

Зеркалирование трафика хоста в VM

Введение

Описание демонстрационного стенда

Настройка зеркалирования

Мониторинг входящего трафика

Окружение

- Версия РЕД ВИРТ: 7.3

Введение

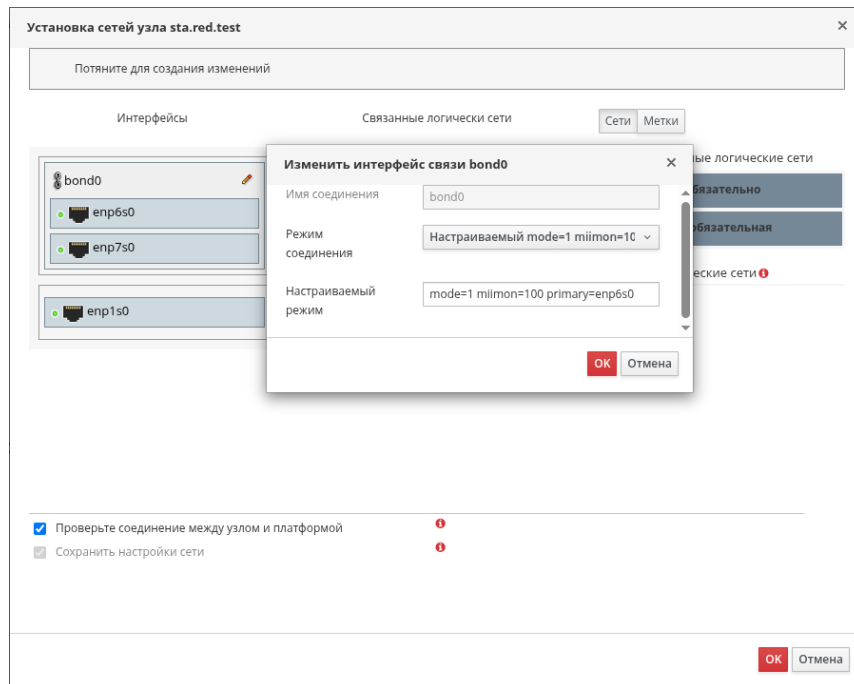
Для зеркалирования трафика хоста в VM необходимо, чтобы хост имел по меньшей мере три сетевых интерфейса, два из которых должны быть объединены в bond.

Описание демонстрационного стенда

На использованном в данной статье стенде хосту были доступны следующие сетевые интерфейсы:

- enp1s0;
- enp6s0;
- enp7s0.

На интерфейсе `enp1s0` работает сеть `ovirtmgmt`. Из интерфейсов `enp6s0` и `enp7s0` было собрано bond соединение, работающее в режиме `mode1` - активное резервирование (active-backup):



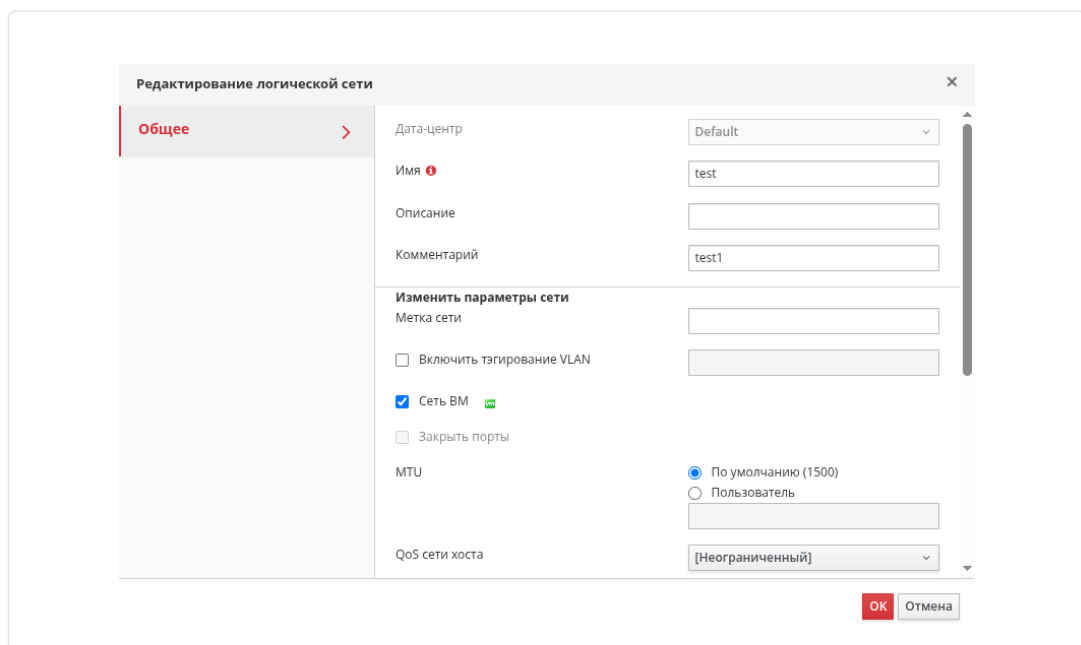
Окно «Изменить интерфейс связи bond0»

Настройка зеркалирования

Для настройки зазеркаливания трафика хоста в ВМ необходимо выполнить следующие действия:

1. Создайте логическую сеть с произвольным названием.

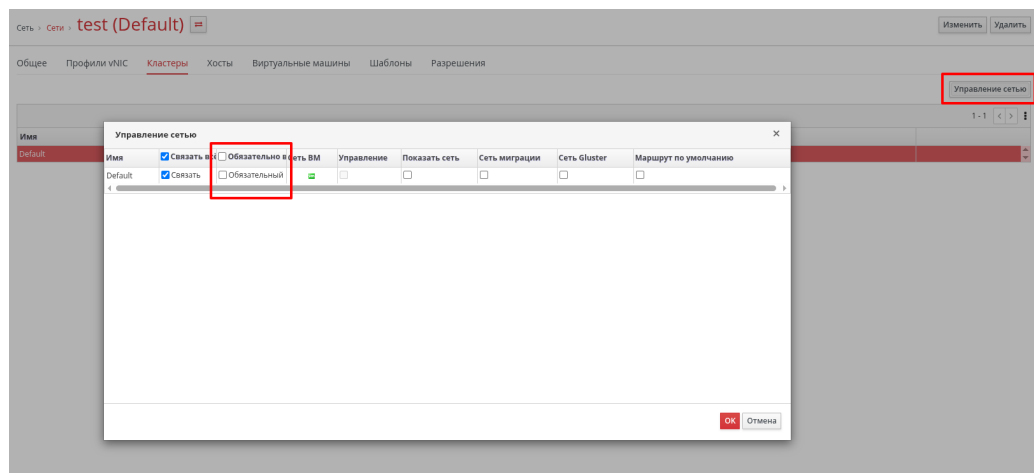
В примере используется название **test**:



Окно «Редактирование логической сети»

2. Сделайте сеть необязательной.

Для этого перейдите на вкладку **Сеть→Сети→Имя сети→Управление сетью** и снимите галочку с поля **Обязательный**:



Окно «Управление сетью»

3. В параметрах vNIC-профиля отключите сетевой фильтр и включите зеркалирование порта:

Изменить профиль интерфейса виртуальной машины

Центр обработки данных

Default

Сеть

test

Имя

test

Описание

QoS

[Неограниченный]

Фильтр сети

Нет сетевого фильтра

☐ Проброс устройств

☒ Мигрируемый

Профиль отказоустойчивости vNIC

None

☒ Зеркалирование порта

Настраиваемые параметры

Пожалуйста, выберите ключ...

+

-

OK

Отмена

Окно «Изменить профиль интерфейса виртуальной машины»

- Назначьте созданную сеть подготовленному bond (active-backup) соединению хоста:

Установка сетей узла sta.red.test

Потяните для создания изменений

Интерфейсы

Связанные логические сети

Сети

Метки

bond0

enp6s0

enp7s0

test

enp1s0

ovirtmgmt

Несвязанные логические сети

Обязательно

Не обязательная

Внешние логические сети

☒ Проверьте соединение между узлом и платформой

☒ Сохранить настройки сети

OK

Отмена

Окно «Установка сетей узла sta.red.test»

5. Созданный vNIC-профиль назначьте VM, в которую необходимо пробросить трафик:

Редактирование сетевого интерфейса

Имя:

Профиль:

Тип:

☐ Пользовательский MAC адрес:
Пример: 00:14:4a:23:67:55

Состояние соединения: ☒ Включено ☐ Выключен ☐ Подключён ☐ Не подключён

Состояние карты:

Параметры сетевого фильтра

Имя: Значение:

Окно «Редактирование сетевого интерфейса»

Мониторинг входящего трафика

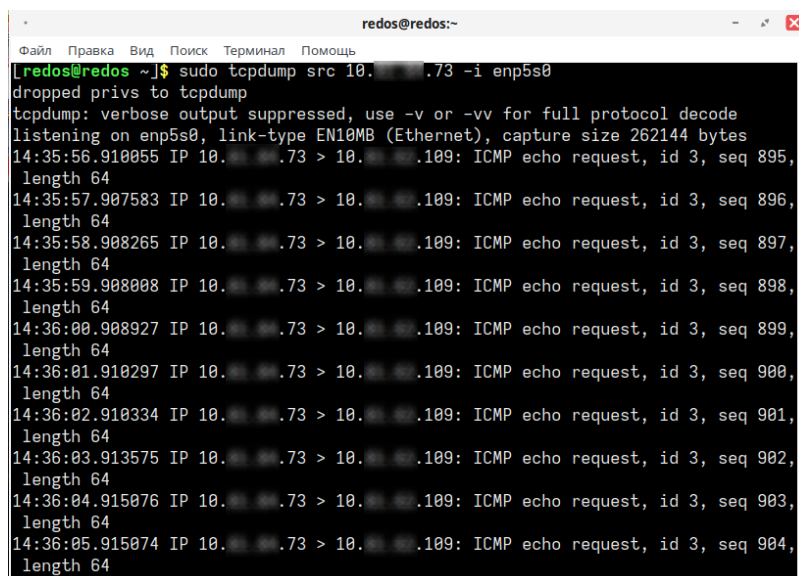
Примечание:

VM будет перехватывать трафик только того хоста, на котором она выполняется.

На интерфейс **test** хоста были отправлены ping-запросы:

```
[root@sta ~]# sudo tcpdump src 10.x.x.73 -i test
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on test, link-type EN10MB (Ethernet), capture size 262144 bytes
14:20:49.640911 IP 10.x.x.73 > sta.red.test: ICMP echo request, id 2, seq 20, length 64
14:20:50.647146 IP 10.x.x.73 > sta.red.test: ICMP echo request, id 2, seq 21, length 64
14:20:51.645152 IP 10.x.x.73 > sta.red.test: ICMP echo request, id 2, seq 22, length 64
14:20:52.647159 IP 10.x.x.73 > sta.red.test: ICMP echo request, id 2, seq 23, length 64
14:20:53.650584 IP 10.x.x.73 > sta.red.test: ICMP echo request, id 2, seq 24, length 64
...
```

В результате отправленные пакеты успешно перехватываются со стороны ВМ:



```
redos@redos:~
Файл  Правка  Вид  Поиск  Терминал  Помощь
redos@redos ~]$ sudo tcpdump src 10.x.x.73 -i enp5s0
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:35:56.910055 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 895,
length 64
14:35:57.907583 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 896,
length 64
14:35:58.908265 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 897,
length 64
14:35:59.908008 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 898,
length 64
14:36:00.908927 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 899,
length 64
14:36:01.910297 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 900,
length 64
14:36:02.910334 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 901,
length 64
14:36:03.913575 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 902,
length 64
14:36:04.915076 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 903,
length 64
14:36:05.915074 IP 10.x.x.73 > 10.x.x.109: ICMP echo request, id 3, seq 904,
length 64
```

Терминал

Вывод `ip a` с хоста после настройки зеркалирования:

```
[root@sta ~]# ip a
...
2: enp1s0: mtu 1500 qdisc mq master ovirtmgmt state UP group default qlen 1000
link/ether 56:6f:64:d5:00:2e brd ff:ff:ff:ff:ff:ff
```

```
3: enp6s0: mtu 1500 qdisc mq master bond0 state UP group default qlen 1000
  link/ether 56:6f:64:d5:00:33 brd ff:ff:ff:ff:ff:ff
4: enp7s0: mtu 1500 qdisc mq master bond0 state UP group default qlen 1000
  link/ether 56:6f:64:d5:00:33 brd ff:ff:ff:ff:ff:ff permaddr 56:6f:64:d5:01:67
...
7: ovirtmgmt: mtu 1500 qdisc noqueue state UP group default qlen 1000
  link/ether d2:ad:7a:41:8a:ad brd ff:ff:ff:ff:ff:ff
  inet 10.x.x.224/24 brd 10.x.x.255 scope global noprefixroute ovirtmgmt
    valid_lft forever preferred_lft forever
  inet6 fe80::d0ad:7aff:fe41:8aad/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
8: ip_vti0@NONE: mtu 1480 qdisc noop state DOWN group default qlen 1000
  link/ipip 0.0.0.0 brd 0.0.0.0
...
49: bond0: mtu 1500 qdisc noqueue master test state UP group default qlen 1000
  link/ether 56:6f:64:d5:00:33 brd ff:ff:ff:ff:ff:ff
50: test: mtu 1500 qdisc prio state UP group default qlen 1000
  link/ether 0a:f9:cd:9a:43:7a brd ff:ff:ff:ff:ff:ff
  inet 10.x.x.109/24 brd 10.x.x.255 scope global dynamic noprefixroute test
    valid_lft 369sec preferred_lft 369sec
52: vnet1: mtu 1500 qdisc noqueue master test state UNKNOWN group default qlen
1000
  link/ether fe:6f:e8:86:00:00 brd ff:ff:ff:ff:ff:ff
  inet6 fe80::fc6f:e8ff:fe86:0/64 scope link
    valid_lft forever preferred_lft forever
```

Использованные IP-адреса были частично скрыты в соответствии с политикой компании.

Источник: <https://redvirt.red-soft.ru/base/knowledge-base/zerkalirovanie-trafika-khosta-v-vm/>