阿里云 | 奥运会全球指定云服务商

自上而下：可见可控的云上审计合规

2021年9月沙龙

阿里云企业IT治理 产品专家 予与

某多账号部署的外企公司在云上IT管理中潜藏的风险

- 70%的主账号未启用持续的审计日志收集 不满足等保
- 32%的主账号存在多个超级权限持有者 超大权限
- 30%的主账号使用弱密码策略 账号被盗
- 13%的ECS磁盘未启用加密 数据泄露
- 22%的ECS 计算实例未开启释放保护 业务中断
- 5%的ECS计算实例在预期之外绑定了公网IP 公网攻击
- 11%的安全组对全网段公开风险端口 公网攻击
- 7%的OSS Bucket未开启服务端加密 数据泄露
- 42%的OSS Bucket未设置限定HTTPS访问 数据泄露
- 存在大量未被挂载的磁盘 成本浪费
- …

审计合规来源于企业的IT管理风控

国家法律法规

- 2017年6月1日正式实施《中华人民共和国网络安全法》
- 2019年12月1日正式实施《信息安全技术网络安全等级保护基本要求》
- 2021年9月1日正式实施《中华人民共和国数据安全法》

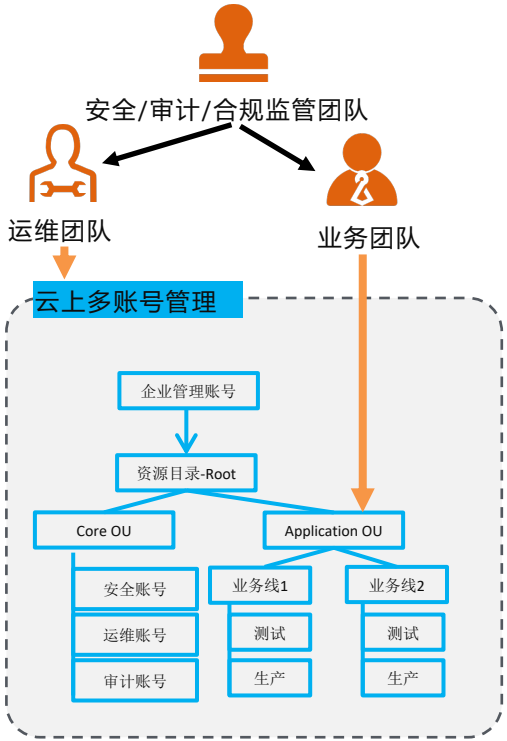
行业通用标准

- ISO 27001，国际公认的信息安全管理体系标准
- PCI-DSS，支付卡业务数据安全认证
- CIS Benchmark，公认可实施的网络安全标准

企业自定义内控基线

- 账号权限安全管理
- 网络安全防护基线
- 数据防泄漏防篡改防护基线
- 主机安全防护基线
- 全面监控基线

企业云上IT管理面对风险升级



组织管理风险

监管者风险

中心监管团队缺少抓手，丧失监管职能

实施者风险

运维团队日常工作风险高，伴有故障风险

业务风险

数据泄露风险

核心业务数据泄露，面对巨额罚款、赔款甚至法律责任。

业务中断风险

服务挂机致使业务长时间中断，面对巨大经济损失。

成本溢出风险

云上IT消费更灵活、更复杂，造成预算失控、资源空置等，挤压营收空间。

合规资质风险

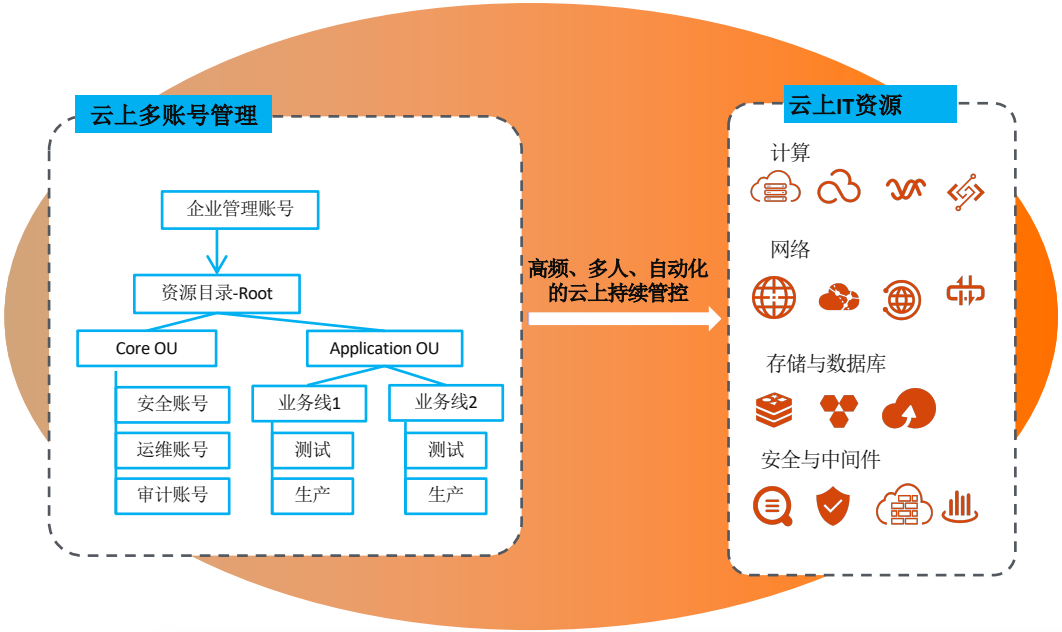
IT合规得不到合规资质认证，影响企业开展商务活动甚至影响经营资质。

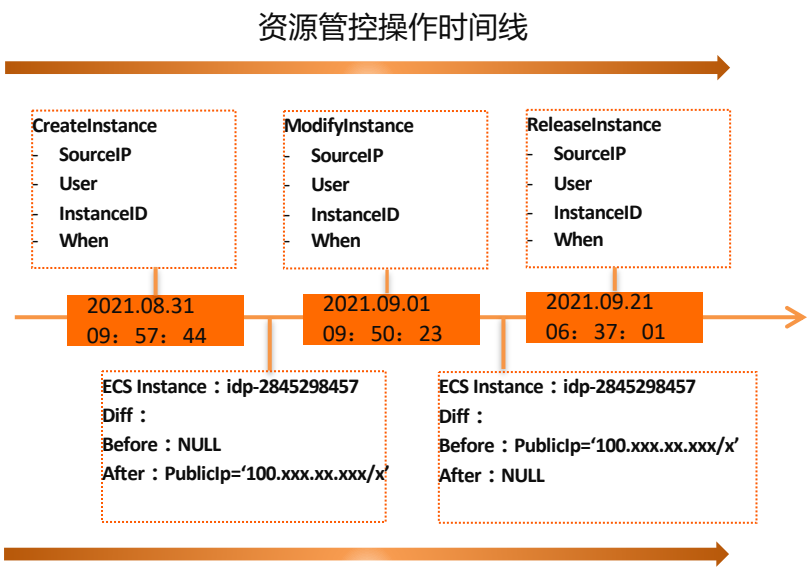
云上审计合规框架—安全可控的IT管理环境

审计合规**制度和手段**的变革

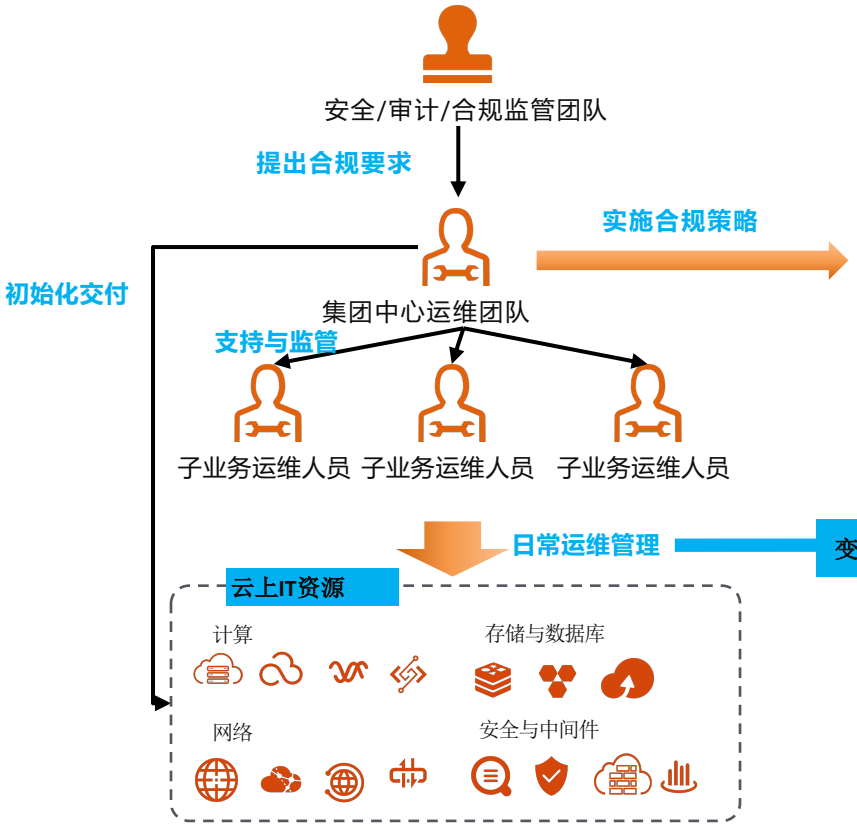
可见—可见的才是可控的

阿里云 | 企业IT治理





可控—组织上和技术上的可控



数据安全基线

- ✓开启静止存储加密
- ✓开启传输HTTPS加密
- ✓开启数据访问审计
- ✓细粒度的数据访问权限控制

业务连续性基线

- ✓业务关键性分级
- ✓公网隔离，开启网络安全防护
- ✓开启核心资源的释放保护
- ✓启用快照、备份、恢复策略

成本控制基线

- ✓限制采购的区域、规格
- ✓限制采购权限开放
- ✓闲置资源释放回收
- ✓禁止异常采购行为

辅助外审合规

- ✓等保2.0三级合规自检测模板
- ✓CIS网络安全框架合规自检测模板
- ✓RMiT马来西亚金融合规自检测模板

变更请求到达云平台 → 云平台执行变更 → 变更执行完成

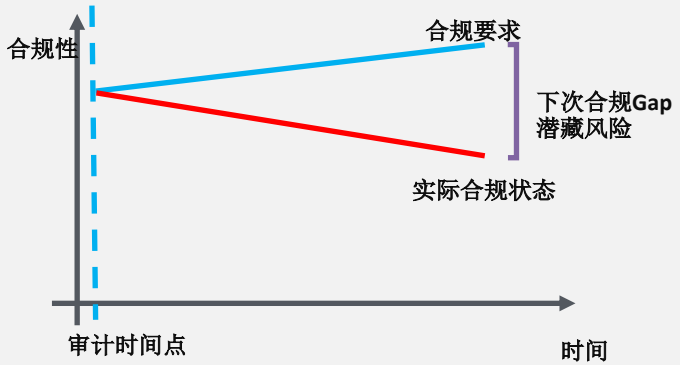
预防性管控策略

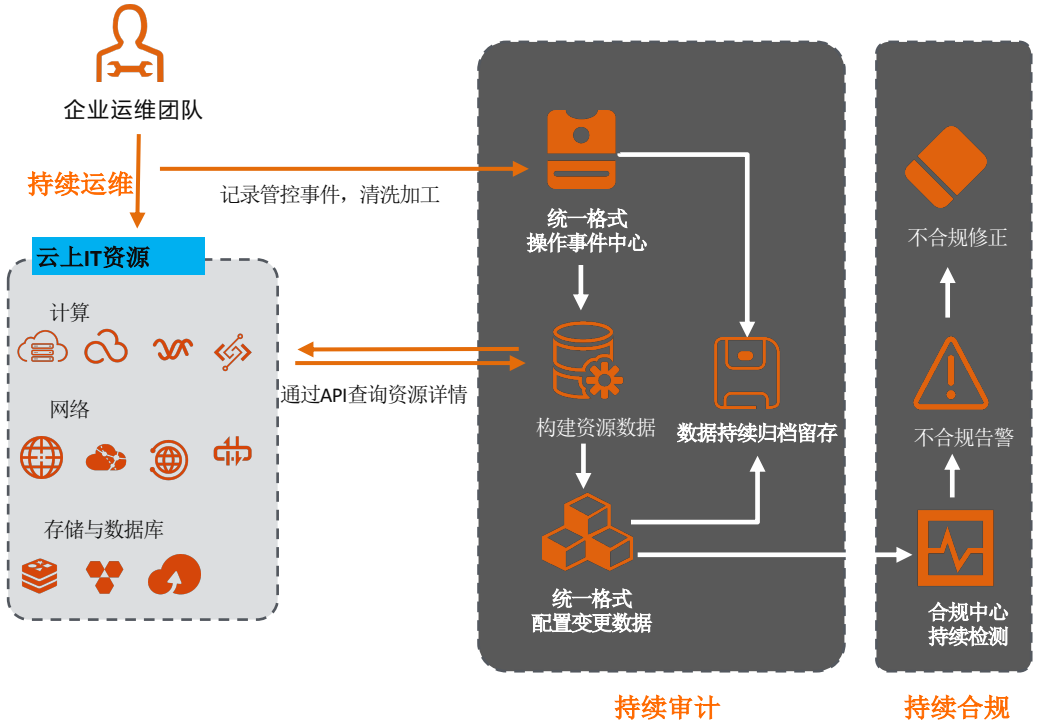
发现性管控策略

可持续—基于变更的持续监管

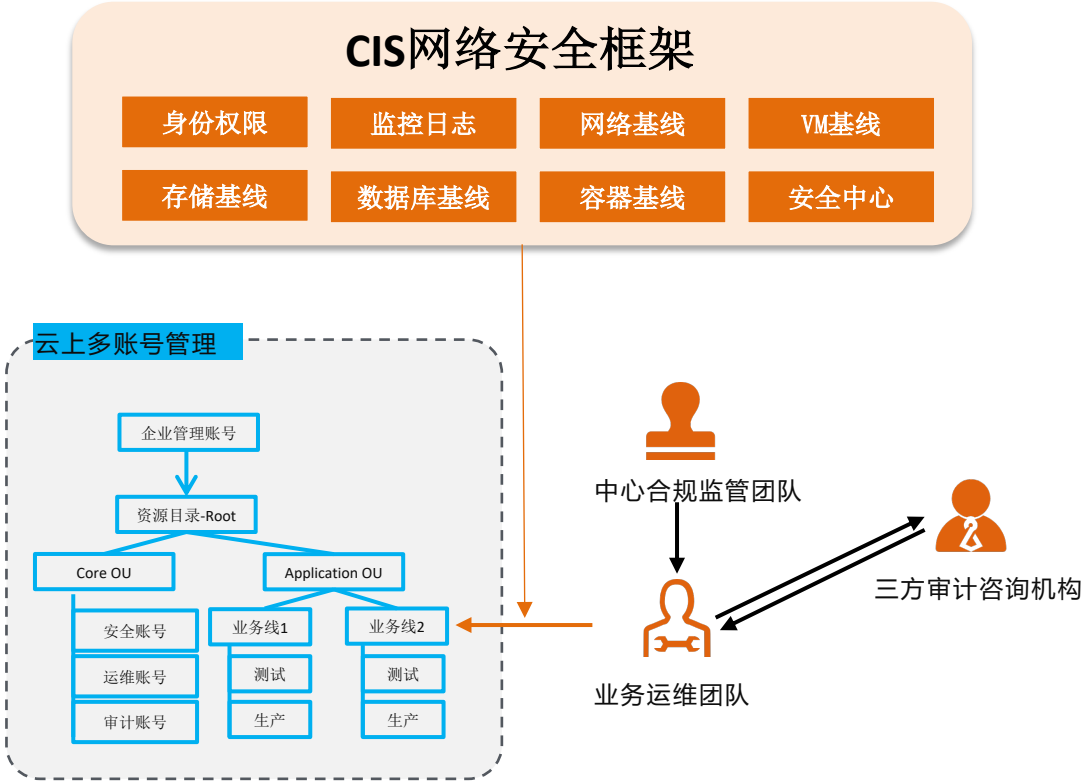
阿里云 | 企业IT治理

非持续审计合规的弊端





某多账号企业基于云审计框架的收益



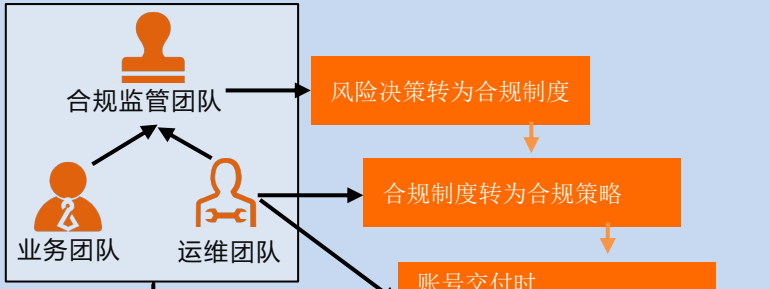
收益

- ✓ 企业在1天内完成全量自检扫描
- ✓ 企业在15天内完成问题整改
- ✓ 企业花费2天完成与外审机构的咨询评测
- ✓ 企业在后续长期管理中，具备了持续风控的能力
- ✓ 企业在后续的内审外审环节中，缩短自评、整改、评测的周期，减少人力投入
- ✓ 三方咨询机构基于云审计能力，快速完成评测，且规避篡改问题

企业如何开始审计合规的构建

企业随业务发展的合规迭代

组织管理制度的保障



内部合规培训

周期性复盘合规制度

合规制度迭代

合规治理与业务迭代的平衡

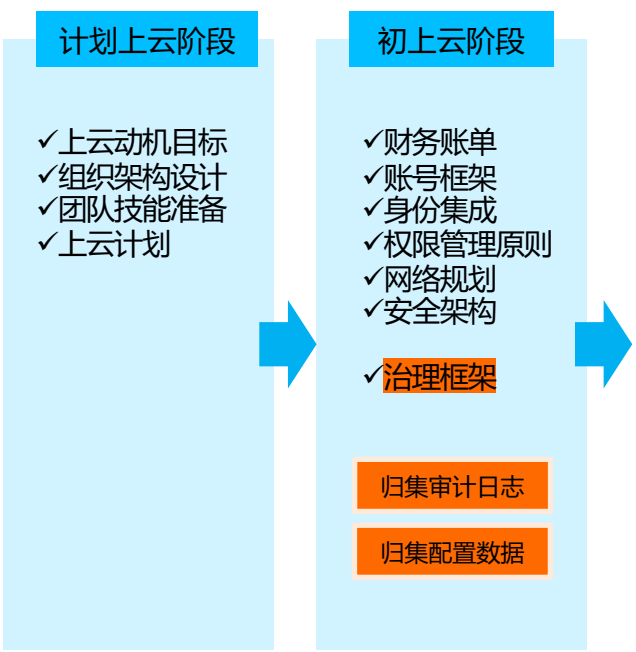
无业务性的MVP合规起点

测试环境上云	身份权限、采购限制
业务数据迁移上云	数据存储加密、传输加密、访问控制
核心业务上云	主机防护、公网隔离、备份恢复、全面监控
云上规模化发展	模板化管理、一致性管理、预算控制

企业上云过程中的审计合规规划

阿里云 | 企业IT治理

一个成熟企业的审计合规，**管理策略+治理策略**才是可持续的IT管理方案，技术+管理的可持续。



基于审计合规的持续运营和风控

资源&成本管理

- ✓资源管理
  - ✓基于CMDB的申购
  - ✓资源关系拓扑
  - ✓资源一致性管理
- ✓成本优化
  - ✓闲置资源清扫
  - ✓资源采购约束
  - ✓资源&成本大盘

可控的持续运维

- ✓阻止不合规发生
  - ✓禁止创建不加密磁盘
  - ✓禁止删除预设角色
  - ✓...
- ✓发现&止血不合规
  - ✓RAM User 超90天未登录
  - ✓未启用全局审计

可见的持续运维

- ✓支持内部透明化运维
  - ✓谁给A操作授权
  - ✓哪些应用（IP）使用AK
  - ✓异地登录监控告警
  - ✓异常访问监控告警
  - ✓资源生命周期时间线
- ✓应对外部审计
  - ✓180天及以上审计日志

资源配置数据　　运维审计日志

阿里云审计合规产品族支持企业实现合规框架

阿里云审计合规产品组合

阿里云 | 企业IT治理

预防性管控

管控策略

发现性管控

配置审计

操作日志

操作审计

事前

限制

- 不能创建非Golden Image的ECS
- 不能自行修改SSO配置
- 不能创建用户
- 不能新购和更改网络配置

事中

发现 处理

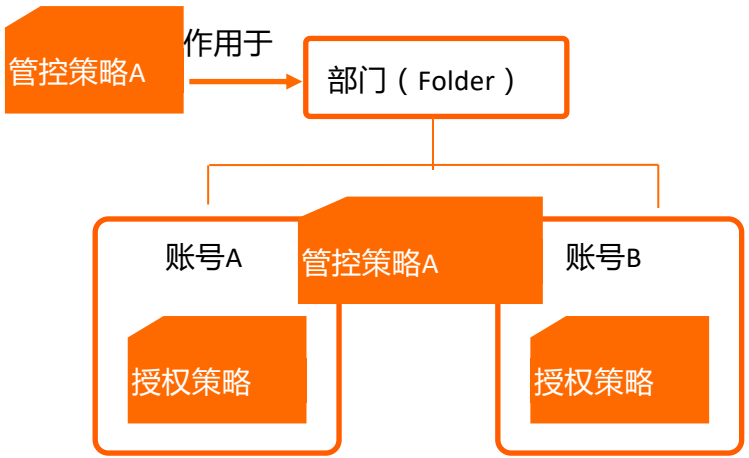
- 安全组不能设置为0.0.0.0/0
- 云上磁盘必须启用加密
- 负载均衡必须开启HTTPS监听
- ECS实例挂载到指定的VPC实例上

事后

谁 何时 哪里 哪些 什么操作

- 系统故障后，查看系统操作记录
- 数据泄露，查看对于该数据的访问记录
- AK泄露后，查看某个AK使用记录
- 监控高危操作，如修改权限策略

持续运维风控-事前约束



管控策略取代纸质条例
- 禁止创建于明
- 禁止自建网络资源

自上而下

禁止不合规操作

-样例：各业务团队必须使用企业的Golden Image

```
{
  "Statement": [
    {
      "Action": ["ecs:RunInstances","ecs:CreateInstance"],
      "Effect": "Deny",
      "Resource": "acs:ecs:*:*:instance/*",
      "Condition": {
        "StringEquals": {
          "ecs:ImageSource": "System"
        }
      }
    },
    {
      "Action": ["ecs:RunInstances","ecs:CreateInstance"],
      "Effect": "Deny",
      "Resource": "acs:ecs:*:*:image/*",
      "Condition": {
        "StringNotLike": {
          "Resource": "acs:ecs:*:*:image/m-bp14vmgrtj134p0****"
        }
      }
    }
  ],
  "Version": "1"
}
```

持续运维风控-事中记录

-使用**操作审计**追踪对云上资源的操作日志，在线查询日志或归档到SLS和OSS

-将所有成员账号的日志集中到**独立日志账号**存档

持续运维风控-操作事件demo

查看事件详情

阿里云 | 企业IT治理

每个事件被单独记录为一份日志
每个事件均包含固定格式的基本字段：

- eventName
- eventSource
- request Parameters
- sourceIpAddress
- userIdentity
- eventTime
- referencedResources

部分事件可能存在额外的补充字段。


```
{
  "eventId": "96F7F750-62CC-4651-977F-D81A1A566DE7",
  "eventVersion": "1",
  "eventSource": "resourcemanager-share.aliyuncs.com",
  "requestParameters": {
    "PolicyType": "Custom",
    "AcsHost": "resourcemanager-share.aliyuncs.com",
    "ResourceGroupId": 1208863178612953,
    "AcsProduct": "ResourceManager",
    "RequestId": "96F7F750-62CC-4651-977F-D81A1A566DE7",
    "PolicyName": "管理1个ECS实例",
    "AcceptLanguage": "zh-CN",
    "AkProxySuffix": "ram",
    "PrincipalName": "hantaotest@1208863178612953.onaliyun
    "HostId": "resourcemanager-share.aliyuncs.com",
    "PrincipalType": "IMSUser",
    " charset": "UTF-8"
  },
  "sourceIpAddress": "106.11.34.9",
  "userAgent": "Apache-HttpClient/4.5.7 (Java/1.8.0_152)",
  "eventType": "ApiCall",
  "referencedResources": {
    "Policy": [
      "管理1个ECS实例"
    ]
  },
  "userIdentity": {
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-05-28T11:14:00Z"
      }
    },
    "accountId": "1208863178612953",
    "principalId": "1208863178612953",
    "type": "root-account",
    "userName": "root"
  },
  "serviceName": "ResourceManager",
```

持续运维风控-事后合规检测

身份权限基线

- 可信身份白名单
- 最小授权，高权限限定时效
- 启用多维度认证策略，强密码策略
- 仅授权给用户组和角色

安全基线

- 攻击检测、恶意文件检测防护主机安全
- 隔离公网，启用WAF、DDoS防护网络安全
- 数据分类，静止加密，传输加密，保障数据安全
- 标记并保障核心IT实例，使用热备份、高可用模式

审计监控基线

- 必须开启管控、数据、数据库、网络流量的事件采集
- 为所有应用和服务启用监控
- 审计监控与资源运维权限隔离

一致性管理基线

- 一致性的资源命名和标记模式
- VM开启自动更新
- 使用模板部署
- 将权限、安全基线、治理基线写入模板

成本控制基线

- 可视化的成本中心，持续监控利用率和性能
- 拦截超限采购的异常行为
- 采购规格标准化
- 使用弹性管理

MVP治理基线-风险治理的起点

- 资源具备部门、计费单元、地理位置、SLA承诺、环境、应用、owner标签
- 限定资源创建的区域，限定可信身份白名单，开启删除保护
- 启用强密码策略，确保仅开启必要的公网端口并被WAF、云防火墙保护
- 被若为混合云，云上云下通讯必须经过VPN

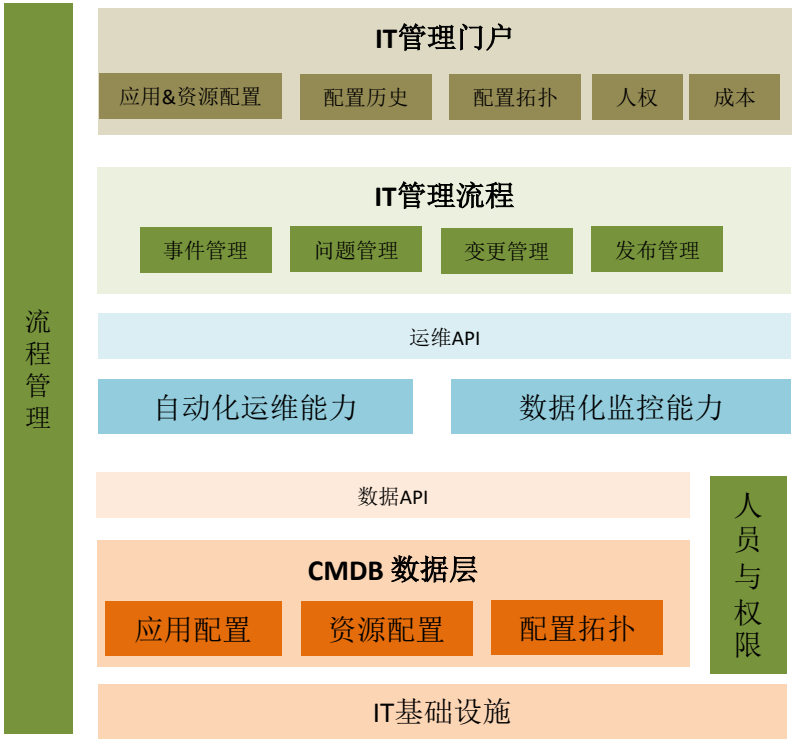
-阿里云内置CIS、等保2.0等合规包

持续运维风控-合规检测结果demo

阿里云 | 企业IT治理

compliance_type config_rule_name	COMPLIANT	NON_COMPLIANT
ack-cluster-deletion-protection-enabled	8	4
ack-cluster-network-type-check	-	12
ack-cluster-node-monitorenabled	6	-
ack-cluster-public-endpoint-check	-	6
actiontrail-enabled	-	1
cdn-domain-https-enabled	31	17
ecs-disk-auto-snapshot-policy	106	415
ecs-disk-encrypted	224	35
ecs-disk-in-use	258	1
ecs-disk-no-lock	521	-
ecs-disk-retain-auto-snapshot	501	20
ecs-instace-chargetype-check	438	13
ecs-instace-login-use-keypair	50	401
ecs-instance-deletion-protection-enabled	219	5
ecs-instance-no-lock	451	-
ecs-instance-no-public-ip	214	10
ecs-instance-status-no-stopped	224	-
ecs-internet-charge-type-check	449	2
ecs-security-group-not-used	76	46
eip-attached	184	1

Config as CMDB：通用基于CMDB的IT服务管理架构



配置生命周期管理

- 应用、模块、资源配置、身份权限的增删改查。
- 配置扫描发现、手动添加和配置模型的自定义。
- 配置拓扑的管理，应用&应用、应用&资源、资源&资源。

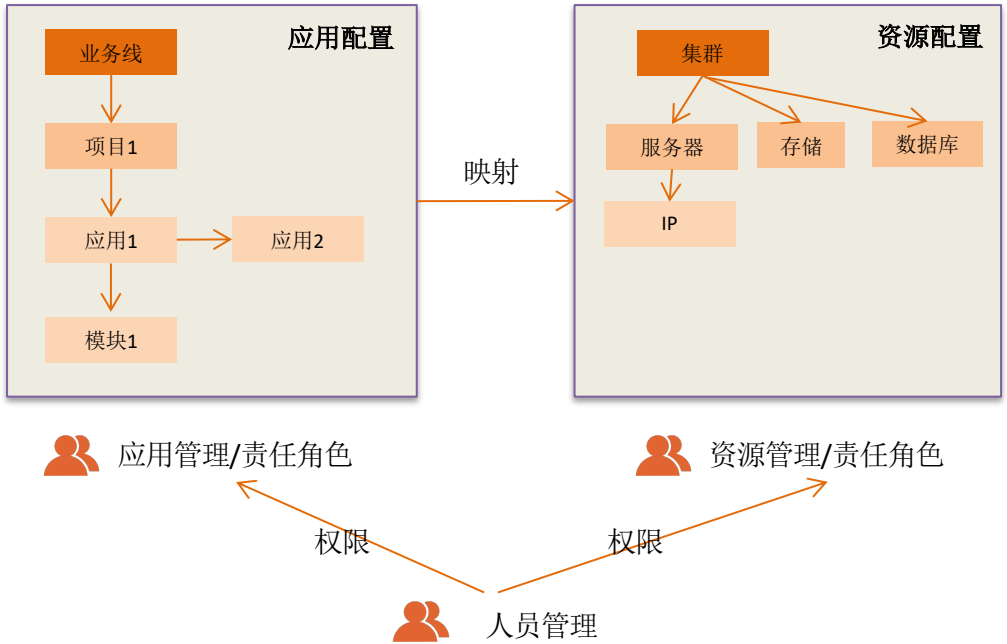
跨平台的统一资源配置门户

- 聚合、标准化且实时的配置数据视图。
- 查询和搜索配置数据、配置拓扑、配置变更历史等，配置包括应用、模块、IT资源、逻辑资源等。
- 为不同角色、不同场景提供不同树结构的CMDB，**标签化能力**

API化的支持其他运维管理流程

- 为日常变更、发布、故障排查、运维监控、权限管理、财务管理等提供可靠的配置数据
- 与人员、权限、流程管理相结合，将人、业务应用、IT配置关联起来，实现流程化运维

基于CMDB的IT服务管理Case



CMDB被认为是构建其他ITIL管理流程的基础，应该优先构建。70%~80%的问题都来自于变更，变更安全的核心在于流程化的控制、评估和执行变更。这需要依赖可靠的CMDB能力。

对人财物权法的管理需求都是源自业务的，不是直接面向IT架构的：

- 人员变更、资源增减，权限随之变更
- 变更前根据拓扑确认影响范围
- 资源变更历史为费用结算和审计提供数据
- 安全监控、合规审计都是业务视角，脱离业务不会关心一组或一台机器。产生故障或合规问题时，先确认影响的IT范围和业务范围

总结：阿里云审计合规能力的核心优势

专业成熟的制度，可行的实施方案

综合多数企业的风控实践和云平台多年经验，为企业内的安全、合规、运维、风控团队提供通用的合规制度和可行的实施方案。辅助实现岗位职责

持续治理，风险最小化

替代定时抽检，实现在日常运维的事前、事中、事后的持续治理，使可控性最大化，实现高频变更下的持续风控

手段变革，高效便利的云审计

相比传统的手工定时抽检和复查，采用系统化自动化的平台手段，分钟级实现启用和自检，快速摸底潜在风险

故障追溯，最快定位最快解决

事后快速追溯问题根源，缩短故障时间；细致审计，责任到人

Thanks

云上审计合规——可见可控可持续

阿里云 | 

奥运会全球指定云服务商