LXD Workshop

Ľubor Jurena

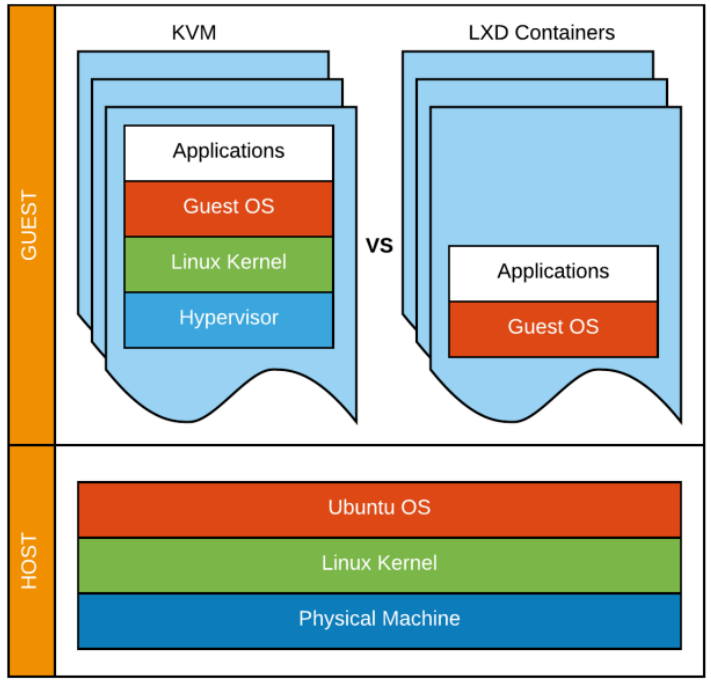
05.02.2017

Cieľ workshopu

- Zoznámiť sa s LXD a kontajnermi
- Inštalácia a úvodná konfigurácia LXD
- Spustenie prvých kontajnerov
- Základné príkazy

Čo je to kontajner?

- Izolovaný operačný systém
    - S pridelenými parametrami (vCPU, RAM, HDD, ...)
- Zdieľané jadro s hostom



Výhody kontajnerov

- Vyššia hustota
- Rýchly boot
- Nulová réžia
- Neemuluje sa hardvérová vrstva

„10x the density of ESX, 25% faster, zero latency“ ubuntu.com

Nevýhody kontajnerov

- Zdieľané jadro
- Žiadna správa zariadení, filesystému, partícii, ...

LXD

- Kontajner “hypervisor”
- Kernel >=3.13
- Apache License 2.0
- Bezpečnosť
    - User namespaces, cgroups, AppArmor, ...
- Intuitívne CLI
- Jednoduchá inštalácia v Ubuntu
- RestAPI

Inštalácia

- `# add-apt-repository ppa:ubuntu-lxc/lxd-stable`
- `# apt-get update`
- `# apt-get install lxd`
- `# apt-get install zfs`

- Ubuntu 16.04 repository: LXD 2.0.2
- ppa:ubuntu-lxc/lxd-stable repository: LXD 2.10

Úvodná konfigurácia

- `# lxd init`

```
Do you want to configure a new storage pool (yes/no) [default=yes]?
Name of the new storage pool [default=default]:
Name of the storage backend to use (dir or zfs) [default=zfs]:
Create a new ZFS pool (yes/no) [default=yes]? no
Name of the existing ZFS pool or dataset: data
Would you like LXD to be available over the network (yes/no) [default=no]?
Would you like stale cached images to be updated automatically (yes/no) [default=yes]?
Would you like to create a new network bridge (yes/no) [default=yes]?
What should the new bridge be called [default=lxdbr0]?
What IPv4 address should be used (CIDR subnet notation, “auto” or “none”) [default=auto]?
What IPv6 address should be used (CIDR subnet notation, “auto” or “none”) [default=auto]?
LXD has been successfully configured.
```

Inštalácia kontajneru

- `# lxc launch ubuntu:16.10 <name>`
- `# lxc launch ubuntu:16.04 <name>`
- `# lxc launch images:debian/jessie/amd64 <name>`

Práca s kontajnerom

- `# lxc exec <name> <command>`
- `# lxc pause <name>`
- `# lxc delete <name>`
- `# lxc file pull <container>/<path> <dest>`
- `# lxc file push <source> <container>/<path>`
- `# lxc file edit <container>/<path>`

Informácie

- `# lxc list`
- `# lxc list --fast`
- `# lxc info <name>`
- `# lxc config show --expanded <name>`

Bezpečnosť

- Privilegovaný kontajner
  - Root v kontajneri je root-om na hostiteľskom serveri
  - Kontajner beží pod root užívateľom
  - -c security.privileged=true
- Neprivilegovaný kontajner
  - Safe by design
  - Kernel funkcia, ktorá umožňuje namapovať rozsah UIDs na hostiteľovi do namespace, v ktorom môže existovať užívateľ s UID 0 (root)
  - Root v kontajneri != root na hostiteľskom serveri
  - -c security.privileged=false

Limity

- CPU
- Memory
- Disk
- Network
- Kernel resources

Limity

- `# lxc config set <name> limits.cpu 2`
- `# lxc config set <name> limits.memory 512MB`
- `# lxc config set <name> limits.memory.swap false`
- `# lxc config device set <name> root size 20GB`

Profily

- `# lxc profile list`
- `# lxc profile show <profile>`
- `# lxc profile create <profile>`
- `# lxc profile edit <profile>`
- `# lxc profile apply <container> <profile1>,<profile2>,…`

- `# lxc profile set <profile> limits.cpu 1`
- `# lxc launch ubuntu:16.04 -p <profile> -p <profile2>`

Snapshoty

- `# lxc snapshot <name> <name_snapshot>`
- `# lxc copy <name>/<name_snapshot> <new_container>`

Image management

- `# lxc image list images:`
- `# lxc image alias list ubuntu:`

- images.linuxcontainers.org

Vlastný image

- `# lxc launch ubuntu:16.04 <name>`
- `# lxc exec <name> bash`
- `# lxc publish <name> --alias my-new-image`

Sieťovanie

- `# lxc network show lxdbr0`
- `# lxc config device add <name> eth1 nic nictype=bridged parent=lxdbr0`

Sieťovanie

- Nictype:
  - Physical
  - Bridged
  - Macvlan
  - P2P

Problémy na záver ...

- `# dmesg`
  - `# echo 1 > /proc/sys/kernel/dmesg_restrict`
- `# cat /proc/meminfo`
- `Load Average`

Ďakujem za pozornosť :-)