阿里云
专有云Enterprise版

安全白皮书

产品版本：V3.5.0

文档版本：20180709

为了无法计算的价值 | 阿里云

法律声明

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

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

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	**禁止**： 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	**警告**： 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	**说明**： 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	**设置** > **网络** > **设置网络类型**
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

法律声明.....I
通用约定.....I
1 安全白皮书介绍.....1
2 安全责任共担.....2
2.1 阿里云安全责任.....2
2.2 用户安全责任.....2
3 安全合规和隐私.....4
3.1 安全合规.....5
3.2 隐私保护.....6
4 阿里云专有云安全架构.....8
4.1 云平台安全架构.....8
4.1.1 基础设施安全.....8
4.1.1.1 物理安全.....8
4.1.1.2 服务器设备安全.....9
4.1.1.3 网络设备安全.....9
4.1.1.4 基础网络安全.....10
4.1.2 云操作系统安全.....10
4.1.2.1 虚拟化安全.....10
4.1.2.2 基础系统服务安全.....11
4.1.2.3 系统管理和调度安全.....12
4.1.2.4 云服务器安全.....12
4.1.3 网络服务安全.....13
4.1.3.1 负载均衡.....13
4.1.3.2 专有网络.....13
4.1.3.3 分布式防火墙.....13
4.1.3.4 DDoS攻击防御.....14
4.1.4 云数据库安全.....14
4.1.4.1 租户层隔离.....14
4.1.4.2 数据库账号.....14
4.1.4.3 IP白名单.....14
4.1.4.4 专有网络隔离.....14
4.1.5 云存储安全.....15
4.1.5.1 身份验证.....15
4.1.5.2 访问控制.....15
4.1.5.3 租户层隔离.....15
4.1.6 应用安全.....15

4.1.7 大数据计算安全 16
4.1.7.1 授权管理 16
4.1.7.2 跨项目空间的资源分享 16
4.1.7.3 数据保护机制 16
4.1.8 数据安全 17
4.1.8.1 数据安全体系 17
4.1.8.2 数据所有权 17
4.1.8.3 多副本冗余存储 17
4.1.8.4 全栈加密 17
4.1.8.5 镜像管理 17
4.1.8.6 残留数据清除 17
4.1.8.7 运维数据安全 17
4.1.9 云产品代码安全 18
4.1.10 安全审计 19
4.1.11 云平台安全运营服务 19
4.2 云用户（租户）侧安全 20
4.2.1 账户安全 20
4.2.2 主机安全 20
4.2.3 应用安全 21
4.2.4 数据安全 21
4.2.5 安全产品（云盾） 21
4.2.6 安全运营服务 22
4.2.7 安全最佳实践 22
5 专有云云产品安全 23
5.1 账号安全 23
5.1.1 云账户 23
5.1.2 超级管理员 23
5.1.3 身份凭证（Credential） 23
5.2 运维权限管理（OAM） 24
5.2.1 OAM权限模型 24
5.2.2 OAM授权 24
5.3 天基权限管理（数据中心管理） 25
5.4 访问控制RAM 25
5.4.1 RAM用户身份类型 25
5.4.2 权限 26
5.4.3 授权策略 26
5.5 云服务器ECS 27
5.5.1 安全隔离 27
5.5.2 鉴权认证 28
5.5.2.1 身份验证 28
5.5.2.2 权限控制 28

5.5.2.3 RAM和STS支持.....29
5.5.3 数据安全.....29
5.5.3.1 三副本存储技术.....29
5.5.3.2 ECS磁盘加密.....31
5.5.4 传输加密.....31
5.5.5 日志审计.....32
5.5.6 其他安全能力.....32
5.6 容器服务.....33
5.6.1 信息加密传输.....33
5.6.2 证书密钥管理.....33
5.6.3 漏洞扫描.....33
5.7 弹性伸缩.....34
5.7.1 安全隔离.....34
5.7.2 鉴权认证.....34
5.7.2.1 身份验证.....34
5.7.2.2 RAM支持.....34
5.7.3 日志审计.....35
5.8 对象存储OSS.....35
5.8.1 安全隔离.....35
5.8.2 鉴权认证.....35
5.8.2.1 身份验证.....35
5.8.2.2 权限控制.....35
5.8.2.3 RAM和STS支持.....36
5.8.3 数据安全.....36
5.8.4 传输加密.....37
5.8.4.1 服务器端加密.....37
5.8.4.2 客户端加密.....37
5.8.4.3 KMS加密.....37
5.8.5 日志审计.....37
5.8.6 防盗链.....38
5.9 表格存储TableStore.....38
5.9.1 安全隔离.....38
5.9.2 鉴权认证.....38
5.9.2.1 身份验证.....38
5.9.2.2 VPC 访问控制.....38
5.9.2.3 RAM和STS支持.....38
5.9.3 数据安全.....39
5.10 文件存储NAS.....39
5.10.1 安全隔离.....39
5.10.2 鉴权认证.....39
5.10.3 数据安全.....41

5.10.4 日志审计 42
5.11 分布式文件系统 42
5.11.1 安全隔离 42
5.11.2 鉴权认证 42
5.11.3 数据安全 44
5.11.4 日志审计 44
5.12 云数据库RDS版 45
5.12.1 安全隔离 45
5.12.2 鉴权认证 45
5.12.2.1 身份验证 45
5.12.2.2 权限控制 46
5.12.2.3 RAM和STS支持 46
5.12.3 数据安全 46
5.12.4 传输加密 46
5.12.4.1 SSL 46
5.12.4.2 TDE 47
5.12.5 日志审计 47
5.12.6 IP白名单 47
5.12.7 软件升级 47
5.12.8 防DDoS攻击 48
5.13 云数据库Redis版 48
5.13.1 租户隔离 48
5.13.2 访问控制 49
5.13.3 网络隔离 49
5.13.4 备份恢复 50
5.13.5 RAM和STS支持 50
5.13.6 软件升级 50
5.13.7 数据传输加密 50
5.14 云数据库MongoDB版 51
5.14.1 安全隔离 51
5.14.2 鉴权认证 51
5.14.2.1 身份验证 51
5.14.2.2 权限控制 52
5.14.2.3 RAM和STS支持 52
5.14.3 数据安全 52
5.14.4 日志审计 52
5.14.5 IP白名单 53
5.14.6 DDoS防护 53
5.15 云数据库Memcache版 53
5.15.1 租户隔离 53
5.15.2 访问控制 53

5.15.3 网络隔离.....54
5.15.4 备份恢复.....54
5.15.5 RAM和STS支持.....54
5.15.6 软件升级.....54
5.16 HybridDB for MySQL.....55
5.16.1 租户隔离.....55
5.16.2 主备节点.....55
5.16.3 访问控制.....55
5.16.4 网络隔离.....55
5.16.5 备份恢复.....56
5.16.6 RAM和STS支持.....56
5.16.7 软件升级.....56
5.17 HybridDB for PostgreSQL.....57
5.17.1 租户隔离.....57
5.17.2 主备节点.....57
5.17.3 访问控制.....57
5.17.4 网络隔离.....57
5.17.5 SQL审计.....58
5.17.6 备份恢复.....58
5.17.7 RAM和STS支持.....58
5.17.8 软件升级.....58
5.18 云数据库OceanBase版.....59
5.18.1 安全隔离.....59
5.18.2 鉴权认证.....59
5.18.3 数据安全.....59
5.18.4 传输加密.....60
5.18.5 日志审计.....60
5.18.6 高可用架构.....60
5.18.7 兼容性.....61
5.18.8 软件升级.....61
5.18.9 产品特有的安全能力.....61
5.19 数据传输服务DTS.....62
5.19.1 传输安全.....62
5.19.2 存储安全.....62
5.19.3 访问安全.....62
5.20 数据管理（DMS）.....63
5.20.1 访问控制.....63
5.20.2 网络安全.....63
5.20.3 传输安全.....63
5.20.4 操作审计.....64
5.21 负载均衡SLB.....64

5.21.1 访问控制.....64
5.21.2 支持HTTPS协议.....64
5.21.3 RAM和STS支持.....64
5.22 专有网络VPC.....65
5.22.1 安全隔离.....65
5.22.2 网络访问控制.....65
5.22.3 RAM和STS支持.....65
5.23 日志服务.....65
5.23.1 安全隔离.....65
5.23.2 鉴权认证.....66
5.23.3 数据安全.....66
5.23.4 传输加密.....67
5.23.5 服务监控.....67
5.24 密钥管理服务KMS.....68
5.24.1 安全隔离.....68
5.24.2 鉴权认证.....68
5.24.2.1 身份验证.....68
5.24.2.2 权限控制.....69
5.24.2.3 RAM和STS支持.....69
5.24.3 数据安全.....69
5.24.4 传输加密.....69
5.24.5 日志审计.....69
5.25 云解析DNS.....70
5.25.1 RAM鉴权.....70
5.25.2 账号数据隔离.....70
5.26 企业级分布式应用服务EDAS.....70
5.26.1 全链路加密.....70
5.26.2 RAM支持.....72
5.26.3 权限控制.....72
5.26.4 API鉴权.....73
5.26.5 API审计.....73
5.27 分布式关系型数据库DRDS.....73
5.27.1 访问控制.....74
5.27.2 网络隔离.....75
5.27.3 慢SQL审计.....75
5.27.4 监控信息.....75
5.28 消息队列MQ铂金版安全.....75
5.28.1 消息队列MQ.....75
5.28.2 访问控制.....76
5.28.3 数据加密.....77
5.28.4 网络隔离.....77

5.28.5 日志审计 78
5.29 消息队列MQ专业版安全 78
5.29.1 消息队列MQ 78
5.29.2 访问控制 79
5.29.3 数据加密 80
5.29.4 网络隔离 80
5.29.5 日志审计 81
5.30 业务实时监控服务ARMS 81
5.30.1 访问控制 81
5.30.2 数据隔离 82
5.31 全局事务服务GTS 82
5.31.1 访问控制 82
5.32 云服务总线CSB 83
5.32.1 访问控制 83
5.32.2 API鉴权 84
5.32.3 API审计 84
5.33 MaxCompute 85
5.33.1 安全隔离 85
5.33.2 权鉴认证 85
5.33.2.1 身份验证 85
5.33.2.2 权限控制 86
5.33.2.3 RAM支持 93
5.33.3 数据安全 93
5.33.4 传输加密 93
5.33.5 日志审计 94
5.33.6 访问控制-IP白名单 94
5.33.7 MaxCompute支持VPC 101
5.33.8 ElasticSearch on MaxCompute支持VPC 101
5.34 分析型数据库 102
5.34.1 安全隔离 102
5.34.2 鉴权认证 102
5.34.2.1 身份验证 102
5.34.2.2 权限控制 103
5.34.2.3 RAM和STS支持 103
5.34.3 数据安全 103
5.34.4 日志审计 104
5.34.5 VPC支持 104
5.35 关系网络分析 105
5.35.1 安全隔离 105
5.35.2 鉴权认证 105
5.35.2.1 身份验证 105

5.35.2.2 权限控制 105
5.35.3 数据安全 105
5.35.4 传输加密 105
5.35.5 日志审计 106
5.35.6 系统安全 106
5.35.6.1 漏洞扫描机制 106
5.35.6.2 安全漏洞更新修复方案 106
5.35.6.3 系统防御机制 106
5.35.7 基础设施安全 106
5.35.8 等保认证 106
5.36 E-MapReduce 107
5.36.1 安全隔离 107
5.36.2 用户认证 107
5.36.3 权限控制 108
5.36.4 容灾 110
5.36.4.1 数据容灾 110
5.36.4.2 服务容灾 112
5.37 流计算 112
5.37.1 账号安全 112
5.37.2 业务安全 113
5.37.3 数据安全 113
5.38 实时数据分发平台（DataHub） 114
5.38.1 安全隔离 114
5.38.2 鉴权认证 114
5.38.2.1 身份验证 114
5.38.2.2 权限控制 114
5.38.2.3 RAM和STS支持 115
5.38.3 数据安全 116
5.38.4 传输加密 116
5.38.5 日志审计 116
6 专有云云盾 117
6.1 云盾基础版 117
6.2 云盾高级版 118

1 安全白皮书介绍

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

阿里云专有云竭诚为用户提供稳定、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云安全体系，主要包括下列内容：

- 安全责任共担
- 安全合规和隐私
- 专有云平台架构安全
- 专有云各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 安全责任共担

基于专有云平台的用户应用，其安全责任由双方共同承担：阿里云确保专有云平台本身架构的安全性，用户负责专有云平台运营以及基于专有云平台构建的应用系统的安全。

阿里云

阿里云负责专有云飞天分布式云操作系统及之上的各种云服务产品本身的安全，从而为用户提供高可用和高安全的专有云平台。同时，专有云基于阿里巴巴集团多年攻防技术积累，为用户提供云盾安全服务，进一步保障用户的专有云环境的安全。

用户

用户负责以安全的方式配置和使用专有云平台以及云服务器（ECS）、数据库（RDS）实例等云产品，并基于这些云产品以安全可控的方式构建自己的应用。同时，用户可使用专有云云盾安全产品及服务为其专有云环境提供安全防护。

2.1 阿里云安全责任

阿里云负责分布式云操作系统及云服务产品本身的安全，并为用户提供保护专有云平台、云端应用及数据的技术手段。

- 保障专有云云平台架构安全
- 提供及时发现专有云云平台的安全漏洞并修复（修复漏洞过程不影响业务可用性）的安全服务及技术
- 提供协助用户与外部第三方独立安全监管与审计机构合作，对阿里云专有云进行安全合规与审计评估的服务
- 为用户提供保护云端信息系统的技术手段
- 为用户提供安全审计手段
- 为用户提供数据加密手段
- 为用户提供云盾安全服务

2.2 用户安全责任

用户基于阿里云提供的专有云平台构建自己的云端应用系统，综合运用专有云产品的安全功能、云盾安全产品及服务保护自己的专有云环境。

用户应妥善管理专有云环境中的账户，为每个运维管理人员授予完成运维管理工作需要的最小权限，通过群组授权实现职责分离。同时，通过操作审计服务记录管理控制台操作及OpenAPI调用日志。

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

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

3 安全合规和隐私

阿里云的安全流程机制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，并通过独立的第三方评估验证。至目前为止，阿里云一共获得了海内外十余家机构的认证，是亚洲资质最全的云服务商。

阿里云具备表 *3-1:* 阿里云获得的资质中所列出的资格认证。

表 3-1: 阿里云获得的资质

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

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

3.1 安全合规

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

阿里云面对不同角度、不同行业、不同地区的合规需求，整体合规工作可以划分为以下四类：

管理体系合规

这些合规认证体现了阿里云成熟的管理机制和遵从的行业最佳实践：

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

- 中国CNAS云计算国家标准测试

体系化合规报告

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

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

法务合规

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

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

其它

部分无法通过上述的三种形式展现的合规认证。

阿里云一直致力协助各个地区的监管机构建立和完善标准，分享阿里云的最佳实践。

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

3.2 隐私保护

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

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

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

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

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

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

4 阿里云专有云安全架构

阿里云为专有云设计了多个层面的纵深防御安全体系，包括基础设施安全、云操作系统安全、网络服务安全、云数据库安全、云存储安全、应用安全、大数据计算安全、数据安全、云产品代码安全、安全审计、云平台安全运营服务等云平台层面的安全架构保障；以及账户安全、主机安全、应用安全、数据安全、安全运营等云用户（租户）层面的安全架构保障。

4.1 云平台安全架构

4.1.1 基础设施安全

4.1.1.1 物理安全

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。

4.1.1.2 服务器设备安全

阿里云对专有云物理服务器本身的安全进行加固，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。

主机入侵检测

在服务器设备上部署主机入侵检测系统（HIDS），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。

4.1.1.3 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。

4.1.1.4 基础网络安全

微隔离

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。

网络入侵检测

专有云平台部署网络入侵检测系统，实时发现网络中的异常行为并告警。网络入侵检测系统的功能包括HTTP异常入侵检测、HTTP漏洞发现等。同时，对于部分系统服务进行安全漏洞检测，包括但不限于Redis、MongoDB、MySQL等服务。

4.1.2 云操作系统安全

4.1.2.1 虚拟化安全

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ECS虚拟机实例使用网络连接，阿里云将虚拟机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ECS虚拟机访问。

逃逸检测

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

专有云虚拟化管理程序通过使用高级虚拟机布局算法以防止恶意用户的虚拟机运行在特定物理机上。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

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

4.1.2.2 基础系统服务安全

飞天操作系统

- **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中的数据，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。

- **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。

- **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。

基础设施

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。

4.1.2.3 系统管理和调度安全

专有云平台管理系统采用Docker容器化的部署方式。由阿里云安全专家对云平台管理系统进行SDL安全审核，通过代码审核、线上测试、需求分析、威胁建模的方式，保障云平台管理系统的整体安全性。

4.1.2.4 云服务器安全

宿主机的操作系统

专有云平台云服务器宿主机的操作系统采用阿里云根据云特点定制的、重新增减并进行编译的加固操作系统。同时，对操作系统的安全策略和安全访问上进行了大量的深度加固定制。

实例的操作系统（Guest OS）

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，阿里云强烈建议用户采用安全的方式对ECS实例上的操作系统进行访问和操作。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。

镜像

阿里云基础镜像集成了所有已知的高危漏洞补丁，最大限度防止ECS实例上线后即处于高风险状态。同时，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。

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。

4.1.3 网络服务安全

4.1.3.1 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。

访问控制

负载均衡支持白名单访问控制，通过添加负载均衡监听的访问白名单，仅允许特定的IP地址访问负载均衡服务。

证书管理

针对HTTPS协议，负载均衡提供统一的证书管理服务。证书无需上传到后端ECS实例，解密操作直接在负载均衡上进行，降低后端ECS实例的CPU消耗。

4.1.3.2 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。

4.1.3.3 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。

4.1.3.4 DDoS攻击防御

专有云云盾提供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，保证云平台网络的稳定性。同时，阿里云的DDoS防护系统在防护触发条件上不仅仅依赖流量阈值，还基于网络行为的统计判断，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。

4.1.4 云数据库安全

4.1.4.1 租户层隔离

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。

4.1.4.2 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。

4.1.4.3 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RDS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。

4.1.4.4 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。

4.1.5 云存储安全

4.1.5.1 身份验证

用户可以在专有云控制台中自行创建Access Key。Access Key由AccessKey ID和AccessKey Secret组成：其中ID部分是公开的，用于标识用户身份；Secret部分是私密的，用于用户身份的鉴别。当用户向云存储服务发送请求时，需要首先将发送的请求按照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（验证码包含时间戳，以防止重放攻击）。云存储服务收到请求后，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，云存储服务将拒绝处理这次请求，并返回HTTP 403错误。

4.1.5.2 访问控制

对云存储服务的资源访问分为拥有者访问和第三方用户访问：拥有者是指存储空间（bucket）的拥有者，第三方用户是指访问该bucket资源的其他用户。访问方式分为匿名访问和带签名访问：如果请求中没有携带任何与身份相关的信息即为匿名访问；带签名访问是指按照云存储服务API规定在请求头部或者在请求URL中携带签名的相关信息的请求。

4.1.5.3 租户层隔离

云存储服务将用户数据切片，按照一定规则离散地存储在分布式文件系统中，并且将用户数据和数据索引分离存储。云存储服务的用户认证采用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。在用户通过验证后，再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。

4.1.6 应用安全

专有云平台针对中间件应用和平台应用安全应采用Web应用防火墙（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，保障中间件应用和平台应用的安全性。

同时，阿里云安全专家对专有云平台的中间件应用和平台应用进行SDL安全审核、以及持续化的红蓝军对抗，保障中间件和平台应用的安全。

4.1.7 大数据计算安全

4.1.7.1 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。

4.1.7.2 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。

4.1.7.3 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。

4.1.8 数据安全

4.1.8.1 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理管控，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。

4.1.8.2 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。

4.1.8.3 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。

4.1.8.4 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。

4.1.8.5 镜像管理

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。

4.1.8.6 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。

4.1.8.7 运维数据安全

运维人员未经用户许可，不得以任意方式访问用户未经公开的数据内容。

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。

4.1.9 云产品代码安全

在云产品安全生命周期（SPLC）中，阿里云安全专家在各个开发节点中都进行严格审核并评估代码的安全性，保障阿里云提供给用户的产品的代码安全。

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。

4.1.10 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。

4.1.11 云平台安全运营服务

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。

云产品安全策略梳理以及加固

针对云平台的系统、产品默认安全策略等进行安全梳理和加固。

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。

4.2 云用户（租户）侧安全

专有云在用户侧安全提供了多个层面的安全保障，其中包括了账户安全、主机安全、应用安全、数据安全、云盾、安全运营服务、以及安全最佳实践。

4.2.1 账户安全

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。

4.2.2 主机安全

入侵检测

专有云平台用户可以通过在主机上配置云盾安骑士客户端，实现与云盾安全中心的联动防护，获取入侵检测的安全能力。主机的入侵检测包括异地登录提醒、识别暴力破解攻击、网站后门查杀、主机异常检测等功能。

漏洞管理

专有云平台用户可以通过在主机上配置云盾安骑士客户端，实现与云盾安全中心的联动防护，获取漏洞管理的安全能力。主机的漏洞管理综合了多套扫描引擎（网络端、本地端、PoC验证），全面批量检测出系统存在的所有漏洞，并提供一键修复、生成修复命令、一键批量验证功能，实现漏洞管理的闭环。

镜像加固

镜像是云服务器 ECS 虚拟机实例运行环境的模板，一般包括操作系统和预装的软件。ECS租户可以使用镜像创建新的ECS实例或更换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。同时，阿里云保持对基础镜像操作系统漏洞以及三方软件漏洞的实时监测，确保所有阿里云提供的基础镜像的高危漏洞在第一时间得到修复。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。

4.2.3 应用安全

Web应用防护

通过Web应用防火墙，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，保障网站应用的安全与可用性。

代码安全

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

4.2.4 数据安全

对于用户云平台上的数据安全进行保护，包括数据脱敏、数据发现、数据水印等：

- **数据发现**是数据安全的基础，通过数据发现来发现敏感的数据，并且根据数据类型进行自定义化的数据安全控制；数据发现主要包括身份证、手机号、银行卡号、家庭地址等敏感信息。
- **数据脱敏**主要解决敏感数据的脱敏操作，把原始数据转化成可以特定格式但是没有特殊含义的数据。
- **数据水印**是将数据库的数据通过增加伪行和伪列的形式插入到原始数据中，一旦发生大规模窃取的情况下，可以进行溯源操作。伪行和伪列的数据都是模拟的真实数据，黑客无法通过肉眼来进行数据的辨别以及伪行、伪列的数据删除以及数据水印的清除操作。

4.2.5 安全产品（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。

云盾由流量安全监控、主机入侵检测、安骑士、安全审计、DDoS流量清洗、Web应用防火墙、云防火墙、堡垒机、数据库审计、数据发现与脱敏、态势感知等功能组成，结合阿里云专业的安全运营服务为云用户提供了入侵防御、安全审计、态势感知和集中管控等一站式安全保障。

4.2.6 安全运营服务

阿里云提供对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。

4.2.7 安全最佳实践

为保障租户业务安全，租户在迁移上云时应将之前的安全策略一同迁移，并结合以下安全配置最佳实践：

- **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 账号安全

5.1.1 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。

云账户是阿里云资源归属、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。

5.1.2 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。

5.1.3 身份凭证（Credential）

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。

5.2 运维权限管理（OAM）

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。

5.2.1 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。

5.2.2 OAM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。

5.3 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**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** > **集群管理**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** > **Service** > **运维**中的服务信息并执行该节点下的相关操作。

5.4 访问控制RAM

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。

5.4.1 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（EMR/MTS/...）关联，与外部实体身份（如企业本地账号）关联。

5.4.2 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。

5.4.3 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）。

5.5 云服务器ECS

5.5.1 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*。

5.5.2 鉴权认证

5.5.2.1 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（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。

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。ECSD通过使用 Access Key ID 和 Access Key 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 Access Key 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 Access Key ID 用于标识访问者的身份；Access Key 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，只有阿里云和用户知道。

5.5.2.2 权限控制

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Access Key，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，只有在获得显式授权的条件下RAM 用户才能代表云账户进行资源操作。

使用RAM，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、访问时间段、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。

5.5.2.3 RAM和STS支持

RAM 是阿里云提供的资源访问控制服务。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、CreatInstance 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 Access Key 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。

5.5.3 数据安全

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。

5.5.3.1 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

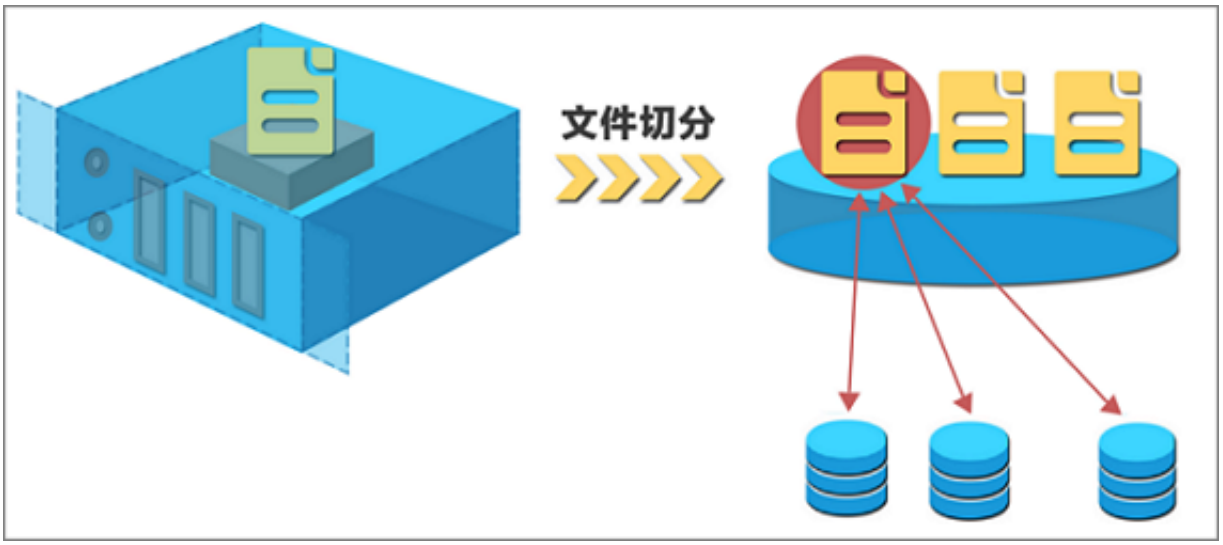
个Chunk，都会复制出3个副本，并将这些副本按照一定的策略存放在集群中的不同节点上，保证用户数据的可靠。

在专有云数据存储系统中，有3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3份副本的存放位置。
3. Client根据Master返回的结果，向对应的3个Chunk Server发出写请求。
4. 如果3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、电源供电情况以及机器负载情况。尽量保证一个Chunk的3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3。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3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3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。

5.5.3.2 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，无需做额外的加解密操作，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）。

加解密是在ECS实例所在的宿主机上进行的，对从ECS实例传输到云盘的数据进行加密。

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

5.5.4 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。

5.5.5 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和诊断安全状况。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。

5.5.6 其他安全能力

支持块存储

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。

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。

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。

5.6 容器服务

容器服务企业版（Docker EE）是一种高性能可伸缩的容器管理服务，支持在一组阿里云云服务器上通过Docker 容器来运行或编排应用。

容器服务免去了用户对容器管理集群的搭建，整合了负载均衡、专有网络等云产品，让用户可以通过云控制台或简单的API（兼容Docker API）进行容器生命周期管理。

5.6.1 信息加密传输

用户集群

用户VM上的证书权限限制在Cluster级别以内，区分为Agent（host） client证书和Service client证书，这些证书在虚拟机初始化的时候传入。整个初始化流程的控制链路通过HTTPS进行校验，证书中间过程不落地。

- Agent证书：用于tunnel agent向tunnel server传输的注册请求，约束范围为host。
- Service证书：用于haproxy和skydns向Etcd传输的只读请求，约束范围为cluster。

ACS共享服务（Tunnel Server/Etcd）

Tunnel Server配置region server证书，用于验证 Tunnel Agent和Swarm Master之间的请求。
Etcd配置region server证书，用于验证Swarm Master、Region Controller、ACS Agent的请求。

ACS集群控制（RegionController/Swarm Master）

RegionController配置region server证书，用于验证Provision Service的请求。

Swarm Master配置每个cluster独立的server证书，用于验证Portal和用户Docker CLI的请求。

5.6.2 证书密钥管理

对于容器应用，传统的秘密分发方式（例如将秘钥存放在容器镜像中，或是利用环境变量、volume动态挂载方式动态传入）都存在着潜在的安全风险。阿里云容器服务通过Docker Secret有效解决这个风险。

5.6.3 漏洞扫描

支持针对容器的镜像进行CVE漏洞扫描等操作。

5.7 弹性伸缩

5.7.1 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。

5.7.2 鉴权认证

5.7.2.1 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，用于用户身份的鉴别。

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 Access Key ID 和 Access Key Secret 对称加密的方法来验证请求的发送者身份。

Access Key ID 和 Access Key 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Access Key ID 用于标识访问者的身份，而Access Key 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，只有阿里云和用户知道。

5.7.2.2 RAM支持

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。

5.7.3 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。

5.8 对象存储OSS

5.8.1 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。

5.8.2 鉴权认证

5.8.2.1 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。

5.8.2.2 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：
用户新创建一个bucket时，如果不指定bucket权限，OSS会自动为该bucket设置private权限。

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

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

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。

5.8.2.3 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。

5.8.3 数据安全

数据在客户端和服务器之间传输时有可能会出错。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。

5.8.4 传输加密

5.8.4.1 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。

5.8.4.2 客户端加密

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。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。

5.8.4.3 KMS加密

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。

5.8.5 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。

5.8.6 防盗链

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

5.9 表格存储TableStore

5.9.1 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。

5.9.2 鉴权认证

5.9.2.1 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。

5.9.2.2 VPC 访问控制

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。

5.9.2.3 RAM和STS支持

表格存储已经接入 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。

表格存储支持的授权粒度到表级别及 API 级别。

5.9.3 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系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。

5.10 文件存储NAS

5.10.1 安全隔离

NAS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。NAS采用多种认证技术，在用户建立连接以及每个请求前，进行权限检查，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。

5.10.2 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（读写且不限制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 5-1: 权限组属性

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

RAM支持

NAS 接入了 RAM 服务，支持控制台设置 RAM，主子账号授权。

通过RAM，用户可以授权子用户对文件存储NAS的操作权限。

表 5-2: 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
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

5.10.3 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。

5.10.4 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。

5.11 分布式文件系统

5.11.1 安全隔离

网络隔离

DFS 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 DFS 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。

DFS 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。

5.11.2 鉴权认证

权限控制

DFS 支持 HDFS 系统标准的目录/文件权限操作，并支持用户/组的读/写权限。

DFS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，DFS 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：

表 5-3: 权限组属性

属性	取值	含义
授权地址	单个IP地址或网段（经典网络类型只支持单个IP）	本条规则的授权对象。
读写权限	只读、读写	允许授权对象对文件系统进行只读操作或读写操作。
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。

RAM支持

DFS 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分布式文件存储 DFS 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 DFS。

表 5-4: RAM 中可授权的分布式文件存储 DFS 操作列表

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

操作（Action）	说明
ModifyMountTargetAccessGroup	修改挂载点权限组
ModifyAccessGroup	修改权限组
ModifyAccessRule	修改权限组规则

5.11.3 数据安全

数据多副本存储

DFS 中存储的数据分为两部分：元数据和用户数据。DFS 通过多副本存储方式保证这两种数据的安全。

- 元数据：DFS 用户进行 IO 操作时，相关操作会传递到服务端。DFS 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：DFS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。

5.11.4 日志审计

DFS 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。

DFS 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。

5.12 云数据库RDS版

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

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

- **网络**：IP 白名单、VPC 网络
- **存储**：自动备份

5.12.1 安全隔离

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。

VPC专有网络

除了IP白名单外，RDS还支持您使用VPC来获取更高程度的网络访问控制。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白名单将极大程度提升RDS实例的安全性。

5.12.2 鉴权认证

5.12.2.1 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（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。

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Access Key ID和Access Key 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Access Key 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，Access Key ID用于标识访问者的身份，

Access Key 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，只有阿里云和用户知道。

5.12.2.2 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。

5.12.2.3 RAM和STS支持

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中子您。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。

5.12.3 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。您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，分别为数据备份和日志备份。

5.12.4 传输加密

5.12.4.1 SSL

RDS提供MySQL和SQL Server的安全套接层协议（Secure Sockets Layer，简称SSL）。您可以使用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，从而可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，以便用户按需更替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。

5.12.4.2 TDE

RDS提供MySQL和SQL Server的透明数据加密（Transparent Data Encryption，简称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OSS、归档存储OAS）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，秘钥长度为128比特。秘钥由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秘钥。您可以自行通过KMS控制台对秘钥进行更替。

5.12.5 日志审计

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。

5.12.6 IP白名单

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，因此不会影响您的使用。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。

5.12.7 软件升级

RDS会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。

5.12.8 防DDoS攻击

当您使用外网连接和访问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，会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

  只针对外网流入流量进行清洗，处于流量清洗状态的RDS实例可正常访问。

  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：

  — PPS（Package Per Second）达到3万；

  — 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

  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。黑洞处理是保证RDS整体服务可用性的一种手段。

  黑洞触发条件如下：

  — BPS（Bits Per Second）达到2GB；

  — 流量清洗无效。

  黑洞结束条件为：黑洞在2.5小时后自动解除。

5.13 云数据库Redis版

5.13.1 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。

5.13.2 访问控制

数据库账号

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

IP 白名单

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

默认情况下，云数据库Redis版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。

5.13.3 网络隔离

针对不同的网络环境，阿里云提供了不同的网络隔离策略。

VPC专有网络

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数据包隔离，在数据链路层完成访问控制。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。

Internet

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。

5.13.4 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。云数据库Redis版支持基于备份集数据恢复实例。

5.13.5 RAM和STS支持

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Redis版支持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。

5.13.6 软件升级

- 云数据库Redis版定期提供数据库软件的新版本。
- 版本升级是非强制性的，只有您主动要求，才会升级到指定版本。
- 当云数据库Redis版团队评估您的版本存在重大安全隐患时，会主动通知业务安排时间进行升级。云数据库Redis版团队将会全程支持进行升级过程。
- 云数据库Redis版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。

5.13.7 数据传输加密

云数据库Redis版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，以便用户按需更替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。

5.14 云数据库MongoDB版

云数据库MongoDB版完全兼容MongoDB协议，提供稳定可靠、弹性伸缩的数据库服务。为用户提供容灾、备份、恢复、监控、报警等方面的全套数据库解决方案。

云数据库 MongoDB版默认部署三节点副本集架构，主节点（Primary）支持读写访问，其中一个备节点（Secondary）提供日常只读操作，另外一个备节点（Hidden）用于高可用保障。

云数据MongoDB版从多个角度提供方案来保障服务安全可靠，包括但不限于：

- 访问控制
- 网络隔离
- 数据备份

5.14.1 安全隔离

VPC专有网络

云数据库 MongoDB版支持用户使用VPC来获取更高程度的网络隔离。

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。

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。

5.14.2 鉴权认证

5.14.2.1 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（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Access Key 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Access Key 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Access Key ID用于标识访

问者的身份；Access Key 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，只有阿里云和用户知道。

5.14.2.2 权限控制

数据库账号

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。

5.14.2.3 RAM和STS支持

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，您可以将云账户下MongoDB资源的访问及管理权限授予RAM中子您。

5.14.3 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，解决99.99%以上的系统故障，以保证数据的完整可靠。

用户可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用户将数据恢复到备份存储周期内的任意一个秒级时间点。

5.14.4 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客户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。

5.14.5 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。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MongoDB实例，因此不会影响用户的使用。

5.14.6 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。

5.15 云数据库Memcache版

5.15.1 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。

5.15.2 访问控制

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。

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。

5.15.3 网络隔离

针对不同的网络环境，阿里云提供了不同的网络隔离策略。

VPC专有网络

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数据包隔离，在数据链路层完成访问控制。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。

Internet

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。

5.15.4 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。Memcache支持基于备份集数据恢复实例。

5.15.5 RAM和STS支持

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。

5.15.6 软件升级

- 云数据库Memcache版定期提供数据库软件的新版本。
- 版本升级是非强制性的，只有您主动要求，才会升级到指定版本。

- 当云数据库Memcache版团队评估您的版本存在重大安全隐患时，会主动通知业务安排时间进行升级。云数据库Memcache版团队将会全程支持进行升级过程。
- 云数据库Memcache版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。

5.16 HybridDB for MySQL

5.16.1 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。

5.16.2 主备节点

HybridDB for MySQL实例的数据节点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，HybridDB for MySQL能够根据备份策略按备份集恢复，提高了数据的可回溯性。

5.16.3 访问控制

数据库账号

当用户创建实例时，HybridDB for MySQL需要指定一个超级账户。初始化后，用户还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Grant语句进行授权。

IP白名单

默认情况下，HybridDB for MySQL 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。更新IP 白名单无需重启HybridDB for MySQL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。

5.16.4 网络隔离

针对不同的网络环境，阿里云提供了不同的网络隔离策略。

VPC专有网络

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数据包隔离，在数据链路层完成访问控制。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。

Internet

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。

5.16.5 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。HybridDB for MySQL支持基于备份集数据恢复实例。

5.16.6 RAM和STS支持

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。

HybridDB for MySQL支持RAM服务和STS服务。通过RAM服务，用户可以将云账户下的HybridDB for MySQL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。

5.16.7 软件升级

- 云数据库HybridDB for MySQL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HybridDB for MySQL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HybridDB for MySQL团队将会全程支持进行升级过程。

- 云数据库HybridDB for MySQL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。

5.17 HybridDB for PostgreSQL

5.17.1 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。

5.17.2 主备节点

HybridDB 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，HybridDB 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。

5.17.3 访问控制

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。

IP白名单

默认情况下，HybridDB 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HybridDB 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。

5.17.4 网络隔离

针对不同的网络环境，阿里云提供了不同的网络隔离策略。

VPC专有网络

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数据包隔离，在数据链路层完成访问控制。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。

Internet

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。

5.17.5 SQL审计

HybridDB 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HybridDB 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、执行时间点等信息。

5.17.6 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。HybridDB for PostgreSQL支持基于备份集数据恢复实例。

5.17.7 RAM和STS支持

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。

HybridDB 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HybridDB 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。

5.17.8 软件升级

- 云数据库HybridDB 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HybridDB 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HybridDB for PostgreSQL团队将会全程支持进行升级过程。
- 云数据库HybridDB 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。

5.18 云数据库OceanBase版

5.18.1 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。

5.18.2 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

5.18.3 数据安全

OceanBase通过以下手段实现网络安全访问控制：

- 登陆账号

  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。

- 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。

5.18.4 传输加密

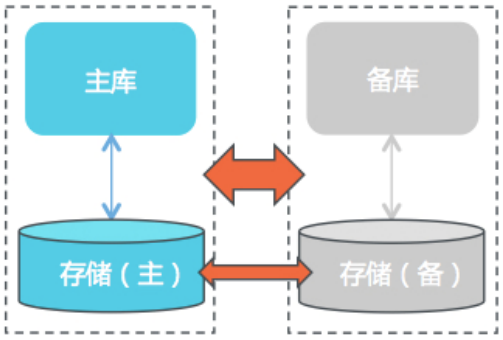
当前版本不涉及。

5.18.5 日志审计

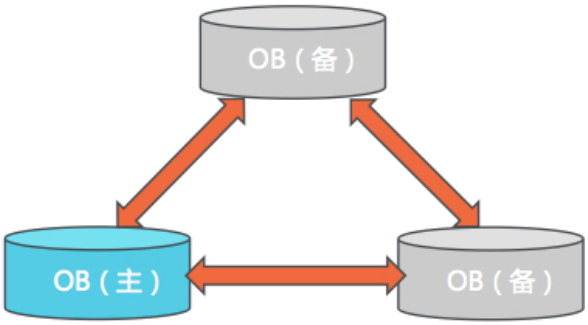
OceanBase提供查看SQL明细功能，您可以审计SQL，及时发现问题。gv$sql_audit记录了所有发往OceanBase的SQL语句，内容包括server IP，访问的数据库名称、执行语句的账号、SQL语句、执行时长、排队时长、执行时间点等信息。

5.18.6 高可用架构

对OceanBase而言，同一数据保存在多台(>=3)台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。



传统关系数据库：主备库



OceanBase：分布式投票

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。

5.18.7 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

5.18.8 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

5.18.9 产品特有的安全能力

无

5.19 数据传输服务DTS

数据传输服务DTS (Data Transmission Service) 支持关系型数据库、及大数据等数据源之间的数据传输。它是一种集数据迁移、数据库增量日志实时订阅及数据实时同步于一体的数据传输服务。

DTS提供了多样化的安全防护策略来保护用户数据，其中包括但不限于：

- 传输安全：支持数据传输加密。
- 存储安全：支持数据加密存储、租户隔离。
- 访问控制：支持RAM账号隔离、HTTPS证书加密。

5.19.1 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，会对传输的日志进行加密。

5.19.2 存储安全

存储数据加密

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。

租户隔离

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等。

5.19.3 访问安全

RAM支持

用户通过云账号创建的DTS实例，为该账户自己拥有的资源。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的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。

HTTPS加密

DTS支持HTTPS加密协议，同时支持HTTPS 证书加密，有效提升用户访问安全。

5.20 数据管理（DMS）

数据管理（Data Management Service，简称DMS）提供关系型数据库和OLAP数据库的统一管理。它源自阿里数据库服务平台iDB，为数万研发人员提供数据库研发支撑，已在线上运行8年。用户可以使用数据管理DMS轻松构建企业独有的数据库DevOps，促进数据库研发自助化，提升研发效率，同时保证员工数据库访问安全及数据库高性能。

数据管理DMS支持MySQL、SQL Server、PostgreSQL、DRDS等关系型数据库和AnalyticDB等OLAP数据库的管理。它是一种集数据管理、结构管理的数据管理服务。

5.20.1 访问控制

- **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。

5.20.2 网络安全

VPC网络支持

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。

5.20.3 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。

5.20.4 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。

5.21 负载均衡SLB

阿里云负载均衡（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。

5.21.1 访问控制

SLB可以屏蔽后端服务器IP地址，对外只提供SLB的服务地址。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。

5.21.2 支持HTTPS协议

SLB提供HTTPS负载均衡功能，转发来自HTTPS协议的请求：

- 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，无须部署在每台ECS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证书和密钥，您上传到证书管理系统的私钥都会加密存储。

5.21.3 RAM和STS支持

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

SLB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。

5.22 专有网络VPC

专有网络（Virtual Private Cloud, VPC）是一个隔离的网络环境，专有网络之间逻辑上彻底隔离。您可以完全掌控自己的专有网络，例如选择IP地址范围、配置路由表和网关等，您可以在自己定义的专有网络中使用阿里云资源如ECS、RDS、SLB等。

5.22.1 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。

5.22.2 网络访问控制

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。

5.22.3 RAM和STS支持

VPC支持RAM服务，您可以将云账号下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。

5.23 日志服务

日志服务（Log Service，简称 LOG）是针对日志类数据的一站式服务，在阿里巴巴集团经历大量大数据场景锤炼而成。您无需开发就能快捷完成日志数据采集、消费、投递以及查询分析等功能，提升运维、运营效率，建立 DT 时代海量日志处理能力。

日志服务通过Logtail客户端、移动端、JS等方式实时采集Event、Binlog、TextLog等多种格式的日志数据，对于采集到服务端的日志数据提供实时消费接口，例如实时检索、日志分析，并根据分析场景和检索结果建立样式丰富的数据报表。

5.23.1 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。

5.23.2 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。

5.23.3 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。

5.23.4 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。

5.23.5 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。

5.24 密钥管理服务KMS

密钥管理服务（Key Management Service，简称KMS）是一款安全易用的管理类服务。用户无需花费大量成本来保护密钥的保密性、完整性和可用性。

借助密钥管理服务，用户可以安全、便捷地使用密钥，从而专注于开发用户真正需要关注的加解密功能场景。

KMS实现了多种严格的安全保护措施来保障用户的数据安全。

5.24.1 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。

5.24.2 鉴权认证

5.24.2.1 身份验证

用户可以在云控制台中自行创建Access Key。Access Key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。

5.24.2.2 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。

5.24.2.3 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。

5.24.3 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。

5.24.4 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。

5.24.5 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 云解析DNS

5.25.1 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，可以创建、管理用户账号，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密码或密匙，按需为用户分配最小权限，从而降低信息安全风险。

专有云DNS会对用户请求进行RAM鉴权操作，通过RAM返回的鉴权结果判定用户此请求是否合法，主账号可以对子账号进行相应的授权操作。

5.25.2 账号数据隔离

身份验证

专有云DNS可以通过对用户的uid和parentid判定用户是否拥有相关数据的操作权限，若此账号和数据属主不存在主子账号关系，则界定账号无权操作。

日志分析

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 企业级分布式应用服务EDAS

企业级分布式应用服务（Enterprise Distributed Application Service，简称EDAS）是企业级互联网架构解决方案的核心产品。

EDAS充分利用阿里云现有资源管理和服务体系，引入中间件成熟的整套分布式计算框架（包括分布式服务化框架、服务治理、运维管控、链路追踪和稳定性组件等），以应用为中心，帮助企业级客户轻松构建并托管分布式应用服务体系。

5.26.1 全链路加密

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EDAS Agent的AK/SK（这里不是EDAS的AK/SK，而是EDAS Agent专用的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 Server和EDAS Agent之间支持IP地址限制。

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。

5.26.2 RAM支持

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。

5.26.3 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的层面，通过IP地址的白名单进行限制；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。

5.26.4 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。

5.26.5 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。

5.27 分布式关系型数据库DRDS

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

5.27.1 访问控制

数据库账号

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@'%'”。

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。

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)
```

5.27.2 网络隔离

除了IP白名单外，DRDS还支持使用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。

5.27.3 慢SQL审计

用户可以在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。用户可以通过DRDS控制台查询到具体的慢 SQL 信息从而进行优化调整。

5.27.4 监控信息

DRDS控制台提供不同维度的监控指标，用户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。

5.28 消息队列MQ铂金版安全

5.28.1 消息队列MQ

消息队列（Message Queue，简称MQ）是阿里云商用的专业消息中间件，是企业级互联网架构的核心产品。基于高可用分布式集群技术，搭建包括消息发布订阅、消息轨迹查询、资源统计、定

时（延时）消息、监控报警等一套完整的消息云服务，帮您实现分布式计算场景中所有异步解耦功能。

消息队列从多个角度提供方案来保障服务安全，包括但不限于：

- 访问控制：资源与账号管理，应用场景可覆盖跨账号资源授权、子账号授权、账户黑名单控制等功能。
- 数据加密：支持传输层安全性协议（TLS）。
- 网络隔离：支持VPC专有网络环境和VPC访问类型切换。
- 日志审计：对接运维监控平台，实时收集操作日志。

5.28.2 访问控制

鉴权

消息队列的安全访问控制包括以下几个要素：

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

消息队列的权限类型包括：

- 发布权限
- 订阅权限

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

消息队列管控平台会对每一次请求进行鉴权和访问控制。除此之外，消息队列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。

账号黑名单

在提供鉴权机制的同时，消息队列提供了“用户黑名单”来实现安全访问控制。

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

授权管理

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

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

授权方式包括以下两种：

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

5.28.3 数据加密

消息队列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，配合消息队列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，虽然消息队列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，对消息队列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。

5.28.4 网络隔离

VPC（专有网络）

消息队列支持用户使用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服务器同时访问消息队列的目的。

同时，消息队列支持多套部署，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。

VPC访问限制

队列提供两种VPC网络访问类型：Any Tunnel和Single Tunnel。当消息队列部署完成时，默认情况下，消息队列服务提供Any Tunnel的访问模式，即在所有的VPC环境都可畅通无阻地使用消息队列服务。这种访问模式能满足大部分的用户需求。用户也可以通过消息队列控制台或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。

5.28.5 日志审计

日志审计是网络安全中非常重要的一环，消息队列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。

5.29 消息队列MQ专业版安全

5.29.1 消息队列MQ

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

消息队列从多个角度提供方案来保障服务安全，包括但不限于：

- 访问控制：资源与账号管理，应用场景可覆盖跨账号资源授权、子账号授权、账户黑名单控制等功能。
- 数据加密：支持传输层安全性协议（TLS）。
- 网络隔离：支持VPC专有网络环境和VPC访问类型切换。
- 日志审计：对接运维监控平台，实时收集操作日志。

5.29.2 访问控制

鉴权

消息队列的安全访问控制包括以下几个要素：

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

消息队列的权限类型包括：

- 发布权限
- 订阅权限

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

消息队列管控平台会对每一次请求进行鉴权和访问控制。除此之外，消息队列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。

账号黑名单

在提供鉴权机制的同时，消息队列提供了“用户黑名单”来实现安全访问控制。

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

授权管理

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

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

授权方式包括以下两种：

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

5.29.3 数据加密

消息队列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，配合消息队列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，虽然消息队列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，对消息队列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。

5.29.4 网络隔离

VPC（专有网络）

消息队列支持用户使用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服务器同时访问消息队列的目的。

同时，消息队列支持多套部署，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。

VPC访问限制

队列提供两种VPC网络访问类型：Any Tunnel和Single Tunnel。当消息队列部署完成时，默认情况下，消息队列服务提供Any Tunnel的访问模式，即在所有的VPC环境都可畅通无阻地使用消息队列服务。这种访问模式能满足大部分的用户需求。用户也可以通过消息队列控制台或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。

5.29.5 日志审计

日志审计是网络安全中非常重要的一环，消息队列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 业务实时监控服务ARMS

业务实时监控服务（Application Real-Time Monitoring Service，简称ARMS）是一款阿里云应用性能管理（APM）类监控产品。借助本产品，您可以基于前端、应用、业务自定义等维度，迅速便捷地为企业构建秒级响应的业务监控能力。

5.30.1 访问控制

鉴权

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

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

1. 用户使用在ARMS控制台上创建的凭证（包含一对AccessKey和SecretKey）。
2. 在访问的时候时，使用ARMS SDK对用户的任何请求进行以下鉴权操作：
   a. 先进行签名验证，确认消息没有被篡改。
   b. 进行鉴权，检查相应的AccessKey是否有权限调用该服务。

HTTPS

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

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

5.30.2 数据隔离

ARMS保障从计算到存储之间用户数据完全隔离。

计算隔离

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

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

存储隔离

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

5.31 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。

5.31.1 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。

5.32 云服务总线CSB

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

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

5.32.1 访问控制

鉴权

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

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

1. 需使用在CSB控制台上创建的凭证（包括一对AccessKey和SecretKey）订购相应的服务。
2. 在访问的时候，CSB SDK对服务调用消息进行相应的签名。在消息到达Broker后，CSB Broker会进行如下鉴权操作：

   a. 进行签名验证，确认消息没有被篡改。

   b. 进行鉴权，检查相应的AccessKey 是否有权限调用该服务。

IP黑白名单

在提供鉴权机制的同时，CSB提供了IP黑白名单来实现网络安全访问控制。

默认情况下，CSB Broker实例被设置为允许任何IP访问。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。

5.32.2 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）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。

5.32.3 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。

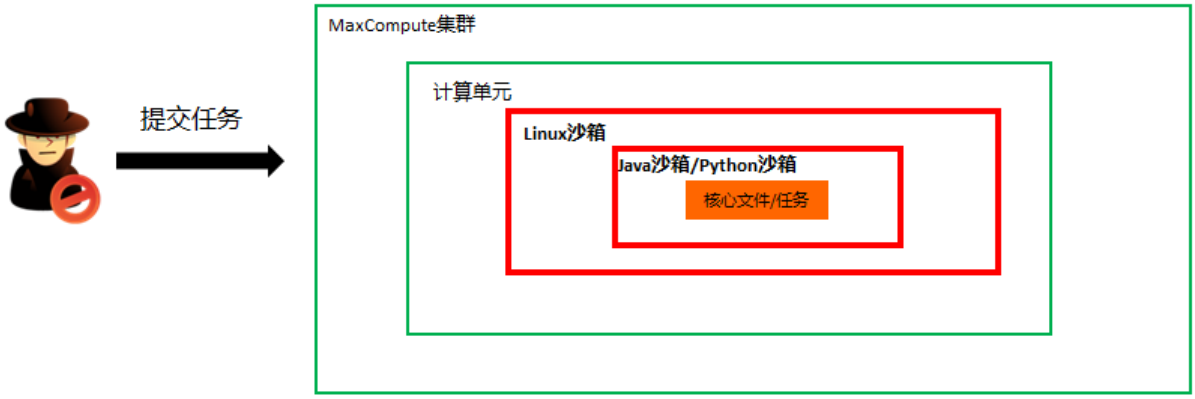
5.33 MaxCompute

5.33.1 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，以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



5.33.2 权鉴认证

5.33.2.1 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。

5.33.2.2 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。

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。只有当主体（用户或角色）存在时，才能进行Policy授权操作。当主体被删除时，通过Policy授权的权限数据会被自动删除。Policy授权使用MaxCompute自定义的一种访问策略语言来进行授权，允许或禁止主体对项目空间对象的访问权限。

两套体系的关系如下表所示：

表 5-5: ACL授权和Policy授权的关系

ACL授权	Policy授权
每次权限管理操作均是对效果（授权、撤销）、对象（如表、资源等）、主体（用户或是角色）、操作（读、写、删除等）的组合描述，例如“允许用户zinan.tang读取表table1中的数据”。	
N/A	支持条件授权，目前支持20种条件操作。

ACL授权	Policy授权
N/A	支持Allow（允许访问）和Deny（拒绝访问）授权。
授权或撤销授权时，对象和主体必须存在。	支持对“不存在”或“不确定”的对象和主体授权，授权时不会验证授权存在性，支持用通配符描述对象或主体。
删除一个对象时，会自动撤销与该对象关联的授权。	删除一个对象时，系统不会自动修改与该对象关联的Policy。
支持经典的Grant/Revoke语句。	通过上传Policy文本描述授权操作。

MaxCompute还支持更多的访问权限控制机制。

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
```

说明：

- 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"
}]
}
```

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道项目空间之外。

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。

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。

5.33.2.3 RAM支持

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。

5.33.3 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。

5.33.4 传输加密

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

5.33.5 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。

5.33.6 访问控制-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NATIP。
- 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。

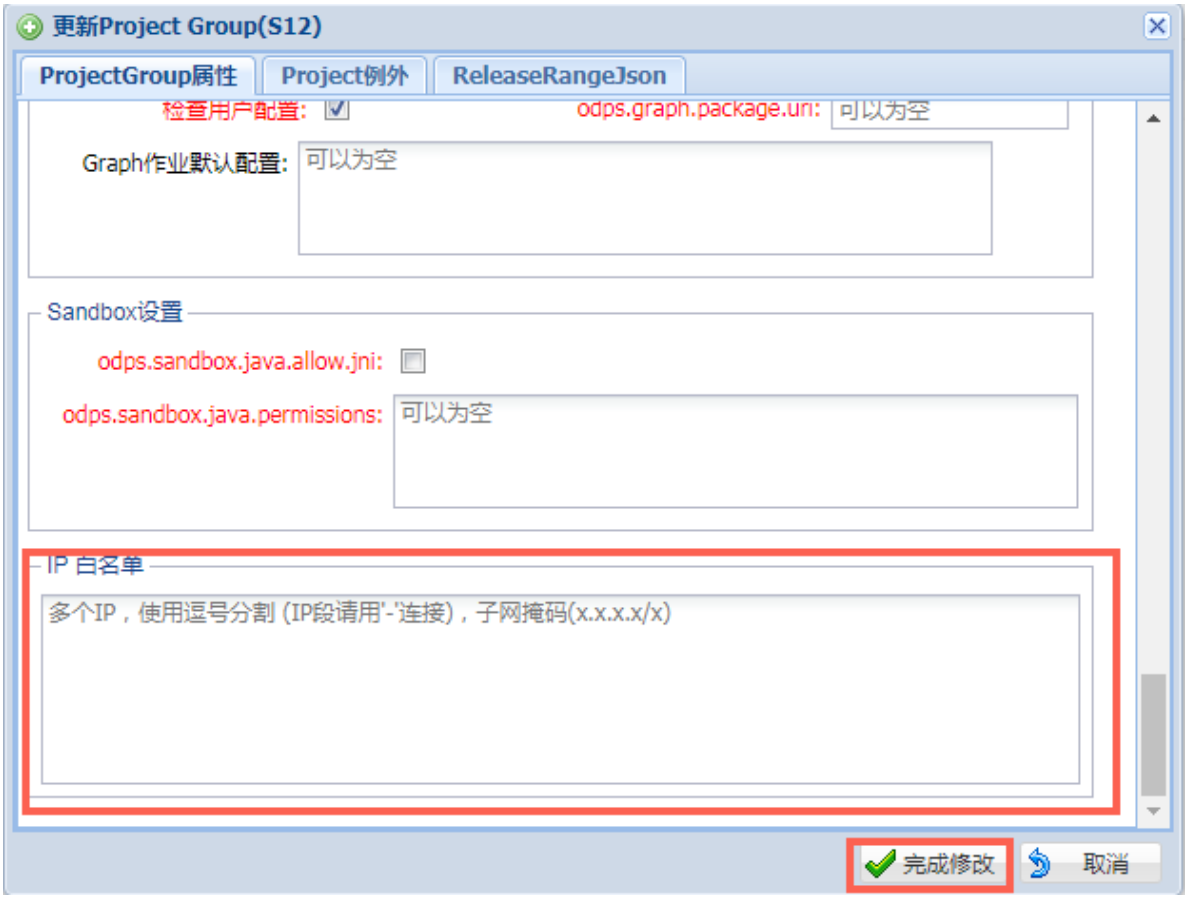
Project group级别IP白名单配置

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 5-4: 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 5-5: Project group级别IP白名单配置2

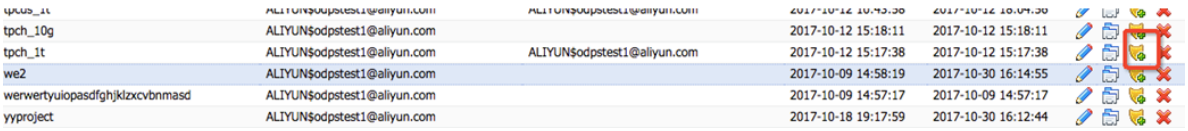
Project级别IP白名单配置

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。

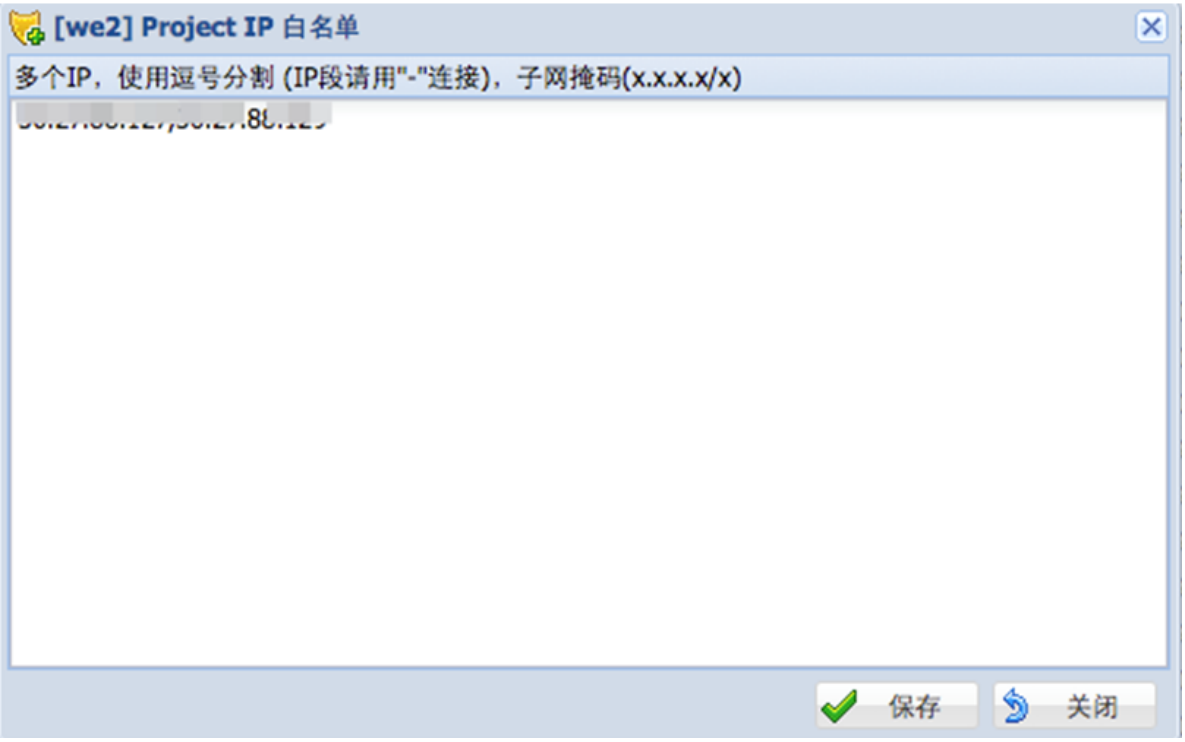
1. 在**AdminConsole**中选择**ODPS配置** > **Project管理**，选中需要配置的project，单击最右侧的IP白名单设置图标。

图 5-6: Project级别IP白名单配置1



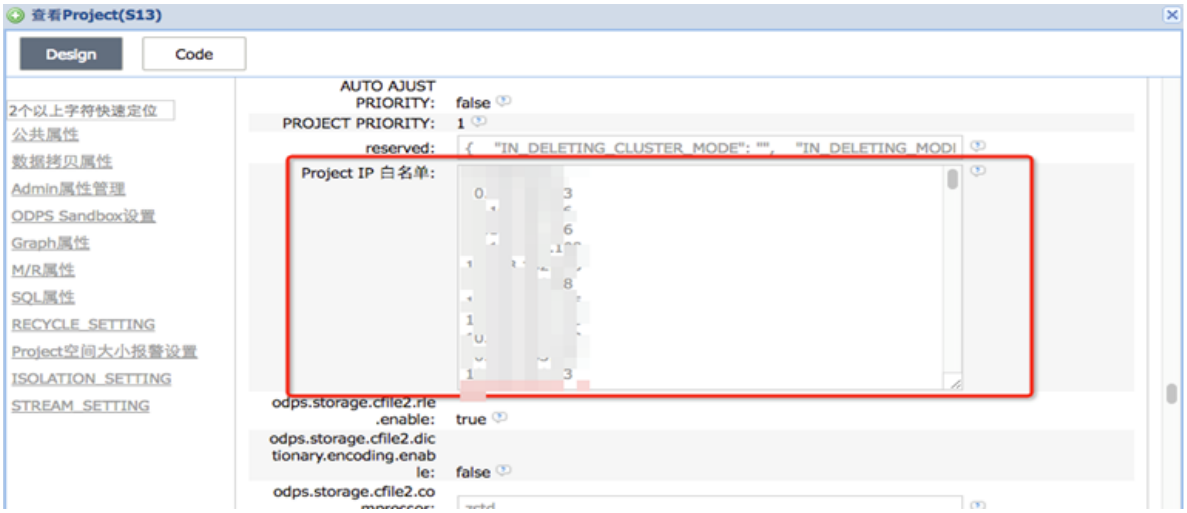
2. 在弹出的配置框中完成相关配置后，单击**保存**。

图 5-7: 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 5-8: Project级别IP白名单配置3



说明：

Project owner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”。

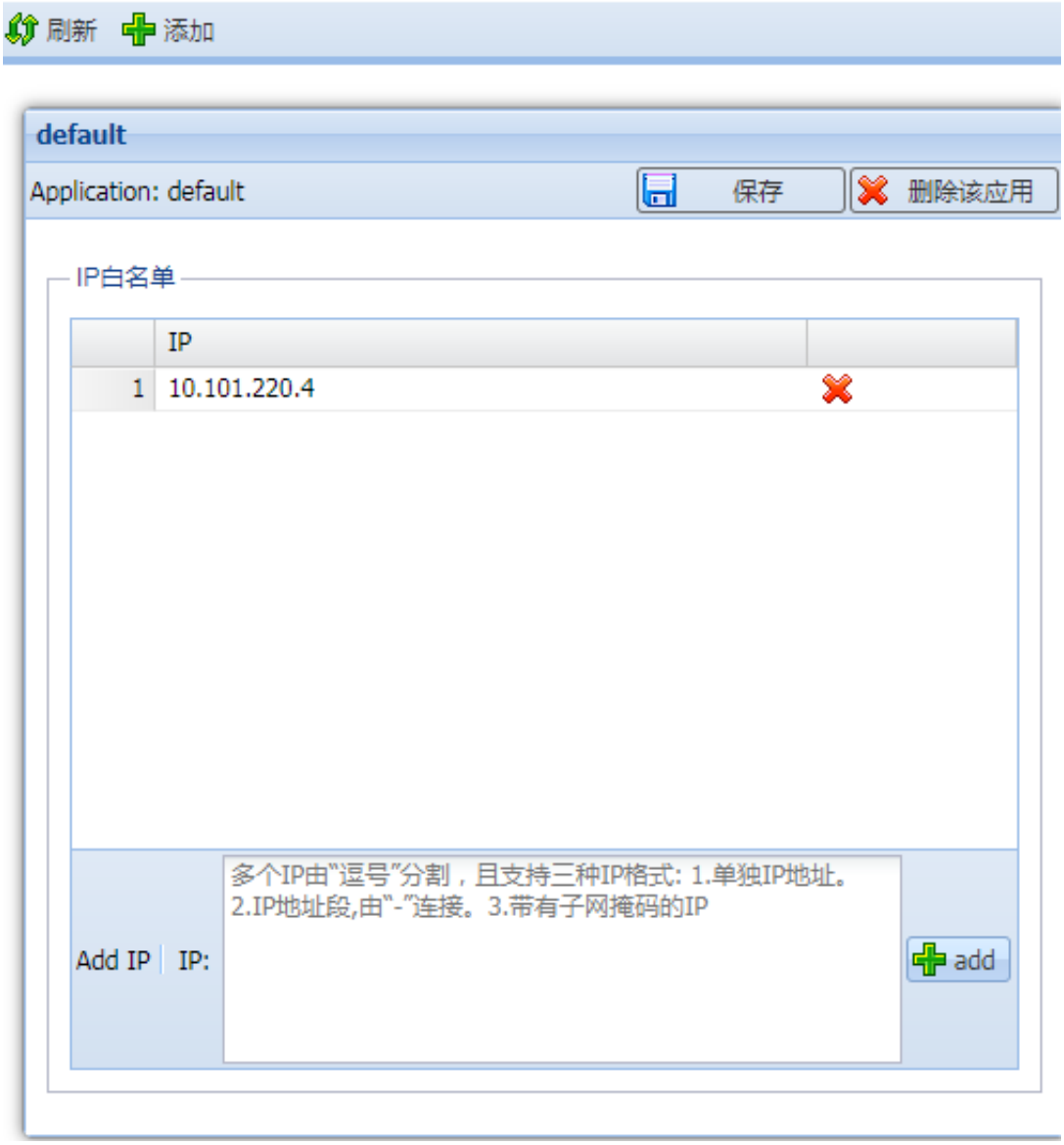
系统级别IP白名单配置

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。

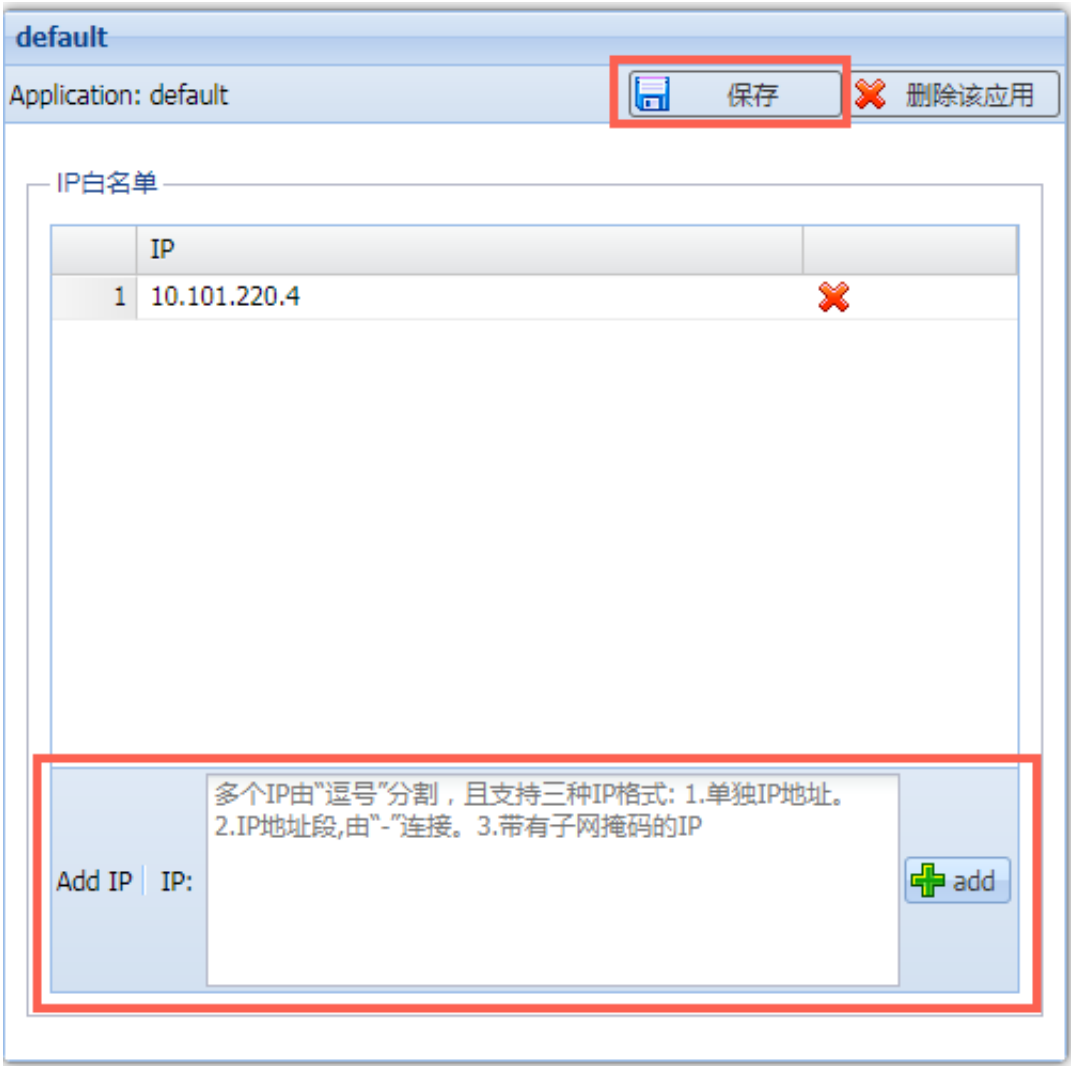
1. 在`AdminConsole`中选择**ODPS配置** > **系统级白名单管理**，默认打开配置框。

图 5-9: 系统级别IP白名单配置1



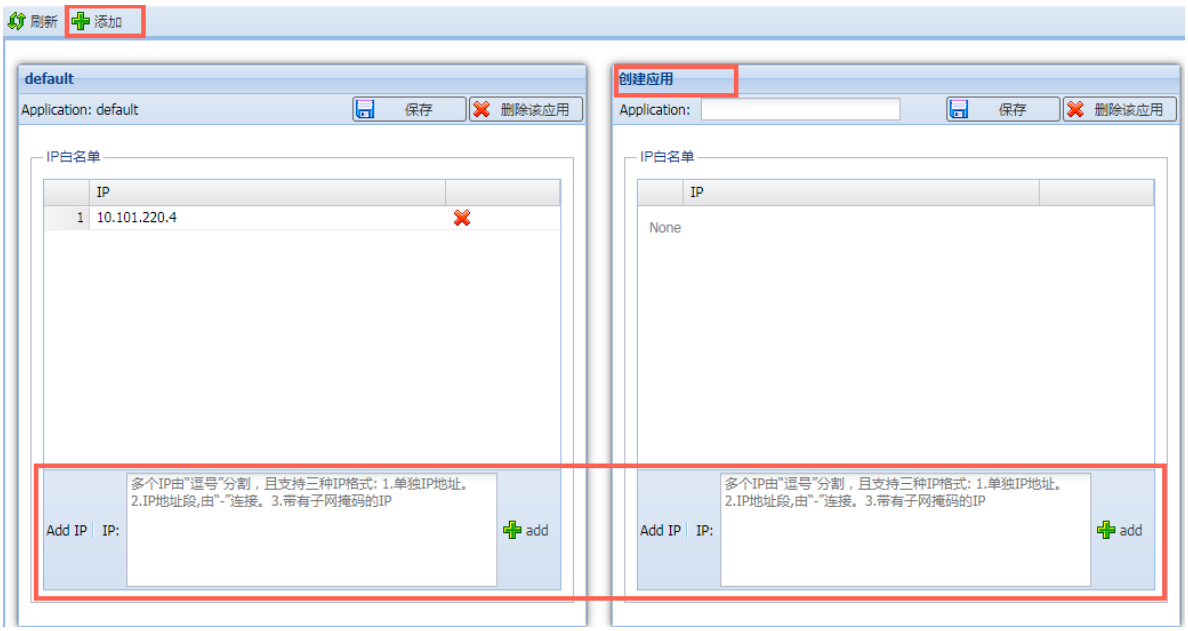
2. 在打开的配置框中完成相关配置后，单击**保存**。

图 5-10: 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 5-11: 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注意需要设置正确的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。

5.33.7 MaxCompute支持VPC

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end point及VIP。
- 经典网络能够访问所有project 。
- 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 。

5.33.8 ElasticSearch on MaxCompute支持VPC

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end point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 分析型数据库

5.34.1 安全隔离

AnalyticDB以数据库作为租户隔离的基本单元，数据库创建者的云账号为数据库的Owner。未经数据库创建者授权，任何其他云账号不能访问该数据库的数据。用户的数据库在自己独享的进程级别实例上运行，从进程级别实现了数据库的隔离。

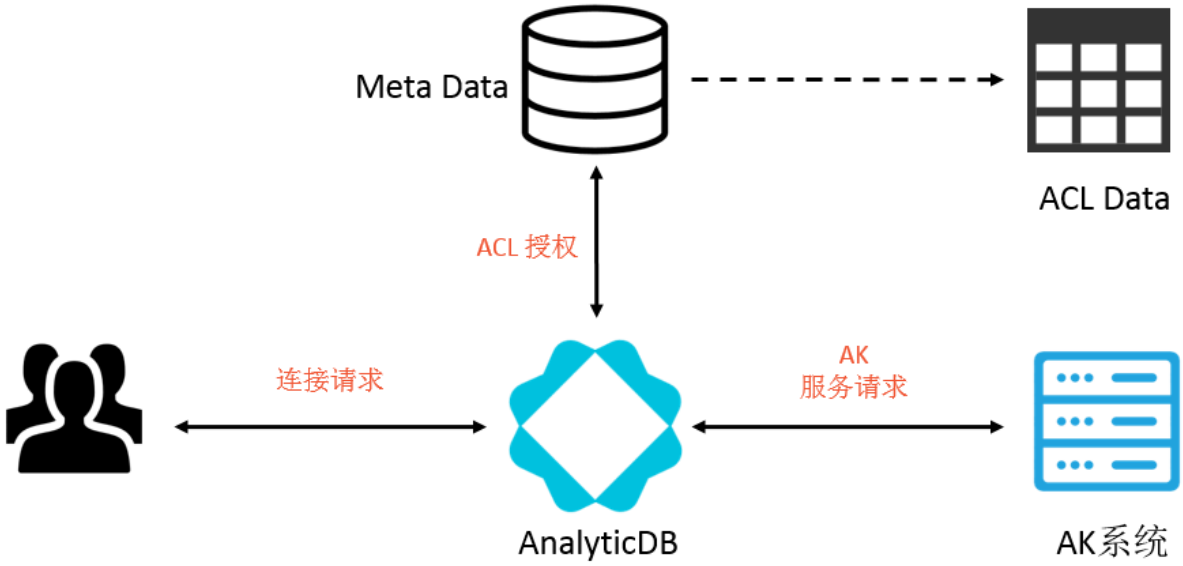
AnalyticDB集群中的每个数据库均采用多租户机制，每个数据库都有完全独立的服务进程。多租户机制对每个数据库的物理资源进行隔离（包括CPU、内存、存储空间），不允许跨数据库的访问。

AnalyticDB可以按数据库进行版本管理、资源扩容/缩容、数据库服务启动/停止。

从用户的访问权限认证角度来讲，每个数据库都有独立的AccessKey。

5.34.2 鉴权认证

AnalyticDB的身份验证和权限控制如下：



5.34.2.1 身份验证

AnalyticDB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，AnalyticDB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账户并进行登录，使用访问Key通过JDBC/ODBC连接数据库服务，通过AK服务请求实现身份认证。

用户可以在Apsara Stack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（相当于用户名）；AccessKeySecret是私密的，用于用户身份的鉴别（相当于密码）。

主账号和子账号均需要使用对应的AccessKey ID和Access Key Secret来访问AnalyticDB数据库。

5.34.2.2 权限控制

AnalyticDB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，AnalyticDB不支持针对用户在host上授权。

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AnalyticDB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AnalyticDB的缓存来加速DML/DDL语句授权。

用户连接到AnalyticDB后，AnalyticDB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。

AnalyticDB中的授权对象如下：

- Database（库）：即 db_name.* 或 * （默认数据库），指定数据库或数据库上所有表/表组。
- TableGroup（表组）：即 db_name.table_group_name 或 table_group_name，指定特定表组。
- Table（表）：即 db_name.table_name 或 table_name，指定特定表。
- Column（列）：语法上由 column_list 和 Table 组成，指定表的特定列。

5.34.2.3 RAM和STS支持

AnalyticDB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。

5.34.3 数据安全

多租户

AnalyticDB提供多租户机制，不同数据库间通过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

AnalyticDB的全量数据保存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，提供数据持久化的高可靠性保证。实时表数据的DML语句（INSERT/DELETE）操作提交成功后，同步保存到飞天分布式文件系统中；对于批量表，数据加载时也全量写入到飞天分布式文件系统。

数据一致性

对于实时表的数据更新操作（INSERT/DELETE），AnalyticDB采用多版本并发控制MVCC（Multi-Version Concurrency Control）机制进行存储，以保证并发数据更新操作时查询所见数据为发起查询时的数据版本。

说明：
对于更新过的历史版本，如果不需要再查询引用，其空间将可定期清理。

5.34.4 日志审计

AnalyticDB支持开启审计日志，开启审计日志后可以记录所有SQL操作记录信息，包括：

- 查询发生时间。
- 客户端IP地址。
- 所执行SQL语句。

您可通过SQL语句可回看客户查看的数据信息。

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=20171010133756010003163108099998380 42\;CLUSTER=ayads-bjyz

5.34.5 VPC支持

AnalyticDB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到Any Tunnel方式。

专有网络VPC可以帮助您基于阿里云构建出一个隔离的网络环境。您可以完全掌控自己的虚拟网络，包括选择自有IP地址范围、配置路由表和网关等。此外您也可以通过专线 、VPN等连接方式将VPC与传统数据中心组成一个按需定制的网络环境，实现应用的平滑迁移上云。

- **Single Tunnel模式**：默认的VPC方式，仅支持在指定的VPC环境中访问并使用AnalyticDB。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来使配置变更生效。Any Tunnel模式下，您可在任意的VPC环境中访问并使用AnalyticDB。Any Tunnel模式无法实现VPC之间的网络隔离。

5.35 关系网络分析

5.35.1 安全隔离

I+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。

5.35.2 鉴权认证

5.35.2.1 身份验证

I+关系网络分析目前在专有云支持两种身份验证：

- I+自己的身份验证：通过I+用户系统创建的用户密码登录，I+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，有效防止了密码泄漏的情况。
- 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。

5.35.2.2 权限控制

I+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。

5.35.3 数据安全

I+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。

5.35.4 传输加密

I+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。

5.35.5 日志审计

I+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。

5.35.6 系统安全

5.35.6.1 漏洞扫描机制

I+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：I+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：I+关系网络分析产品使用到的中间件。
- 代码漏洞扫描：I+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。

5.35.6.2 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，I+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。

5.35.6.3 系统防御机制

I+关系网络分析产品是基于阿里云专有云环境发布的，I+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。

5.35.7 基础设施安全

I+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。

5.35.8 等保认证

I+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。

I+关系网络分析在专有云V3.3版本以后通过https协议访问。

5.36 E-MapReduce

5.36.1 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。

5.36.2 用户认证

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。

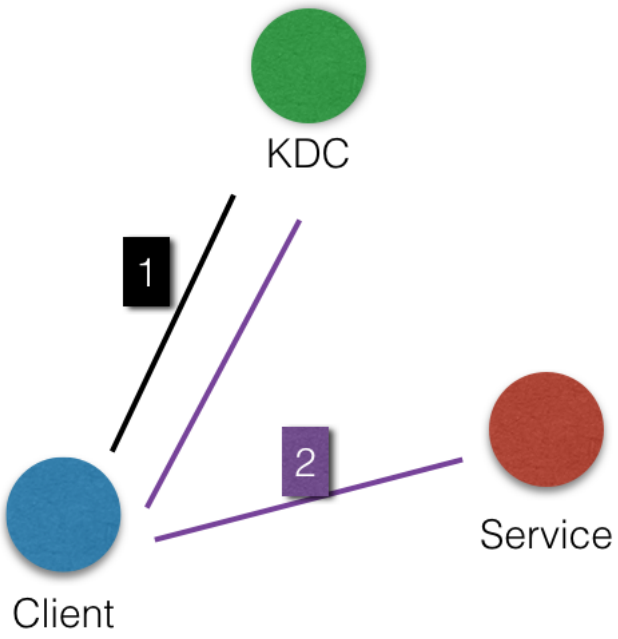
所有组件都可以使用HAS提供的原有Kerberos的认证机制。

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 5-12: 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。

5.36.3 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。

5.36.4 容灾

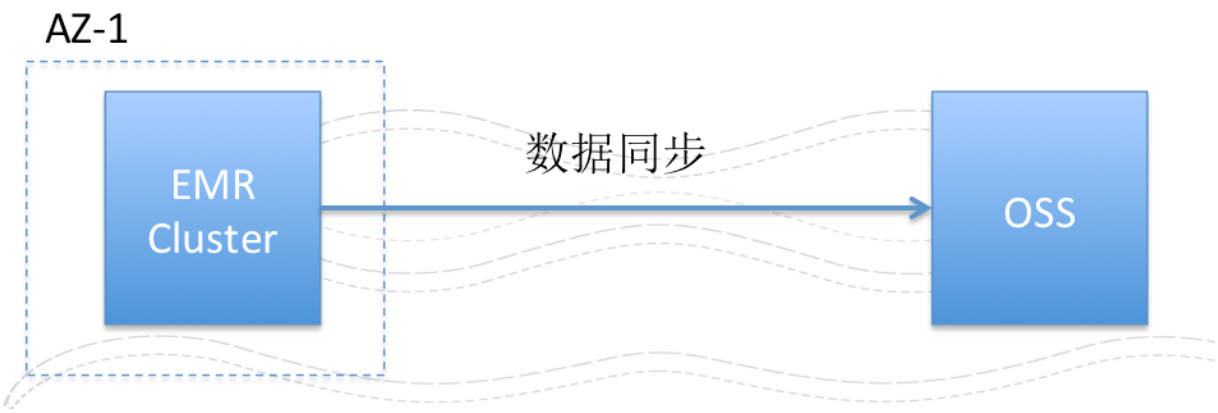
5.36.4.1 数据容灾

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。

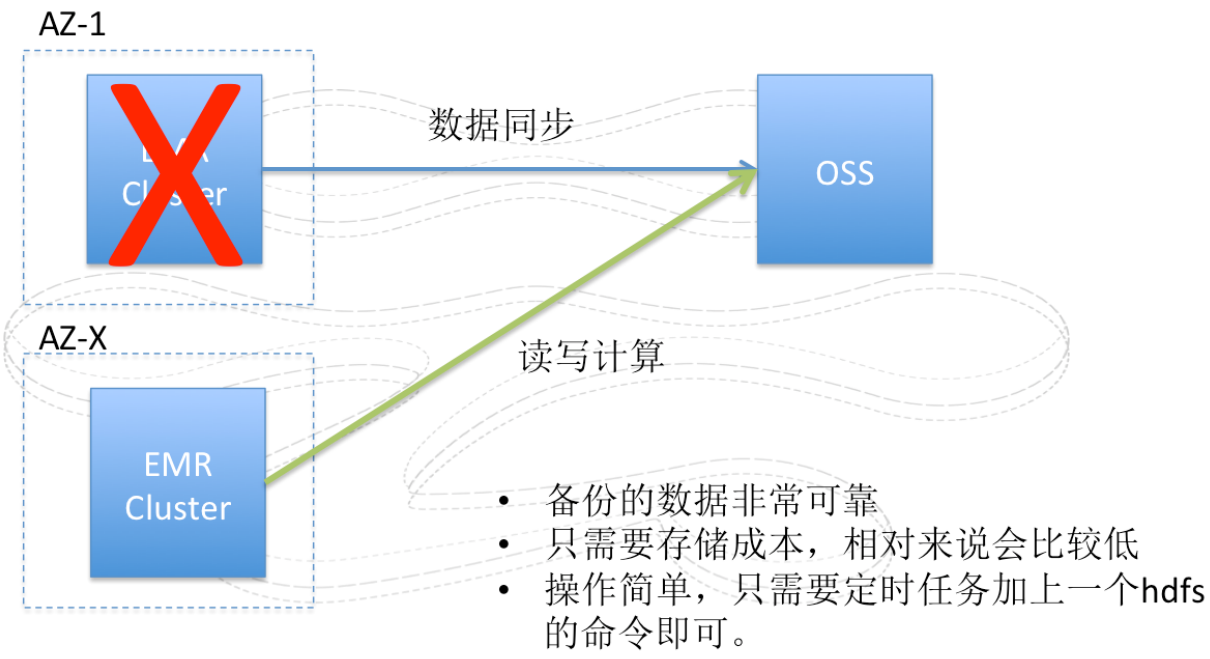
图 5-13: 数据同步



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。

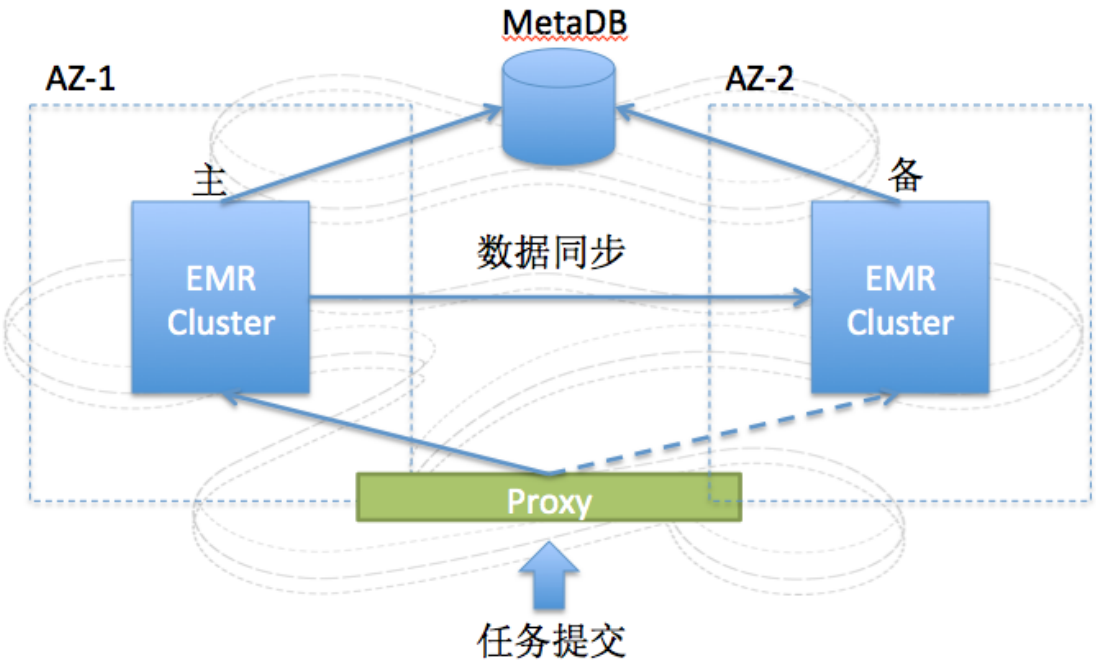
图 5-14: 数据备份



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，如果原集群中还存有元数据的信息，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。

5.36.4.2 服务容灾

图 5-15: 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。

5.37 流计算

5.37.1 账号安全

流计算账号安全

流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。

数据存储账号安全

流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。

5.37.2 业务安全

项目隔离安全

流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。阿里云流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。

业务流程安全

流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，在尽可能不影响用户使用体验基础上，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。用户调试完成后，通过上线任务将作业提交到数据运维系统。此时正在运行的流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。

5.37.3 数据安全

数据安全分为流计算系统数据安全和业务数据安全。

系统数据安全

流计算系统数据安全交由系统本身安全保证，流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，阿里云安全团队为流计算保驾护航。

业务数据安全

流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。

5.38 实时数据分发平台（DataHub）

5.38.1 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。

5.38.2 鉴权认证

5.38.2.1 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。

5.38.2.2 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便用户可以灵活使用。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。

5.38.2.3 RAM和STS支持

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（更多详情可参见DataHub官网的相关文档）。

5.38.3 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。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。

5.38.4 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。

5.38.5 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。

6 专有云云盾

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

6.1 云盾基础版

云盾基础版由流量安全监控、安骑士基础版、主机入侵检测、安全审计功能模块组成。

流量安全监控

流量安全监控模块是阿里云安全自主研发的毫秒（ms）级攻击监控产品。通过对专有云入口镜像流量包的深度解析，实时地检测出各种攻击和异常行为，并与其他防护模块联动防护。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：

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

最佳实践

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

主机入侵检测

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。

主机入侵检测模块提供关键目录完整性检测、异常进程告警、异常端口告警、异常网络连接告警等功能。

最佳实践

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

安骑士基础版

安骑士基础版模块通过日志监控、文件分析、特征扫描等手段，为云服务器提供账号暴力破解防护、网站后门查杀、异地登录报警等安全防护措施。安骑士分为客户端和服务器端。安骑士客户端配合安骑士服务器，监测系统层和应用层的攻击行为，实时发现黑客入侵行为。

安骑士基础版提供网站后门查杀、暴力破解攻击拦截、异地登录告警等功能。

最佳实践

通过安骑士基础版功能及时发现并拦截针对云服务器的暴力破解攻击，保障云服务器主机安全。

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：

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

最佳实践

根据定义的审计策略，管理人员可以及时收到告警邮件。例如，为ECS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 云盾高级版

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

安骑士高级版

安骑士高级版模块通过日志监控、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器端。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。

安骑士高级版包含以下功能：

- **主机漏洞检测和修复**：全面的漏洞管理，包括系统软件CVE漏洞、Windows系统漏洞、Web-CMS漏洞、其它高危漏洞。
- **高危配置基线核查**：主机安全配置全面核查，包括账户安全检测、弱口令检查、数据库安全基线检测、主机配置项风险检测。
- **主机入侵实时检测**：实时检测主机入侵行为，包括异常登录行为、暴力破击拦截、网站后门查杀、异常进程检测。
- **主机资产指纹清点**：主机进程、端口、账号信息批量管理，自主发现异常资产变动。
- **主机全量日志检索**：集中管理主机日志，实时检索定位主机安全问题。

最佳实践

使用安骑士高级版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。

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：

- **DDoS攻击清洗能力**：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，并进行该事件的Top10 主机IP展示。

最佳实践

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

Web应用防火墙

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

WAF的主要功能是将Web流量引流到WAF上，由WAF将流量进行检测、过滤、清洗后再代理转发到应用服务器，完成整个Web应用防护。

WAF包含以下功能：

- **Web应用攻击防护**：防护OWASP常见Web攻击威胁，快速防护0Day漏洞，隐藏网站源站服务器真实地址。
- **缓解恶意CC攻击**：过滤恶意的Bot流量，保障网站服务器性能。
- **HTTP/HTTPS访问控制**：IP访问控制、URL访问控制、基于地理区域的访问封禁，从多维度对访问流量实现精准控制。

最佳实践

- **使用WAF来防止敏感信息泄露**

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

  通过精准访问控制规则有效防御WordPress反射攻击。

云防火墙

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

最佳实践

- **实现微隔离**：通过云防火墙实现精细化的微隔离，通过业务分区、角色分组将原来为了防止业务出现中断而不得不开放的端口进行更精细的管理，缩小受攻击面，降低安全隐患。
- **协助甄别流量是否安全**：例如，HTTP流量是否都已切换为HTTPS的流量，连接TCP 3306（MySQL的业务端口）的流量是否有来自互联网的流量，这些信息，在云防火墙的流量视图中，一目了然。

- **判断服务器变更是否对业务造成影响**：服务器需要迁移和下线时，可以通过云防火墙先观察是否还存在相关流量，从而判断是否可以安全的变更。
- **发现是否存在端口滥用**：不同的业务开发部门，可能导致服务器提供同一服务（相同应用和进程）却使用了不同的业务端口。这样既浪费了端口资源，也不便于运维。通过流量的可视化，云防火墙可以清晰的甄别出此种端口滥用情况。

态势感知

态势感知通过机器学习和数据建模发现潜在的入侵和攻击威胁，从攻击者的角度有效捕捉高级攻击者使用的0Day漏洞攻击、新型病毒攻击事件，以及有效展示正在发生的安全攻击行为，实现业务安全可视和可感知，解决因网络攻击导致数据泄露的问题，并通过溯源服务追踪黑客身份。

- **弱点分析**：基于无状态扫描技术，并与网络流量安全监控联动，结合动态检测和静态匹配两种扫描模式，提供自动化、高性能的精准Web漏洞扫描能力。
- **大数据安全分析平台**：通过机器学习和数据建模发现潜在的入侵和攻击威胁，从攻击者的角度有效捕捉高级攻击者使用的0Day漏洞攻击、新型病毒攻击事件，以及有效展示正在发生的安全攻击行为，实现业务安全可视和可感知，解决因网络攻击导致数据泄露的问题，并通过溯源服务追踪黑客身份。

最佳实践

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

- **弱点扫描**

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

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

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

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

- **日志分析**

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

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

- **大屏实时监控**

  态势感知为用户提供可视化大屏，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。

- **代码外泄感知**

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

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：

- **操作审计**：多方位记录运维人员操作行为，作为事件追溯的保障和事故分析的依据。
- **职权管控**：通过账号管控和权限组管理，分职权实现人员和资产的管理。
- **安全认证**：支持双因子认证机制，防止运维人员身份冒用和复用。
- **高效运维**：从架构、工具、云服务器接入等多方面提升运维效率。

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。

数据库审计

数据库审计支持对云端自建数据库、RDS数据库访问的全面精确审计，以及100%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。

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。

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。

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。