**Breaking the Root Password**

1. **Method 1:**
   * Restart the server.
   * Press the arrow key on the GRUB menu to select the boot entry.
   * Press e to edit the boot parameters.
   * Add rd.break to the end of the line.
   * Press Ctrl+x to boot with the modified parameters.
   * Remount the sysroot with read-write permissions:

bash

mount -o remount,rw /sysroot

* + Change the root to sysroot:

bash

chroot /sysroot

* + Set a new root password:

bash

passwd

* + Relabel SELinux:

bash

touch /.autorelabel

* + Exit twice to reboot.

1. **Method 2:**
   * Follow the same steps as Method 1, but add selinux=0 along with rd.break.
   * The rest of the steps are identical to Method 1.

**Linux Boot Process**

1. **Hardware Boot:**
   * Power on.
   * POST (Power-On Self-Test) checks.
   * BIOS (Basic Input/Output System) runs and finds the first boot device.
2. **Boot Loader:**
   * Loads the operating system.
   * RHEL 5, 6, 7 use GRUB (Grand Unified Boot Loader).
   * RHEL 8, 9 use GRUB2.
   * Configuration file: /boot/grub2/grub.cfg.
3. **Kernel:**
   * Interface between hardware and the operating system.
   * Kernel image: /boot/initramfs-5.14.0-412.el9.x86\_64.img.
4. **Systemd:**
   * Starts processes.
   * View process tree with pstree.
5. **Login Screen:**
   * Username information: /etc/passwd.
   * Password information: /etc/shadow.

**GRUB Corruption and Recovery**

1. **Recovering GRUB:**
   * Change to the GRUB directory:

bash

cd /boot/grub2

* + Remove the grub.cfg file:

bash

rm -f grub.cfg

* + Reboot the system:

bash

init 6

* + In GRUB rescue mode, shut down the VM and access BIOS.
  + Set the first boot device to CD-ROM.
  + Boot into rescue mode from CentOS Stream.
  + Chroot to the mounted system image:

bash

chroot /mnt/sysimage

* + Recreate the GRUB configuration:

bash

grub2-mkconfig -o /boot/grub2/grub.cfg

* + Relabel SELinux:

bash

touch /.autorelabel

* + Exit twice to reboot.

**GRUB Password Management**

1. **Setting a GRUB Password:**
   * Change to the GRUB directory:

bash

cd /boot/grub2

* + Set the GRUB password:

bash

grub2-setpassword

* + Reboot the system:

bash

init 6

1. **Breaking the GRUB Password:**
   * Access BIOS and set the first boot device to CD-ROM.
   * Boot into rescue mode from CentOS Stream.
   * Chroot to the mounted system image:

bash

chroot /mnt/sysimage

* + Change to the GRUB directory:

bash

cd /boot/grub2

* + Remove the user.cfg file:

bash

rm -f user.cfg

**Kernel Panic Troubleshooting**

1. **Recovering from Kernel Panic:**
   * Change to the boot directory:

bash

cd /boot

* + Remove the problematic initramfs file:

bash

rm -f initramfs-5.14.0-412.el9.x86\_64.img

* + Reboot the system:

bash

init 6

* + Use the current kernel version:

bash

uname -r

* + Create a new initramfs image:

bash

dracut initramfs-<version>.img

* + If the file already exists, force create it:

bash

mkinitrd --force <version>.img <version>

* + Reboot the system:

bash

init 6

1. **Fstab File Errors:**
   * If the system stops at Control-D prompt, provide the root password.
   * Edit the /etc/fstab file to correct any errors:

bash

vim /etc/fstab

* + Save and exit:

bash

:wq

* + Reboot the system:

bash

init 6

**Additional Concepts**

**GRUB (Grand Unified Boot Loader)**

* Boot loader package managing the boot process of your OS.
* **GRUB Legacy (GRUB 1)**: Used in older Linux distributions.
* **GRUB 2**: Default for modern Linux distributions.
* **Commands**: grub2-mkconfig, grub2-setpassword.

**Kernel**

* Core component acting as a bridge between hardware and software.
* **Kernel Panic**: When the kernel cannot proceed.
* **Commands**: uname -r, dracut, mkinitrd.

**initramfs (Initial RAM File System)**

* Temporary file system loaded into memory at boot time.
* Contains necessary drivers and scripts for hardware initialization.

**systemd**

* System and service manager initializing the system and managing services.
* **Commands**: systemctl get-default, systemctl isolate, systemctl set-default.