ALIBABA CLOUD

阿里云

信任中心

信任中心（阿里云文档中心合集）

文档版本：20210105

阿里云

法律声明

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

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.阿里云安全白皮书

阿里云于2017年首次发布《阿里云安全白皮书》（以下简称“白皮书”）。企业可参考白皮书构建安全和稳固的信息化架构。白皮书将客户隐私和数据安全列为第一原则，并于2015年全球首家将不碰客户数据写入正式文件，其中明确了数据是客户资产，云计算平台不得移作它用。

完整版阿里云白皮书下载链接如下：

- 中文版：阿里云安全白皮书（2020年1月版本）
- 英文版：Security White Paper of Alibaba Cloud (January 2020)

2.常见问题

2.1. 重点合规资质FAQ

关于等保2.0、阿里云SOC报告、重点ISO系列认证的常见问题。

关于等保2.0

1、阿里云自身过等保了吗？

阿里云积极按照监管部门要求开展等保2.0测评，通过等保2.0的系统包含：

（1）【等级保护三级】公共云基础服务平台（IaaS产品）

（2）【等级保护三级】公共云数据及开发服务平台（PaaS产品）

（3）【等级保护三级】公共云应用服务平台（SaaS产品）

（4）【等级保护三级】阿里云电子政务云平台系统

（5）【等级保护四级】阿里云金融云

（6）【等级保护三级】CDN内容分发系统

2、云上用户过等保，阿里云可以协助提交什么材料？

云上用户过等保只需要关注自身IT系统的安全建设情况，阿里云协助提供云平台的安全建设材料，主要包括：

（1）云平台等级测评结论扩展表（云计算安全）；

（2）网络安全测评报告对云平台网络安全等级测评的总体评价；

（3）云平台主要安全问题及整改建议；

（4）云服务商针对这些主要安全问题的整改情况的详细说明。

关于阿里云系统与组织控制（SOC）报告

1、阿里云SOC报告是什么？

阿里云SOC报告是独立的第三方审计师针对阿里云为客户提供的云服务进行检查验证而出具的独立审计报告。该报告向阿里云的客户及其审计师说明了阿里云的关键控制及控制目标，以帮助客户更好地评估阿里云的内控机制并有效地管理其外包风险。

2、阿里云SOC报告有几类，分别是什么？

阿里云SOC报告分为以下3种类型：

（1）SOC 1报告 (I类型)

该报告是针对阿里云的内控描述以及其控制目标的第三方审计报告。该审计是第三方独立审计师根据国际认证标准第18号标准(SSAE No. 18)下AT-C 320章节(AT-C section 320)，针对服务组织进行的与用户财务报表相关的内控审计。该报告可帮助客户及其审计师了解阿里云侧已建立的支持客户侧与其财务报告相关的控制(Internal Control over Financial Reporting,ICOFR)，并进行控制有效性评估。

（2）SOC 2报告 (II类型)

该报告是针对阿里云提供的云服务的安全性、可用性及机密性相关的内控机制进行检查验证的独立审计报告。该审计是根据美国注册会计师协会(AICPA)制定的SOC 2可信服务标准与安全、可用及机密性相关的原则标准的第三方独立审计。阿里云的客户可以通过该报告了解阿里云系统及内控描述，以及阿里云对AICPA可信服务标准中关于安全性、可用性和机密性原则的符合性。

（3）SOC 3报告（III类型）

该报告是针对阿里云对AICPA可信服务标准中关于安全性、可用性和机密性原则符合性描述的第三方独立审计报告。

有关ISO20000认证

1、企业为什么要做ISO20000认证？

通过独立第三方审核确认企业符合ISO20000标准，能向客户及利益相关方展示对IT服务的承诺，不但能增强客户、合作伙伴、投资方的信心，也可以向政府及行业主管部门证明对相关法律法规的符合，并能得到国际上的认可。

2、企业如何进行ISO20000认证？

如果企业需要进行ISO20000认证，前提是要了解ISO20000相关标准，然后陆续开展认证策划与准备、确定IT服务管理体系的认证范围、现状调研、体系文件编写、体系文件运行与改进、体系认证审核等相关工作。

3、阿里云上用户如何借助阿里云快速通过ISO20000认证？

云上用户如果需要通过ISO20000认证，阿里云已通过认证的结果可直接使用，同时可以申请相关证据支持。

有关ISO22301认证

1、企业为什么要做ISO22301认证？

通过独立第三方审核确认企业符合ISO22301标准，能向客户及利益相关方展示对业务连续性服务的承诺，不但能增强客户、合作伙伴、投资方的信心，也可以向政府及行业主管部门证明对相关法律法规的符合，并能得到国际上的认可。

2、企业如何进行ISO22301认证？

如果企业需要进行ISO22301认证，前提是要了解ISO22301相关标准，然后陆续开展认证策划与准备、确定业务连续性管理体系的认证范围、业务影响分析与风险评估、体系文件编写、体系文件运行与改进、体系认证审核等相关工作。

3、阿里云上用户如何借助阿里云快速通过ISO22301认证？

云上用户如果需要通过ISO22301认证，阿里云已通过认证的结果可直接使用，同时可以申请相关证据支持。

有关ISO9001认证

1、企业为什么要做ISO9001认证？

通过独立第三方审核确认企业符合ISO9001标准，能向客户及利益相关方展示对产品质量服务的承诺，不但能增强客户、合作伙伴、投资方的信心，也可以向政府及行业主管部门证明对相关法律法规的符合，并能得到国际上的认可。

2、企业如何进行ISO9001认证？

如果企业需要进行ISO9001认证，前提是要了解ISO9001相关标准，然后陆续开展认证策划与准备、确定质量管理体系的认证范围、现状调研、体系文件编写、体系文件运行与改进、体系认证审核等相关工作。

3、阿里云上用户如何借助阿里云快速通过ISO9001认证？

云上用户如果需要通过ISO9001认证，阿里云已通过认证的结果可直接使用，同时可以申请相关证据支持。

有关ISO27001认证

1、企业为什么要做ISO27001认证？

通过独立第三方审核确认企业符合ISO27001标准，能向客户及利益相关方展示对信息安全的承诺，不但能增强客户、合作伙伴、投资方的信心，也可以向政府及行业主管部门证明对相关法律法规的符合，并能得到国际上的认可。

2、企业如何进行ISO27001认证？

如果企业需要进行ISO27001认证，前提是要了解ISO27001相关标准，然后陆续开展认证策划与准备、确定信息安全管理体系的认证范围、现状调研与风险评估、体系文件编写、体系文件运行与改进、体系认证审核等相关工作。

3、阿里云上用户如何借助阿里云快速通过ISO27001认证？

阿里云提供ISO27001自评估模板，旨在帮助用户了解自身的安全管理措施满足标准的情况。另外，对于阿里云用户来说，阿里云的云平台已通过ISO27001认证，云上企业只需对自身云上系统和业务做认证审核即可。

2.2. 数据隐私FAQ

本文介绍数据隐私相关常见问题。

Q1：客户如何控制自己在云上的数据？

客户数据（Member Content）是指客户使用自己的帐户，提交或上传到阿里云服务的数据内容，这些数据内容在阿里云服务上运行。作为客户，您可以：

- 控制数据内容在阿里云上的生命周期，包括数据的创建、使用、存储期限及销毁；
- 决定数据内容的存储位置，包括存储类型和该存储的地理区域（国际地区及阿里云数据中心）；
- 决定对数据内容采取何种安全措施。阿里云为客户的静态数据和动态数据提供强大的加密功能，并为客户提供管理加密密钥的工具；
- 决定对数据内容采取何种安全措施。阿里云为客户的静态数据和动态数据提供强大的加密功能，并为客户提供管理加密密钥的工具；
- 通过自行控制用户、组、权限及身份验证凭证来管理对数据内容的访问以及对阿里云服务和资源的访问。

Q2：阿里云会访问客户数据吗？

阿里云自成立第一天，严格遵守公司数据安全和用户个人信息保护这第一原则开展工作。2015年阿里云在业内率先发起“数据保护倡议”，将不碰客户数据写入正式文本，明确数据是客户资产，云计算平台不得移作它用，并有责任和义务帮助客户保障其数据的私密性、完整性和可用性。未经客户同意，阿里云不会访问或使用客户数据。例如客户使用阿里云提供的云服务器（Elastic Computing Service，简称ECS）或阿里云关系型数据库（Relational Database Service，简称RDS），相关服务实例完全由客户控制，客户的数据也完全由客户管理。阿里云不会访问任何的客户数据。

阿里云只有在获得客户许可后才能访问客户数据，以便为客户提供阿里云产品和服务，而阿里云只能在客户允许的范围内访问和使用这些数据。 所有此类访问和使用都将记录并审核。例如，客户在使用智能语音交互（Intelligent Speech Interaction，简称ISI）产品时，ISI产品仅在得到客户的授权才能访问客户提供的音频数据，提供语音识别、语音合成、自然语言理解等产品服务。

阿里云也在探索更多增加透明度的方式，通过将与特定客户相关的内部操作透传给客户的方式，进一步消除客户对阿里云内部“黑盒”的疑虑（详见Q5）。这种突破了静态展示的界限而主动将动态的信息传递给客户的方式，将是阿里云“透明度”的长期方向。

Q3：未经我的许可，阿里云会移动（包括跨境传输）我的数据内容吗？

阿里云仅在客户选择的阿里云区域中存储和处理每个客户的内容，未经客户同意，阿里云不会移动客户的任何数据内容。

如果客户选择将数据内容存储在一个以上的区域中，或者在区域之间复制或移动内容，那完全是客户的选择，并且无论移动和处理的内容是什么，客户都需要考虑适用于此类操作的法律要求。

如果客户需要使用其他地区提供的阿里云服务，则阿里云将采取必要措施，以确保跨境转移符合适用的数据保护法规。例如，阿里云提供了GDPR Addendum，其中包含经欧盟委员会第2010/87 / EU号决定（或任何后续决定）或GDPR第46条提及的标准合同条款，适用于阿里云客户从欧盟向欧洲经济区以外的国家/地区转移包含个人数据的内容。

Q4：多租户云上，如何防止未经授权的第三方访问我的客户数据？

首先，除非获得客户的明确授权，阿里云不会访问或使用客户的数据。客户对其数据的访问进行控制，也对其使用阿里云服务及资源的访问进行管理。

其次，阿里云提供了一系列高级的访问控制、加密和日志记录功能，可帮助您有效地防止第三方非授权访问。例如，用户可以使用其云账号（即主账号）或其云账号下RAM用户的密码登录云服务控制台并对其云上资源进行操作；通过阿里云AK（Access Key）调用云服务API身份凭证，用于通过API访问阿里云上的资源；也可以通过STS（Security Token Service）管理短期访问资源的凭证；使用MFA认证为用户名和密码额外增加安全保护；对于云上服务来说，在身份认证完成后，使用阿里云的RAM（Resource Access Management）资源访问控制服务，用于用户身份管理与资源访问控制。

第三，客户存储在阿里云上的所有数据均具有强大的租户隔离安全性和控制能力，阿里云提供了一系列先进的数据访问控制解决方案以保障租户间的隔离。例如用户可以使用安全沙箱容器对内存、网络、IO等进行强隔离，从而在单宿主机上更好的其他多租户进行安全隔离；使用专有网络（Virtual Private Cloud，简称VPC），实现数据链路层的隔离，从而构建安全的网络环境；使用实例级别虚拟化防火墙-安全组，划分各个ECS实例安全域；使用云防火墙对南北向和东西向访问的网络流量进行分析，并支持全网流量（互联网访问流量，安全组间流量等）可视化，并支持对主动外联行为的分析和阻断。可通过“阿里云安全白皮书”了解更多的安全解决方案。

Q5：如何知道云平台内部进行了哪些操作？

阿里云操作审计（ActionTrail）服务支持对平台操作日志（Inner-ActionTrail）的审计功能，结合全链路数据加密体系、密钥管理服务，共同帮助用户构建云上全栈数据保护体系。

用户可通过此功能跟踪、监控云平台内部操作：一是阿里云内部人员根据用户授权的操作，比如用户的工单申请；二是阿里云内部根据稳定性等需要做的调度操作；三是根据合规要求进行的处置操作。目前覆盖的产品类别包括对象存储OSS、云服务器ECS、云数据库RDS、容器服务Kubernetes版ACK、E-MapReduce五类，并在持续丰富中。

此功能已通过国际知名会计师事务所安永的审计，保证了信息完整性和准确性。如需获取该商定程序报告，请提交工单或联系自己的客户经理。

平台操作日志（Inner-ActionTrail）功能介绍

云平台内部操作透明化最佳实践