Application Confinement with User namespaces

Serge Hallyn, Scott Moser

Canonical, Inc

serge.hallyn@ubuntu.com, scott.moser@canonical.com

October 30, 2014

Overview

- Quick Introduction to Containers
- 2 State of Containers Prior to User namespaces
- User namespaces
- 4 Graphical Demo

Linux Containers?

- operating system-level virtualization method for running multiple isolated Linux systems (containers) on a single control host.
- "chroot on steroids"
- "it's like bsd jails" (or solaris zones)
- from the inside looks like a vm
- from the outside looks like processes

Containers prior to user namespaces

Namespaces

- ullet id o resource mapping
 - Prevent resource access by not providing a handle
 - i.e. pid 1 is not global init
 - /etc/shadow not accessible
- Many leaks (/proc/pid/fd/N

Control groups

- Resource limits and accounting
- 2 Limit device access
- If root, re-mount cgroups and change/escape limits.

Capabilities bounding set

- Limit privs of root in container
- 2 Root still owns most host files
- http://www.sevagas.com/IMG/pdf/exploiting_capabilities_the_dark_side.pdf
- Prevents useful things like tmpfs mounts

LSMs

- Paper of the (huge) remaining holes
- ② i.e. prevent /proc/sys/* writing, etc
- Safe from accidental damage by container root
- People always want unsafe exceptions
- Lack of policy nesting limits use in containers

Seccomp

- Prevent use of some syscalls
- Reduce exposed kernel surface
- Hard to do generally

- Nevertheless
 - Root in container is still root on host
 - Any leak = game over
 - 4 Answer: "Wait for user namespaces"

Demo Time [sort of].

- Ubuntu 14.10 instance with hostname 'lxc-host'.
- 2 users (elsa, anna) are each configured to run lxc unprivileged.
- 3 'showinfo': simple shell filter to 'find' or 'ps' or 'grep'.
- 'mywait': Very Exciting. Run it, it prints its pid, uid, gid. Then creates a file named 'sleeper-user@hostname' and sleeps forever. copied into each container's /usr/local/bin.

Host Processes / Users.

```
🙆 🖨 📵 ubuntu@lxc-host (10.5.0.232) - byobu
 oot@lxc-host# showinfo files
                                                                 root@lxc-host# showinfo config
fname
                             uid
                                          gid
                                                       mode
                                                                anna-c1/config:lxc.id map = u 0 2000000 65535
sleeper-elsa@lxc-host.info
                                          gid=elsa
                                                       mode=664 anna-c1/config:lxc.id_map = g 0 2000000 65535
                             uid=elsa
sleeper-root@lxc-host.info
                             uid=root
                                          aid=root
                                                       mode=644 anna-c2/config:lxc.id map = u 0 2100000 65535
sleeper-anna@lxc-host.info
                             uid=anna
                                          aid=anna
                                                       mode=664 anna-c2/config:lxc.id map = g 0 2100000 65535
sleeper-root@anna-c1.info
                             uid=2000000
                                          gid=2000000
                                                       mode=664 elsa-c1/config:lxc.id map = u 0 3000000 65535
sleeper-root@anna-c2.info
                             uid=2100000
                                         gid=2100000
                                                      mode=664 elsa-c1/config:lxc.id map = g 0 3000000 65535
sleeper-ubuntu@elsa-c1.info uid=3001000
                                         gid=3001000 mode=644 elsa-c2/config:lxc.id map = u 0 3100000 65535
sleeper-root@elsa-c2.info
                             uid=3100000
                                          gid=3100000
                                                      mode=664 elsa-c2/config:lxc.id map = g 0 3100000 65535
 root@lxc-host# showinfo ps
                                                                      lxc-host# cat /etc/subuid
                                 aid
                                          pid
command
                        uid
                                                 userns
                                                                anna:2000000:1000000
/sbin/init
                                                                elsa:3000000:1000000
                        root
                                                 4026532171
/sbin/init
                        2000000
                                 2000000
                                          6900
                                                                 cot@lxc-host# cat /etc/subgid
                                                 4026532294
/sbin/init
                        2100000
                                 2100000
                                          7704
                                                                anna:2000000:1000000
/sbin/init
                                                                elsa:3000000:1000000
                        3000000
                                 3000000
                                          8590
                                                 4026532233
/sbin/init
                        3100000
                                 3100000
                                          9340
                                                 4026532356
                                                                             # moreinfo
sleeper-anna@lxc-host
                        anna
                                 1001
                                          11826
                                                                https://github.com/hallyn/ods-2014-userns
                                                 4026531837
sleeper-root@anna-c1
                        2000000
                                 2000000
                                          12177
                                                 4026532171
                                                                cubswin:)
                                                                 root@lxc-host#
sleeper-root@anna-c2
                        2100000
                                 2100000
                                          12426
                                                 4026532294
sleeper-elsa@lxc-host
                        elsa
                                 1002
                                          13113 4026531837
sleeper-ubuntu@elsa-c1 3001000 3001000 14280
                                                 4026532233
sleeper-root@elsa-c2
                        3100000
                                 3100000
                                          14535
                                                 4026532356
sleeper-root@lxc-host
                        root
                                 0
                                          15506
                                                 4026531837
root@lxc-host#
elsa@lxc-host$ mvwait
                                                          anna@lxc-hostS mywait
[sleeper-elsa@lxc-host] pid=13109 uid=1002 gid=1002
                                                          [sleeper-anna@lxc-host] pid=11822 uid=1001 gid=1001
elsa@lxc-host$ lxc_attach elsa-c1
                                                           anna@lxc-host$ lxc attach anna-c1
root@elsa-c1# sudo -Hu ubuntu mvwait
                                                          root@anna-c1# mywait
[sleeper-ubuntu@elsa-c1] pid=597 uid=1000 gid=1000
                                                           [sleeper-root@anna-c1] pid=592 uid=0 gid=0
root@elsa-c2# mywait
                                                          root@anna-c2# mywait
[sleeper-root@elsa-c2] pid=597 uid=0 gid=0
                                                           [sleeper-root@anna-c2] pid=593 uid=0 gid=0
 uº 14.10 0:-*
                                                                       20m 0.00 2.0GHz 2.0G15% 2014-10-30 18:25:41
```

LXC Containers and Configuration

```
🙆 🖨 🗈 ubuntu@lxc-host (10.5.0.232) - byobu
 root@lxc-host# showinfo files
                                                                 root@lxc-host# showinfo config
fname
                             mi d
                                           aid
                                                       mode
                                                                 anna-c1/config:lxc.id map = u 0 2000000 65535
sleeper-elsa@lxc-host.info
                             uid=elsa
                                          gid=elsa
                                                       mode=664 anna-c1/config:lxc.id map = q 0 2000000 65535
sleeper-root@lxc-host.info
                             uid=root
                                          gid=root
                                                       mode=644 anna-c2/config:lxc.id map = u 0 2100000 65535
sleeper-anna@lxc-host.info
                                          gid=anna
                                                       mode=664 anna-c2/config:lxc.id map = g 0 2100000 65535
                             uid=anna
sleeper-root@anna-c1.info
                             uid=2000000
                                          aid=2000000
                                                       mode=664 elsa-c1/config:lxc.id map = u 0 3000000 65535
sleeper-root@anna-c2.info
                             uid=2100000
                                          aid=2100000
                                                       mode=664 elsa-c1/config:lxc.id_map = g 0 3000000 65535
sleeper-ubuntu@elsa-c1.info
                             uid=3001000
                                          aid=3001000
                                                       mode=644 elsa-c2/config:lxc.id_map = u 0 3100000 65535
sleeper-root@elsa-c2.info
                             uid=3100000
                                          aid=3100000
                                                       mode=664 elsa-c2/config:lxc.id map = q 0 3100000 65535
 oot@lxc-host# showinfo ps
                                                                           ost# cat /etc/subuid
                                 gid
                                          pid
                                                                 anna:2000000:1000000
command
                        uid
                                                  userns
/sbin/init
                        root
                                                  4026531837
                                                                 elsa:3000000:1000000
/sbin/init
                        2000000
                                 2000000
                                                  4026532171
                                                                  oot@lxc-host# cat /etc/subgid
                                           6900
/sbin/init
                        2100000
                                 2100000
                                          7704
                                                                 anna:2000000:1000000
                                                  4026532294
                        3000000
                                                                 elsa:3000000:1000000
/sbin/init
                                 3000000
                                          8590
                                                  4026532233
                                                                   oot@lxc-host# moreinfo
/sbin/init
                        3100000
                                 3100000
                                          9340
                                                  4026532356
sleeper-anna@lxc-host
                        anna
                                 1001
                                          11826 4026531837
                                                                 https://github.com/hallyn/ods-2014-userns
sleeper-root@anna-c1
                        2000000
                                 2000000
                                                 4026532171
                                                                 cubswin:)
                                          12426
                                                                 root@lxc-host#
sleeper-root@anna-c2
                        2100000
                                 2100000
                                                 4026532294
sleeper-elsa@lxc-host
                        elsa
                                          13113 4026531837
                                 1002
sleeper-ubuntu@elsa-c1
                        3001000
                                 3001000
                                          14280
                                                 4026532233
sleeper-root@elsa-c2
                                 3100000
                                          14535
                                                 4026532356
                        3100000
sleeper-root@lxc-host
                        root
                                 Θ
                                          15506
                                                 4026531837
elsa@lxc-host$ mywait
                                                           anna@lxc-host$ mywait
[sleeper-elsa@lxc-host] pid=13109 uid=1002 gid=1002
                                                           [sleeper-anna@lxc-host] pid=11822 uid=1001 gid=1001
elsa@lxc-host$ lxc attach elsa-c1
                                                           anna@lxc-host$ lxc attach anna-c1
root@elsa-c1# sudo -Hu ubuntu mywait
                                                           root@anna-c1# mywait
[sleeper-ubuntu@elsa-c1] pid=597 uid=1000 gid=1000
                                                           [sleeper-root@anna-c1] pid=592 uid=0 gid=0
 -oot@elsa-c2# mywait
                                                           root@anna-c2# mvwait
[sleeper-root@elsa-c2] pid=597 uid=0 gid=0
                                                           [sleeper-root@anna-c2] pid=593 uid=0 gid=0
 uº 14.10 0:-*
                                                                        20m 0.00 2.0GHz 2.0G15% 2014-10-30 18:25:41
```

Anna's containers: **anna-c1**, anna-c2

```
🙆 🖨 📵 ubuntu@lxc-host (10.5.0.232) - byobu
 oot@lxc-host# showinfo files
                                                                 root@lxc-host# showinfo config
fname
                             uid
                                          gid
                                                                anna-c1/config:lxc.id map = u 0 2000000 65535
                                                       mode
sleeper-elsa@lxc-host.info
                             uid=elsa
                                          gid=elsa
                                                       mode=664 anna-c1/config:lxc.id_map = g 0 2000000 65535
sleeper-root@lxc-host.info
                             uid=root
                                          aid=root
                                                       mode=644 anna-c2/config:lxc.id map = u 0 2100000 65535
sleeper-anna@lxc-host.info
                             uid=anna
                                          aid=anna
                                                       mode=664 anna-c2/config:lxc.id map = g 0 2100000 65535
 sleeper-root@anna-c1.info
                             uid=2000000
                                          gid=2000000
                                                       mode=664 elsa-c1/config:lxc.id map = u 0 3000000 65535
sleeper-root@anna-c2.info
                                                       mode=664 elsa-c1/config:lxc.id map = q 0 3000000 65535
                             uid=2100000
                                         gid=2100000
sleeper-ubuntu@elsa-c1.info uid=3001000
                                          gid=3001000
                                                       mode=644 elsa-c2/config:lxc.id_map = u 0 3100000 65535
sleeper-root@elsa-c2.info
                             uid=3100000 gid=3100000 mode=664 elsa-c2/config:lxc.id_map = g 0 3100000 65535
 root@lxc-host# showinfo ps
                                                                             # cat /etc/subuid
command
                        uid
                                 aid
                                          pid
                                                 userns
                                                                anna:2000000:1000000
/sbin/init
                                 ō
                                                 4026531837
                                                                elsa:3000000:1000000
                        root
/sbin/init
                        2000000
                                 2000000
                                                 4026532171
                                                                 cot@lxc-host# cat /etc/subgid
/sbin/init
                        2100000 2100000
                                          7704
                                                 4026532294
                                                                 anna:2000000:1000000
/sbin/init
                        3000000
                                 3000000
                                          8590
                                                 4026532233
                                                                 elsa:3000000:1000000
/sbin/init
                        3100000
                                 3100000
                                          9340
                                                 4026532356
                                                                 root@lxc-host# moreinfo
sleeper-anna@lxc-host
                                 1001
                                          11826
                                                 4026531837
                                                                 https://github.com/hallyn/ods-2014-userns
                        anna
sleeper-root@anna-c1
                        2000000
                                 2000000
                                                 4026532171
                                                                 cubswin:)
                                                                 root@lxc-host#
sleeper-root@anna-c2
                        2100000 2100000 12426 4026532294
sleeper-elsa@lxc-host
                        elsa
                                 1002
                                                 4026531837
sleeper-ubuntu@elsa-c1
                        3001000
                                 3001000
                                          14280
                                                 4026532233
sleeper-root@elsa-c2
                        3100000
                                 3100000 14535 4026532356
sleeper-root@lxc-host
                                                 4026531837
                        root
                                 0
                                          15506
root@lxc-host#
elsa@lxc-host$ mywait
                                                          anna@lxc-host$ mywait
[sleeper-elsa@lxc-host] pid=13109 uid=1002 gid=1002
                                                           [sleeper-anna@lxc-host] pid=11822 uid=1001 gid=1001
elsa@lxc-host$ lxc_attach elsa-c1
                                                           anna@lxc-host$ lxc_attach anna-c1
root@elsa-c1# sudo -Hu ubuntu mvwait
                                                          root@anna-c1# mywait
                                                           [sleeper-root@anna-c1] pid=592 uid=0 gid=0
[sleeper-ubuntu@elsa-c1] pid=597 uid=1000 gid=1000
root@elsa-c2# mywait
                                                          root@anna-c2# mywait
[sleeper-root@elsa-c2] pid=597 uid=0 gid=0
                                                          [sleeper-root@anna-c2] pid=593 uid=0 gid=0
 uº 14.10 0:-*
                                                                           0.00 2.0GHz 2.0G15% 2014-10-30 18:25:41
```

Anna's containers: anna-c1, anna-c2

```
🙆 🖨 📵 ubuntu@lxc-host (10.5.0.232) - byobu
 oot@lxc-host# showinfo files
                                                                 root@lxc-host# showinfo config
fname
                             uid
                                                                anna-c1/config:lxc.id map = u 0 2000000 65535
                                          aid
                                                       mode
sleeper-elsa@lxc-host.info
                             uid=elsa
                                          gid=elsa
                                                       mode=664 anna-c1/config:lxc.id_map = g 0 2000000 65535
sleeper-root@lxc-host.info
                             uid=root
                                          aid=root
                                                       mode=644 anna-c2/config:lxc.id map = u 0 2100000 65535
sleeper-anna@lxc-host.info
                             uid=anna
                                          aid=anna
                                                       mode=664 anna-c2/config:lxc.id map = g 0 2100000 65535
sleeper-root@anna-c1.info
                             uid=2000000
                                          gid=2000000
                                                       mode=664 elsa-c1/config:lxc.id map = u 0 3000000 65535
                                                       mode=664 elsa-c1/config:lxc.id map = q 0 3000000 65535
sleeper-root@anna-c2.info
                             uid=2100000
                                         gid=2100000
sleeper-ubuntu@elsa-c1.info uid=3001000
                                          gid=3001000
                                                       mode=644 elsa-c2/config:lxc.id_map = u 0 3100000 65535
sleeper-root@elsa-c2.info
                             uid=3100000
                                         gid=3100000 mode=664 elsa-c2/config:lxc.id map = g 0 3100000 65535
 root@lxc-host# showinfo ps
                                                                             # cat /etc/subuid
command
                        uid
                                 aid
                                          pid
                                                 userns
                                                                anna:2000000:1000000
/sbin/init
                                                 4026531837
                                                                 elsa:3000000:1000000
                        root
/sbin/init
                        2000000
                                 2000000
                                          6900
                                                 4026532171
                                                                 root@lxc-host# cat /etc/subgid
/sbin/init
                        2100000
                                 2100000
                                                                 anna:2000000:1000000
/sbin/init
                        3000000 3000000 8590
                                                 4026532233
                                                                 elsa:3000000:1000000
/sbin/init
                        3100000
                                 3100000
                                                 4026532356
                                                                 root@lxc-host# moreinfo
                                          9340
sleeper-anna@lxc-host
                                          11826
                                                 4026531837
                                                                https://github.com/hallyn/ods-2<u>014-userns</u>
                        anna
                                 1001
sleeper-root@anna-c1
                        2000000
                                 2000000
                                          12177
                                                 4026532171
                                                                 cubswin:)
                                                                 root@lxc-host#
sleeper-root@anna-c2
                        2100000 2100000 12426 4026532294
sleeper-elsa@lxc-host
                        elsa
                                 1002
                                          13113 4026531837
sleeper-ubuntu@elsa-c1
                        3001000
                                 3001000
                                          14280
                                                 4026532233
sleeper-root@elsa-c2
                        3100000 3100000 14535 4026532356
sleeper-root@lxc-host
                                                 4026531837
                        root
                                 0
                                          15506
root@lxc-host#
elsa@lxc-host$ mywait
                                                          anna@lxc-host$ mywait
[sleeper-elsa@lxc-host] pid=13109 uid=1002 gid=1002
                                                           [sleeper-anna@lxc-host] pid=11822 uid=1001 gid=1001
elsa@lxc-host$ lxc_attach elsa-c1
                                                           anna@lxc-host$ lxc_attach anna-c1
root@elsa-c1# sudo -Hu ubuntu mvwait
                                                           root@anna-c1# mywait
[sleeper-ubuntu@elsa-c1] pid=597 uid=1000 gid=1000
                                                           [sleeper-root@anna-c1] pid=592 uid=0 gid=0
root@elsa-c2# mywait
                                                          root@anna-c2# mywait
[sleeper-root@elsa-c2] pid=597 uid=0 gid=0
                                                          [sleeper-root@anna-c2] pid=593 uid=0 gid=0
 uº 14.10 0:-*
                                                                        20m 0.00 2.0GHz 2.0G15% 2014-10-30 18:25:41
```

Elsa's Containers: **elsa-c1**, elsa-c2

```
🙆 🖨 📵 ubuntu@lxc-host (10.5.0.232) - byobu
 oot@lxc-host# showinfo files
                                                                 root@lxc-host# showinfo config
fname
                             uid
                                          gid
                                                                anna-c1/config:lxc.id map = u 0 2000000 65535
                                                       mode
                                                       mode=664 anna-c1/config:lxc.id_map = g 0 2000000 65535
sleeper-elsa@lxc-host.info
                                          gid=elsa
                             uid=elsa
sleeper-root@lxc-host.info
                             uid=root
                                          aid=root
                                                       mode=644 anna-c2/config:lxc.id map = u 0 2100000 65535
sleeper-anna@lxc-host.info
                             uid=anna
                                          aid=anna
                                                       mode=664 anna-c2/config:lxc.id map = g 0 2100000 65535
sleeper-root@anna-c1.info
                             uid=2000000
                                          aid=2000000
                                                       mode=664 elsa-c1/config:lxc.id map = u 0 3000000 65535
                                         gid=2100000
                                                       mode=664 elsa-c1/config:lxc.id_map = g 0 3000000 65535
sleeper-root@anna-c2.info
                             uid=2100000
                             uid=3001000
                                          qid=3001000
                                                       mode=644 elsa-c2/config:lxc.id_map = u 0 3100000 65535
sleeper-ubuntu@elsa-c1.info
sleeper-root@elsa-c2.info
                             uid=3100000
                                         gid=3100000 mode=664 elsa-c2/config:lxc.id map = g 0 3100000 65535
 root@lxc-host# showinfo ps
                                                                              # cat /etc/subuid
command
                        uid
                                 aid
                                          pid
                                                 userns
                                                                 anna:2000000:1000000
/sbin/init
                                                 4026531837
                                                                 elsa:3000000:1000000
                        root
/sbin/init
                        2000000
                                 2000000
                                          6900
                                                 4026532171
                                                                 cot@lxc-host# cat /etc/subgid
/sbin/init
                        2100000
                                 2100000
                                          7704
                                                 4026532294
                                                                 anna:2000000:1000000
 /sbin/init
                        3000000
                                 3000000
                                          8590
                                                 4026532233
                                                                 elsa:3000000:1000000
/sbin/init
                        3100000
                                 3100000
                                                 4026532356
                                                                 oot@lxc-host# moreinfo
                                          9340
sleeper-anna@lxc-host
                                                 4026531837
                                                                 https://github.com/hallyn/ods-2014-userns
                        anna
                                 1001
                                          11826
sleeper-root@anna-c1
                        2000000
                                 2000000
                                          12177
                                                 4026532171
                                                                 cubswin:)
sleeper-root@anna-c2
                                                                 root@lxc-host#
                        2100000 2100000
                                          12426 4026532294
sleeper-elsa@lxc-host
                        elsa
                                 1002
                                          13113 4026531837
sleeper-ubuntu@elsa-c1
                        3001000
                                 3001000
                                          14280
                                                 4026532233
sleeper-root@elsa-c2
                        3100000
                                 3100000 14535
                                                 4026532356
sleeper-root@lxc-host
                                                 4026531837
                        root
                                 0
                                          15506
root@lxc-host#
elsa@lxc-host$ mywait
                                                          anna@lxc-host$ mywait
[sleeper-elsa@lxc-host] pid=13109 uid=1002 gid=1002
                                                           [sleeper-anna@lxc-host] pid=11822 uid=1001 gid=1001
elsa@lxc-host$ lxc_attach elsa-c1
                                                           anna@lxc-host$ lxc_attach anna-c1
root@elsa-c1# sudo -Hu ubuntu mywait
                                                          root@anna-c1# mywait
[sleeper-ubuntu@elsa-c1] pid=597 uid=1000 gid=1000
                                                           [sleeper-root@anna-c1] pid=592 uid=0 gid=0
root@elsa-c2# mywait
                                                          root@anna-c2# mywait
[sleeper-root@elsa-c2] pid=597 uid=0 gid=0
                                                          [sleeper-root@anna-c2] pid=593 uid=0 gid=0
 uº 14.10 0:-*
                                                                           0.00 2.0GHz 2.0G15% 2014-10-30 18:25:41
```

Elsa's Containers: elsa-c1, elsa-c2

```
🙆 🖨 📵 ubuntu@lxc-host (10.5.0.232) - byobu
 oot@lxc-host# showinfo files
                                                                              t# showinfo config
fname
                             uid
                                                                 anna-c1/config:lxc.id map = u 0 2000000 65535
                                          aid
                                                        mode
                                                        mode=664 anna-c1/config:lxc.id_map = g 0 2000000 65535
sleeper-elsa@lxc-host.info
                             uid=elsa
                                          gid=elsa
sleeper-root@lxc-host.info
                             uid=root
                                          aid=root
                                                        mode=644 anna-c2/config:lxc.id map = u 0 2100000 65535
sleeper-anna@lxc-host.info
                             uid=anna
                                          aid=anna
                                                        mode=664 anna-c2/config:lxc.id map = g 0 2100000 65535
sleeper-root@anna-c1.info
                             uid=2000000
                                          aid=2000000
                                                       mode=664 elsa-c1/config:lxc.id map = u 0 3000000 65535
sleeper-root@anna-c2.info
                                                       mode=664 elsa-c1/config:lxc.id map = q 0 3000000 65535
                             uid=2100000
                                          gid=2100000
sleeper-ubuntu@elsa-c1.info
                                          gid=3001000
                                                       mode=644 elsa-c2/config:lxc.id_map = u 0 3100000 65535
                             uid=3001000
                             uid=3100000
                                          gid=3100000 mode=664 elsa-c2/config:lxc.id map = g 0 3100000 65535
 sleeper-root@elsa-c2.info
                                                                              # cat /etc/subuid
 pot@lxc-host# showinfo ps
command
                        uid
                                 aid
                                          pid
                                                  userns
                                                                 anna:2000000:1000000
/sbin/init
                                                  4026531837
                                                                 elsa:3000000:1000000
                        root
/sbin/init
                        2000000
                                 2000000
                                           6900
                                                  4026532171
                                                                  cot@lxc-host# cat /etc/subgid
/sbin/init
                        2100000 2100000
                                         7704
                                                 4026532294
                                                                 anna:2000000:1000000
/sbin/init
                        3000000 3000000
                                          8590
                                                 4026532233
                                                                 elsa:3000000:1000000
                                                                 root@lxc-host# moreinfo
https://github.com/hallyn/ods-2014-userns
 /sbin/init
                        3100000
                                                 4026532356
sleeper-anna@lxc-host
                                          11826
                                                 4026531837
                        anna
                                                                 cubswin:)
sleeper-root@anna-c1
                        2000000
                                 2000000
                                          12177
                                                 4026532171
                                                                  root@lxc-host#
sleeper-root@anna-c2
                        2100000
                                 2100000
                                          12426 4026532294
sleeper-elsa@lxc-host
                        elsa
                                 1002
                                          13113 4026531837
sleeper-ubuntu@elsa-c1
                        3001000
                                 3001000
                                          14280
                                                 4026532233
sleeper-root@elsa-c2
                                 3100000 14535
                                                 4026532356
sleeper-root@lxc-host
                                           15506
                                                 4026531837
                        root
                                 0
root@lxc-host#
elsa@lxc-host$ mywait
                                                           anna@lxc-host$ mywait
[sleeper-elsa@lxc-host] pid=13109 uid=1002 gid=1002
                                                           [sleeper-anna@lxc-host] pid=11822 uid=1001 gid=1001
elsa@lxc-host$ lxc_attach elsa-c1
                                                           anna@lxc-host$ lxc_attach anna-c1
root@elsa-c1# sudo -Hu ubuntu mvwait
                                                           root@anna-c1# mywait
[sleeper-ubuntu@elsa-c1] pid=597 uid=1000 gid=1000
                                                           [sleeper-root@anna-c1] pid=592 uid=0 gid=0
root@elsa-c2# mywait
                                                           root@anna-c2# mywait
[sleeper-root@elsa-c2] pid=597 uid=0 gid=0
                                                           [sleeper-root@anna-c2] pid=593 uid=0 gid=0
 u° 14.10 0:-*
                                                                            0.00 2.0GHz 2.0G15% 2014-10-30 18:25:41
```

User namespaces

Goals

- Uid separation
 - c1.500 != c2.500
 - Separate access controls (kill, open, etc)
 - Separate accounting, limits
- Container root privileged over container
 - uids
 - network
 - etc
- Ontainer root has no privilege outside of container
 - Root in container as safe as unpriv user on host
 - Safe for use by untrusted users
- Able to be nested

User namespace design

- By Eric Biederman
- ② Uids map 1-1 to kuids
 - Translated at kernel-user boundary
 - Default mapping 0-4294967295:0-4294967295
 - Unmapped userids show up as -1, has 'o' perms
 - 4 Unpriv user can only map own host uid
- Other namespaces owned by a user ns
 - Root in ns has full privilege over what it owns

Uid delegation

- Root delegates subuids to users
 - 1 /etc/subuid and /etc/subgid: serge:100000:65536
 - Set using usermod: usermod -v 100000-200000 -w 100000-200000 serge
- Setuid-root programs write to /proc/self/{ug}id_map
- Each user may be delegated a set of subuids and subgids