阿里云
专有云Enterprise版

安全白皮书

产品版本：V3.1.0

文档版本：20171129

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
	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。	 **禁止**： 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **说明**： 导出的数据中包含敏感信息，请妥善保存。
	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。	**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。	单击 **确定**。
courier字体	命令。	执行 cd /d C:/windows 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。	swich *{stand | slave}*

目录

法律声明 I
通用约定 I
1 安全白皮书介绍 1
2 安全责任共担 2
2.1 阿里云安全责任 2
2.2 用户安全责任 3
3 安全合规和隐私 4
3.1 安全合规 5
3.2 隐私保护 7
4 阿里云安全架构 8
4.1 云平台安全架构 8
4.1.1 硬件安全 8
4.1.2 虚拟化安全 9
4.1.3 云产品开发安全 10
4.2 云用户侧安全架构 11
4.2.1 账户安全 11
4.2.2 主机安全 12
4.2.3 应用安全 13
4.2.4 网络安全 13
4.2.5 数据安全 14
4.2.6 安全运营 16
5 云产品安全 17
5.1 云服务器ECS 17
5.1.1 产品介绍 17
5.1.2 实例安全 17
5.1.2.1 宿主机的操作系统安全 17
5.1.2.2 实例的操作系统（Guest OS）安全 17
5.1.2.3 镜像安全 17
5.1.2.4 防止IP/MAC/ARP欺骗 18
5.1.3 存储安全 18
5.1.3.1 Chunk 18
5.1.3.2 三份副本的原理 18
5.1.3.3 数据保护机制 19
5.1.4 网络安全 19
5.1.4.1 实例的安全隔离 19
5.1.4.2 安全组 20

5.2 对象存储OSS....20
5.2.1 什么是对象存储OSS....20
5.2.2 身份验证....21
5.2.3 访问控制....21
5.2.4 RAM和STS....22
5.2.5 高可用性....22
5.2.6 租户隔离....22
5.2.7 服务器端加密....22
5.2.8 客户端加密....23
5.2.9 数据传输安全....23
5.2.10 数据传输完整性....23
5.2.11 访问日志记录....23
5.2.12 跨资源共享....23
5.2.13 防盗链....24
5.3 表格存储TableStore....24
5.3.1 什么是表格存储....24
5.3.2 身份认证....24
5.3.3 高可用性....24
5.3.4 强一致性....25
5.3.5 监控集成....25
5.3.6 RAM 和 STS 支持....25
5.3.7 VPC 支持....25
5.4 文件存储NAS....25
5.4.1 产品介绍....25
5.4.2 产品安全和可靠性方案....25
5.4.2.1 访问控制....25
5.4.2.2 RAM支持....25
5.4.2.3 权限组支持....26
5.4.2.4 高可用性....27
5.5 云数据库RDS版....27
5.5.1 产品概述....27
5.5.2 租户隔离....28
5.5.3 高可用性....28
5.5.4 访问控制....28
5.5.5 网络隔离....28
5.5.6 SQL审计....29
5.5.7 备份恢复....29
5.5.8 软件升级....29
5.5.9 RAM和STS支持....29
5.5.10 最佳实践....29
5.6 云数据库Redis版....30

5.6.1 产品介绍.....30
5.6.2 产品安全和可靠性方案.....30
5.6.2.1 访问控制.....30
5.6.2.2 高可用架构.....31
5.6.2.3 软件升级.....32
5.6.2.4 服务授权.....32
5.7 云数据库Memcache版.....33
5.7.1 产品介绍.....33
5.7.2 产品安全和可靠性方案.....33
5.7.2.1 访问控制.....33
5.7.2.2 高可用架构.....33
5.7.2.3 软件升级.....35
5.7.2.4 服务授权.....35
5.8 负载均衡SLB.....36
5.8.1 概述.....36
5.8.2 高可用性.....36
5.8.3 防御CC攻击.....36
5.8.4 访问控制.....36
5.8.5 日志功能.....36
5.8.6 HTTPS.....36
5.8.7 RAM和STS支持.....37
5.8.8 健康检查.....37
5.8.9 最佳实践.....37
5.9 专有网络VPC.....37
5.9.1 概述.....37
5.9.2 安全隔离.....37
5.9.3 自定义网络.....37
5.9.4 防火墙.....38
5.9.5 网络访问控制.....38
5.9.6 弹性外网IP.....38
5.9.7 路由器接口.....38
5.9.8 NAT 网关.....38
5.9.9 RAM和STS支持.....38
5.10 日志服务.....39
5.10.1 高可用性.....39
5.10.2 离线归档.....39
5.10.3 身份认证.....39
5.10.4 RAM支持.....39
5.11 企业级分布式应用服务EDAS.....39
5.11.1 产品介绍.....39
5.11.2 安全和可靠性方案.....39

5.11.2.1 权限控制 39
5.11.2.2 高可用架构 40
5.11.2.3 软件升级 41
5.11.2.4 服务授权 41
5.12 分布式关系型数据库DRDS 41
5.12.1 产品介绍 41
5.12.2 产品安全和可靠性方案 41
5.12.2.1 访问控制 41
5.12.2.2 高可用架构 43
5.12.2.3 软件升级 43
5.12.2.4 服务授权 43
5.13 消息队列MQ（铂金版） 44
5.13.1 产品介绍 44
5.13.2 产品安全和可靠性方案 44
5.13.2.1 访问控制 44
5.13.2.2 高可用架构 45
5.13.2.3 软件升级 46
5.14 企业实时监控服务ARMS 46
5.14.1 产品介绍 46
5.14.2 产品安全和可靠性方案 46
5.14.2.1 访问控制 46
5.14.2.2 数据隔离 47
5.14.2.3 QoS保障策略 47
5.14.2.4 高可用和容灾保障 48
5.14.2.5 软件升级 50
5.15 全局事务服务GTS 50
5.15.1 产品介绍 50
5.15.2 产品安全和可靠性方案 50
5.15.2.1 访问控制 50
5.15.2.2 流量控制 51
5.15.2.3 数据多份落盘 51
5.15.2.4 集群容灾 51
5.15.2.5 软件升级 51
5.16 云服务总线CSB 52
5.16.1 产品介绍 52
5.16.2 产品安全和可靠性方案 52
5.16.2.1 访问控制 52
5.16.2.2 流量控制 53
5.16.2.3 容灾 54
5.16.2.4 软件升级 54
5.17 MaxCompute 54

5.17.1 安全体系.....54
5.17.2 身份认证.....55
5.17.3 授权管理.....55
5.17.4 跨项目空间的资源分享.....56
5.17.5 数据保护机制（Project Protection）.....56
5.18 EMR.....56
5.18.1 产品介绍.....56
5.18.2 产品安全和可靠性方案.....56
5.18.2.1 用户认证-Kerberos.....56
5.18.2.1.1 简介.....56
5.18.2.1.2 在E-MapReduce中的应用.....58
5.18.2.1.3 使用说明.....59
5.18.2.1.3.1 认证开启.....59
5.18.2.1.3.2 模式选择.....59
5.18.2.1.3.3 添加用户.....60
5.18.2.1.3.4 导出keytab.....60
5.18.2.2 权限控制.....60
5.18.2.2.1 新建用户与用户组.....60
5.18.2.2.2 Hadoop YARN.....61
5.18.2.2.3 Hadoop HDFS.....62
5.18.2.2.3.1 资源被创建者本人读写.....62
5.18.2.2.3.2 资源被组读写.....62
5.18.2.2.3.3 资源被指定用户读写.....63
5.18.2.2.3.4 资源被指定组读写.....63
5.18.2.2.3.5 资源临时目录.....64
5.18.2.2.4 Hive.....64
5.18.2.2.5 HBase.....64
5.18.2.2.6 Knox.....65
5.18.2.2.6.1 使用集群中的LDAP服务.....65
5.18.2.2.6.2 使用自有LDAP服务.....66
5.18.2.2.7 Hue.....66
5.18.2.3 附录.....66
5.18.2.3.1 附录一.....66
5.18.2.3.2 附录二.....67
6 专有云云盾.....71
6.1 云盾基础版.....71
6.2 云盾高级版.....72

1 安全白皮书介绍

数据安全和用户隐私是阿里云专有云最重要的原则，阿里云致力于打造公共、开放、安全的专有云云计算服务平台。通过技术创新，不断提升计算能力与规模效益，将云计算变成真正意义上的基础设施。

阿里云专有云竭诚为您提供稳定、可靠、安全、合规的云计算基础服务，帮助保护您的系统及数据的可用性、机密性和完整性。

本白皮书介绍了阿里云专有云云安全体系，主要包括下列内容：

- 安全责任共担
- 安全合规和隐私
- 专有云平台架构安全
- 专有云各产品提供的安全功能
- 专有云云盾提供的安全服务

同时，本白皮书提供了安全使用阿里云产品和云盾安全产品的最佳实践来帮助您更好地使用阿里云专有云平台以及理解安全控制整体环境。

2 安全责任共担

基于专有云平台的用户应用，其安全责任由双方共同承担：阿里云确保住专有云平台的安全性，用户负责基于专有云平台构建的应用系统的安全。

阿里云

阿里云负责专有云飞天分布式云操作系统及之上的各种云服务产品的安全控制、管理和运营，从而为用户提供高可用和高安全的云服务平台。

同时，专有云基于阿里巴巴集团多年攻防技术积累，为用户提供云盾安全服务，保障用户的应用系统安全。

用户

用户负责以安全的方式配置和使用云服务器（ECS）、数据库（RDS）实例及其他云产品，并基于这些云产品以安全可控的方式构建自己的应用。

用户可使用云盾安全服务或者阿里云安全生态中的第三方安全厂商的安全产品为其应用系统提供安全防护。

2.1 阿里云安全责任

阿里云负责分布式云操作系统及云服务产品安全，并为用户提供保护云端应用及数据的技术手段。

- 保障专有云云平台自身安全
- 保障专有云云平台硬件、软件和网络安全，如操作系统及数据库的补丁管理、网络访问控制、DDoS防护、灾难恢复等
- 及时发现专有云云平台的安全漏洞并修复，且修复漏洞过程不影响业务可用性
- 通过与外部第三方独立安全监管与审计机构合作，对阿里云专有云进行安全合规与审计评估
- 云账户支持主子账号、多因素认证、分组授权、细粒度授权、临时授权
- 为用户提供保护云端信息系统的技术手段
- 为用户提供安全审计手段
- 为用户提供数据加密手段
- 为用户提供云盾安全服务

2.2 用户安全责任

用户基于阿里云提供的专有云平台构建自己的云端应用系统，综合运用专有云产品的安全功能、云盾安全服务以及安全生态提供的第三方安全产品保护自己的业务系统。

用户应妥善管理专有云账户，使用访问控制服务（Resource Access Management，RAM）为每个运维管理人员分配独立的RAM用户账号，授予完成运维管理工作需要的最小权限，通过群组授权实现职责分离。阿里云建议用户为重要账户启用多因素（MFA）认证，使用操作审计服务记录管理控制台操作及OpenAPI调用日志，并使用阿里云加密服务对敏感数据进行加密。

对于专有云提供的云服务器（ECS）、专有网络（VPC）服务的实例完全由用户控制，用户应妥善管理实例并进行安全配置。例如，用户应及时加固租用的云服务器操作系统、升级补丁，配置安全组防火墙进行网络访问控制。

对于专有云提供的其他服务，例如云数据库（RDS）、大数据计算服务（MaxCompute），用户只需要管理这些服务的账户及授权，并使用这些服务提供的安全功能。例如，配置RDS服务的源IP白名单。

3 安全合规和隐私

阿里云的安全流程机制已经得到国内外相关权威机构的认可，阿里云将阿里巴巴集团基于互联网安全威胁的长期对抗经验融入到云平台的安全防护中，将众多的合规标准融入云平台合规内控管理和产品设计中，同时广泛参与各类云平台相关的标准制定并贡献最佳实践，并通过独立的第三方评估验证。至目前为止，阿里云一共获得了海内外十余家机构的认证，是亚洲资质最全的云服务商。

阿里云具备表 *3-1:* 阿里云获得的资质中所列出的资格认证：

表 3-1: 阿里云获得的资质

资质	说明
ISO 27001	信息安全管理体系国际认证，从数据安全、网络安全、通信安全、操作安全等各个方面充分证明阿里云平台履行的安全职责。
CSA STAR	云安全管理体系国际认证，阿里云获得全球首个金牌。
ISO 20000	IT服务管理体系认证，意味着阿里云建立了标准的服务流程，并严格执行，云平台服务规范化，提高效率并降低IT整体风险。
ISO 22301	业务连续性管理体系认证，意味着阿里云具备业务连续性计划、灾备建设和定期演练，提升云平台稳定性。
等级保护测评（四级）	阿里云金融云成为全国首个通过云计算等级保护四级测评的云平台，意味着阿里云金融云正稳步成为国家关键信息基础设施。
中央网信办党政部门云服务网络安全审查	阿里云是全国首批通过网信办云安全审查的社区云的服务商中，唯一通过增强级别审查（500多项检查点）的服务商。
工信部云服务能力标准测试	云产品国家实验室认证是基于国家标准的唯一产品级分级认证。
支付卡行业数据安全标准（PCI DSS）	PCI DSS主要关注支付卡信息在组织范围内全生命周期的管理和控制，包括产生 / 进入、传输、存储、处理和销毁等。
MTCS T3	新加坡云服务商安全最高等级认证，意味着阿里云具备参与新加坡政府项目的能力。

资质	说明
服务组织控制（SOC)审计认证	阿里云通过了SOC1、2的TYPEI、TYPEII、SOC3审计。
TRUSTe	阿里云国际站通过美国企业隐私标准认证，标志着阿里云采集、使用、管理和销毁个人信息的合规性。
HIPAA	阿里云支持HIPAA的业务伙伴协议以满足客户的需求，遵守美国健康保险可携性和责任法案，以保护健康信息的隐私和安全。
MPAA	阿里云遵守美国电影协会(MPAA)的最佳实践指引。
PDPA	阿里云遵守新加坡个人信息保护要求。
Trusted Cloud会员	阿里云成为德国联邦经济和能源部推动的Trusted Cloud会员。
SCOPE云守则创始会员	阿里云作为创始会员积极参与欧盟机构SCOPE，为GDPR实施准备的云行为准则标准。
发起"数据保护倡议"	中国云计算服务商首个"数据保护倡议"，明确数据所有权，以及阿里云的责任和义务。
发布《阿里云数据安全白皮书》	通过完善的数据安全管理和先进的技术支撑实现对用户数据安全的承诺。

3.1 安全合规

阿里云依据标准和行业最佳实践不断完善自身的管理与机制，通过了一系列的标准认证、三方审计以及自评估，力求更好地向用户展示阿里云的合规实践。

阿里云面对不同角度、不同行业、不同地区的合规需求，整体合规工作可以划分为如下几类：

管理体系合规

这些合规认证体现了阿里云成熟的管理机制和遵从的行业最佳实践：

- ISO 27001：信息安全管理体系
- ISO 20000：IT服务管理体系
- ISO 22301：业务可持续性管理体系
- CSA STAR：云服务安全的成熟度模型
- 等级保护测评（四级）

- 中国CNAS云计算国家标准测试

体系化合规报告

这些合规认证展示了阿里云云平台管控的完整性和有效性，包括体系控制是否持续有效、职责分离是否准确、运维操作审计是否完善等。

- PCI-DSS：支付卡行业数据安全标准
- MPAA：美国电影协会（MPAA）的最佳实践指引
- TRUSTe：TRUSTe企业隐私认证
- SOC 1/2 TYPE II: 服务组织控制 (SOC) 报告是阿里云邀请第三方机构出具的一系列独立的第三方检查报告，证明阿里云关键合规性控制和目标的持续有效性。这些报告的目的是帮助用户和用户的审计机构了解支持运营和合规性的控制措施。

  阿里云SOC 报告分为三种类型：

  - SOC 1 TYPE II： 针对财报的内控报告
  - SOC 2 TYPE II：安全性、可用性与机密性报告
  - SOC 3：安全性、可用性与机密性报告

法务合规

在不同地区开展云服务时，符合当地的法律法规是首要条件，由于法务合规的独特性，无法完全证书或审计报告的形式来体现。

- HIPAA：阿里云支持HIPAA的业务伙伴协议（BAA）以满足客户的需求，遵守美国健康保险可携性和责任法案（HIPAA），以保护健康信息的隐私和安全。
- GDPR ：阿里云在努力满足欧盟数据保护法规的同时也致力于为阿里云的客户和伙伴提供支持。

其它

部分无法通过上述的三种形式展现的合规认证。阿里云一直致力协助各个地区的监管机构建立和完善标准，分享阿里云的最佳实践。

- MTCS：多层云安全MTCS是由新加坡政府的新加坡资讯通讯发展管理局发起，新加坡标准、生产力与创新局推出的云安全标准。其安全认证分为三个层次，其中阿里云得到第三级，为最高、最安全。

3.2 隐私保护

阿里云个人信息处理原则：用户对所有提供给阿里云的个人信息拥有所有权和控制权。

每个用户在使用阿里云服务的时候，出于信任将最宝贵的个人信息托付给我们。阿里云也致力于保护每个用户的个人信息，并严格保障在用户期望范围内使用。阿里云在隐私政策方面对于公众完全透明，可以参考阿里云官网的隐私政策。同时，阿里云采用各种技术手段确保用户的个人信息仅存在于阿里云业务范围。

阿里云的信任中心提供了全面的合规信息，希望可以帮助用户更好地理解阿里云在合规方面的各种实践，并希望用户不仅可以一如既往地信任阿里云，也可以从阿里云的实践中获取合规方面的经验，与我们一起提高全球范围内的合规能力。同时，阿里云与TrustArc合作，为云上客户提供隐私合规服务。

在此，阿里云再一次声明，阿里云致力于保护世界各地用户的个人信息，并遵守经营业务市场所属国家或地区的适用法律。

阿里云的隐私政策可以在官方网站上找到， 任何隐私相关问题都可以通过我们的信任中心网页提交。

阿里云官方隐私政策： https://www.alibabacloud.com/help/faq-detail/42425.html

4 阿里云安全架构

阿里云提供了多个层面的纵深防御安全体系，包括硬件安全、虚拟化安全、云产品安全等云平台层面的安全架构保障；以及账户安全、主机安全、应用安全、网络安全、数据安全、安全运营等云用户层面的安全架构保障。

4.1 云平台安全架构

阿里云云平台的安全架构主要包括了硬件安全、虚拟化安全以及云产品开发安全三个重要组成部分。

4.1.1 硬件安全

硬件固件安全

硬件固件是云计算安全依赖的安全基础，为了保障硬件固件安全，阿里云对底层硬件固件进行加固，其中包括硬件固件基线扫描、高性能GPU实例保护、BIOS固件验签、BMC固件保护。

- **硬件固件基线扫描**：定期对硬件和固件基本信息及相应版本进行扫描，检测可能的异常硬件固件信息。
- **高性能GPU实例保护**：通过对开放给用户虚拟机的GPU关键寄存器保护，确保用户虚拟机除了进行高性能计算之外，无法篡改GPU的固件程序等重要资源。
- **BIOS固件验签**：确保只有阿里云签名过的BIOS固件才可以被刷写在相关服务器上，从而避免了恶意的BIOS固件刷写。
- **BMC固件保护**：确保在主机操作系统中，无法对BMC固件进行非授权的恶意刷写。

加密计算

专有云平台的芯片级加密计算使用了处理器提供的硬件可信执行环境。用户可以通过应用软件建立一个可信的执行环境，保护敏感数据和加解密密钥。用户可以通过自己编写支持可信执行环境技术的代码来保护用户自己的数据，从而确保只有用户编写的授权运行在可信执行环境内的代码可以访问和操作用户关键数据。通过阿里云加密计算技术，阿里云为用户数据安全上云提供了更强大的数据安全方案。

可信计算

阿里云在关键服务器上采用了基于TPM 2.0的可信计算技术，通过TPM 2.0的主动度量技术对基础软件的启动过程进行度量，基础软件包括了BIOS，操作系统内核等。同时，阿里云的密钥管理服务也使用了TPM 2.0进行根密钥的保护。

4.1.2 虚拟化安全

虚拟化技术是云计算的主要技术支撑，通过计算虚拟化、存储虚拟化、网络虚拟化来保障云计算环境下的多租户隔离。阿里云虚拟化安全技术主要包括租户隔离、补丁热修复、逃逸检测三大基础安全部分来保障阿里云虚拟化层的安全。

租户隔离

虚拟化层在租户隔离中起到至关重要的作用。基于硬件虚拟化技术的虚拟机管理将多个计算节点的虚拟机在系统层面进行隔离，租户不能访问相互之间未授权的系统资源，从而保障计算节点的基本计算隔离。同时虚拟化管理层还提供了存储隔离和网络隔离。

- **计算隔离**

  阿里云提供各种基于云的计算服务，包括各种计算实例和服务，可自动伸缩以满足应用程序或企业的需求。这些计算实例和服务在多个级别提供计算隔离以保护数据，同时保障了用户需求的配置灵活性。计算隔离中关键的隔离边界是管理系统与用户虚拟机以及用户虚拟机之间的隔离，这种隔离由Hypervisor直接提供。阿里云平台使用的虚拟化环境，将用户实例作为独立虚拟机运行，并且通过使用物理处理器权限级别强制执行此隔离，确保用户虚拟机无法通过未授权的方式访问物理主机和其他用户虚拟机的系统资源。

- **存储隔离**

  作为云计算虚拟化基础设计的一部分，阿里云将基于虚拟机的计算与存储分离。这种分离使得计算和存储可以独立扩展，从而更容易提供多租户服务。在虚拟化层，Hypervisor采用分离设备驱动模型实现I/O虚拟化。虚拟机所有I/O操作都会被Hypervisor截获处理，保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机硬盘空间的安全隔离。云用户实例服务器释放后，原有的磁盘空间将会被可靠的清零以保障用户数据安全。

- **网络隔离**

  为了支持ECS虚拟机实例使用网络连接，阿里云将虚拟机连接到阿里云虚拟网络。阿里云虚拟网络是建立在物理网络结构之上的逻辑结构。每个逻辑虚拟网络与所有其他虚拟网络隔离。这种隔离有助于确保部署中的网络流量数据不能被其它ECS虚拟机访问。

逃逸检测

虚拟机逃逸攻击主要包括两个基本步骤：首先将攻击方控制的虚拟机置于与其中一个攻击目标虚拟机相同的物理主机上，然后破坏隔离边界，以窃取攻击目标的敏感信息或实施影响攻击目标功能的破坏行为。

阿里云虚拟化管理程序通过使用高级虚拟机布局算法以防止恶意用户的虚拟机运行在特定物理机上。阿里云在虚拟化管理软件层面还提供了虚拟化管理程序加固、虚拟化管理程序下攻击检测、虚拟化管理程序热修复三大核心技术来防范恶意虚拟机的攻击。

补丁热修复

阿里云虚拟化平台支持补丁热修复技术，通过补丁热修复技术使得系统缺陷或者漏洞的修复过程不需要用户重启系统，从而不影响用户业务。

4.1.3 云产品开发安全

阿里云为用户提供了多种不同的云产品，其中包括云服务器ECS，云数据库RDS，对象存储OSS，大数据计算服务MaxCompute等等。

云产品安全生命周期（SPLC）

Secure Product Lifecycle（SPLC）是阿里云为云上产品量身定制的云产品安全生命周期，目标是将安全融入到整个产品开发生命周期中。SPLC在产品架构审核、开发、测试审核、应急响应的各个环节层层把关，每个节点都有完整的安全审核机制确保产品的安全性能够满足严苛的云上要求，从而有效地提高云产品的安全能力并降低安全风险。

整个云产品安全生命周期可以分为六大阶段：产品立项、安全架构审核、安全开发、安全测试审核、应用发布、应急响应。

1. **在产品立项阶段**，安全架构师和产品方一同根据业务内容、业务流程、技术框架建立功能需求文档（FRD）、绘制详细架构图，并在阿里云产品上云的所有安全基线要求中确认属于产品范围的《安全基线要求》。同时，本阶段会安排针对性的安全培训课程与考试给产品方人员，从而避免在后续产品开发中出现明显的安全风险。
2. **在安全架构审核阶段**，安全架构师在上一阶段产出的FRD和架构图的基础上对产品进行针对性的安全架构评估并做出产品的威胁建模。在威胁建模的过程中，安全架构师会对产品中的每一个需要保护的资产、资产的安全需求、可能的被攻击场景做出详细的模型，并提出相对应的安全解决方案。安全架构师会综合《安全基线要求》和威胁建模中的安全解决方案，一并与产品方确认对于该产品的所有《安全要求》。
3. **在安全开发阶段**，产品方会根据《安全要求》在产品开发中遵守安全编码规范，并实现产品的相关安全功能和要求。为了保证云产品快速持续的开发，发布与部署效率，产品方会在本阶段进行自评确认《安全要求》都已经实现，并提供相对应的测试信息（如代码实现地址，自测结果报告等）给负责测试的安全工程师，为下阶段的安全测试审核做好准备。

4. **在安全测试审核阶段**，安全工程师会根据产品的《安全要求》对其进行架构、设计，服务器环境等全方位的安全复核，并对产品的代码进行代码审核和渗透测试。在此阶段发现的安全问题会要求产品方进行安全修复和加固。
5. **在应用发布阶段**，只有经过安全复核，并且得到安全审批许可后，产品才能通过标准发布系统部署到生产环境，以防止产品携带安全漏洞在生产环境运行。
6. **在应急响应阶段**，安全应急团队会不断监控云平台可能的安全问题，并通过外部渠道（如ASRC等）或者内部渠道（如内部扫描器、安全自测等）得知安全漏洞。在发现漏洞后应急团队会对安全漏洞进行快速评级，确定安全漏洞的紧急度和修复排期，从而合理分配资源，做到快速并合理的修复安全漏洞，保障阿里云用户、自身的安全。

4.2 云用户侧安全架构

阿里云在用户侧安全架构如上图所示，提供了六个层面的安全保障，其中包括了账户安全、主机安全、应用安全、网络安全、数据安全、及安全运营。

4.2.1 账户安全

阿里云提供多种安全机制来帮助客户保护账户安全以防止未授权的用户操作。这些安全机制包括云账户登录及MFA管理、创建子用户、集中管理子用户权限、数据传输加密、子用户操作审计。客户可以使用这些机制来保护其云账户安全。

账户认证

阿里云账户认证的基础是用身份凭证来证明用户的真实身份。身份凭证通常是指登录密码或访问密钥（Access Key，AK）。身份凭证是秘密信息，用户必须保护好身份凭证的安全。

通过阿里云的RAM 资源访问控制服务，每个云账户可以独立开通一个RAM服务, 并通过RAM创建子用户，为每个子用户分配不同的密码或访问密钥，消除了云账户共享带来的安全风险；同时可为不同的子用户分配不同的工作权限，大大降低了因账户权限过大带来的风险。用户可以通过RAM控制台为子用户创建密码策略，以保证各个子用户使用定期轮转的强密码从而提高整体账户的安全性。RAM同时支持颁发STS (Security Token Service) 安全令牌给在短时间内需要访问某些资源的临时用户，并根据需要来定义令牌的权限和自动过期时间（默认为1小时过期），从而避免颁发和防止泄露长期AK。

阿里云强烈建议用户使用RAM用户的Access Key，而不要使用云账户的Access Key。云账户可以理解为根账号，它具有所有云产品的完全控制权限。根账号Access Key一旦泄露将可能造成极大风险，所以建议客户使用RAM用户进行资源操作并遵循最小授权原则。

多因素认证(MFA, Multi-Factor Authentication)

MFA是一种简单有效的最佳安全实践方法，它能够在用户名和密码之外再额外增加一层安全保护。启用MFA 后，用户登录阿里云时，系统将要求输入用户名和密码（第一安全要素），然后要求输入来自其MFA设备的可变验证码（第二安全要素）。这些多重要素结合起来将为用户的账户提供更高的安全保护。阿里云可以支持基于软件的虚拟MFA设备。虚拟MFA设备是产生一个6位数字认证码的应用程序，它遵循基于时间的一次性密码 (TOTP) 标准(RFC 6238)。此应用程序可在移动硬件设备（包括智能手机）上运行。

访问控制

RAM (Resource Access Management) 是阿里云为用户提供的集中式用户管理与资源访问控制服务。使用RAM，用户可以为其企业员工、系统或应用程序创建独立的用户账号，并可以控制这些用户对其云资源的操作权限。每个RAM用户可以拥有独立的登录密码或Access Key，可以登录阿里云控制台，或以程序方式操作云服务API。RAM用户创建时默认没有任何资源操作权限，只有在获得显式授权的条件下RAM用户才能代表云账户进行资源操作。

使用RAM，用户可以有效避免与其他用户共享云账户密钥，并根据最小权限原则为不同用户分配最小的工作权限，从而降低企业信息安全管理风险。RAM使得一个阿里云账户（主账号）可拥有多个子用户，并可以使用多因素认证、强密码策略、控制台用户与API用户分离、支持自定义细粒度授权策略，支持用户分组授权、临时授权令牌、账户临时禁用等功能。RAM 授权可以细化到对某个 API-Action 和 Resource-ID 的细粒度授权，还可以支持多种限制条件（源IP地址、安全访问通道SSL/TLS、访问时间段、多因素认证等等）。

4.2.2 主机安全

入侵检测

阿里云用户可以通过在主机上配置云盾主机入侵防御系统（安骑士），实现与云端安全中心的联动，获取入侵检测的安全能力。主机的入侵检测包括异地登录提醒、识别暴力破解攻击、网站后门查杀、主机异常检测等功能。

漏洞管理

阿里云用户可以通过在主机上配置主机入侵防御系统（安骑士），实现与云端安全中心的联动，获取漏洞管理的安全能力。主机的漏洞管理综合了多套扫描引擎（网络端、本地端、PoC验证），可以全面批量检测出系统存在的所有漏洞，并提供一键修复、生成修复命令、一键批量验证功能，实现漏洞管理的闭环。

镜像加固

镜像是云服务器 ECS 虚拟机实例运行环境的模板，一般包括操作系统和预装的软件。ECS租户可以使用镜像创建新的 ECS 实例和更换 ECS 实例的系统盘。阿里云官方公共镜像（支持 Linux 和 Windows 的多个发行版本）安全主要包括镜像基础安全配置、镜像漏洞修复、默认镜像主机安全软件三个部分，阿里云保持对阿里云公共镜像操作系统漏洞以及三方软件漏洞的实时监测，以确保所有阿里云公共镜像高危漏洞在第一时间得到修复，阿里云公共镜像默认进行主机最佳安全实践配置，并且所有阿里云公共基础镜像会默认添加阿里云主机安全软件以保障租户在实例启动时第一时间得到安全保障。

自动宕机迁移

云服务器部署在宿主机（承载云服务器的物理服务器）上，宿主机可能因性能异常或者硬件原因导致故障，当检测到云服务器所在的宿主机发生故障时，系统会启动保护性迁移，把云服务器迁移到正常的宿主机上，恢复实例正常运行，保障应用的高可用性。

4.2.3 应用安全

Web应用防护

Web应用防火墙(Web Application Firewall, 简称WAF),基于云安全大数据能力实现，通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，过滤海量恶意访问，避免网站资产数据泄露，保障网站的安全与可用性。

代码安全

在云产品安全生命周期（SPLC）中，阿里云的安全专家在各个开发节点中都会严格审核和评估代码的安全性，从而保障阿里云提供给用户的产品的代码安全质量。同时，阿里云强烈建议企业用户对其上线的应用进行黑白盒代码安全检测，务求上线后的应用不会存在安全漏洞，增加用户本身的业务的安全强壮性。

4.2.4 网络安全

网络隔离

阿里云对生产网络与非生产网络进行了安全隔离，从非生产网络不能直接访问生产网络的任何服务器和网络设备。阿里云把对外提供服务的**云服务网络**和支撑云服务的**物理网络**进行安全隔离，通过网络ACL确保云服务网络无法访问物理网络。阿里云也采取网络控制措施防止非授权设备私自联到云平台内部网络，并防止云平台物理服务器主动外联。

虚拟专用网络（VPN）

VPN 网关（Virtual Pirvate Network Gateway）是一款基于 Internet，通过加密通道将企业数据中心、企业办公网络、阿里云专有网络（VPC）安全可靠连接起来的服务。阿里云VPN网关在中华人民共和国国家相关政策法规内提供服务，不提供访问Internet功能。

专有网络（VPC）

专有网络（Virtual Private Cloud）可以帮助用户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等连接方式实现云上VPC与传统IDC的互联，构建混合云业务。

分布式防火墙

安全组是阿里云提供的分布式虚拟化防火墙，具备状态检测和包过滤功能。

安全组是一个逻辑上的分组，这个分组是由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。使用安全组可设置单台或多台云服务器的网络访问控制，它是重要的网络安全隔离手段，用于在云端划分网络安全域。

每个实例至少属于一个安全组。同一安全组内的实例之间网络互通，不同安全组的实例之间默认内网不通，可以授权某个源安全组或某个源网段访问目的安全组。

DDoS防御

阿里云使用自主研发的DDoS防护系统保护所有数据中心，提供DDoS攻击自动检测、调度和清洗功能，可以在5秒钟内完成攻击发现、流量牵引和流量清洗全部动作，保证云平台网络的稳定性。同时，阿里云的DDoS防护系统在防护触发条件上不仅仅依赖流量阈值， 还基于网络行为的统计判断，做到精准识别DDoS攻击，保障了在遇到DDoS攻击时客户业务的可用性。

4.2.5 数据安全

数据安全体系

阿里云数据安全体系从数据安全生命周期角度出发，采取管理和技术两方面的手段，进行全面、系统的建设。通过对数据生命周期（数据生产、数据存储、数据使用、数据传输、数据传播、数据销毁）各环节进行数据安全管理管控，实现数据安全目标。

在数据安全生命周期的每一个阶段，都有相应的安全管理制度以及安全技术保障。

数据所有权

2015年7月，阿里云发起中国云计算服务商首个“数据保护倡议”，这份公开倡议书明确：运行在云计算平台上的开发者、公司、政府、社会机构的数据，所有权绝对属于用户；云计算平台不得将这些数据移作它用。平台方有责任和义务，帮助用户保障其数据的私密性、完整性和可用性。

多副本冗余存储

阿里云使用分布式存储，文件被分割成许多数据片段分散存储在不同的设备上，并且每个数据片段存储多个副本。分布式存储不但提高了数据的可靠性，也提高了数据的安全性。

全栈加密

阿里云对于数据安全提供了全栈的加密保护能力，其中包括从应用程序敏感数据加密、RDS数据库透明加密、块存储数据加密、对象存储系统加密、硬件加密模块、和网络数据传输加密。 对于应用程序敏感数据加密，阿里云支持使用处理器提供的硬件可信执行环境下的加密解决方案。

- **数据传输加密**

  阿里云的传输协议支持标准的TLS协议，可提供高达256位密钥的加密强度，完全满足敏感数据加密传输需求。

- **数据存储加密**

  阿里云加密服务使用经国家密码管理局检测认证的硬件密码机，帮助您满足数据安全方面的监管合规要求，保护云上业务数据的机密性。借助加密服务，您可以实现对加密密钥的完全控制并进行解密操作。不同的云产品也支持数据加密以满足用户的要求：

  - 在RDS数据库透明加密层，数据库数据可以被加密的形式存放到数据库系统中。
  - 块存储数据加密支持虚拟机内部使用的块存储设备的自动加密，确保块存储的数据在分布式系统中加密存放。
  - 对象存储(OSS)系统也直接支持加密能力，用户可以选择是否使用加密保存对象数据。

镜像管理

ECS提供快照与自定义镜像功能，快照可以保留某个时间点上的系统数据状态，用于数据备份，便于用户可以快速灾难恢复。用户可以使用快照创建自定义镜像，将快照的操作系统、数据环境信息完整的包含在镜像中， 快照使用增量的方式，两个快照之间只有数据变化的部分才会被拷贝。

残留数据清除

对于曾经存储过用户数据的内存和磁盘，一旦释放和回收，其上的残留信息将被自动进行零值覆盖。

运维数据安全

专有云运维人员未经用户许可，不得以任意方式访问用户未经公开的数据内容。

阿里云遵循生产数据不出生产集群的原则，从技术上控制了生产数据流出生产集群的通道，防止运维人员从生产系统拷贝数据。

4.2.6 安全运营

态势感知

态势感知利用大数据技术，从攻击者的角度，有效捕捉高级攻击者使用的0day漏洞攻击、新型病毒攻击事件、和正在发生的安全攻击行为有效的展示，帮助专有云上租户实现云上业务安全可视和可感知。态势感知区别于传统IDC和SIEM（仅支持被识别的告警事件关联），从海量的原始数据中分析信息并通过机器学习的模型完成对安全事件过程的完整还原 。同时，态势感知聚焦在“敌我态势”，对敌方的实体（黑客本人，黑客组织）进行长期的威胁情报监控和行动点技术手段观测，对我方薄弱环节进行实时感知，对安全决策具有重要参考意义。

安全审计

安全审计对标信息系统安全等级保护基本要求，从物理服务器层面、网络设备层面、云计算平台应用层面分别进行，实现了行为日志的收集、存储、分析、报警等功能。

5 云产品安全

5.1 云服务器ECS

5.1.1 产品介绍

云服务器（Elastic Compute Service，简称ECS）是一种简单高效、处理能力可弹性伸缩的计算服务，帮助您快速构建更稳定、安全的应用，提升运维效率，降低IT成本，使您更专注于核心业务创新。

云服务器（ECS）从实例安全、存储安全、网络安全三个方面保障服务的安全可靠。

5.1.2 实例安全

云服务器（ECS）在多个层面上保护用户的实例，包括：

- 物理服务器上的虚拟化平台
- ECS实例上的操作系统（Guest OS）
- 防火墙

多重安全措施相互作用，共同保护用户的ECS实例（包括实例本身和实例中的数据），确保用户的ECS实例不会通过未授权的方式被访问。

5.1.2.1 宿主机的操作系统安全

宿主机的操作系统是阿里云根据云特点定制的、重新增减并进行编译的加固操作系统。同时，对安全策略和安全访问上做了大量的深度加固定制。

5.1.2.2 实例的操作系统（Guest OS）安全

用户拥有对ECS实例的操作系统的完全控制权，阿里云没有任何权限访问用户的实例及实例上的操作系统。

同时，阿里云强烈建议用户采用安全的方式对ECS实例上的操作系统进行访问和操作。比如使用SSH公钥和私钥对，并妥善保存私钥（至少要求使用复杂密码，可在创建实例时设置）；采用更安全的SSHv2方式远程登录；采用 sudo指令的方式做提权等。

5.1.2.3 镜像安全

阿里云基础镜像集成了所有已知的高危漏洞补丁，最大限度防止ECS实例上线后即处于高风险状态。阿里云使用数据校验算法和单向散列算法确保镜像完整性，防止被恶意篡改。

在发现新的高危安全漏洞后，用户可以迅速更新基础镜像。同时，用户可以完全自主地对ECS实例上的操作系统进行升级或漏洞修复。

强烈建议在不影响用户业务部署的情况下，使用阿里云的基础镜像作为上云的第一步。

5.1.2.4 防止IP/MAC/ARP欺骗

在传统网络环境里，IP/MAC/ARP欺骗一直是网络面临的严峻考验。通过IP/MAC/ARP欺骗，黑客可以扰乱网络环境，窃听网络机密。

阿里云云平台通过宿主机上的网络底层技术机制，彻底解决了这一问题。在宿主机数据链路层隔离由ECS实例向外发起的异常协议访问，阻断ECS实例ARP/MAC欺骗，并在宿主机网络层防止ECS实例IP欺骗。

5.1.3 存储安全

5.1.3.1 Chunk

ECS用户对虚拟磁盘的读写最终都会被映射为对阿里云数据存储平台上的文件的读写。阿里云提供一个扁平的线性存储空间，并在内部对线性地址进行切片，一个分片称为一个Chunk。对于每一个Chunk，阿里云都会复制出三个副本，并将这些副本按照一定的策略存放在集群中的不同节点上，保证用户数据的可靠。

5.1.3.2 三份副本的原理

在阿里云数据存储系统中，有三类角色，分别称为Master、Chunk Server和Client。ECS用户的每一个写操作经过层层转换，最终会交由Client来执行，执行过程如下：

1. Client计算出这个写操作对应的Chunk。
2. Client向Master查询该Chunk的三份副本的存放位置。
3. Client根据Master返回的结果，向对应的三个Chunk Server发出写请求。
4. 如果三份副本都写成功，Client向用户返回成功；反之，Client向用户返回失败。

Master的分布策略会综合考虑集群中所有Chunk Server的磁盘使用情况、在不同交换机机架下的分布情况、电源供电情况、及机器负载情况，尽量保证一个Chunk的三个副本分布在不同机架下的不同 Chunk Server 上，从而有效防止由于一个Chunk Server或一个机架的故障导致的数据不可用。

5.1.3.3 数据保护机制

当有数据节点损坏，或者某个数据节点上的部分硬盘发生故障时，集群中部分Chunk的有效副本数会小于三。一旦发生这种情况，Master就会启动复制机制，在Chunk Server之间复制数据，保证集群中所有Chunk的有效副本数达到三份。

综上所述，对云盘上的数据而言，所有用户层面的操作都会同步到底层三份副本上，无论是新增、修改还是删除数据。通过这种机制，保障用户数据的可靠性和一致性。

另外，在用户进行删除操作后，释放的存储空间由分布式文件系统回收，禁止任何用户访问，并在被再次使用前进行内容擦除（包括云盘的每一块上的内容），最大限度保证用户的数据安全性。

5.1.4 网络安全

5.1.4.1 实例的安全隔离

实例的安全隔离包括：

CPU隔离

阿里云ECS支持Xen和KVM两种Hypervisor，基于硬件虚拟化技术VT-x，Hypervisor运行在vmx root模式，而ECS实例运行在vmx non-root模式。通过硬件机制进行隔离，有效地防止了ECS实例访问特权资源，同时也实现了 ECS 实例之间的有效隔离。

内存隔离

在虚拟化层，Hypervisor隔离内存。ECS实例运行时，使用硬件辅助的扩展页表（Extended Page Tables，简称EPT）技术，确保ECS实例之间无法互访对方内存。

ECS实例释放后，它所有的内存会被Hypervisor清零，防止ECS实例关闭后释放的物理内存页内容被其他ECS实例访问到。

存储隔离

在虚拟化层，Hypervisor采用分离设备驱动模型实现I/O虚拟化，ECS实例不能直接访问物理磁盘，所有I/O操作都会被Hypervisor截获处理。Hypervisor保证ECS实例只能访问被分配到的虚拟磁盘空间，从而实现不同ECS实例磁盘空间的安全隔离。

网络隔离

ECS采用虚拟交换机（Virtual Switch）。发往某个ECS实例的报文只会送到这个ECS实例的虚拟网卡所对应的虚拟交换机端口，其他ECS实例不可能接收或嗅探这个报文。

运行在混合（Promiscuous）模式下的虚拟实例也不可能接收或嗅探到去往其他虚拟实例的流量。即使把网络接口设置为混合模式，Hypervisor也不会传送任何到其他目的地址的流量给其他虚拟实例。

同时，阿里云还采用专有网络VPC和安全组防火墙进行网络隔离。

通过以上隔离措施，即使同一个用户拥有的运行在同一台物理服务器上的两个虚拟实例之间也不能嗅探到对方流量。

除此之外，阿里云建议您采用更加安全的方式进行数据加密后存储到ECS实例的虚拟磁盘上，例如采用加密的文件系统等方法。

5.1.4.2 安全组

安全组是阿里云提供的分布式虚拟化防火墙，具备状态检测包过滤功能，是ECS实例网络安全防护的另一层保障。安全组独立于ECS实例上操作系统内部的防火墙，是在ECS实例外部提供的另一种防护手段。安全组允许设置到单IP单端口粒度的出入方向的策略，可用于安全域隔离控制等。

安全组是一个逻辑上的分组，这个分组是由同一个地域（Region）内具有相同安全保护需求并相互信任的实例组成。通过安全组可设置单台或多台ECS实例的网络访问控制，是重要的网络安全隔离手段，用于在云端划分网络安全域。

每个ECS实例至少属于一个安全组。同一安全组内的实例之间网络互通，不同安全组的实例之间默认内网不通。通过设置，可以授权某个源安全组或某个源网段，访问或者不能访问目的安全组中的实例；也可以授权允许或者不允许某个目标安全组或者目标网段被目的安全组中的实例访问。

阿里云强烈建议用户使用专有网络VPC、安全组和ECS实例中操作系统内含的防火墙共同作用的策略，以最大限度保障网络安全。

5.2 对象存储OSS

5.2.1 什么是对象存储OSS

对象存储服务（Object Storage Service，简称 OSS）提供海量、安全、低成本、高可靠的云存储服务。它可以理解为一个即开即用，无限大空间的存储集群。相比传统自建服务器存储，OSS 在可靠性、安全性、成本和数据处理能力方面都有着突出的优势。使用 OSS，您可以通过网络随时存储和调用包括文本、图片、音频和视频等在内的各种非结构化数据文件。

OSS 将数据文件以对象/文件（object）的形式上传到存储空间（bucket）中。 您可以进行以下操作：

- 创建一个或者多个存储空间
- 每个存储空间中添加一个或多个文件
- 通过获取已上传文件的地址进行文件的分享和下载
- 通过修改存储空间或文件的属性或元信息来设置相应的访问权限
- 通过云控制台执行基本和高级 OSS 任务
- 通过开发工具包 SDK 或直接在应用程序中进行 RESTful API 调用执行基本和高级 OSS 任务。

5.2.2 身份验证

阿里云用户可以在云控制台里自行创建 Access Key。Access Key 由 AccessKey ID 和 AccessKey Secret 组成，其中 ID 是公开的，用于标识用户身份，Secret 是秘密的，用于用户身份的鉴别。

当用户向 OSS 发送请求时，需要首先将发送的请求按照 OSS 指定的格式生成签名字符串，然后使用 AccessKey Secret 对签名字符串进行加密（基于 HMAC 算法）产生验证码。验证码带时间戳，以防止重放攻击。OSS 收到请求以后，通过 AccessKey ID 找到对应的 AccessKey Secret ，以同样的方法提取签名字符串和验证码，如果计算出来的验证码和提供的一致即认为该请求是有效的；否则，OSS 将拒绝处理这次请求，并返回 HTTP 403 错误。

5.2.3 访问控制

对 OSS 的资源访问分为拥有者访问和第三方用户访问。拥有者是指 bucket 的拥有者，第三方用户是指访问 bucket 资源的其他用户。访问分为匿名访问和带签名访问。对于 OSS 来说，如果请求中没有携带任何和身份相关的信息即为匿名访问。带签名访问是指按照 OSS API 文档中规定的在请求头部或者在请求 URL 中携带签名的相关信息。

OSS 提供 bucket 和 object 的权限访问控制。

Bucket 有三种访问权限：public-read-write，public-read 和 private。

- public-read-write：任何人（包括匿名访问）都可以对该 bucket 中的 object 进行 PUT、Get 和 Delete 操作。
- public-read：只有该 bucket 的创建者可以对该 bucket 内的 object 进行写操作（包括 Put 和 Delete Object）；任何人（包括匿名访问）可以对该 bucket 中的 object 进行读操作（Get Object）。
- private：只有该 bucket 的创建者可以对该 bucket 内的 object 进行读写操作（包括 Put、Delete 和 Get Object）；其他人无法访问该 bucket 内的 object。

用户新创建一个 bucket 时，如果不指定 bucket 权限，OSS 会自动为该 bucket 设置 private 权限。

Object 有四种访问权限：public-read-write，public-read，private 和 default。

- public-read-write：所有用户拥有此 object 的读写权限。
- public-read：非此 object 的 Owner 拥有此 object 的读权限，只有此 object 的 Owner 拥有此 object 的读写权限。
- private：此 object 的 Owner 拥有该 object 的读写权限，其他的用户对此 object 没有读、写权限。
- default：object 遵循 bucket 的访问权限。

用户上传 object 时，如果不指定 object 权限，OSS 会为 object 设置为 default 权限。

5.2.4 RAM和STS

OSS 已经接入 RAM/STS 鉴权。

RAM (Resource Access Management) 是阿里云提供的资源访问控制服务。通过 RAM，主账号可以创建出子账号，子账号从属于主账号，所有资源都属于主账号，主账号可以将所属资源的访问权限授予给子账号。

STS（Security Token Service）是阿里云提供的临时访问凭证服务，提供短期访问权限管理。STS 可以生成一个短期访问凭证给用户使用，凭证的访问权限及有效期限由用户定义，访问凭证过期后会自动失效。

5.2.5 高可用性

OSS 服务可用性高达 99.9%。

在一个 Region 内，OSS 数据采用三副本存储，可靠性达到 99.99999999%。

5.2.6 租户隔离

OSS 将用户数据切片，按照一定规则，离散存储在分布式文件系统中，并且用户数据和数据索引分离存储。OSS 用户认证采用 Access Key 对称密钥认证技术，对于用户的每个 HTTP 请求都验证签名。在用户验证通过后，重组用户离散存储的数据，从而实现多租户间的数据存储隔离。

5.2.7 服务器端加密

OSS支持在服务器端对用户上传的数据进行加密（Server-Side Encryption）。当用户上传数据时，OSS对收到的用户数据使用AES256进行加密，然后再将加密得到的数据永久保存下来。用户下载

数据时，OSS自动对保存的加密数据解密后把原始数据返回给用户，并在返回的HTTP请求Header中声明该数据进行了服务器端加密。

用户创建Object时，只需要在Put Object的请求中携带x-oss-server-side-encryption的HTTP header，并指定其值为AES256，即可以实现该Object的服务器端加密存储。

5.2.8 客户端加密

客户端加密是指用户数据在发送给远端服务器之前就完成加密，而加密所用的密钥明文只保留在用户本地，从而可以保证用户数据安全，即使数据泄漏别人也无法解密得到原始数据。

5.2.9 数据传输安全

OSS 支持用户使用安全套接层协议访问 OSS。用户通过访问 OSS 持有证书的域名，保证数据信道安全，避免中间人攻击。

5.2.10 数据传输完整性

数据在客户端和服务器之间传输时有可能会出错。OSS现在支持对各种方式上传的Object返回其CRC64值，客户端可以和本地计算的CRC64值做对比，从而完成数据完整性的验证。

5.2.11 访问日志记录

OSS 提供自动保存访问日志记录（logging）功能，用户开启 Bucket 的日志保存功能后，OSS自动将访问这个Bucket的请求日志，以小时为单位，按照固定的命名规则，生成一个Object写入用户指定的目标Bucket（ Target Bucket），作为审计或者特定行为分析使用。请求日志中包含请求时间、来源 IP、请求对象、返回码、处理时长等内容。

5.2.12 跨资源共享

跨域访问，或者说JavaScript的跨域访问问题，是浏览器出于安全考虑而设置的一个限制，即同源策略。当来自于A网站的页面中的JavaScript代码希望访问B网站的时候，浏览器会拒绝该访问，因为A、B两个网站是属于不同的域。

在实际应用中，经常会有跨域访问的需求，比如用户的网站www.a.com，后端使用了OSS。在网页中提供了使用JavaScript实现的上传功能，但是在该页面中，只能向www.a.com发送请求，向其他网站发送的请求都会被浏览器拒绝。这样就导致用户上传的数据必须从www.a.com中转。如果设置了跨域访问的话，用户就可以直接上传到OSS而无需从www.a.com中转。

OSS 支持 CORS 协议，可以支持用户配置跨域访问权限。用户可以设置 Bucket 允许的跨域请求来源。Bucket 默认不开启 CORS 功能，所有跨域请求都不允许。

5.2.13 防盗链

为了防止用户在OSS上的数据被其他人盗链，OSS支持基于HTTP header中表头字段referer的防盗链方法。用户可以通过OSS管理控制台或者API的方式对一个Bucket设置referer字段的白名单和是否允许referer字段为空的请求访问。例如，对于一个名为oss-example的Bucket，设置其referer白名单为**http://www.aliyun.com/**。则所有referer为**http://www.aliyun.com/**的请求才能访问oss-example这个Bucket中的Object。

5.3 表格存储TableStore

5.3.1 什么是表格存储

表格存储（Table Store）是构建在阿里云飞天分布式系统之上的 NoSQL 数据存储服务，提供海量结构化数据的存储和实时访问。

- 表格存储以实例和表的形式组织数据，通过数据分片和负载均衡技术，达到规模的无缝扩展。
- 表格存储向应用程序屏蔽底层硬件平台的故障和错误，能自动从各类错误中快速恢复，提供非常高的服务可用性。
- 表格存储管理的数据全部存储在 SSD 中并具有多个备份，提供了快速的访问性能和极高的数据可靠性。

5.3.2 身份认证

表格存储根据 AccessKey 对请求进行身份认证和鉴权，每个合法的表格存储请求都必须携带正确的 AccessKey 信息。

表格存储对应用的每一次请求都进行身份认证和鉴权，以防止未授权的数据访问，确保数据访问的安全性。

5.3.3 高可用性

通过自动的故障检测和数据迁移，表格存储对应用屏蔽了机器和网络的硬件故障，提供 99.9% 的高可用性。

表格存储通过存储多个数据备份及备份失效时的快速恢复，提供不低于 99.99999999% 的数据可靠性。

5.3.4 强一致性

表格存储保证数据写入强一致，写操作一旦返回成功，应用就能立即读到最新的数据。

5.3.5 监控集成

用户可以从表格存储控制台实时获取每秒请求数、平均响应延时等监控信息。

5.3.6 RAM 和 STS 支持

表格存储支持 RAM 服务。

使用阿里云的 RAM 服务，用户可以将云账户下表格存储资源的访问及管理权限授予 RAM 中子用户。

表格存储同时支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

5.3.7 VPC 支持

表格存储支持 VPC 内访问，可以登录表格存储云控制台绑定 VPC。

5.4 文件存储NAS

5.4.1 产品介绍

阿里云文件存储（Network Attached Storage，NAS）是面向阿里云ECS实例、HPC和Docker的文件存储服务，提供标准的文件访问协议，用户无需对现有应用做任何修改，即可使用具备无限容量及性能扩展、单一命名空间、多共享、高可靠和高可用等特性的分布式文件系统。

5.4.2 产品安全和可靠性方案

5.4.2.1 访问控制

NAS支持文件系统标准的目录/文件权限操作，并支持用户/组的读/写/执行权限。NAS支持VPC挂载点和经典网络挂载点，并只允许同一VPC内或同一账号下的ECS实例访问其文件系统。NAS同时提供了IP级别的权限组进行细粒度的访问权限控制。

5.4.2.2 RAM支持

NAS接入了RAM服务，支持控制台设置RAM，主子账号授权。

通过RAM，您可以授权子用户对文件存储NAS的操作权限。为了遵循最佳安全实践，强烈建议您使用子用户来操作文件存储NAS。

表 5-1: RAM中可授权的文件存储NAS操作列表

操作（Action）	说明
DescriptFileSystems	列出文件系统实例
DescriptMountTargets	列出文件系统挂载点
DescriptAccessGroup	列出权限组
DescriptAccessRule	列出权限组规则
CreateFileSystem	创建文件系统实例
CreateMountTarget	为文件系统添加挂载点
CreateAccessGroup	创建权限组
CreateAccessRule	添加权限组规则
DeleteFileSystem	删除文件系统实例
DeleteMountTarget	删除挂载点
DeleteAccessGroup	删除权限组
DeleteAccessRule	删除权限组规则
ModifyMountTargetStatus	禁用或激活挂载点
ModifyMountTargetAccessGroup	修改挂载点权限组
ModifyAccessGroup	修改权限组
ModifyAccessRule	修改权限组规则

5.4.2.3 权限组支持

在文件存储NAS中，权限组是一个白名单机制，通过向权限组添加规则，来允许指定的IP或网段访问文件系统，并可以给不同的IP或网段授予不同级别的访问权限。

初始情况下，每个账号都会自动生成一个**VPC默认权限组**，该默认权限组允许VPC内的任何IP以最高权限（读写且不限制root用户）访问挂载点。

经典网络类型挂载点不提供默认权限组，且经典网络类型权限组规则授权地址只能是单个IP而不能是网段。

一条权限组规则包含四个属性，分别是：

表 5-2: 权限组属性

属性	取值	含义
授权地址	单个IP地址或网段（经典网络类型只支持单个IP）	本条规则的授权对象。
读写权限	只读、读写	允许授权对象对文件系统进行只读操作或读写操作。
用户权限	不限制root用户、限制root用户、限制所有用户	是否限制授权对象的Linux系统用户对文件系统的权限：在判断文件或目录访问权限时，限制root用户将把root用户视为nobody处理，限制所有用户将把包括root在内的所有用户都视为nobody。
优先级	1-100，1为最高优先级	当同一个授权对象匹配到多条规则时，高优先级规则将覆盖低优先级规则。

5.4.2.4 高可用性

NAS提供99.99999999%的数据可靠性，相比自建NAS存储，可以大量节约维护成本，降低数据可靠性风险。

5.5 云数据库RDS版

5.5.1 产品概述

阿里云关系型数据库（Relational Database Service，RDS）是一种稳定可靠、可弹性伸缩的在线数据库服务。基于阿里云分布式文件系统和高性能存储，RDS 支持 MySQL数据库引擎，并且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案 。

云数据库RDS提供了多样化的安全加固功能来保障用户数据的安全，其中包括但不限于：

- **网络**：IP 白名单、VPC 网络
- **存储**：自动备份
- **容灾**：同城容灾（多可用区实例）、异地容灾（容灾实例）

5.5.2 租户隔离

RDS通过虚拟化技术进行租户隔离，每个租户拥有自己独立的数据库权限。同时阿里云对运行数据库的服务器进行了安全加固，例如禁止用户通过数据库读写操作系统文件，确保用户无法接触其他用户的数据。

5.5.3 高可用性

高可用版RDS实例拥有两个数据库节点进行主从热备，主节点发生故障可以迅速切换至备节点，月服务可用性承诺为99.95%。

用户可以随时发起数据库的备份，RDS能够根据备份策略将数据库恢复至任意时刻，提高了数据可回溯性。

5.5.4 访问控制

- **数据库账号**

  当用户创建实例后，RDS并不会为用户创建任何初始的数据库账户。用户可以通过控制台或者Open API来创建普通数据库账户，并设置数据库级别的读写权限。如果用户需要更细粒度的权限控制，比如表/视图/字段级别的权限，也可以通过控制台或者Open API先创建超级数据库账户，并使用数据库客户端和超级数据库账户来创建普通数据库账户。超级数据库账户可以为普通数据库账户设置表级别的读写权限。

- **IP白名单**

  默认情况下，RDS实例被设置为不允许任何IP访问，即127.0.0.1。用户可以通过控制台的数据安全性模块或者Open API 来添加IP白名单规则。IP 白名单的更新无需重启RDS实例，因此不会影响用户的使用。IP白名单可以设置多个分组，每个分组可配置1000个IP或IP段。

5.5.5 网络隔离

- **VPC网络**

  除了IP白名单外，RDS还支持用户使用VPC来获取更高程度的网络访问控制。VPC是用户在公共云里设定的私有网络环境，通过底层网络协议严格地将用户的网络包隔离，在网络2层完成访问控制；用户可以通过VPN或者专线，将自建IDC的服务器资源接入阿里云，并使用VPC自定义的RDS IP段来解决IP资源冲突的问题，实现自有服务器和阿里云ECS同时访问RDS的目的。

  使用VPC和IP白名单将极大程度提升RDS实例的安全性。

- **Internet**

部署在VPC中的RDS实例默认只能被同一个VPC中的ECS实例访问。如果有需要也可以通过申请公网IP的方式接受来自公网的访问（不推荐），包括但不限于：

- 来自ECS EIP的访问。
- 来自用户自建IDC公网出口的访问。

IP白名单对RDS实例的所有连接方式生效，建议在申请公网IP前先设置相应白名单规则。

5.5.6 SQL审计

RDS提供查看SQL明细功能，用户可定期审计SQL，及时发现问题。RDS Proxy记录所有发往RDS的SQL语句，内容包括连接IP、访问的数据库名称、执行语句的账号、SQL语句、执行时长、返回记录数、执行时间点等信息。

5.5.7 备份恢复

为了保证数据完整可靠，数据库需要常规的自动备份来保证数据的可恢复性。RDS提供两种备份功能，分别为数据备份和日志备份。

5.5.8 软件升级

RDS 为用户提供数据库软件的新版本。在绝大多数情况下版本升级都是非强制性的。只有用户主动重启了RDS实例的时候，RDS才会将被重启实例的数据库版本升级到新的兼容版本。在极少数情况下（如致命的重大Bug、安全漏洞），RDS会在实例的可运维时间内发起数据库版本的强制升级。需要注意的是，强制升级的影响仅仅是几次数据库连接闪断，在应用程序正确配置了数据库连接池的情况下不会对应用程序造成明显的影响。用户可以通过控制台或者Open API来修改可运维时间，以避免RDS在业务高峰期发生了强制升级。

5.5.9 RAM和STS支持

用户通过云账户创建的RDS实例，都是该账户自己拥有的资源。默认情况下，云账户对自己的资源拥有完整的操作权限。

RDS已支持RAM服务。使用阿里云的RAM服务，用户可以将云账户下RDS资源的访问及管理权限授予RAM中子用户。RDS同时支持STS服务，通过临时访问凭证提供短期访问权限管理。

5.5.10 最佳实践

- **网络设置**

RDS支持公网的访问和私网的访问，如果仅在阿里云内部使用，建议设置为私网访问。如果再VPC内访问，建议选择VPC实例。

- **IP白名单设置**

  通过RDS控制台，设置RDS连接IP白名单为对应的ECS私网IP或者云服务的私网IP。

5.6 云数据库Redis版

5.6.1 产品介绍

云数据库Redis版是兼容Redis协议标准的、提供持久化的内存数据库服务，基于高可靠双机热备架构，满足高读写性能场景及容量需弹性变配的业务需求。

云数据库 Redis版采用主从（Replication）模式搭建。主节点提供日常服务访问，备节点提供 HA高可用，当主节点发生故障，系统会自动在30秒切换至备节点，保证业务平稳运行。

云数据库Redis版从多个角度提供方案来保障服务安全可靠，包括但不限于：

- 访问控制：数据库账号密码、IP 白名单
- 高可用架构：双机高可用架构

5.6.2 产品安全和可靠性方案

5.6.2.1 访问控制

数据库账号

访问Redis必须通过强制密码认证，是访问Redis的凭证。云数据库Redis版针对短连接等模式做了性能优化，开启密码认证并不会影响Redis的实例性能。

IP 白名单

云数据库Redis版提供了IP白名单来实现网络安全访问控制，支持为每个云数据库Redis版实例单独设置IP白名单。

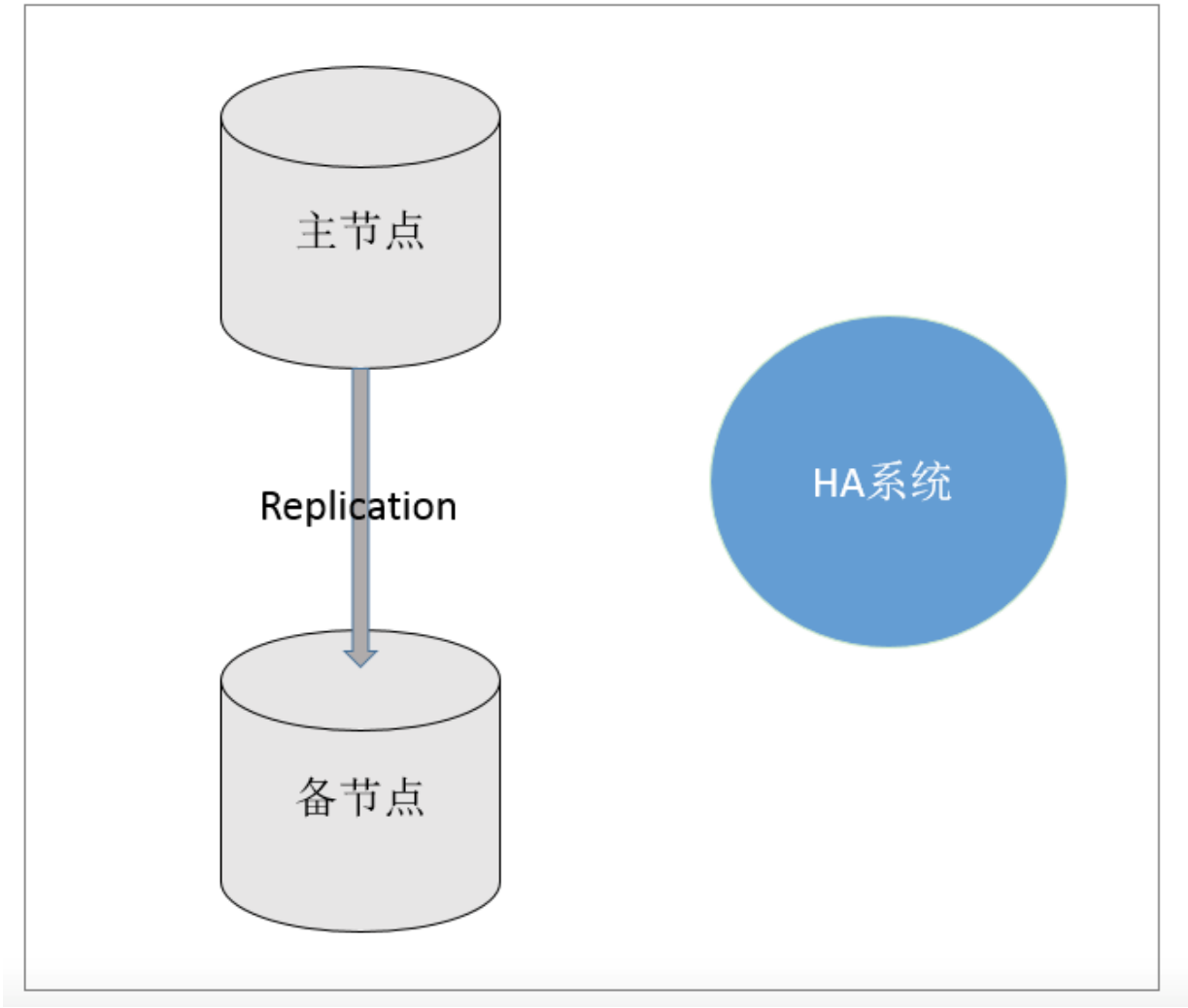
默认情况下，云数据库Redis版实例被设置为允许任何IP访问。您可以通过控制台的**实例信息** > **修改白名单**页面来添加IP白名单规则。IP白名单的更新无需重启实例，不影响使用。同时，IP白名单支持设置IP地址或IP段。

5.6.2.2 高可用架构

云数据库 Redis采用主从（Replication）模式搭建。

主节点提供日常服务访问，备节点提供 HA 高可用，当主节点发生故障，系统会自动在30秒切换至备节点，保证业务平稳运行。

图 5-1: Redis主从（Replication）架构



可靠性

- 服务可靠

  采用双机主备架构，主备节点位于不同物理机。主节点对外提供访问，您可通过 Redis 命令行和通用客户端进行数据的增删改查操作。当主节点出现故障，自研的 HA 系统会自动进行主备切换，保证业务平稳运行。

- 数据可靠

默认开启数据持久化功能，数据全部落盘。支持数据备份功能，您可以针对备份集回滚实例或者克隆实例，有效的解决数据误操作等问题。

兼容性

云数据库 Redis 版标准版在 Redis 2.8基础上进行开发，100%兼容 Redis 协议命令。自建的 Redis 数据库可以平滑迁移至 Redis 标准版。并且提供数据传输工具（DTS）可以进行增量的 Redis 迁移，保证业务平稳过渡。

阿里云自研

- 故障探测切换系统（HA）

  阿里云 Redis 服务封装 HA 切换系统，时时探测主节点的异常情况，可以有效解决磁盘 IO 故障、CPU 故障等问题导致的服务异常，及时进行主备切换从而保证服务高可用。

- 主备复制机制

  阿里云针对 Redis 主从复制机制进行了定制修改，采用增量日志格式进行复制传输。当主备复制中断后，对系统性能及稳定性影响极低，有效避免 Redis 原生复制的弊端。

5.6.2.3 软件升级

- 云数据库Redis定期提供数据库软件的新版本。
- 版本升级是非强制性的，只有您主动要求，才会升级到指定版本。
- 当云数据库Redis团队评估您的版本存在重大安全隐患时，会主动通知业务安排时间进行升级。云数据库Redis团队将会全程支持进行升级过程。
- 云数据库Redis升级过程通常在五分钟以内完成，升级期间可能有数次数据库连接闪断并且存在1分钟的实例只读。在应用程序正确配置了数据库连接重连（或连接池）的情况下，不会对应用程序造成明显的影响。

5.6.2.4 服务授权

在没有您授权的情况下，阿里云的售后团队和云数据库Redis开发团队只能查看Redis实例资源、资费和性能相关的信息（例如，云数据库Redis实例的购买时间和到期时间，云数据库Redis的CPU、内存、存储空间的使用情况等。）

只有在获得您授权后，阿里云的售后团队和云数据库Redis开发团队才能在您指定时间查看和修改云数据库Redis实例的配置信息（例如，云数据库Redis实例的IP白名单、审计日志等。）

在任何情况下，阿里云的售后团队和云数据库Redis开发团队不会主动变更云数据库Redis实例的链接信息（包含连接地址和数据库账号。）

5.7 云数据库Memcache版

5.7.1 产品介绍

云数据库Memcache版是兼容Memcache协议标准的、提供持久化的内存数据库服务，基于高可靠双机热备架构，满足高读写性能场景及容量需弹性变配的业务需求。

云数据库 Memcache版采用主从（Replication）模式搭建。主节点提供日常服务访问，备节点提供HA高可用，当主节点发生故障，系统会自动在30秒切换至备节点，保证业务平稳运行。

云数据库Memcache版从多个角度提供方案来保障服务安全可靠，包括但不限于：

- 访问控制：数据库账号密码、IP 白名单
- 高可用架构：双机高可用架构

5.7.2 产品安全和可靠性方案

5.7.2.1 访问控制

- 数据库账号

  访问Memcache必须通过强制密码认证，是访问Memcache的凭证。同时针对特殊需求的客户，可以在控制台上配置免密访问。

  云数据库Memcache版针对短连接等模式做了性能优化，开启密码认证并不会影响Memcache的实例性能。

- IP 白名单

  云数据库Memcache版提供了IP白名单来实现网络安全访问控制，支持为每个云数据库Memcache版实例单独设置IP白名单。

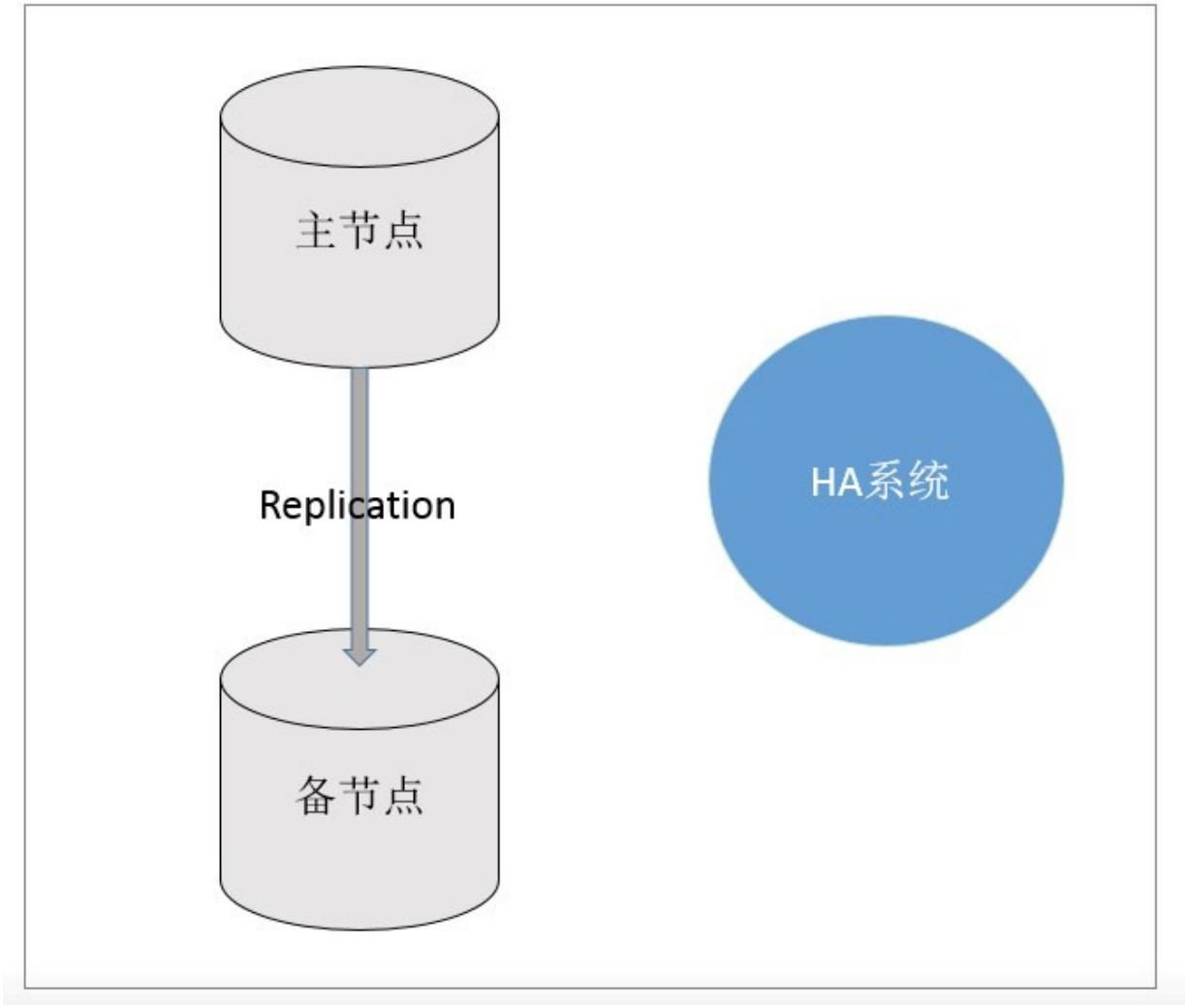
  默认情况下，云数据库Memcache版实例被设置为允许任何IP访问。您可以通过控制台的**实例信息** > **修改白名单** 页面来添加IP白名单规则。IP白名单的更新无需重启实例，不影响使用。同时，IP白名单支持设置IP地址或IP段。

5.7.2.2 高可用架构

云数据库 Memcache采用主从（Replication）模式搭建。

主节点提供日常服务访问，备节点提供 HA 高可用，当主节点发生故障，系统会自动在30秒切换至备节点，保证业务平稳运行。

图 5-2: Memcache主从（Replication）架构



- 可靠性
  - 服务可靠

    采用双机主备架构，主备节点位于不同物理机。主节点对外提供访问，您可通过 Memcache 命令行和通用客户端进行数据的增删改查操作。当主节点出现故障，自研的 HA 系统会自动进行主备切换，保证业务平稳运行。
  - 数据可靠

    默认开启数据持久化功能，数据全部落盘。支持数据备份功能，您可以针对备份集回滚实例或者克隆实例，有效的解决数据误操作等问题。

- 兼容性

  云数据库 Memcache 版100%兼容 Memcache 协议命令。

- 阿里云自研

  - 故障探测切换系统（HA）

    阿里云 Memcache 服务封装 HA 切换系统，时时探测主节点的异常情况，可以有效解决磁盘 IO 故障、CPU 故障等问题导致的服务异常，及时进行主备切换从而保证服务高可用。

  - 主备复制机制

    阿里云针对 Memcache 主从复制机制进行了定制修改，采用增量日志格式进行复制传输。当主备复制中断后，对系统性能及稳定性影响极低，有效避免 Memcache 原生复制的弊端。

5.7.2.3 软件升级

- 云数据库Memcache定期提供数据库软件的新版本。
- 版本升级是非强制性的，只有您主动要求，才会升级到指定版本。
- 当云数据库Memcache团队评估您的版本存在重大安全隐患时，会主动通知业务安排时间进行升级。云数据库Memcache团队将会全程支持进行升级过程。
- 云数据库Memcache升级过程通常在五分钟以内完成，升级期间可能有数次数据库连接闪断并且存在1 分钟的实例只读。在应用程序正确配置了数据库连接重连（或连接池）的情况下，不会对应用程序造成明显的影响。

5.7.2.4 服务授权

在没有您授权的情况下，阿里云的售后团队和云数据库Memcache开发团队只能查看Memcache实例资源、资费和性能相关的信息（例如，云数据库Memcache实例的购买时间和到期时间，云数据库Memcache的CPU、内存、存储空间的使用情况等。）

只有在获得您授权后，阿里云的售后团队和云数据库Memcache开发团队才能在您指定时间查看和修改云数据库Memcache实例的配置信息（例如，云数据库Memcache实例的IP白名单、审计日志等。）

在任何情况下，阿里云的售后团队和云数据库Memcache开发团队不会主动变更云数据库Memcache实例的链接信息（包含连接地址和数据库账号。）

5.8 负载均衡SLB

5.8.1 概述

阿里云负载均衡（Server Load Balancer，SLB）是对多台云服务器进行流量分发的负载均衡服务。负载均衡可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。

5.8.2 高可用性

采用全冗余设计，无单点，支持同城容灾。同时SLB可以根据应用负载进行弹性扩容，在流量波动情况下不中断对外服务。

5.8.3 防御CC攻击

阿里云对开源四层负载均衡LVS的管理软件Keepalived进行了全面优化，使得基于LVS的四层负载均衡具备接近于实时防御的能力。结合云盾，可提供5G以下的防DDOS攻击能力。

采用Tengine作为负载均衡基础模块的七层负载均衡具备多维度的CC攻击防御能力。

5.8.4 访问控制

SLB可以屏蔽后端服务器IP地址，对外只提供SLB的服务地址。

SLB提供源IP白名单功能，可以控制允许哪些可信的IP访问负载均衡服务。

5.8.5 日志功能

负载均衡提供日志管理功能，用户可以查看某个实例的操作日志和健康检查日志。

5.8.6 HTTPS

SLB支持HTTPS/SSL/TLS负载均衡功能：

- 对于需要进行证书认证的服务，可以集中、统一在SLB上管理证书和密钥。而无须部署在每台ECS（Real Server）上。
- 解密处理统一在SLB上进行，降低后端ECS CPU开销。

SLB提供证书管理系统管理，存储用户证书和密钥，用户上传到证书管理系统的私钥都会加密存储。

5.8.7 RAM和STS支持

用户通过自己云账号创建的SLB实例，都是该账号拥有的资源。默认情况下，账号对自己的资源拥有完整的操作权限。

SLB已支持RAM服务。用户可以将用户云账号下负载均衡资源的访问及管理权限授予RAM中子用户。SLB同时支持STS服务，通过临时访问凭证提供短期访问权限管理。

5.8.8 健康检查

SLB服务会检查云服务器池中ECS的健康状态，自动隔离异常状态的ECS，该ECS恢复正常后自动解除屏蔽，从而解决了单台ECS的单点问题，同时提高了应用的整体服务能力。

5.8.9 最佳实践

- 在使用SLB的时候，需要检查勿将后端ECS实例的管理端口通过SLB转发至公网，比如ECS的22、3389、3306、6379等高危端口端口。
- 如果仅仅是做私网负载均衡，用户可以选择私网SLB实例。公网实例和私网实例的不同：
  - 公网实例：负载均衡实例仅提供公网IP，可以通过Internet访问的负载均衡服务。私网实例：负载均衡实例仅提供阿私网IP地址，只能通过内部网络访问该负载均衡服务，Internet用户无法访问。
- SLB提供了HTTPS监听，支持单向和双向认证，建议使用。

5.9 专有网络VPC

5.9.1 概述

用户可以使用阿里云提供的专有网络（Virtual Private Cloud，VPC）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。

5.9.2 安全隔离

不同VPC之间通过VxLAN隧道ID进行隔离。VPC内部由于虚拟交换机和虚拟机路由器的存在，所以可以像传统网络环境一样划分子网，每一个子网内部的不同云服务器使用同一个虚拟交换机互联，不同子网间使用虚拟路由器互联。

5.9.3 自定义网络

客户可以在VPC内自定义网络地址，划分子网，自定义路由。

5.9.4 防火墙

可以通过具备状态检测包过滤功能的安全组防火墙进行网络安全域的划分。

5.9.5 网络访问控制

VPC使用安全组防火墙进行三层网络访问控制。

不同VPC之间内部网络完全隔离，可以通过路由器接口互联。

5.9.6 弹性外网IP

弹性外网IP（Elastic IP Address，EIP），是可以独立持有的外网IP地址资源，能动态绑定到不同的ECS实例上，绑定和解绑时无需停机。

EIP是一种NAT IP，通过NAT方式映射到了被绑定ECS实例的私网网卡上。因此，绑定了EIP的ECS实例可以直接使用这个IP进行公网通信，但是在网卡上并不能看到这个IP地址。EIP可以用于不同VPC之间的互联。

5.9.7 路由器接口

路由器接口支持位于相同地域或不同地域，同一账户或不同账户的VPC之间进行内网互通。阿里云通过在两侧VPC的路由器上分别创建虚拟路由器接口，以及自有的骨干传输网络来搭建高速通道，实现两个VPC之间安全可靠，方便快捷的通信。

5.9.8 NAT 网关

NAT网关（NAT Gateway）是一款企业级的VPC公网网关，提供NAT代理（SNAT、DNAT）、10Gbps级别的转发能力以及跨可用区的容灾能力。

NAT网关作为一个网关设备，需要配置公网IP和公网带宽才能正常工作。NAT网关上的公网IP和公网带宽，被抽象为共享带宽包。一个共享带宽包由一份公网带宽和一组公网IP组成，这些公网IP共享带宽。

NAT网关与共享带宽包需要配合使用，组合成为高性能、配置灵活的企业级网关。

5.9.9 RAM和STS支持

VPC已支持RAM服务。用户可以将用户云账号下VPC资源的访问及管理权限授予RAM中子用户。VPC同时支持STS服务，通过临时访问凭证提供短期访问权限管理。

5.10 日志服务

5.10.1 高可用性

Log服务的日志数据存放在分布式文件系统上，提供三副本存储机制，保障文件存储的可靠性。

5.10.2 离线归档

Log服务除了本身提供的实时查询与分析功能外，还提供日志归档保存到MaxCompute与OSS的功能，以便用户利用MaxCompute以及开源大数据软件做数据分析。

5.10.3 身份认证

Log服务认证采用由阿里云颁发给用户的访问服务的密钥（Access Key），在身份认证时使用HMAC-SHA1签名算法。

5.10.4 RAM支持

Log服务接入了阿里云的访问控制RAM服务，用户可以将云账户下Log资源的访问及管理权限授予RAM中子用户。

5.11 企业级分布式应用服务EDAS

5.11.1 产品介绍

企业级分布式应用服务（Enterprise Distributed Application Service，简称EDAS）是企业级互联网架构解决方案的核心产品，充分利用阿里云现有资源管理和服务体系，引入中间件成熟的整套分布式计算框架（包括分布式服务化框架、服务治理、运维管控、链路追踪和稳定性组件等），以应用为中心，帮助企业级客户轻松构建并托管分布式应用服务体系。

企业级分布式应用服务（EDAS）从多个角度提供方案来保障服务安全可靠，包括但不限于：

- 权限控制：服务鉴权，应用管控鉴权
- 高可用架构：EDAS Console负载均衡，无中心化服务注册中心

5.11.2 安全和可靠性方案

5.11.2.1 权限控制

服务鉴权

在EDAS的远程过程调用协议（Remote Procedure Call Protocol，简称RPC）服务调用过程中，每一次调用都需经过服务鉴权，服务的发布和订阅过程都需要进行服务鉴权。

- 被访问资源：服务名称，服务分组
- 访问对象：用户账号（包括主账号、子账号）

需要鉴权的服务权限类型包括：

- 发布权限
- 订阅权限
- 调用权限

当某用户在 EDAS 创建服务分组（ServiceGroup）时，系统默认为该用户创建与该服务分组（ServiceGroup）相关的服务发布、订阅和调用的权限。当用户为该服务分组（ServiceGroup）创建发布者或者订阅者时，EDAS管控平台会对该服务分组（ServiceGroup）进行鉴权；当用户使用该服务分组（ServiceGroup）进行服务发布和订阅时，EDAS也会对该服务分组（ServiceGroup）进行鉴权；当用户创建EDAS实例后，对于发布在EDAS上的服务调用同样需要鉴权。

鉴权流程使用阿里云AccessKey和SecretKey机制进行签名验证以及资源的权限验证。

应用管控鉴权

在EDAS平台上，明确区分主、子账号。主账号可以通过分配和授权，将指定应用的管控权限授予给指定子账号。

授权范围包括：

- 机器资源
- 负载均衡资源
- 应用资源

5.11.2.2 高可用架构

EDAS Console负载均衡

EDAS Console实例由多个机器构成，通过负载均衡设备以单一连接串的方式提供服务。当一个EDAS Console机器出现故障时，流量可在短时间内切换到其他EDAS Console机器上。整个切换过程对用户透明，应用代码无需变更，应用进程无需重启。

EDAS无中心化的服务注册中心

服务注册中心由阿里巴巴集团自主研发的软负载产品构成，RPC框架无中心单点。所有的服务调用过程，发布者和消费者均直连，无须经过中间层处理。服务注册中心仅用于服务的发现（即服务的发布和订阅）。

5.11.2.3 软件升级

- EDAS定期为您提供软件的新版本。
- 版本升级是非强制性的，只有您主动要求，才会升级到指定版本。
- EDAS升级通常在一个工作日内完成，升级期间不会出现任何应用业务异常。

5.11.2.4 服务授权

License管理

在您通过合法手段购买EDAS产品后，根据合同内容，EDAS项目组会向您发放一个包含产品系列、产品版本、节点规模、使用期限等信息在内的License。

您在第一次使用 EDAS产品时，输入该License后可正常使用。

5.12 分布式关系型数据库DRDS

5.12.1 产品介绍

分布式关系型数据库服务（Distributed Relational Database Service，简称DRDS）专注于解决单机关系型数据库扩展性问题，具备轻量(无状态)、灵活、稳定、高效等特性，是阿里巴巴集团自主研发的中间件产品。DRDS高度兼容MySQL协议和语法，支持分库分表、平滑扩容、服务升降配、透明读写分离和分布式事务等特性，具备分布式数据库全生命周期的运维管控能力。

分布式关系型数据库服务（DRDS）从多个角度提供方案来保障服务安全可靠，包括但不限于：

- 访问控制：数据库账号权限、IP白名单、危险SQL误操作保护
- 高可用架构：计算节点高可用、RDS/MySQL高可用

5.12.2 产品安全和可靠性方案

5.12.2.1 访问控制

数据库账号

DRDS支持类MySQL的账号和权限体系，具备GRANT、REVOKE、SHOW GRANTS、CREATE USER、DROP USER、SET PASSWORD等相关指令和功能。

创建DRDS数据库时，默认可以指定一个具有所有权限的账号。用此账号可以创建一个或者多个新的账号。

- 权限支持粒度：数据库和表级别（暂不支持全局、列级别）

- 支持相关联的八个基本权限项：CREATE、DROP、ALTER、INDEX、INSERT、DELETE、UPDATE、SELECT
- 支持“user@‘host’” 用户形式，对host进行访问匹配验证。

> **说明**：
> 但当业务机器处于专有网络VPC内时，因技术原因无法获取 IP，建议改成“user@‘%’”。

IP 白名单

DRDS提供了IP白名单来实现网络安全访问控制，支持为每个DRDS数据库单独设置IP白名单。

默认情况下，DRDS实例被设置为允许任何IP访问。您可以通过控制台的**DRDS数据库** > **白名单设置**页面来添加IP白名单规则。IP白名单的更新无需重启DRDS实例，不影响使用。同时，IP白名单支持设置IP地址或IP段。

> **说明**：
> 当业务机器处于专有网络VPC内时，因技术原因无法获取IP，建议去掉IP白名单。

危险SQL误操作保护

默认禁止全表删除与全表更新的高危操作，可通过加 HINT 临时跳过此限制。

下列语句默认会被禁止：

- DELETE 语句不带 WHERE 条件或者 LIMIT 条件；
- UPDATE 语句不带 WHERE 条件或者 LIMIT 条件。

效果如下：

```
mysql> delete from tt;
ERR-CODE: [TDDL-4620][ERR_FORBID_EXECUTE_DML_ALL] Forbid execute DELETE
ALL or UPDATE ALL sql. More: [http://middleware.alibaba-inc.com/faq/faqByFaqCode.html?
faqCode=TDDL-4620]
```

加 HINT 则可执行成功：

```
mysql> /*TDDL:FORBID_EXECUTE_DML_ALL=false*/delete from tt;
```

```
Query OK, 10 row affected (0.21 sec)
```

5.12.2.2 高可用架构

DRDS Server自动切流

DRDS实例由多个DRDS Server（服务进程）构成，通过负载均衡设备以单一连接串的方式提供服务。当一个DRDS Server出现故障时，流量以秒级切换到其他DRDS Server上。整个切换过程对用户透明，应用代码无需变更，应用进程无需重启。

只读实例自动切流

DRDS支持读写分离功能，可以在控制台的 **DRDS数据库** > **读写分离**页面进行配置。将部分读流量分配到备实例上。DRDS将识别出读SQL命令请求，并按照配置的比例下发到主、备RDS/MySQL实例执行，达到读写分离的目的。分配了读流量的备实例称为只读实例。

如果配置了多个只读实例，当其中一个只读实例出现故障（具体表现为无法连接）时，DRDS会自动收回故障实例上的读流量，并按照剩余正常只读实例的读流量比例重新分配执行。

只读实例自动切流过程对用户透明，应用无需重启。当所有只读实例都不可用时，为了防止主实例压力过大，将仍然按比例分配读SQL命令请求到只读实例和主实例上，并对分配到只读实例上的读SQL命令请求快速报错。

说明：
所有写SQL命令请求和事务均自动下发到主实例上执行，与只读实例的可用性无关。

5.12.2.3 软件升级

- DRDS定期提供数据库软件的新版本。
- 版本升级是非强制性的，只有您主动要求，才会升级到指定版本。
- 当DRDS评估您的版本存在重大安全隐患时，会主动通知业务安排时间进行升级。DRDS团队将会全程支持升级过程。
- DRDS升级过程通常在五分钟以内完成，升级期间可能有数次数据库连接闪断。在应用程序正确配置了数据库连接重连（或连接池）的情况下，不会对应用程序造成明显的影响。

5.12.2.4 服务授权

权限管理

在没有您授权的情况下，阿里云的售后团队和DRDS开发团队只能查看DRDS实例资源、资费和性能相关的信息（例如，DRDS实例的购买时间和到期时间，DRDS Server的CPU、内存、存储空间的使用情况，SQL 审计日志等。）

只有在获得您授权后，阿里云的售后团队和DRDS开发团队才能在您指定时间查看和修改DRDS实例的配置信息（例如，DRDS实例的IP白名单、DRDS Server的流量权重等。）

在任何情况下，阿里云的售后团队和DRDS开发团队不会主动变更DRDS实例的链接信息（包含连接地址和数据库账号。）

5.13 消息队列MQ（铂金版）

5.13.1 产品介绍

消息队列（Message Queue，简称MQ）是阿里云商用的专业消息中间件，是企业级互联网架构的核心产品。基于高可用分布式集群技术，搭建包括发布订阅、消息轨迹、资源统计、定时（延时）、监控报警等一套完整的消息云服务，帮您实现分布式计算场景中所有异步解耦功能。

MQ由阿里巴巴集团中间件技术部自主研发，是原汁原味的阿里集团中间件技术精华之沉淀，是性价比最高、最可靠的企业级消息中间件产品。

消息队列（MQ）从多个角度提供方案来保障服务安全可靠，包括但不限于：

- 访问控制：资源与账号管理，应用场景可覆盖跨账号资源授权、子账号授权、账户黑名单控制等功能。
- 高可用架构：多节点集群化部署、多副本数据存储、主备复制方式保证服务高可用以及数据高可靠。

5.13.2 产品安全和可靠性方案

5.13.2.1 访问控制

鉴权

消息队列的安全访问控制包括以下几个要素：

- 被访问资源：消息主题（Topic）
- 访问对象：用户账号（包括主账号、子账号）

消息队列的权限类型包括：

- 发布权限

- 订阅权限

当用户在消息队列上创建消息主题（Topic）时，系统会默认为该用户创建与该Topic相关的消息发布与消息订阅的权限。当用户为该Topic创建发布者或者订阅者时，消息队列管控平台会对该Topic进行鉴权；当用户使用该Topic进行消息发送和消息订阅时，MQ Broker服务也会对该Topic进行鉴权。当用户创建MQ Broker实例后，对于发布在Broker上的服务调用同样需要鉴权。

鉴权流程使用阿里云AccessKey和SecretKey机制进行签名验证以及资源的权限验证。

账号黑名单

在提供鉴权机制的同时，消息队列提供了"用户黑名单"来实现安全访问控制。

消息队列可以通过设置用户黑名单的方式，控制非法用户（恶意攻击等不合理使用的用户）对MQ进行访问，从而阻止其对消息队列进行恶意的攻击。

授权管理

每个资源有且仅有一个所有者，资源 Owner，且必须是云账号（或者专有云账号）。资源Owner对资源拥有完全控制权限。资源Owner不一定是资源创建者（例如，RAM子账号被授予消息队列管理的权限，该RAM子账号创建的资源仍归属于主账号，该RAM子账号是资源创建者但不是资源Owner。）

在未经过资源所有者授权的情况下，其他主账号或者 RAM 子账号是无法对资源进行访问的。资源所有者可以对资源进行授权或者取消授权。

授权方式包括以下两种：

- 消息队列支持在管控平台上为资源Owner提供授权功能，包括跨账号授权和子账号授权。
- 在阿里云访问控制平台上，主账号对子账号进行授权时，可根据不同的授权策略，为子账号赋予不同的权限。

5.13.2.2 高可用架构

Broker集群部署

为保证服务的可用性，消息队列支持多节点集群化部署。

- 同一个Region内支持跨机房、跨地域部署，提高网络问题的容灾能力。
- 支持集群化部署方式，提高部分节点不可用时的容灾能力。
- 消息重发机制。当某个节点服务不可用时，迅速切换到其他节点，提高集群的服务能力。

Broker主备部署

- 为保证数据的可靠性，消息队列支持一主多备部署方式。主备复制模式包括同步复制和异步复制。
- MQ Broker同时支持主备间自动切换。一旦主机出现不可用时，根据主备切换策略进行切换，迅速恢复服务。

5.13.2.3 软件升级

升级采取兼容性灰度升级策略，总体上分为MQ客户端升级、MQ Broker升级和MQ Name Server升级。

- 消息队列定期提供客户端的最新版本，每个 Release 版本都有详细说明。客户端升级为非强制性升级，只有您主动要求，才会升级到指定版本。
- MQ Name Server采取灰度发布的策略，采用分批升级的策略，升级过程对用户透明。同时，Name Server升级会保持与客户端以及Broker的兼容。
- MQ Broker升级采取灰度发布的策略，采用分批升级的策略，升级过程对用户透明。同时，Broker升级会保持与客户端的兼容。

5.14 企业实时监控服务ARMS

5.14.1 产品介绍

业务实时监控服务（Application Real-Time Monitoring Service,简称ARMS）是一款端到端一体化实时监控解决方案的PaaS级阿里云产品。通过ARMS，您可以基于海量的数据迅速便捷地通过定制化为企业带来秒级的业务监控和响应能力。ARMS产品孵化于阿里巴巴内部业务，经过长时间考验，目前已被广泛用于阿里巴巴内外的商品、物流、风控和各种云产品的各类业务监控场景。

5.14.2 产品安全和可靠性方案

5.14.2.1 访问控制

鉴权

当您访问ARMS Console实例时，ARMS将为每个用户创建独特的账户机制保障安全性。

鉴权流程使用阿里云 AccessKey 和 SecretKey 机制。具体流程如下：

1. 用户使用在ARMS控制台上创建的凭证（包含一对AccessKey和SecretKey），并用该凭证订购相应的服务获得通过。

2. 在访问的时候时，使用ARMS SDK对您的任何请求进行以下鉴权操作：

   a. 先进行签名验证，确认消息没有被篡改。

   b. 进行鉴权，检查相应的AccessKey是否有权限调用该服务。

HTTPS

ARMS Console提供将服务开放成为HTTP协议的能力，同时可以在链路上支持SSL，即HTTPS。

说明：

虽然ARMS Console提供了应用到Console之间的连接加密功能，但是SSL需要应用开启服务器端验证才能正常运转。另外，SSL也会带来额外的CPU开销，ARMS Console实例的吞吐量和响应时间都会受到一定程度的影响，具体影响视您的连接次数和数据传输频度而定。

5.14.2.2 数据隔离

ARMS保障从计算到存储之间用户数据完全隔离。

计算隔离

对于每个用户的任务，ARMS会在JStorm集群中不同的拓扑结构（Topology）进行计算。每个Topology属于且仅属于一个用户，而每个用户视情况可以拥有不同规模不同数量的Topology，以支撑其计算需求。

对于不同用户的任务，如出现异常，例如数据量过大导致内存泄露或者其他潜在程序问题，由于计算隔离，可保障不同用户之间不会受到任何干扰。

存储隔离

对于每个任务的数据集，ARMS后台在列式存储中使用单独的表来存放。其中，每张表都设置有单独的数据生命存放周期（Time to live，简称TTL），以及对应的协处理器（Coprocessor），保证任何用户的数据在升级或销毁时都不会对其他任何用户造成影响。

5.14.2.3 QoS保障策略

ARMS提供数据计算、存储写入、API 读取等多方面端到端的服务质量（Quality of Service，简称QoS）控制。

数据计算策略

- Topology配置限制策略

ARMS针对每个Topology上的数据流入模块（Storm Spout）设置了数据计算的最大内存值和最大CPU核数。这样可以保证在数据量突发暴涨的情况下造成的影响有限，不会对整个ARMS计算集群造成影响。

如果您需要应对可预估的数据量暴涨情况，则建议在突发情况下增加 Topology配 置，增大相应的任务并发数以及内存数，以解决计算规模问题。

- Topology公共任务保护策略

  对于公共任务，ARMS把多个任务放置在一个Topology进行计算。为了防止一个任务拖垮所有Topology，ARMS设置了流量和维度限制上限，防止一个任务过量计算而拖垮整个集群。

存储写入策略

ARMS针对每个用户对存储的写入做了限制，限制大小跟Topology的数量和大小成正比。

这样可以防止当数据量暴涨时，某个用户将整个存储写挂。列式存储的写入限制不会造成用户的数据丢失。当写入实际速度小于数据实际的产生速度时，计算任务会相应地被阻塞，也就是实时监控数据会有相应的延时产生。

如果您需要解决可预见的列式存储写入瓶颈，只需要增加Topology的数量和大小，以提高存储的写入QoS限制。

API读取策略

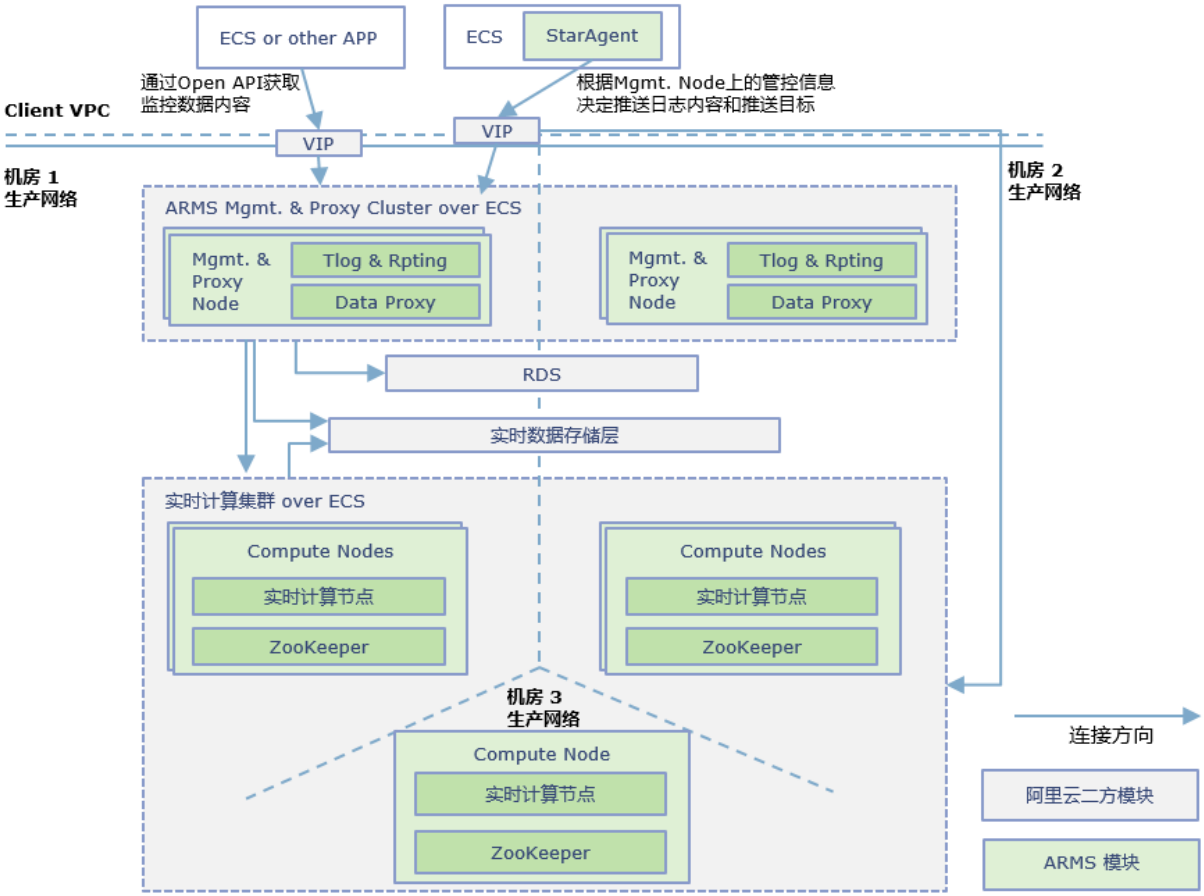
ARMS上的存储数据结果可以通过API被用户或者其他应用读取。为了防止应用将ARMS的API代理节点（ARMS Console）或存储读挂，ARMS 对 API 读取速度做了限制。默认每个用户的API读取速度限制是100。

如果有大量的API读取峰值需求，可通过调整相应QoS策略来解决。

5.14.2.4 高可用和容灾保障

ARMS的系统架构达到总体无单点，支持双站点双活式容灾。

图 5-3: ARMS系统架构图



站点内高可用

ARMS系统架构无论在数据输入层、计算层、存储层、还是 API 调用层，都采用高可用架构，且理论上支持无限横向扩张。

- 数据输入层在专有云或公共云上均可对接简单日志服务（SLS）及消息队列服务（MQ），在可用性和性能上均无单点。
- 计算层采用JStorm集群。当计算节点宕机，JStorm主控节点（Nimbus）将根据Zookeeper信息自动在健康的Supervisor上重新启动计算任务。
- 存储层采用列式存储，本身三份备份。即使两台节点同时宕机，数据仍可用。
- API调用代理层均为无状态节点，通过DNS/VIP将负载均衡分散到各代理节点，整个代理层可横向扩展。

站点间容灾策略

ARMS机房发生整体宕机时，理论上会存在分钟级恢复时间目标（RTO）和几乎为零的恢复点目标（RPO）。

- 数据接入层、计算层、数据代理层需要故障切换到容灾站点时，理论上会存在些许RTO。
- 列式存储通过多活部署，集群直接跨站点。灾难时，理论RTO为零。数据通过集群内数据复制功能，理论上能达到近乎为零的RPO 。

5.14.2.5 软件升级

- 升级采取兼容性灰度升级策略。
- 升级总体上就是ARMS Console升级。列式存储、JStorm集群以及数据接入层几乎无需或很少需要升级。
- ARMS Console升级采取灰度发布的策略，分批进行升级。

5.15 全局事务服务GTS

5.15.1 产品介绍

全局事务服务（Global Transaction Service，简称 GTS）是一款高性能、高可靠、接入简单的分布式事务中间件，用于解决分布式环境下的事务一致性问题。

传统的事务主要是指单机数据库的原子性、一致性、隔离性、持久性（Atomicity、Consistency、Isolation、Durability，简称ACID）特性。GTS在支持分布式数据库事务的基础上，将事务的范围拓展到了多种资源，让分布式环境下的多个资源的操作加入事务的范畴，赋予了分布式资源操作ACID特性。

GTS是阿里云商用的企业级产品，产品稳定性及可用性完全按照阿里巴巴内部标准来实施，应用只需要极少的代码改造和配置，即可享受分布式事务带来的便利。

全局事务服务（GTS）提供了多样化的安全加固功能来保障使用的安全，包括但不限于：

- 访问鉴权
- 流量控制
- 数据多份落盘
- 集群容灾

5.15.2 产品安全和可靠性方案

5.15.2.1 访问控制

鉴权

当用户创建GTS分组后，在使用GTS服务时需要鉴权。

鉴权过程使用阿里云AccessKey和SecretKey机制，具体流程如下：

1. 获取用户在GTS控制台上创建的分组ID，并获取阿里云给用户派发的一对AccessKey和SecretKey。
2. 在访问GTS服务端的时候，使用GTS SDK对事务调用消息进行相应的签名。
3. 在消息到达GTS服务端后，GTS服务端会进行如下鉴权操作：
   a. 进行签名验证，确认消息没有被篡改。
   b. 进行鉴权，检查相应的AccessKey和分组ID是否有权限调用该事务分组。

5.15.2.2 流量控制

在提供访问控制机制的同时，GTS提供流量控制来实现事务创建消息的访问控制，控制的量可以通过Diamond配置中心进行配置。根据用户的实际业务使用需求，GTS可以配置流量控制量的大小，保证机器不会因为事务量的突然暴增而出现异常。

5.15.2.3 数据多份落盘

GTS将事务的中间状态多份落盘存储在多台机器上，经过严格断电测试，严格保证数据一致性。

5.15.2.4 集群容灾

GTS的服务端是以集群的形式存在，一组GTS服务由三台物理机组成，提供高可用服务。即使突发事件造成集群中某一台机器崩溃，GTS仍然能够提供一半的服务能力。并且，重启崩溃的机器后，这台机器将恢复之前的事务场景，继续进行事务的处理。

5.15.2.5 软件升级

- 升级采取兼容性升级策略。
- 升级总体上分为GTS client升级和GTS server升级。
- 升级GTS client前一般要先升级GTS server。
- GTS server升级向下兼容，并在内部集成了灰度策略，升级时对用户完全没有影响。
- GTS client升级时，可以采用灰度发布策略，对于GTS client的分批升级不会造成整体的事务不可用。

5.16 云服务总线CSB

5.16.1 产品介绍

云服务总线（Cloud Service Bus，简称CSB）应用于专有云、公共云、以及混合云场景，实现跨系统、跨协议的服务互通。主要针对需要进行管理和控制，包括安全授权、流量限制的系统间服务访问和对外开放场景。

越来越多的企业组织需要以API方式把自己的核心业务资产贯通整理并开放给合作伙伴、或者让第三方的应用整合，以发掘业务模式、提高服务水平、拓展合作空间。云服务总线（CSB）面向专有云和专有域，帮助企业在自己的多个系统之间、或者与合作伙伴以及第三方的系统之间实现跨系统跨协议的服务能力互通。各个系统以发布、订购服务API的形式相互开放，并对服务API进行统一管理和组织、围绕API互动，实现企业内部各部门之间、以及企业与合作伙伴或者第三方开发者之间业务能力的融合、重塑、和创新。

云服务总线（CSB）提供了多样化的安全加固功能来保障服务调用的安全，其中包括但不限于：

- 访问控制：鉴权、IP黑白名单、防止重放、HTTPS
- 流量控制：整体流控、服务级别流控
- 容灾：服务注册中心多级存储容灾、Broker 集群容灾、Broker 同城容灾（多可用区实例）

5.16.2 产品安全和可靠性方案

5.16.2.1 访问控制

鉴权

当用户创建CSB Broker实例后，对于发布在Broker上的服务调用都需要鉴权。

鉴权过程使用阿里云AccessKey和SecretKey机制，具体流程如下：

1. 需使用在CSB控制台上创建的凭证（包括一对AccessKey和SecretKey)订购相应的服务。
2. 在访问的时候，CSB SDK对服务调用消息进行相应的签名。在消息到达Broker后，CSB Broker会进行如下鉴权操作：
   a. 进行签名验证，确认消息没有被篡改。
   b. 进行鉴权，检查相应的AccessKey 是否有权限调用该服务。

IP黑白名单

在提供鉴权机制的同时，CSB提供了IP黑白名单来实现网络安全访问控制。

默认情况下，CSB Broker实例被设置为允许任何IP访问。您可以通过控制台的来添加IP黑白名单规则。IP黑白名单的更新无需重启CSB Broker实例，不会影响使用。

- IP黑名单：支持将恶意用户的IP或者IP段加入黑名单，以阻止该用户的访问，从而阻止其对Broker进行攻击。
- IP白名单：提供了跳过鉴权控制的机制。

防止重放

CSB提供了防止请求重放的功能。默认该功能关闭，可以根据相应安全要求打开。

防止请求重放提供了如下机制：根据请求时间戳和Broker上的时间进行对比，如果超过设定的阈值，则拒绝超时的请求。

HTTPS

CSB Broker提供将服务开放成为HTTP协议的能力，同时可以在链路上支持SSL，即HTTPS。同时，在Broker之间级联的时候，也支持HTTPS协议。

说明：
虽然CSB Broker提供了应用到Broker之间的连接加密功能，但是SSL需要应用开启服务器端验证才能正常运转。另外，SSL也会带来额外的CPU开销，CSB Broker实例的吞吐量和响应时间都会受到一定程度的影响，具体影响视您的连接次数和数据传输频度而定。

5.16.2.2 流量控制

流量控制用于防止CSB Broker集群过载，防止出现极端大量请求同时到来的情况下出现的集群雪崩现象。

CSB Broker支持两个级别的流量控制：实例级别和服务级别。

实例级别流控

实例级别流控用于对每一个CSB Broker实例进行流量控制，对Broker单一实例进行过载保护。在当前的流量超过实例级别的最大流量的时候，Broker会拒绝新的请求直到流量低于最大流量。

服务级别流控

服务级别流控用于对后端接入的服务进行保护，防止通过CSB进行调用的服务流量过大，对后端的服务造成较大的影响。

服务级别的流控支持对接入CSB的每一个服务单独的设置流量控制，CSB会把服务级别的流量控制分配到每一个对应的CSB Broker实例对应的服务上。对每一个Broker而言，在当前的流量超过该实例对应服务的最大流量的时候，Broker会拒绝新请求对该服务的访问，直到流量低于最大流量。

5.16.2.3 容灾

服务注册中心多级容灾

为了保证数据完整可靠，CSB的服务注册中心采用了多级容灾的策略。

- 服务注册信息保存在数据库里，利用数据库提供的备份功能，可以采用每天或者定时备份的策略。
- CSB设计了缓存结构，Broker只和缓存的注册中心进行通信，不直接使用数据库，以防止Broker集群重启对数据库造成冲击。
- CSB Broker自身也设计了本地的内存缓存，在无法连接到缓存注册中心的时候，可以采用本地数据继续提供服务。

Broker集群容灾

CSB Broker采用无状态的设计策略，全部的状态都放在注册中心中，因此CSB Broker具备线性可扩展的特性。整个集群具备当单台机器不可用时，整体服务质量不受到大的影响的能力，并且支持集群灰度升级（需要接入层进行配合。）

5.16.2.4 软件升级

- 升级采取兼容性灰度升级策略。
- 升级总体上分为注册中心升级和CSB Broker升级。
- 注册中心升级采取灰度发布的策略，采取分批升级策略，不会造成注册中心的整体不可用。
- 注册中心在升级的过程中可能会造成短暂的服务更新延迟，在升级完毕后，可以恢复。
- 注册中心升级保持向下兼容。
- CSB Broker升级同样采取灰度发布的策略，采用分批升级策略。

5.17 MaxCompute

5.17.1 安全体系

阿里云大数据计算服务（MaxCompute）是一种快速、完全托管的GB/TB/PB级数据仓库解决方案。MaxCompute为用户提供了完善的数据导入方案以及多种经典的分布式计算模型，能够更快速的解决海量数据计算问题，有效降低企业成本，并保障数据安全。

5.17.2 身份认证

MaxCompute支持两种账号体系：阿里云账号体系和RAM账号体系。

说明：

在默认情况下，MaxCompute项目只能够识别阿里云账号系统。

5.17.3 授权管理

项目空间（Project）是MaxCompute实现多租户体系的基础，是用户管理数据和计算的基本单位。当用户申请创建一个项目空间之后，该用户就是这个空间的所有者（Owner）。也就是说，这个项目空间内的所有对象（eg、表、实例、资源、UDF 等）都属于该用户。除了Owner之外，任何人都无权访问此项目空间内的对象，除非有Owner的授权许可。

当项目空间的Owner决定对另一个用户授权时，Owner需要先将该用户添加到自己的项目空间中来。只有添加到项目空间中的用户才能够被授权。

角色（Role）是一组访问权限的集合。当需要对一组用户赋予相同的权限时，可以使用角色来授权。基于角色的授权可以大大简化授权流程，降低授权管理成本。当需要对用户授权时，应当优先考虑是否应该使用角色来完成。

MaxCompute可以对项目空间里的用户或角色，针对Project、Table、Function、Resource Instance四种对象，授予不同权限。

MaxCompute支持两种授权机制来完成对用户或角色的授权：

- **ACL授权**：ACL授权是一种基于对象的授权。通过ACL授权的权限数据（即访问控制列表，Access Control List）被看做是该对象的一种子资源，只有当对象已经存在时，才能进行ACL授权操作。当对象被删除时，通过ACL授权的权限数据会被自动删除。ACL授权支持的授权方法是采用类似SQL92定义的GRANT/REVOKE命令进行授权，通过对应的授权命令来完成对已存在的项目空间对象的授权或撤销授权。
- **Policy授权**：Policy授权是一种基于策略的授权。通过Policy授权的权限数据（即访问策略）被看做是授权主体的一种子资源。只有当主体（用户或角色）存在时，才能进行Policy授权操作。当主体被删除时，通过Policy授权的权限数据会被自动删除。Policy授权使用MaxCompute自定义的一种访问策略语言来进行授权，允许或禁止主体对项目空间对象的访问权限。

5.17.4 跨项目空间的资源分享

假设用户是项目空间的Owner或管理员（admin角色），有人需要申请访问用户的项目空间资源。如果申请人属于用户的项目团队，此时建议用户使用项目空间的用户与授权管理功能。但是如果申请人并不属于用户的项目团队， 此时用户可以使用基于Package的跨项目空间的资源分享功能。

Package是一种跨项目空间共享数据及资源的机制，主要用于解决跨项目空间的用户授权问题。

使用Package之后，A项目空间管理员可以对B项目空间需要使用的对象进行打包授权（也就是创建一个Package），然后许可B项目空间安装这个Package。在B项目空间管理员安装Package之后，就可以自行管理Package是否需要进一步授权给自己Project下的用户。

5.17.5 数据保护机制（Project Protection）

如果项目空间中的数据非常敏感，绝对不允许流出到其他项目空间中去，那么可以使用项目空间保护机制——设置ProjectProtection，明确要求项目空间中**“数据只能流入，不能流出”**。

5.18 EMR

5.18.1 产品介绍

E-MapReduce 是一套利用开源大数据生态系统，包括 Hadoop、Spark、Kafka、Storm，为用户提供集群、作业、数据等管理的一站式大数据处理分析服务。

5.18.2 产品安全和可靠性方案

5.18.2.1 用户认证-Kerberos

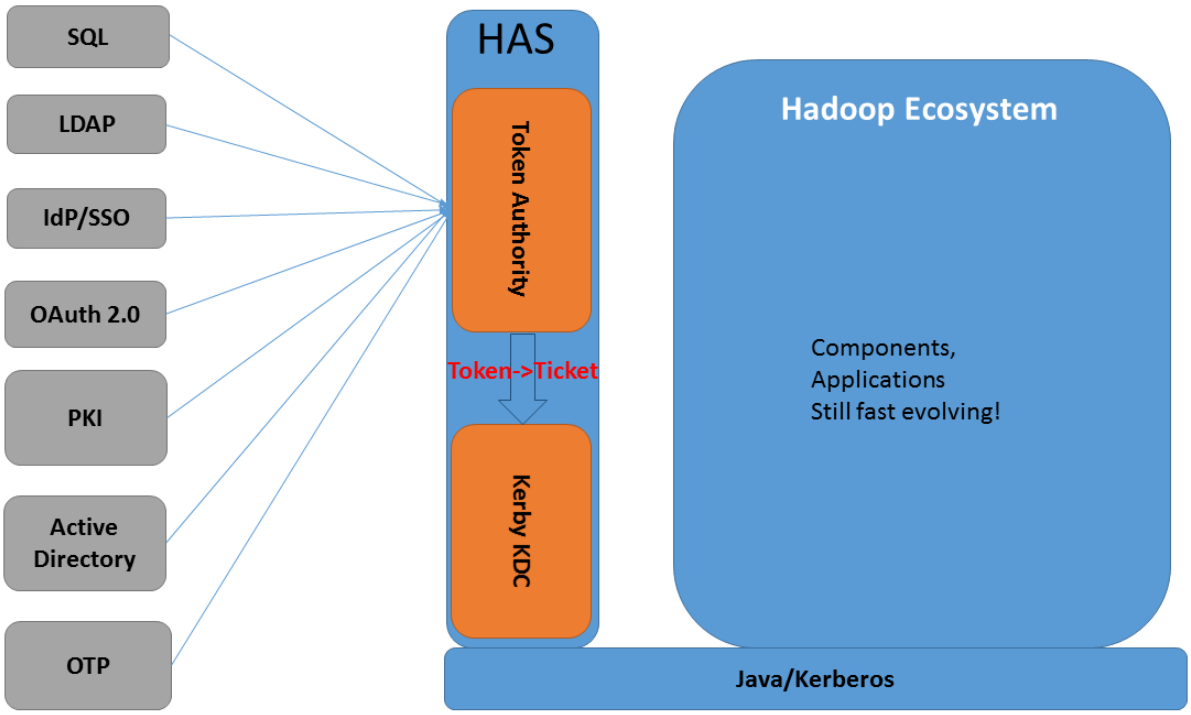
E-MapReduce目前支持的认证系统是Kerberos。

5.18.2.1.1 简介

Kerberos是一套安全的认证系统。E-MapReduce使用的是HAS(Hadoop Authentication Service)。目前开源大数据（Hadoop/Spark）在安全认证上只内置支持了Kerberos方式，HAS提供的新的认证方式(Kerberos-based token authentication)， 通过与现有的认证和授权体系进行对接，使得在Hadoop/Spark上支持Kerberos以外的认证方式变成可能，并对最终用户简化和隐藏Kerberos的复杂性。

HAS支持多种认证方式，如图 *5-4:* 认证方式所示。

图 5-4: 认证方式



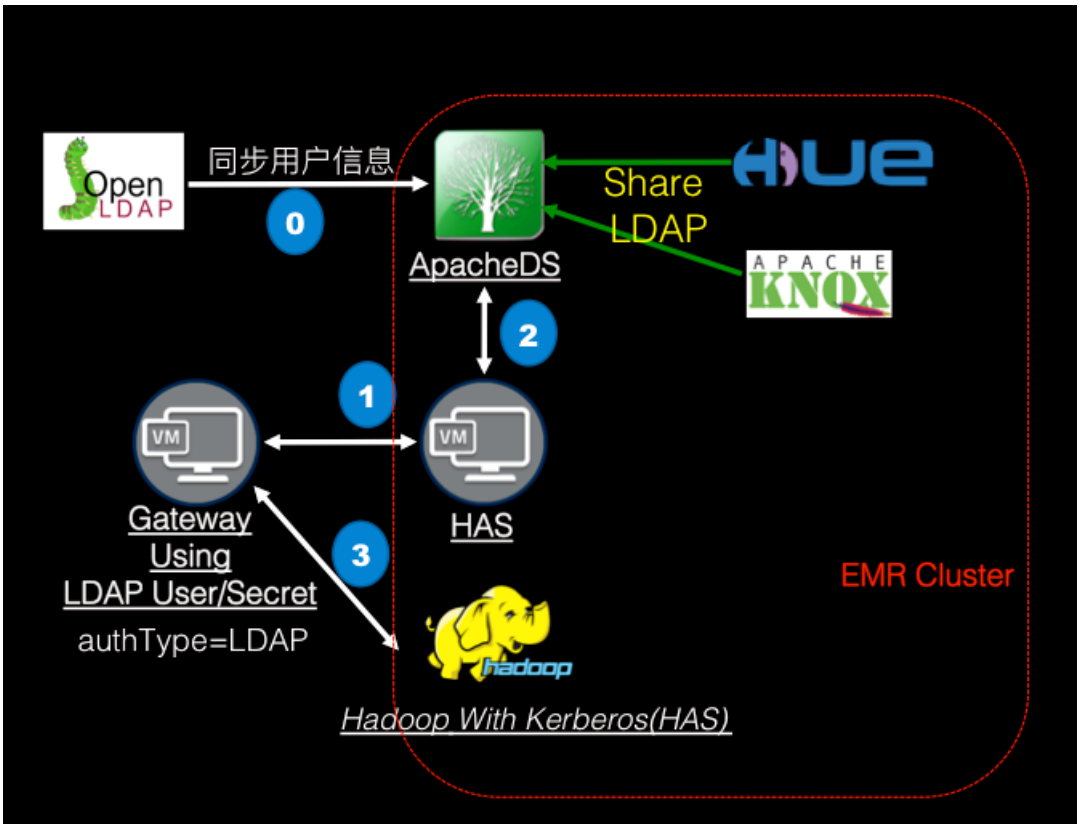
目前HAS中提供的新的认证机制Kerberos-based token authentication可以支持大数据生态系统中的大部分组件，并且对组件的改动很少或者无需改动。

所有组件都可以使用HAS提供的原有Kerberos的认证机制。

5.18.2.1.2 在E-MapReduce中的应用

LADP + Kerberos

图 5-5: LADP + Kerberos

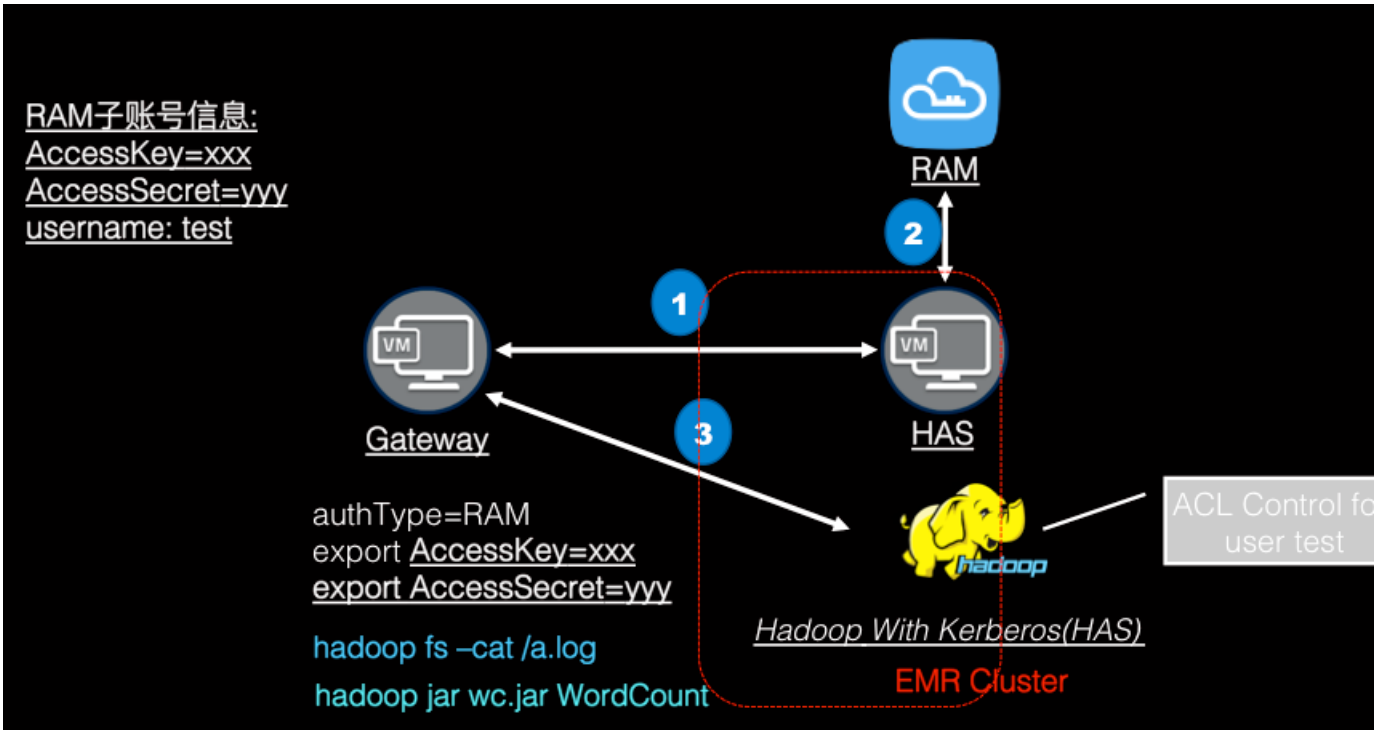


社区推荐的方式。

优势：若用户当前系统已使用了LDAP的方式，且LDAP的系统可以和HAS对接，则可以直接对接到用户已有的LDAP系统数据上。

RAM + Kerberos

图 5-6: RAM + Kerberos



RAM是阿里云上自有的一套用户权限体系，提供了在云上的统一的集中式访问控制服务。通过访问控制可以将阿里云资源的访问及管理权限分配给您的企业成员或合作伙伴。

5.18.2.1.3 使用说明

5.18.2.1.3.1 认证开启

创建集群时选择高安全模式，集群的Kerberos配置即被打开。

5.18.2.1.3.2 模式选择

修改Hadoop配置的core-site.xml文件中配置，如下所示：

```
<property>
    <name>hadoop.security.authentication.use.has</name>
    <value>false</value>
</property>
```

参数说明：

- false：LDAP模式。
- true：RAM模式。

5.18.2.1.3.3 添加用户

登录到集群的header-1节点上，一般提示为emr-header-1，进行如下操作：

1. 切换到root账号下。
2. sh /usr/lib/has-current/bin/hadmin-local.sh /etc/ecm/has-conf -k /etc/ecm/has-conf/admin.keytab
3. addprinc -pw ${password} ${username}

   其中，username是新增的KB认证用户名，password是对应的密码。

5.18.2.1.3.4 导出keytab

登录到集群的header-1节点上，一般提示为emr-header-1，进行如下操作：

1. 切换到root账号下。
2. Sh /usr/lib/has-current/bin/hadmin-local.sh /etc/ecm/has-conf -k /etc/ecm/has-conf/admin.keytab
3. ktadd -k ${username}.keytab ${username}

   其中，username是对应要导出的KB认证用户名。
4. ${username}.keytab文件在/usr/lib/has-current/ 路径下。

5.18.2.2 权限控制

创建用户后，可以将各个组件和用户进行权限授权。权限控制并不和认证强相关，即使没有认证体系，权限控制任然有效。

5.18.2.2.1 新建用户与用户组

新建用户

在集群上新建用户，需要在所有节点上（包括Master节点、Core节点、Task节点、Gateway节点）执行如下命令：

```
useradd ${username}
```

其中，username就是需要添加的集群用户，后续所有的认证和授权也将针对这个用户来进行操作。

新建用户组

如果需要使用组来聚合多个不同的用户，需要执行如下命令来创建一个用户组：

```
groupadd ${groupname}
```

其中，groupname是要新建的用户组名。

将用户加入组

如果要将用户加入到某些用户组中，则需要执行如下命令：

```
usermod –G ${groupname} ${username}
```

E-MapReduce集群上已经打通了各个节点间的访问，请参考附录一的脚本进行操作。

5.18.2.2.2 Hadoop YARN

本节主要介绍在YARN的capacity scheduler调度器下的权限控制。

使用场景

集群分配有多个队列。

关键参数

- yarn.scheduler.capacity.queue-mappings

  指定用户和queue的映射关系。

  默认用户上来，不用指定queue参数就能直接到对应的queue。这个比较方便，参数的格式为：[u|g]:[name]:[queue_name][,next mapping]*
- yarn.scheduler.capacity.root.{queue-path}.acl_administer_queue

  指定谁能管理这个队列里面的job，英文解释为“The ACL of who can administer jobs on the default queue.”。

  星号*表示all，一个空格表示none。
- yarn.scheduler.capacity.root.{queue-path}.acl_submit_applications

  指定谁能提交job到这个队列，英文解释是“The ACL of who can administer jobs on the queue.”。

  星号*表示all，一个空格表示none。

修改相关配置来支持queue acl。

- **yarn-site.xml**

  yarn.acl.enable=true
- **mapred-site.xml**

  mapreduce.cluster.acls.enabled=true
- **hdfs-site.xml**

dfs.permissions.enabled=true

这个跟capacity scheduler queue的acl无，是控制hdfs acl的，这里一并设置了。

- **hdfs-site.xml**

  mapreduce.job.acl-view-job=*

  如果配置了dfs.permissions.enabled=true，就需要配置此参数，否则无法在hadoop ui上查看job信息。

所有的配置完成以后，重启YARN和HDFS服务以生效配置。

配置示例，请参考附录二。

5.18.2.2.3 Hadoop HDFS

HDFS的认证通过Kerberos来实现。

HDFS基于社区的HDFS 权限控制方案来实施。

社区方案参考：*http://hadoop.apache.org/docs/r2.8.2/hadoop-project-dist/hadoop-hdfs/HdfsPermissionsGuide.html*

HDFS上有类似Linux的POSIX的模型，有三种权限维度：用户（user）、组（group）、其他所有人（other）。可以通过设置这三个维度的权限达到权限控制的目的，如：

- 资源只能被创建者本人读写
- 资源可以被创建者所在组内读写
- 资源可以被所有人读写
- 资源可以被指定用户读写
- 资源可以被指定组读写
- 资源临时目录

5.18.2.2.3.1 资源被创建者本人读写

```
hadoop fs -chmod 700 /user/ali
drwx------ - hadoop hadoop 0 2017-11-11 11:52 /user/ali
```

将/user/ali这个目录限制为只有用户hadoop可以访问，其他人或者是相同组内的用户不能读写。

5.18.2.2.3.2 资源被组读写

```
hadoop fs -chmod 770 /user/ali
```

```
drwxrwx---   - hadoop hadoop          0 2017-11-11 11:52 /user/ali
```

将/user/ali这个目录限制为用户hadoop和hadoop组的成员都可以读写，其他人不能读写。

5.18.2.2.3.3 资源被指定用户读写

当你做了资源被创建人本人读写、资源被组读写等限制后，又想给指定的用户做额外的设置，可以

```
hadoop fs -setfacl –m user:${username}:rwx /user/ali
drwx------+   - hadoop hadoop          0 2017-11-11 11:52 /user/ali
```

路径/user/ali除了用户hadoop可以访问外，这里写入的username这个用户也可以对这个路径进行读写访问。-m 代表在已有的权限上进行追加。

当路径后有+号时，表示这个路径除了直接看到的权限以外，还有额外的acl授权，可以通过如下方式查看：

```
hadoop fs -getfacl /user/ali
# file: /user/ali
# owner: hadoop
# group: hadoop
user::rwx
user:alibaba:rwx
group::r-x
mask::rwx
other::---
```

由上可知，有一个user:alibaba:rwx的授权，即用户alibaba有这个路径的读写访问权限。这样的授权可以有多个。

5.18.2.2.3.4 资源被指定组读写

```
hadoop fs -setfacl –m group:${groupname}:rwx /user/ali
drwx------+   - hadoop hadoop          0 2017-11-11 11:52 /user/ali
```

路径/user/ali除了用户hadoop可以访问外，这里写入的groupname这个组内的所有用户也可以对这个路径进行读写访问。

当路径后有+号时，表示这个路径除了直接看到的权限以外，还有额外的acl授权，可以通过如下方式查看：

```
hadoop fs -getfacl /user/ali
# file: /user/ali
# owner: hadoop
# group: hadoop
user::rwx
group::r-x
group:ali:rwx
mask::rwx
```

```
other::---
```

由上可知，有一个group:ali:rwx的授权，即用户组ali下的所有用户有这个路径的读写访问权限。这样的授权可以有多个。

5.18.2.2.3.5 资源临时目录

和Linux文件系统的/tmp目录一样，HDFS也有类似的临时目录。所有人都有写权限，但是默认只有创建者可以读写他创建的目录文件。许多目录就会需要拥有这种属性，比如Spark的SparkHistory目录。

```
hadoop fs -chmod 1750 /user/ali
 drwxr-x---T   - hadoop hadoop          0 2017-11-11 11:52 /user/ali
```

由上可知，在临时目录的属性里，会有一个T的标识。

5.18.2.2.4 Hive

Hive的ACL依赖于HDFS的ACL。

关键参数hive-site.xml

```
hive.metastore.pre.event.listeners=org.apache.hadoop.hive.ql.security.authorization.AuthorizationPreEventListener
hive.security.metastore.authorization.manager=org.apache.hadoop.hive.ql.security.authorization.StorageBasedAuthorizationProvide
hive.security.metastore.authenticator.manager=org.apache.hadoop.hive.ql.security.HadoopDefaultMetastoreAuthenticator
```

设置了HDFS的权限后，Hive在访问对应的资源时会进行权限的判断。同时Hive 表的meta信息也会根据HDFS的权限情况进行权限控制。例如，如果用户没有访问该表的权限，那么他也无法操作对应表的meta信息。

5.18.2.2.5 HBase

通过HBase的NameSpace的权限来进行控制。指定的用户只能在指定的NameSpace中进行表的增删改查。管理员可以授权或者收回用户的权限。

关键参数hbase-site.xml

```
hbase.security.authorization=true
hbase.coprocessor.master.classes=
org.apache.hadoop.hbase.security.access.AccessController
hbase.coprocessor.region.classes=
```

```
org.apache.hadoop.hbase.security.token.TokenProvider,org.apache.hadoop.hbase.security.
access.AccessControllerKafka
```

使用管理员进入hbase shell后，执行如下命令：

```
create_namespace 'emr'
grant 'ali','C','@emr
```

创建一个名为emr的NameSpace，然后将集群中的ali用户授权可以创建表，由这个用户新建的表该用户拥有所有的操作权限。

5.18.2.2.6 Knox

由于各个组件（YARN，HDFS等）并没有安全且可以独立控制权限的访问方式，所以引入了Knox。通过Knox可以非常方便的控制哪些页面可以被哪些用户访问。

目前Knox支持的页面如下：

- HDFS
- YARN
- Spark History
- Ganglia
- Oozie

Knox的用户身份验证基于LDAP，用户可以配置自有LDAP服务，也可以使用集群中的Apache Directory Server的LDAP服务配置。

5.18.2.2.6.1 使用集群中的LDAP服务

1. 登录集群header节点。
2. 切换到knox用户，命令如下：

   ```
   su knox
   ```

3. 执行如下命令：

   ```
   cd /usr/lib/knox-current/templates
   vi users.ldif
   ```

   将文件中所有的emr-guest替换为授权用户名。例如用户名为tom，则将“cn:EMR GUEST”替换为“cn:tom”，同时将“userPassword”的值替换为该用户密码。

   说明：

该用户与Kerbero体系的用户无关，是一个独立的账号。

4. 执行导入命令，导入到LDAP，命令如下：

```
sh ldap-sample-users.sh
```

5.18.2.2.6.2 使用自有LDAP服务

关键参数cluster-topo

```
main.ldapRealm.userDnTemplate
main.ldapRealm.contextFactory.url
```

1. 将main.ldapRealm.userDnTemplate设置为自有的用户DN模板。
2. 将main.ldapRealm.contextFactory.url设置为自有的LDAP服务器域名和端口。
3. 保存并重启Knoxcluster-topo。

一般自有的LDAP服务不在集群上运行，所以需要开启Knox访问公网LDAP服务的端口，如：10389。

说明：
为了安全起见，在此设置的授权对象必须是您的Knox所在集群的公网IP，禁止使用0.0.0.0/0。

5.18.2.2.7 Hue

Hue有自己独立的账号体系，Hue的管理员可以新建用户。

新建Hue用户时，要保证用户名和在集群上新建并进行了授权的用户名是一致的，那么在Hue上执行操作时，这个用户会受集群已有权限的限制。

例如，现在在集群上已经配置好了一个用户叫ali，在Hue中也同样要创建一个用户ali，则该用户在Hue中使用时权限会和集群上的ali用户完全一致。

5.18.2.3 附录

5.18.2.3.1 附录一

在emr-header-1节点上，保存如下的脚本并切换到hadoop用户以后，进行操作后，将会在header的2个节点，以及worker的所有节点上都添加上这个新的用户

```
sh adduser.sh ${username} ${workernum}
```

参数说明：

- username ：需要添加的用户名，如ali。

- workernum ：需要增加的集群的worker节点数量，如20。

```
echo "Start to add user..."
echo "New username is:" $1

echo "Master node start"
for i in `seq 1 2`;
do echo "deal emr-header-"$i
ssh emr-header-$i sudo useradd $1
done
echo "Master node end"

echo "Worker node start"
for i in `seq 1 $2`;
do echo "deal emr-worker-"$i
ssh emr-worker-$i sudo useradd $1
done
echo "Worker node end"
```

5.18.2.3.2 附录二

```
<configuration>
  <property>
    <name>yarn.scheduler.capacity.maximum-applications</name>
    <value>10000</value>
    <description>
      Maximum number of applications that can be pending and running.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.maximum-am-resource-percent</name>
    <value>0.25</value>
    <description>
      Maximum percent of resources in the cluster which can be used to run
      application masters i.e. controls number of concurrent running
      applications.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.resource-calculator</name>
    <value>org.apache.hadoop.yarn.util.resource.DefaultResourceCalculator</value>
    <description>
      The ResourceCalculator implementation to be used to compare
      Resources in the scheduler.
      The default i.e. DefaultResourceCalculator only uses Memory while
      DominantResourceCalculator uses dominant-resource to compare
      multi-dimensional resources such as Memory, CPU etc.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.root.queues</name>
    <value>a,b,default</value>
    <description>
      The queues at the this level (root is the root queue).
    </description>
  </property>
```

```
<property>
  <name>yarn.scheduler.capacity.root.default.capacity</name>
  <value>20</value>
  <description>Default queue target capacity.</description>
</property>

<property>
  <name>yarn.scheduler.capacity.root.a.capacity</name>
  <value>30</value>
  <description>Default queue target capacity.</description>
</property>

<property>
  <name>yarn.scheduler.capacity.root.b.capacity</name>
  <value>50</value>
  <description>Default queue target capacity.</description>
</property>


<property>
  <name>yarn.scheduler.capacity.root.default.user-limit-factor</name>
  <value>1</value>
  <description>
    Default queue user limit a percentage from 0.0 to 1.0.
  </description>
</property>

<property>
  <name>yarn.scheduler.capacity.root.default.maximum-capacity</name>
  <value>100</value>
  <description>
    The maximum capacity of the default queue.
  </description>
</property>

<property>
  <name>yarn.scheduler.capacity.root.default.state</name>
  <value>RUNNING</value>
  <description>
    The state of the default queue. State can be one of RUNNING or STOPPED.
  </description>
</property>

<property>
  <name>yarn.scheduler.capacity.root.a.state</name>
  <value>RUNNING</value>
  <description>
    The state of the default queue. State can be one of RUNNING or STOPPED.
  </description>
</property>

<property>
  <name>yarn.scheduler.capacity.root.b.state</name>
  <value>RUNNING</value>
  <description>
    The state of the default queue. State can be one of RUNNING or STOPPED.
  </description>
</property>


<property>
  <name>yarn.scheduler.capacity.root.acl_submit_applications</name>
```

```
    <value> </value>
    <description>
      The ACL of who can submit jobs to the root queue.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.root.a.acl_submit_applications</name>
    <value>root</value>
    <description>
      The ACL of who can submit jobs to the default queue.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.root.b.acl_submit_applications</name>
    <value>hadoop</value>
    <description>
      The ACL of who can submit jobs to the default queue.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.root.default.acl_submit_applications</name>
    <value>root</value>
    <description>
      The ACL of who can submit jobs to the default queue.
    </description>
  </property>

<property>
    <name>yarn.scheduler.capacity.root.acl_administer_queue</name>
    <value> </value>
    <description>
      The ACL of who can administer jobs on the default queue.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.root.default.acl_administer_queue</name>
    <value>root</value>
    <description>
      The ACL of who can administer jobs on the default queue.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.root.a.acl_administer_queue</name>
    <value>root</value>
    <description>
      The ACL of who can administer jobs on the default queue.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.root.b.acl_administer_queue</name>
    <value>root</value>
    <description>
      The ACL of who can administer jobs on the default queue.
    </description>
  </property>
```

```
  <property>
    <name>yarn.scheduler.capacity.node-locality-delay</name>
    <value>40</value>
    <description>
      Number of missed scheduling opportunities after which the CapacityScheduler
      attempts to schedule rack-local containers.
      Typically this should be set to number of nodes in the cluster, By default is setting
      approximately number of nodes in one rack which is 40.
    </description>
  </property>

  <property>
    <name>yarn.scheduler.capacity.queue-mappings</name>
    <value>u:hadoop:b,u:root:a</value>
  </property>

  <property>
    <name>yarn.scheduler.capacity.queue-mappings-override.enable</name>
    <value>false</value>
    <description>
      If a queue mapping is present, will it override the value specified
      by the user? This can be used by administrators to place jobs in queues
      that are different than the one specified by the user.
      The default is false.
    </description>
  </property>

</configuration>
```

6 专有云云盾

云盾是阿里巴巴集团多年来安全技术研究积累的成果，结合阿里云云计算平台强大的数据分析能力，为用户提供如DDoS防护、主机入侵防护、Web应用防火墙、态势感知等一站式安全服务。

6.1 云盾基础版

云盾基础版由网络流量监控、主机入侵防御、安全审计功能模块组成。

流量安全监控

流量安全监控模块是阿里云安全自主研发的毫秒（ms）级攻击监控产品。通过对专有云入口镜像流量包的深度解析，实时地检测出各种攻击和异常行为，并与其他防护模块联动防护。网络流量监控模块在整个云盾防御体系中，提供了丰富的信息输出与基础的数据支持。

流量安全监控包含以下功能：

- **DDoS攻击检测**：通过流量镜像方式，旁路检测云边界流量中的DDoS攻击。
- **流量统计**：对云产品使用流量进行计量，生成流量图。
- **网络层Web攻击拦截**：根据内嵌的Web匹配规则，对常见的Web攻击进行网络层拦截、旁路阻断。
- **IP黑名单**：对添加的IP黑名单库进行旁路TCP阻断。
- **恶意主机识别**：对云计算平台内部的恶意主机进行识别和告警。

最佳实践

通过查看不同时期、区域或单个 IP 的流量情况，可以定位流量的高峰和低谷时间、速率和地域等流量分布规律，同时通过 TOP5 流量的 IP，有效甄别恶意的 IP 访问。

主机入侵防御

主机入侵防御模块是阿里云自主研发，专门面向云服务器的安全防护模块。主机入侵防御模块默认部署在云服务器上，联动云盾云安全防护体系中的其他安全模块在主机层面为用户提供多项安全防护能力。

主机入侵防御模块提供密码暴力破解防御、木马文件检测和处理、异地登录告警等功能。

最佳实践

通过主机入侵检测功能，查看主机文件篡改、异常进程、异常网络连接、及异常端口监听记录信息，及时发现并修复主机层潜在安全风险。

安全审计

安全审计是指由专业审计人员根据有关法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价。在管理员需要对系统过往的操作做回溯时，可以进行安全审计。

阿里云的安全审计能够收集系统安全相关的数据，分析系统运行情况中的薄弱环节，上报审计事件，并将审计事件分为高、中、低三种风险等级，管理员关注和分析审计事件，从而持续改进系统，保证云服务的安全可靠。

- 安全审计模块覆盖云计算的多个业务和物理宿主机，从各个角度对行为进行收集，确保了不会因为覆盖面不够导致的审计缺失。日志收集中心集中、准实时、同步回收行为日志。
- 审计日志的存储基于云计算存储业务，通过集群化三备份，保障存储安全稳定性。存储空间也可快速扩充。
- 通过对海量日志数据构建全文索引，安全审计模块具备大量数据的快速检索查询能力。

最佳实践

根据定义的审计策略，管理人员可以及时收到告警邮件。例如，为ECS 日志的登录尝试事件设置了高风险事件的审计策略，那么在ECS日志中如果出现相关的内容，所设定的管理人员会收到告警邮件。

6.2 云盾高级版

云盾高级版在基础版的基础上增加了DDoS流量清洗、Web应用防火墙、云防火墙、和态势感知等功能，结合阿里云专业的安全运营服务为云用户提供了入侵防御、安全审计、态势感知和集中管控等一站式安全保障。

流量安全监控

流量安全监控模块是阿里云安全自主研发的毫秒（ms）级攻击监控产品。通过对专有云入口镜像流量包的深度解析，实时地检测出各种攻击和异常行为，并与其他防护模块联动防护。网络流量监控模块在整个云盾防御体系中，提供了丰富的信息输出与基础的数据支持。

流量安全监控包含以下功能：

- **DDoS攻击检测**：通过流量镜像方式，旁路检测云边界流量中的DDoS攻击。
- **流量统计**：对云产品使用流量进行计量，生成流量图。
- **网络层Web攻击拦截**：根据内嵌的Web匹配规则，对常见的Web攻击进行网络层拦截、旁路阻断。

- **IP黑名单**：对添加的IP黑名单库进行旁路TCP阻断。
- **恶意主机识别**：对云计算平台内部的恶意主机进行识别和告警。

最佳实践

通过查看不同时期、区域或单个 IP 的流量情况，可以定位流量的高峰和低谷时间、速率和地域等流量分布规律，同时通过 TOP5 流量的 IP，有效甄别恶意的 IP 访问。

主机入侵防御（高级版）

主机入侵防御模块是阿里云自主研发，专门面向云服务器的安全防护模块。主机入侵防御模块默认部署在云服务器上，联动云盾云安全防护体系中的其他安全模块在主机层面为用户提供多项安全防护能力。

主机入侵防御（高级版）模块实现以下功能：

- 通过日志监控、文件分析、特征扫描等手段，提供账号暴力破解防护、WebShell查杀、异地登录报警等防入侵措施。
- 针对性防御SQL Server、MySQL、SSH、RDP、FTP等服务的暴力破解攻击。
- 主机异常登录报警。
- 主机高危漏洞的检测和修复。

主机入侵防御（高级版）模块在基础版功能之上增加了安全基线检查功能，用户可以手动或自动对服务器做安全巡检。检测内容包括特定DDoS木马、可疑进程、系统帐户安全、数据库合规、文件访问控制、进程访问控制、文件完整性、Apache配置合规、弱口令等。

最佳实践

使用主机入侵防御功能对云服务器定期进行基线检查，发现主机存在的安全威胁漏洞并及时进行修复，提升主机的安全性。

安全审计

安全审计是指由专业审计人员根据有关法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价。在管理员需要对系统过往的操作做回溯时，可以进行安全审计。

阿里云的安全审计能够收集系统安全相关的数据，分析系统运行情况中的薄弱环节，上报审计事件，并将审计事件分为高、中、低三种风险等级，管理员关注和分析审计事件，从而持续改进系统，保证云服务的安全可靠。

- 安全审计模块覆盖云计算的多个业务和物理宿主机，从各个角度对行为进行收集，确保了不会因为覆盖面不够导致的审计缺失。日志收集中心集中、准实时、同步回收行为日志。
- 审计日志的存储基于云计算存储业务，通过集群化三备份，保障存储安全稳定性。存储空间也可快速扩充。
- 通过对海量日志数据构建全文索引，安全审计模块具备大量数据的快速检索查询能力。

最佳实践

根据定义的审计策略，管理人员可以及时收到告警邮件。例如，为ECS 日志的登录尝试事件设置了高风险事件的审计策略，那么在ECS日志中如果出现相关的内容，所设定的管理人员会收到告警邮件。

DDoS流量清洗

DDoS流量清洗模块是阿里云基于自主开发的大型分布式操作系统和十余年安全攻防的经验，为广大专有云平台用户提供基于云计算架构设计和开发的云盾海量DDoS攻击防御产品。

DDoS流量清洗模块提供以下功能：

- **海量DDoS清洗能力**：完美防御SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood 、SSDP Flood、DNS Flood、HTTP Flood、CC攻击。
- **应用层DDoS防护**：具备应用层抗DDoS攻击的能力，通过重认证、身份识别、验证码等多种手段精确识别恶意访问和真实访问者，针对网站类CC和游戏类CC攻击均可防御。
- **弹性扩展**：与阿里云DDoS攻击高防服务联动，将DDoS攻击防护能力最大扩容到1000+ Gbps。

最佳实践

DDoS流量清洗模块自动对专有云平台中的公网IP进行DDoS攻击检测及防御，在遭受DDoS攻击时，通过网络流量监控模块的检测和调度，对网络流量进行牵引、清洗和回注，有效清洗攻击流量。同时，通过查看DDoS攻击事件详细信息，了解攻击事件的流量成分及攻击源分析。

Web应用防火墙

Web应用防火墙(Web Application Firewall, WAF),基于云安全大数据能力实现，通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，过滤海量恶意访问，避免网站资产数据泄露，保障网站的安全与可用性。

WAF的工作方式是通过修改DNS记录，将Web流量引流到WAF上，由WAF将流量进行检测，过滤，清洗后再代理转发到应用服务器，完成整个WEB应用防护。

最佳实践

- **使用WAF来防止敏感信息泄露**

  防泄漏功能主要覆盖包括网站存在敏感信息泄漏，尤其是手机号、身份证、信用卡等信息的过滤。WAF可以有效防御URL未授权访问、通过越权查看漏洞访问、网页存在敏感信息被恶意爬虫爬取访问等安全威胁。

- **使用WAF有效防御WordPress反射攻击防御**

  通过精准访问控制规则有效防御WordPress反射攻击。

云防火墙

云防火墙是一款针对云环境的防火墙安全产品，主要解决云上业务快速变化带来的安全边界模糊甚至无法定义的问题。云防火墙首创性地采用基于业务可视的结果进行业务梳理和业务隔离的技术，实现专有云环境中东西向流量的安全访问控制。

最佳实践

- **实现微隔离**：通过云防火墙实现精细化的微隔离，通过业务分区、角色分组将原来为了防止业务出现中断而不得不开放的端口进行更精细的管理，缩小受攻击面，降低安全隐患。
- **协助甄别流量是否安全**：例如，HTTP流量是否都已切换为HTTPS的流量，连接TCP 3306（MySQL的业务端口）的流量是否有来自互联网的流量，这些信息，在云防火墙的流量视图中，一目了然。
- **判断服务器变更是否对业务造成影响**：服务器需要迁移和下线时，可以通过云防火墙先观察是否还存在相关流量，从而判断是否可以安全的变更。
- **发现是否存在端口滥用**：不同的业务开发部门，可能导致服务器提供同一服务（相同应用和进程）却使用了不同的业务端口。这样既浪费了端口资源，也不便于运维。通过流量的可视化，云防火墙可以清晰的甄别出此种端口滥用情况。

态势感知

态势感知区别于传统IDC和SIEM（仅支持被识别的告警事件关联），从海量的原始数据中分析信息并通过机器学习的模型完成对安全事件过程的完整还原 。同时，态势感知聚焦在"敌我态势"，对敌方的实体（黑客本人，黑客组织）进行长期的威胁情报监控和行动点技术手段观测，对我方薄弱环节进行实时感知，对安全决策具有重要参考意义。

- **弱点分析**：基于无状态扫描技术，并与网络流量安全监控联动，结合动态检测和静态匹配两种扫描模式，提供自动化、高性能的精准Web漏洞扫描能力。
- **大数据安全分析平台**：通过机器学习和数据建模发现潜在的入侵和攻击威胁，从攻击者的角度有效捕捉高级攻击者使用的0Day漏洞攻击、新型病毒攻击事件，以及有效展示正在发生的安全攻

击行为，实现业务安全可视和可感知，解决因网络攻击导致数据泄露的问题，并通过溯源服务追踪黑客身份。

最佳实践

态势感知拥有资产管理、安全监控、入侵回溯、黑客定位、情报预警等功能特性。建议在以下场景使用态势感知为云上业务提供安全天生可视和可感知：

- **弱点扫描**

  通过弱点功能及时发现主机漏洞和应用漏洞，并及时修复。同时，可以利用在弱点扫描中添加自定义的弱口令库，针对性地加强专有云平台中的口令强度，保障平台账户、应用服务安全。

- **安全态势感知**

  全面了解云上业务的安全态势，如攻击情况，漏洞情况，入侵情况，防御效果，自身业务弱点，主机对外提供服务的安全状态等。态势感知可提供网络攻击和主机攻击识别，网络异常连接检测，APT攻击识别，业务层安全威胁识别，以及安全日报发送等功能。

- **入侵行为对策**

  当用户的云上业务遭到入侵，如主机负载突然增加，收到告警短信主机ECS被入侵；或存在对外攻击行为，或网站页面出现各种恶意广告链接；或数据被加密，黑客要求给比特币赎金时，态势感知可提供以下功能：

  - **入侵检测**：可识别WannaCry勒索软件、后门Webshell、一句话木马、软件病毒、主机连接中控源等数十种入侵行为
  - **入侵行为分析**：分析入侵原因、入侵过程，支持黑客全链路行为取证
  - **安全事件详情**：查看DDoS攻击协议分析、后门地址、进程地址、攻击防御效果等

- **日志分析**

  态势感知提供全SaaS化的日志检索平台，免安装免维护，即开即用，支持逻辑（布尔表达式）检索，支持50个维度的数据逻辑组合，秒级出结果的检索引擎等功能来达到以下效果：

  - **日志分析**：通过日志证据进行调查，评估资产受损范围和影响
  - **操作审计**：对主机服务器的操作日志进行审计，对高危操作做排查
  - **业务统计**：对Web访问日志进行统计和分析，追踪来访者的环境和状态

- **大屏实时监控**

  态势感知为用户提供九块可视化大屏界面，可实时监控云上安全态势，提升团队工作效率，并进行对外形象展示和汇报。

- **代码外泄感知**

  态势感知情报采集系统，可以通过网络爬虫，抓取代码托管网站，对企业相关的情报进行实时监控和通知，避免了企业因为管理问题导致的数据外泄（如公司源码上传至Github等代码托管平台，导致企业的数据库连接地址和密码，服务器登陆密码，在代码中直接外泄）。提供企业客户相关的情报内容，包括数据泄露情报，用户名密码泄露情报，暗网相关情报，IM群攻击预谋情报等。