

- Контейнеризация
 - Урок 2. Механизмы контрольных групп
 - Задание 1:
 - Задание 2*:
 - Решение
 - Задача 1.1
 - Задача 1.2
 - Задача 2

Контейнеризация

GeekBrains

Ростислав Ромашин

группа 4992

Урок 2. Механизмы контрольных групп

Задание 1:

1. запустить контейнер с ubuntu, используя механизм LXC
2. ограничить контейнер 256 Мб ОЗУ и проверить, что ограничение работает

Оценка Отлично

Задание 2*:

настроить автоматическую маршрутизацию между контейнерами. Адреса можно взять: 10.0.12.0/24 и 10.0.13.0/24. е.х. `sudo lxc-create -n test123 -t ubuntu -f /usr/share/doc/lxc/examples/lxc-veth.conf` (файл может лежать по другому пути, можно найти командой `sudo find / -name lxc-veth.conf`) Выполнять не обязательно

Задание со звездочкой - повышенной сложности, это нужно учесть при выполнении (но сделать его необходимо).

Решение

Прежде чем приступить к выполнению заданий, необходимо установить *lxc*

```
apt install lxc-utils lxc-templates
```

```
Rostislav@fen:~$ sudo su
[sudo] пароль для Rostislav:
root@fen:/home/Rostislav# lxc-create -n test456 -t ubuntu -f /usr/share/doc/lxc/examples/lxc-veth.conf
lxc-create: test456: parse.c: lxc_file_for_each_line mmap: 78 No such file or directory - Failed to open file "/usr/share/doc/lxc/examples/lxc-veth.conf"
Checking cache download in /var/cache/lxc/jammy/rootfs-amd64 ...
Copy /var/cache/lxc/jammy/rootfs-amd64 to /var/lib/lxc/test456/rootfs ...
Copying rootfs to /var/lib/lxc/test456/rootfs ...
Generating locales (this might take a while)...
  ru.RU.UTF-8... done
Generation complete.
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:ucTPfwVkfjtwMJ3JKB/5AX/UGx1jYe2FuXyf51TPo+k root@fen (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:H4/8nS1VdfhBTiff/UoQLz029AtBdhScZMK8bePVehA root@fen (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:5uC/4es355mtfqX44ur+RRF0ko1Y920HoU0z/orNz1A root@fen (ED25519)
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of start.

Current default time zone: 'Etc/UTC'
Local time is now:      Tue Aug 29 08:52:50 UTC 2023.
Universal Time is now:  Tue Aug 29 08:52:50 UTC 2023.

##
# The default user is 'ubuntu' with password 'ubuntu'!
# Use the 'sudo' command to run tasks as root in the container.
##
```

Так же, необходимо скачать файлы примеров с оф.гита

<https://github.com/lxc/lxc/tree/main/doc/examples> и поместить в директорию */usr/share/doc/lxc/examples*

Задача 1.1

Установим два экземпляра *ubuntu*

```
lxc-create -n test123 -t ubuntu -f /usr/share/doc/lxc/examples/lxc-
veth.conf.in
lxc-create -n test123 -t ubuntu -f /usr/share/doc/lxc/examples/lxc-
veth.conf.in
```

Приведенные выше команды установят системы из шаблона *ubuntu*, используя конфигурационный файл *lxc-veth.conf.in*

Запуск инстанса осуществляется командой

```
lxc-start -d -n test123
```

При запуске, для отладки, можно задать файлы для логирования

```
lxc-start -d -n test456 --logfile /var/log/test123.log --logpriority DEBUG
```

```
test123 x test456
root@fen:/home/Rostislav# lxc-start -d -n test123
root@fen:/home/Rostislav# lxc-start -d -n test456 --logfile /var/log/test123.log --logpriority DEBUG
root@fen:/home/Rostislav# lxc-ls -f
NAME      STATE    AUTOSTART  GROUPS  IPV4          IPV6          UNPRIVILEGED
test123   RUNNING  1          -       10.0.3.253, 10.2.3.5 2003:db8:1:0:214:1234:fe0b:3597 false
test456   RUNNING  1          -       10.0.3.249, 10.2.3.6 2003:db8:1:0:214:1234:fe0b:3598 false
root@fen:/home/Rostislav# tail /var/log/test123.log
lxc-start test456 20230829100233.480 DEBUG conf - conf.c:capabilities_deny:3200 - Dropped sys_rawio (17) capability
lxc-start test456 20230829100233.480 DEBUG conf - conf.c:capabilities_deny:3203 - Capabilities have been setup
lxc-start test456 20230829100233.480 NOTICE conf - conf.c:lxc_setup:4469 - The container "test456" is set up
lxc-start test456 20230829100233.480 INFO apparmor - lsm/apparmor.c:apparmor_process_label_set_at:1186 - Set AppArmor label to "lxc-container-default-cgns"
lxc-start test456 20230829100233.480 INFO apparmor - lsm/apparmor.c:apparmor_process_label_set:1231 - Changed AppArmor profile to lxc-container-default-cgns
lxc-start test456 20230829100233.481 WARN cgfsng - cggroups/cgfsng.c:cgfsng_setup_limits_legacy:2767 - Invalid argument - Ignoring legacy cgroup limits on pure cgroup2 system
lxc-start test456 20230829100233.482 DEBUG terminal - terminal.c:lxc_terminal_peer_default:695 - No such device - The process does not have a controlling terminal
lxc-start test456 20230829100233.483 NOTICE utils - utils.c:lxc_drop_groups:1368 - Dropped supplementary groups
lxc-start test456 20230829100233.483 NOTICE start - start.c:start:2161 - Exec'ing "/sbin/init"
lxc-start test456 20230829100233.484 NOTICE start - start.c:post_start:2172 - Started "/sbin/init" with pid "2869"
root@fen:/home/Rostislav#
```

```
lxc-ls -f
```

Вышеприведенная команда выводит информацию о виртуальных машинах.

Из картинки видим, что два экземпляра имеют статус RUNNING

Дополнительную информацию о процессе запуска можно получить из логов

```
tail /var/log/test123.log
```

Задача 1.2

Настроим конфиг для *test123*

```
vim /var/lib/lxc/test123/config
```

```
test123 x test456
# Template used to create this container: /usr/share/lxc/templates/lxc-ubuntu
# Parameters passed to the template:
# For additional config options, please look at lxc.container.conf(5)

# Uncomment the following line to support nesting containers:
#lxc.include = /usr/share/lxc/config/nesting.conf
# (Be aware this has security implications)

# Container with network virtualized using a pre-configured bridge named br0 and
# veth pair virtual network devices

# Common configuration
lxc.include = /usr/share/lxc/config/ubuntu.common.conf

# Container specific configuration
lxc.uts.name = beta
lxc.rootfs.path = dir:/var/lib/lxc/test123/rootfs
lxc.uts.name = test123
lxc.arch = amd64
lxc.cgroup2.memory.max = 256M
lxc.start.auto=1
# Network configuration
lxc.net.0.type = veth
lxc.net.0.flags = up
lxc.net.0.link = lxcbr0
lxc.net.0.hwaddr = 4a:49:43:49:79:bf
lxc.net.0.ipv4.address = 10.2.3.5/24
lxc.net.0.ipv6.address = 2003:db8:1:0:214:1234:fe0b:3597
~
```

Настроим конфиг для *test456*

```
vim /var/lib/lxc/test123/config
```

```
test123 x test456
# Template used to create this container: /usr/share/lxc/templates/lxc-ubuntu
# Parameters passed to the template:
# For additional config options, please look at lxc.container.conf(5)

# Uncomment the following line to support nesting containers:
#lxc.include = /usr/share/lxc/config/nesting.conf
# (Be aware this has security implications)

# Common configuration
lxc.include = /usr/share/lxc/config/ubuntu.common.conf

# Container specific configuration
lxc.rootfs.path = dir:/var/lib/lxc/test456/rootfs
lxc.uts.name = test456
lxc.arch = amd64
lxc.cgroup2.memory.max = 256M
lxc.start.auto=1
# Network configuration
lxc.net.0.type = veth
lxc.net.0.flags = up
lxc.net.0.link = lxcbr0
lxc.net.0.hwaddr = 4a:49:43:49:79:bb
lxc.net.0.ipv4.address = 10.2.3.6/24
lxc.net.0.ipv6.address = 2003:db8:1:0:214:1234:fe0b:3598
~
```

Подсоединяемся к терминалам наших виртуальных машин

```
lxc-attach -n test123
lxc-attach -n test456
```

```
test123 x test456
root@fen:/home/Rostislav# lxc-attach -n test123
root@test123:/# free -m
              total        used        free      shared  buff/cache   available
Память:      256          27         228           0           0          228
Подкачка:      0           0           0           0           0           0
root@test123:/#
```

Убеждаемся что указанный параметр в конфиге ограничил оперативную память на обеих машинах до 256M

```
free -m
```

```
test123 x test456
root@fen:/home/Rostislav# lxc-attach -n test456
root@test456:/# free -m
              total        used        free      shared  buff/cache   available
Память:      256          27         228           0           0          228
Подкачка:      0           0           0           0           0           0
root@test456:/#
```

Задача 2

На каждой машине на один сетевой интерфейс назначено по два адреса Один присвоился автоматически через DHCP, а второй мы статически указали в конфигах. Юникс позволяет на один интерфейс повесить несколько адресов.

```
test123 x test456
root@fen:/home/Rostislav# lxc-ls -f
NAME    STATE   AUTOSTART GROUPS IPV4                                IPV6                                UNPRIVILEGED
test123 RUNNING 1         -    10.0.3.253, 10.2.3.5 2003:db8:1:0:214:1234:fe0b:3597 false
test456 RUNNING 1         -    10.0.3.249, 10.2.3.6 2003:db8:1:0:214:1234:fe0b:3598 false
root@fen:/home/Rostislav#
```

```
lxc-ls -f
```

Также отображается *AUTOSTART 1*, это говорит, что наши виртуальные системы будут запускаться автоматически вместе с запуском основной системы.

Убеждаемся в работоспособности сети, ping проходит в обе стороны.

test123

x

test456

```
root@test123:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 4a:49:43:49:79:bf brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.2.3.5/24 brd 10.2.3.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet 10.0.3.253/24 metric 100 brd 10.0.3.255 scope global dynamic eth0
        valid_lft 2107sec preferred_lft 2107sec
    inet6 2003:db8:1:0:214:1234:fe0b:3597/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::4849:43ff:fe49:79bf/64 scope link
        valid_lft forever preferred_lft forever
root@test123:~# ping 10.2.3.6
PING 10.2.3.6 (10.2.3.6) 56(84) bytes of data.
64 bytes from 10.2.3.6: icmp_seq=1 ttl=64 time=0.263 ms
64 bytes from 10.2.3.6: icmp_seq=2 ttl=64 time=0.101 ms
64 bytes from 10.2.3.6: icmp_seq=3 ttl=64 time=0.098 ms
^C
--- 10.2.3.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2052ms
rtt min/avg/max/mdev = 0.098/0.154/0.263/0.077 ms
root@test123:~# ping 10.0.3.249
PING 10.0.3.249 (10.0.3.249) 56(84) bytes of data.
64 bytes from 10.0.3.249: icmp_seq=1 ttl=64 time=0.156 ms
64 bytes from 10.0.3.249: icmp_seq=2 ttl=64 time=0.100 ms
64 bytes from 10.0.3.249: icmp_seq=3 ttl=64 time=0.097 ms
64 bytes from 10.0.3.249: icmp_seq=4 ttl=64 time=0.095 ms
^C
--- 10.0.3.249 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.095/0.112/0.156/0.025 ms
root@test123:~# █
```

test123

x

test456

```
root@test456:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 4a:49:43:49:79:bb brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.2.3.6/24 brd 10.2.3.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet 10.0.3.249/24 metric 100 brd 10.0.3.255 scope global dynamic eth0
        valid_lft 2237sec preferred_lft 2237sec
    inet6 2003:db8:1:0:214:1234:fe0b:3598/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::4849:43ff:fe49:79bb/64 scope link
        valid_lft forever preferred_lft forever
root@test456:~# ping 10.2.3.5
PING 10.2.3.5 (10.2.3.5) 56(84) bytes of data.
64 bytes from 10.2.3.5: icmp_seq=1 ttl=64 time=0.145 ms
64 bytes from 10.2.3.5: icmp_seq=2 ttl=64 time=0.099 ms
64 bytes from 10.2.3.5: icmp_seq=3 ttl=64 time=0.101 ms
^C
--- 10.2.3.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2052ms
rtt min/avg/max/mdev = 0.099/0.115/0.145/0.021 ms
root@test456:~# ping 10.0.3.253
PING 10.0.3.253 (10.0.3.253) 56(84) bytes of data.
64 bytes from 10.0.3.253: icmp_seq=1 ttl=64 time=0.250 ms
64 bytes from 10.0.3.253: icmp_seq=2 ttl=64 time=0.100 ms
64 bytes from 10.0.3.253: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 10.0.3.253: icmp_seq=4 ttl=64 time=0.099 ms
^C
--- 10.0.3.253 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.099/0.137/0.250/0.065 ms
root@test456:~# █
```