ALIBABA CLOUD

阿里云

阿里云最佳实践

安全合规

文档版本：20220628

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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.EMR集群安全认证和授权管理 05
2.企业办公安全访问一体化最佳实践 06
3.RAM角色集成企业OpenLDAP身份认证 07
4.云上日志集中审计 08
5.云上资源操作审计和配置审计 09
6.基于IDaaS的AD账号同步 10
7.ACK容器平台集群安全控制 11
8.RAM账号权限管理 12
9.RAM用户集成企业AD FS身份认证 13
10.数据库运维安全管理 14
11.AK防泄漏 15
12.RAM角色集成企业AD FS身份认证 16
13.传统企业业务上云基础安全 18
14.电商网站业务安全 20
15.混合云多云统一安全 21
16.企业上云等保二级合规 23
17.企业上云等保三级合规 24
18.企业上云数据安全 25
19.图片违规检测和跨国际区域备份 26
20.网络安全升级支持IPv6 27
21.云平台内部操作透明化 28

1.EMR集群安全认证和授权管理

介绍EMR高安全集群如何使用Kerberos和Apache Ranger进行鉴权和访问授权管理。

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

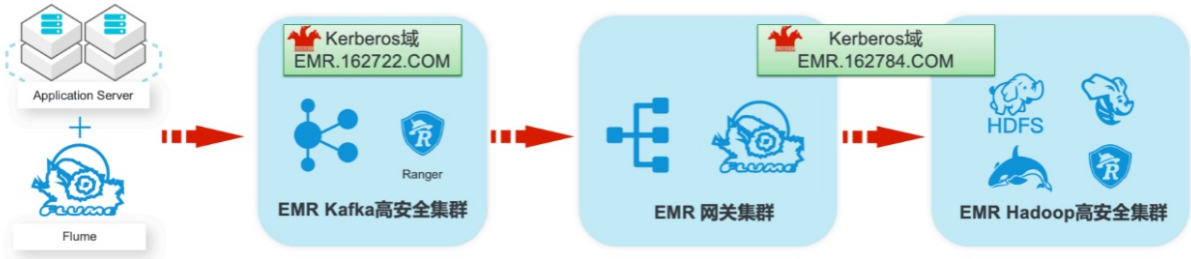
场景描述

阿里云EMR服务Kafka和Hadoop安全集群使用Kerberos进行用户安全认证，通过ApacheRanger服务进行访问授权管理。本最佳实践中以Apache Web服务器日志为例，演示基于Kafka和Hadoop的生态组件构建日志大数据仓库，并介绍在整个数据流程中，如何通过Kerberos和Ranger进行认证和授权的相关配置。

解决问题

- 创建基于Kerberos的EMR Kafka和Hadoop集群。
- EMR服务的Kafka和Hadoop集群中Kerberos相关配置和使用方法。
- Ranger中添加Kafka、HDFS、Hive和Hbase服务和访问策略。
- Flume中和Kafka、HDFS相关的安全配置。

部署架构



2.企业办公安全访问一体化最佳实践

本场景模拟企业办公环境，基于CSAS服务构建企业办公安全一体化方案，将“安全+网络”能力无缝融合，实现了对云下办公终端安全的统一管理，企业无需在投资复杂且昂贵的传统硬件安全设备，即可快速构建安全、可靠、低成本的办公安全防护体系。

直达最佳实践

点击查看最佳实践详情

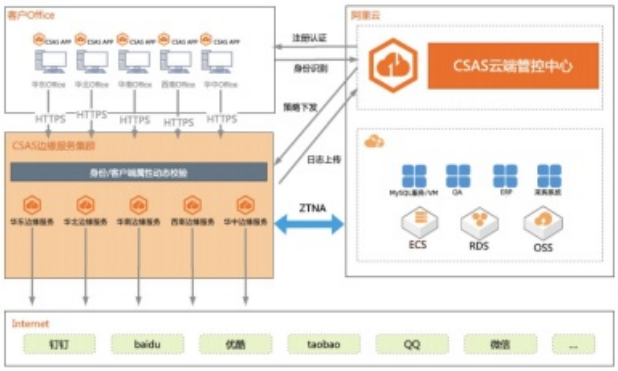
更多最佳实践

点击查看更多最佳实践

解决问题

- 企业办公环境访问互联网的安全管理
- 企业办公环境访问内网服务的安全管理
- 企业办公网络、安全一体化管理

方案架构



3.RAM角色集成企业OpenLDAP身份认证

介绍阿里云RAM使用KeyCloak集成企业OpenLDAP，管理员工的身份及权限。配置RAM角色与KeyCloak用户/用户组的映射关系，实现企业员工使用企业OpenLDAP账号以单点登录（SSO）的方式访问阿里云控制台。

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

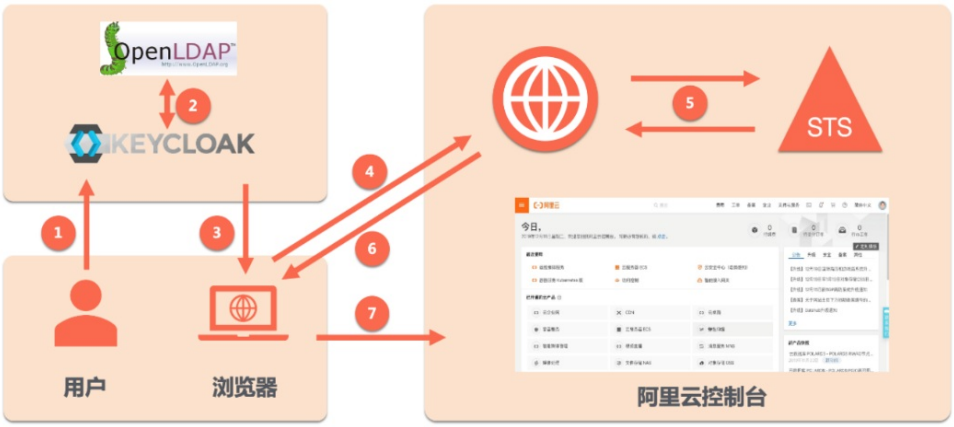
场景描述

本文介绍阿里云RAM使用KeyCloak集成企业OpenLDAP，管理员工的身份及权限。配置RAM角色与KeyCloak用户/用户组的映射关系，实现企业员工使用企业OpenLDAP账号以单点登录（SSO）的方式访问阿里云控制台。

解决问题

- 快速部署OpenLDAP及用户创建。
- 快速部署KeyCloak，并与OpenLDAP实现用户联合。
- 阿里云角色SSO配置。
- KeyCloak用户绑定RAM 角色SSO。
- KeyCloak用户组绑定RAM 角色SSO。

部署架构



4.云上日志集中审计

在SLS的日志审计应用的基础上，集中汇聚云安全产品日志、Web服务日志等，进行集中审计。

直达实践

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

云上的各类云产品和客户部署的业务系统会产生各类日志，企业合规及安全运营等都需要在一个地方能集中的查看和分析日志；目前各云产品日志大部分都进了日志服务SLS，但都是产品独立的project，不方便集中审计；客户的业务系统日志各种形态都有；多云和混合云的场景，日志也需要能集中审计。

解决问题

- 所有日志集中到SLS一个中心project下。
- 满足等保合规和内部合规需求。
- 满足运维和安全运营需求。

部署架构

5.云上资源操作审计和配置审计

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

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

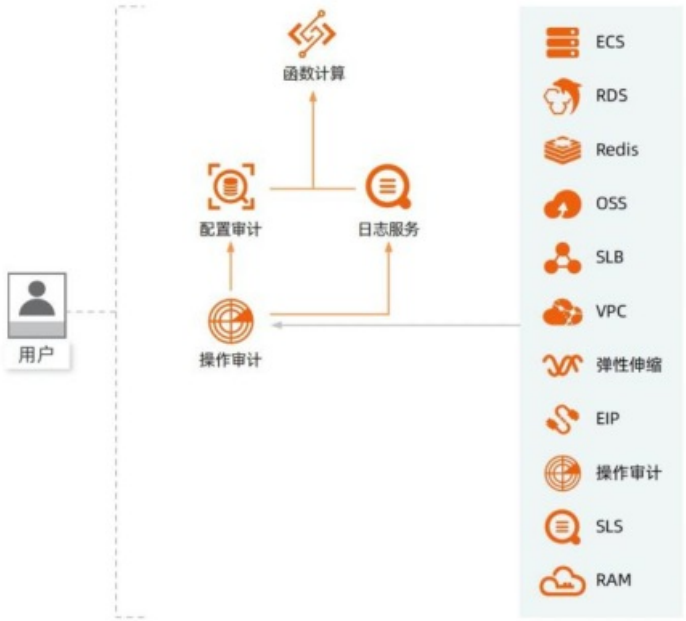
场景描述

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。

方案架构



6.基于IDaaS的AD账号同步

通过IDaaS产品，把客户AD域和云上RAM账号体系打通，并实现准实时的同步。

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

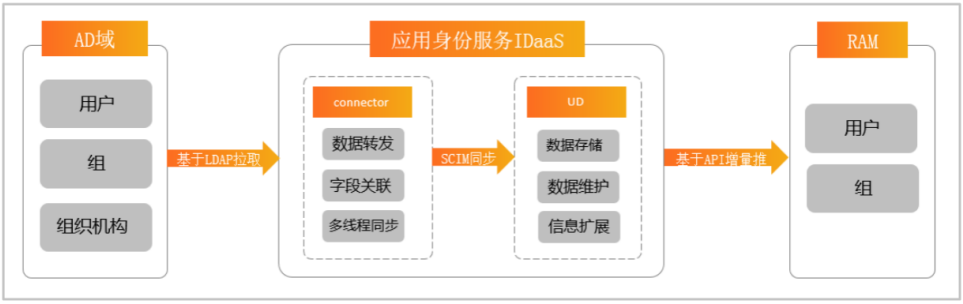
场景描述

应用身份服务IDaaS支持基于LDAP协议（LDAP-Light Directory Access Portocol，它是基于X.500标准的轻量级目录访问协议）的数据同步，本文介绍企业内部AD域与应用身份服 务IDaaS进行账号同步，然后IDaaS把账号推送到RAM中，最终实现通过应用身份服务IDaaS将AD域与RAM域的用户数 据全面打通实现准实时的同步。

解决问题

- AD账号同步到RAM
- AD账号变化后的自动更新

部署架构



7.ACK容器平台集群安全控制

阿里云容器服务ACK的Kubernetes集群平台安全管控实践。

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

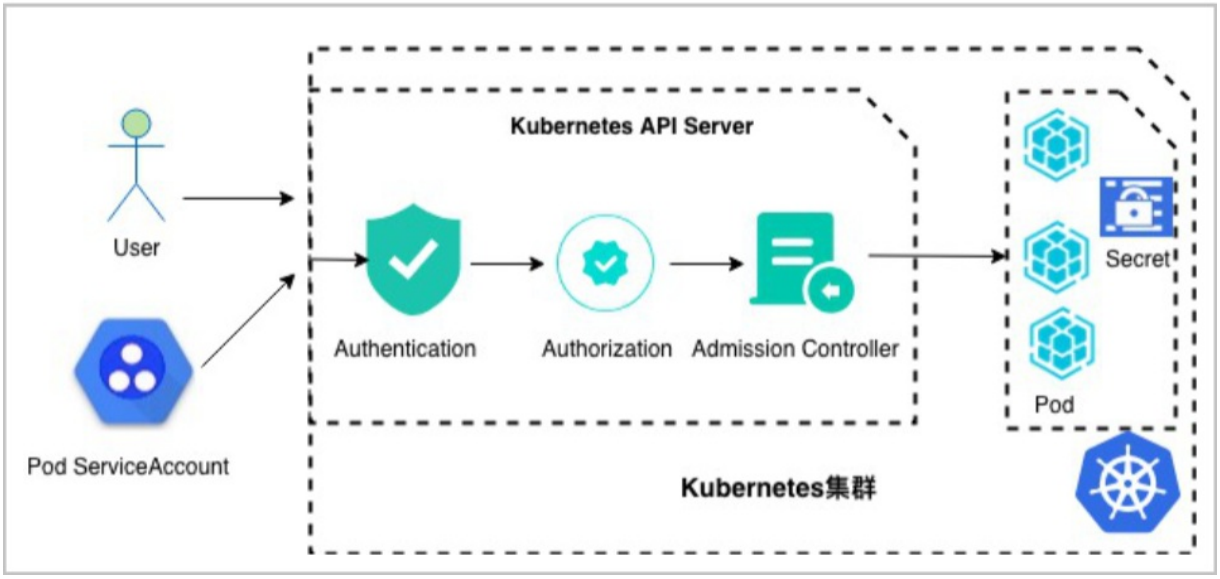
场景描述

本方案实践主要是通过一些实践示例来介绍用户对于在阿里云上使用Kubernetes集群服务的容器平台安全管控的实践验证与使用建议。

方案优势

- 容器集群部署快捷
- 授权与安全策略配置方便
- 丰富的安全控制实践介绍

业务架构



解决问题

- 容器集群API Server的安全访问控制
- 容器服务多租户场景下的授权管理
- 容器中的敏感信息数据的存储
- 容器服务集群安全策略配置管理

8.RAM账号权限管理

以电商网站场景为例介绍如何使用访问控制服务（RAM）进行账号权限管理。

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

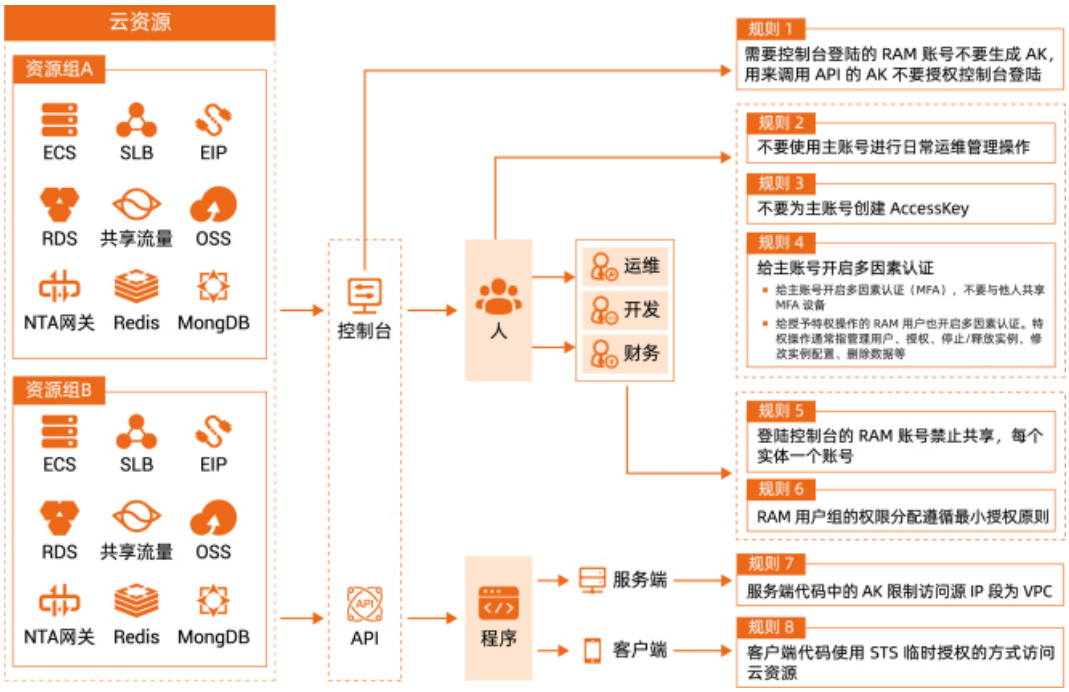
场景描述

介绍单账号体系下用户管理、资源分组、权限配置、访问控制的治理方法及原则。以某电商网站项目为例，根据研发、测试、生产环境划分及业务流程，使用阿里云访问控制服务RAM规划实现资源分组、账号用户体系、权限分配、安全加固、定期安全检查等措施的最佳实践。

解决问题

- 基于用户、用户组、角色建立用户体系及安全加固原则。
- 用户、程序使用用户/角色身份原则。
- 典型授权策略编写及授权配置示例。
- 云上资源分组管理实践。

部署架构图



9.RAM用户集成企业AD FS身份认证

企业AD用户与RAM用户映射，实现与阿里云的用户SSO。

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

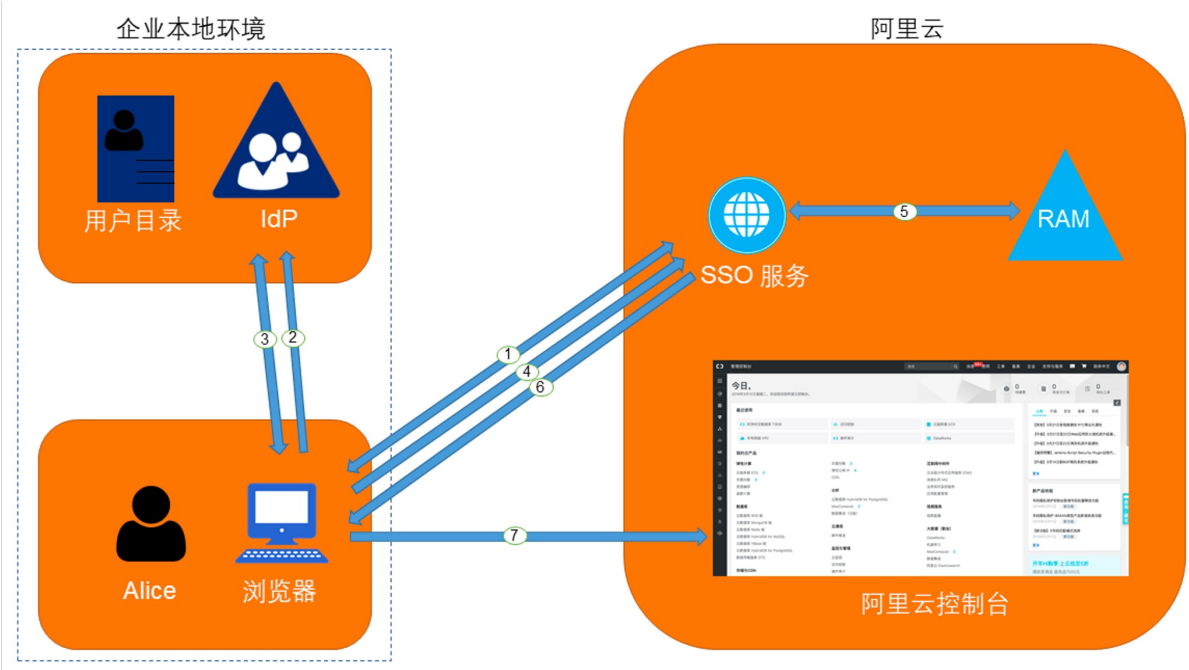
场景描述

介绍阿里云RAM集成Windows AD FS，使用企业AD对员工的身份认证及管理功能，配置RAM用户与AD用户的映射关系，实现企业员工使用企业AD域账号以单点登录（SSO）的方式访问阿里云控制台。

解决问题

- Windows AD域部署。
- Windows AD证书服务及Web部署。
- Windows AD FS部署。
- 阿里云角色SSO配置。
- AD FS集成RAM用户SSO。

部署架构图



10.数据库运维安全管理

通过数据管理DMS产品，对不同用户进行数据库、表、字段级别的细粒度授权，保障数据库运维安全。

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

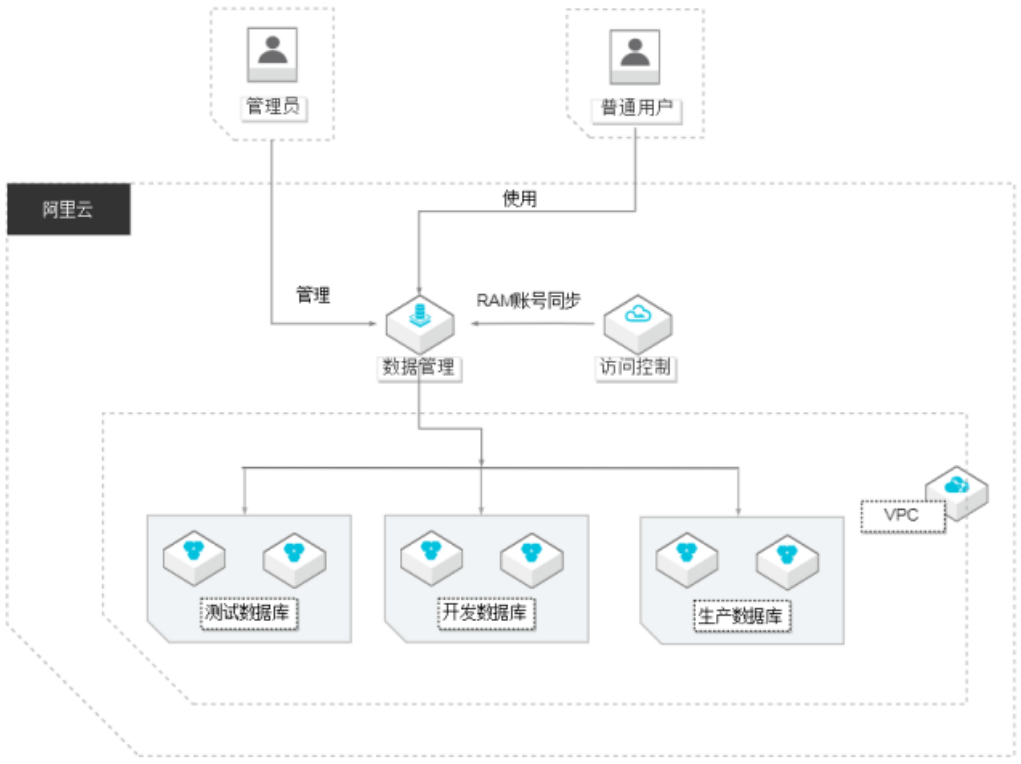
场景描述

企业的数据库数量比较多、使用的人比较多的情况下，因为不同角色的人访问数据库的权限是不一样的，这时候就需要有一个完整的数据库访问的授权方案，不同角色按需分配最小够用的权限。DMS的授权粒度可以是库、表、字段的维度。

解决问题

- 数据库细粒度授权。
- 权限申请和审批流程。
- 数据库里敏感数据脱敏。
- 数据库运维人员操作的事后审计。

部署架构图



11.AK防泄漏

正确使用AK可以有效降低安全风险，建议您尽量使用临时AK Token或最小粒度授权的子账号AK。

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

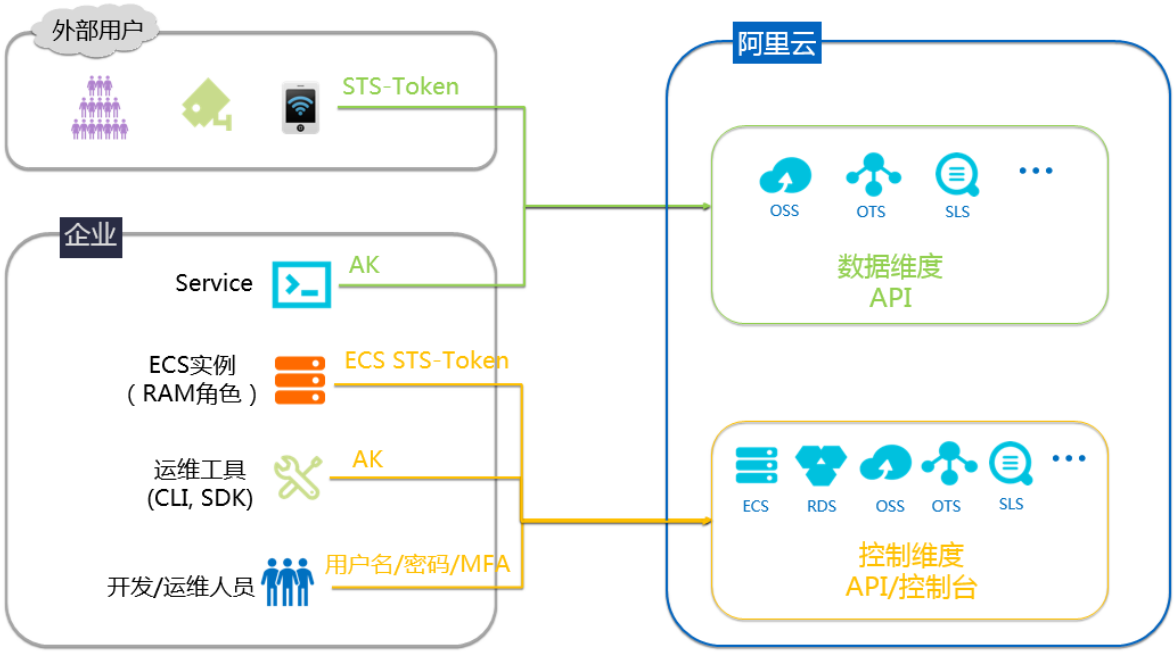
场景描述

用户名密码是开发运维人员访问阿里云控制台的凭据，AK是软件程序访问阿里云资源的凭据。 如果AK被泄露，那么会造成非常严重的后果， 例如：资源被释放导致业务不可用、大量服务器被创建用来挖矿等。采用合适的方式使用和保护AK，是每一个云客户都必须关注的问题。

解决的问题

- 避免AK被泄露
- 改进已经错误使用AK的方法

部署架构图



12.RAM角色集成企业AD FS身份认证

企业AD用户组与RAM角色映射，实现与阿里云的角色SSO。

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

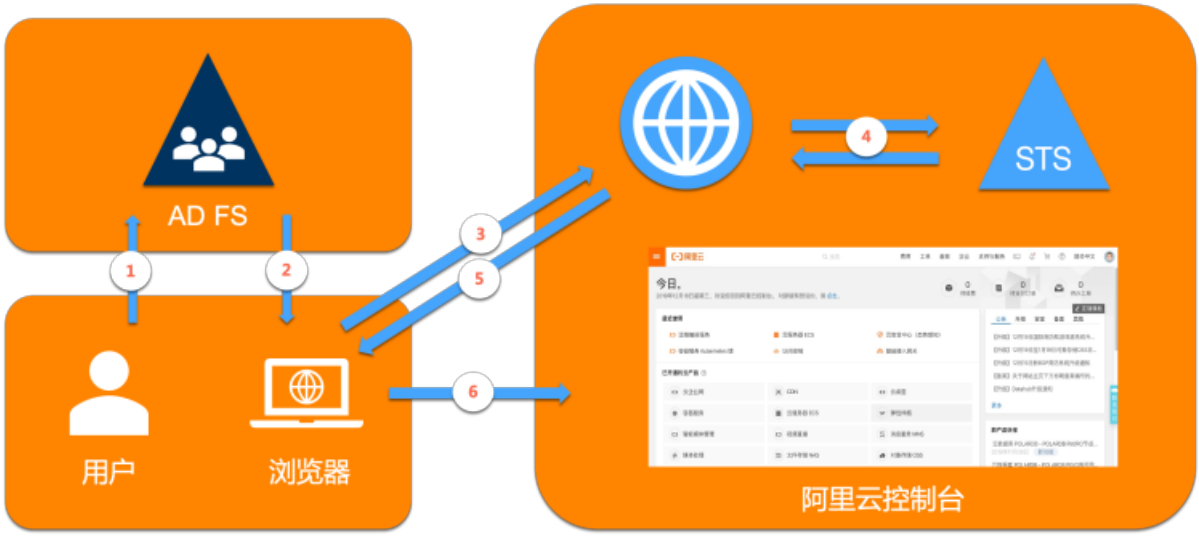
场景描述

介绍阿里云RAM集成Windows AD FS， 使用企业AD对员工的身份及权限管理功能，配置RAM角色与AD用户组的映射关系，实现企业员工使用企业AD域账号以单点登录（SSO）的方式访问阿里云控制台。

解决的问题

- Windows AD域部署
- Windows AD证书服务及Web部署
- Windows AD FS部署
- 阿里云角色SSO配置
- AD FS集成RAM角色SSO

部署架构图



选用的产品

- **访问控制**

  RAM 使您能够安全地集中管理对阿里云服务和资源的访问。您可以使用 RAM 创建和管理用户和组，并使用各种权限来允许或拒绝他们对云资源的访问。

  更多关于访问控制的介绍，参见访问控制产品详情页。

- **专有网络VPC**

  专有网络VPC帮助您基于阿里云构建出一个隔离的网络环境，并可以自定义IP 地址范围、网段、路由表和网关等；此外，也可以通过专线/VPN/GRE等连接方式实现云上VPC与传统IDC的互联，构建混合云业务。

  更多关于专有网络VPC的介绍，参见专有网络VPC产品详情页。

- **云服务器ECS**

  云服务器（Elastic Compute Service，简称ECS）是阿里云提供的性能卓越、稳定可靠、弹性扩展的IaaS（Infrastructure as a Service）级别云计算服务。云服务器ECS免去了您采购IT硬件的前期准备，让您像使用水、电、天然气等公共资源一样便捷、高效地使用服务器，实现计算资源的即开即用和弹性伸缩。阿里云ECS持续提供创新型服务器，解决多种业务需求，助力您的业务发展。

  更多关于云服务器ECS的介绍，参见云服务器ECS产品详情页。

13.传统企业业务上云基础安全

本文档提供传统企业业务上云后，如何在云上构建网络安全、主机安全、入侵检测、运维审计等可实操的最佳实践。

直达最佳实践

单击查看最佳实践详情

更多最佳实践

单击查看更多阿里云最佳实践

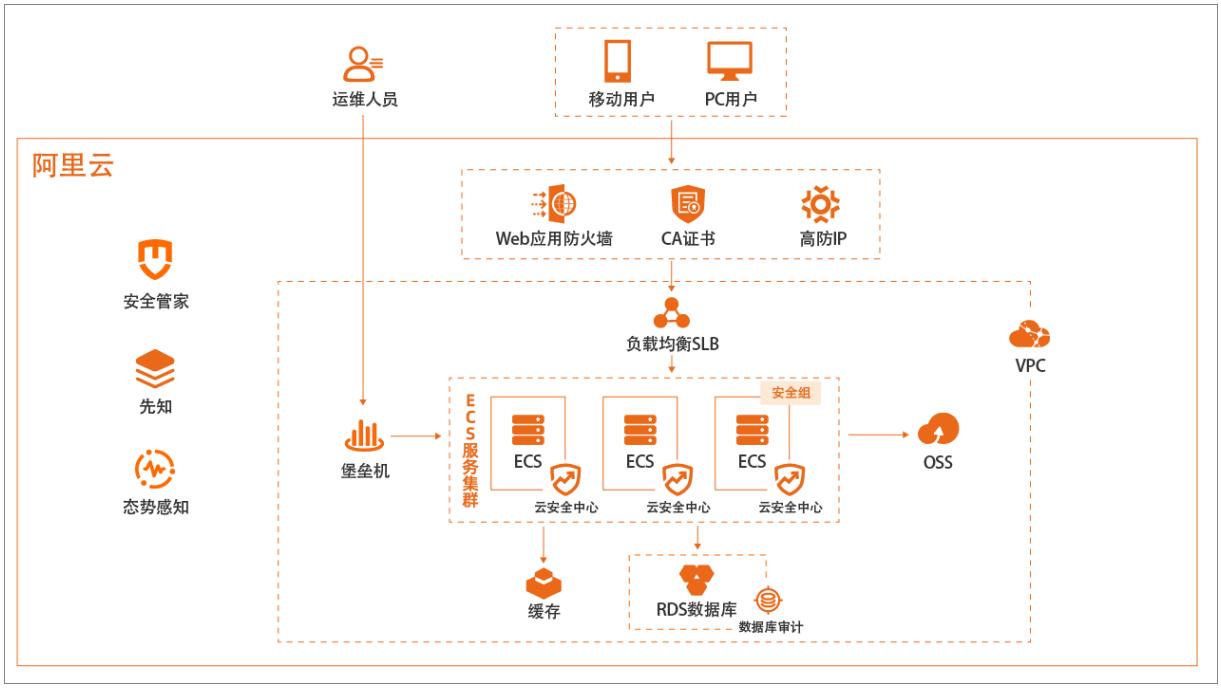
场景描述

越来越多的企业客户选择把自己的生产系统部署在公共云平台上，以满足自身业务的发展及弹性扩缩容、稳定性等方面的需求。如何在公共云 上构建基本的网络安全、主机安全、入侵检测、 运维审计等方案，是企业首选的最佳实践。

解决的问题

- 服务器安全、应用安全
- 网络安全、数据安全
- 安全审计、安全管理

部署架构图



选用的产品

- 云安全中心

云安全中心是一个实时识别、分析、预警安全威胁的统一安全管理系统，通过防勒索、防病毒、防篡改、合规检查等安全能力，帮助用户实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产和本地主机并满足监管合规要求。

更多关于云安全中心的介绍，参见云安全中心产品详情页。

- **Web应用防火墙**

  阿里云Web应用防火墙（WAF）对网站或者APP的业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。

  更多关于Web应用防火墙的介绍，参见Web应用防火墙产品详情页。

- **云防火墙**

  集中管理公网IP的访问策略，内置威胁入侵防御模块（IPS），支持失陷主机检测、主动外联行为的阻断、业务间访问关系可视，留存6个月网络流量日志，等保必备。

  更多关于云防火墙的介绍，参见云防火墙产品详情页。

- **SSL证书**

  在云上签发各品牌数字证书，实现网站HTTPS化，使网站可信，防劫持、防篡改、防监听、安全加密。统一生命周期管理，简化证书部署，一键分发到CDN、负载均衡、OSS等其它云上产品。

  更多关于SSL证书的介绍，参见SSL证书产品详情页。

- **数据库审计**

  智能解析数据库通信流量，细粒度审计数据库访问行为，帮助企业精准识别、记录云上数据安全威胁，为云端数据库提供全方位的安全、诊断、维护及合规能力。

  更多关于数据库审计的介绍，参见数据库审计详情页。

- **堡垒机**

  集中管理资产权限，全程记录操作数据，实时还原运维场景，助力企业用户构建云上统一、安全、高效运维通道；保障云端运维工作权限可管控、操作可审计、合规可遵从。

  更多关于堡垒机的介绍，参见堡垒机产品详情页。

14.电商网站业务安全

本文档介绍了使用阿里云产品实现电商网站运营期间的安全防护，包括爬虫风险管理、DDoS防御、风险管理产品的能力及操作。

最佳实践

点击查看最佳实践详情

更多最佳实践

单击查看更多阿里云最佳实践

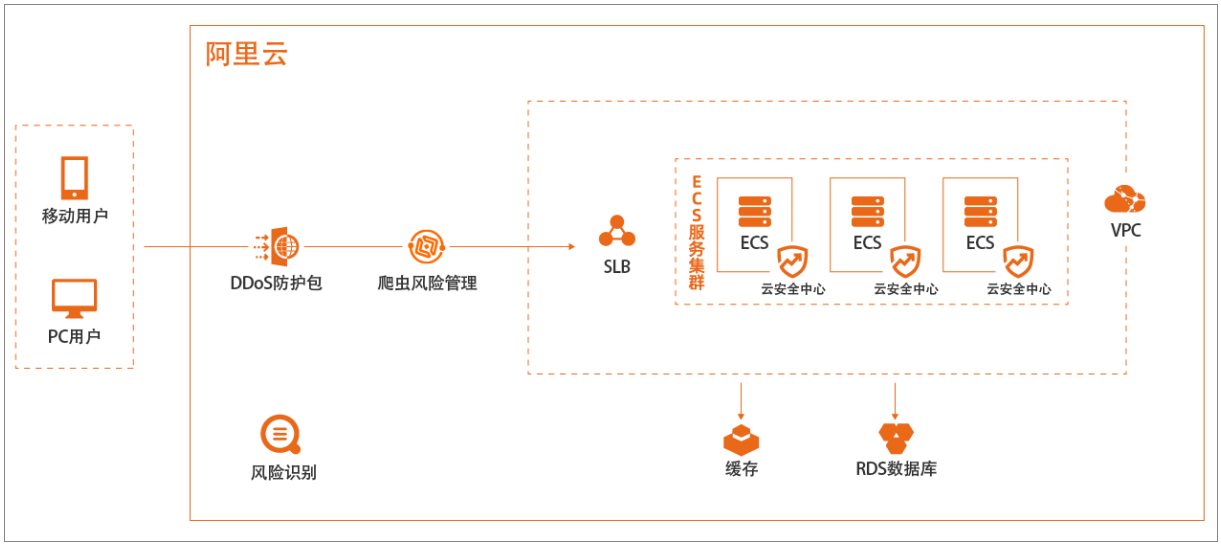
场景描述

业务运营活动是电商行业开展业务必不可少的手段，但大流量带来的系统可用性、优惠券带来的“薅羊毛”等问题屡见不鲜，这些都会影响到运营效果、甚至出现负面影响。阿里云基于阿里巴巴集团电商业务多年的运营经验，为云上客户提供完整的电商网站运营期间的防护方案。

解决的问题

- 保障业务运维活动系统稳定运行
- 防止“薅羊毛”
- 运营优惠给到真正的客户

部署架构图



15.混合云多云统一安全

企业业务部分上云或部署在多个公共云平台，通过公共云安全统一进行安全管理和防护，满足等保合规要求。

直达最佳实践

点击查看最佳实践详情

更多最佳实践

单击查看更多阿里云最佳实践

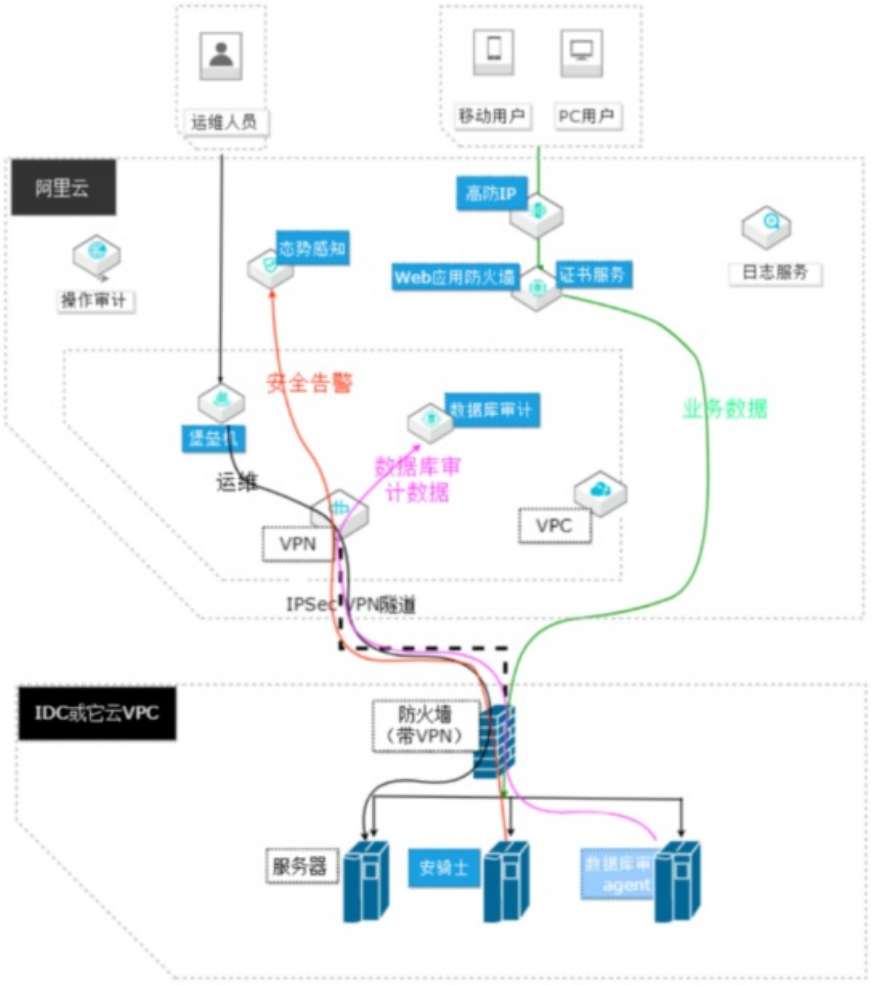
场景描述

有些客户的业务系统部分上云、或者还没上云，但想使用阿里云公共云的安全服务；或者业务系统部署在多个云平台上，想使用阿里云的安全来提供统一服务。

解决的问题

- 通过阿里云的安全产品和服务，统一管理阿里云、IDC和非阿里云资产。
- 满足混合云、多云的等保需求。

部署架构图


运维人员
移动用户
PC用户
阿里云
高防IP
态势感知
Web应用防火墙
证书服务
日志服务
操作审计
安全告警
数据库审计
堡垒机
业务数据
运维
数据库审计数据
VPC
VPN
IPSec VPN隧道
IDC或它云VPC
防火墙（带VPN）
服务器
安骑士
数据库审agent

16.企业上云等保二级合规

云原生高性价比的等保二级最佳实践，包括详细的解决方案和网络架构，涉及到云安全产品的开通配置及攻防演练。

直达最佳实践

点击查看最佳实践详情

更多最佳实践

单击查看更多阿里云最佳实践

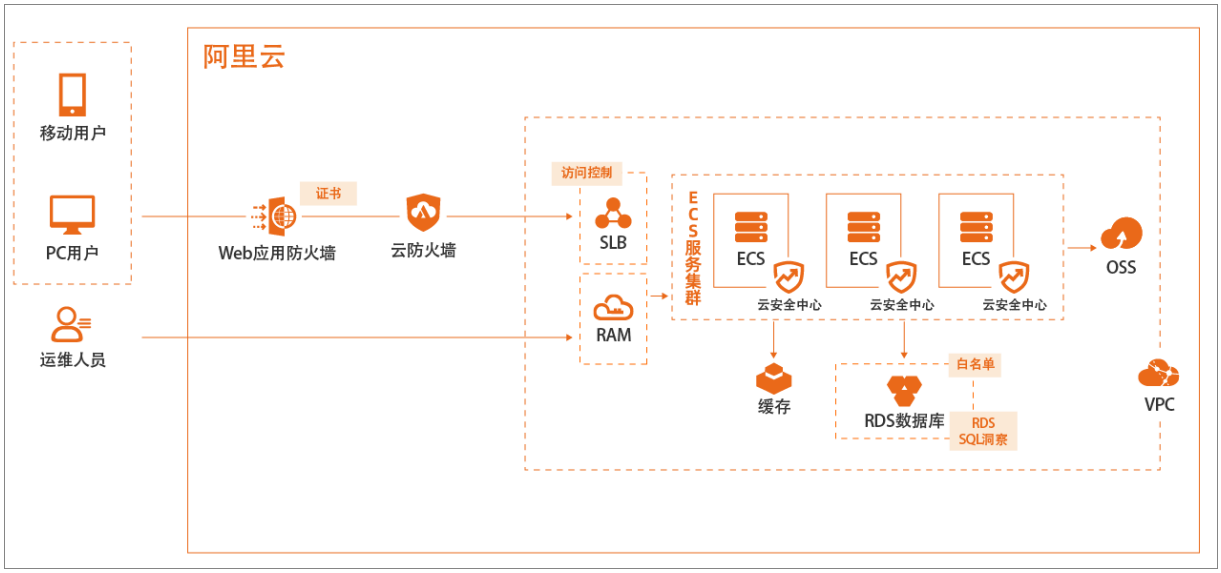
场景描述

阿里云安全帮助您快速、省心地通过等保合规。 在阿里云，您可享受一站式等保测评，包括完备的攻击防护、数据审计、数据备份与加密、安全管理服务。可充分利用云平台的免费管理软件，包括RAM、ActionTrail、云监控等，满足等保2.0需求。

解决的问题

- 等保2.0合规要求
- 云上安全体系建设

部署架构图



17.企业上云等保三级合规

云原生高性价比的等保三级最佳实践。在等保二级基础上，叠加必要的安全产品及高可用架构，满足三级要求。

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。

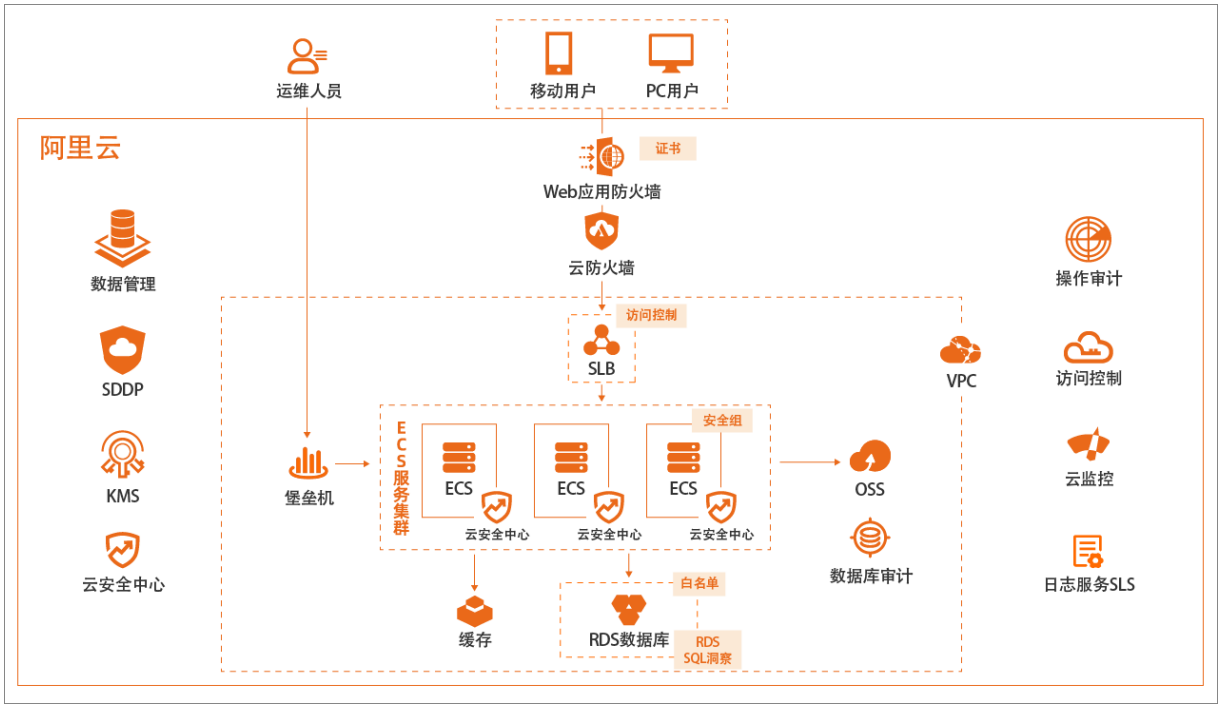
场景描述

网络安全法中明确要求国家实行网络安全保护制度，网络运营者有义务履行等级保护制度要求。阿里云除了提供满足等保合规要求的云平台外，还为用户的应用系统提供完整的云原生、高性价比的等保三级解决方案。

解决的问题

- 等保2.0合规要求
- 云上高等级安全体系建设

部署架构图



18.企业上云数据安全

使用SDDP产品进行敏感数据发现和分级分类，然后对高级别敏感数据进行按需加密存储。

直达最佳实践

点击查看最佳实践详情

更多最佳实践

单击查看更多阿里云最佳实践

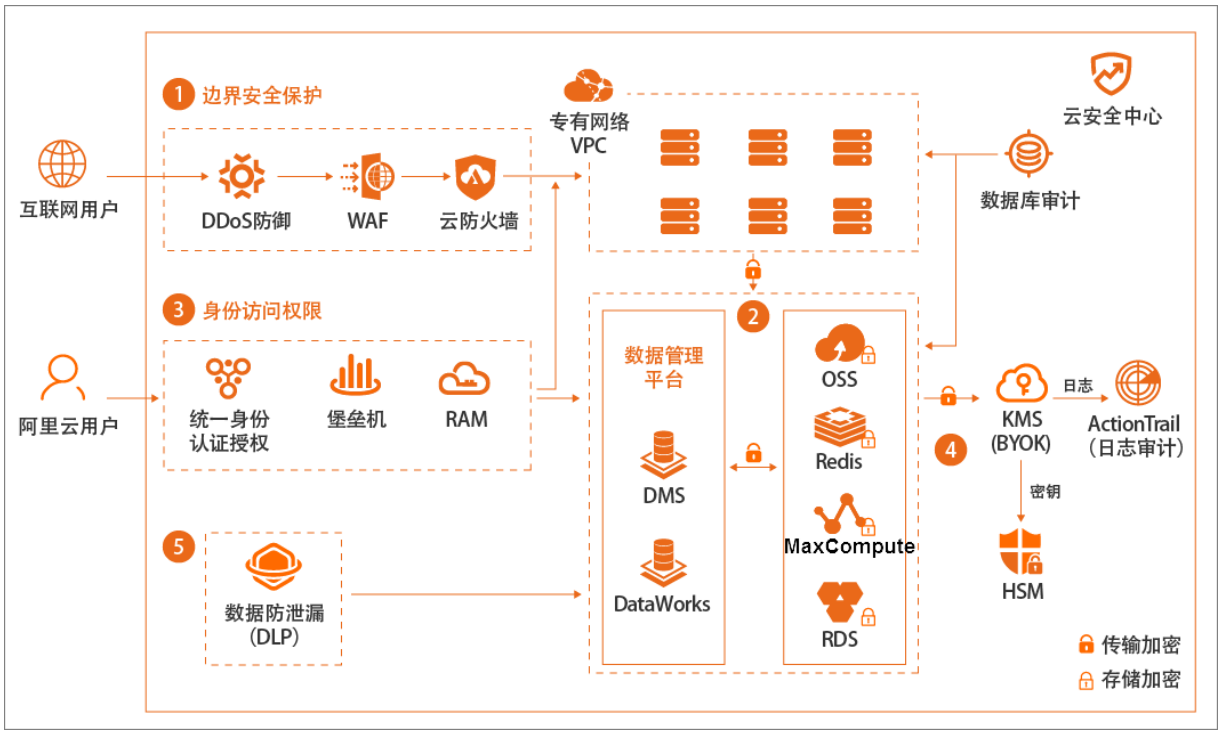
场景描述

企业是否选择上公共云或者哪些系统、数据上公共云，数据安全是重要的考虑因素之一。本最佳实践重点在于介绍狭义的数据加密存储安全范畴，即首先使用SDDP产品进行敏感数据发现和分级分类，然后对高级别敏感数据按根据需要和不同类型的全链路加密存储。

解决的问题

- 帮助客户发现敏感数据
- 对敏感数据进行分类、分级
- 不同级别的数据如何进行加密
- 数据具体如何进行加密

部署架构图



19.图片违规检测和跨国际区域备份

本文档介绍了如何将图片、附件等静态资源上传到阿里云OSS、并基于阿里云内容安全对OSS图片进行违规检测和人工审核的最佳实践。

直达最佳实践

点击查看最佳实践详情

更多最佳实践

单击查看更多阿里云最佳实践

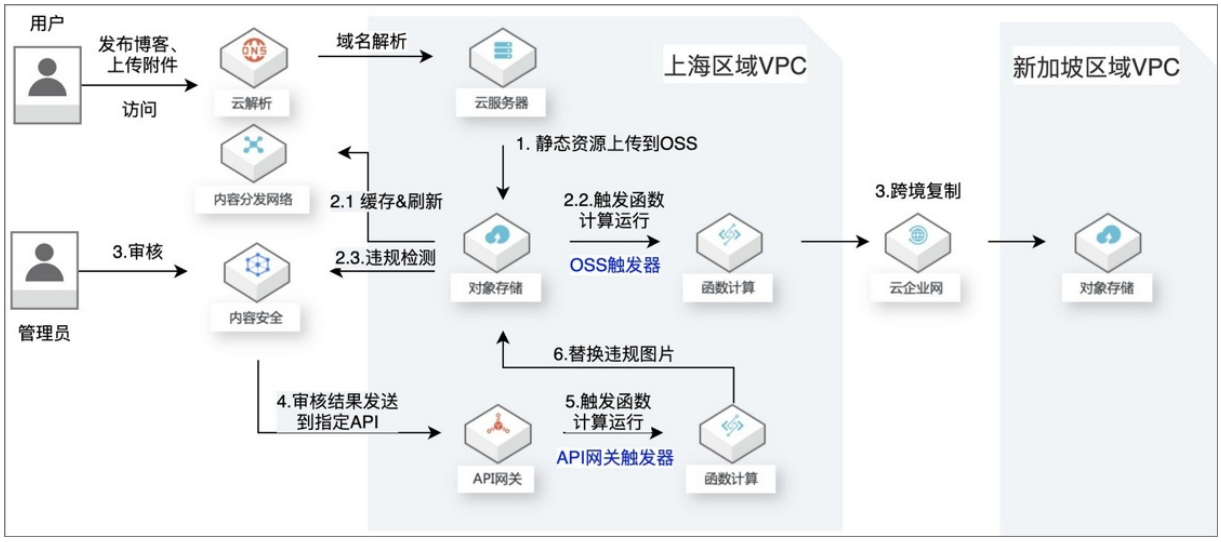
场景描述

本实践通过搭建WordPress博客系统，向用户展示如何将图片、附件等静态资源上传到阿里云OSS，并通过阿里云CDN进行加速。同时演示了基于函数计算托管函数完成OSS存储空间中数据的跨境复制、基于阿里云内容安全对OSS图片进行违规检测和人工审核的流程。

解决的问题

- 静态资源（图片、视频等）CDN访问加速和刷新
- OSS对象跨国际区域进行复制
- OSS静态图片、视频文件的内容检测（涉黄、涉暴、涉政等）和处理

部署架构图



20.网络安全升级支持IPv6

在现有WAF和高防IP作为网络安全架构基础上，如何升级支持IPv6，云上和线下IDC业务都支持，满足合规要求。

直达最佳实践

点击查看最佳实践详情

更多最佳实践

单击查看更多阿里云最佳实践

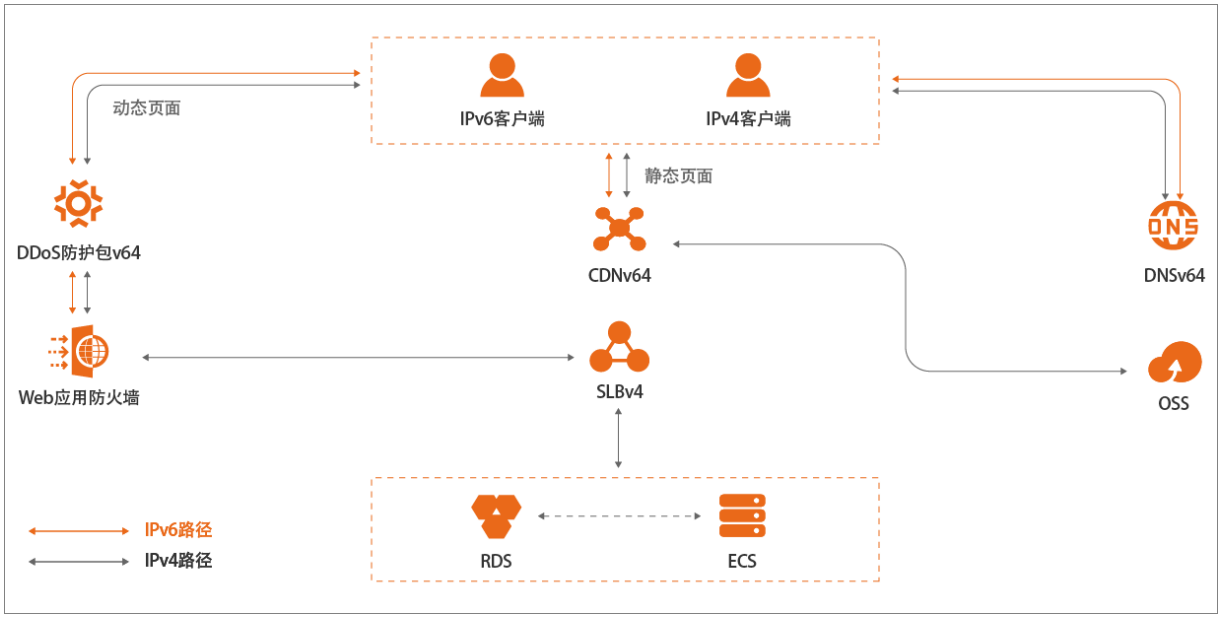
场景描述

基础设施支持IPv6已经上升到国家战略。阿里云公共云基础设施为云上客户系统支持IPv6提供了完整的解决方案。本最佳实践是在现有WAF和高防IP作为网络安全架构的基础上，介绍了如何升级支持IPv6，同时满足云上和线下IDC需求，以及满足合规要求。

解决的问题

- 网络支持IPv6
- 支持V4和V6双栈
- 满足监管合规要求

部署架构图



21.云平台内部操作透明化

云平台对用户云产品规格和不合格内容处罚操作，通过审计产品透明给客户。

直达最佳实践

点击查看最佳实践详情

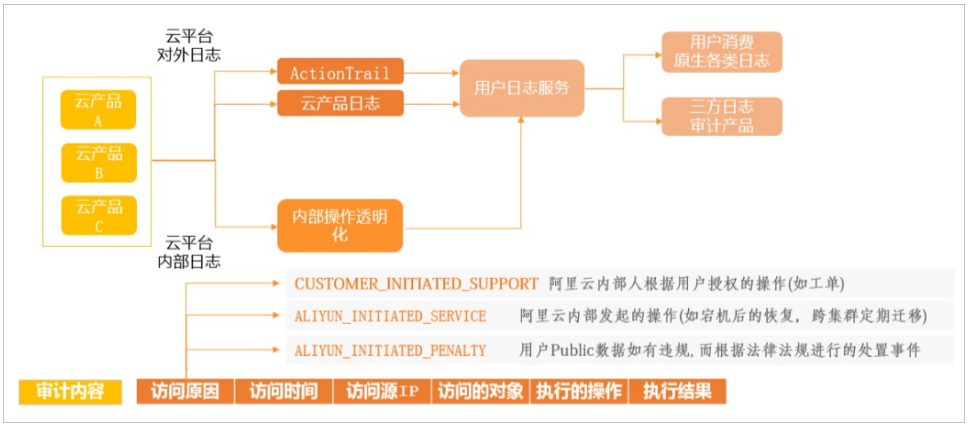
更多最佳实践

点击查看更多阿里云最佳实践

场景描述

云平台基于用户的请求或监管要求等，进行的内部操作对用户如果不可见，用户可能会担心自己的数据是否收到了影响或者是否被触碰了，影响用户对平台的信任。

业务逻辑图



解决问题

- 内部操作对用户可见。
- 增强用户对平台的可信度。