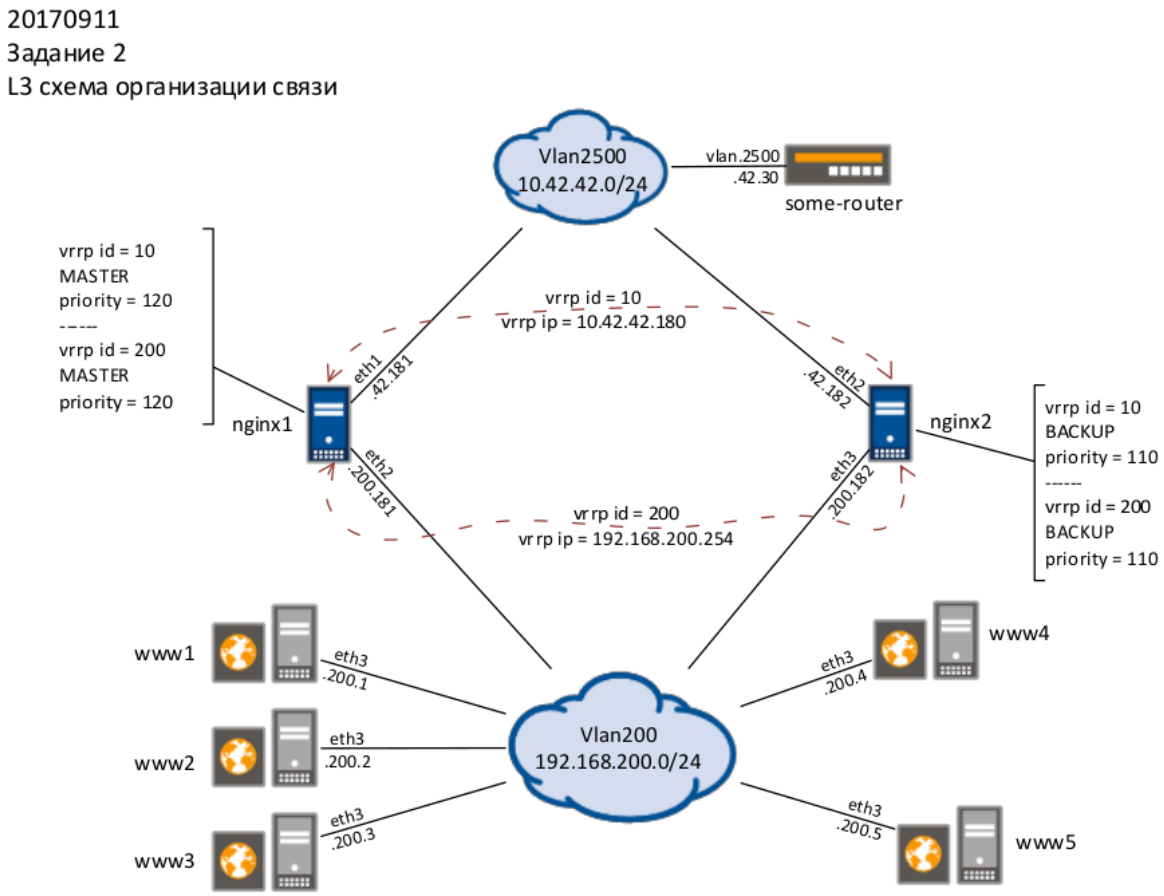
20170911
Ермошин К.С.
Отчет по заданию 2.

1 L3 схема



2 Концепция

На сервера nginx1 и nginx2 установлен Centos 6.9 в минимальной поставке.

Каждый сервер имеет по два интерфейса. Первыми интерфейсами сервера смотрят во внешнюю сеть 10.42.42.0/24 (принимаем допущение, что сеть 10.42.42.0/24 глобально маршрутизируема), вторыми во внутреннюю сеть 192.168.200.0/24.

Есть сайт www.domain.ru. А-запись для этого адреса указывает на 10.42.42.180.

Есть сервера www[1..5], стоящие в сети 192.168.200.0/24, отвечающие за статическую и динамическую составляющую сайта www.domain.ru.

Задачи серверов nginx1 и nginx2:
– Опубликовать ip адрес 10.42.42.180.
– Работать как шлюз по умолчанию для серверов www[1..5] и выпускать их в интернет.
– Работать в отказоустойчивом схеме active/passive, выход из строя одного из серверов не должен привести к недоступности сайта www.domain.ru.
– Сервера должны проксировать и распределять запросы к сайту www.domain.ru между серверами www[1..5]. Сервера www[1..3] обрабатывают динамический контент сайта, сервера www[4..5] статический.

2.1 VRRP

IP адрес сайта 10.42.42.180 будет опубликован серверами nginx1\2 с помощью протокола VRRP.

В Linux за работу протокола VRRP отвечает ПО keepalived.

 # yum info keepalived
Loaded plugins: fastestmirror
...
Installed Packages
Name : keepalived
Arch : i686
Version : 1.2.13
Release : 5.el6_6
Size : 607 k
Repo : installed
From repo : base
Summary : Load balancer and high availability service
URL : http://www.keepalived.org/
License : GPLv2+
Description : Keepalived provides simple and robust facilities for load balancing
: and high availability. The load balancing framework relies on the
: well-known and widely used Linux Virtual Server (IPVS) kernel module
: providing layer-4 (transport layer) load balancing. Keepalived
: implements a set of checkers to dynamically and adaptively maintain
: and manage a load balanced server pool according their health.
: Keepalived also implements the Virtual Router Redundancy Protocol
: (VRRPv2) to achieve high availability with director failover.

Так же, со стороны сети 192.168.200.0/24, будет запущен второй VRRP процесс который опубликует адрес 192.168.200.254. Этот адрес будут использовать сервера www[1..5] как шлюз по умолчанию для выхода в интернет.

Nginx1, в обоих VRRP процессах, будет основным сервером, а nginx2 резервным.

2.2 Шлюз по умолчанию для www[1...5]

На серверах nginx1\2 будет разрешено прохождение транзитного трафика между интерфейсами и настроен source nat из сети в 192.168.200.0/24 в интернет.

Обратиться напрямую к серверам www[1..5], со стороны интернета, будет нельзя.

2.3 NGINX

Проксировать и распределять запросы к сайту www.domain.ru на серверах nginx1\2 будет веб-сервер nginx.

 # yum info nginx
Loaded plugins: fastestmirror
...
Installed Packages
Name : nginx
Arch : i386
Version : 1.12.1
Release : 1.el6.ngx
Size : 2.4 M
Repo : installed
From repo : nginx
Summary : High performance web server
URL : http://nginx.org/
License : 2-clause BSD-like license
Description : nginx [engine x] is an HTTP and reverse proxy server, as well as
: a mail proxy server.

В nginx задаем две группы серверов – BACKEND-STATIC и BACKEND-DYNAMIC.
Группке BACKEND-STATIC будут отправлены запросы которые заканчиваются расширениями популярных графических форматов (jpg|jpeg|gif|png|pdf|bmp).
Группа BACKEND-DYNAMIC будет обрабатывать все остальные запросы.

Каждому серверу в группе выставлен вес **10**, тип балансировки **round-robin.**

Одному из серверов в каждой группе изменены дефолтные значения max_fails и fail_timeout. Сделано это для того, что бы при кратковременных проблемах в сети 192.168.200.0/24 не все сервера разом выпали из работы.

Входящий трафик сайта будет приходтить на один из серверов nginx1\2. На какой конкретно будет зависить от того, с какого сервера VRRP публикует адрес 10.42.42.180.

3 Конфигурации.

3.1 NGINX

Конфигурации на серверах nginx1 и nginx2 одинаковые.

```
[root@nginx1 ~]# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful

[root@nginx1 ~]# cat /etc/nginx/nginx.conf
user  nginx;
worker_processes  1;

error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;


events {
    worker_connections  1024;
}

http {
## DEF CONFIG ###
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    keepalive_timeout  65;

    #gzip  on;

#    include /etc/nginx/conf.d/*.conf;
## /DEF CONFIG ###

    upstream BACKEND-DYNAMIC {
        server 192.168.200.1 weight=10;
        server 192.168.200.2 weight=10 max_fails=3 fail_timeout=30s;
        server 192.168.200.3 weight=10;
    }
    upstream BACKEND-STATIC {
        server 192.168.200.4 weight=10;
        server 192.168.200.5 weight=10 max_fails=3 fail_timeout=30s;
    }
```

```
    server {
        listen       80;
        server_name  www.domain.ru;

     location / {
        proxy_pass http://BACKEND-DYNAMIC;
     }

     location ~* ^.+\.(jpg|jpeg|gif|png|pdf|bmp)$ {
        proxy_pass http://BACKEND-STATIC;
     }

    }
}
```

3.2 Настройки сети

nginx1

[root@nginx1 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=08:00:27:A5:D4:17
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
IPADDR=10.42.42.181
PREFIX=24
GATEWAY=10.42.42.30
DNS1=8.8.8.8
DEFROUTE=yes

[root@nginx1 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
HWADDR=08:00:27:62:15:A9
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
IPADDR=192.168.200.181
PREFIX=24

nginx2

[root@nginx2 run]# cat /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
HWADDR=08:00:27:76:11:38
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
IPADDR=10.42.42.182
PREFIX=24
GATEWAY=10.42.42.30
DNS1=8.8.8.8
DEFROUTE=yes

[root@nginx2 run]# cat /etc/sysconfig/network-scripts/ifcfg-eth3
DEVICE=eth3
HWADDR=08:00:27:2B:D3:93
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
IPADDR=192.168.200.182
PREFIX=24

3.3 Keepalived

nginx1

```
[root@nginx1 ~]# cat /etc/keepalived/keepalived.conf
! Configuration File for keepalived

vrrp_instance VRRP-10  {
   state MASTER
   interface eth0
   virtual_router_id 10
   priority 120
   advert_int 1
   authentication {
      auth_type PASS
      auth_pass vrrp-pass-1
   }
   virtual_ipaddress {
      10.42.42.180
   }
}

vrrp_instance VRRP-200  {
   state MASTER
   interface eth1
   virtual_router_id 200
   priority 120
   advert_int 1
   authentication {
      auth_type PASS
      auth_pass vrrp-pass-1
   }
   virtual_ipaddress {
      192.168.200.254
   }
}
```

nginx2

```
[root@nginx2 run]# cat /etc/keepalived/keepalived.conf
! Configuration File for keepalived

vrrp_instance VRRP-10  {
    state BACKUP
    interface eth2
    virtual_router_id 10
    priority 110
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass vrrp-pass-1
    }
    virtual_ipaddress {
        10.42.42.180
    }
}

vrrp_instance VRRP-200  {
    state BACKUP
    interface eth3
    virtual_router_id 200
    priority 110
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass vrrp-pass-1
    }
    virtual_ipaddress {
        192.168.200.254
    }
}
```

3.4 Iptables

Конфигурация на серверах nginx1\2 в целом одинаковая, различаются только имена интерфейсов. На nginx2 eth0 меняется на eth2, а eth1 на eth3.

nginx1

```
[root@nginx1 ~]# cat /etc/sysconfig/iptables
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A POSTROUTING -o eth0 -s 192.168.200.0/24 -j MASQUERADE
COMMIT
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -i eth1 -o eth0 -j ACCEPT
-A FORWARD -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
#SSH
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -s 10.42.42.0/24 -j ACCEPT
#VRRP
-A INPUT -i eth0 -d 224.0.0.18/32 -p 112 -j ACCEPT
-A INPUT -i eth1 -d 224.0.0.18/32 -p 112 -j ACCEPT
#HTTP
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -d 10.42.42.180/32 -j ACCEPT
#LAST RULES
-A INPUT -j LOG -m limit --limit 30/minute --log-prefix "IN-R-ANY: "
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j LOG -m limit --limit 30/minute --log-prefix "FRW-R-ANY: "
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```