

ALIBABA CLOUD

阿里云

阿里云最佳实践
云上运维

文档版本：20210527

 阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1. 资源管理	05
2. 云上成本管理最优化实践	06
3. 基于API自建云资源管控平台	07
4. 云上Prometheus监控运维	08
5. API使用实践	09
6. Terraform应用	10
7. Terraform云资源管理	11
8. 弹性计算OOS批量运维自动化运维	12
9. 弹性计算OOS审批流程自动化运维	13
10. 弹性计算OOS事件驱动自动化运维	14
11. 云上资源操作和配置审计	17
12. 阿里云DDH集群运维管理最佳实践	19
13. 单账户下企业分账	21

1.资源管理

指定结算账号统筹管理企业多个阿里云账号及资源，使用资源组按照项目或应用视角来进行分组管理和访问管控。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

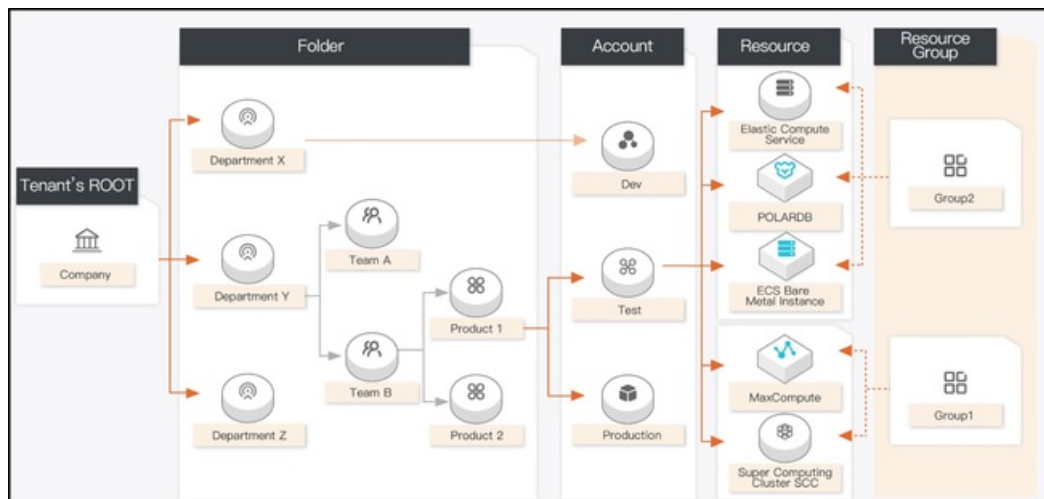
场景描述

随着企业IT成熟度不断提高、管理的云上资源不断增多，如何对资源进行高效管理的问题就会凸显出来。阿里云的资源管理服务支持您按照业务需要搭建适合的资源组织关系，使用资源目录、资源夹、账号、资源组分层次组织与管理您的全部资源，更好的实现项目成功。

解决的问题

- 按照企业组织结构管理账号体系
- 指定结算账号进行统一结算
- 统一管理成员账号权限系统
- 账号下的资源按照资源组进行分类
- 可以按照自定义财务单元进行分账管理

部署架构图



2.云上成本管理最优化实践

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多最佳实践](#)

场景描述

随着业务发展，客户在云上管理了大规模的机器，如何做好云资源成本管理，合理利用云资源支持好业务发展，成为企业重点关注的领域，需要数字化管理云上资源成本。

本示例借助云成本管家和监控体系，提供统一费用展示、预算管控、成本优化等，是客户了解成本管理的最优化实践。

实践收益

借助云成本管家和监控体系，提供统一费用展示、预算管控、成本优化；全景费用透视，按照标签/资源组分类等，提升云费用协同效率；结合监控分析和资源使用量，形成数字化的用量预测和云资源优化。

业务架构



3.基于API自建云资源管控平台

提供业务上云过程中自建管控接入云资源的最佳实践，覆盖核心场景，通过预留实例券节省成本。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

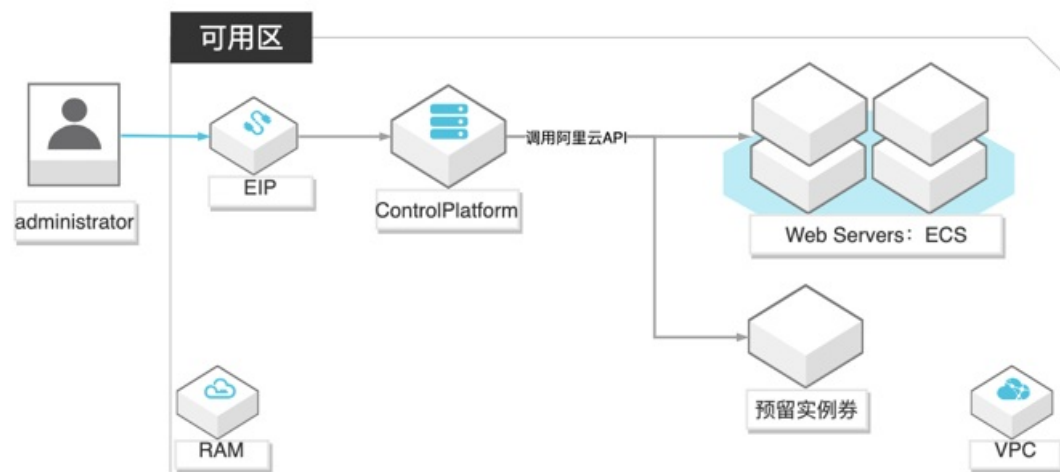
场景描述

- 客户自建资源管控。
- 快速接入云资源：选型后，希望快速对接云上资源，将云上资源集成到管控平台。
- 发挥上云优势，适应devops等需求：在上云过程中，希望上云后能充分发挥云上资源弹性和灵活的特点，同时能节省成本。

方案优势

- 简单：最佳实践提供无基础要求快速入门学习API的方式。
- 快速：覆盖业务常见使用场景，开箱即用。
- 利用云上优势，从容应对业务变化：针对 IAAS层资源变化快，但按量付费实例成本高的问题，本例介绍预留实例券的使用场景和选购细节。

部署架构图



4.云上Prometheus监控运维

本文主要介绍使用Kubernetes集成部署或者托管版Prometheus免运维的部署监控方案。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

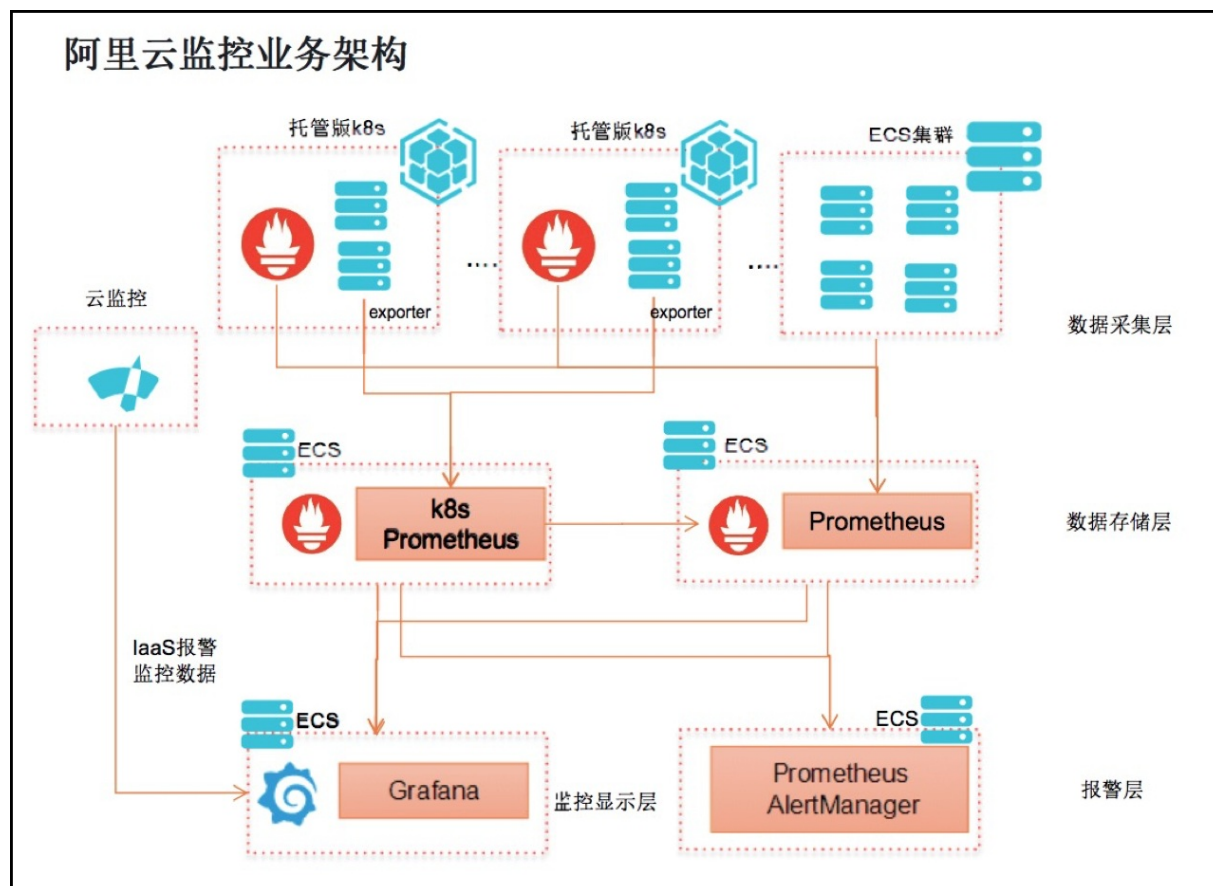
场景描述

Prometheus是一款面向云原生应用程序的开源监控工具。本实践主要介绍基于阿里云容器服务Kubernetes集成部署Prometheus监控方案，通过grafana对监控数据进行可视化展示，通过Alertmanager配置统一的监控告警服务，轻松实现云原生监控运维。

解决的问题

- Helm/Chart一键部署Prometheus监控套件。
- 默认集成Alertmanager和Grafana。
- 支持钉钉以及邮件告警。
- 支持自定义监控任务。

部署架构图



5.API使用实践

阿里云API、SDK以及CLI的介绍和示例代码最佳实践。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

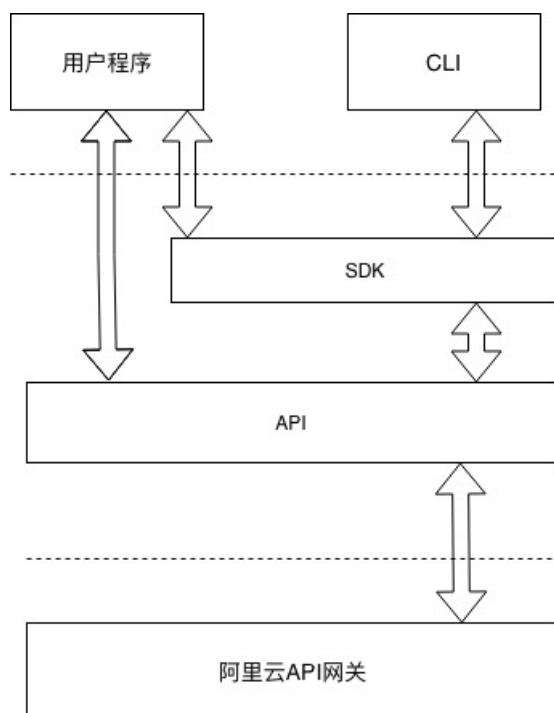
场景描述

阿里云用户使用阿里云产品的过程中，某些具备一定开发能力的用户不需要通过控制台的界面操作方式来管理云产品资源，可以通过API、SDK&CLI的方式来进行云资源管理。

解决的问题

阿里云API、SDK&CLI的原理和基本使用。

部署架构图



6.Terraform应用

使用Terraform工具进行云上业务架构的应用实践和代码示例。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

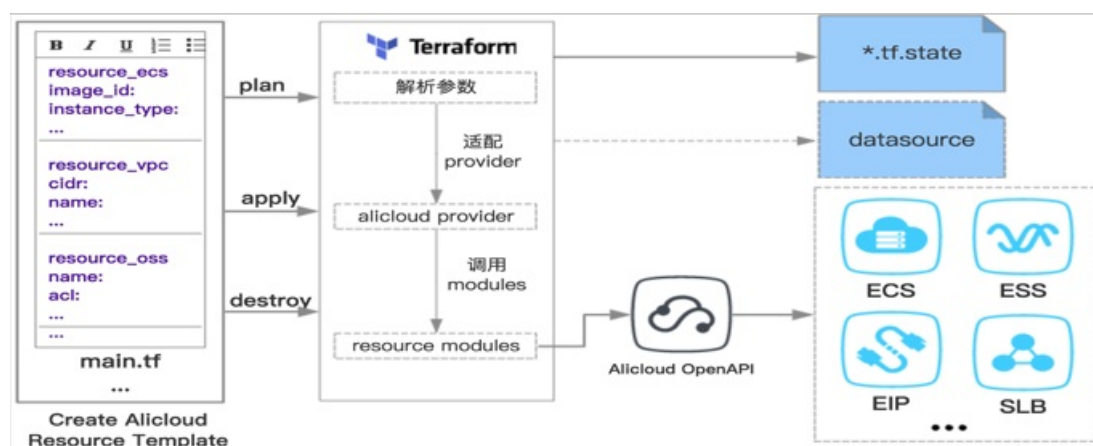
场景描述

云上资源规模复杂，提升自动化云上资源部署能力。

解决的问题

- 人工资源部署运维效率低，易出错
- 复杂云上资源架构管理困难
- 云资源变更回滚困难，变更记录无法记录和审计

部署架构图



7.Terraform云资源管理

云上资源基于Terraform来管理和维护，包括资源的创建、修改、变配、删除、打标签、执行计划等。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

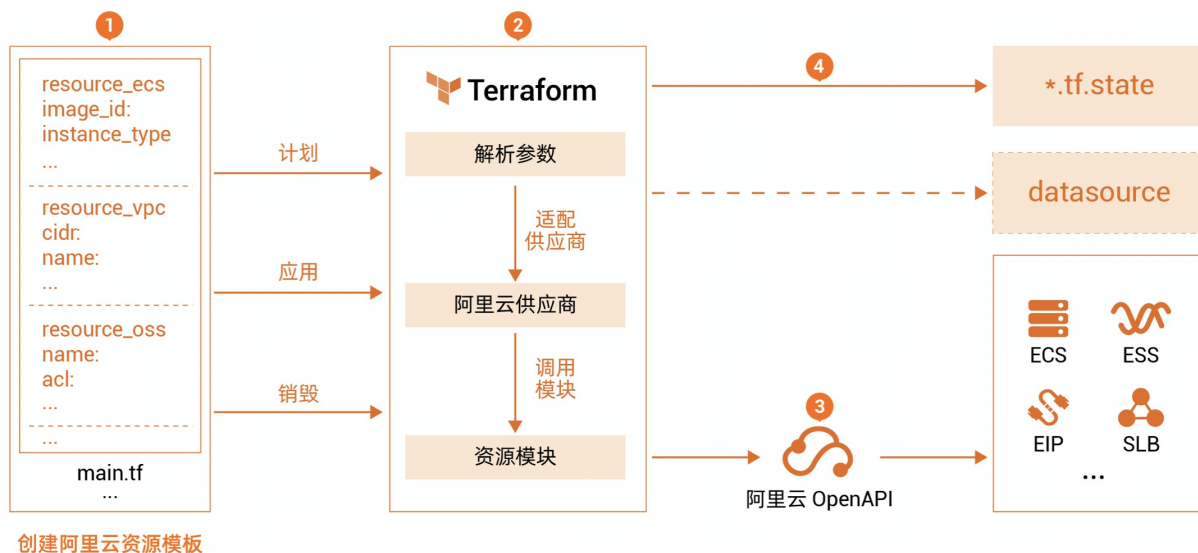
场景描述

本方案适合Terraform的迁移用户或准备使用Terraform的用户。可以帮助客户在阿里云安全、高效地预配和管理云基础产品。用户在正式使用前，对Terraform模块与实际使用模块的基本验证。用于对管理和维护IT资源的日常操作的验证。

解决的问题

- Terraform管理云资源
- 跨云管理云资源
- 混合云管理云资源
- 批量管理云资源

部署架构图



8.弹性计算OOS批量运维自动化运维

OOS是全面、免费的云上自动化运维平台，通过批量运维提供的自动化运维能力，免去人为因素，提高运维效率。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

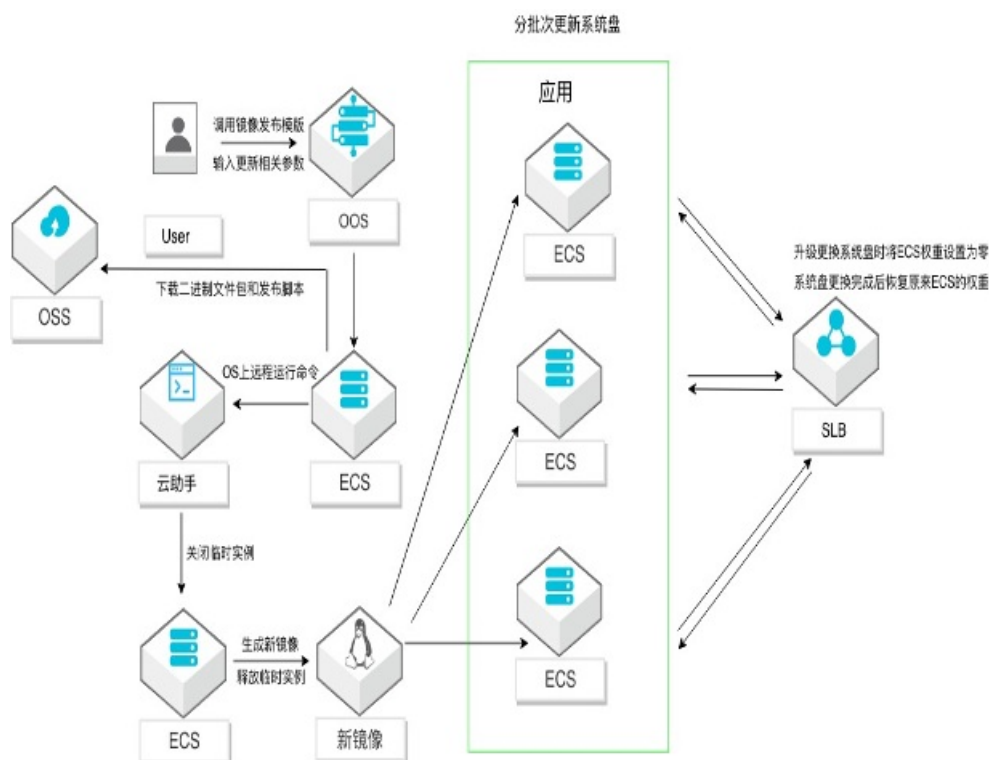
场景描述

阿里云推出了运维编排OOS，支持所有的云上资源操作和ECS实例内部操作。弹性计算OOS是全面、免费的云上自动化运维平台，提供运维任务的管理和执行。本实践以5个场景为例介绍阿里云OOS在批量运维的能力。

解决的问题

- 人工运维效率低下，易出错
- 运维动作权限管控困难

部署架构图



9.弹性计算OOS审批流程自动化运维

利用OOS在运维常见的部署系统、扩容系统、回收系统三个场景中添加审批流程，并以钉钉通知审批人员。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

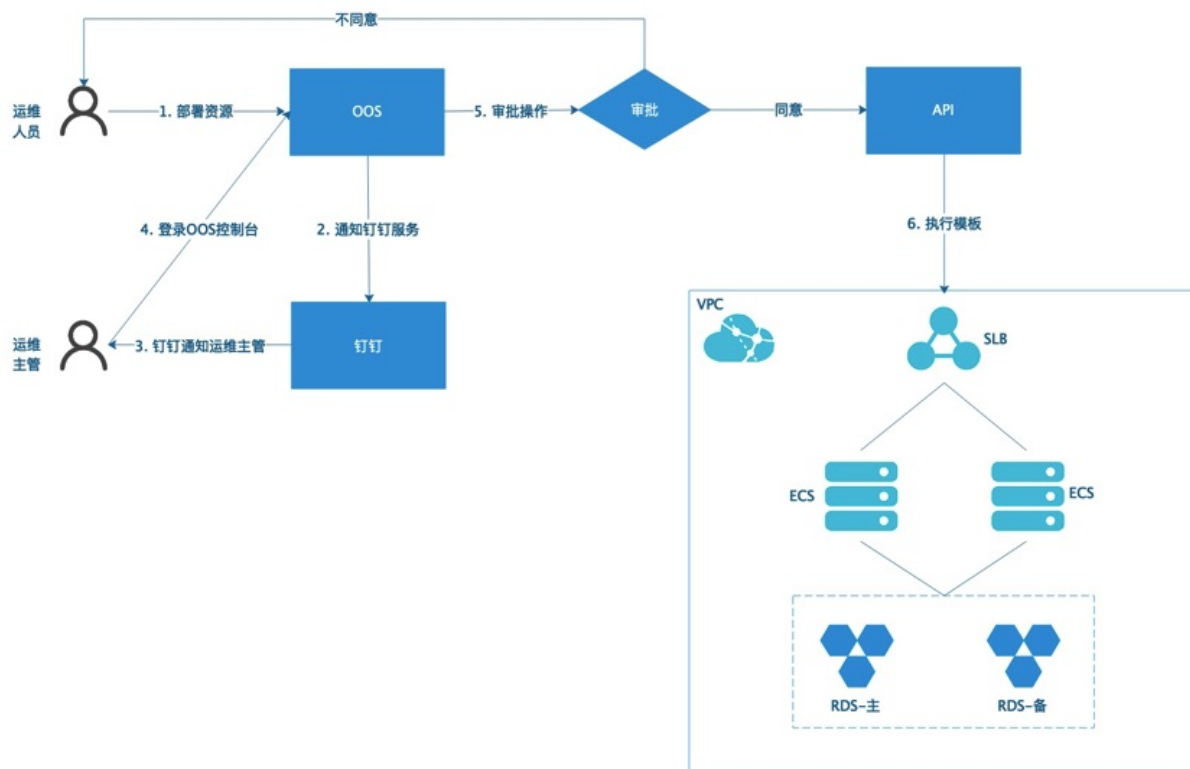
场景描述

本文以ECS、RDS、SLB搭建一个小型的WEB系统为例，介绍如何利用OOS在运维常见的部署系统、扩容系统、回收系统三个场景中添加审批流程，并以钉钉通知到对应的审批人员。

解决的问题

- 对接阿里云API，通过OOS模板执行运维任务，实现了运维自动化与可视化。
- 运维操作集成了RAM访问控制权限管理，无需担心操作安全，并可以快速增加审批流程，提高运维安全与效率。

部署架构图



10.弹性计算OOS事件驱动自动化运维

OOS是全面、免费的云上自动化运维平台，通过事件驱动提供自动化运维，免去人为因素，提高运维效率。

直达最佳实践

[点击查看最佳实践详情页](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

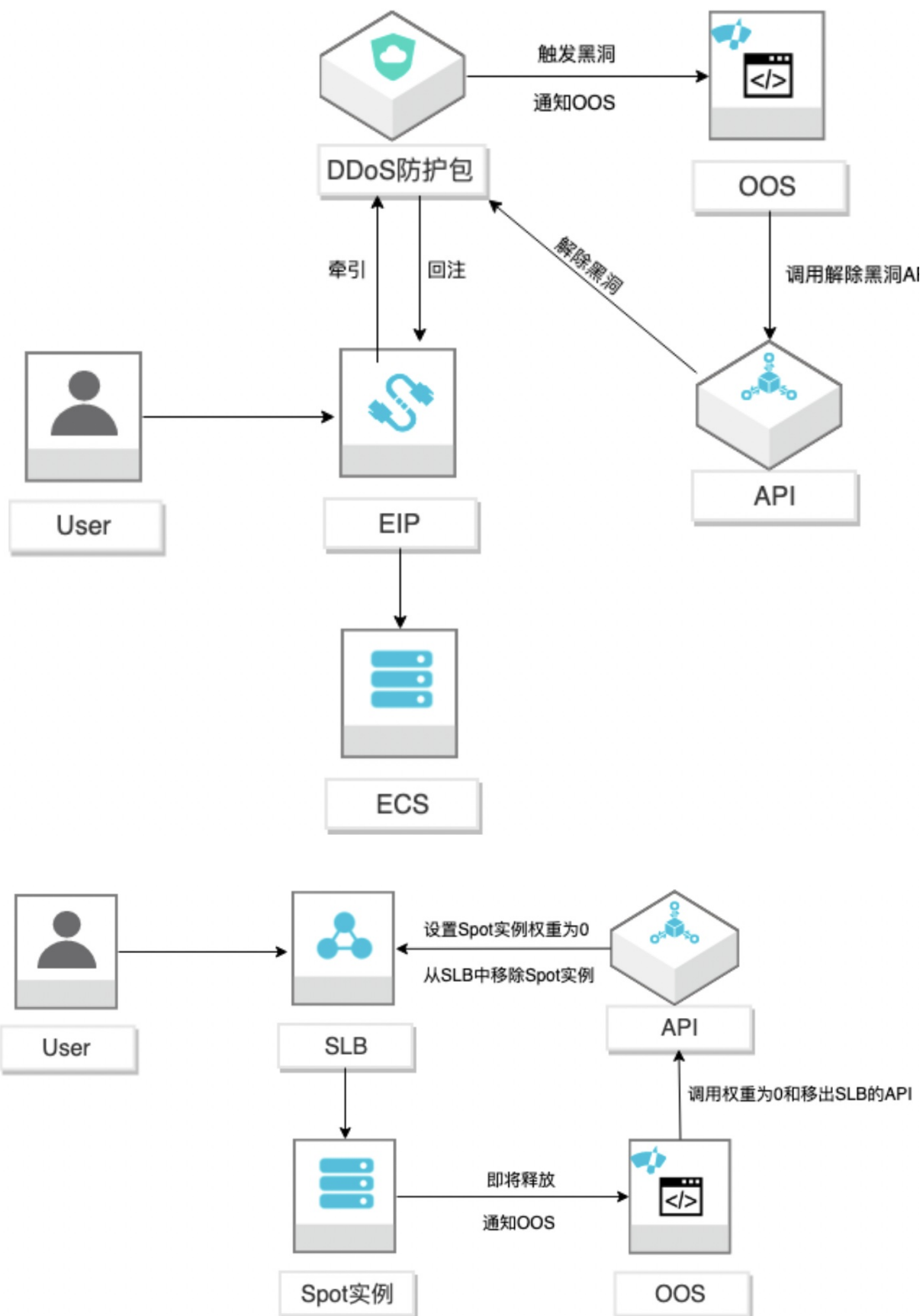
场景描述

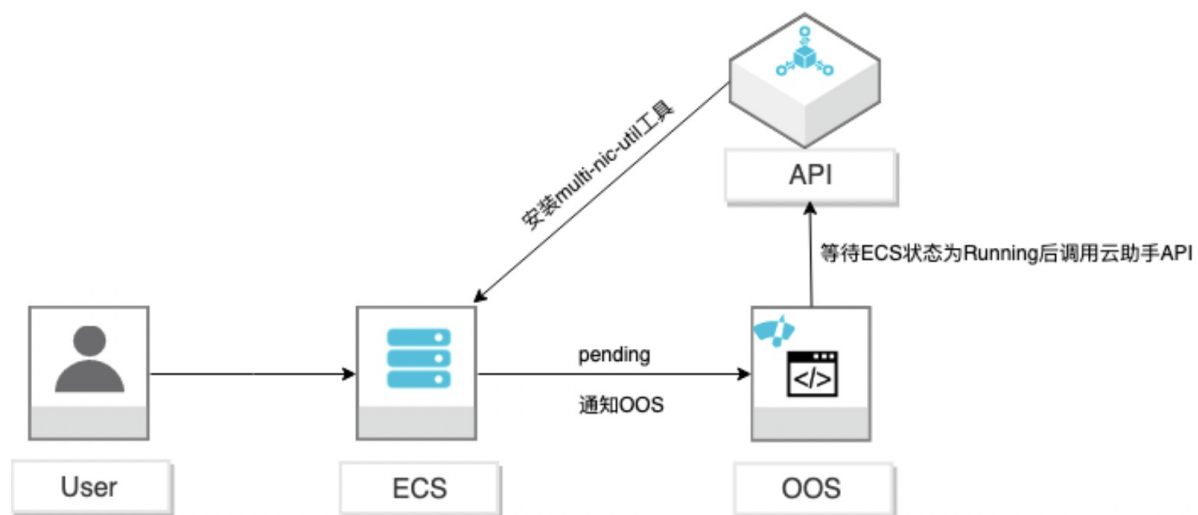
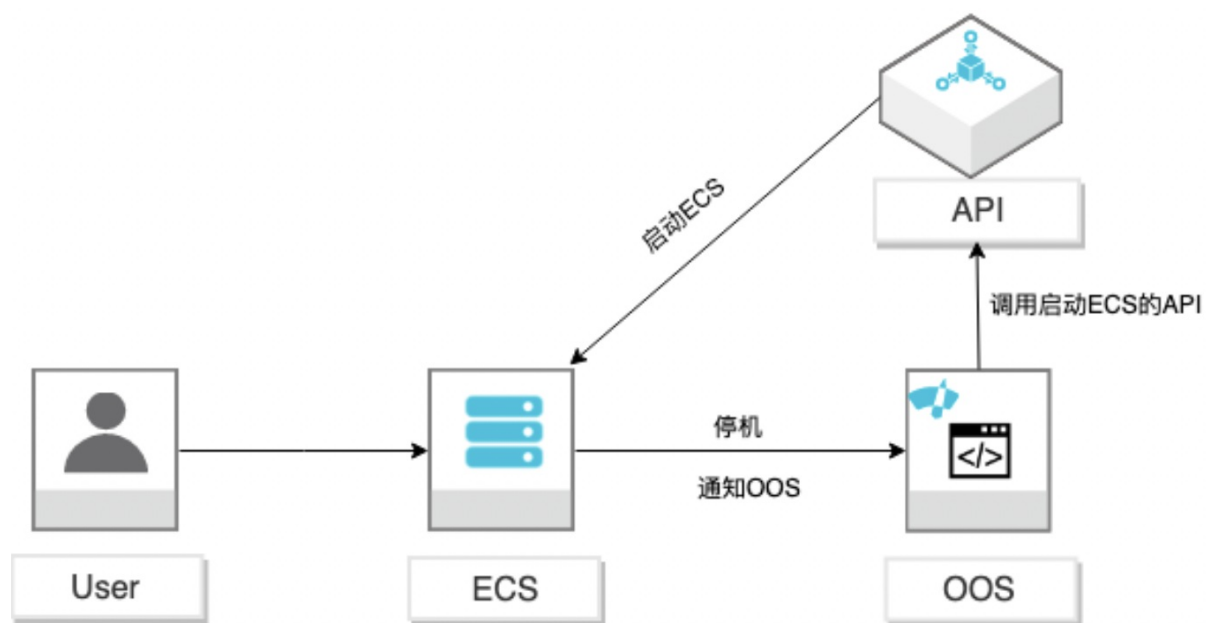
弹性计算OOS是全面、免费的云上自动化运维平台，提供运维任务的管理和执行。本方案以四个事件驱动、一个告警驱动的自动化运维模板为例，介绍使用OOS的事件驱动自动化运维能力，提供主动运维支持，免去中间的人为因素，提高运维效率。

解决的问题

- 事件驱动自动化运维
- 告警驱动自动化运维
- 批量操作的运维场景
- 更新镜像的运维场景
- 需要审批的运维场景
- 定时任务的运维场景
- 跨地域、多地域运维

部署架构图





11.云上资源操作和配置审计

企业会面临外部对企业云上信息系统的合规要求，提供云上资源的操作审计和配置审计最佳实践。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

场景描述

本方案是面向云上资源的操作审计和配置审计提供的最佳实践。适用于企业型客户。

通过最佳实践帮助客户在本场景下更好的使用阿里云，涉及到配置审计、操作审计、函数计算、SLS、OSS等服务的实践操作。

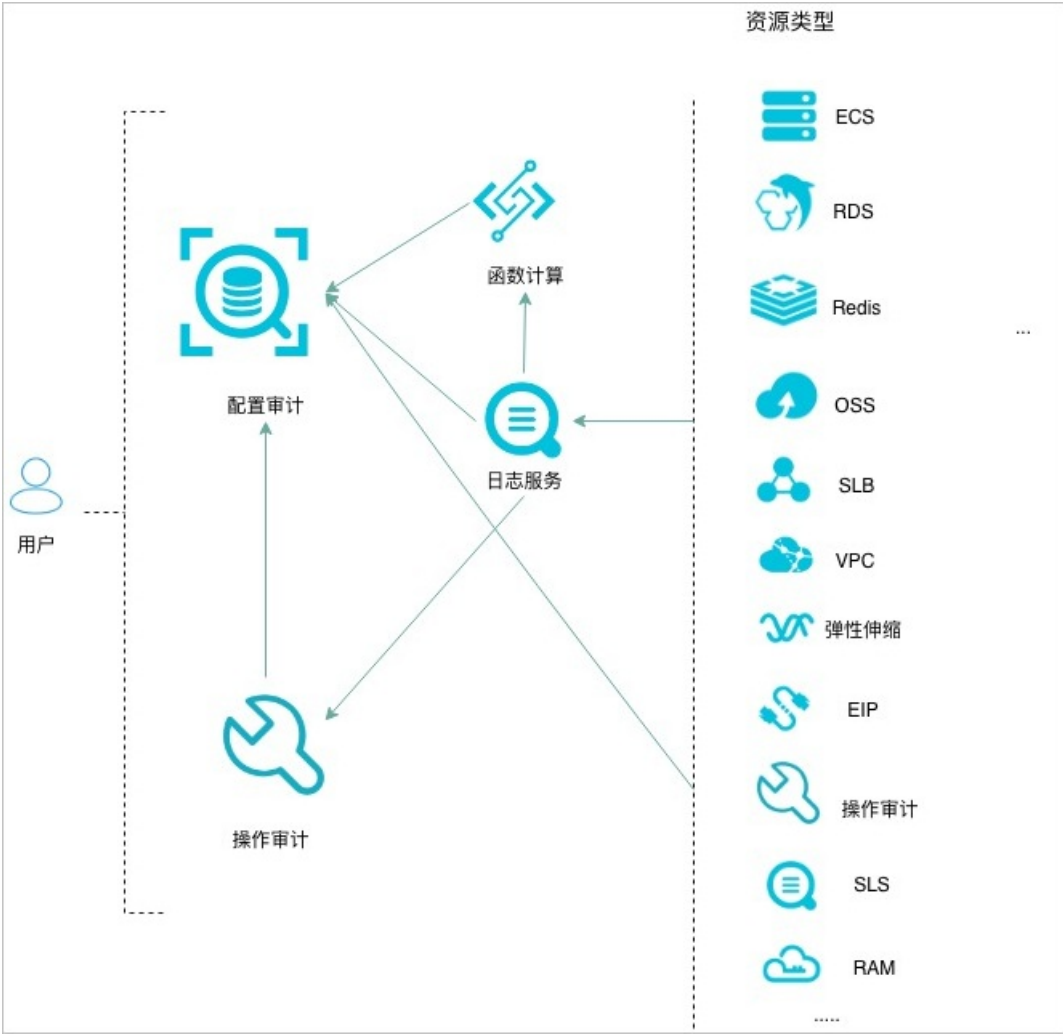
解决问题

企业会面临外部对企业云上信息系统的合规要求，如等保2.0法规要求。

同时当云上资源达到一定规模时，在内部会制定合规管控的基线，满足自身管理效率和安全合规的需求。

包括记录云上资源管理的操作日志、资源配置变更日志，还需依赖云平台提供的持续监控和自动告警能力，实现合规性的自主监管。

业务架构图



12. 阿里云DDH集群运维管理最佳实践

本文介绍阿里云专有宿主机（DDH）运维管理方法，针对CPU负载较低的业务场景，通过CPU超分比，可以有效提高资源利用率，节省整体成本。并且可以通过RAM授权业务团队，结合云监控资源使用率，方便业务使用的同时又能有效遏制资源浪费。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

方案概述

当前许多企业的IDC业务场景，资源管理等使用习惯与公共云不同，使用DDH集群管理，继承IDC虚拟化使用习惯，比如自定义ECS规格。同时针对CPU负载较低的场景，通过CPU超分，可以有效提高资源利用率，节省整体成本。并且可以通过账号授权业务团队，结合云监控资源使用率，方便业务使用的同时又能有效遏制资源浪费。

适用场景

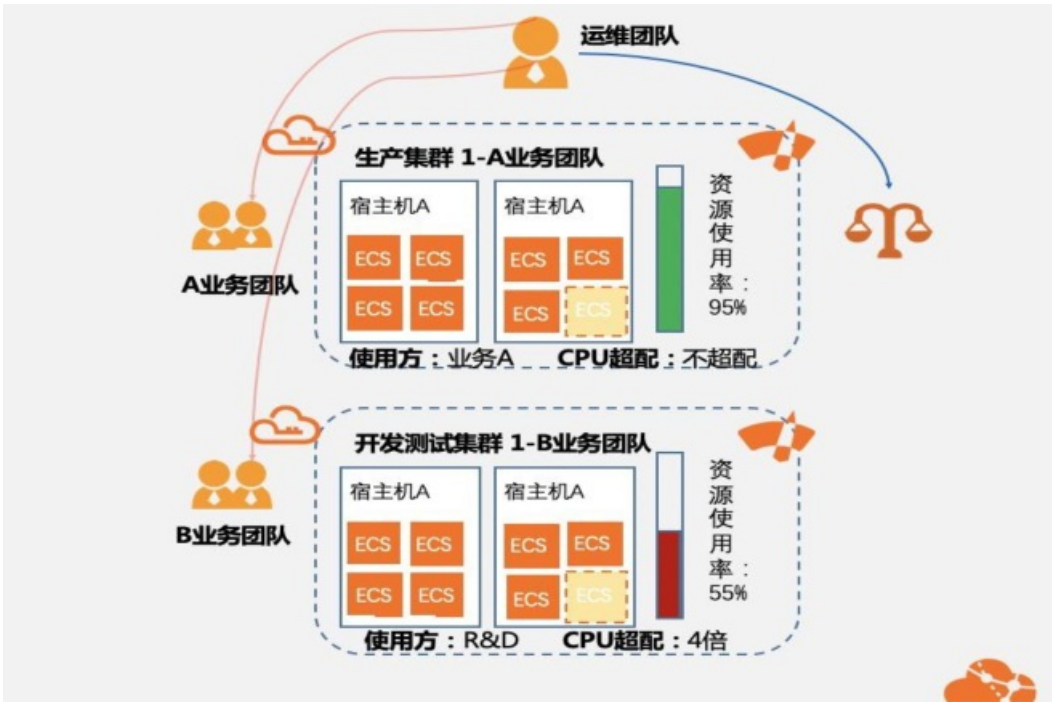
- 针对CPU负载较低的场景，尤其是传统IDC企业客户有降本诉求，使用专有宿主机集群构建云上环境，通过超分提高资源利用率。
- 需要沿用传统IDC资源管理方式，通过访问控制授权，云监控资源，完成专有宿主机集群运维管理使用闭环。

技术架构

本实践方案主要操作步骤：

1. 根据规划创建VPC网络环境，根据规划创建DDH资源，ECS资源。
2. 自定义权限设置，RAM子账号授权。
3. 监控DDH资源使用率。

4. DDH实例迁移验证。



13. 单账户下企业分账

从集中化的运维到分散化运维，整个企业在模式的转化过程中，面临着权限拆分和账单拆分的业务挑战，为了应对这个挑战，阿里云根据许多客户的真实场景，总结了分权分账的解决方案。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

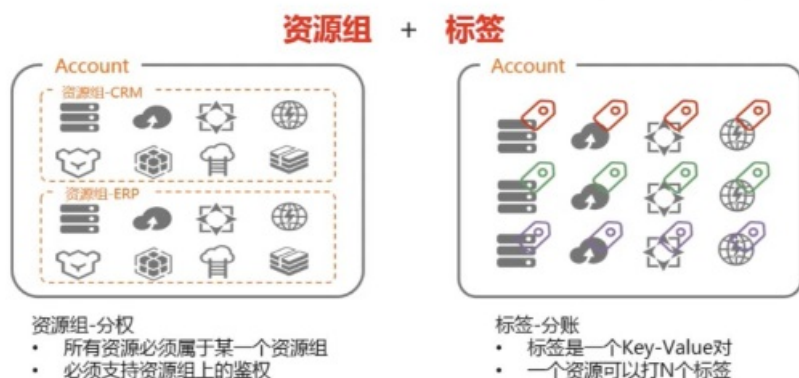
[点击查看更多阿里云最佳实践](#)

方案概述

随着数字化转型浪潮的袭来，越来越多的企业通过云计算来加速业务的创新能力，相对于传统IT的运维，云计算具有快速创建，弹性伸缩等优势，正是由于云的出现，重构了传统企业IT治理、财务预算审计等流程。不同企业上云后，在企业IT治理分账方面，表现为不同的形态，大致分为以下三种类型的企业：

1. 集中型的企业，所有云资源由统一的一个部门进行规划和统筹。
2. 分散型的企业，每个部门和团队，对云资源的管理，拥有自主管理权。
3. 混合型企业，部分业务由上级主管单位管理，部分业务由下级业务方管理。

方案架构



云上的主账号，可以看做资源的容器，很多企业没有按照组进行资源的管理，也没有按照组进行授权，没有将资源划分到每个部门或者业务线进行分账。

- 分权：按照资源进行分组，按照分组进行授权，基于资源组，我们能有序进行分组管理，关于分权的最佳实践，请参考：《[资源管理](#)》。
- 分账：在我们对于资源的使用过程中产生费用，大多数情况下需要进行费用分摊，比如按照使用者、部门、业务、应用等进行成本分摊，针对不同资源，我们可以通过标签进行标识，更加灵活的进行分组分账。

方案优势

- 满足企业应对分权分账、账户内资源的有序管理的需求
- 快速管理阿里云资源与人权钱关系
- 随着您云上资源的增加，管理难度也随之变化，您可以通过标签实现批量管理资源。标签是人员、财务、物品管理的重要分组工具，帮助您横向连通云产品。

- 通过多种方式实现基于Tag的分账管理，满足大部分分账场景。