

PID (Process ID) уровень изоляции

означает, что процессы, запущенные внутри какого-либо контейнера, не видны никому, кроме самого контейнера, но есть исключения, например при запуске контейнера можно указать “родительский контейнер” и теперь оба контейнера смогут увидеть процессы друг друга.

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker run -d --name isolation1 ubuntu:latest bash -c "sleep 1000"
2963c2c7375331d50161f9872b3f20244270b5144c78148bea0825f507293f9d
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker run -d --name isolation2 --user nobody ubuntu:latest bash -c "sleep 1000"
bc54d646b3ac6948d9008ff019fee9d737ee4d97697da02f9db1396b3be05de4
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker run -d --name isolation3 --pid container:isolation2 ubuntu:latest bash -c "sleep 1000"
02058a39ade2c5a44fe8c33103e964b9f2b280304aFd772ce9f65d22a2566167
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
```

создали 3 контейнера isolation1, isolation2, isolation3.
Для контейнера isolation3 сделали контейнер isolation2 родительским, это означает что они смогут видеть процессы друг друга, а процессы внутри isolation1 останутся изолированными от остальных контейнеров.

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation1 ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0   2696   1408 ?        Ss   12:32    0:00 sleep 1000
root           7 50.0  0.0   7888   3968 pts/0    Rs+  12:36    0:00 ps aux
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation2 ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
nobody         1  0.0  0.0   2696   1408 ?        Ss   12:33    0:00 sleep 1000
root           7  0.0  0.0   2696   1536 ?        Ss   12:33    0:00 sleep 1000
nobody        13 33.3  0.0   7888   3968 pts/0    Rs+  12:36    0:00 ps aux
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation3 ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
nobody         1  0.0  0.0   2696   1408 ?        Ss   12:33    0:00 sleep 1000
root           7  0.0  0.0   2696   1536 ?        Ss   12:33    0:00 sleep 1000
root          19 33.3  0.0   7888   3968 pts/0    Rs+  12:36    0:00 ps aux
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
```

IPC (Inter process communication) уровень изоляции

создадим и запустим еще один контейнер isolation4
следующей командой: `docker run -d --name isolation4
--ipc=host ubuntu:latest bash -c "sleep 1000"`

в качестве ipc укажем ему использование пространства
имен хоста

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker run -d --name isolation4 --ipc=host ubuntu:latest bash -c "sleep 1000"
6faea3ad6d2d3e2179bd35176c63098ecf1b01afa1eee7cc200bac45fdc3d82a
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS   NAMES
6faea3ad6d2d   ubuntu:latest  "bash -c 'sleep 1000'"  6 seconds ago Up 5 seconds             isolation4
02058a39ade2   ubuntu:latest  "bash -c 'sleep 1000'"  11 minutes ago Up 11 minutes             isolation3
bc54d646b3ac   ubuntu:latest  "bash -c 'sleep 1000'"  11 minutes ago Up 11 minutes             isolation2
2963c2c73753   ubuntu:latest  "bash -c 'sleep 1000'"  11 minutes ago Up 11 minutes             isolation1
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation4 ipcs -a
----- Message Queues -----
```

Введем с помощью команды `docker exec -it <имя_контейнера> ipcs -a` все наши Message Queues, Shared Memory Segments и Semaphore Arrays

```
----- Message Queues -----
key          msqid      owner      perms      used-bytes   messages

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes        nattch     status

----- Semaphore Arrays -----
key          semid      owner      perms      nsems

root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation2 ipcs -a

----- Message Queues -----
key          msqid      owner      perms      used-bytes   messages

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes        nattch     status

----- Semaphore Arrays -----
key          semid      owner      perms      nsems

root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation3 ipcs -a

----- Message Queues -----
key          msqid      owner      perms      used-bytes   messages

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes        nattch     status

----- Semaphore Arrays -----
key          semid      owner      perms      nsems

root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation4 ipcs -a

----- Message Queues -----
key          msqid      owner      perms      used-bytes   messages

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes        nattch     status
0x00000000  655418    ubuntu    600        67108864     2         dest

----- Semaphore Arrays -----
key          semid      owner      perms      nsems

root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
```

Как мы видим, контейнеры `isolation1`, `isolation2`, `isolation3` имеют свое пространство `ipcs`, а контейнер `isolation4` имеет общее с `host` машиной пространство `ipcs`, потому что мы

специально указали в параметрах запуска контейнера соответствующие настройки

Network isolation level

Каждый контейнер имеет свой сетевой интерфейс, с адресом отличным от любого другого контейнера

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:17ff:fe13:d658 prefixlen 64 scopeid 0x20<link>
    ether 02:42:17:13:d6:58 txqueuelen 0 (Ethernet)
    RX packets 257 bytes 11972 (11.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 306 bytes 29497 (29.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp12s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 84:a9:38:93:a4:d4 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5313 bytes 587176 (587.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5313 bytes 587176 (587.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

vethf4aa0c7: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::84c3:6bff:fec9:4f4f prefixlen 64 scopeid 0x20<link>
    ether 86:c3:6b:c9:4f:4f txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 3609 (3.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.12 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::4ca8:acaf:ad04:8347 prefixlen 64 scopeid 0x20<link>
    ether f4:a4:75:1f:98:11 txqueuelen 1000 (Ethernet)
    RX packets 879379 bytes 708989064 (708.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 331000 bytes 80769309 (80.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
```

с помощью `ifconfig` вывели все сетевые интерфейсы, интерфейс `docker0` будет являться по сути “базовым” интерфейсом для всех остальных интерфейсов контейнеров запущенных в `docker`.

inet 172.17.0.2 - контейнер `isolation1`

```
Setting up net-tools (2.10-0.1ubuntu4) ...
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation1 ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
    ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
    RX packets 148  bytes 219794 (219.7 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 132  bytes 11465 (11.4 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

inet 172.17.0.3 - контейнер `isolation2` (поверьте наслово потому что нельзя скачать `net-tools` из-за проблем с правами, поскольку пользователь не `root`)

inet 172.17.0.4 - контейнер isolation3

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation3 ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.4 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:ac:11:00:04 txqueuelen 0 (Ethernet)
    RX packets 5436 bytes 25769845 (25.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2686 bytes 198609 (198.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
```

inet 172.17.0.5 - контейнер isolation4

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation4 ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.5 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:ac:11:00:05 txqueuelen 0 (Ethernet)
    RX packets 3240 bytes 25609333 (25.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1559 bytes 107195 (107.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
```


создадим еще один контейнер isolation5, и укажем в параметрах запуска использование совместного сетевого интерфейса вместе с host

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker run -d --name isolation5 --network=host ubuntu:latest bash -c "sleep 1000"
```

точно такие же сетевые интерфейсы как и у host в контейнере isolation5

```
Selecting previously unselected package net-tools.
(Reading database ... 4378 files and directories currently installed.)
Preparing to unpack .../net-tools_2.10-0.1ubuntu4_amd64.deb ...
Unpacking net-tools (2.10-0.1ubuntu4) ...
Setting up net-tools (2.10-0.1ubuntu4) ...
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation5 ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:17ff:fe13:d658 prefixlen 64 scopeid 0x20<link>
    ether 02:42:17:13:d6:58 txqueuelen 0 (Ethernet)
    RX packets 8255 bytes 466754 (466.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15076 bytes 102400836 (102.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp12s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 84:a9:38:93:a4:d4 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 6090 bytes 671413 (671.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6090 bytes 671413 (671.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth54fb241: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::94ba:45ff:fedf:2ac8 prefixlen 64 scopeid 0x20<link>
    ether 96:ba:45:df:2a:c8 txqueuelen 0 (Ethernet)
    RX packets 1559 bytes 107195 (107.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3248 bytes 25610041 (25.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

vethaa96032: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::f440:beff:fe4b:4d04 prefixlen 64 scopeid 0x20<link>
    ether f6:40:be:4b:4d:04 txqueuelen 0 (Ethernet)
    RX packets 2686 bytes 198609 (198.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5447 bytes 25770789 (25.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Users изоляция

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation1 id
uid=0(root) gid=0(root) groups=0(root)
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation2 id
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation3 id
uid=0(root) gid=0(root) groups=0(root)
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation4 id
uid=0(root) gid=0(root) groups=0(root)
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation5 id
uid=0(root) gid=0(root) groups=0(root)
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
```

у контейнеров свои root, root системы != root контейнера, у isolation2 свой uid, поскольку мы задали его при создании

Mount изоляция

У docker контейнеров изолирована файловая система

```
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation1 touch someFile
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation1 ls
bin bin usr-is-merged boot dev etc home lib lib64 media mnt opt proc root run sbin sbin usr-is-merged somefile srv sys tmp usr var
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~# docker exec -it isolation2 ls
bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
root@wireless-monkey-IdeaPad-Gaming-3-15IMH05:~#
```

Hostname изоляция

у docker контейнеров свои hostname, по умолчанию они равны id контейнера