In unprivileged LXC

Preparation

https://wiki.debian.org/LXC

```
apt-get install lxc
```

Create user:

```
sudo useradd -s /bin/bash -c 'Unifi lxc user' -m unifi
```

```
sudo passwd unifi
```

Find subuids and subgids for created user

```
sudo grep unifi /etc/sub{gid,uid}
```

```
/etc/subgid:unifi:1738400:65536
/etc/subuid:unifi:1738400:65536
```

Allow new user create network interfaces:

/etc/lxc/lxc-usernet

```
unifi veth br-lan 10
```

man 5 lxc-usernet

Now login as new user (using ssh or su). Create default lxc configureation in user directory:

```
mkdir -p ~/.config/lxc
cp /etc/lxc/default.conf ~/.config/lxc/default.conf
```

Edit file below and put subuid and subgid:

~/.config/lxc/default.conf

```
lxc.include = /etc/lxc/default.conf

lxc.idmap = u 0 1738400 65536
lxc.idmap = g 0 1738400 65536

# "Secure" mounting
lxc.mount.auto = proc:mixed sys:ro cgroup:mixed

lxc.net.0.type = veth
```

```
lxc.net.0.link = br-lan
lxc.net.0.flags = up
lxc.net.0.hwaddr = 00:FF:xx:xx:xx:xx

# Disable AppArmor confinement for containers started by non-root
# See
https://discuss.linuxcontainers.org/t/unprivileged-container-wont-start
-cgroups-sysvinit/6766 and
#
https://discuss.linuxcontainers.org/t/cannot-use-generated-profile-appa
rmor-parser-not-available/4449

lxc.apparmor.profile = unconfined
# Unprivileged containers started by ROOT can use lxc.apparmor.profile
= generated

/var/lib/lxc/ = ~/.local/share/lxc
/var/cache/lxc = ~/.cache/lxc
```

Create container:

```
lxc-create -t download -n unifi
```

- Distribution: debian
- Release: stretch
- Architecture: amd64

```
lxc-start -n unifi
lxc-ls -f
NAME  STATE   AUTOSTART GROUPS IPV4 IPV6 UNPRIVILEGED
unifi RUNNING 0         -      -    -    true
```

```
cat .ssh/authorized_keys | lxc-attach -n unifi -- /bin/sh -c 'cd /root &&
mkdir -p .ssh && cat > .ssh/authorized_keys'
lxc-attach -n unifi
passwd
...
<CTRL+D>
<code>

</code bash>
lxc-console -n unifi
apt-get install openssh-server gnupg2 sudo ca-certificates apt-transport-
https wget
<CTRL+D>
```

Add autostarting:

~/.local/share/lxc/unifi/config

```
lxc.start.auto = 1
lxc.start.delay = 5
lxc.start.order = 100
lxc.group = onboot
</code>


Edit cron <code bash>crontab -e</code>
<file>
@reboot /usr/bin/lxc-autostart --all
```

Issues

lxc-start: unifi: lxccontainer.c: wait_on_daemonized_start: 850 Received container state "STOPPING" instead of "RUNNING"

```
lxc-start -n unifi -l DEBUG -o debug.log
cat debug.log

lxc-start unifi 20210320203918.294 DEBUG    conf -
conf.c:chown_mapped_root:3146 - trying to chown "/dev/pts/1" to 1025
lxc-start unifi 20210320203918.310 INFO     start - start.c:lxc_init:926 -
Container "unifi" is initialized
lxc-start unifi 20210320203918.310 ERROR    cgfsng -
cgroups/cgfsng.c:mkdir_eexist_on_last:1275 - Permission denied - Failed to
create directory
"/sys/fs/cgroup/user.slice/user-1025.slice/session-73473.scope/lxc.monitor/"
lxc-start unifi 20210320203918.310 ERROR    cgfsng -
cgroups/cgfsng.c:monitor_create_path_for_hierarchy:1296 - Failed to create
cgroup
"/sys/fs/cgroup/user.slice/user-1025.slice/session-73473.scope/lxc.monitor/u
nifi"
lxc-start unifi 20210320203918.310 ERROR    cgfsng -
cgroups/cgfsng.c:cgfsng_monitor_create:1385 - Failed to create cgroup
"/sys/fs/cgroup/user.slice/user-1025.slice/session-73473.scope/lxc.monitor/u
nifi"
```

```
$ lxc-checkconfig
...
Cgroup v1 systemd controller: missing
Cgroup v1 freezer controller: missing
Cgroup namespace: required
...
```

Solution for unprivileged containers:

```
systemd-run --user --scope -p "Delegate=yes" lxc-start
```

Reason: https://wiki.debian.org/LXC/CGroupV2 Problem solved in LXC v4.0.2-1~1. Solution:

```
apt-get install lxc -t bullseye
```

Workaround 1: Add to container config:

```
lxc.cgroup.devices.allow =
lxc.cgroup.devices.deny =
# for unpriv container:
#lxc.apparmor.profile = unconfined
lxc.init.cmd = /sbin/init systemd.unified_cgroup_hierarchy=1
```

lxc.init.cmd = /sbin/init systemd.unified_cgroup_hierarchy

Workaround 2: CGroupsV2 is the new default. Set kernel commandline option: systemd.unified_cgroup_hierarchy=0 to retain the old default and lxc-start start container.

Workaround 3:

```
mount -o remount,rw /sys/fs/cgroup
mkdir /sys/fs/cgroup/devices
mount -t cgroup devices -o devices /sys/fs/cgroup/devices
mount -o remount,ro /sys/fs/cgroup
```

lxc-start: unifi: tools/lxc_start.c: main: 329 The container failed to start

```
lxc-start -n unifi -l DEBUG -o debug.log
cat debug.log

...
lxc-start unifi 20200720135645.187 ERROR    start -
start.c:print_top_failing_dir:120 - Permission denied - Could not access
/home/unifi/.local. Please grant it x access, or add an ACL for the
container root
...

sudo setfacl -m u:1738400:x . .local .local/share
```

Error: lxc-create: unifi: confile.c: set_config_net: 261 lxc.net must not have a value

LXC3 is using different config keys. Easiest way is to convert config file:

```
lxc-update-config -c default.conf
```

lxc-create: unifi: conf.c: chown_mapped_root: 3206 lxc-usernsexec failed: No such file or directory - Failed to open tt

```
sysctl kernel.unprivileged_userns_clone
kernel.unprivileged_userns_clone = 0

sudo echo "kernel.unprivileged_userns_clone=1" >> /etc/sysctl.conf
sysctl -p
```