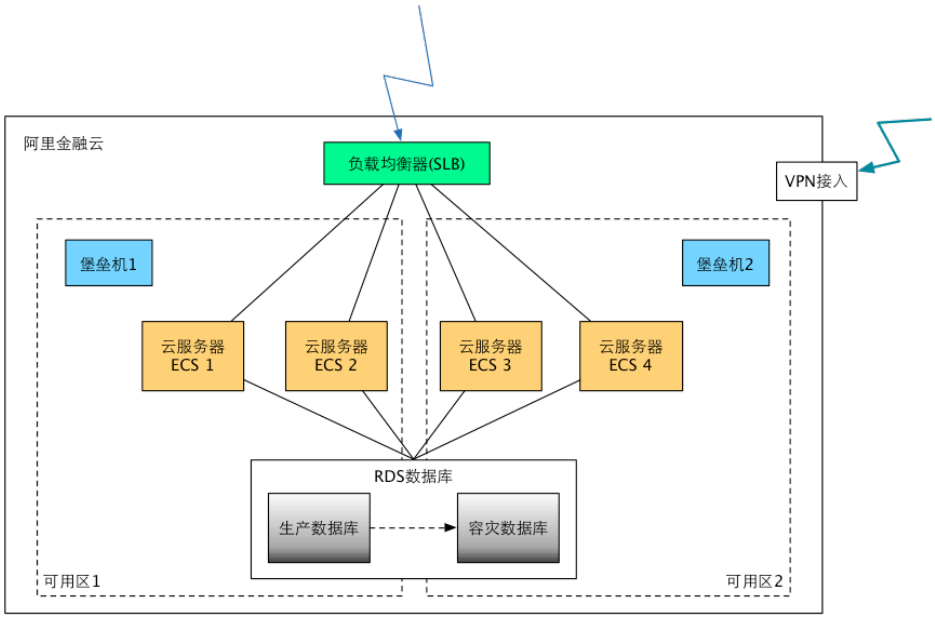
金融云

使用金融云产品

使用金融云产品

金融云经典网络集群：华东I（杭州）；华北I（青岛），

在金融云上，我们强烈建议应用按以下架构搭建。



该架构的要点如下：

- 互联网用户通过SLB访问服务；
- ECS服务器在两个可用区分别购买数量相等的多台(如果应用架构支持，优先选择多台较低配置，而不是少量高配置)；RDS会自动在两个可用区之间进行复制，自动具有两份完全相同的数据副本，具有优良的性能和可靠性，请优先使用RDS MySQL或RDS SQL Server服务，而不要自己搭建数据库服务器。
- 在两个可用区各购买一台低配置（1U,1G的ECS即可）的服务器，用做堡垒机。管理用户登录VPN后，先访问堡垒机，再通过堡垒机管理后面的服务器。
- 设置安全组，建议使用多级跳板的安全组策略保证运维安全。

具体如何搭建推荐架构，请参见接下来的章节。

常见问题

Q：专有网络与经典网络区别？

A： 经典网络类型的云产品，统一部署在阿里云的公共基础网络内，网络的规划和管理由阿里云负责，更适合对网络易用性要求比较高的客户。专有网络，是指用户在阿里云的基础网络内建立一个可以自定义的专有隔离网络，用户可以自定义这个专有网络的网络拓扑和IP地址，与经典网络相比，专有网络比较适合有网络管理能力和需求的客户。

Q：是否一定要按这个架构进行应用搭建？

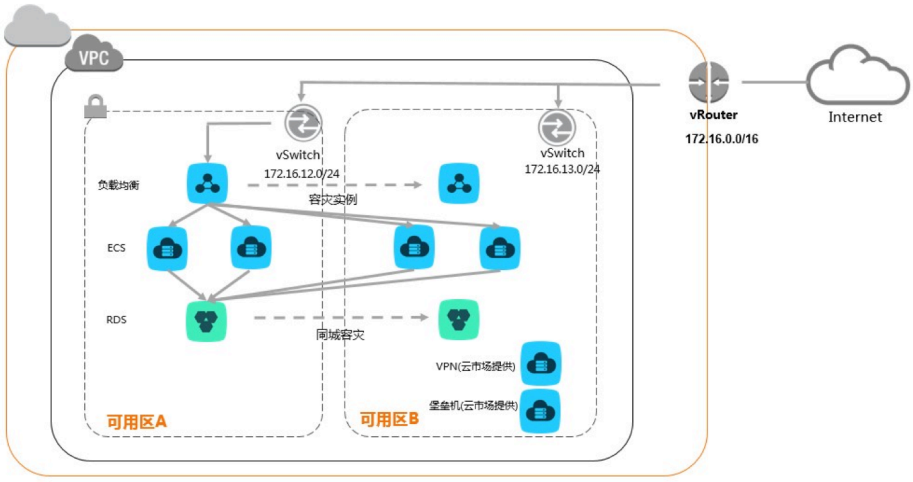
A：阿里金融云建议您遵循这个架构背后的思路搭建系统，这样可以用很小的代价实现双机房高可用。当一个机房出现故障时，不会引起服务中断。这里主要的思路是：通过SLB接入，ECS使用低配多台并分别放在不同的可用区，使用RDS服务而不要自己搭建数据库。

Q：堡垒机或跳板机是否是必须的？

A：不是必须的。但强烈建议使用堡垒机的方式进行服务器的管理，这样更安全。

金融云专有网络集群：华东II（上海）；华南I（深圳）

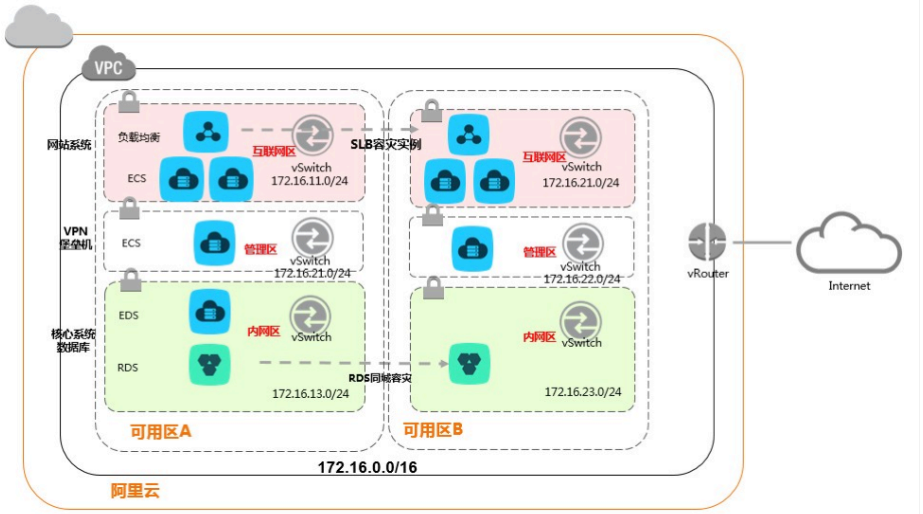
专有网络下标准的推荐架构如下图所示：



- 用户需要创建自己的专有网络，需要配置自己的虚拟路由器与虚拟交换机。
- 用户需要在两个可用区各建一套虚拟交换机。
- 互联网用户通过SLB或EIP访问服务。
- ECS服务器在两个可用区分别购买数量相等的多台，ECS创建时可以指定相应的虚拟交换机。
- RDS会自动在两个可用区之间进行复制，自动具有两份完全相同的数据副本，具有优良的性能和可靠性，请优先使用RDS MySQL或RDS SQL Server服务，而不要自己搭建数据库服务器。RDS在创建时可以指定相应的虚拟交换机。
- 专有网络下的堡垒机与VPN方案通过云市场由第三方提供解决方案 客户可以访问 https://market.aliyun.com/ 来进行购买

- 设置安全组，建议使用多级跳板的安全组策略保证运维安全。

对于安全管理要求比较高的金融客户我们推荐采取以下设计方案:



- 根据不同安全等级通过不同的虚拟交换机设置 互联网（DMZ区），管理区，内网区
- 通过交换机的路由策略以及安全组来对不同安全等级的网络进行隔离。
- 推荐只有互联网区可以访问互联网以及接受用户互联网访问。
- VPN与跳板机安装在管理区内。
- 具体如何搭建推荐架构，请参见接下来的章节。

常见问题

Q：专有网络与经典网络区别？

A：经典网络类型的云产品，统一部署在阿里云的公共基础网络内，网络的规划和管理由阿里云负责，更适合对网络易用性要求比较高的客户。专有网络，是指用户在阿里云的基础网络内建立一个可以自定义的专有隔离网络，用户可以自定义这个专有网络的网络拓扑和IP地址，与经典网络相比，专有网络比较适合有网络管理能力和需求的客户。

Q：是否一定要按这个架构进行应用搭建？

A：阿里金融云建议您遵循这个架构背后的思路搭建系统，这样可以用很小的代价实现双机房高可用。当一个机房出现故障时，不会引起服务中断。这里主要的思路是：通过SLB接入，ECS使用低配多台并分别放在不同的可用区，使用RDS服务而不要自己搭建数据库。

Q：堡垒机或跳板机是否是必须的？

A：不是必须的。但强烈建议使用堡垒机的方式进行服务器的管理，这样更安全。

使用金融云ECS（经典网络）

本篇文档主要针对金融云华东1地域的ECS操作介绍，针对专有网络华东2和华南1的ECS管理可以参考金融云连

接示例(专有网络)。

1. 金融云（经典网络）ECS特性

(1) ECS外网入方向安全策略限制，默认UDP ACCEPT ALL，TCP/ICMP等其他协议默认DROP ALL。出方向无策略限制。

(2) 对于需要对外访问互联网上的资源的服务器，需要购买外网带宽。

(3) 日常管理可以使用SSL_VPN，具体可参考开通管理VPN。39178(4) 线下和云上的业务通信需求推荐用专线和IPSEC_VPN接入。

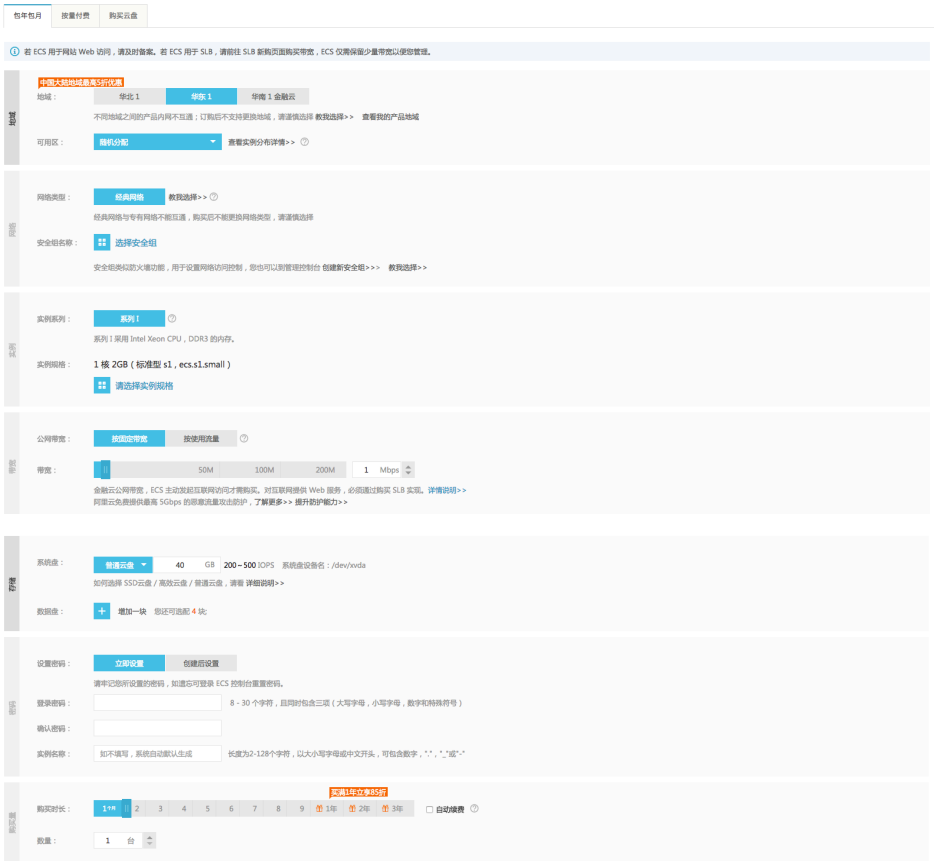
(5) 登录ECS，可以参考金融云主机连接示例(经典网络)。

2. 开通ECS

在ECS云服务器的主页上，点击“立即购买”，或直接访问购买链接开通ECS云服务器时，有以下选项：

选项	说明	建议选项
地域	选择服务器所在的地域，金融云的生产服务器建议选择在华东1。华东1的ECS只能连接华东1的RDS，华东1的RDS是双机房高可用的。	建议将生产系统放在杭州地域
可用区	可用区相当于物理机房的概念，指的是所购买ECS物理位于的哪个机房	同一功能的服务器，一半选择在“杭州可用区B”，另一半选择在“杭州可用区C”
CPU/内存	选择服务器的配置	根据需要选择。如果应用程序支持，建议选择多台低配置(而不是少量高配置)的服务器分布在两个可用区。
公网带宽	如果ECS需要访问互联网上的资源，比如下载互联网上的文件、调用短信网关等，则需要在这里选择一个公网带宽。需要注意的是，即使这里选择了公网带宽，互联网用户还是无法通过ECS分配到的公网IP访问到ECS。	根据需要选择
镜像类型	公共镜像是阿里云提供的标准操作系统。	默认公共镜像 。也可以根据需求选择自定义或者云市场镜像
公共镜像	选择所需要的操作系统和版本	根据需要选择
数据盘	给云服务器增加新的磁盘。添加后在云服务器的操作系统上看起来就是一块新硬盘。	根据需要添加并设置大小。
登录密码	设置云服务器的登录密码	
实例名称	对实例的描述	建议设置为有意义的名称，便于

		以后管理
购买时长	实例购买多长时间	按需要选择，一年的价格相当于一个月的价格乘10
数量	按以上的选择的购买数量	按需要选择。



选择完成后，可点击“立即购买”，也可点击“加入清单”然后再点击“批量购买”完成购买。


当前配置
地域： 杭州（杭州可用区C）
配置： CPU1核、内存512MB
镜像： CentOS 6.5 32位
存储： -
网络： 带宽0Mbps（经典网络）
购买量： 1个月 x 1台
免费开通云盾服务
配置费用：
￥48.00
立即购买
加入清单

3. 使用控制台管理ECS

ECS云服务器可通过管理控制台进行管。在ECS云服务器的管理界面上，可以对服务器进行停止、重启、升级、更换操作系统等操作，具体请参考ECS的基本操作和帮助文档

4. 连接ECS服务器

使用Windows远程桌面、SecureCRT等客户端连接之前，请确认管理VPN已拨入，已经设置相应的安全组规则

VPN拨入成功后，会为客户端分配IP地址。然后需要配置ECS安全组规则，以允许管理VPN的源IP访问。如上

可见，通过配置VPN和安全组规则，即可通过Windows远程桌面或SSH客户端远程管理ECS和上传下载文件。通过这种方式可管理纯内网的ECS（无公网带宽），不但没有流量费用，安全性也得到增强。

5. 上传下载文件

出于安全和合规的要求，金融云对外部端口进行了限制。上传文件之前，请先通过安全组开通远程管理端口（sftp协议需要22端口，暂不支持FTP传输）。Linux操作系统请使用sftp协议进行文件上传(可使用图形化的sftp协议工具winscp，参考winscp官方帮助)，Windows操作系统请使用远程桌面的连接本地驱动器功能，参考这里和这里。

6. 使用阿里云内建的YUM源

金融云为CentOS系统提供了内部Yum源，下载一键更新源脚本即可，阿里云的Yum源使用内网流量，没有选择宽带的ECS也可以正常使用。更多关于yum源的配置，可访问该链接查看。

7. 搭建金融云推荐架构

金融云推荐架构对应的ECS部分实现方法如下：

(1) 将生产服务器加入清单在ECS购买页面上，选择杭州可用区B，选择适应的配置和服务器数量后，点击“加入清单”。再选择杭州可用区C，点击“加入清单”。现在，购买清单中包含两个可用区的多台同配置服务器。

(2) 将堡垒机加入清单在ECS购买页面上，选择杭州可用区B，选择1C/1G内存的ECS一台，操作系统与生产服务器一致，公网带宽选择为0，点击“加入清单”再选择杭州可用区C，点击“加入清单”。现在，购买清单中包含两个可用区各一台堡垒机。

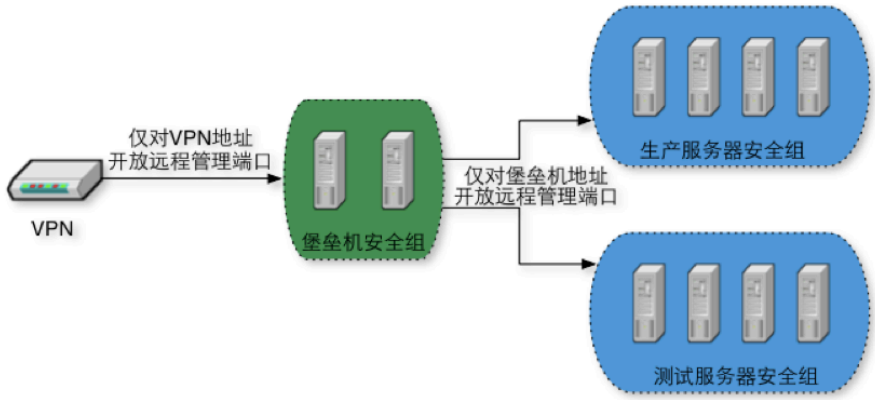
(3) 完成购买在页面上点击“批量购买”，完成付款。然后进入ECS管理控制台，记录所有服务器的内网IP地址。

(4) 配置堡垒机安全组创建一个安全组，名称为sg-bastion，将规则中加入“我的VPN”中列出的所有客户端IP地址(见3.2.2)，端口设置为22(堡垒机是Linux)或3389(堡垒机是Windows)。所属服务器选择为2台堡垒机。

(5) 配置生产服务器安全组创建一个安全组，名称为sg-production，将规则中加入2个堡垒机的IP地址，端口设置为22(堡垒机是Linux)或3389(堡垒机是Windows)。所属服务器选择为所有的生产服务器。

(6) 其它配置如果有需要，再创建测试服务器和测试服务器安全组。如果创建了新的服务器，需要手工添加到相应的安全组后才可被堡垒机访问。

最终实现的访问路径如下图：



金融云ECS与公有云的ECS在使用上略有不同，在搭建应用时还需要注意以下几点：

1. **互联网带宽及端口限制。**目前公有云互联网访问带宽可在ECS或 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。主要包括：
    - ECS外网TCP不能被外网直接访问，互联网用户可通过SLB访问ECS，带宽或流量在SLB上选取
    - ECS需要主动发起互联网访问时，在ECS需选取外网带宽，否则，带宽选0
2. 因为**金融云的SLB（负载均衡）和RDS（数据库）默认是同城双中心。**控制台上只能看到一个实例，但实际上会由分布在两个或多个可用区（机房）的服务集群提供SLB和RDS服务。所以只要**把购买的ECS均分到不同的可用区**，则整个系统就是一个具有容灾能力的同城双中心的高可用系统。
3. 构建业务系统的服务器（ECS），建议选配多台低配，而不是一台高配，通常2核CPU/2G内存或4核CPU/4G内存即可。如果某台ECS发生故障，其它ECS还在正常提供服务，从而达到高可用的目的。**从高可用的角度考虑，提供相同功能的ECS台数越多，故障期间对整体性能影响越小，可用性也越高。**
4. 建议每个业务模块，至少部署在两台ECS上（前端部署公网/私网SLB）。否则整体系统存在单点，虽然能够正常运行，但是也要有发生故障（业务软件故障或ECS故障）暂停业务的预期。虽然云服务的可用性较高，但从概率上讲，在某个时点故障一定会发生。
5. **业务模块须配置成开机自启动**，当ECS故障自动迁移后，业务模块也能自动启动并提供服务。ECS自身和操作系统故障会触发自动迁移，业务模块故障不会触发。
6. 通常不需要购买公网带宽，而是在SLB上购买带宽，除非ECS有主动访问外网的需求。
7. ECS普通云盘单盘最高支持2TB存储空间（不包括系统盘），详细的介绍可以参考创建云盘。

8. 常见问题

Q：什么叫可用区？如何选择可用区？

A：可用区相当于物理机房的概念，指的是所购买ECS物理位于的哪个机房。同一功能的服务器，一半选择在一个可用区，另一半选择在同一地域的另一个可用区。

Q：ECS上的公网带宽有什么用？

A：如果ECS需要访问互联网上的资源，比如下载互联网上的文件、调用短信网关等，则需要选择公网带宽。需要注意的是，即使这里选择了公网带宽，互联网用户还是无法通过ECS分配到的公网IP访问到ECS。

Q：我购买了ECS上的公网带宽，但还是无法访问外网

A：如果是后加的公网带宽，必须通过**控制台对ECS进行重启**。在ECS内进行重启无效。

Q：我VPN登录后，无法ping通我的ECS

A：ECS默认不允许ping操作。建议通过堡垒机去ping。如果想从VPN客户端直接ping，可创建一个新的安全组，名称为sg-icmp，入站规则处，选择ICMP协议，源地址写为VPN登录后分配的IP地址，然后点击“添加规则”，并将服务器添加进该安全组。

Q：我无法登陆我的ECS

A：首先你要登录VPN，请参考前面的VPN相关内容。然后ECS默认不允许登陆，需要通过ECS安全组配置防火墙，允许SSH协议或RDP协议后才可以登陆ECS。SSH使用TCP协议22端口，RDP使用TCP协议3389端口。配置的源IP地址要配置为VPN自服务控制台中看到的“客户端IP列表”。建议通过堡垒机登录，请参考上面的内容实现堡垒机。

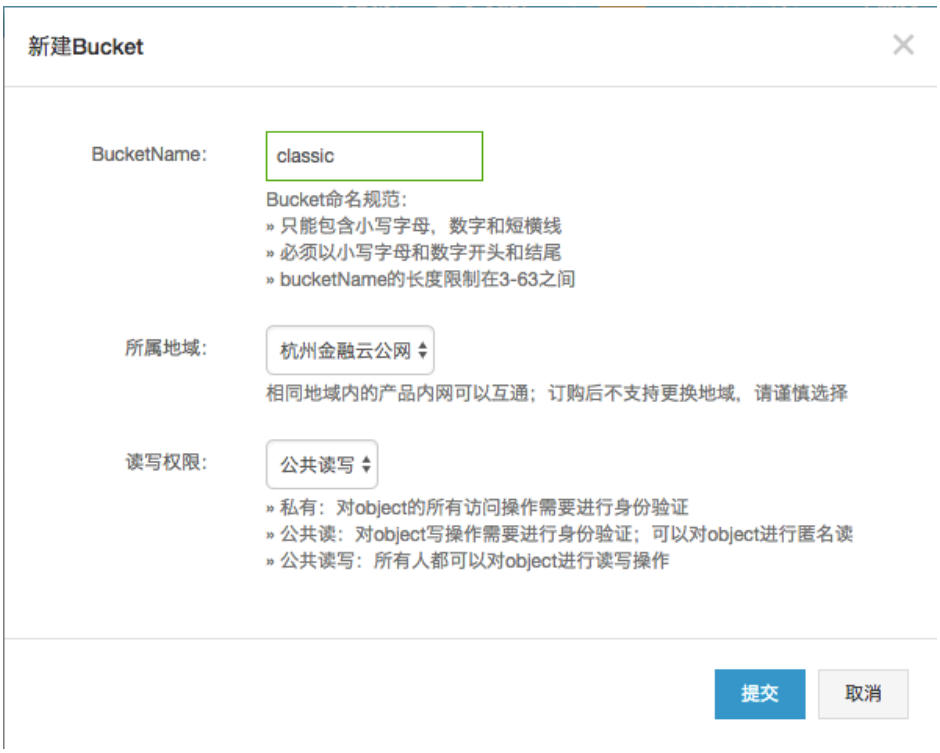
Q：互联网用户无法访问到我的ECS

A：互联网用户需要通过SLB才能访问到ECS，具体能参考SLB的配置方法。

Q：如何上传下载文件

A：上传文件之前，请先通过安全组开通远程管理端口。Linux操作系统请使用sftp协议进行文件上传(可使用图形化的sftp协议工具winscp，参考winscp官方帮助)，Windows操作系统请使用远程桌面的连接本地驱动器功能，参考这里和这里。

也可以利用OSS进行数据中转，bucket创建如下。



在SLB产品主页点击“立即购买”，或直接访问购买链接

其中的选项如下：

选 项	说明	建议选项
实例类型	“公网”用于对互联网服务，实例创建后的服务地址是公网IP地址；“私网”用于阿里云内部服务器之间进行负载平衡，服务地址是内网IP地址。	按需要选择。由于金融云ECS不能被互联网直接访问，因此如果服务要对互联网提供，至少要创建一台“公网”类型的SLB。
地域	可选华东1，华东2，华北1，华南1，华东2。SLB所在地域必须与ECS服务器所在地域相同。	生产ECS和SLB选择在华东1

公网带宽	按流量计费或按带宽计费。	根据自己的业务特点，选择最经济的方式。一般按带宽。

SLB配置

SLB开通后，在SLB管理控制台上可以看到SLB实例的信息，包括地域、服务地址等。将域名解析到服务地址即可对外提供服务。

接下来要配置SLB，点击“管理”进入实例监听配置页面。

监听配置添加-> “监听” -> “监听配置” -> “添加监听”

在这里要修改“基本设置”和“健康检查设置”。

选项	说明	建议选项
SLB协议	网站一般选择HTTP协议或TCP协议。如果是HTTPS协议的网站，可以选择HTTPS 或 TCP 443端口。如果是用户自定义协议，选择TCP，自定义端口允许的范围是80,443,2800-3300,5000-10000,13000-14000	HTTP，80端口
后端协议	协议会自动与SLB协议一致，端口选择为后端服务的监听端口，一般与上一个选项相同	
转发规则	“轮询模式”会将外部和内部的访问请求依序分发给后端ECS进行处理，而“最小连接数模式”会将外部和内部的访问请求分发给当前连接数最小的一台后端ECS进行处理。	轮询模式
会话保持	是否将同一用户的请求转发到同一台ECS处理。如果后台程序无法做到完全无状态，这里需要打开	打开
虚拟服务器组	虚拟服务器组可满足需要在监听	根据需要配置

	级别设置后端服务器和端口以及需要使用域名和URL转发的需求。具体使用可以参考虚拟服务器组使用要点	

TCP健康检查设置 TCP协议的健康检查设置中，最关键的是其中的“端口检查”，一定要确认后端的ECS服务器上的端口是正确的。否则会导致SLB认为后端服务不可用，从而不再向后端ECS转发请求。

HTTP健康检查设置 HTTP协议的健康检查设置中，最关键的是其中的“检查路径”，一定要确认后端的ECS服务器上的这个HTTP路径是可访问的。否则会导致SLB认为后端服务不可用，从而不再向后端ECS转发请求。

其它选项请参考SLB帮助

接下来要添加后端服务器，选择“服务器”->点击“未添加的服务器”，选中要添加的服务器，点击“添加或批量添加”

这时候SLB就配置完成了。

金融云SLB特性

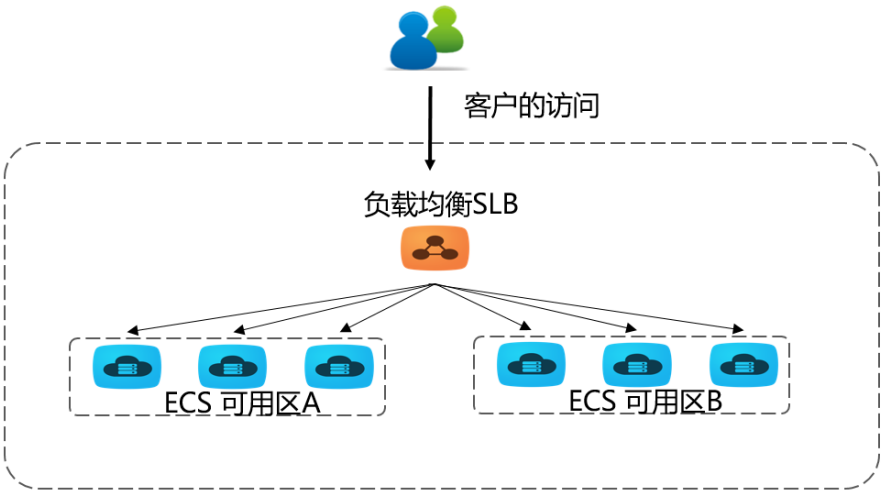
1. SLB是金融云的唯一公网接口，必须通过SLB对外提供互联网服务。
2. SLB服务默认是同城双中心，并会生成一个固定的公网IP地址，用户需要把DNS解析至这个IP地址。故障可能会导致提供服务的机房发生变化，但此时实例的公网IP地址不会发生变化，对用户是透明的。
3. 会话保持功能，开启后会把用户请求转发到同一台ECS上处理。会话保持的流量转发逻辑：4层是源IP，7层是Cookie。详见SLB配置页面及相关帮助。
4. 健康检查功能，开启后会自动隔离故障服务器，故障恢复后自动重新加入SLB。
5. 可以提供4层和7层负载均衡，分为公网和私网两种类型。
    - 公网SLB。公网流入带宽可以认为无限大，流出带宽按购买规格而定。
    - 私网SLB。每个监听端口最大1G带宽，每个实例最大累计10G带宽。
    - 后端服务器只能是ECS，不支持RDS、SLB等其它云产品。
    - 4层只支持TCP和UDP。
    - 7层负载均衡支持HTTP和HTTPS。如果为HTTPS，安全证书需要托管在SLB上。
    - 4层的源IP地址（客户端IP）不发生变化；7层是应用层代理，源IP地址会被替换，如果要获得真实的源IP，可以使用Http Header:X-Forwarded-For，请参见：[https://help.aliyun.com/document_detail/27650.html]
    - 不支持FTP、SFTP协议。
6. SLB是后付费服务，即开即用。开通有两个前提：
    - 至少有一台ECS，正常运行时，一台后端服务器也可以，只是这样存在单点风险。
    - 实名认证，并有100元余额：[https://help.aliyun.com/knowledge_detail/37100.html]
7. 计费规则，请参见：[https://www.aliyun.com/price/product#/slb/detail]请确保余额充足，以免因欠费而影响业务。

搭建金融云推荐架构

金融云推荐架构对应的SLB部分实现方法如下：

1. 在华东1地域购买一台固定带宽5Mbps的公网SLB(与购买的ECS在同地域)
2. 在华东1两个可用区的多台生产服务器上部署并测试应用
3. 在SLB上创建服务监听，协议为HTTP/80，打开会话保持，确认健康检查路径可用
4. 将所有的生产服务器加入SLB的后端服务器

这样，就搭建完成了推荐架构的ECS和SLB部分：



常见问题

Q：SLB上可以开放哪些端口？

A：金融云SLB上允许以下端口：80,443,2800-3300,5000-10000,13000-14000，不在此列的端口暂不支持。

Q：通过SLB后，访问我的网站显示503错误，可是我在ECS 上测试是正常的

A：这是由于SLB健康检查失败，SLB无法找到可转发的服务器。请检查SLB服务监听的健康检查设置，比如ECS上的网站部署在/app/访问路径下，根路径下未部署任何应用，而健康检查中的检查路径设置的是/，这样当健康检查去访问根路径时，ECS返回404错误，导致ECS认为网站无法正常提供服务。这时只要把健康检查的路径也设置为/app/就可以了。可参考：SLB健康检查配置文档

Q：如何支持HTTPS协议？

A：在服务监听上选择HTTPS协议或TCP协议的443端口。

Q：我无法开通SLB，开通SLB的按钮是灰色的。

A：SLB开通要求先有ECS，完成实名认证，并且有100元以上的余额。

Q：通过SLB之后，我无法看到客户端的源IP地址了

A：请参考SLB帮助文档

Q：SLB的流量和带宽如何计算？

A：只计算公网出流量(从阿里云流向互联网)，公网入流量(从互联网流入阿里云)不计流量、不计费。

开通数据库服务

在RDS产品主页点击“立即购买”，或直接访问购买链接

其中选项如下:

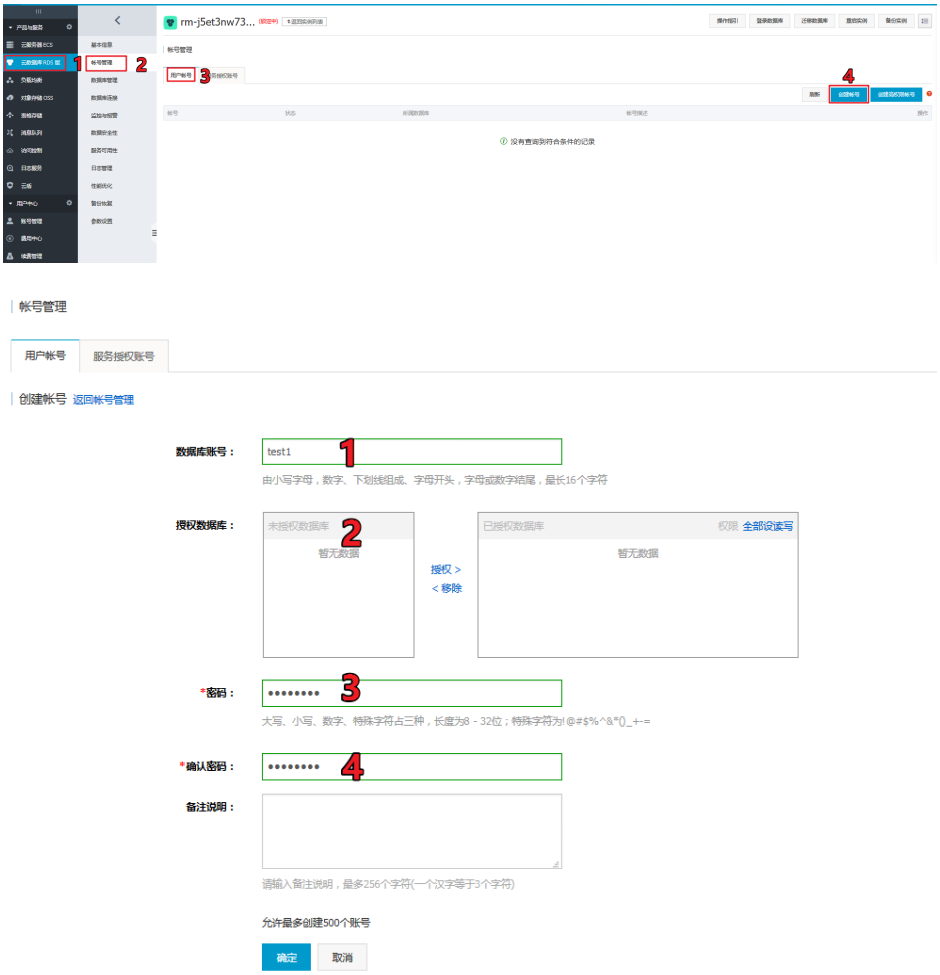
选项	说明	建议选项
地域	生产中心选择华南1，华南1自动同城容灾（可用区A+B）。ECS、SLB、RDS都必须在同地域。	华南1，华东2
数据库类型	可选MySQL/SQL Server/PostgreSQL/PPAS（兼容Oracle）	MySQL
系列	金融云集群有且仅有双机高可用版本	
规格	数据库可用内存/CPU大小，选择不同的规格对应不同的连接数和IOPS并发	根据需要选择。
存储空间	选择数据库可用的存储空间	根据需要选择

配置数据库服务

数据库建立后，在数据库管理控制台上可以看到数据库实例的基本信息：

其中的内网地址比较重要，ECS上的程序访问数据库服务器就是通过这个内网地址。（内网地址的开通前提条件，需要设置RDS白名单才可以开通。）

之后需要创建帐号，在“帐号管理”中选择“创建帐号”。



设置好用户名、密码，点击提交完成。（数据库授权可以完成账号添加后，进行授权）

然后创建数据库，选择“数据库管理”，点击“创建数据库”。创建时将权限授予刚才创建的帐号，并设置为“读写”

设置允许哪些ECS访问：

点击“数据安全性”，再点击“添加白名单分组-加载ECS内网IP添加”。

请选择需要访问RDS的服务器，然后点击“确定”。

金融云RDS产品特性

1. 连接数据库不使用IP地址，而是使用域名，形如：sy52d0hz76w.mysql.rds.aliyuncs.com。
2. 默认具有同城灾备功能，并且故障时自动切换。如果对数据安全性要求较高，需要再开通青岛灾备实例。
3. 发生故障切换后，可能会断开网络连接，建议业务程序中要有自动重连的容错逻辑。
4. RDS单实例的处理能力有明确上限，且只能向上升级。如果需要分布式数据库，可以使用DRDS。
5. 不支持外网连接，且只允许ECS访问RDS。
6. 如果需要更高级别的高可用，则建议采用两地三中心方案，分为以下两种情况：
    - 数据(RDS)。只需要在青岛节点开通RDS灾备实例即可，杭州地域全部不可用后，手动切换到青岛实例。
    - 业务系统。除了开通青岛节点的RDS灾备实例外，还需要在青岛部署同等/降低配置和数量的SLB和ECS。杭州地域级别的灾难发生后，通过DNS切换到青岛节点来保证业务系统的整体高可用。
7. 选型建议
    - 存储空间（G）= 天交易量(笔/天) *每笔交易大小（KB）* 保留天数 /1024/1024

- 规格的选取与业务峰值IOPS,连接数有关，详细参照
  https://help.aliyun.com/document_detail/26312.html

搭建金融云推荐架构

金融云推荐架构对应的RDS部分实现方法如下：

(1) 在杭州新建一个RDS实例(2) 新建用户(3) 新建数据库，并把新建的用户授权为读写权限(4) 在白名单中加入ECS生产服务器

至此，完成了完整的金融云推荐架构搭建工作。

OSS是阿里云提供的海量文件存储服务，它适用存储照片、视频、HTML/JS等静态文件。同时它也是一种在线服务，不需要借助于SLB和ECS，只使用OSS就可以搭建出一个静态网站。在分布式架构设计中，OSS也常被用做静态文件的共享存储。

使用OSS前，需要熟悉它的概念和原理，例如Bucket和Object等。它也提供了丰富的API和SDK，也提供了一个Python命令行工具，使用这个工具能够方便地完成大部分OSS操作：
http://docs.aliyun.com/?pos=7#/oss/utilities/osscmd&install。

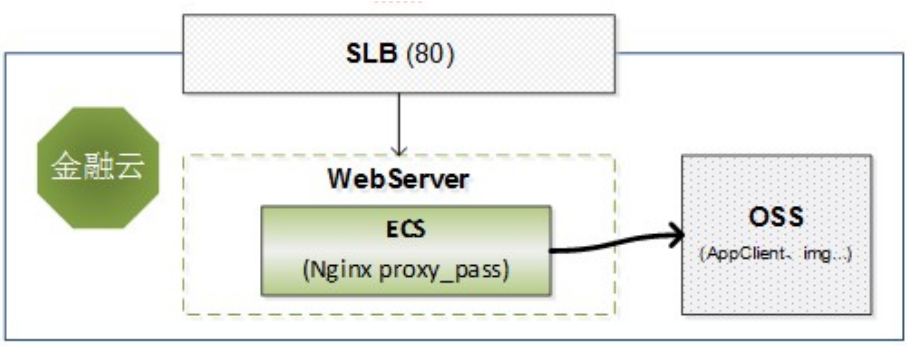
金融云Region的OSS服务有如下的特点，在使用中需要注意：

1. 默认bucket仅限于金融云内部访问，与公网是物理隔离的。需要对公网访问需要创建外网类型bucket对外提供服务。
2. 如果把默认纯内网Bucket的访问权限设置为public，只是在金融云内部可以被其它用户访问，互联网用户不能访问。如果需要，必须由ECS转发，再由SLB提供互联网服务，或直接使用公共云OSS。如下图，在金融云中可以通过Nginx转发实现的OSS公网服务，也可能使用apache等或自已实现。微金融用户无此限制。
3. 计费规则，按实际存储容量计费，同时是后付费类型。请参见：
   http://www.aliyun.com/product/oss/?#price。

   金融云各地域的OSS的Host是：

```
oss-cn-hzfinance-internal.aliyuncs.com(华东1)
oss-cn-shenzhen-finance-1-internal.aliyuncs.com(华南1)
oss-cn-shanghai-finance-1-internal.aliyuncs.com(华东2)
```

5. 金融云oss暂时不支持流量包。



金融云杭州、青岛区域使用的都是经典网络，系统会直接分配IP地址给云产品。在金融云深圳区域，我们提供了VPC，使得用户可以更加自由的使用网络环境。通过以下步骤，您将会学习通过控制台来搭建1个VPC网络(网段为192.168.0.0/16)，在这个VPC内创建1台交换机，并开通1个ECS实例。

1.登录控制台

开通VPC服务后，通过管理控制台，点击“专有网络(VPC)"，进入VPC产品控制台。

2.创建专有网络

选择深圳地域，点击右上“创建专有网络” ，创建名为“SZproduction”的专有网络。用户可以在私有网段10.0.0.0/8,172.16.0.0/12,192.168.0.0/16中根据自身需要进行选择，这里我们选择192.168.0.0/16。

3.创建交换机

在交换机列表，点击右上“创建交换机”，创建名为“A区生产交换机”的交换机，可用区选择深圳呢可用区A，网段填写专有网络的子网，比如192.168.0.0/25。

4.创建ECS实例

点击交换机列表右侧“创建实例”，可以进入购买页面。在购买页面需要选择专有网络所在的地域深圳、深圳可用区A，然后选择网络类型为“专有网络”，选择已经创建好的“SZproduction”和“A区生产交换机”。

至此，VPC环境下的ECS创建完成，后续可以添加SLB或绑定EIP来开通对外服务。

关于VPC的详细介绍及使用，请查阅
https://docs.aliyun.com/?spm=5176.775975630.2.5.zm7Kvx#/pub/vpc

亲爱的金融云用户
因当前经典网络VPN服务产品暂时调整，目前决定暂停新用户的经典网络VPN接入，具体开放日期请等待通知，谢谢。

本篇文档针对的是杭州金融云经典网络的硬件IPSEC VPN接入，VPC环境的IPSEC VPN搭建可以参考[VPC VPN搭建]。

IPSec VPN使用的是互联网线路，链路质量比专线差，它的优点是费用低（阿里云侧目前免费接入），使业务数据可以在公网上通过IP加密信道进行传输，不再受地域和运营商的限制， 实现业务间的快速对接。如果客户对链路质量和安全性要求较高，建议使用**专线**接入方式。

1.IPSEC VPN对接条件

必备条件：

1）.申请IPSEC VPN的单位需要在金融云上拥有ECS的服务器数量大于或等于五台。

备注：不允许通过IPSEC VPN方式对接其它机构的ECS，只能访问自己的ECS。

2）.机构侧需要具备一台支持IPSEC VPN的网关设备，推荐采用JUNIPER的防火墙设备，如ISG，SSG，SRX系统防火墙，其它品牌的网关设备不保证能对接成功，请自行联系代理商或厂商进行配合。

3）具有独立的公网地址，不支持NAT环境，动态的公网地址。

2.IPSEC VPN对接说明

1）提交申请

在满足上面必备条件后，可以在售后工单系统中提交接入申请，填写附件：2016金融云VPN对接需求申请表

2）参数说明

对接VPN的参数全部以阿里的附件中规范的参数为准，不提供个性化的定制参数的需求。

预共享密钥，感兴趣流，IPSEC VPN的所有参数均由阿里提交，机构端只要提交相应的公网地址。

3）阿里侧配置

阿里网工在收到相关的工单后，进行接入配置。通常为两周左右，其它品牌的网关设备不保证能对接成功，需自行联系代理商或厂商进行配合。

其它说明

接入周期

1. IPSEC_VPN涉及软件联调，接入过程时间长，通常为两周左右，且有可能两端设备不匹配，导致接入失败。

线路备份

1. VPN没有线路备份能力，只能与阿里云建立一条VPN隧道。

费用

1. IPSec-VPN目前暂时全免费，所有VPN线路共享固定带宽，不限制单个VPN的实际带宽。
2. 阿里云把专线/VPN上的数据流量和带宽视为内网流量，不收取任何费用。

常见问题

Q: VPN联调时，如果阿里云访问机构不通怎么办？

A: 需机构网工确认，是否机构端已做好表格中应用调用的VIP到机构真实IP的防火墙策略，阿里云出口未做策略限制。

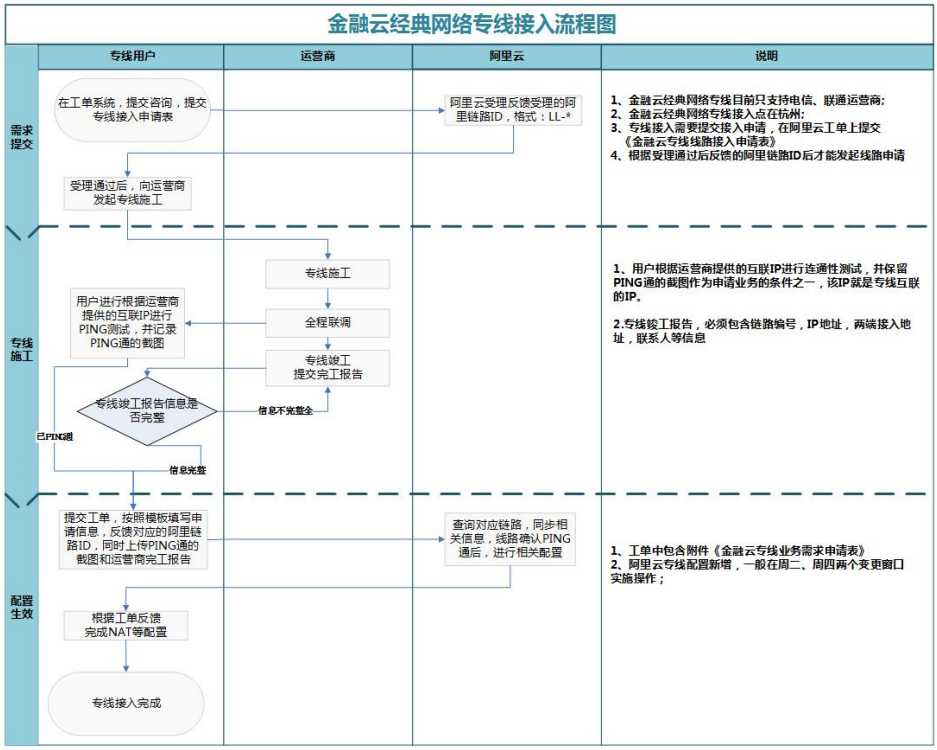
Q:专线/VPN联调时，如果机构访问阿里云不通怎么办？

A:确认您在阿里云上的ECS安全组防火墙是否打开，ECS安全组默认不允许任何源访问,安全组的操作可以参考安全组使用帮助。

本篇文章主要针对的是杭州金融云经典网络专线接入，金融云VPC集群的专线接入可参考VPC物理专线接入。

为了实现企业与阿里云机房的互通，金融云经典网络提专线接入支持。专线类型支持MSTP，一般网络端口类型是RJ45。金融机构可以复用其与阿里集团的现有专线链路，网络上进行安全控制。也可新增一条物理链路，建立与阿里集团的连接。机构间通过防火墙进行隔离。

接入流程



接入主要分为三大部分

专线接入申请。目前金融云经典网络只在杭州有专线接入点。如需要进行专线接入需要提交工单，选择工单类型：“金融云相关问题 > 申请专线/VPN接入”。在工单中阿里云会提供《金融云专线接入申请表》，用户填写完毕上传后，后台进行申请审批，审批完工后会返回给用户唯一的阿里链路ID：如：LL-20161124112421450。

联系运营商进行专线施工。

专线施工，需要与运营商协商专线价格及服务协议等事项。

提交工单进行专线业务接入申请。

进行业务接入申请的前提是物理链路已经到位并测试通过，需用户在工单中已提交专线施工完毕的完工报告，同时提交链路PING通对端的截图。

填写金融云业务需求申请表，通过控制台的工单模块提交到阿里云，选择工单类型：“金

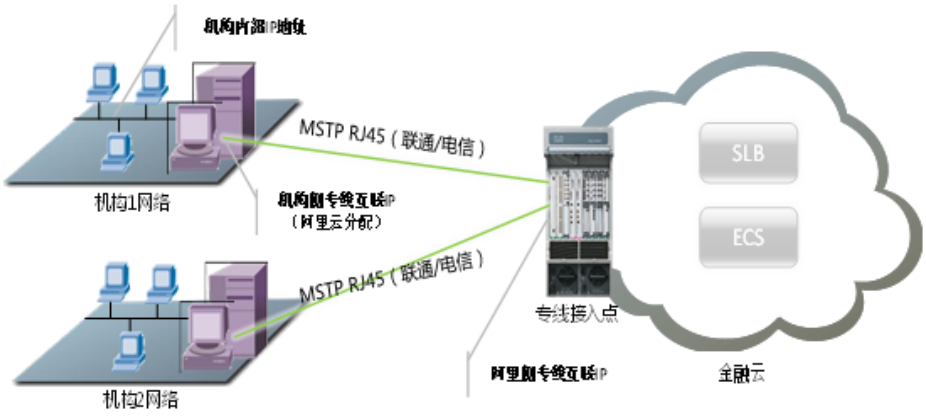
融云相关问题 > 申请专线/VPN接入”。

- 金融云专线业务需求申请表
- 完工报告(样例)

所有专线接入过程，都是通过工单形式交互，阿里网工暂不提供电话支持。专线施工时，运营商员工会向阿里网工协商施工时间、技术支持等事项。

在经典网络环境下，专线接入成功后，会由阿里云分配几个互联IP地址，机构与金融云之间的访问需要通过分配的IP地址进行，也就是需要在机构侧配置NAT转换。例如从机构主动发起到金融云的访问，需要把源地址转换成分配的互联地址（源NAT，如下图）；从金融云主动发起到机构的访问，需要把目的地址转换成机房内部的地址（目的NAT）。因为阿里云分配的IP地址个数有限，必要时需要结合目的IP和端口转换到机构内部的某个服务。

从机构访问金融云上的ECS服务器，还需要在ECS上进行防火墙配置（安全组），允许来自机构侧互联IP地址（阿里云分配）的访问。机构侧的防火墙也应进行相应的安全配置。



其它说明

支持运营商

1. 目前杭州经典网络专线只支持电信和联通运营商线路，暂不支持***移动***线路的接入；

接入周期

专线接入周期，市内链路1个月左右，省际链路1个半月左右，具体以运营商施工时间为准。

专线业务对接周期：在链路状态已经为调通状态下，五个工作日完成网络相关配置。 一般在周二/周四两个变更窗口实施操作。

线路备份

1. 如果对线路备份有要求，可以同时接入双运营商线路。这两条线路可以同时承担业务流量，当故障发生时，一条线路上的流量会自动切换到另一条线路；
2. 每条专线都由阿里云分配了固定的接入IP地址，每条专线上传输的流量是由IP地址控制的，所以能够做到线路的双活。阿里侧检测到线路故障，会自动把两条专线的IP地址都合并到健康的专线上，用户的网络配置也需要支持此种模式；
3. 双线都接入后，建议进行故障演练。

地址规划

由于金融云经典网络的IP地址均统一由阿里云规划，而且阿里云会为每一个客户初始化分配一个掩码为/29 的IP地址段，共8个地址。可根据ECS的实际数量进行IP地址扩容。

扩容规则如下：

10台>ECS数量 > 0 台 只分配8个业务IP

100台>ECS数量 >10 台 每增加10台可新增8个业务IP

1000台>ECS数量>100台 每增加100台可新增64个IP地址，最多只能申请254个IP地址。

费用

1. 专线费用需要与运营商洽谈，非浙江省为长途专线；
2. 如果已经与阿里云建立专线，则新业务可以复用原来的专线，必要时进行扩容；
3. 阿里云把专线上的数据流量和带宽视为内网流量，不收取任何费用。

常见问题

Q：金融云是否支持专线接入？如果支持的话，支持何种线路？如何收费？

A:支持专线接入，接入点位于杭州，只支持电信、联通。接口方式为MSTP和千兆光纤专线接入时，阿里云不进行任何收费，物理链路的费用需要用户自行与运营商进行洽谈，金融云配合物理接入机房并参与网络联调。

Q：专线接入对带宽的要求是什么？

A:用户根据自己的实际情况计算所需内网专线带宽bps，TPS（笔/秒） X 每秒交易大小（KB） X 8/1000，带宽接口类型推荐如下：

2M 及以上推荐MSTP。

Q:是否支持NAT服务？

A：支持NAT服务，但是需要收取每条nat规则50元/天的费用。

比如您添加了4条nat规则，那我方每天收取200元的费用。

Q:金融云如何与支付宝业务对接？

A：金融云与支付宝对接已经不支持直接通过内网地址进行通讯，目前的方案是通过阿里的ABTN网络互通，要求被访问端具体公网的负载均衡地址，请求访问端需要具体出公网的环境。

简单来说：

支付宝访问金融云，用户需要有SLB的公网VIP，在SLB的公网VIP上打开支付宝公网出口地址的白名单，保证访问的安全。

金融云访问支付宝，就要求金融云ECS具备公网地址，同时支付宝具备有LVS的VIP，这个VIP一般是互联网VIP开443的端口访问。如果是其它非标希望不暴露到公网的形式，可以开办公网VIP，加白名单的方式实现，具体的地址用户可以咨询支付宝方面咨询。

Q:金融云的专线复用说明

A：金融云的专线和支付宝的专线由于分属于不同的安全域，因此不能够相互进行复用，所以在申请线路的时候一定要明确线路是对接到金融云还是对接到支持宝，否则后续会造成无法对接的情况。

Q:专线联调时，如果阿里云访问机构不通怎么办？

A：需机构网工确认，是否机构端已做好表格中应用调用的VIP到机构真实IP的防火墙策略，阿里云出口未做策略限制。

Q:专线联调时，如果机构访问阿里云不通怎么办？

A:首先，确认您在阿里云上的云盾防火墙是否打开，ECS安全组默认不允许任何源访问，其次，确认您的机构是否已完成机构端客户端到表格中NAT_IP的映射，您可以通过telnet命令进行验证端口是否已打开，详细操作请参考http://bbs.aliyun.com/read/157768.html?spm=5176.7189909.0.0.kLl0cY 。

Q:发起网络申请后，多久能得到反馈？

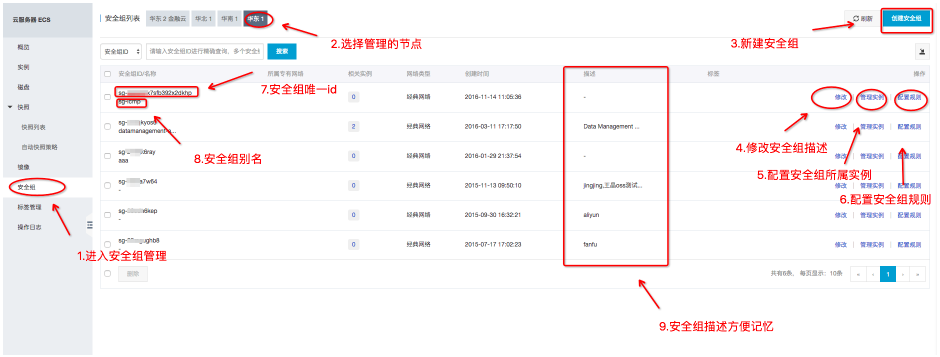
A:网工会在24小时内响应工单、反馈配置表，用户请先完成ECS防火墙、机构防火墙的策略设置，阿里云的策略生效日在每周二、四的晚上。整个联调完成按照经验值，专线需要3-5工作日。

安全组配置

在金融云上，安全组在ECS控制台-安全组进行配置，也可以通过API配置，这里推荐可以使用api封装的aliyuncli工具。安全组的基本限制可以参考安全组使用注意。

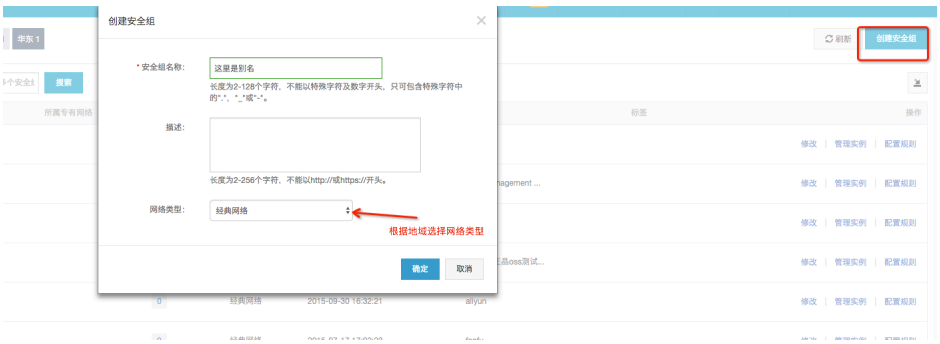
安全组配置步骤

1.进入“云服务器ECS”。选择左侧菜单中的“安全组”。



2.创建安全组

tips:华东1/华北1为经典网络，华南1和华东2为专有网络。创建的时候注意选择网络类型，默认都为经典网络。



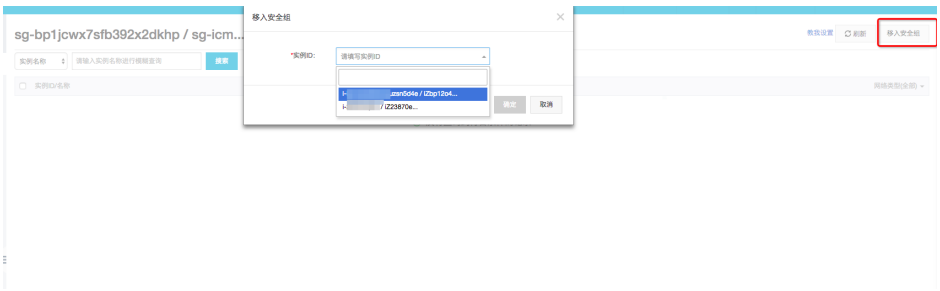
3.添加规则

tips1:创建管理VPN用户时，会为其分配新的客户端IP（最多5个），客户端内网IP与创建的VPN用户没有严格的对应关系，即每次登录管理VPN，你的内网IP都是从客户端IP列表中随机选择一个。因此在配置安全组规则时，需要你在将所有的源IP都添加到对应的规则中。

tips2:金融云经典网络ECS公网入方向默认放行UDP，TCP默认DROP。即使在安全组设置公网入方向TCP策略，也不会生效。其他的策略优先级可以参考下授权安全组规则。

tips3:专有网络下只有私网网卡，如需要对安全组授权配置私网策略即可，需要注意的是华东2/华南1的弹性公网IP默认屏蔽了22、3389等敏感端口，安全组即使放行也无法通信。

4.添加服务器进安全组



除了在云服务器控制台配置安全组外，还可以使用aliyuncli来进行配置，详细的可以参考。

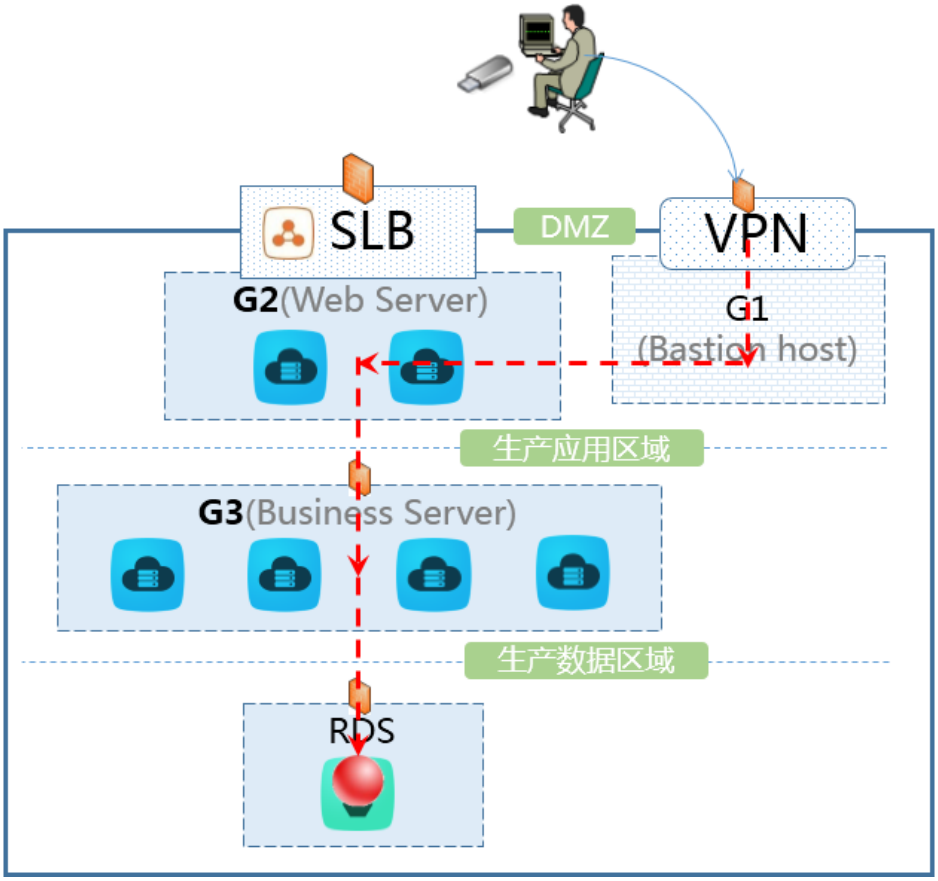
aliyuncli：https://help.aliyun.com/product/29991.html?spm=5176.doc30013.3.1.0Fmwby

ecsopenapi：
https://help.aliyun.com/document_detail/25553.html?spm=5176.product25365.6.308.NCXBI8

安全组推荐架构

经典网络中没有网段和网络边界，每个云服务器在网络中都处于同一层次，但可以利用安全组和安全规则来模拟传统网络体系中的各个层次（安全域）。例如可以划分出跳板机区、DMZ区、Web接入区、中间件区、核心数据区等，并能灵活地指定各区之间的ACL规则。

以一个典型的三层架构为例，可分为几个安全域：跳板机（G1）、Web接入（G2）、中间件（G3）和数据区（RDS）。如下图：



安全组	规则
G1	允许VPN拨入的IP地址访问22（SSH）或3389（远程桌面）端口
G2	允许SLB内网IP地址访问80端口
	允许G1安全组的内网22端口
G3	允许G2安全组的内网22端口
RDS	允许G3安全组的内网IP地址访问

通过以上安全组规则，运维路径是：

1. 拨入VPN；
2. 登录G1（跳板机或堡垒机）；
3. 登录G2（Web Server）；
4. 登录G3（Business Server）；
5. 通过G3上的数据库客户端登录RDS。

以上示例的是串行运维路径，通过多级跳板，深入到更敏感的运维区域；此种方式更安全，但登录操作稍复杂。还有一种是星型运维路径，G2/G3/RDS都允许G1（跳板机访问）。此种方式只有G1一级跳板，登录简单，但其它组没有层次，安全性相比串行方式要差一些。

目前跳板机就是普通ECS，金融云用户需要自行配置。专业的堡垒机目前正在产品化过程中，后续会开放，简要介绍请参见：
http://help.aliyun.com/knowledge_detail.htm?categoryId=8315059&knowledgeId=5974748&pos=1

。

安全组用户来划分ECS的安全域，不适用于其它云产品。例如RDS不适用安全组，RDS有自己的白名单，可以通过控制台来进行设置。不建议把跳板机IP地址加到RDS的白名单中，RDS运维通常在Web控制台进行，否则建议先登录跳板机再通过业务服务器做跳板（多级跳板），来运维RDS。

金融云专属数据中心

阿里金融云为金融用户提供在杭州、青岛、深圳、上海四地可以实现两地三中心的高等级绿色数据中心作为整个云计算平台的基础设施。相关的数据中心具备以下特性：

- 专属集群：阿里金融云服务是为金融行业量身定制的云计算服务，具备低成本、高弹性、高可用、安全合规的专属云计算集群，金融机构需要认证准入才能进行购买。
- 绿色数据中心：通过设备节能、节能监控、供电设备节能、制冷设备节能、节能建筑、节能管理制度等措施建设了全国绿色节能示范的数据中心。
- 容灾备份：阿里云为适应金融行业对灾备的硬性管理规定，提供两地双中心和两地三中心的容灾方案。为一般业务提供双中心，核心业务提供两地三中心的独立专属定制的物理集群，享有独立网络带宽资源，避免性能争抢，提供高性能稳定的云服务。同时与公众集群隔离，单独管理，提供更高级别的安全和稳定。
- 专线接入：提供安全的，私密的通讯机制，杜绝网络安全及传输过程中的敏感信息泄露，满足相关规范的要求。专线接入保证了和金融机构网络的高速连接，并确保业务的实时性要求。
- 多线BGP网络：阿里多线BGP网络实现了IDC直接和多个运营商互联，确保了不同运营商用户的高速访问。
- CDN服务：阿里云的CDN全国分布300多个节点，有效覆盖了全国不同地区，不同运营商，让每个用户都能快速访问。通过先进的系统架构、充足的带宽、节点资源应对大量用户集中的访问冲击。通过完善的监控体系和服务体系，以及丰富的CDN运营管理经验，为用户提供快速、高效、弹性的CDN服务。

堡垒机

堡垒机是为满足高端行业用户对运维人员远程访问系统资源进行集中身份认证、实现细粒度权限控制所开发的，具备实时操作审计能力的IT运维管理平台，堡垒机具备以下功能：

1、集中管理操作

图形操作（RDP/X-Window/VNC）

指令操作（Telnet/SSH）

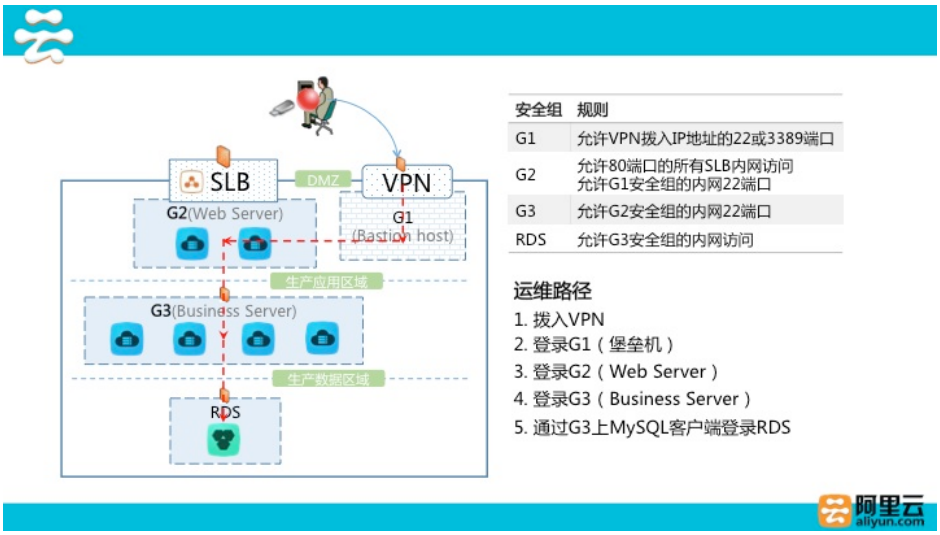
Web界面操作（HTTP/HTTPS）

2、严格权限控制

基于用户、设备/应用程序、协议类型、时间、IP等组合，实现细粒度的操作授权。

3、实时操作审计

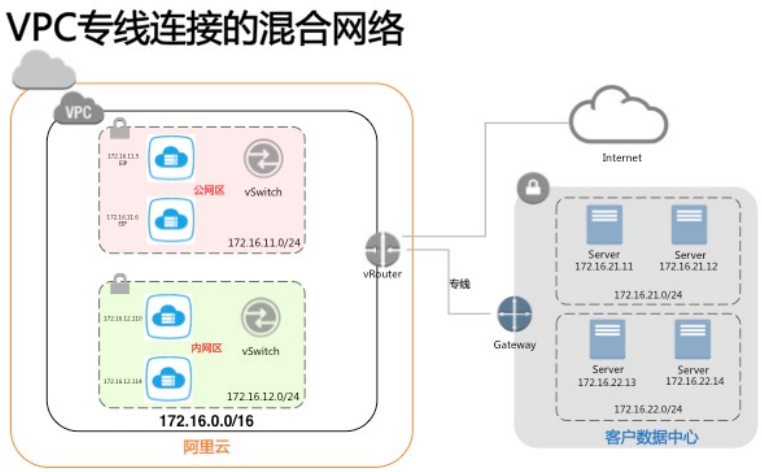
终端指令操作以文本方式记录，可搜索到操作的输入和输出的任一字段，Windows系统支持录屏操作。



阿里金融云提供多种第三方堡垒机服务，提供单点登录、账号管理、身份认证、资源授权、访问控制、操作审计等。

用户可以采购ECS，并在阿里云云市场选择堡垒机镜像，来搭建适合自己的堡垒机，例如安恒提供的堡垒机镜像：

https://market.aliyun.com/products/56844019/cmjj009962.html?spm=5176.730005.0.0.KKr1vP
可以利用阿里金融云的基础设施把客户数据中心网络扩展到阿里金融云，并划分互联网区和内网区。 通过专线连接到企业私有数据中心，以实现阿里云上的资源和自有数据中心的资源内网互联互通。 以下为VPC环境下的混合云示例，经典网络环境同样支持。

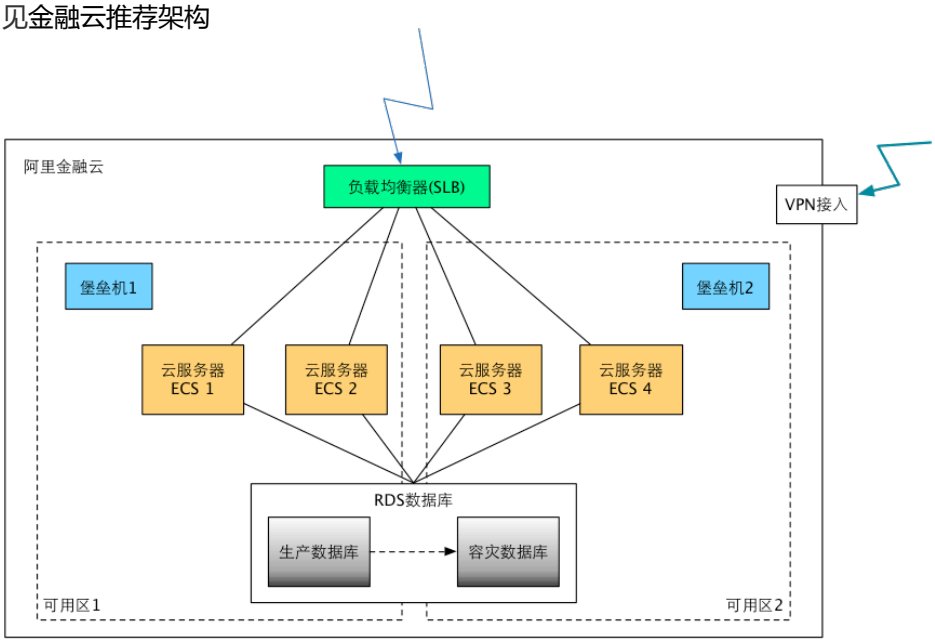


您可以通过VPC产品页面了解更多详情
http://www.aliyun.com/product/vpc/?spm=5176.383338.201.39.FeSVU6#Help

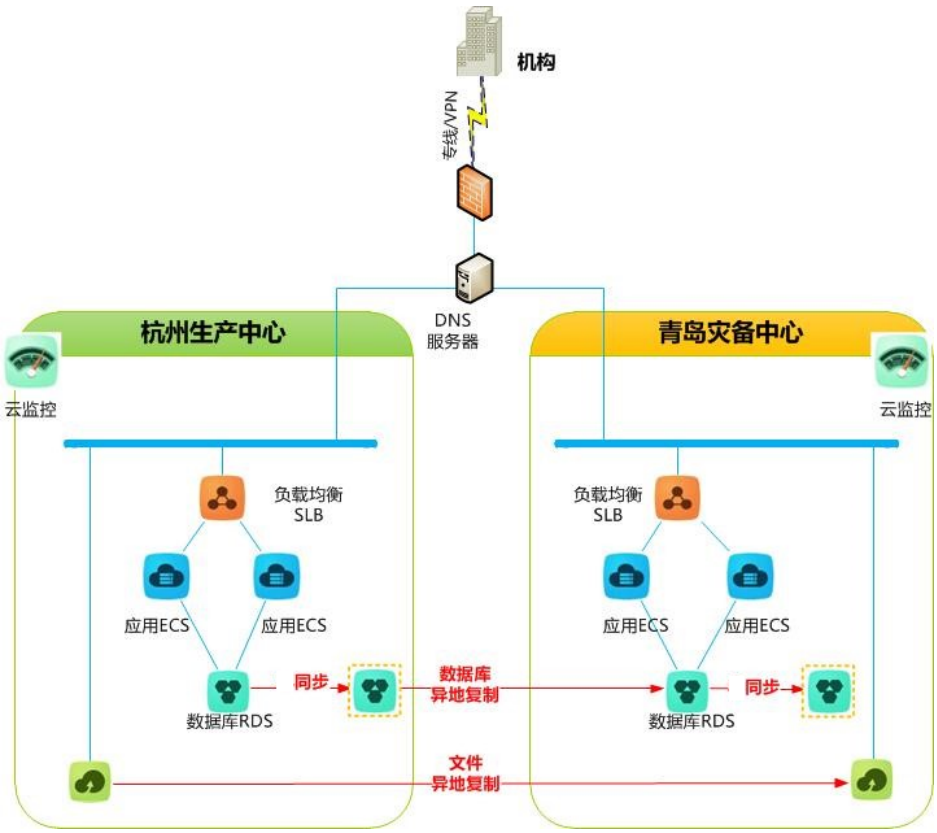
阿里金融云可以支持同城双活/灾备、异地双中心灾备、两地三中心等架构方式。

1. 同城双活/灾备

同城双活、灾备是阿里金融云的缺省特性，用户可以在30分钟内轻松搭建高可用的同城双活架构，具体方法参见金融云推荐架构

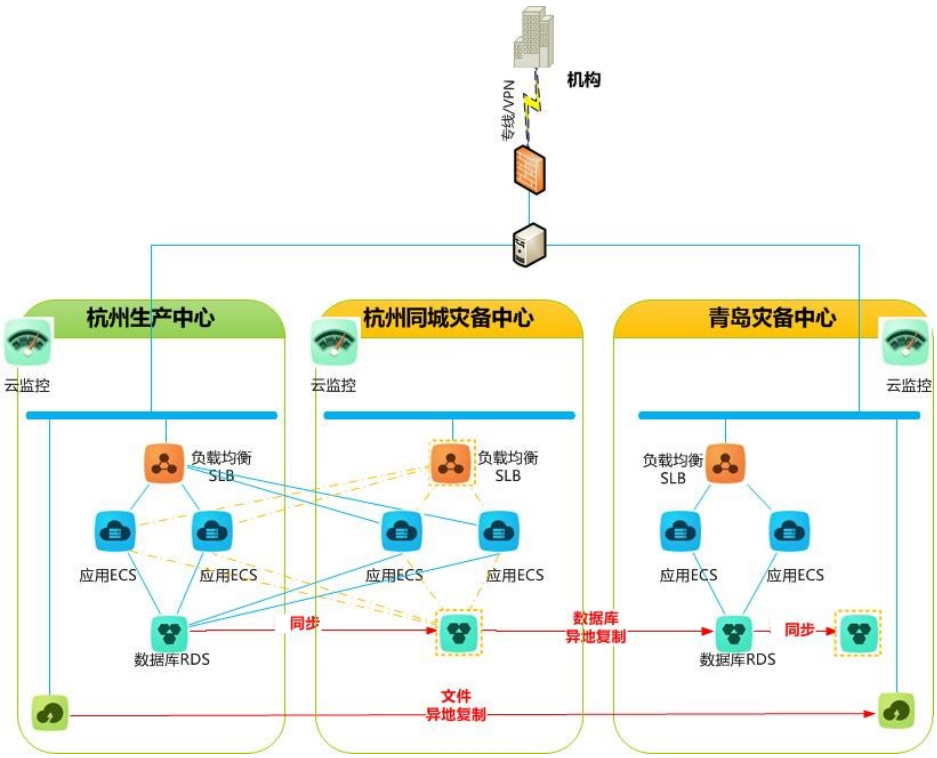


2. 异地双中心



1. 业务部署模式：相同的业务应用分别部署在阿里云两个节点（杭州和青岛），生产中心处于Active模式，灾备中心处于Standby模式。
2. 数据复制方式：RDS通过秒级准实时数据异地单向复制，将业务数据从生产中心传至灾备中心OSS通过分钟级数据异地单向复制，将文件数据从生产中心传至灾备中心。
3. 故障切换回切：通过DNS将应用IP从原生产中心修改到灾备中心，实现故障切换和服务恢复机制主站发生故障时，由备站继续提供服务。

3. 两地三中心



1. 业务部署模式：目前相同的业务应用可以分别部署在阿里云两个城市的三个数据中心中（杭州两个机房和青岛1个机房）。生产中心和同城灾备中心处于Active模式，应用访问同一数据库实例（数据在两个同城中心各存储一份），异地灾备中心处于Standby模式。
2. 数据复制方式：RDS服务实现从杭州生产到杭州同城灾备，再到青岛异地灾备的单向串级数据复制，OSS服务实现从杭州生产到杭州同城灾备，再到青岛异地灾备的单向串级数据复制。
3. 故障切换回切：DNS将生产IP从原生产中心修改到灾备中心，实现杭州到青岛的故障切换和服务恢复机制，主站发生故障时，由备站继续提供服务。

全方位安全服务

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，为互联网用户提供DDoS防护、CC攻击防护、云服务器入侵防护、WEB攻击防护、弱点分析、安全态势感知、渗透测试、信息内容安全检测及管控等一站式安全服务，帮助互联网用户轻松应对各种攻击、安全漏洞问题，确保云服务稳定正常。另外提供一系列的专家服务，输出阿里巴巴安全专家的经验保障客户的安全。针对金融行业日益严峻的安全威胁,金融云客户对安全需求的特殊性，阿里巴巴集团安全为金融云客户推出金融云安全评估服务。针对金融云客户的应用系统和云上业务系统，提供全体系的阿里安全服务体系，包括：安全咨询评估、应用安全评估服务、安全体系咨询和规划、安全教育与培训。

安全解决方案（云盾）	分类	产品	解决问题	
	安全管理	态势感知	构建安全管理体系，全面了解自身安全状况，让安全决策变得简单。	

	网络安全	DDoS基础防护	为ECS和SLB客户免费提供最高5Gb的DDoS防护功能	
		DDoS高防IP	提供20-300Gb的DDoS防护能力，同时具备200万QPS的CC攻击防护能力	
	服务器安全	安骑士	暴力破解密码拦截；木马查杀；异地登录提醒；高危漏洞修复。	
	信息安全	阿里绿网	提供多种违规内容（如赌博、色情、枪支等）的实时监控、检测和拦截	
	专家服务	渗透测试服务	通过模拟黑客攻击的方式，进行入侵尝试，评估出重大安全漏洞或隐患	
		服务器安全托管服务	服务器安全体检和加固，高危漏洞检测与修复，7*24小时安全事件响应	
		网络安全专家服务	提供重大活动进行人工值守和保障，99.9%的可用性SLA	
金融云安全咨询评估服务（SDL安全体系）	安全体系咨询评估服务	安全咨询评估	为金融云上客户量身定制安全咨询评估服务，帮助金融行业客户提升安全等级防御安全风险。	
		应用安全评估服务	为金融云客户提供，应用系统及移动端的安全扫描及加固方案，安全基线检查加固方案，黑盒安全测试及加固方案、白盒代码审计及加固方案。	
		安全体系咨询和	为金融云客户提	

		规划	供，安全管理及技术体系的设计和输出、安全SDL咨询服务全套体系的咨询、设计及输出。
		安全教育与培训	为金融云客户提供，信息安全意识培训、威胁建模培训、安全渗透测试培训、代码安全审计培训、安全应急响应培训、云上安全运维培训等
第三方产品	堡垒机		堡垒机主要解决包括账号管理、认证管理、权限管理、审计管理、自动化运维等功能，解决系统账号复用、运维权限混乱、运维过程不透明等IT运维难题。
	SSL/IPSEC VPN		VPN主要解决用户远程访问私有应用服务的敏感数据的安全问题，也是最简单最安全的解决方案。
	防火墙		防火墙主要保护保护内部网免受非法用户的侵入，在用户网络内部之间建立起安全网关，提供访问规则、验证、数据包过滤和隔离等功能。
	OTP双因素认证		OTP双因素认证主要解决服务器密码破解的问题，登录密码+密令的组合有效防止账号被破解的可能
	日志审计		对各种资产进行日志采集，对日志进行智能关联分析，实现多维度关联，内置众多的关联规则

			，支持多种攻防检测、合规性检测，并做出可视化展示	