ALIBABA CLOUD

阿里云

金融云解决方案
使用金融云产品（经典网络）

文档版本：20220211

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

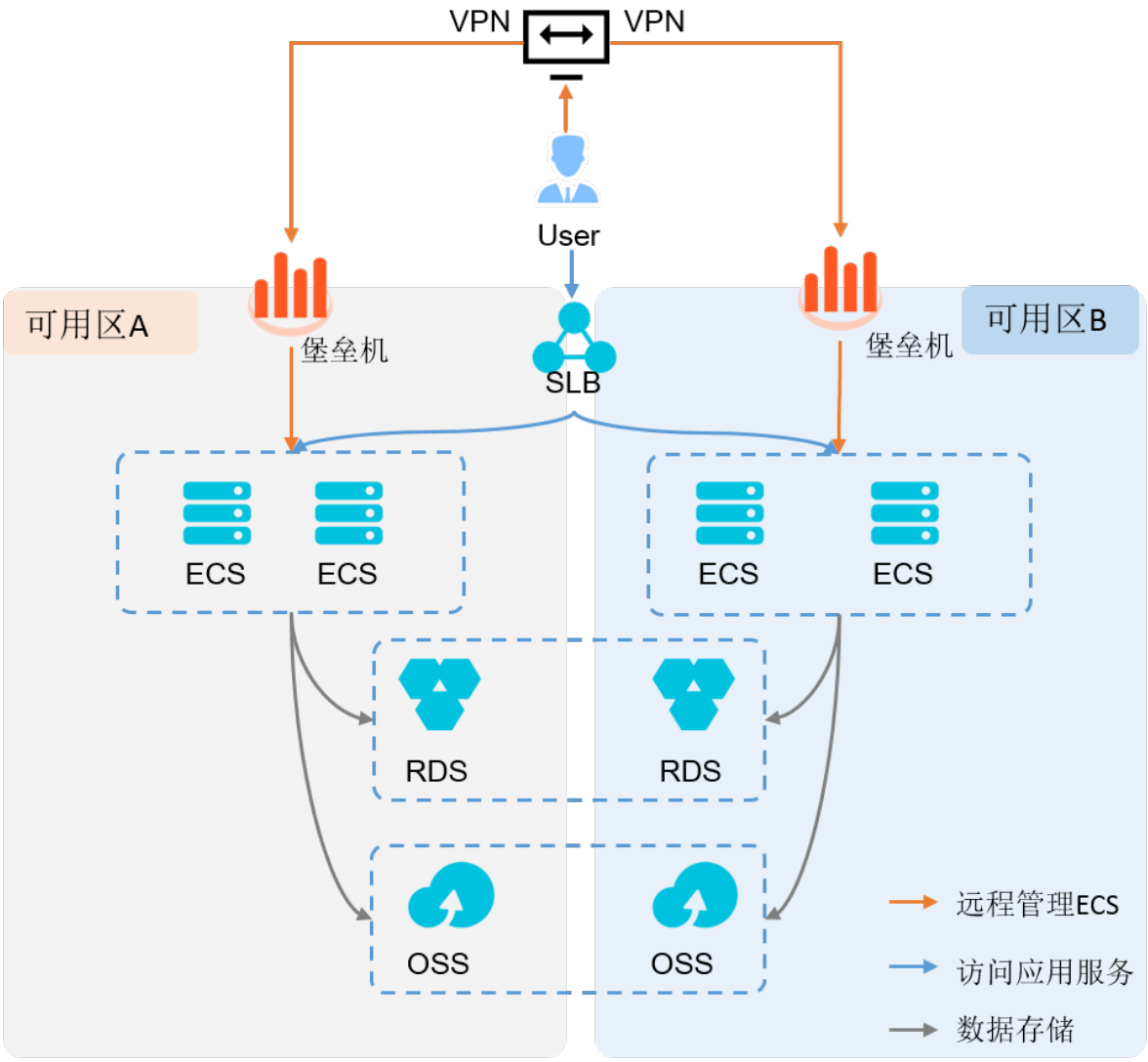
格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**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.金融云推荐架构（经典网络）

经典网络推荐架构

金融云在华东1（杭州）地域的集群为经典网络集群，在经典网络环境中，建议应用按以下架构搭建金融云环境。



架构说明：

- SLB： SLB用于互联网用户访问应用服务。
- VPN：金融云默认提供SSL VPN，可通过VPN接入进行服务管理。

  您也可以通过物理专线接入管理服务。
- 堡垒机：在两个可用区各购置一台堡垒机。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ECS服务器。
- ECS：在两个可用区分别购买数量相等的多台ECS服务器，如果应用架构支持，优先选择多台较低配置的ECS，而非少量高配置ECS。
- RDS：RDS会自动在两个可用区之间进行数据复制，两个可用区间自动保存两份完全相同的数据副本，具有优良的性能和可靠性，建议优先使用RDS MySQL或RDS SQL Server服务，而非自己搭建数据库服务器。

- OSS：OSS会自动在两个可用区之间进行数据复制，两个可用区间自动保存两份完全相同的数据副本，具有优良的性能和可靠性。

常见问题

Q：是否一定要按这个架构搭建金融云系统？

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。

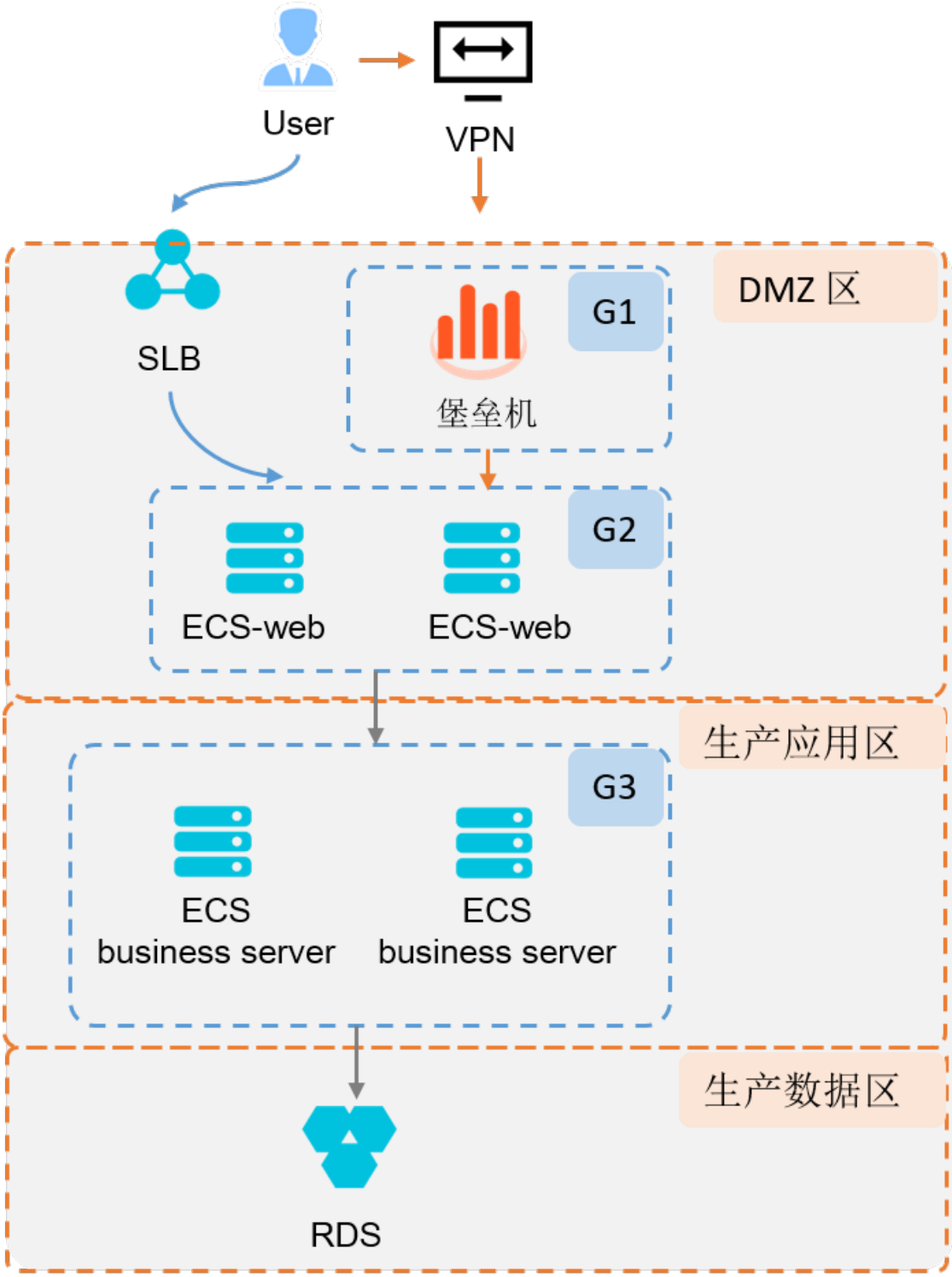
Q：堡垒机或跳板机是否是必需的？

A：不是必需的。但强烈建议使用堡垒机的方式管理服务器，这样更安全。堡垒机可以将所有在ECS服务器上进行的操作都详细记录下来（包括登录用户、IP信息、时间、操作行为、操作结果等，甚至提供操作的录像回放功能），一方面是解决金融行业企业安全运维的需求，更重要的是满足金融行业面临的针对审计机制的安全监管要求。

2.安全策略

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。您可以规划经典网络中的安全策略，例如划分出跳板机区、DMZ区、Web接入区、中间件区、核心数据区等网络隔离区，并能灵活地指定各区之间的ACL规则。通过此安全策略来模拟传统网络体系中的各个网络层次（安全域），实现网络隔离。

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



安全策略说明：

金融云产品	安全域	接入规则	接出规则
SLB	DMZ	允许互联网用户访问。	• 接出到ECS_Web。 • 协议/端口：tcp/80、443、6443、8080等，具体请参见金融云产品限制。
堡垒机	DMZ-G1	• 允许VPN拨入。 • 协议/端口：SSH/22；远程桌面（RDP）/3389	• 接出到ECS_Web。 • 协议/端口：Web管理/443；SSH和SFTP/60022；RDP/63389
ECS_Web	DMZ-G2	• 允许SLB访问。 • 协议/端口：http/https/tcp/1~65535 • 允许堡垒机访问。 • 协议/端口：TCP/22~3389	• 接出到ECS_APP。 • 协议/端口：tcp/1~65535
ECS_APP	生产应用区-G3	• 允许ECS-Web访问。 • 协议/端口：TCP/具体的应用端口	• 接出到RDS/OSS。 • 协议/端口：tcp/1~65535
RDS	生产数据区	• 允许ECS-APP访问。 • 协议/端口：TCP/3306	-
OSS		-	-

通过以上安全策略，运维路径是：

1. 拨入VPN；
2. 登录G1（堡垒机）；
3. 登录G2（Web Server）和G3（Business Server），堡垒机对所有ECS进行操作审计；
4. 通过G3上的数据库客户端登录RDS。

互联网用户访问应用的路径是：

1. 接入SLB
2. 通过SLB接入应用

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。

此外还有一种星型运维路径，G2/G3/RDS都允许G1（堡垒机访问）。此种方式只有G1一级跳板，登录较简单，但安全性相比串行方式要差一些。金融云场景下建议您使用串行运维路径，提高整体的安全性。

3.配置安全组

前提条件

已完成阿里云账号注册、实名认证、金融云认证。

配置规划

安全组为ECS的关键概念，在新建ECS实例前需要先创建好安全组。根据安全策略，您需要创建2个安全组，安全组与安全规则详细规划如下：

地域	安全组名称	关联ECS	安全规则-入方	安全规则-出方
华东1	sg_g1	ECS_Web	允许SLB、堡垒机接入。 金融云场景下默认放行SLB；堡垒机的接入在开通堡垒机时可自动生成安全规则，因此此规则无需手动配置。	接出到ECS-APP。 • 授权类型：安全组授权（请根据实际ECS所属账号选择**本账号授权**或**跨账号授权**，本示例为**本账号授权**） • 授权对象：sg_g2
	sg_g2	ECS_APP	允许ECS-Web接入。 • 授权类型：安全组授权（请根据实际ECS所属账号选择**本账号授权**或**跨账号授权**，本示例为**本账号授权**） • 授权对象：sg_g1	接出到RDS/OSS。 金融云场景下默认放行ECS到RDS/OSS，因此此规则无需手动配置。

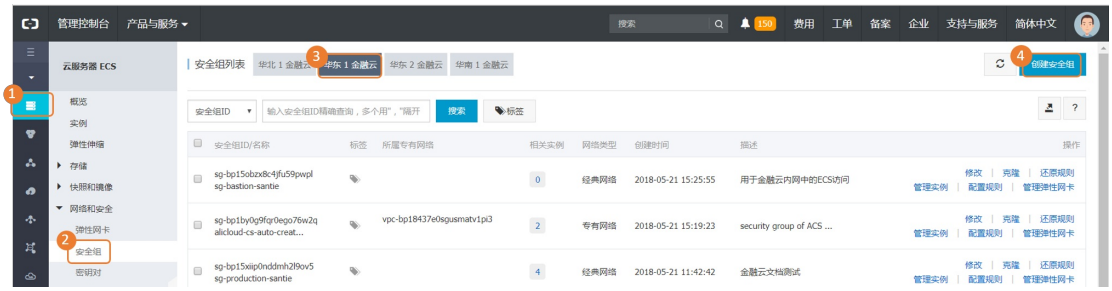
因此，根据规划，需要创建两个安全组，且每个安全组分别配置一条安全规则。

操作步骤

ECS的安全组配置可直接在控制台操作，也可以使用SDK来进行配置。以下以控制台操作为例，示例安全组的配置步骤。

1. 登录阿里云官网并单击右上方的**控制台**进入控制台页面。
2. 在左侧导航栏中选择**云服务器ECS**，进入ECS页面。
3. 创建安全组。

i. 在左侧导航栏中选择**网络和安全 > 安全组**，选择华东1金融云地域并单击**创建安全组**，进入创建安全组页面。



ii. 按照规划，输入安全组名称“sg_g1”，完成后单击**确定**。

iii. 重复上述步骤，完成另外1个安全组的创建。

iv. 记录sg_g1安全组的ID，用于后续堡垒机配置使用。

4. 添加ECS-Web的出方向安全规则。

i. 在左侧导航栏中选择**网络和安全 > 安全组**，进入安全组页面。

ii. 选择“sg_g1”安全组后单击**配置规则**，在配置规则页面单击**添加安全组规则**。

iii. 配置sg_g1的安全规则。

- 规则方向：出方向
- 端口范围：1/65535
- 权限类型：安全组授权（请根据实际ECS所属账号选择**本账号授权**或**跨账号授权**，本示例为**本账号授权**）
- 授权对象：sg_g2

iv. 单击**确定**。

5. 添加ECS-APP的入向安全规则。

i. 选择“sg_g2”安全组后单击**配置规则**，在配置规则页面单击**添加安全组规则**。

ii. 配置sg_g2的安全规则。

- 规则方向：入方向
- 端口范围：1/65535（此处为端口示例，请根据实际应用的端口配置）
- 权限类型：安全组授权（请根据实际ECS所属账号选择**本账号授权**或**跨账号授权**，本示例为**本账号授权**）
- 授权对象：sg_g1

iii. 单击**确定**。

至此您已完成经典网络下金融云推荐架构中需要手动配置的安全组。ECS安全组的基本限制可参考安全组使用注意章节。

4.创建ECS实例

前提条件

1. 已完成阿里云账号注册、实名认证、金融云认证。
2. 已根据安全组规划完成安全组创建。

背景信息

金融云ECS特性

金融云ECS（经典网络）有以下特性：

- 对于需要对外访问互联网上的资源的服务器，需要购买公网带宽。
- 日常管理可以使用SSL_VPN，具体可参考配置VPN。
- 线下和云上的业务通信需求推荐用经典网络专线接入和经典网络IPSecVPN接入接入。建议使用专线接入，提高网络的稳定性。
- 登录ECS可以参考金融云主机连接示例（经典网络）。

配置规划

根据金融云在经典网络下的金融云推荐架构（经典网络）及安全策略，您需要在华东1金融云地域的两个可用区分别创建2个ECS实例，分别用作Web接入服务器与应用服务器，配置ECS的规划如下表。

地域	区域	实例名称	所属安全域	所属安全组
华东1	可用区B	ECS_Web_01	G2	sg_g1
		ECS_APP_01	G3	sg_g2
	可用区D	ECS_Web_02	G2	sg_g1
		ECS_APP_02	G3	sg_g2

操作步骤

1. 登录阿里云官网并单击右上方的**控制台**进入控制台页面。
2. 在左侧导航栏中选择**云服务器ECS**，进入ECS页面。
3. 在左侧导航栏中选择**实例**，选择华东1金融云地域并单击**创建实例**，进入创建实例页面。
4. 基础配置：根据实际ECS服务器性能需求配置基础配置，然后单击**下一步：网络和安全组**。

   > 说明
   > - 此创建实例的步骤需重复两次，地域分别选择在可用区B与可用区D，每次购买2台。
   > - 建议选择多台低配的ECS而非少量高配ECS，本示例以企业级实例为例。企业级实例相关问题，请参见实例FAQ。

5. 网络和安全配置：

   经典网络场景下，网络选择**经典网络**，安全组请按照规划分别关联对应安全组，其他参数请根据实际需要配置。

6. 系统配置。

- 根据界面提示完成系统配置，建议您使用SSH密钥对以提高安全性。
- 完成后请记录root用户的密钥对或密码用于后续堡垒机的配置。

7. 完成后单击**确认订单**。

5.配置VPN

金融云架构下，使用VPN时建议您使用阿里云VPN网关。**旧版VPN产品已不再为新用户提供服务**。本文为您提供旧版本VPN产品的使用指导，仅作为老用户参考用。

前提条件

> **说明**
> - 如果您是新用户：建议使用阿里云VPN网关，使用VPN运维管理ECS请参考 SSL VPN入门 章节。
> - 如果您是老用户，已使用旧版的VPN产品，可参考以下步骤进行操作。

已完成阿里云账号注册、实名认证、金融云认证。

背景信息

根据经典网络下的金融云推荐架构及安全策略，ECS需要通过VPN接入堡垒机后进行管理。因此在配置堡垒机前您需要先完成VPN的配置，并将VPN客户端的所有IP地址添加至堡垒机的内网接入中。

操作步骤

1. 安装风云令。

   金融云管理VPN通过安装在手机上的动态密码软件实现强认证，因此在开通管理VPN之前，必须先安装风云令

   i. 在浏览器中打开风云令官方网站，在网站中下载对应版本的风云令客户端，或用手机扫描以下二维码：

   ii. 风云令安装成功后，选择**设置 > >查看序列号**，查看并记录序列号，用于后续VPN绑定。

2. 开通VPN服务。

   i. 在浏览器中打开VPN自助服务控制台：http://cloudvpn.console.aliyun.com/。

   ii. 如果：

   - 首次访问VPN自助服务控制台：
     a. 在页面中单击**立即开通**。
     b. 在弹出的窗口中设置VPN组名称并单击**确定**。进入VPN页面。
   - 此前已开通过VPN服务：
     a. 在页面中单击登录。
     b. 在弹出的页面上输入原来可登录的VPN登录用户名、风云令SN（Serial Numbers，序列号）和密码，进入VPN页面。

3. 添加VPN用户。

i. 在VPN页面选择**终端管理**页签。

ii. 单击**添加终端用户**。

iii. 在弹出的页面中输入用户名、上述步骤中记录的风云令SN码、邮件地址，并单击“OK”。

在终端管理页面中查看已添加的终端用户，并记录完整用户名（形式为“*用户名@VPN组名*”，例如：sample@aliyuntest），用户后续VPN登录。

4. 查看并记录客户端IP。

i. 在VPN页面选择**我的VPN**页签。

ii. 记录所有的客户端IP，用于后续添加于堡垒机的内网接入IP中。

5. 登录VPN。

您可以使用浏览器或使用PC客户端登录VPN：

- 使用浏览器登录时：
  a. 在VPN页面选择**我的VPN**页签。
  b. 单击**VPN登录地址**的链接，跳转至VPN登录页面。
  c. 输入用户名与密码。
     - 用户名：上述步骤中记录的完整用户名，例如：sample@aliyuntest。
     - 密码：首次登录时请打开风云令客户端，输入动态密码，完成后需设置PIN码。后续登录的密码为“PIN码”+“风云令动态密码”组成的完整密码。
  d. 浏览器登录后，界面提示安装VPN客户端，您可以选择安装客户端，后续直接使用客户端登录。
- 使用客户端登录时：
  a. （可选）下载客户端。
  b. 在浏览器中打开下载页面：http://106.15.64.216:8080/zh/troubleshooting。
  c. 在AG产品页下载合适版本的客户端及使用手册
  d. 按照使用手册的指导安装客户端并登录VPN。

6.配置堡垒机

前提条件

1. 已完成阿里云账号注册、实名认证、金融云认证。
2. 已完成安全组创建、ECS实例创建。
3. 已完成配置VPN且VPN正常登录。

背景信息

配置规划

根据金融云在经典网络下的金融云推荐架构（经典网络）及安全策略，您需要在华东1地域购置两台堡垒机，分别用于两个区域的VPN接入。详细规划如下。

地域	数量	堡垒机名称	所属安全域	关联安全组	凭据
华东1	2	• Bastion_01 • Bastion_02	G1	sg_g1_02	ecs_web_01 ecs_web_02

操作步骤

1. 登录阿里云官网并单击右上方的**控制台**进入控制台页面。
2. 在左侧导航栏中选择**安全（云盾）> 堡垒机（安全管理）**，进入堡垒机页面。
3. 购买堡垒机。
   i. 左侧导航栏中选择**实例列表**，单击**购买堡垒机**，进入购买页面。
   ii. 配置堡垒机基本参数：地域：华东1；网络：经典网络；数量：2；其他参数根据实际需求配置。
   iii. 单击**立即购买**，根据界面提示完成支付、购买。
4. 启用堡垒机。
   i. 在实例列表中找到购买的堡垒机，修改堡垒机名称，并单击**启用**。
   ii. 弹出的窗口中配置堡垒机的网络参数。

- 安全组：选择用于堡垒机接入ECS的安全组sg_g1。

  此处选择完成安全组后，系统自动在ECS的此安全组中创建一条安全规则，允许堡垒机接入此安全组中的ECS。
- 内网访问控制：将VPN所有客户端IP地址添加进来；
- 公网访问控制：经典网络的金融云场景下，禁止公网直接接入堡垒机管理ECS，所以这里请选择**不对公网开放**。

iii. 单击**确定**。

iv. 堡垒机启动需要约10分钟，请10分钟后刷新页面，堡垒机正常启动后进行管理配置。

5. 添加待管理ECS。

i. 在实例列表中找到购买的堡垒机，单击**管理**。

ii. 在弹出的页面中单击**内网接入**。

iii. 在弹出的页面左侧导航栏中选择**资产 > 服务器** ，并单击**同步阿里云ECS**。

iv. 在弹出的页面中搜索用于堡垒机访问的ECS，勾选后单击**加入云堡垒机**。

v. 关闭**同步阿里云ECS页面**，在堡垒机的服务器页面出现上述步骤勾选的ECS服务器。

6. 添加管理凭据。
   i. 在堡垒机页面的左侧导航栏中选择**资产 > 凭据**，单击**新建凭据**。
   ii. 在弹出的页面中配置凭据参数。

   - 登录名为root。
   - 凭据类型选择**密码**，密码为ECS操作系统root用户登录的密码。

   iii. 单击**确定**。
   iv. 重复上述步骤，完成另一个用于Web接入的ECS的管理凭据。
7. 新建用户。
   i. 在堡垒机页面的左侧导航栏中选择**用户 > 用户管理**，单击**新建本地用户**。
   ii. 在弹出的页面中填写运维人员的用户信息。后续SSH运维等操作可由此用户操作。
   iii. 单击**确定**。
8. 配置管理授权。
   i. 在堡垒机页面的左侧导航栏中选择**授权 > 授权组**，单击**新建授权组**。
   ii. 在弹出的窗口中自定义授权组名称。
   iii. 在授权组页面单击服务器列、用户列、凭据列，将上述步骤添加的服务器、用户、凭据添加至此授权组中。

执行结果

经典网络下，用户通过拨入VPN接入堡垒机管理ECS。完成上述安全组配置、ECS配置、VPN配置、堡垒机配置后，您可通过连接ECS服务器、上传下载文件等操作验证上述配置是否正确。

通过堡垒机远程登录ECS请参考SSH协议运维或RDP协议运维章节。

7.配置SLB

前提条件

已完成阿里云账号注册、实名认证、金融云认证。

背景信息

金融云SLB特性（经典网络）

- SLB是金融云经典网络下的唯一公网接口，必须通过SLB对外提供互联网服务。
- 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。
- 健康检查功能开启后，SLB会自动隔离故障服务器，故障恢复后自动重新加入SLB。
- 会话保持功能开启后，SLB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。
- SLB可以提供4层和7层负载均衡，分为公网和私网两种类型。
- 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。不支持FTP、SFTP协议。
- 7、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，请参见保留客户端真实源地址（七层监听）。
- 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。

配置规划

根据金融云在经典网络下的金融云推荐架构（经典网络）及安全策略，您需要在华东1地域使用SLB将互联网用户的访问请求转发至Web接入ECS。配置前的规划如下。

地域	主可用区	备可用区	规划说明
华东1	华东1金融云可用区B	华东1金融云可用区D	SLB优先将流量转发至主可用区，当主可用区不可用时，SLB将流量转发至备可用区。

操作步骤

1. 登录阿里云官网并单击右上方的**控制台**进入控制台页面。
2. 创建负载均衡实例。
   i. 在左侧导航栏中选择**负载均衡**，在**实例管理**中单击**创建负载均衡**。
   ii. 根据规划配置负载均衡参数。
   iii. 单击**立即购买**，根据界面提示完成开通。
3. 配置监听。
   i. 在实例管理页面找到上述添加的实例，单击**管理**，进入实例管理页面。
   ii. 选择**监听**页签，单击**添加监听**。
   监听配置包括**基本配置**与**健康检查**配置。详细的监听介绍和健康检查原理请参考监听概述、健康

检查概述章节。

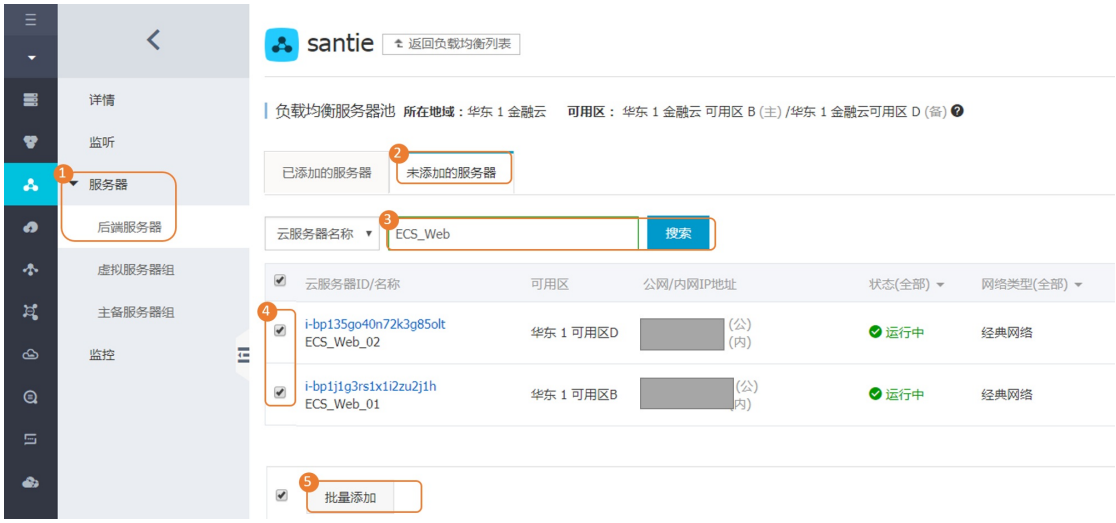
本示例以使用HTTP协议监听为例，实际配置时请根据您的ECS监听协议情况选择，更多的监听配置和健康检查配置请参考监听概述、配置健康检查章节。

选项	配置说明	示例选项
基本配置		
前端协议	■ 网站一般选择HTTP协议（七层监听）或TCP协议（四层监听）。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	HTTP，80端口
调度算法	SLB支持轮询、加权轮询（WRR）、加权最小连接数（WLC）三种调度算法。 ■ 轮询：按照访问顺序依次将外部请求依序分发到后端服务器。 ■ 加权轮询：权重值越高的后端服务器，被轮询到的次数（概率）也越高。 ■ 加权最小连接数：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。	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，需要打开会话保持。 会话保持配置可参考配置服务器Cookie章节。	打开

选项	配置说明	示例选项
基本配置		
虚拟服务器组	虚拟服务器组可满足需要在监听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。具体使用可以参考创建虚拟服务器组。	根据需要配置
健康检查配置		
检查端口	健康检查服务访问后端时的探测端口。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。	443
检查路径	指定用来进行健康检查探测的路径。请确认后端的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。	/
其他参数	建议保持默认值。	默认值

iii. 单击**确认**。

4. 添加后端服务器。
   i. 在实例管理页面选择**服务器 > 后端服务器**，进入后端服务器页面。
   ii. 在**未添加的服务器**页签中搜索用于Web接入的ECS服务器，勾选后单击**批量添加**。



iii. 在弹出的页面中单击**确定**。
在后端服务页面中查看已添加的后端服务器。

后续步骤

常见问题

Q：SLB上可以开放哪些端口？

A：金融云SLB上允许开放的端口有80、443、6443、8080等，具体限制请参见金融云产品限制。

Q：通过SLB后，访问我的网站显示404错误，开始我在ECS上测试时正常的

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。可参考配置健康检查。

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：请参考保留客户端真实源地址（七层监听）。

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。

8.配置RDS

前提条件

已完成阿里云账号注册、实名认证、金融云认证。

背景信息

金融云RDS特性（经典网络）

- 连接数据库不使用IP地址，而是使用域名，形如：sy52d0hz76w.mysql.rds.aliyuncs.com。
- 默认具有同城灾备功能，并且故障时自动切换。
- 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。
- RDS单实例的处理能力有明确上限，且只能纵向升级。如果需要分布式数据库，可以使用DRDS。
- 不支持外网连接，且只允许ECS访问RDS。
- 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，详细参照实例规格表。

根据经典网络金融云推荐架构，在华东1需要购置RDS，且RDS在两个可用区自动进行数据备份。详细的操作步骤如下。

操作步骤

1. 登录阿里云官网并单击右上方的**控制台**进入控制台页面。
2. 在左侧导航栏中选择**云数据库 RDS版**，进入RDS页面。
3. 创建实例。
   i. 在**实例列表**页面单击**创建实例**。
   ii. 配置RDS实例参数。
      - 地域：华东1
      - 可用区：多可用区7（可用区B+可用区D）
      - 网络类型：经典网络

   iii. 单击**立即购买**，根据页面提示完成支付。
   iv. RDS实例创建需要约10分钟，请约10分钟后进入**实例列表**页面查看RDS实例状态。
4. 添加ECS白名单。
   i. 在**实例列表**页面中找到上述步骤中创建的实例，单击**管理**，进入实例详细信息页面。

ii. 在**基本信息**模块查看内网地址，内网地址未显示，单击**设置白名单**。

iii. 在创建白名单页面单击**添加白名单分组**，输入白名单组名称。

iv. 单击**加载ECS内网IP**，勾选G3安全域内的应用ECS服务器。

v. 单击**确定**。

5. 创建用户。

i. 在实例详情页面左侧导航栏中选择**账号管理**，并单击**创建账号**。

ii. 配置账号信息。

- 输入账号用户名、密码。
- 数据库授权暂无需配置，完成账号创建后再授权。

iii. 单击**确定**。

6. 创建数据库。

i. 在实例详情页面左侧导航栏中选择**数据库管理**，并单击**创建数据库**。

ii. 配置数据库信息。

- 输入数据库名称并选择支持字符集。
- 授权账号选择上述步骤创建的账号。
- 账号类型选择**读写**。

iii. 单击**确定**。

在数据库管理页面查看数据库创建状态。

9.配置OSS

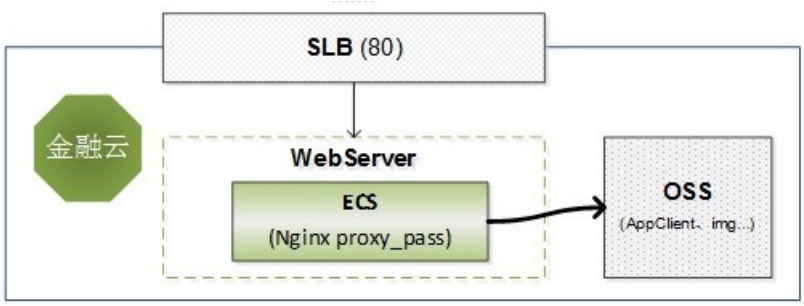
前提条件

已完成阿里云账号注册、实名认证、金融云认证。

背景信息

金融云OSS特性

- 金融云场景下，创建OSS的Bucket时可选择纯内网的场景（地域选择**华东1金融云**、**华东2金融云**或**华南1金融云**），也可选择公网场景（地域选择**华东1金融云公网**、**华东2金融云公网**或**华南1金融云公网**）。
- 纯内网类型的Bucket仅限于金融云内部访问，与公网是物理隔离的。公网直接访问Bucket时，需要创建公网类型的Bucket对外提供服务。
- 如果把默认纯内网Bucket的访问权限设置为**公共读**或**公共读写**，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，也可利用Apache实现转发服务。

- 金融云各地域的OSS的Host是：
  - 纯内网访问场景：

Region中文名	Region英文名	Endpoint地址
华东1	oss-cn-hzjbp	■ oss-cn-hzjbp-a-internal.aliyuncs.com（内网地址） ■ oss-cn-hzjbp-b-internal.aliyuncs.com（内网地址）
华东2	oss-cn-shanghai-finance-1	oss-cn-shanghai-finance-1-internal.aliyuncs.com（内网地址）
华南1	oss-cn-shenzhen-finance-1	oss-cn-shenzhen-finance-1-internal.aliyuncs.com（内网地址）

- 公网访问场景：

Region中文名	Region英文名	Endpoint地址
华东1	oss-cn-hzfinance	■ oss-cn-hzfinance.aliyuncs.com（外网地址） ■ oss-cn-hzfinance-internal.aliyuncs.com（内网地址）
华东2	oss-cn-shanghai-finance-1-pub	■ oss-cn-shanghai-finance-1-pub.aliyuncs.com（外网地址） ■ oss-cn-shanghai-finance-1-pub-internal.aliyuncs.com（内网地址）
华南1	oss-cn-szfinance	■ oss-cn-szfinance.aliyuncs.com（外网地址） ■ oss-cn-szfinance-internal.aliyuncs.com（内网地址）

- 计费规则，按实际存储容量计费，同时是后付费类型。请参见：对象存储 OSS。
- 金融云OSS暂时不支持流量包。

根据经典网络金融云推荐架构，在华东1需要开通OSS。详细的操作步骤如下。

操作步骤

1. 登录阿里云官网并单击右上方的**控制台**进入控制台页面。
2. 创建Bucket。
   i. 在OSS页面的右上方单击**新建Bucket**。
   ii. 输入Bucket名称，区域选择**华东1 金融云**，其他参数根据实际需要配置。
   iii. 单击**确定**。
3. 在OSS页面搜索找到上述步骤创建的Bucket，在Bucket的概览页面可查看Bucket的EndPoint和访问域名。
4. （可选）配置反向代理。

   如果您创建的Bucket是纯内网使用的Bucket，但是需要可以通过SLB、ECS的反向代理直接由外网访问，请参考以下配置进行反向代理的配置。

   i. 请参考绑定自定义域名，将创建的Bucket绑定您的自定义域名。

   > **说明** 请确保您的自定义域名已在阿里云已经备案，否则您的域名访问会被拦截。

ii. 参考配置SLB，创建一个SLB实例并配置完成80端口监听。

> **说明** 如果您需要使用加密的传输方式，需同时配置443端口的监听。

iii. 参考创建ECS实例完成ECS实例创建。

iv. 在ECS上安装Nginx。

- 如果您使用的ECS操作系统为CentOS，则使用Root用户远程登录后，运行以下命令即可一键安装Nginx。

  ```
  yum install -y nginx
  ```

- 如果您的ECS为全新的环境，您也可以安装镜像市场已经安装好nginx环境的镜像。
- 您也可以在Nginx官网自行下载Nginx安装包，手动安装。

v. 配置反向代理到OSS。

a. 执行以下命令进入反向代理配置文件目录。

```
cd /etc/nginx/conf.d/
```

b. 新建配置文件。

新建反向代理配置文件，包含以下反向代理配置内容。

```
upstream ossproxy {
server testsample.oss-cn-hzjbp-b-internal.aliyuncs.com;  #OSS的内网地址
}
server {
listen 80;
server_name aliyundoc.com;  #ECS网站对外访问的域名
access_log logs/ossproxy.access.log;
error_log logs/ossproxy.error.log;
root html;
index index.html index.htm index.php;
location / {
proxy_pass http://ossproxy;
proxy_redirect off;
proxy_set_header Host aliyundoc.com;  #Host要修改为OSS的域名或OSS控制台绑定的域名，否则OSS无法识别会报错
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_next_upstream error timeout invalid_header http_500 http_502 http_503 htt
p_504;
proxy_max_temp_file_size 0;
proxy_connect_timeout 90;
proxy_send_timeout 90;
proxy_read_timeout 90;
proxy_buffer_size 4k;
proxy_buffers 4 32k;
proxy_busy_buffers_size 64k;
proxy_temp_file_write_size 64k;
}
}
```

vi. 使用浏览器测试验证通过外网访问OSS，如能正常访问说明反向代理配置正常。

10.结果验证

完成金融云环境搭建后，您可根据本文介绍的方法验证环境搭建结果。

操作步骤

1. 登录ECS。

   请参见SSH协议运维或RDP协议运维，通过堡垒机远程登录ECS。

2. 部署应用。

   搭建一个WordPress网站，验证金融云环境搭建结果。WordPress网站搭建请参见云市场镜像搭建WordPress。

11.经典网络专线接入

如您使用的是金融云经典网络专线接入，建议您迁移至金融云VPC集群专线接入，详情请参见接入金融云专有网络。

12.经典网络IPSecVPN接入

> 注意　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。

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。

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。

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。