Debian

1、欢迎信息

清空motd内容

```
root@ispsrv:~# > /etc/motd
```

注释显示内核版本

```
root@ispsrv:~# vim /etc/update-motd.d/10-uname
#!/bin/sh
#uname -snrvm
```

编辑20-welcome

```
root@ispsrv:~# vim /etc/update-motd.d/20-welcome
#!/bin/sh
echo "*********************************
   ChinaSkills 2020 - Jiangsu
         Module A Linux
          lnxserver1
             zzz

        >>$(hostname)<<
>>$(grep PRETTY /etc/os-release | cut -d '"' -f 2)<<
      >> $(date +%T) <<
*********************************"

root@ispsrv:~# chmod +x /etc/update-motd.d/20-welcome
```

效果

```
Connecting to 81.6.63.100:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

*********************************
   ChinaSkills 2020 - Jiangsu
         Module A Linux
          lnxserver1
             zzz

        >>ispsrv<<
>>Debian GNU/Linux 10 (buster)<<
      >> 06:37:45 <<
*********************************
Last login: Tue May 25 06:37:25 2021 from 81.6.63.109
```

2、网络管理

2.1、网络属性信息

将Linux主机接入到网络，需要配置网络相关设置

一般包括如下内容：

- 主机名
- IP/netmask
- 路由：默认网关
- DNS服务器
    - 主DNS服务器
    - 次DNS服务器

2.2、网络配置

2.2.1、配置文件方式

1、编辑网卡配置文件interfaces

```
vim /etc/network/interfaces
...
auto ens33
iface ens33 inet static
address 81.6.63.100
netmask 255.255.255.0
dns-nameserver 81.6.63.100

# auto ens33 启动服务的时候激活网卡，ens33为网卡名称
# iface ens33 inet static 接口属性配置，支持static（静态）、dhcp（动态)、none（默认）模式
# address，IP地址配置，支持IP/PREFIX方式
# netmask，掩码
# gateway，网关地址
# dns-search 搜索域 需要安装resolvconf软件包
# dns-nameserver DNS服务器 需要安装resolvconf软件包
```

2、重启网络服务

```
systemctl restart networking
```

2.2.2、命令行方式

2.2.2.1、IP命令

获取帮助

```
root@debian:~# ip help
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
OBJECT := { link | address | route }
```

address配置相关

```
root@debian:~# ip addr help
Usage: ip address {add|change|replace} IFADDR dev IFNAME [ LIFETIME ]
                                                      [ CONFFLAG-LIST ]
       ip address del IFADDR dev IFNAME [mngtmpaddr]
       ip address {save|flush} [ dev IFNAME ] [ scope SCOPE-ID ]
                            [ to PREFIX ] [ FLAG-LIST ] [ label LABEL ] [up]
       ip address [ show [ dev IFNAME ] [ scope SCOPE-ID ] [ master DEVICE ]
                         [ type TYPE ] [ to PREFIX ] [ FLAG-LIST ]
                         [ label LABEL ] [up] [ vrf NAME ] ]
       ip address {showdump|restore}
```

添加IP地址（add）

```
root@debian:~# ip addr add 172.16.100.199/25 dev ens33
```

查看ip地址

```
root@debian:~# ip add
...
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:7e:9c:34 brd ff:ff:ff:ff:ff:ff
    inet 172.16.100.201/25 brd 172.16.100.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet 172.16.100.199/25 scope global secondary ens33
       valid_lft forever preferred_lft forever
```

删除ip地址（del）

```
root@debian:~# ip addr del 172.16.100.199/25 dev ens33
```

route相关

```
root@debian:~# ip route help
Usage: ip route { list | flush } SELECTOR
       ip route { add | del | change | append | replace } ROUTE
```

查看路由信息（list）

```
root@debian:~# ip route
default via 172.16.100.254 dev ens33 onlink
172.16.100.128/25 dev ens33 proto kernel scope link src 172.16.100.201
```

2.3、DNS配置

设置DNS服务器地址

```
root@debian:~# vim /etc/resolv.conf
search chinasskills.cn        #搜索域，即www自动补齐为www.sdskills.com
nameserver 81.6.63.100        #DNS服务器地址
```

2.4、路由转发

1、修改sysctl.conf配置文件

```
vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

2、重载配置文件

```
sysctl -p
net.ipv4.ip_forward = 1
```

3、软件包管理

3.1、默认源

系统安装的时候已经默认添加了CDROM源，DLBD版无需修改即可直接使用，注意光驱的连接状态

```
apt-cdrom add命令用于自动添加光驱源

默认配置
cat /etc/apt/sources.list
deb cdrom:[Debian GNU/Linux 10.6.0 _Buster_ - Official amd64 DLBD Binary-1
20200926-10:17]/ buster contrib main
```

注意：如存在网络源，请注释掉网络源。

3.2、dpkg命令

dpkg命令无法解决软件包依赖

3.2.1、获取帮助

```
root@debian:~# dpkg --help
Usage: dpkg [<option> ...] <command>
Commands:
  -i|--install       <.deb file name>... | -R|--recursive <directory>...
  -r|--remove        <package>... | -a|--pending
  -L|--listfiles <package>...      List files 'owned' by package(s).
```

3.2.2、install

安装deb软件包

```
#挂载光驱
mount /dev/cdrom /mnt

#安装zsh软件包
root@debian:~# dpkg -i /mnt/pool/main/z/zsh/zsh-common_5.7.1-1_all.deb
```

3.2.3、listfile

查看软件包生成的文件

```
root@debian:~# dpkg -L zsh-common
/etc
/etc/zsh
/etc/zsh/newuser.zshrc.recommended
/etc/zsh/zlogin
/etc/zsh/zlogout
/etc/zsh/zprofile
/etc/zsh/zshenv
/etc/zsh/zshrc
...
```

3.2.4、remove

移除zsh软件包

```
root@debian:~# dpkg -r zsh-common
```

3.3、apt命令

3.3.1、获取帮助 help

```
root@debian:~# apt help
apt 1.8.2.1 (amd64)
Usage: apt [options] command

Most used commands:
  list - list packages based on package names
  search - search in package descriptions
  show - show package details
  install - install packages
  reinstall - reinstall packages
  remove - remove packages
  autoremove - Remove automatically all unused packages
  update - update list of available packages
  upgrade - upgrade the system by installing/upgrading packages
  full-upgrade - upgrade the system by removing/installing/upgrading packages
  edit-sources - edit the source information file
```

3.3.2、list

列出软件源里的软件包

```
root@debian:~# apt list
Listing...
0ad-data-common/unknown 0.0.23.1-1 all
0ad-data/unknown 0.0.23.1-1 all
0ad/unknown 0.0.23.1-2 amd64
0install-core/unknown 2.12.3-2 amd64
...
```

3.3.3、install

安装软件，如vim

```
root@debian:~# apt install vim
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  vim-runtime
Suggested packages:
  ctags vim-doc vim-scripts
The following NEW packages will be installed:
  vim vim-runtime
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/7,055 kB of archives.
After this operation, 33.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

3.3.4、remove

卸载软件包

```
root@debian:~# apt remove vim
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  vim-runtime
Use 'apt autoremove' to remove it.
The following packages will be REMOVED:
  vim
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 2,867 kB disk space will be freed.
Do you want to continue? [Y/n] y
```

4、squid

Squid cache（简称为Squid）是一个流行的自由软件（GNU通用公共许可证）的代理服务器和Web缓存服务器。Squid有广泛的用途，从作为网页服务器的前置cache服务器缓存相关请求来提高Web服务器的速度，到为一组人共享网络资源而缓存万维网，域名系统和其他网络搜索，到通过过滤流量帮助网络安全，到局域网通过代理上网。Squid主要设计用于在Unix一类系统运行。

1.安装squid服务

```
apt install -y squid
```

2.查看服务运行状态

```
systemctl status squid
```

3.配置squid服务

```
cd /etc/squid
mv squid.conf squid.conf.bak    //备份原有配置文件
vim squid.conf
http_port 3128                 #监听端口
http_access allow all          #允许所有客户端访问
```

4.重启squid服务

```
systemctl restart squid
```

5、iptables

IPTABLES 是与 Linux 内核集成的 IP 信息包过滤系统。如果 Linux 系统连接到因特网或 LAN、服务器或连接 LAN 和因特网的代理服务器， 则该系统有利于在 Linux 系统上更好地控制 IP 信息包过滤和防火墙配置。

1、添加规则

```
iptables -t nat -I PREROUTING -p tcp --dport 53 -d 81.6.63.254 -j DNAT --to-
destination  192.168.100.100
iptables -t nat -I PREROUTING -p udp --dport 53 -d 81.6.63.254 -j DNAT --to-
destination  192.168.100.100
iptables -t nat -I PREROUTING -p tcp --dport 80 -d 81.6.63.254 -j DNAT --to-
destination  192.168.100.100
iptables -t nat -I PREROUTING -p tcp --dport 443 -d 81.6.63.254 -j DNAT --to-
destination  192.168.100.100
iptables -t nat -I PREROUTING -p tcp --dport 465 -d 81.6.63.254 -j DNAT --to-
destination  192.168.100.100
iptables -t nat -I PREROUTING -p tcp --dport 993 -d 81.6.63.254 -j DNAT --to-
destination  192.168.100.100
iptables -t nat -I PREROUTING -p tcp --dport 21 -d 81.6.63.254 -j DNAT --to-
destination  192.168.100.100

iptables -t nat -I POSTROUTING -s 192.168.100.0/24 -j SNAT --to-source
81.6.63.254
iptables -t nat -I POSTROUTING -s 192.168.0.0/24 -j SNAT --to-source 81.6.63.254

iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -I OUTPUT -m state --state ESTABLISHED -j ACCEPT
iptables -I FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

2、查看规则状态

```
root@routersrv:~# iptables -vnL
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

   27  1704 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
       state RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

```
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
      state RELATED,ESTABLISHED

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

   18  1944 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
      state ESTABLISHED

root@routersrv:~# iptables -t nat -vnL
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            81.6.63.254
      tcp dpt:21 to:192.168.100.100
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            81.6.63.254
      tcp dpt:993 to:192.168.100.100
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            81.6.63.254
      tcp dpt:465 to:192.168.100.100
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            81.6.63.254
      tcp dpt:443 to:192.168.100.100
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            81.6.63.254
      tcp dpt:80 to:192.168.100.100
    0     0 DNAT       udp  --  *      *       0.0.0.0/0            81.6.63.254
      udp dpt:53 to:192.168.100.100
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            81.6.63.254
      tcp dpt:53 to:192.168.100.100

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 SNAT       all  --  *      *       192.168.0.0/24       0.0.0.0/0
      to:81.6.63.254
    0     0 SNAT       all  --  *      *       192.168.100.0/24     0.0.0.0/0
      to:81.6.63.254

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

6、DHCP配置

6.1、DHCP服务

DHCP（动态主机配置协议）是一个局域网的网络协议。指的是由服务器控制一段IP地址范围，客户机登录服务器时就可以自动获得服务器分配的IP地址和子网掩码。

1、安装软件包

```
root@ispsrv:~# apt install isc-dhcp-server -y
```

2、监听网卡

```
root@Rserver:~# vim /etc/default/isc-dhcp-server
INTERFACESv4="ens33"        //根据实际网卡编号而定
INTERFACESv6=""
```

3、修改dhcpd.conf配置文件

```
root@ispsrv:~# vim /etc/dhcp/dhcpd.conf

# IspSrv给outsidecli客户端网络分配地址
subnet 81.6.63.0 netmask 255.255.255.0 {
  range 81.6.63.110 81.6.63.190;
  option domain-name-servers 81.6.63.100;
  option domain-name "chinaskills.cn";
  option routers 81.6.63.254;
  default-lease-time 600;
  max-lease-time 7200;
}

# 注意当前网卡的IP地址段必须在分配的地址段中有体现
# AppSrv给insidecli客户端网络分配地址
subnet 192.168.100.0 netmask 255.255.255.0 {}
subnet 192.168.0.0 netmask 255.255.255.0 {
  range 192.168.0.110 192.168.0.190;
  option domain-name-servers 192.168.100.100;
  option domain-name "chinaskills.cn";
  option routers 192.168.0.254;
  default-lease-time 600;
  max-lease-time 7200;
}


# 给insidecli分配固定IP地址
host insidecli {
  hardware ethernet 00:0c:29:78:25:e3;
  fixed-address 192.168.0.190;
}

# 注释
#subnet：定义分配的地址网段
#range：分配给客户端的地址
#option domain-name-servers：分配给客户端的DNS地址
#option domain-name：分配给客户端的域名
#option routers：客户端的网关
#default-lease-time：默认租约时长
#max-lease-time：最大租约时长
#hardware ethernet：MAC地址
#fixed-address：分配固定IP地址
```

4、重新启动服务

```
systemctl restart isc-dhcp-server
```

5、查看DHCP获取

```
root@outsidecli:~# dhclient -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens33/00:0c:29:22:af:15
Sending on   LPF/ens33/00:0c:29:22:af:15
Sending on   Socket/fallback
DHCPREQUEST for 81.6.63.111 on ens33 to 255.255.255.255 port 67
DHCPACK of 81.6.63.111 from 81.6.63.100
RTNETLINK answers: File exists
bound to 81.6.63.111 -- renewal in 235 seconds.
```

6.2、DHCP中继

1、安装isc-dhcp-relay软件包

```
apt install isc-dhcp-relay -y
```

2、编辑isc-dhcp-relay配置文件

```
vim /etc/default/isc-dhcp-relay
SERVERS="192.168.100.100"   #dhcp服务器地址
INTERFACES="ens33:1"        #要为该接口的网段分配地址
```

3、重启服务

```
systemctl restart isc-dhcp-relay
```

7、SSH服务

SSH 为 Secure Shell 的缩写，由 IETF 的网络小组（Network Working Group）所制定；SSH 为建立在应用层基础上的安全协议。SSH 是较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。SSH最初是UNIX系统上的一个程序，后来又迅速扩展到其他操作平台。SSH在正确使用时可弥补网络中的漏洞。SSH客户端适用于多种平台。几乎所有UNIX平台—包括HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix，以及其他平台，都可运行SSH。

7.1、用户登录限制

1、安装openssh-server软件包

```
apt install openssh-server
```

2、编辑sshd_conf配置文件

```
vim /etc/ssh/sshd_config
Port 2021                  #监听端口
PermitRootLogin no         #是否允许root登录，no表示不允许
#AllowUsers *@10.10.100.*  #允许10.10.100网段的主机访问
AllowUsers user01          #仅允许用户user01访问
```

3、重启服务

```
systemctl restart sshd
```

或

1、编辑hosts.deny配置文件

```
vim /etc/hosts.allow
sshd: 10.10.100.1

vim /etc/hosts.deny
sshd: ALL

#服务：客户端
```

2、连接测试

```
root@Rserver:~# ssh 192.168.10.3 -p 2233
ssh_exchange_identification: read: Connection reset by peer
```

7.2、免密登录

1、登录Chinaskill20用户，生成密钥

```
ssh-keygen
```

2、将密钥发送给服务器（一定要在Chinaskill20用户下）

```
ssh-copy-id root@192.168.10.2 -p 2222

# root@192.168.0.2
#root：用户名
#192.168.0.2：服务器IP地址
```

3、登录测试

```
ssh root@192.168.10.2 -p 2222
#
```

7.3、用户登录次数限制

1、编辑sshd PAM文件

```
vim /etc/pam.d/sshd
auth required pam_tally2.so deny=3 unlock_time=60 even_deny_root
root_unlock_time=60
...

# deny：                设置普通用户和root用户连续错误登陆的最大次数，超过最大次数，则锁定该
用户
# unlock_time：         设定普通用户锁定后，多少时间后解锁，单位是秒
# root_unlock_time：    设定root用户锁定后，多少时间后解锁，单位是秒
```

2、查看用户状态

```
pam_tally2 -u user01     #失败次数
pam_tally2 -r -u user01  #重置失败次数
```

7.4、日志设置

1、修改sshd_config日志设置

```
vim /etc/ssh/sshd_config
#SyslogFacility AUTH       # 设施
#LogLevel INFO  # 日志级别，QUIET,FATAL,ERROR,INFO,VERBOSE,DEBUG,DEBUG1,DEBUG2,and
DEBUG3.The default is INFO.
SyslogFacility local0
LogLevel VERBOSE
```

2、修改rsyslog

```
vim /etc/rsyslog.conf
local0.*            -/var/log/ssh.log

#local0.* 表示local0设施的所有级别的日志消息
```

3、重启服务

```
systemctl restart sshd rsyslog
```

8、CA

1、修改配置文件，指定CA路径

```
vim /usr/lib/ssl/openssl.cnf...dir = /CA
...
dir     = /csk-rootca                     #CA目录
certificate = $dir/csk-ca.pem             #CA证书
private_key = $dir/private/csk-key.pem    #CA私钥
...
```

2、生成CA相关目录

```
mkdir /csk-rootca/{private,newcerts} -p
touch /csk-rootca/index.txt
echo 01 > /csk-rootca/serial
```

3、生成私钥和自签名证书

```
openssl genrsa -out /csk-rootca/private/csk-key.pem
openssl req -new -x509 -key /csk-rootca/private/csk-key.pem -out /csk-rootca/csk-ca.pem -subj "/C=CN/ST=China/L=BeiJing/O=skills/OU=Operations Departments/CN=CSK Global Root CA"

-subj
/C=CN ： 设置国家
/ST=GD ： 设置省份
/L=GZ ： 设置城市
/O=Inc ：设置组织
/OU=www.skills.com ： 设置组织机构
/CN=Skill Global Root CA ： 设置公用名
```

3、查看证书

```
root@appsrv:~# openssl x509 -in /csk-rootca/csk-ca.pem -text -noout
Certificate:
 Data:
   Version: 3 (0x2)
   Serial Number:
       33:9f:ad:b5:27:3b:63:67:29:40:91:0f:08:f5:40:37:05:1e:89:68
   Signature Algorithm: sha256WithRSAEncryption
   Issuer: C = CN, ST = China, L = BeiJing, O = skills, OU = Operations
Departments, CN = CSK Global Root CA
   Validity
       Not Before: May 31 03:18:54 2021 GMT
       Not After : Jun 30 03:18:54 2021 GMT
  Subject: C = CN, ST = China, L = BeiJing, O = skills, OU = Operations
Departments, CN = CSK Global Root CA
   Subject Public Key Info:
       Public Key Algorithm: rsaEncryption
          RSA Public-Key: (2048 bit)
...
```

9、用户和组管理

```
用户加组groupadd ldsgp
useradd –g ldsgp –s /bin/bash zsuser
useradd –g ldsgp –s /bin/bash lsuse
ruseradd –g ldsgp –s /bin/bash wuuser
```

10、存储管理

10.1、RAID5

独立磁盘冗余阵列（RAID，redundant array of independent disks）是把相同的数据存储在多个硬盘的不同的地方的方法。通过把数据放在多个硬盘上，输入输出操作能以平衡的方式交叠，改良性能。因为多个硬盘增加了平均故障间隔时间（MTBF），储存冗余数据也增加了容错。

1、添加硬盘，让系统重新扫描SCSI总线

```
echo "- - -" > /sys/class/scsi_host/host2/scan
echo "- - -" > /sys/class/scsi_host/host0/scan
```

2、安装mdadm

```
apt install mdadm -y
```

3、创建raid5，空闲盘一个

```
mdadm -C -n 3 -l 5 -a yes -x 1 /dev/md0 /dev/sd{b,c,d,e}

-C：创建RAID阵列
-n：磁盘或分区数
-l：raid级别
-x：空闲盘，热备盘
/dev/md0：设备名称
```

4、查看raid5设备信息

```
root@ispsrv:~# mdadm -D /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Tue May 25 10:07:45 2021
        Raid Level : raid5
        Array Size : 20953088 (19.98 GiB 21.46 GB)
     Used Dev Size : 10476544 (9.99 GiB 10.73 GB)
      Raid Devices : 3
     Total Devices : 4
       Persistence : Superblock is persistent

       Update Time : Tue May 25 10:08:38 2021
             State : clean
    Active Devices : 3
   Working Devices : 4
    Failed Devices : 0
     Spare Devices : 1

            Layout : left-symmetric
        Chunk Size : 512K

Consistency Policy : resync

              Name : ispsrv:0  (local to host ispsrv)
              UUID : 4b327bf2:750e9d3d:bcdd660a:6d31b5cf
            Events : 18

    Number   Major   Minor   RaidDevice State
       0       8       16        0      active sync   /dev/sdb
       1       8       32        1      active sync   /dev/sdc
       4       8       48        2      active sync   /dev/sdd

       3       8       64        -      spare   /dev/sde
```

5、写入配置文件

```
mdadm --detail --scan >> /etc/mdadm/mdadm.conf
update-initramfs -u
```

6、格式化并挂载

```
mkfs.ext4 /dev/md0
mkdir /backup
mount /dev/md0 /backup/

#mkfs 命令用于格式化文件系统，linux操作系统一般支持ext2,ext3,ext4文件系统
#mount DEVICE POINT  命令用于挂载设备
```

10.2、磁盘加密

1、安装cryptsetup

```
apt install cryptsetup -y
```

2、磁盘/分区加密

```
cryptsetup luksFormat /dev/sdf

WARNING!
========
This will overwrite data on /dev/sdf irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase for /dev/sdf:
Verify passphrase:

```

3、映射分区

```
cryptsetup open /dev/sdf crypt
Enter passphrase for /dev/sdf:
```

4、格式化分区，挂载设备

```
mkfs.ext4 /dev/mapper/crypt

mkdir /mut/crypt -p
mount /dev/mapper/crypt /mut/crypt/
```

5、开机自动挂载

```
vim /etc/fstab
/dev/mapper/crypt   /mut/crypt  ext4    defaults 0 0
```

6、设备映射

```
vim /etc/crypttab
# <target name> <source device>     <key file>  <options>
crypt   /dev/sdf    /etc/.sdfpasswd
```

7、生成key文件

```
echo "CSK2021!" > /etc/.sdfpasswd
```

8、为加密的设备添加密码校验文件

```
cryptsetup luksAddKey /dev/sdf /etc/.sdfpasswd
Enter any existing passphrase:
```

9、删除加密设备

```
vim /etc/fstab
#/dev/mapper/crypt  /mut/crypt  ext4    defaults 0 0

vim /etc/crypttab
# <target name> <source device>     <key file>  <options>
#crypt  /dev/sdf    /etc/.sdfpasswd

umount /dev/mapper/crypt

cryptsetup close crypt
```

10.3、LVM

LVM（Logical Volume Manager）逻辑卷管理，是在硬盘分区和文件系统之间添加的一个逻辑层，为文件系统屏蔽下层硬盘分区布局，并提供一个抽象的盘卷，在盘卷上建立文件系统。管理员利用LVM可以在硬盘不用重新分区的情况下动态调整文件系统的大小，并且利用LVM管理的文件系统可以跨越物理硬盘。当服务器添加了新的硬盘后，管理员不必将原有的文件移动到新的硬盘上，而是通过LVM直接扩展文件系统来跨越物理硬盘。

LVM就是通过将底层的物理硬盘封装，然后以逻辑卷的方式呈现给上层应用。当我们对底层的物理硬盘进行操作时，不再是针对分区进行操作，而是通过逻辑卷对底层硬盘进行管理操作。

1、安装lvm2软件包

```
apt install lvm2 -y
```

2、创建逻辑卷

```
pvcreate /dev/md0
vgcreate vg01 /dev/md0
lvcreate -l 100%FREE -n lv01 vg01
mkfs.ext4 /dev/mapper/vg01-lv01



#lvcreate
#-l：指定要创建的逻辑卷的大小，count的个数，
#-L #：指定要创建的逻辑卷的大小，100G
#-n NAME：逻辑卷的名称
```

3、挂载

```
# 手动挂载
mkdir /webdata
mount /dev/mapper/vg01-lv01 /webdata
touch /webdata/disk.txt

# 开机自动挂载
vim /etc/fstab
/dev/mapper/vg01-lv01   /webdata    ext4    defaults    0 0

root@Server01:~# mount -a
#mount -a  #根据/etc/fstab文件内容自动挂载设备
```

4、查看挂载

```
root@Server01:~# mount | grep vg01
/dev/mapper/vg01-lv01 on /data type ext4 (rw,relatime,stripe=256)
```

10.4、ISCSI

10.4.1、服务端配置

1、安装targetcli-fb软件包

```
apt install targetcli-fb -y
```

2、进入交互式界面配置

```
targetcli
/>
```

3、添加后端存储，LVM逻辑卷的创建参考LVM章节

```
/> cd backstores/block/
/backstores/block> create dev=/dev/iscsivg/iscsistore name=serverc.iscsistore
```

4、创建iqn

```
cd /iscsi
/iscsi> create iqn.2021-03.com.rj.iscsi:serverc
```

5、设置监听地址和端口

```
cd /iscsi/iqn.2021-03.com.rj.iscsi:serverc/tpg1/portals/
/iscsi/iqn.20.../tpg1/portals> delete 0.0.0.0 ip_port=3260
/iscsi/iqn.20.../tpg1/portals> create 192.168.100.200 ip_port=3260
```

6、关联后端存储

```
cd /iscsi/iqn.2021-03.com.rj.iscsi:serverc/tpg1/luns/
/iscsi/iqn.20...erc/tpg1/luns> create /backstores/block/serverc.iscsistore lun=0
```

7、关闭认证

```
cd /iscsi/iqn.2021-03.com.rj.iscsi:serverc/tpg1/
/iscsi/iqn.20...:serverc/tpg1> set attribute authentication=0
```

8、关闭ACL

```
/iscsi/iqn.20...:serverc/tpg1> set attribute generate_node_acls=1
```

9、exit退出

10.4.2、客户端配置

1、安装open-iscsi软件包

```
apt install open-iscsi -y
```

2、扫描iscsi设备

```
iscsiadm -m discovery -t st -p 192.168.100.200
```

3、关联设备

```
iscsiadm -m node -T iqn.2021-03.com.rj.iscsi:serverc -l
```

11、NFS

网络文件系统，英文Network File System(NFS)，是由SUN公司研制的UNIX表示层协议(presentation layer protocol)，能使使用者访问网络上别处的文件就像在使用自己的计算机一样。

1、安装软件包

```
apt install nfs-kernel-server -y
```

2、编辑exports配置文件实现共享目录

```
vim /etc/exports
/webdata    192.168.100.100/32(rw,no_root_squash)

#共享目录       共享目标(权限)
#ro：只读
#rw：读写
#no_root_squash：不压缩root权限
```

3、重新启动服务

```
systemctl restart nfs-server
```

4、查看共享

```
exportfs -arv

exportfs: /etc/exports [1]: Neither 'subtree_check' or 'no_subtree_check'
specified for export "192.168.100.100/32:/webdata".
  Assuming default behaviour ('no_subtree_check').
  NOTE: this default has changed since nfs-utils version 1.0.x

exporting 192.168.100.100/32:/webdata
```

5、客户端挂载

```
# 命令行方式挂载
mkdir /webdata
mount 192.168.100.200:/webdata /webdata
注意：需要安装nfs-kernel-server软件包

# 配置文件方式挂载
vim /etc/fstab
192.168.100.200:/webdata    /webdata    nfs defaults,_netdev    0 0

mount -a
注意：此处需要安装nfs-kernel-server软件包，让操作系统支持nfs文件系统
```

12、DNS

域名系统（英文：Domain Name System，缩写：DNS）是互联网的一项服务。它作为将域名和IP地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。DNS使用TCP和UDP端口53。当前，对于每一级域名长度的限制是63个字符，域名总长度则不能超过253个字符。

12.1、master配置

1、安装bind9软件包

```
apt install bind9 dnsutils -y
```

2、添加区域

```
root@appsrv:~# vim /etc/bind/named.conf.default-zones

// prime the server with knowledge of the root servers
view inside {
match-clients { 127.0.0.0/8; 192.168.100.0/24; 192.168.0.0/24; };
zone "." {
    type hint;
    file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};

zone "chinaskills.cn" {
    type master;
    file "/etc/bind/db.inside.chinaskills.cn";
};

};
view outside {
match-clients { 0.0.0.0/0; };

zone "chinaskills.cn" {
    type master;
    file "/etc/bind/db.outside.chinaskills.cn";
};

};
```

3、添加解析记录

```
cp /etc/bind/db.local /etc/bind/db.inside.chinaskills.cn
cp /etc/bind/db.local /etc/bind/db.outside.chinaskills.cn

# inside配置
root@appsrv:~# vim /etc/bind/db.inside.chinaskills.cn

;
; BIND data file for local loopback interface
;
$TTL    604800
@   IN  SOA localhost. root.localhost. (
                  2     ; Serial
             604800     ; Refresh
              86400     ; Retry
            2419200     ; Expire
             604800 )   ; Negative Cache TTL
;
@   IN  NS  localhost.
@   IN  A   127.0.0.1
@   IN  MX  10 mail
mail    IN  A   192.168.100.100
www IN  A   192.168.100.100
download    A   192.168.100.100
smtp    IN  A   192.168.100.100
```

```
imap    IN  A   192.168.100.100
appsrv  IN  A   192.168.100.100
storagesrv  A   192.168.100.200

# outside配置
root@appsrv:~# vim /etc/bind/db.outside.chinaskills.cn
;
; BIND data file for local loopback interface
;
$TTL    604800
@   IN  SOA localhost. root.localhost. (
                  2     ; Serial
             604800     ; Refresh
              86400     ; Retry
            2419200     ; Expire
             604800 )   ; Negative Cache TTL
;
@   IN  NS  localhost.
@   IN  A   127.0.0.1
@   IN  MX  10 mail
mail    IN  A   81.6.63.254
www IN  A   81.6.63.254
download    A   81.6.63.254
smtp    IN  A   81.6.63.254
imap    IN  A   81.6.63.254
ispsrv  IN  A   81.6.63.100
```

4、转发设置

```
root@appsrv:~# vim /etc/bind/named.conf.options
    forwarders {
        81.6.63.100;
    };
    dnssec-validation no;
```

5、重新启动服务

```
systemctl restart bind9
```

6、测试

```
root@appsrv:~# host www.chinaskills.cn 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

www.chinaskills.cn has address 192.168.100.100

root@appsrv:~# host 1 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

1.localdomain has address 81.6.63.100
```

12.2、slave配置

1、安装bind9软件包

```
apt install bind9 dnsutils -y
```

2、添加区域

```
vim /etc/bind/named.conf.default-zones

zone "." {
    type master;
    file "/etc/bind/root.ca";
};

zone "chinaskills.cn" {
    type slave;
    file "chinaskills.cn";
    masters { 81.6.63.254; };
};
```

3、添加解析记录

```
root@ispsrv:~# cp /etc/bind/db.local /etc/bind/root.ca
root@ispsrv:~# vim /etc/bind/root.ca
;
; BIND data file for local loopback interface
;
$TTL    604800
@   IN  SOA localhost. root.localhost. (
                  2     ; Serial
             604800     ; Refresh
              86400     ; Retry
            2419200     ; Expire
             604800 )   ; Negative Cache TTL
;
@   IN  NS  localhost.
@   IN  A   127.0.0.1
*   IN  A   81.6.63.100
```

4、重新启动服务

```
root@ispsrv:~# systemctl restart bind9
```

5、设置DNS解析服务器

```
root@ispsrv:~# vim /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 81.6.63.100
```

6、测试

```
root@ispsrv:~# host 1
1 has address 81.6.63.100
```

13、LAMP/LNMP

13.1、apache

1、安装软件包

```
apt install apache2 -y
```

2、修改服务运行用户

```
# 添加webuser系统用户
useradd -r webuser

# 修改服务运行用户
vim /etc/apache2/apache2.conf
User webuser
Group webuser
```

3、修改站点配置文件

```
<VirtualHost *:80>
  ServerName www.chinaskills.cn
  Redirect permanent / https://www.chinaskills.cn/
</VirtualHost>

<VirtualHost *:80>
  ServerName download.chinaskills.cn
  Redirect permanent / https://download.chinaskills.cn/
</VirtualHost>

<VirtualHost *:443>
  ServerName www.chinaskills.cn
  DocumentRoot "/webdata/wordpress"
  SSLEngine ON
  SSLCertificateFile "/csk-rootca/apache.crt"
  SSLCertificateKeyFile "/csk-rootca/apache.key"
  <Directory "/webdata/wordpress">
    Require all granted
  </Directory>
</VirtualHost>

# 采用basic userfile认证
<VirtualHost *:443>
  ServerName download.chinaskills.cn
  DocumentRoot "/webdata/download"
  ServerSignature Off
  SSLEngine ON
  SSLCertificateFile "/csk-rootca/apache.crt"
  SSLCertificateKeyFile "/csk-rootca/apache.key"
  <Directory "/webdata/download">
    options Indexes
    AuthType Basic
    AuthName "login"
    AuthUserFile "/etc/apache2/.htpasswd"
    Require valid-user
  </Directory>
</VirtualHost>

# 采用basic ldap认证，ldap参考ldap章节,需要安装libapache2-mod-authnz-pam软件包
<VirtualHost *:443>
  ServerName download.chinaskills.cn
  DocumentRoot "/webdata/download"
  ServerSignature Off
  SSLEngine ON
  SSLCertificateFile "/csk-rootca/apache.crt"
  SSLCertificateKeyFile "/csk-rootca/apache.key"
  <Directory "/webdata/download">
    options Indexes
    AuthType Basic
    AuthName "ldap auth"
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://192.168.100.200/dc=chinaskills,dc=cn"
    Require ldap-group cn=ldsgp,ou=groups,dc=chinaskills,dc=cn
    #Require valid-user
  </Directory>
</VirtualHost>
```

4、生成证书

```
openssl genrsa -out /csk-rootca/apache.key

openssl req -new -key /csk-rootca/apache.key -out /csk-rootca/apache.csr -subj "/C=CN/ST=China/L=BeiJing/O=skills/OU=Operations Departments/CN=*.chinaskills.cn"

openssl ca -in /csk-rootca/apache.csr -out /csk-rootca/apache.crt
y
y
```

5、启用ssl模块

```
a2enmod ssl
```

6、生成目录和测试文件

```
mkdir /webdata/{wordpress,download} -p
touch /webdata/download/test.{mp3,pdf}
dd if=/dev/zero of=/webdata/download/test.mp4 bs=1M count=100
```

7、生成.htpasswd文件

```
groupadd ldsgp
useradd -g ldsgp wsus
htpasswd -c /etc/apache2/.htpasswd wsus
```

8、重启服务

```
systemctl restart apache2
```

限制内存

1、修改grub启动参数

```
vim /etc/default/grub
GRUB_CMDLINE_LINUX="cgroup_enable=memory"
```

2、更新grub设置，重启系统

```
update-grub
reboot
```

3、查看当前内存限制

```
cat /sys/fs/cgroup/memory/system.slice/apache2.service/memory.limit_in_bytes
```

4、修改内存限制

```
echo 500M >
/sys/fs/cgroup/memory/system.slice/apache2.service/memory.limit_in_bytes
```

13.2、nginx

13.2.1、nginx+php-fpm

1、安装nginx

```
apt install nginx php-fpm curl -y
```

2、删除默认配置文件，编辑ispweb.conf

```
rm /etc/nginx/sites-enabled/default

vim /etc/nginx/conf.d/ispweb.conf
server {
    listen 80 default_server;
    root /mut/crypt;
    index index.php index.html index.htm index.nginx-debian.html;
    server_name _;
    location / {
        try_files $uri $uri/ =404;
    }
    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.3-fpm.sock;
    }
}
```

3、提供主页

```
echo "Welcome to 2020 Computer Network Application contest!" >>
/mut/crypt/index.php
```

4、重启服务

```
systemctl restart nginx
```

5、访问测试

```
curl localhost
Welcome to 2020 Computer Network Application contest!
```

13.2.2、web站点配置

1、安装nginx

```
apt install nginx -y
```

2、修改服务运行用户

```
# 添加webuser系统用户
useradd -r webuser

# 修改服务运行用户
vim /etc/nginx/nginx.conf
user webuser;
```

3、生成目录和测试文件

```
mkdir /webdata
echo "This is the front page of CSK's website." > /webdata/index.html
echo "Staff Information" > /webdata/staff.html
```

4、生成证书

```
openssl genrsa -out /csk-rootca/nginx.key

openssl req -new -key /csk-rootca/nginx.key -out /csk-rootca/nginx.csr -subj
"/C=CN/ST=China/L=BeiJing/O=skills/OU=Operations
Departments/CN=*.chinaskills.cn"

openssl ca -in /csk-rootca/nginx.csr -out /csk-rootca/nginx.crt
y
y
```

5、生成basic认证用户数据文件

```
useradd tom
htpasswd -cbm /etc/nginx/.htpasswd tom 123456
```

6、修改站点配置文件

```
rm /etc/nginx/sites-enabled/default
vim /etc/nginx/sites-enabled/default

server{
    listen 80 default_server;
    rewrite / https://www.chinaskills.cn permanent;
}
server {
    listen 443 ssl;
    server_name www.chinaskills.cn;
    ssl_certificate /csk-rootca/nginx.crt;
    ssl_certificate_key /csk-rootca/nginx.key;
    root /webdata;
    location / {
    }
    location ~ ^/staff\.html$ {
        auth_basic "login password";
        auth_basic_user_file /etc/nginx/.htpasswd;
    }
}
```

7、重启服务

```
systemctl restart nginx
```

13.2.3、proxy配置

1、创建配置文件

```
vim /etc/nginx/conf.d/proxy.conf
proxy_cache_path /etc/nginx/proxy_cache levels=1:2:2 keys_zone=proxycache:20m
inactive=120s max_size=1g;
server {
   listen 80;
   server_name www.chinaskills.cn;
   location / {
      proxy_pass https://www.chinaskills.cn;
      proxy_ssl_trusted_certificate /etc/nginx/csk-ca.pem;
      proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
      proxy_cache proxycache;
      proxy_cache_key $request_uri;
      proxy_cache_valid 200 302 301 1h;
      proxy_cache_valid any 1m;
   }
}
```

2、添加hosts解析

```
vim /etc/hosts
81.6.63.254 www.chinaskills.cn
```

3、测试

```
root@ispsrv:/etc/nginx# curl localhost
This is the front page of CSK's website.
```

4、查看缓存

```
root@ispsrv:/etc/nginx# tree proxy_cache/
proxy_cache/
└── 9
    └── 7d
        └── cc
            └── 6666cd76f96956469e7be39d750cc7d9
```

5、日志收集

```
###后端web服务器配置
1、Apache:
[root@c82 ~]# vim /etc/httpd/conf/httpd.conf
LogFormat "%{X-Forwarded-For}i %h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
###重启apache访问web界面并验证apache日志：
172.16.0.1 172.16.0.129 - - [27/Feb/2020:23:54:16 +0800] "GET /index.html HTTP/1.0" 200 18 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36 chrome-extension"

2、Nginx：
[root@c82 ~]# cat /etc/nginx/nginx.conf
log_format  main  '$remote_addr - $remote_user [$time_local] "$request"'
                        '$status $body_bytes_sent "$http_referer"'
                        '"$http_user_agent" "$http_x_forwarded_for" "$server_name"';
access_log /var/log/nginx/access.log main;
```

6、脚本

```
nginx的upstream自带健康检测功能

#!/bin/bash
...
```

13.3、php

php模块方式和php-fpm方式二选一

13.3.1、php模块方式（apache)

1、安装php模块

```
apt install libapache2-mod-php7.3  php-mysqli -y
```

2、重启apache服务

```
systemctl restart apache2
```

13.3.2、php-fpm方式（nginx）

1、安装php-fpm服务

```
apt install php-fpm php-mysql -y
```

2、重启php-fpm服务

```
systemctl restart php-fpm
```

13.4、mariadb

1、安装软件包

```
apt install mariadb-server -y
```

2、修改50-server.cnf配置文件

```
vim /etc/mysql/mariadb.conf.d/50-server.cnf
[mysqld]
...
skip_name_resolve   = ON
bind-address        = 0.0.0.0
#bind-address        = 192.168.100.200
```

3、重启服务

```
systemctl restart mariadb
```

4、修改密码

```
# mysqladmin修改密码
mysqladmin -uroot password 'Chinaskill21!'

# SET PASSWORD命令修改密码
MariaDB [mysql]> SET PASSWORD for root@localhost = password('Chinaskill21!');
```

13.4.1、mariadb备份

使用mysqldump备份数据库

```
mysqldump -uroot -p' ' -hlocalhost --all-databases > all-datebases-$(date +%Y%m%d%H%M%S)
```

脚本

```
vim /shells/mysqlbk.sh
#!/bin/sh
while true；do
  mysqldump -uroot -p' ' -hlocalhost --all-databases > /root/mysqlbackup/all-datebases-$(date +%Y%m%d%H%M%S)
  sleep 1800
done

chmod +x /shells/mysqlbk.sh
nohup /shells/mysqlbk.sh &
```

13.5、wordpress

1、安装软件包

```
apt install wordpress -y
```

2、拷贝文件到站点根目录

```
cp -r /usr/share/wordpress/* /webdata/wordpress/
```

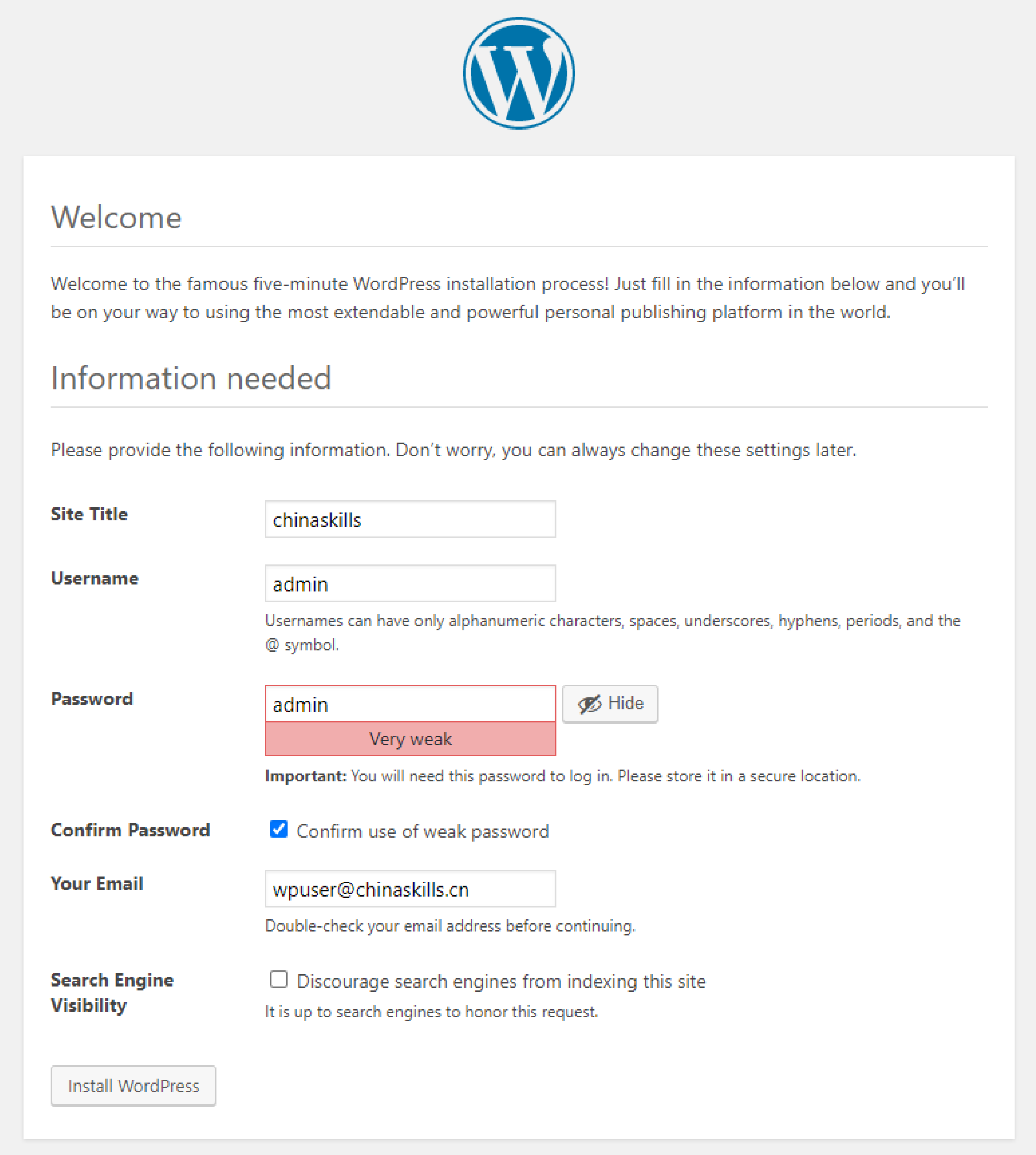
3、在mysql服务器上授权wpuser@192.168.100.100用户拥有所有权限管理wordpress数据库

```
mysql
MariaDB [(none)]> create database wordpress;
MariaDB [(none)]> grant all on wordpress.* to 'wpuser'@'192.168.100.100' identified by 'wppass';
```

4、编辑wordpress配置文件

```
cd /webdata/wordpress/
cp wp-config-sample.php wp-config.php
vim wp-config.php
...
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'wpuser');

/** MySQL database password */
define('DB_PASSWORD', 'wppass');

/** MySQL hostname */
define('DB_HOST', '192.168.100.200');

...
```

5、浏览器访问安装



Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you’ll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don’t worry, you can always change these settings later.

Site Title: chinaskills

Username: admin

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password: admin

Very weak

Important: You will need this password to log in. Please store it in a secure location.

Confirm Password: ☑ Confirm use of weak password

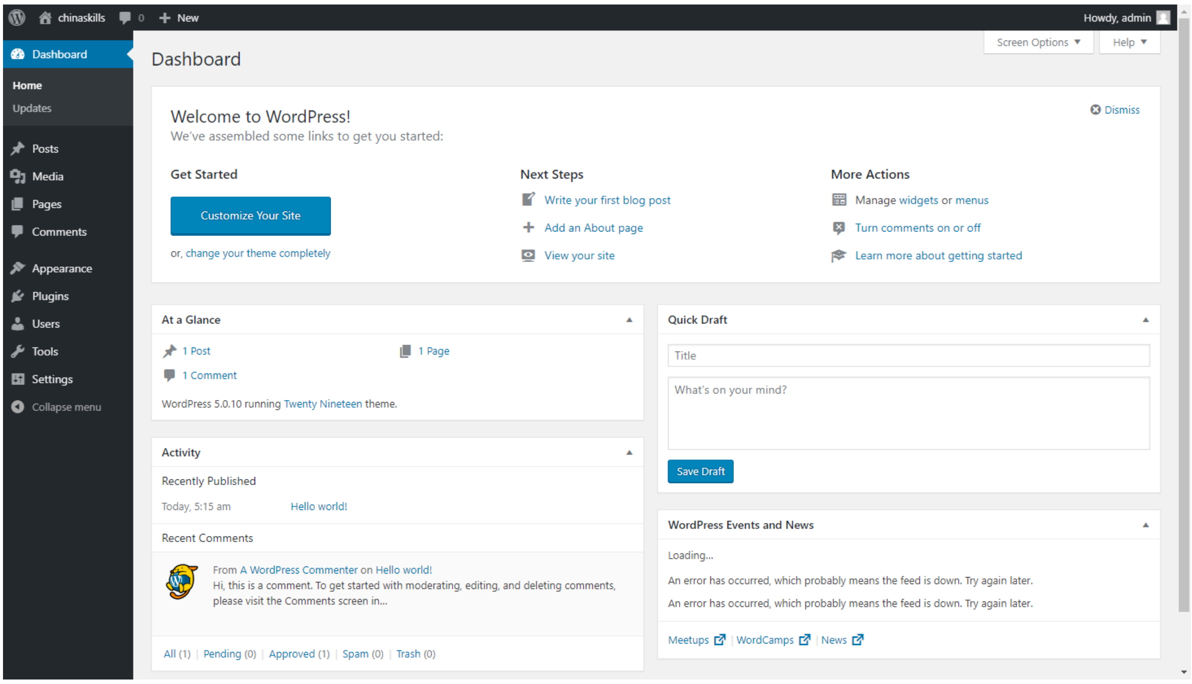
Your Email: wpuser@chinaskills.cn

Double-check your email address before continuing.

Search Engine Visibility: □ Discourage search engines from indexing this site

It is up to search engines to honor this request.

6、登录admin账号



Dashboard

Welcome to WordPress!

We’ve assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

- Write your first blog post
- Add an About page
- View your site

More Actions

- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started

At a Glance

1 Post　1 Page

1 Comment

WordPress 5.0.10 running Twenty Nineteen theme.

Activity

Recently Published

Today, 5:15 am　Hello world!

Recent Comments

From A WordPress Commenter on Hello world!

Hi, this is a comment. To get started with moderating, editing, and deleting comments, please visit the Comments screen in…

All (1) | Pending (0) | Approved (1) | Spam (0) | Trash (0)

Quick Draft

Title

What’s on your mind?

WordPress Events and News

Loading…

An error has occurred, which probably means the feed is down. Try again later.

An error has occurred, which probably means the feed is down. Try again later.

Meetups | WordCamps | News

13.6、phpmyadmin

1、解压软件包

```
tar xf phpMyAdmin-5.0.4-all-languages.tar.gz -C /webdata/phpmyadmin
```

2、创建符号链接

```
cd /webdata/phpmyadmin
ln -sv phpMyAdmin-5.0.4-all-languages/ phpmyadmin
```

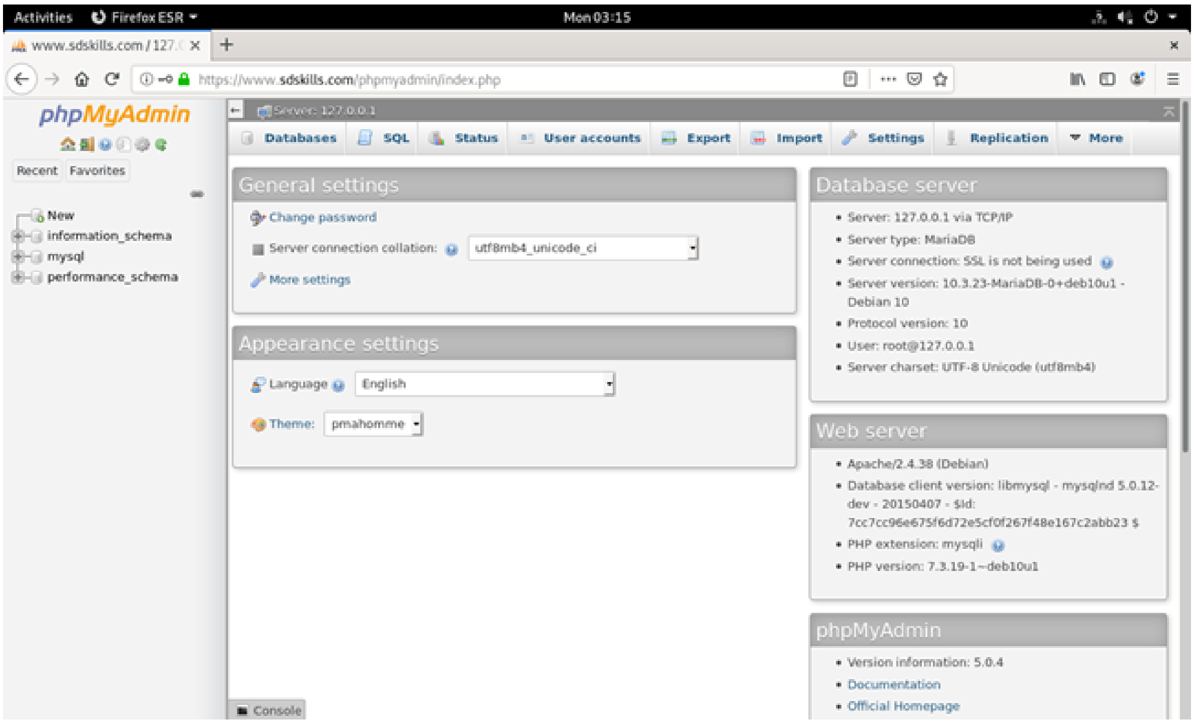
3、创建配置文件

```
 cd /webdata/phpmyadmin
 cp config.sample.inc.php config.inc.php
 vim config.inc.php
 $cfg['blowfish_secret'] = 'asdfasdfawercxz23@!';  //随机字符
 $cfg['Servers'][$i]['host'] = '192.168.100.200';        //服务器IP地址
```

4、登录mariadb，授权

```
mysql
MariaDB [mysql]> grant all on *.* to 'root'@'192.168.100.100' identified by
'Chinaskill20!' WITH GRANT OPTION;
MariaDB [(none)]> quit
```

5、登录phpmyadmin



https://www.sdskills.com/phpmyadmin/index.php

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci
- More settings

Appearance settings

- Language: English
- Theme: pmahomme

Database server

- Server: 127.0.0.1 via TCP/IP
- Server type: MariaDB
- Server connection: SSL is not being used
- Server version: 10.3.23-MariaDB-0+deb10u1 - Debian 10
- Protocol version: 10
- User: root@127.0.0.1
- Server charset: UTF-8 Unicode (utf8mb4)

Web server

- Apache/2.4.38 (Debian)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: 7cc7cc96e675f6d72e5cf0f267f48e167c2abb23 $
- PHP extension: mysqli
- PHP version: 7.3.19-1~deb10u1

phpMyAdmin

- Version information: 5.0.4
- Documentation
- Official Homepage

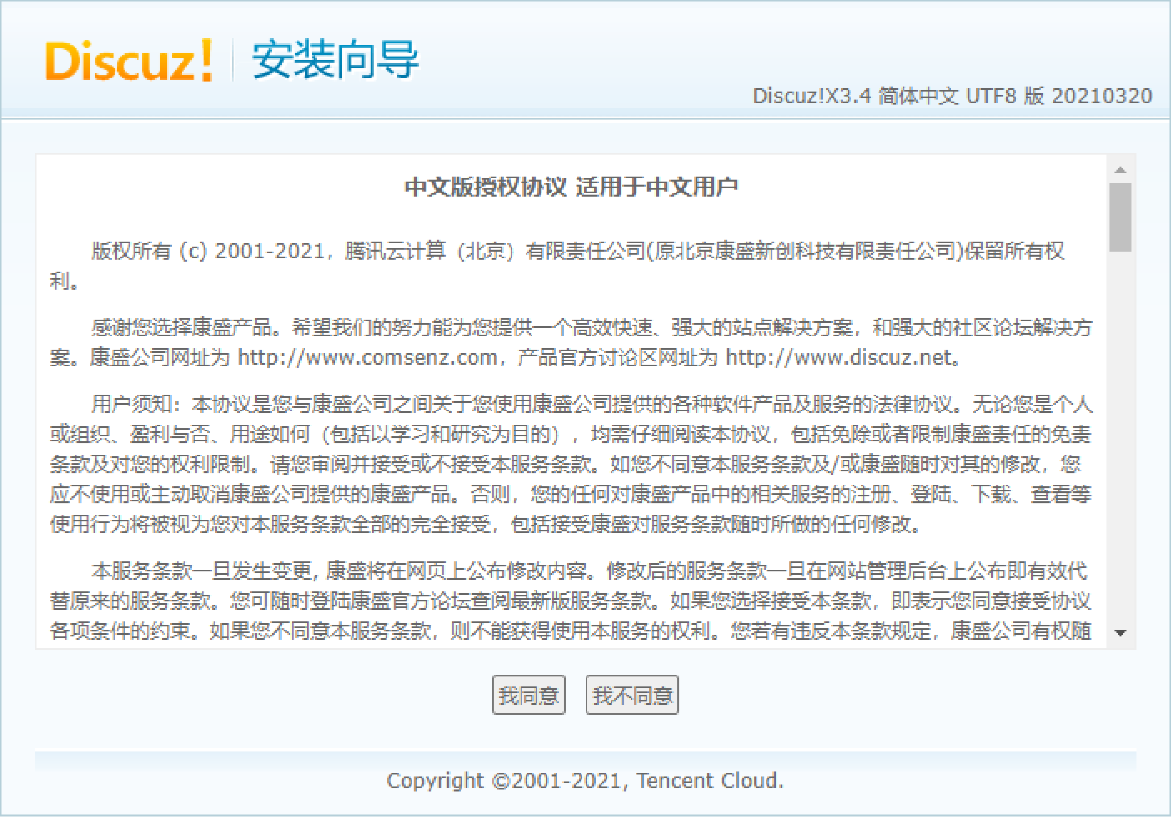
13.7、Discuz

1、下载discuz软件包，解压，将upload文件夹到站点根目录，并重命名为discuz

下载站点：https://www.discuz.net/forum-10-1.html

```
mv upload discuz
```

2、使用浏览器访问站点，按照向导完成安装



Discuz!X3.4 简体中文 UTF8 版 20210320

中文版授权协议 适用于中文用户

版权所有 (c) 2001-2021，腾讯云计算（北京）有限责任公司(原北京康盛新创科技有限责任公司)保留所有权利。

感谢您选择康盛产品。希望我们的努力能为您提供一个高效快速、强大的站点解决方案，和强大的社区论坛解决方案。康盛公司网址为 http://www.comsenz.com，产品官方讨论区网址为 http://www.discuz.net。

用户须知：本协议是您与康盛公司之间关于您使用康盛公司提供的各种软件产品及服务的法律协议。无论您是个人或组织、盈利与否、用途如何（包括以学习和研究为目的），均需仔细阅读本协议，包括免除或者限制康盛责任的免责条款及对您的权利限制。请您审阅并接受或不接受本服务条款。如您不同意本服务条款及/或康盛随时对其的修改，您应不使用或主动取消康盛公司提供的康盛产品。否则，您的任何对康盛产品中的相关服务的注册、登陆、下载、查看等使用行为将被视为您对本服务条款全部的完全接受，包括接受康盛对服务条款随时所做的任何修改。

本服务条款一旦发生变更，康盛将在网页上公布修改内容。修改后的服务条款一旦在网站管理后台上公布即有效代替原来的服务条款。您可随时登陆康盛官方论坛查阅最新版服务条款。如果您选择接受本条款，即表示您同意接受协议各项条件的约束。如果您不同意本服务条款，则不能获得使用本服务的权利。您若有违反本条款规定，康盛公司有权随

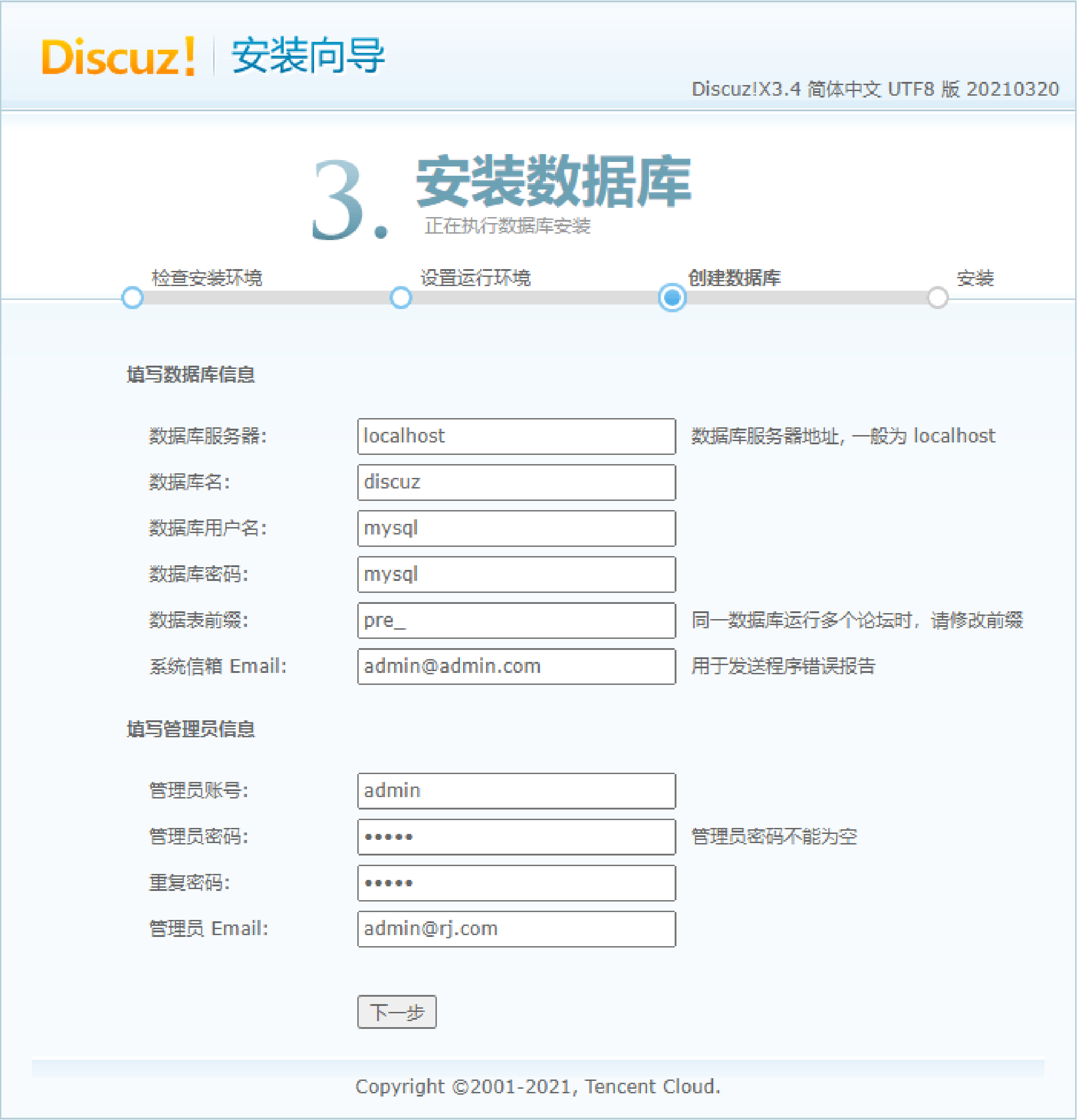
Copyright ©2001-2021, Tencent Cloud.

3、安装依赖，修改目录权限

```
apt install php-mysqli php-xml              # 需要重启服务
chown www-data.www-data discuz/ -R          # php-fpm方式，模块方式授权调用模块的进程的用户
```

4、在mysql上授权discuz访问

```
mysql
MariaDB [(none)]> create database discuz;
MariaDB [(none)]> grant all on discuz.* to 'mysql'@'localhost' identified by 'mysql';
```



Discuz! 安装向导

Discuz!X3.4 简体中文 UTF8 版 20210320

3. 安装数据库

正在执行数据库安装

检查安装环境　设置运行环境　创建数据库　安装

填写数据库信息

数据库服务器: localhost　数据库服务器地址, 一般为 localhost

数据库名: discuz

数据库用户名: mysql

数据库密码: mysql

数据表前缀: pre_　同一数据库运行多个论坛时，请修改前缀

系统信箱 Email: admin@admin.com　用于发送程序错误报告

填写管理员信息

管理员账号: admin

管理员密码: •••••　管理员密码不能为空

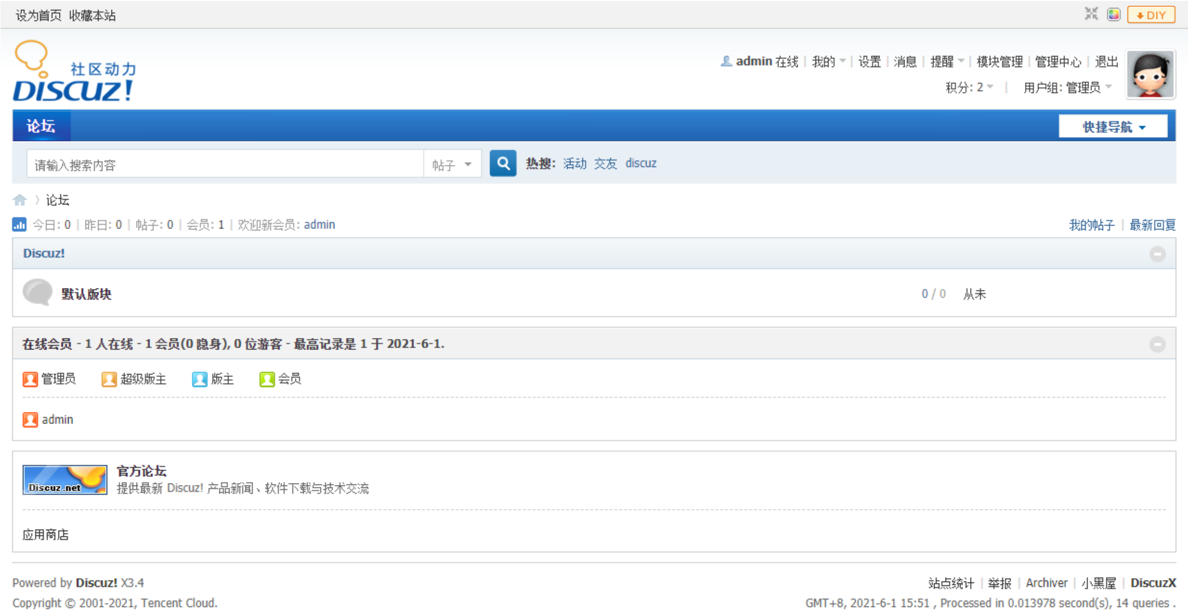
重复密码: •••••

管理员 Email: admin@rj.com

下一步

Copyright ©2001-2021, Tencent Cloud.

5、安装完成，登录admin账号



今日: 0 | 昨日: 0 | 帖子: 0 | 会员: 1 | 欢迎新会员: admin

Discuz!

默认版块　0 / 0　从未

在线会员 - 1 人在线 - 1 会员(0 隐身), 0 位游客 - 最高记录是 1 于 2021-6-1.

管理员　超级版主　版主　会员

admin

官方论坛

提供最新 Discuz! 产品新闻、软件下载与技术交流

Powered by Discuz! X3.4

Copyright © 2001-2021, Tencent Cloud.

GMT+8, 2021-6-1 15:51 , Processed in 0.013978 second(s), 14 queries .

14、ftp服务

14.1、vsftpd

1、安装软件包

```
apt install vsftpd db5.3-util lftp -y
```

2、创建ftpuser用户

```
useradd -r -d /webdata ftpuser
```

3、生成vuser.db数据库文件

```
vim vuser.txt
webadmin
Chinaskill20!

db5.3_load -T -t hash -f vuser.txt /etc/vuser.db
```

4、生成vsftpd.vu pam文件

```
vim /etc/pam.d/vsftpd.vu
auth    required    pam_userdb.so db=/etc/vuser
account required    pam_userdb.so db=/etc/vuser
```

5、编辑vsftpd.conf配置文件

```
vim /etc/vsftpd.conf
#pam_service_name=vsftpd
pam_service_name=vsftpd.vu
ssl_enable=YES
rsa_private_key_file=/csk-rootca/vsftpd.key
rsa_cert_file=/csk-rootca/vsftpd.crt
guest_enable=YES
guest_username=ftpuser
allow_writeable_chroot=YES
local_root=/webdata
anon_umask=022
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES
anon_other_write_enable=YES
deny_file={*.doc,*.docx,*.xlsx}
max_per_ip=2
local_max_rate=100000

# 注释
# ssl_enable=YES      #启用ssl功能
# deny_file={*.doc,*.docx,*.xlsx}   #拒绝指定文件
# max_clients=0       #最大并发连接数
# max_per_ip=0        #每个IP同时发起的最大连接数
# anon_max_rate=0     #匿名用户的最大传输速率
# local_max_rate=0    #本地用户的最大传输速率
```

6、生成证书

```
openssl genrsa -out /csk-rootca/vsftpd.key

openssl req -new -key /csk-rootca/vsftpd.key -out /csk-rootca/vsftpd.csr -subj
"/C=CN/ST=China/L=BeiJing/O=skills/OU=Operations
Departments/CN=ftp.chinaskills.cn"

# CA上签署
openssl ca -in /csk-rootca/vsftpd.csr -out /csk-rootca/vsftpd.crt
y
y
```

7、重启服务

```
systemctl restart vsftpd
```

8、导入证书

```
cp csk-ca.pem /usr/share/ca-certificates/

vim /etc/ca-certificates.conf
csk-ca.pem

update-ca-certificates
```

9、测试

```
root@storagesrv:~# touch 1.doc 1.docx 1.xlsx 1.txt
root@storagesrv:~# lftp -u webadmin,Chinaskill20! ftp.chinaskills.cn
lftp webadmin@ftp.chinaskills.cn:~> ls
-rw-r--r--    1 998      998             0 May 31 16:59 disk.txt
drwxr-xr-x    2 998      998          4096 May 31 17:13 download
drwx------    2 998      998         16384 May 31 16:55 lost+found
drwxr-xr-x    8 998      998          4096 May 31  2021 roundcube
drwxr-xr-x    5 998      998          4096 May 31 17:59 wordpress
lftp webadmin@ftp.chinaskills.cn:/> put 1.doc
put: Access failed: 550 Permission denied. (1.doc)
lftp webadmin@ftp.chinaskills.cn:/> put 1.docx
put: Access failed: 550 Permission denied. (1.docx)
lftp webadmin@ftp.chinaskills.cn:/> put 1.xlsx
put: Access failed: 550 Permission denied. (1.xlsx)
lftp webadmin@ftp.chinaskills.cn:/> put 1.txt
lftp webadmin@ftp.chinaskills.cn:/> ls
-rw-r--r--    1 998      998             0 May 31 21:01 1.txt
-rw-r--r--    1 998      998             0 May 31 16:59 disk.txt
drwxr-xr-x    2 998      998          4096 May 31 17:13 download
drwx------    2 998      998         16384 May 31 16:55 lost+found
drwxr-xr-x    8 998      998          4096 May 31  2021 roundcube
drwxr-xr-x    5 998      998          4096 May 31 17:59 wordpress
lftp webadmin@ftp.chinaskills.cn:/> get disk.txt
lftp webadmin@ftp.chinaskills.cn:/> !ls
1.doc  1.docx  1.txt  1.xlsx  disk.txt  vuser.txt
```

14.2、proftpd

1、安装proftpd软件包

```
apt install proftpd -y
```

2、编辑proftpd.conf配置文件，类似apache的配置文件格式

```
Umask                           066  066

DefaultRoot                     /public
<Directory /public>
  <Limit DELE>
    DenyAll
  </Limit>
  <Limit STOR RETR>
    AllowAll
  </Limit>
</Directory>

<Anonymous /public>
   User                         ftp
   Group                        nogroup
   UserAlias                    anonymous ftp
   RequireValidShell            off
    <Directory upload>
       <Limit READ WRITE>
           DenyAll
       </Limit>
       <Limit STOR>
           AllowAll
       </Limit>
    </Directory>
</Anonymous>



#<LIMIT>容器内有以下权限:
# CWD:改变所在目录
# MKD/XMKD:新建目录
# RNFR/RNTO:重命名目录的(一起使用)
# DELE:删除文件
# RMD/XRMD:删除目录
# RETR:下载
# STOR:上传
# LOGIN:登陆
# READ:包括了RETR,SITE,SIZE,STAT
# WRITE:包括了APPE， DELE， MKD， RMD， RNTO， STOR， XMKD， XRMD
# DIRS:包括了DUP， CWD， LIST， MDTM， NLST， PWD， RNFR， XCUP， XCWD， XPWD
# ALL:包括了READ WRITE DIRS
#以上权限结合动作一起使用:
# AllowUser:允许某个用户
# DenyUser:禁止某个用户
# AllowGroup:允许某个用户组
# DenyGroup:禁止某个用户组
# AllowAll:允许所有用户
# DenyAll:禁止所有用户
```

3、权限设置

```
chmod 777 /public /public/upload
```

4、重启服务

```
systemctl restart proftpd
```

5、匿名用户测试

```
echo "test file" > 1.txt

root@ispsrv:~# ftp localhost
Connected to localhost.
220 ProFTPD Server (Debian) [::1]
Name (localhost:root): ftp
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 EPRT command successful
150 Opening ASCII mode data connection for file list
drwxrwxrwx   2 root     root         4096 Jun  1 07:23 upload
226 Transfer complete
ftp> cd upload
250 CWD command successful
ftp> put 1.txt
local: 1.txt remote: 1.txt
200 EPRT command successful
150 Opening BINARY mode data connection for 1.txt
226 Transfer complete
10 bytes sent in 0.00 secs (187.8005 kB/s)
ftp> ls
200 EPRT command successful
150 Opening ASCII mode data connection for file list
-rw-------   1 ftp      nogroup        10 Jun  1 07:23 1.txt
226 Transfer complete
ftp> get 1.txt
local: 1.txt remote: 1.txt
200 EPRT command successful
550 1.txt: Operation not permitted
```

6、普通用户登录测试

```
root@ispsrv:~# ftp localhost
Connected to localhost.
220 ProFTPD Server (Debian) [::1]
Name (localhost:root): ftpuser
331 Password required for ftpuser
Password:
230 User ftpuser logged in
Remote system type is UNIX.
Using binary mode to transfer files.
```

```
ftp> ls
200 EPRT command successful
150 Opening ASCII mode data connection for file list
drwxrwxrwx    2 root     root         4096 Jun  1 07:23 upload
226 Transfer complete
ftp> put 1.txt
local: 1.txt remote: 1.txt
200 EPRT command successful
150 Opening BINARY mode data connection for 1.txt
226 Transfer complete
10 bytes sent in 0.00 secs (305.1758 kB/s)
ftp> get 1.txt
local: 1.txt remote: 1.txt
200 EPRT command successful
150 Opening BINARY mode data connection for 1.txt (10 bytes)
226 Transfer complete
10 bytes received in 0.00 secs (63.0040 kB/s)
ftp> del 1.txt
550 1.txt: Operation not permitted
ftp> ls
200 EPRT command successful
150 Opening ASCII mode data connection for file list
-rw-------    1 ftpuser  ftpuser        10 Jun  1 07:25 1.txt
drwxrwxrwx    2 root     root         4096 Jun  1 07:23 upload
226 Transfer complete
```

15、mail

15.1、posfix+dovecot

1、安装软件包

```
apt install postfix dovecot-imapd mailutils -y
```

2、修改配置文件

```
vim /etc/postfix/main.cf
...
smtpd_tls_cert_file=/csk-rootca/smtp.crt
smtpd_tls_key_file=/csk-rootca/smtp.key
mydestination = $myhostname, chinaskills.cn, localhost, localhost.localdomain, localhost
mynetworks = 127.0.0.0/8 192.168.0.0/24 192.168.10.0/24 [::ffff:127.0.0.0]/104 [::1]/128
...
```

3、修改mainame

```
vim /etc/mailname
chinaskills.cn
```

4、修改master.cf配置文件

```
vim /etc/postfix/master.cf
smtps     inet  n       -       y       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
```

5、提供证书

```
openssl genrsa -out /csk-rootca/smtp.key

openssl req -new -key /csk-rootca/smtp.key -out /csk-rootca/smtp.csr -subj
"/C=CN/ST=China/L=BeiJing/O=skills/OU=Operations
Departments/CN=smtp.chinaskills.cn"

openssl ca -in /csk-rootca/smtp.csr -out /csk-rootca/smtp.crt
```

6、编辑dovecot.conf配置文件

```
vim /etc/dovecot/conf.d/10-ssl.conf
ssl=required
ssl_cert = </csk-rootca/imap.crt
ssl_key = </csk-rootca/imap.key
```

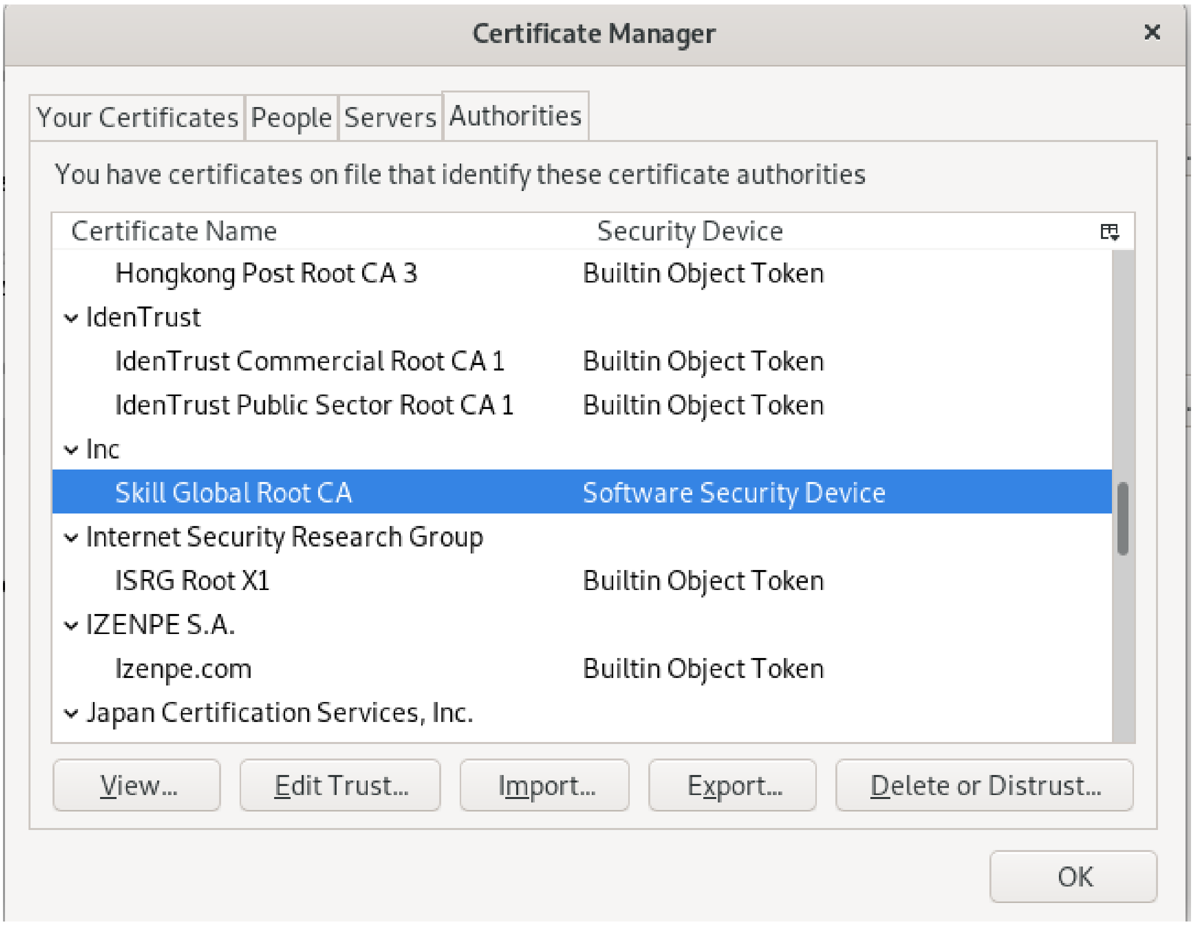
7、生成imap证书

```
openssl genrsa -out /csk-rootca/imap.key

openssl req -new -key /csk-rootca/imap.key -out /csk-rootca/imap.csr -subj
"/C=CN/ST=China/L=BeiJing/O=skills/OU=Operations
Departments/CN=imap.chinaskills.cn"

openssl ca -in /csk-rootca/imap.csr -out /csk-rootca/imap.crt
```

8、重启服务

```
systemctl restart postfix dovecot
```

9、导入证书

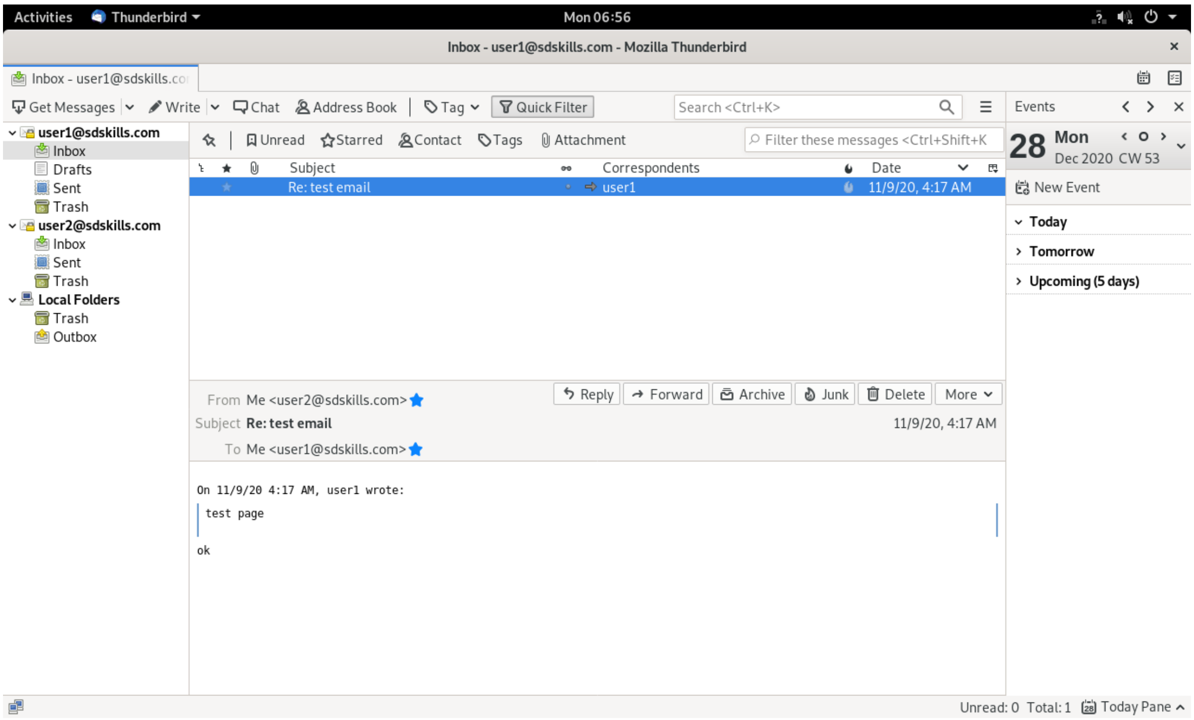


Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
Hongkong Post Root CA 3	Builtin Object Token
IdenTrust	
IdenTrust Commercial Root CA 1	Builtin Object Token
IdenTrust Public Sector Root CA 1	Builtin Object Token
Inc	
Skill Global Root CA	Software Security Device
Internet Security Research Group	
ISRG Root X1	Builtin Object Token
IZENPE S.A.	
Izenpe.com	Builtin Object Token
Japan Certification Services, Inc.	

10、登录测试



Subject	Correspondents	Date
Re: test email	user1	11/9/20, 4:17 AM

From Me <user2@sdskills.com>
Subject **Re: test email** 11/9/20, 4:17 AM
To Me <user1@sdskills.com>

```
On 11/9/20 4:17 AM, user1 wrote:
test page

ok
```

15.2、roundcube

1、安装roundcube软件包

```
root@appsrv:~# apt install roundcube -y
```

2、拷贝文件，创建目录

```
cp -r /var/lib/roundcube/* /webdata/roundcube/
cp -r /usr/share/roundcube/SQL /webdata/roundcube/
cp -r /usr/share/roundcube/installer /webdata/roundcube/
rm /webdata/roundcube/logs
mkdir /webdata/roundcube/{temp,logs}
```

3、修改时区

```
vim /etc/php/7.3/apache2/php.ini
date.timezone = Asia/Shanghai
```

4、安装IDNA

```
apt install php-net-idna2 -y
```

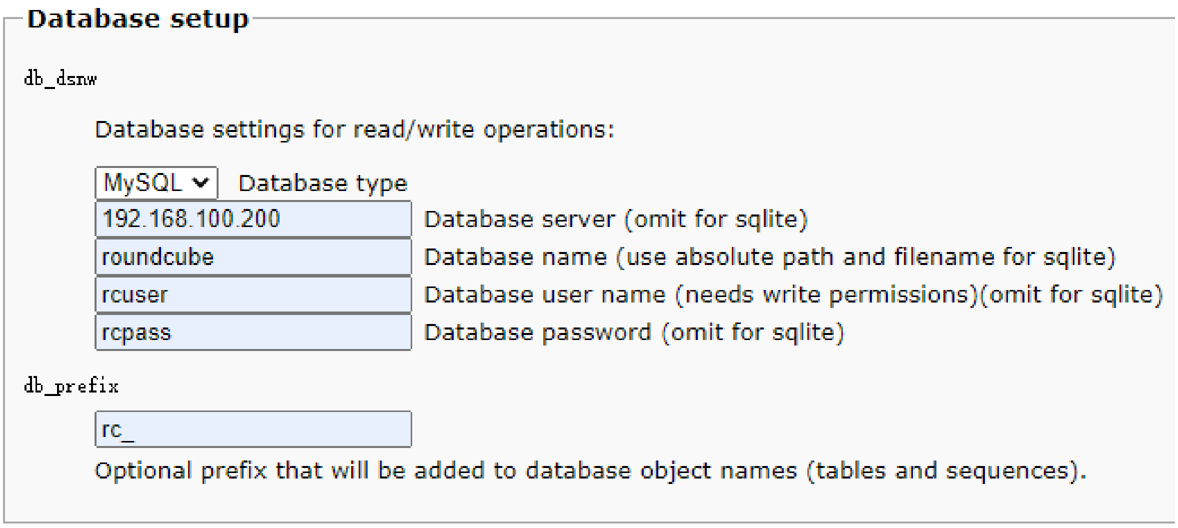
5、添加apache邮件站点配置，重启apache服务

```
vim /etc/apache2/sites-enabled/000-default.conf
...
<VirtualHost *:443>
  ServerName mail.chinaskills.cn
  DocumentRoot "/webdata/roundcube"
  SSLEngine ON
  SSLCertificateFile "/csk-rootca/apache.crt"
  SSLCertificateKeyFile "/csk-rootca/apache.key"
  <Directory "/webdata/roundcube">
    Require all granted
  </Directory>
</VirtualHost>
...

systemctl restart apache2
```

6、在mysql服务器上授权rcuser@192.168.100.100用户拥有所有权限管理wordpress数据库

```
mysql
MariaDB [(none)]> create database roundcube;
MariaDB [(none)]> grant all on roundcube.* to 'rcuser'@'192.168.100.100'
identified by 'rcpass';
```

7、浏览器访问安装http://mail.chinaskills.cn/installer



Database setup

db_dsnw

Database settings for read/write operations:

MySQL Database type

192.168.100.200 Database server (omit for sqlite)

roundcube Database name (use absolute path and filename for sqlite)

rcuser Database user name (needs write permissions)(omit for sqlite)

rcpass Database password (omit for sqlite)

db_prefix

rc_

Optional prefix that will be added to database object names (tables and sequences).

8、生成配置文件

从生成的模板复制粘贴到文件就行

```
vim /webdata/roundcube/config/config.inc.php
<?php

/* Local configuration for Roundcube Webmail */

// ----------------------------------
// SQL DATABASE
// ----------------------------------
// Database connection string (DSN) for read+write operations
// Format (compatible with PEAR MDB2): db_provider://user:password@host/database
// Currently supported db_providers: mysql, pgsql, sqlite, mssql, sqlsrv, oracle
// For examples see http://pear.php.net/manual/en/package.database.mdb2.intro-
dsn.php
// NOTE: for SQLite use absolute path (Linux):
'sqlite:////full/path/to/sqlite.db?mode=0646'
//       or (Windows): 'sqlite:///C:/full/path/to/sqlite.db'
$config['db_dsnw'] = 'mysql://rcuser:rcpass@192.168.100.200/roundcube';

// you can define specific table (and sequence) names prefix
$config['db_prefix'] = 'rc_';

// ----------------------------------
// IMAP
// ----------------------------------
// The IMAP host chosen to perform the log-in.
// Leave blank to show a textbox at login, give a list of hosts
// to display a pulldown menu or set one host as string.
// To use SSL/TLS connection, enter hostname with prefix ssl:// or tls://
// Supported replacement variables:
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %s - domain name after the '@' from e-mail address provided at login screen
// For example %n = mail.domain.tld, %t = domain.tld
// WARNING: After hostname change update of mail_host column in users table is
//          required to match old user data records with the new host.
$config['default_host'] = 'localhost';
```

```
// provide an URL where a user can get support for this Roundcube installation
// PLEASE DO NOT LINK TO THE ROUNDCUBE.NET WEBSITE HERE!
$config['support_url'] = '';

// This key is used for encrypting purposes, like storing of imap password
// in the session. For historical reasons it's called DES_key, but it's used
// with any configured cipher_method (see below).
$config['des_key'] = 'vwQkZzOPDbUV190FEZNiYboI';

// ----------------------------------
// PLUGINS
// ----------------------------------
// List of active plugins (in plugins/ directory)
$config['plugins'] = array();
```

9、修改文件属主属组

```
chown webuser.webuser /webdata/roundcube/ -R
```

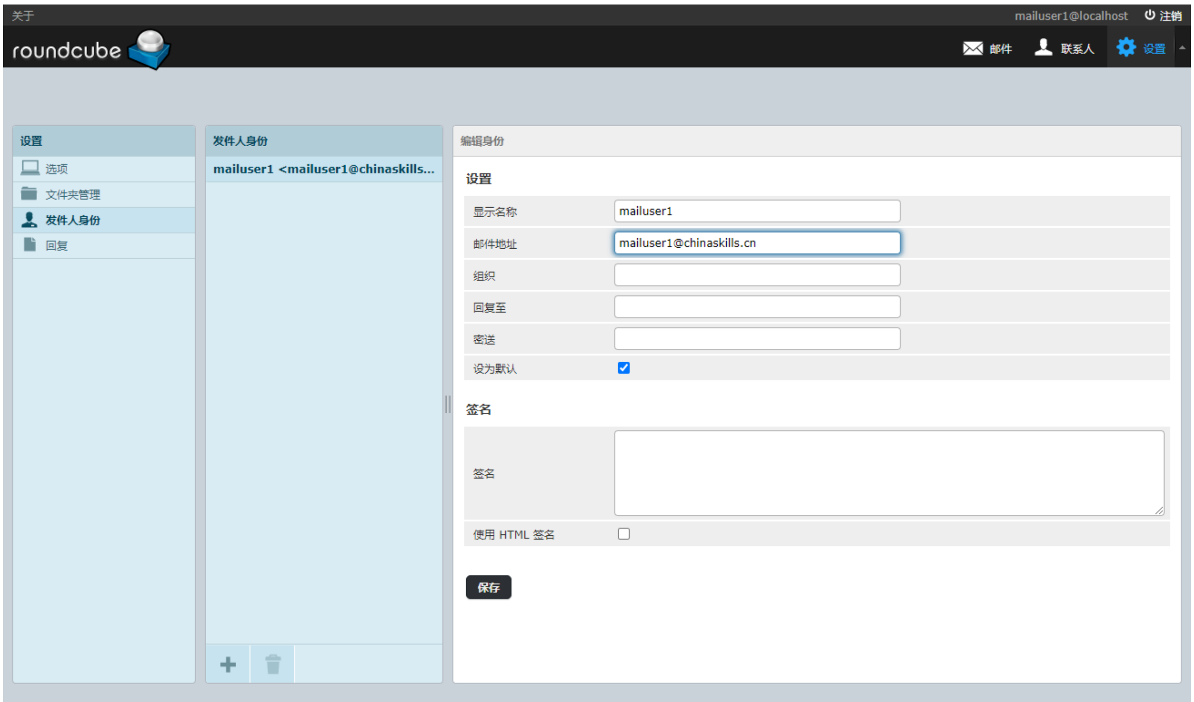
10、初始化数据库

Initialize database

11、创建用户

```
useradd -m mailuser1
useradd -m mailuser2
echo "mailuser1:chinaskills" | chpasswd
echo "mailuser2:chinaskills" | chpasswd
```

12、登录，修改邮箱后缀



mailuser1 <mailuser1@chinaskills...

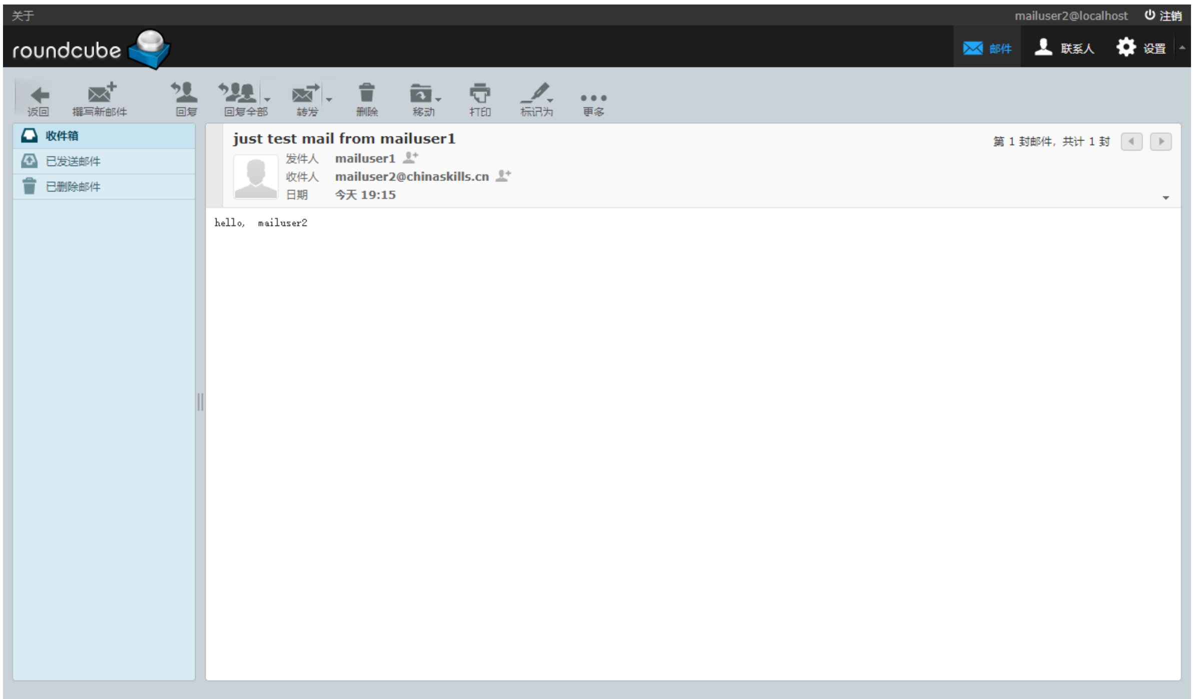
设置

显示名称	mailuser1
邮件地址	mailuser1@chinaskills.cn
组织	
回复至	
密送	
设为默认	☑

签名

签名	
使用 HTML 签名	☐

13、发送测试邮件



just test mail from mailuser1

第 1 封邮件，共计 1 封

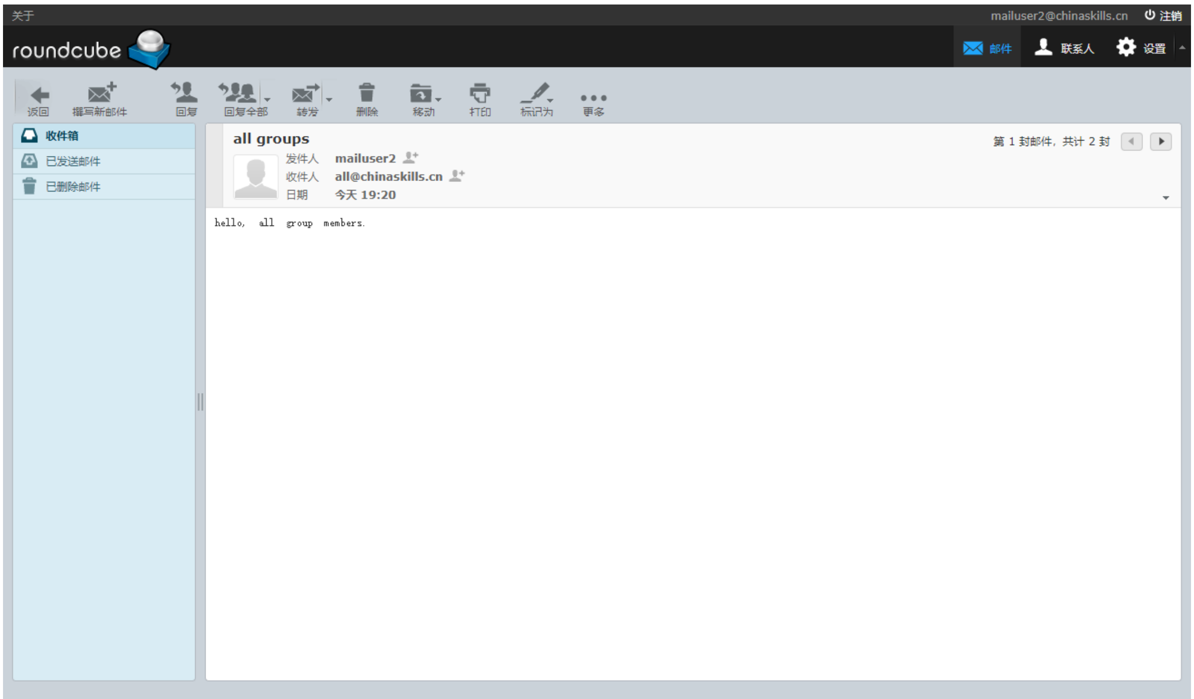
发件人 mailuser1
收件人 mailuser2@chinaskills.cn
日期 今天 19:15

hello, mailuser2

14、邮件组设置

```
vim /etc/aliases
# See man 5 aliases for format
postmaster:     root
all:    mailuser1,mailuser2

# 重新查询别名数据文件
postalias /etc/aliases
```

15、邮件组测试



all groups

第 1 封邮件，共计 2 封

发件人 mailuser2
收件人 all@chinaskills.cn
日期 今天 19:20

hello, all group members.

16、AIDE

1、安装aide软件包

```
apt install aide -y
```

2、编辑配置文件

```
vim /etc/aide/aide.conf
Change = p+i+n+u+g+s+m+c+md5+sha256
/webdata = Change
```

3、初始化数据库

```
aide -c /etc/aide/aide.conf --init
```

4、修改文件，测试

```
aide -c /etc/aide/aide.conf --check
```

17、samba

17.1、samba服务

1、安装软件包

```
apt install samba samba-client cifs-utils -y
```

2、编辑smb.conf配置文件

```
vim /etc/samba/smb.conf
[csk-share]
path = /var/skills
write list = user01


每个共享目录应该有独立的[ ]部分
- [共享名称] 远程网络看到的共享名称
- comment 注释信息
- path 所共享的目录路径
- public 能否被guest访问的共享，默认no，和guest ok 类似
- browsable 是否允许所有用户浏览此共享,默认为yes,no为隐藏
- writable=yes 可以被所有用户读写，默认为no
- read only=no 和writable=yes等价，如与以上设置冲突，放在后面的设置生效，默认只读
- write list 三种形式：用户，@组名，+组名,用，分隔
  - 如writable=no，列表中用户或组可读写，不在列表中用户只读
- valid users 特定用户才能访问该共享，如为空，将允许所有用户，用户名之间用空格分隔
```

3、创建用户

```
useradd -m user01
useradd -m user02
smbpasswd -a user01
smbpasswd -a user02
```

4、创建目录和文件

```
mkdir /var/skills
chmod 777 /var/skills
```

5、重启服务

```
systemctl restart smbd nmbd
```

6、测试

```
root@storagesrv:~# smbclient //192.168.100.200/csk-share -U user01
Enter WORKGROUP\user01's password:
Try "help" to get a list of possible commands.
smb: \> put 1.doc
putting file 1.txt as \1.doc (1.9 kb/s) (average 1.9 kb/s)
smb: \> ls
  .                                   D        0  Mon May 31 22:18:22 2021
  ..                                  D        0  Mon May 31 22:10:05 2021
  1.doc                               A       19  Mon May 31 22:18:22 2021

        7924168 blocks of size 1024. 7163328 blocks available
smb: \> put 1.txt
putting file 1.txt as \1.txt (18.6 kb/s) (average 3.4 kb/s)
smb: \> del 1.doc
smb: \> get 1.txt
getting file \1.txt of size 19 as 1.txt (9.3 KiloBytes/sec) (average 9.3
KiloBytes/sec)
smb: \> quit


root@storagesrv:~# smbclient //192.168.100.200/csk-share -U user02
Enter WORKGROUP\user02's password:
Try "help" to get a list of possible commands.
smb: \> more 1.txt
getting file \1.txt of size 19 as /tmp/smbmore.NDTWWj (6.2 KiloBytes/sec)
(average 6.2 KiloBytes/sec)
smb: \> get 1.txt
getting file \1.txt of size 19 as 1.txt (9.3 KiloBytes/sec) (average 7.4
KiloBytes/sec)
smb: \> del 1.txt
NT_STATUS_ACCESS_DENIED deleting remote file \1.txt
smb: \> quit
```

17.2、ldap认证

1、在ldap中注册samba服务

```
cp /usr/share/doc/samba/examples/LDAP/samba.ldif.gz /etc/ldap/schema
cp /usr/share/doc/samba/examples/LDAP/samba.schema.gz /etc/ldap/schema
cd /etc/ldap/schema
gzip -d samba.ldif.gz
gzip -d samba.schema.gz
ldapadd -Q -Y EXTERNAL -H ldapi:/// -f samba.ldif
```

2、修改samba配置文件

```
[global]
...
passdb backend = ldapsam:ldap://192.168.100.200/
ldap suffix = dc=chinaskills,dc=cn
ldap admin dn = cn=admin,dc=chinaskills,dc=cn
ldap user suffix = ou=users
ldap group suffix = ou=groups
ldap delete dn = no
ldap passwd sync = yes
ldap ssl = no

smbpasswd -W  #输入LDAP密码
```

3、重启samba服务

```
systemctl restart smbd nmbd
```

4、添加用户

```
vim useradd.ldif
dn: uid=zsuser,ou=users,dc=chinaskills,dc=cn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: zsuser
sn: zsuser
userPassword: {SSHA}ywnzywnzywnzywnzywnz
loginShell: /bin/bash
homeDirectory: /home/zsuser
uidNumber: 3001
gidNumber: 3000

dn: uid=lsusr,ou=users,dc=chinaskills,dc=cn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: lsusr
sn: lsusr
userPassword: {SSHA}ywnzywnzywnzywnzywnz
loginShell: /bin/bash
homeDirectory: /home/lsusr
uidNumber: 3002
gidNumber: 3000

dn: uid=wuusr,ou=users,dc=chinaskills,dc=cn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: wuusr
sn: wuusr
userPassword: {SSHA}ywnzywnzywnzywnzywnz
loginShell: /bin/bash
homeDirectory: /home/wuusr
uidNumber: 3003
gidNumber: 3000
```

```
ldapadd -x -h 192.168.100.200 -D cn=admin,dc=chinaskills,dc=cn -W -f
useradd.ldif

useradd zsuser
useradd lsusr
useradd wuusr
smbpasswd -a zsuser
smbpasswd -a lsusr
smbpasswd -a wuusr

# 查看
ldapsearch -x -h 192.168.100.200
# wuusr, users, chinaskills.cn
dn: uid=wuusr,ou=users,dc=chinaskills,dc=cn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
cn: wuusr
sn: wuusr
loginShell: /bin/bash
homeDirectory: /home/wuusr
uidNumber: 3003
gidNumber: 3000
uid: wuusr
sambaSID: S-1-5-21-1202905782-2648429379-3463704853-1009
sambaNTPassword: 422318F3EA9E8F7318A11577FAFA4CF5
sambaPasswordHistory: 00000000000000000000000000000000000000000000000000000000
 00000000
sambaPwdLastSet: 1622642904
sambaAcctFlags: [U          ]
```

5、添加组成员

```
vim ldapgroup.ldif
dn: cn=ldsgp,ou=groups,dc=chinaskills,dc=cn
cn: ldsgp
objectClass: groupOfUniqueNames
uniqueMember: uid=wuusr,ou=users,dc=chinaskills,dc=cn
uniqueMember: uid=lsusr,ou=users,dc=chinaskills,dc=cn
uniqueMember: uid=zsuser,ou=users,dc=chinaskills,dc=cn

# 添加group
ldapadd -x -h 192.168.100.200 -D cn=admin,dc=chinaskills,dc=cn -W -f
ldapgroup.ldif

# 查看
ldapsearch -x -h 192.168.100.200
# ldsgp, groups, chinaskills.cn
dn: cn=ldsgp,ou=groups,dc=chinaskills,dc=cn
cn: ldsgp
objectClass: groupOfUniqueNames
uniqueMember: uid=wuusr,ou=users,dc=chinaskills,dc=cn
uniqueMember: uid=lsusr,ou=users,dc=chinaskills,dc=cn
uniqueMember: uid=zsuser,ou=users,dc=chinaskills,dc=cn
```

18、ldap

1、安装slapd软件包

```
apt install slapd ldap-utils -y
```

2、修改ldap.conf配置文件

```
BASE    dc=chinaskills,dc=cn
URI ldap://ldap.chinaskills.cn ldap://192.168.100.200:666
```

3、重新配置LDAP

```
dpkg-reconfigure slapd
<No>
chinaskills.cn   <ok>
chinaskills   <ok>
adminpass
adminpass
MDB
<Yes>
<Yes>
```

4、配置监听地址，重启服务

```
vim /etc/default/slapd
SLAPD_SERVICES="ldap://192.168.100.200 ldapi:///"

systemctl restart slapd.service
```

5、查看

```
ldapsearch -x -h 192.168.100.200
# extended LDIF
#
# LDAPv3
# base <dc=chinaskills,dc=cn> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# chinaskills.cn
dn: dc=chinaskills,dc=cn
objectClass: top
objectClass: dcObject
objectClass: organization
o: chinaskills
dc: chinaskills

# admin, chinaskills.cn
dn: cn=admin,dc=chinaskills,dc=cn
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
```

```
description: LDAP administrator
```

命令行方式管理ldap

1、添加OU

```
vim basedn.ldif
dn: ou=groups,dc=chinaskills,dc=cn
objectClass: organizationalUnit
ou: groups
dn: ou=users,dc=chinaskills,dc=cn
objectClass: organizationalUnit
ou: users

# 添加OU
ldapadd -x -h 192.168.100.200 -D cn=admin,dc=chinaskills,dc=cn -W -f basedn.ldif

# 查看
ldapsearch -x -h 192.168.100.200
# users, chinaskills.cn
dn: ou=users,dc=chinaskills,dc=cn
objectClass: organizationalUnit
ou: users

# groups, chinaskills.cn
dn: ou=groups,dc=chinaskills,dc=cn
objectClass: organizationalUnit
ou: groups
```

19、时间服务

19.1、chrony

1、安装服务

```
apt install chrony -y
```

2、修改配置文件

```
vim /etc/chrony/chrony.conf
...
allow 192.168.100.0/24
allow 192.168.0.0/24
allow 81.6.63.0/24
local stratum 10     #即使server指令中时间服务器不可用，也允许将本地时间作为标准时间授时给其它客户端
```

3、重启服务

```
systemctl restart chrony
```

4、修改客户端配置文件

```
vim /etc/chrony/chrony.conf
server 192.168.10.3 iburst
```

5、查看客户端同步状态

```
chronyc clients
```

6、通过crontab使用ntpdate同步时间

```
root@appsrv:~# apt install ntpdate -y
root@appsrv:~# vim /etc/crontab

*/5 * * * * root /usr/sbin/ntpdate 81.6.63.100
```

19.2、ntp

1、安装ntp服务

```
apt install ntp
```

2、编辑ntp.conf配置文件

```
vim /etc/ntp.conf
...
server 127.127.1.0
fudge 127.127.1.0 stratum 8
```

3、客户端通过crontab使用ntpdate同步时间

```
apt install ntpdate -y
vim /etc/crontab

*/5 * * * * root /usr/sbin/ntpdate 81.6.63.254
```

20、openvpn

20.1、服务端配置

1、安装软件包

```
apt install openvpn easy-rsa -y
```

2、拷贝配置文件

```
cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/server/
cp -rf /usr/share/easy-rsa/ /etc/openvpn/
cd /etc/openvpn/easy-rsa/
mv vars.example vars
```

3、生成服务器证书

```
./easyrsa init-pki
./easyrsa build-ca nopass <<EOF

EOF
./easyrsa gen-req server nopass <<EOF

EOF
./easyrsa sign server server <<EOF
yes
EOF
./easyrsa gen-dh
```

4、拷贝证书文件

```
cp pki/dh.pem /etc/openvpn/server/
cp pki/ca.crt /etc/openvpn/server/
cp pki/issued/server.crt /etc/openvpn/server/
cp pki/private/server.key /etc/openvpn/server/
```

5、解压服务端配置文件，修改服务配置文件

```
cd /etc/openvpn/server/
gunzip server.conf.gz
vim server.conf
local 81.6.63.254
port 1194
proto tcp
dev tun
ca ca.crt
cert server.crt
key server.key  # This file should be kept secret
dh dh.pem
server 172.16.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt
push "route 192.168.100.200 255.255.255.255"
push "route 192.168.0.190 255.255.255.255"
keepalive 10 120
cipher AES-256-CBC
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
verb 3
```

6、重启服务

```
systemctl restart openvpn-server@server
```

20.2、客户端配置

1、在服务端生成客户端证书

```
./easyrsa gen-req client nopass<<EOF

EOF
./easyrsa sign client client <<EOF
yes
EOF

cp pki/ca.crt /etc/openvpn/client/
cp pki/issued/client.crt /etc/openvpn/client/
cp pki/private/client.key /etc/openvpn/client/
```

2、编辑客户端配置文件

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
/etc/openvpn/client/csk.conf
vim /etc/openvpn/client/csk.conf
client
dev tun
proto tcp
remote 81.6.63.254 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
remote-cert-tls server
cipher AES-256-CBC
verb 3
```

3、安装openvpn软件包

```
apt install openvpn -y
```

4、从服务端拷贝配置文件

```
scp 81.6.63.254:/etc/openvpn/client/* /etc/openvpn/client/
```

5、重启服务

```
systemctl restart openvpn-client@csk
```

6、在服务端上修改客户端的分配地址

```
vim /var/log/openvpn/ipp.txt
client,172.16.0.100
```

7、重启客户端服务

```
systemctl restart openvpn-client@csk
```

8、查看虚拟网卡

```
11: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 172.16.0.102 peer 172.16.0.101/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::57b:bb5f:3d19:3fd8/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```