•注意事项：

1、无论题目是否有要求，都要安装一些常用测试工具、还有题目中定义的所有服务的客户端，例如：vim man bash-completion ssh curl wget dnsutils mailutils ftp lftp nmap traceroute tcptraceroute smbclient
2、建议不要放行 ssh root 用户，复制文件就复制到普通用户家目录即可
3、如果机器或者服务同时拥有 IPv6 和 IPv4，那么它们会优先通过 IPv6 来通信，所以这个时候就要同时考虑 IPv4 和 IPv6 的通信问题（特别是防火墙），要记得放行 IPv6；并且也不要忘记 IPv4 的放行。
4、Linux 一些密码文件权限需要是 600，例如 ansible .vault_pass
5、如果 目录权限是 644，而不是 755，缺少 x 权限，就会导致很多问题，例如 ftp 登陆后无法查看目录内容，无法列出目录文件。
6、如果密码中带有 *，就不能直接在控制台输入，要加上双引号 或单引号；如果密码中带有 $ 就必须加单引号或 转义符。还有很多符号都会导致这个问题，所以建议只要有符号的密码，就在外层加上单引号
7、配置 反向代理时，要配置把真实的 Web Host 传给后端：
apache2 代理要添加：ProxyPreserveHost on
nginx 代理要添加 proxy_set_header $http_host;haproxy 默认就能够把 Host 传给后端。
8、在 debian 13.3 中 roundcube，不要改它的 web 目录，就用 /usr/share/roundcube 作为 web 根目录，因为它有的软连接是 ../../.. 这样指到 /usr/share/中的，改了路径会导致访问不到。
9、Ikev2 VPN，防火墙要放行 udp 500/4500 端口，和 esp protocol。两种场景：
没有 NAT，放行 udp 500、esp protocol
经过 NAT，放行 udp 500、4500

•初始化：

```
apt install -y vim man dbus bash-completion ssh python3 curl wget dnsutils mailutils ftp lftp nfs-common nmap traceroute tcptraceroute

systemctl start dbus

timedatectl set-timezone Asia/Shanghai

echo "set nu" >> /etc/vim/vimrc

echo -e 'WSC2026!shanghai\nWSC2026!shanghai' | adduser mailuser1
echo -e 'WSC2026!shanghai\nWSC2026!shanghai' | adduser mailuser2

hostnamectl set-hostname
```

```
sed -i "s/^127.0.1.1.*/127.0.1.1 $(hostname).hq.int $(hostname)/" /etc/hosts
```

一、DNS（TCP/UDP 53）：

1、bind9：

```
# 第一个是 2，剩下四个都写成 600000 即可
```

```
@       SOA     server1.shanghai.org. server1.shanghai.org. ( 2 600000 600000 600000 600000 )
@       NS      server1.shanghai.org.
@       A       172.16.1.1
server1 A       172.16.1.1
server2 A       172.16.1.2
```

•TSIG 主从 DNS：

```
tsig-keygen shanghai.org >> /etc/bind/named.conf
```

```
// This is the primary configuration file for the BIND DNS server nam
//
// Please read /usr/share/doc/bind9/README.Debian for information on
// structure of BIND configuration files in Debian, *BEFORE* you cust
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.co

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
key "shanghai.org" {
        algorithm hmac-sha256;
        secret "j6q+KO6azYls0864n/1AeCWCtI6wD6n5KO9qFiS9LUg=";
};

zone "shanghai.org" {
        type master;
        file "/etc/bind/db.shanghai";
        allow-transfer { key "shanghai.org"; };
};
```

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
key "shanghai.org" {
        algorithm hmac-sha256;
        secret "j6q+KO6azYls0864n/1AeCWCtI6wD6n5KO9qFiS9LUg=";
};

server 192.168.1.1 { keys "shanghai.org"; };

zone "shanghai.org" {
        type slave;
        file "db.shanghai";
        masters { 192.168.1.1; };
};
```

•ddns:

配置后在客户端重新获取一遍地址，如果还是不行，就重启服务器（isc-dhcp-server 有时需要等待几分钟）

dhcp 必须下发域名，才能够成功 ddns

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
key "shanghai.org" {
        algorithm hmac-sha256;
        secret "j6q+KO6azYls0864n/1AeCWCtI6wD6n5KO9qFiS9LUg=";
};

zone "shanghai.org" {
        type master;
        file "/etc/bind/db.shanghai";
        allow-update { key "shanghai.org"; };
};
```

```
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style standard;

key "shanghai.org" {
        algorithm hmac-sha256;
        secret "j6q+KO6azYls0864n/1AeCWCtI6wD6n5KO9qFiS9LUg=";
};

zone shanghai.org {
        primary 192.168.1.1;
        key "shanghai.org";
}
```

•RPZ 非法域名：

如果要配置 RPZ + View 区域分离，那么 view 的两个区域要同时配置 RPZ 非法域名的 zone，否则重启会报错

或者单独在 view 中指定 RPZ

出现 timeout 的原因（debian 13 后新增）：本地存在的域名就不会这样。当解析本地区域不存在的 RPZ 域名时，dns 服务器默认会先进行递归，因为我们是测试环境，因此这个递归大概率找不到，因此就会提示 timeout，配置了这个 qname-wait-recurse no; 之后，对于 rpz 域名就不会进行递归了，而是直接返回 RPZ 的 NXDOMAIN。

```
113 view dmz {
114 include "/etc/bind/named.conf.root-hints";
115 zone "wsc48.test" {
116 type master;
117 file "/etc/bind/db.wsc48.test";
118 allow-transfer { key "tsig-key"; };
119 allow-update { key "tsig-key"; };
120 };
121
122 zone "rpz.local" {
123 type master;
124 file "/etc/bind/db.rpz.local";
125 };
126
127 response-policy { zone "rpz.local"; } qname-wait-recurse no;
128
```

```
;
; 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      server.
$GENERATE       1-9     virus0$.net     CNAME   .
$GENERATE       10-99   virus$.net      CNAME   .
skill39.fun     CNAME   .
skill39.cc      CNAME   .
skill39.art     CNAME   .
skill39.live    CNAME   .
~
~
~
```

记得要加上 response-policy

•allow-query/blackhole:

allow-query 是白名单

blackhole 是黑名单

只允许指定网段解析指定域名：

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "skills39.edu" {
        type master;
        file "/etc/bind/db.skills39.edu";
        allow-query { 192.168.10.0/24; };
};

zone "cisco.com" {
        type master;
        file "/etc/bind/db.cisco.com";
};

```

blackhole 禁止指定 IP 查询

```
blackhole { 100.100.100.0/24; };
```

•隐藏版本号:

只有两种写法：
1、none //不显示任何信息
2、“” //自定义信息，（“”内可以自定义内容）也可以“”，什么内容都不输入，就会显示为“”

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you
        // to talk to, you may need to fix the firewall to allow
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800

        // If your ISP provided one or more IP addresses for stab
        // nameservers, you probably want to use them as forwarde
        // Uncomment the following block, and insert the addresse
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================
        // If BIND logs error messages about the root key being e
        // you will need to update your keys.  See https://www.is
        //========================================================
        dnssec-validation no;

        masterfile-format text;
        allow-recursion { any; };
        version "unknow";
        listen-on-v6 { any; };
};
~
~
```

•dns 查询日志:

这里直接写相对路径 file "queries.log"，不写绝对路径，日志默认就会存储到/var/cache/bind 下

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

key "skills39.edu" {
        algorithm hmac-sha256;
        secret "ReaGq6XusC2XldGJukXjC8eLBB7ADVxO5b2Nw/U2igg=";
};

zone "skills39.edu" {
        type master;
        file "/etc/bind/db.skills39.edu";
        allow-update { key "skills39.edu"; };
};

zone "cisco.com" {
        type master;
        file "/etc/bind/db.cisco.com";
};


logging {
        channel query_log {
                file "queries.log";
                print-category yes;
                print-time yes;
};
category queries { query_log; };
};
```

自定义路径需要修改 apparmor，并给那个目录 bind 用户读写权限

•IPv6 DNS 反向解析记录：

可以先用 nslookup 获取 IPv6 地址段

```
zone "0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.8.4.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
type master;
file "/etc/bind/db.20-6";
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.8.4.0.0.8.b.d.0.1.0.0.2.ip6.arpa" {
type master;
file "/etc/bind/db.30-6";
};
```

db 文件中地址的顺序也是反过来的：

例如：::10 需要表示为：0.1.0.0

```
$TTL 100        ; 0 seconds
@                       IN SOA  core.lab.example. root.lab.example. (
                                2           ; serial
                                1           ; refresh (0 seconds)
                                1           ; retry (0 seconds)
                                1           ; expire (0 seconds)
                                1           ; minimum (0 seconds)
                                )
@       NS      core.lab.example.
0.1.0.0 PTR     core.lab.example.
1.0.0.0 PTR     sz-gw.lab.example.
~
~
```

•SRV 记录：

_服务._协议.域名，例如：ldap 服务记录为 auth
_ldap._tcp.auth.wsc2026.net.

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     int-srv01.int.worldskills.org. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      int-srv01.int.worldskills.org.
@       IN      A       10.1.10.10
int-srv01       A       10.1.10.10
int-srv01       AAAA    2001:db8:1001:10::10

_ldap._tcp.auth.int.worldskills.org.    SRV     10   50   389   int-srv01.int.worldskills.org.
~
~
~
```

16、DNS SRV 记录要这样写：_服务名._TCP/UDP 协议.域名 SRV 优先级 权重 端口 目标域名。就是这样的格式：
_service._protocol.name SRV priority weight port target
例如：
_ldap._tcp.auth.skills.cn. SRV 10 50 389 dc1.skills.cn. //ldap
_ldaps._tcp.auth.skills.cn. SRV 10 50 636 dc1.skills.cn. //ldaps
_kerberos._tcp.auth.skills.cn. SRV 10 50 88 dc1.skills.cn. //kerberos
_kerberos._udp.auth.skills.cn. SRV 10 50 88 dc1.skills.cn. //kerberos
_ldap._tcp.dc._msdcs.skills.cn. SRV 10 50 389 dc1.skills.cn. //查找域控时用的 SRV
_submission._tcp.skills.cn. SRV 10 50 587 mail.skills.cn. //显式邮件 SRV 记录
_submissions._tcp.skills.cn. SRV 10 50 465 mail.skills.cn. //隐式邮件 SRV 记录
_imap._tcp.skills.cn. SRV 10 50 143 mail.skills.cn. //IMAP
_imaps._tcp.skills.cn. SRV 10 50 993 mail.skills.cn. //IMAPS

•解决 view + 主从 组合的问题：

假如同一个 zone：wsc48.test，主服务器定义了不同网段访问获得不同的解析结果，但是

从服务器在向主服务器同步时，不知道哪个文件才是对的，因此从服务器上就会同步过来两个文件名不同，但是内容一样的区域文件，导致客户端解析时无法解析到正确的 view 定义的地址
这样就需要配置 tsig key，让每个 view 都用一个不同的 tsig 密钥，让从服务器根据这个不同的 tsig 密钥来进行同步

•主服务器：

生成两个 tsig 密钥，每个 view 使用不同的 tsig key：
tsig-keygen -a hmac-sha256 >> named.conf
tsig-keygen -a hmac-sha256 >> named.conf

vim named.conf
要用 ! 拒绝其他不允许的 tsig key

```
12 key "tsig-key" {
13         algorithm hmac-sha256;
14         secret "FCQa/RzetbdwcxmAGftEAJvv81P9oghYf56C6FZJi4U=";
15 };
16
17 key "tsig-key-sh" {
18         algorithm hmac-sha256;
19         secret "vxLXaiu3+/uVTp/cPBRV8oasU9obcDucv/Q0nUoCtRA=";
20 };
21 key "tsig-key-sz" {
22         algorithm hmac-sha256;
23         secret "sQrmJluTjO1+T/991jsNfUf1pIgxzg1RrduMCJCNU6c=";
24 };
25
26 view sh {
27 match-clients { !key "tsig-key"; !key "tsig-key-sz"; key "tsig-key-sh"; 10.48.10.0/24; };
28 include "/etc/bind/named.conf.root-hints";
29 zone "wsc48.test" {
30 type master;
31 file "/etc/bind/db.sh";
32 allow-transfer { key "tsig-key-sh"; };
33 #allow-update { key "tsig-key"; };
34 };
35
```

```
69
70 view sz {
71 match-clients { !key "tsig-key"; key "tsig-key-sz"; !key "tsig-key-sh"; 10.48.20.0/24; };
72 include "/etc/bind/named.conf.root-hints";
73 zone "wsc48.test" {
74 type master;
75 file "/etc/bind/db.sz";
76 allow-transfer { key "tsig-key-sz"; };
77 #allow-update { key "tsig-key"; };
78 };
79
```

```
113 view dmz {
114
115 match-clients { key "tsig-key"; !key "tsig-key-sz"; !key "tsig-key-sh"; any; };
116 include "/etc/bind/named.conf.root-hints";
117 zone "wsc48.test" {
118 type master;
119 file "/etc/bind/db.wsc48.test";
120 #allow-transfer { key "tsig-key"; };
121 allow-transfer { key "tsig-key"; };
122 #allow-update { key "tsig-key"; };
123 };
124
```

•从服务器：

vim named.conf

```
key "tsig-key" {
        algorithm hmac-sha256;
        secret "FCQa/RzetbdwcxmAGftEAJvv81P9oghYf56C6FZJi4U=";
};

key "tsig-key-sh" {
        algorithm hmac-sha256;
        secret "vxLXaiu3+/uVTp/cPBRV8oasU9obcDucv/Q0nUoCtRA=";
};
key "tsig-key-sz" {
        algorithm hmac-sha256;
        secret "sQrmJluTjO1+T/991jsNfUf1pIgxzg1RrduMCJCNU6c=";
};


#server 10.48.30.5 { keys "tsig-key"; };


view sh {
#server 10.48.30.5 { keys "tsig-key"; };
match-clients { any; };
include "/etc/bind/named.conf.root-hints";
zone "wsc48.test" {
type slave;
file "/etc/bind/db.sh";
#masters { 10.48.30.5; };
masters { 10.48.30.5 key "tsig-key-sh"; };
};
```

```
view sz {
#server 10.48.30.5 { keys "tsig-key"; };
#match-clients { key "tsig-key-sz"; 10.48.20.0/24; };
match-clients { 10.48.20.0/24; };
include "/etc/bind/named.conf.root-hints";
zone "wsc48.test" {
type slave;
file "/etc/bind/db.sz";
#masters { 10.48.30.5; };
masters { 10.48.30.5 key "tsig-key-sz"; };
};
```

```
view dmz {
#server 10.48.30.5 { keys "tsig-key"; };
#match-clients { key "tsig-key"; 10.48.99.0/30; 10.48.40.0/24; 10.48.30.0/24; };
match-clients { 10.48.99.0/30; 10.48.40.0/24; 10.48.30.0/24; };
include "/etc/bind/named.conf.root-hints";
zone "wsc48.test" {
type slave;
file "/etc/bind/db.wsc48.test";
#masters { 10.48.30.5 key tsig-key; };
#masters { 10.48.30.5; };
masters { 10.48.30.5 key "tsig-key"; };
};
```

•根提示：

/usr/share/dns/root.hints

```
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     January 01, 2023
;       related version of root zone:     2023010101
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000        NS      ca.isp.net.
ca.isp.net.     3600000 A       1.214.51.1
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     199.9.14.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
```

•转发器：

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                192.168.100.254;
        };                                  填写要转发给的 DNS服务器地址

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation no;               关闭 dnssec 验证

        listen-on-v6 { any; };
};
~
~
```

•条件转发器：

only //只转发给这个服务器
first //当这个服务器返回失败时，尝试进行本地递归

```bind
zone "beijing.cn" {
    type forward;
    forward first;
    forwarders {
        10.0.0.20;
    };
};
```

•dnssec:

用于递归服务器校验权威服务器：

权威服务器：

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";

logging {
     category queries { log; };
     channel log {
          file "/var/log/dns_query.log";
          print-category yes;
          print-severity yes;
     };
};



view "internal" {
match-clients { 192.168.0.0/24; 192.168.1.0/24; 192.168.2.0/24; localhost; };
include "/etc/bind/named.conf.root-hints";
zone "shenzhen.cn" {
  type primary;
  file "/etc/bind/db.shenzhen.cn.in";
  allow-update { 192.168.1.1; };
  allow-transfer { 192.168.1.1; };
  dnssec-policy default;
  inline-signing yes;
};

zone "0.168.192.in-addr.arpa" {
  type primary;
  file "/etc/bind/db.0";
  allow-transfer { 192.168.1.1; };
};

zone "1.168.192.in-addr.arpa" {
  type primary;
  file "/etc/bind/db.1";
  allow-transfer { 192.168.1.1; };
};

zone "2.168.192.in-addr.arpa" {
  type primary;
```

重启后就会在 /var/cache/bind 目录生成公钥私钥

```
root@srv1:/etc/bind# ls /var/cache/bind/
external.mkeys      internal.mkeys      Kshenzhen.cn.+013+44824.key      Kshenzhen.cn.+013+44824.state  managed-keys.bind.jnl  tmp-xaUrmNO7sY
external.mkeys.jnl  internal.mkeys.jnl  Kshenzhen.cn.+013+44824.private  managed-keys.bind              tmp-FdvblzsSEd
```

然后复制这个 key：

```
; This is a key-signing key, keyid 44824, for shenzhen.cn.
; Created: 20260812062304 (Wed Aug 12 02:23:04 2026)
; Publish: 20260812062304 (Wed Aug 12 02:23:04 2026)
; Activate: 20260812062304 (Wed Aug 12 02:23:04 2026)
; SyncPublish: 20260813062804 (Thu Aug 13 02:28:04 2026)
shenzhen.cn. 3600 IN DNSKEY 257 3 13 CwrADX5qFzZZkFTWeyQ4xhBHj5KOItdNcHE4V5h6fFx0thapw13Mc2de S0JC/GbnzlNtSQ5cUEmCyyTAJy1E2g==
```

在从服务器开启 dnssec 校验，并信任 key：

trustj-anchors { "域名.com." static-key <key>; };

```
options {
        directory "/var/cache/bind";
        recursion yes;
allow-recursion { any; };

dnssec-validation yes;
};
```

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.root-hints";

trust-anchors { "shenzhen.cn." static-key 257 3 13 "CwrADX5qFzZZkFTWeyQ4xhBHj5KOItdNcHE4V5h6fFx0thapw13Mc2de S0JC/GbnzlNtSQ5cUEmCyyTAJy1E2g=="; };
zone "." {
  type primary;
  file "/etc/bind/db.root";

};

zone "shanghai.cn" {
  type primary;
  file "/etc/bind/db.shanghai.cn";
};

#logging {
#     category rsyslog { log; };
#     channel log {
#          file "/var/log/dns_query.log";
#          print-category true;
#          print-severity true;
#          print-time local;
#          syslog local6;
#     };
#};

```

2、dnsmasq:

设置接受指定接口传入的 dns 请求：

vim /etc/dnsmasq.conf

如果有多个接口，可以用 ， 分割

```
# interface (eg eth0) here.
# Repeat the line for more than one interface
interface=ens33

#interface=ens33,ens37

```

systemctl restart dnsmasq

•A 记录：

```
74 local=/shanghai.org/
```

```
 79 address=/www.shanghai.org/1.1.1.10
 80 address=/shanghai.org/1.1.1.1
```

```
155 domain=shanghai.org
```

•反向解析：

```
652 #ptr-record=_http._tcp.dns-sd-services,"New Employee Page
653 ptr-record=1.10.168.192.in-addr.arpa,shanghai.org
654 ptr-record=10.10.168.192.in-addr.arpa,www.shanghai.org
```

•CNAME 记录：

```
670 # "bert" another name, bertrand
671 #cname=bertand,bert
672 cname=cname.shanghai.org,www.shanghai.org
673
```

不能这样写：（这样写只会把 cname 变成 A 记录）

```
669 # "bert" another name
670 #cname=bertand,bert
671 cname=cname,www
672
```

•mx 记录：

```
607 # servermachine.com and preference 50
608 #mx-host=maildomain.com,servermachine.com,50
609 mx-host=mx.shanghai.org,shanghai.org,10
610
```

•ipv6 正向解析：

```
73 # from /etc/hosts or DHCP
74 local=/wsc2026.org/
75
```

```
81 # --address (and --server) work with IPv6 addresses too.
82 #address=/www.thekelleys.org.uk/fe80::20d:60ff:fe36:f83
83 address=/wsc2026.org/2001:db8:abcd::1
84 address=/www.wsc2026.org/2001:db8:abcd::1
85
```

•ipv6 反向解析：

vim /etc/dnsmasq.conf
结尾与 ipv4 反解不同，是 ip6.arpa

```
651 # domain-name expansion done for SRV records _does_not
652 # occur for PTR records.)
653 #ptr-record=_http._tcp.dns-sd-services,"New Employee Page._http._tcp.dns-sd-services"
654 ptr-record=1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a.8.b.d.0.1.0.0.2.ip6.arpa,www.wsc2026.
    org
655 ptr-record=1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a.8.b.d.0.1.0.0.2.ip6.arpa,wsc2026.org
656
```

分为 8 段，每段 4 个字节，不能省略 0
例如这里的，2001:db8 = 2001:0db8

•配置转发器：

```
65 # non-public domains.
66 #server=/localnet/192.168.0.1
67 server=1.1.1.254
68
```

二、DHCP（UDP 67、546）：

1、isc-dhcp-server：

•isc-dhcp-relay 监听接口要同时监听 dhcp 服务器和客户端接口，与 Windows 不一样，Windows 只需要监听客户端接口即可。

注意要同时指定一个本地网段的地址池，否则启动会报错

2、kea-dhcp-server：

•分配 IPv4 地址：

注释原本 192.0.2.0/24 网段的默认内容，否则启动会报错：

这里只显示了部分，要全部注释掉

```
347                 // be defined for any identifier type, not just client-id.
348                 //{
349                 //    "client-id": "01:11:22:33:44:55:66",
350                 //    "ip-address": "192.0.2.202",
351                 //    "hostname": "special-snowflake"
352                 //},
353
354                 // The third reservation is based on DUID. This reservation defines
355                 // a special option values for this particular client. If the
356                 // domain-name-servers option would have been defined on a global,
357                 // subnet or class level, the host specific values take preference.
358                 //{
359                 //    "duid": "01:02:03:04:05",
360                 //    "ip-address": "192.0.2.203",
361                 //    "option-data": [ {
362                 //        "name": "domain-name-servers",
363                 //        "data": "10.1.1.202, 10.1.1.203"
364                 //    } ]
365                 //},
366
```

分配固定地址：

```
329             // your configurations.
330             "reservations": [
331
332                 // This is a reservation for a specific hardware/MAC address.
333                 // It's a rather simple reservation: just an address and nothing
334                 // else.
335                 {
336                     "hw-address": "1a:1b:1c:1d:1e:1f",
337                     "ip-address": "10.1.10.101"
338                 },
339
340                 // This is a reservation for a specific client-id. It also shows
341                 // the this client will get a reserved hostname. A hostname can
342                 // be defined for any identifier type, not just client-id.
343                 {
344                     "client-id": "01:11:22:33:44:55:66",
345                     "ip-address": "192.0.2.202",
346                     "hostname": "special-snowflake"
347                 },
```

•ddns:

vim /etc/kea/kea-dhcp4.conf

```
27 "Dhcp4": {
28     // Add names of your network interfaces to listen on.
29     "interfaces-config": {
30         // See section 8.2.4 for more details. You probably want to add just
31         // interface name (e.g. "eth0" or specific IPv4 address on that
32         // interface name (e.g. "eth0/192.0.2.1").
33         "interfaces": [ "ens33" ]
34
35         // Kea DHCPv4 server by default listens using raw sockets. This ensures
36         // all packets, including those sent by directly connected clients
37         // that don't have IPv4 address yet, are received. However, if your
38         // traffic is always relayed, it is often better to use regular
39         // UDP sockets. If you want to do that, uncomment this line:
40         // "dhcp-socket-type": "udp"
41 },
42
43 "dhcp-ddns": {
44   "enable-updates": true,
45   #"server-ip": "127.0.0.1",
46   #"server-port": 53001,
47 },
48
49 #"ddns-send-updates": true,
50 #"ddns-qualifying-suffix": "wsc48.lan.",
51 #"ddns-override-no-update": true,
52 #"ddns-override-client-update": true,
53 #"ddns-replace-client-name": "when-not-present",
54
```

vim /etc/kea/kea-dhcp-ddns.conf

```
20 "DhcpDdns":
21 {
22   "ip-address": "127.0.0.1",
23   "port": 53001,
24   "control-socket": {
25       "socket-type": "unix",
26       "socket-name": "kea-ddns-ctrl-socket"
27   },
28   "tsig-keys": [],
29
30   "forward-ddns" : {
31 "ddns-domains": [
32 {
33 "name":"wsc48.lan.",
34 "dns-servers":[
35 {
36 "ip-address":"127.0.0.1",
37 "port":53
38 }
39 ]
40 }
41 ]
42 },
43   "reverse-ddns" : {
44 "ddns-domains":[
45 {
46 "name":"10.48.10.in-addr.arpa.",
47 "dns-servers":[
48 {
49 "ip-address":"127.0.0.1",
50 "port":53
51 }
52 ]
53 }
54 ]
55 },
56
57 // Logging configuration starts here. Kea uses different loggers to log va
58 // activities. For details (e.g. names of loggers), see Chapter 18.
```

加上 tsig：

```
// See Section 11 for examples and details description.
"DhcpDdns":
{
  "ip-address": "127.0.0.1",
  "port": 53001,
  "control-socket": {
      "socket-type": "unix",
      "socket-name": "kea-ddns-ctrl-socket"
  },
  "tsig-keys": [
{
"name":"tsig-key",
"algorithm":"hmac-sha256",
"secret":"FCQa/RzetbdwcxmAGftEAJvv81P9oghYf56C6FZJi4U="
}
],
  "forward-ddns" : {
"ddns-domains":[
{
"name":"wsc48.test.",
"dns-servers":[
{
"ip-address":"127.0.0.1",
"port":53
}
]
}
]
},
  "reverse-ddns" : {
"ddns-domains":[
{
"name":"10.48.10.in-addr.arpa.",
"dns-servers":[
{
"ip-address":"127.0.0.1",
"port":53
}
]
}
]
},
```

•DHCPv6:

```
// and will be ignored by other components.
"Dhcp6": {
    // Add names of your network interfaces to listen on.
    "interfaces-config": {
        // You typically want to put specific interface names here, e.g. eth0
        // but you can also specify unicast addresses (e.g. eth0/2001:db8::1) if
        // you want your server to handle unicast traffic in addition to
        // multicast. (DHCPv6 is a multicast based protocol).
        "interfaces": [ "ens192/fdab:cdef:1234:10::10" ]
    },

    // Kea supports control channel, which is a way to receive management commands
    // while the server is running. This is a Unix domain socket that receives
    // commands formatted in JSON, e.g. config-set (which sets new configuration),
    // config-reload (which tells Kea to reload its configuration from file),
    // statistic-get (to retrieve statistics) and many more. For detailed
    // description, see Sections 9.12, 16 and 15.
    "control-socket": {
        "socket-type": "unix",
        "socket-name": "kea6-ctrl-socket"
    },

    // Use Memfile lease database backend to store leases in a CSV file.
:x_
```

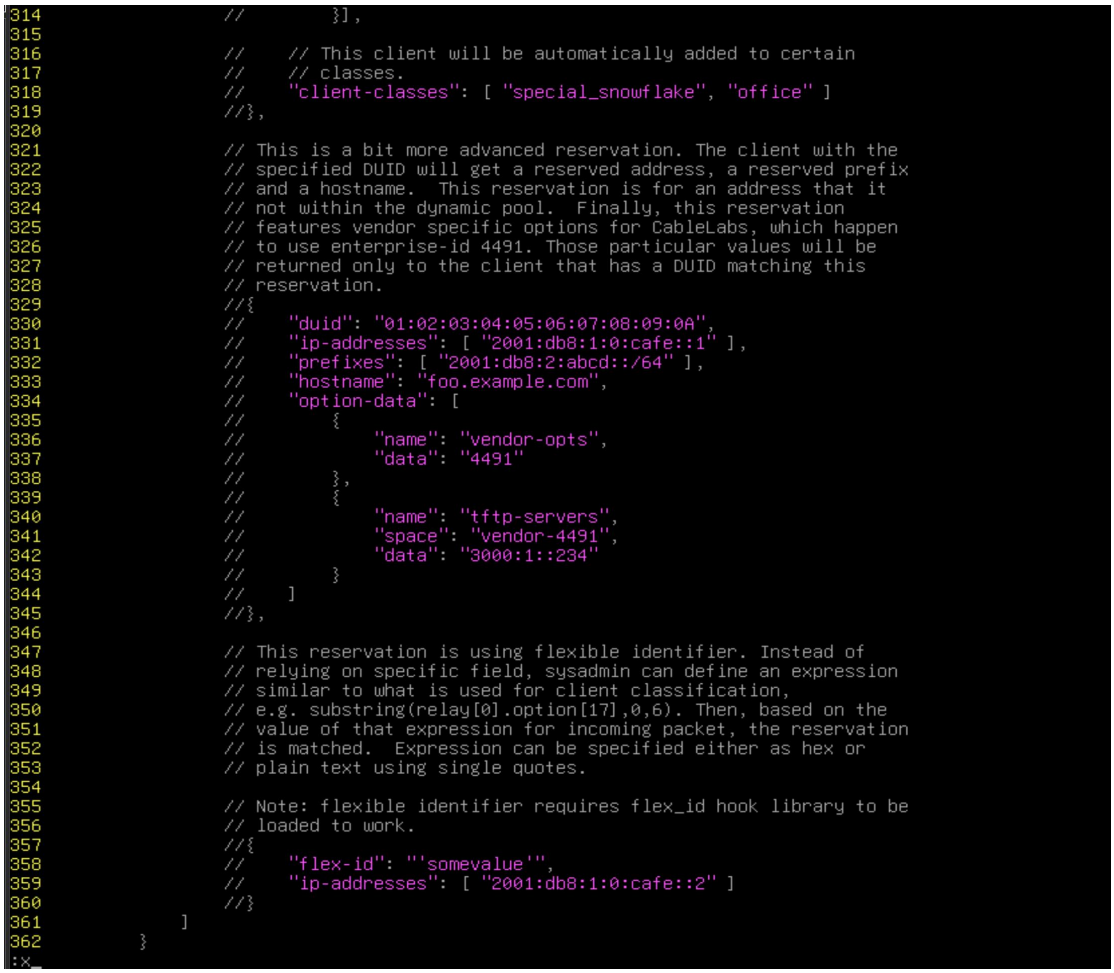
```
233     "subnet6": [
234         {
235             "interface": "ens33",
236             // This defines the whole subnet. Kea will use this information to
237             // determine where the clients are connected. This is the whole
238             // subnet in your network.
239
240             // Subnet identifier should be unique for each subnet.
241             "id": 1,
242
243             // This is mandatory parameter for each subnet.
244             "subnet": "2001:db8:10::/64",
245
246             // Pools define the actual part of your subnet that is governed
247             // by Kea. Technically this is optional parameter, but it's
248             // almost always needed for DHCP to do its job. If you omit it,
249             // clients won't be able to get addresses, unless there are
250             // host reservations defined for them.
251             //"pools": [ { "pool": "2001:db8:10::/80" } ],
252             "pools": [ { "pool": "2001:db8:10::100-2001:db8:10::200" } ],
253
254             // Kea supports prefix delegation (PD). This mechanism delegates
255             // whole prefixes, instead of single addresses. You need to specify
256             // a prefix and then size of the delegated prefixes that it will
257             // be split into. This example below tells Kea to use
258             // 2001:db8:1::/56 prefix as pool and split it into /64 prefixes.
259             // This will give you 256 (2^(64-56)) prefixes.
260             //"pd-pools": [
261             //    {
262             //        "prefix": "2001:db8:8::",
263             //        "prefix-len": 56,
264             //        "delegated-len": 64
265
266             //        // Kea also supports excluded prefixes. This advanced option
267             //        // is explained in Section 9.2.9. Please make sure your
268             //        // excluded prefix matches the pool it is defined in.
269             //        // "excluded-prefix": "2001:db8:8:0:80::",
270             //        // "excluded-prefix-len": 72
271             //    }
272             //],
273             "option-data": [
274                 // You can specify additional options here that are subnet
275                 // specific. Also, you can override global options here.
276                 //{
277                 //    "name": "dns-servers",
278                 //    "data": "2001:db8:2::dead:beef, 2001:db8:2::cafe:babe"
279                 //}
280             ],
281
:q
```

新增

注释掉 subnet 内部的 option，它会覆盖掉前面定义的全局 dns，或者在这里修改 option：

```
272             "option-data": [
273                 // You can specify additional options here that are subnet
274                 // specific. Also, you can override global options here.
275                 //{
276                 //    "name": "dns-servers",
277                 //    "data": "2001:db8:2::dead:beef, 2001:db8:2::cafe:babe"
278                 //}
279             ],
```

最后把一些地址保留注释掉：



然后需要安装配置 radvd，下发 ra：

apt install -y radvd

```
11 interface ens33
12 {
13         AdvSendAdvert on;
14
15 # This may be needed on some interfaces which are not active when
16 # radvd starts, but become available later on; see man page for d
17
18         # IgnoreIfMissing on;
19
20 #
21 # These settings cause advertisements to be sent every 3-10 secon
22 # range is good for 6to4 with a dynamic IPv4 address, but can be
23 # increased when not using 6to4 prefixes.
24 #
25
26         MinRtrAdvInterval 3;
27         MaxRtrAdvInterval 10;
28
29         AdvManagedFlag on;
30         AdvOtherConfigFlag on;
31 #
32 # You can use AdvDefaultPreference setting to advertise the prefe
33 # the router for the purposes of default router determination.
34 # NOTE: This feature is still being specified and is not widely s
35 #
36         AdvDefaultPreference low;
37
38 #
39 # Disable Mobile IPv6 support
40 #
41         AdvHomeAgentFlag off;
42
43 #
44 # example of a standard prefix
45 #
46         prefix 2001:db8:10::/64
47         {
48                 AdvOnLink on;
49                 #AdvAutonomous on;
50                 AdvAutonomous off;
51                 AdvRouterAddr off;
52         };
53
```

•如果有防火墙，并且要求 output 策略为 drop，那么 DHCPv6 必须要在 output 放行 udp 546 端口，否则客户端获取不到 IPv6 地址

3、dnsmasq:

```
168 # service.
169 #dhcp-range=192.168.0.50,192.168.0.150,12h
170 dhcp-range=1.1.1.0,1.1.1.100,12h
171 _
```

网关：

```
344 #dhcp-option=3,1.2.3.4
345 dhcp-option=3,1.1.1.254
346
```

•DHCPv6：

dnsmasq 自己就能发 ra，不需要安装 radvd

```
224 # advertisements will have the M and
225 # get addresses and configuration fr
226 # clients don't use SLAAC addresses
227 enable-ra
228 _
229 # Supply parameters for specified ho
```

```
192 # and defaults to 64 if missing/
193 #dhcp-range=1234::2, 1234::500, 64, 12h
194 dhcp-range=2001:db8:abcd::100, 2001:db8:abcd::ffff, 64, 12h
195
```

```
365 #dhcp-option=option6:dns-server,[::],[1234::88]
366 dhcp-option=option6:dns-server,2001:db8:abcd::1,2001:db8:abcd::2
```

•仅 SLAAC：

```
224 # advertisements will have the M and
225 # get addresses and configuration fr
226 # clients don't use SLAAC addresses
227 enable-ra
228 _
229 # Supply parameters for specified ho
```

```
209 #dhcp-range=1234::, ra-only, 48h
210 dhcp-range=2001:db8:abcd::, ra-only, 48h
211
```

4、中继：

•IPv6 中继：

```
# 只能用命令配置：
```

```
dhcrelay -6 -d -l ens192 -u fdab:cdef:1234:10::10%ens256
```

配置持久化：

```
[Unit]
#Description=OpenBSD Secure Shell server
#Documentation=man:sshd(8) man:sshd_config(5)
#After=network.target nss-user-lookup.target auditd.service
#ConditionPathExists=!/etc/ssh/sshd_not_to_be_run

[Service]
#EnvironmentFile=-/etc/default/ssh
#ExecStartPre=/usr/sbin/sshd -t
ExecStart=/usr/sbin/dhcrelay -6 -d -l ens192 -u fdab:cdef:1234:10::10%%ens256
#ExecReload=/usr/sbin/sshd -t
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartPreventExitStatus=255
#Type=notify
Type=simple
#RuntimeDirectory=sshd
RuntimeDirectoryMode=0755

[Install]
WantedBy=multi-user.target
#Alias=sshd.service
Alias=dhcrelay.service
~
~
```

5、radvd 配置 SLAAC:

```
apt install -y radvd
```

```
10
11 interface ens33
12 {
13         AdvSendAdvert on;
14
15 # This may be needed on some interfaces which are not active when
16 # radvd starts, but become available later on; see man page for details.
17
18         # IgnoreIfMissing on;
19
20 #
21 # These settings cause advertisements to be sent every 3-10 seconds.  This
22 # range is good for 6to4 with a dynamic IPv4 address, but can be greatly
23 # increased when not using 6to4 prefixes.
24 #
25
26         MinRtrAdvInterval 3;
27         MaxRtrAdvInterval 10;
28
29 #
30 # You can use AdvDefaultPreference setting to advertise the preference of
31 # the router for the purposes of default router determination.
32 # NOTE: This feature is still being specified and is not widely supported!
33 #
34         AdvDefaultPreference low;
35
36 #
37 # Disable Mobile IPv6 support
38 #
39         AdvHomeAgentFlag off;
40
41 #
42 # example of a standard prefix
43 #
44         prefix 2001:db8:10::/64
45         {
46                 AdvOnLink on;
47                 AdvAutonomous on;
48                 AdvRouterAddr off;
49         };
50
51 #
52 # example of a 6to4 prefix
```

三、CA:

•有时生成出来的证书（在子 CA 环境遇到的问题），私钥是被密码加密的

我们可以通过 openssl rsa -in client.key -out client.key 来解密，因为加密的私钥服务是无法直接读取的（特别是排错时）要确定私钥是否是加密的，除了看服务日志的报错，还可以直接 vim 打开私钥文件查看开头，如果这里是 ENCRYPTED 就表示该私钥是被加密的

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIHdTBfBgkqhkiG9w0BBQ0wUjAxBgkqhkiG9w0BBQwwJAQQWAjq2qnxMYe4mYPp
p0JBRQICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEEJQK6OvwK/DCxpUj
+B851pgEggcQ+LUt092auUxfBD0XKLItt87RNbDd0U6q1iiWXJcqM6/LjC4M/cgX
qIIBHRZlfqis1zzlcE9Y+aNTP9DMS6MfqkdOjtjpoyq+9oyoyzz2JsZXQRHR2xHF
vby4IYkemyiTj2NUyX+IviCnoBCHPYd9MaG2GT4EhqOQF9Zg9WqOyNz+AMXjIwOr
5rZA86FJ0qt61WGB6fwEq+LesGBCRpj6KgFqcIPgrC9IJ7yvgOQaeT5vOn6drHIW
aNg5PQuy6Kk2E3J833ZUVyrXUl0tAKT8WJdjvMY7Dp59JPBLj2uwGSomSVMeLxyO
0M1cjnbmRY1EmZ76r5mQWC3EJE2ow1f2zha+nkXB7juxoJxbNJR2L8pulB2M/IMt
7yqaVDodI5tha+fZyJMgBcPkyBbvE1K3ebWk5O697oiWw96KStS46lGOOqykdjba
X1X0hGjTQsWMHjzxYzD9oWTZCDdog5ikciE5evKv8rRdsndHCaUdaW1zXfcs1KBM
3SL5dk1oEXuNPW1HI81RK/QttkXZEuyIBb2Q8KJtnN2D0wycLpAIqxpEG8hSIrE8
YItWTUVhsX0YwSJGi7fDXepQJW5G8HXRtT3rZoAez2aZkPU9fTpAp7Wu7dQ/DRs/
PPNl2bdvl749CWLUPwi6IdrJkil67e8szNP2xzurOpwmaeldHNc1eCqazitLEezI
YfzmLE/Cipid8rpm6wtvfpPUzEVfsk6WqS5C+dtIeCHq/NIjNI1bJCDm/gwAg3hD
4vLgu1orX7zYZVxLS+Afnoq8ukllTi1V7Hh63HovZ2zk1PDbgGo/ljjOhA92qI3M
```

1、命令 申请证书：

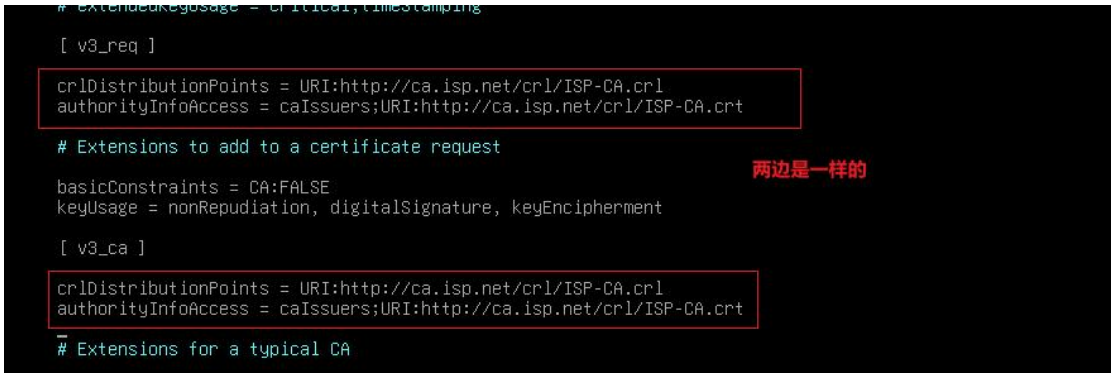
创建证书申请前要设置：
vim /etc/ssl/openssl.cnf
取消注释，这样 openssl 就会自动调用 extension

```
 99 # Comment out the following two lines fo
100 # (and highly broken) format.
101 name_opt         = ca_default
102 cert_opt         = ca_default
103
104 # Extension copying option: use with cau
105 copy_extensions = copy
106
107 # Extensions to add to a CRL. Note: Nets
108 # so this is commented out by default to
109 # crlnumber must also be commented out t
110 # crl_extensions        = crl_ext
```

openssl req -out newreq.pem -newkey rsa:2048 -nodes -keyout newkey.pem -subj "/CN=mail.shenzhen.cn/C=CN" -addext "subjectAltName=DNS:mail.shenzhen.cn, DNS:smtp.shenzhen.cn" //这里如果要写多个 DNS，必须要 逗号 + 空格

签发：
/usr/lib/ssl/misc/CA.pl -sign
注意这里的 DNS，必须是 subjectAltName，这里是严格区分大小写的

2、CDP、AIA：




```
# 手动生成 crl：
openssl ca -gencrl -out ISP-CA.crl
# 将 crl 的 pem 格式转换为 der（否则 web 网站和命令无法识别）：
openssl crl -in ISP-CA.crl -inform PEM -outform DER -out ca.crl

# 吊销证书：
openssl ca -revoke web.crt

# 吊销后要手动重新生成 crl，并且转格式为 DER（如果要放到 web 中）：
openssl ca -gencrl -out capem.crl
```

3、pkcs12：

```
## 合成 pkcs12：
# 只合并证书和私钥：
openssl pkcs12 -export -inkey server.key -in server.crt -out server.p12

# 合并证书+私钥+CA 根证书：
openssl pkcs12 -export -inkey server.key -in server.crt -certfile ca.crt -out server.p12
```

```
## 拆分 pkcs12：
# 导出证书：
openssl pkcs12 -in server.p12 -clcerts -nokeys -out server.crt

# 导出私钥：
openssl pkcs12 -in server.p12 -nocerts -out server.key

# 导出 CA（如果有）：
openssl pkcs12 -in server.p12 -cacerts -nokeys -out ca.crt
```

4、子 CA：

注意子 CA 的字段需要是： CA：TRUE
并且颁发完子 CA 后记得改回：CA：FALSE

•如果有子 CA，一些服务的需求的 ca 根证书（例如 openvpn），那个文件中必须同时包含 根 CA 证书和 subCA 证书

```
# 解决方法：将根 CA 根证书和子 CA 根证书放在同一张文件 ca.crt 中（需要注意根 CA 需要在前面）（服务和客户端都需要使用这张根证书来建立 openvpn）
cat Root-CA.crt Sub-CA.crt > ca.crt
```

四、nftables

直接放行：iifname lo accept、meta l4proto { icmp, icmpv6 } accept

一些点对点的，例如：S2S、dns 主从 等，可以同时写上 iifname、oifname、ip saddr、ip daddr
如果一些影响比较大的，例如 web，可能从其他服务端测试的，就可以不配置 iifname、ip saddr 来限定源地址

防火墙不要对 dhcp 端口设置 ip saddr 的限制，因为 dhcp 客户端默认源地址为：0.0.0.0，目标为：255.255.255.255，如果配置了 ip saddr，就会导致客户端无法获取 dhcp 地址

•防火墙放行 53 端口时，建议同时放行 udp 和 tcp 53，因为有时解析可能会用到 tcp 53

•要写注释、自定义链、拒绝日志：

```
table ip filter {
        chain log_chain {
                log prefix "NFT-DROP:" level info counter packets 0 bytes 0 drop
        }

        chain input {
                type filter hook input priority filter; policy drop;
                ct state established,related accept
                ip protocol icmp accept
                iifname "lo" accept
                iifname "ens224" ip saddr 210.103.5.4 ip daddr 210.103.5.1 udp dport 1194 accept
                iifname "ens224" ip daddr 210.103.5.1 tcp dport 443 accept
                iifname "ens256" ip daddr 10.11.47.129 tcp dport 443 accept
                tcp dport { 80, 443 } accept
                iifname { "tun0", "ens161", "ens192" } ip saddr { 10.11.47.0/25, 10.96.0.0/30, 172.16.10.0/24 } accept
                jump log_chain
        }

        chain forward {
                type filter hook forward priority filter; policy drop;
                ct state established,related accept
                iifname "lo" accept
                ip protocol icmp accept
                iifname { "tun0", "ens161", "ens192" } ip saddr { 10.11.47.0/25, 10.96.0.0/30, 172.16.10.0/24 } accept
                iifname "ens256" ip saddr 10.11.47.128/26 ip daddr 10.11.47.11 udp dport 53 accept comment "Internal DNS"
                iifname "ens256" ip saddr 10.11.47.128/26 ip daddr 10.11.47.11 tcp dport 53 accept comment "Internal DNS"
                iifname "ens256" ip saddr 10.11.47.128/26 ip daddr 10.11.47.11 tcp dport { 514, 6514 } accept
                iifname "ens224" ip daddr 210.103.5.1 udp dport 53 accept
                iifname "ens224" ip daddr 210.103.5.1 tcp dport 53 accept
                iifname "ens256" oifname "ens161" ip saddr { 10.11.47.131, 10.11.47.132, 10.11.47.141 } ip daddr 10.11.47.11 tcp dport 389 accept
                iifname "ens256" ip saddr 10.11.47.128/26 ip daddr 210.103.5.4 tcp dport 22 accept
                tcp dport 80 accept
                jump log_chain
        }

        chain output {
                type filter hook output priority filter; policy drop;
                ct state established,related accept
                ip protocol icmp accept
                iifname "lo" accept
                oifname "ens161" ip saddr 10.11.47.1 ip daddr 10.11.47.11 udp dport 53 accept
                oifname "ens161" ip saddr 10.11.47.1 ip daddr 10.11.47.11 tcp dport 80 accept
                oifname "ens256" ip saddr 10.11.47.129 ip daddr { 10.11.47.131, 10.11.47.132, 10.11.47.141 } udp dport 53 accept
                oifname "ens256" ip saddr 10.11.47.129 ip daddr { 10.11.47.131, 10.11.47.132, 10.11.47.141 } tcp dport 8080 accept
                oifname "ens224" ip saddr 210.103.5.1 ip daddr 210.103.5.4 udp dport 1194 accept
                jump log_chain
        }
}
```

•拒绝之后记录日志：

记录拒绝日志，日志前缀为：WSC48-SZ-DROP:
需要创建一个自定义链，专门用来记录日志，然后将拒绝条目重定向到这个链
vim /etc/nftables.conf

```
1 table ip filter {
2         chain log_drop {
3                 log prefix "WSC48-SZ-DROP:" level warn counter drop
4         }
5         chain input {
6                 type filter hook input priority filter; policy drop;
7                 iifname lo accept
8                 ct state established,related accept
9                 # Accept VPN Traffic
10                iifname ens33 ip saddr 203.0.113.1 ip daddr 203.0.113.2 udp dport 51821 accept comment "WireGuard [UDP/51821]"
11                iifname ens39 ip saddr 10.48.30.5 tcp dport 22 accept comment "SSH [TCP/22]"
12                iifname ens33 ip saddr 203.0.113.1 ip daddr 203.0.113.2 udp dport 67 accept
13                iifname ens38 ip saddr 10.48.20.0/24 ip daddr 10.48.20.100 tcp dport { 80, 443 } accept
14                meta l4proto icmp limit rate 20/second accept
15
16
17
18                iifname ens39 ip saddr 10.48.30.5 tcp dport 22 accept
19
20                #ct state invalid drop
21                ct state invalid jump log_drop
22                jump log_drop
23        }
24
```

末尾加一条 jump 将所有没有匹配到的条目跳过去

查看：

journalctl -k -f | grep --line-buffered 'WSC48-SZ-DROP:'

```
root@sz-gw:~# journalctl -k -f | grep --line-buffered 'WSC48-SZ-DROP:'
Jul 30 11:05:54 sz-gw kernel: WSC48-SZ-DROP:IN=ens37 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:3c:b1:dd:08:00 SRC=10.48.40.2 DST=10.48.40.3 LEN=270 TOS=0x00 PREC=0x00
 TTL=64 ID=52869 DF PROTO=UDP SPT=138 DPT=138 LEN=250
Jul 30 11:05:54 sz-gw kernel: WSC48-SZ-DROP:IN=ens37 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:3c:b1:dd:08:00 SRC=10.48.40.2 DST=10.48.40.3 LEN=239 TOS=0x00 PREC=0x00
 TTL=64 ID=52870 DF PROTO=UDP SPT=138 DPT=138 LEN=219
Jul 30 11:06:11 sz-gw kernel: WSC48-SZ-DROP:IN=ens37 OUT= MAC=00:50:56:2a:f2:e1:00:50:56:3c:b1:dd:08:00 SRC=10.48.40.2 DST=10.48.40.1 LEN=60 TOS=0x10 PREC=0x00
TTL=64 ID=28430 DF PROTO=TCP SPT=43226 DPT=22 WINDOW=64240 RES=0x00 SYN URGP=0
Jul 30 11:06:12 sz-gw kernel: WSC48-SZ-DROP:IN=ens37 OUT= MAC=00:50:56:2a:f2:e1:00:50:56:3c:b1:dd:08:00 SRC=10.48.40.2 DST=10.48.40.1 LEN=60 TOS=0x10 PREC=0x00
TTL=64 ID=28431 DF PROTO=TCP SPT=43226 DPT=22 WINDOW=64240 RES=0x00 SYN URGP=0
Jul 30 11:06:12 sz-gw kernel: WSC48-SZ-DROP:IN=ens37 OUT= MAC=00:50:56:2a:f2:e1:00:50:56:3c:b1:dd:08:00 SRC=10.48.40.2 DST=10.48.40.1 LEN=60 TOS=0x10 PREC=0x00
TTL=64 ID=37873 DF PROTO=TCP SPT=49158 DPT=22 WINDOW=64240 RES=0x00 SYN URGP=0
```

•同时放行 ICMPv4、ICMPv6：

```
meta l4proto { icmp, ipv6-icmp } accept
```

或：

```
ip protocol icmp accept
ip6 nexthdr icmpv6 accept
```

•防火墙速率限制：

```
table ip filter {
        chain input {
                type filter hook input priority filter; policy drop;
                iifname lo accept
                ct state established,related accept
                # Accept VPN Traffic
                iifname ens33 ip saddr 203.0.113.1 ip daddr 203.0.113.2 udp dport 51821 accept comment "WireGuard [UDP/518
                iifname ens39 ip saddr 10.48.30.5 tcp dport 22 accept comment "SSH [TCP/22]"
                iifname ens33 ip saddr 203.0.113.1 ip daddr 203.0.113.2 udp dport 67 accept
                iifname ens38 ip saddr 10.48.20.0/24 ip daddr 10.48.20.100 tcp dport { 80, 443 } accept
                meta l4proto icmp limit rate 20/second accept



                tcp dport 22 accept
                ct state invalid drop
        }
```

•如果防火墙要求 output 策略为 drop，那么一定要配置放行 oifname lo accept，否则会导致一些服务无法访问。

五、LDAP（TCP 389、636）：

1、设置 ssl、禁止匿名用户登陆：

```
1 dn: cn=config
2 ad: olcTLSCACertificateFile
3 olcTLSCACertificateFile: /etc/ssl/root-ca.crt
4 -
5 add: olcTLSCertificateFile
6 olcTLSCertificateFile: /etc/ssl/core.lab.example.crt
7 -
8 add: olcTLSCertificateKeyFile
9 olcTLSCertificateKeyFile: /etc/ssl/core.lab.example.key
~
~
```

ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl.ldif

```
root@ds01:/etc/ldap# ldapmodify -Y EXTERNAL -H ldapi:/// -f ld.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"

root@ds01:/etc/ldap#
```

当设置错误了 可以这样修改：

```
dn: cn=config
changetype: modify
replace: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/root-ca.crt
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/core.lab.example.crt
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/core.lab.example.key
~
~
```

```
root@core:/etc/ldap# ldapmodify -Y EXTERNAL -H ldapi:/// -f ssl.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"

root@core:/etc/ldap#
```

关闭匿名访问：

```
dn: cn=config
add: olcDisallows
olcDisallows: bind_anon
~
~
```

```
root@ds01:/etc/ldap# ldapmodify -Y EXTERNAL -H ldapi:/// -f ld.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"

root@ds01:/etc/ldap#
```

2、导入 用户表：

注意用户的 CN 等于 givenname + sn，然后用户的 givenname 和 sn 正常填写就行

vim usertemp

```
dn: cn=<user>,<usuffix>,<suffix>
objectClass: inetOrgPerson // 必须将account更换为inetOrgPerson，否则无法添加mail属性
objectClass: posixAccount
objectClass: shadowAccount
cn: <user>
sn: <user>          // 必须添加 sn 属性
uid: <user>
uidNumber: <uid>
gidNumber: <gid>
homeDirectory: <home>
loginShell: <shell>
mail: <user>@cisco.com     // 新增 mail 属性，域名根据实际题目进行修改
gecos: <user>
description: User account
~
~
~
```

```
#! /bin/bash

cat users | while read line; do
Name=$(echo $line | cut -d ',' -f 1)
Pwd=$(echo $line | cut -d ',' -f 2)
Group=$(echo $line | cut -d ',' -f 3)
Phone=$(echo $line | cut -d ',' -f 4)


ldapaddgroup $Group
ldapadduser $Name $Group
ldapsetpasswd $Name $Pwd

echo "dn: uid=$Name,ou=users,dc=cisco,dc=com
changeType: modify
add: telephoneNumber
telephoneNumber: $Phone
" >> /etc/ldap/phones.ldif

done
~
~
```

•连接 ldap 用户之后记得允许用户登陆的时自动创建家目录：

```
pam-auth-update
```

六、 S2S VPN （UDP 500、4500； esp

protocol）：

1、wireguard:

apt install -y wireguard ncat

生成私钥公钥：
wg genkey > key1
cat key1 | wg pubkey > pub1
vim wg0
注意：预共享密钥是 presharedkey

```
[Interface]
ListenPort=51820
PrivateKey = yBouYqpNQvFPxw39YdgdRphT0pOCOyO5hl73mekXD1c=
Address = 10.255.255.1, fdab:cdef:fedc:abcd::1
#DNS = 8.8.8.8, 8.8.4.4, 1.1.1.1, 1.0.0.1

[Peer]
presharedkey = yTLnfqtSARjNOvkOjx9Y/tFEK+0CF5VO8xErgVDgN6U=
PublicKey = x0Yz/VvC2IK5lzqKktU+mjyDQ70VUa2Br1pEmQm4yyk=
Endpoint = 198.51.100.254:51820
AllowedIPs = 10.255.255.2, fdab:cdef:fedc:abcd::2, 172.30.0.0/24, fdab:cdef:ac:1e::/64

~
```

2、openvpn:

证书要有 serverAuth 和 clientAuth 字段
开启 ccd 配置，在后续能够配置 ccd
在服务端本地推送客户端路由，让服务端有路由能够访问客户端内网

```
155 client-config-dir ccd
156 route 172.16.1.0 255.255.255.0
```

还有 ccd 目录下的配置

```
iroute 172.16.1.0 255.255.255.0
~
```

iroute　//它告诉 OpenVPN 服务器：“如果你想访问客户端 172.16.1.0/24 这个网段，请把数据包发送给当前这个客户端（client）

给客户端 push 路由，让它有路由能够访问服务端的内网：

```
141 push "route 192.168.1.0 255.255.255.0"
```

3、strongswan：

证书字段：
证书 1:vpn1.crt：CN=fw01.shanghai.cn，SAN DNS=fw01.shanghai.cn
证书 2:vpn2.crt：CN=fw02.shenzhen.cn，SAN DNS=fw02.shenzhen.cn
apt install -y strongswan libstrongswan-extra-plugins
将证书、私钥复制到对应路径：
cp ca.crt /etc/swanctl/x509ca
cp vpn1.crt vpn2.crt /etc/swanctl/x509
cp vpn1.key vpn2.key /etc/swanctl/private

配置 strongswan：
vim /etc/swanctl/swanctl.conf
注意 local 和 remote 需要分别指定不同的证书

```
# Section defining IKE connection configurations.
connections {

    # Section for an IKE connection named <conn>.
    ikev2 {

        # IKE major version to use for connection.
        version = 2

        # Local address(es) to use for IKE communication,
        local_addrs = 1.1.1.1

        # Remote address(es) to use for IKE communication,
        remote_addrs = 2.2.2.1

        # Local UDP port for IKE communication.
        # local_port = 500
```

```
109         # Section for a local authentication round.
110         local<suffix> {
111
112             # Optional numeric identifier by which au
113             # sorted.  If not specified rounds are or
114             # the config file/VICI message.
115             # round = 0
116
117             # Comma separated list of certificate car
118             # authentication.
119             certs = vpn1.crt
120
121             # Section for a certificate candidate to
122             # cert<suffix> =
123
124             # Comma separated list of raw public key
125             # authentication.
126             # pubkeys =
127
128             # Authentication to perform locally (pubk
129             # eap[-method]).
130             auth = pubkey
131
132             # IKE identity to use for authentication
133             id = 1.1.1.1
134
135             # Client EAP-Identity to use in EAP-Ident
136             # method.
```

```
160
161         }
162
```

```
164         remote<suffix> {
165
166             # Optional numeric identifier by which authentication rounds
167             # sorted.  If not specified rounds are ordered by their posit
168             # the config file/VICI message.
169             # round = 0
170
171             # IKE identity to expect for authentication round.
172             id = 2.2.2.1
173
174             # Identity to use as peer identity during EAP authentication.
175             # eap_id = id
176
177             # Authorization group memberships to require.
178             # groups =
179
180             # Certificate policy OIDs the peer's certificate must have.
181             # cert_policy =
182
183             # Comma separated list of certificate to accept for authentic
184             certs = vpn2.crt
185
186             # Section for a certificate to accept for authentication.
187             # cert<suffix> =
188
189             # Comma separated list of CA certificates to accept for
190             # authentication.
191             # cacerts =
192
193             # Section for a CA certificate to accept for authentication.
194             # cacert<suffix> =
195
196             # Identity in CA certificate to accept for authentication.
197             # ca_id =
198
199             # Comma separated list of raw public keys to accept for
200             # authentication.
201             # pubkeys =
202
203             # Certificate revocation policy, (strict, ifuri or relaxed).
204             # revocation = relaxed
205
206             # Authentication to expect from remote (pubkey, psk, xauth[-b
207             # or eap[-method]).
208             auth = pubkey
209
```

```
243         }
244
```

```
245         children {
246
247             # CHILD_SA configuration sub-section.
248             net {
249
250                 # AH proposals to offer for the CHI
251                 # ah_proposals =
252
253                 # ESP proposals to offer for the CH
254                 # esp_proposals = default
255
256                 # Use incorrect 96-bit truncation f
257                 # sha256_96 = no
258
259                 # Local traffic selectors to includ
260                 local_ts = 172.16.100.0/24
261
262                 # Remote selectors to include in CH
263                 remote_ts = 3.3.3.0/24
264
```

```
387
388             }
389
390         }
391
392     }
393
394 }
395
```

指定私钥文件名

```
398 secrets {
399
```

```
450     private<suffix> {
451
452         # File name in the priva
453         # used.
454         file = vpn1.key
455
456         # Value of decryption pa
457         # secret =
458
459     }
460 }
461     # Private key decryption pas
```

```
swanctl --load-all
```

•配置自动发起连接：

```
vim /etc/swanctl/swanctl.conf
# 主要是 start_action 这一条就是
```

```
309
310                 # Action to perform on DPD timeout (clear, trap or restart).
311                 dpd_action = restart
312
```

```
379
380                 # Action to perform after loading the configuration (none, trap,
381                 # start).
382                 start_action = start
383
384                 # Action to perform after a CHILD_SA gets closed (none, trap,
385                 # start).
386                 close_action = start
387
```

七、Web（TCP 80、443）：

1、Apache2：

•301 重定向保留 URI：

vim /etc/apache2/sites-enabled/000-default.conf

要在最后加 /

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        redirect 301 / https://www.shanghai.org/

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

```

•虚拟目录（别名）：

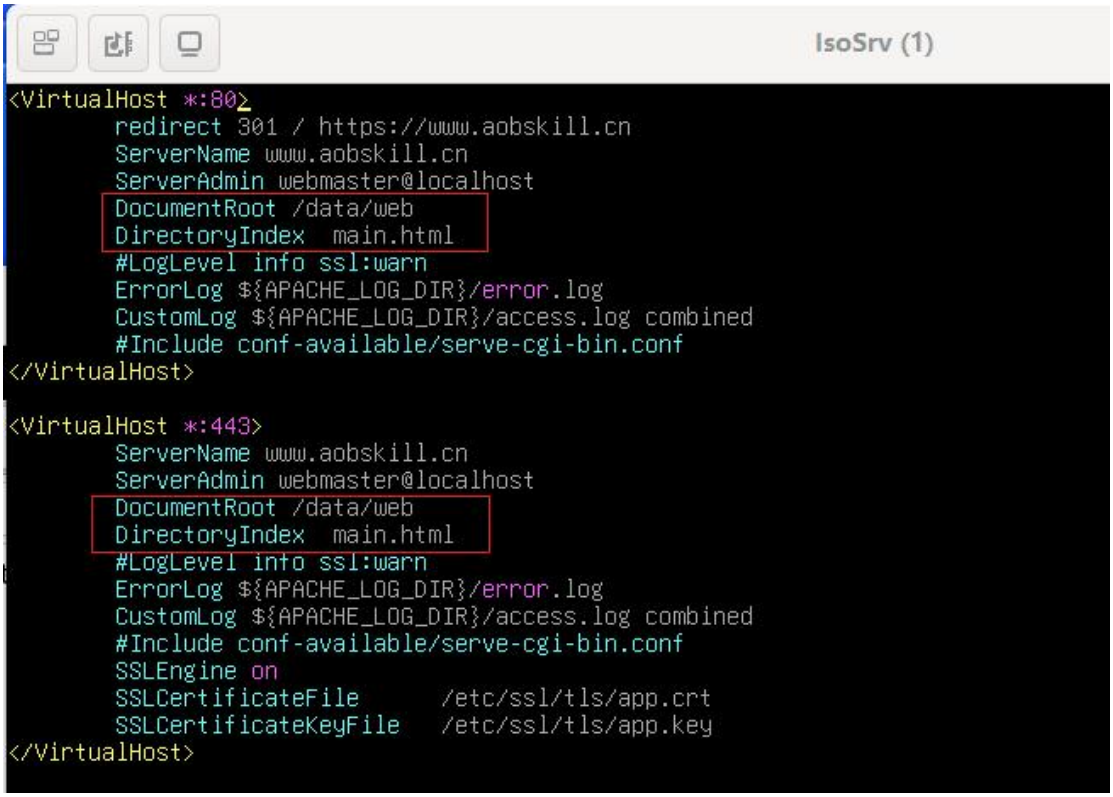
直接访问 /whoami 就能访问到 /opt/wwwroot/whoami.html 文件
末尾不会有斜杠

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.

        ServerAdmin webmaster@localhost
DocumentRoot /opt/wwwroot

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
directoryindex main.html
Alias /whoami /opt/wwwroot/whoami.html

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
~
```

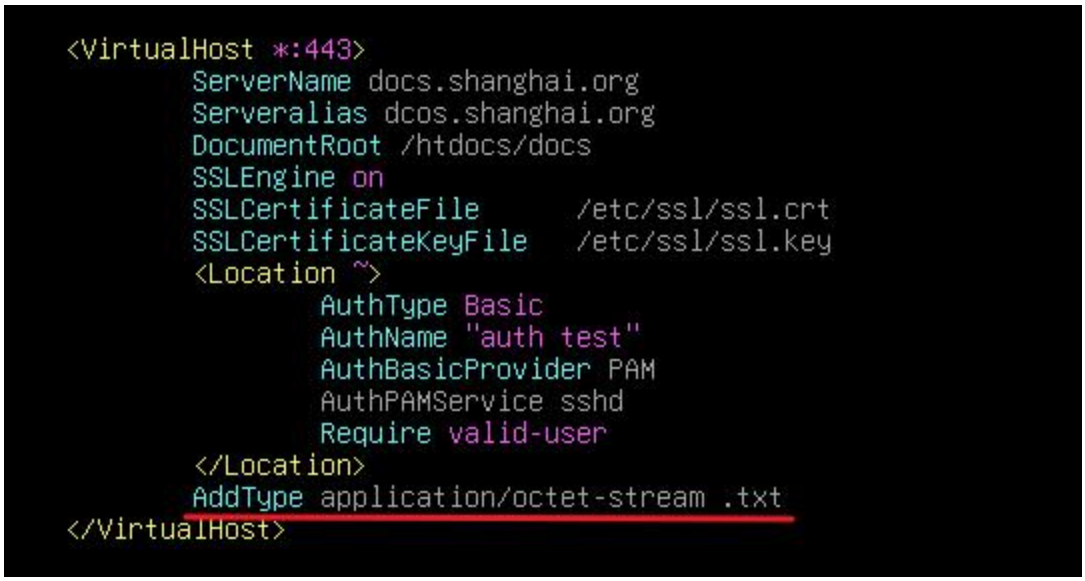
当客户端访问 [uri]/whoami 时，就会返回这个 whoami.html 文件

```
root@Server1:/opt/ansible# curl 192.168.10.3/whoami
Server3
root@Server1:/opt/ansible# _
```

•指定默认页面文件：



•对指定文件类型强制下载：



•仅支持 IPv6/IPv4：

仅 IPv6：

```
# If you just change the port or add more ports here,
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen [2001:db8:1001:20::15]:80

<IfModule ssl_module>
        Listen [2001:db8:1001:20::15]:443
</IfModule>

<IfModule mod_gnutls.c>
        Listen [2001:db8:1001:20::15]:443
</IfModule>
~
```

仅 IPv4：

```
# If you just change the port or add more ports her
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 0.0.0.0:80

<IfModule ssl_module>
        Listen 0.0.0.0:443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 0.0.0.0:443
</IfModule>
~
```

•开启 目录浏览（默认开启）：

```
# your system is serving content from a sub-directo
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

#<Directory /srv/>
```

•身份认证：

•Basic：

```
htpasswd -cB /etc/apache2/.htpasswd user01
htpasswd -B /etc/apache2/.htpasswd user02
-c  //创建新文件
-B  //（可选）密码加密算法
```

```
<VirtualHost *:80>
        ServerName www.up02.com
        DocumentRoot /up02
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        <Directory /up02>
                Options Indexes FollowSymLinks
                AuthName "Please enter your username and password"
                AuthType Basic
                AuthUserfile /etc/apache2/.htpasswd
                Require valid-user
        </Directory>
</VirtualHost>

<VirtualHost *:443>
        ServerName www.up01.com
        DocumentRoot /up01
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile      /etc/ssl/tls/newcert.pem
        SSLCertificateKeyFile   /etc/ssl/tls/newkey.pem
</VirtualHost>
~
~
```

用于页面用户身份认证

•PAM 本地认证：

```
apt install -y libapache2-mod-authnz-pam
# 或者用 Directory 直接指定网页根目录
```

```
<VirtualHost *:443>
        ServerName docs.shanghai.org
        Serveralias dcos.shanghai.org
        DocumentRoot /htdocs/docs
        SSLEngine on
        SSLCertificateFile      /etc/ssl/ssl.crt
        SSLCertificateKeyFile   /etc/ssl/ssl.key
        <Location ~>
                AuthType Basic
                AuthName "auth test"
                AuthBasicProvider PAM
                AuthPAMService sshd
                Require valid-user
        </Location>
</VirtualHost>
```

•LDAP:

a2enmod authnz_ldap
a2enmod ldap

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        <Directory "/var/www/html">
                AuthName "Enter your Username and Password"
                AuthType Basic
                AuthBasicProvider ldap
                AuthLDAPURL ldap://ldap.lyon2024.fr/dc=lyon2024,dc=fr
                AuthLDAPBINDDN  cn=admin,dc=lyon2024,dc=fr
                AuthLDAPBindPassword Skills39
                require valid-user
        </Directory>
</VirtualHost>
~
~
```

•仅允许某个网段认证:

使用 require：
要求 192.168.1.0/24 网段进行身份认证：
Require ip 192.168.1.0/24

要求 192.168.1.0/24、172.16.1.0/24 网段、123.1.1.1 机器进行身份认证：
并列写多个即可
Require ip 192.168.1.0/24
Require ip 172.16.1.0/24
Require ip 123.1.1.1

排除某个网段、IP：

```
Require not ip 192.168.1.0/24
```

•WebDAV:

```
# 注意要开放 WebDAV 根目录读写权限
mkdir /var/www/html/webdav
chmod 777 /var/www/html/webdav

a2enmod dav
a2enmod dav_fs

htpasswd -c .htpasswd admin
```

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn
        Alias /webdav /var/www/html/webdav

        <Directory /var/www/html/webdav>
                DAV on
                AuthType Basic
                AuthName "WebDAV"
                AuthUserFile /etc/apache2/.htpasswd
                Require valid-user
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
~
~
```

•拒绝使用 IP 地址访问:

```
33 <VirtualHost *:80>
34     ServerName 10.0.220.101
35     <Location />
36         Require all denied
37     </Location>
38 </VirtualHost>
39
40 <VirtualHost *:443>
41     ServerName 10.0.220.101
42     <Location />
43         Require all denied
44     </Location>
45 </VirtualHost>
:q
```

•添加 Header：

a2enmod headers

```
<VirtualHost *:8080>
        # The ServerName directive sets the request scheme, hostname and
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerNa
        # specifies what hostname must appear in the request's Host: head
        # match this virtual host. For the default virtual host (this fil
        # value is not decisive as it is used as a last resort host regar
        # However, you must set it for any further virtual host explicitl
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        #DocumentRoot /var/www/html
        DocumentRoot /var/www/shared

Header always set X-WSC48-Stage "A-Linux"

<Directory /var/www/shared/app/>
    directoryindex info.php
</Directory>


<Directory "/var/www/shared/secure/">
    AuthName "ldap"
    AuthType Basic
    AuthBasicProvider ldap
    AuthLDAPURL ldaps://ldap.wsc48.lan/ou=People,dc=wsc48,dc=lan
    AuthLDAPBindDN "cn=admin,dc=wsc48,dc=lan"
    AuthLDAPBindPassword "Skill39@2026"
```

请求头：

作为代理服务器传给后端 Web 时需要配置

requestheader set X-Test "abc"

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        requestheader set X-Test "abc"
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

•自定义错误页面：

vim /etc/apache2/apache2.conf

这个路径是 Web 根路径，404 文件放到 web 根目录即可

```
# Customizable error responses come in three flavors:
# 1) plain text
# 2) local redirects
# 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /opt/wwwroot/404.html
#ErrorDocument 404 /opt/wwwroot/404.html
ErrorDocument 404 /404.html
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
```

•（mTLS）客户端证书身份认证：

```
<VirtualHost *:80>
        #ServerName www.example.com
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:443>
        #ServerName www.example.com
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        SSLEngine on
        SSLCertificateFile      /etc/ssl/ext.crt
        SSLCertificateKeyFile   /etc/ssl/ext.key

        SSLCACertificateFile    /etc/ssl/ca.crt
        SSLVerifyClient require
        SSLVerifyDepth  2

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

在 /usr/share/doc/apache2/下有配置摘抄：

grep -r SSLVerify /usr/share/doc/apache2/examples/*

```
root@R-SRV:~# grep -r SSLVerify /usr/share/doc/apache2/examples/*
/usr/share/doc/apache2/examples/apache2/extra/httpd-ssl.conf:#SSLVerifyClient require
/usr/share/doc/apache2/examples/apache2/extra/httpd-ssl.conf:#SSLVerifyDepth  10
root@R-SRV:~# _
```

合成证书为 pkcs12 给客户端：

openssl pkcs12 -export -out client.p12 -in skill39.crt -inkey skill39.key -certfile ca.crt

•mTLS 在子目录下：

禁用 TLS 1.3：

```
209 # Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
210 # Use mod_remoteip instead.
211 #
212 LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\""
213 LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combir
214 LogFormat "%h %l %u %t \"%r\" %>s %O" common
215 LogFormat "%{Referer}i -> %U" referer
216 LogFormat "%{User-agent}i" agent
217
218 # Include of directories ignores editors' and dpkg's backup files,
219 # see README.Debian for details.
220
221 # Include generic snippets of statements
222 IncludeOptional conf-enabled/*.conf
223
224 SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 -TLSv1.3
225 # Include the virtual host configurations:
226 IncludeOptional sites-enabled/*.conf
```

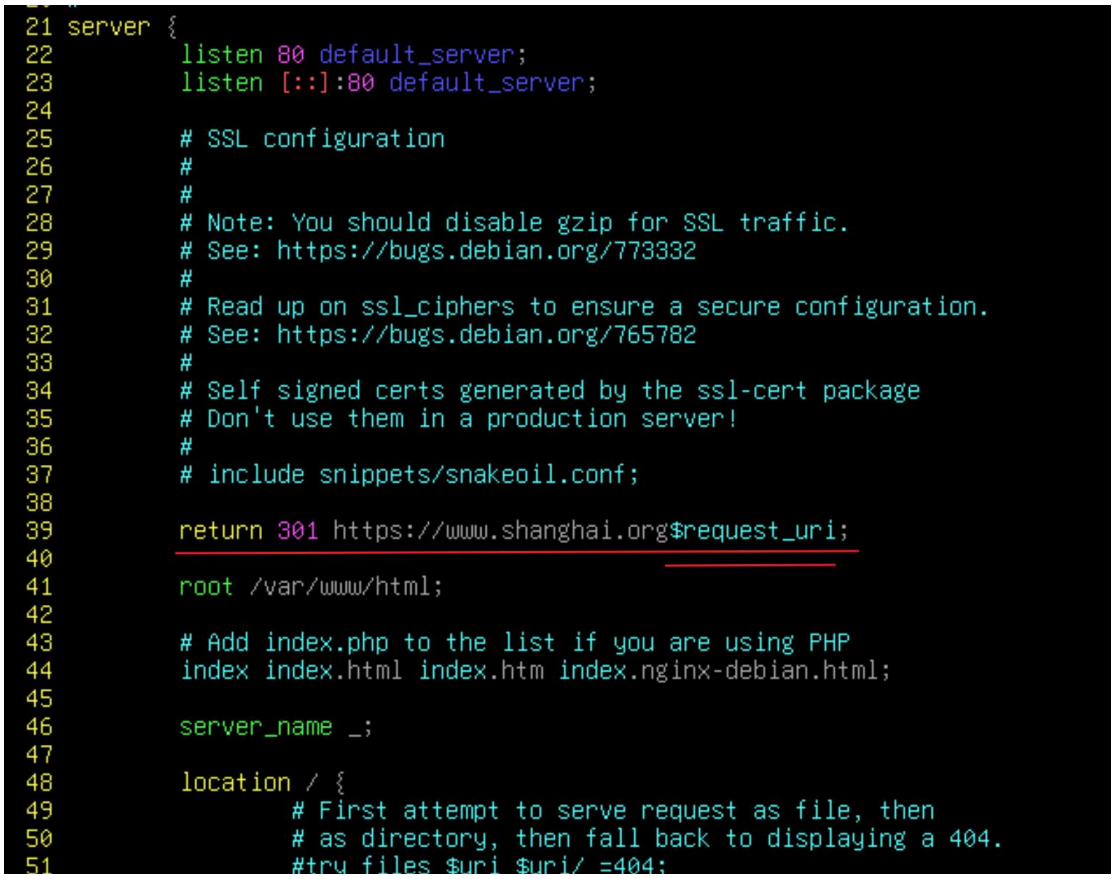
模板在：/etc/apache2/mods-available/ssl.conf 中：

```
 59 # SSL server cipher order preference:
 60 # Use server priorities for cipher algorithm choice.
 61 # Clients may prefer lower grade encryption.  You should enable this
 62 # option if you want to enforce stronger encryption, and can afford
 63 # the CPU cost, and did not override SSLCipherSuite in a way that puts
 64 # insecure ciphers first.
 65 # Default: Off
 66 #SSLHonorCipherOrder on
 67
 68 #   The protocols to enable.
 69 #   Available values: all, SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
 70 #   SSL v2  is no longer supported
 71 SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
 72
 73 #   Allow insecure renegotiation with clients which do not yet suppor
 74 #   secure renegotiation protocol. Default: Off
 75 #SSLInsecureRenegotiation on
 76
```

```
<VirtualHost *:443>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName www.wsc2024.fr

        SSLEngine on
        SSLCertificateFile      /etc/ssl/ssl.crt
        SSLCertificateKeyFile   /etc/ssl/ssl.key
        SSLCACertificateFile /etc/ssl/cert.crt
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

<Directory /var/www/managers>
SSLVerifyClient require
SSLVerifyDepth  10
</Directory>

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

2、Nginx：

•301 重定向保留 URI：



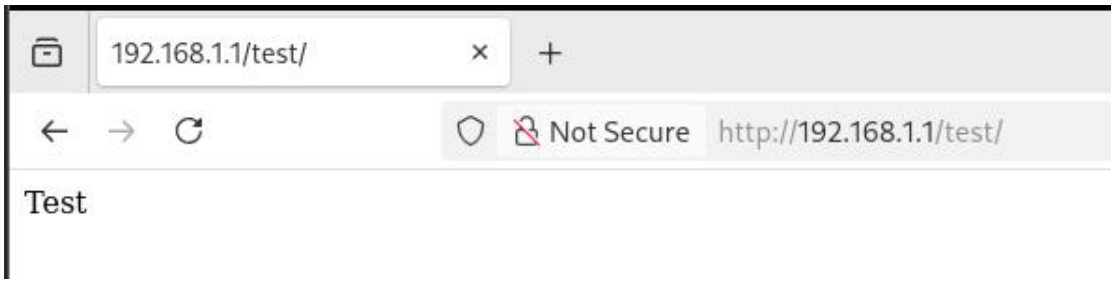
```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        return 301 https://www.shanghai.org$request_uri;

        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                #try_files $uri $uri/ =404;
```

•虚拟目录（别名）：

•末尾带斜杠 /：

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        error_page 404 /404.html;
        root /opt/wwwroot;

        # Add index.php to the list if you are using PHP
        index main.html index.html index.htm index.nginx-debian.html;

        server_name _;

        location /whoami {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                #try_files $uri $uri/ =404;
                alias /opt/wwwroot;
                index whoami.html;
        }

        # pass PHP scripts to FastCGI server
        #
        #location ~ \.php$ {
        #       include snippets/fastcgi-php.conf;
        #
:x
```

这个会在末尾自动加斜杠

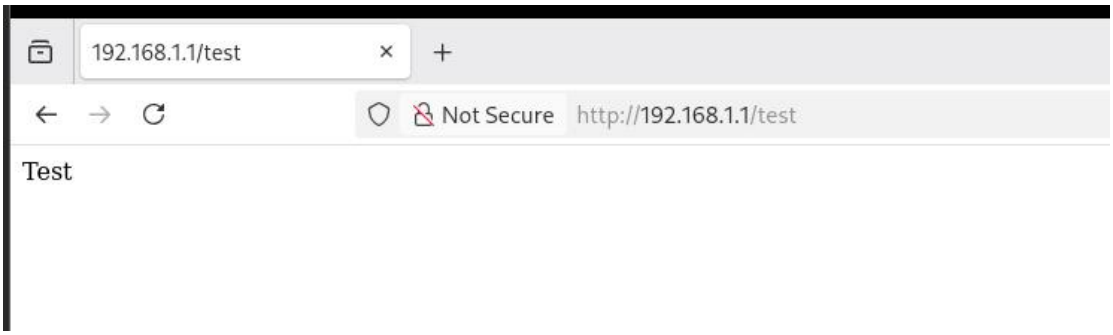


•末尾不带斜杠：

直接指定文件（文件名不必须是 index）
需要加上 default_type text/html；否则会直接下载

```
21 server {
22         listen 80 default_server;
23         listen [::]:80 default_server;
24
25         # SSL configuration
26         #
27         # listen 443 ssl default_server;
28         # listen [::]:443 ssl default_server;
29         #
30         # Note: You should disable gzip for SSL traffic.
31         # See: https://bugs.debian.org/773332
32         #
33         # Read up on ssl_ciphers to ensure a secure configuration.
34         # See: https://bugs.debian.org/765782
35         #
36         # Self signed certs generated by the ssl-cert package
37         # Don't use them in a production server!
38         #
39         # include snippets/snakeoil.conf;
40
41         root /var/www/html;
42
43         # Add index.php to the list if you are using PHP
44         index index.html index.htm index.nginx-debian.html;
45
46         server_name _;
47
48         location /test {
49                 # First attempt to serve request as file, then
50                 # as directory, then fall back to displaying a 404.
51                 #try_files $uri $uri/ =404;
52                 alias /var/www/nginx/main.html;
53                 default_type text/html;
54         }
55
56         # pass PHP scripts to FastCGI server
57         #
58         #location ~ \.php$ {
```

这个不会在末尾加斜杠，但是访问加斜杠的路径会报错



•指定默认页面文件：

在这里指定

```
20 #
21 server {
22         listen 80 default_server;
23         listen [::]:80 default_server;
24
25         # SSL configuration
26         #
27         # listen 443 ssl default_server;
28         # listen [::]:443 ssl default_server;
29         #
30         # Note: You should disable gzip for SSL traffic.
31         # See: https://bugs.debian.org/773332
32         #
33         # Read up on ssl_ciphers to ensure a secure configuration.
34         # See: https://bugs.debian.org/765782
35         #
36         # Self signed certs generated by the ssl-cert package
37         # Don't use them in a production server!
38         #
39         # include snippets/snakeoil.conf;
40
41         root /var/www/html;
42
43         # Add index.php to the list if you are using PHP
44         index index.html index.htm index.nginx-debian.html;
45
46         server_name _;
47
48         location /test {
49                 # First attempt to serve request as file, then
50                 # as directory, then fall back to displaying a 404.
51                 #try_files $uri $uri/ =404;
52                 alias /var/www/nginx/;
53                 #default_type text/html;
54         }
55
```

•对指定文件类型强制下载：

```
#
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        location ~* \.(pdf|zip|docx|xlsx)$ {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                #try_files $uri $uri/ =404;
                add_header Content-Disposition "attachment";
        }
```

•仅支持 IPv6/IPv4：

仅 IPv4：

```
#
server {
        listen 80 default_server;
        #listen [::]:80 default_server;

        # SSL configuration
```

仅 IPv6：

```
server {
        #listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        # listen 443 ssl default_server;
```

```
root@debian:/etc/nginx/sites-enabled# curl 127.0.0.1 -I
curl: (7) Failed to connect to 127.0.0.1 port 80 after 0 ms: Could not connect to server
root@debian:/etc/nginx/sites-enabled# curl [::1] -I
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 15 Sep 2026 06:45:08 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Tue, 15 Sep 2026 06:18:44 GMT
Connection: keep-alive
ETag: "6aa8e344-267"
Accept-Ranges: bytes

root@debian:/etc/nginx/sites-enabled# _
```

•开启 目录浏览：

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configurati
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        autoindex on;
        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;
```

•身份认证：

•Basic：

```
htpasswd -c /etc/nginx/.htpasswd user1
htpasswd /etc/nginx/.htpasswd user2
```

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        root /var/www/html;
        index index.html index.htm index.nginx-debian.html;
        server_name _;
        location / {
                auth_basic "authentication";
                auth_basic_user_file /etc/nginx/.htpasswd;
        }
}
```

•PAM：

apt install -y libnginx-mod-http-auth-pam

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        root /var/www/html;
        index index.html index.htm index.nginx-debian.html;
        server_name _;
        location / {
                auth_pam "pam_authentication";
                auth_pam_service_name "nginx";
        }
}
```

•LDAP（PAM）：

就是用上面 PAM 的方式，然后本地连接 nslcd 即可

•拒绝使用 IP 地址访问：

单独定义 Virtual，然后其他域名、IP 都放到 default_server 然后拒绝即可
444 是直接断开连接（nginx 专有）

```nginx
server {
    listen 80;
    listen [::]:80;

    server_name www.shanghai.org;
    root /var/www/html;
}

server {
    listen 80 default_server;
    listen [::]:80 default_server;

    server_name _;
    return 444;
}
```

•**添加 Header**:

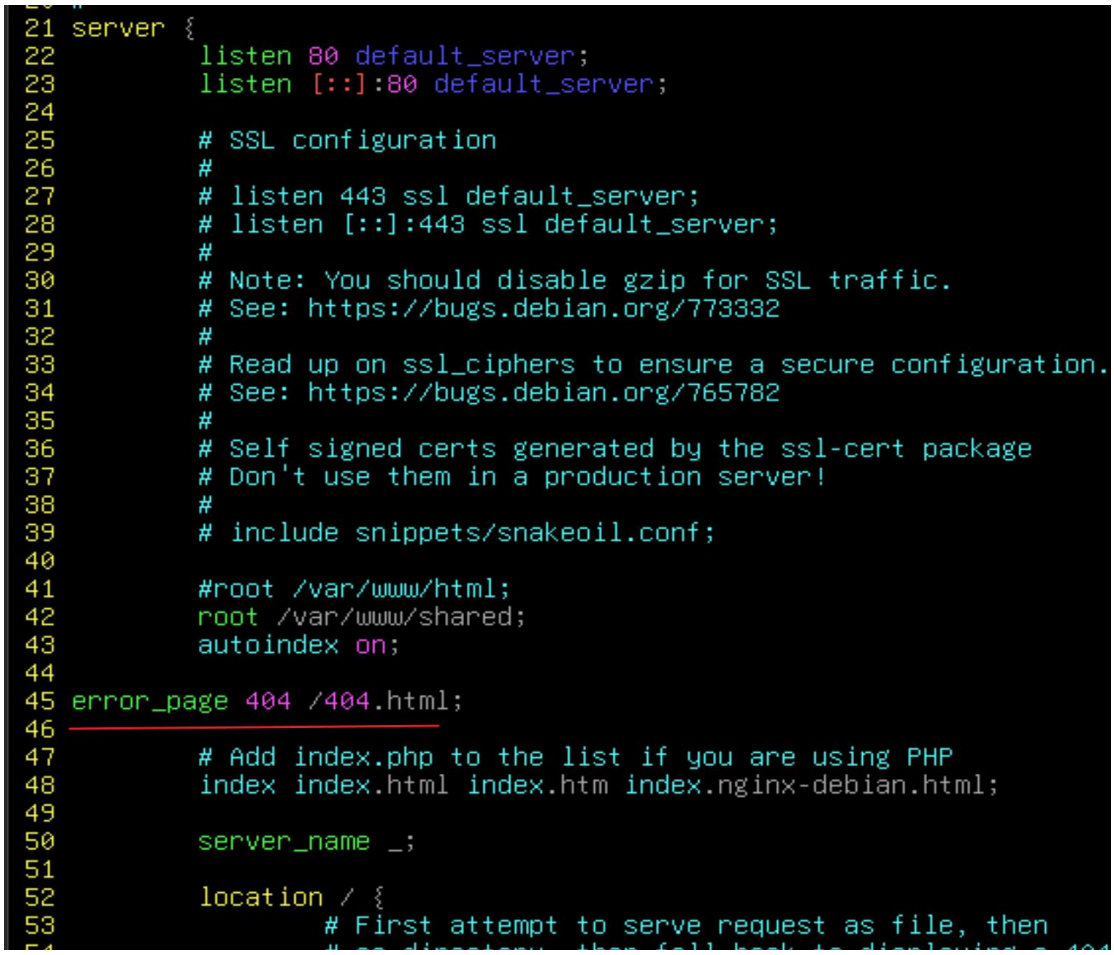
```
server {
        listen 80;
        listen [::]:80;

        root /central/website/www;
        index index.php;

        server_name www.cloud.com;

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php8.4-fpm.sock;
        }

        location / {
                try_files $uri $uri/ =404;
        }

        access_log /var/log/nginx/public.log;
        error_log /var/log/nginx/public_err.log;
        add_header X-Served-By $hostname always;
}

server {
        listen 80;
        listen [::]:80;

        root /central/website/ca;
        autoindex on;

        server_name subca.cloud.com;

        location / {
                try_files $uri $uri/ =404;
        }
}
~
```

•添加 request header：

```
# 用于反向代理：
proxy_set_header X-Test "WSC2026";
```

•自定义错误页面：

```
# 这个路径是 Web 根路径，404 文件放到 web 根目录即可
```



```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        # SSL configuration
        #
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        #
        # Note: You should disable gzip for SSL traffic.
        # See: https://bugs.debian.org/773332
        #
        # Read up on ssl_ciphers to ensure a secure configuration.
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        #root /var/www/html;
        root /var/www/shared;
        autoindex on;

error_page 404 /404.html;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
```

- **（mTLS）客户端证书身份认证：**

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        # listen 443 ssl default_server;
        # listen [::]:443 ssl default_server;
        root /var/www/html;
        index index.html index.htm index.nginx-debian.html;
        server_name _;
        location / {
                try_files $uri $uri/ =404;
        }
}

server {
        listen 443 ssl default_server;
        listen [::]:443 ssl default_server;
        root /var/www/html;
        index index.html index.htm index.nginx-debian.html;
        server_name _;
        ssl on;
        ssl_certificate /etc/ssl/ext.crt;
        ssl_certificate_key /etc/ssl/ext.key;

        ssl_client_certificate /etc/ssl/ca.crt;
        ssl_verify_client on;

        location / {
                try_files $uri $uri/ =404;
        }
}
~
~
```

合成证书为 pkcs12 给客户端：
openssl pkcs12 -export -out client.p12 -in skill39.crt -inkey skill39.key -certfile ca.crt

•mTLS 放在子目录下：

```
101         server_name _;
102
103         location / {
104                 # First attempt to serve request as file, then
105                 # as directory, then fall back to displaying a 40
106                 try_files $uri $uri/ =404;
107         }
108
109         ssl_verify_client optional;
110         location /secure {
111                 #alias /var/www/html/secure;
112                 #ssl_verify_client on;
113                 if ($ssl_client_verify != SUCCESS) {
114                         return 403;
115                 }
116
117         }
118         # pass PHP scripts to FastCGI server
```

八、Proxy（TCP 80、443、3128）：

1、Haproxy：

•ACL：

use_backend www1 if { hdr_beg(host) -i web1 }　//以 web1 开头的域名
use_backend www1 if { hdr(host) -i web1.wsc2026.org }　//匹配 web1.wsc2026.org 域名
use_backend api if { path_beg /api }　//匹配指定的 URI（不论是否有斜杠）

•调度算法：

balance roundrobin　//（默认算法）权重轮询，将请求按顺序分配给后端服务器，可以手动调整权重，默认所有后端服务器权重一样，可以在运行中通过 Runtime API/stats socket 调整权重，roundrobin 可以动态生效
balance static-rr　//也是权重轮询，但是是静态算法，手动指定好之后，就不能在运行时更改了
balance leastconn　//最少连接，将新连接分配给当前连接数最少的后端服务器
balance first　//优先使用第一台服务器，优先把连接发给编号最小、排在最前面的服务器，只有这台服务器达到 maxconn（最大连接数，可以自定义）后，才使用下一台
balance source　//源 IP 哈希模式，根据客户端源 IP 做 hash，让同一个客户端 IP 尽量固定到同一台后端服务器
balance uri　//根据 HTTP URI 做 hash，

•TCP 代理：

•代理 ftp、ftp 被动端口：

将 mode 设置为 mode tcp 即可

```
67
68 #frontend ftp
69 #        bind            *:21
70 #       bind            *:40000-40099
71 #       mode            tcp
72 #       option          tcplog
73 #       log             global
74 #       default_backend ftp1
75 #
76 #backend ftp1
77 #       mode            tcp
78 #       balance         leastconn
79 #       stick-table     type ip size 100k expire 1h
80 #       stick           on src
81 #       server ftphost1 172.16.1.1 check port 21
82 #       server ftphost2 172.16.1.2 check port 21
83
```

•添加头部信息：

```
defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        timeout connect 5000
        timeout client  50000
        timeout server  50000
        errorfile 400 /etc/haproxy/errors/400.http
        errorfile 403 /etc/haproxy/errors/403.http
        errorfile 408 /etc/haproxy/errors/408.http
        errorfile 500 /etc/haproxy/errors/500.http
        errorfile 502 /etc/haproxy/errors/502.http
        errorfile 503 /etc/haproxy/errors/503.http
        errorfile 504 /etc/haproxy/errors/504.http

frontend public
        bind            *:80
                                    添加头部信息
        http-response add-header via-proxy ha-prx01

        bind            *:443 ssl crt /etc/haproxy/ssl.pem
        http-request redirect scheme https code 301 if !{ ssl_fc }
        default_backend static
                                    301重定向
backend static
        mode            http
        balance         roundrobin
        server          statsrv1 10.1.20.31:80 check
        server          statsrv2 10.1.20.32:80 check


~
~
```

```
root@GW1:/usr/share/doc/haproxy/examples# grep -r header ./*
./basic-config-edge.cfg:        http-after-response set-header Strict-Transport-Security "
./basic-config-edge.cfg:        http-request del-header x-forwarded-for
./basic-config-edge.cfg:        process-vary on           # handle the Vary header (otherw
./wurfl-example.cfg:    # list of WURFL capabilities, virtual capabilities, property names
./wurfl-example.cfg:    # inject a header called X-Wurfl-All with all the WURFL informatio
./wurfl-example.cfg:    http-request set-header X-Wurfl-All %[wurfl-get-all()]
./wurfl-example.cfg:    # inject a header called X-WURFL-PROPERTIES with the "wurfl_id" in
./wurfl-example.cfg:    #http-request set-header X-WURFL-PROPERTIES %[wurfl-get(wurfl_id)]
root@GW1:/usr/share/doc/haproxy/examples# grep -r http- ./*
./basic-config-edge.cfg:        timeout http-keep-alive 2m
./basic-config-edge.cfg:        http-after-response set-header Strict-Transport-Security "
./basic-config-edge.cfg:        http-request redirect scheme https code 301 if !{ ssl_fc }
./basic-config-edge.cfg:        option http-ignore-probes
./basic-config-edge.cfg:        http-request del-header x-forwarded-for
./basic-config-edge.cfg:        http-request  cache-use cache
./basic-config-edge.cfg:        http-response cache-store cache
./basic-config-edge.cfg:        http-check send meth GET uri / ver HTTP/1.1 hdr host svc1.
./option-http_proxy.cfg:        http-request deny if !allow_host
./option-http_proxy.cfg:        http-request deny if forbidden_dst
./option-http_proxy.cfg:        http-request deny if !valid_method
./option-http_proxy.cfg:        http-request set-dst url_ip
./option-http_proxy.cfg:        http-request set-dst-port url_port
./option-http_proxy.cfg:        http-request set-uri %[pathq]
./option-http_proxy.cfg:        http-response deny if { res.hdr(content-type) audio/mp3 }
./wurfl-example.cfg:    http-request set-header X-Wurfl-All %[wurfl-get-all()]
./wurfl-example.cfg:    #http-request set-header X-WURFL-PROPERTIES %[wurfl-get(wurfl_id)]
root@GW1:/usr/share/doc/haproxy/examples# _
```

•mTLS:

```
frontend public
        bind      *:80 #name clear
        bind      *:443 ssl crt /etc/haproxy/haproxy.pem ca-file /etc/ssl/ca.crt verify required
        mode      http
        #http-request deny unless { ssl_c_used }
        #http-request deny unless { ssl_c_verify 0 }
        #log             global
        #option          httplog
        #option          dontlognull
        #monitor-uri     /monitoruri
        #maxconn         8000
        #timeout client  30s

        #stats uri       /admin/stats
        #use_backend     static if { hdr_beg(host) -i img }
        #use_backend     static if { path_beg /img /css   }
        default_backend static

# The static backend backend for 'Host: img', /img and /css.
backend static
        mode            http
        balance         roundrobin
        option prefer-last-server
        retries         2
        option redispatch
        timeout connect 5s
        timeout server  5s
        option httpchk  HEAD /favicon.ico
        server          statsrv1 192.168.20.10:8088 #check inter 1000
```

合成证书为 pkcs12 给客户端：

openssl pkcs12 -export -out client.p12 -in skill39.crt -inkey skill39.key -certfile ca.crt

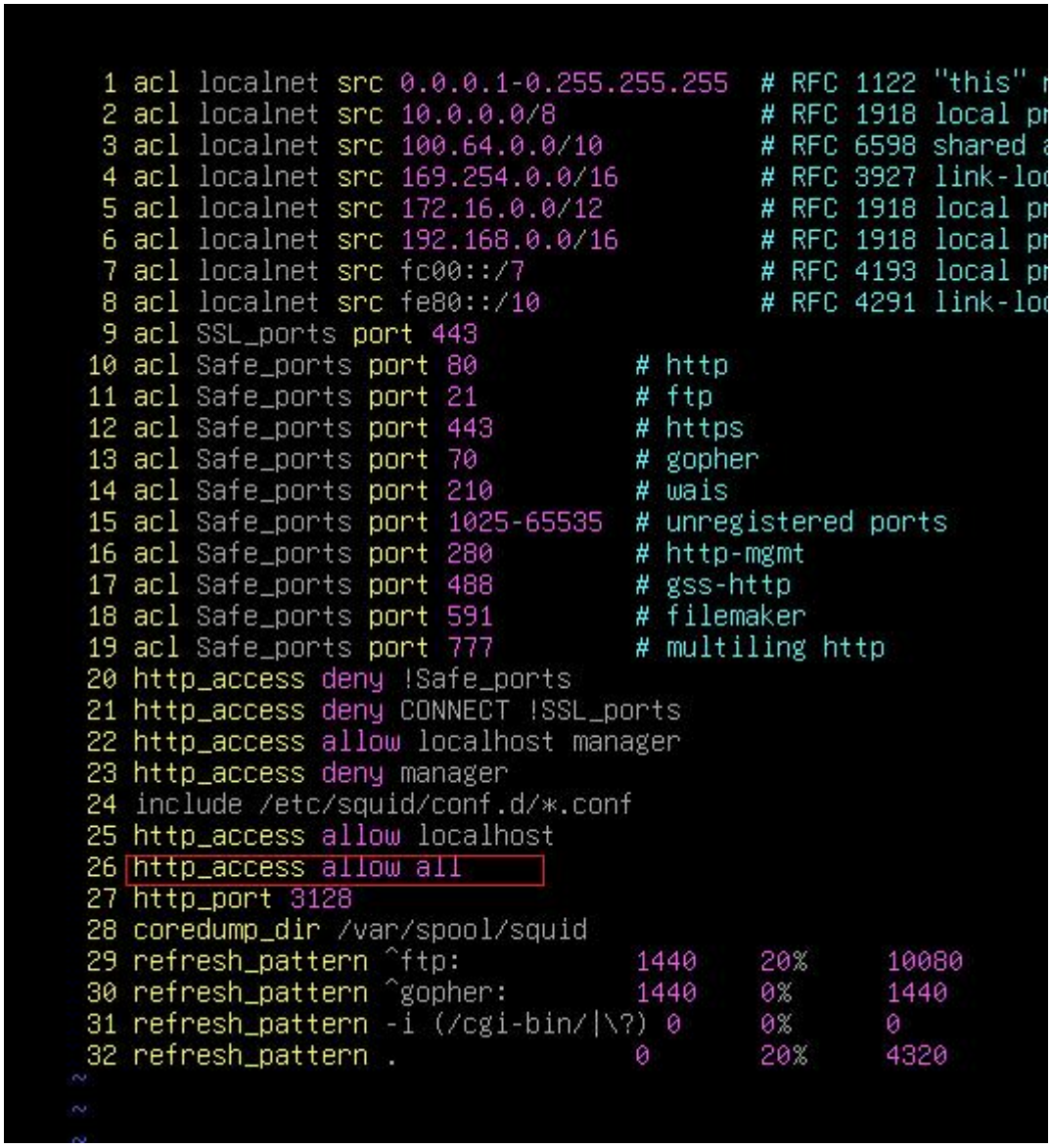
2、Squid（能透明代理）：

•过滤配置，生成配置文件：

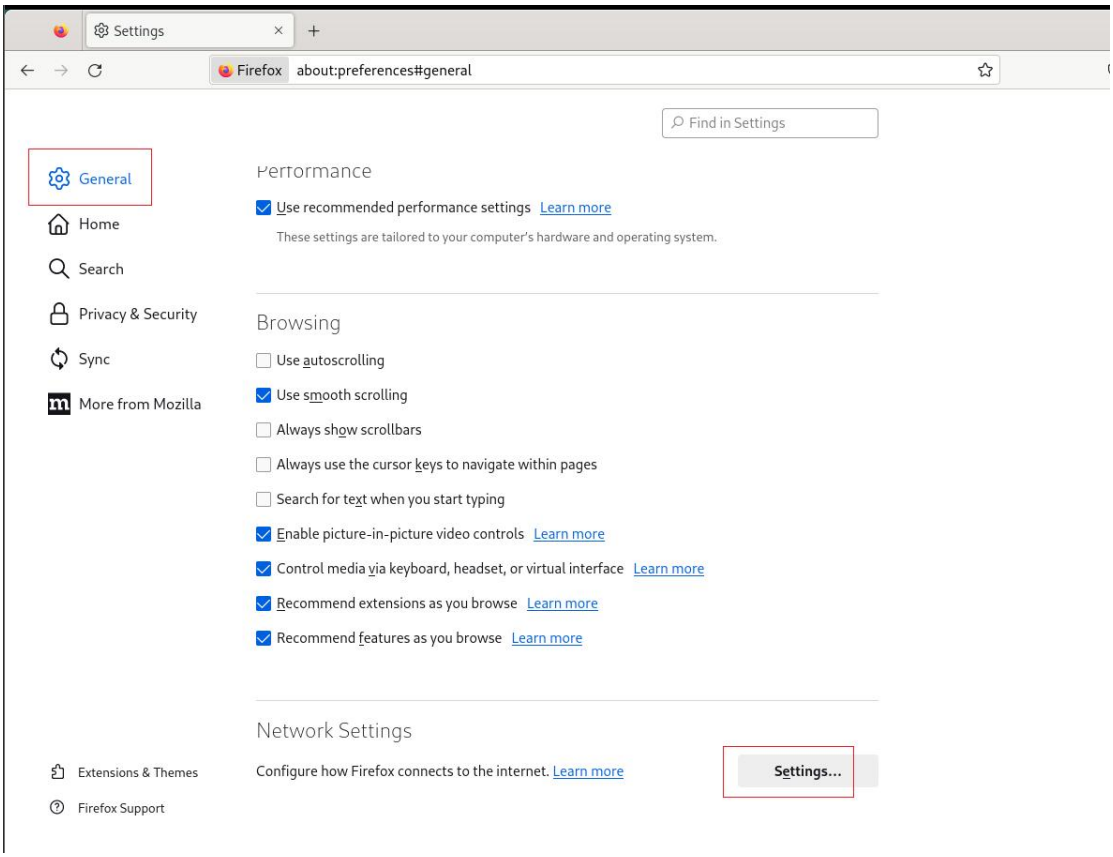
```
cp squid.conf squid.conf.bak
egrep -v "^#|^$" squid.conf.bak > squid.conf
```

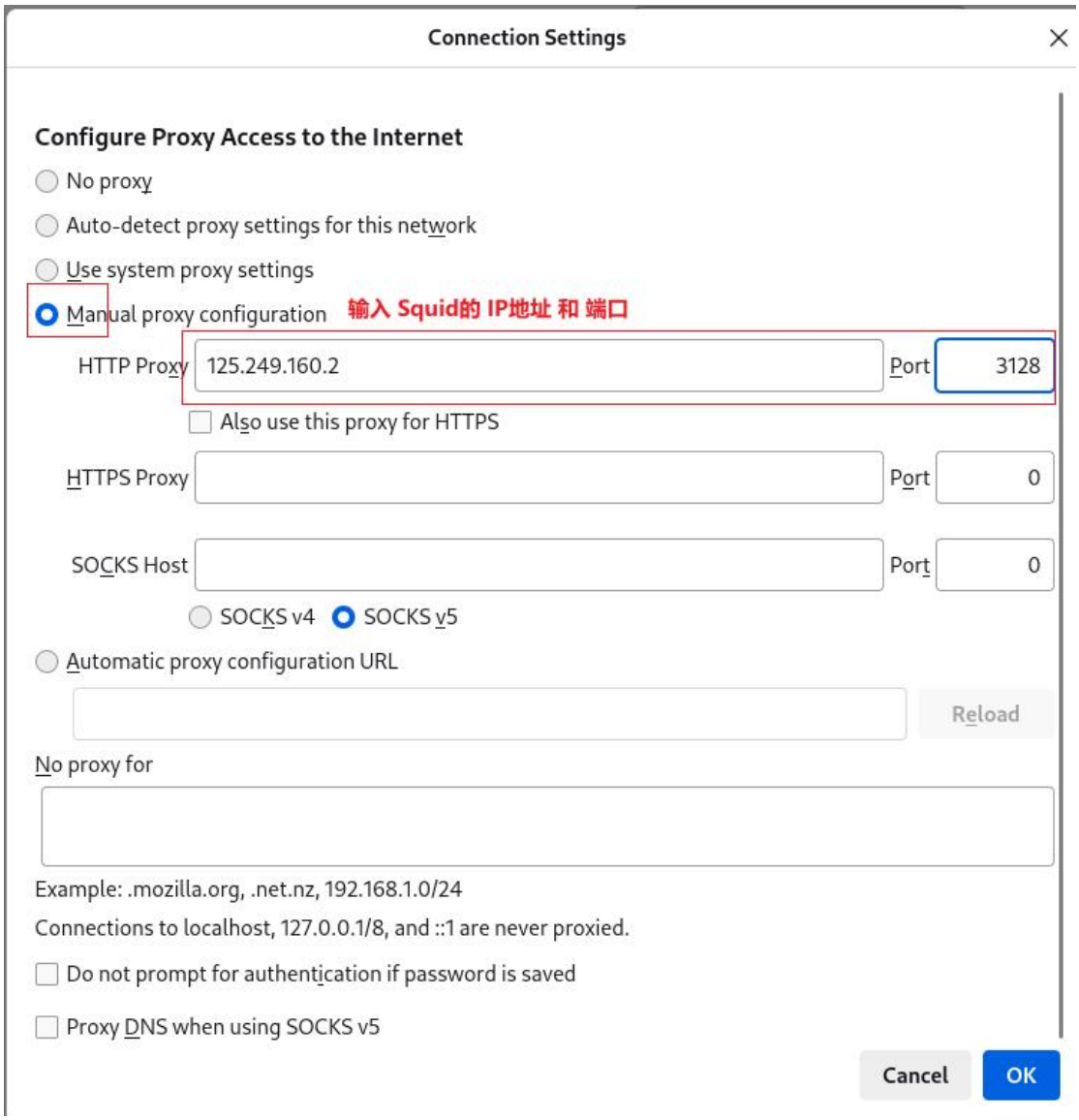
•反向代理：

•正向代理：


1 acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this"
2 acl localnet src 10.0.0.0/8 # RFC 1918 local
3 acl localnet src 100.64.0.0/10 # RFC 6598 shared
4 acl localnet src 169.254.0.0/16 # RFC 3927 link-lo
5 acl localnet src 172.16.0.0/12 # RFC 1918 local
6 acl localnet src 192.168.0.0/16 # RFC 1918 local
7 acl localnet src fc00::/7 # RFC 4193 local
8 acl localnet src fe80::/10 # RFC 4291 link-lo
9 acl SSL_ports port 443
10 acl Safe_ports port 80 # http
11 acl Safe_ports port 21 # ftp
12 acl Safe_ports port 443 # https
13 acl Safe_ports port 70 # gopher
14 acl Safe_ports port 210 # wais
15 acl Safe_ports port 1025-65535 # unregistered ports
16 acl Safe_ports port 280 # http-mgmt
17 acl Safe_ports port 488 # gss-http
18 acl Safe_ports port 591 # filemaker
19 acl Safe_ports port 777 # multiling http
20 http_access deny !Safe_ports
21 http_access deny CONNECT !SSL_ports
22 http_access allow localhost manager
23 http_access deny manager
24 include /etc/squid/conf.d/*.conf
25 http_access allow localhost
26 http_access allow all
27 http_port 3128
28 coredump_dir /var/spool/squid
29 refresh_pattern ^ftp: 1440 20% 10080
30 refresh_pattern ^gopher: 1440 0% 1440
31 refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
32 refresh_pattern . 0 20% 4320

浏览器设置：


Settings
Firefox
about:preferences#general
Find in Settings
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
Performance
Use recommended performance settings Learn more
These settings are tailored to your computer's hardware and operating system.
Browsing
Use autoscrolling
Use smooth scrolling
Always show scrollbars
Always use the cursor keys to navigate within pages
Search for text when you start typing
Enable picture-in-picture video controls Learn more
Control media via keyboard, headset, or virtual interface Learn more
Recommend extensions as you browse Learn more
Recommend features as you browse Learn more
Network Settings
Configure how Firefox connects to the internet. Learn more
Settings...



•透明代理：

必须要有一个普通端口才能启动
intercept 可以使用和它一样的端口，也可以自定义一个端口

```
acl localnet src 0.0.0.1-0.255.255.255  # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8             # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10          # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16         # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12          # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16         # RFC 1918 local private network (LAN)
acl localnet src fc00::/7               # RFC 4193 local private network range
acl localnet src fe80::/10              # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access deny to_localhost
http_access deny to_linklocal
include /etc/squid/conf.d/*.conf

http_access allow all

http_port 3129 intercept
http_port 3128

coredump_dir /var/spool/squid
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320
~
~
```

或：

```
acl localnet src 0.0.0.1-0.255.255.255  # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8             # RFC 1918 local private networ
acl localnet src 100.64.0.0/10          # RFC 6598 shared address space
acl localnet src 169.254.0.0/16         # RFC 3927 link-local (directly
acl localnet src 172.16.0.0/12          # RFC 1918 local private networ
acl localnet src 192.168.0.0/16         # RFC 1918 local private networ
acl localnet src fc00::/7               # RFC 4193 local private networ
acl localnet src fe80::/10              # RFC 4291 link-local (directly
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access deny to_localhost
http_access deny to_linklocal
include /etc/squid/conf.d/*.conf

http_access allow all

http_port 3128 intercept
http_port 3128

coredump_dir /var/spool/squid
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320
~
~
~
```

在本机配置防火墙，将 web 流量重定向到这个端口：

```
table ip nat {
        chain prerouting {
                type nat hook prerouting priority dstnat; policy accept;
                iif ens37 tcp dport 80 redirect to :3128
        }
```

•透明代理 https:

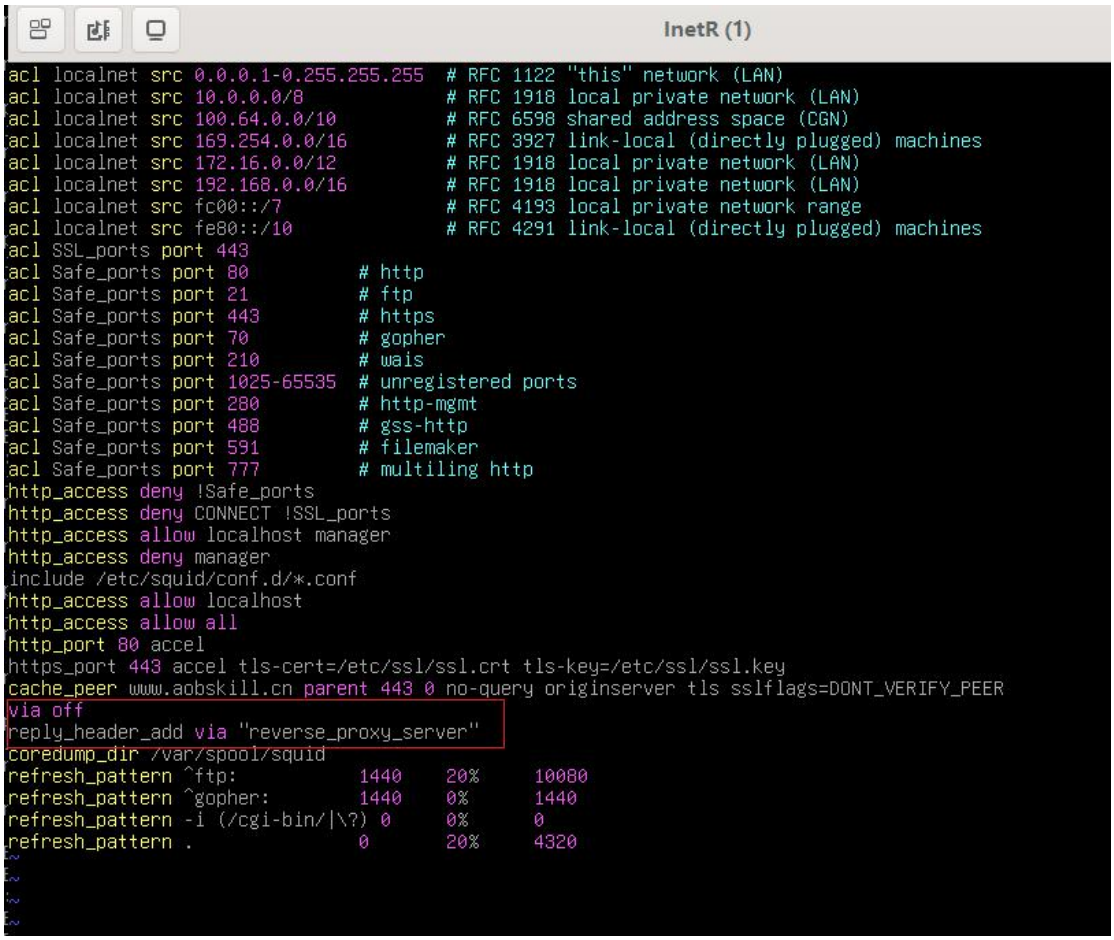
```
# 不能和 80 的透明代理一个端口
apt install -y squid-openssl
```

```
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
http_access allow all

http_port 3128 intercept
http_port 3128
https_port 3129 intercept ssl-bump cert=/etc/ssl/ssl.crt key=/etc/ssl/ssl.key generate-host-certific
ates=off

coredump_dir /var/spool/squid
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320
~
~
```

```
nft add rule ip nat prerouting iif ens37 tcp dport 443 redirect to 3129
```

•添加头部信息：

```
reply_header_replace
reply_header_add

request_header_replace
request_header_add
```



•允许身份认证头部：

带有身份认证的网页，通过 squid 代理后，客户端访问就不会弹出身份认证框，会直接 401 报错。

需要加上这个参数

vim /etc/squid/squid.conf

3、Nginx 代理：

•代理一台：

```
        server {
                listen 80;
                listen [::]:80;
                root /var/www/html;
                index index.html index.htm index.nginx-debian.html;
                server_name _;
                return 301 https://www.baidu.com;
                location / {
                        try_files $uri $uri/ =404;
                }
        }
        server {
                listen 443 ssl;
                listen [::]:443 ssl;
                ssl_certificate /etc/ssl/web.crt;
                ssl_certificate_key /etc/ssl/web.key;
                server_name www.baidu.com;
                index index.php index.html index.htm index.nginx-debian.html;
                root /var/www/html;
                location / {
                        try_files $uri $uri/ =404;
                }
                location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php8.2-fpm.sock;
                }
        }

        server {
                listen 8000 default_server;
                server_name _;
                location  / {
                        proxy_pass http://192.168.100.10:80;
                }

        }
"default" 44L, 912B                                           44,2-9        Bot
```

•负载均衡代理：

Location 这里直接用默认的就行了，不要加 ~

```
                location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php8.2-fpm.sock;
                }
        }

        upstream ServerGroup1 {
                server 192.168.100.10:80 weight=2;
                server 192.168.100.11:80;
                server 192.168.100.12:80 backup;
        }

        server {
                listen 8000 default_server;
                server_name _;

                location ~ / {
                        proxy_pass http://ServerGroup1;
                }
        }
```

定义一个后端服务器组

权重默认为1，weight可以设置权重值越高，负载的权重就越高

当其它服务器都正常运行时，不使用backup
当其它所有服务器都出现故障时，才使用backup

4、Apache2 代理：

这里就必须加 ProxyPreserveHost，这样就不会传 IP 给后端服务器，如果证书字段中没有 IP，不配置这个，就会导致 proxy 和 后端服务器这个链路的 web 不信任

•代理一台：

http：

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        ProxyPreserveHost on
        ProxyPass / http://172.16.10.10/
#       ProxyPassReverse / http://172.16.10.10/

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

```

https:

```

<VirtualHost *:443>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        SSLProxyEngine on
        ProxyPreserveHost on
        ProxyPass / https://172.16.10.10/
#       ProxyPassReverse / https://172.16.10.10/

        SSLEngine on
        SSLCertificateFile      /etc/ssl/www.crt
        SSLCertificateKeyFile   /etc/ssl/www.key
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
```

•代理多个服务器：

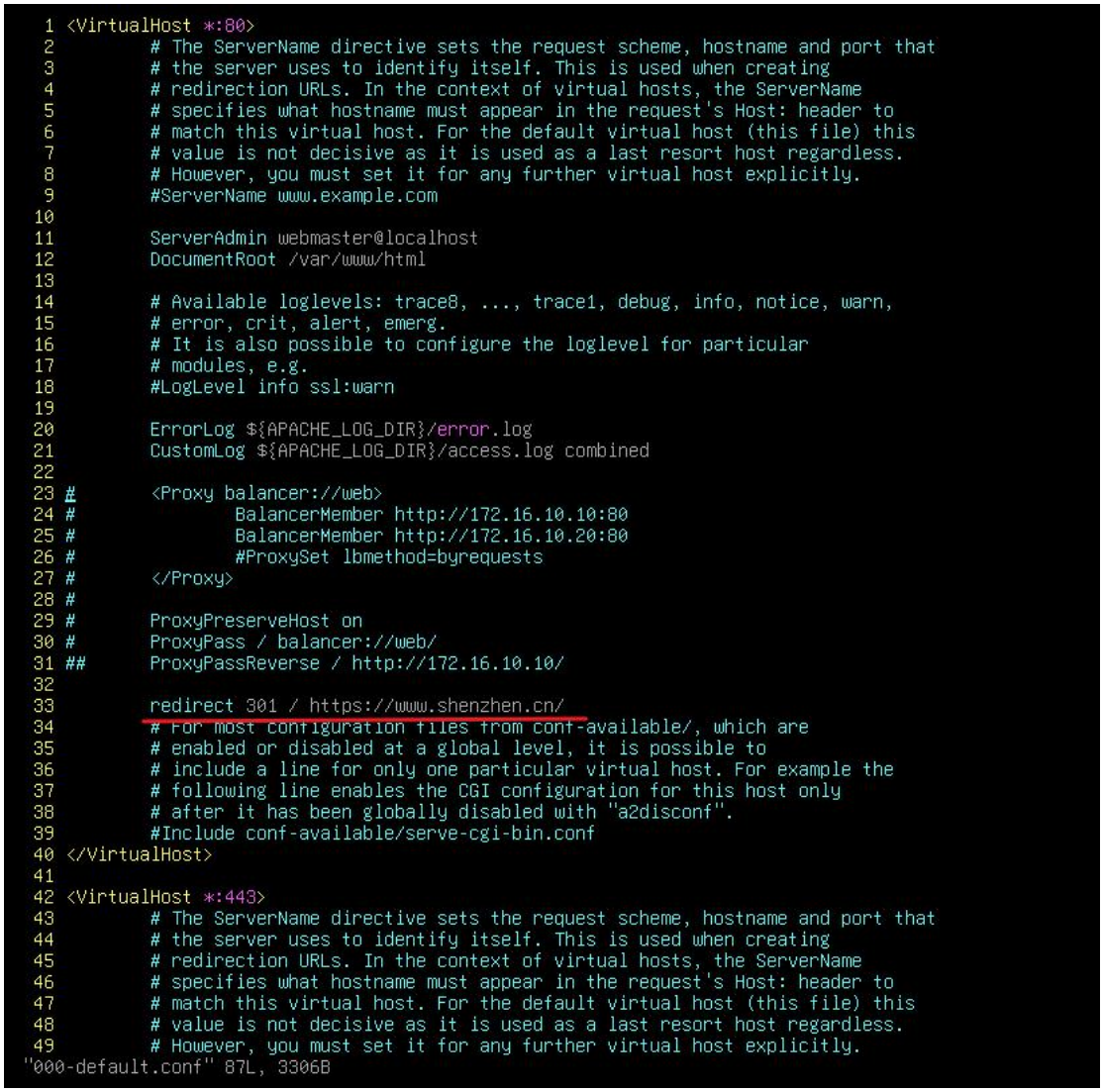
可以调度方式：

必须要 a2enmod lbmethod_... 启用，例如：a2enmod lbmethod_byrequests
byrequests　//默认算法，按权重分配。默认权重都是 1，所以就是轮询
bytraffic　//尽量让 后端 web1 和 web2 处理的总字节量一样。如果更改权重，例如 web1 = 2，web2 = 1，那么 web1 就会承担两倍于 web2 的流量（字节量）
bybusyness　//给最空闲的后端 web（目前处理请求最少的 web）

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        <Proxy balancer://web>
                BalancerMember http://172.16.10.10:80
                BalancerMember http://172.16.10.20:80
                #ProxySet lbmethod=byrequests
        </Proxy>

        ProxyPreserveHost on
        ProxyPass / balancer://web/
#       ProxyPassReverse / http://172.16.10.10/

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

```

•如果要配置重定向：

直接在 80 重定向即可



```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

#       <Proxy balancer://web>
#               BalancerMember http://172.16.10.10:80
#               BalancerMember http://172.16.10.20:80
#               #ProxySet lbmethod=byrequests
#       </Proxy>
#
#       ProxyPreserveHost on
#       ProxyPass / balancer://web/
##      ProxyPassReverse / http://172.16.10.10/

        redirect 301 / https://www.shenzhen.cn/
        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

<VirtualHost *:443>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
"000-default.conf" 87L, 3306B
```

九、Mail（TCP 143、25、465、993、587）：

•postfix/dovecot 如果使用了 lmtp 来投递文件，就必须使用 Maildir 格式来存储邮件，否则无法接收的邮件

•可以使用 postconf 查看配置属性

```
root@dmz1:/etc/postfix# postconf | grep local_reci
local_recipient_limit = $default_recipient_limit
local_recipient_maps = proxy:unix:passwd.byname $alias_maps
local_recipient_refill_delay = $default_recipient_refill_delay
local_recipient_refill_limit = $default_recipient_refill_limit
proxy_read_maps = $local_recipient_maps $mydestination $virtual_alias_ma
t_maps $relay_domains $canonical_maps $sender_canonical_maps $recipient_
der_bcc_maps $recipient_bcc_maps $smtp_generic_maps $lmtp_generic_maps $
```

•postfix 写本地域名时，假设邮件域名是 mail.dmz.skills.cn，不仅要写 mail.dmz.skills.cn，同时还要写 dmz.skills.cn

```
33 # List of domains (maptype:mapname allowed) that this machine considers
34 # itself the final destination for.
35 mydestination = $myhostname, dmz1.dmz.skills.cn, mail.dmz.skills.cn, dmz.skills.cn
36
```

•连接 ldap：

apt install -y dovecot-ldap
vim /etc/dovecot/conf.d/10-auth.conf

vim /etc/dovecot/conf.d/10-auth.conf

```
115
116 !include auth-system.conf.ext
117 #!include auth-sql.conf.ext
118 !include auth-ldap.conf.ext
119 #!include auth-passwdfile.conf.ext
120 #!include auth-static.conf.ext
:x_
```

vim /etc/dovecot/conf.d/auth-ldap.conf.ext
将 uri 改为 ldaps 就能连接 ldaps 了

```
## See <https://doc.dovecot.org/latest/core/config/dict.html#ldap>

ldap_uris = ldap://dc1.skills.cn
ldap_auth_dn = cn=admin,dc=skills,dc=cn
ldap_auth_dn_password = Skill39@Shanghai
ldap_base=dc=skills,dc=cn
                                    新增base
passdb ldap {
  ldap_filter = (&(objectClass=posixAccount)(uid=%{user}))
  ldap_bind = yes

  fields {
     user=%{ldap:uid}
    # password=%{ldap:userPassword}
    # userdb_home=%{ldap:homeDirectory}
    # userdb_uid=%{ldap:uidNumber}
    # userdb_gid=%{ldap:gidNumber}
  }
}

# "prefetch" user database means that the passdb already provided the
# needed information and there's no need to do a separate userdb lookup.
# <https://doc.dovecot.org/latest/core/config/auth/databases/prefetch.html>
#userdb prefetch {
#}

userdb ldap {
  ldap_filter = (&(objectClass=posixAccount)(uid=%{user}))

# Default fields can be used to specify defaults that LDAP may override
  fields {
#    home=/home/virtual/%{user}
    uid = %{ldap:uidnumber}
    gid = %{ldap:gidnumber}      新增这两个
    home=/home/%{user}
  }
}

# If you don't have any user-specific settings, you can avoid the userdb LDAP
# lookup by using userdb static instead of userdb ldap, for example:
# <https://doc.dovecot.org/latest/core/config/auth/databases/static.html>
#userdb static {
  #fields {
  #  uid = vmail
  #  gid = vmail
:q_
```

•注意要给 /home 权限，否则用户无法创建邮件目录：

```
chmod -R 777 /home
```

•starttls：

submission 就是 starttls（TCP 587）

```
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: https://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
#smtp      inet  n       -       y       -       -       smtpd
#smtps      inet  n       -       y       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
# Choose one: enable submission for loopback clients only, or for any client.
#127.0.0.1:submission inet n -   y       -       -       smtpd
submission inet n       -       y       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_forbid_unauth_pipelining=no
  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_tls_auth_only=yes
#  -o local_header_rewrite_clients=static:all
#  -o smtpd_hide_client_session=yes
#  -o smtpd_reject_unlisted_recipient=no
#     Instead of specifying complex smtpd_<xxx>_restrictions here,
#     specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
#     here, and specify mua_<xxx>_restrictions in main.cf (where
#     "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
#  -o smtpd_client_restrictions=
#  -o smtpd_helo_restrictions=
#  -o smtpd_sender_restrictions=
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
# Choose one: enable submissions for loopback clients only, or for any client.
#127.0.0.1:submissions inet n  -       y       -       -       smtpd
#submissions     inet  n       -       y       -       -       smtpd
#  -o syslog_name=postfix/submissions
#  -o smtpd_forbid_unauth_pipelining=no
#  -o smtpd_tls_wrappermode=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o local_header_rewrite_clients=static:all
#  -o smtpd_hide_client_session=yes
#  -o smtpd_reject_unlisted_recipient=no
```

•sasl：

postfix：

master.conf

```
12 #smtp      inet  n       -       y       -       -       smtpd
13 smtps      inet  n       -       y       -       -       smtpd
14 #smtp      inet  n       -       y       -       1       postscreen
15 #smtpd     pass  -       -       y       -       -       smtpd
16 #dnsblog   unix  -       -       y       -       0       dnsblog
17 #tlsproxy  unix  -       -       y       -       0       tlsproxy
18 # Choose one: enable submission for loopback clients only, or for any client.
19 #127.0.0.1:submission inet n -   y       -       -       smtpd
20 submission inet n       -       y       -       -       smtpd
21   -o syslog_name=postfix/submission
22   -o smtpd_forbid_unauth_pipelining=no
23   -o smtpd_tls_security_level=encrypt
24   -o smtpd_sasl_auth_enable=yes
25 #  -o smtpd_tls_auth_only=yes
26 #  -o local_header_rewrite_clients=static:all
27 #  -o smtpd_hide_client_session=yes
28 #  -o smtpd_reject_unlisted_recipient=no
29 #     Instead of specifying complex smtpd_<xxx>_restrictions here,
30 #     specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
31 #     here, and specify mua_<xxx>_restrictions in main.cf (where
32 #     "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
33 #  -o smtpd_client_restrictions=
34 #  -o smtpd_helo_restrictions=
35 #  -o smtpd_sender_restrictions=
36   -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
37 #  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
38 #  -o milter_macro_daemon_name=ORIGINATING
39 # Choose one: enable submissions for loopback clients only, or for any client.
40 #127.0.0.1:submissions inet n  -       y       -       -       smtpd
41 submissions     inet  n       -       y       -       -       smtpd
42   -o syslog_name=postfix/submissions
43   -o smtpd_forbid_unauth_pipelining=no
44   -o smtpd_tls_wrappermode=yes
45   -o smtpd_sasl_auth_enable=yes
46 #  -o local_header_rewrite_clients=static:all
47 #  -o smtpd_hide_client_session=yes
48 #  -o smtpd_reject_unlisted_recipient=no
49 #     Instead of specifying complex smtpd_<xxx>_restrictions here,
50 #     specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
51 #     here, and specify mua_<xxx>_restrictions in main.cf (where
52 #     "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
53 #  -o smtpd_client_restrictions=
54 #  -o smtpd_helo_restrictions=
55 #  -o smtpd_sender_restrictions=
56 #  -o smtpd_relay_restrictions=
57   -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
58 #  -o milter_macro_daemon_name=ORIGINATING
59 #628       inet  n       -       y       -       -       qmqpd
60 pickup    unix  n       -       y       60      1       pickup
:x_
```

main.cf

```
84 # SMTP Client TLS session cache
85 smtp_tls_session_cache_database = btree:$
86 smtpd_relay_restrictions = permit_mynetwor
87 myhostname = mail1.wsc48.lan
88 inet_interfaces = all
89
90 home_mailbox = Maildir/
91 #mail_spool_directory=/var/Mails/
92
93 smtpd_sasl_type = dovecot
94 smtpd_sasl_path = private/auth
```

dovecot：

```
 87 service auth {
 88   # auth_socket_path points to this userdb socket by de
 89   # used by dovecot-lda, doveadm, possibly imap process
 90   # full permissions to this socket are able to get a l
 91   # get the results of everyone's userdb lookups.
 92   #
 93   # The default 0666 mode allows anyone to connect to t
 94   # userdb lookups will succeed only if the userdb retu
 95   # matches the caller process's UID. Also if caller's
 96   # socket's uid or gid the lookup succeeds. Anything e
 97   #
 98   # To give the caller full permissions to lookup all u
 99   # something else than 0666 and Dovecot lets the kerne
100   # permissions (e.g. 0777 allows everyone full permiss
101   unix_listener auth-userdb {
102     #mode = 0666
103     #user =
104     #group =
105   }
106
107   # Postfix smtp-auth
108   unix_listener /var/spool/postfix/private/auth {
109     mode = 0666
110   }
111
```

•邮件分离：

postfix：

main.cf

```
26 # TLS parameters
27 smtpd_tls_cert_file=/etc/ssl/tls/app1.skill2025.cn.crt
28 smtpd_tls_key_file=/etc/ssl/tls/app1.skill2025.cn.key
29 smtpd_tls_security_level=may
30
31 smtp_tls_CApath=/etc/ssl/certs
32 smtp_tls_security_level=may
33 smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
34
35
36 smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated de
37 myhostname = app1.skill2025.cn
38 alias_maps = hash:/etc/aliases
39 alias_database = hash:/etc/aliases
40 myorigin = /etc/mailname
41 mydestination = $myhostname, mail.skill2025.cn, app1.skill2025.cn, localh
42 relayhost =
43 mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 0.0.0.0/0
44 mailbox_size_limit = 0
45 recipient_delimiter = +
46 inet_interfaces = all
47 inet_protocols = all
48 mailbox_transport = lmtp:172.16.10.102:24
49 local_recipient_maps =
:set nu
```

dovecot：

```
55 service lmtp {
56   unix_listener lmtp {
57     #mode = 0666
58   }
59
60   # Create inet listener only if you ca
61   inet_listener lmtp {
62     # Avoid making LMTP visible for the
63     address = 0.0.0.0
64     port = 24
65   }
66 }
67
```

取消注释，然后填写内容

•邮件群发：

/etc/aliases

```
15 all: zhangsan,lisi
```

postalias /etc/aliases

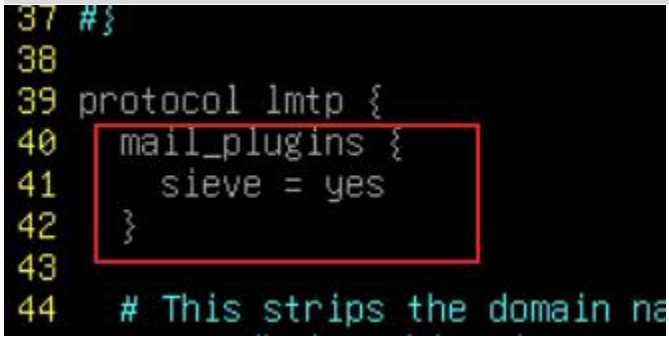
•邮件自动回复：

需要配置 lmtp 来投递

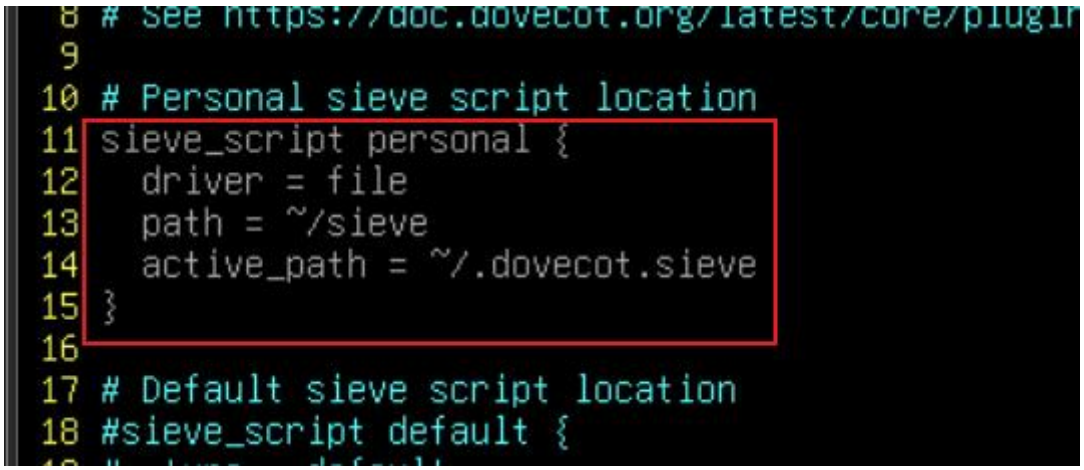
```
apt install -y dovecot-sieve dovecot-lmtpd
```

这个方式还需要配置 使用 lmtp 进行投递

```
vim /etc/dovecot/conf.d/20-lmtp.conf
# 取消注释
```




```
vim /etc/dovecot/conf.d/90-sieve.conf
# 取消注释
```



这个 .dovecot.sieve 就是脚本文件名

```
# 编写脚本：
## 去到用户家目录（ldap 用户定义的是哪个就是哪个，没有就创建）：
vim /home/bob/.dovecot.sieve
```

```
require ["vacation"];

vacation
   :days 1
   :subject "Automatic Reply"
   "reply";
```

systemctl restart dovecot 此时就能够自动进进行回复了

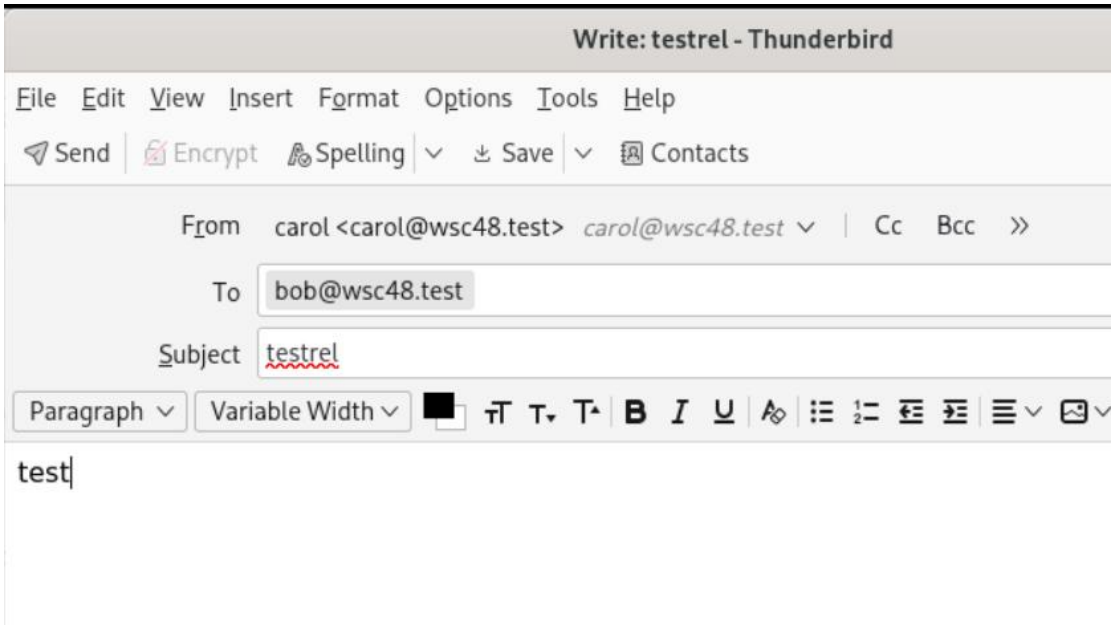
但是这个在一天内只会回复一次，要让它每次都回复，需要配置一个脚本，删除目录下的 .dovecot.lda-dupes* 两个文件

•写脚本骗过 sieve 脚本：

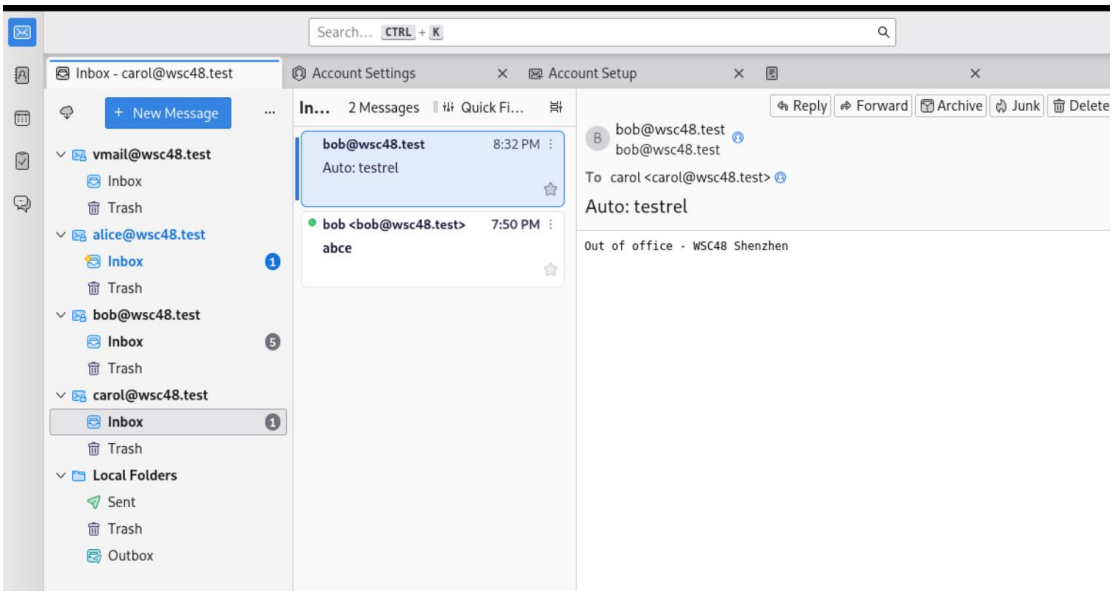
因为 sieve 脚本是通过检测.dovecot.lda-dupes 文件中定义的重复用户来判断的，因此直接删掉它就行了

```
#!/bin/bash

while true; do

rm -rf /home/bob/.dovecot.lda-dupes*

sleep 0.5
done &
```

客户端测试：



可以看到已经接受了 自动回复邮件：



•Mailbox、Maildir:

•Maildir:

maildir 需要使用 lmtp 来投递

main.cf

```
73 # SMTP server RSA key and certificate in PEM format
74 smtpd_tls_key_file = /opt/grading/ca/mail.key
75 smtpd_tls_cert_file = /opt/grading/ca/mail.pem
76 # SMTP Server security level: none|may|encrypt
77 smtpd_tls_security_level = may
78
79 # List of CAs for SMTP Client to trust
80 # Prefer this over _CApath when smtp is running chrooted
81 smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
82 # SMTP Client TLS security level: none|may|encrypt|...
83 smtp_tls_security_level = may
84 # SMTP Client TLS session cache
85 smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
86 smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destina
87 myhostname = dmz1.dmz.skills.cn
88 inet_interfaces = all
89
90 mailbox_transport=lmtp:127.0.0.1:24
91 local_recipient_maps=
~
:q_
```

dovecot:

10-master.conf

```
55 service lmtp {
56   unix_listener lmtp {
57     #mode = 0666
58   }
59
60   # Create inet listener only if you ca
61   inet_listener lmtp {
62     # Avoid making LMTP visible for the
63     address = 0.0.0.0
64     port = 24
65   }
66 }
67
```

取消注释，然后填写内容

10-mail.conf

```
21 #
22 # See https://doc.dovecot.org/latest/core/settings/
23 # of variables.
24 #
25 # Example:
26   mail_driver = maildir
27   mail_path = ~/Maildir
28 #  mail_inbox_path = ~/Maildir/.INBOX
29 #
30
31 # Debian defaults
32 # Note that upstream considers mbox deprecated and
33 # against its use in production environments. See f
34 # at
```

取消注释这两行

•Maildir 自定义路径：

dovecot:

10-mail.conf

```
21 #
22 # See https://doc.dovecot.org/latest/core/settings/variables.html for f
23 # of variables.
24 #
25 # Example:
26   mail_driver = maildir
27 # mail_path = ~/Maildir
28   mail_path = /var/vmail/wsc48.test/%{user | username}
29 #  mail_inbox_path = ~/Maildir/.INBOX
30 #
31
32 # Debian defaults
```

其他全部注释

```
# 需要给目录权限，否则无法创建用户目录
chmod 777 /var/vmail/wsc48.test
```

postfix:

```
82 # SMTP Client TLS security level: none|may|encrypt|...
83 smtp_tls_security_level = may
84 # SMTP Client TLS session cache
85 smtp_tls_session_cache_database = btree:${data_directory}/s
86 smtpd_relay_restrictions = permit_mynetworks permit_sasl_au
87 myhostname = sz-app.wsc48.test
88 inet_interfaces = all
89 #home_mailbox = Maildir/
90 mailbox_transport = lmtp:127.0.0.1:24
91 local_recipient_maps =
92 #mail_spool_directory = /var/vmail/wsc48.test/
:q_
```

•Mailbox:

自定义 mbox 路径：

```
23 # of variables.
24 #
25 # Example:
26 #  mail_driver = maildir
27 #  mail_path = ~/Maildir
28 #  mail_inbox_path = ~/Maildir/.INBOX
29 #
30
31 # Debian defaults
32 # Note that upstream considers mbox deprecated and strongly recommends
33 # against its use in production environments. See further information
34 # at
35 # https://doc.dovecot.org/2.4.1/core/config/mailbox/formats/mbox.html
36 mail_driver = mbox
37 mail_home = /home/%{user | username}
38 mail_path = %{home}/mail
39 mail_inbox_path = /var/mail/%{user}
40
41 # If you need to set multiple mailbox locations or want to change default
42 # namespace settings, you can do it by defining namespace sections.
43 #
```

改 mail_inbox_path 路径即可

•postfix 配置 mTLS:

main.cf 指定根证书：

```
67
68 # Where to look for Cyrus SASL configuration files.  Upstream defau
69 # (use compiled-in SASL library default), Debian Policy says it sho
70 # /etc/postfix/sasl.
71 cyrus_sasl_config_path = /etc/postfix/sasl
72
73 # SMTP server RSA key and certificate in PEM format
74 smtpd_tls_key_file = /etc/ssl/mail.key
75 smtpd_tls_cert_file = /etc/ssl/mail.crt
76 # SMTP Server security level: none|may|encrypt
77 smtpd_tls_security_level = may
78
79 # List of CAs for SMTP Client to trust
80 # Prefer this over _CApath when smtp is running chrooted
81 smtp_tls_CAfile = /etc/ssl/ca.crt
82 smtpd_tls_CAfile = /etc/ssl/ca.crt
83 # SMTP Client TLS security level: none|may|encrypt|...
84 smtp_tls_security_level = may
85 # SMTP Client TLS session cache
```

vim /etc/postfix/master.cf

配置只在 587 和 465 端口启用：

添加一行 smtpd_tls_req_ccert=yes，并将 smtpd_tls_security_level 复制到下面

```
10 #               (yes)   (yes)   (no)    (never) (100)
11 # ==========================================================================
12 smtp      inet  n       -       y       -       -       smtpd
13 smtps     inet  n       -       y       -       -       smtpd
14 #smtp      inet  n       -       y       -       1       postscreen
15 #smtpd     pass  -       -       y       -       -       smtpd
16 #dnsblog   unix  -       -       y       -       0       dnsblog
17 #tlsproxy  unix  -       -       y       -       0       tlsproxy
18 # Choose one: enable submission for loopback clients only, or for any client.
19 #127.0.0.1:submission inet n -   y       -       -       smtpd
20 submission inet n       -       y       -       -       smtpd
21   -o syslog_name=postfix/submission
22   -o smtpd_forbid_unauth_pipelining=no
23   -o smtpd_tls_security_level=encrypt
24   -o smtpd_tls_req_ccert=yes
25 #  -o smtpd_sasl_auth_enable=yes
26 #  -o smtpd_tls_auth_only=yes
27 #  -o local_header_rewrite_clients=static:all
28 #  -o smtpd_hide_client_session=yes
29 #  -o smtpd_reject_unlisted_recipient=no
30 #     Instead of specifying complex smtpd_<xxx>_restrictions here,
31 #     specify "smtpd_<xxx>_restrictions=$mua_<xxx>_restrictions"
32 #     here, and specify mua_<xxx>_restrictions in main.cf (where
33 #     "<xxx>" is "client", "helo", "sender", "relay", or "recipient").
34 #  -o smtpd_client_restrictions=
35 #  -o smtpd_helo_restrictions=
36 #  -o smtpd_sender_restrictions=
37 #  -o smtpd_relay_restrictions=
38 #  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
39 #  -o milter_macro_daemon_name=ORIGINATING
40 # Choose one: enable submissions for loopback clients only, or for any client.
41 #127.0.0.1:submissions inet n  -       y       -       -       smtpd
42 submissions     inet  n       -       y       -       -       smtpd
43   -o syslog_name=postfix/submissions
44   -o smtpd_forbid_unauth_pipelining=no
45   -o smtpd_tls_wrappermode=yes
46   -o smtpd_tls_security_level=encrypt
47   -o smtpd_tls_req_ccert=yes
48 #  -o smtpd_sasl_auth_enable=yes
49 #  -o local_header_rewrite_clients=static:all
50 #  -o smtpd_hide_client_session=yes
51 #  -o smtpd_reject_unlisted_recipient=no
```

合成证书为 pkcs12 给客户端：
openssl pkcs12 -export -out client.p12 -in skill39.crt -inkey skill39.key -certfile ca.crt

•Webmail：

roundcube 中，如果 postfix 开启了 SASL 认证，这里就必须有 %u 和 %p，如果没有开启，那么就建议将它们清空

```
19
20 $config = [];
21
22 // Do not set db_dsnw here, use dpkg-reconfigure roundcube-core to configure databa
23 include("/etc/roundcube/debian-db-roundcube.php");
24
25 // IMAP host chosen to perform the log-in.
26 // See defaults.inc.php for the option description.
27 $config['imap_host'] = ["ssl://mx.wsc2026.sh:993"];
28
29 // SMTP server host (for sending mails).
30 // See defaults.inc.php for the option description.
31 $config['smtp_host'] = 'tls://mx.wsc2026.sh:587';
32
33 // SMTP username (if required) if you use %u as the username Roundcube
34 // will use the current username for login
35 $config['smtp_user'] = '%u';
36
37 // SMTP password (if required) if you use %p as the password Roundcube
38 // will use the current user's password for login
39 $config['smtp_pass'] = '%p';
40
41 //$config['imap_conn_options'] = [
```

十、Samba（TCP 445）：

•基础参数：

browseable　//是否能在网络浏览中看到
available　//共享是否可用
valid users =　//允许哪些用户访问
invalid users =　//禁止哪些用户访问
write list　//可读写用户/组 列表
read list　//可读用户/组 列表

•samba 连接 ldap：

man smb.conf

```
encrypt passwords = true
passdb backend = ldapsam

ldapsam:trusted=yes
ldapsam:editposix=yes

ldap admin dn = cn=admin,dc=samba,dc=org
ldap delete dn = yes
ldap group suffix = ou=groups
ldap idmap suffix = ou=idmap
ldap machine suffix = ou=computers
ldap user suffix = ou=users
ldap suffix = dc=samba,dc=org

idmap backend = ldap:"ldap://localhost"

idmap uid = 5000-50000
idmap gid = 5000-50000
```

有时需要加上： idmap backend=ldap:"ldap://ldap.devops.com"

```
#======================= Global Settings =======================

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
   workgroup = WORKGROUP

                passdb backend = ldapsam:"ldap://ldap.devops.com/"
                ldap suffix = dc=devops,dc=com
                ldap admin dn = cn=admin,dc=devops,dc=com
                ldap ssl=no
#                ldap delete dn = no
#                ldap idmap suffix = ou=users
```

```
apt install -y smbldap-tools

ldapadd -Q -Y EXTERNAL -H ldapi:/// -f /usr/share/doc/samba/examples/LDAP/samba.ldif

smbpasswd -W    //root 密码

net getlocalsid >> smbldap.conf
vim smbldap.conf
```

```
36 SID="S-1-5-21-3973319813-3909002216-2079265846"
```

```
57 # Slave LDAP server URI
58 # Ex: slaveLDAP=ldap://slave.ldap.example.com/
59 # If not defined, parameter is set to "ldap://127.0.0.1/"
60 slaveLDAP="ldap://127.0.0.1/"
61
62 # Master LDAP server URI: needed for write operations
63 # Ex: masterLDAP=ldap://master.ldap.example.com/
64 # If not defined, parameter is set to "ldap://127.0.0.1/"
65 masterLDAP="ldap://127.0.0.1/"
66
67 # Use TLS for LDAP
68 # If set to 1, this option will use start_tls for connection
69 # (you must also used the LDAP URI "ldap://...", not "ldaps://...")
70 # If not defined, parameter is set to "0"
71 ldapTLS="0"
72
73 # How to verify the server's certificate (none, optional or require)
```

如果是不加密ldap，就是0，加密的就是1

```
88
89 # LDAP Suffix
90 # Ex: suffix=dc=IDEALX,dc=ORG
91 suffix="dc=devops,dc=com"
92
93 # Where are stored Users
94 # Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
95 # Warning: if 'suffix' is not set here, you must se
96 usersdn="ou=users,${suffix}"
97
98 # Where are stored Computers
99 # Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
100 # Warning: if 'suffix' is not set here, you must se
101 computersdn="ou=Computers,${suffix}"
102
103 # Where are stored Groups
104 # Ex: groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
105 # Warning: if 'suffix' is not set here, you must se
106 groupsdn="ou=users,${suffix}"
107
```

```
174
175 # The UNC path to home drives location (%U username substituti
176 # Just set it to a null string if you want to use the smb.conf
177 # directive and/or disable roaming profiles
178 # Ex: userSmbHome="\\PDC-SMB3\%U"
179 userSmbHome=""
180
181 # The UNC path to profiles locations (%U username substitution
182 # Just set it to a null string if you want to use the smb.conf
183 # directive and/or disable roaming profiles
184 # Ex: userProfile="\\PDC-SMB3\profiles\%U"
185 userProfile=""
186
187 # The default Home Drive Letter mapping
188 # (will be automatically mapped at logon time if home director
189 # Ex: userHomeDrive="H:"
190 userHomeDrive=""
191
192 # The default user netlogon script name (%U username substitut
193 # if not used, will be automatically username.cmd
194 # make sure script file is edited under dos
195 # Ex: userScript="startup.cmd" # make sure script file is edit
196 userScript=""
197
198 # Domain appended to the users "mail"-attribute
199 # when smbldap-useradd -M is used
200 # Ex: mailDomain="idealx.com"
```

vim smbldap_bind.conf

```
# $Id$
#
##############################
# Credential Configuration #
##############################
# Notes: you can specify two differents configuration if you use
# master ldap for writing access and a slave ldap server for read
# By default, we will use the same DN (so it will work for standa
# release)
slaveDN="cn=admin,dc=devops,dc=com"
slavePw="Skill2024"
masterDN="cn=admin,dc=devops,dc=com"
masterPw="Skill2024"
~
~
```

smbldap-populate

•smbldap 工具:

smbldap-useradd　//创建用户
-a　//同时创建 samba 用户（不加-a 只创建 ldap 用户）
-m　//创建 home 目录

```
-P   //同时指定密码
-g   //指定主要组
-G   //指定附加组
-u   //指定 UID

smbldap-usermod   //修改已经存在的用户
-a   //将 LDAP 用户转换为 Samba 用户（添加 Samba 属性）

smbldap-passwd   //不加参数时同时修改 LDAP/Samba 用户密码（在修改 samba 用户密码时，它必须有 samba 属性）
-s   //只修改 samba 用户密码（必须有 samba 属性）
-u   //只修改 LDAP 用户密码
```

•如果要使用 @group 这样匹配 LDAP 用户组：

```
# 最简单的方式就是安装 nslcd：
apt install -y nslcd
## getent group shenzhen 能够列出用户即成功（一般连接成功就行了）
```

```
root@int01:~# getent group shenzhen
shenzhen:*:10001:szuser1,szuser2,szuser3
root@int01:~# _
```

•用户映射：

smb.conf

```
23
24 [global]
25
26 username map=/etc/samba/map
27 ## Browsing/Identification ###
28
```

```
adduser smbuser
adduser user1

smbpasswd -a smbuser
smbpasswd -a user1

vim /etc/samba/map
```

```
1 smbuser = administrator, test
2 user1 = user2, user3, user4, user5
~
~
```

valid users 中要写左边的真实用户

•DFS:

```
# host msdfs=yes 表示这台 Samba 提供 DFS
# msdfs root=yes 表示这个共享是 DFS 命名空间的根
```

```
237 [global]
238 host msdfs=yes
239
240 [resources]
241 path=/resources
242 read only=no
243
244 [dfs]
245 path=/dfsroot
246 msdfs root=yes
247
```

```
# 假如本机是 srv02.wsc2026.sh
## 这里可以写 主机名，也可以写 FQDN（但是必须要能够访问到，主机名还要写 hosts，所以直接写 fqdn）：
ln -s 'msdfs:srv02.wsc2026.sh\resources' /dfsroot/resources
```

```
root@srv02:/etc/samba# hostname -f
srv02.wsc2026.sh
root@srv02:/etc/samba# ln -s 'msdfs:srv02.wsc2026.sh\resources' /dfsroot/resrouces
root@srv02:/etc/samba# ls -l /dfsroot
total 0
lrwxrwxrwx 1 root root 32 Aug 20 08:23 resrouces -> 'msdfs:srv02.wsc2026.sh\resources'
root@srv02:/etc/samba#
```

其他机器的也是这样添加，只要能够访问到

•定义多个 target:

```
ln -s 'msdfs:fw01.wsc2026.sh\resources,srv02.wsc2026.sh\resources' /dfsroot/resources
```

此时两个文件夹的数据不会自动同步，这里可以使用 rsync 进行数据同步：

```
# 两边同时安装 rsync：
apt install -y rsync


ssh-keygen
ssh-copy-id root@fw01.wsc2026.sh
rsync -aHAX --delete /resources/ root@fw01.wsc2026.sh:/resources/
# -a 保留文件属性、权限
# -H 保留硬链接（不加也行）
# -A 保留 ACL（不加也行）
# -X 保留扩展属性（不加也行）
# --delete 表示本地删除的文件，远端也删除
```

```
root@srv02:~# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
/root/.ssh/id_ed25519 already exists.
Overwrite (y/n)?
root@srv02:~#
root@srv02:~# ssh-copy-id root@fw01.wsc2026.sh
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@fw01.wsc2026.sh's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@fw01.wsc2026.sh'"
and check to make sure that only the key(s) you wanted were added.

root@srv02:~# rsync -aHAX --delete /resources/ root@fw01.wsc2026.sh:/resources/
root@srv02:~#
```

十一、 Docker （TCP 9090、 9100、 3000）：

1、docker 常用命令：

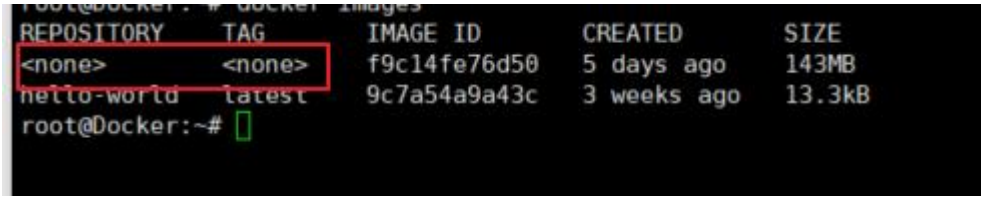
（1）查看容器、镜像：

```
# 查看正在运行的容器：
docker ps

# 查看所有容器，包括未运行的容器
docker ps -a

# 查看所有镜像：
docker images
```

（2）删除容器、镜像：

```
# 删除容器：
docker rm [容器名]  //只能删除未在运行的容器
要强制删除正在运行的容器，需要加上参数： -f
docker rm -f [容器名]
删除所有容器：
docker rm `docker ps -aq`

# 删除镜像：
```

```
docker rmi [镜像名]  //只能删除未被容器使用的镜像
docker rmi -f [镜像名]  //伪强制删除，只是删除了名称和 TAG，镜像还存在（需要先删除容器，才能删除镜像）
```



（3）进入容器：

```
# 进入容器：
docker exec -u root -it [容器名] /bin/bash
# -i: 交互式操作。
# -t: 终端。
# /bin/bash 自选 shell，一般为 /bin/bash
exit 退出容器
```

（4）在容器和本地机器之间传输文件：

```
# 复制本地文件到 docker 中：
docker cp server.crt nginx:/

# 复制 docker 文件到本地：
docker cp nginx:/etc/nginx/nginx.conf .
```

（5）启动、停止容器：

```
# 停止容器：
docker stop nginx
强制停止容器：
docker kill nginx

# 启动容器：
docker start nginx

# 启动所有容器：
docker start `docker ps -aq`
```

（6）设置容器为开机自启动：

```
docker update --restart=always nginx
## 如果是 --restart always 将无法生效
```

```
docker update --restart always `docker ps -aq`
```

（7）关闭容器开机自启动：

```
docker update --restart no nginx

docker update --restart no `docker ps -aq`
```

（8）重新加载配置：

```
docker restart prometheus
```

```
root@Server1:~# docker restart prometheus
prometheus
root@Server1:~# _
```

•重命名镜像（对镜像打 tag）：

```
docker tag grafana/grafana:latest grafana-v1:latest

# 然后删掉旧镜像即可：
docker rmi oldname:latest
```

```
root@mon:~# docker images
REPOSITORY        TAG       IMAGE ID       CREATED        SIZE
grafana/grafana   latest    6a8d9cef0bf1   5 months ago   761MB
prom/prometheus   latest    5a2c7fe42427   6 months ago   390MB
root@mon:~# docker tag grafana/grafana:latest grafana-v1:latest
root@mon:~# docker images
REPOSITORY        TAG       IMAGE ID       CREATED        SIZE
grafana/grafana   latest    6a8d9cef0bf1   5 months ago   761MB
grafana-v1        latest    6a8d9cef0bf1   5 months ago   761MB
prom/prometheus   latest    5a2c7fe42427   6 months ago   390MB
root@mon:~#
```

2、创建 prometheus docker（TCP 9090）：

prometheus-node-exporter（TCP 9100）

```
apt install -y prometheus
systemctl disable prometheus --now
```

/etc/prometheus/prometheus.yml

```
26 scrape_configs:
27   # The job name is added as a label `job=<job_name>` to any timeseries scr
28   - job_name: 'prometheus'
29
30     # Override the global default and scrape targets from this job every 5
31     scrape_interval: 5s
32     scrape_timeout: 5s
33
34     # metrics_path defaults to '/metrics'
35     # scheme defaults to 'http'.
36
37     static_configs:
38       - targets: ['localhost:9090']
39
40   - job_name: Server2.shanghai.org
41     # If prometheus-node-exporter is installed, grab stats about the local
42     # machine by default.
43     static_configs:
44       - targets: ['Server2.shanghai.org:9100']
45
46   - job_name: Server3.shanghai.org
47     # If prometheus-node-exporter is installed, grab stats about the local
48     # machine by default.
49     static_configs:
50       - targets: ['Server3.shanghai.org:9100']
```

或者这样写：

```yaml
- job_name: 'linux'
  static_configs:
    - targets:
        - 'Server2.shanghai.org:9100'
        - 'Server3.shanghai.org:9100'
```

```
# 创建容器网络：
docker network create mo
docker network ls

# 创建 docker volume：
docker volume create prometheus-data
docker volume ls

# 创建 prometheus dockers：
docker run -d --name prometheus --network mo --restart always -p 9090:9090 -v /etc/prometheus/prometheus.yml:/etc/prometheus/prometheus.yml:ro -v prometheus-data:/prometheus prom/prometheus:v3.10.0 --config.file=/etc/prometheus/prometheus.yml --storage.tsdb.path=/prometheus
```

3、创建 grafana docker（TCP 3000）：

```
docker volume create grafana-data

docker run -d --name grafana --network mo --restart always -p 3000:3000 -v grafana-data:/var/lib/grafana grafana/grafana-oss:12.4.2
```

4、监控值：

（1）UP/DOWN 状态：

Stat 图表

```
up{instance=~".*:9100"}
```

（2）去掉端口：

```
label_replace(up{instance=~".*:9100"}, "host","$1","instance","(.*):.*")
```

（3）CPU：

```
100 - (avg by(instance)(rate(node_cpu_seconds_total{mode="idle"}[5m])) * 100)
```

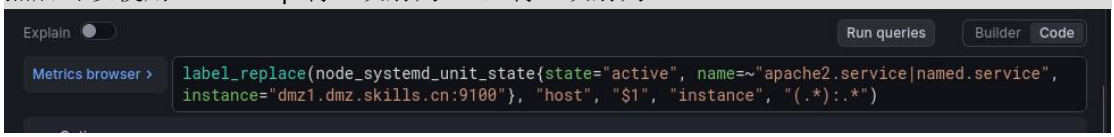
（4）内存：

```
100 * (1 - node_memory_MemAvailable_bytes / node_memory_MemTotal_bytes)
```

（5）服务状态：

```
# 使用 node_systemd_unit_state 参数
```

node_system.. 可以在 Builder 中补全
name=~ 可以定义多个服务，能够同时查看多个服务是否 up/down
然后可以使用 value map 将 1 映射为 UP，将 0 映射为 DOWN



十二、Ansible、Git：

1、Ansible：

（1）读取文件：

•万能读取法：

这个方法不论文件中写了什么，都能读取到

```
## 这个 name 是变量名称，可以随便定义
- set_fact:
   name: "{{ lookup('file', '/data/ansible/users.json') }}"
```

```yaml
---
- name: task
  hosts: all
  gather_facts: false
  tasks:
    - name: read file
      set_fact:
        name: "{{ lookup('file', '/data/ansible/users.json') }}"

    - name:
      debug:
        var: name
```

用这个方法所有格式的文件都能直接读取，然后在后面用 | [方法] 来处理不同格式的文件

1）json 文件：

```
# 使用 | from_json
```

```yaml
---
- name: task
  hosts: all
  gather_facts: false
  tasks:
    - name: read file
      set_fact:
        name: "{{ lookup('file', '/data/ansible/users.json') | from_json }}"

    - name:
      debug:
        var: name
```

2）yaml、yml 文件：

```
# 使用 | from_yaml
```

```yaml
---
- name: task
  hosts: all
  gather_facts: false
  tasks:
    - name: read file
      set_fact:
        name: "{{ lookup('file', '/data/ansible/users.yaml') | from_yaml }}"

    - name:
      debug:
        var: name
```

•如果一个 yaml 文件中包含多个 yaml：

```
## 用 --- 来表示不同的 yaml
```

```
# 例如：
---
name: user1
age: 20

---
name: user2
age: 21
```

```yaml
---
- name: task
  hosts: all
  gather_facts: false
  tasks:
    - name: read file
      set_fact:
        name: "{{ lookup('file', '/data/ansible/users.yaml') | from_yaml_all | list }}"

    - name:
      debug:
        var: name
```

3）csv 文件：

这个方法与直接使用 read_csv 模块是一样的

```
# 使用 | community.general.from_csv
## 必须写 community.general.
```

```yaml
---
- name: task
  hosts: all
  gather_facts: false
  tasks:
    - name: read file
      set_fact:
        name: "{{ lookup('file', '/data/ansible/test') | community.general.from_csv }}"

    - name:
      debug:
        var: name
```

直接使用 read_csv 文件：

```yaml
---
- name: task
  hosts: all
  gather_facts: false
  tasks:
    - name: read file
      read_csv:
        path: /data/ansible/test
      register: csv
      delegate_to: localhost
      vars:
        ansible_shell_type: sh


    - name:
      debug:
        var: csv
```

2、Git:

2.1、Git 在本地:

```
mkdir /data
cd /data
git init
git config --global user.name "root"
git config --global user.email "root@shanghai.org"
```

```
# 然后就能 提交 git 了:
touch test
git add .
git commit -m "test file"
```

2.2、搭建 git 仓库（git 仓库在服务端上，使用客户端连接 git 仓库）:

配置 服务端:

```
apt install -y git

# 搭建 git 仓库：
mkdir /git
cd /git
git init --bare git.git
# git init --bare [仓库名称]  //会自动在当前目录下创建仓库
adduser git  //不是必要的，主要是看题目想要你使用哪个用户来 push 和 clone（如果没有指定，直接使用 root 也可以）（要用哪个用户，就将哪个用户设置为属主和属组）
chown -R git:git git.git/  //这个必须设置，git 的用户必须对 git 服务器文件夹拥有属主和属组的权限
```

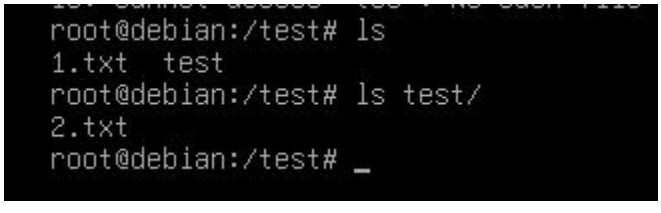
配置 客户端 push：

```
apt install -y git

git clone git@192.168.1.2:/git/git.git  /ansible  //把前面的‘git clone’替换成 scp，就能够理解这行代码了，一样的作用
git config --global user.email "git@a.com"
git config --global user.name "gitte"
cd /ansible
# 随意上传一些 文件、目录：（git 也能够 push 和 拉取 目录[前提是目录中有内容]）
echo 1 > 1.txt
mkdir test
echo 2 > test/2.txt
# push 到 git 仓库：
git add .  //将更改添加
git commit -m "Add"  //每次 push 都必须些 commit，否则无法 push
git push  //完成 push（这样才算 push 成功）
# push 会提示需要输入密码
```

从 git 仓库拉取代码：

其实和 push 是一样的，甚至操作更加简单

```
apt install -y git

git clone git@192.168.1.2:/git/git.git /test
# 拉取成功，这样就可以看到上面 push 的代码
```



十三、Bash Script：

1、自动备份文件和 mysql 数据库，并删除超过 7 天的文件：

```
apt install -y mariadb-server
mkdir mysql_backup
```

```
#!/bin/bash

date=$(date +%Y%m%d%H%M%S)

# Backup Files Folder:
tar -czf /bash_scripts/backup_dir/files_backup_$date.tar.gz /bash_scripts/files

# Backup Mysql:
mysqldump -uroot -pSkills39 -A > /bash_scripts/backup_dir/mysql_backup_$date.sql

find /bash_scripts/backup_dir -type f -name "*.sql" -mtime +7 -exec rm -rf {} \;
~
~
```

如果要只保留 3 个最新文件：

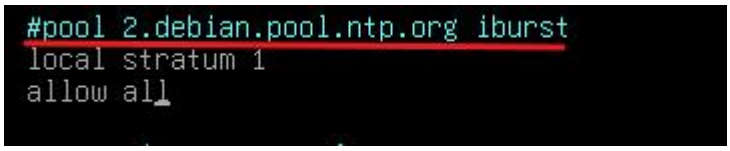
```
ls -t /bash_scripts/backup_dir/*.sql | tail -n +4 | xargs rm -f
```

十四、NTP（UDP 123）：

1、NTPSec：

```
22
23 # Comment this out if you have a refclock and want it to be able to
24 # the clock by itself (e.g. if the system is not connected to the n
25 tos minclock 4 #minsane 3
26 server 127.127.1.0 prefer
27 fudge 127.127.1.0 stratum 2
28
29 # Specify one or more NTP servers.
30
31 # Public NTP servers supporting Network Time Security:
32 # server time.cloudflare.com nts
33
34 # pool.ntp.org maps to about 1000 low-stratum NTP servers.  Your se
35 # pick a different set every time it starts up.  Please consider jo
36 # pool: <https://www.pool.ntp.org/join.html>
37 #pool 0.debian.pool.ntp.org iburst
38 #pool 1.debian.pool.ntp.org iburst
39 #pool 2.debian.pool.ntp.org iburst
40 #pool 3.debian.pool.ntp.org iburst
41
```

2、Chrony：

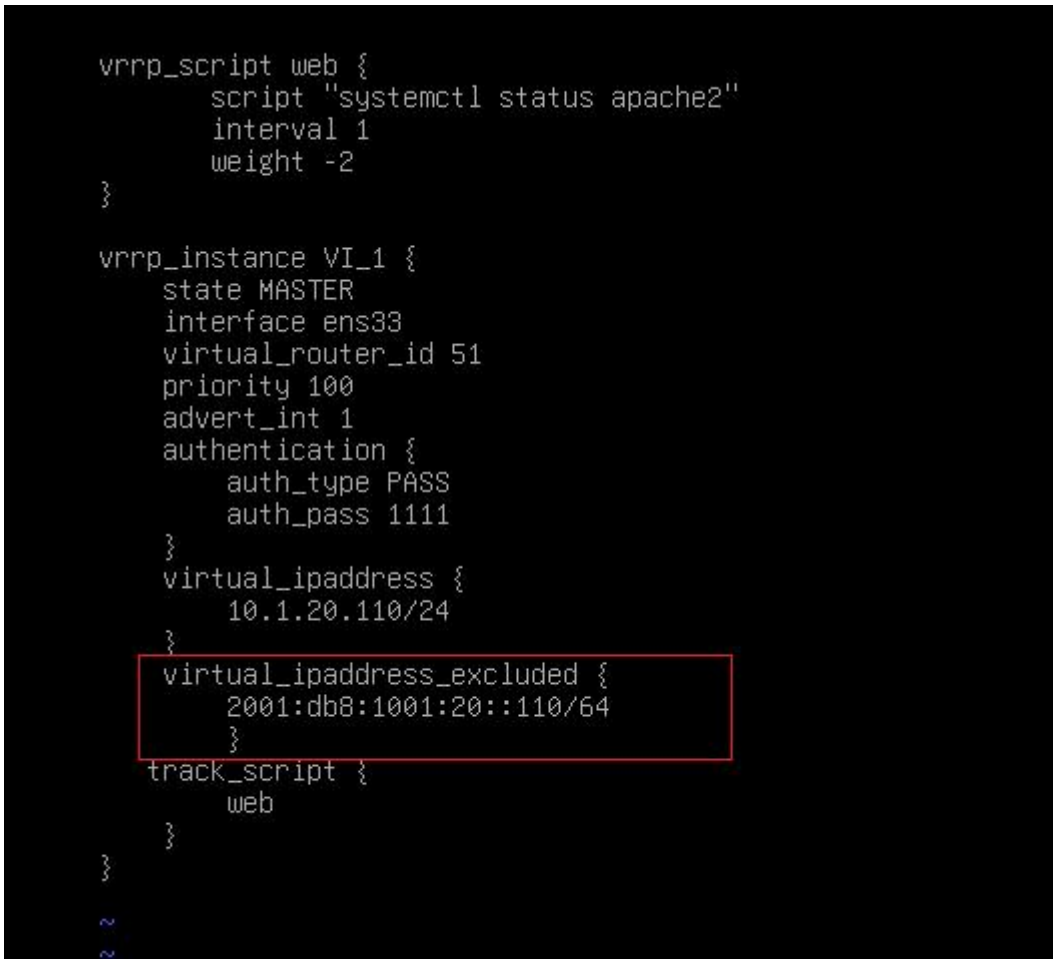


十五、Keepalived：

•配置 keepalived 抢占时，优先级不能是 255，否则不会被抢占

•记得看题目，判断 keepalived ip 是否需要写掩码

•配置 IPv6 虚拟地址：



如果记不住，配置两个 vrrp instance 也可以

十六、磁盘：

1、为磁盘创建分区：

```
fdisk   /dev/sdb   //指定要创建分区的磁盘
n   //创建分区
p
默认为 1   //指定分区的数量
默认
默认
w   /完成
```

2、raid：

```
apt install -y mdadm
```

RAID 会按照最小磁盘的大小来计算，例如三块盘：10G、20G、30G，会按照 10G 为标准来计算 RAID 磁盘大小

注意：RAID 冗余盘和热备盘不是一个东西，热备盘是手动使用 -x 指定的，可以不指定，冗余盘是根据不同的格式固定的

下面都是只计算冗余盘，不计算热备盘，因为热备盘不参与计算，要添加热备盘直接额外加 -x 添加即可

配置 raid 1：

最少需要 2 块磁盘，RAID 磁盘大小等于单块磁盘大小：
不论添加多少块磁盘，容量大小都不变，都等于单块磁盘大小，因为只有一块磁盘用来存储数据，剩下的磁盘全部用来做备份
mdadm -C /dev/md1 -l 1 -n 2 /dev/sd[bc]

配置 raid 5：

最少需要 3 块磁盘，固定一块冗余磁盘，剩余两块存储数据
假如最终 RAID 大小要为 20G：
3 块磁盘（1 块冗余），每块 10G
5 块磁盘（1 块冗余），每块 5G
mdadm -C /dev/md5 -l 5 -n 3 /dev/sd[bcd]

配置 raid 6：

最少需要 4 块磁盘，固定需要 2 块磁盘冗余，最终 RAID 磁盘大小为减去两块磁盘后 剩余磁盘大小的总和
假如最终 RAID 大小要 20G：
4 块磁盘（2 块冗余），每块 10G
6 块磁盘（2 块冗余），每块 5G
mdadm -C /dev/md6 -l 6 -n 4 /dev/sd[bcde]

配置 raid 10：

最少需要 4 块磁盘，磁盘数量必须是偶数，一半的磁盘会被用作冗余磁盘，磁盘大小等于磁盘数量 除于 2 之后的总和
假如最终 RAID 大小要 20G：
4 块磁盘（2 块冗余），每块 10G
8 块磁盘（4 块冗余），每块 5G
mdadm -C /dev/md10 -l 10 -n 4 /dev/sd[bcde]

配置 raid 50：

RAID 50 = 多个 RAID 5，再做 RAID 0
最少磁盘数量 6 块，假如有两组 raid 5 阵列（每组固定一块冗余磁盘），就可以对它们做 raid 0
假如 RAID 磁盘大小需要为 20G：
6 块磁盘（分成两组，每组一块冗余盘），每块 5G

```
# 创建两个 RAID5：
mdadm -C /dev/md51 -l 5 -n 3 /dev/sd[bcd]
mdadm -C /dev/md52 -l 5 -n 3 /dev/sd[efg]

# 做成 RAID50：
mdadm -C /dev/md50 -l 0 -n 2 /dev/md51 /dev/md52
```

配置 raid 60：
与 raid 50 一样，但是每组固定要 2 块冗余磁盘

```
# 最少磁盘数量 8 块，假如有两组 raid 6 阵列（每组固定两块冗余磁盘），就可以对它们做 raid 0
假如 RAID 磁盘大小需要为 20G：
8 块磁盘（分成两组，每组两块冗余盘），每块 5G
# 创建两个 RAID6：
mdadm -C /dev/md61 -l 6 -n 4 /dev/sd[bcde]
mdadm -C /dev/md62 -l 6 -n 4 /dev/sd[fghi]

# 做成 RAID60：
mdadm -C /dev/md60 -l 0 -n 2 /dev/md61 /dev/md62
```

3、lvm：

```
pvcreate /dev/sdb
vgcreate vg01 /dev/sdb
lvcreate -L 1G -n lv01 vg01

apt install -y  xfsdump
mkfs.xfs /dev/vg01/lv01
或用 mkfs.ext4 ...
```

4、NFS（TCP 2049）：

•将所有用户的请求映射为 匿名用户：

（1）配置 服务端：

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

mkdir /test
```

chown nobody:nogroup /test　//只有配置了这条才能生效

vim /etc/exports

共享目录的所属者、所属组和 exports 文件中定义的 uid 要一样

将 all_squash 改为 root_squash 即可

AppSrv (1)

```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/test   *(rw,sync,no_subtree_check,all_squash,anonuid=65534,anongid=65534)
```

exportfs -av

（2）配置 客户端：

apt install -y nfs-client

mkdir /test

vim /etc/fstab

AutoSrv (1)

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/vda1 during installation
UUID=99b0fe5f-9c60-4a09-8bbd-ff75c8b1ef97 /               ext4    errors=remount-ro 0       1
# swap was on /dev/vda5 during installation
UUID=d7612e50-67ab-4088-b82a-a49629225e4d none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
192.168.1.1:/test       /test   nfs4    defaults        0       0
```

```
root@AutoSrv:~# systemctl daemon-reload
root@AutoSrv:~# mount -a
root@AutoSrv:~# df -h
Filesystem         Size  Used Avail Use% Mounted on
udev               962M     0  962M   0% /dev
tmpfs              197M  640K  197M   1% /run
/dev/vda1           19G  1.9G   16G  11% /
tmpfs              984M     0  984M   0% /dev/shm
tmpfs              5.0M     0  5.0M   0% /run/lock
tmpfs              197M     0  197M   0% /run/user/0
192.168.1.1:/test   19G  1.4G   17G   8% /test
root@AutoSrv:~# ls -la /test
total 8
drwxr-xr-x  2 nobody nogroup 4096 May  8 13:35 .
drwxr-xr-x 22 root   root    4096 May  8 13:50 ..
root@AutoSrv:~# ls
root@AutoSrv:~# _
```

•映射为其它普通用户：

如果要映射为其它普通用户，就在服务器上将属组改为普通用户，exportfs 文件中的 uid 也要改为它，同时客户端和服务器都需要同时创建该用户（uid 最好要一样）

假如要映射为 skills 用户：

server：

```
#
/test    *(rw,sync,no_subtree_check,root_squash,anonuid=1000,anongid=1000)
~
```

```
root@AppSrv:~# chown -R skills. /test
chown: warning: '.' should be ':': ‘skills.’
root@AppSrv:~#
```

client：

```
root@AutoSrv:~# systemctl daemon-reload
root@AutoSrv:~# mount -a
root@AutoSrv:~# df -h
Filesystem         Size  Used Avail Use% Mounted on
udev               962M     0  962M   0% /dev
tmpfs              197M  640K  197M   1% /run
/dev/vda1           19G  1.9G   16G  11% /
tmpfs              984M     0  984M   0% /dev/shm
tmpfs              5.0M     0  5.0M   0% /run/lock
tmpfs              197M     0  197M   0% /run/user/0
192.168.1.1:/test   19G  1.4G   17G   8% /test
root@AutoSrv:~# ls -la /test
total 8
drwxr-xr-x  2 skills skills 4096 May  8 13:35 .
drwxr-xr-x 22 root   root   4096 May  8 13:50 ..
root@AutoSrv:~#
```

十七、FTP（TCP 20、21；990）：

1、vsftpd：

•定义根目录：

```
158 local_root=/ftp
:set nu
```

指定用户根目录（必须要有写入权限）

```
anon_root=/anon
```

•允许匿名用户 上传、删除文件：

```
39 # obviously need to create a directory writable by the
40 anon_upload_enable=YES
41 #
42 # Uncomment this if you want the anonymous FTP user to
43 # new directories.
44 anon_mkdir_write_enable=YES
45 anon_other_write_enable=YES
46 #
```

取消注释（允许匿名用户上传文件）

取消注释（允许匿名用户创建目录）

这条是新增的（允许匿名用户修改、删除 文件）

•显式 ftp：

```
152 rsa_cert_file=/etc/ssl/ftp.crt
153 rsa_private_key_file=/etc/ssl/ftp.key
154 ssl_enable=YES
```

•隐式 ftp:

```
152 rsa_cert_file=/etc/ssl/ftp.crt
153 rsa_private_key_file=/etc/ssl/ftp.key
154 ssl_enable=YES
155 implicit_ssl=yes
156 listen_port=990
157
158
```

启用隐式ftp

设置监听端口为 990

•chroot：

```
114 chroot_local_user=YES
115 allow_writeable_chroot=YES
```

•被动模式：

需要指定一个地址，这个地址就是 防火墙的地址

```
143 #
144 # This string is the name of the PAM service vsftpd
145 pam_service_name=vsftpd
146 #
147 # This option specifies the location of the RSA cert
148 # encrypted connections.
149 rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
150 rsa_private_key_file=/etc/ssl/private/ssl-cert-snake
151 ssl_enable=NO
152
153 #
154 # Uncomment this to indicate that vsftpd use a utf8
155 #utf8_filesystem=YES
156
157 pasv_enable=yes
158 pasv_min_port=30000
159 pasv_max_port=40000
160 pasv_address=1.1.1.1
:q
```

2、proftpd：

•允许匿名用户登陆：

```
164  <Anonymous ~ftp>
165    User ftp
166    Group nogroup
167    # We want clients to be able to login with "anonymous" as well as "ftp"
168    UserAlias anonymous ftp
169    # Cosmetic changes, all files belongs to ftp user
170    DirFakeUser on ftp
171    DirFakeGroup on ftp
172
173    RequireValidShell off
174
175    # Limit the maximum number of anonymous logins
176    MaxClients 10
177
178    # We want 'welcome.msg' displayed at login, and '.message' displayed
179    # in each newly chdired directory.
180    DisplayLogin welcome.msg
181    DisplayChdir .message
182
183    # Limit WRITE everywhere in the anonymous chroot
184    <Directory *>
185      <Limit WRITE>
186        DenyAll
187      </Limit>
188    </Directory>
189
190    # Uncomment this if you're brave.
191    # <Directory incoming>
192    #   # Umask 022 is a good standard umask to prevent new files and dirs
193    #   # (second parm) from being group and world writable.
194    #   Umask 022  022
195    #   <Limit READ WRITE>
196    #     DenyAll
                                                          191,1         91%
```

匿名可写：

```
170    DirFakeUser on ftp
171    DirFakeGroup on ftp
172
173    RequireValidShell off
174
175    # Limit the maximum number of anonymous logins
176    MaxClients 10
177
178    # We want 'welcome.msg' displayed at login, and '.message' displayed
179    # in each newly chdired directory.
180    DisplayLogin welcome.msg
181    DisplayChdir .message
182
183    # Limit WRITE everywhere in the anonymous chroot
184    <Directory *>
185      <Limit WRITE>
186        #DenyAll
187        allowall
188      </Limit>
189    </Directory>
190
191    # Uncomment this if you're brave.
192    # <Directory incoming>
193    #   # Umask 022 is a good standard umask to prevent new files and dirs
194    #   # (second parm) from being group and world writable.
195    #   Umask 022  022
196    #   <Limit READ WRITE>
197    #     DenyAll
198    #     </Limit>
199    #       <Limit STOR>
200    #         AllowAll
201    #     </Limit>
202    # </Directory>
203
204  </Anonymous>
```

注释 DenyAll，添加 allowall 即可

•隐式 ssl：

```
apt install -y proftpd proftpd-mod-crypto
```

注意要安装 crypto 这个软件包，否则 ssl 无法起来

vim /etc/proftpd/proftpd.conf

```
#
# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#

# Includes DSO modules
Include /etc/proftpd/modules.conf

Include /etc/proftpd/tls.conf

```

vim /etc/proftpd/modules.conf

取消注释

```
ModuleControlsACLs insmod,rmmod allow user root
ModuleControlsACLs lsmod allow user *

#This is required only if you need to set IdentLookups on
#LoadModule mod_ident.c

LoadModule mod_ctrls_admin.c

# Debian #1103154: needed to make default config executable
LoadModule mod_delay.c
LoadModule mod_ls.c
LoadModule mod_xfer.c

# Install proftpd-mod-crypto to use this module for TLS/SSL support.
LoadModule mod_tls.c
# Even these modules depend on the previous one
#LoadModule mod_tls_fscache.c
#LoadModule mod_tls_shmcache.c

# Install one of proftpd-mod-mysql, proftpd-mod-pgsql or any other
# SQL backend engine to use this module and the required backend.
# This module must be mandatory loaded before anyone of
# the existent SQL backeds.
#LoadModule mod_sql.c

# Install proftpd-mod-ldap to use this for LDAP support.
#LoadModule mod_ldap.c

#
```

vim /etc/proftpd/tls.conf

UseImplicitSSL 需要背，没得抄

```
  8
  9 <IfModule mod_tls.c>
 10 TLSEngine                              on
 11 TLSLog                                /var/log/proftpd/tls.log
 12 TLSProtocol                           SSLv23
 13 #
 14 # Server SSL certificate. You can generate a self-signed certificate using
 15 # a command like:
 16 #
 17 # openssl req -x509 -newkey rsa:1024 \
 18 #          -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
 19 #          -nodes -days 365
 20 #
 21 # The proftpd.key file must be readable by root only. The other file can be
 22 # readable by anyone.
 23 #
 24 # chmod 0600 /etc/ssl/private/proftpd.key
 25 # chmod 0640 /etc/ssl/private/proftpd.key
 26 #
 27 TLSRSACertificateFile                  /etc/ssl/ssl.crt
 28 TLSRSACertificateKeyFile               /etc/ssl/ssl.key
 29 #
 30 # CA the server trusts...
 31 TLSCACertificateFile                    /etc/ssl/ca.crt
 32 # ...or avoid CA cert and be verbose
 33 TLSOptions              UseImplicitSSL
 34 # ... or the same with relaxed session use for some clients (e.g. FireFtp)
 35 #TLSOptions                    NoCertRequest EnableDiags NoSessionReuseRequired
 36 #
:set nu                                                          14,1          Top
```

```
 29 #
 30 # CA the server trusts...
 31 #TLSCACertificateFile                  /etc/ssl/certs/CA.pem
 32 # ...or avoid CA cert and be verbose
 33 #TLSOptions                    NoCertRequest EnableDiags
 34 TLSOptions      UseImplicitSSL
 35 # ... or the same with relaxed session use for some clients (e.g. FireFtp)
 36 #TLSOptions                    NoCertRequest EnableDiags NoSessionReuseRequired
 37 #
 38 #
 39 # Per default drop connection if client tries to start a renegotiate
 40 # This is a fix for CVE-2009-3555 but could break some clients.
 41 #
 42 TLSOptions                                                AllowClientRenegotiations
 43 #
 44 # Authenticate clients that want to use FTP over TLS?
 45 #
 46 TLSVerifyClient                        off
 47 #
 48 # Are clients required to use FTP over TLS when talking to this server?
 49 #
 50 TLSRequired                            on
 51 #
 52 # Allow SSL/TLS renegotiations when the client requests them, but
 53 # do not force the renegotations.  Some clients do not support
 54 # SSL/TLS renegotiations; when mod_tls forces a renegotiation, these
 55 # clients will close the data connection, or there will be a timeout
 56 # on an idle data connection.
 57 #
 58 #TLSRenegotiate                        required off
 59 </IfModule>
 60
                                                                  56,1          Bot
```

•显式 ssl：

与上面隐式加密配置一样，甚至配置更少，只要不将端口改为 990，保持默认的 21，也不添加 UseImplicitSSL 配置即是显示加密

•chroot：

指定目录后自动配置：

```
#
# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#

# Includes DSO modules
Include /etc/proftpd/modules.conf
Include /etc/proftpd/tls.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 on
# If set on you can experience a longer connection delay in many cases.
<IfModule mod_ident.c>
  IdentLookups off
</IfModule>

defaultroot /ftp
ServerName "Debian"
# Set to inetd only if you would run proftpd by inetd/xinetd/socket.
# Read README.Debian for more information on proper configuration.
ServerType standalone
DeferWelcome off

# Disable MultilineRFC2228 per https://github.com/proftpd/proftpd/issues/1085
# MultilineRFC2228on
DefaultServer on
ShowSymlinks on

TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200
:q
```

•被动模式：

vim /etc/proftpd/proftpd.conf

```
32 TimeoutIdle 1200
33
34 DisplayLogin welcome.msg
35 DisplayChdir .message true
36 ListOptions "-l"
37
38 DenyFilter \*.*/
39
40 # Use this to jail all users in their homes
41 # DefaultRoot ~
42
43 # Users require a valid shell listed in /etc/shells to login.
44 # Use this directive to release that constrain.
45 # RequireValidShell off
46
47 # Port 21 is the standard FTP port.
48 Port 21
49
50 # In some cases you have to specify passive ports range to by-pass
51 # firewall limitations. Ephemeral ports can be used for that, but
52 # feel free to use a more narrow range.
53 PassivePorts 49000 50000
54
55 # If your host was NATted, this option is useful in order to
56 # allow passive tranfers to work. You have to use your public
57 # address and opening the passive ports used on your firewall as well.
58 MasqueradeAddress 192.168.20.254
59
60 # This is useful for masquerading address with dynamic IPs:
61 # refresh any configured MasqueradeAddress directives every 8 hours
62 <IfModule mod_dynmasq.c>
63 # DynMasqRefresh 28800
:x
```

十八、数据库：

1、mysql（TCP 3306）：

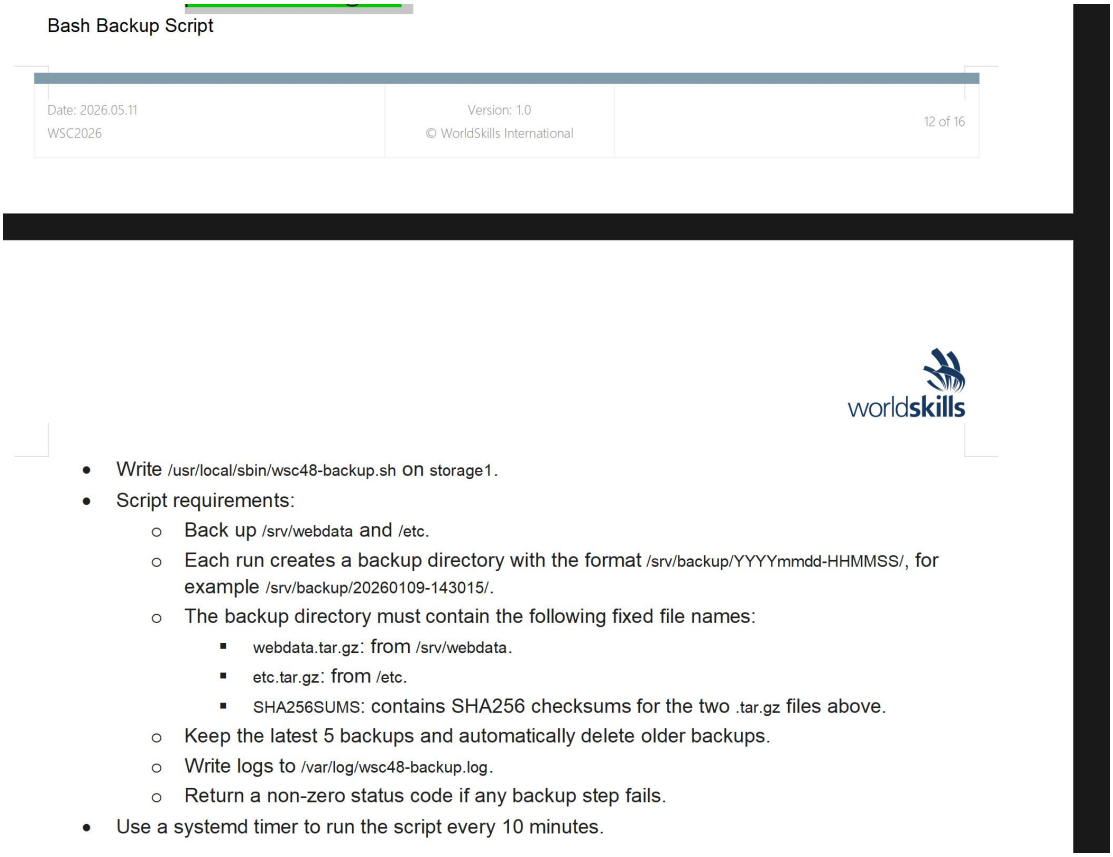
```
# 创建数据库、用户：
create database wordpress;
grant all privileges on wordpress.* to 'admin'@'172.16.1.101' identified by 'Skills39';
flush privileges;
```

十九、fail2ban：

二十、cron：

```
* * * * *  //每分钟
*/2 * * * *  //每 2 分钟
*/3 * * * *  //每 3 分钟
0 * * * *  //每小时
0 0 * * *  //每天
0 1 * * *  //每天 01:00
0 2 * * 1  //每周一 02:00
```

二十一：system timer：



1、编写脚本：

vim /usr/local/sbin/wsc48-backup.sh

```
#!/bin/bash

date=$(date +%Y%m%d-%H%M%S)

mkdir -p /srv/backup/$date || exit 1

tar -czf /srv/backup/$date/webdata.tar.gz /srv/webdata || exit 1

tar -czf /srv/backup/$date/etc.tar.gz /etc || exit 1

cd /srv/backup/$date

sha256sum webdata.tar.gz etc.tar.gz > SHA256SUMS || exit 1

echo "Time:$date Backup Success" >> /var/log/wsc48-backup.log

ls -dt /srv/backup/*/ 2>/dev/null | tail -n +6 | xargs -r rm -rf
```

chmod +x wsc48-backup.sh

2、配置为 systemd：

cd /etc/systemd/system/
cp sshd.service wsc48-backup.service
vim wsc48-backup.service

```
[Unit]

[Service]
ExecStart=/usr/local/sbin/wsc48-backup.sh
Type=oneshot

[Install]
WantedBy=multi-user.target
```

systemctl daemon-reload
systemctl restart wsc48-backup

3、配置 systemd timer：

cd /etc/systemd/system/
cp /usr/lib/systemd/system/man-db.timer wsc48-backup.timer
vim wsc48-backup.timer　//timer 需要有一个同名的 .service
配置为每 10 分钟运行一次

```
[Unit]

[Timer]
OnCalendar=*:0/10
Persistent=true

[Install]
WantedBy=multi-user.target
```

但是这个配置是在 每小时的第 0、10、20 分钟进行执行，但是如果是每隔 7 分钟，就是从每小时的 0、7、14 … 56，但是这里差 4 分钟就到下一个小时了，因此不是严格的每 7 分钟运行一次，要配置严格每 7 分钟运行一次需要配置：

```
[Unit]

[Timer]
OnBootSec=7m
OnUnitActiveSec=7m
Persistent=true

[Install]
WantedBy=timers.target
```

```
# 启动计时器：
systemctl enable wsc48-backup.timer --now
```

查看计时器下一次执行时间

```
root@storage1:/srv/backup# systemctl list-timers | grep wsc48
Tue 2026-05-19 21:50:00 CST           9min Tue 2026-05-19 21:40:01 CST 44s ago wsc48-backup.timer          wsc48-backup.service
root@storage1:/srv/backup#
```

二十二：日志（TCP/UDP 514）：

1、根据主机名来定义 日志文件存储文件名：

vim /etc/rsyslog.conf

```
 9 ##################
10
11 module(load="imuxsock") # provides support for local system logging
12 module(load="imklog")   # provides kernel logging support
13 #module(load="immark")  # provides --MARK-- message capability
14
15 # provides UDP syslog reception
16 #module(load="imudp")
17 #input(type="imudp" port="514")
18
19 # provides TCP syslog reception
20 module(load="imtcp")
21 input(type="imtcp" port="514")
22
23 input(type="imtcp" port="6514" ruleset="remote")
24
25 template(name="dmz_log" type="string"
26         string="/var/log/dmz/%hostname%.log")
27
28 ruleset(name="remote") {
29         action(
30         type="omfile"
31         dynaFile="dmz_log"
32         createDirs="on"
33         )
34 }
35
```