

## 7-1 选购云主机

140.143.132.225:8000/project-1/doc-133

### 一、购买云主机

云服务商有很多，但是我推荐大家使用腾讯云。之前我讲过阿里云超卖的事情，云主机IO性能非常差劲，我们要在云主机上面安装MySQL、MongoDB这样的数据库，硬盘IO能力必须要强一些。所以根本不能选用阿里云。除非你只用阿里云主机部署Java项目，然后再另花钱购买阿里云的MySQL和MongoDB服务。

购买云主机的时候，首选要则 **包年包月**，因为国内服务器绑定域名备案要三周时间，而且云主机想要申请域名备案，必须要 **包月半年以上** 才可以，否则腾讯云域名备案界面里根本无法找到你的云主机。

如果你等不及三周时间，你可以选购国外IDC机房的云主机，例如东京机房。国外服务器绑定域名是不需要备案的，但是从国内访问国外云主机的项目，网速很慢，切记！

快速配置

自定义配置

1.选择机型

2.设置主机

3.确认配置信息

计费模式

包年包月

按量计费

竞价实例

② 详细对比

地域

华南地区

华东地区

华北地区

西南地区

港澳台地区

广州

上海

南京

北京

成都

重庆

中国香港

亚太东南

亚太南部

亚太东北

美国西部

美国东部

北美地区

新加坡

曼谷

孟买

首尔

东京

硅谷

弗吉尼亚

多伦多

欧洲地区

法兰克福

莫斯科

② 更多地域

不同地域云产品之间内网不互通；选择最靠近您客户的地域，可降低访问时延。创建成功后不支持切换地域。[查看我的云服务器地域](#) [详细对比](#)

可用区

随机可用区

北京二区

北京三区

北京四区

北京五区

北京六区

NEW 北京七区

NEW

②

网络

vpc-ofywoqpw | Default-VPC (默认) | 17

subnet-h34141df | Default-Subnet (默认)

②

子网剩余可用IP 4091个

当前网络为默认私有网络/子网，建议您根据业务需要进行调整  
如现有私有网络/子网不符合您的要求，可以去控制台 [新建私有网络](#) 或 [新建子网](#)。云服务器购买后可以通过控制台切换私有网络完成私有网络/子网的切换

想要部署Emos项目，云主机至少要 **2核心4GB** 的配置，如果能有更高的硬件配置就更好了。

Emos项目中对内容存要求最高的就属人脸识别程序了，人脸识别程序包含 **TensorFlow** 机器学习功能，所以至少要消耗600MB内存才能运行起来，否则没得谈。

实例

2核

4GB

全部机型

标准型

高IO型

内存型

计算型

GPU机型

FPGA机型

大数据型

黑石物理服务器2.0

全部实例类型

标准型S5

标准型SA2

标准型S4

标准网络优化型SN3ne

标准型S3

标准型SA1

标准型S2

标准型S1

机型	规格	vCPU	内存	处理器型号(主频)	内网带宽	网络收发包	支持可用区	备注	费用
标准型S3	S3.MEDI...	2核	4GB	Intel Xeon Skylake 6133(2.5 GHz)	1.5Gbps	25万PPS	19个可用区	无	180元/月

共1项 ☒ 只显示北京支持机型

< 上一页 1 下一页 >

镜像

公共镜像

自定义镜像

共享镜像

镜像市场

CentOS

64位

CentOS 7.8 64位

高性能云硬盘

50

GB

购买成功后，系统盘不支持更换介质

云主机的系统一定还是选用 **CentOS**，而且版本必须是 **7.X**，大家千万不要选择 **8.X** 版本。因为那个版本是最糟糕的，大量程序包不兼容，谁用谁后悔。

系统盘

高性能云硬盘

50

GB

购买成功后，系统盘不支持更换介质

数据盘

+ 新建云硬盘数据盘 还可增加20块数据盘

定期快照

☐ 对系统盘设置定期快照

default-policy|星期六...|14:00|保留30天后自动删除

☐ 对数据盘设置定期快照

default-policy|星期六...|14:00|保留30天后自动删除

公网带宽

☒ 免费分配独立公网IP

按带宽计费

按使用流量

1Mbps 50Mbps 200Mbps 1000Mbps 2 Mbps

IPv6地址

所选的VPC/子网未开通IPv6

建议大家网络方面选择 **2M** 带宽，毕竟我们要向云主机上传大量的文件，例如人脸识别镜像就几个GB，网络带宽还是大一点更好。另外，不建议大家选用按流量计费这种宽带模式，有时候你的主机被大量DDos攻击的时候，或者中了病毒，疯狂攻击其他主机，都会产生 **巨大的网络流量**，流量费更是贵的惊人。

## 二、SSH连接云主机

在云主机控制面板中找到云主机的公网IP，然后用MobaXterm软件连接云主机

ID/名称	监控	状态	可用区	实例类型	实例配置	主IPv4地址	实例计费模式	网络计费模式	操作
ins- cent-5141		运行中	北京二区	标准型S2		140.225.172.210.14 (公)	包年包月 2022-11-20 00:52:28到期	按带宽包年包月计费	登录 续费 更多

共 1 条 20 条 / 页 1 / 1 页

### 三、在云主机上面开放端口

在云主机上面开放一些端口，这样外界才能远程管理MySQL、MongoDB，以及访问后端Java项目等等。我们在云主机的安全组面板上面可以设置要开放的端口。

入站规则

出站规则

添加规则

导入规则

排序

删除

一键放通

教我设置

<input type="checkbox"/> 来源	协议端口	策略	备注	修改时间	操作
<input type="checkbox"/> 0.0.0.0/0	TCP:4000	允许		2021-01-14 11:22:15	编辑 插入 删除
<input type="checkbox"/> 0.0.0.0/0	TCP:4000	允许		2021-01-14 11:21:05	编辑 插入 删除
<input type="checkbox"/> 0.0.0.0/0	TCP:27017	允许		2020-12-25 23:30:00	编辑 插入 删除
<input type="checkbox"/> 0.0.0.0/0	TCP:6379	允许		2020-12-25 22:56:22	编辑 插入 删除

因为Redis非常容易被注入挖矿脚本，所以Redis不对外提供访问，只能CentOS本机自己访问。当你的云主机一上线，就有很多国外的黑客主机开始做端口扫描，然后发送轮询请求，不停的组合碰撞你的SSH密码、MySQL密码、Redis密码等等。MySQL被攻破无非就是丢失很多商业数据，如果Redis被攻破，就被注入挖矿病毒。你的云主机CPU会立即飙高到100%，其他程序则无法正常运行。

我用 `journalctl -xe` 命令查询到有黑客在恶意扫描的云主机，然后尝试登陆SSH

```
-- The start-up result is done.
Feb 23 10:51:01 VM-0-14-centos CROND[10919]: (root) CMD (flock -xn /tmp/stargate.lock -c '/usr/lo
Feb 23 10:51:07 VM-0-14-centos sshd[10945]: Failed password for root from 42.193.108.100 port 365
Feb 23 10:51:07 VM-0-14-centos sshd[10945]: Received disconnect from 42.193.108.100 port 36558:11
Feb 23 10:51:07 VM-0-14-centos sshd[10945]: Disconnected from authenticating user root 42.193.108
Feb 23 10:52:01 VM-0-14-centos systemd[1]: Started Session 1157 of user root.
```

抵御撞库攻击正确的做法是维护云主机的时候，在安全组面板上开放相关的一些端口，维护完成后，立即关闭这些端口，只保留80、443、8080这样的业务端口。所有的数据库端口和SSH端口全部关闭。

序号	端口	来源	用途	临时开放
1	3306	0.0.0.0/0	MySQL端口	是
2	6379	0.0.0.0/0	Redis端口	是
3	27017	0.0.0.0/0	MongoDB端口	是
4	4369	0.0.0.0/0	RabbitMQ端口	否
5	5671	0.0.0.0/0	RabbitMQ端口	否
6	5672	0.0.0.0/0	RabbitMQ端口	否
7	8080	0.0.0.0/0	emos-wx-api项目端口	否
8	9090	0.0.0.0/0	emos-workflow项目端口	否
9	3000	0.0.0.0/0	人脸识别项目端口	否

