阿里云
金融云解决方案

金融云介绍

文档版本：20191017

法律声明

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

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

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意:** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **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。	执行`cd /d C:/window`命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{}或者{a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1 金融云特性

金融云是服务于银行、证券、保险、基金等金融机构的行业云，采用独立的机房集群提供满足一行两会监管要求的云产品，并为金融客户提供更加专业周到的服务。

安全合规

金融云按照人民银行和银保监会的合规标准建设，在安全性、服务可用性和数据可靠性等方面作了大幅增强。

金融云建设和管理参照的行业标准有：

- **《中华人民共和国金融行业标准JR/T 0167-2018 云计算技术金融应用规范安全技术要求》**
- **《中华人民共和国金融行业标准 JR/T 0166-2018云计算技术金融应用规范技术架构》**
- **《中华人民共和国金融行业标准 JR/T 0168-2018云计算技术金融应用规范-容灾》**
- **《金融业信息系统机房动力系统测评规范》**
- **《金融行业信息系统信息安全等级保护测评指南》**
- **《银行业信息系统灾难恢复管理规范》**
- **《网上银行系统信息安全通用规范》**
- **《商业银行业务连续性监管指引》**
- **《银行业金融机构信息科技外包风险监管指引》**
- **《保险信息安全风险评估指标体系规范》**
- **《保险公司信息系统安全管理指引（试行）》**
- **《证券公司网上证券信息系统技术指引》**
- **《证券期货业信息系统安全等级保护测评要求》**
- ……

与公共云的差异

下图是金融云与公共云在产品与服务上的对比。

	项目	公共云	金融云
合规	ISO27001	★	★
	CSA-STAR	★	★
	等保级别	等保三级	华东1金融云:等保三级 其他地域：等保四级
	金融行业合规		★
	ISO20000	★	★
	ISO22301	★	★
	PCI_DSS		★
	SOC审计	★	★
	可信云	★	★
	CNAS测评	★	★
安全	DDOS防护	★	★
	堡垒机	★	★
	云防火墙	★	★ 公共云客户需要自行购买 金融云客户提供金融云专属 基础版本功能
	磁盘消磁	★	★
	物理安全加固	★	★
可用性	两地三中心	★	★
	同城容灾	★	金融云数据库默认 提供同城容灾功能
	ECS（SLA）	99.95%	99.97%
	RDS（SLA）	99.95%	99.97%
	SLB（SLA）	99.95%	99.97%
其他	金融监管风险评估调查		★
	金融行业监管报告提交		★
	专线	★	★
	特殊设备混合云		★
	客户准入	开放注册	行业认证客户
	售后服务	标准	金融商用

金融云专享产品与服务

- **独立的资源集群**
- **更严格的机房管理**
- **更高的安全容灾能力**
- **更严格的网络安全隔离要求**
- **更严格的访问控制**
- **遵从银行级的安全监管及合规要求**
- **专门的金融云行业安全运营团队、安全合规团队、安全解决方案团队**
- **专门的金融云客户经理和云架构师**
- **更严格的用户准入机制**

2 微金融专区

微金融专区简介

金融云-微金融专区是阿里云为微金融行业量身定制的云计算服务。针对微金融的行业特点，提供高可用、高级别、低成本、稳定的云计算服务，让微金融企业轻松应对业务增长，没有后顾之忧。

说明:
微金融行业包括P2P、小贷、众筹等行业。阿里云微金融专区目前已暂停新服务申请，已在用的服务仍继续提供微金融服务。

金融云与微金融专区的对比

1. **金融云是专门为银行、证券、基金、保险等行业客户提供解决方案的云平台；微金融云是金融云专门为P2P、小贷、众筹等行业提供解决方案的一个子品牌；**
2. **两者都提供同城双活的灾备能力；金融云还可选异地灾备，即两地三中心；**
3. **金融云有华东1、华东2、华南三个地域；微金融只有华东1一个地域；**
4. **价格：金融云相比微金融高30%左右。**

微金融专区增值服务

1. **专享高规格物理集群。**
2. **同城双活灾备模式，保障应用7X24小时运行，高安全级别的物理集群。**
3. **微金融专区客户尊享5Gbps防DDoS特高安全清洗等级。**
4. **安全团队会时刻对客户暴露在公网的端口进行实时监测，一旦发现安全风险，将第一时间通知客户进行修补。**
5. **专业的售后工程师团队提供7X24小时不间断的技术服务，超快响应速度，高效处理客户需求。**

3 上云须知

金融云主要服务于金融用户，出于合规需求及安全考虑，金融云与公共云在使用上有部分区别，请在使用金融云之前仔细阅读本文档。

金融云开放地域

金融云采用独立机房集群部署，将根据客户需求逐步开放，目前已经开放的地域有华东1(杭州)、华南1金融云(深圳)、华东2金融云(上海)，其中：

- 杭州有三个可用区，上海、深圳分别有两个可用区，缺省支持同城双活/灾备架构。
- 深圳、上海为VPC网络环境，可以支持用户自定义网络地址。

账号使用须知

一旦被成功认证为金融云客户，账户将无法使用公共云的资源；账户中有公共云资源的，需先释放原有的公共云资源才可以进行认证。建议为金融云申请专门的账户以方便管理。

不同的账号的云资源之间相互隔离，可通过账号隔离实现环境隔离。可为每种环境（如生产环境、预生产环境、UAT测试环境、开发/集成测试环境）申请单独的阿里云账号。同一个实体可以为多个账户提供认证。

阿里云资源访问服务（RAM）已经上线，RAM的主子账户体系为云服务资源提供了细粒度的权限控制，RAM目前不支持跨账户的授权，详细使用说明请参见 *RAM*产品 。

互联网访问限制

在互联网访问上，金融云做了严密的符合金融行业规范的风控措施。具体的访问限制有以下几点：

- 访问控制台

  金融云客户访问网页控制台需要绑定开通MFA（多因素认证），在输入账户的用户名密码之后再次对动态密钥进行验证。绑定MFA认证的教程请参见 *MFA*绑定 。

- 远程运维操作

  对ECS进行远程运维操作的时候，需首先拨入管理VPN并设置相应的安全组规则，开通管理VPN的过程请参见 配置*VPN* 。金融云为管理VPN分配的内网IP不能用来直接访问RDS，RDS仅对内网的ECS开放。

- 互联网访问云产品

  目前公共云互联网访问带宽可在ECS或者SLB上选取，但是金融云在网络访问方向和端口上进行了限制。ECS不能被外网直接访问，互联网用户只能通过SLB间接访问ECS，带宽在SLB上选

取。ECS需要主动发起互联网访问时，在ECS选取外网带宽，否则带宽选0；SLB允许对互联网开放的端口为80,443,2800-3300,5000-10000,13000-14000,21234,22223,22225。

4 金融云产品限制

产品	功能点	杭州(经典网络)	杭州(专有网络)	深圳(专有网络)	上海(专有网络)
ECS	远程管理	支持,具体参考	支持,具体参考	支持,具体参考	支持,具体参考
	镜像导入	支持	不支持	支持	支持
	镜像导出	支持(外网bucket)	不支持	支持	支持
	镜像复制	支持	支持	支持	支持
	和公共云账号镜像共享	支持	不支持	不支持	不支持
	和金融云账号镜像共享	支持	支持	支持	支持
	共享块存储	支持	支持	支持	支持
OSS	bucket 跨地域复制	支持	支持	支持	支持
	图片处理	支持	支持	支持	支持
	RTMP 推流上传	不支持	不支持	不支持	不支持
	存储容量包	支持	支持	支持	支持
	公网类型 bucket	支持	支持	支持	支持
网络	网络类型	经典网络	专有网络	专有网络	专有网络
	ECS 外网	公网 IP	EIP/NAT 网关	EIP/NAT 网关	EIP/NAT 网关
	ECS 入方向默认限制	默认只允许 ICMP，可以通过云防火墙产品对相关端口开放策略进行定义	默认只允许 ICMP，可以通过云防火墙产品对相关端口开放策略进行定义	2 W 以上端口全开，具体限制可参考 *VPC* 端口限制	2 W 以上端口全开，具体限制可参考 *VPC* 端口限制
	ECS 出方向默认限制	无	无	无	无

产品	功能点	杭州(经典网络)	杭州(专有网络)	深圳(专有网络)	上海(专有网络)
	SLB 开放的监听端口	80,443,2800-3300,5000-10000,13000-14000,21234,22223,22225	80,443,2800-3300,5000-10000,13000-14000,21234,22223,22225	80,443,2800-3300,5000-10000,13000-14000,21234,22223,22225	80,443,2800-3300,5000-10000,13000-14000,21234,22223,22225
	SLB管理扩展域名功能	不支持	不支持	不支持	不支持
	VPN网关	支持	支持	支持	支持
	专线	支持，接入参考	支持，接入参考	支持，接入参考	支持，接入参考
	专线互访范围	只支持 ECS/SLB 和线下资源互通	VPC 内所有资源	VPC 内所有资源	VPC 内所有资源
	ssl_vpn	VPN网关或镜像市场	VPN网关或镜像市场	VPN网关或镜像市场	VPN网关或镜像市场
	ipsec_vpn	VPN网关或镜像市场	VPN网关或镜像市场	VPN网关或镜像市场	VPN网关或镜像市场
RDS	外网地址	不支持	不支持	不支持	不支持
安全	ECS 默认黑洞阈值	5 G	5 G	2 G	2 G
	SLB 默认黑洞阈值	5 G	5 G	2 G	2 G

5 金融云产品列表

目前金融云有三个集群，杭州，上海和深圳。

云产品	杭州(华东一)	深圳（华南一）	上海（华东二）
ECS	部署	部署	部署
经典网络	部署	无	无
VPC	部署	部署	部署
SLB	部署	部署	部署
OSS	部署	部署	部署
RDS(MYSQL& MSSQL&PPAS)	部署	部署	部署
OTS(表格存储)	部署	部署	部署
OCS(Memcache)	部署	部署	部署
Redis	部署	部署	部署
MNS	部署	部署	部署
Mongodb	无	部署	部署
Hbase	部署中	部署中	部署中
PPAS	部署	部署	部署
Greenplum	无	无	无
EDAS	部署	部署	部署
DRDS	部署	部署	部署
MQ	部署	部署	部署
SLS	部署	部署	无
ODPS	部署	无	无
DPC	部署	无	无
DTS	部署	部署	部署
ESS	部署	部署	部署
Greenplum(RDS)	无	待定	待定
HPC	无	部署	部署
NAT网关	部署	部署	部署

云产品	杭州(华东一)	深圳（华南一）	上海（华东二）
oceanbase	部署	无	部署
容器服务	部署	部署	部署中
云堡垒机	部署	部署	部署
云盾加密服务	无	部署	部署
VPN网关	部署	部署	部署
NAS	部署	部署	部署
块存储	部署	部署	部署
共享块存储	无	部署	部署
opensearch	无	无	无