阿里云
专有云Agility版

安全白皮书

产品版本：V1.1.0

文档版本：20180416

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

表 -1: 格式约定

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

目录

1 安全白皮书介绍

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

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

本白皮书介绍了阿里云专有云云安全体系，主要包括下列内容：

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

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

2 安全责任共担

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

阿里云

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

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

用户

用户负责以安全的方式配置和使用云产品，并基于这些云产品以安全可控的方式构建自己的应用。

用户可使用阿里云安全生态中的第三方安全厂商的安全产品为其应用系统提供安全防护。

2.1 阿里云安全责任

阿里云负责分布式云操作系统及云服务产品本身的安全，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

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。

对于专有云提供的服务，例如容器服务、对象存储 OSS，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。

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客户和伙伴提供支持。

其它

部分无法通过上述的三种形式展现的合规认证。

阿里云一直致力协助各个地区的监管机构建立和完善标准，分享阿里云的最佳实践。

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

3.2 隐私保护

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

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

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

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

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

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

4 阿里云安全架构

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

4.1 云平台安全架构

4.1.1 基础设施安全

4.1.1.1 云平台安全架构

阿里云云平台的安全架构主要包括了硬件安全以及云产品开发安全。

4.1.1.2 硬件安全

硬件固件安全

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

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

加密计算

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

可信计算

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

4.1.1.3 云产品开发安全

阿里云为用户提供了多种不同的云产品，并保障这些云产品的开发安全。

云产品安全生命周期（SPLC）

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

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

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

5. **在应用发布阶段**，只有经过安全复核，并且得到安全审批许可后，产品才能通过标准发布系统部署到生产环境，以防止产品携带安全漏洞在生产环境运行。
6. **在应急响应阶段**，安全应急团队会不断监控云平台可能的安全问题，并通过外部渠道（如ASRC等）或者内部渠道（如内部扫描器、安全自测等）得知安全漏洞。在发现漏洞后应急团队会对安全漏洞进行快速评级，确定安全漏洞的紧急度和修复排期，从而合理分配资源，做到快速并合理的修复安全漏洞，保障阿里云用户、自身的安全。

4.1.2 云操作系统安全

4.1.2.1 基础系统服务安全

飞天操作系统

- **盘古安全**

  分布式文件系统（盘古）使用三副本技术，将盘古系统中的数据保存三份。如果其中一份副本丢失，盘古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。

  所有访问盘古系统的操作，必须通过Capability认证，只有携带了允许的Capability才能与盘古系统进行通信，从而解决未经授权访问的操作。

  存储在盘古系统中的数据，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。

- **夸父安全**

  远程过程调用模块（夸父）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。

- **伏羲安全**

  任务调度模块（伏羲）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。

4.1.2.2 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。

4.1.3 云存储安全

4.1.3.1 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。

4.1.3.2 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。

4.1.3.3 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。

4.1.4 数据安全

4.1.4.1 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。

4.1.4.2 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。

4.1.4.3 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。

4.1.4.4 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、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。

4.1.4.5 残留数据清除

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

4.1.4.6 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。

4.1.5 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。

4.1.6 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。

4.1.7 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 云用户侧安全架构

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

4.2.1 账户安全

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 应用安全

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。

4.2.3 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。

5 云产品安全

5.1 容器服务

5.1.1 产品简介

容器服务-专有云Agility版深度整合了Docker套件和阿里云容器服务，是国内唯一具有全商业版支持能力的容器云平台，可以部署在客户自有数据中心，包含从容器的创建到运行以及镜像的全生命周期管理。支持研发运维一体化、云原生应用架构和机器学习等场景，支持混合云管理，允许应用在公共云，和自有数据中心物理机统一部署管理，支持应用无缝迁云、弹性伸缩应对突发流量等场景。此外，容器服务-专有云Agility版提供开放的接口，全面兼容Docker原生API和命令行以及第三方工具，为客户提供敏捷、弹性、开放的容器云平台。

5.1.2 产品安全方案

产品架构设计之初充分考虑了自身的健壮性，包括产品的部署架构安全、核心组件的高可用能力等。

5.1.2.1 高可靠的部署架构

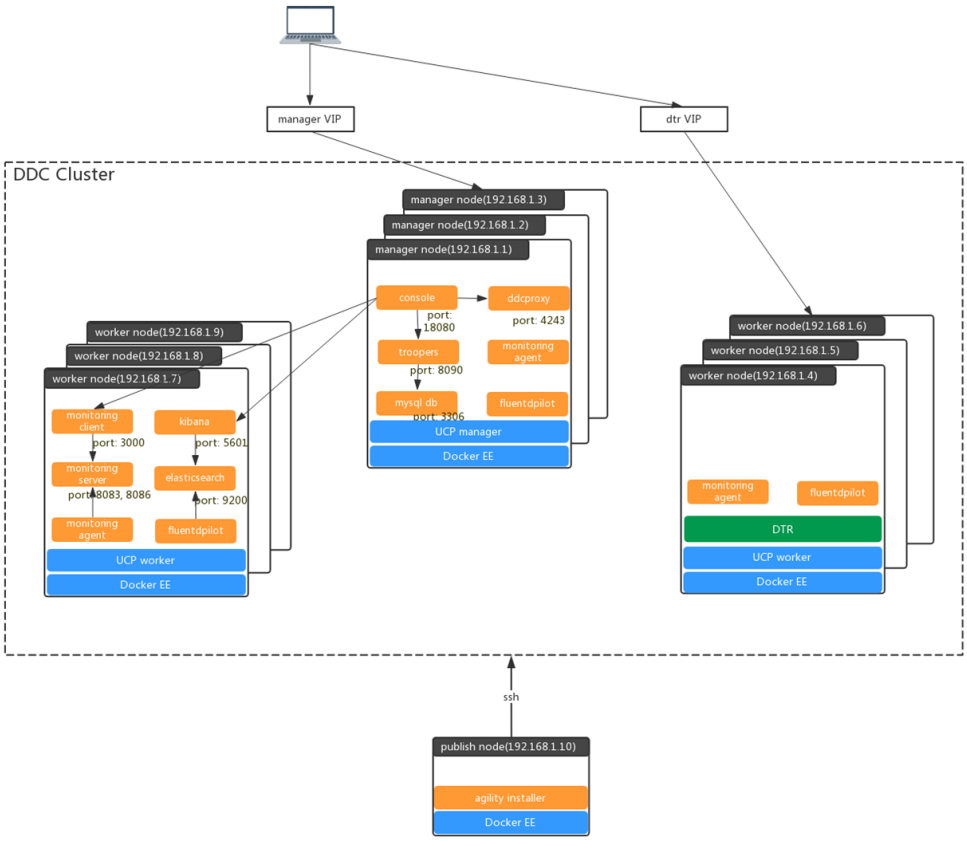
容器服务-专有云Agility版是在Docker UCP的基础架构上进行了深度定制，提供了包含多集群管理、混合云支持、完整的应用生命周期管理等诸多功能的容器云平台。集群可以运行在任何形式的X86环境中，不同的公共云环境、企业IDC机房、物理机以及各种虚拟化环境。

容器云平台包含两种类型的节点：

- **Managers**：管理集群并且持久化集群配置。
- **Workers**：应用工作节点。

其典型的部署架构如下：

图 5-1: 架构图



高可靠的部署架构通过以下方式实现：

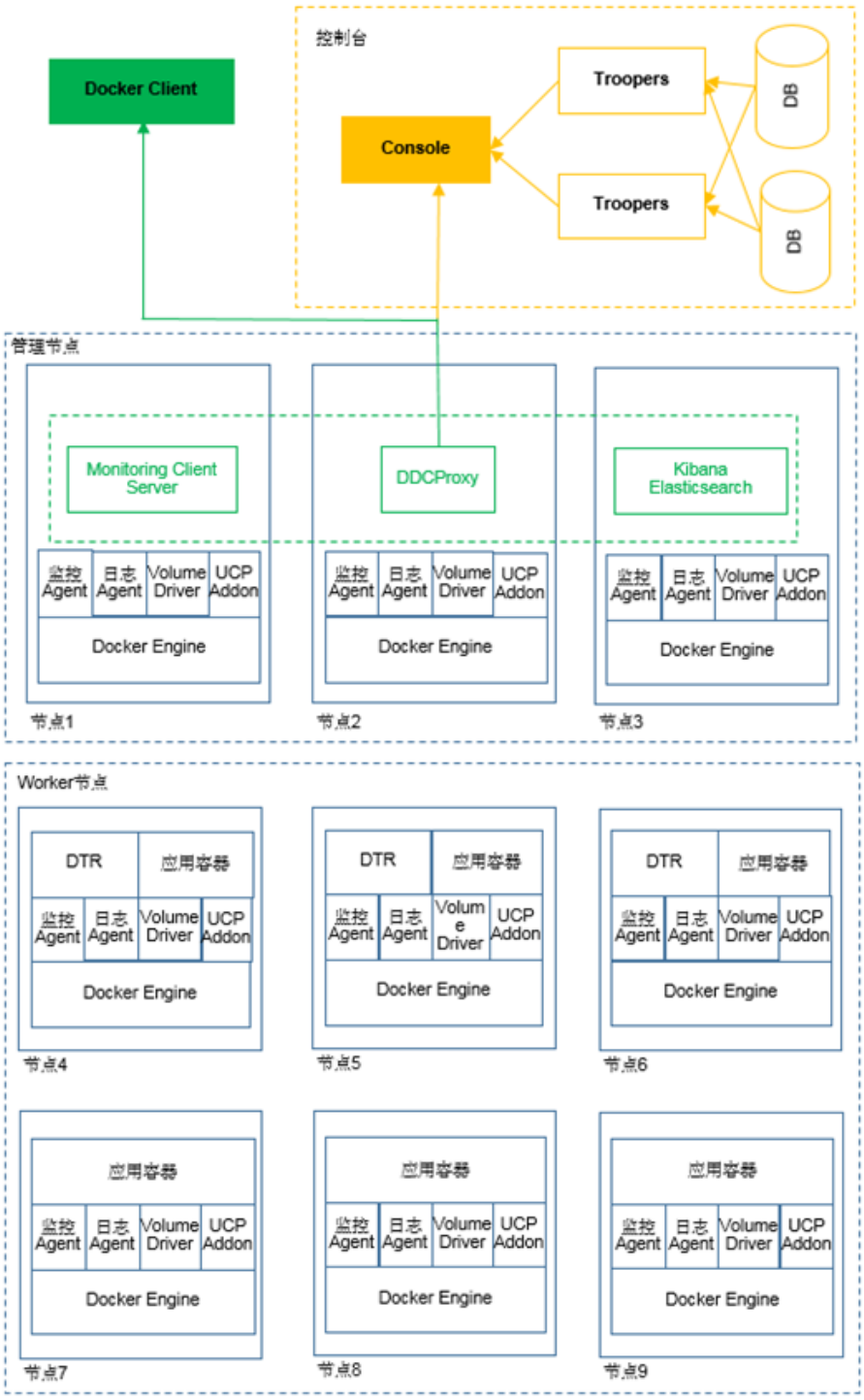
- 多管理节点（至少3个以上），内置RAFT协议，在管理节点异常时选举出新的leader节点，确保管理节点的高可用。
- 集群管理入口绑定到负载均衡，提供负载和高可用能力。
- 管理节点按照可用区、跨机架方式部署，具备异地机房容灾和本地机架容灾能力。
- 镜像仓库后端使用共享存储，为镜像提供高可靠的数据持久化能力。
- 工作节点上的应用可实现故障无缝切换。

5.1.2.2 各组件安全架构设计

5.1.2.2.1 控制台高可用架构

控制台是整个集群的管理入口，由一个Console、两个Troopers权限验证和两个MySQL（Master/Slave高可用）实例组成。

图 5-2: 控制台架构



- **控制台（CONSOLE）**

  控制台提供操作管理平台的界面，也是所有操作的入口。在控制台中，可以管理集群、管理集群中的应用、服务、节点和数据卷、管理用户和用户模板。

- **TROOPERS集群验证**

Troopers负责集群、机器信息、证书管理、账号接入验证。以主备的方式部署，无单点隐患。

- **MYSQL数据库**

  负责管控系统的集群和账号相关数据的存储和管理，提供Master/Slave高可用能力。

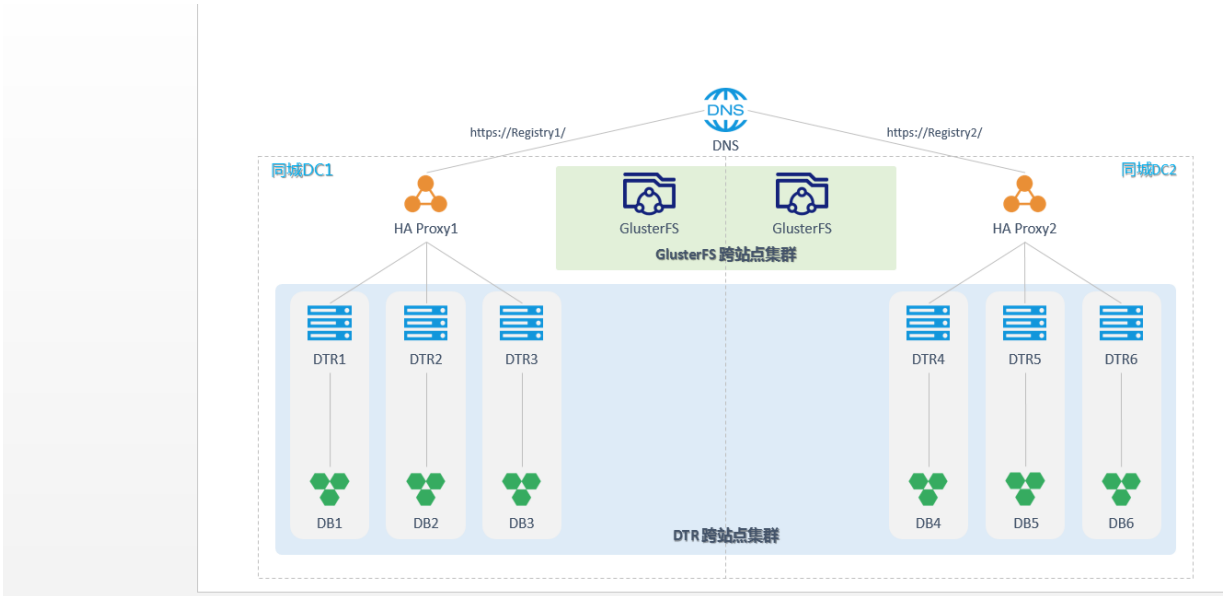
- **UCP集群管控**

  UCP是集群管理的管控系统，由Manager节点、Worker节点组成。一般系统中Manager由3个节点组成，其中1个leader，2个slave节点。通过多个Manager互为主备，实现UCP的高可用。Manger之间通过raft协议实现数据的同步。

5.1.2.2.2 镜像仓库高可用架构

镜像仓库的前端应用是无状态，支持部署在两个机房。通过负载均衡对外暴露统一的控制台和API。底层存储依赖共享存储实现HA，部署架构图如下所示。

图 5-3: 镜像仓库架构图



1. 6个DTR属于一个大集群（跨站点）。
2. 每一个站点有一个域名（绑定HA Proxy），当容灾切换时，需要修改域名。
3. DB和DTR实际部署在一个节点（物理机 or 虚拟机）之内。
4. DB中包含metadata（存在RethinkDB）以及CVE（存在PostgreSQL）。
5. 单站点内的3台DTR都挂在同一个volume上，同一个volume指向同一个GlusterFS。
6. GlusterFS也做成跨站点集群。

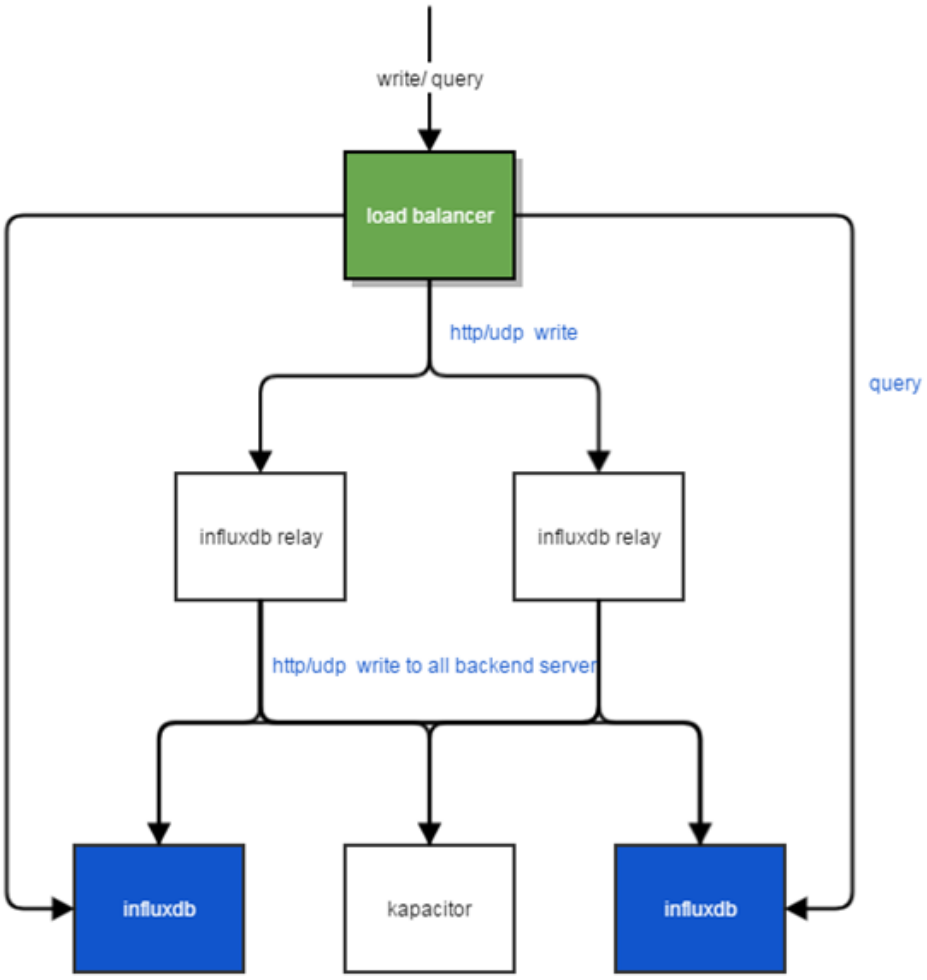
- 跨机房构建一个大的DTR集群，原信息同步通过DTR自身实现（cve、repo、account）。
- glusterfs、ceph等分布式存储可以是一个跨两个机房的大集群，也可以是每个机房一个集群。通过集群间数据同步实现高可用。
- 每个DTR实例挂载本机房的存储。

- 每个机房一个haproxy作为接入入口，DNS默认指向一个机房的haproxy，出现问题后切换到另外一个机房。

5.1.2.2.3 监控高可用架构

完整的监控架构包括，数据写入通道、监控数据持久化数据库和数据展示dashboard。其中数据写入和数据存储均配置了高可用。

图 5-4: 监控架构



- 所有的数据上报通过swarm mode自带的routing mesh来做负载均衡。
- 数据写入时，通过influxdb-relay将一份数据同时写入多个后端数据源，其中后端数据源包括2个influxdb的实例和一个kapacitor实例。
- 监控服务存储部分的高可用通过多数据库实例的方式来保证。
- kapacitor的高可用采用swarm mode默认的replica的机制，挂掉重启，其数据库通过本地volume 存储，重启后的kapacitor状态仍然可以从数据库自动恢复。

5.1.3 环境安全建议

容器服务-专有云Agility版云平台以软件产品模式交付客户使用，最终会部署在客户自建的IDC机房。产品可以运行在任何形式的X86服务器之上，包括不同的虚拟化平台、物理机等。在部署的环境上建议开启以下安全策略：

- 路由及安全设备进行策略控制，对端口、服务进行严格控制，并对进出数据进行过滤。
- 在网络出口部署负载均衡，进行流量控制与负载分担。
- 配置态势感知与监控告警平台。
- 对安全与系统资源的情况进行监控、分析与告警。

5.1.4 网络安全

5.1.4.1 管理与应用网络隔离

容器服务-专有云Agility版提供了管理网络和应用运行网络的隔离能力，平台默认创建apsara_network网络为集群管理控制网络。其他应用连接到应用网络，管理网络和应用运行网络隔离。

5.1.4.2 跨主机的容器网络，应用之间隔离

容器服务-专有云Agility版支持Overlay与MacVlan两种模式的跨主机容器网络。在Overlay模式下，同应用下的不同容器间网络可以互通，不同应用之间相互隔离。MacVlan模式依赖于宿主机的路由，通过配置不同主机之间的路由表实现隔离。

5.1.4.3 网络访问控制策略

- 为容器划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。
- 在网络边界区域边界配置访问控制列表对进出的数据进行过滤，控制粒度为端口级。
- 会话处于非活跃一定时间或会话结束后终止网络连接。

5.1.5 主机安全

5.1.5.1 操作系统账号要求

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

5.1.5.2 非法登录限制策略

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

5.1.5.3 访问控制

启用访问控制功能，依据安全策略控制用户对资源的访问。

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

5.1.5.4 默认账号删除

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

5.1.6 应用安全

容器使用非root运行

为了防止容器逃逸而获得宿主机的权限，容器内应用以非root用户身份运行。

使用安全的基础镜像

用户可根据自身需求定制基础镜像，并强制要求组织内使用认可的基础镜像；也可使用第三方安全的镜像，这里推荐使用Alpine-linux，docker所有的官方镜像都使用其作为基础镜像。

镜像最小化安装

安全的普适法则，镜像中不安装任何与应用无关的东西。

配置Docker守护程序的TLS身份验证

Docker守护程序和Docker Swarm API配置TLS身份验证。

设置容器CPU优先级

使用CPU共享功能来设定优先级。CPU共享允许将一个容器优先于另一个容器，并禁止较低优先级的容器频繁地占用CPU资源。这样可确保高优先级的容器更好地运行，且可以有效的防止资源耗尽攻击。

限制容器内存使用量

默认情况下，容器可以使用主机上的所有内存。可以使用内存限制机制来防止一个容器消耗所有主机资源的拒绝服务攻击，具体可使用使用**-m**或**–memory**参数运行容器。

磁盘限额

默认情况下Docker镜像、容器rootfs、数据卷都存放在*/var/lib/docker*目录里，跟host是共享同一个文件系统。目前无法控制该目录大小，通过*/var/lib/docker*单独挂载，避免影响宿主机根文件系统。

身份鉴别

- 提供账户/密码以及证书等登录方式
- 提供登录失败处理能力，结束会话，限制登录和自动退出
- 会话空闲一段时间后，自动锁定
- 初始预设密码在首次登录后，提示修改
- 密码配置复杂度，修改密码不能与上一次重复，提示定期修改密码

安全审计

- 系统提供账号安全审计功能，对系统账号的修改操作实现审计记录，且记录无法更改。
- 系统平台上所有的操作清晰、完整，包括事件的日期、时间、发起者信息、类型、描述和结果等，并定期备份审计记录，保存时间不少于半年。

通信安全、保密性

- 系统各组件之间采用TLS加密通信
- 系统中的涉密信息通过密文保存，且在需要时下发至特定节点

角色权限控制

- 系统内置多租户权限管理模型，可根据团队、角色设定不同的访问权限，在集群、应用和管理维度进行细粒度管控
- 系统支持LDAP等外部权限管理方式
- 镜像仓库支持多租户、只读等权限控制

5.1.7 数据安全及备份恢复

5.1.7.1 集群管理控制台数据库高可用及备份

集群管理控制台后端MySQL数据库采用Master/Slave架构分别部署在不同宿主机，起到本地容灾能力。同时数据库配置了定时备份任务，备份介质通过分布式存储实现跨地域复制、存储。在系统面临恢复重建时，能够实现数据的恢复。

5.1.7.2 DTR备份

DTR提供了备份接口，可实现元数据以及部分配置数据的备份恢复能力。其中DTR可实现以下数据的备份。

数据	是否备份	说明
配置	是	-
镜像仓库元数据	是	-
对镜像仓库和镜像的访问控制	是	-
Notary数据	是	-
扫描结果	是	-
证书和密钥	是	-
镜像内容	否	需要单独备份，具体取决于DTR配置
用户、组织、团队	否	创建UCP备份以备份此数据
漏洞数据库	否	可在恢复后重新下载

5.1.7.3 UCP备份

由于UCP在所有管理节点上存储相同数据，因此只需定期备份一个管理节点即可。备份的数据包括：

- 用户、团队和权限信息
- UCP配置选项，如DDC许可证、调度选项、Content Trust和身份验证后端

有两种方法恢复UCP集群：

- 在新的swarm的管理节点上，可以根据提示备份恢复UCP集群。
- 在未参与swarm的Docker引擎上，将创建新的swarm并根据其恢复UCP

5.1.8 等保测评

5.1.8.1 测评目的

通过对容器服务-专有云Agility版云平台等级保护测评，确保产品达到国家等级保护要求，也为其信息资产安全和业务持续稳定运行提供有力的保障。

依据以下标准和规范，对容器服务-专有云Agility版云平台进行了等保测评：

- 《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）
- 《金融行业信息系统信息安全等级保护实施指引》（JR/T 0071-2012）
- 《金融行业信息系统信息安全等级保护测评指南》（JR/T 0072-2012）
- 《信息安全技术 信息系统安全等级保护测评要求》（GB/T 28448-2012）

5.1.8.2 测评内容

依据信息系统确定的业务信息安全保护等级和系统服务安全保护等级，选择《金融行业信息系统信息安全等级保护实施指引》（JR/T 0071-2012）中对应级别的安全要求作为等级测评的基本指标，具体如下：

安全层面	测评对象	安全控制点	测评项数
网络安全	网络结构安全	结构安全	6
		访问控制	4
		入侵防范	2
		恶意代码防范	2
主机安全	阿里云容器服务-专有云Agility版云平台发布机	身份鉴别	6
		访问控制	4
		安全审计	6
		剩余信息保护	2
		入侵防范	3
		恶意代码防范	4
		资源控制	6
	阿里云容器服务-专有云Agility版云平台镜像仓库入口服务器	身份鉴别	6
		访问控制	4
		安全审计	6
		剩余信息保护	2
		入侵防范	3
		恶意代码防范	4
		资源控制	6

安全层面	测评对象	安全控制点	测评项数
	阿里云容器服务-专有云Agility版云平台数据库	身份鉴别	6
		访问控制	7
		安全审计	6
		资源控制	6
	阿里云容器服务-专有云Agility版云平台跳板机	身份鉴别	6
		访问控制	4
		安全审计	6
		剩余信息保护	2
		入侵防范	3
		恶意代码防范	4
		资源控制	6
应用安全	阿里云容器服务-专有云Agility版云平台	身份鉴别	5
		访问控制	4
		安全审计	4
		剩余信息保护	2
		通信完整性	1
		通信保密性	2
		抗抵赖	2
		软件容错	2
		资源控制	5
数据安全及备份恢复	阿里云容器服务-专有云Agility版云平台数据	数据完整性	2
		数据保密性	2
		数据备份和恢复	4
安全管理制度	制度机构人员及系统	管理制度	4
		制定和发布	5
		评审和修订	2
安全管理机构		岗位设置	4
		人员配备	3

安全层面	测评对象	安全控制点	测评项数
		授权和审批	4
		沟通和合作	5
		审核和检查	4
人员安全管理		人员录用	4
		人员离岗	3
		人员考核	3
		安全意识教育和培训	4
		外部人员访问管理	2
系统建设管理		系统定级	4
		安全方案设计	5
		产品采购和使用	4
		自行软件开发	5
		工程实施	3
		测试验收	5
		系统交付	5
		系统备案	3
		等级测评	2
		安全服务商选择	3
系统运维管理		环境管理	4
		资产管理	4
		介质管理	6
		设备管理	5
		监控管理和安全管理中心	3
		网络安全管理	8
		系统安全管理	7
		恶意代码防范管理	4
		密码管理	1

安全层面	测评对象	安全控制点	测评项数
		变更管理	4
		备份与恢复管理	5
		安全事件处置	6
		应急预案管理	5

5.1.8.3 测评结论

综合所有测评结果与风险分析，根据《金融行业信息系统信息安全等级保护实施指引》（JR/T 0071-2012），符合性判定依据给出等级测评结论：**阿里云飞天敏捷版容器云平台等级测评达到金融等保三级认证要求。**

5.2 对象存储OSS

5.2.1 什么是对象存储OSS

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

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

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

5.2.2 身份验证

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

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

5.2.3 访问控制

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

OSS 提供 bucket 和 object 的权限访问控制。

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

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

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

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

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

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

5.2.4 RAM和STS

OSS 已经接入 RAM/STS 鉴权。

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

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

5.2.5 高可用性

OSS 服务可用性高达 99.9%。

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

5.2.6 租户隔离

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

5.2.7 服务器端加密

OSS 支持在服务器端对用户上传的数据进行加密（Server-Side Encryption）。当用户上传数据时，OSS 对收到的用户数据加密，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。换句话说，下载一个进行服务器端加密编码的Object和下载一个普通的Object没有多少区别，因为OSS会为用户管理整个编解码过程。

OSS服务端加密提供由OSS完全托管的服务端加密功能：

数据加密密钥的生成和管理，由OSS负责，并采用高强度、多因素的安全措施进行保护。数据加密的算法使用行业标准的强加密算法AES-256（即256位高级加密标准）。OSS的服务器端加密编码是Object的一个属性。用户创建 Object 时，只需要在 Put Object 的请求中携带 x-ossserver-side-encryption 的 HTTP Header，并指定其值为 AES256，即可以实现该 Object 的服务器端加密存储。

5.2.8 客户端加密

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

5.2.9 数据传输安全

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

5.2.10 数据传输完整性

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

5.2.11 访问日志记录

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

5.2.12 跨资源共享

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

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

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

5.2.13 防盗链

为了防止用户在OSS上的数据被其他人盗链，OSS支持基于HTTP header中表头字段referer的防盗链方法。用户可以通过OSS管理控制台或者API的方式对一个Bucket设置referer字段的白名单和是

否允许referer字段为空的请求访问。例如，对于一个名为oss-example的Bucket，设置其referer白名单为**http://www.aliyun.com/**。则所有referer为**http://www.aliyun.com/**的请求才能访问oss-example这个Bucket中的Object。

5.3 块存储EBS

5.3.1 产品概述

弹性块存储（Elastic Block Service，简称EBS）是基于分布式文件系统实现的一个高可靠、高可用的块设备存储服务。EBS数据通过多份冗余存放在不同的机架下，在硬件出现故障时，提供可靠的数据安全保护能力。

EBS卷（EBS Volume）即一块虚拟的块存储设备，用户可以像使用物理硬盘一样来使用，可以格式化，可以挂载，可以执行I/O操作。

EBS卷有多种类型，不同类型的卷提供不同等级的I/O能力，以适应不同的工作负载。

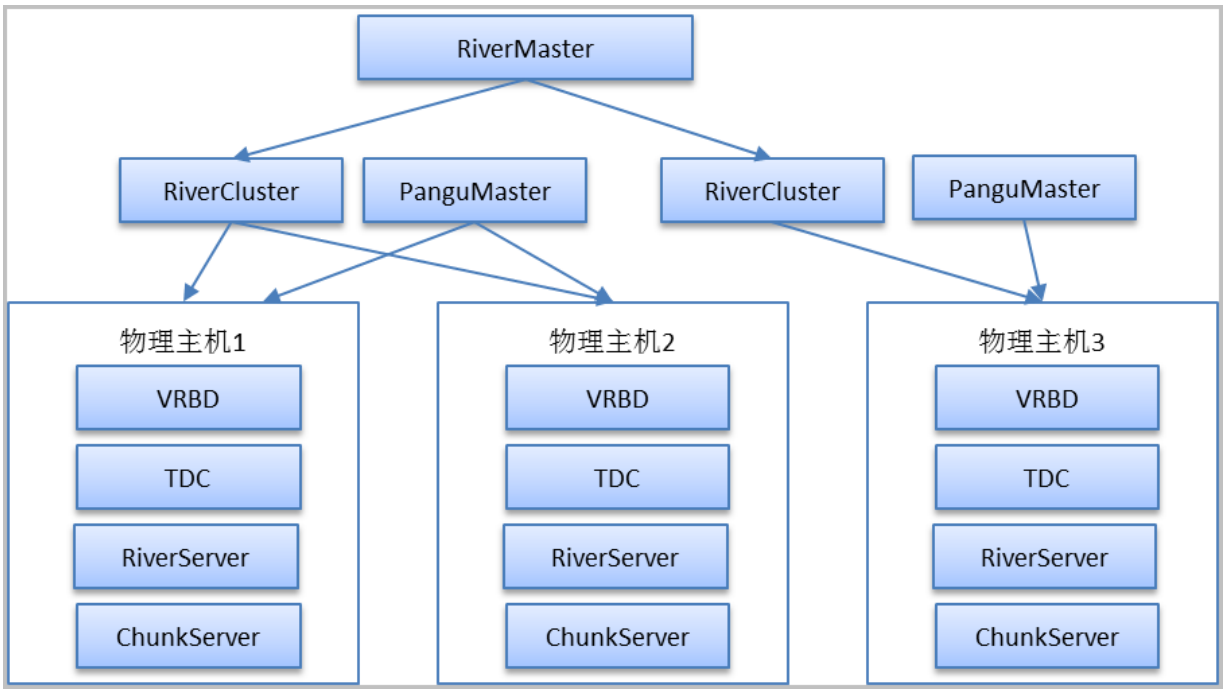
EBS快照（EBS Snapshot）是EBS卷某一时刻的数据备份，EBS快照所备份的数据按照固定大小的数据块存储在对象存储中。快照主要用于数据灾备、数据审计以及制作基础镜像等。

5.3.2 技术架构及特点

5.3.2.1 技术架构

块存储的技术架构如图 *5-5: EBS*软件架构所示。

图 5-5: EBS软件架构



其中，各组件及其功能如表 *5-1:* 各组件功能说明所示。

表 5-1: 各组件功能说明

组件	功能
VRBD	虚拟块设备驱动，部署在计算节点，通过VRBD能创建虚拟的块设备，能够被挂载到物理主机上，能进行IO读写，完全和物理介质的磁盘一样的使用体验。
TDC	TDC负责将后端存储和前端组件如VRBD桥接起来，承载块设备IO，同时提供形态丰富的CLI接口，如磁盘的创建、销毁，快照的创建与回滚等。
PanguMaster	盘古中最重要的角色，维护了文件和数据块之间的映射quota数据、chunkserver元数据、和checkpoint等。盘古通过多master机制保证master的高可用性，同时使得盘古具备热升级的能力。master之间log的同步和主master的选举采用了Paxos算法来保证其一致性。
ChunkServer	运行在数据物理服务器上，主要的职责是管理本地的硬盘和支撑对硬盘的读写删操作。
RiverMaster	在块存储系统中管控角色，负责磁盘在集群见的调度，包括磁盘创建的的调度、动态负载调度等，以及相关的管理工作，如存储库存水位管理等。

组件	功能
RiverCluster	负责管理一个集群，RiverCluster通过心跳维护RiverServer的状态。当RiverServer不可服务时，负责将RiverServer的磁盘动态迁移到另一台RiverServer上。
RiverServer	运行在每台物理主机上，RiverServer负责块层的IO读写处理，同时将IO请求转化后投递到Pangu文件层。

5.3.2.2 技术特点

5.3.2.2.1 高可用

块存储具备高可用特性：

- 提供多master机制，保证服务的高可用性和元数据的安全性。
- 多集群支持。

5.3.2.2.2 高可靠

块存储具备高可靠性：

- 用户通过minCopy和maxCopy分别指定盘古文件的副本数。

  盘古保证数据最少有minCopy份副本；尽可能的有maxCopy份副本。

  一般情况下，minCopy和maxCopy取值是2和3。
- 实现端到端的CheckSum，盘古在IO整个链路的各个环节中，都会对数据进行checksum校验。

5.3.2.2.3 规模性能

块存储具备如下性能：

- 提供用户自定义的数据聚簇方式，用户根据应用场景可以选择数据打散存放，或本地优先扎堆存放，又或者所有副本都扎堆存放。
- 提供优先级控制，保证后台复制的过程中，不影响前端的读写服务。
- 提供数据rebalance操作，保证数据均衡。
- 支持慢盘规避，pangu会定期检查物理磁盘的性能，并识别出性能异常的磁盘，隔离这些性能异常的磁盘，从而保证服务中的物理磁盘性均能符合预期。
- 支持SATA、混合存储及SSD。

5.3.2.2.4 易用性

块存储具备良好的易用性：

- 支持平滑热升级与回滚，对上层业务无影响。
- 损坏磁盘自动运维。

5.3.3 技术原理

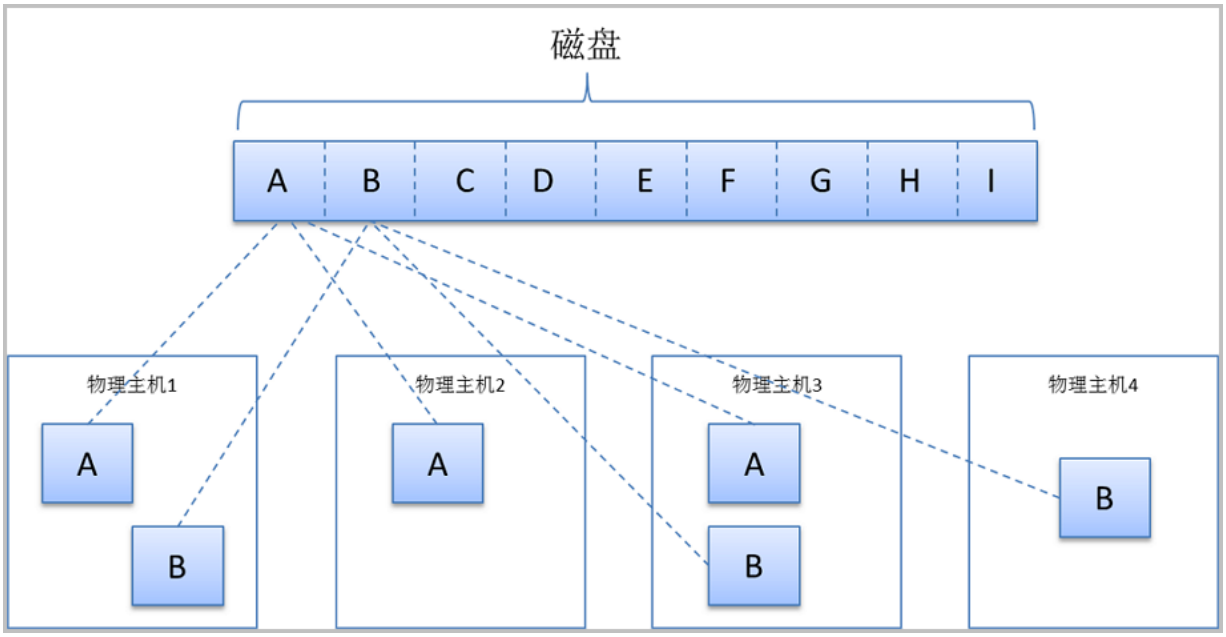
5.3.3.1 数据组织

EBS卷的数据组织具有如下几个特点：

- EBS卷全局按照一定的大小进行切片，一般都是基于64MB为单位进行分割。
- 切片的数据块，可以根据用户数据安全性的要求，存储多份冗余，一般是3个冗余。
- 不同的数据库冗余，分布在不同的物理主机上，防止单台主机异常后，EBS卷不可访问。

EBS卷的磁盘数据组织如图 5-6: 磁盘数据组织所示。

图 5-6: 磁盘数据组织



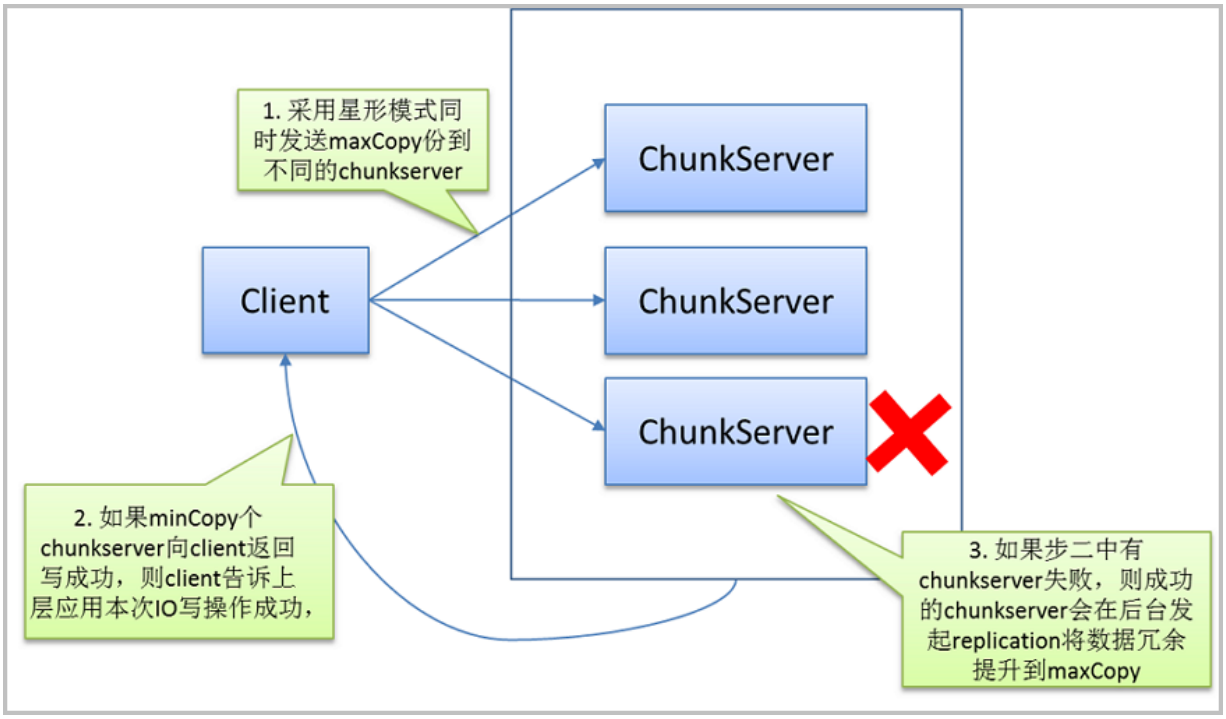
5.3.3.2 多副本机制

如图 5-7: 多副本机制所示，盘古多副本机制的内部实现原理如下：

1. Clinet采用星形模式，同时向服务器发送maxCopy份副本到不同的chunkserver。
2. 如果minCopy个chunkserver向Clinet返回写成功，则Client报告上层应用，本次IO写操作成功。

3. 如果上一步中有chunkserver失败，则成功的chunkserver会在后台发起replication，将数据冗余提升到maxCopy。

图 5-7: 多副本机制



5.3.3.3 数据重建

盘古具备强大的数据保护和智能恢复机制。

数据存储时已被切片打散到多个节点上，这些分片数据通过算法被分配在不同的存储节点、不同机柜之间以提供最大数据安全保障，同时数据存储时采用多副本技术，支持两副本或三副本，数据会自动保存多份，每一个分片的不同副本也被分散保存到不同的存储节点上。

在硬件发生故障导致数据不一致时，盘古一方面通过异步机制来保证服务的可用性，另一方面通过优化的自检机制，能够快速比较不同节点上的副本分片，自动发现数据故障，并在发现故障后启动数据修复机制。

在后台修复数据，由于数据被分散到多个不同的存储节点上保存，数据修复时，在不同的节点上同时启动修复，每个节点上只需修复一小部分数据，多个节点并行工作，配合精准的流控机制不仅能充分利用剩余网络资源，还可以有效避免单个节点修复大量数据所产生的性能瓶颈，对上层业务的影响做到最小化。

5.3.3.4 掉电保护

系统运行过程中，可能会出现服务器突然下电的情况，盘古在内存的元数据和写缓存数据会随着掉电而丢失，需要使用NVDIMM或SSD Cache来保存和恢复元数据和缓存数据。

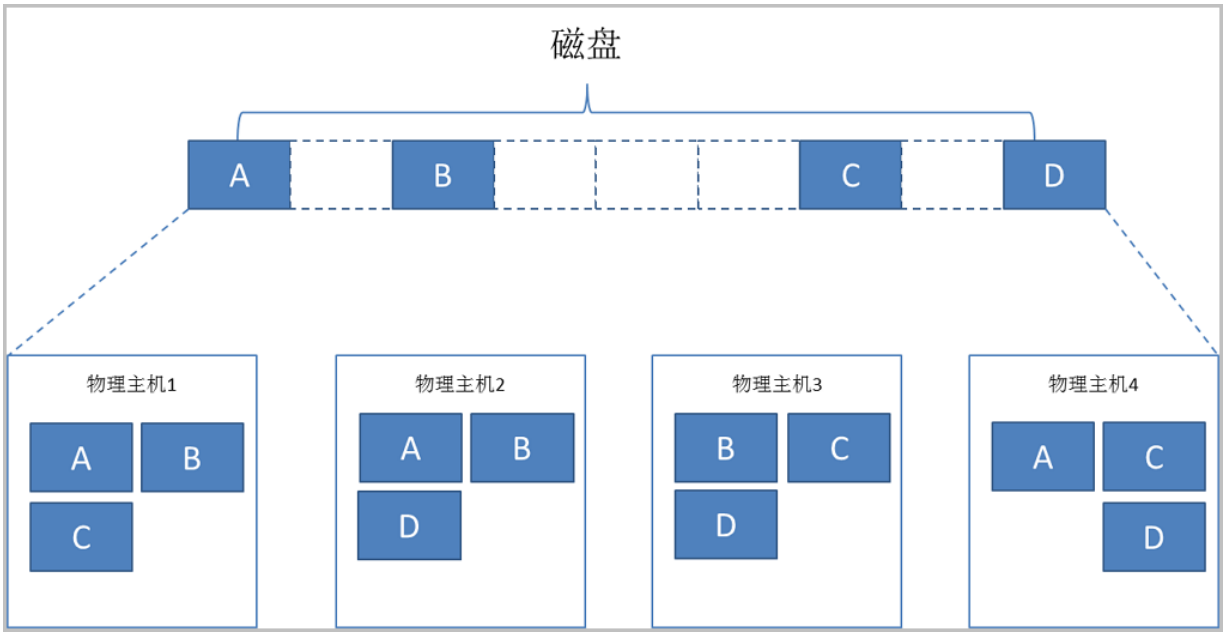
部署盘古软件的每一台服务器上要求配备SSD Cache，服务器掉电时，会把元数据和缓存数据写入SSD Cache中，上电后会自动把数据还原到内存中。盘古能够识别出系统中的SSD Cache，并根据用户对成本、性能的需求提供不同的存储服务，若需要提供掉电保护的支持，需要在配置表中明确设置。

5.3.3.5 精简配置

阿里云EBS块服务，默认支持精简配置，以降低存储的成本，提高资源利用率。

如图 *5-8:* 精简装置所示，用户磁盘真正写入的只有四个块，虽然磁盘的容量是9个块的容量。所以，落在底层盘古，也并不是按照9个块空间进行分配与存储，而只是存储了真实有数据的块，并进行索引维护，从而实现了精简配置。

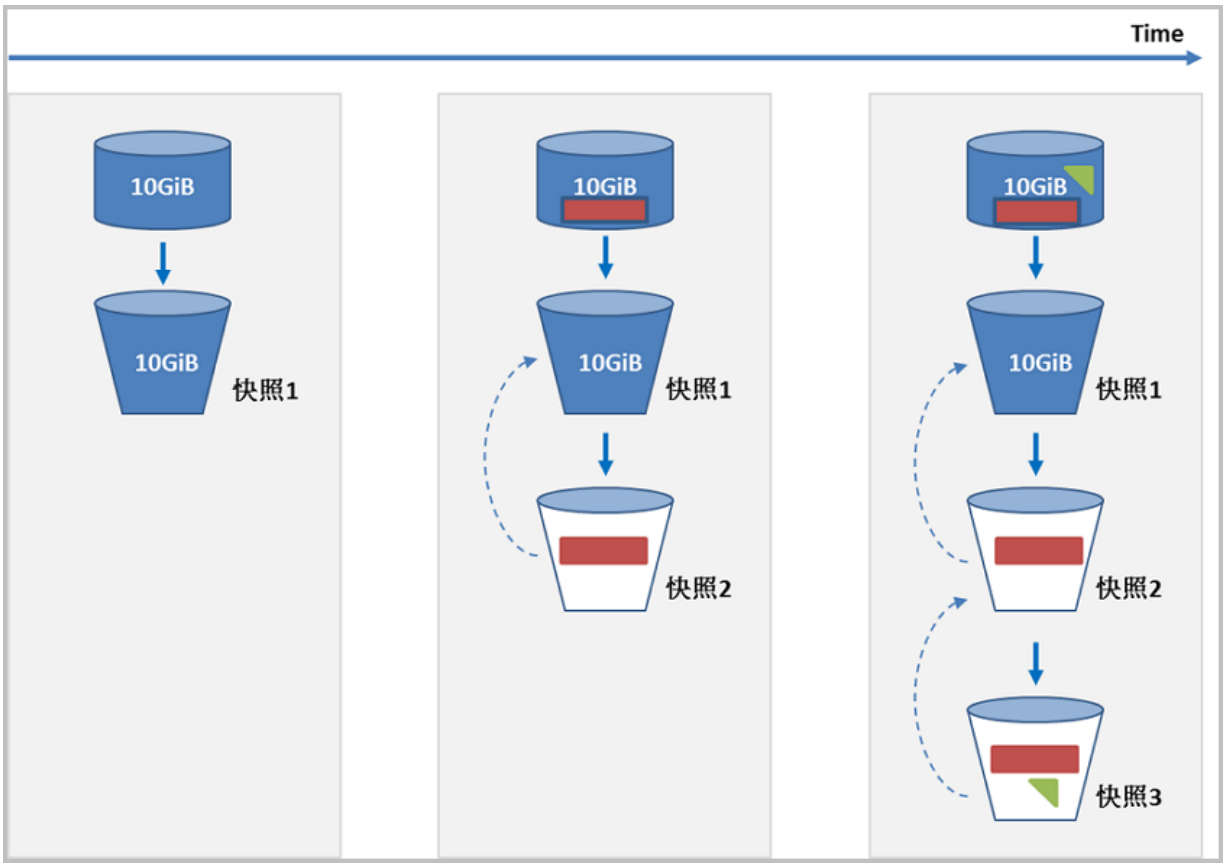
图 5-8: 精简装置



5.3.3.6 快照原理

EBS卷的快照原理如图 *5-9:* 快照原理所示。

图 5-9: 快照原理



EBS卷的快照具备如下特点：

- 快照通过增量技术实现，创建的第一个快照是卷的数据的全量备份，后续创建的快照均是自上次卷的数据量，进行增量备份。
- 快照是按照一定大小进行切割，并将数据有变化的数据块压缩后，备份到对象存储系统中。
- 快照的指令下发是秒级完成，快照数据同步是在系统后台进行的，不需要停止卷的运行状态。
- 快照删除后，不会影响后续快照的数据完备性，被删除的快照的数据块，只有引用计数为0时，才会被回收。

5.3.4 产品分类

EBS卷的分类如表 *5-2: EBS卷类型及其使用场景*所示。

表 5-2: EBS卷类型及其使用场景

EBS卷	主要场景	存储目标
SSD卷	• I/O密集型应用	• 单卷IOPS能力上万能力

EBS卷	主要场景	存储目标
	• 中大型关系数据库 • NoSQL数据库	• 单卷BPS能力上百MB能力
高效卷	• 开发与测试业务 • 系统盘 • 小型负载数据库	• 单卷IOPS能力数千能力 • 单卷BPS能力数十MB能力

5.3.5 技术指标

EBS弹性块存储的产品技术指标如表 5-3: 技术指标所示。

表 5-3: 技术指标

项目	描述
存储介质	支持HDD机械硬盘和SSD固态硬盘
部署模式	支持计算存储分离部署架构
硬件要求	支持通用X86架构服务器
单集群最大规模	10000
单集群最大硬盘数量	120000
单集群最大管理容量	480000 TB
单集群最大逻辑卷数量	500000
单卷最大容量	10TB
单计算节点挂载逻辑卷最大数量	200
资源管理和监控	• 支持块存储Volume的创建、挂载、卸载、删除、扩容 • 支持对资源池的利用率、性能等进行实时监控
存储访问协议	块设备访问协议
QOS	支持不同用户之间的资源隔离和QOS性能保障
冗余能力	支持块设备的多副本部署，副本数量可调
可靠性	支持服务器和机架级别可靠性
兼容性	支持Openstack、KVM、容器等虚拟化技术

项目	描述
GuestOS	支持Linux、Windows等主流操作系统
高级存储服务	• 支持快照功能，支持手动和自动快照 • 支持镜像功能 • 支持多租户 • 支持自动精简配置
管理接口	支持RestfulAPI、CLI及图形化管理界面

5.4 表格存储Table Store

5.4.1 什么是表格存储

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

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

5.4.2 身份认证

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

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

5.4.3 高可用性

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

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

5.4.4 强一致性

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

5.4.5 监控集成

用户可以从表格存储控制台实时获取每秒请求数、平均响应延时等监控信息。

5.4.6 RAM 和 STS 支持

表格存储支持 RAM 服务。

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

表格存储同时支持 STS 服务，通过临时访问凭证提供短期访问权限管理。

5.5 文件存储NAS

5.5.1 什么是文件存储

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

您创建NAS文件系统实例和挂载点后，即可在ECS、HPC和Docker等计算节点内通过标准的NFS协议挂载文件系统，并使用标准的Posix接口对文件系统进行访问。多个计算节点可以同时挂载同一个文件系统，共享文件和目录。

5.5.2 产品安全和可靠性方案

5.5.2.1 访问控制

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

5.5.2.2 RAM支持

NAS接入了RAM服务，支持控制台设置RAM，主子账号授权。

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

表 5-4: RAM中可授权的文件存储NAS操作列表

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

5.5.2.3 权限组支持

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

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

一条权限组规则包含四个属性，如表 *5-5:* 权限组属性所示。

表 5-5: 权限组属性

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

5.5.2.4 高可用性

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