

Лабораторная работа №11

Управление загрузкой системы (GRUB2)

Щемелев Илья Владимирович

Цель работы

Получить навыки работы с загрузчиком системы **GRUB2** в ОС **Rocky Linux**: изменение параметров загрузки, запуск в специальных режимах `systemd` и восстановление доступа (сброс пароля `root`).

Ход выполнения

Редактирование /etc/default/grub



```
GNU nano 8.1 /etc/default/grub Modified
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="resume=UUID=c87df1f1-f426-49f0-a032-e36dfbf38f76 rd.lvm.lv=r\ vbox/root rd.lvm.lv=>"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
```

Рис. 1: Редактирование файла /etc/default/grub

```
ivschemelev@ivschemelev:~$ su
Password:
root@ivschemelev:/home/ivschemelev# nano /etc/default/grub
root@ivschemelev:/home/ivschemelev# grub2-mkconfig > /boot/grub2/grub.cfg
Generating grub configuration file ...
Adding boot menu entry for UEFI Firmware Settings ...
done
```

Рис. 2: Генерация конфигурации GRUB2



Рис. 3: Меню загрузчика GRUB

A screenshot of a terminal window with a black background and white text. At the top, it says 'GRUB version 2.12'. Below that, a list of commands is entered: 'load_video', 'set gfxpayload=keep', 'insmod gzio', and a multi-line 'linux' command with various parameters including root, resume UUID, rd.lvm.lv, systemd.unit, crashkernel, and initrd. At the bottom, there is a block of text explaining Emacs-like screen editing features.

```
GRUB version 2.12

load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-6.12.0-124.21.1.el10_1.x86_64 root=/dev/mapper/rl_vbo\
x-root ro resume=UUID=c87df1f1-f426-49f0-a032-e36dfbf38f76 rd.lvm.lv=rl_vbo\
x/root rd.lvm.lv=rl_vbox/swap systemd.unit=rescue.target crashkernel=2G-64G\
:256M,64G-:512M
initrd ($root)/initramfs-6.12.0-124.21.1.el10_1.x86_64.img $tuned_initrd

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
a command-line or ESC to discard edits and return to the GRUB menu.
```


Проверка окружения rescue.target

```
system-modprobe.slice      loaded active active   Slice /system/modprobe
system.slice              loaded active active   System Slice
dm-event.socket           loaded active listening Device-mapper event daemon FIFOs
lvm2-lvmpolld.socket      loaded active listening LVM2 poll daemon socket
systemd-journald-dev-log.socket loaded active running  Journal Socket (/dev/log)
systemd-journald.socket   loaded active running  Journal Sockets
systemd-udevd-control.socket loaded active running  udev Control Socket
systemd-udevd-kernel.socket loaded active running  udev Kernel Socket
dev-disk-by\x2duuid-c87df1f1\x2d426\x2d49f0\x2da832\x2dc36dfbf3bf76.swap loaded active active   /dev/disk/by-uuid/c87df1f1-f426-49f0-a832-c36dfbf3bf76
cryptsetup.target         loaded active active   Local Encrypted Volumes
integritysetup.target     loaded active active   Local Integrity Protected Volumes
local-fs-pre.target       loaded active active   Preparation for Local File Systems
local-fs.target           loaded active active   Local File Systems
network-pre.target        loaded active active   Preparation for Network
rescue.target             loaded active active   Rescue Mode
sound.target              loaded active active   Sound Card
swap.target               loaded active active   Swaps
sysinit.target            loaded active active   System Initialization
veritysetup.target        loaded active active   Local Verity Protected Volumes

Legend: LOAD    + Reflects whether the unit definition was properly loaded.
          ACTIVE + The high-level unit activation state, i.e. generalization of SUB.
          SUB    + The low-level unit activation state, values depend on unit type.

69 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
root@ivschemelev:~#
```

Рис. 5: Список загруженных модулей systemd

Переход в emergency.target через параметры ядра

```
GRUB version 2.12

load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-6.12.0-124.21.1.el10_1.x86_64 root=/dev/mapper/rl_vbo\
x-root ro resume=UUID=c87df1f1-f426-49f0-a032-e36dfbf38f76 rd.lvm.lv=rl_vbo\
x/root rd.lvm.lv=rl_vbox/swap systemd.unit=emergency.target crashkernel=2G-\
64G:256M,64G-:512M
initrd ($root)/initramfs-6.12.0-124.21.1.el10_1.x86_64.img $tuned_initrd

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
a command-line or ESC to discard edits and return to the GRUB menu.
```

Рис. 6: Загрузка в режиме emergency.target

Проверка минимального набора модулей

```
● dev-disk-by\x2dpath-pci\x2d0000:00:0d.0\x2data\x2d1\x2dpart1.device loaded activating tex
● dev-disk-by\x2dpath-pci\x2d0000:00:0d.0\x2data\x2d1\x2dpart2.device loaded activating tex
● dev-disk-by\x2dpath-pci\x2d0000:00:0d.0\x2data\x2d1\x2dpart3.device loaded activating tex
● dev-disk-by\x2duuid-2825\x2d07\x2d14\x2d13\x2d06\x2d31\x2d55.device loaded activating tex
● dev-disk-by\x2duuid-cb669862\x2da8eb\x2d4e76\x2d8bca\x2d2beb4d488045e.device loaded activating tex
● dev-sda.device loaded activating tex
● dev-sda1.device loaded activating tex
● dev-sda2.device loaded activating tex
● dev-sda3.device loaded activating tex
● dev-sr0.device loaded activating tex
● dev-ttyS0.device loaded activating tex
1 ● dev-ttyS1.device loaded activating tex
● dev-ttyS2.device loaded activating tex
● dev-ttyS3.device loaded activating tex
● sys-devices-pci0000:00-0000:00:01.1-ata3-host2-target2:0:0-2:0:0:0-block-sr0.device loaded activating tex
● sys-devices-pci0000:00-0000:00:03.0-net-eth0s3.device loaded activating tex
● sys-devices-pci0000:00-0000:00:0d.0-ata1-host0-target0:0:0-0:0:0:0-block-sda-sda1.device loaded activating tex
● sys-devices-pci0000:00-0000:00:0d.0-ata1-host0-target0:0:0-0:0:0:0-block-sda-sda2.device loaded activating tex
1 ● sys-devices-pci0000:00-0000:00:0d.0-ata1-host0-target0:0:0-0:0:0:0-block-sda-sda3.device loaded activating tex
● sys-devices-pci0000:00-0000:00:0d.0-ata1-host0-target0:0:0-0:0:0:0-block-sda.device loaded activating tex
● sys-devices-platform-serial18250-serial18250:0-serial18250:0.0-tty-ttyS0.device loaded activating tex
● sys-devices-platform-serial18250-serial18250:0-serial18250:0.1-tty-ttyS1.device loaded activating tex
● sys-devices-platform-serial18250-serial18250:0-serial18250:0.2-tty-ttyS2.device loaded activating tex
● sys-devices-platform-serial18250-serial18250:0-serial18250:0.3-tty-ttyS3.device loaded activating tex
● sys-devices-virtual-block-dm\x2d0.device loaded active plu
● sys-devices-virtual-block-dm\x2d1.device loaded active plu
● sys-module-configfs.device loaded activating tex
● sys-module-fuse.device loaded activating tex
1 ● sys-subsystem-net-devices-eth0s3.device loaded activating tex
- .mount loaded active mon
  sys-kernel-config.mount loaded active mon
  init.scope loaded active ru
  emergency.service loaded active ru
X plymouth-start.service loaded active ex
systemd-journald.service loaded active ru
- .slice loaded active act
1 system-modprobe.slice loaded active act
system.slice loaded active act
systemd-journald-dev-log.socket loaded active ru
systemd-journald.socket loaded active ru
emergency.target loaded active act

Legend: LOAD    + Reflects whether the unit definition was properly loaded.
              ACTIVE + The high-level unit activation state, i.e. generalization of SUB.
              SUB    + The low-level unit activation state, values depend on unit type.
```

78 Loaded units listed. Pass --all to see loaded but inactive units, too.

To show all installed unit files use 'systemctl list-unit-files'.

root@vachemelev:~#

Остановка загрузки на этапе initramfs (rd.break)

GRUB version 2.12

```
load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-6.12.0-124.21.1.el10_1.x86_64 root=/dev/mapper/rl_vbo\
x-root ro resume=UUID=c87df1f1-f426-49f0-a032-e36dfbf38f76 rd.lvm.lv=rl_vbo\
x/root rd.lvm.lv=rl_vbox/swap rd.break_crashkernel=2G-64G:256M,64G-:512M
initrd ($root)/initramfs-6.12.0-124.21.1.el10_1.x86_64.img $tuned_initrd
```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.

Рис. 8: Загрузка в режиме rd.break

Действия в окружении восстановления

```
Give root password for maintenance
(or press Control-D to continue):
sh-5.2# mount -o remount,rw /sysroot
sh-5.2# chroot /sysroot/
sh-5.2# reboot[ 56.124540] sched: DL replenish lagged too much
sh-5.2#
sh-5.2# passwd
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
sh-5.2# load_policy -i
[ 90.186495] audit: type=1404 audit(1768562724.284:2): enforcing=1 old_enforcing=0 auid=4294967295 ses=4294967295 en
[ 90.320706] SELinux: policy capability network_peer_controls=1
[ 90.320837] SELinux: policy capability open_perms=1
[ 90.320953] SELinux: policy capability extended_socket_class=1
[ 90.321042] SELinux: policy capability always_check_network=0
[ 90.321139] SELinux: policy capability cgroup_seclabel=1
[ 90.321225] SELinux: policy capability mnp_nosuid_transition=1
[ 90.321309] SELinux: policy capability genfs_seclabel_symlinks=1
[ 90.321395] SELinux: policy capability ioctl_skip_cloexec=0
[ 90.321481] SELinux: policy capability userspace_initial_context=0
[ 90.745710] audit: type=1403 audit(1768562724.839:3): auid=4294967295 ses=4294967295 lsm=selinux res=1
sh-5.2# chcon -t shadow_t /etc/shadow
[ 103.479103] audit: type=1400 audit(1768562737.576:4): avc: denied { create } for pid=859 comm="sh" scontext=syste
u:system_r:kernel_t:s0 tclass=netlink_audit_socket permissive=0
[ 103.480426] audit: type=1400 audit(1768562737.578:5): avc: denied { read write } for pid=865 comm="chcon" path="
system_u:system_r:kernel_generic_helper_t:s0 tcontext=system_u:object_r:device_t:s0 tclass=chr_file permissive=0
[ 103.480795] audit: type=1400 audit(1768562737.578:6): avc: denied { read write } for pid=865 comm="chcon" path="
system_u:system_r:kernel_generic_helper_t:s0 tcontext=system_u:object_r:device_t:s0 tclass=chr_file permissive=0
[ 103.481159] audit: type=1400 audit(1768562737.578:7): avc: denied { read write } for pid=865 comm="chcon" path="
system_u:system_r:kernel_generic_helper_t:s0 tcontext=system_u:object_r:device_t:s0 tclass=chr_file permissive=0
[ 103.481695] audit: type=1400 audit(1768562737.578:8): avc: denied { read write } for pid=865 comm="chcon" path="
system_u:system_r:kernel_generic_helper_t:s0 tcontext=system_u:object_r:device_t:s0 tclass=chr_file permissive=0
[ 103.481698] audit: type=1400 audit(1768562737.579:9): avc: denied { getattr } for pid=865 comm="chcon" path="/etc
system_u:system_r:kernel_generic_helper_t:s0 tcontext=system_u:object_r:unlabeled_t:s0 tclass=file permissive=0
[ 103.481699] audit: type=1400 audit(1768562737.579:10): avc: denied { getattr } for pid=865 comm="chcon" path="/e
t=system_u:system_r:kernel_generic_helper_t:s0 tcontext=system_u:object_r:unlabeled_t:s0 tclass=file permissive=0
sh-5.2#
```

Итоги работы

В работе изучены практические приёмы управления загрузчиком **GRUB2** в **Rocky Linux**: изменение параметров меню загрузки, запуск системы в режимах **rescue** и **emergency**, а также восстановление доступа путём сброса пароля **root** с учётом требований **SELinux**.