

# 金融云

## 金融云介绍

# 金融云介绍

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三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。

在为金融机构打造的金融云之外，阿里云还为P2P、小贷等企业提供微金融专区解决方案。微金融专区同样采取独立的集群资源，与公共云物理隔离，并享有高规格的服务。关于微金融专区的介绍，可点击[微金融专区](#)详细了解。

## 1. 安全合规

金融云按照人民银行和银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：《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》等。

## 2. 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。

| 类别  | 项目           | 公共云                                 | 金融云                                 |
|-----|--------------|-------------------------------------|-------------------------------------|
| 合规  | ISO27001     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | CSA-STAR     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | 等级级别         | 等保三级                                | 等保四级                                |
|     | 金融合规         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | ISO 20000    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | ISO 22301    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | PCI_Dss      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | SOC审计        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | 可信云          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | CNAS测评       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 安全  | 防 DDoS       | 动态防护                                | 动态防护                                |
|     | 堡垒机镜像        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | 磁盘消磁         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | 网络隔离         | /                                   | 只能通过SLB提供互联网访问                      |
|     | 物理安全         | /                                   | 铁笼隔离/生物识别/监控等                       |
| 可用性 | 两地三中心        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | 同城容灾         | <input checked="" type="checkbox"/> | 默认                                  |
|     | ECS          | 99.95%                              | 99.97%                              |
|     | RDS          | 99.95%                              | 99.97%                              |
|     | SLB          | 99.95%                              | 99.99%                              |
| 其它  | 架构师服务        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | 经典网络专线/VPN接入 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | 特殊设备托管       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
|     | 服务等级         | /                                   | 高                                   |

### 3. 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

## 金融云-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。

**tips：**微金融行业包括P2P、小贷、众筹等行业。

## 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控，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。

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)、华北1(青岛)、华南1金融云(深圳)、华东2金融云(上海)，其中：

- 杭州、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（微金融）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VPN管理。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。

| 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        | 不支持                       | 不支持                       |
|     | 镜像导出         | 支持(外网bucket) | 不支持        | 不支持                       | 不支持                       |
|     | 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           | 不支持        | 支持                        | 不支持                       |
|     | 图片处理         | 不支持          | 不支持        | 不支持                       | 不支持                       |
|     | 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  | 只允许 ICMP     | 无限制        | 2 W 以上端口全开，具体限制可参考 VPC 端口 | 2 W 以上端口全开，具体限制可参考 VPC 端口 |

|     |             |   |   |   |   |
|-----|-------------|---|---|---|---|
|     |             |   |   | 限制  | 限制  |
|     | ECS 出方向默认限制 | 无   | 无   | 无   | 无   |
|     | 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 |
|     | VPN网关       | 不支持   | 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     | 阿里云免费提供   | 镜像市场  | 镜像市场  | 镜像市场  |
|     | ipsec_vpn   | 不支持   | 镜像市场  | 镜像市场  | 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   |

## 金融云产品列表概览

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  |
| 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          | 无   | 无   | 无   |
| 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   |

|