

# 阿里云 专有云企业版 安全白皮书

产品版本：V3.9.0

文档版本：20191018

# 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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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。	 <b>禁止：</b> 重置操作将丢失用户配置数据。
	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。	 <b>警告：</b> 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 <b>注意：</b> 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 <b>说明：</b> 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。
<b>粗体</b>	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。	执行cd /d C:/window命令，进入Windows系统文件夹。
##	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

法律声明.....	I
通用约定.....	I
1 安全白皮书介绍.....	1
2 安全责权归属与安全能力共建.....	2
2.1 权利归属.....	2
2.2 安全能力共建.....	2
2.2.1 阿里云安全责任.....	2
2.2.2 用户安全责任.....	2
3 安全合规.....	4
3.1 概述.....	4
3.2 安全合规.....	5
3.3 阿里专有云等保2.0合规能力白皮书.....	6
4 阿里云专有云安全架构.....	7
4.1 专有云安全架构概述.....	7
4.2 云平台安全.....	8
4.2.1 物理基础设施安全.....	8
4.2.2 系统安全.....	9
4.2.2.1 物理主机系统安全.....	9
4.2.2.2 虚拟化系统安全.....	10
4.2.3 分布式系统（飞天）安全.....	11
4.2.3.1 分布式文件系统安全.....	11
4.2.3.2 远程过程调用模块安全.....	11
4.2.3.3 任务调度模块安全.....	11
4.2.3.4 基础服务安全.....	11
4.2.4 网络安全.....	11
4.2.4.1 基础网络安全.....	11
4.2.4.2 网络设备安全.....	12
4.2.5 应用安全.....	12
4.2.5.1 云产品安全生命周期.....	12
4.2.5.2 云盾Web应用防火墙（平台侧）.....	13
4.2.6 数据安全.....	14
4.2.6.1 数据安全体系.....	14
4.2.6.2 数据所有权.....	14
4.2.6.3 多副本冗余存储.....	14
4.2.6.4 全栈加密.....	14
4.2.6.5 残留数据清除.....	14
4.2.6.6 运维数据安全.....	14
4.2.7 安全审计.....	15
4.2.8 账号体系安全.....	15

4.2.8.1 概述.....	15
4.2.8.2 超级管理员.....	15
4.2.8.3 云账户.....	15
4.2.8.4 身份凭证.....	16
4.2.8.5 访问控制.....	16
4.2.9 运维安全.....	17
4.2.9.1 概述.....	17
4.2.9.2 运维权限管理.....	17
4.2.9.3 天基权限管理（数据中心管理） .....	18
4.2.9.4 云盾堡垒机.....	19
4.3 安全运营服务（平台侧） .....	19
4.4 云用户（租户）安全.....	19
4.4.1 网络安全.....	20
4.4.1.1 专有网络.....	20
4.4.1.2 分布式防火墙.....	20
4.4.1.3 负载均衡.....	20
4.4.1.4 云盾流量安全监控.....	20
4.4.1.5 云盾DDoS流量清洗.....	21
4.4.1.6 云盾云防火墙.....	21
4.4.2 主机安全.....	21
4.4.2.1 云服务器操作系统.....	21
4.4.2.2 镜像加固.....	21
4.4.2.3 镜像快照.....	22
4.4.2.4 云盾安骑士.....	22
4.4.3 应用安全.....	22
4.4.3.1 代码安全.....	22
4.4.3.2 云盾Web应用防火墙.....	22
4.4.4 数据安全.....	23
4.4.4.1 云数据库.....	23
4.4.4.2 大数据计算.....	24
4.4.4.3 云盾数据库审计.....	25
4.4.4.4 云盾数据发现与脱敏.....	25
4.4.4.5 云盾加密服务.....	25
4.4.4.6 云盾敏感数据保护.....	26
4.4.5 安全管理.....	26
4.4.5.1 云盾态势感知.....	26
4.4.5.2 云盾安全审计.....	26
4.4.6 安全运营服务（租户侧） .....	27
4.4.7 安全最佳实践.....	27
<b>5 专有云云产品安全.....</b>	<b>28</b>
5.1 云服务器ECS.....	28
5.1.1 平台侧安全设计.....	28
5.1.1.1 安全隔离.....	28
5.1.1.2 鉴权认证.....	29
5.1.1.2.1 身份验证.....	29

5.1.1.2.2 访问控制.....	29
5.1.1.3 数据安全.....	30
5.1.1.3.1 概述.....	30
5.1.1.3.2 三副本存储技术.....	30
5.1.1.3.3 ECS磁盘加密.....	32
5.1.1.4 传输加密.....	32
5.1.1.5 防止ARP欺骗.....	32
5.1.2 租户侧安全功能.....	32
5.1.2.1 日志审计.....	32
5.1.2.2 安全的镜像.....	33
5.1.2.3 块存储.....	33
5.2 容器服务.....	33
5.2.1 平台侧安全设计.....	33
5.2.1.1 安全隔离.....	33
5.2.1.2 账号鉴权.....	34
5.2.1.3 链路安全.....	34
5.2.2 租户侧安全功能.....	34
5.2.2.1 应用安全.....	34
5.2.2.2 主机安全.....	36
5.3 弹性伸缩ESS.....	37
5.3.1 平台侧安全设计.....	37
5.3.1.1 安全隔离.....	37
5.3.1.2 鉴权认证.....	37
5.3.1.2.1 身份验证.....	37
5.3.1.2.2 访问控制.....	37
5.3.2 租户侧安全功能.....	38
5.3.2.1 日志审计.....	38
5.4 对象存储OSS.....	38
5.4.1 平台侧安全设计.....	38
5.4.1.1 安全隔离.....	38
5.4.1.2 鉴权认证.....	38
5.4.1.2.1 身份验证.....	38
5.4.1.2.2 权限控制.....	38
5.4.1.2.3 RAM和STS支持.....	39
5.4.1.3 数据安全.....	40
5.4.1.4 数据加密.....	40
5.4.1.4.1 服务器端加密.....	40
5.4.1.4.2 客户端加密.....	40
5.4.2 租户侧安全功能.....	40
5.4.2.1 密钥管理.....	40
5.4.2.2 日志审计.....	41
5.4.2.3 防盗链.....	41
5.5 表格存储Table Store.....	41
5.5.1 平台侧安全设计.....	41
5.5.1.1 安全隔离.....	41

5.5.1.2 鉴权认证.....	42
5.5.1.3 数据安全.....	42
5.6 文件存储NAS.....	42
5.6.1 平台侧安全设计.....	43
5.6.1.1 安全隔离.....	43
5.6.1.2 鉴权认证.....	43
5.6.1.3 数据安全.....	45
5.6.2 租户侧安全功能.....	45
5.6.2.1 日志审计.....	45
5.6.2.2 目录级读写权限 ACL.....	45
5.7 文件存储HDFS.....	47
5.7.1 平台侧安全设计.....	47
5.7.1.1 安全隔离.....	47
5.7.1.2 鉴权认证.....	47
5.7.1.3 数据安全.....	49
5.7.2 租户侧安全功能.....	49
5.7.2.1 日志审计.....	49
5.8 云数据库RDS版.....	50
5.8.1 平台侧安全设计.....	50
5.8.1.1 安全隔离.....	50
5.8.1.2 鉴权认证.....	50
5.8.1.3 数据安全.....	51
5.8.1.4 数据加密.....	51
5.8.1.5 防DDoS攻击.....	52
5.8.2 租户侧安全功能.....	53
5.8.2.1 日志审计.....	53
5.8.2.2 IP白名单.....	53
5.8.2.3 软件升级.....	53
5.9 云数据库KVStore for Redis.....	53
5.9.1 平台侧安全设计.....	53
5.9.1.1 安全隔离.....	53
5.9.1.2 鉴权认证.....	54
5.9.1.3 传输加密.....	54
5.9.2 租户侧安全功能.....	54
5.9.2.1 数据库账号.....	55
5.9.2.2 IP 白名单.....	55
5.9.2.3 备份恢复.....	55
5.9.2.4 软件升级.....	55
5.10 云数据库MongoDB版.....	55
5.10.1 平台侧安全设计.....	55
5.10.1.1 安全隔离.....	55
5.10.1.2 鉴权认证.....	56
5.10.1.3 数据安全.....	56
5.10.1.4 DDoS防护.....	57
5.10.2 租户侧安全功能.....	57

5.10.2.1 日志审计.....	57
5.10.2.2 IP白名单.....	57
5.11 云数据库KVStore for Memcache.....	57
5.11.1 平台侧安全设计.....	57
5.11.1.1 安全隔离.....	57
5.11.1.2 鉴权认证.....	58
5.11.2 租户侧安全功能.....	58
5.11.2.1 数据库账号.....	58
5.11.2.2 IP 白名单.....	58
5.11.2.3 备份恢复.....	59
5.11.2.4 软件升级.....	59
5.12 分析型数据库PostgreSQL版.....	59
5.12.1 平台侧安全设计.....	59
5.12.1.1 安全隔离.....	59
5.12.1.2 鉴权认证.....	60
5.12.1.3 主备节点.....	60
5.12.2 租户侧安全功能.....	60
5.12.2.1 数据库账号.....	60
5.12.2.2 IP白名单.....	60
5.12.2.3 SQL审计.....	60
5.12.2.4 备份恢复.....	61
5.12.2.5 软件升级.....	61
5.13 云数据库OceanBase版.....	61
5.13.1 平台侧安全设计.....	61
5.13.1.1 安全隔离.....	61
5.13.1.2 鉴权认证.....	61
5.13.1.3 高可用架构.....	62
5.13.1.4 兼容性.....	62
5.13.2 租户侧安全功能.....	63
5.13.2.1 数据库帐号.....	63
5.13.2.2 IP白名单.....	63
5.13.2.3 日志审计.....	63
5.13.2.4 软件升级.....	63
5.13.5 关于OceanBase产品存在Mysql扫描版本漏洞问题的说明函.....	64
5.14 云数据库HBase.....	65
5.14.1 平台侧安全设计.....	65
5.14.1.1 安全隔离.....	65
5.14.1.2 鉴权认证.....	65
5.14.1.3 数据安全.....	65
5.14.1.4 传输加密.....	66
5.15 数据传输服务DTS.....	66
5.15.1 平台侧安全设计.....	66
5.15.1.1 安全隔离.....	66
5.15.1.2 鉴权认证.....	66
5.15.1.3 传输安全.....	66



5.15.1.4 数据安全.....	66
5.16 数据管理DMS.....	67
5.16.1 平台侧安全设计.....	67
5.16.1.1 安全隔离.....	67
5.16.1.2 鉴权认证.....	67
5.16.1.3 传输安全.....	67
5.16.2 租户侧安全功能.....	67
5.16.2.1 操作审计.....	67
5.17 数据管理DMS企业版.....	68
5.17.1 平台侧安全设计.....	68
5.17.1.1 安全隔离.....	68
5.17.1.2 鉴权认证.....	68
5.17.1.3 数据安全.....	68
5.17.1.4 数据加密.....	69
5.17.1.5 变更安全.....	69
5.17.2 租户侧安全功能.....	70
5.17.2.1 日志审计.....	70
5.18 分布式关系型数据库DRDS.....	70
5.18.1 平台侧安全设计.....	70
5.18.1.1 安全隔离.....	70
5.18.1.2 鉴权认证.....	71
5.18.2 租户侧安全功能.....	71
5.18.2.1 IP 白名单.....	71
5.18.2.2 危险SQL误操作保护.....	71
5.18.2.3 慢SQL审计.....	72
5.18.2.4 监控信息.....	72
5.19 时间序列数据库TSDB.....	72
5.19.1 平台侧安全设计.....	72
5.19.1.1 鉴权认证.....	72
5.19.1.2 安全隔离.....	73
5.19.1.3 数据安全.....	73
5.19.2 租户侧安全功能.....	73
5.19.2.1 IP白名单.....	73
5.19.2.2 软件升级.....	74
5.20 负载均衡SLB.....	74
5.20.1 平台侧安全设计.....	74
5.20.1.1 鉴权认证.....	74
5.20.2 租户侧安全功能.....	74
5.20.2.1 HTTPS.....	74
5.20.2.2 IP白名单.....	74
5.20.2.3 日志管理.....	75
5.21 专有网络VPC.....	75
5.21.1 平台侧安全设计.....	75
5.21.1.1 安全隔离.....	75
5.21.1.2 访问控制.....	75

5.21.2 租户侧安全功能.....	75
5.21.2.1 安全组.....	75
5.22 日志服务.....	75
5.22.1 平台侧安全设计.....	75
5.22.1.1 安全隔离.....	75
5.22.1.2 鉴权认证.....	76
5.22.1.3 数据安全.....	76
5.22.1.4 传输加密.....	77
5.22.2 租户侧安全功能.....	77
5.22.2.1 服务监控.....	77
5.23 资源编排.....	78
5.23.1 平台侧安全设计.....	78
5.23.1.1 数据安全.....	78
5.23.1.2 鉴权认证.....	78
5.23.2 租户侧安全功能.....	78
5.23.2.1 日志审计.....	78
5.24 密钥管理服务KMS.....	78
5.24.1 平台侧安全设计.....	78
5.24.1.1 安全隔离.....	78
5.24.1.2 鉴权认证.....	79
5.24.1.2.1 身份验证.....	79
5.24.1.2.2 权限控制.....	79
5.24.1.2.3 RAM和STS支持.....	79
5.24.1.3 数据安全.....	79
5.24.1.4 传输加密.....	80
5.24.2 租户侧安全功能.....	80
5.24.2.1 日志审计.....	80
5.25 专有云DNS.....	80
5.25.1 租户侧安全设计.....	80
5.25.1.1 租户隔离.....	80
5.25.1.2 网络安全加固.....	80
5.25.1.3 日志审计.....	80
5.26 媒体处理MPS.....	80
5.26.1 安全隔离.....	81
5.26.2 鉴权认证.....	81
5.26.2.1 身份认证.....	81
5.26.2.2 RAM和STS支持.....	81
5.27 API网关.....	81
5.27.1 平台侧安全设计.....	81
5.27.1.1 安全隔离.....	81
5.27.1.2 鉴权认证.....	81
5.27.1.2.1 身份验证.....	81
5.27.1.2.2 API权限控制.....	82
5.27.1.2.3 RAM和STS支持.....	82
5.27.1.3 数据安全.....	82

5.27.1.4 传输加密.....	82
5.27.2 租户侧安全功能.....	82
5.27.2.1 日志审计.....	83
5.27.2.2 IP访问控制.....	83
5.28 企业级分布式应用服务EDAS.....	83
5.28.1 平台侧安全设计.....	83
5.28.1.1 鉴权认证.....	83
5.28.1.2 传输加密.....	84
5.28.2 租户侧安全功能.....	86
5.29 消息队列Apache RocketMQ版.....	86
5.29.1 平台侧安全设计.....	86
5.29.1.1 鉴权认证.....	86
5.29.1.2 安全隔离.....	87
5.29.1.3 传输加密.....	87
5.29.2 租户侧安全功能.....	88
5.29.2.1 账号黑名单.....	88
5.29.2.2 日志审计.....	88
5.30 微消息队列MQTT.....	88
5.30.1 平台侧安全设计.....	88
5.30.1.1 鉴权认证.....	88
5.30.1.2 安全隔离.....	89
5.30.1.3 传输加密.....	89
5.30.2 租户侧安全功能.....	89
5.30.2.1 账号黑名单.....	89
5.30.2.2 日志审计.....	90
5.31 业务实时监控服务ARMS.....	90
5.31.1 平台侧安全设计.....	90
5.31.1.1 安全隔离.....	90
5.31.1.2 鉴权认证.....	90
5.31.2 租户侧安全功能.....	91
5.31.2.1 HTTPS.....	91
5.32 全局事务服务GTS.....	91
5.32.1 全局事务服务GTS.....	91
5.32.2 访问控制.....	91
5.33 云服务总线CSB.....	92
5.33.1 平台侧安全设计.....	92
5.33.1.1 鉴权认证.....	92
5.33.2 租户侧安全功能.....	92
5.34 MaxCompute.....	93
5.34.1 平台侧安全设计.....	93
5.34.1.1 安全隔离.....	93
5.34.1.2 鉴权认证.....	95
5.34.1.3 数据安全.....	100
5.34.1.4 存储加密 (KMS) .....	101
5.34.1.5 传输加密.....	105

5.34.2 租户侧安全功能.....	105
5.34.2.1 跨项目空间的资源分享.....	105
5.34.2.2 数据保护机制 (Project Protection) .....	108
5.34.2.3 日志审计.....	110
5.34.2.4 IP白名单.....	110
5.35 数据工场DataWorks.....	117
5.35.1 开发/生产权限隔离.....	117
5.35.2 鉴权认证.....	118
5.35.2.1 访问控制.....	118
5.35.2.2 权限管理.....	118
5.35.3 数据加密.....	119
5.35.4 敏感数据保护.....	119
5.36 分析型数据库MySQL版.....	119
5.36.1 平台侧安全设计.....	119
5.36.1.1 安全隔离.....	119
5.36.1.2 鉴权认证.....	120
5.36.1.3 数据安全.....	121
5.36.1.4 VPC支持.....	122
5.36.2 租户侧安全功能.....	122
5.36.2.1 日志审计.....	122
5.37 实时计算Realtime Compute.....	123
5.37.1 平台侧安全设计.....	123
5.37.1.1 安全隔离.....	123
5.37.1.2 鉴权认证.....	123
5.37.1.3 数据安全.....	123
5.37.1.4 业务流程.....	124
5.38 E-MapReduce.....	124
5.38.1 平台侧安全设计.....	124
5.38.1.1 安全隔离.....	124
5.38.1.2 鉴权认证.....	125
5.38.1.3 数据安全.....	127
5.38.2 权限控制.....	129
5.39 关系网络分析Graph Analytics.....	131
5.39.1 平台侧安全设计.....	131
5.39.1.1 安全隔离.....	131
5.39.1.2 鉴权认证.....	131
5.39.1.3 数据安全.....	131
5.39.1.4 传输加密.....	131
5.39.1.5 系统安全.....	131
5.39.1.5.1 漏洞扫描机制.....	131
5.39.1.5.2 安全漏洞更新修复方案.....	132
5.39.1.5.3 系统防御机制.....	132
5.39.1.6 基础设施安全.....	132
5.39.1.7 等保认证.....	132
5.39.2 租户侧安全功能.....	132

5.39.2.1 日志审计.....	132
5.40 机器学习.....	132
5.40.1 安全隔离.....	132
5.40.2 鉴权认证.....	133
5.40.2.1 身份验证.....	133
5.40.2.2 权限控制.....	134
5.40.2.3 RAM 和 STS 支持.....	134
5.40.3 数据安全.....	136
5.40.4 日志审计.....	136
5.41 实时数据分发平台DataHub.....	136
5.41.1 平台侧安全设计.....	136
5.41.1.1 安全隔离.....	136
5.41.1.2 鉴权认证.....	137
5.41.1.3 传输加密.....	138
5.41.1.4 数据安全.....	138
5.41.2 租户侧安全功能.....	139
5.41.2.1 日志审计.....	139
5.42 DataQ.....	139
5.42.1 账号体系.....	139
5.42.2 安全隔离.....	139
5.42.3 数据安全.....	140
5.42.4 传输加密.....	140
<b>6 专有云云盾.....</b>	<b>141</b>
6.1 概述.....	141
6.2 云盾标准版.....	141
6.2.1 态势感知.....	141
6.2.2 流量安全监控.....	143
6.2.3 漏洞扫描.....	143
6.2.4 主机入侵检测.....	145
6.2.5 安骑士.....	145
6.2.6 安全审计.....	148
6.2.7 Web应用防火墙.....	149
6.2.8 云安全管理中心（SOC）.....	150
6.2.9 安全运营驻场服务.....	151
6.3 可选安全产品.....	151
6.3.1 DDoS流量清洗.....	151
6.3.2 云防火墙.....	151
6.3.3 内容安全.....	153
6.3.4 堡垒机.....	153
6.3.5 数据库审计.....	154
6.3.6 数据发现与脱敏.....	156
6.3.7 数据梳理.....	158
6.3.8 敏感数据保护.....	160
6.3.9 加密服务.....	162



# 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用户提供稳定、可靠、安全、合规的云计算基础服务，帮助保护用户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安全体系，主要包括以下内容：

- 安全责权归属与安全能力共建
- 安全合规
- 专有云平台架构安全
- 专有云各云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 安全责权归属与安全能力共建

---

### 2.1 权利归属

除非合同另有明确约定，各类专有云环境中由阿里云提供的所有产品、设计、模型算法、程序及其知识产权均归属于阿里云所有。用户在License授权许可时间段内拥有上述对象的使用权。

参考国家标准《GBT 31167-2014 信息安全技术-云计算服务安全指南》（该标准针对政府上云提出了国标安全控制方案，适用于包含专有云（私有云）的四种云计算部署形态，政府之外的其他客户使用专有云服务也可以参考该标准）中“客户提供给云服务商的数据、设备等资源，以及云计算平台上客户业务系统运行过程中收集、产生、存储的数据和文档等都应属客户所有，客户对这些资源的访问、利用、支配等权限不受限制。”专有云环境中，用户对项目规划建设的数据、运维过程中产生的运行数据、转移到云环境中的业务数据等均拥有所有权。阿里云在客户授权许可范围内拥有相关数据的使用权，用户应避免将业务数据的使用权限授予阿里云人员。

### 2.2 安全能力共建

#### 2.2.1 阿里云安全责任

在专有云环境中，阿里云负责为用户提供云计算相关产品以及解决方案、在合同约定的范围内配合在客户环境中完成部署或协助运维，承担如下责任：

- 为用户提供阿里云专有云的合规相关安全证明。
- 提供专有云相关产品漏洞识别安全服务及技术并配合客户完成专有云产品侧的修复。
- 为用户保护专有云相关信息系统或者基础环境提供解决方案和技术手段，包括但不限于权限管理、加密功能、审计功能等，并基于上述方案与手段为用户提供安全管理最佳实践，推进安全能力共建。
- 根据阿里云安全制度或者客户要求与参与专有云项目中的阿里云人员签署保密协议，并实施安全培训与教育。

#### 2.2.2 用户安全责任

参考国家标准《GBT 31167-2014 信息安全技术-云计算服务安全指南》中“信息安全管理责任不应随服务外包而转移，无论客户数据和业务是位于内部信息系统还是云服务商的云计算平台上，客户都是信息安全的最终责任人。”专有云环境中，用户负责基于阿里云或第三方提供的安全解决方案与技术手段执行专有云环境中的安全管控，并对管控结果负责，承担如下责任：



- 建立支撑专有云环境运营的安全管控人员与组织、安全制度与运营体系，管控对象应包括阿里云相关项目人员。
- 根据国家法律法规以及用户方安全制度的要求针对专有云环境中的阿里云相关项目人员进行入场审查、签署保密协议、安全培训与教育。
- 执行专有云环境中相关代码、程序等的流转管控要求，并承担由于用户方过失而导致的外泄责任。
- 主导专有云相关产品的漏洞修复过程，并在升级过程中评审相关实施方案和执行变更授权。
- 执行专有云环境中各类操作平台的账号分配、权限授予、日志审计等，做到最小化授权、常态化审计。
- 执行专有云环境中各类系统、产品的安全配置或授权阿里云驻场人员完成配置。
- 用户应对重要数据进行常态化备份与恢复演练，确保关键数据有备份且可恢复。

## 3 安全合规

### 3.1 概述

阿里云的安全流程机制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专有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。

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。阿里云具备的资格认证如下所示。

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）	阿里专有云平台具备依据GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》制定的云计算平台等级保护2.0合规能力规范（第四级）要求的安全技术能力。
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。
服务组织控制（SOC）审计认证	阿里云通过了SOC1/2的TYPEII、SOC3审计。

表 3-2: 专有云国内获得资质列表

资质/认证	颁证机构
ITSS云计算服务能力（私有云IaaS服务/一级）	中国电子工业标准化技术协会
可信云-云服务用户数据保护能力（私有云）	中国信息通信研究院
公安部信息系统安全等级评估报告（四级，专有云）	公安部信息安全等级保护评估中心
公安部信息系统专有云V3.0安全等级保护测评报告	公安部信息安全等级保护评估中心
公安部信息系统安全大数据轻量专有云平台安全评估报告	中国信息通信研究院
云测评证书-云计算参考架构-云解决方案	中国电子技术标准化研究院
可信云-开源解决方案（私有云敏捷版）/虚拟化及虚拟化管理软件	中国信息通信研究院

## 3.2 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以下部分：

### 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。

**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。阿里云具备的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**

### 3.3 阿里专有云等保2.0合规能力白皮书

针对等级保护2.0要求，在中国云计算安全等级保护合规能力规范体系技术社区指导下，依据《云计算安全等级保护合规能力框架》，由公安部信息安全等级保护评估中心和阿里云计算有限公司共同编制，发布了《阿里专有云网络安全等级保护2.0合规能力白皮书》，从等保能力验证技术架构、阿里专有云等保2.0合规状况及白皮书使用建议等方面做了详细阐述。借助白皮书，客户能够快速获取多交付场景下的专有云平台侧的合规防护能力，同时结合客户侧的应用、安全管理、物理环境等方面的保护措施，共同构筑满足等保和客户需求的信息系统整体安全防御体系。

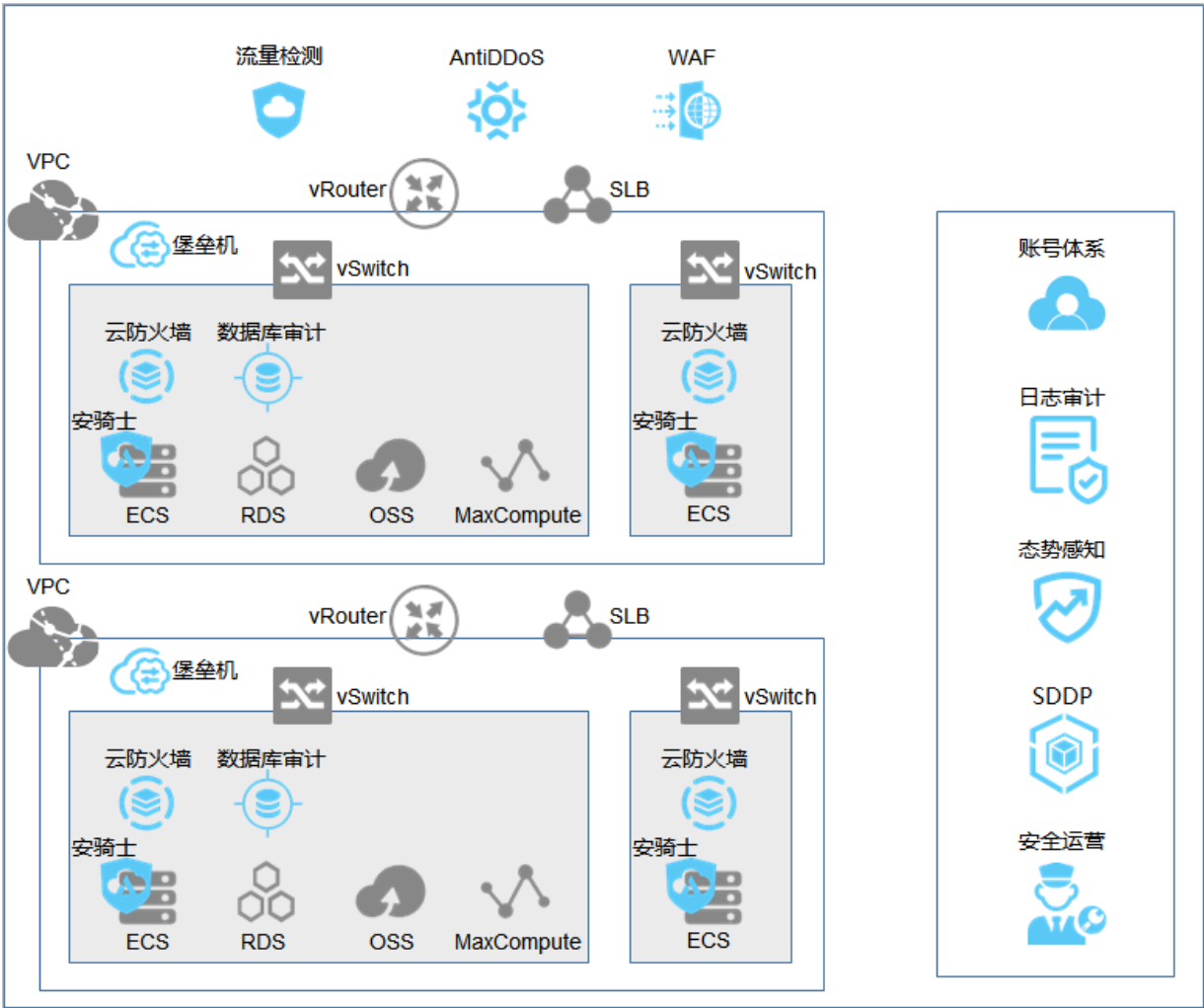
## 4 阿里云专有云安全架构

### 4.1 专有云安全架构概述

阿里云为专有云设计了多个层面的纵深防御安全体系，包括云平台侧的物理基础设施安全、系统安全、分布式系统（飞天）安全、网络安全、应用安全、数据安全、安全审计、云平台账号安全、运维安全、安全运营服务等安全架构保障；以及云用户（租户）侧的网络安全、主机安全、应用安全、数据安全、租户安全运营服务等层面的安全架构保障。



在专有云环境中，各安全产品的简单部署情况如安全部署示意图所示。



## 4.2 云平台安全

### 4.2.1 物理基础设施安全

对于专有云机房物理安全方面的要求，主要包括但不限于双路供电、访问控制、视频监控、火灾检测、热备机房等安全措施。

#### 双路供电

为保障业务7\*24小时持续运行，专有云的数据中心机房的每一个负载均由两个电源供电，两个电源之间可以进行切换。若电源发生故障，在其中一个电源失电的情况下可以投切到另一个电源供电。

#### 访问控制

对于专有云数据中心的物理设备和机房的访问要具备访问控制，包括机房的进出访问控制。例如，对于进出机房或者携带设备进出机房，物理设备的配置、启动、关机、故障恢复等，均需具备相应的访问控制策略。

## 视频监控

专有云数据中心机房应装设视频监控系统或者有专人24小时值守，对通道等重要部位进行监视。例如，对出入通道进行视频监控，同时报警设备应该能与视频监控系统或者出入口控制设备联动，实现对于监控点的有效监视。

## 火灾检测

专有云数据中心机房应配备火灾自动报警系统，包括火灾自动探测器、区域报警器、集中报警器和控制器等。火灾自动报警系统能够对于火灾发生的部位以声、光或点的形式发出报警信号，并启动自动灭火设备，切断电源、关闭空调设备等。

## 热备机房

在故障发生时，按照预先设定的故障恢复方案，使用热备份单元自动替换故障单元，实现故障的自动恢复。

## 4.2.2 系统安全

### 4.2.2.1 物理主机系统安全

阿里云对专有云物理服务器系统本身进行全面的安全加固，主要包括但不限于账号安全、文件权限、系统服务、主机入侵检测系统等方面。

## 账号安全

针对物理服务器账号的口令长度、复杂度、密码长度、口令生命期进行安全策略设置，删除空口令的账号，设置登录超时（TIMEOUT）时间等。

## 文件权限

针对重要目录进行完整性监控，在黑客篡改和写入文件时，能第一时间发现入侵行为。

## 系统服务

禁用物理服务器上不必要的系统服务，减少服务器的受攻击面。

## 云盾-主机入侵检测

在物理服务器上部署专有云云盾的主机入侵检测（HIDS）模块，其主要功能包括异常进程检测、异常端口检测、异常行为检测等。

更多关于主机入侵检测模块的介绍，查看《云盾技术白皮书》中功能特性 > 云盾标准版 > 主机入侵检测章节的描述。

## 4.2.2.2 虚拟化系统安全

虚拟化技术是云计算平台的主要技术支撑，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。阿里云的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专有云平台虚拟化层的安全。

### 租户隔离

虚拟化管理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存储隔离和网络隔离。

- 计算隔离

专有云平台提供各种基于云的计算服务，包括各种计算实例和服务，同时支持自动伸缩以满足应用程序及各用户的需求。这些计算实例和服务从多个级别提供计算隔离以保护数据，同时保障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之间、以及用户虚拟机之间的隔离，这种隔离由Hypervisor直接提供。在专有云平台使用的虚拟化环境中，将用户实例作为独立的虚拟机运行，并且通过使用物理处理器权限级别强制执行隔离，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截获并处理，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。用户实例服务器释放后，原有的磁盘空间将会被可靠地清零以保障用户数据安全。

- 网络隔离

为了支持虚拟机实例使用网络连接，阿里云将虚拟机实例连接到专有云的虚拟网络。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。

专有云平台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。同时，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

专有云平台虚拟化系统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。

## 4.2.3 分布式系统（飞天）安全

### 4.2.3.1 分布式文件系统安全

分布式文件系统使用三副本技术，将系统中的数据保存三份。如果其中一份副本丢失，系统会自动进行三副本的拷贝操作，始终保持拥有三份副本。同时，根据安全策略，三份副本不会存储在同一个物理存储介质上，保持存储的分离操作。

所有访问分布式文件系统的操作，必须通过Capability认证，只有携带了允许的Capability才能与系统进行通信，从而解决未经授权访问的操作。

存储在分布式文件系统的数据，采用二进制格式化存储的方式，避免直接查看到明文信息，造成信息泄露。

### 4.2.3.2 远程过程调用模块安全

远程过程调用模块在飞天操作系统进行通信时，采用指定的二进制格式进行通信，保证传输过程中的效率以及传输的安全，保证即使数据被中间人劫持也无法还原数据。

### 4.2.3.3 任务调度模块安全

任务调度模块采用沙箱的方式对程序进行隔离。

### 4.2.3.4 基础服务安全

针对NTP、DNS服务部署DDoS攻击防护、DNS区域传送、DNS放大攻击防御、NTP放大攻击防御等安全措施，保障NTP和DNS服务器的安全。

## 4.2.4 网络安全

### 4.2.4.1 基础网络安全

#### 逻辑隔离

专有云平台对专有云网络环境中的管理网络（OPS）、业务网络、物理网络进行了三网安全隔离。OPS网络、业务网络、物理网络三张网络之间通过网络访问控制策略实现三网逻辑隔离，彼此之间不能互相访问。同时，采取网络控制措施防止非授权设备私自连接云平台内部网络，并防止云平台物理服务器主动外连。

## IP、MAC、ARP防欺骗

在传统网络环境中，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。专有云平台通过物理服务器上的网络底层技术机制，彻底解决地址欺骗问题。

专有云平台在物理服务器数据链路层隔离由服务器向外发起的异常协议访问，阻断服务器的MAC、ARP欺骗，并在宿主机网络层防止服务器IP欺骗。

## 云盾-流量安全监控

流量安全监控模块是阿里云安全团队自主研发的毫秒（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。

更多关于流量安全监控模块的介绍，查看《云盾技术白皮书》中功能特性 > 云盾标准版 > 流量安全监控章节的描述。

## 4.2.4.2 网络设备安全

### 账号安全

针对网络设备的账号口令策略、密码配置文件的存储加密进行安全加固。

- 为网络设备建立只读账号，只允许查看配置，实现读、改配置的账号分离。
- 通过集中管控策略，实现账号的统一管理。
- 采用多因素认证的方式保障网络设备的账号安全。

### 服务

禁用网络设备上的服务，减少网络设备的受攻击面；并且禁用与网络设备不相关的功能。

### 日志集中化

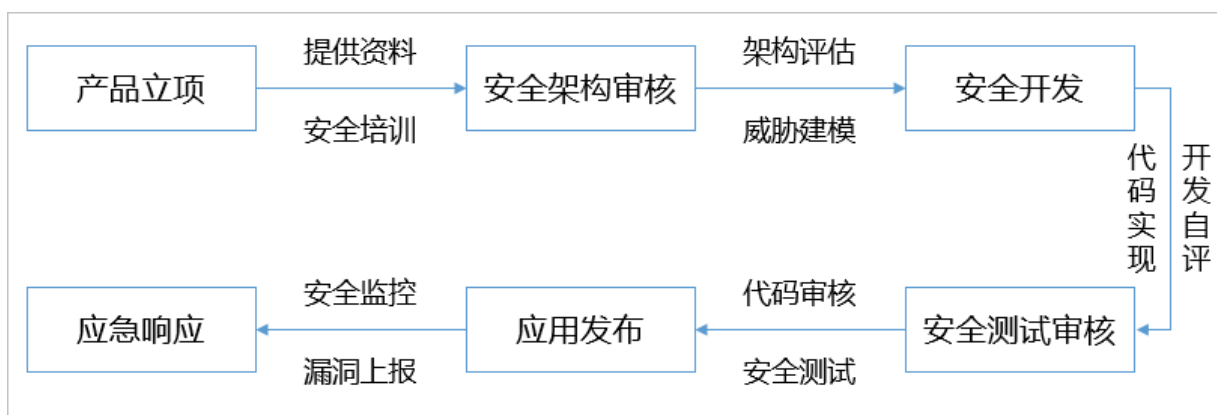
将网络设备产生的日志进行集中化收集和管理。

## 4.2.5 应用安全

### 4.2.5.1 云产品安全生命周期

云产品安全生命周期（Secure Product Lifecycle，简称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。



- 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。
- 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》。
- 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，为下一阶段的安全测试审核做好准备。
- 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。
- 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。
- 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。

#### 4.2.5.2 云盾Web应用防火墙（平台侧）

专有云平台针对平台应用安全应采用云盾-Web应用防火墙（Web Application Firewall，简称WAF）来进行安全防御。WAF主要解决的问题是针对应用的OWASP TOP10的攻击（包括SQL注入攻击、XSS攻击等Web应用攻击）进行阻断和拦截，保障中间件和平台应用的安全性。

更多关于云盾Web应用防火墙模块的介绍，查看《云盾技术白皮书》中功能特性 > 云盾标准版 > Web应用防火墙章节的描述。

## 4.2.6 数据安全

### 4.2.6.1 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控，实现数据安全目标。

专有云平台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。

### 4.2.6.2 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。

### 4.2.6.3 多副本冗余存储

专有云使用分布式存储技术，将文件分割成许多数据片段分散存储在不同的设备上，并且将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。

### 4.2.6.4 全栈加密

专有云对于数据安全提供了全栈的加密保护能力，包括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，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。

### 4.2.6.5 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。

### 4.2.6.6 运维数据安全

运维人员未经用户许可，不得以任何方式访问用户未经公开的数据内容。

专有云平台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。

## 4.2.7 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进行回溯时，可以进行安全审计。

阿里云的安全审计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。管理员通过关注和分析审计事件，持续改进系统，保证云服务的安全可靠。

安全审计覆盖云计算平台多个业务和物理宿主机，从各个角度对行为进行收集，确保不存在因覆盖面不够而导致的审计缺失。

审计日志收集中心集中、准实时、同步回收所有行为日志。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，其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，安全审计同时具备大量数据的快速检索查询能力。

## 4.2.8 账号体系安全

### 4.2.8.1 概述

专有云平台提供多种安全机制来帮助用户保护账户安全，防止未授权的用户操作。这些安全机制包括云账户登录、创建子用户、集中管理子用户权限、数据传输加密、子用户操作审计等，用户可以使用这些机制来保护云账户的安全。

### 4.2.8.2 超级管理员

专有云平台默认有一个超级管理员，超级管理员可以用来创建系统管理员并以短信、邮件的形式通知缺省密码。首次登录专有云管控平台需要修改登录用户名的密码，务必按照提示完成密码修改。同时，为提高安全性，密码必须满足最小复杂度要求，即包含英文大/小写字母（A~Z、a~z）、数字（0~9）、特殊符号（如!、@、#、\$、%等）中的两种，并且密码长度为8~20位。

### 4.2.8.3 云账户

无论是专有云平台的运维管理，还是云租户的资源管理，都统一使用云账户。

云账户是云产品资源归属、资源使用计量的基本主体。当用户开始使用专有云服务时，首先需要注册一个云账户。云账户对其名下所有资源拥有完全权限。默认情况下，资源只能被属主（ResourceOwner）所访问，任何其他用户访问都需要获得属主的显式授权（即将对象授权给用户）。因此，从权限管理的角度来看，云账户相当于操作系统的Root或Administrator账户，云账户有时也被称为根账户或主账户。

通过对云账户授权，可使其拥有云资源的管理权限或者云平台的运维权限。云平台的运维权限通过OAM管理，云租户的资源管理权限通过RAM管理，同时RAM支持主子账号体系。

#### 4.2.8.4 身份凭证

身份凭证是用于证明用户真实身份的凭据，通常指登录密码或访问密钥（AccessKey）。身份凭证是秘密信息，用户必须保护好身份凭证的安全。

- 登录名/密码（Password）

用户可以使用登录名和密码登录Apsara Stack控制台，申请资源并通过控制台进行资源操作。

- 访问密钥（AccessKey）

用户可以使用访问密钥构造一个API请求（或者使用云服务SDK）来操作资源。

#### 4.2.8.5 访问控制

云租户可以使用RAM建立主子账号体系。

访问控制管理（Resource Access Management，简称RAM）是专有云平台为用户提供的用户身份管理与访问控制服务。通过RAM，可以创建、管理用户账号（比如员工、系统或应用程序），并可以分配这些用户账号对其名下资源具有的操作权限。当存在多用户协同操作资源时，使用RAM可以避免与其他用户共享云账号密码或访问密钥，按需为用户分配最小权限，从而降低信息安全风险。

##### RAM用户身份类型

RAM支持两种不同的用户身份类型：RAM-User和RAM-Role。

- RAM-User

RAM-User是一种实体身份，有确定的身份ID和身份认证密钥，它通常与某个确定的人或应用程序一一对应。

- RAM-Role

RAM-Role是一种虚拟身份，有确定的身份ID，但没有确定的身份认证密钥。RAM-Role需要与某个实体身份进行关联之后才能被使用。一个RAM-Role可以与多种实体身份关联，比如可以与当前云账号下的RAM-User关联，与其他云账号下的RAM-User关联，与专有云服务（例如ECS）关联，与外部实体身份（如企业本地账号）关联。

##### 权限

权限是允许（Allow）或拒绝（Deny）一个用户对某种资源执行某种操作。

操作可以分为两大类：资源管控操作和资源使用操作。

- 资源管控操作是指云资源的生命周期管理及运维管理操作。例如，ECS实例的创建、停止、重启等，OSS存储空间的创建、修改、删除等。资源管控所面向的用户一般是资源拥有者或企业组织内的运维员工。
- 资源使用操作是指使用资源的核心功能。例如，ECS实例操作系统中的用户操作，OSS存储空间的数据上传/下载。资源使用所面向的用户则是企业组织内的研发员工或应用系统。

对于弹性计算和数据库产品，资源管控操作可以通过RAM来管理，而资源使用操作是在每个产品的实例内进行管理。例如，ECS实例操作系统的权限控制，MySQL数据库的权限控制。对于存储类产品（如OSS、Table Store等），资源管控操作和资源使用操作都可以通过RAM来管理。

## 授权策略

授权策略是描述权限集的一种简单语言规范。

RAM支持两种类型的授权策略：专有云平台管理的系统访问策略和用户管理的自定义访问策略。

对于专有云平台管理的系统访问策略，用户只能使用，不能修改，云平台会自动完成系统访问策略的版本更新；对于用户管理的自定义访问策略，用户可以自主创建和删除，策略版本由用户自己维护。

RAM允许在云账号下创建并管理多个授权策略，每个授权策略本质上是一组权限的集合。管理员可以将一个或多个授权策略分配给RAM用户（包括RAM-User和RAM-Role）。RAM授权策略语言可以表达精细的授权语义，可以指定对某个API-Action和Resource-ID授权，也可以支持多种限制条件（源IP、访问时间等）。

## 4.2.9 运维安全

### 4.2.9.1 概述

专有云提供一套集中化的运维管理系统，Apsara Stack运维系统 ASO，面向专有云的各类运维管理角色，包括驻场的运维工程师、用户自身的运维工程师、云平台运维管理工程师、运维安全管理或审计人员等，通过Apsara Stack运维系统，运维工程师能够及时掌控系统运行状况，并进行相应的运维操作。

### 4.2.9.2 运维权限管理

运维权限管理系统（Operation Administrator Manager，简称OAM）是Apsara Stack运维系统的权限管理平台。OAM采用一种简化的基于角色的访问控制（RBAC）模型，管理员可以通过OAM为运维人员授予角色，运维人员依据各自的角色，对各运维系统拥有相应的操作权限。

## OAM权限模型

基于角色的访问控制，即管理员不直接将系统操作的各种权限授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角

色后，该用户就拥有此角色的所有操作权限。因此，不必在每次创建用户时都进行分配权限的操作，只需分配用户相应的角色即可。而且，角色的权限变更比用户的权限变更要少得多，这样既能简化用户的权限管理，又能减少系统的开销。

#### OAM授权体系

管理人员需要通过设置以下参数项根据运维人员的不同角色进行授权：

- 主体 (Subject)：访问控制系统的操作者，在OAM中包括用户和组两种类型的主体。
- 用户 (User)：运维系统的管理员和操作员。
- 组 (Group)：多个用户的集合。
- 角色 (Role)：基于角色访问控制系统的核心。通常情况下，角色可以理解为一系列权限的集合。一个角色内可以包含多个角色单元和/或多个角色。
- 角色嵌套 (RoleHierarchy)：OAM系统中，一个角色可以包含其他角色，形成角色嵌套。
- 角色单元 (RoleCell)：权限点的具体描述，一个角色单元由资源、操作集合和授权选项组成。
- 资源 (Resource)：授权客体的描述。关于各运维平台的资源说明，参见各运维平台操作权限列表。
- 操作集 (ActionSet)：授权操作的描述，一个操作集可以包含多个操作。各运维平台的操作说明请参见各运维平台操作权限列表。
- 授权选项 (WithGrantOption)：级联授权的最大授权次数，必须是一个大于或等于0的整数。数值为非0时，代表该权限可下放；数值为0则权限不可下放。

例如：管理员A为管理员B授权时填写的授权选项为5，意味着该权限最多还可以被下放5次；管理员B可以为管理员C授权该权限，此时授权选项能够填写的值，最大为4；管理员B也可以为操作员D授权该权限，设置授权选项为0，操作员D仅能使用该权限，无法把权限再次授权给其他人。

#### 4.2.9.3 天基权限管理（数据中心管理）

天基是一套自动化的数据中心管理系统，管理专有云数据中心的硬件生命周期与各类静态资源，包括程序、配置、操作系统镜像、数据等。

天基为飞天系统及专有云各种产品的应用及服务提供了一套通用的版本管理、部署以及热升级方案，使得基于天基的服务在大规模分布式的环境下达到自动化运维的效果，极大地提高运维效率，并提高系统可用性。

#### 权限管理

天基的权限管理也采用OAM系统。天基用户权限包括天基Admin权限、Project权限和Service权限：



- **Admin权限**：Admin用户可以对整个天基平台的页面进行操作。
- **Project权限**：
  - 普通用户需要由管理员开通Project权限，才能查看天基平台中运维 > Project运维中的Project信息。
  - 普通用户需要由管理员开通Project权限，才能查看天基平台中运维 > 集群运维中的集群信息并执行该节点下的相关操作。
- **Service权限**：普通用户需要由管理员开通Service权限，才能查看天基平台中运维 > 服务运维中的服务信息并执行该节点下的相关操作。

#### 4.2.9.4 云盾堡垒机

云盾堡垒机模块为专有云平台物理服务器的运维提供完整的审计回放和权限控制服务。基于账号（Account）、认证（Authentication）、授权（Authorization）、审计（Audit）的AAAA统一管理方案，通过身份管理、授权管理、双因子认证、实时会话监控与切断、审计录像回放、高危指令查询等功能，增强运维管理的安全性。

更多关于堡垒机模块的介绍，查看《云盾技术白皮书》中功能特性 > 可选安全产品 > 堡垒机章节的描述。

### 4.3 安全运营服务（平台侧）

针对专有云平台侧，专有云云盾提供多种平台安全运营服务。

#### 安全巡检

调研整理云平台业务清单，包括各个产品的物理机数量、产品版本等。同时，对云平台提供的基础安全产品的事件日志进行分析，并对产生的安全风险进行处理。

#### 安全评估与加固

对云平台的系统进行安全评估，发现云平台中存在的网络安全、主机安全、应用安全隐患，并针对发现的安全隐患进行加固。

#### 漏洞修复

对云平台运行过程中发现的安全漏洞（口令问题、配置问题等）进行修复。

#### 安全应急响应

出现类似于入侵的紧急安全事件时，及时应急止血并分析事件成因。

### 4.4 云用户（租户）安全

## 4.4.1 网络安全

### 4.4.1.1 专有网络

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，并支持自定义IP 地址范围、网段、路由表和网关等。同时，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。

#### 安全隔离

使用隧道技术，达到与传统VLAN方式相同的隔离效果。在网卡级别实现广播域的隔离；通过VLAN级别的隔离，彻底阻断网络通讯；通过划分不同的安全域，进行访问控制。

#### 访问控制

基于安全组防火墙实现灵活的访问控制规则。

### 4.4.1.2 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，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云服务器的网络访问控制规则，安全组作为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，通过授权某个源安全组或某个源网段访问目的安全组实现互通。

### 4.4.1.3 负载均衡

负载均衡（Server Load Balancer，简称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。

### 4.4.1.4 云盾流量安全监控

云盾流量安全监控是阿里云安全团队自主研发的毫秒（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。同时，将安全事件上报到专有云云盾安全中心，与其他防护系统产生联动，提供丰富的信息输出与基础的数据支撑。

更多关于流量安全监控模块的介绍，查看《云盾技术白皮书》中功能特性 > 云盾标准版 > 流量安全监控章节的描述。

### 4.4.1.5 云盾DDoS流量清洗

云盾DDoS流量清洗结合云盾流量安全监控模块提供DDoS攻击自动检测、调度和清洗功能，可以在五秒内完成攻击发现、流量牵引和流量清洗全部动作，保证云租户业务网络的稳定性。同时，云盾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，实现精准识别DDoS攻击，保障遭受DDoS攻击时用户业务的可用性。

更多关于DDoS流量清洗模块的介绍，查看《云盾技术白皮书》中功能特性 > 可选安全产品 > DDoS流量清洗章节的描述。

### 4.4.1.6 云盾云防火墙

云盾云防火墙是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。首创性地采用“基于业务可视化的结果进行业务梳理和业务隔离”的技术，云防火墙帮助用户实现专有云环境中东西向流量的安全访问控制。

更多关于云防火墙模块的介绍，查看《云盾技术白皮书》中功能特性 > 可选安全产品 > 云防火墙章节的描述。

## 4.4.2 主机安全

### 4.4.2.1 云服务器操作系统

用户拥有对云服务器ECS实例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，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。例如，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` 指令的方式实现临时提权等。

### 4.4.2.2 镜像加固

镜像是云服务器 ECS实例运行环境的模板，一般包括操作系统和预装的软件。用户可以使用镜像创建新的ECS实例或更换ECS实例的系统盘。

阿里云基础镜像（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。基础镜像默认采用主机最佳安全实践配置，并且所有阿里云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。

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，用户应迅速更新基础镜像。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。

### 4.4.2.3 镜像快照

专有云平台的云服务器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，便于用户快速实现灾难恢复。用户可以使用快照创建自定义镜像，将快照的操作系统、数据环境信息完整地包含在镜像中。快照采用增量方式，两个快照之间只有数据变化的部分才会被拷贝。

### 4.4.2.4 云盾安骑士

云盾安骑士模块通过日志监控、文件分析、特征扫描等手段，为云服务器ECS提供漏洞管理、基线检查、入侵检测、资产管理等安全防护措施。安骑士模块包含客户端和服务端，客户端配合服务端监测针对主机系统层和应用层的攻击行为及漏洞信息，实时防护主机安全。

#### 漏洞管理

安骑士提供的云服务器漏洞管理综合了多套扫描引擎（网络端、本地端、PoC验证），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。

#### 基线检查

安骑士的基线检查功能自动检测云服务器上的系统、数据库、账号配置存在的风险点，并针对所发现的问题项提供修复建议。

#### 入侵检测

安骑士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。

更多关于安骑士模块的介绍，查看《云盾技术白皮书》中功能特性 > 云盾标准版 > 安骑士章节的描述。

## 4.4.3 应用安全

### 4.4.3.1 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。

### 4.4.3.2 云盾Web应用防火墙

云盾Web应用防火墙是面向云租户Web应用的安全防护系统，基于智能语义分析引擎实现，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。

更多关于Web应用防火墙模块的介绍，查看《云盾技术白皮书》中功能特性 > 云盾标准版 > Web应用防火墙章节的描述。

## 4.4.4 数据安全

### 4.4.4.1 云数据库

#### 租户隔离

专有云环境云数据库采用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访问系统文件，确保用户无法接触其他用户的数据。

#### 数据库账号

用户创建云数据库实例后，系统并不会为用户创建任何初始的数据库账户。用户需要通过控制台或者API的方式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（如表、视图、字段级别的权限控制），也可以通过控制台或者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，并用超级数据库账户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，云数据库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API的方式添加IP白名单规则。IP白名单规则更新无需重启云数据库实例即可生效，因此不会影响用户的正常使用。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。

#### 专有网络隔离

除IP白名单外，云数据库还支持用户使用VPC来获取更高程度的网络访问控制。VPC是用户在云平台中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，在网络二层完成访问控制。同时，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平台，并使用VPC自定义的云数据库实例IP段来解决可能的IP资源冲突的问题，实现自有服务器和云服务器同时访问云数据库实例的目的。

使用VPC和IP白名单将极大程度提升云数据库实例的安全性。

#### 数据传输加密

云数据库支持安全套接层协议（Secure Sockets Layer，简称SSL）。用户可以使用服务器端的根证书来验证目标地址和端口的数据库服务是否由云数据库提供的，从而有效避免中间人攻击。除此之外，云数据库还提供服务器端SSL证书的启用和更新能力，以使用户按需更换SSL证书以保障安全性和有效性。

## 主备节点

云数据库采用三节点副本集的高可用架构，三个数据节点位于不同的物理服务器上，自动同步数据。Primary和Secondary节点提供服务，当Primary节点出现故障，系统自动选举新的Primary节点，当Secondary节点不可用，由备用节点接管服务。

同时，云数据库提供自动备份功能，支持一键式数据恢复，保证数据的完整可靠。

## 4.4.4.2 大数据计算

### 授权管理

项目空间（Project）是专有云平台大数据计算服务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（如表、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，除非获得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，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。

大数据计算服务支持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。

### 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），其它用户需要申请访问用户的项目空间资源。如果申请人属于该用户的项目团队，建议用户使用项目空间的用户与授权管理功能；如果申请人并不属于该用户的项目团队，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。

### 数据保护机制

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时，可以使用项目空间保护机制（设置ProjectProtection）。明确要求该项目空间中的数据只能流入，不能流出。

#### 4.4.4.3 云盾数据库审计

云盾数据库审计是随着用户应用上云、云端数据安全面临挑战而推出的适用于专有云环境中数据库安全审计的产品。基于阿里巴巴集团多年数据库安全技术积累，数据库审计系统将传统产品与云端相结合，在专有云环境中形成一套为数据库运维和安全管理提供安全、诊断与维护能力为一体的安全管理工具。

数据库审计系统实现了对云端自建数据库、云数据库访问的精确审计及准确的应用用户关联审计，并具备风险状况、运行状况、性能状况、语句分布的实时监控能力。

更多关于数据库审计模块的介绍，查看《云盾技术白皮书》中功能特性 > 可选安全产品 > 数据库审计章节的描述。

#### 4.4.4.4 云盾数据发现与脱敏

在专有云业务场景中，随着数据资产的不断增加，管理员往往很难直观的了解云上自己的数据库有多少台、如何分布、是否启用。通过数据库发现功能，能够扫描云数据库的分布，自动发现专有云内的所有数据库。同时，通过数据脱敏功能有效防止企业内部对隐私数据的滥用，防止隐私数据在未经脱敏的情况下从企业流出。满足专有云环境中，既要保护隐私数据，又要满足开发、测试、模型训练等业务对数据的需求；同时也保持监管合规，满足企业合规性。

- 数据发现：通过扫描IP段设备流量信息检测数据资产，发现数据库分布；通过系统内置发现规则发现敏感数据，对其敏感数据分级分类，呈现可视化敏感数据分布；通过对资产SQL语句量和会话并发量判断资产使用热度，根据流量统计发现静默资产；通过数据库授权发现资产权限分布及权限详情。
- 数据脱敏：通过对敏感数据进行数据抽取、数据漂白、和动态掩码的脱敏处理，满足生产数据面向测试、开发、培训和数据共享场景的数据安全需求，实现“用”、“护”结合。

更多关于数据库发现与脱敏模块的介绍，查看《云盾技术白皮书》中功能特性 > 可选安全产品 > 数据库发现与脱敏章节的描述。

#### 4.4.4.5 云盾加密服务

数据是企业核心资产，每个企业都有自己的核心敏感数据，包括企业自身的敏感数据（如合同、交易、流水信息等）、企业用户的敏感数据（如身份证、银行卡信息等），这些数据都需要加密服务来保护不会被他人获取。

云盾加密服务是一款云上加密解决方案。服务底层使用经国家密码管理局检测认证的硬件密码机，通过虚拟化技术，帮助用户满足数据安全方面的监管合规要求，保护云上业务数据的隐私性要求。借助加密服务，用户能够对密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

更多关于加密服务模块的介绍，查看《云盾技术白皮书》中功能特性 > 可选安全产品 > 加密服务章节的描述。

#### 4.4.4.6 云盾敏感数据保护

敏感数据保护（SDDP）系统充分使用阿里巴巴大数据分析能力以及人工智能相关技术，通过智能化敏感数据识别，基于业务需求实现分类分级，并在精准识别基础上实现动态与静态脱敏、全域流转监控与异常检测，达到精准识别、精准检测、精准分析、有效保护，实现可见、可控、合规的安全保护要求。该产品支持MaxCompute、OSS、ADS、OTS等阿里云大数据产品。

更多关于敏感数据保护模块的介绍，查看《云盾技术白皮书》中功能特性 > 可选安全产品 > 敏感数据保护章节的描述。

### 4.4.5 安全管理

#### 4.4.5.1 云盾态势感知

云盾态势感知模块是一款由阿里云安全团队自主研发的大数据安全分析系统。通过机器学习和数据建模对专有云环境中主机流量和网络流量进行深度解析，检测各种威胁、攻击、访问等异常行为，从攻击者的角度有效捕捉高级攻击者使用的漏洞攻击、新型病毒攻击事件，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。

同时，态势感知基于互联网可视化技术，将大数据威胁分析成果以直观的图形呈现于可视化大屏，提供安全整体态势信息，作为用户专有云平台安全决策的重要支撑工具。

更多关于态势感知模块的介绍，查看《云盾技术白皮书》中功能特性 > 云盾标准版 > 态势感知章节的描述。

#### 4.4.5.2 云盾安全审计

云盾安全审计模块提供基于云计算平台的一体化审计解决方案。对标信息系统安全等级保护基本要求，安全审计模块从物理服务器层面、网络设备层面、云计算平台应用层面分别进行审计，实现行为日志的收集、存储、分析、报警等功能。

通过采集各个云产品、网络设备、主机、数据库等数据源的相关日志，并通过所设置的审计规则结合审计规则引擎完成对整个专有云的安全审计工作，对于触发规则的操作进行报警提示。同时，安全审计提供日志查询与规则配置功能，全面满足用户的等保需求。

更多关于安全审计模块的介绍，查看《云盾技术白皮书》中功能特性 > 云盾标准版 > 安全审计章节的描述。



## 4.4.6 安全运营服务（租户侧）

阿里云提供对云租户的安全运营服务，针对租户使用专有云平台的资源和管理策略进行安全运营的工作，包括安全产品配置托管、安全事件响应、事故溯源、安全巡检、监控扫描、安全流程管理等工作。从安全运营的角度，持续保障租户业务的持续、安全地运行。

## 4.4.7 安全最佳实践

为保障租户业务安全，强烈建议租户在将业务迁移上云时应将之前的安全策略一同迁移，同时结合阿里云为租户提供诸多安全配置最佳实践进行迁移。例如：

- 云资源安全：云资源主体的安全，应采用VPC网络保证安全性。
- 云盾：使用云盾保证租户业务的安全，并且使用同步中心功能及时同步最新版云盾安全规则。同时，建议用户使用WAF来进行Web应用的安全防护。
- 云产品安全配置：
  - ECS实例的密码策略应足够复杂，避免被暴力破解入侵成功。
  - SSH和RDP管理端口应通过安全组进行限制。
  - ECS实例开放高危端口应通过IP白名单进行访问限制。
  - 不允许将SSH、RDP、MySQL、Redis等高危端口服务通过SLB实例对互联网开放访问。
  - RDS实例的密码必须设置高强度密码，并且使用IP白名单进行访问控制。
  - OSS实例的访问应通过访问控制规则进行限制，禁止公共读写的操作。
- 应用部署安全：代码部署上线之前必须删除压缩包、.svn隐藏目录、.git隐藏目录；Linux和Windows等操作系统必须进行安全加固的配置；同时，对于Web应用服务，建议用户使用Web应用防火墙进行防护。

## 5 专有云云产品安全

---

### 5.1 云服务器ECS

#### 5.1.1 平台侧安全设计

##### 5.1.1.1 安全隔离

实例的安全隔离包括以下几个方面：

##### CPU隔离

阿里云ECS支持KVM这种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云服务器采用虚拟交换机（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。

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。

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

此外，建议您对数据进行安全加密后存储到ECS实例的磁盘上，例如采用加密的文件系统或加密盘等方式，详情参见[ECS磁盘加密](#)。

## 5.1.1.2 鉴权认证

### 5.1.1.2.1 身份验证

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（AccessKey，AK）。用户可以在云控制台中自行创建AccessKey。AccessKey由AccessKey Id和AccessKey Secret组成，其中AccessKey Id是公开的，用于标识用户身份。AccessKey Secret是加密签名字符串和服务器端验证签名字符串时的密钥，用于用户身份的鉴别，必须严格保密。

云服务器ECS会对每个访问的请求进行身份验证，所以无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。ECS通过使用AccessKey Id和AccessKey Secret进行对称加密的方法来验证请求的发送者身份。

AccessKey Id和AccessKey Secret由阿里云官方颁发给访问者（可以通过阿里云官方网站申请和管理），其中AccessKey Id用于标识访问者的身份；AccessKey Secret是加密签名字符串和服务器端验证签名字符串时的密钥，必须严格保密。

### 5.1.1.2.2 访问控制

RAM（Resource Access Management）是阿里云为客户提供的集中式用户管理与资源访问控制服务。使用RAM，客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AccessKey，可以登录云控制台，或以程序形式操作云服务API。RAM用户创建时默认没有任何资源操作权限，只有在获得授权的前提下RAM用户才能代表云账户进行资源操作。

使用RAM，客户可以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，从而降低客户的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、多因素认证等等）。

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。

ECS用户可以通过RAM创建子用户账号和不同的群组来管理和控制用户资源的访问权限。

RAM可以帮助管理用户对资源的访问权限控制。例如，为了加强网络安全控制，用户可以给某个群组附加一个授权策略，该策略规定：如果原始IP地址不是来自特定的企业网络，则拒绝此类访问请求。

用户可以给不同群组设置不同权限来管理ECS资源，例如：

- **SysAdmins**：该群组需要创建和管理ECS镜像、实例、快照、安全组等权限。用户可以给SysAdmins组附加了一个授权策略，该策略授予组成员执行所有ECS操作的权限。
- **Developers**：该群组只需要使用ECS实例的权限。用户可以给Developers组附加一个授权策略，该策略授予组成员调用DescribeInstances、StartInstance、StopInstance、CreateInstance和 DeleteInstance 等API的权限。

如果某开发人员的工作职责发生转变，成为一名系统管理人员，用户可以方便的将其从Developers群组移到SysAdmins群组。

ECS同时通过接入STS来支持ECS实例RAM角色的功能。实例RAM角色属于RAM角色的一种，它的目的是让 ECS实例扮演具有某些权限的角色，从而赋予实例一定的访问权限。

实例RAM角色允许用户将一个RAM角色关联到 ECS 实例，在实例内部基于STS临时凭证（临时凭证将周期性更新）访问其他云产品。这样，一方面可以保证AccessKey安全，另一方面也可以借助RAM实现权限的精细化控制和管理。

### 5.1.1.3 数据安全

#### 5.1.1.3.1 概述

对于云平台运行需要用到的敏感数据，例如授权凭证、用户密码、密钥，统一使用阿里云密钥管理服务（KMS）提供的密钥管理及加密机制进行加密存储。

#### 5.1.1.3.2 三副本存储技术

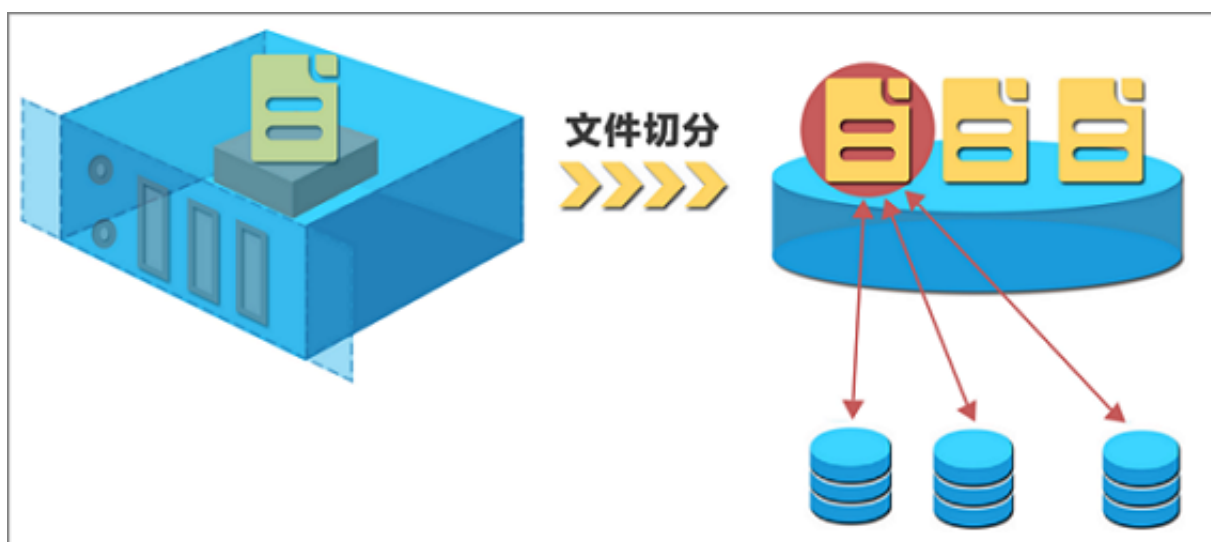
ECS用户对虚拟磁盘的读写，最终都会被映射为对专有云数据存储平台上的文件的读写。专有云提供一个扁平的线性存储空间，并在内部对线性地址进行切片，一个分片称为一个Chunk。对于每一个Chunk，都会复制出三个副本，并将这些副本按照一定的策略存放在集群中的不同节点上，保证用户数据的可靠。

在专有云数据存储系统中，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；如果一份或一份以上写失败，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、电源供电情况以及机器负载情况。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。

图 5-1: 三副本备份



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的有效副本数达三份。

图 5-2: 自动复制



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（包括云盘每一块上的内容），最大限度保证用户的数据安全性。

### 5.1.1.3.3 ECS磁盘加密

ECS磁盘加密为用户提供了一种简单安全的加密手段，能够对新创建的云盘进行加密处理。

您无需构建、维护和保护自己的密钥管理基础设施，也无需更改任何已有的应用程序和运维流程，无需做额外的加密操作，磁盘加密功能对于业务没有任何影响。在创建加密云盘并将其挂载到ECS实例后，将对以下类型的数据进行加密：

- 云盘中的数据。
- 云盘和实例间传输的数据（实例操作系统内数据不再加密）。
- 加密云盘创建的所有快照（加密快照）。

加密对从ECS实例传输到云盘的数据进行加密，在ECS实例所在的宿主机上进行。

磁盘加密支持面向所有专有云中的可用云盘（普通云盘、高效云盘和SSD云盘）和共享块存储（高效和SSD）。

### 5.1.1.4 传输加密

阿里云为用户访问提供了HTTPS协议来保证数据传输的安全。如果用户通过阿里云控制台操作，阿里云控制台会使用HTTPS进行数据传输。所有的阿里云服务都为客户提供了支持HTTPS的API访问点，允许用户使用Access Key以程序形式来调用阿里云服务API。阿里云的传输协议支持标准的SSL/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。

### 5.1.1.5 防止ARP欺骗

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

为了防御ARP欺骗，专有云在网络出口设置了ARP防火墙。只有使用平台统一分配的MAC地址才能进行正常通讯，将非法流量阻隔在攻击者的实例之内。

## 5.1.2 租户侧安全功能

### 5.1.2.1 日志审计

用户认证凭证和权限控制是为了避免产生安全问题，而安全日志则可以帮助更好地理解 and 诊断安全状况。阿里云为客户提供统一的云资源操作安全日志管理，记录账户下的用户登录及资源访问操作，包括操作人、操作时间、源IP地址、资源对象、操作名称及操作状态。保存的所有操作记

录，客户可以实现安全分析、入侵检测、资源变更追踪以及合规性审计。为了满足用户的合规性审计需要，用户往往需要获取主账户和其子用户的详细操作记录。

### 5.1.2.2 安全的镜像

阿里云镜像集成了所有已知的高危漏洞补丁，防止主机上线之后即处于高风险状态。在发现新的高危安全漏洞后，阿里云会迅速更新镜像并提供给客户。同时，阿里云会使用数据校验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。

### 5.1.2.3 块存储

阿里云块存储（Block Storage），是阿里云为云服务器ECS提供的低时延、持久性、高可靠的数据块级随机存储。块存储支持在可用区内自动复制用户的数据，防止意外的硬件故障导致数据不可用，以保护用户的业务免于组件故障的威胁。就像对待硬盘一样，用户可以对挂载到ECS实例上的块存储做格式化、创建文件系统等操作，并对数据持久化存储。

块存储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。

## 5.2 容器服务

### 5.2.1 平台侧安全设计

#### 5.2.1.1 安全隔离

容器服务提供多种安全隔离方式，确保集群安全。

独享Kubernetes集群

通过容器服务控制台创建的Kubernetes集群，属于当前操作控制台的用户。用于部署Kubernetes集群的资源：ECS、SLB等，都由当前Kubernetes集群独享，不会和其他用户共享。通过物理层面的强隔离，避免由于资源共享导致的潜在安全风险。

ECS安全组

每个Kubernetes集群使用的ECS属于同一个ECS安全组，基于最小权限原则，安全组只包含如下入网规则：

- 允许ICMP协议访问ECS。
- 允许Pod地址段访问ECS。

## 容器网络隔离

Kubernetes 集群中不同节点间 Pod 默认是可以互相访问的。在部分场景中，不同业务之间不应该网络互通，为了减少风险，您需要引入网络隔离（Network Policy）。在 Kubernetes 集群中，您可以使用 Canal 网络驱动实现网络隔离支持。

### 5.2.1.2 账号鉴权

您可通过容器服务提供的账号鉴权功能，来保障容器服务的安全。

Kubernetes 集群支持集群级别的子账号授权。通过授权，将集群的操作权限赋予特定的子账号。平时使用子账号操作，降低主账号泄露的风险。

## RBAC

Role-Based Access Control (RBAC) 使用 Kubernetes 内置的 API 组来驱动鉴权管理，您可以通过 API 来管理不同的 Pod 对应到不同的角色，以及各自的角色拥有的访问权限。

### 5.2.1.3 链路安全

容器服务支持 TLS 证书校验确保链路安全。

在容器服务提供的 Kubernetes 集群中，以下通信链路均会进行 TLS 证书校验，以保证通信不被窃听或篡改。

- 位于 Worker 节点上的 kubelet 主动连接位于 Master 节点上的 apiserver。
- 位于 Master 节点上的 apiserver 主动连接位于 Worker 节点上的 kubelet。

在初始化过程中，发起初始化的 Master 节点会通过 SSH 隧道连接到其他节点的 SSH 服务（22 端口）进行初始化。

## 5.2.2 租户侧安全功能

### 5.2.2.1 应用安全

容器服务支持丰富的应用安全策略。

表 5-1: 应用安全策略表

安全策略	安全策略说明
容器使用非root运行	为了防止容器逃逸而获得宿主机的权限，容器内应用以非root用户身份运行。



安全策略	安全策略说明
使用安全的基础镜像	用户可根据自身需求定制基础镜像，并强制要求组织内使用认可的基础镜像；也可使用第三方安全的镜像，这里推荐使用Alpine-linux, Docker官方镜像都使用Alpine-linux作为基础镜像。
镜像最小化安装	镜像中不安装任何与应用无关的东西。
配置Docker守护程序的TLS身份验证	Docker守护程序和Docker Swarm API配置TLS身份验证。
设置容器CPU优先级	使用Docker的CPU共享功能来设定容器的优先级。CPU共享功能允许一个容器CPU使用级别优先于另一个容器，并禁止较低优先级的容器频繁地占用CPU资源。这样可确保高优先级的容器更好地运行，且可以有效地防止资源耗尽攻击。
限制容器内存使用量	默认情况下，容器可以使用主机上的所有内存。可以使用内存限制机制防止一个容器消耗所有主机资源，这通常用于发起拒绝服务攻击（DoS），具体可使用-m或-memory参数运行容器。
磁盘限额	默认情况下Docker镜像、容器rootfs、数据卷都存放在/var/lib/docker目录里，跟host是共享同一个文件系统。目前无法控制该目录大小，通过将/var/lib/docker目录单独挂载到云存储中（如云盘、OSS），避免影响宿主机根文件系统。
身份鉴别	<ul style="list-style-type: none"> <li>提供账户/密码以及证书等登录方式</li> <li>提供登录失败处理能力，结束会话，限制登录和自动退出</li> <li>会话空闲一段时间后，自动锁定</li> <li>初始预设密码在首次登录后，提示修改</li> <li>密码配置复杂度，修改密码不能与上一次重复，提示定期修改密码</li> </ul>

安全策略	安全策略说明
安全审计	<ul style="list-style-type: none"> <li>系统提供账号安全审计功能，对系统账号的修改操作实现审计记录，且记录无法更改</li> <li>系统平台上所有的操作清晰、完整，包括事件的日期、时间、发起者信息、类型、描述和结果等，并定期备份审计记录，保存时间不少于半年</li> </ul>
通信安全、保密性	<ul style="list-style-type: none"> <li>系统各组件之间采用TLS加密通信</li> <li>系统中的涉密信息通过密文保存，且在需要时下发至特定节点</li> </ul>
角色权限控制	<ul style="list-style-type: none"> <li>系统内置多租户权限管理模型，可根据团队、角色设定不同的访问权限，在集群、应用和管理维度进行细粒度管控</li> <li>系统支持LDAP等外部权限管理方式</li> <li>镜像仓库支持多租户、只读等权限控制</li> </ul>

## 5.2.2.2 主机安全

### 操作系统账号要求

操作系统口令长度在8位数以上，大写字母、小写字母、数字、特殊符号四种中的三种组合，不允许弱口令（如：规律或连续字符、工号、域账号前缀等）。系统中设置了定期更换的相关策略，时间为90天。

### 非法登录限制策略

启用登录失败处理功能，限制非法登录次数，登录失败次数超限后结束会话、自动退出。

### 访问控制

启用访问控制功能，依据安全策略控制用户对资源的访问。

- `passwd`文件权限：644
- `shadow`文件权限：000
- `rc3.d`文件权限：755
- `profile`文件权限：644
- `profile.d`文件夹权限：755

### 默认账号删除

删除多余的、过期的账户，避免共享账户。禁用默认账户名称：`sync`、`shutdown`、`halt`。

## 5.3 弹性伸缩ESS

### 5.3.1 平台侧安全设计

#### 5.3.1.1 安全隔离

弹性伸缩功能基于用户账户进行隔离。其中，伸缩组、配置、规则等均由用户自主管理（包括创建、修改或删除等操作），并且弹性伸缩功能只能操作该用户账户所拥有的实例资源。对实例资源操作的用户认证，采用AccessKey对称密钥认证技术，对用户的访问请求进行身份验证，保证安全隔离。

#### 5.3.1.2 鉴权认证

##### 5.3.1.2.1 身份验证

用户可以在云控制台中自行创建AccessKey。AccessKey由AccessKey Id和AccessKey Secret组成，其中AccessKey Id是公开的，用于标识用户身份。AccessKey Secret是加密签名字符串和服务器端验证签名字符串时的密钥，用于用户身份的鉴别，必须严格保密。

弹性伸缩会对每个访问的请求进行身份验证，无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。弹性伸缩通过使用AccessKey Id和AccessKey Secret对称加密的方法来验证请求的发送者身份。

AccessKey Id和AccessKey Secret由阿里云官方颁发给访问者（可以通过阿里云官方网站申请和管理）。其中AccessKey Id用于标识访问者的身份，而AccessKey Secret是加密签名字符串和服务器端验证签名字符串时的密钥，必须严格保密。

##### 5.3.1.2.2 访问控制

RAM（Resource Access Management）是阿里云为客户提供的用户身份管理与访问控制服务。使用RAM，您可以创建、管理用户账号（比如员工、系统或应用程序），并可以设置这些用户账号对其名下资源的操作权限。当您的企业存在多用户协同操作资源时，使用RAM可以让您避免与其他用户共享云账号密钥，按需为用户分配最小权限，从而降低您的企业信息安全风险。

RAM支持创建不同的角色，不同角色对各云产品具有不同的操作权限。弹性伸缩配置新增了RamRoleName参数。您可以通过设置该参数，让您的ECS实例来扮演不同的角色，这些实例便拥有了这些角色对不同云产品的操作权限。在对伸缩配置指定RamRoleName参数时，您需要确保当前的RamRole策略中允许您的ECS实例来扮演该角色，否则伸缩配置将无法有效地弹出ECS实例。

## 5.3.2 租户侧安全功能

### 5.3.2.1 日志审计

弹性伸缩会提供伸缩活动的记录，包含每次伸缩活动的活动ID、状态、状态信息、开始时间、结束时间、活动动因、详细信息等内容。

其中伸缩活动的状态包括拒绝（Rejected）、执行中（InProgress）、成功（Successful）、部分成功（Warning）、全部失败（Failed）；状态信息包括状态的具体信息；活动动因包括伸缩组执行的伸缩结果；详细信息包括伸缩活动所操作的实例信息。

## 5.4 对象存储OSS

### 5.4.1 平台侧安全设计

#### 5.4.1.1 安全隔离

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的用户认证采用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。

#### 5.4.1.2 鉴权认证

##### 5.4.1.2.1 身份验证

用户可以在Apsara Stack控制台中自行创建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。

##### 5.4.1.2.2 权限控制

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。



说明：

用户新建一个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。



说明：

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

### 5.4.1.2.3 RAM和STS支持

OSS支持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。

### 5.4.1.3 数据安全

数据在客户端和服务端之间传输时有可能出错。OSS支持通过CRC和MD5两种校验方式保证数据安全。

#### CRC校验

OSS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值作对比，从而完成数据完整性的验证。

OSS对新上传的Object进行CRC64的计算，并将结果存储为Object的元信息，随后在返回的response header中增加x-oss-hash-crc64ecma头部，表示其CRC64值，该64位CRC根据[ECMA-182标准](#)计算得出。

#### MD5校验

如果需要通过MD5校验上传到OSS的文件和本地文件是否一致，可以在上传文件时携带文件的Content-MD5值，这时OSS服务端会帮用户进行MD5校验，只有在OSS服务器接收到的文件MD5值和Content-MD5一致时才可以上传成功，从而保证上传数据的一致性。

### 5.4.1.4 数据加密

#### 5.4.1.4.1 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。

#### 5.4.1.4.2 客户端加密

客户端加密（Client-Side Encryption）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。OSS通过SDK中的函数针对OSS Bucket中的数据进行客户端加密，在本地加密后再上传到OSS Bucket中。

### 5.4.2 租户侧安全功能

#### 5.4.2.1 密钥管理

阿里云Key Management Service（KMS）是一项将安全、高度可用的硬件和软件相结合，提供可扩展到云端的密钥管理系统的服务。KMS使用客户主密钥（CMK）加密OSS Bucket对

象，通过KMS API集中创建加密密钥，定义策略以控制密钥的使用方法，以及审核密钥使用情况来证明它们使用得当。用户可以利用这些密钥来保护在OSS Bucket中的数据。

### 5.4.2.2 日志审计

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。

### 5.4.2.3 防盗链

为了防止您在OSS上的数据被其他人盗链而产生额外费用，用户可以通过Apsara Stack控制台或者API方式对Bucket设置防盗链功能。防盗链包括以下参数：

- Referer白名单。仅允许指定的域名访问OSS资源。
- 是否允许空Referer。如果不允许空Referer，则只有HTTP或HTTPS header中包含Referer字段的请求才能访问OSS资源。

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。

## 5.5 表格存储Table Store

### 5.5.1 平台侧安全设计

#### 5.5.1.1 安全隔离

表格存储使用共享存储机制，支持不同用户的多个实例共享同一集群资源，以数据分区为最小服务单位，支持以数据分区级别的负载均衡机制来隔离不同实例之间的影响。

#### 网络隔离

表格存储支持实例级别的VPC访问控制，支持如下三种VPC访问设置：

- 允许任意网络访问：支持来自于公网及绑定的VPC的访问。
- 限定VPC访问：仅支持来源于绑定的VPC的访问，非绑定VPC的访问将会被拒绝。
- 限定控制台或VPC访问：仅支持来源于绑定的VPC及表格存储控制台的访问，其他来源的访问将会被拒绝。

## 存储隔离

表格存储使用共享存储机制，支持不同用户的多个实例共享同一集群资源，以数据分区为最小服务单位，支持以数据分区级别的负载均衡机制来隔离不同实例之间的影响。

### 5.5.1.2 鉴权认证

#### 身份验证

表格存储根据 Access Key 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 Access Key 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。

#### 访问控制

表格存储已经接入 STS 鉴权，支持用户对子账号进行授权管理。STS 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。

表格存储支持的授权粒度到表级别及 API 级别。

### 5.5.1.3 数据安全

表格存储使用盘古分布式共享存储系统，由盘古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，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。

表格存储的数据经过序列化之后调用盘古接口写到磁盘上进行持久化，每个数据块会写到1到多个Chunk上。

盘古的分布策略会综合考虑集群中所有服务节点的磁盘使用情况、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机器上，从而有效防止由于一个机器或一个机架的故障导致的数据不可用。

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，盘古就会启动复制机制，在不同的服务节点之间复制数据，保证集群中所有Chunk的有效副本数达到三份。

表格存储的写操作则在盘古返回三份拷贝均持久化到磁盘之后再返回给用户，以此来保证数据的强一致性。

## 5.6 文件存储NAS



## 5.6.1 平台侧安全设计

### 5.6.1.1 安全隔离

#### 网络隔离

NAS通过权限组机制对访问自身的网络进行控制。用户可以向权限组中添加规则，指定能够访问文件系统的IP地址或网段，并为不同的IP地址或网段授予不同级别的访问权限，从而实现网络之间的相互隔离。

#### 存储隔离

在NAS中，文件系统的挂载点实例与服务端存储池的存储单元之间是一一映射关系，不同文件系统挂载点实例对应的服务端存储单元互相隔离。

NAS服务端访问控制模块通过VPC与文件系统挂载点实例之间的映射关系对用户的IO请求进行验证，检查其携带的存储单元信息与服务端存储单元信息是否一致，以此保证服务端的存储隔离。

### 5.6.1.2 鉴权认证

#### 权限控制

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。

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root用户）访问挂载点。



#### 说明：

- 经典网络类型挂载点不提供默认权限组。
- 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，如下表所示。

表 5-2: 权限组规则属性

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）	本条规则所授权对象的IP地址或地址段。

属性	取值	含义
读写权限	<ul style="list-style-type: none"> <li>· 只读</li> <li>· 读写</li> </ul>	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	<ul style="list-style-type: none"> <li>· 不限制root用户</li> <li>· 限制root用户</li> <li>· 限制所有用户</li> </ul>	<p>是否限制授权对象的Linux系统用户对文件系统的权限。</p> <p>在判断文件或目录访问权限时：</p> <ul style="list-style-type: none"> <li>· 不限制root用户将允许使用root用户访问文件系统</li> <li>· 限制root用户将把root用户视为nobody处理</li> <li>· 限制所有用户将把包括root在内的所有用户都视为nobody。</li> </ul>
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。

## 访问控制

NAS接入了RAM 服务，支持控制台设置 RAM，主子账号授权。

通过RAM，用户可以授权子用户对文件存储NAS的操作权限。

表 5-3: RAM中可授权的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

操作 (Action)	说明
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

### 5.6.1.3 数据安全

#### 数据多副本存储

NAS 通过多副本存储方式保证数据的安全。

**用户数据：**NAS 服务端以 3 副本方式存储用户数据，可以承受两个副本的损失。服务端会不断监控数据的副本数目，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，集群中部分数据的有效副本数会小于 3。一旦发生这种情况，服务端就会启动复制机制，保证集群中所有数据的有效副本数达到 3 份。

此外，服务端通过对比所存数据与其校验信息是否匹配来防止偶发的静默错误。当发现静默错误后，通过复制健康副本来保证数据的有效副本数达到 3 份，从而保障数据可靠性。

#### 数据回收

用户进行删除操作后，释放的存储空间由服务端系统回收，禁止任何用户访问。在存储空间被再次使用前，其中的内容会被擦除，最大限度保证用户的数据安全性。

## 5.6.2 租户侧安全功能

### 5.6.2.1 日志审计

NAS 的管理系统会记录与文件系统实例相关操作的日志，包括文件系统实例的创建、删除等。

NAS 的日志会随着操作自动记录在服务端。日志中包括了操作执行用户、操作执行时间等详细信息，可以用于故障的调查和分析。

### 5.6.2.2 目录级读写权限 ACL

NAS 文件系统目前支持目录级读写权限 ACL。本节介绍如何配置目录级读写权限 ACL。

#### 前提条件

- 所有的客户端必须使用 NFSv4 协议挂载 NAS 文件系统。
- 必须使用 `alinas acl` 工具设置 ACL。请不要直接修改 `mode`，也不要使用 `chmod` 等命令修改文件权限，否则不能保证权限设置结果。

## 操作步骤

1. 执行以下命令格式 `sudo mount -t nfs -o vers=4.0 <挂载点域名>:<文件系统内目录>  
<当前服务器上待挂载目标目录>`，如 `mount -t nfs -o vers=4.0 014544bbf6-wdt41.cn-hangzhou.nas.aliyuncs.com:/ /mnt` 确保已使用 NFSv4 协议正确挂载文件系统。



### 说明:

- 不同版本的客户端，使用的 `vers` 参数不同，如果您输入 `vers=4.0` 出错，请使用 `vers=4`。
- 如文件系统在未开启 ACL 的版本中已经被挂载使用，建议重新挂载以确保 ACL 功能正确生效。

2. 在 CentOS 中安装 `nfs4-acl-tools`。

```
sudo yum install nfs4-acl-tools -y
```

3. 确保已安装 Python 2.7。

```
python --version Python 2.7.5
```

4. 使用 `alinas-acl` 设置 ACL 权限。

```
./alinas_acl set ./foo --add --user Alice --rule r #为文件foo添加用户Alice的读权限
./alinas_acl set ./foo -a -u Alice -r r #前一条命令的缩写
./alinas_acl set ./dir --add --group Staff --rule rwx #为目录dir添加组Staff的读写执行权限
./alinas_acl set ./foo --add --user EVERYONE@ --rule none #EVERYONE@没有任何权限
./alinas_acl set ./foo --add --user 1001 --rule none #uid为1001的用户也没有任何权限
./alinas_acl set ./dir -d -u Bob #删除用户Bob对dir目录的权限
```



### 说明:

- 建议尽量仅父目录上设置关键的 ACL 权限，而不要为整个目录中的所有文件分别设置 ACL，以防性能损失。
- 每个文件的 ACE (Access Control Entry) 数目建议不要超过 10 条。

5. 查看 ACL 权限。

```
./alinas_acl get ./foo #查看文件foo的已有权限 # file: foo/ # owner:
root # group: root OWNER@::rw- GROUP@::r-- EVERYONE
@::--- Alice::r-- Staff:g:rw-
1001::---
```



### 说明:

设置ACL自动生成的OWNER@、GROUP@、EVERYONE@是3个特殊的用户名，分别对应mode中的user、group和others。当mode与ACL不一致时，由于客户端版本的不同，判定顺序可能会产生不同的权限效果。

## 5.7 文件存储HDFS

### 5.7.1 平台侧安全设计

#### 5.7.1.1 安全隔离

文件存储HDFS的安全隔离包括网络隔离和存储隔离。

##### 网络隔离

文件存储HDFS通过权限组机制对访问自身的网络进行控制。用户可以向权限组中添加规则，指定能够访问文件系统的IP地址或网段，并为不同的IP地址或网段授予不同级别的访问权限，从而实现网络之间的相互隔离。

##### 存储隔离

在文件存储HDFS中，文件系统的挂载点实例与服务端存储池的存储单元之间是一一映射关系，不同文件系统挂载点实例对应的服务端存储单元互相隔离。

文件存储HDFS服务端访问控制模块通过VPC与文件系统挂载点实例之间的映射关系对用户的IO请求进行验证，检查其携带的存储单元信息与服务端存储单元信息是否一致，以此保证服务端的存储隔离。

#### 5.7.1.2 鉴权认证

本文介绍文件存储HDFS的权限控制的多种方式，以及通过RAM授予子用户操作文件存储HDFS的权限。

##### 权限控制

文件存储HDFS支持HDFS系统标准的目录、文件权限操作，并支持用户或用户组的读、写权限。

文件存储HDFS支持VPC挂载点，并只允许同一VPC内的ECS实例访问其文件系统。

此外，文件存储HDFS还通过权限组机制对访问权限进行控制。权限组是一个白名单机制，用户可以向权限组添加规则，为不同的IP或网段授予不同级别的访问权限。

一条权限组规则包含四个属性，如下表所示：

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。
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。

## 访问控制

文件存储HDFS接入了RAM服务，支持控制台设置RAM主子账号授权。

通过RAM，您可以向子用户授予对文件存储HDFS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HDFS。

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

### 5.7.1.3 数据安全

本文介绍文件存储HDFS如何通过数据多副本存储及数据回收的方式来保障数据安全性。

#### 数据多副本存储

文件存储HDFS中存储的数据分为元数据和用户数据两部分。文件存储HDFS通过多副本存储方式保证这两种数据的安全。

- **元数据：**用户进行IO操作时，相关操作会传递到服务端。文件存储HDFS服务端使用分布式一致性协议Paxos对元数据进行处理。典型配置下，一个Paxos组由三台机器组成。相应地，服务端以三副本方式存储元数据，并借助Paxos保证不同副本间的一致性。
- **用户数据：**文件存储HDFS服务端以三副本方式存储用户数据，可以承受两个副本的损失。服务端会不断监控数据的副本数目，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，集群中部分数据的有效副本数会小于 3。一旦发生这种情况，服务端就会启动复制机制，保证集群中所有数据的有效副本数达到三份。

此外，服务端通过对比所存数据与其校验信息是否匹配来防止偶发的静默错误。当发现静默错误后，通过复制健康副本来保证数据的有效副本数达到三份，从而保障数据可靠性。

#### 数据回收

用户进行删除操作后，释放的存储空间由服务端系统回收，禁止任何用户访问。在存储空间被再次使用前，其中的内容会被擦除，最大限度保证用户的数据安全性。

## 5.7.2 租户侧安全功能

### 5.7.2.1 日志审计

您可以使用文件存储HDFS记录的日志来帮助您调查和分析故障。

文件存储HDFS的管理系统会记录与文件系统实例相关操作的日志，包括文件系统实例的创建、删除等。

文件存储HDFS的日志会随着操作自动记录在服务端。日志中包括了操作执行用户、操作执行时间等详细信息，可以用于故障的调查和分析。

## 5.8 云数据库RDS版

### 5.8.1 平台侧安全设计

#### 5.8.1.1 安全隔离

云数据库通过租户隔离和网络隔离来保护数据安全。

##### 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。

##### 网络隔离

除了IP白名单外，RDS还支持您使用VPC来获取更高层次的网络访问控制。VPC是您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您的网络包隔离，在网络二层完成访问控制。您可以通过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白名单能极大程度提升RDS实例的安全性。

#### 5.8.1.2 鉴权认证

云数据库通过鉴权认证来保护数据安全。

##### 身份验证

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）。您可以在云控制台中自行创建AK，AK由AccessKeyID和AccessKeySecret组成。其中AccessKeyID是公开的，用于标识用户的身份；AccessKeySecret是用于加密签名字符串和服务器端验证签名字符串的密钥，用户必须严格保密，用于用户身份的鉴别。

RDS服务会对每个访问的请求进行身份验证，所以无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。RDS通过使用AccessKeyID和AccessKeySecret进行对称加密的方法来验证请求的发送者身份。AccessKeyID和AccessKeySecret由专有云平台颁发给访问者（可以通过阿里云官方网站申请和管理），必须严格保密。

##### 权限控制

创建实例后，RDS并不会为您创建任何初始的数据库账户。您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。如果您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。

#### 访问控制

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支持RAM服务。通过RAM服务，您可以将云账户下RDS资源的访问及管理权限授予RAM中的子账户。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。

### 5.8.1.3 数据安全

云数据库通过主从热备、数据备份、日志备份来保护数据安全。

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。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。

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：数据备份和日志备份。

### 5.8.1.4 数据加密

#### SSL

RDS提供MySQL和SQL Server的安全套接层协议（Secure Sockets Layer, SSL）。用户可以使用RDS提供的服务器端的根证书来验证目标地址和端口的数据库服务是不是RDS提供的，从而有效避免中间人攻击。除此之外，RDS还提供了服务器端SSL证书的启用和更新能力，以便用户按需更换SSL证书以保障安全性和有效性。

需要注意的是，虽然RDS提供了应用到数据库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，RDS实例的吞吐量和响应时间都会受到一定程度的影响，具体影响与您的连接次数和数据传输频度有关。

#### TDE

RDS提供MySQL和SQL Server的透明数据加密（Transparent Data Encryption, TDE）功能。MySQL版的TDE由阿里云自研，SQL Server版的TDE是基于SQL Server企业版的功能改造而来。

当RDS实例开启TDE功能后，您可以指定参与加密的数据库或者表。这些数据库或者表中的数据在写入到任何设备（磁盘、SSD、PCIe卡）或者服务（表格存储TableStore、对象存储OSS）前都会进行加密，因此实例对应的数据文件和备份都是以密文形式存在的。

TDE加密采用国际流行的AES算法，密钥长度为128比特。密钥由KMS服务加密保存，RDS只在启动实例和迁移实例时动态读取一次密钥。您可以自行通过KMS控制台对密钥进行更换。

### 5.8.1.5 防DDoS攻击

云数据库通过流量清洗和黑洞处理来防止DDoS攻击。

当您使用外网连接访问RDS实例时，可能会遭受DDoS攻击。当RDS安全体系认为您的实例正在遭受DDoS攻击时，首先启动流量清洗的功能，如果流量清洗无法抵御攻击或者攻击达到黑洞阈值时，将会进行黑洞处理。

流量清洗和黑洞处理的方法及触发条件如下：

#### · 流量清洗

流量清洗只针对外网流入流量进行清洗，流量从原始网络路径中重定向到清洗设备上，通过清洗设备对该IP的流量成分进行正常和异常判断，丢弃异常流量，并对最终到达服务器的流量实施限流，减缓攻击对服务器造成的损害，但对流量中正常的部分可能造成损伤。

流量清洗的触发和结束由系统自动完成，单个RDS实例满足以下任一条件即触发流量清洗：

- 包转发率PPS（Packets Per Second）达到3万；
- 比特率BPS（Bits Per Second）达到180Mb；
- 每秒新建并发连接达到1万；
- 激活并发连接数达到1万；
- 非激活并发连接数达到10万。

#### · 黑洞处理

黑洞处理是保证RDS整体服务可用性的一种手段，只针对外网流入流量进行黑洞处理，处于黑洞状态的RDS实例不可被外网访问，此时应用程序通常也处于不可用状态。单个RDS实例满足以下任一条件即触发黑洞处理：

- BPS（Bits Per Second）达到2GB；
- 流量清洗无效。

黑洞结束条件：黑洞在2.5小时后自动解除，然后自动进入流量清洗状态，检查是否还有攻击。若攻击依然存在，会再次进入黑洞处理；若攻击已经停止，系统会自动解封。

## 5.8.2 租户侧安全功能

### 5.8.2.1 日志审计

通过日志审计功能可以及时发现安全问题。

RDS提供查看SQL明细功能，您可定期审计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。

### 5.8.2.2 IP白名单

IP白名单可以有效阻止非法IP的访问。

默认情况下，RDS实例被设置为允许任何IP访问，即0.0.0.0/0。您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，不会影响您的使用。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。

### 5.8.2.3 软件升级

RDS的软件升级分为重启后升级和强制升级。

RDS为您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。但在您主动重启RDS实例时，该实例的数据库版本会在重启时升级到最新的兼容版本。

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，强制升级仅会引起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。

您可以通过控制台或者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。

## 5.9 云数据库KVStore for Redis

### 5.9.1 平台侧安全设计

#### 5.9.1.1 安全隔离

租户隔离

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。

网络隔离

在专有云环境中，用户除了用白名单进行访问控制之外，还可使用VPC进一步地控制网络访问。

VPC是用户在专有云平台中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，在网络层完成访问控制。用户还可以通过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IP段来解决IP资源冲突的问题，使得自有服务器和阿里云ECS可以同时访问云数据库。VPC和IP白名单的双重保护使得实例的安全性进一步提升。

部署在VPC中的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），这些情况包括但不限于：

- 来自 ECS EIP的访问。
- 来自用户自建IDC公网出口的访问。



注意：

IP白名单对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。

### 5.9.1.2 鉴权认证

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

云数据库KVStore for Redis支持RAM服务和STS服务。通过RAM服务，用户可以将云账户下的Redis资源的访问及管理权限授予RAM中的子用户；通过STS服务，用户可通过临时访问凭证提供短期访问权限。

### 5.9.1.3 传输加密

云数据库KVStore for Redis提供基于安全套接层协议（Secure Sockets Layer，简称SSL）和安全传输层协议（Transport Layer Security，简称TLS）的安全加密。用户可以使用Redis提供的服务器端根证书来验证目标地址和端口的数据库服务是否为Redis提供，从而有效避免中间人攻击。除此之外，Redis还提供了服务器端SSL/TLS证书的启用和更新功能，以使用户按需更替SSL/TLS证书以保障安全。



说明：

- 传输加密功能要求应用开启服务器端验证。
- 传输加密功能会带来额外的CPU开销，实例的吞吐量和响应时间都会受到一定程度的影响，具体影响与您的连接次数和数据传输频度有关。

## 5.9.2 租户侧安全功能

### 5.9.2.1 数据库账号

访问云数据库KVStore for Redis必须通过强制的密码认证，账号密码是访问Redis的凭证。云数据库KVStore for Redis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。

### 5.9.2.2 IP 白名单

云数据库KVStore for Redis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KVStore for Redis实例单独设置IP白名单。

默认情况下，云数据库KVStore for Redis的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实例信息页面的修改白名单按键来添加IP白名单规则。IP白名单的更新无需重启实例，不影响使用。IP白名单可以设置多个分组，每个分组最多可配置1000个IP或IP段。

### 5.9.2.3 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。云数据库KVStore for Redis支持基于备份集数据恢复实例。

### 5.9.2.4 软件升级

- 云数据库KVStore for 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KVStore for 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KVStore for Redis团队将会全程支持升级过程。
- 云数据库KVStore for 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。

## 5.10 云数据库MongoDB版

### 5.10.1 平台侧安全设计

#### 5.10.1.1 安全隔离

##### 网络隔离

云数据库 MongoDB版支持您使用VPC来获取更高层次的网络隔离。

VPC是您在专有云里设定的私有网络环境，通过底层网络协议严格地将您的网络包隔离，在网络层完成访问控制。

## 租户隔离

MongoDB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，例如禁止您通过数据库读写操作系统文件，确保您无法接触其他用户的数据。

### 5.10.1.2 鉴权认证

#### 身份验证

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）。用户可以在云控制台中自行创建AccessKey。AccessKey由AccessKeyId和AccessKeySecret组成，其中AccessKeyId是公开的，用于标识用户身份；AccessKeySecret是用于加密签名字符串和服务器端验证签名字符串的密钥，用户必须严格保密，用于用户身份的鉴别。

MongoDB服务会对每个访问的请求进行身份验证，所以无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。MongoDB服务通过使用Access Key ID和AccessKey Secret进行对称加密的方法来验证请求的发送者身份。Access Key ID和AccessKey Secret由专有云平台颁发给访问者，其中Access Key ID用于标识访问者的身份；AccessKey Secret是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密。

#### 权限控制

云数据库MongoDB在登录数据库时必须通过强制的账号及密码认证。云数据库MongoDB实例创建后，会默认生产初始化root账号。用户可以在创建时指定root账号密码，或在实例创建后重置root账号密码。

root账号默认拥有完整的云数据库MongoDB管理权限，用户可以通过root账号登录数据，对其他账号进行增删或授权操作。

#### 访问控制

通过云账户创建的MongoDB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。

MongoDB支持RAM服务。通过RAM服务，可以将云账户下MongoDB资源的访问及管理权限授予RAM中子账号。

### 5.10.1.3 数据安全

云数据库MongoDB服务采用三节点副本集的高可用架构，三个数据节点位于不同的物理服务器上，自动同步数据。Primary和Secondary节点提供服务，当Primary节点出现故障，系统自动选举新的Primary节点，当Secondary节点不可用，由备用节点接管服务。

云数据库MongoDB版提供自动备份功能，一键式数据恢复，保证数据的完整可靠。

您可以自行设定每周进行全量物理备份的频率（要求每周最少两次）及每次进行备份的起始时间段。另外也可以根据运维需要，通过控制台或者Open API随时发起全量的临时物理备份。

对MongoDB实例产生的增量日志，系统会自动进行备份，通过全量备份+增量日志的方式来支持您将数据恢复到备份存储周期内的任意一个秒级时间点。

#### 5.10.1.4 DDoS防护

DDoS防护，在网络入口实时监测，当发现超大流量攻击时，对源IP进行清洗，清洗无效情况下可以触发黑洞机制。

### 5.10.2 租户侧安全功能

#### 5.10.2.1 日志审计

日志审计用于记录客户端连接后对数据库执行的所有操作。便于后续的故障分析、行为分析、安全审计等行为。日志审计行为能有效帮助您获取数据的执行情况，加以自助分析。同时，审计日志的记录，也逐步成为金融云等核心业务场景的监管必备需求。

#### 5.10.2.2 IP白名单

云数据库MongoDB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MongoDB版实例单独设置IP白名单。

默认情况下，MongoDB实例被设置为允许任何IP访问，即0.0.0.0/0。您可以通过控制台或者Open API来添加IP白名单规则。IP白名单的更新无需重启MongoDB实例，因此不会影响用户的使用。

### 5.11 云数据库KVStore for Memcache

#### 5.11.1 平台侧安全设计

##### 5.11.1.1 安全隔离

##### 网络隔离

在专有云环境中，用户除了用白名单进行访问控制之外，还可使用VPC进一步地控制网络访问。

VPC是用户在专有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，在网络层完成访问控制。用户还可以通过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IP段来解决IP资源冲突的问题，使得自有服务器和阿里云ECS可以同时访问云数据库。VPC 和IP 白名单的双重保护使得实例的安全性进一步提升。

部署在VPC中的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），这些情况包括但不限于：

- 来自ECS EIP的访问。
- 来自用户自建IDC公网出口的访问。



注意：

IP白名单对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。

## 租户隔离

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。

### 5.11.1.2 鉴权认证

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

Memcache支持RAM服务和STS服务。通过RAM服务，用户可以将云账户下的Memcache资源的访问及管理权限授予RAM中的子用户；通过STS服务，用户可通过临时访问凭证提供短期访问权限。

## 5.11.2 租户侧安全功能

### 5.11.2.1 数据库账号

访问Memcache必须通过强制密码认证，账号密码是访问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。

### 5.11.2.2 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。用户可以通过控制台的安全设置页面来添加IP白名单规则。IP白名单的更新无需重启实例，不影响使用。IP白名单可以设置多个分组，每个分组最多可配置1000个IP或IP段。

### 5.11.2.3 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。Memcache支持基于备份集数据恢复实例。

### 5.11.2.4 软件升级

- 云数据库KVStore for 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KVStore for 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KVStore for Memcache团队将会全程支持升级过程。
- 云数据库KVStore for 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。

## 5.12 分析型数据库PostgreSQL版

### 5.12.1 平台侧安全设计

#### 5.12.1.1 安全隔离

##### 网络隔离

在专有云环境中，用户除了用白名单进行访问控制之外，还可使用VPC进一步地控制网络访问。

VPC是用户在专有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，在网络层完成访问控制。

部署在VPC中的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），这些情况包括但不限于：

- 来自ECS EIP的访问。
- 来自用户自建IDC公网出口的访问。



说明：

IP白名单对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。

## 租户隔离

AnalyticDB for PostgreSQL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。

### 5.12.1.2 鉴权认证

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

AnalyticDB for PostgreSQL支持RAM服务和STS服务。通过RAM服务，用户可以将云账户下的AnalyticDB for PostgreSQL资源的访问及管理权限授予RAM中的子用户；通过STS服务，用户可通过临时访问凭证提供短期访问权限。

### 5.12.1.3 主备节点

AnalyticDB for PostgreSQL实例的Master、Segment节点均拥有一主一备两个副本进行主从热备，主节点发生故障可以迅速切换至备节点。用户可以随时发起数据库的备份，AnalyticDB for PostgreSQL能够根据备份策略按备份集恢复，提高了数据的可回溯性。

## 5.12.2 租户侧安全功能

### 5.12.2.1 数据库账号

当用户创建实例后可以通过控制台或者OpenAPI来创建数据库超级账户。用户权限可用过Grant语句进行授权。

### 5.12.2.2 IP白名单

默认情况下，AnalyticDB for PostgreSQL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OpenAPI来添加IP白名单规则。更新IP白名单无需重启AnalyticDB for PostgreSQL实例，不会影响用户的使用。IP白名单可以设置多个分组，每个分组最多可配置1000个IP或IP段。

### 5.12.2.3 SQL审计

AnalyticDB for PostgreSQL提供查看SQL明细功能，用户可定期审计SQL操作，及时发现问题。Proxy模块记录所有发往AnalyticDB for PostgreSQL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、返回记录数和执行时间点等信息。

### 5.12.2.4 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。AnalyticDB for PostgreSQL支持基于备份集数据恢复实例。

### 5.12.2.5 软件升级

- 云数据库AnalyticDB for PostgreSQL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AnalyticDB for PostgreSQL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AnalyticDB for PostgreSQL团队将会全程支持升级过程。
- 云数据库AnalyticDB for PostgreSQL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。

## 5.13 云数据库OceanBase版

### 5.13.1 平台侧安全设计

#### 5.13.1.1 安全隔离

多租户隔离

OceanBase可以通过在数据库内部实现多租户隔离，实现一个集群可以服务多个租户。在数据安全方面，不允许跨租户的数据访问，确保用户的数据资产没有泄露的风险；在资源使用方面表现为租户“独占”其资源配额，该租户对应的前端应用，无论是响应时间还是TPS/QPS都比较平稳，不会受到其他租户负载轻重的影响。

#### 5.13.1.2 鉴权认证

极限支持力度

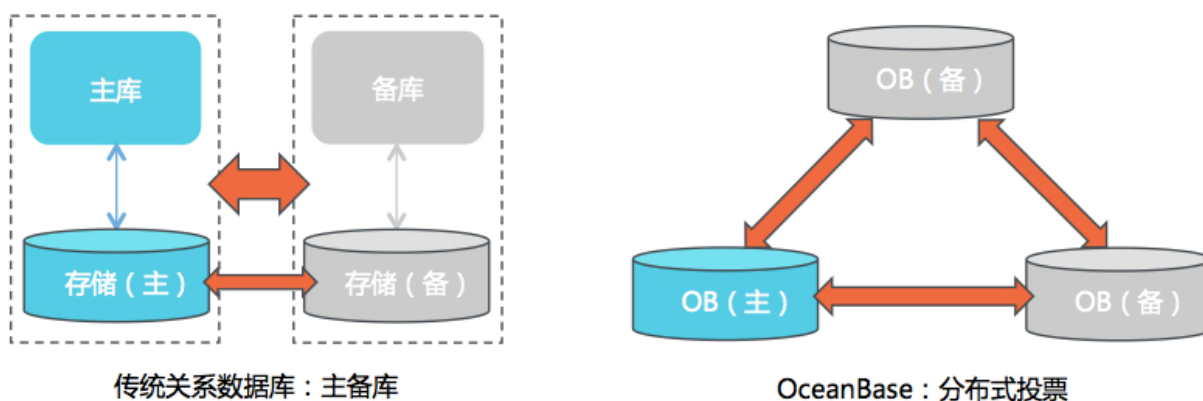
创建租户的时候，默认会有一个具有所有权限的账号，登陆数据库使用“账号@租户#集群名”的方式，使用该账号可以创建一个或者多个账户，并且可以赋予不同的权限。

- 权限支持粒度：租户级别，数据库级别和表级别
  - 全局层级：适用于所有的数据库
  - 数据库层级：适用于一个给定数据库中的所有目标
  - 表层级：适用于一个给定表中的所有列

- 支持相关联的八个基本权限项：CREATE、DROP、ALTER、INDEX、INSERT、DELETE、UPDATE、SELECT

### 5.13.1.3 高可用架构

对OceanBase而言，同一数据保存在多台( $\geq 3$ )服务器中的半数以上服务器上(例如3台中的2台)，每一笔写事务也必须到达半数以上服务器才生效，因此当少数服务器故障时不会有任何数据丢失，能够做到RPO等于零。不仅如此，OceanBase底层实现的Paxos高可用协议，在主库故障后，剩余的服务器会很快自动选举出新的主库，实现自动切换，并继续提供服务，在实际的生产系统中做到RTO在30秒之内。



OceanBase的多副本特性和Paxos高可用协议将多样的异地多活、多城市多中心部署的高可用方案变为可能。通过典型的同城三机房、两地三中心、三地五中心部署，OceanBase可以满足用户跨IDC、跨城容灾的多种业务需求。

### 5.13.1.4 兼容性

OceanBase目前兼容MySQL5.6大部分功能，基于MySQL的业务可以零修改或者少量修改迁移到OceanBase，同时OceanBase在数据库内部实现了分区表和二级分区功能，可以完全取代传统数据库常用的分库分表方案，提高了应用开发和迁移的效率。

OceanBase的MySQL兼容性主要包括：

- 接口层面：OceanBase广泛使用的接口主要是JDBC和ODBC，使用MySQL的驱动就可以无障碍地访问OceanBase
- 数据模式层面：完整地支持了数据库（database）、表（table）、视图（view）、自增列（auto increment）等SQL标准的以及MySQL专有的数据模式，并且在数据库系统中实现了多租户（multi-tenant）

- SQL语句层面：
  - 支持SQL标准定义的增、删、改、查语句
  - 支持MySQL数据库特有的但在应用中比较常用的语句，如REPLACE、insert on duplicate key update语句
  - 支持MySQL特有的有实用价值的选项，如DML语句中的ignore选项、select语句中用来指定使用特定索引的hint等
- 系统对象层面，主要是指系统视图、系统变量、系统函数
- 事务层面：OceanBase采用的是多版本的并发控制协议，读写不等待，支持Read Committed隔离级别

## 5.13.2 租户侧安全功能

### 5.13.2.1 数据库帐号

访问OceanBase控制台必须通过强制用户名和密码认证，认证通过之后才可以进行创建租户、集群管控和运维的操作。

### 5.13.2.2 IP白名单

OceanBase提供了IP白名单来实现网络安全访问控制，支持为每个OceanBase的租户单独设置IP白名单。

默认情况下，OceanBase实例在创建之后，被设置为允许任何IP访问。您可以通过命令行ALTER TENANT tenantname SET VARIABLES ob\_tcp\_invited\_nodes = '192.168.0.0/16,10.125.227.255/255.255.252.0' 进行修改。

### 5.13.2.3 日志审计

OceanBase提供查看SQL明细功能，您可以审计SQL，及时发现问题。gv\$sql\_audit记录了所有发往OceanBase的SQL语句，内容包括server IP，访问的数据库名称、执行语句的账号、SQL语句、执行时长、排队时长、执行时间点等信息。

### 5.13.2.4 软件升级

- OceanBase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
- 当OceanBase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
- OceanBase的升级通常在几十分钟到一个小时内完成（取决于集群规模大小），升级期间不会对应用业务产生任何影响

## 5.13.5 关于OceanBase产品存在Mysql扫描版本漏洞问题的说明函

### 关于 OceanBase 产品存在 Mysql 扫描版本漏洞问题的说明函

阿里云专有云客户：

近期在安全审计过程中，检测出 OceanBase 产品使用了 Mysql server 5.6.25 版本，Mysql server 5.6.25 版本存在被攻击的风险。

实际上 Mysql server 5.6.25 版本号只是 OceanBase 为了实现 Mysql 兼容性，暴露的逻辑版本号，OceanBase 使用的是自主研发的数据内核，并没有真正使用 Mysql server 5.6.25 版本，不存在因使用 Mysql server 5.6.25 版本导致安全漏洞的风险。

今后任何项目的 OceanBase 产品如果被检测出使用 Mysql server 存在版本安全漏洞的问题，皆适用于以上解释，不再另出说明。

特此说明！

北京蚂蚁云金融信息服务有限公司  
2019 年 5 月 16 日

## 5.14 云数据库HBase

### 5.14.1 平台侧安全设计

#### 5.14.1.1 安全隔离

实例部署在利用OverLay技术在物理网络基础上构建的专有VPC虚拟网络上，在TCP层直接进行网络隔离保护。

DDoS防护在网络入口实时监控，当发现超大流量攻击时，对源IP进行清洗，清洗无效情况下可以直接恶意IP拉进黑洞。

#### 5.14.1.2 鉴权认证

##### 身份验证

账号密码验证与ACL权限控制可以抵御恶意数据损毁。访问集群上的开源组件，如HBase、Ganglia和HDFS，需要使用用户名和密码。用户第一次访问时，需要初始化访问用户名与密码；每次访问的设置都会覆盖之前的用户名和密码，即同一时间只会会有一个用户名和密码有效。通过开源软件的链接输入所设置的用户名密码，就可以直接访问对应组件的Web页面了。

##### 权限控制

HBase支持设置IP白名单。为了数据库的安全，新创建的集群被默认设置为无法访问，包括了两部分：

- 对集群上开源组件的访问，HBase，Ganglia和HDFS等
- 对集群的HBase服务的数据读写操作

在使用前，需要根据实际的访问情况，将要访问数据库的机器的IP列表加入到IP白名单中。最多支持配置1000个以上的白名单规则，直接从访问源进行风险控制。

##### 访问控制

HBase支持RAM鉴权。RAM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。

#### 5.14.1.3 数据安全

高可靠架构：数据多副本，存储在HDFS和云盘上，并支持数据备份到OSS上。数据可靠性高。

高可用架构：集群无单点故障。

#### 5.14.1.4 传输加密

HBase使用客户端加密的传输方式。客户端加密（Server-Side Encryption）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。

### 5.15 数据传输服务DTS

#### 5.15.1 平台侧安全设计

##### 5.15.1.1 安全隔离

DTS通过独立的进程、文件进行租户的实例和数据隔离。例如，禁止用户读写实例的操作系统文件，确保用户无法接触其他用户的数据。

##### 5.15.1.2 鉴权认证

用户通过云账号创建的DTS实例，为该账号拥有的资源。默认情况下，云账号只对自己的DTS资源拥有完整的操作权限。

DTS已支持RAM服务，使用阿里云的RAM服务。用户可以将云账号下，DTS资源的访问和管理权限授予RAM子账号。通过RAM机制，帮助用户按需分配权限，最大程度降低企业信息安全风险。

##### 5.15.1.3 传输安全

DTS日志格式为自定义格式，提升数据传输的安全性。

DTS内部对传输数据进行加密，保证数据的传输安全性。例如，增量同步过程中，日志读取模块和日志同步模块之间进行增量数据交互时，会对传输日志进行加密。

同时，DTS支持HTTPS证书加密协议，有效提升用户访问安全。

##### 5.15.1.4 数据安全

在增量同步、增量订阅过程中，DTS服务器上会存储部分增量数据。这些增量数据会按照DTS自定义的存储格式进行序列化存储。通过自定义的存储格式有效提升存储数据安全。



说明：

所有存储数据超过7天自动删除。



## 5.16 数据管理DMS

### 5.16.1 平台侧安全设计

#### 5.16.1.1 安全隔离

VPC网络具有天然的网络隔离特性，非常适合于高安全要求的场景，因此许多数据库实例使用了VPC网络作为基础网络设施。

DMS支持对VPC中实例的访问。在保证网络安全的同时，为数据操作提供非常大的便利。

#### 5.16.1.2 鉴权认证

阿里云账号与数据库账号认证

用户使用DMS前，需要先通过Apsara Stack控制台或者阿里云的其他控制台，用专有云的账号和密码进行登录。当用户登录状态过期或者登录失败或者切换账号后，DMS的登录状态也将失败，并停止用户对DMS的任何访问，要求用户重新登录阿里云账号和DMS系统。具有阿里云登录状态（云账号）是使用DMS的前提条件。

数据库账号权限控制

当用户使用阿里云账号登录后，通过DMS系统连接数据库时，DMS会对用户进行权限检查。当前登录的用户必须是要访问的数据库资源的Owner，或者数据库资源的Owner已授权当前用户，否则当前用户无法通过DMS访问该数据库资源。

#### 5.16.1.3 传输安全

HTTPS/SSL支持

DMS支持HTTPS/SSL协议，将HTTPS/SSL应用于用户浏览器和DMS服务器之间的网络连接，保证数据在传输过程中不被监听和窃取。

### 5.16.2 租户侧安全功能

#### 5.16.2.1 操作审计

操作行为审计

DMS提供了审计功能，对用户的登录、登出、SQL操作、表结构变更、表数据变更、导入、导出等操作及操作是否成功都有详细的记录，可以通过天基的日志审计功能tianjiMon进行用户操作日志的查询，可详细查出哪个用户访问了哪个实例、执行了什么操作、及操作对应的SQL语句，做到了事后有据可查。

## 5.17 数据管理DMS企业版

### 5.17.1 平台侧安全设计

#### 5.17.1.1 安全隔离

DMS企业版通过云账号、产品内的用户管理、产品内的访问IP白名单、产品内的权限体系四层来对用户的访问进行管控。

- 云账号支持RAM主子账号，也支持普通云账号作为第一层用户认证。【必选】
- 产品内的用户管理，每个企业独立管控相互之间完全隔离不影响；非本企业员工通过第一层云账号用户认证也不可进入本企业的DMS企业版。【必选】
- 产品内的访问IP白名单管理，针对公网访问时可限制来源服务器地址访问DMS企业版。【可选】
- 产品内的权限体系管理，用户在通过前三层管控后如果没有对应权限无法进行对应数据库表的相关查询与变更动作。【必选】

#### 5.17.1.2 鉴权认证

- 身份验证

- 阿里云账号认证

用户使用DMS前，需要先通过DTCenter或者阿里云的其他控制台，用专有云的账号和密码进行登录。当用户登录状态过期或者登录失败或者切换账号后，DMS的登录状态也将失败，并停止用户对DMS的任何访问，要求用户重新登录阿里云账号和DMS系统。具有阿里云登录状态（云账号）是使用DMS的前提条件。

- 数据库账号权限控制

当用户使用阿里云账号登录后，通过DMS企业版录入数据库实例时，DMS企业版会对用户进行权限检查。当前企业版内的用户必须有一个是要访问的数据库资源的Owner，或者数据库资源的Owner已授权当前用户，否则当前用户无法通过DMS企业版录入该目标实例进行后续的管理。

#### 5.17.1.3 数据安全

数据安全管控

SQLConsole数据查询安全。

- 细粒度权限管控：在规避用户接触数据库账号密码的基础上，提供库、表细粒度的权限管理，最细字段级别可管理身份证、手机号、密码等关键字段避免不必要的接触。

- 单次查询返回行数上限限制：如果SQL查询返回结果行数大于设置的上限值则只会按照上限行数进行返回，避免大量数据的流出。【产品内所有用户生效，全局可调】
- 当天查询返回总行数上限限制：如果当天累计返回总的数据库记录行数到达此阈值，则不可再发起查询操作，避免大量数据的流出。【产品内所有用户生效，单个用户可调】
- 当天查询返回总次数上限限制：如果当天累计查询的总次数到达此阈值，则不可再发起查询操作，避免大量数据的流出。【产品内所有用户生效，单个用户可调】
- 单个SQL查询超时限制：如果SQL执行时间超过既定的最长查询时间则会主动中断当前查询操作，避免影响数据库性能进而影响在线业务。【产品内所有用户生效，单个实例可调】
- 单个SQL查询表大小限制：如果SQL中涉及的表超过一定的空间大小，并且当前SQL无法走上索引查询需要全表遍历，则会直接中断不发起此查询到数据库，避免影响数据库性能进而影响在线业务。【产品内所有用户生效，数据库类型级别全局可调】

#### 5.17.1.4 数据加密

- KMS加密

服务器端加密是为了保护静态数据。阿里云Key Management Service (KMS) 是一项将安全、高度可用的硬件和软件相结合，提供可扩展到云端的密钥管理系统的服务。KMS使用客户主密钥 (CMK) 加密DMS企业版的数据库密码对象以及DMS企业版本身敏感信息与敏感配置，通过KMS API集中创建加密密钥，定义策略以控制密钥的使用方法，以及审核密钥使用情况来证明它们使用得当。

- HTTPS/SSL支持

DMS企业版支持HTTPS/SSL协议，将HTTPS/SSL应用于用户浏览器和DMS企业版服务器之间的网络连接，保证数据在传输过程中不被监听和窃取。

#### 5.17.1.5 变更安全

##### 数据变更安全

- 变更权限准入限制：若无对应目标库的变更权限，则不允许提交变更工单，避免非业务相关人员误操作。【产品内所有用户生效，申请权限后可提交】
- 变更正确性保障：对于变更工单提交时所涉及到的所有SQL语句必须满足语法正确，若不正确则中断不允许提交工单，避免语法错误引发误更新。【产品内所有用户生效】
- 变更行数控制：在提交变更工单通过语法检测后，会进行变更行数的检测，若实际变更行数与预估影响行数不一致则会提醒用户，避免SQL逻辑与预期不一致产生误更新。【产品内所有用户生效】
- 变更流程控制：可针对不同影响行数、不同变更类型配置不同的审批流程，即保障安全也保障研发效率。【产品内所有用户生效，可实例级别配置调整】

- **变更脚本事务性支持**：对于MySQL等关系型数据库在变更执行时可按需开启事务，若变更生效则全部生效，若串行到中间某一条失败则全部回滚；保障事务性要求严格的变更需求。【产品内所有用户生效，可按需开启与关闭，DRDS不支持开启】
- **变更脚本定时执行支持**：对于变更操作需要在业务低峰期执行的需求，可定时指定时间系统自动调度并反馈变更结果，避免人为定时的疲劳等不可控因素。【产品内所有用户生效，可按需启用】
- **变更脚本的备份支持**：对于变更脚本在执行前可进行即将变更数据的全记录行insert脚本备份，防止变更不符合预期可进行快速回滚恢复。【产品内所有用户生效，上限50W每个工单】
- **变更执行前风险管控**：在执行变更前会检测目标表的元数据锁，等待10s内获取不到锁则会失败退出再次重试，若重试3次都失败则认为数据库繁忙任务失败退出；防止加重数据库负载影响数据库性能进而影响在线业务。【产品内所有用户生效】
- **变更执行前风险管控**：在执行变更前会检测目标数据库实例的活跃连接数，超过阈值则会失败退出再次重试，若重试3次都失败则认为数据库繁忙任务失败退出；防止加重数据库负载影响数据库性能进而影响在线业务。【产品内所有用户生效】
- **变更执行中管控**：在单个SQL执行完成后会进行一定时长的sleep，保障数据库负载过于集中做到平缓执行，防止加重数据库负载影响数据库性能进而影响在线业务。【产品内所有用户生效】

## 5.17.2 租户侧安全功能

### 5.17.2.1 日志审计

DMS企业版提供产品内所有操作的操作日志可审计的功能，在系统管理->操作日志页面供产品内管理员角色可随时多维度审计；每一个操作详细记录了执行人、执行时间、执行动作、执行影响等内容。

## 5.18 分布式关系型数据库DRDS

### 5.18.1 平台侧安全设计

#### 5.18.1.1 安全隔离

网络隔离

DRDS支持使用VPC来获取更高程度的网络访问控制。

VPC是用户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，在网络层完成访问控制，使用VPC和IP白名单将极大程度提升DRDS实例的安全性。

### 5.18.1.2 鉴权认证

DRDS支持类MySQL的账号和权限体系，支持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@'%'”。

## 5.18.2 租户侧安全功能

### 5.18.2.1 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。用户可以通过控制台的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。

### 5.18.2.2 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

实际禁止效果如下：

```
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]
```

增加HINT后, 该语句执行成功:

```
mysql> /*TDDL:FORBID_EXECUTE_DML_ALL=false*/delete from tt;  
Query OK, 10 row affected (0.21 sec)
```

### 5.18.2.3 慢SQL审计

您可以在DRDS控制台上查询到客户端发送至DRDS的逻辑慢SQL, 慢SQL会增大整个链路的响应时间, 降低DRDS的吞吐量。

慢SQL内容包括: 执行开始时间、数据库名、SQL语句、客户端IP、执行时间。您可以通过DRDS控制台查询到具体的慢SQL信息从而进行优化调整。

### 5.18.2.4 监控信息

DRDS控制台提供不同维度的监控指标, 您可以根据监控信息进行相应的处理。

DRDS 监控信息分为两类:

- 资源监控, 包括CPU和网络。
- 引擎监控, 包括逻辑QPS、物理QPS、逻辑RT(ms)、连接数和活跃线程数。

DRDS实例的QPS和CPU性能是正向相关的。当DRDS性能出现瓶颈时, 主要表现为实例的CPU利用率居高不下。如果发现CPU利用率超出90%或持续超出80%, 则意味着当前实例性能出现瓶颈。在DRDS不存在瓶颈的情况下, 可以判断当前的DRDS实例规格无法满足业务的QPS性能需求, 需要通过升配解决。

## 5.19 时间序列数据库TSDB

### 5.19.1 平台侧安全设计

#### 5.19.1.1 鉴权认证

只有经用户许可, 阿里云团队才会查看和修改数据库的配置。

权限管理

在没有经过用户同意的情况下, 阿里云的售后团队和TSDB开发团队只能查看TSDB实例资源、费用和性能相关的信息, 例如TSDB实例的购买时间和到期时间、TSDB实例的CPU、内存和存储空间的使用情况、服务异常日志。

只有经过用户许可后，阿里云的售后团队和TSDB 开发团队才会在用户指定时间查看和修改TSDB实例的配置信息，例如TSDB实例服务配置和TSDB的流量权重。在任何情况下，阿里云的售后团队和TSDB开发团队不会主动变更TSDB实例的链接信息。

### 5.19.1.2 安全隔离

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，在数据链路层完成访问控制。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TSDB 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TSDB实例的目的VPC，同时隔离VPC以外的访问请求，保证服务的安全性。

### 5.19.1.3 数据安全

TSDB实例通过多种方式保证数据安全。

#### 引擎节点高可用

TSDB实例由多个TSDB引擎节点构成，通过负载均衡设备以单一服务出口的方式提供读写服务。当其中的一个TSDB引擎节点出现故障时，流量可以在短时间内切换到其他的TSDB引擎节点上，以保证服务的正常运行。整个切换过程对用户透明，应用代码无需更新，应用进程无需重启。

#### 存储节点高可用

TSDB存储服务有多个TSDB存储节点构成，多个存储节点之间通过服务协调组件进行服务的高可靠性保障，同时相互协调保证数据的冗余性。当其中的一个节点出现故障时，其他的存储节点可以继续提供正常的数据存储服务，并保证数据的完整性，同时会进一步进行冗余保证数据的可靠性。

#### 数据三副本策略

TSDB允许数据在同一个实例的多个服务器上共享，一个本地服务器可以存取不同物理地点的远程服务器上的数据，也可以使所有的服务器均持有数据的拷贝。在默认情况下，TSDB将数据进行三份备份，这样，在拥有三个副本的文件系统的情况下，将极少出现无法访问的情况，从而提高了系统的可用性；更保证数据的安全性，极少出现数据损坏的情况。另外，系统可以通过其他完好的副本对发生错误的副本进行修复，从而提高系统的容错性。

## 5.19.2 租户侧安全功能

### 5.19.2.1 IP白名单

TSDB提供了IP白名单来实现网络安全访问控制。

默认情况下，TSDB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TSDB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。用户可以根据需要进行部分IP或IP段的访问权限控制，保证细粒度的网络安全。

### 5.19.2.2 软件升级

TSDB定期为用户提供数据库软件的新版本。版本升级是非强制性的，只有用户主动要求，才会升级到指定版本。

TSDB升级过程通常在5分钟以内完成，升级期间可能会造成部分读写性能的下降。

## 5.20 负载均衡SLB

### 5.20.1 平台侧安全设计

#### 5.20.1.1 鉴权认证

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。同时，SLB支持STS服务，通过临时访问凭证提供短期访问权限管理。

### 5.20.2 租户侧安全功能

#### 5.20.2.1 HTTPS

SLB提供HTTPS负载均衡功能，转发来自HTTPS协议的请求。

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提供证书管理功能，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。

#### 5.20.2.2 IP白名单

SLB可以屏蔽后端服务器IP地址，对外只提供SLB的服务地址。

同时，SLB提供源IP白名单访问控制功能，通过添加负载均衡监听的访问白名单，仅允许特定IP访问负载均衡服务。



### 5.20.2.3 日志管理

负载均衡提供日志管理功能，您可以查看某个实例的操作日志和健康检查日志。

## 5.21 专有网络VPC

### 5.21.1 平台侧安全设计

#### 5.21.1.1 安全隔离

VPC采用隧道技术，达到与传统VLAN方式相同的隔离效果，广播域隔离可达实例、网卡级别。通过相当于VLAN级别的隔离，彻底阻断网络通讯。同时，划分不同的安全域，实现访问控制。

每个VPC都有一个独立的隧道号，一个隧道号对应着一张虚拟化网络。

一个VPC内的ECS之间的传输数据包都会加上隧道封装，带有唯一的隧道ID标识，然后送到物理网络上进行传输。

不同VPC内的ECS因为所在的隧道ID不同，本身处于两个不同的路由平面，所以不同VPC内的ECS无法进行通信，天然地进行了隔离。

#### 5.21.1.2 访问控制

VPC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。

### 5.21.2 租户侧安全功能

#### 5.21.2.1 安全组

VPC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，并基于安全组实现三层网络的访问控制。

不同VPC之间内部网络完全隔离，可以通过路由器接口互联。

## 5.22 日志服务

### 5.22.1 平台侧安全设计

#### 5.22.1.1 安全隔离

日志服务Logtail支持多租户隔离功能。与当前主流的开源采集Agent相比，Logtail采用的是更加精细的架构，事件发现、数据读取、解析、发送等都采用固定数量的线程，解析线程可配置，且线程规模不会随配置数增多。虽然所有配置都运行在同一执行环境，但日志服务采用了多种技术手段

保障各个配置处理流程的相互隔离、配置间调度的公平、数据采集可靠性、可控性以及非常高的资源性价比。

Logtail在多租户隔离功能中的技术特点：

- 支持时间片采集调度，保证各个配置数据入口的隔离性和公平性。
- 支持多级高低水位反馈队列，在极低的资源占用下依然可以保证各处理流程间以及多个配置间的隔离性和公平性。
- 支持事件处理不阻塞的机制，保证即使在配置阻塞或停采期间发生文件轮转依然具有较高的可靠性。
- 支持各个配置不同的流控、停采策略以及配置动态更新，保证数据采集具备较高的可控性。

### 5.22.1.2 鉴权认证

为保证用户日志数据的安全，Log Service API 的所有 HTTP 请求都必须经过安全验证。目前，该安全验证基于阿里云的访问秘钥、使用对称加密算法完成。

其工作流程如下：

1. 请求端根据 API 请求内容（包括 HTTP Header 和 Body）生成签名字符串。
2. 请求端使用阿里云的访问秘钥对（AccessKey ID 和 AccessKey Secret）对第一步生成的签名字符串进行签名，生成该 API 请求的数字签名。
3. 请求端把 API 请求内容和数字签名一同发送给服务端。
4. 服务端在接到请求后会重复如上的第一、二步工作，并在服务端计算出该请求期望的数字签名。



说明：

服务端会在后台取得该请求使用的用户访问秘钥对。

5. 服务端用期望的数字签名和请求端发送过来的数字签名做比对，如果完全一致则认为该请求通过安全验证。否则直接拒绝该请求。

### 5.22.1.3 数据安全

日志服务用户的数据写入最终都会被映射为对专有云数据存储平台上的文件的读写。

专有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，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。

在专有云数据存储系统中，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。

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。

#### 5.22.1.4 传输加密

日志服务从以下方面保证您的数据传输安全：

- 日志服务认证采用由阿里云颁发给用户的访问秘钥（Access Key）。为保证您的数据在发送过程中不会被篡改，Logtail客户端会主动获取用户的阿里云访问秘钥，并对所有发送日志的数据包进行数据签名，并在身份认证时使用HMAC-SHA1签名算法。



说明：

Logtail客户端在获取您的阿里云访问秘钥时采用HTTPS通道，保障您的访问秘钥安全性。

- API层提供签名+授权机制，保证数据被访问的权限与安全性。
- 日志服务支持HTTPS/SSL协议，将HTTPS/SSL应用于用户端和服务端之间的网络连接，保证数据在传输过程中不被监听和窃取。用户与服务通信的数据保密性也由HTTPS协议提供保护。

### 5.22.2 租户侧安全功能

#### 5.22.2.1 服务监控

日志服务支持对机器组状态和Logtail日志采集状态的实时监控。

- 机器组状态监控

日志服务支持对您的机器组中所有服务器的心跳状态实时监控。其中，服务器状态包括OK和Fail。心跳Fail状态说明机器组状态异常，无法正常完成日志采集工作。

- 日志采集状态监控

使用Logtail收集日志时，如果遇到正则解析失败、文件路径不正确、流量超过Shard服务能力等错误，日志服务会在采集错误诊断中发出告警提示信息。告警信息中包含错误发生时间、发生错误的服务器IP、错误次数和错误类型。

## 5.23 资源编排

### 5.23.1 平台侧安全设计

#### 5.23.1.1 数据安全

无。

#### 5.23.1.2 鉴权认证

ROS支持RAM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予子账号。

### 5.23.2 租户侧安全功能

#### 5.23.2.1 日志审计

ROS提供历史事件的信息展示，包括以资源栈为维度的事件日志，提供包括：资源名称、关联资源ID、资源类型、资源状态、状态描述和事件发生时间等内容。该事件日志提供了资源栈的变更历史信息。

## 5.24 密钥管理服务KMS

### 5.24.1 平台侧安全设计

#### 5.24.1.1 安全隔离

密钥管理服务并非实例化部署的产品，因此不存在实例产品虚拟化带来的资源隔离问题。

密钥服务产品中的资源为用户主密钥，用户只能通过Open API的访问间接使用密钥，用户对密钥资源并没有直接访问的能力，安全隔离实现在Open API的网络层。

## 5.24.1.2 鉴权认证

### 5.24.1.2.1 身份验证

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

当用户向KMS发送请求时，需要首先将发送的请求按照KMS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。KMS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，KMS将拒绝处理这次请求，并返回HTTP 403错误。

### 5.24.1.2.2 权限控制

对KMS的访问控制通过RAM来实现。可以通过RAM的权限策略定义不同的身份类型，授予用户KMS的使用权限。

KMS的权限主要通过如下两个RAM概念来描述：

- 操作：KMS OpenAPI的Action，包括对密钥的增删改查，以及使用密钥对数据进行加解密等操作。每一个API都对应到一个Action，可以独立被授权给一个身份。
- 资源：KMS的资源为密钥，通过密钥的ID来描述。

### 5.24.1.2.3 RAM和STS支持

KMS支持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。

## 5.24.1.3 数据安全

KMS的数据就是用户创建和管理的用户主密钥。用户主密钥通过冗余RDS（主备模式）存储，RDS每一个备份同时具有自己的冗余和备份机制，因此可以实现对用户数据的多层次冗余。

用户主密钥的密钥材料落盘时被KMS系统进行了加密，KMS系统实现了多层次的密钥结构，并有对上层次密钥进行自动轮转的能力。KMS也支持接入硬件TPM模块从而实现对KMS根密钥的硬件保护，从而保证用户数据的私密性。

#### 5.24.1.4 传输加密

密钥管理服务实现了数据传输的全链路加密。用户向KMS发起的请求，必须通过HTTPS协议进行，以保证信息交换的私密性和完整性。

### 5.24.2 租户侧安全功能

#### 5.24.2.1 日志审计

密钥管理服务利用阿里云日志服务对KMS操作进行记录，用户可以在日志服务中对KMS的操作进行安全审计。

## 5.25 专有云DNS

### 5.25.1 租户侧安全设计

#### 5.25.1.1 租户隔离

专有云DNS对租户数据进行了隔离，通过请求中传入的AK信息识别当前请求是否对当前数据进行相应操作。对于绑定的VPC和ZONE数据，通过tunnel id进行一一关联，后端解析服务通过对用户请求中的tunnel id进行相应的数据返回，实现租户与租户之间的数据安全隔离。

#### 5.25.1.2 网络安全加固

专有云DNS为云内用户提供了递归能力，为防止公网链路引入的安全风险，对解析服务进行了安全加固，实施了单向隔离，仅允许出方向的流量通过，对于入方向（公网）进行了丢弃处理。

#### 5.25.1.3 日志审计

日志分析是安全保障中非常重要的一环。专有云DNS系统提供相关日志详情，所有的操作数据都会被实时收集，一旦出现安全问题，用户可通过日志进行分析调查。

## 5.26 媒体处理MPS

## 5.26.1 安全隔离

媒体处理引入了管道的概念，保证了租户之间的共享资源隔离。同时采用管道限流策略，保证了单用户使用大量资源的情况。

## 5.26.2 鉴权认证

### 5.26.2.1 身份认证

媒体处理接入POP网关，由POP网关来完成身份验证。根据Access Key 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Access Key 信息。媒体处理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。

### 5.26.2.2 RAM和STS支持

媒体处理所有的接口已经接入 RAM/STS 鉴权，支持用户对子账号进行授权管理。

- 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。

## 5.27 API网关

### 5.27.1 平台侧安全设计

#### 5.27.1.1 安全隔离

API网关对用户的资源进行租户隔离。租户创建的资源都归属于该租户的账号下，不同租户间资源相互隔离。

#### 5.27.1.2 鉴权认证

##### 5.27.1.2.1 身份验证

用户可以在云管控中心中自行创建AccessKey。AccessKey由AccessKeyId和AccessKeySecret组成，其中AccessKeyId是公开的，用于标识用户身份，AccessKeySecret是秘密的，用于用户身份的鉴别。

当用户向API网关发送请求时，需要首先将发送的请求按照API网关指定的格式生成签名字符串，然后使用AccessKeySecret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。API网关收到请求以后，通过AccessKeyId找到对应的AccessKeySecret，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，API网关将拒绝处理这次请求，并返回HTTP 403错误。

#### 5.27.1.2.2 API权限控制

API网关的用户分为API提供者和第三方用户。当API提供者希望将API授权给第三方用户使用，需要第三方用户提供能够确认该用户身份的AppId。API提供者将API授权该AppId的访问权限后，第三方用户即可通过该App上对应的AppKey和AppSecret发起访问。

进行API访问时，需要携带用户身份的签名才能访问，带签名访问是指按照API网关文档中规定的在请求头部携带签名信息。

#### 5.27.1.2.3 RAM和STS支持

API网关的管控API支持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予子账号。

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。

#### 5.27.1.3 数据安全

API网关可通过签名认证保证API调用时用户数据的一致性和完整性。除此之外，API网关提供数据清洗功能。数据清洗是指清洗非法参数，保证请求的安全性。

首先，API网关需要调用者在调用API网关时携带用户身份信息，并对传输内容进行签名加密处理。API网关在收到调用请求后，会进行验签来校验用户的身份以及数据的完整性和一致性。

除此之外，API网关可根据用户预设的请求参数，对非法参数进行过滤和清洗。保证调用请求的合法性和安全性。

#### 5.27.1.4 传输加密

API网关支持HTTPS协议支持，保证用户数据的传输过程安全可靠。

### 5.27.2 租户侧安全功能



### 5.27.2.1 日志审计

LOG是阿里云提供的一款高效的日志相关管理软件。API网关通过与LOG产品的结合，为用户提供所需的访问、监控和审计等内容的查询和展示。API网关实时记录客户请求，并定时将日志内容同步到LOG。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。

### 5.27.2.2 IP访问控制

API网关可以根据调用者的ClientIP设置黑白名单。

将IP访问控制策略绑定到对应的API上，即可生效。有效防止非法来源的API请求。

- 黑名单：禁止该IP来源的请求访问API网关。
- 白名单：只允许该IP来源的请求访问API。

## 5.28 企业级分布式应用服务EDAS

### 5.28.1 平台侧安全设计

平台侧安全设计主要包括鉴权认证和传输加密。

#### 5.28.1.1 鉴权认证

鉴权认证主要包括权限控制、访问控制和API鉴权。

权限控制

- EDAS Agent

EDAS Agent分成两个层面的认证和授权：一是客户端到服务端进行认证；第二个层面是下发指令需要由AK/SK的认证授权来保证最小特权原则的实现。

- DAuth

- 安全凭证：通过EDAS DAuth可以针对EDAS的访问生成App\_KEY和App\_SECRET，实现认证控制。
- 鉴权设置：支持针对EDAS的鉴权进行细颗粒度的策略设置，包括对开启鉴权、验证签名、日志开关、自定义日志、日志缓存、日志检测等策略进行设置。

- DiamondServer

DiamondServer对于HTTP/HTTPS接口的访问使用DAuth生成的App\_KEY和App\_SECRET来进行鉴权。

- ConfigServer

- 流量限速：针对ConfigServer的HTTP请求，进行流量限速限制，避免对ConfigServer造成访问压力过大导致的不稳定。
- 认证：ConfigServer对于HTTP/HTTPS接口的访问使用DAuth生成的App\_KEY和App\_SECRET来进行鉴权。

#### 访问控制

EDAS RAM授权支持通过STS获取到用户的临时AK/SK（临时AK/SK有时效性，经过一段时间就会过期，需要重新生成AK/SK），通过临时AK/SK来访问用户的ECS API执行创建ECS的操作。ECS的API权限进行了限制，只有使用指定的API权限才可进行操作，从而避免使用ECS RAM FullAccess权限导致权限授权过大的问题。

#### API鉴权

针对API访问的权限通过AccessKey进行鉴权，鉴权也可以使用子账号的AccessKey来进行。EDAS API使用基于密钥Hash Message Authentication Code（HMAC）的自定义HTTPS方案进行身份验证。对请求进行身份验证，用户首先需要合并请求的选定元素，以形成一个字符串。然后，使用EDAS密钥来计算该字符串的HMAC。通常，将此过程称为“签署请求”，输出HMAC的算法称为“签名”，因为它会模拟真实签名的安全属性。最后，用户可以使用EDAS API的语法，作为请求的参数添加此签名。

系统收到经身份验证的请求时，将提取EDAS密钥，并以相同的使用方式将它用于计算已收到的消息的签名。然后，将计算出的签名与请求者提供的签名进行对比。如果两个签名相匹配，则系统认为请求者拥有对EDAS密钥的访问权限，因此充当向其颁发密钥的委托人的颁发机构。如果两个签名不匹配，那么请求将被丢弃，同时系统将返回错误消息。

### 5.28.1.2 传输加密

EDAS服务使用的TLS证书部署方案实现全链路加密。同时，考虑到证书存在有效期，EDAS服务支持证书更新功能。

#### EDAS管控安全

EDAS管控流程主要包含以下角色：

- EDAS Console：通过控制台进行集群创建、包的部署等操作。
- EDAS Agent：即部署在用户ECS上的EDAS客户端，进行各种相关的操作。EDAS Agent分为StarAgent以及EDAS Agent两个组件。
- EDAS Server：EDAS Server接收EDAS Console的指令并下发到EDAS Agent。

EDAS管控的具体安全流程如下：

1. EDAS Console收到用户的部署指令（例如部署WAR包等操作），EDAS Console进行API鉴权，使用 RAM 用户的 AK/SK 连接到EDAS Server API。
2. EDAS Server通过加密通道把加密指令传送到EDAS Agent。

#### EDAS RPC调用安全

EDAS RPC调用流程涉及以下角色：

- EDAS Dauth：生成EDAS用户AK/SK，并且进行鉴权等操作。
- EDAS CS：ConfigServer（CS）提供服务注册、IP地址、调用API等信息。
- EDAS Dubbo & HSF：分布式RPC产品。
- EDAS Pandora：轻量级容器隔离服务，实现类的隔离和加载。

EDAS RPC调用的具体按流程如下：

1. 消费者和提供者都启动Pandora进程，Pandora提供HSF和Dubbo的调用服务。
2. 提供者在ECS上和EDAS CS服务进行服务注册操作。连接CS注册服务的过程中使用TLS安全来保护链路安全，并且使用EDAS AK/SK来进行鉴权操作，只有指定的用户才能发布调用的接口，注册到CS服务上。
3. 消费者通过EDAS CS服务拉取相关信息，包括提供者提供的服务名、服务IP地址等。
4. 消费者直接调用提供者的Pandora进程来进行访问，通过EDAS AK/SK来进行认证授权，进而调用服务。

#### EDAS Docker安全

EDAS Docker的调用流程如下：

1. EDAS使用Docker API创建Docker集群，并且使用RAM的STS临时Token来进行鉴权操作。
2. 创建集群证书，每个集群生成一个证书。
3. 创建资源（包括ECS,SLB等），使用RAM的STS临时Token来调用ECS、SLB的OpenAPI来进行调用。根据需要用到的API，对该API进行授权。
4. 配置节点。
  - a. 生产节点证书。集群会生成一个根证书，然后使用集群的根证书来生成节点证书，使用cloud-init直接进行传递。
  - b. 安装Docker，使用cloud-init来安装Docker服务。
  - c. 安装EDAS-Agent等系统服务，使用EDAS安装脚本来进行安装服务和EDAS-Agent等服务，后续使用EDAS管控流程进行管控操作。

## 5.28.2 租户侧安全功能

租户侧安全功能主要为API审计。

操作审计（ActionTrail）会记录云账户资源操作，提供操作记录查询，并可以将记录文件保存到用户指定的OSS存储空间。利用ActionTrail保存的所有操作记录，可以实现安全分析、资源变更追踪以及合规性审计。

ActionTrail收集云服务的API调用记录（包括用户通过控制台触发的API调用记录），规格化处理后将操作记录以文件形式保存到指定的OSS Bucket。用户还可以使用OSS提供的所有管理功能来管理这些记录文件，比如授权、开启生命周期管理、归档管理等。

## 5.29 消息队列Apache RocketMQ版

### 5.29.1 平台侧安全设计

#### 5.29.1.1 鉴权认证

身份鉴权

消息队列Apache RocketMQ版（简称RocketMQ）的安全访问控制包括以下几个要素：

- 被访问的实例：实例（InstanceId）
- 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）

RocketMQ的权限类型包括：

- 发布权限
- 订阅权限

当用户在RocketMQ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，RocketMQ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，RocketMQ Broker服务也会对该Topic进行鉴权。

RocketMQ管控平台会对每一次请求进行鉴权和访问控制。除此之外，RocketMQ的所有服务组件包括mq-namesrv，mq-broker等都提供API级别的鉴权。每一次API调用都会使用HmacSHA1方法对调用进行签名和权限校验，保障用户的数据安全性。

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。

## 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RocketMQ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：

- RocketMQ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。

## 访问限制

队列提供两种网络访问类型：Any Tunnel和Single Tunnel。当RocketMQ部署完成时，默认情况下，RocketMQ服务提供Any Tunnel的访问模式，即在所有的VPC环境都可畅通无阻地使用RocketMQ服务。这种访问模式能满足大部分的用户需求。用户也可以通过RocketMQ控制台或API将访问类型切换为Single Tunnel，即只允许在某个指定的VPC环境使用消息服务。

### 5.29.1.2 安全隔离

RocketMQ支持用户使用VPC来获取更高程度的网络访问控制。VPC是用户在专有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，在数据链路层完成访问控制；用户可以通过VPN或者专线，将自建IDC的服务器资源接入专有云，并使用VPC自定义的IP段来解决IP资源冲突的问题，实现自有服务器和专有云ECS服务器同时访问RocketMQ的目的。

同时，RocketMQ支持多套部署，不同的服务集群可绑定至不同的VPC网络环境，在物理上和网络上做到彻底隔离，做到对测试、预发以及生产等环境的细粒度保护。

### 5.29.1.3 传输加密

RocketMQ提供对传输层安全性协议（TLS）的支持，为所有服务组件之间，以及客户端与服务组件之间的通信提供安全及数据完整性保障。同时，考虑到TLS证书存在有效期，RocketMQ的服务支持动态证书和私钥更新功能，无需停机重启即可更换证书。对于私钥，支持密文存储，运行时自动解密，保障私钥的安全性。

同时，在传输层加密的基础上，配合RocketMQ已经具备的访问控制机制，每次网络调用请求都将进行签名认证和权限校验，更充分地保障数据的安全性和完整性。

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

## 5.29.2 租户侧安全功能

### 5.29.2.1 账号黑名单

在提供鉴权机制的同时，RocketMQ提供了“用户黑名单”来实现安全访问控制。

RocketMQ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RocketMQ进行访问，从而阻止其对RocketMQ进行恶意的攻击。

### 5.29.2.2 日志审计

日志审计是网络安全中非常重要的一环，RocketMQ的所有基于控制台的人为运维操作都会有审计日志记录。

审计日志的事件种类包括删除、创建以及更新等，比如Topic资源的创建和删除、权限的授予和撤销。所有的日志都有能保存较长时间的审计日志。

审计日志已对接运维监控平台，所有的数据都会被实时收集，并被离线存储，方便用户进行离线查询与对账。

## 5.30 微消息队列MQTT

### 5.30.1 平台侧安全设计

#### 5.30.1.1 鉴权认证

身份鉴权

微消息队列MQTT的安全访问控制包括以下几个要素：

- 被访问的实例：实例（InstanceId）
- 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）

微消息队列MQTT的权限类型包括：

- 发布权限
- 订阅权限

当用户在微消息队列MQTT上创建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，微消息队列MQTT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，MQTT Broker服务也会对该Topic进行鉴权。

微消息队列MQTT管控平台会对每一次请求进行鉴权和访问控制。除此之外，微消息队列MQTT的消息服务器也提供API级别的鉴权。每一次API调用都会使用HmacSHA1方法对调用进行签名和权限校验，保障用户的数据安全性。

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。

### 5.30.1.2 安全隔离

微消息队列MQTT支持用户使用多实例方式来实现服务和数据的逻辑隔离，避免不同实例的应用之间相互影响。

同时，消息队列支持多套部署，不同的服务集群提供不同的接入点地址，在物理上和网络上做到彻底隔离。

### 5.30.1.3 传输加密

微消息队列MQTT提供对传输层安全性协议（TLS）的支持，为所有服务组件之间，以及客户端与服务组件之间的通信提供安全及数据完整性保障。同时，考虑到TLS证书存在有效期，消息队列的服务支持动态证书和私钥更新功能，无需停机重启即可更换证书。对于私钥，支持密文存储，运行时自动解密，保障私钥的安全性。

同时，在传输层加密的基础上，配合微消息队列MQTT已经具备的访问控制机制，每次网络调用请求都将进行签名认证和权限校验，更充分地保障数据的安全性和完整性。

需要注意的是，虽然微消息队列MQTT提供了应用到消息队列之间的连接加密功能，但是TLS需要应用开启服务器端验证才能正常运转。另外，TLS也会带来额外的CPU开销，对消息的吞吐量和响应时间都会受到一定程度的影响，具体影响视用户的连接次数和数据传输频度而定。

## 5.30.2 租户侧安全功能

### 5.30.2.1 账号黑名单

在提供鉴权机制的同时，微消息队列MQTT提供了“用户黑名单”来实现安全访问控制。

微消息队列MQTT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）对微消息队列MQTT进行访问，从而阻止其对微消息队列MQTT进行恶意的攻击。

### 5.30.2.2 日志审计

日志审计是网络安全中非常重要的一环，微消息队列MQTT的所有基于控制台的人为运维操作都会有审计日志记录。

审计日志的事件种类包括删除、创建以及更新等，比如Topic资源的创建和删除、权限的授予和撤销。所有的日志都有能保存较长时间的审计日志。

审计日志已对接运维监控平台，所有的数据都会被实时收集，并被离线存储，方便用户进行离线查询与对账。

## 5.31 业务实时监控服务ARMS

### 5.31.1 平台侧安全设计

#### 5.31.1.1 安全隔离

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，以满足计算需求。

如果一个用户的任务出现异常，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，可保障其他用户任务不会受到任何干扰。

##### 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。

#### 5.31.1.2 鉴权认证

ARMS 通过 AccessKey 和 RAM 主子账号体系进行权限管控。

##### 身份验证

您可以在云控制台自行创建 AccessKey。AccessKey 包含以下部分：

- AccessKeyID：公开，用于标识用户身份。
- AccessKeySecret：保密，用于鉴别用户身份。



ARMS 支持 RAM 主子账号

访问控制 RAM（Resource Access Management）是阿里云提供的资源访问控制服务。您可以使用 RAM 主账号创建从属于主账号的子账号。默认情况下，子账号具有主账号的全部权限。

## 5.31.2 租户侧安全功能

### 5.31.2.1 HTTPS

ARMS 控制台提供将服务开放成为 HTTP 协议的能力，也可以在链路上支持 SSL，即 HTTPS。

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

## 5.32 全局事务服务GTS

### 5.32.1 全局事务服务GTS

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。

### 5.32.2 访问控制

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。

## 5.33 云服务总线CSB

### 5.33.1 平台侧安全设计

#### 5.33.1.1 鉴权认证

CSB 在平台侧主要做了身份鉴权和API鉴权。

##### 身份鉴权

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 是否有权调用该服务。

##### API鉴权

针对API访问的权限通过AccessKey进行鉴权。CSB API使用基于密钥Hash Message Authentication Code (HMAC) 进行身份验证。对请求进行身份验证，用户首先需要合并请求的选定元素，以形成一个字符串。然后，使用CSB密钥来计算该字符串的HMAC。通常，将此过程称为“签署请求”，输出HMAC的算法称为“签名”，因为它会模拟真实签名的安全属性。最后，用户可以使用CSB API的语法，作为请求的参数添加此签名。

系统收到经身份验证的请求时，将提取CSB密钥，并以相同的使用方式将它用于计算已收到的消息的签名。然后，将计算出的签名与请求者提供的签名进行对比。如果两个签名相匹配，则系统认为请求者拥有对CSB密钥的访问权限，因此充当向其颁发密钥的委托人的颁发机构。如果两个签名不匹配，那么请求将被丢弃，同时系统将返回错误消息。

### 5.33.2 租户侧安全功能

租户侧的安全功能主要包括 IP黑白名单、防止重放、HTTP和API审计。

##### 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。用户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。

## API审计

操作审计（ActionTrail）会记录云账户资源操作，提供操作记录查询，并可以将记录文件保存到用户指定的OSS存储空间。利用ActionTrail保存的所有操作记录，可以实现安全分析、资源变更追踪以及合规性审计。

ActionTrail收集云服务的API调用记录（包括用户通过控制台触发的API调用记录），规格化处理后将操作记录以文件形式保存到指定的OSS Bucket。用户还可以使用OSS提供的所有管理功能来管理这些记录文件，比如授权、开启生命周期管理、归档管理等。

## 5.34 MaxCompute

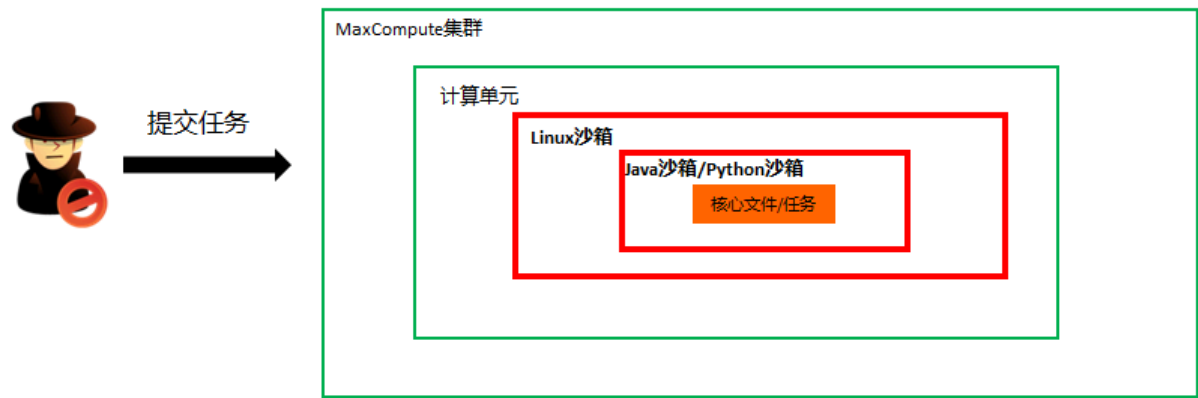
### 5.34.1 平台侧安全设计

#### 5.34.1.1 安全隔离

MaxCompute支持多租户的使用场景，通过阿里云账号认证体系，即认证方式采用AccessKey对称密钥认证技术，同时对于用户的每一个HTTP请求都会进行签名认证，针对不同的用户数据进行数据存储隔离，用户数据被离散存储在分布式文件系统中。可以同时满足多用户协同、数据共享、数据保密和安全的需要，做到真正的多租户资源隔离。

同时，MaxCompute中所有计算是在受限的沙箱中运行的，多层次的应用沙箱，从KVM级到Kernel级。系统沙箱配合鉴权管理机制，用来保证数据的安全，避免出现内部人员恶意或粗心造成服务器故障。

图 5-3: 沙箱保护



网络隔离

大数据计算服务（MaxCompute）作为阿里云开发的海量数据处理平台，在安全性方面需要满足安全隔离规范的要求。因此，MaxCompute团队增加了MaxCompute对专有网络（VPC）的支持，为MaxCompute配置使用限制，即MaxCompute VPC的限制。

目前MaxCompute支持VPC的具体情况如下所示：

- 经典网络/VPC网络/Internet网络三网隔离，只能访问各自对应的endpoint及VIP。
- 没有配置VPC ID及IP白名单的project可以被三种网络中请求通过的相应域名访问，没有限制。
- 配置了VPC ID的project只能被对应的VPC访问。
- 配置了IP白名单的project只能被对应的机器访问。
- 对于加了代理的访问请求，判断为最后一跳代理IP及VPC ID为准。

ElasticSearch on MaxCompute作为阿里云开发的企业级海量数据检索系统，在安全性方面也需要满足安全隔离规范的要求。因此，MaxCompute团队在原有的MaxCompute支持专有网络（VPC）的基础上，增加了ElasticSearch on MaxCompute支持专有网络（VPC），为ElasticSearch on MaxCompute配置使用限制，即ElasticSearch VPC的限制。

目前ElasticSearch on MaxCompute支持VPC的具体情况如下所示：

- 经典网络/VPC网络/Internet网络三网隔离，只能访问各自对应的endpoint及VIP。
- 没有配置VPC ID及IP白名单的project可以被三种网络中请求通过的相应域名访问，没有限制。

- 某个MaxCompute Project启动一个ElasticSearch服务实例时，两者使用同一个vpclist，即VPC白名单共用，VPC限制范围相同。
- MaxCompute启动多套ElasticSearch服务实例时，由于资源分配模型目前默认为启动一套ElasticSearch服务实例占满所有资源，因此需要先扩容或者对原有ElasticSearch服务实例先缩容。

具体的使用场景为：MaxCompute专有云部署时默认创建一个project启动一个ElasticSearch服务实例，即每一个project启动一个ElasticSearch服务实例。用户可以在自己的project中启动自己的ElasticSearch实例，启动后申请域名及VIP，并在ElasticSearch frontend中进行VPC校验。

### 5.34.1.2 鉴权认证

#### 身份验证

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

当用户向MaxCompute发送请求时，首先需要将发送的请求按照MaxCompute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以生成请求签名。

MaxCompute收到用户请求后，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，MaxCompute将拒绝处理这次请求，并返回HTTP 403错误。

#### 权限控制

用户对MaxCompute资源访问分为两种，即用户主账号访问和用户子账号访问。主账号是阿里云的一个账号主体，主账号下可以包含不同的子账号以便用户可以灵活使用。MaxCompute支持主子账号的权限访问策略。

- 当用户使用主账号访问时，MaxCompute会校验该主账号是否为对应资源的所有者，只有对应资源的所有者才具备访问该资源的权限。
- 当用户使用子账号访问时，此时会触发子账号授权策略。MaxCompute会校验该子账号是否被对应主账号授予了访问该资源的权限，同时也会校验该子账号对应的主账号是否具有该资源的所有者权限。



#### 说明：

上述对主账号及子账号的描述，只是针对未进行授权操作的主账号及子账号。若主账号和子账号已通过相应的授权，则均可以获得资源权限，而不是只有资源的所有者才具备访问该资源的权限。

MaxCompute目前支持两种授权机制来完成对子账号的访问权限控制。

- **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，支持对“不存在”或“不确定”的对象和主体进行Policy授权操作，授权时不会验证授权存在性。当删除一个对象时，系统不会自动修改及删除与该对象关联的Policy。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。

MaxCompute还支持更多的访问权限控制机制。

#### 列级别访问控制

基于标签的安全（LabelSecurity）是项目空间级别的一种强制访问控制策略（Mandatory Access Control, MAC），它的引入可以让项目空间管理员更加灵活地控制用户对列级别敏感数据的访问。

LabelSecurity需要将数据和访问数据的人进行安全等级划分。一般来讲，会将数据的敏感度标记分为如下四类：

- 0级（不保密，Unclassified）。
- 1级（秘密，Confidential）。
- 2级（机密，Sensitive）。
- 3级（高度机密，Highly Sensitive）。

MaxCompute也遵循这一分类方法，ProjectOwner需要定义明确的数据敏感等级和访问许可等级划分标准。默认时所有用户的访问许可等级为0级，数据安全级别默认为0级。

LabelSecurity对敏感数据的粒度可以支持列级别，管理员可以对表的任何列设置敏感度标记（Label），一张表可以由不同敏感等级的数据列构成。而对于view，也支持和表相同的设置，即管理员可以对view设置label等级。View的等级和它对应的基表的label等级是独立的，在view创建时，默认的等级也是0级。

在对数据和人分别设置安全等级标记之后，LabelSecurity的默认安全策略如下：

- **No-ReadUp**：不允许用户读取敏感等级高于用户等级的数据，除非显式授权。
- **Trusted-User**：允许用户写任意等级的数据，新建数据默认为0级（不保密）。

**说明:**

- 在一些传统的强制访问控制系统中，为了防止数据在项目空间内部的任意分发，一般还支持更多复杂的安全策略，例如：不允许用户写敏感等级不高于用户等级的数据（No-WriteDown）。但在MaxCompute平台中，考虑到项目空间管理员对数据敏感等级的管理成本，默认安全策略并不支持No-WriteDown，如果项目空间管理员有类似需求，可以通过修改项目空间安全配置（SetObjectCreatorHasGrantPermission=false）以达到控制目的。
- 如果是为了控制数据在不同项目空间之间的流动，则可以将项目空间设置为受保护状态（ProjectProtection）。设置之后，只允许用户在项目空间内访问数据，这样可以有效防止数据流出到项目空间之外。

项目空间中的LabelSecurity安全机制默认是关闭的，ProjectOwner需要自行开启。需要注意，LabelSecurity安全机制一旦开启，上述的默认安全策略将被强制执行。此时，当用户访问数据表时，除了必须拥有Select权限外，还必须获得读取敏感数据的相应许可等级。

LabelSecurity安全机制的开/关命令如下。

```
Set LabelSecurity=true|false;
--开启或关闭LabelSecurity机制，默认为false。
--此操作必须由ProjectOwner完成，其他操作则可以由Admin角色完成。
```

基于权限模型2.0的列级别细粒度授权/鉴权

为了提供更精细的MaxCompute权限管理能力，进一步提升产品的安全能力，MaxCompute支持基于权限模型2.0的列级别细粒度授权/鉴权。

基于权限模型2.0的列级别细粒度授权/鉴权提供统一的权限操作及查询接口。

- MaxCompute + DataWorks能够达到租户内细粒度授权及跨租户通过Package资源共享后细粒度授权。
- MaxCompute提供人到表和表到人的授权数据查询能力。

下面将通过在表类型中增加colume相关控制操作的示例说明基于权限模型2.0的列级别细粒度授权方法。

**说明:**

由于Policy不支持细粒度授权（因为会导致细粒度授权像label一样无法管控，违背安全设计的初衷），因此以下示例为ACL细粒度授权方法的相关示例。

ACL细粒度授权语法



- Project内部授权/取消授权。

```
grant/revoke <privileges> on table <name>(<column_list>) to|from
USER/ROLE <user/role name>;
```

语法说明：

1. 当授权 (grant) 表 (table) 的权限时，默认授权 (grant) 了所有列 (column) 的权限，包含：
    - a. 增加的列 (column)。
    - b. 改名的列 (column)。
  2. 当授权 (grant) /取消授权 (revoke) 列 (column) 的权限时，对应的权限能够区分、合并，例如：
    - a. (区分) 授权 (grant) select给col1, col2, 授权 (grant) desc给col2, col3, 那么这两条授权都是有效的，不会被覆盖。
    - b. (合并) 授权 (grant) select给col1, col2, 然后授权 (grant) select给col3, col4, 那么select权限最终在col1, col2, col3, col4上生效。
  3. 授权的主体是当前project owner或者具备授权权限的人。
- 跨Project加入列 (column) 到package中。

```
add table <name>(<column list>) to package pkgdel1 with privileges <
privilege list>;
```



说明：

重复加入列 (column) 到package中时，会进行区分/归并的操作，不会产生报错。

语法说明：

1. allow的时候语法不变。
  2. install/uninstall的时候语法不变，但是需要考虑到列 (column) 的情况。
  3. 授权的主体是当前project owner或者具备授权权限的人。
- 跨Project授权/取消授权。

```
grant/revoke <privileges> on table <name>(<column_list>) to|from
USER|ROLE <user/role name>
```



```
PRIVILEGEPROPERTIES("refobject"="true", "refproject"="<project_name>", "package"="<package name>");
```

语法说明：

1. project内部授权 (grant) /取消授权 (revoke) 原则，对于跨project的授权 (grant) /取消授权 (revoke)，会在如下的情况下生效：表 (table) 在多个package中存在时。
2. 授权 (grant) /取消授权 (revoke) 的列 (column) 权限的范围不能超过加入进package的范围，但是要考虑到所有package同一张表的并集。
3. 授权的主体是当前project owner或者具备授权权限的人。

鉴权策略：根据授予的权限进行鉴权，与原本的ACL鉴权策略的逻辑一致，但是需要考虑到列 (column) 级别。

权限查询

- project内部权限查询。

```
show grants for <user|role name>; #无变化，但是查出来的结果到列 (column) 级别
show grants for table <name>(columns);
show grants on table <name>(columns) for user|role <name>;
```



说明：

如果指定了列 (column) 则仅显示对应列 (column) 的权限。

- Package权限查询。

```
describe package <pkg name>;
describe package <pkg name> PRIVILEGEPROPERTIES ("allowedonly"="true");
describe package <pkg name> PRIVILEGEPROPERTIES ("contentonly"="true");
```



说明：

上述几个desc package的命令都能够显示到列 (column) 级别。

- 跨project权限查询。

```
show grants for <user|role name> PRIVILEGEPROPERTIES ("refobject"="true", "refproject"="<project>"); #无变化，但是查出来的结果到column级别
show grants for table <name>(columns) PRIVILEGEPROPERTIES("refobject"="true", "refproject"="<project>");
show grants on table <name>(columns) for user|role <name> PRIVILEGEPROPERTIES ("refobject"="true", "refproject"="<project>");
```

审计策略：相关的信息会在审计日志中得到体现。

## 访问控制

MaxCompute支持RAM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。

### 5.34.1.3 数据安全

专有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, 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。

在专有云数据存储系统中, 有三类角色, 分别称为Master、Chunk Server和Client。MaxCompute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。

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MaxCompute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, 释放的存储空间由飞天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, 最大限度保证用户的数据安全性。

### 5.34.1.4 存储加密（KMS）

#### 背景信息

随着MaxCompute国际化部署，对于系统的安全要求愈发提高，尤其是系统中保存的用户隐私、金融资产等敏感数据，在分布式文件系统裸存是不可接受的，需要对敏感数据进行相应的保护。同时为了满足合规和监管的需求，需要MaxCompute支持Data at rest的加密。

因此，MaxCompute提供了数据存储加密功能，通过底层Apsara Pangu文件系统，实现对用户数据的加解密存储与操作，通过密钥管理服务（Key Management Service，简称：KMS）实现密钥管理，保证用户数据与密钥的安全性。

MaxCompute的存储加密功能，在更大程度上保障了用户数据的安全，即使出现数据遗失、被盗等情况，也可以做到相关数据无法被解读出有意义的内容，从而减轻数据遗失所造成的损失。



#### 说明：

- MaxCompute的存储加密功能，在保障用户持有密钥的基础上，实现透明的加解密，减少用户操作。
- MaxCompute的存储加密功能，在加密配置上以project为单位，即对设置为需要加密的project的后续所有的写数据操作均进行加密，从而降低安全风险。
- MaxCompute的存储加密功能，在兼容性上做到后向兼容，允许非加密project向加密project转换，允许在一个project中加密和非加密数据共存。

#### 功能概述

相关的功能介绍如下。

- 目前MaxCompute以project为单位，支持对project下的table数据进行加密存储。目前只支持全表加密，暂不支持resource和volume的加密。
- 支持数据存储加密的Task类型包括：SQL Task 2.0（含Service mode）、MergeTask和Tunnel。在project开启存储加密功能后，通过这些类型任务写入的表数据会以加密的形式进行存储。
- 用户可以自主选择以下三种加密算法：AES 128算法、AES 256算法以及RC4算法。
- MaxCompute接入KMS密钥管理系统以保障密钥的安全性，加解密密钥由KMS进行生成和管理，为此用户需要开通KMS服务。用户提交存储加密开启申请后，MaxCompute后台会自动访问KMS服务，为用户生成加密所需的密钥。



#### 说明：

同一个Project owner所属的多个Project共用同一份密钥。

- 数据加密后对用户使用保持透明，各种类型的任务不需额外改变，可以正常读取加密数据和非加密数据，Project内部支持加密和加密数据共存。

#### 数据加密流程

1. 用户申请开通KMS密钥管理服务。
2. 用户申请开通MaxCompute存储加密功能。



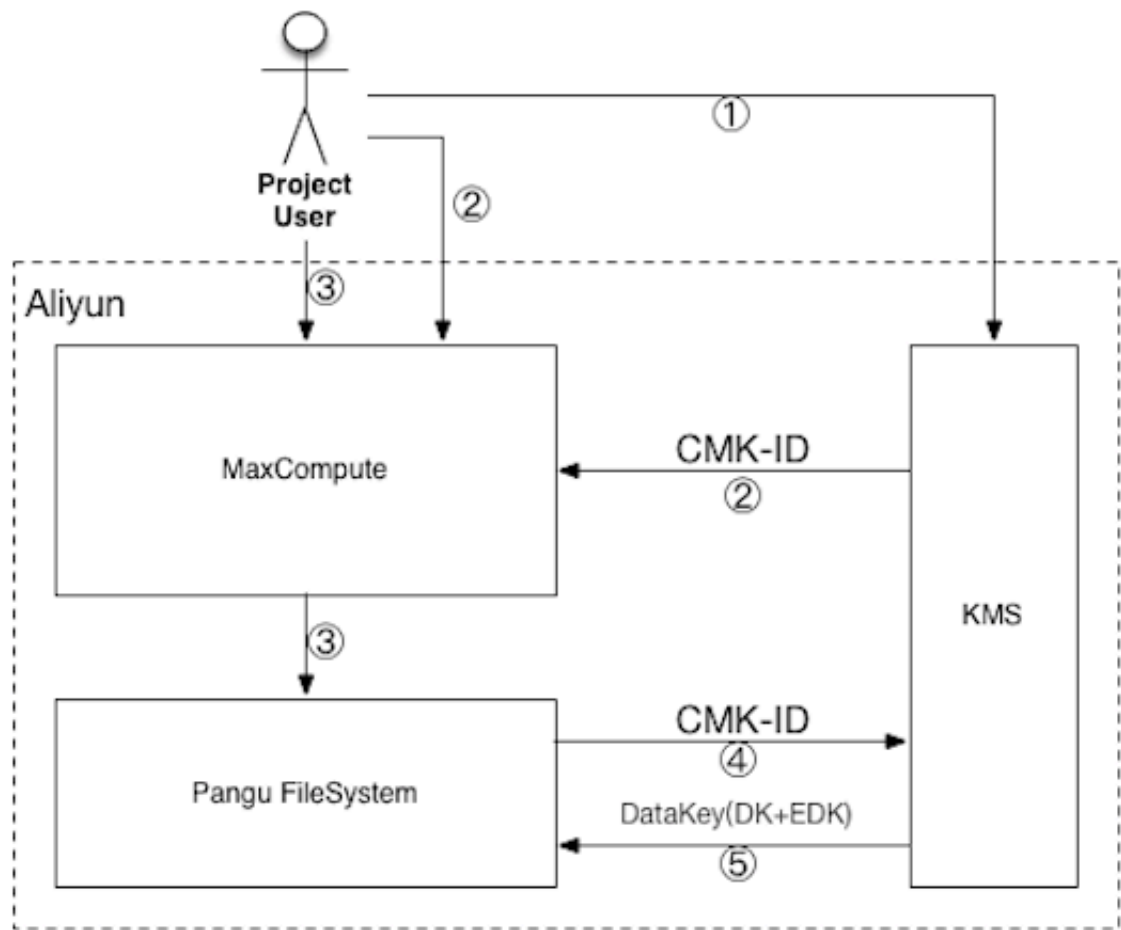
说明:

在开启存储加密功能时，系统会向KMS申请为用户创建CMK（Customer Master Key），CMK主要用于保护真正加密使用的数据密钥。

3. 服务及功能开通后，用户可以在MaxCompute上提交作业进行计算处理，处理完成后MaxCompute通过Pangu FileSystem实现数据的加密存储。
4. Pangu FileSystem通过向KMS提供用户创建的CMK，来获取真正加密使用的DataKey。
5. 从KMS获取到的DataKey包含两部分：加密数据使用的明文数据密钥DK，和通过信封加密技术保密后的密文数据密钥EDK。在使用DK对用户数据进行加密后，会将加密后的数据和EDK进行存储，从而最终完成数据加密的操作。

相关的数据加密流程图如下所示。

图 5-4: 数据加密流程



加密数据计算处理流程

在用户通过MaxCompute进行加密数据的计算处理时，系统会自动对数据进行解密，不需要用户的额外操作。具体流程如下。

1. 用户提交MaxCompute任务，处理加密数据。
2. Pangu FileSystem读取加密文件的EDK，并发送给KMS进行解密来获取DK。



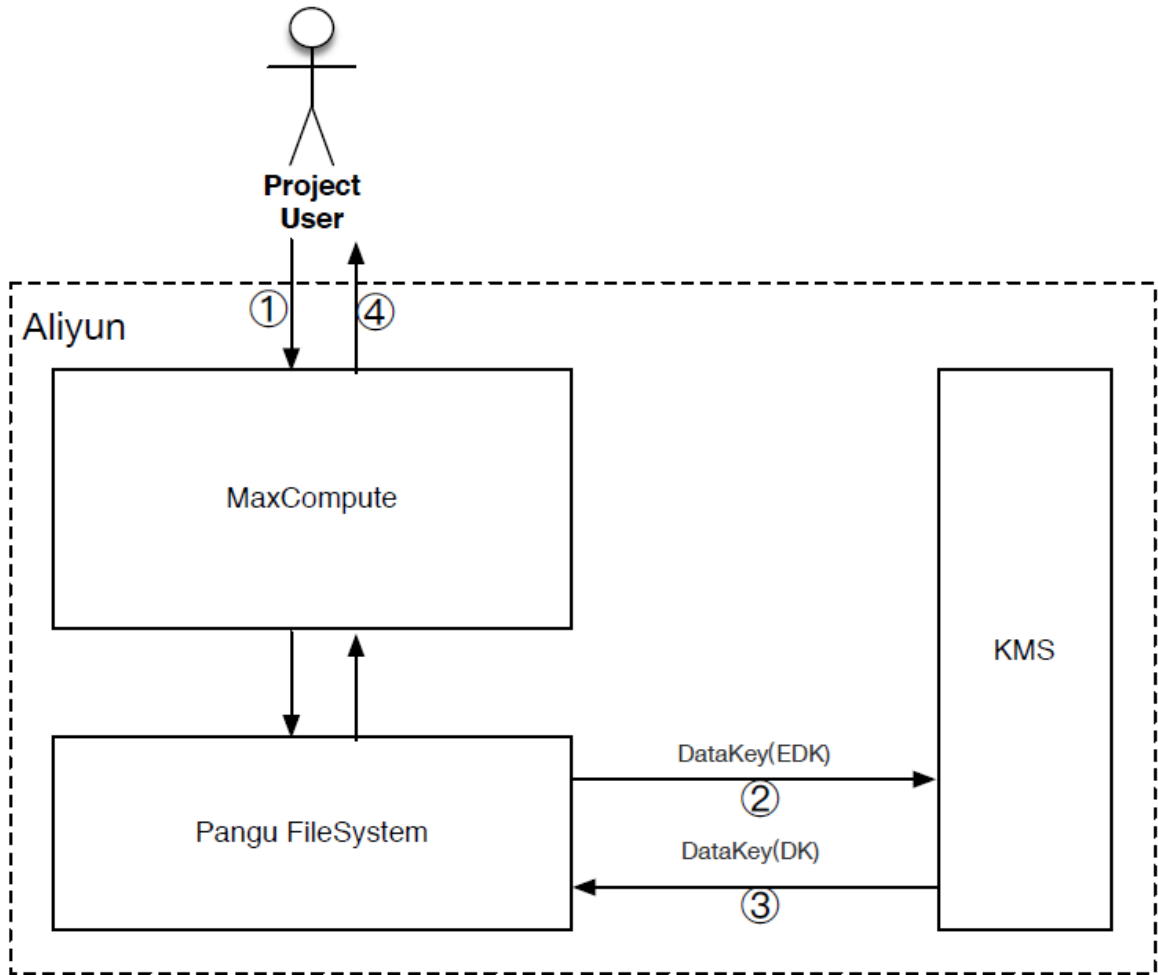
说明:

为保证数据安全性，EDK无法直接用来解密数据。

3. Pangu FileSystem根据收到的DK进行数据解密。
4. MaxCompute处理解密后的数据，向用户返回计算结果。

相关的加密数据计算处理流程图如下所示。

图 5-5: 加密数据计算处理流程



存储加密支持用户自定义密钥

为了支持用户不同场景的业务和安全需求，MaxCompute支持用户自定义密钥。在这种场景下，用户在创建project时，可以自己指定特定的CMK，进行数据加密。

用户使用自定义密钥加解密场景的相关操作流程如下。

1. 用户在创建project时，申请开通存储加密功能。
2. 打开存储加密功能的同时，指定该project使用的CMK-ID。

此时，用户可以选择MaxCompute代为创建CMK，也可以使用用户自己在KMS已创建或者上传的CMK。

需要注意，如果使用的CMK是用户自定义密钥，用户同时需要对MaxCompute进行授权，以便MaxCompute可以正常使用该CMK，创建及使用相应的数据密钥，完成数据加解密。

3. 选定对应的加密算法。

4. 完成其他对于project创建时需要进行的配置后，完成project创建。
5. Project创建完成后，存储加密功能就会生效，用户通过SQL、Tunnel等任务写入MaxCompute的数据将会以加密的形式进行保存。

#### 注意事项

为Project开通存储加密功能时，为了确保功能能够生效及正常使用，需要关注以下几点。

- 用户需要拥有阿里云账户，确认已开通KMS服务。对于未开通KMS服务的用户，会在前端进行提示，提示用户无法打开存储加密。
- 用户提交申请为特定的Project打开存储加密功能时，需要指定加密算法，如未指定，则默认加密算法为AES 128算法。
- MaxCompute PE需要通过adminconsole为Project打开存储加密开关并设定加密算法。同时，adminconsole后台会自动访问KMS服务，为用户生成加密所需的CMK。
- Project配置生效后，通过支持存储加密的Task生成或导入的Table数据，将会以加密的形式进行存储。
- 对于打开存储加密之前的用户数据，不会自动转化为非加密数据；如有此类需求，需以加密方式重写旧数据进行转换。

#### 特殊说明

- 存储加密生效后，数据加解密操作对用户完全透明，用户在使用过程中不需额外操作。
- 除了在功能概述中提到支持的Task类型，目前对于其他的Task类型，如OpenMR，可以正常使用，但暂不支持数据加密。
- Project存储加密功能生效后，用户可以通过KMS查询自己的密钥，但不支持对密钥和加密算法进行修改。
- 存储加密功能支持配置关闭。功能关闭后，新增数据不再以加密方式存储，已加密的数据依旧保持加密状态，直到数据被重写。在KMS服务正常情况下，原有加密数据可以正常读取。
- MaxCompute访问用户密钥时需要在ram签发sts token，因此要注意评估对ram的压力。

### 5.34.1.5 传输加密

MaxCompute提供Restful的传输接口，其传输安全性由HTTPS保证。

## 5.34.2 租户侧安全功能

### 5.34.2.1 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。

Package使用方法示例如下。

- Package创建者的操作示例如下。

```
create package <pkgname>
-- 创建Package
```



注意：

- 仅project的owner有权限进行该操作。
- 目前创建的package名称不能超过128个字符。

```
add project_object to package package_name [with privileges
privileges]
remove project_object from package package_name
project_object ::= table table_name |
instance inst_name |
function func_name |
resource res_name
privileges ::= action_item1, action_item2, ...
-- 添加资源到Package
```



说明：

- 目前支持的对象类型不包括Project类型，即不允许通过Package在其他Project中创建对象。
- 添加到Package中的不仅仅是对象本身，还包括相应的操作权限。当没有通过[with privileges privileges]来指定操作权限时，默认为只读权限，即Read/Describe/Select。“对象及其权限”被看作一个整体，添加后不可被更新。若有需要，只能删除和重新添加。

```
allow project <prjname> to install package <pkgname> [using label <
number>]
-- 赋予其它项目空间使用权限
```

```
disallow project <prjname> to install package <pkgname>
-- 撤销其它项目空间使用权限
```

```
delete package <pkgname>
```



```
-- 删除Package
```

```
show packages
-- 查看Package列表
```

```
describe package <pkgname>
-- 查看Package详细信息
```

- Package使用者的操作示例如下。

```
install package <pkgname>
-- 安装Package
```



说明:

- 仅project的owner有权限进行该操作。
- 对于安装Package来说, 要求pkgName的格式为: <projectName>.<packageName>。

```
uninstall package <pkgname>
-- 卸载Package
```



说明:

对于卸载Package来说, 要求pkgName的格式为: <projectName>.<packageName>。

```
show packages
-- 查看已创建和已安装的package列表
```

```
describe package <pkgname>
-- 查看package详细信息
```

被安装的Package是独立的MaxCompute对象类型, 若要访问Package里的资源(即其他项目空间分享给用户的资源), 必须拥有对该Package的Read权限。若请求者无Read权限, 则需向ProjectOwner或Admin申请, ProjectOwner或Admin可以通过ACL授权或Policy授权机制来完成授权。

示例如下, 仅供参考: 通过ACL授权允许云账号odps\_test@aliyun.com访问Package里的资源。

```
use prj2;
install package prj1.testpkg;
grant read on package prj1.testpackage to user
aliyun$odps_test@aliyun.com;
```

通过Policy授权允许项目空间prj2中任何用户都可以访问Package里的资源。

```
use prj2;
install package prj1.testpkg;
```

```
put policy /tmp/policy.txt;
```



#### 说明:

/tmp/policy.txt的内容如下。

```
{
  "Version": "1",
  "Statement":
  [{
    "Effect": "Allow",
    "Principal": "*",
    "Action": "odps:Read",
    "Resource": "acs:odps:*:projects/prj2/packages/prj1.testpkg"
  }]
}
```

### 5.34.2.2 数据保护机制（Project Protection）

同时在多个项目空间中拥有访问权限的用户，可以自由地使用任意支持跨Project的数据访问操作来转移项目空间的数据。但是，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，此时管理员可以使用项目空间保护机制——设置ProjectProtection，明确要求项目空间中“数据只能本地循环，允许写入，不能读出”。

具体设置如下：

```
set projectProtection=true
-- 设置ProjectProtection规则为：数据只能流入，不能流出。
```



#### 说明:

需要注意，默认ProjectProtection不会被设置，默认值为false，即数据保护机制按需开启。

开启数据保护机制后的数据流出方法

在用户的项目空间被设置了ProjectProtection之后，用户可能会遇到如下的需求：某人向用户提出申请，因正常的业务需求，需要将某张表的数据导出用户的项目空间。而且经过用户的审查之后，那张表也的确没有泄漏用户关心的敏感数据。此时，为了不影响正常的业务需求，MaxCompute为用户提供了在ProjectProtection被设置之后的两种数据导出途径。

设置ExceptionPolicy

ProjectOwner在设置ProjectProtection时可以附带一个exception策略，命令如下：

```
SET ProjectProtection=true WITH EXCEPTION <policyFile>
```



#### 说明:

此时的policy不同于Policy授权（尽管它与Policy授权语法完全一样），它只是对项目空间保护机制的例外情况的一种描述，即所有符合policy中所描述的访问情形都可以打破ProjectProtection规则。

Exception policy相关示例如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "ALIYUN$Alice@aliyun.com",
      "Action": ["odps:Select"],
      "Resource": "acs:odps:*:projects/alipay/tables/table_test",
      "Condition": {
        "StringEquals": {
          "odps:TaskType": ["DT", "SQL"]
        }
      }
    }
  ]
}
-- 允许云账号Alice@aliyun.com可以通过SQL任务对表alipay.table_test执行Select
操作时将数据流出到alipay项目空间之外。
```



说明：

- Exception policy并不是一种普通的授权。如果上述示例中，云账号Alice并没有对表alipay.table\_test的Select操作权限，那么即使设置了上述exception policy，Alice仍然是无法导出数据。
- ProjectProtection是一种数据流向的控制，而不是访问控制。只有在用户能访问数据的前提下，控制数据流向才是有意义的。

## 设置TrustedProject

若当前项目空间处于受保护状态，如果将数据流出的目标空间设置为当前空间的TrustedProject，那么向目标项目空间的数据流向将不会被视为触犯ProjectProtection规则。如果多个项目空间之间两两互相设置为TrustedProject，那么这些项目空间就形成了一个TrustedProject Group，数据可以在这个Project Group内流动，但禁止流出到Project Group之外。

管理TrustedProject的命令如下：

```
list trustedprojects;
-- 查看当前project中的所有TrustedProjects。
add trustedproject <projectname>;
-- 在当前project中添加一个TrustedProject。
remove trustedproject <projectname>;
```

-- 在当前project中移除一个TrustedProject。

#### 资源分享与数据保护的关系

在MaxCompute中，基于package的资源分享机制与ProjectProtection数据保护机制是正交的，但在功能上却是相互制约的。

MaxCompute规定：资源分享优先于数据保护。即如果一个数据对象是通过资源分享方式授予其他项目空间用户访问，那么该数据对象将不受ProjectProtection规则的限制。

#### 防止数据从项目空间流出的更多检查

如果要防止数据从项目空间的流出，在设置ProjectProtection=true之后，还需检查如下配置：

- 确保没有添加trustedproject。如果有设置，则需要评估可能的风险。
- 确保没有设置exception policy。如果有设置，则需要评估可能的风险，尤其要考虑TOC2TOU数据泄露风险。
- 确保没有使用package数据分享。如果有设置，则需要确保package中没有敏感数据。

### 5.34.2.3 日志审计

MaxCompute会针对不同用户不同日志数据进行日志审计。在MaxCompute内部，MaxCompute提供元数据仓库进行日志数据存储，包括静态数据、运行记录及安全信息等内容。

- 静态数据：是指一旦产生就不会自动消失的数据。
- 运行记录：表示一个任务的运行过程，该记录只会出现在一个分区中。
- 安全信息：都来自TableStore，用于保存白名单、ACL列表等。

元数据仓库：就是使用MaxCompute来分析MaxCompute自己的运行状况，将MaxCompute中的各种元信息整理汇总成MaxCompute中的表，方便用户查询和统计。

### 5.34.2.4 IP白名单

MaxCompute安全上的访问控制有多个层次：如项目空间的多租户及安全认证机制，只有获取了正确的经过授权的AccessKey ID及AccessKey Secret才能通过鉴权，在已经赋予的权限范围内进行数据访问和计算。本文主要介绍在以上访问认证基础上增强的一种以IP白名单的方式，进行访问控制的配置方法和策略，并指导用户完成相关配置。



说明：

• 获取需要配置的IP地址的方式如下：

1. 如果使用MaxCompute Console (odpscmd) 在集群内部使用（如ag上使用），可以直接获取机器的IP地址。
2. 如果使用应用系统（如base或者datax）进行项目空间数据访问，需要配置base或者datax所在的部署server机器的IP地址。
3. 如果使用了代理服务器或者经过了多跳代理服务器来访问MaxCompute服务实例，需要添加的IP地址为最后一跳代理服务器的IP地址。
4. 如果是ECS机器中访问MaxCompute服务，获取到的IP地址为NAT IP。

• IP地址配置的格式如下：

多个IP由“逗号”分割，且支持三种IP格式：1、单独IP地址。2、IP地址段，由“-”连接。3、带有子网掩码的IP。

示例如下：

```
10.32.180.8,10.32.180.9,10.32.180.10
-- 单独IP地址。
10.32.180.8-10.32.180.12
-- IP地址段。
10.32.180.0/23
-- 带子网掩码的IP地址。
```

下面将分别介绍project group级别IP白名单，project级别IP白名单以及系统级别IP白名单所涉及的相关配置操作。

#### Project group级别IP白名单配置

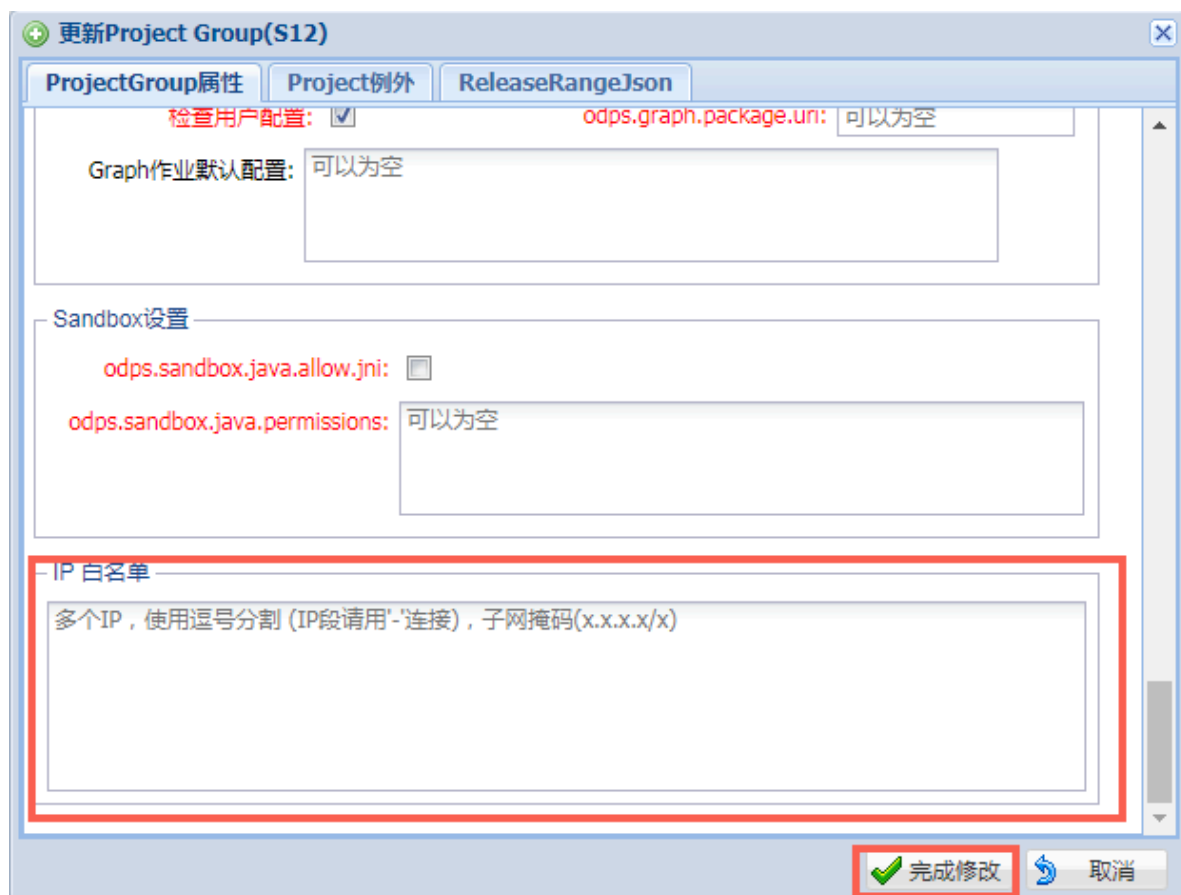
Project group级别进行白名单控制时，如果某一个project属于project group，那么在project group中配置白名单后，该project也受此配置限制。

具体的配置方式如下所示。

1. 在AdminConsole中选择ODPS配置 > Group管理，选中需要配置的group，双击打开配置框。

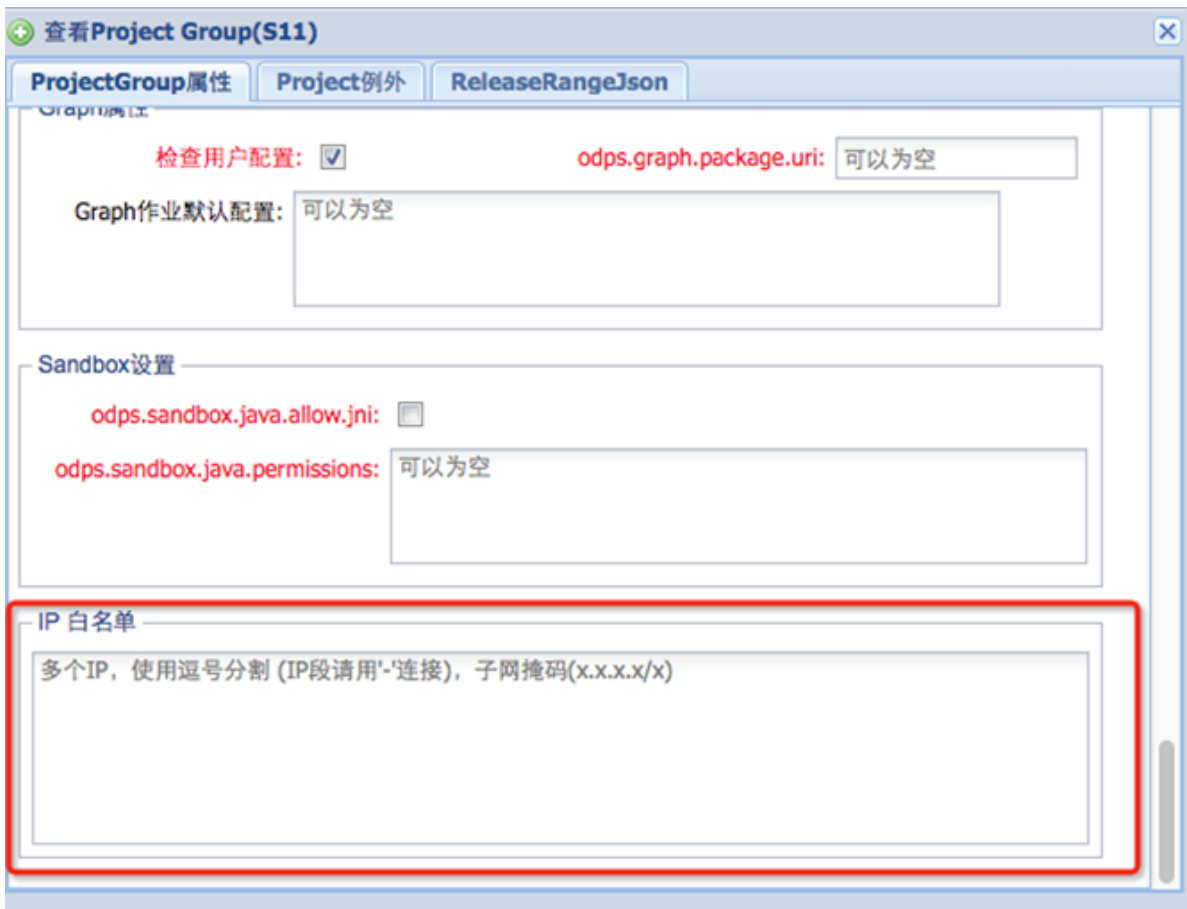
2. 在弹出的配置框中完成相关配置后，单击完成修改。

图 5-6: Project group级别IP白名单配置1



3. 配置完成后可以在project group属性配置中查看配置结果。

图 5-7: Project group级别IP白名单配置2



Project级别IP白名单配置

如果某一个project不在project group中时，则可以单独进行project级别白名单配置。

具体的配置方式如下所示。

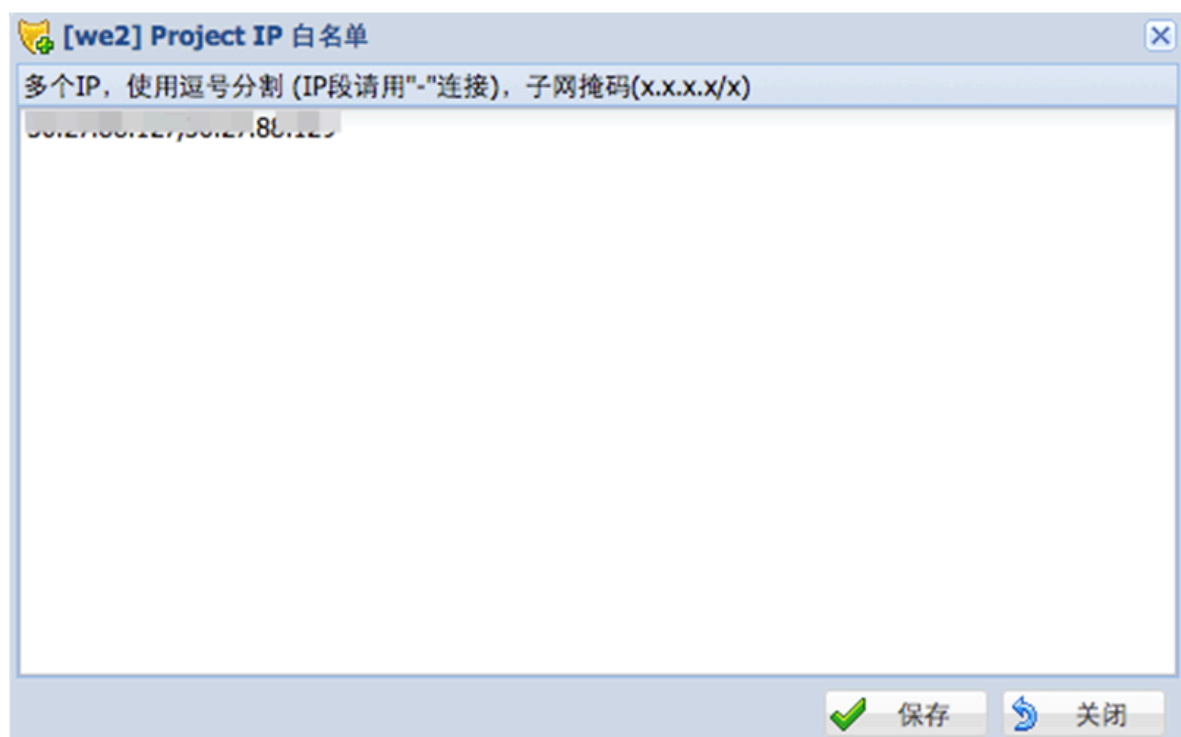
1. 在AdminConsole中选择ODPS配置 > Project管理，选中需要配置的project，单击最右侧的IP白名单设置图标。

图 5-8: Project级别IP白名单配置1

ipwss_01			2017-10-16 10:13:20	2017-10-16 10:17:20	
tpch_10g			2017-10-12 15:18:11	2017-10-12 15:18:11	
tpch_1t			2017-10-12 15:17:38	2017-10-12 15:17:38	
we2			2017-10-09 14:58:19	2017-10-30 16:14:55	
wenwertyuioasdfghjklzxcvbnmasd			2017-10-09 14:57:17	2017-10-09 14:57:17	
yyproject			2017-10-18 19:17:59	2017-10-30 16:12:44	

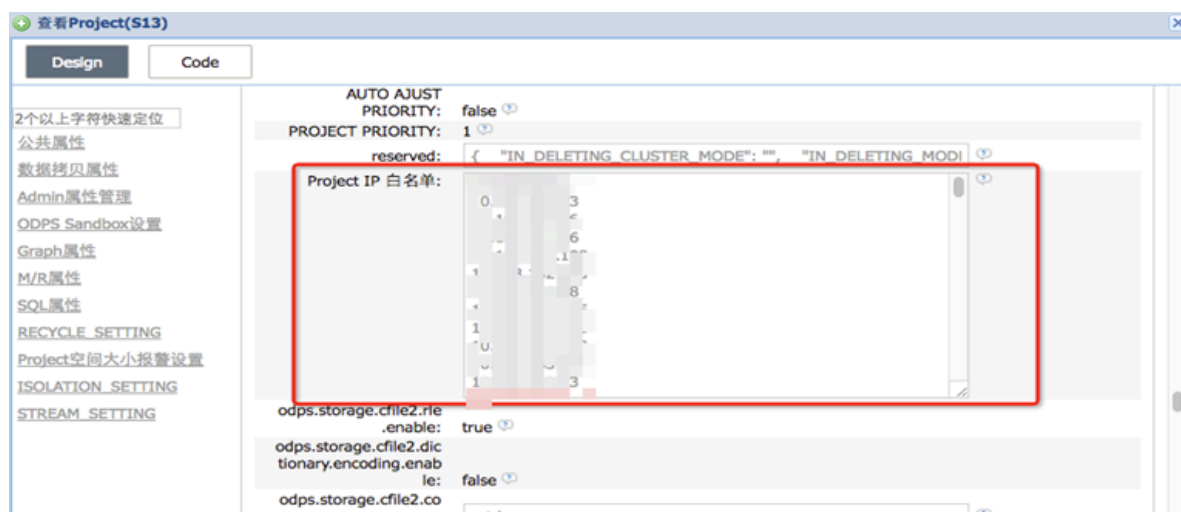
2. 在弹出的配置框中完成相关配置后，单击保存。

图 5-9: Project级别IP白名单配置2



3. 配置完成后可以到project属性配置中查看配置结果。

图 5-10: Project级别IP白名单配置3



说明:

ProjectOwner也可以使用SetProject命令设置project的属性，如：setproject odps.security.ip.whitelist=“IP列表以逗号分隔”。



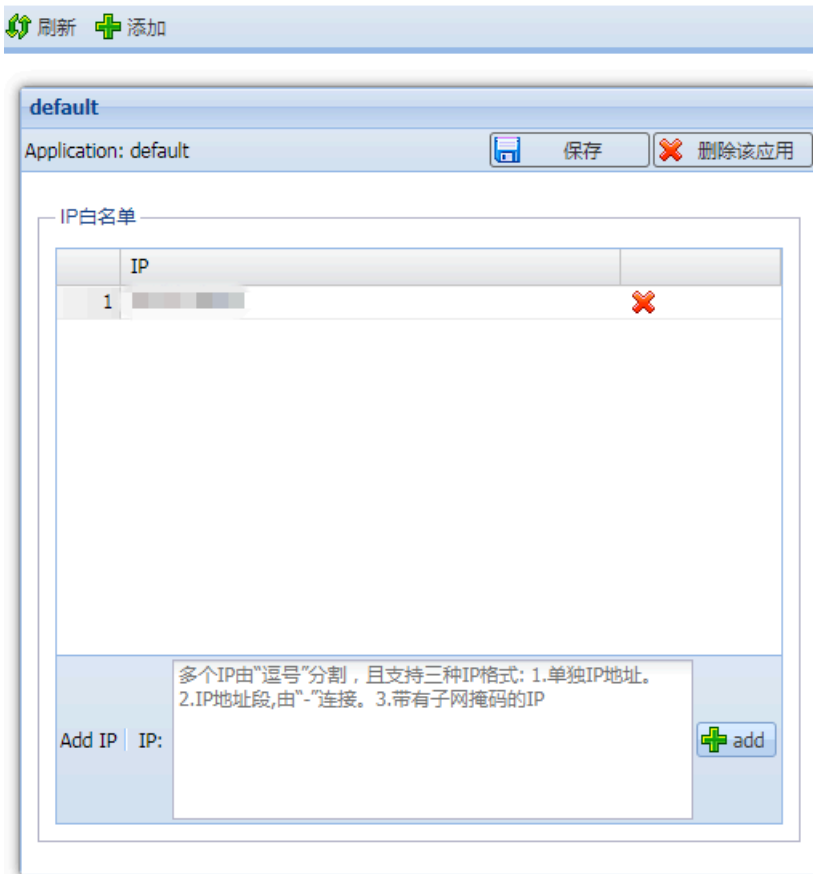
## 系统级别IP白名单配置

一些其他需要访问MaxCompute服务实例中所有project的其他上层业务系统（如Dataworks系统）IP发生变化的时候，如果没有全局性IP白名单配置，需要找到所有设置白名单的project列表一个个进行新IP的修改配置，非常容易出错。为此MaxCompute实现了系统级别IP白名单功能，系统级别IP白名单是MaxCompute实例服务级全局性配置。配置系统级别白名单是按照应用进行分类的。

具体的配置方式如下所示。

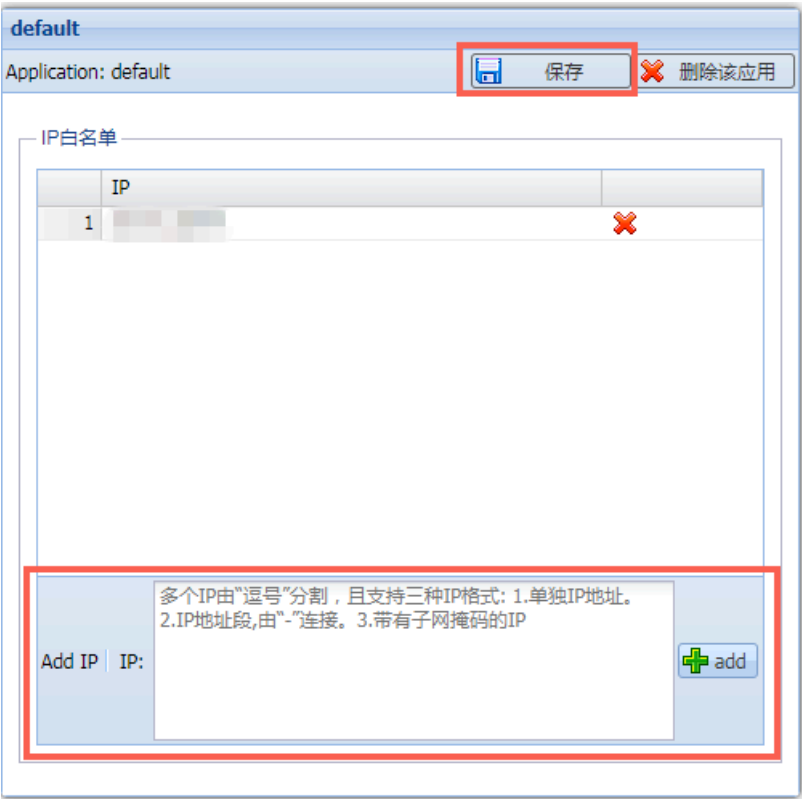
1. 在AdminConsole中选择ODPS配置 > 系统级白名单管理，默认打开配置框。

图 5-11: 系统级别IP白名单配置1



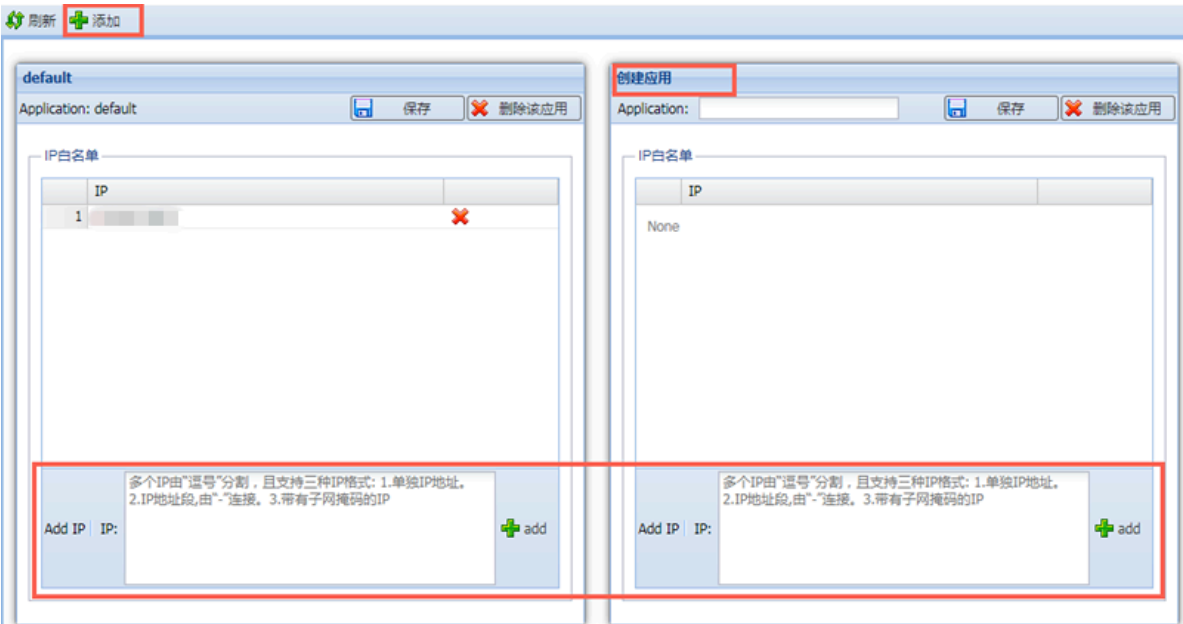
2. 在打开的配置框中完成相关配置后，单击保存。

图 5-12: 系统级别IP白名单配置2



3. 当前应用配置完成后，可以通过单击添加，继续配置新建应用的IP白名单。

图 5-13: 系统级别IP白名单配置3



## 相关注意事项

1. AdminConsole的专有云地址为：`http://{odps_ag}:9090`，即odps ag的9090端口。
2. 首次设置白名单时一定要注意需要设置正确的白名单且包含本机IP地址，否则设置生效后本机IP地址不在白名单列表也会被限制不能访问。一旦设置错了之后，需要系统管理员从管理系统如AdminConsole中进行配置更改。
3. 给project或者project group设置完白名单之后，白名单之外的IP地址将无法访问受影响project，一些公用系统（如base）如果也需要访问该project，则需要设置base所在机器IP地址到白名单列表中。
4. 出于信息安全的考虑，即使IP白名单允许访问，用户也可以通过policy限制服务，这是另外一个层次更细粒度的访问控制。
5. 如果通过代理服务器访问MaxCompute服务，需要添加到IP白名单的为最后一跳的代理服务器IP地址。

## 影响与效果

1. 配置之前MaxCompute服务针对访问项目空间的机器IP地址没有限制。
2. 配置之后，满足配置规则的IP地址及IP地址段才能访问该项目空间。在原有AccessKey ID及AccessKey Secret认证基础上叠加了IP规则的检查。
3. 一些公共系统，如Base、Datax、DPC系统原来需要访问到MaxCompute服务项目空间的，如果需要访问某一个项目空间，也需要找到这些服务部署机器的IP地址添加到IP白名单中。

## 5.35 数据工场DataWorks

### 5.35.1 开发/生产权限隔离

DataWorks支持以工作空间为单位管理代码与配置。工作空间分为标准模式和简单模式。

标准模式的工作空间可以隔离开发环境和生产环境。以MaxCompute引擎为例，标准模式的工作空间对应两个MaxCompute项目，分别为开发环境与生产环境，两种环境的数据完全隔离。

开发人员通过DataWorks数据开发页面，仅能操作开发环境数据。对于生产环境数据的变更，需要由运维人员执行发布操作后，方可实现。标准模式的工作空间可以严格控制表权限，禁止随意操作生产环境的表，保证生产表的数据安全。

简单模式的工作空间开发与生产环境合二为一，优势在于迭代快，代码提交后，无需发布即可生效，但无法保证开发/生产环境的权限隔离。

## 5.35.2 鉴权认证

### 5.35.2.1 访问控制

#### 登录控制

主账号在阿里云访问控制的控制台中，可以新建多个RAM子账号。通过授予对应的授权策略，使子账号在一定条件下可以访问DataWorks。包括IP地址/地址段、MFA多因素认证和HTTPS访问协议等。

通过限制能够访问DataWorks的来源IP或IP地址段，可以进一步防止非法访问，保障数据与业务安全。例如，当用户自身的访问密钥不慎丢失或被盗时，用户在更换新密钥之前，能够防止来自非法IP（例如非公司内网来源IP）的访问登录。

#### 沙箱隔离

工作空间是DataWorks用户数据隔离的基本单位，工作空间内的所有任务均运行在沙箱内，以保证数据不被泄露。同时也防止开发人员擅自操作外部资源，对公网环境造成危害。默认情况下，仅可访问：

- 数据开发任务仅可访问指定的计算引擎。
- 数据集成任务仅可访问已添加的数据源。

如果需要在工作空间中访问除以上两种情形之外的外部资源，需要由工作空间管理员进行沙箱白名单设置。

### 5.35.2.2 权限管理

#### 角色管理

DataWorks自带的权限托管策略中包括所有者、管理员、开发、运维、部署、访客和安全管理员7种角色。

角色	权限说明
所有者	工作空间的最高权限者，具有所有权限。
管理员	所有者委托的管理者，具有除删除工作空间之外的所有权限。
开发	开发环境的操作者，具有开发节点、业务流程并操作开发环境数据的权限。
运维	生产环境的操作者，可以对生产环境的任务节点进行中止、重跑等操作，同时具备部署权限。
部署	开发、生产环境的连接者，具有将开发环境的代码发布至生产环境的权限。

角色	权限说明
安全管理员	数据安全的管理者，具备操作数据保护伞配置的权限。
访客	具备最小权限，仅能查看代码，无法进行任何操作。

#### 权限管理

DataWorks支持对工作空间中的数据权限进行管理。支持表级、字段级授权，并支持权限的查看与审计。

#### 数据下载控制

DataWorks支持配置数据下载控制，可以降低用户数据外泄的风险，保障用户数据安全。

### 5.35.3 数据加密

DataWorks所有底层数据均为加密存储、传输，包括用户代码、业务流程配置、数据源连接等信息。只有合法并具备权限的用户，方可查看、使用和修改这些数据。

### 5.35.4 敏感数据保护

DataWorks为您提供数据识别、敏感数据发现、数据分类分级、脱敏、访问监控、风险发现预警与审计能力。

- 通过数据识别，可以按照预设的规则，自动识别工作空间中的敏感数据。
- 通过数据分级分类，可以对数据的密级进行定义，并分别进行访问控制。
- 通过数据脱敏，可以通过遮蔽、假名、哈希等方式，对敏感数据进行脱敏。
- 通过访问监控，可以对敏感数据的导出、访问进行监控。
- 通过风险发现，可以对特定场景下的敏感数据访问行为进行监控。

## 5.36 分析型数据库MySQL版

### 5.36.1 平台侧安全设计

#### 5.36.1.1 安全隔离

分析型数据库MySQL版以数据库作为租户隔离的基本单元，数据库创建者即为数据库的拥有者。未经数据库创建者授权，任何人无法访问该数据库的数据。用户数据库运行在自己独享的进程级别实例上，从进程级别实现数据库的隔离。

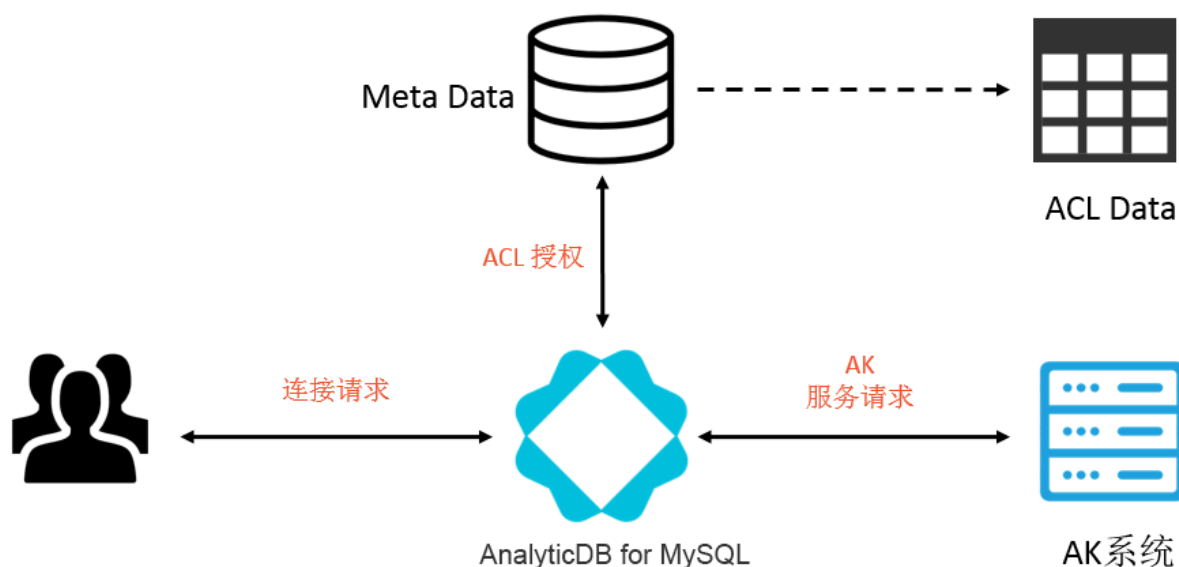
分析型数据库MySQL版中的每个数据库均采用多租户机制，每个数据库都有完全独立的服务进程。多租户机制对每个数据库的物理资源进行隔离（包括CPU、内存、存储空间），不允许跨数据库访问。

分析型数据库MySQL版可以按数据库进行版本管理、资源扩容/缩容、启动/停止数据库服务。

每个数据库都有独立的AccessKey。

### 5.36.1.2 鉴权认证

分析型数据库MySQL版的身份验证和权限控制流程如下图所示。



#### 身份认证

分析型数据库MySQL版提供基于MySQL协议身份认证体系，支持类似MySQL的用户名/密码的身份认证机制。

作为阿里云产品栈产品，分析型数据库MySQL版使用阿里云AK（AccessKey）系统和机制实现身份认证。用户通过注册AK账户连接分析型数据库MySQL版，也可以使用AK通过JDBC/ODBC连接分析型数据库MySQL版。

用户可以在Apsara Stack控制台中自行创建AK。AK由AccessKeyId和AccessKeySecret组成，其中AccessKeyId是公开的，用于标识用户身份（相当于用户名）；AccessKeySecret是私密的，用于鉴别用户身份（相当于密码）。

主账号和子账号均使用对应的AccessKeyId和AccessKeySecret访问分析型数据库MySQL版数据库。

## 权限控制

分析型数据库MySQL版支持基于数据库表的层级权限管理模型，提供类似MySQL的访问控制列表ACL（Access Control List）授权模式。与MySQL不同的是，分析型数据库MySQL版不支持针对用户在HOST上的授权。

一个ACL授权由被授权用户、授权对象和操作权限组成。ACL数据存储在分析型数据库MySQL版的元数据系统中，元数据系统使用RDS持久化存储，同时元数据通过分析型数据库MySQL版的缓存来加速DML/DDDL语句授权。

连接分析型数据库MySQL版后，分析型数据库MySQL版通过ACL的元数据控制用户对数据库对象的操作权限，例如，用户对Table（表）、Column（列）等的SELECT、INSERT、DELETE、CREATE、SHOW、DROP、ALTER、DESCRIBE、LOAD DATA、DUMP DATA操作权限。

分析型数据库MySQL版中的授权对象如下所示。

- DataBase（库）：即db\_name.\* 或 \*（默认数据库），指定数据库或数据库上的所有表/表组。
- TableGroup（表组）：即db\_name.table\_group\_name或table\_group\_name，指定表组。
- Table（表）：即db\_name.table\_name或table\_name，指定表。
- Column（列）：语法上由column\_list和Table组成，指定表的列。

## 访问控制

分析型数据库MySQL版支持RAM（Resource Access Management）鉴权，不支持STS（Security Token Service）鉴权。

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

### 5.36.1.3 数据安全

#### 多租户

分析型数据库MySQL版提供多租户机制，不同数据库之间通过CPU、内存、磁盘空间、网络带宽资源的完全隔离实现数据的隔离。

#### 数据可靠性

分析型数据库MySQL版的全量数据存储在飞天分布式文件系统中，支持采用三副本或纠删码EC（Erasure Code）方式存储，保证数据持久化的高可靠性。实时表数据的DML（INSERT/DELETE）操作提交成功后，数据同步存储到飞天分布式文件系统中；加载批量表数据时，数据也将全量写入飞天分布式文件系统。

## 数据一致性

更新（INSERT/DELETE）实时表数据时，分析型数据库MySQL版采用多版本并发控制MVCC（Multi-Version Concurrency Control）机制存储数据，保证有并发数据更新操作时，查询返回的数据即为发起查询时的数据版本。



说明：

可定期清理不再需要的历史版本数据。

### 5.36.1.4 VPC支持

分析型数据库MySQL版支持专有网络VPC（Virtual Private Cloud）功能，默认使用Single Tunnel方式，也可以通过配置切换为Any Tunnel方式。

专有网络VPC帮助您基于阿里云构建一个隔离的网络环境。您可以完全掌控自己的虚拟网络，选择自有IP地址范围、配置路由表和网关等。也可以通过专线、VPN等连接方式将VPC与传统数据中心组成按需定制的网络环境，实现应用的平滑迁移上云。

- Single Tunnel模式：默认VPC方式，仅支持在指定的VPC环境中访问并使用分析型数据库MySQL版。Single Tunnel模式可以实现不同VPC之间的网络隔离。
- Any Tunnel模式：通过修改配置，可从Single Tunnel模式切换到Any Tunnel模式。配置修改后在下一次创建数据库时生效，您也可通过修改元数据并重启FrontNode使配置修改生效。Any Tunnel模式下，您可以在任意的VPC环境中访问并使用分析型数据库MySQL版。



说明：

Any Tunnel模式无法实现VPC之间的网络隔离。

## 5.36.2 租户侧安全功能

### 5.36.2.1 日志审计

分析型数据库MySQL版支持审计日志功能，审计日志可以记录所有SQL操作信息，包括：

- 查询发生时间；
- 客户端IP地址；
- 所执行的SQL语句。

您可以通过SQL语句查询客户历史数据信息。

审计日志格式示例如下：

```
[2017-10-10 13:37:57,351] INFO [pool-31-thread-22] c.a.c.a.f.l.  
AccessLog.info - Client=127.0.0.1 Total_time=1044 Exec_time=1043
```



```
Queue_time=1 - [2017-10-10 13:37:56 308] 1 SQL Statement \;process=
2017101013375601000316310809999838042\;CLUSTER=ayads-bjyz
```

## 5.37 实时计算Realtime Compute

### 5.37.1 平台侧安全设计

实时计算对不同的项目进行了严格的项目权限区分，不同用户/项目之间是无法进行访问、操作，包括项目下属的所有子产品实体均无法操作。

项目级别的资源隔离能够保证不同用户的资源使用情况相互之间不相互干扰影响，例如一个用户任务在运行期间随着数据量的突增提升了其作业CPU使用。阿里云实时计算在底层使用虚拟化技术进行资源隔离，保证该用户的作业CPU使用率增加不会影响到其他用户作业的CPU使用情况。

#### 5.37.1.1 安全隔离

实时计算对不同的项目进行了严格的项目权限区分，不同用户/项目之间是无法进行访问、操作，包括项目下属的所有子产品实体均无法操作。

项目级别的资源隔离能够保证不同用户的资源使用情况相互之间不相互干扰影响，例如一个用户任务在运行期间随着数据量的突增提升了其作业CPU使用。阿里云实时计算在底层使用虚拟化技术进行资源隔离，保证该用户的作业CPU使用率增加不会影响到其他用户作业的CPU使用情况。

#### 5.37.1.2 鉴权认证

##### 实时计算账号

阿里云实时计算账号当前支持且仅支持阿里云账号体系（包括登录用户名+密码、签名密钥），这部分全部遵守阿里云现有安全体系，同时传输链路全部使用HTTPS协议，保证全链路的用户账户安全。

##### 数据存储账号

实时计算涉及到保存数据存储连接账号问题，我们提供基于RAM/STS方式，避免您因为账户信息丢失导致业务信息泄露。

#### 5.37.1.3 数据安全

数据安全分为实时计算系统数据安全和业务数据安全。

##### 系统数据安全

阿里云实时计算系统数据安全交由系统本身安全保证，实时计算为系统安全做了诸多工作。

- 访问链路全部HTTPS化，保证传输链路的安全。
- 数据存储连接信息使用AES高强度加密方式，保证敏感信息不泄露。

- 全面且深入的攻击测试，阿里云安全团队为实时计算保驾护航。

#### 业务数据安全

实时计算本身不负责存储用户的业务数据，具体业务数据安全交由不同的阿里云存储系统保证，详情请参见不同的数据存储的安全模型以及最佳安全实践。

### 5.37.1.4 业务流程

#### 业务流程安全

实时计算对于流式计算开发进行了严格的流程定义，区分了数据开发和数据运维，在尽可能不影响您的使用体验基础上，保证了整体业务流程的完整和安全性。

- 提供代码版本

支持代码版本回滚和对比，方便您对代码进行追溯、比对、排错。

- 提供IDE单机调试容器

避免代码线下运行影响线上真实数据。您可以对输入表、维表、输出表自行构造数据，以避免线下任务调试对于线上生产任务影响。

- 提供发布流程

避免线下代码改动直接影响生产运行。调试完成后，通过上线任务将作业提交到数据运维系统。此时正在运行的实时计算任务并不直接使用新代码运行，而需要您经过人工确认后将运行任务停止并使用新代码启动，从流程上保证发布的严谨性。

## 5.38 E-MapReduce

### 5.38.1 平台侧安全设计

#### 5.38.1.1 安全隔离

E-MapReduce 支持使用 RAM 来隔离不同子账号的数据权限。通过创建不同的授权策略，然后将策略赋给子账号，可以控制不同用户的数据访问范围。用户应使用对应的子账号登录 E-MapReduce控制台。对于存放在OSS中的数据，E-MapReduce 在读取时有如下限制：

- 涉及OSS的选择界面，可以看到所有的 bucket，但是只能进入被授权的 bucket。
- 只能看到被授权的 bucket 下的内容，无法看到其他 bucket 内的内容。
- 作业中只能读写被授权的 bucket，读写未被授权的 bucket 会报错。

### 5.38.1.2 鉴权认证

E-MapReduce支持Kerberos认证，即集群中的开源组件以Kerberos的安全模式启动，在这种安全环境下只有经过认证的客户端(Client)才能访问集群的服务(Service，如HDFS)。

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。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。

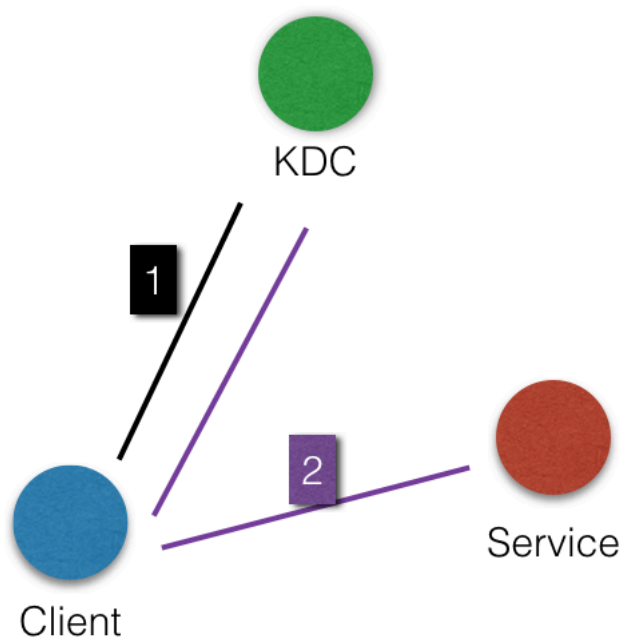
所有组件都可以使用HAS提供的原有Kerberos的认证机制。

Kerberos身份认证原理

Kerberos是一种基于对称密钥技术的身份认证协议，它作为一个独立的第三方的身份认证服务，可以为其它服务提供身份认证功能，且支持SSO(即客户端身份认证后，可以访问多个服务如HBase/HDFS等)。

Kerberos协议过程主要有两个阶段，第一个阶段是KDC对Client身份认证，第二个阶段是Service对Client身份认证。

图 5-14: Kerberos认证原理



- KDC: Kerberos的服务端程序。

- **Client**: 需要访问服务的用户(principal), KDC和Service会对用户的身份进行认证。
- **Service**: 集成了Kerberos的服务, 如HDFS/YARN/HBase等。

### KDC对Client身份认证

当客户端用户(principal)访问一个集成了Kerberos的服务之前, 需要先通过KDC的身份认证。若身份认证通过则客户端会拿到一个TGT(Ticket Granting Ticket), 后续就可以拿该TGT去访问集成了Kerberos的服务。

### Service对Client身份认证

用户拿到TGT后, 就可以继续访问Service服务。它会使用TGT以及需要访问的服务名称(如HDFS)去KDC获取SGT(Service Granting Ticket), 然后使用SGT去访问Service, Service会利用相关信息对Client进行身份认证, 认证通过后就可以正常访问Service服务。

## 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, 权限控制仍然有效。

### · HDFS授权

HDFS开启了权限控制后, 用户访问HDFS需要有合法的权限才能正常操作HDFS, 如读取数据/创建文件夹等。

### · YARN授权

YARN的授权根据授权实体, 可以分为服务级别的授权、队列级别的授权。

#### #服务级别的授权

- 控制特定用户访问集群服务, 如提交作业
- 配置在hadoop-policy.xml
- 服务级别的权限校验在其他权限校验之前(如HDFS的permission检查/yarn提交作业到队列控制)

#### #队列级别的授权

- YARN可以通过队列对资源进行授权管理, 有两种队列调度CapacityScheduler和FairScheduler。

### · Hive授权

Hive内置如下两种授权机制, 两种授权机制可以同时配置, 不冲突。

- 基于底层HDFS的权限(StorageBasedAuthorization)
- 基于标准SQL的grant等命令(SQLStandardsBasedAuthorization)

- HBase授权

HBase在不开启授权的情况下，任何账号对HBase集群可以进行任何操作，比如disabletable/droptable/majorcompact等等。对于没有Kerberos认证的集群，即使开启了HBase授权，用户也可以伪造身份访问集群服务。因此建议创建高安全模式(即支持Kerberos)的集群。

- Kafka授权

如果没有开启Kafka认证(如Kerberos认证或者简单的用户名密码)，即使开启了Kafka授权，用户也可以伪造身份访问服务。因此建议创建高安全模式(即支持Kerberos)的Kafka集群。

- Ranger

ApacheRanger提供集中式的权限管理框架，可以对Hadoop生态中的HDFS/Hive/YARN/Kafka/Storm/Solr等组件进行细粒度的权限访问控制，并且提供了UI方便管理员进行操作。

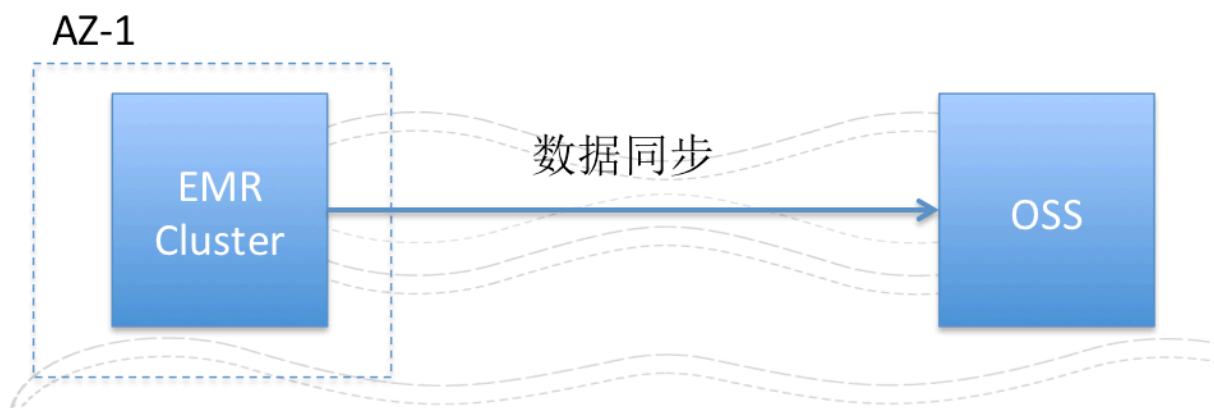
### 5.38.1.3 数据安全

Hadoop分布式文件系统（HDFS）将每一个文件的数据进行分块存储，同时每一个数据块又保存有多个副本（系统默认为每一个数据块存放3个副本），尽量保证这些数据块副本分布在不同的机架之上（在大多数情况下，副本系数是3，HDFS的存放策略是将一个副本存放在本地机架节点上，一个副本存放在同一个机架的另一个节点上，最后一个副本放在不同机架的节点上）。

HDFS会定期扫描数据副本，若发现数据副本发生丢失，则会快速的进行数据的复制以保证副本的数量。若发现节点丢失，则节点上的所有数据也会快速的进行复制恢复。在阿里云上，如果是使用云盘的技术，则在后台每一个云盘都会对应三个数据副本，当其中的任何一个出现问题时，副本数据都会自动被复制，以保证数据的可靠性。

Hadoop HDFS是一个经历了长时间考验且具有高可靠性的数据存储系统，已经能够实现海量数据的高可靠性存储。同时基于云上的特性，也可以在OSS等服务上进行数据的额外备份，来达到更高的数据可靠性。

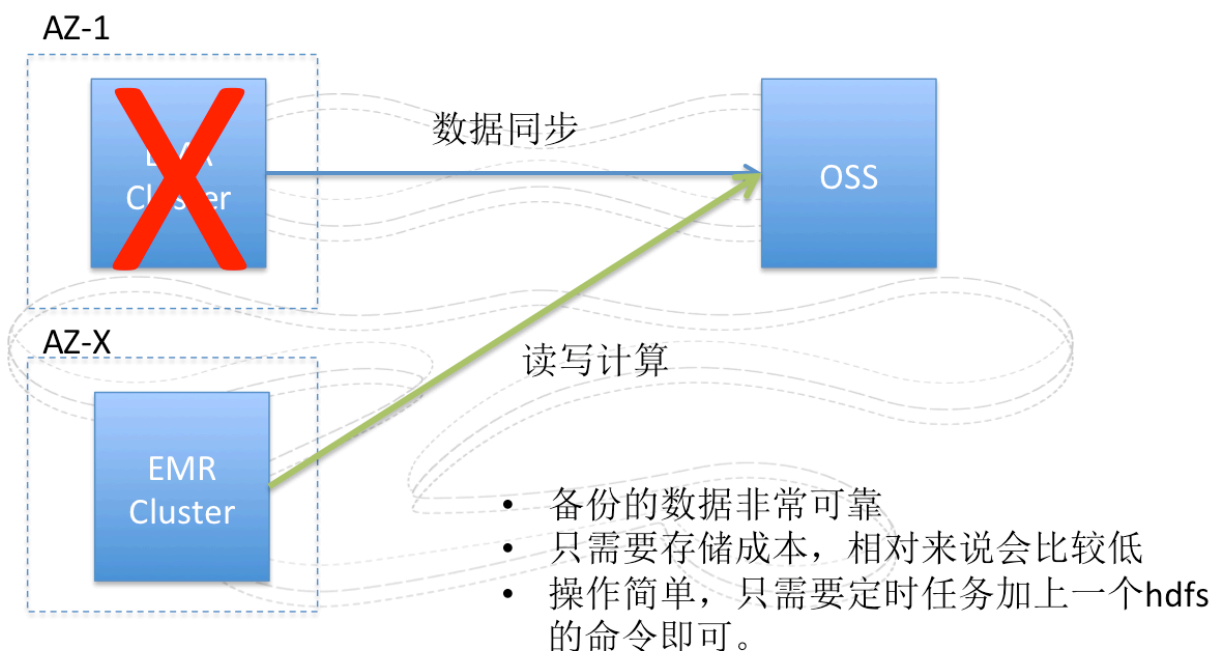
图 5-15: 数据同步



通过EMR的定时任务或者其他的定时任务，定时的同步数据到OSS上。

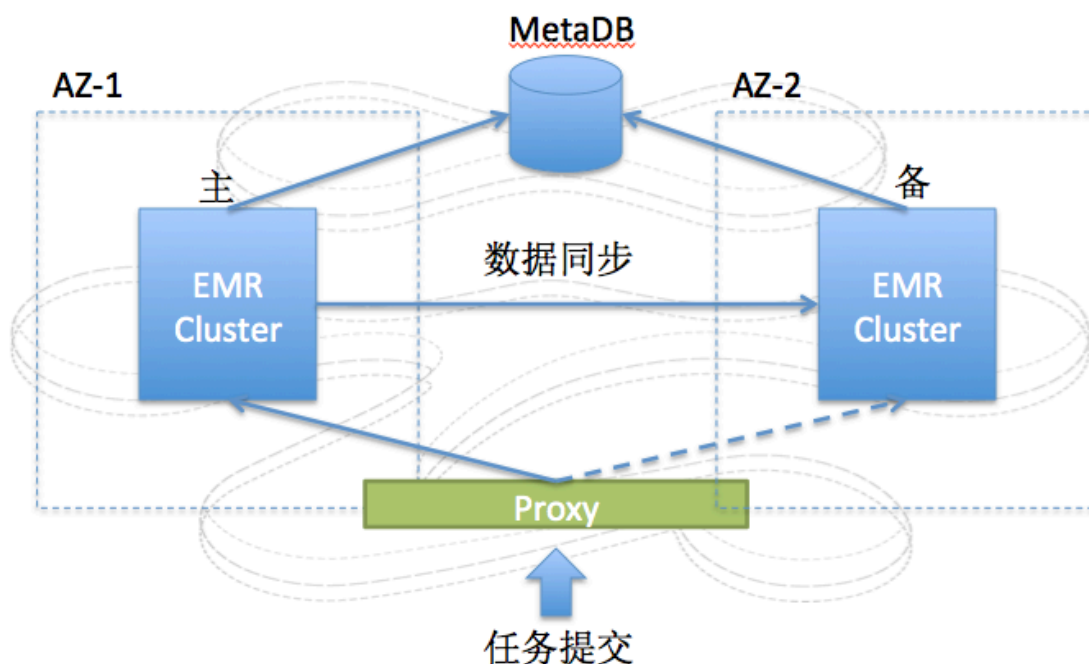
同步的时间间隔决定了数据的丢失的可容忍时间范围。比如每一个小时同步一次，那么丢失的数据的范围就是一个小时内的数据。如果30分钟同步一次，那么丢失的数据范围就是30分钟。

图 5-16: 数据备份



当集群发生问题的时候，直接新建一个集群，并读写OSS上的数据进行处理，如果原集群中还存在元数据的信息，元数据也需要进行重建，以保证服务。当原集群恢复以后，可以直接从OSS上将变化的数据同步回原集群。

图 5-17: 服务容灾



采用双集群的方式，在不同的AZ上创建完全相同的2个集群（计算能力，存储能力都相同），2个集群使用同一个meta数据库，这个meta数据也要使用类似RDS的三节点这样的容灾数据库。集群间通过数据同步保证主集群的数据能近实时的同步到备集群。同步的方式可以采用定时的DistCp的方式，但是数据的容灾时效性可能不高。另一种方案是提供一个对主集群的数据的监控的方式，一旦变化就是实时的同步增量数据到备集群，可以做到近乎秒级别的数据同步。

前端有一个proxy，用户通过proxy提交作业，而且用户不用感知到底提交到的是哪个集群，默认是提交到主集群，当主集群不可访问的时候，会自动切换到备集群。

需要注意的是，如果有外部的数据的写入，那么在主集群发生故障切换的时候，所有的外部的数据写入也都要切换到备集群上去，所以外部的数据源也是要容灾的。

### 5.38.2 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，权限控制仍然有效。

- HDFS授权

HDFS开启了权限控制后，用户访问HDFS需要有合法的权限才能正常操作HDFS，如读取数据/创建文件夹等。

- YARN授权

YARN的授权根据授权实体，可以分为服务级别的授权、队列级别的授权。

- 服务级别的授权

- 控制特定用户访问集群服务，如提交作业

- 配置在hadoop-policy.xml

- 服务级别的权限校验在其他权限校验之前(如HDFS的permission检查/yarn提交作业到队列控制)

- 队列级别的授权

YARN可以通过队列对资源进行授权管理，有两种队列调度 Capacity Scheduler和Fair Scheduler。

- Hive授权

Hive内置如下两种授权机制，两种授权机制可以同时配置，不冲突。

- 基于底层HDFS的权限(Storage Based Authorization)

- 基于标准SQL的grant等命令( SQL Standards Based Authorization)

- HBase授权

HBase在不开启授权的情况下，任何账号对HBase集群可以进行任何操作，比如disable table/drop table/major compact等等。对于没有Kerberos认证的集群，即使开启了HBase授权，用户也可以伪造身份访问集群服务。因此建议创建高安全模式(即支持Kerberos)的集群。

- Kafka授权

如果没有开启Kafka认证(如Kerberos认证或者简单的用户名密码)，即使开启了Kafka授权，用户也可以伪造身份访问服务。因此建议创建高安全模式(即支持Kerberos)的Kafka集群。

- Ranger

Apache Ranger提供集中式的权限管理框架，可以对Hadoop生态中的HDFS/Hive/YARN/Kafka/Storm/Solr等组件进行细粒度的权限访问控制，并且提供了UI方便管理员进行操作。



## 5.39 关系网络分析Graph Analytics

### 5.39.1 平台侧安全设计

#### 5.39.1.1 安全隔离

Graph Analytics 针对用户的数据，进行了租户级的隔离，即不同租户相互之间不能查询到数据。租户只能获取自己租户下的元数据配置，而不同的元数据对应不同的业务数据，所以同一租户只能查询到自己元数据对应的业务数据。

#### 5.39.1.2 鉴权认证

身份认证

Graph Analytics 关系网络分析目前在专有云支持两种身份验证：

- Graph Analytics 自己的身份验证：通过 Graph Analytics 用户系统创建的用户密码登录，Graph Analytics 用户系统的密码经过 MD5 加密，并且在网络传输上也经过加密，有效防止了密码泄露的情况。
- 对接的外部系统身份验证：对接客户的用户系统，该种方式的用户安全由外部系统承担。

权限控制

Graph Analytics 关系网络分析产品，所有功能都有权限控制，可以根据不同的用户权限对产品功能模块、数据行列进行管控。

#### 5.39.1.3 数据安全

Graph Analytics 关系网络分析采用分布式集群部署，管理节点和计算节点分离，能有效防止系统的单点故障，并且集群之间采用分布式缓存同步，有效防止了系统在故障转移时出现的数据丢失。

#### 5.39.1.4 传输加密

Graph Analytics 关系网络分析产品以HTTPS协议提供web服务。HTTPS协议是一种安全可靠的数据传输协议，能有效防止数据在网络中传输带来的安全问题。

#### 5.39.1.5 系统安全

##### 5.39.1.5.1 漏洞扫描机制

Graph Analytics 关系网络分析产品在发布前，已经经过专有云安全漏洞扫描，并且通过安全扫描，扫描内容包括：

- 系统安全扫描：Graph Analytics 关系网络分析产品发布的操作系统的安全扫描。

- 中间件依赖扫描：Graph Analytics 关系网络分析产品使用到的中间件。
- 代码漏洞扫描：Graph Analytics 关系网络分析产品自己的代码，以及依赖的第三方开源框架。

### 5.39.1.5.2 安全漏洞更新修复方案

根据阿里云安全部分、专有云安全测试、以及其他途径获取的安全漏洞，Graph Analytics 产品研发团队将根据安全漏洞的影响程度，进行紧急版本更新或者版本迭代更新，而且无论哪种更新都会保障更新流程符合阿里云安全生产管理规范。

### 5.39.1.5.3 系统防御机制

Graph Analytics 关系网络分析产品是基于阿里云专有云环境发布的，Graph Analytics 关系网络分析产品的系统防御机制依赖于阿里云专有云系统的防御机制。

### 5.39.1.6 基础设施安全

Graph Analytics 关系网络分析产品是基于阿里云专有云环境发布的，基础设施的安全有阿里云专有云基础设施安全保障，可参见阿里云安全白皮书基础设施安全。

### 5.39.1.7 等保认证

Graph Analytics 关系网络分析产品已经对接了专有云V3.3的安全等保4级。从阿里云专有云天基环境获的安全证书包括：cacert.pem、privatecloud.pem、privatecloud\_key.pem、privkey.pem。

Graph Analytics 关系网络分析在专有云V3.3版本以后通过https协议访问。

## 5.39.2 租户侧安全功能

### 5.39.2.1 日志审计

Graph Analytics 关系网络分析产品中所有的用户请求均记录日志，作为审计或者特定行为分析使用。日志中包含用户名、IP、操作内容、操作状态等信息。

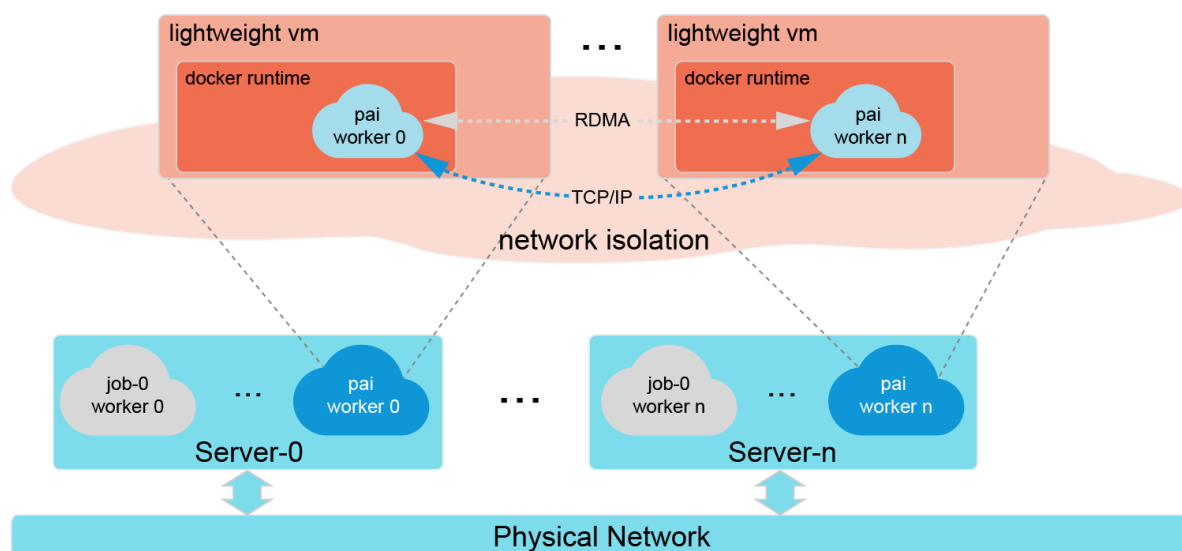
## 5.40 机器学习

### 5.40.1 安全隔离

租户隔离

基于多租户技术（Multi-Tenancy Technology），多个用户共同使用相同的阿里云机器学习应用服务时，仍可以确保各个用户之间对于计算资源和存储资源的隔离性、安全性。

- 网络虚拟化在租户隔离中起到了至关重要的作用。基于在物理网络的上层创建的虚拟网络，阿里云机器学习平台保障用户在执行算法任务时调用的计算资源时与其他用户实现隔离，使得独立的作业各自管理自己在分布式集群上的计算资源和存储资源。下图展示了用户提交的深度学习分布式作业执行时，系统框架在GPU 和 docker 实例之间采用了 PCIe 技术，在安全隔离的前提下同时保障 GPU 的计算性能。



- 用户开通阿里云机器学习产品时，同时会开通 DataWorks 产品，DataWorks 平台会通过统一的资源管理服务，为用户创建专属的网关（Gateway）资源组，用于安全地运行用户的 SQL、MapReduce 等类型的任务，避免用户之间的相互影响。

#### 在线预测服务安全隔离

在线预测服务将服务的部署人 AccessKey 记录于 RDS 中，对于每一次控制请求都会进行一次验证，如果鉴权失败则拒绝该请求。资源方面，在线预测服务使用容器技术隔离资源，租户使用的资源包括内存、CPU 受到限制，不会影响同机部署的其他业务。

## 5.40.2 鉴权认证

### 5.40.2.1 身份验证

#### 阿里云机器学习平台身份验证

用户通过浏览器访问机器学习应用时，校验流程如下：

1. 用户浏览器的请求都会经过 LoginFilter，LoginFilter 调用 DataWorks 的 sso 模块的接口进行身份校验。如果用户未登录，则会跳转到阿里云登录页，登录成功后会写入用户相关 cookie。
2. 所有的请求中会带上 ctoken 参数，防止 CSRF 攻击。
3. 所有的请求中，任何对资源进行增删改查的操作，都会对资源的权限进行校验，防止越权攻击。

4. DataWorks 调度等第三方模块调用机器学习服务接口时，所有的请求中都会使用 DataWorks 的 Token Center 进行权限校验。

#### 在线预测服务身份验证

用户可以在云控制台中自行创建 AccessKey。AccessKey 由 AccessKeyId 和 AccessKeySecret 组成，其中 AccessKeyId 是公开的，用于标识用户身份，AccessKeySecret 是秘密的，用于用户身份的鉴别。

当用户向在线预测服务发送请求时，在线预测服务会按照以下步骤对用户进行身份验证。

1. 将发送的请求按照在线预测服务指定的格式生成签名字符串。
2. 使用 AccessKeySecret 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。
3. 在线预测服务收到请求以后，通过 AccessKeyId 找到对应的 AccessKeySecret，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：认为该请求是有效的。
  - 如果计算出来的验证码和提供的不一致：在线预测服务将拒绝处理这次请求，并返回 HTTP 403 错误。

### 5.40.2.2 权限控制

用户的机器学习应用通过在线预测服务部署完成后，系统会生成预测接口访问 token，用户只有使用该 token 才可访问已经部署的应用。该 token 是私密的，服务创建者应该确保 token 由真正的使用者保留。

### 5.40.2.3 RAM 和 STS 支持

RAM (Resource Access Management) 是阿里云提供的资源访问控制服务。通过 RAM，您可以避免和其他用户共享云账号密钥，并且根据最小权限原则为不同用户分配最小的工作权限。RAM 使同一个阿里云账户（主账号）创建子账号，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予账号。

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。

用户在使用深度学习模块的过程中，可以使用 DTCenter 控制台提供的 OSS 快捷授权页面进行一键授权：

1. OSS 一键授权会将用户所在项目的 OSS bucket 的读写权限授权给 MaxCompute 的服务账号 odps.aliyuncs.com。

2. 授权完成后，会在 RAM 中创建一个名为 AliyunODPSPAIDefaultRole 的角色，每个角色都会有一个唯一的全局资源描述符，叫 RoleArn，格式为 `acs:ram::${accountID}:role/${roleName}`。
3. 角色创建成功后，机器学习服务能够使用 `odps.aliyuncs.com` 服务账号的 AK 请求 STS 的 AssumeRole 接口。
4. 请求成功后会获取到临时 AK (AccessKeyId、AccessKeySecret) 以及 STS token (SecurityToken)。默认有效期是3600s，通过临时 AK 和 STS token 可以读写指定项目的 OSS。

AliyunODPSPAIDefaultRole 角色信息如下：

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "odps.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

角色的授权策略如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "oss:GetObject",
        "oss:ListObjects",
        "oss:DeleteObject",
        "oss:ListParts",
        "oss:PutObject",
        "oss:AbortMultipartUpload"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

```
}
```

### 5.40.3 数据安全

#### 阿里云机器学习应用数据安全

阿里云机器学习使用大数据计算服务（MaxCompute）实现对大数据的计算和存储过程。通过 MaxCompute 的项目空间（Project）隔离用户数据，不同用户之间的数据存在于不同的项目空间中，互不可见。

对于数据安全性要求高的应用场景，例如金融机构等，MaxCompute 还提供了一种机制，即通过开启或关闭项目空间的数据保护机制，禁止或允许数据流出项目空间。具体可参考：[设置项目保护模式](#)。

#### 在线预测服务数据安全

在线预测服务的数据主要有三类：

- 在线预测服务元数据：在线预测服务元数据托管于 RDS 服务，由 RDS 确保数据安全。
- Kubernetes (k8s) 元数据：Kubernetes 元数据保存于 etcd 中，提供服务及数据三备份。访问 etcd 需要有特定的证书文件，需要由 k8s 集群管理员保管。
- 监控数据：监控数据保存于阿里云云盘，数据备份类型由实际使用的云盘类型保证。

### 5.40.4 日志审计

阿里云机器学习平台自动保存了用户访问的日志记录，以用户访问的次数为准，按照固定的格式，写入到固定的文件中，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、请求方式、请求接口、请求用户id、处理时长、错误码等内容。

## 5.41 实时数据分发平台DataHub

### 5.41.1 平台侧安全设计

#### 5.41.1.1 安全隔离

DataHub认证方式采用AccessKey对称密钥认证技术，同时对于用户的每一个HTTP请求都会进行签名认证，针对不同的用户数据进行数据存储隔离，用户数据被离散存储在分布式文件系统中。

同时，在服务内部，DataHub会对用户数据和数据索引进行分离存储，保证用户数据和系统数据隔离。

### 5.41.1.2 鉴权认证

#### 身份验证

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

当用户向DataHub发送请求时，首先需要将发送的请求按照DataHub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以生成请求签名。DataHub收到用户请求后，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，DataHub将拒绝处理这次请求，并返回HTTP 403错误。

#### 权限控制

用户对DataHub资源访问分为两种，即用户主账号访问和用户子账号访问。主账号是阿里云的一个账号主体，主账号下可以包含不同的子账号以使用户可以灵活使用。DataHub支持主子账号的权限访问策略。

- 当用户使用主账号访问时，DataHub会校验该主账号是否为对应资源的所有者，只有对应资源的所有者才具备访问该资源的权限。
- 当用户使用子账号访问时，此时会触发子账号授权策略，即RAM（详见下一章节介绍）。DataHub会校验该子账号是否被对应主账号授予了访问该资源的权限，同时也会校验该子账号对应的主账号是否具有该资源的所有者权限。



说明：

DataHub目前暂不支持不同主账号之间的授权策略。

#### 访问控制

DataHub支持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。

DataHub遵循RAM权限和授权策略。DataHub的RAM权限体系主要包括Action、Resource、Affect三个概念，采用POLICY授权方式，格式示例如下所示：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [ "dhs:GetRecords" ],
      "Resource": "acs:dhs:cn-hangzhou:1001:projects/A/topics/B",
      "Effect": "Allow"
    }
  ]
}
```



说明：

其中Resource的具体格式为：`acs:dhs:{Region}:{User}:{DataHubResource}`

针对上述示例，表示某个用户对某个Region下DataHub的某个资源的访问权限控制。例如上述示例中，Policy权限表示：子账号1001有权限去读取region为cn-hangzhou，Project为A且Topic为B的数据。

目前DataHub提供细粒度的权限控制策略，用户可以根据不同的需求进行不同的权限控制。

### 5.41.1.3 传输加密

考虑到DataHub高吞吐的服务要求，DataHub内部并没有对用户的数据进行存储加密。同时由于DataHub提供Restful的传输接口，其传输安全性由HTTPS保证。

### 5.41.1.4 数据安全

专有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，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。

在专有云数据存储系统中，有三类角色，分别称为Master、Chunk Server和Client。DataHub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。

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DataHub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，释放的存储空间由飞天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，最大限度保证用户的数据安全性。

## 5.41.2 租户侧安全功能

### 5.41.2.1 日志审计

DataHub会针对不同用户不同日志数据进行日志审计。在服务内部，DataHub会创建内部Topic进行日志数据存储，包括用户传输数据的QPS、请求时长、处理时长、来源IP以及返回码等内容。同时在用户控制台中，DataHub也会将一些统计信息展现给用户，方便用户分析问题。

## 5.42 DataQ

### 5.42.1 账号体系

本章介绍数据资源平台账号。

数据资源平台（DataQ）对接阿里云账号体系或者客户现场账号登录体系（视安装部署场景定），登录鉴权由依赖的系统保障，DataQ本身不提供额外的登录入口，确保账号认证和平台系统的安全等级对齐。

### 5.42.2 安全隔离

本章介绍数据资源平台安全隔离。

DataQ支持多租户（Tenant）模式，租户下再切分工作空间（Workspace），用户登录之后，DataQ有基于RBAC的权限管控，不同的工作空间，不同的用户角色具有不同的权限，管理员可以根据实际情况，灵活的分配账号权限。

DataQ依赖的各计算资源由用户提供，其中涉及到的用户认证敏感信息在系统中加密存储，遵循只进不出的原则，确保信息不泄露，同时这些计算资源本身的安全措施由各计算资源提供保障。

### 5.42.3 数据安全

本章介绍数据资源平台数据安全。

DataQ基于阿里云自建的计算存储引擎，都具备高可用性，其存储数据分片多副本，确保数据不丢失，数据存储的可靠性非常高。

DataQ中的数据加工、查询、分析过程都不会产生任何的缓存落地，确保数据都在用户提供的计算资源中流转，不在额外的存储中停留，从而避免泄露。

### 5.42.4 传输加密

本章介绍数据资源平台传输加密。

DataQ的所有访问都接入https，确保通讯可靠不泄露。

## 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。

关于专有云云盾产品的详细介绍，查看《云盾技术白皮书》

### 6.1 概述

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。

#### 云盾标准版

云盾标准版包含流量安全监控、安骑士、主机入侵检测、安全审计、Web应用防火墙、态势感知等一系列安全产品和安全运营驻场服务，保障用户的专有云环境中的业务系统及数据的可用性、机密性和完整性。

通过“产品+服务”的方式，充分发挥专有云产品及云盾安全产品的安全特性，为专有云用户提供入侵防御、安全审计、态势感知和集中管控等一站式安全保障。云盾标准版从技术和管理的角度提升专有云环境的安全性，切实保障用户的专有云平台。

#### 可选安全产品

同时，专有云云盾提供多款可选安全产品，供用户根据专有云平台上的业务场景进行选择。

关于专有云云盾产品的详细介绍，查看《云盾技术白皮书》。

### 6.2 云盾标准版

#### 6.2.1 态势感知

态势感知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0 Day漏洞攻击、新型病毒攻击事件，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。

态势感知包含以下功能：

功能项	功能说明
安全态势总览	提供安全整体态势信息，包括防护资产统计信息、安全攻击趋势和网络流量趋势等信息。

功能项	功能说明
可视化大屏	提供安全信息的大屏展示，包括以下两个大屏： <ul style="list-style-type: none"> <li>· 基于地图的流量监控大屏。</li> <li>· 主机业务安全状态大屏。</li> </ul>
安全告警处理	查看和处理安全告警事件，包括异常登录检测、异常账户、网站后门查杀、恶意进程（云查杀）、进程异常行为、敏感文件篡改、异常网络连接等。
攻击分析	防护暴力破解攻击和常见的Web应用攻击。 <ul style="list-style-type: none"> <li>· 暴力破解成功：主机遭受暴力破解攻击且被恶意攻击者成功登录。</li> <li>· 常见的Web应用攻击，包括SQL注入、代码执行、命令执行、脚本木马、文件包含、上传漏洞利用、常见CMS漏洞利用等Web攻击。</li> </ul>

## 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态势可视和可感知：

### · 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。

### · 大屏实时监控

态势感知为用户提供可视化大屏，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。

## 6.2.2 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。流量安全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：

功能项	功能说明
流量统计分析	通过流量镜像方式旁路对进出互联交换机（ISW）的流量进行统计，生成流量图。
异常流量检测	通过流量镜像方式旁路检测超过阈值的异常流量，并牵引到DDoS流量清洗产品进行清洗。阈值支持设置流速（Mbps）、包速（PPS）、HTTP请求速率（QPS）、新建连接数等参数。
恶意主机识别	针对专有云内部的恶意主机对外发起的攻击行为进行检测，发现内部已经被控制的云服务器。
Web应用攻击防护	根据内嵌的Web应用攻击检测规则，对常见的Web应用攻击进行网络层拦截旁路阻断，防护包括SQL注入、代码执行、命令执行、脚本木马、文件包含、上传漏洞利用、常见CMS漏洞利用等Web攻击。
异常TCP连接阻断	通过旁路向服务端和客户端发送TCP Reset报文，阻断四层TCP连接。
网络日志记录	记录四层UDP、TCP流量日志，HTTP请求的Request和Response日志，供态势感知模块进行大数据模型分析。

### 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。

## 6.2.3 漏洞扫描

漏洞扫描模块是结合人工智能技术帮助企业及时发现安全风险的智能安全产品。

漏洞扫描模块根据用户设置的已知资产结合内置的资产学习模型，对资产进行分析，准确分辨资产来源，帮助企业自动发现未知资产。同时根据漏洞检测覆盖能力，帮助企业及时发现未知的安全风险。

漏洞扫描模块可以7\*24小时对资产、资产漏洞、ACL、安全基线进行监控，实时发现安全风险，并通过短信、邮件等方式及时告知用户，帮助用户第一时间发现企业安全风险。

漏洞扫描模块提供以下功能：

功能项	功能说明
资产发现	系统内置资产学习模型，根据用户提供的已知资产，准确分辨资产来源，定期进行资产巡检以发现更多的未知资产，并添加至资产库中。资产学习模型将其企业资产进行智能化识别，例如精准识别主机服务及主机资产的变更状态，支持资产存活状态自动发现，支持配置资产巡检，支持对子域名和多级域名的发现。
资产管理	系统支持资产导入、删除、分组及导出管理，资产归属及负责人管理，资产检索及监控管理；同时利用深度学习技术对不同应用与服务的协议请求数据进行拆分，提取特征值，通过指纹模型自动识别应用和服务；就近调度监控检测服务实现对企业资产进行监控。
资产监测	系统利用HTTP和PING方式对资产进行监测，通过自定义告警策略后，可查看该监控网站在被监控期间的可用性详情及监控基础信息。
漏洞扫描	系统支持基础漏洞扫描、弱口令扫描、安全漏洞扫描、漏洞自动化巡检、基线检测及CVE漏洞扫描，其中包括常见的Web漏洞类型、最新高危CVE漏洞、常见CMS漏洞和运维安全漏洞，弱口令扫描支持MySQL、SSH、FTP、SQL Server等常见服务。
漏洞管理	系统支持扫描后的漏洞与资产进行自动关联，使资产风险可视化，帮助企业及时发现和管理风险。支持漏洞流程管理，针对漏洞进行忽略、确认以及重新检测等操作。支持查看漏洞详情、提供修复建议和漏洞分享，帮助企业及时加固。
外部风险监测	外部风险监测基于员工行为特征和企业关键信息进行外部巡检。例如GitHub代码外泄监测，及时发现企业员工上传代码到GitHub的行为并预警，包括代码泄露监测、代码泄露详情查看、代码泄露处理等操作，从而降低代码泄露的风险。

## 最佳实践

### · 小规模网络安全运维

小规模网络下单机部署漏洞扫描模块的专有云产品，完成全部网络的安全检查。漏洞扫描模块可以部署应用在小规模网络安全运维环境中，通过简单部署即可全面检查业务系统的各种安全脆弱性问题。

### · 中等规模多子网网络安全运维

对于中等规模企业，网络规模也不大，但一般会划分为多个业务子网，不同子网对应着不同的区域，多机部署方案适应于企业多区域保护从而实现全网的保护，监控节点分布在不同的网络环境中，漏洞扫描模块云端统一管理。

#### · 大规模跨地区网络安全运维

在大型企业中，通常是大规模跨地区的网络，漏洞扫描模块分布式部署在各地区，在总部云端进行集中管理，集群部署方案适应于企业多地区保护从而实现全网的保护，监控节点分布在不同地区的网络环境中，漏洞扫描模块云端统一管理。

### 6.2.4 主机入侵检测

主机入侵检测模块通过在物理服务器上部署的客户端进行信息搜集和检测，实时检测专有云环境中所有物理服务器主机，并及时发现文件篡改、异常进程、异常网络连接、可疑端口监听等行为，帮助用户及时发现服务器安全隐患。

主机入侵检测模块包含以下功能：

功能项	功能说明
关键目录完整性检测	监控主机系统特定目录（ <code>/etc/init.d</code> ）中文件的完整性，及时发现篡改行为并进行告警。
异常进程告警	及时发现异常进程启动并进行告警，支持对XOR DDoS木马、Bill Gates DDoS木马、Minred挖矿程序等异常进程的检测。
异常端口告警	及时发现新建的端口监听并进行告警。
异常网络连接告警	及时发现主动外连公网的网络连接并进行告警。

#### 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。


### 6.2.5 安骑士

安骑士模块通过日志监控、文件分析、特征扫描等手段，为云服务器提供漏洞管理、基线检查、入侵检测、资产管理等安全防护措施。

安骑士分为客户端和服务端。安骑士客户端配合安骑士服务器，监测针对主机系统层和应用层的攻击行为、漏洞信息、基线配置，实时防护云服务器主机安全。

安骑士包含以下功能：

功能分类	功能项	功能说明
漏洞管理	Linux软件漏洞检测	通过检测云服务器上安装软件的版本信息，与CVE官方的漏洞库进行匹配，检测出存在漏洞的软件（包括SSH、OpenSSL、MySQL等软件漏洞），并推送漏洞信息，提供修复建议。

功能分类	功能项	功能说明
	Windows漏洞检测与修复	<p>通过订阅微软官方更新源，检测云服务器中存在的未修复的高危官方漏洞，并推送微软官方补丁进行修复（如“SMB远程执行漏洞”）。</p> <div>  <p><b>说明：</b> 默认系统只推送高危漏洞，安全更新和低危漏洞支持手动更新。</p> </div>
	Web-CMS漏洞检测与修复	同步阿里云安全情报源，通过目录及文件的检测方案检测Web-CMS软件漏洞，提供云盾自研补丁（修复如Wordpress、Discuz等软件漏洞），且支持漏洞修复及回滚操作。
	配置型、组件型的漏洞检测	检测无法通过版本匹配和文件判断方式发现的漏洞，精准识别软件高危配置漏洞，例如Redis未授权访问、ImageMagick等配置型、组件型漏洞。
基线检查	账号安全基线检查	<ul style="list-style-type: none"> <li>检测SSH、RDP、FTP、MySQL、PostgreSQL、SQLServer服务中存在的弱口令账号。</li> <li>检测云服务器中存在的可疑的隐藏账号、克隆账号等风险账号。</li> <li>检测Linux系统服务器中的密码策略合规性。</li> <li>检测云服务器中存在的空密码账户。</li> </ul>
	系统配置检测	<p>对系统组策略、登录基线策略、注册表配置风险进行检测，包括：</p> <ul style="list-style-type: none"> <li>检测Linux系统服务器的定时任务中是否包含可疑的自启动项目。</li> <li>检测Windows系统服务器中的自启动项。</li> <li>检测系统共享配置。</li> <li>检测Linux系统服务器的SSH登录安全策略配置。</li> <li>检测Windows系统服务器中账号相关的安全策略。</li> </ul>
	数据库安全基线检查	检测服务器上的Redis服务是否对公网开放、是否存在未授权访问漏洞并向系统关键文件写入异常数据的情况。
	合规对标检测	按照CIS-Linux Centos7最新基线标准进行系统层面基线合规检测。



功能分类	功能项	功能说明
入侵检测-异常登录	异地登录告警	自动记录所有登录记录，通过分析和记录用户常用登录位置，识别常用的登录区域（精确到地市级），对疑似的非常用地登录行为进行告警，且支持自定义常用登录地配置。
	非白名单IP登录告警	配置登录白名单IP后，对来自非白名单IP的登录事件进行告警。
	非法时间登录告警	配置合法登录时间后，对非合法时间段内的登录事件进行告警。
	非法账号登录告警	配置合法登录账号后，对非合法账号的登录事件进行告警。
	暴力破解登录拦截	对非法暴力破解密码的异常登录行为进行识别，实时检测并拦截暴力破解攻击，避免被黑客多次猜解密码而导致入侵。支持对SSH和RDP服务的暴力破解行为进行监控。
入侵检测-网站后门查杀	网站后门（Webshell）查杀	通过自研网站后门查杀引擎对云服务器中存在的脚本后门进行精准查杀（支持配置定时查杀和实时防护扫描策略），识别包括以ASP、PHP、JSP编写的脚本后门文件，并支持手动对脚本后门文件进行隔离。
入侵检测-主机异常进程	进程异常行为检测	检测诸如反弹Shell、JAVA进程执行CMD命令、Bash异常文件下载等进程异常行为。
资产管理	资产分组	支持对云服务器进行最多四级分组，并可按照地域、在线状态等信息进行筛选，且支持资产标签管理功能。
	资产指纹	<ul style="list-style-type: none"> <li>· 端口监听：收集、展示端口监听信息，对变动进行记录，便于清点端口开放情况</li> <li>· 账号管理：收集账户及对应权限信息，清点特权账户、发现提权行为</li> <li>· 进程管理：通过进程快照信息的收集和呈现，清点合法进程、发现异常进程</li> <li>· 软件管理：清点软件安装信息，在高危漏洞爆发时快速定位受影响资产</li> </ul>

功能分类	功能项	功能说明
主机日志	日志检索	<ul style="list-style-type: none"> <li>· 登录流水：系统登录成功的日志记录</li> <li>· 暴力破解：系统登录失败的日志记录</li> <li>· 进程快照：某一时刻主机上的进程运行信息</li> <li>· 端口监听快照：某一时刻主机上的监听端口信息</li> <li>· 账号快照：某一时刻主机上的账号登录信息</li> <li>· 进程启动日志：主机上进程启动的相关信息</li> <li>· 网络连接日志：主机对外主动连接的日志</li> </ul>

### 最佳实践

使用安骑士的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。

## 6.2.6 安全审计

安全审计模块是基于云计算平台的一体化解决方案。对标信息系统安全等级保护基本要求，安全审计模块从物理服务器层面、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。

安全审计包含以下功能：

功能项	功能说明
审计一览	支持根据时间、数据库、网络、主机、用户操作、运维操作等多种维度查询并生成审计报表。通过报表反馈原始日志、审计事件、审计风险、日志用量、存储用量等审计系统运营情况。
原始日志	根据审计对象、审计类型、风险级别、时间、关键字等多种维度查询7天内的所有原始日志。
审计查询	根据审计对象、审计类型、风险级别、时间、关键字等多种维度查询触发审计规则的30天内的审计日志。
策略设置	<ul style="list-style-type: none"> <li>· 审计策略：查询已接入的云产品、主机、网络设备、数据库配置的审计规则，并支持审计规则的添加、修改、删除。</li> <li>· 类型设置：查询或添加新的审计类型。</li> <li>· 告警设置：根据审计规则、审计风险设定报警接收人。</li> <li>· 存档管理：查询、下载185天内的所有原始日志文件。</li> <li>· 导出管理：查询、管理日志导出任务。</li> <li>· 系统设置：配置审计系统的全局参数，包括每天报警次数、全天日志审计量、主机日志量、网络设备日志量、用户操作与运维操作日志量等参数的配置。</li> </ul>

## 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实例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实例的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。

### 6.2.7 Web应用防火墙

Web应用防火墙（Web Application Firewall，简称WAF），基于智能语义分析引擎实现，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包含以下功能：

功能项	说明
Web常见攻击防护	支持SQL注入检测、XSS检测、情报、CSRF检测、SSRF检测、PHP反序列化检测、Java反序列化检测、ASP代码注入检测、文件包含攻击检测、文件上传攻击检测、PHP代码注入检测、命令注入检测，机器人爬虫检测和服务器响应检测模块。  内置五种模式防护模板（默认防护策略、观察模式、高防模式、金融类客户、互联网客户），针对模板中的解码算法可自定义，攻击检测模块可单独开关或设置检测粒度。
缓解CC攻击	支持设定针对域名和URL的访问频次控制规则，实现对违规IP和session的访问控制，对满足条件的IP/SESSION进行访问频率限制或者封禁。  对已知的IP/SESSION进行访问频率限制或者封禁。  其中，CC防护规则不会对CC白名单中的用户（IP或SESSION）生效。
自定义精准访问控制规则	可对站点进行HTTP细粒度的访问控制：包括URI，GET参数，解码后路径，HOST头部，完整COOKIE，POST参数，完整BODY，HTTP状态码，响应内容等条件及条件组合。

## 最佳实践

- 使用WAF来防止敏感信息泄露

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

通过自定义精准访问控制规则有效防御WordPress反射攻击。

## 6.2.8 云安全管理中心（SOC）

云安全管理中心（SOC）为安全部门提供全局用户及平台集中管理能力和专有云日志分析功能。

云安全管理中心（SOC）提供以下功能：

功能项	功能说明
仪表盘	仪表盘为安全管理员提供总体统计分析展示和总体操作入口。
安全监控	查看全局用户安全事件列表和平台安全事件列表。
资产管理	从资产角度查看全局用户资产和平台资产安全情况。
日志分析	日志分析主要对来自多个数据源的日志进行分析，发现异常告警，完善专有云告警检测能力。
报表管理	报表管理功能为安全管理员提供自动化的各类场景报表导出能力。
系统配置	系统配置功能主要提供全局的系统配置能力，如告警设置、升级中心、全局策略、账号管理等。

### 最佳实践

#### · 场景1：日常监控

定期进行安全巡检，目前主要关注用户安全。

- 监控新增紧急风险：每日查看是否有新增紧急需要处理的用户安全告警和脆弱性。
- 风险处置：研判和处理高危安全告警或脆弱性风险。
- 攻击统计：查看攻击数量和抵御情况。
- 安全报表：形成安全日报/周报/月报发送给用户。

#### · 场景2：新资产上线安全评估

监测资产变化，发现新上线的资产，对新上线资产进行安全评估。生成新上线资产的安全评估报告，从而确定是否允许上线。

- 漏洞扫描（主机和Web扫描）。
- 配置核查。
- 云产品基线检查。

#### · 场景3：应急响应/溯源分析

发生紧急事件后进行应急响应溯源分析。

## 6.2.9 安全运营驻场服务

安全运营驻场服务旨在帮助用户更好地利用专有云产品及云盾安全产品的安全特性，管理租户层应用安全。

安全运营服务包括业务上线前安全评估、安全访问控制策略优化、周期性安全评估、安全巡检、安全应急等一系列服务内容，全面覆盖专有云平台租户业务的完整安全生命周期。通过安全运营驻场服务，帮助用户梳理并建立云上安全运营体系，全面提升应用系统安全性，保障用户业务的安全和稳定运行。

## 6.3 可选安全产品

### 6.3.1 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流量清洗包含以下功能：

功能项	功能说明
DDoS攻击清洗能力	检测并防御SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood、DNS Flood、HTTP Flood等攻击。
DDoS攻击查看	支持在界面查看DDoS攻击事件，可通过IP地址、状态、事件信息搜索到对应的DDoS攻击事件。
DDoS流量分析	支持针对某DDoS攻击进行流量分析，查看DDoS攻击的流量协议，并展示发起该攻击事件的Top10主机IP。



说明：

DDoS流量清洗不支持专有云的内网接入交换机。

#### 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。

### 6.3.2 云防火墙

云防火墙可统一管理南北向的流量，提供访问控制、流量分析等功能，全面保护您的网络安全。

云防火墙包含以下功能：

功能项	功能说明
访问控制	<ul style="list-style-type: none"> <li>支持互联网应用访问控制（南北向）。</li> <li>同时控制入流量和出流量的访问。</li> <li>支持基于域名的访问控制，严格控制主动外联的出流量。</li> <li>支持主动外联分析，帮助您主动发现主机的异常行为。</li> </ul>
实时流量监控	<ul style="list-style-type: none"> <li>可对主动外联行为进行监控。</li> <li>支持对互联网访问流量进行分析。</li> <li>支持内网ECS互访流量分析。</li> <li>支持业务可视，让您全面了解资产的信息和访问关系，从而及时发现异常流量。</li> </ul>
实时防御	<ul style="list-style-type: none"> <li>支持入侵防御功能并同步进行智能阻断。支持被阻断访问分析，识别被云防火墙和IPS阻断的网络流量。</li> <li>威胁情报联动：同步阿里云全网的恶意IP，如恶意访问源、扫描源、中控服务等，对威胁和入侵做到提前防御。</li> <li>内置云平台长期攻防实战中积累的入侵防御规则，威胁识别率高、误报率小。</li> <li>支持虚拟补丁，无需在业务系统上安装补丁即可实时修复。可对热门漏洞、高危0-day和N-day的利用进行精准防护。</li> </ul>
行为回溯	<ul style="list-style-type: none"> <li>提供事件日志，可实时查看被入侵防御模块检测和拦截到的威胁或入侵事件。</li> <li>提供流量日志，可查看经过云防火墙的所有流量数据。您可在威胁事件发生的时候通过查看流量日志进行流量和访问源分析，并查看配置的访问控制策略是否生效。</li> <li>提供系统操作日志，可查看云防火墙所有的配置和操作记录。</li> </ul>

## 最佳实践

### 云防火墙模块适用于下列场景：

- 互联网业务防护：例如某金融用户除了HTTP业务外，还有其他类型业务暴露在互联网上。用户需要使用入侵检测模块（IPS）进行防护。
- 主动外联防护：例如某政府行业用户，除了关注从互联网到业务的防御，也同时关注业务主动外联的分析，以判断哪些主机已经处于风险状态，并对这些异常行为进行实时阻断，规避潜在的风险。

### 6.3.3 内容安全

内容安全模块为用户提供成熟的、轻量化接入的内容安全解决方案，帮助用户快速发现图片、视频的各类风险，保障应用的信息内容安全。

内容安全模块主要对包含色情、广告、垃圾信息的文本、图片及视频进行检测和识别，同时还提供审核建议、打标、自定义配置等功能来满足个性化需求，保障用户的使用效果。

#### 最佳实践

通过内容安全对于业务中的直播、视频、图片、文本、语音等可能存在内容风险进行统一检测，一次性发现存在的内容所有风险。

### 6.3.4 堡垒机

堡垒机为云服务器的运维提供完整的审计回放和权限控制服务。基于账号（Account）、认证（Authentication）、授权（Authorization）、审计（Audit）的AAAA统一管理方案，通过身份管理、授权管理、双因子认证、实时会话监控与切断、审计录像回放、高危指令查询等功能，增强运维管理的安全性。

堡垒机包含以下功能：

功能项	功能说明
登录认证机制	支持本地认证方式，同时支持手机App动态口令、短信口令等双因子认证方式。
凭据托管、单点登录	支持托管云服务器ECS的账户和密码（或SSH密钥），运维人员只需要登录到云盾堡垒机后即可直接登录ECS云服务器，无需使用ECS云服务器的账户密码信息。
系统运维	支持Web端调用本地工具实现单点登录；支持“本地客户端登录堡垒机，再选择服务器”的方式进行运维。
运维监控及阻断	针对运维人员的操作过程进行实时监控，并支持以切断操作会话的方式阻断违规操作等异常行为。
日志回放、事后追溯	<ul style="list-style-type: none"> <li>提供录像式日志回放功能，并且可通过关键信息进行定位回放。</li> <li>提供指令记录功能，并且可基于关键指令进行过滤检索。</li> <li>提供图像记录功能，并且可基于关键文字进行过滤检索。</li> <li>提供文件审计功能，并且可详细记录上传下载的文件名等信息。</li> </ul>

#### 最佳实践

- 审计合规要求严格的场景
  - 部门权限隔离：基于部门隔离功能，实现各部门有效管理和审计。
  - 统一运维入口：为操作人员提供了统一的运维入口，解决分散登录的问题。
  - 满足合格审核：建立健全的云上运维审计机制，满足行业监管要求。
- 高效稳定的运维管理场景
  - 高并发会话：支撑千人级别的并发会话。
  - 稳定运行：有高稳定性的SLA保障。
  - 运维故障回溯：运维人员难免发生误操作，通过回溯操作内容，建立运维红线。

### 6.3.5 数据库审计

数据库审计支持对云端自建数据库、RDS数据库访问的精确审计，以及准确的应用用户关联审计，并具备风险状况、运行状况、性能状况、语句分布的实时监控能力。

数据库审计系统通过数据库化的界面语言、智能化的协议识别、可视化的运行状况呈现、可交互可下钻的风险追踪能力，完美实现快速部署、方便维护的云数据库审计。

数据库审计包含以下功能：

功能项	功能说明
审计内容	<p>数据库审计的审计内容包括：</p> <ul style="list-style-type: none"> <li>· 会话的终端信息：IP、MAC地址、端口、客户端工具名(程序名)、数据库用户名</li> <li>· 会话的主机信息：IP、MAC地址、端口、数据库名（实例名）</li> <li>· 会话的其它信息：登录时间、会话时长</li> <li>· 操作信息：操作类型（DDL、DML、DCL等）、操作时间、执行时长、操作成功与失败、受影响行数、操作对象（表、列、存储过程名称）、SQL语句</li> </ul>
审计过滤规则	<p>数据库审计的审计过滤规则包含以下审计策略要素：</p> <ul style="list-style-type: none"> <li>· who：数据库用户名、应用用户、主机名称、操作系统账号</li> <li>· what：表、字段、包、存储过程、函数、视图</li> <li>· where：IP地址、用户名、端口号、数据库类型</li> <li>· when：操作时间、登录时间等</li> <li>· how：客户端工具</li> <li>· Range：修改、删除或查询的行数</li> <li>· ResultSet：返回结果集</li> </ul>



功能项	功能说明
审计信息展示	<p>支持从会话维度、语句类型纬度、风险纬度三个纬度进行导航展示。</p> <p>审计信息包括告警级别、事件发生时间、客户端IP、目标数据库IP、操作类型、客户端MAC地址、目标数据库MAC地址、客户端端口、操作信息大小、返回状态、结果信息、客户端执行命令等详细信息内容。</p>
审计查询	支持基于时间、客户端IP、数据库服务器IP、用户名、数据库操作命令、数据库表名/字段名等多种丰富的查询检索条件。
统计分析	<ul style="list-style-type: none"> <li>· 事件分析：依据安全策略，以时间为基线，统计异常事件的发生数量和趋势。</li> <li>· 告警分析：依据安全策略，以时间为基线，统计严重告警事件的发生数量和趋势。</li> <li>· 综合分析：以数据库操作类型为基线统计各类操作状况。</li> <li>· 会话统计：以时间和IP为基线统计会话的数量、流量、操作的语句数量。</li> </ul>
审计报表	<ul style="list-style-type: none"> <li>· 支持（系统级）多数据库聚合报表展现和单数据库综合性报表展现。</li> <li>· 基于总体概况、性能、会话、语句、风险多层面展现报表。</li> <li>· 支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式。</li> <li>· 支持报表定时推动功能，自定义推送周期以邮件形式推送报表文档。</li> <li>· 支持日、周、月等综合性报表和自定义分析型报表功能。</li> </ul>
业务化语言	支持业务化语言展现，可自定义SQL语句转换业务化语言展现方式。

### 最佳实践

- **安全事件追查：**数据库审计系统提供语句、会话、IP、数据库用户、业务用户、响应时间、影响行等多种维度的数据库操作记录和事后分析能力，成为安全事件后最为可靠的追查依据和来源。通过SQL行为与业务用户的准确关联，使数据库访问行为有效定位到业务工作人员，实现有效追责、定责。
- **数据库性能诊断：**数据库审计系统实时显示数据库的运行状况、数据库访问流量、并发吞吐量、SQL语句的响应速度；提供最慢语句、访问量最大语句的分析，帮助运维人员进行性能诊断。
- **发现程序后门：**数据库审计系统提供SQL学习和SQL白名单能力，实现对业务系统的SQL建模；通过合法系统行为的建模，使隐藏在软件系统中的后门程序在启动时，提供实时的告警能力，降低数据泄漏损失。
- **数据库攻击响应：**数据库审计系统提供数据库风险告警能力，对于SQL注入、数据库漏洞攻击、过量数据下载、危险SQL语句（如No where delete）等风险行为的策略制定能力，提供实时告警能力。

### 6.3.6 数据发现与脱敏

通过数据库发现功能，能够扫描云数据库的分布，自动发现专有云内的所有数据库。同时，通过数据脱敏功能有效防止企业内部对隐私数据的滥用，防止隐私数据在未经脱敏的情况下从企业流出。

满足专有云环境中，既要保护隐私数据，又要满足开发、测试、模型训练等业务对数据的需求；同时也保持监管合规，满足企业合规性。

数据发现与脱敏包含以下功能：

功能项	功能说明
云数据库自动嗅探	提供自动搜索专有云环境中数据库的功能，也支持指定IP段和端口的范围进行搜索。自动发现数据库的端口号、数据库类型、数据库实例名、数据库服务器IP地址等基本信息。
自动识别敏感数据	提供敏感信息的自动发现能力，通过内置的敏感数据特征库，对常见的如姓名、证件号、银行账户、金额、日期、住址、电话号码、Email地址、车牌号、车架号、企业名称、工商注册号、组织机构代码、纳税人识别号等敏感数据自动识别。
敏感数据分类分级	根据不同数据特征，对常见的敏感数据进行分类。根据不同的数据类型指定的不同敏感级别，自动对包含敏感数据的表、模式、库进行敏感度评分。
权限梳理	对数据库中不同用户、不同对象的权限进行梳理并监控权限变化。权限梳理主要从以下两个维度展开： <ul style="list-style-type: none"> <li>· 监控数据库中的用户的启用状态、权限划分、角色归属等基本信息。</li> <li>· 对数据库中的对象可被哪些用户访问的情况进行归纳总结，特别是对包含了敏感列的表或者敏感度评分较高的对象，着重监测其访问权限划分情况。</li> </ul>
敏感数据管理	<p>敏感数据发现：根据指定的部分敏感数据特征或预定义的敏感数据特征，在执行任务过程中对抽取的数据进行自动的识别，发现敏感数据，并自动根据规则对发现的敏感数据进行脱敏处理。</p> <p>敏感数据字典管理：对敏感字段进行分类管理，对同类敏感数据实施统一的脱敏算法和策略，保证同一组织内跨系统、跨库之间的脱敏一致性；并支持敏感数据字典导入、导出等功能。</p>

功能项	功能说明
脱敏算法	<p>根据不同数据特征，内置了丰富高效的脱敏算法，可对常见的姓名、证件号、银行账户、金额、日期、住址、电话号码、Email地址、车牌号、车架号、企业名称、工商注册号、组织机构代码、纳税人识别号等敏感数据进行脱敏，内置脱敏算法具有如下特性：</p> <ul style="list-style-type: none"> <li>· 同义替换：使用相同含义的数据替换原有的敏感数据。例如，姓名脱敏后仍然为有意义的姓名，住址脱敏后仍然为住址。</li> <li>· 部分数据遮蔽：将原数据中部分或全部内容，用“*”或“#”等字符进行替换，遮盖部分或全部原文。</li> <li>· 混合屏蔽：将相关的列作为一个组进行屏蔽，以保证这些相关列中被屏蔽的数据保持同样的关系。例如，城市、省、邮编在屏蔽后保持一致。</li> <li>· 确定性屏蔽：确保在运行屏蔽后生成可重复的屏蔽值。可确保特定的值（如客户号、身份证号码、银行卡号）在所有数据库中屏蔽为同一个值。</li> <li>· 可逆脱敏：确保脱敏后的数据可还原，便于将第三方分析机构和内部经分团队基于脱敏后数据的分析结果还原为业务数据。</li> </ul> <p>支持的脱敏算法包括屏蔽、变形、替换、随机、格式保留加密（FPE）和强加密算法（如AES加密算法）。</p>
数据子集管理	支持对目标数据库中一部分数据进行脱敏。提供多种数据子集抽取方式，包括基于事实表发起的百分比抽取方式；基于基础表中的身份、商品信息发起的向下延展的数据抽取方式；针对多表的灵活条件设定的抽取方式。根据过滤条件，对数据来源进行过滤筛选形成数据子集，以适应不同场景下脱敏需求。
脱敏策略和方案管理	针对不同脱敏项目，可以配置定制化的脱敏策略，或实现脱敏算法的扩展；支持脱敏策略的导入导出，以实现策略复用。对于同一类应用场景，可将若干脱敏策略组合成为适用于该场景的脱敏方案。脱敏方案制定后，可被重复利用于该场景下不同批次数据的脱敏需求。
脱敏任务管理	可对脱敏任务进行停止、启动、重启、暂停、继续，并且支持任务并发，充分利用系统资源，提高脱敏效率。同时，脱敏任务可兼容执行过程中遇到的异常情况，支持跳过异常数据继续执行任务。
脱敏数据验证	支持对脱敏后的数据进行“验证”，确定哪些数据是“漏网”的真实数据，从而帮助用户在使用这些数据前能够及时的发现并相应的弥补脱敏脚本的不足。

## 最佳实践

- 协助完善数据分级分类机制：在数据的使用中，不同的数据拥有不同的敏感级别和密级，不同级别的数据所需的安全策略和加固方式都是不同的。数据梳理模块对敏感数据支持完善的定级机制，能够协助管理员判断数据库中表、模式和整库的敏感级别，便于进一步制定专有云数据安全策略或采取其他数据加固措施。

- 保护隐私数据，满足合规性：通过丰富的内置脱敏算法和灵活的、流程化的策略和方案管理能力，支持对多种数据源进行脱敏处理，帮助在专有云环境中不改变业务流程的前提下快速部署实施，有效的降低脱敏的复杂度和风险，控制脱敏成本。

### 6.3.7 数据梳理

云盾数据梳理系统是一款资产自动发现及数据分级分类管理的安全产品，具有高性能、高易用性、高管理融合性等特点。

数据梳理支持Oracle、MSSQL、Mysql、DB2、Informix、Sybase等国际主流数据库，并支持达梦、金仓、GBASE等国产数据库。

数据梳理支持以下模块。

功能项	功能说明
数据库自动嗅探	<p>系统提供自动搜索网内数据库的功能，也可以指定IP段和端口的范围进行搜索。</p> <ul style="list-style-type: none"> <li>· 支持自动发现数据库的基本信息包括：端口号、数据库类型、数据库实例名、数据库服务器IP地址等。</li> <li>· 支持动态发现数据库能力，通过自动抓取访问数据库流量包，对流量包信息进行解析。</li> </ul>
自动识别敏感数据	<p>系统根据用户指定的部分敏感数据或预定义的敏感数据特征，在执行任务过程中对抽取的数据进行自动识别和发现敏感数据，并可以根据规则导出发现的敏感数据清单。</p> <p>系统支持通过旁路链路的动态流量包进行解析，获取访问对象信息，根据用户指定的部分敏感数据或预定义的敏感数据特征对访问对象自动识别，从而能够动态发现敏感数据分布。</p> <p>通过自动识别敏感数据，可以减少按照字段定义敏感数据元的繁琐工作，同时能够持续的发现新的敏感数据。</p>
敏感数据分级分类	<p>根据不同数据特征，内置了丰富高效的算法，可识别常见的敏感数据。用户可以针对不同的数据类型指定不同的敏感级别，系统会自动的对包含了敏感数据的表、模式、库进行敏感度评分。</p>

功能项	功能说明
权限梳理	<p>能够对数据库中不同用户，不同对象的权限进行梳理并监控权限变化，权限梳理从用户维度或者对象维度展开。一旦用户维度或者对象维度权限发生了变更，能够及时向用户反馈。</p> <ul style="list-style-type: none"> <li>· 用户维度：可以监控数据库中的用户的启用状态、权限划分、角色归属等基本信息。</li> <li>· 对象维度：能够对数据库中的对象可被哪些用户访问的情况进行归纳总结，特别是对包含了敏感列的表或者敏感度评分较高的对象，可以着重监测其访问权限划分情况。</li> </ul>
资产使用分析	<ul style="list-style-type: none"> <li>· 数据源访问分析：能够对数据访问源进行分析，包括访问数据库的数据库用户信息、访问数据库的应用信息、访问数据库的主机信息、访问数据库的客户端信息等，并能够根据分析结果，绘制出数据库的日常访问拓扑图。</li> <li>· 访问行为分析：能够对访问数据库的操作行为进行分析统计，包括 SELECT（查询）、DML、DCL、DDL类型的操作。</li> <li>· 资产访问热度分析：能够对数据库的日常访问流量进行分析，按照不同维度汇总出数据库访问热度统计图，包括按照语句、流量、会话三个维度。</li> </ul>
任务管理	<p>针对目标数据库，系统可以创建授权任务对该库进行敏感数据发现和权限梳理。</p> <ul style="list-style-type: none"> <li>· 支持用户创建自定义定时任务，帮助企业定期检查资产，核查资产分布和使用情况。</li> <li>· 系统支持用户创建批量任务，可以批量执行敏感数据发现任务。</li> </ul>
资产周期统计与对比分析	<p>系统将数据资产梳理按日、周、月三个周期进行统计，统计结果可以以报告的形式导出。用户可以查看该周期内发现数据源分布、敏感数据、权限梳理以及资产使用情况。也可以将任意两个周期资产梳理结果对比分析，通过对比分析发现资产差异性。</p>
丰富的报表与技术报告呈现	<p>系统内嵌了报表功能模块，能够提供给用户丰富的专项报表，如整体资产统计报表、敏感数据梳理报表、资产使用报表、资产对比分析报表等供用户分析审核。</p> <p>管理员还可以利用报表自定义功能生成定制化的报告，支持word、pdf、html格式导出。</p> <p>系统按周期资产梳理进行统计分析，形成季度、月化、年化运维工作分析报告。</p>

## 最佳实践

数据梳理在国家等级保护、分级保护等领域均具有很强的政策合规性，在制度与技术有效结合的方面做出了创新。广泛适用于银行、证券、保险等金融机构，同时在政府部门、涉密单位也有良好适用场景。

典型应用场景如下：

- 小规模应用场景

适用于地市级政府单位的业务系统或数据中心、小型城商行或小规模的企业等。

- 中等规模应用场景

适合各省级政府单位的业务系统或数据中心，社保业务系统、工商、税务、财政、审计等行业的省厅单位；银行业的国有行省分公司大中型保险公司等企业。

- 大规模应用场景

政府部委级全国数据中心，如税务总局、海关总署等；国有大型银行总部，大型保险集团公司等。

### 6.3.8 敏感数据保护

敏感数据保护SDDP（Sensitive Data Discovery and Protection）是一款数据安全产品，主要用于发现和识别大数据产品的敏感数据。

SDDP充分使用阿里巴巴大数据分析能力以及人工智能相关技术，通过智能化敏感数据识别，基于业务需求实现分类分级，并在精准识别基础上实现动态与静态脱敏、全域流转监控与异常检测，达到精准识别、精准检测、精准分析、有效保护，实现可见、可控、合规的安全保护要求。该产品支持MaxCompute、OSS、ADS、OTS等专有云大数据产品。

SDDP提供以下功能：

功能项		功能说明
敏感数据分类识别	新增数据检测功能	部门管理员根据业务需求授权SDDP扫描与保护本部门的数据资产，只监测与扫描授权范围内的数据资产。
	敏感数据分类分级功能	系统针对MaxCompute、ADS、OTS、OSS、RDS等产品的敏感数据识别，支持分类分级配置功能，配置方式支持关键字、正则表达式等常见方式。
	敏感数据识别功能	系统内置敏感数据发现算法，通过文件聚类、深度神经网络、机器学习等算法实现敏感图片识别、文字识别、敏感字段识别。

功能项		功能说明
敏感数据权限管控	资产识别权限	系统支持在MaxCompute项目/MaxCompute表/MaxCompute列/MaxCompute包、ADS库/ADS表、OSS文件桶、OTS实例/OTS表上直接定位该数据资产对应权限，并支持集中展示持有该数据资产权限的账号。
	账号识别权限	系统支持根据部门名称检索部门所属人员；提供模糊查询部门（或人员）能力；支持层次化、可视化方式展示部门和人员的对应关系。
	权限使用异常检测	系统支持智能检测大数据环境下MaxCompute、ADS、OTS、OSS等数据产品的权限使用异常情况。
数据流转与操作监控	数据流转监控功能	系统支持大数据环境下，数据存储产品（MaxCompute、ADS、OSS、OTS），数据传输产品（Datahub、CDP），数据流处理产品（Blink），外部数据库，外部文件等实体的数据链路监控。实现了可视化动态数据流转图，流转图能动态展示数据流转情况/异常产出情况，并能通过流转图中异常位置直接重定向到数据流转异常处理页面。
	数据操作异常检测功能	系统支持智能检测大数据环境下MaxCompute、ADS、OTS、OSS等数据产品的操作异常情况。
	数据流转异常检测功能	系统支持智能检测大数据环境下MaxCompute、ADS、OTS、OSS等数据产品的数据流转异常情况（下载属于数据流转异常范畴）。
	检测规则自定义功能	系统支持自定义数据流转异常的检测规则和数据操作异常的检测规则，用户根据算法结果实现自主配置能力。
异常事件处理	异常事件产出配置功能	系统支持集中配置异常事件产出阈值，支持集中配置异常事件检测模型适用性（包括数据流转异常、数据权限使用异常、数据操作异常）。
	异常事件处理功能	系统内置处理异常事件的控制台，支持通过部门账号、事件类型、责任账号、处理状态、发生时间等多个维度检索异常事件。
	异常事件统计功能	系统支持统计大数据场景中产生的各类异常事件处理情况（包括数据流转异常、数据操作异常、权限使用异常），并动态化展示统计数据。
静态脱敏	静态脱敏功能	<p>系统支持对MaxCompute、OSS、ADS、OTS、RDS等产品的敏感数据进行静态脱敏。</p> <p>系统支持的脱敏算法包括哈希脱敏、遮盖脱敏、替换脱敏、变换脱敏、加密脱敏和洗牌脱敏。</p>

功能项		功能说明
智能审计	智能审计功能	系统收集OSS、MaxCompute、RDS等产品的操作日志并进行审计。

#### 最佳实践

- 满足个人信息保护合规需求

SDDP能从海量数据中识别个人信息，并自动实现敏感等级打标，有效检测数据泄漏，确保企业能够符合《网络安全法》、个人信息保护规范以及其他国内外隐私保护法案的要求。

- 企业敏感数据分级保护

SDDP可根据您设定的规则，通过分级配置与检测、数据产品权限管理、监控数据流转异常、敏感数据操作异常检测、权限使用异常检测、数据操作异常检测，最终实现企业敏感数据分级保护。

- 数据泄漏事件响应与处理

SDDP可根据您设定的异常产出规则，实现各类异常事件的归集并实现集中处理，实现企业数据泄漏事件的应急响应线上化，有效支撑企业安全运维需要。

### 6.3.9 加密服务

加密服务是一款云上加密解决方案。服务底层使用经国家密码管理局检测认证的硬件密码机，通过虚拟化技术，帮助用户满足数据安全方面的监管合规要求，保护云上业务数据的隐私性要求。借助加密服务，用户能够对密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

加密服务包含以下功能：

- 全面支持国产算法以及部分国际通用密码算法，满足用户各种加密的算法需求。
- 符合中国人民银行标准和规范的金融行业定制加密需求，全面支持金融支付领域的加解密需求。
- 密码机设备管理与敏感信息管理权限分隔。
- 敏感指令支持分类授权控制，有效防止越权行为。
- 支持用户名口令认证、数字证书认证等多种权限认证方式。
- 密码机内部采用硬件芯片阵列实现架构设计，即使部分硬件芯片损坏也不影响使用。
- 独有的异常恢复系统，有效应对各种突发事件。

#### 最佳实践

- 用户敏感数据加密：用户身份证号、手机号码加密存储，有效解决黑客攻破网络、拖库导致的数据泄露风险以及内部非授权用户非法访问、篡改数据、泄露数据的风险。



- **满足支付场景的强监管要求：**保证支付数据在传输、存储过程中的完整性、保密性和支付身份的认证、支付过程的不可否认性，满足金融支付场景监管合规需求，保障金融支付业务的安全性。
- **电子票据类应用加密需求：**保证电子病历、电子发票、电子合同、电子保单等在生产、传输、存储过程中的完整性、保密性。