

# Отказоустойчивость: **Keepalived/vrrp.**



Александр  
Зубарев



## **Александр Зубарев**

Председатель цикловой комиссии “Информационной  
безопасности инфокоммуникационных систем”

АКТ (ф) СПбГУТ



[Александр Зубарев](#)

---

# Модуль «Отказоустойчивость»

## Цели модуля:

- Разобраться, как обеспечивается отказоустойчивая работа приложений;
- Изучить основные инструменты кластеризации и балансировки, а также принципы и инструменты резервного копирования;
- Узнать, что такое Disaster Recovery и как его можно реализовать.



---

# Структура модуля

1. Keepalived/vrrp.
2. Кластеризация.
3. Pacemaker.
4. Резервное копирование. Bacula.
5. Балансировка нагрузки. HAProxy/Nginx.
6. Disaster recovery.
7. Отказоустойчивость в облаке.

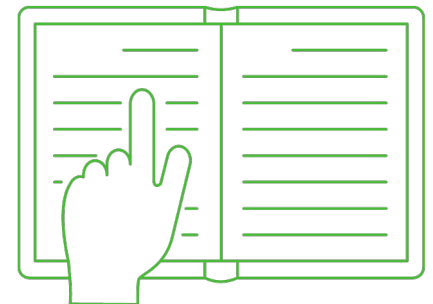


---

# Предисловие

## На этом занятии мы:

- поговорим о сетевой доступности, плавающих IP, протоколах резервирования виртуальных маршрутизаторов;
- посмотрим, как работает Keepalived и vrrp;
- настроим сервис для динамического перераспределения IP адреса для дальнейшего изучения работы кластеров различного назначения.





# План занятия

1. [Плавающие IP](#)
2. [Keepalived](#)
3. [Протоколы FHRP.VRRP](#)
4. [Настройка компонентов](#)
5. [Тестирование модели](#)
6. [Итоги](#)
7. [Домашнее задание](#)



# Плавающие IP



## Плавающие IP

**Плавающие IP (floating IPs)** — это публичные IP-адреса, которые могут перенаправляться системой на приватные IP.

Плавающие IP-адреса позволяют:

- быстро переназначить доступный адрес в пуле на свободный ресурс для увеличения доступности;
- контролировать узлы сети инфраструктуры;
- контролировать работу серверов (как следствие).



---

## Плавающие IP

Плавающие IP-адрес использует IP-адреса из виртуальных интерфейсов для маскировки исходящего трафика через интерфейсы:

- сетевое устройство (NIC);
- виртуальную локальную сеть (VLAN);
- интерфейс связывания (мосты).

Когда используется такой механизм, в сети кластера можно прозрачно распределять адреса между хостами.

## Плавающие IP

Для достижения максимально высокой доступности рекомендуется:

- использовать несколько устройств 3 уровня;
- использовать несколько серверов приложений.

Плавающий IP не меняет публичный IP-адрес, для его работы создаются статические адреса, которые впоследствии и используются для распределения.

---

## Плавающие IP

Если сервис развернут на 2 и более серверах кластера, будет происходить следующее:

- сервера будут реплицироваться между собой;
- исходящий трафик будет замаскирован;
- в случае отказа ip перейдет на другой узел.

Примечание: При конфигурировании кластерной инфраструктуры рекомендуется использовать плавающие IP-адреса.

---

# Представители, реализующие плавающие IP

- Keepalive;
- UCARP;
- clusterIP;



# Keepalived

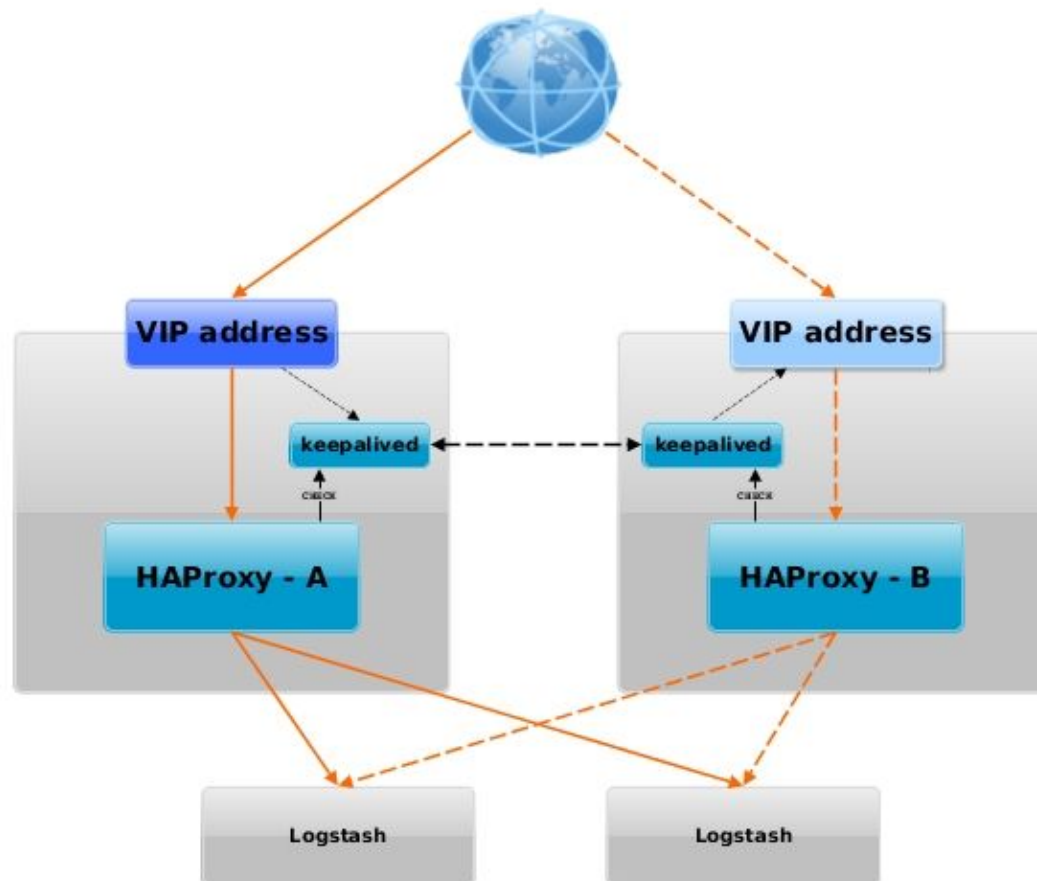


# Keepalived

**Keepalived** – сервис, который позволяет контролировать серверы и процессы для обеспечения высокой доступности инфраструктуры.

Демон keepalived может мониторить веб-серверы и автоматически передавать трафик второму серверу, если первый сервер не отвечает.

# Keepalived



[Ссылка на источник](#)



# Протоколы FHRP. VRRP





# Протоколы FHRP

**FHRP (First Hop Redundancy Protocol)** – это протоколы резервирования первого уровня. То есть это группа протоколов, которая позволяет обеспечить клиентов отказоустойчивым шлюзом.


# Представители протоколов FHRP

VRRP – Virtual Router Redundancy Protocol;

HSRP – Hot Standby Router Protocol, Hot Standby Redundancy Protocol;

CARP – Common Address Redundancy Protocol;

GLBP – Gateway Load Balancing Protocol.




# Протоколы резервирования виртуальных маршрутизаторов

**VRRP (протокол резервирования виртуальных маршрутизаторов)**

– это сетевой протокол, который обеспечивает автоматическое назначение доступных маршрутизаторов протокола Интернета (IP) участвующим хостам.


Данная технология увеличивает доступность и надежность маршрутизации путей за счет автоматического выбора шлюза по умолчанию в подсети IP .



## Протоколы резервирования виртуальных маршрутизаторов

Протокол реализует высокую доступность серверов путем создания виртуальных маршрутизаторов: основного и резервного, действующих как одна группа.


Виртуальный маршрутизатор назначается шлюзом по умолчанию для участвующих хостов вместо физического маршрутизатора.



## Протоколы резервирования виртуальных маршрутизаторов

Если основной маршрутизатор выходит из строя, то протокол позволяет переключиться на резервный маршрутизатор.

Физический маршрутизатор, который пересылает пакеты в любой момент времени, называется **главным маршрутизатором**.



## Протоколы резервирования виртуальных маршрутизаторов

VRRP предоставляет информацию о состоянии маршрутизатора, его активности, нагрузки, функционирования, обрабатываемых и обмениваемых этим маршрутизатором.

Объем каждого экземпляра VRRP ограничен одной локальной сетью.

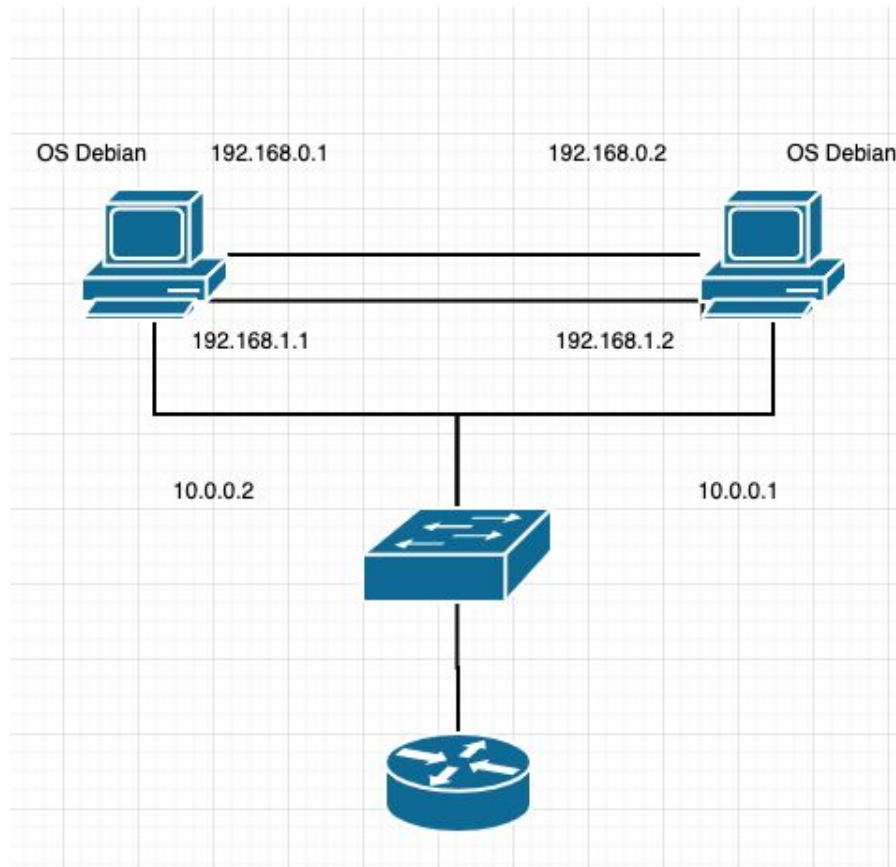
VRRP может использоваться в сетях Ethernet , MPLS и Token Ring с Интернет-протоколом версии 4 (IPv4), а также IPv6 .



# Настройка компонентов

# Модель сети

Для выполнения работы построим следующую топологию:





# Установка keepalived

Установим keepalived:

```
apt install keepalived
```

Установка должна проводиться на двух системах (нодах).

Файл конфигурации находится:

```
/etc/keepalived/keepalived.conf.
```

Если этого файла нет, его нужно создать:

```
touch /etc/keepalived/keepalived.conf
```

# Пример конфигурирование для первой ноды keeralived

```
vrrp_instance failover_test {
state MASTER
interface enp0s8
virtual_router_id 10
priority 110
advert_int 4
authentication {
auth_type AH
auth_pass 1111
}
unicast_peer {
192.168.0.1
}
    virtual_ipaddress {
192.168.0.50 dev enp0s8 label enp0s8:vip
}
}
```

# Запуск keepalived

Запуск службы:

```
systemctl start keepalived
```

Добавление службы в автозагрузку

```
systemctl enable keepalived
```

Проверка работоспособности сервиса:

```
systemctl status keepalived
```

# Запуск keepalived

```
● keepalived.service - Keepalive Daemon (LVS and VRRP)
   Loaded: loaded (/lib/systemd/system/keepalived.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-07-16 09:31:06 EDT; 27s ago
 Main PID: 14055 (keepalived)
    Tasks: 2 (limit: 1134)
   Memory: 4.1M
    CGroup: /system.slice/keepalived.service
            └─14055 /usr/sbin/keepalived --dont-fork
              └─14056 /usr/sbin/keepalived --dont-fork

Jul 16 09:31:06 nodeOne Keepalived_vrrp[14056]: Registering Kernel netlink command channel
Jul 16 09:31:06 nodeOne Keepalived_vrrp[14056]: Opening file '/etc/keepalived/keepalived.conf'.
Jul 16 09:31:06 nodeOne Keepalived_vrrp[14056]: (failover_test) Initial state master is incompatible
Jul 16 09:31:06 nodeOne Keepalived_vrrp[14056]: Registering gratuitous ARP shared channel
Jul 16 09:31:06 nodeOne Keepalived_vrrp[14056]: (failover_test) Entering BACKUP STATE (init)
Jul 16 09:31:19 nodeOne Keepalived_vrrp[14056]: (failover_test) Entering MASTER STATE
Jul 16 09:31:19 nodeOne Keepalived_vrrp[14056]: (failover_test) IPSEC-AH : sequence number 1 already
Jul 16 09:31:23 nodeOne Keepalived_vrrp[14056]: (failover_test) IPSEC-AH : sequence number 2 already
Jul 16 09:31:27 nodeOne Keepalived_vrrp[14056]: (failover_test) IPSEC-AH : sequence number 3 already
Jul 16 09:31:31 nodeOne Keepalived_vrrp[14056]: (failover_test) IPSEC-AH : sequence number 4 already
```

## Пример конфигурирования для второй ноды keeralived

```
vrrp_instance failover_test {
state BACKUP
interface enp0s8
virtual_router_id 10
priority 110
advert_int 4
authentication {
auth_type AH
auth_pass 1111
}
unicast_peer {
192.168.0.2
}
    virtual_ipaddress {
192.168.0.50 dev enp0s8 label enp0s8:vip
}
}
```

# Запуск keepalived на второй ноде

Запуск службы:

```
systemctl start keepalived
```

Добавление службы в автозагрузку:

```
systemctl enable keepalived
```

Проверка работоспособности сервиса:

```
systemctl status keepalived
```

# Запуск keepalived на второй ноде

```
● keepalived.service – Keepalive Daemon (LVS and VRRP)
   Loaded: loaded (/lib/systemd/system/keepalived.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-07-16 09:36:50 EDT; 5s ago
 Main PID: 11046 (keepalived)
    Tasks: 2 (limit: 1134)
   Memory: 4.0M
    CGroup: /system.slice/keepalived.service
            └─11046 /usr/sbin/keepalived --dont-fork
              └─11047 /usr/sbin/keepalived --dont-fork

Jul 16 09:36:50 nodeTwo Keepalived[11046]: Starting Keepalived v2.0.10 (11/12,2018)
Jul 16 09:36:50 nodeTwo Keepalived[11046]: Running on Linux 4.19.0-17-amd64 #1 SMP Debian 4.19.194-
Jul 16 09:36:50 nodeTwo Keepalived[11046]: Command line: '/usr/sbin/keepalived' '--dont-fork'
Jul 16 09:36:50 nodeTwo Keepalived[11046]: Opening file '/etc/keepalived/keepalived.conf'.
Jul 16 09:36:50 nodeTwo Keepalived[11046]: Starting VRRP child process, pid=11047
Jul 16 09:36:50 nodeTwo Keepalived_vrrp[11047]: Registering Kernel netlink reflector
Jul 16 09:36:50 nodeTwo Keepalived_vrrp[11047]: Registering Kernel netlink command channel
Jul 16 09:36:50 nodeTwo Keepalived_vrrp[11047]: Opening file '/etc/keepalived/keepalived.conf'.
Jul 16 09:36:50 nodeTwo Keepalived_vrrp[11047]: Registering gratuitous ARP shared channel
Jul 16 09:36:50 nodeTwo Keepalived_vrrp[11047]: (failover_test) Entering BACKUP STATE (init)
```

# Проверка настройки

Запуск службы:

`ifconfig` или `ip add`.

В итоге получим:

```
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:43:f8:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.1/24 brd 192.168.0.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet 192.168.0.50/32 scope global enp0s8:vip
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe43:f8d2/64 scope link
        valid_lft forever preferred_lft foreve
```

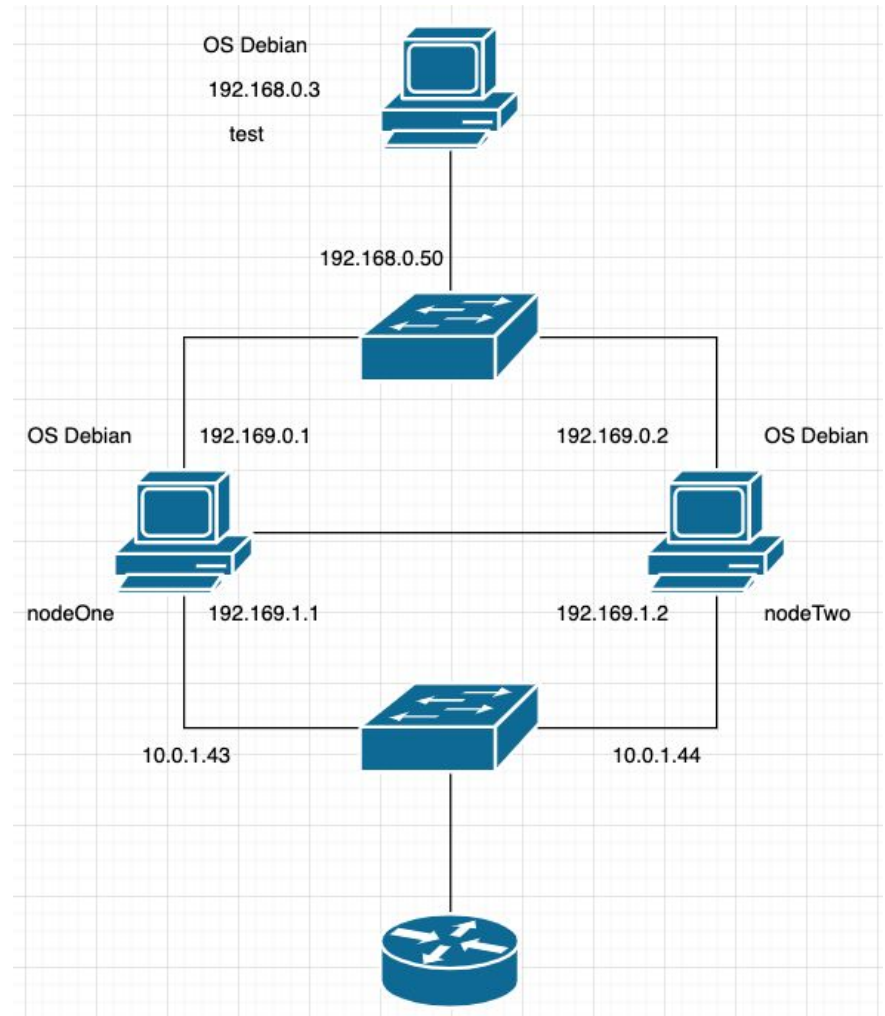




# Тестирование модели

# Тестирование

Для проверки доступности хоста после изменения нужна третья виртуальная машина.



# Тестирование

Запускаем:

```
ip link set dev enp0s8 down
```

Проверяем вторую ноду:

на интерфейсе `enp0s8` должен измениться адрес на виртуальный.

# Тестирование

Запускаем `tcpdump` и смотрим, как это происходит.

Видим, что:

- ICMP пакеты сначала отправляются на MAC-адрес MASTER хоста;
- потом после отключения на нем интерфейса `enp0s8`, запросы начинают идти на MAC-адрес BACKUP;
- после восстановления работы интерфейса запросы снова идут на MASTER сервер.

---

# Итоги

## Сегодня мы:

- поговорили о том, что такое плавающий IP и для чего он нужен;
- узнали, какие сервисы бывают, какие протоколы работают в данной концепции;
- рассмотрели метод создания такого рода сервиса, его работу и принцип действия.





# Домашнее задание

---

# Домашнее задание

Давайте посмотрим ваше [домашнее задание](#).

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

**Задавайте вопросы и  
пишите отзыв о лекции!**

**Александр Зубарев**