

Лабораторная работа №11

Управление загрузкой системы (GRUB2)

Щемелев Илья Владимирович

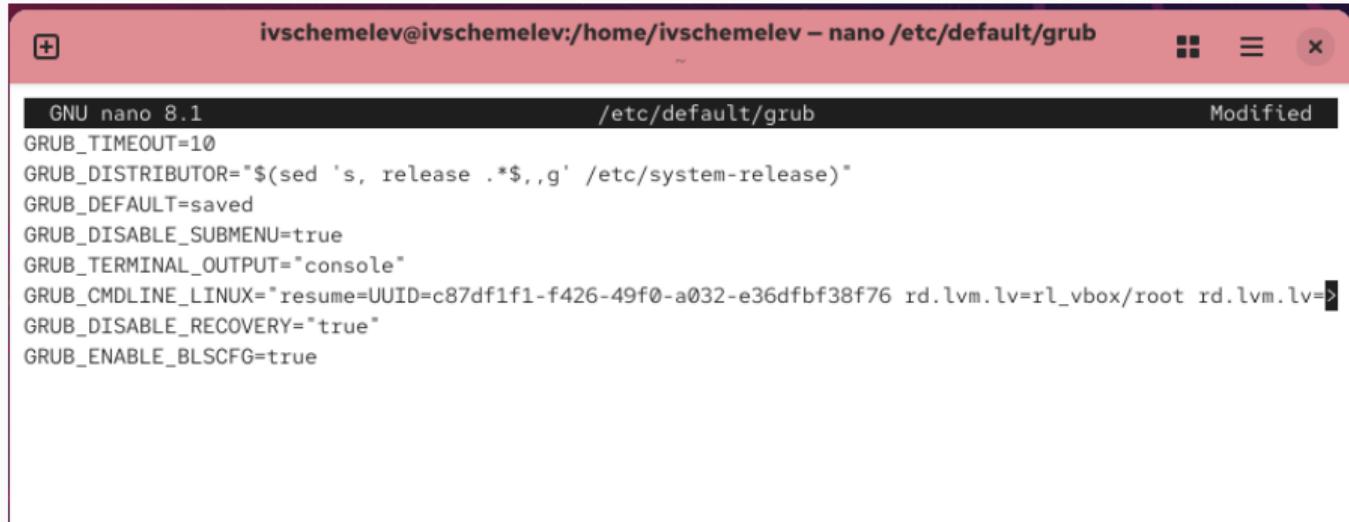
Цель работы

Формулировка цели

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



The screenshot shows a terminal window titled "ivschemelev@ivschemelev: /home/ivschemelev – nano /etc/default/grub". The window has a red header bar. The main area contains the following text:

```
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=rl_vbox/root rd.lvm.lv=>
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
```

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

Генерация новой конфигурации GRUB2

```
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

Проверка меню загрузчика после перезагрузки



Рис. 3: Меню загрузчика GRUB

Редактирование параметров записи загрузки



Рис. 4: Редактирование параметров загрузки ядра

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\x2df426\x2d49f0\x2da832\x2de36dfbf38f76.swap
cryptsetup.target               loaded active active  /dev/disk/by-uuid/c87df1f1-f426-49f0-a832
integritysetup.target           loaded active active  Local Encrypted Volumes
local-fs-pre.target             loaded active active  Local Integrity Protected Volumes
local-fs.target                 loaded active active  Preparation for Local File Systems
network-pre.target              loaded active active  Local File Systems
rescue.target                  loaded active active  Preparation for Network
sound.target                   loaded active active  Rescue Mode
swap.target                    loaded active active  Sound Card
sysinit.target                 loaded active active  Swaps
veritysetup.target              loaded active active  System Initialization
                               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@lvschemelev:~#
```

Рис. 5: Список загруженных модулей systemd

Переход в emergency.target через параметры ядра



Рис. 6: Загрузка в режиме emergency.target

Проверка минимального набора модулей

```
# systemctl list-units --type=service --no-pager
● dev-disk-by\x2dpath-pci\x2d0000:00:0d.0\x2ddata\x2d1\x2dpart1.device          loaded  activating  tex
● dev-disk-by\x2dpath-pci\x2d0000:00:0d.0\x2ddata\x2d1\x2dpart2.device          loaded  activating  tex
● dev-disk-by\x2dpath-pci\x2d0000:00:0d.0\x2ddata\x2d1\x2dpart3.device          loaded  activating  tex
● dev-disk-by\x2duuid-id-2025\x2d87\x2d14\x2d13\x2d06\x2d31\x2d55.device        loaded  activating  tex
● dev-disk-by\x2duuid-cb669862\x2da8eb\x2d4c76\x2d8bcav\x2dbeb4d498045e.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
● dev-ttyS1.device                        loaded  activating  tex
● dev-ttyS2.device                        loaded  activating  tex
● dev-ttyS3.device                        loaded  activating  tex
● sys-devices-pci0000:00:00:08:01.1-ata3-host2-target2:0:0-2:0:0:0-block-sr0.device
● sys-devices-pci0000:00:00:08:03.0-net-emp0s3.device                      loaded  activating  tex
● sys-devices-pci0000:00:00:08:0d.0-ata1-host0-target0:0:0-0:0:0-block-sda-sda1.device
● sys-devices-pci0000:00:00:08:0d.0-ata1-host0-target0:0:0-0:0:0-block-sda-sda2.device
● sys-devices-pci0000:00:00:08:0d.0-ata1-host0-target0:0:0-0:0:0-block-sda-sda3.device
● sys-devices-pci0000:00:00:08:0d.0-ata1-host0-target0:0:0-0:0:0-block-sda.device    loaded  activating  tex
● sys-devices-platform-serial18250-serial18250:0-serial18250:0.0-tty-ttyS0.device
● sys-devices-platform-serial18250-serial18250:0-serial18250:0.1-tty-ttyS1.device
● sys-devices-platform-serial18250-serial18250:0-serial18250:0.2-tty-ttyS2.device
● sys-devices-platform-serial18250-serial18250:0-serial18250:0.3-tty-ttyS3.device
● sys-devices-virtual-block-dm\x2d0.device                                loaded active   phe
● sys-devices-virtual-block-dm\x2d1.device                                loaded active   phe
● sys-module-configure.device                                         loaded  activating  tex
● sys-module-fuse.device                                              loaded  activating  tex
● sys-subsystem-net-devices-emp0s3.device
  - .mount                                                 loaded active   moun
  - sys-kernel-configuration.mount                               loaded active   moun
  - init.scope                                               loaded active   runn
  - emergency.service                                         loaded active   runn
  - plymouth-start.service                                     loaded active   runn
  - systemd-journald.service                                  loaded active   runn
  - .slice                                                 loaded active   acti
  - system-modprobe.slice                                    loaded active   acti
● system.slice                                             loaded active   acti
● systemd-journald-dev-log.socket                            loaded active   runn
● systemd-journald.socket                                 loaded active   runn
● emergency.target                                         loaded active   acti
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@iuschemelev: #
```

Остановка загрузки на этапе initramfs (rd.break)



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
[ 90.321842] SELinux: policy capability always_check_network=0
[ 90.321139] SELinux: policy capability cgroup_seclabel=1
[ 90.321225] SELinux: policy capability npn_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 lsmp=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=system_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 { setattr } 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 { setattr } 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
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.