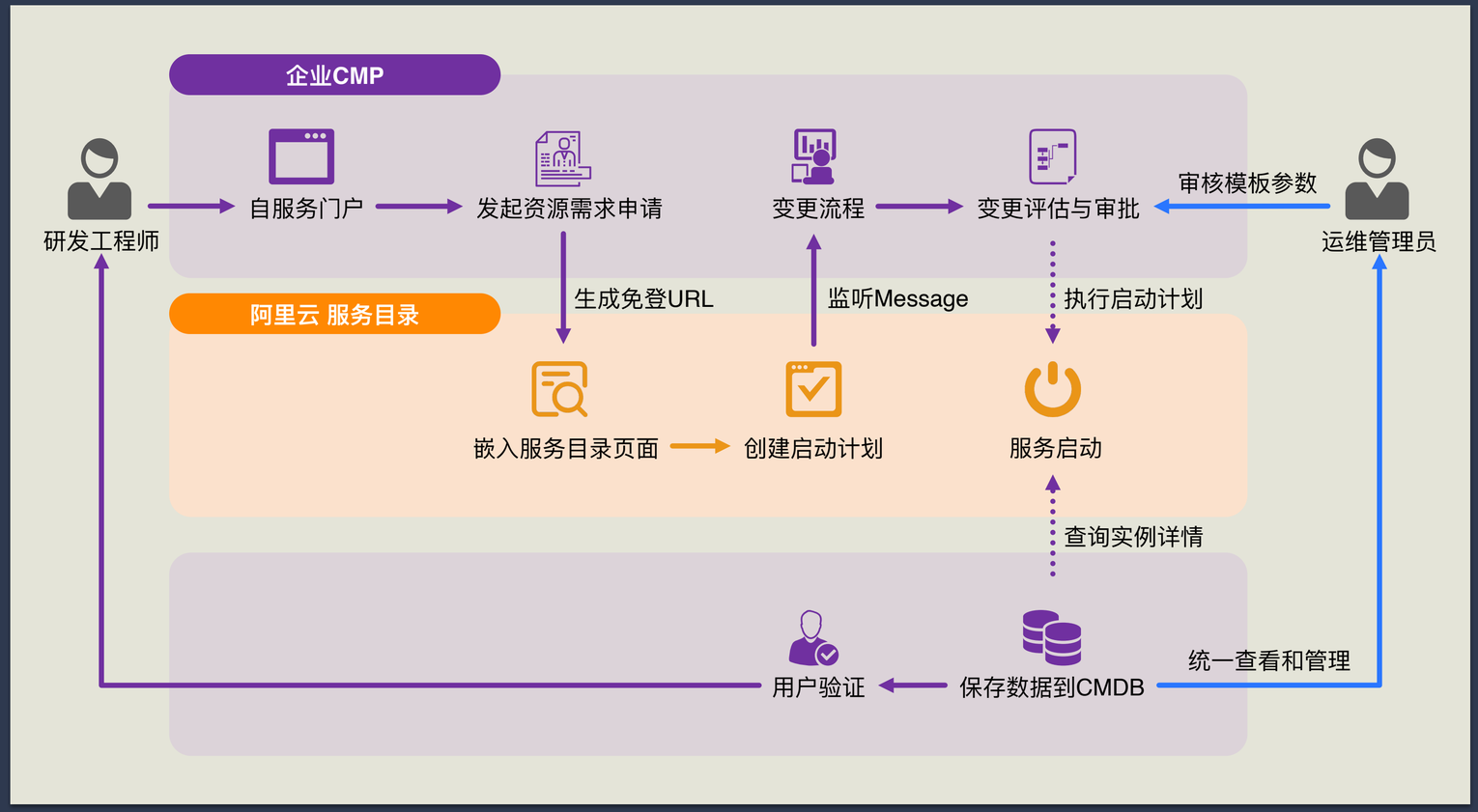
解决方案

- ✓ DMZ VPC设计：企业的WAN能力放到共享服务账号的DMZ VPC，此VPC可以部署NATGW、Proxy、自建FW等公网产品
- ✓ 安全设计：可联动DDoS防护、WAF、云FW等安全产品，保障公网出口安全
- ✓ 权限划分：公网出口能力统一收口到IT部门，部署DNAT+SNAT，业务VPC通过CEN实现跨VPC出公网
- ✓ 监控管理：使用NATGW+流日志组合能力，监控公网出入口流量信息

客户价值

- ✓ 统一管理，由IT部门统一管控公网权限，各业务需要向IT申请权限
- ✓ 安全性高，统一DMZ VPC设计，保障公网出口安全
- ✓ 统一监控，监控出公网访问情况，及时排查异常流量及原因

CMP平台快速创建云资源



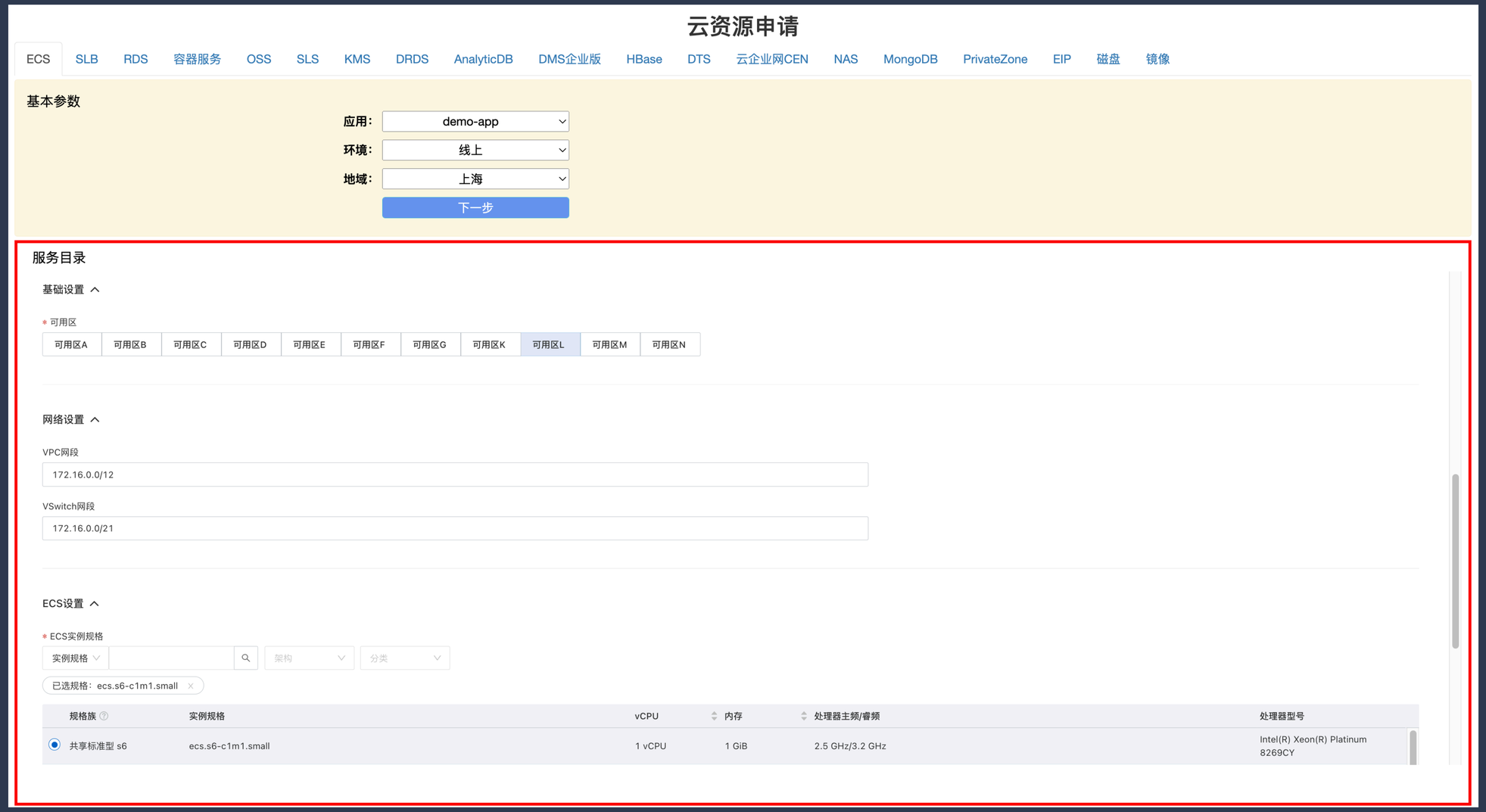
客户收益

- ✓ 企业可以通过Terraform模板定义标准的资源创建流程，同时可以选择开放部分模板参数，允许用户在使用时填写
- ✓ 企业CMP可以复用服务目录的前端界面，通过表单的形式填写模板参数
- ✓ 服务目录可以跟企业内部工作流进行对接，满足企业合规要求

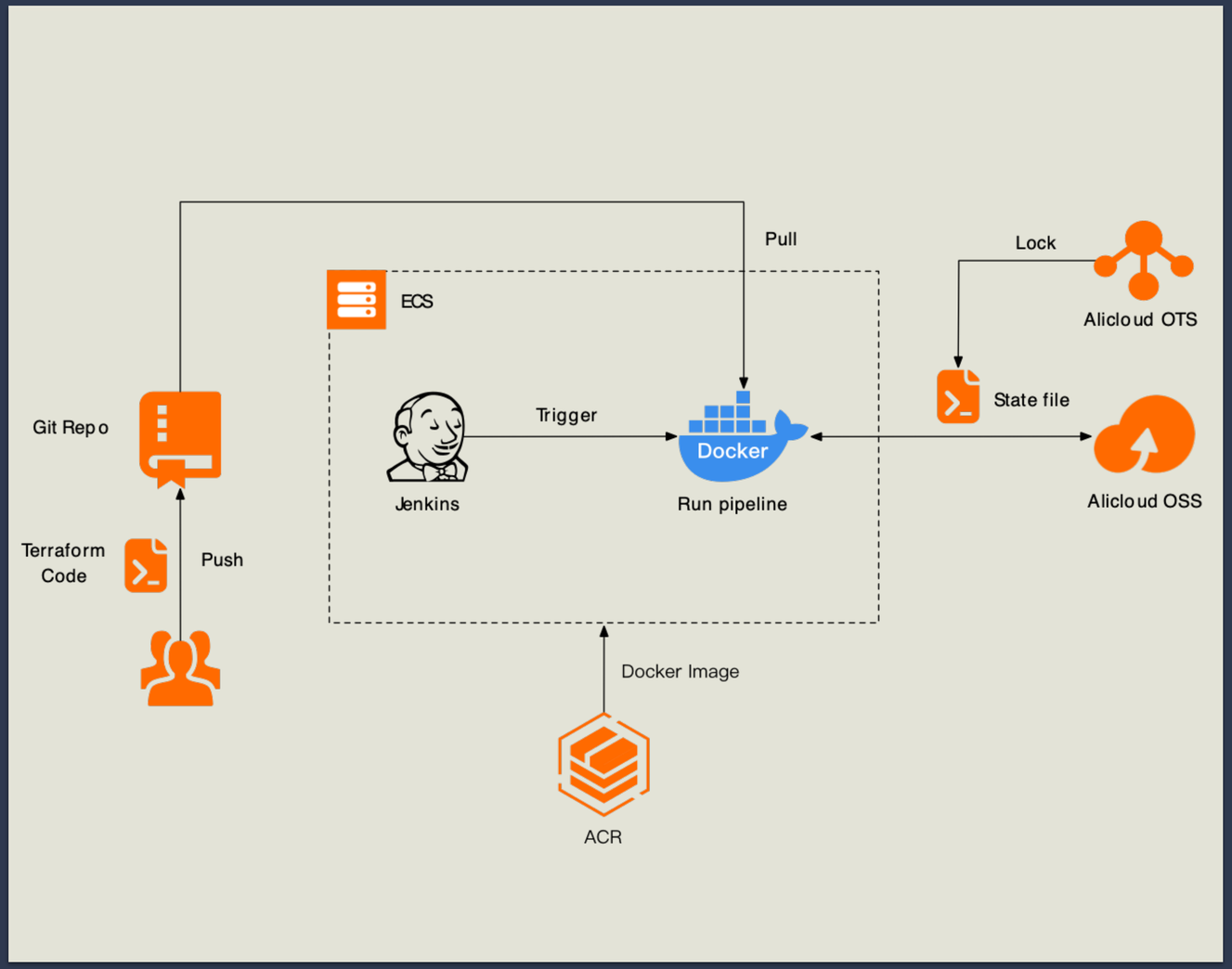
方案建议

- ✓ 通过角色SSO对接阿里云，以生成免登URL，嵌入服务目录页面
- ✓ 服务目录创建启动计划后，企业CMP可以监听服务目录发送给父页面的Message，打通企业内部工作流
- ✓ 审批完成后，调用服务目录的API执行启动计划、查询实例详情

CMP集成服务目录


云资源申请
ECS
SLB
RDS
容器服务
OSS
SLS
KMS
DRDS
AnalyticDB
DMS企业版
HBase
DTS
云企业网CEN
NAS
MongoDB
PrivateZone
EIP
磁盘
镜像
基本参数
应用：
demo-app
环境：
线上
地域：
上海
下一步
服务目录
基础设置
* 可用区
可用区A
可用区B
可用区C
可用区D
可用区E
可用区F
可用区G
可用区K
可用区L
可用区M
可用区N
网络设置
VPC网段
172.16.0.0/12
VSwitch网段
172.16.0.0/21
ECS设置
* ECS实例规格
实例规格
架构
分类
已选规格：ecs.s6-c1m1.small
规格族
实例规格
vCPU
内存
处理器主频/睿频
处理器型号
共享标准型 s6
ecs.s6-c1m1.small
1 vCPU
1 GiB
2.5 GHz/3.2 GHz
Intel(R) Xeon(R) Platinum 8269CY

基于Jenkins实现账号工厂



客户痛点

- ✓ 上云阶段构建多账号体系，多成员账号权限配置繁琐、效率低下，无法保证账号权限、资源配置等基线统一，后续修改维护困难
- ✓ 业务扩张需开设新账号，无法快速创建拥有统一身份权限、资源配置基线的成员账号

解决方案

- ✓ 使用Jenkins + Docker + Terraform 构建账号工厂
- ✓ 使用Jenkins编排账号基线Pipeline，部署至ECS
- ✓ Pipeline步骤使用Docker执行Terraform代码创建云资源，使用OSS + OTS作为Remote Backend
- ✓ 使用ACR作为镜像仓库

客户价值

- ✓ 提供成员账号中用户角色的创建和权限策略绑定的统一规范，保障权限安全
- ✓ 基础设施代码化，减轻管理运维负担，代码可拓展、提供更多基线配置
- ✓ Jenkins提供API可以跟企业内部的DevOps平台高效集成

Alibaba Cloud | LANDING ZONE

LandingZone解决方案大图

	资源规划	身份权限	网络规划	财务管理	合规审计	安全防护	运维管理	自动化
Foundation	多账号架构 Master I Log I Security Share I BizMA	多账号统一身份管理 CloudSSO	多VPC设计及互联	多账号付款管理	中心化的审计日志归集			
	资源管理方案							
Advanced	云资源同步到企业CMDB	企业IdP集成SSO (OktalAzureADIADFS)	DMZ统一网络出口	分账设计	基于配置的多账号合规检查	网络安全- DDoS/防火墙	企业级统一日志	基础设施自动化流水线
	级联资源自动同步标签	自建IDP实现多账号SSO	私网互联方案	代金券额度池管理	企业多账号全局访问边界控制	身份安全-主机身份堡垒机	统一监控管理	基于AzureDevops实现账号工厂
	强制标签 Tag Policy	应用程序使用AK最佳实践	Shared VPC	成本优化	Golden Image	主机安全- SOC	企业云监控方案	基于Jenkins实现账号工厂
	账号标签 RD	多账号单点登录TVM/ CAM方案	混合云互联	预算管理	基于操作日志的业务资源事件分析	数据安全 加密 I 备份	统一事件管理	基于云效实现账号工厂
			多云互联		云上IT基础设施的合规管理方法	应用安全 WAF	服务目录	基于Argo实现账号工厂
								基于gitlab实现账号工厂

云上治理成熟度模型

- **身份权限**
  - ✓ 身份生命周期管理
  - ✓ 身份认证
  - ✓ 权限授予
  - ✓ 身份权限审计
  - ✓ 身份集成
- **资源管理及分类**
  - ✓ 资源分类
  - ✓ 资源配额
- **监控及审计分析**
  - ✓ 日志收集
  - ✓ 洞察分析
  - ✓ 告警响应
  - ✓ 事件处理
- **成本管理及优化**
  - ✓ 成本报告
  - ✓ 成本优化
- **管理自动化**
  - ✓ 基础设施自动化
  - ✓ 管理治理自动化

极客时间 | 企业版 × InfoQ

DTDS
全球数字人才发展线上峰会

建设面向未来数字化全局的人才梯队

2022 年 8 月 9 日 · 线上

入局·链接

扫码预约直播

Thanks