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：20180807

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

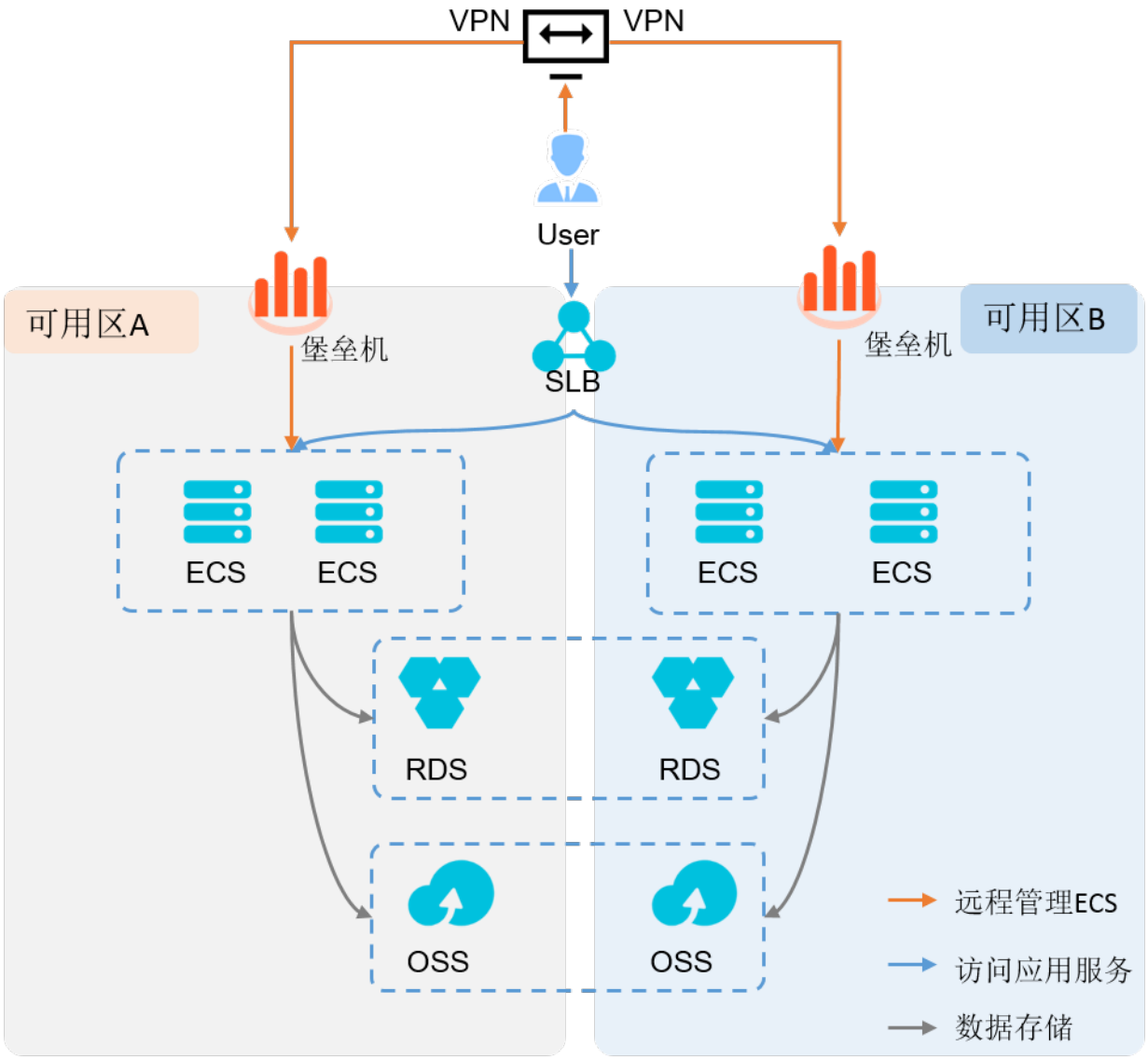
格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 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。	`swich` *`{stand | slave}`*

目录

1 金融云推荐架构（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？

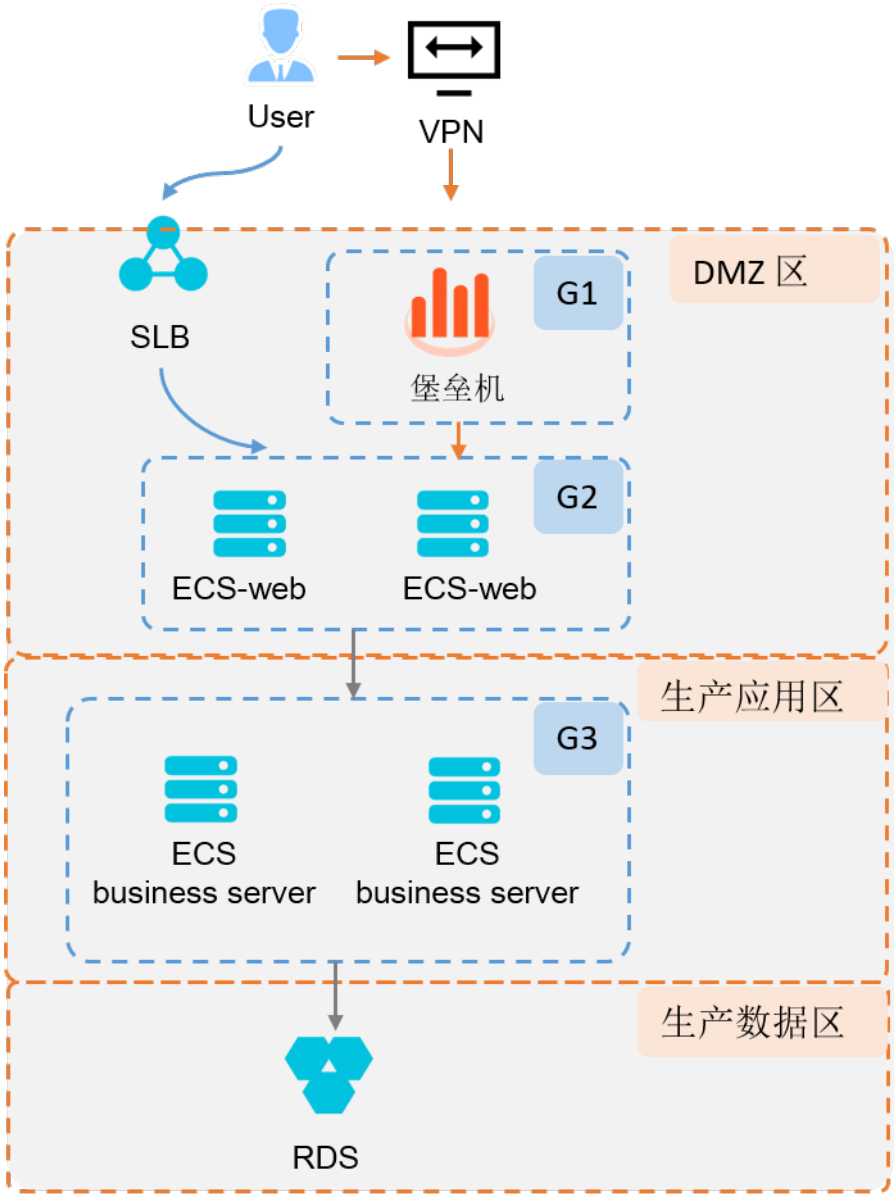
A：不是必需的。但强烈建议使用堡垒机的方式管理服务器，这样更安全。堡垒机可以将所有在ECS服务器上进行的操作都详细记录下来（包括登录用户、IP信息、时间、操作行为、操作结果等，甚至提供操作的录像回放功能），一方面是解决金融行业企业安全运维的需求，更重要的是满足金融行业面临的针对审计机制的安全监管要求

。

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/80,443,2800-3300,5000-10000,13000-14000,21234,22223,22225
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	• 接出到ECS_APP • 协议/端口：tcp/1~65535
		• 允许堡垒机访问。 • 协议/端口：TCP/22~3389	
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（跳板机或堡垒机）；
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

Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_quick

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。
   a. 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。

   b. 按照规划，输入安全组名称“sg_g1”，完成后单击**确定**。
   c. 重复上述步骤，完成另外1个安全组的创建。
   d. 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。
   a. 在左侧导航栏中选择**网络和安全 > 安全组**，进入安全组页面。
   b. 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**。
   c. 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

d. 单击**确定**。

5. 添加ECS-APP的入向安全规则。

a. 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**。

b. 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

c. 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. Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_quick
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（经典网络）

1. 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。
2. 日常管理可以使用SSL_VPN，具体可参考配置*VPN*。
3. 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。
4. 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. Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_login
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。

   完成后单击下一步：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。

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

前提条件

Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_quick

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。

详细操作步骤如下。

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

   a) 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：

   b) 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。

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

   b) 如果：

   - 首次访问VPN自助服务控制台：
     1. 在页面中单击**立即开通**。
     2. 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：
     1. 在页面中单击。

2. 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。

   a) 在VPN页面选择**终端管理**页签。

   b) 单击**添加终端用户**。

   c) 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。

   a) 在VPN页面选择**我的VPN**页签。

   b) 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：

     1. 在VPN页面选择**我的VPN**页签。
     2. 单击**VPN登录地址**的链接，跳转至VPN登录页面。
     3. 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。
     4. 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：

     1. （可选）下载客户端。
     2. 在浏览器中打开下载页面：*http://106.15.64.216:8080/zh/troubleshooting*。
     3. 在AG产品页下载合适版本的客户端及使用手册
     4. 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. Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_quick
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

操作步骤

1. Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_login
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。
   a) 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。
   b) 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。
   c) 单击立即购买，根据界面提示完成支付、购买。
4. 启用堡垒机。
   a) 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。
   b) 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。

c) 单击确定。

d) 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。

a) 在实例列表中找到购买的堡垒机，单击管理。

b) 在弹出的页面中单击内网接入。

c) 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**。

d) 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。

e) 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。

a) 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。

b) 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。

c) 单击**确定**。

d) 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。

a) 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**。

b) 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。

c) 单击**确定**。

8. 配置管理授权。

a) 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**。

b) 在弹出的窗口中自定义授权组名称。

c) 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。

预期结果

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

Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_quick

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：*https://help.aliyun.com/document_detail/27650.html*
- 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

地域	主可用区	备可用区	规划说明
			不可用时，SLB将流量转发至备可用区。

操作步骤

操作步骤

1. Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_login
2. 创建负载均衡实例。
   a) 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。
   b) 根据规划配置负载均衡参数。
   c) 单击立即购买，根据界面提示完成开通。
3. 配置监听。
   a) 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。
   b) 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介绍、健康检查原理章节。

   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配置四层监听、配置七层监听、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

选项	配置说明	示例选项
基本配置		
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
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。具体使用可以参考虚拟服务器组使用要点。	根据需要配置

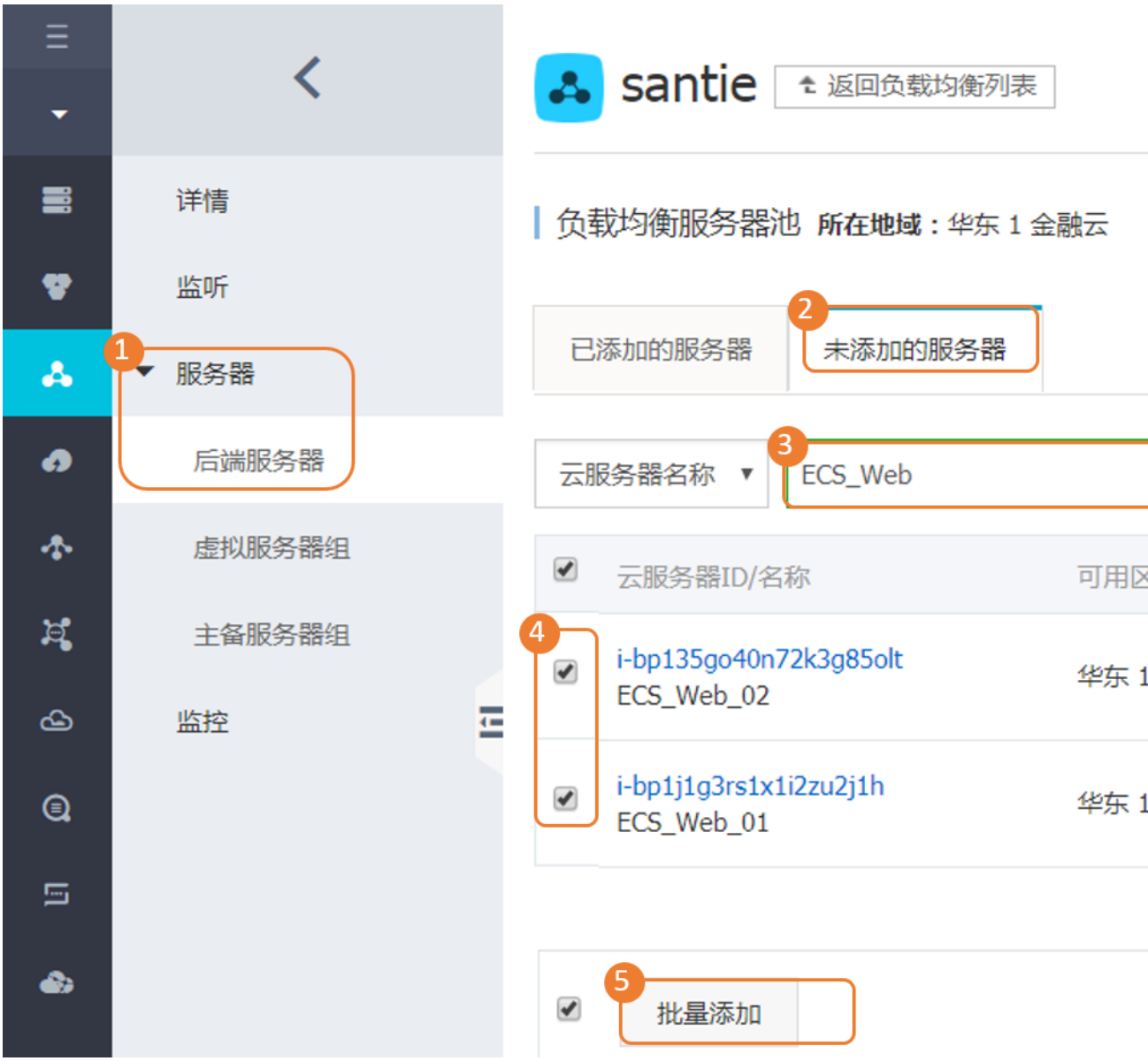
选项	配置说明	示例选项
基本配置		
健康检查配置		
检查端口	健康检查服务访问后端时的探测端口。TCP协议的健康检查设置中，最关键的是其中的“端口检查”，一定要确认后端的ECS服务器上的端口是正确的。	443
检查路径	指定用来进行健康检查探测的路径。请确认后端的ECS服务器上的这个HTTP路径是可访问的。否则会导致SLB认为后端服务不可用，从而不再向后端ECS转发请求。	/
其他参数	建议保持默认值。	默认值

c) 单击**确认**。

4. 添加后端服务器。

a) 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。

b) 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**。



c) 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。

后续操作

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**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：*SLB*健康检查配置文档

Q：如何支持**HTPPS**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。

8 配置RDS

前提条件

Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_quick

背景信息

金融云SLB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) x每笔交易大小#*KB*# x 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*。

操作步骤

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. Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_login
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。
   a) 在实例列表页面单击创建实例。
   b) 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

c) 单击**立即购买**，根据页面提示完成支付。

d) 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。

a) 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。

b) 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**。

c) 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。

d) 单击**加载ECS内网IP**，勾选G3安全域内的应用ECS服务器。

e) 单击**确定**。

5. 创建用户。

a) 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**。

b) 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。

c) 单击**确定**。

6. 创建数据库。

a) 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**。

b) 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**。

c) 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

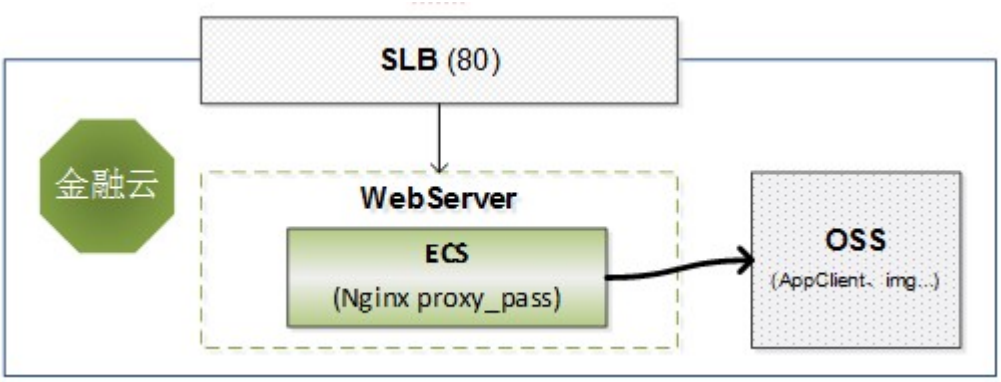
前提条件

Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_quick

背景信息

金融云OSS特性（经典网络）

- 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。
- 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）

Region中文名	Region英文名	Endpoint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：*http://www.aliyun.com/product/oss/?#price*。
- 金融云oss暂时不支持流量包。

操作步骤

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。

- Unresolved content reference to:../DNICMS1873156/ZH-CN_TP_14281_V1.dita#concept_tfc_1pr_zdb/text_login

- 在左侧导航栏中选择对象存储 **OSS**，进入OSS页面。
- 创建Bucket。

  a) 在OSS页面的右上方单击新建**Bucket**。

  b) 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。

  c) 单击确定。
- 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。

10 结果验证

完成上述金融云环境搭建后，您可在进行以下操作验证环境搭建结果：

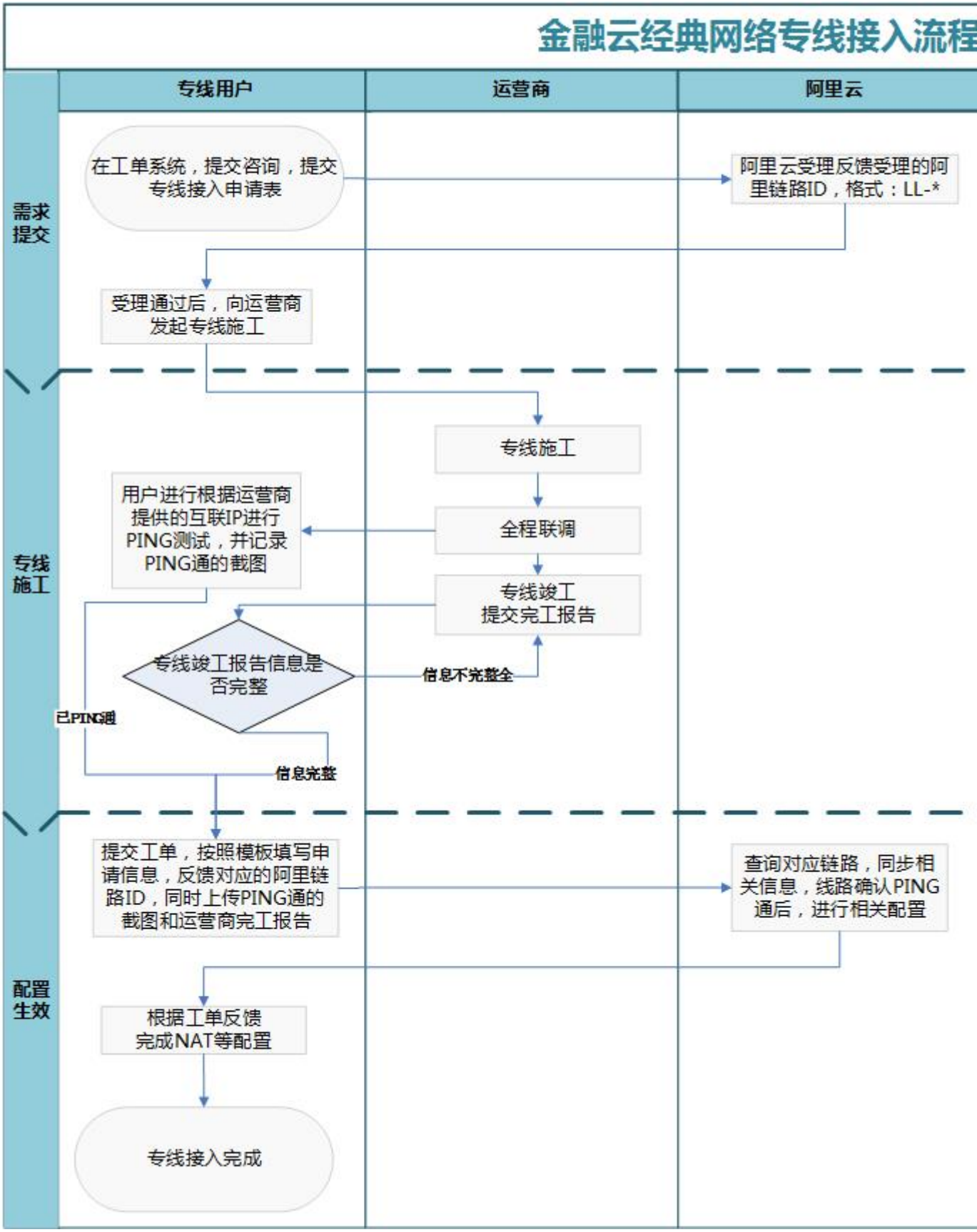
1. 登录ECS：请参考*SSH*协议运维或*RDP*协议运维章节，通过堡垒机远程登录ECS。
2. 部署应用：在此环境中搭建一个WordPress网站，验证金融云环境搭建结果。
   - WordPress网站搭建请参考搭建*WordPress*网站一文。

11 经典网络专线接入

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


金融云经典网络专线接入流程
专线用户
运营商
阿里云
需求提交
专线施工
配置生效
在工单系统，提交咨询，提交专线接入申请表
阿里云受理反馈受理的阿里链路ID，格式：LL-*
受理通过后，向运营商发起专线施工
专线施工
全程联调
用户进行根据运营商提供的互联IP进行PING测试，并记录PING通的截图
专线竣工提交完工报告
专线竣工报告信息是否完整
信息不完整全
已PING通
信息完整
提交工单，按照模板填写申请信息，反馈对应的阿里链路ID，同时上传PING通的截图和运营商完工报告
查询对应链路，同步相关信息，线路确认PING通后，进行相关配置
根据工单反馈完成NAT等配置
专线接入完成

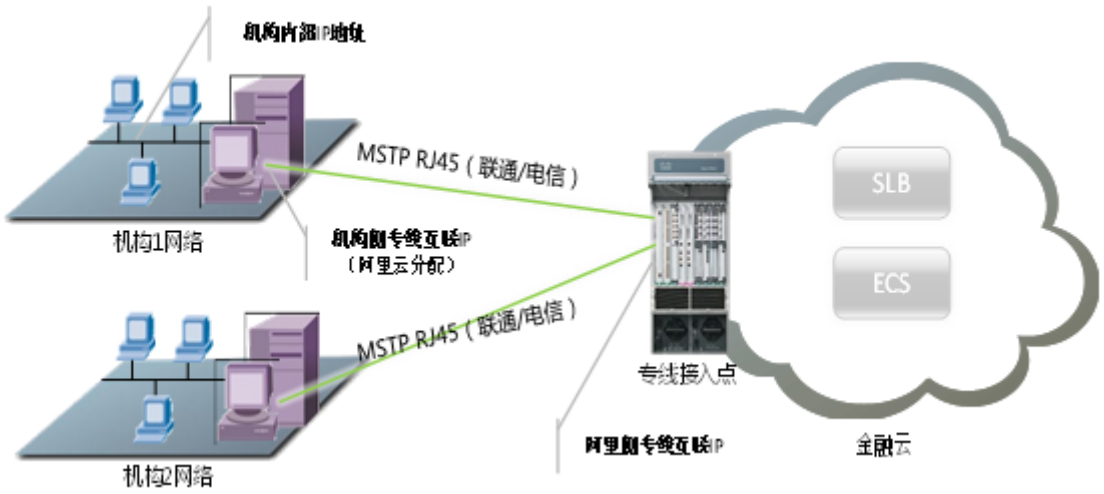
接入主要分为三大部分

1. 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。
2. 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。
3. 提交工单进行专线业务接入申请。
   a. 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。
   b. 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”。
   c. 金融云专线业务需求申请表
   d. 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

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

1. 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。
2. 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。

12 经典网络IPSecVPN接入

> 说明：
> 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。

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。