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

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

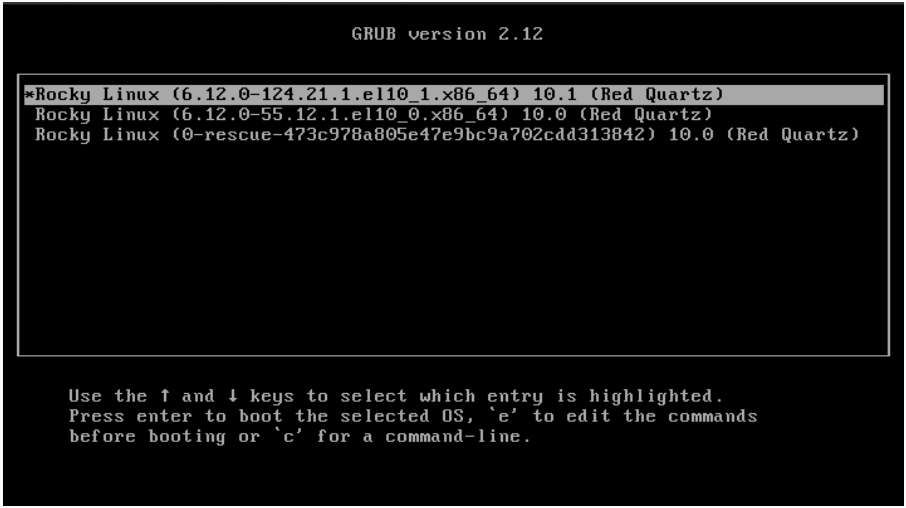


Рис. 3: Меню загрузчика GRUB

Редактирование параметров записи загрузки

Рис. 4: Редактирование параметров загрузки ядра

Проверка окружения rescue.target

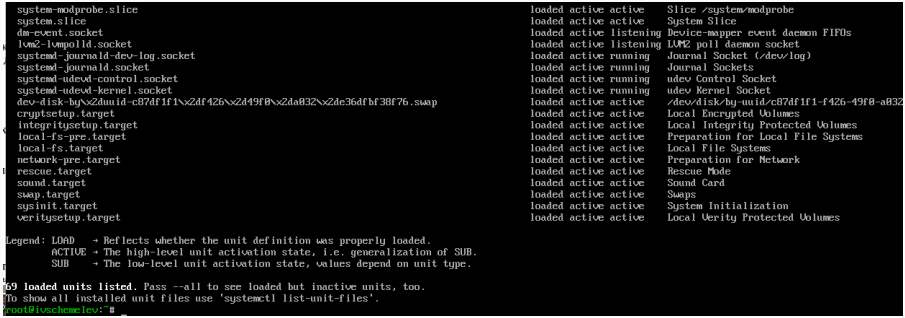
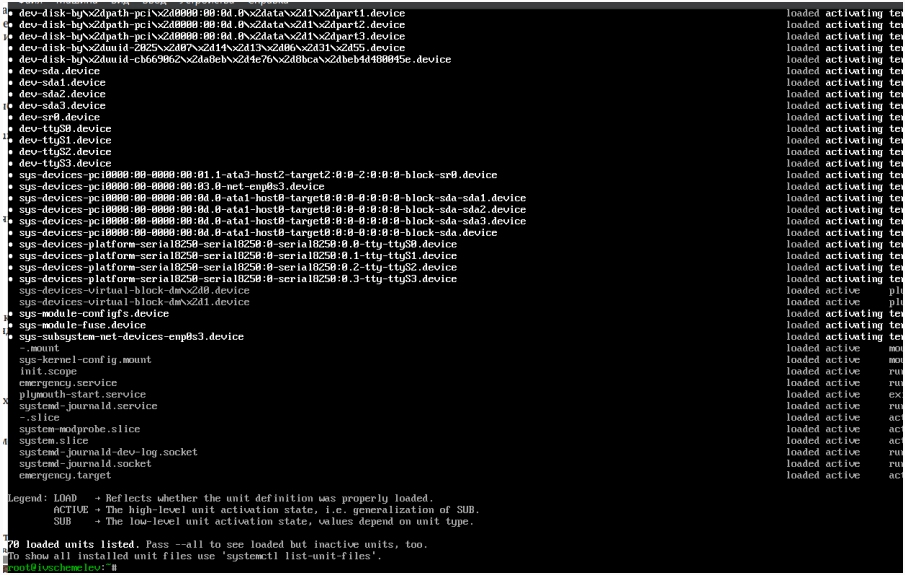


Рис. 5: Список загруженных модулей systemd

Переход в emergency.target через параметры ядра

Рис. 6: Загрузка в режиме emergency.target

Проверка минимального набора модулей



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
[    90.321042] SELinux:  policy capability always_check_network=0
[    90.321139] SELinux:  policy capability cgroup_seclabel=1
[    90.321225] SELinux:  policy capability nnp_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=syst
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="/et
=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

Заключение

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**.