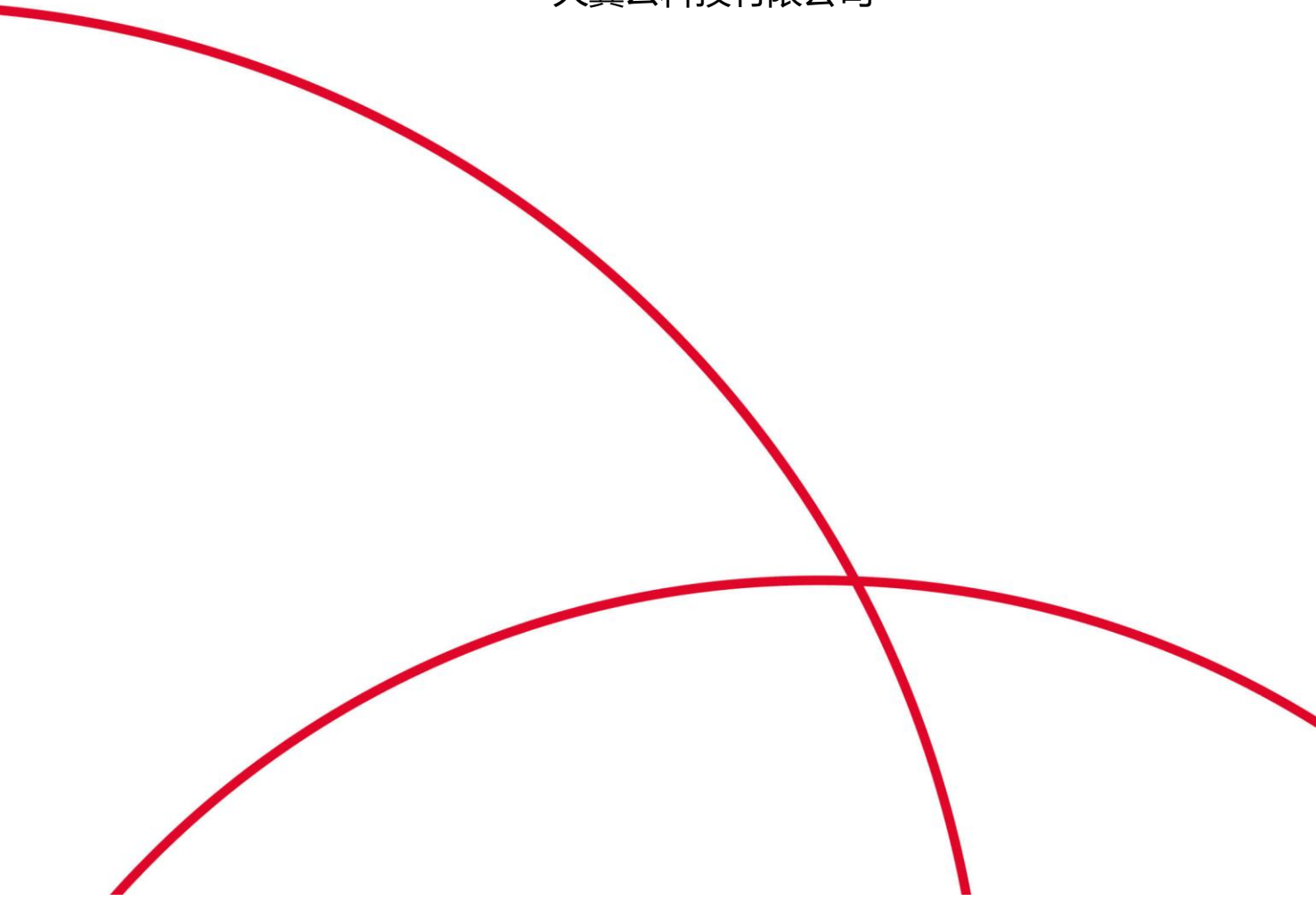


# 弹性文件服务

## 最佳实践

天翼云科技有限公司



# 目录

一、	使用 docker 挂载天翼云弹性文件服务 .....	4
	应用场景 .....	4
	前提条件 .....	4
	准备工作 .....	4
	操作步骤 .....	5
二、	基于弹性文件服务搭建应用 .....	7
1.	使用天翼云弹性文件服务搭建 WordPress 网站 .....	7
	应用场景 .....	7
	方案使用云产品 .....	8
	准备工作 .....	8
	操作步骤 .....	8
2.	使用天翼云弹性文件服务进行 Nextcloud 网盘搭建 .....	15
	应用场景 .....	15
	方案使用云产品 .....	15
	方案优势 .....	15
	操作步骤 .....	15
三、	挂载文件系统 .....	21

1. 跨 AZ 挂载文件系统.....	21
应用场景 .....	21
方案使用云产品.....	21
方案优势 .....	21
操作步骤 .....	21
四、    管理文件系统.....	25
1. 使用 Nginx 代理天翼云弹性文件服务.....	25
应用场景 .....	25
方案使用云产品.....	26
方案架构 .....	26
准备工作 .....	26
操作步骤 .....	27
2. 天翼云弹性文件服务子目录权限隔离 .....	31
应用场景 .....	31
方案使用云产品.....	31
准备工作 .....	32
操作步骤 .....	32

# 一、使用 docker 挂载天翼云弹性文件服务

## 应用场景

本文适用于 docker 容器中实现天翼云弹性文件服务的挂载。

## 前提条件

- 购买一个 NFS 协议的弹性文件系统。
- 购买一台配置弹性 IP 的云主机（或者物理机）。

## 准备工作

1. 登录天翼云官网页面，找到控制中心。
2. 本文以华北 2 资源池为例，购买一台配置弹性 IP 的云主机，具体操作请参考[创建弹性云主机](#)。此次以 CentOS 8.2 系统的弹性云主机为例，部分参数可参考下表：

参数	说明
镜像	CentOS 8.2 64 位
弹性 IP	自动分配
IP 版本	IPV4
带宽	5M

您也可以选择购买一台配置弹性 IP 的物理机，具体操作请参考[自助开通天翼云物理机](#)。

3. 创建一个弹性文件系统，具体操作请参考[创建弹性文件系统](#)，部分参数可参考下表：

参数	说明
存储类型	SFS Turbo 标准型

协议类型	NFS
选择网络	选择与弹性云主机（或物理机）相同的 VPC

## 操作步骤

使用 docker 挂载弹性文件系统可以分为几个关键步骤：**安装 docker>拉取镜像>宿主机挂载文件系统>创建并运行容器，实现文件系统挂载**。具体操作步骤如下：

### 步骤一：安装 docker

**注意：**以下操作同样适用于物理机环境。

1. 以 root 用户登录云主机，登录方式参考[登录 Linux 弹性云主机](#)。

2. 执行以下命令安装 docker:

```
curl -fsSL https://get.docker.com | bash -s docker
```

3. 执行以下命令启动 docker:

```
systemctl start docker
```

4. 执行 vi /etc/selinux/config 文件，将以下两条命令注释掉：

```
SELINUXTYPE=targeted  
SELINUX=enforcing
```

增加以下命令，关闭 SELINUX:

```
SELINUX=disabled
```

单击 ECS 退出编辑，输入 "wq!"，保存退出 config 文件。在命令执行以下命令，使配置生效：

```
setenforce 0 #使配置立即生效
```

### 步骤二：docker 拉取镜像

执行以下命令拉取镜像：

```
docker pull centos:centos8.2
```

查看本地镜像：

```
docker images
```

### 步骤三：宿主机挂载文件系统

挂载已开通的弹性文件系统至弹性云主机，具体操作请参考[使用弹性云主机挂载弹性文件系统](#)。

本文将弹性文件系统挂载至宿主机的/mnt/docker\_test 目录。

### 步骤四：创建并运行容器，实现文件系统挂载

1. 执行以下命令创建并运行容器，将弹性文件挂载至容器的/mnt/mount 目录下：

#命令格式如下：

```
docker run -di --name=容器名称 -v 宿主机挂载目录:容器挂载目录 -d 镜像名称
```

#以本文为例，执行命令如下：

```
docker run -di --name=mounttest -v /mnt/docker_test:/mnt/mount -d centos:centos8.2
```

可以使用 `docker ps -a` 查看容器运行状态。

2. 通过 `exec` 命令进入刚才所创建的容器：

```
# docker exec -it 自己的容器名称 /bin/bash
```

```
docker exec -it mounttest /bin/bash
```

3. 在容器中查看挂载情况：

```
df -h
```

```
104857600 bytes (105 MB) copied, 0.216402 s, 485 MB/s
[root@df1e3108b49f mount]# df -h
Filesystem                Size      Used Avail Use% Mounted on
overlay                   40G        3.4G   37G   9% /
tmpfs                     64M          0   64M   0% /dev
tmpfs                     1.8G          0   1.8G   0% /sys/fs/cgroup
shm                       64M          0   64M   0% /dev/shm
centos:centos8.2         500G      132M   500G   1% /mnt/mount
/dev/vda1                 40G        3.4G   37G   9% /etc/hosts
tmpfs                     1.8G          0   1.8G   0% /proc/acpi
tmpfs                     1.8G          0   1.8G   0% /proc/scsi
tmpfs                     1.8G          0   1.8G   0% /sys/firmware
```

4. 在容器中的/mnt/mount 目录下，写一个文件大小 100M：

```
dd if=/dev/zero of=test.img count=1 bs=100M
```

```
md5sum test.img
```

```
[root@df1e3108b49f mount]# dd if=/dev/zero of=test.img count=1 bs=100M
1+0 records in
1+0 records out
104857600 bytes (105 MB) copied, 0.216402 s, 485 MB/s
```

```
-rw-r--r-- 1 root root 104857600 Dec 25 10:26 test.img
[root@df1e3108b49f mount]# md5sum test.img
2f282b84e7e608d5852449ed940bfc51 test.img
[root@df1e3108b49f mount]#
```

Ctrl+D 退出容器至宿主机，查看/mnt/docker\_test 目录，并验证 md5 值：

```
md5sum test.img
```

```
[root@ecm-... ~]# cd /mnt/docker_test/
[root@ecm-... i docker_test]# ll
total 102400
-rw-r--r-- 1 root root 104857600 Dec 25 18:26 test.img
[root@ecm-... docker_test]#

[root@e... pi docker_test]# md5sum test.img
2f282b84e7e608d5852449ed940bfc51 test.img
```

可以看到，在容器中创建的文件在宿主机中同样存在。

至此，docker 容器中已成功完成弹性文件系统的挂载。

## 二、 基于弹性文件服务搭建应用

### 1. 使用天翼云弹性文件服务搭建 WordPress 网站

#### 应用场景

WordPress 是一款免费开源的内容管理系统 (CMS)，目前已经成为全球使用最多的 CMS 建站程序。根据 W3techs 的最新统计 (截至 2021 年 4 月)，在全球的所有网站中 WordPress 占有 41% 的市场份额 (请注意是全球所有网站)，意味着每 5 个网站中就有 2 个网站是使用 WordPress 搭建的。在使用 CMS 构建的所有网站中 WordPress 占有 64.7% 的市场份额，并且它的市场占有率一直在持续增长。

在本案例中，我们将会搭建一个基础的 WordPress 网站，需要使用到的资源如下：

1. 弹性云主机：用于安装 WordPress 应用程序，是整个网站的核心，更多信息请参考[弹性云主机](#)。
2. 文件系统：存储 WordPress 应用文件和上传资源文件，更多信息请参考[弹性文件服务](#)。
3. 虚拟私有云 VPC：提供一个逻辑隔离的局域网环境，创建云主机和文件系统的必选参数，

更多信息请参考[虚拟私有云](#)。

4. mysql 数据库：用于存储 WordPress 使用中的用户基础信息。
5. Docker：在云主机中启动 mysql 和 WordPress。

## 方案使用云产品

弹性云主机，弹性文件服务

## 准备工作

在开始之前需要创建一个虚拟机私有云 VPC，一台云主机，一个文件系统。具体操作如下：

1. 在需要操作的地域创建虚拟私有云 VPC，具体操作步骤参见[创建虚拟私有云 VPC](#)。
2. 创建该 VPC 下的弹性云主机，操作系统为 Linux，此处以 CTyunOS 2.0.1 为例演示，具体操作步骤参见[创建弹性云主机](#)。
3. 创建该 VPC 下的文件系统，文件系统的协议类型为 NFS，具体操作步骤参见[创建文件系统](#)。

## 操作步骤

注意：

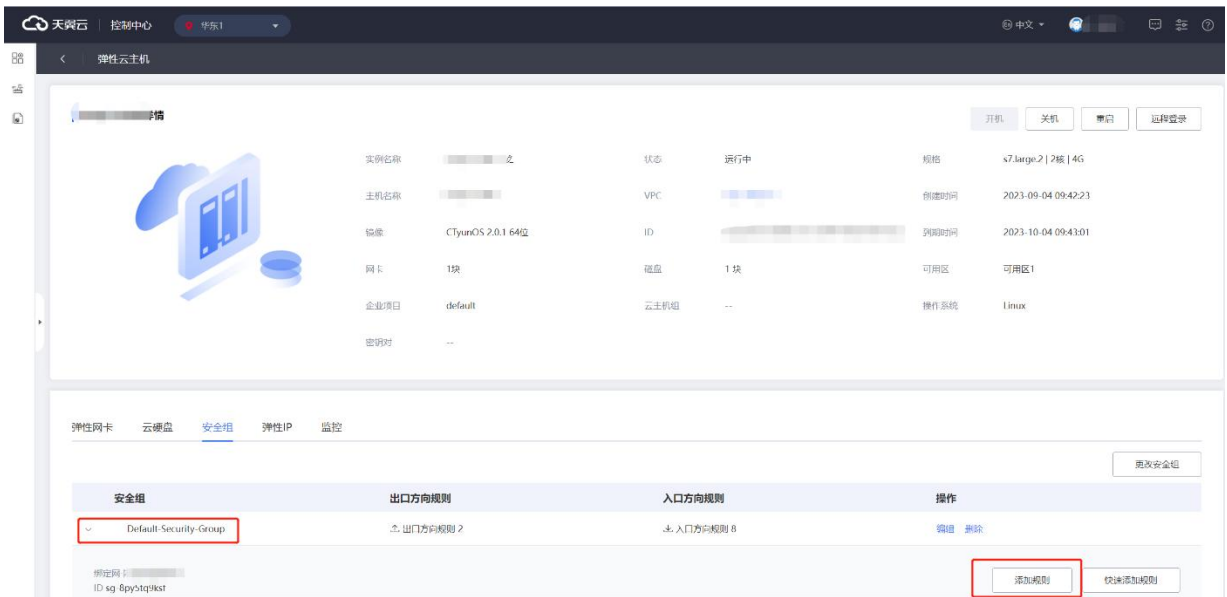
操作都是以 root 账号操作，云主机中没有运行其他的进程，避免端口被占用。

### 步骤一：放开云主机 TCP22330 端口

1. 登录“控制中心”，点击“计算>弹性云主机”进入弹性云主机控制台页面。
2. 找到目标云主机，点击名称进入云主机详情页。
3. 在详情页下方，点击“安全组”页签，在该页签默认安全组下点击“添加规则”，具体操



作请参考[添加安全组规则](#)。



4. 添加“入方向”规则，各参数选项如下图。



5. 添加完成之后，在默认安全组下会显示相应的规则。

## 步骤二：在云主机中挂载文件系统

1. 以 root 用户登录弹性云主机，登录方式参考[登录 Linux 弹性云主机](#)。

2. 执行以下命令安装 NFS 客户端。

```
yum install nfs-utils -y
```

3. 执行如下命令创建本地路径 “/mnt/wordpressdata” 。

```
mkdir /mnt/wordpressdata
```

4. 执行如下命令，挂载文件系统。挂载地址可在文件系统详情页获取，

“/mnt/wordpressdata” 是本地挂载路径。挂载操作请参考[挂载 NFS 文件系统到弹性云主机 \(Linux\)](#)。

```
mount -t nfs -o vers=3,proto=tcp,async,nolock,noatime,nodiratime,wsiz=1048576,rsiz=1048576,timeo=600 挂载地址 /mnt/wordpressdata
```

5. 挂载完成后，通过 df -h 查看挂载情况。

## 步骤三：安装 WordPress

1. 本次测试使用 Docker 容器来安装 WordPress，执行如下命令安装 Docker 容器。

```
yum install docker -y
```

2. 拉取 WordPress 镜像。

```
docker pull wordpress
```

3. 拉取 mysql 镜像。

```
docker pull mysql:5.7
```

4. 安装完成之后，使用 docker image ls 查看容器镜像。

```
[root@node140 ~]#  
[root@node140 ~]# docker image ls  
REPOSITORY          TAG          IMAGE ID          CREATED          SIZE  
wordpress           latest      ed7281630c77     8 days ago     666MB  
mysql                5.7        92034fe9a41f     3 weeks ago    581MB  
[root@node140 ~]#  
[root@node140 ~]#
```

5. 执行如下命令，启动 mysql 容器。此处设置账号：root，密码：{password}，实际操作使用中应该填写自己的复杂密码。

"/root/mysql"表示 Docker 的 mysql 容器映射到云主机中的目录，可以按照自己的使用需求修改目录。

```
docker run --name mysql -d -p 3306:3306 -v /root/mysql:/var/lib/mysql -e MYSQL_ROOT_PASSWORD={password} --restart=always mysql:5.7
```

6. 使用 `docker ps` 查看 mysql 容器的 ID, 见下图。然后执行以下命令进入容器。{mysql\_id} 为查询获得，根据查询结果进行替换。

```
[root@ ~]# docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED        STATUS
PORTS
j297e842      mysql:5.7 "docker-entrypoint.s..." 14 seconds ago Up 13 seconds
0.0.0.0:3306->3306/tcp, 33060/tcp mysql
docker exec -it {mysql_id} /bin/bash
```

7. 在容器内部依次执行以下指令，创建 WordPress 使用的数据库，请注意替换{password} 为自行设置的复杂密码。

```
mysql -uroot -p
alter user 'root'@'localhost' identified by '{password}';
CREATE DATABASE wordpress;
```

```
bash-4.2# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.43 MySQL Community Server (GPL)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> alter user 'root'@'localhost' identified by '{password}';
Query OK, 0 rows affected (0.00 sec)

mysql> CREATE DATABASE wordpress;
Query OK, 1 row affected (0.00 sec)
```

创建完成之后，连续输入两次“exit”退出 mysql 和 mysql 的 Docker 容器。

8. 执行如下命令，启动 WordPress。

```
docker run --name wordpress --link mysql -p 22330:80 -v /mnt/wordpressdata/:/var/www/html -d --restart=always wordpress:latest
```

"--link {name}"表示 WordPress 启动时连接的 mysql 容器名，在步骤 8 中启动 mysql

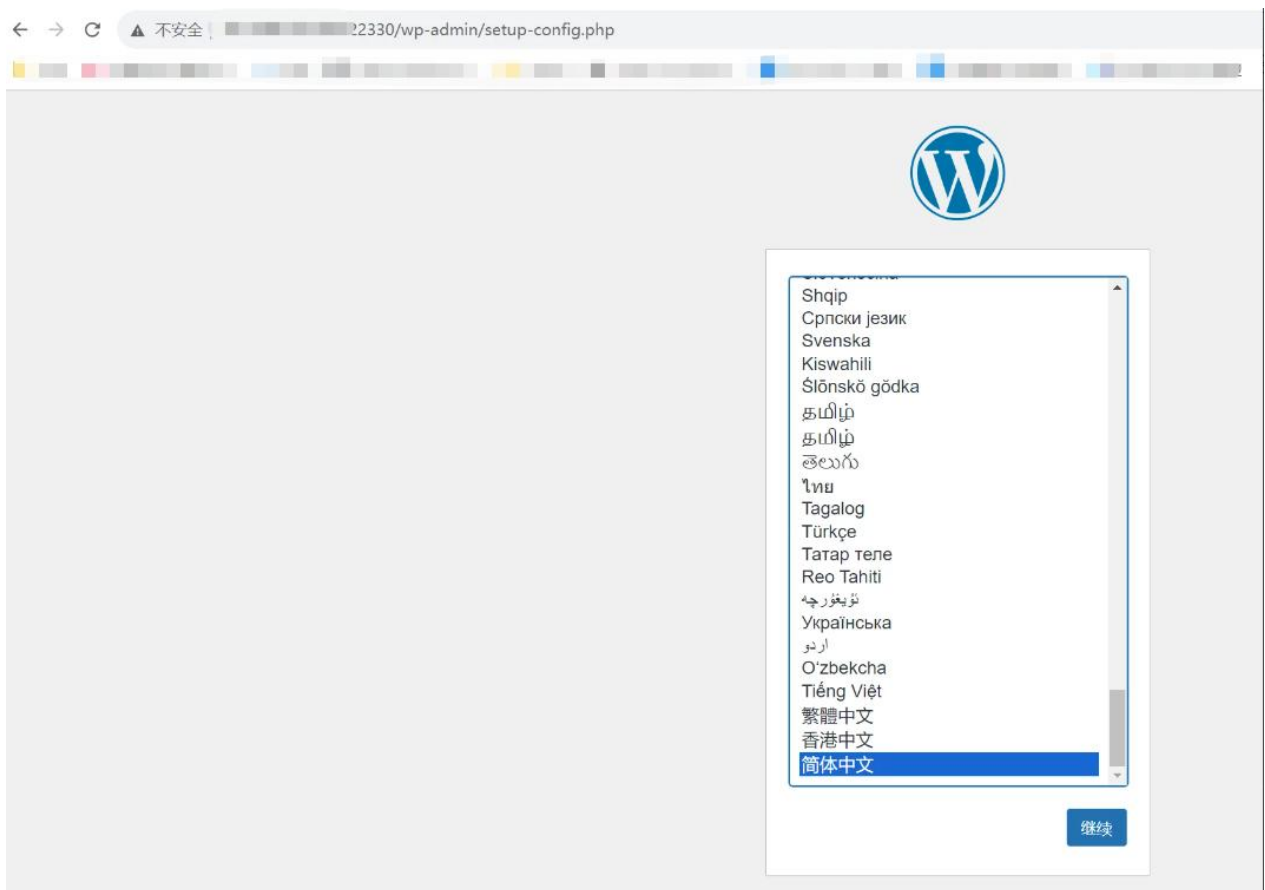
容器时设置的 name 是 mysql，此处按照实际的 name 填写。

## 9. 启动之后执行 docker ps 查看容器：

```
[root@maxy15-001 ~]#  
[root@maxy15-001 ~]# docker ps  
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS  
PORTS  
161b8d6451c2       wordpress:latest   "docker-entrypoint.s..." 5 seconds ago      Up 4 seconds  
0.0.0.0:22330->80/tcp  
d297e842fb73       mysql:5.7          "docker-entrypoint.s..." 3 minutes ago      Up 3 minutes  
0.0.0.0:3306->3306/tcp, 33060/tcp  
mysql  
[root@maxy15-001 ~]#  
[root@maxy15-001 ~]#
```

## 步骤四：初始化配置 WordPress

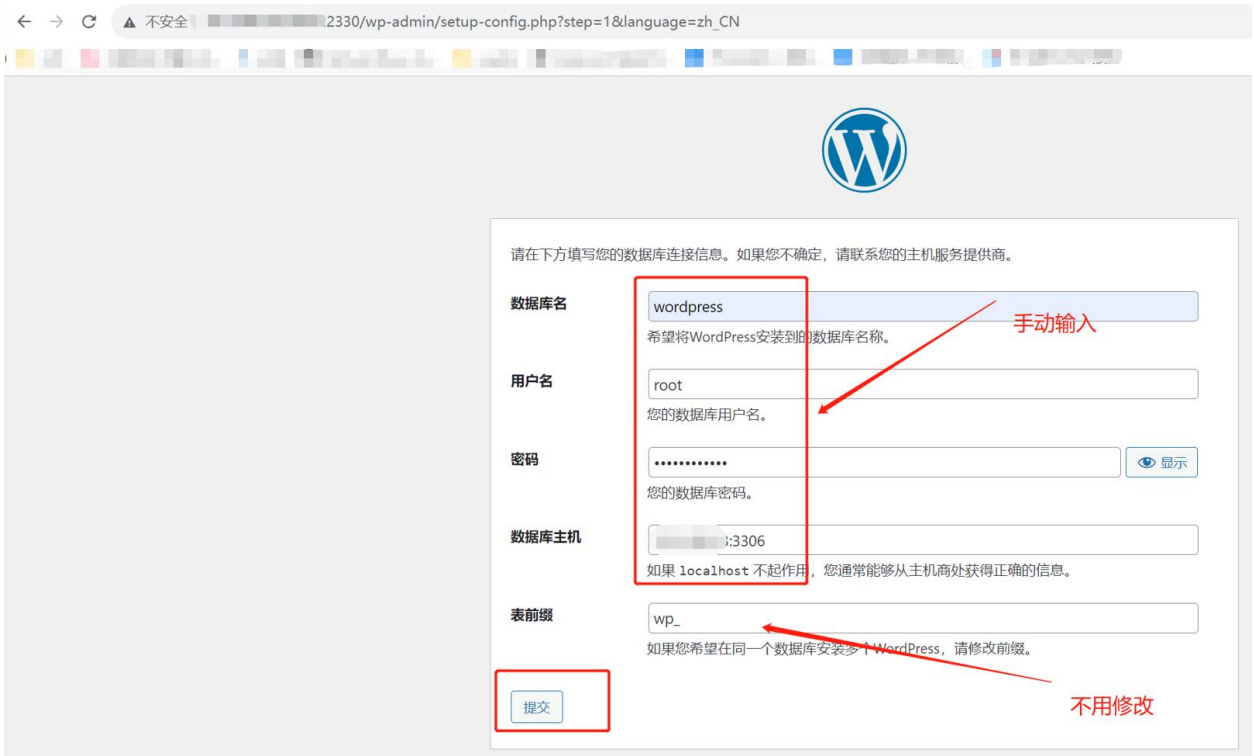
1. 在云主机详情页中“弹性 IP”页签获取该云主机公网 IP 的 IP 地址，在浏览器中输入“{云主机 IP 地址}:22330”，预期出现以下界面。



2. 按界面提示开始配置，需要手动输入以下信息：

参数名	参数值	说明
-----	-----	----

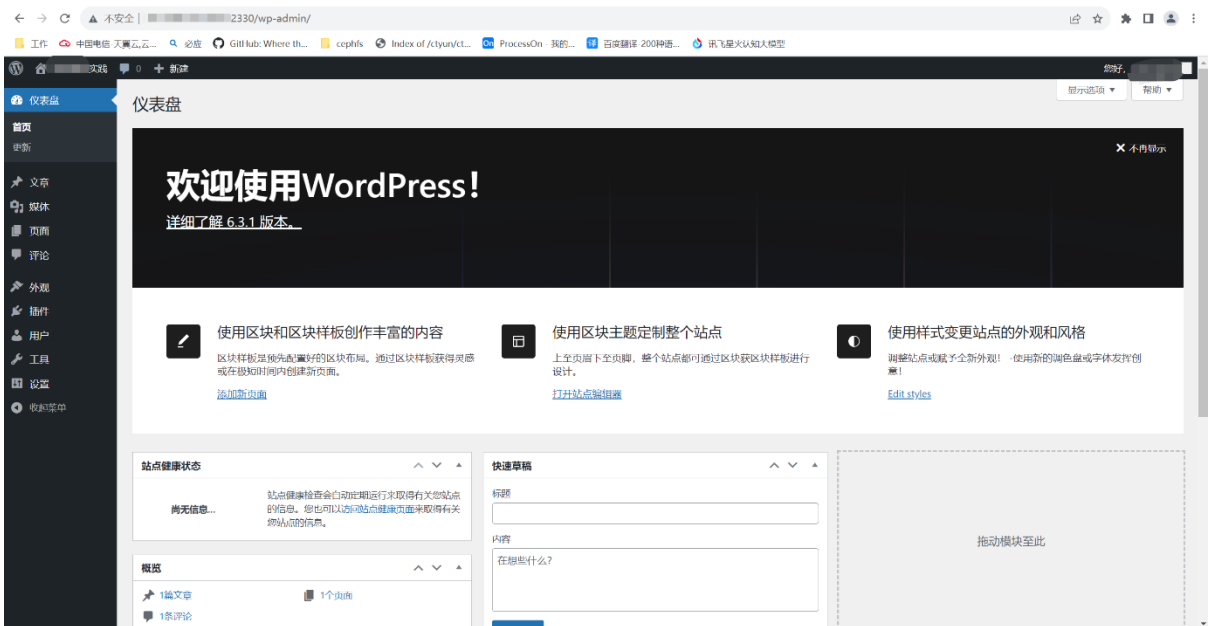
数据库名	wordpress	在操作步骤三第 7 步中创建的数据库名称。
用户名	root	mysql 默认账号名。
密码	{password}	使用自己设置的密码。
数据库主机	{ip}:3306	{ip}为连接数据库使用内网 IP，在云主机详情页“弹性网卡”页签下获取。



3. 提交配置信息，点击“运行安装程序”，设置网站标题、用户名、密码、电子邮箱等信息，点击“安装 WordPress”。



#### 4. 初始化配置完成，使用设置的账户信息登录 WordPress 管理控制界面。



## 2. 使用天翼云弹性文件服务进行 Nextcloud 网盘搭建

### 应用场景

Nextcloud 是一款开源免费的私有云存储网盘项目，可以让你快速便捷地搭建一套属于自己或团队的云同步网盘，从而实现跨平台跨设备文件同步、共享、版本控制、团队协作等功能。

### 方案使用云产品

弹性文件服务，弹性云主机

### 方案优势

- 弹性文件服务可弹性扩容，支持 Nextcloud 网盘的容量需求。
- 实现跨平台文件同步、文件共享和权限控制等功能，满足用户对网盘的使用需求。

### 操作步骤

#### 步骤一：购买弹性云主机和弹性文件服务

1. 本次操作实践中，需要购买弹性云主机作为弹性文件服务的挂载点和创建网盘服务器。网盘上传下载文件数据需要占用弹性云主机公网带宽，因此需要为弹性云主机配置弹性 IP。此次以 CentOS 8.4 系统为例介绍操作。弹性云主机购买流程详见[创建弹性云主机](#)。弹性云主机部分参数可参考下表：

参数	说明
镜像	CentOS 8.4 64 位

参数	说明
弹性 IP	自动分配
IP 版本	IPv4
带宽	5M

2. 创建弹性文件服务，操作详见[创建文件系统](#)，部分参数可参考下表：

参数	说明
存储类型	SFS Turbo 标准型
协议类型	NFS
选择网络	选择与弹性云主机相同 VPC

## 步骤二：挂载弹性文件服务

1. 以 root 用户登录弹性云主机，登录方式参考[登录 Linux 弹性云主机](#)。
2. 执行以下命令安装 NFS 客户端。

```
yum -y install nfs-utils
```

3. 执行如下命令创建本地路径 “/nextcloud”。

```
mkdir /nextcloud
```

4. 执行如下命令挂载文件系统。挂载地址可在文件系统详情页获取，参考[查看文件系统](#)。本地挂载路径为云主机上用于挂载文件系统的本地路径，本文采用上一步创建的 “/nextcloud”。



```
mount -t nfs -o vers=3,proto=tcp,async,nolock,noatime,nodiratime,noresvport,wsiz=1048576,rsiz=1048576,timeo=600 挂载地址 本地挂载路径
```

5. 挂载完成后使用 `mount | grep nextcloud` 查看挂载情况。

### 步骤三：安装 Nextcloud 服务

1. 执行如下命令安装 Docker。

```
curl -fsSL https://get.docker.com | bash -s docker
```

2. 执行如下命令启动 Docker。

```
systemctl start docker
```

3. 依次执行如下命令关闭防火墙。

```
systemctl stop firewalld.service #停止 firewall  
systemctl disable firewalld.service #禁止 firewall 开机启动
```

4. 执行 `vi /etc/selinux/config` 打开 config 文件，将以下两条命令注释掉

```
SELINUX=enforcing  
SELINUXTYPE=targeted
```

增加以下命令，关闭 SELINUX：

```
SELINUX=disabled
```

5. 单击 ECS 退出编辑，输入 "wq!"，保存退出 config 文件。在命令行执行以下命令，使配置

生效：

```
setenforce 0
```

```
# This file controls the state of SELinux on the system.  
# SELINUX= can take one of these three values:  
#   enforcing - SELinux security policy is enforced.  
#   permissive - SELinux prints warnings instead of enforcing.  
#   disabled - No SELinux policy is loaded.  
SELINUX=disabled  
# SELINUXTYPE= can take one of three values:  
#   targeted - Targeted processes are protected,  
#   minimum - Modification of targeted policy. Only selected processes are protected.  
#   mls - Multi Level Security protection.  
# SELINUXTYPE=targeted
```

6. 执行如下命令拉取 Nextcloud 镜像。

```
docker pull nextcloud
```

```

[root@ecm-kyc1 ~]# docker pull nextcloud
Using default tag: latest
latest: Pulling from library/nextcloud
52d2b7f179e3: Downloading [==>] 1.18MB/29.12MB
635676b59bff: Download complete
08dbc2d7054b: Downloading [>] 1.081MB/104.3MB
8748b1b28b49: Download complete
0885630aadb3: Downloading [=>] 621.9kB/20.3MB
7d212700447a: Waiting
8870ab32a8d3: Waiting
5044ddca62e6: Waiting
23ddf7f6968f: Waiting
89c07fc5273e: Waiting
7475029d0c03: Waiting
3e2da362b346: Waiting
051f00ca3658: Waiting
8ace9c74b598: Waiting
01aca9afd95d: Waiting
9d2e0e32bc67: Waiting
cd251c55602a: Waiting
248d1ea5a3e9: Waiting
58459c7b8c1f: Waiting
6a9665ee7be8: Waiting

```

7. 执行如下命令创建 Nextcloud 容器并运行，Nextcloud 参数说明见下表。

```
docker run -p 7080:80 -d -v /nextcloud:/var/www/html nextcloud
```

参数	说明
nextcloud	容器名称
/nextcloud:/var/www/html	目录映射，/nextcloud/为数据文件存储的目录，此项配置可将网盘数据写入弹性文件系统中
-p 7080:80	端口映射，本次使用 7080 端口

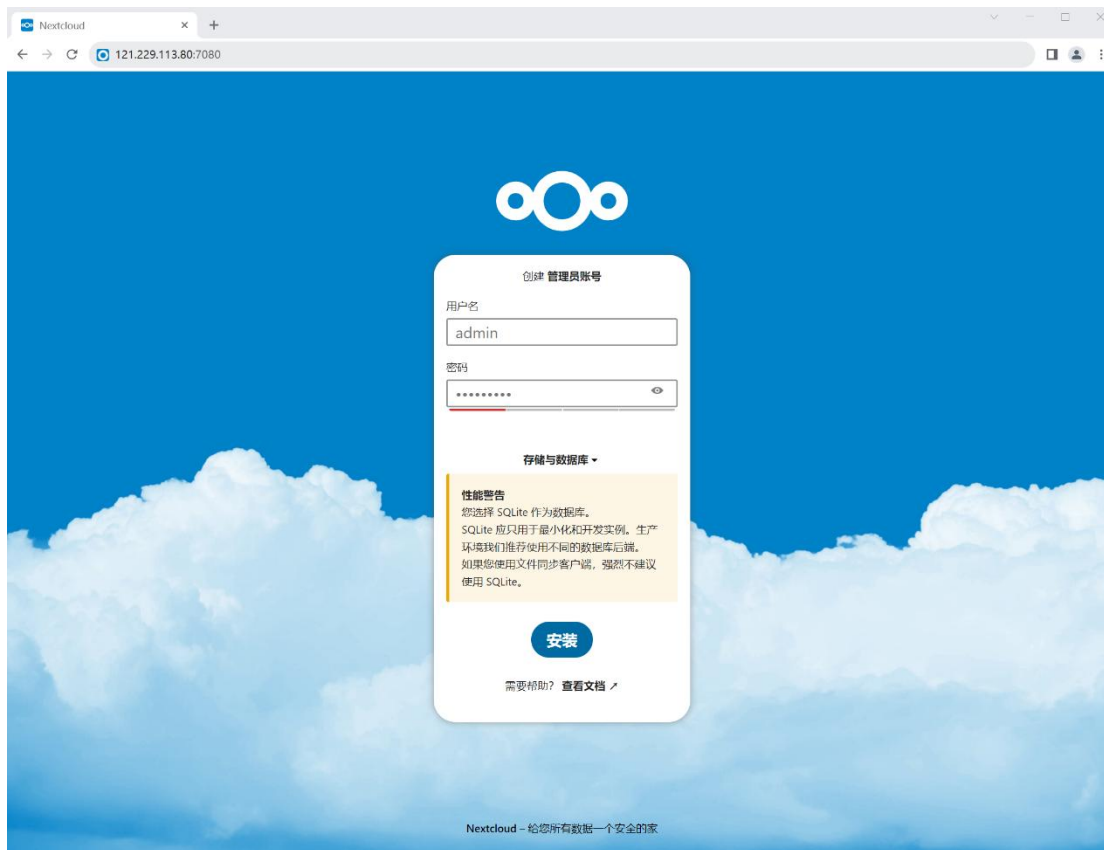
8. 执行如下命令，检查 Nextcloud 容器。可以查看 Nextcloud 的 ContainerID 及端口情况，状态为'up'，说明 Nextcloud 容器运行中。

```
docker ps
```

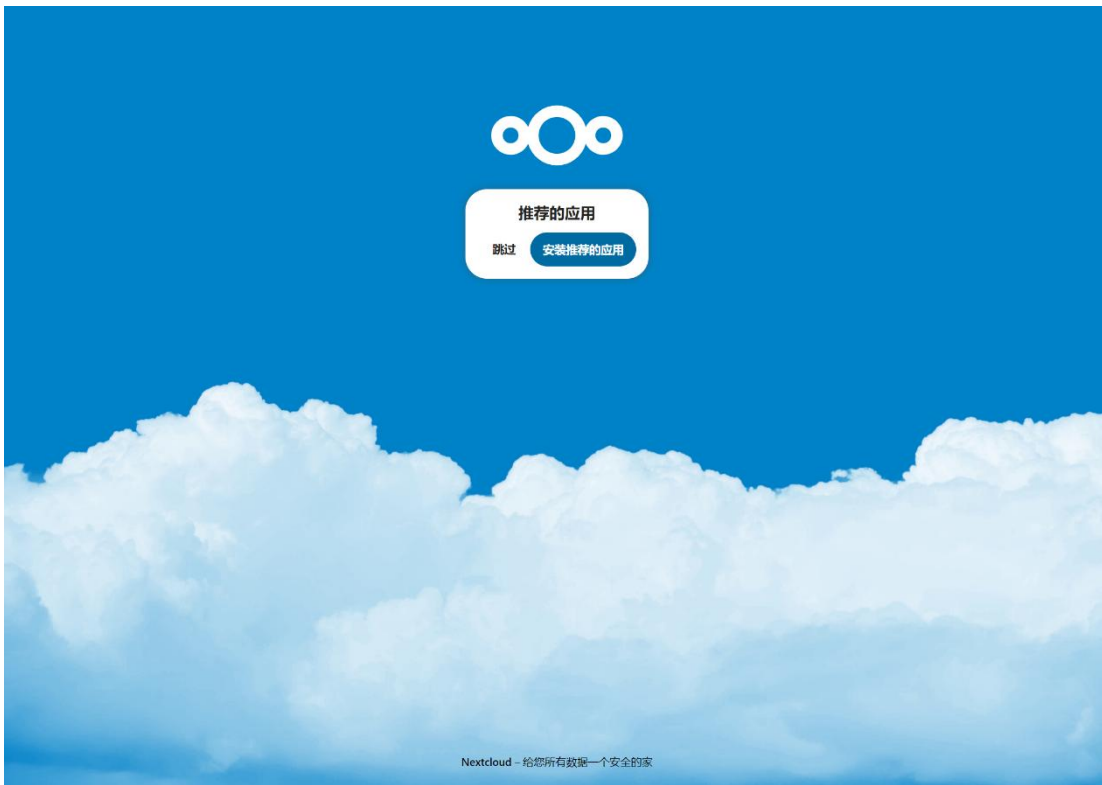
#### 步骤四：浏览器打开 Nextcloud

1.在云主机详情页下方“安全组”页签下，在该页签默认安全组下点击“添加规则”，对浏览器所在机器的 IP 地址和 Nextcloud 所使用的 7080 端口和入方向进行放开。本文采用的是对全部协议及端口进行放通，具体操作请参考[添加安全组规则](#)。

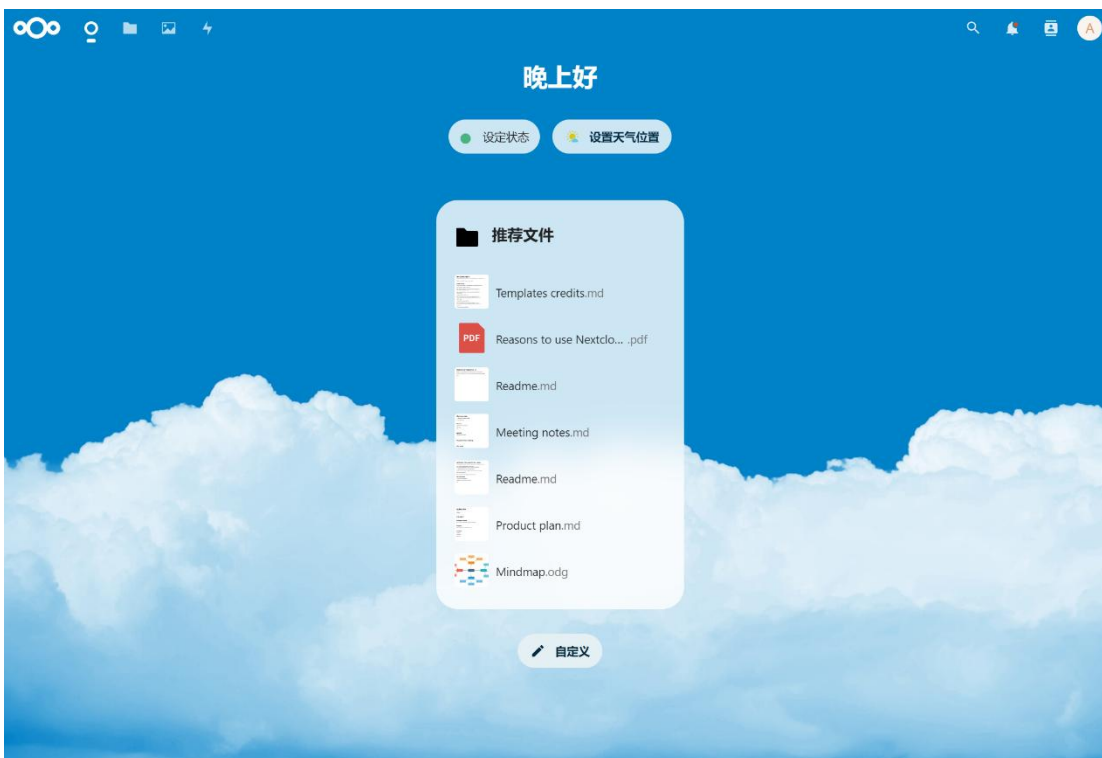
2.在本地浏览器输入{公网 IP 地址:7080}, 打开 Nextcloud 登录页面, 设定管理员账和密码, 点击“安装”。其中公网 IP 地址可在云主机详情页中“弹性 IP”页签下获取。



3.安装成功后, 点击安装推荐的应用。



4.进入欢迎界面。



5.点击左上角第二个文件夹图标，进入网盘页面。在网盘页面可以进行新建文件夹、共享内容等。

## 三、 挂载文件系统

### 1. 跨 AZ 挂载文件系统

#### 应用场景

针对企业而言，不管业务是不是在云上，服务的稳定和连续性都是无法回避的话题，为了降低不可抗力因素对服务提供造成的影响，有了高可用性和容灾的概念。

跨 AZ 部署是实现服务高可用较为有效的方法，本次我们介绍跨 AZ 挂载文件系统，云主机和文件系统部署在不同的机房，通过天翼云内部高速通道实现连通，实现文件存储跨 AZ 级别的高可用。本次以 NFS 文件系统跨 AZ 挂载 Linux 云主机为例。

#### 方案使用云产品

弹性云主机，弹性文件服务

#### 方案优势

- 跨 AZ 挂载文件系统能够实现服务的高可用性，且极具性价比。
- 跨 AZ 挂载文件系统可以消除服务中的单点故障，同时具备很低的网络时延。

#### 操作步骤

##### 步骤一：购买弹性云主机

1. 本次操作实践中，需要购买弹性云主机作为弹性文件服务的挂载点，此次以 CentOS 7.6 系统为例介绍操作。

弹性云主机购买流程详见[弹性云主机-创建弹性云主机](#)。弹性云主机部分参数可参考下表：

参数	说明
可用区	可用区 1
镜像	CentOS 7.6 64 位
弹性 IP	自动分配
IP 版本	IPv4
带宽	5M

2. 配置完成，点击提交订单，等待云主机创建完成。

## 步骤二：创建弹性文件服务

1. 创建弹性文件服务 1，此文件系统与弹性云主机处于同一可用区，作为对照参考，操作详见

[创建文件系统](#)，部分参数可参考下表：

参数	说明
可用区	可用区 1
存储类型	SFS Turbo 性能型
协议类型	NFS
选择网络	选择与弹性云主机相同 VPC

确认配置后，点击“立即购买”，等待文件系统创建完成。

2. 创建弹性文件服务 2，此文件系统与弹性云主机不在同一可用区，操作详见[创建文件系统](#)，

部分参数可参考下表：

参数	说明
可用区	可用区 2 或可用区 3
存储类型	SFS Turbo 性能型

协议类型	NFS
选择网络	选择与弹性云主机相同 VPC

确认配置后，点击“立即购买”，等待文件系统创建完成。

### 步骤三：挂载弹性文件服务

#### 挂载文件系统 1

1. 以 root 用户登录弹性云主机，具体操作请参考[登录 Linux 弹性云主机-弹性云主机-快速入门](#)。

2. 执行以下命令安装 NFS 客户端。

```
yum -y install nfs-utils
```

3. 执行如下命令创建本地挂载路径，用于挂载弹性文件服务 1，例如“/localpath”。

```
mkdir /mnt/localpath
```

4. 执行如下命令挂载文件系统。挂载地址在文件系统详情页获取，本地路径为云主机上用于挂载文件系统的本地路径，例如上一步创建的“/mnt/localpath”。

```
mount -t nfs -o vers=3,proto=tcp,async,nolock,noatime,nodiratime,noresvport,wsiz=1048576,rsiz=1048576,timeo=600 挂载地址 本地挂载路径
```

5. 挂载完成后使用 df -h 查看挂载情况。

```
[root@ecs-0020 ~]# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/vda1                  40G       1.8G   39G   5% /
devtmpfs                   485M          0  485M   0% /dev
tmpfs                       496M          0  496M   0% /dev/shm
tmpfs                       496M       13M   483M   3% /run
tmpfs                       496M          0  496M   0% /sys/fs/cgroup
tmpfs                       100M          0  100M   0% /run/user/0
100.100.100.2:/mnt/sfs_perf/f3a17bcffa40a53654d982efe166a793_0q7p9r5xtm8hzugw 500G       32M   500G   1% /mnt/localpath
```

#### 挂载文件系统 2

1. 在同一台云主机上，执行如下命令创建本地挂载路径，用于挂载弹性文件服务 2，例如“/azpath”。

```
mkdir /mnt/azpath
```

2. 执行如下命令挂载文件系统。挂载地址在文件系统详情页获取，本地路径为云主机上用于挂

载文件系统的本地路径，例如上一步创建的 “/mnt/azpath” 。

```
mount -t nfs -o vers=3,proto=tcp,async,nolock,noatime,nodiratime,noresvport,wsize=1048576,rsize=1048576,timeo=600 挂载地址 本地挂载路径
```

3. 挂载完成后使用 df -h 查看挂载情况。

```
[root@ecm 0020 ~]# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/vda1                  40G       1.8G   39G   5% /
devtmpfs                   485M         0   485M   0% /dev
tmpfs                      496M         0   496M   0% /dev/shm
tmpfs                      496M       13M   483M   3% /run
tmpfs                      496M         0   496M   0% /sys/fs/cgroup
tmpfs                      100M         0   100M   0% /run/user/0
100.100.100.2 /mnt/sfs_perf/f3a17bcffa40a53654d982efe166a793_0q7p9r5xtm8hzugw 500G    32M   500G   1% /mnt/localpath
100.100.100.2 /mnt/sfs_perf/f3a17bcffa40a53654d982efe166a793_0j7z4v3p9g9y324t 500G    32M   500G   1% /mnt/azpath
```

#### 步骤四：验证读写

1. 挂载成功后，可以在 Linux ECS 上访问弹性文件系统，执行读取或写入操作。您可以把弹性文件系统当作一个普通的目录来访问和使用。执行如下命令在两个弹性文件服务中创建文件、文件夹。

```
mkdir /mnt/localpath/test1
mkdir /mnt/azpath/test1
touch /mnt/localpath/file1
touch /mnt/azpath/file1
echo '1234' > /mnt/localpath/file2
echo '1234' > /mnt/azpath/file2
ls /mnt/localpath
ls /mnt/azpath
```

```
[root@ecm 0020 ~]# mkdir /mnt/localpath/test1
[root@ecm 0020 ~]# mkdir /mnt/azpath/test1
[root@ecm 0020 ~]# touch /mnt/localpath/file1
[root@ecm 0020 ~]# touch /mnt/azpath/file1
[root@ecm 0020 ~]# echo '1234' > /mnt/localpath/file2
[root@ecm 0020 ~]# echo '1234' > /mnt/azpath/file2
[root@ecm 0020 ~]# ls /mnt/localpath
file1 file2 test1
[root@ecm 0020 ~]# ls /mnt/azpath
file1 file2 test1
```

2. 依次执行如下命令读取文件内容。

```
cat /mnt/localpath/file2
cat /mnt/azpath/file2
```



```
[root@e-100-100 ~]# cat /mnt/localpath/file2
'1234'
[root@e-100-100 ~]# cat /mnt/azpath/file2
'1234'
```

3. 依次执行如下命令删除文件。

```
rm /mnt/localpath/file1 #输入 y
rm /mnt/azpath/file1 #输入 y
ls /mnt/localpath
ls /mnt/azpath
```

```
[root@e-100-100 ~]# rm /mnt/localpath/file1
rm: remove regular empty file '/mnt/localpath/file1'? y
[root@e-100-100 ~]# rm /mnt/azpath/file1
rm: remove regular empty file '/mnt/azpath/file1'? y
[root@e-100-100 ~]# ls /mnt/localpath
file2  test1
[root@e-100-100 ~]# ls /mnt/azpath
file2  test1
```

## 四、 管理文件系统

### 1. 使用 Nginx 代理天翼云弹性文件服务

#### 应用场景

Nginx (engine x) 是一个高性能的 HTTP 和反向代理 web 服务器。

Nginx 是一款轻量级的 Web 服务器/反向代理服务器及电子邮件 (IMAP/POP3) 代理服务器，在 BSD-like 协议下发行。其特点是占有内存少，并发能力强，事实上 nginx 的并发能力确实在同类型的网页服务器中表现较好，中国大陆使用 nginx 网站用户有：百度、京东、新浪、网易、腾讯、淘宝等。

本案例中，使用 1 台 nginx 做反向代理服务器，3 台 nginx 做负载均衡的代理服务。因为在一般的使用中用户可能非常多，所以需要做负载均衡。后端使用天翼云的 sfs 服务。天翼云 sfs 用

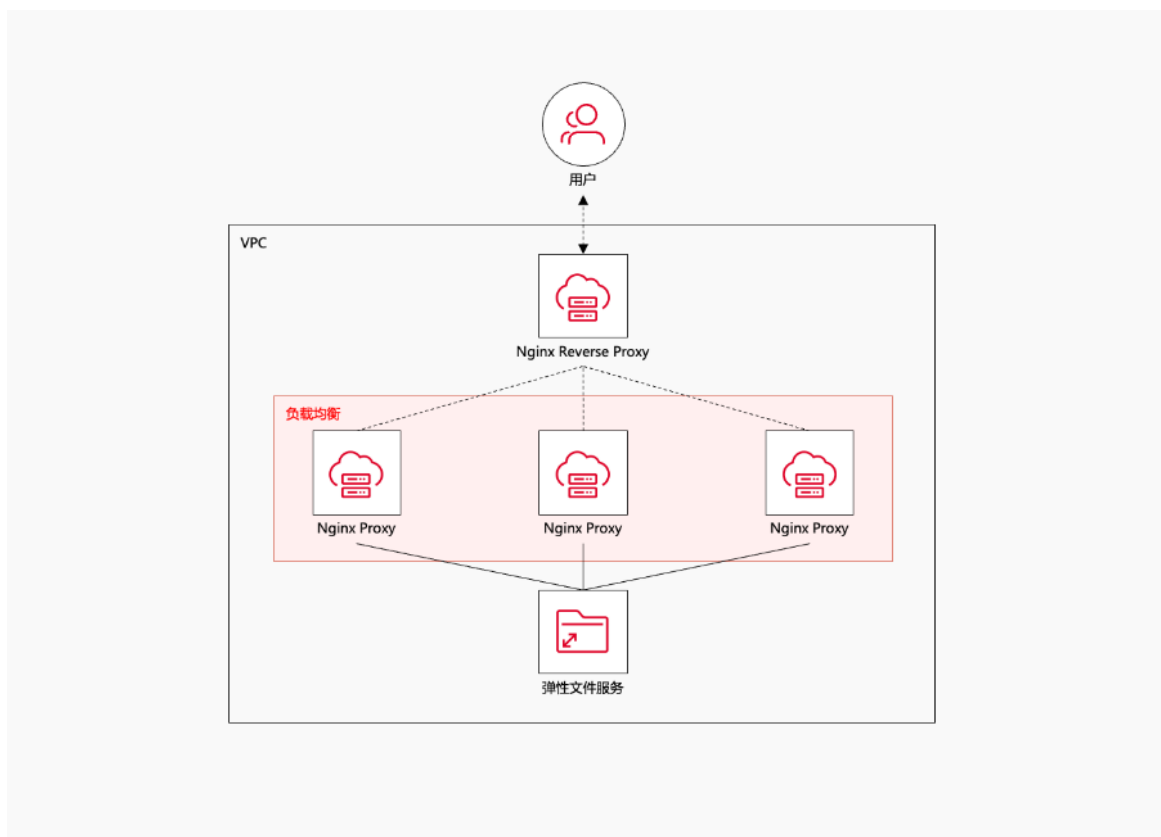
于存储文件，如图片、视频、镜像回源文件或者一些用户的静态数据等。不同的 nginx 代理服务之间共享访问 sfs 数据。此用例中使用 Ctyunos2 完成所有的相关配置。

## 方案使用云产品

弹性文件服务，弹性云主机

## 方案架构

配置的架构如下图：



## 准备工作

在开始之前需要创建一个虚拟机私有云 VPC，一个文件系统，四台云主机，其中一台做反向代理服务器，三台做负载均衡的代理服务。具体操作如下：

1. 在需要操作的地域创建虚拟私有云 VPC，具体操作步骤参见[创建虚拟私有云 VPC](#)。

2. 创建该 VPC 下的弹性云主机，操作系统为 Linux，此处以 CTyunOS 2.0.1 为例演示，具体操作步骤参见[创建弹性云主机](#)。
3. 创建该 VPC 下的文件系统，文件系统的协议类型为 NFS，具体操作步骤参见[创建文件系统](#)。

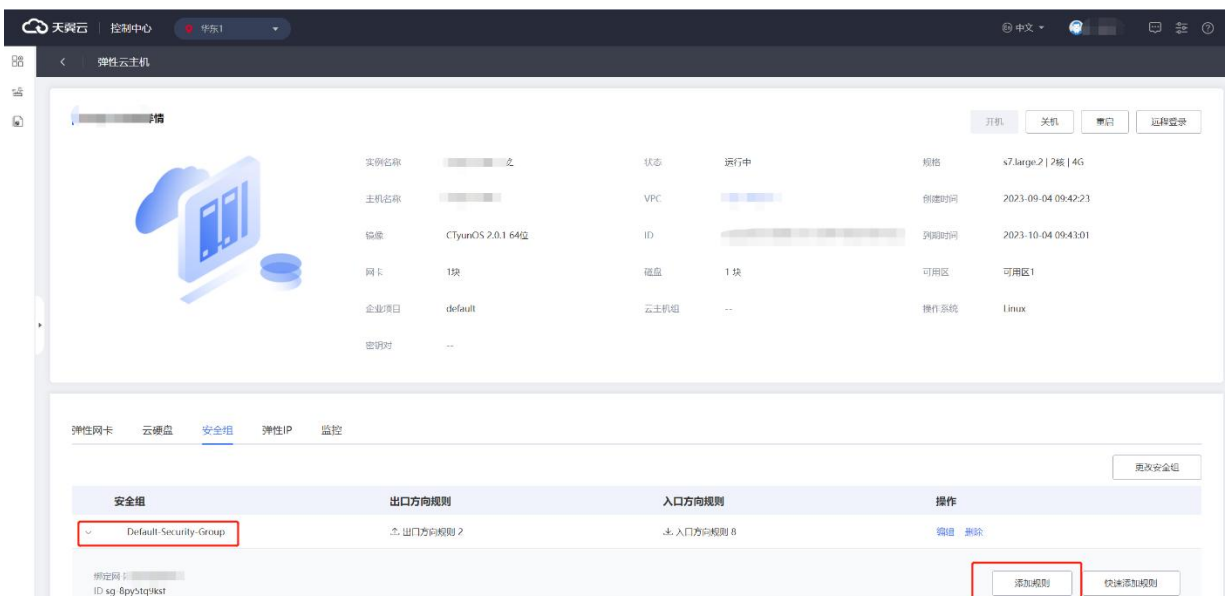
## 操作步骤

### 注意：

操作都是以 root 账号操作，云主机中没有运行其他的进程，避免端口被占用。

### 步骤一：放开云主机 TCP22330 端口

1. 登录“控制中心”，点击“计算>弹性云主机”进入弹性云主机控制台页面。
2. 找到目标云主机，点击名称进入云主机详情页。
3. 在详情页下方，点击“安全组”页签，在该页签默认安全组下点击“添加规则”，具体操作请参考[添加安全组规则](#)。



4. 添加“入方向”规则，各参数选项如下图。添加完成之后，在默认安全组下会显示相应的

规则。

5. 重复以上步骤，对四台云主机均放开 22330 端口。

## 步骤二：部署 nginx 负载均衡代理服务

在三个代理服务器的主机上挂载 nfs，安装部署 nginx。

1. 以 root 用户登录弹性云主机，登录方式参考[登录 Linux 弹性云主机](#)，执行如下命令，安装 NFS 客户端。

```
yum install nfs-utils -y
```

2. 等待安装完成，执行如下命令，安装 Nginx。

```
yum install nginx -y
```

3. 执行如下命令，挂载文件系统到 Nginx 需要代理的目录，参考[挂载 NFS 文件系统到弹性云主机 \(Linux\)](#)。挂载地址在文件系统详情页获取，参考[查看文件系统](#)。

"/usr/share/nginx/html/"是需要挂载在本地主机的目录，也是 Nginx 默认使用的代理目录。

```
mount -t nfs -o vers=3,proto=tcp,async,nolock,noatime,nodiratime,noresvport,wsiz=1048576,rsiz=1048576,timeo=600 挂载地址 /usr/share/nginx/html/
```

4. 执行如下命令，为共享目录下编辑一个 index.html。

```
echo "Test for CT-SFS!" > /usr/share/nginx/html/index.html
```

5. 重复 1-4 步骤，对三台 Nginx 都挂载同一个 NFS 文件系统。

6. 执行 `vi /etc/nginx/nginx.conf` 命令，在该文件中修改 Nginx 的默认端口 80 为 22330，

然后执行以下命令为每一个代理服务器启动 Nginx。

```
systemctl restart nginx
```

```
# Load modular configuration files from the /etc/nginx/conf.d dir
# See http://nginx.org/en/docs/nginx_core_module.html#include
# for more information.
include /etc/nginx/conf.d/*.conf;

server {
    listen      22330;
    listen     [::]:22330;
    server_name _;
    root        /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;
```

7. 验证代理结果。若三台 Nginx 代理服务都可以访问 index.html 文件，则表示配置成功。在

每一个代理服务器上使用 curl 命令验证如下，其中{ip}为云主机的内网 ip，可以在云主机详

情页“弹性网卡”页签下获取。

```
curl "http://{ip}:22330"
```

```
[root@ ~]# curl "http:// 22330"
Test for CT-SFS!
[root@ ~]#
```

在云主机详情页“弹性 IP”页签下找到云主机的公网地址，并在浏览器上输入“{公网 IP 地址}:22330”，预期结果如下：



## Test for CT-SFS!

如网页请求不通但是本地 curl 没有问题，那么关闭防火墙：

```
systemctl stop firewalld
systemctl stop iptables
```

### 步骤三：部署 nginx 反向代理服务

在预先的第四台云主机上安装反向代理。

1. 登录第四台云主机，执行如下命令，安装 Nginx。

```
yum install nginx -y
```

2. 执行如下命令配置反向代理的 Nginx 服务。

```
vi /etc/nginx/nginx.conf
```

修改默认的 http 配置如下，其中 192.168.xxx.xx 为步骤二中三台负载均衡服务器 IP，即三台云主机的内网 IP，可以在云主机详情页“弹性网卡”页签下获取，使用时注意替换。

```
http {
    upstream nfs {
        server 192.168.xxx.xx:22330;
        server 192.168.xxx.xx:22330;
        server 192.168.xxx.xx:22330;
    }

    server {
        listen 22330;
        location / {
            proxy_pass http://nfs;
        }
    }
}
```

3. 执行如下命令，启动反向代理的 Nginx 服务。

```
systemctl restart nginx
```

## 步骤四：测试验证

在第四台云主机，即反向代理服务器上使用 curl 命令请求，其中{ip}为云主机的公网 IP，可以在云主机详情页“弹性 IP”页签下获取。也可以使用内网 IP，在云主机详情页“弹性网卡”页签下获取。

```
curl "http://{ip}:22330"
[root@~]# curl "http://{ip}:22330"
Test for CT-SFS!
[root@~]#
```

在浏览器上输入 "{公网 IP 地址}:22330"，预期结果如下::



如网页请求不通但是本地 curl 没有问题，那么关闭防火墙：

```
systemctl stop firewalld
systemctl stop iptables
```

## 2. 天翼云弹性文件服务子目录权限隔离

### 应用场景

本文主要介绍基于天翼云弹性文件系统，在弹性云主机上挂载后可划分多个子目录并分配给不同用户，通过设置子目录读写权限，已达到多用户之间的访问权限隔离，以便满足安全级别较高的应用场景。

### 方案使用云产品

弹性云主机，弹性文件服务

## 准备工作

- 购买一台弹性云主机，具体操作请参考[创建弹性云主机](#)。
- 购买一个文件系统，具体操作请参考[创建文件系统](#)。

## 操作步骤

### 步骤一：使用 root 帐号登录弹性云主机并添加两个普通用户帐号

1. 以 root 帐号登录弹性云主机，如何登录请参考[登录 Linux 弹性云主机](#)。
2. 添加一个普通用户帐号，如账号 sfsuser1。执行以下命令：

```
useradd sfsuser1  
passwd sfsuser1
```

根据回显提示修改普通用户 sfsuser1 的密码，创建成功后会自动创建账号 sfsuser1 的主目录 “/home/sfsuser1” 。

```
[root@~]# useradd sfsuser1  
[root@~]# passwd sfsuser1  
Changing password for user sfsuser1.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.
```

创建用户sfsuser1并设置登录密码

3. 重复第 2 步继续添加账号 sfsuser2。

### 步骤二：挂载文件系统至弹性云主机

将文件系统挂载到弹性云主机上的一个本地路径上，具体操作请参考[使用弹性云主机挂载文件系统](#)，如已经挂载可忽略此步骤。

### 步骤三：在本地路径创建 2 个子目录并更改目录的属组

1. 执行 `cd /mnt/test` 切换到本地挂载路径，“/mnt/test”为本文步骤二中挂载时创建的本地挂载路径，请根据实际情况替换。



## 2. 创建两个子目录。

```
mkdir subdir1
mkdir subdir2
```

## 3. 更改属组。

```
chown sfsuser1:sfsuser1 subdir1
chown sfsuser2:sfsuser2 subdir2
```

## 步骤四：将 2 个子目录分别挂载至新的本地挂载路径

### 1. 新建 2 个新的本地挂载路径。

```
mkdir /mnt/sfsuser1_test
mkdir /mnt/sfsuser2_test
```

### 2. 将步骤三中 2 个子目录分别挂载至新的本地挂载路径, 挂载地址可在文件系统详情页获取, 参考[查看文件系统](#)。

```
mount -t nfs -o vers=3,nolock,noatime 挂载地址/subdir1 /mnt/sfsuser1_test
mount -t nfs -o vers=3,nolock,noatime 挂载地址/subdir2 /mnt/sfsuser2_test
```

## 步骤五：分别登录两个账号，验证读写权限

### 1. 执行 `su sfsuser1` 命令使用用户 1 (sfsuser1) 登录，验证读写操作。

```
[sfsuser1@... root]$ id 1 ← 检查登录用户
uid=1000(sfsuser1) gid=1000(sfsuser1) groups=1000(sfsuser1)
[sfsuser1@... root]$ cd /mnt/sfsuser1_test 2 ← 切换执行目录
[sfsuser1@... sfsuser1_test]$ echo "hello sfsuser1" > u1.txt 3 ← 写操作验证
[sfsuser1@... sfsuser1_test]$
[sfsuser1@... sfsuser1_test]$ cat u1.txt 4 ← 读操作验证
hello sfsuser1
```

### 2. 执行 `su sfsuser2` 切换到 sfsuser2, 验证访问用户 sfsuser1 子目录的读写权限。验证可发现, sfsuser2 只可读取用户 sfsuser1 的文件，但不具备写和删除权限。

```
[sfsuser2@... sfsuser1_test]$ id 1 ← 用户2
uid=1001(sfsuser2) gid=1001(sfsuser2) groups=1001(sfsuser2)
[sfsuser2@... sfsuser1_test]$ pwd
/mnt/sfsuser1_test 2 ← 切换到sfsuser1用户目录下
[sfsuser2@... sfsuser1_test]$ cat u1.txt 3 ← 读 用户1的文件
hello sfsuser1
[sfsuser2@... sfsuser1_test]$ echo "hello sfsuser2" > u2.txt 4 ← 写文件在用户1的目录下,拒绝
bash: u2.txt: Permission denied
[sfsuser2@... sfsuser1_test]$ rm u1.txt
rm: remove write-protected regular file 'u1.txt'? y 5 ← 删除用户1的文件,拒绝
rm: cannot remove 'u1.txt': Permission denied
[sfsuser2@... sfsuser1_test]$
```

## 步骤六：拒绝其它用户读取权限

1. 如果想进一步缩小权限，拒绝其他用户读权限，可进行以下配置。以修改 sfsuser1 对其它用户的读权限为例：
2. root 用户登录弹性云主机，修改 sfsuser1 子目录的权限为 700。chmod 命令用来变更文件或目录的权限。

```
chmod 700 /mnt/test/subdir1
```

```
[root@... test]# chmod 700 subdir1
[root@... test]# ls -l
total 0
drwx----- 2 sfsuser1 sfsuser1 20 Aug 27 19:24 subdir1
drwxr-xr-x 2 sfsuser2 sfsuser2 6 Aug 27 12:45 subdir2
```

验证 sfsuser2 访问 sfsuser1 目录的读写权限，sfsuser2 无法再次访问 sfsuser1 的子目录。

```
[sfsuser2@... ~]$ id ← 用户2
uid=1001(sfsuser2) gid=1001(sfsuser2) groups=1001(sfsuser2)
[sfsuser2@... ~]$ cd /mnt/sfsuser1_test
bash: cd: /mnt/sfsuser1_test: Permission denied ← 拒绝读写访问权限
[sfsuser2@... ~]$ ls -l /mnt/sfsuser1_test
ls: cannot open directory '/mnt/sfsuser1_test': Permission denied
```

经过以上的实践配置，基本实现在客户端配置多用户访问弹性文件子目录的权限的隔离，您可根据业务需求对子目录或者子目录下的文件进行权限访问控制：

常用权限分类	描述
444 r--r--r--	所属用户只读权限、同组用户只读权限、其他用户只读权限。
600 rw-----	所属用户读写权限、同组用户无权限、其他用户无权限

644 rw-r--r--	所属用户读写权限、同组只读权限、其他用户只读权限
666 rw-rw-rw-	所属用户读写权限、同组用户读写权限、其他用户读写权限
700 rwx-----	所属用户读写和执行权限、同组用户无权限、其他用户无权限
744 rwxr--r--	所属用户读写和执行权限、同组用户只读权限、其他用户无权限
755 rwxr-xr-x	所属用户读写和执行权限、同组用户读和执行权限、其他用户只执行权限。
777 rwxrwxrwx	所属用户、同组用户、其他用户都具备读写执行权限。