

# RHEL System with LVM Fails to Boot After Bare Metal Restore (BMR)

## RHEL System with LVM Fails to Boot After Bare Metal Restore (BMR)

### Summary

After performing a Bare Metal Restore (BMR) on a Red Hat Enterprise Linux (RHEL) based system that uses Logical Volume Manager (LVM), the system may fail to boot normally and instead drop to a dracut prompt or require booting into rescue mode. This issue can often be resolved by regenerating the initramfs and rebuilding the GRUB configuration.

### Symptoms

- System fails to boot after a Bare Metal Restore.
- Boot process stops at a dracut prompt.
- The operating system does not load normally.
- Manual intervention is required to access the system.

```
Warning: /dev/almalinux/root does not exist
Warning: /dev/almalinux/swap does not exist
Warning: /dev/mapper/almalinux-root does not exist

Generating "/run/initramfs/rdsosreport.txt"

Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.

dracut:/# _
```

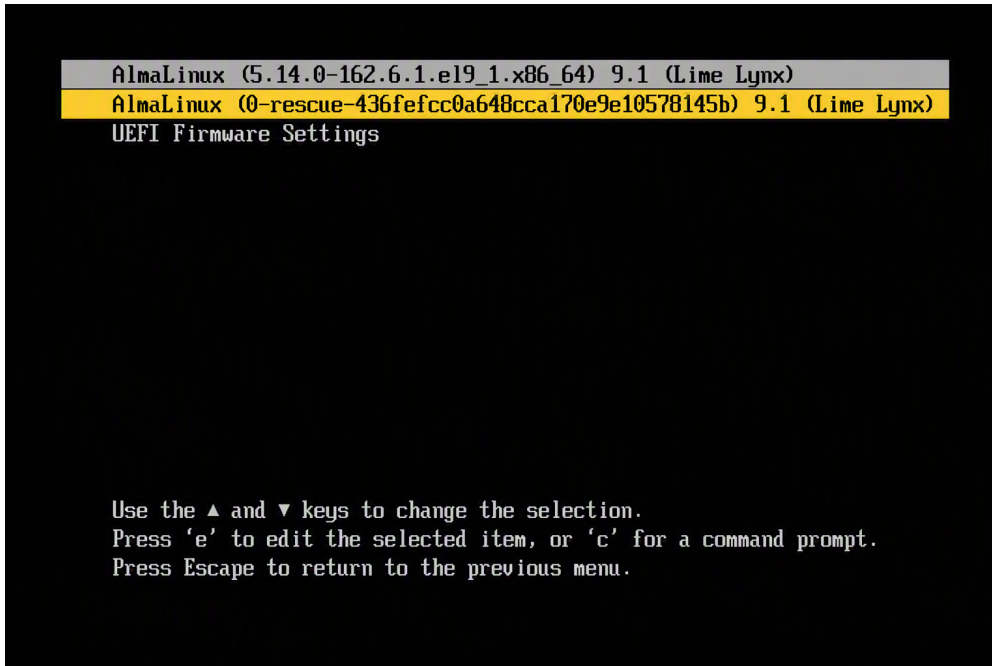
### Environment

- Red Hat Enterprise Linux (RHEL)
- RHEL-based distributions
- Systems using Logical Volume Manager (LVM)
- Systems restored through a Bare Metal Restore (BMR) process

### Resolution

## Step 1: Boot into Rescue Mode

1. Reboot the restored system.
2. From the boot menu, select the Rescue Mode option.
3. Log in to the system when prompted.



## Step 2: Regenerate the Initramfs

At the dracut prompt (or from the rescue environment shell), run the following command:

```
dracut --regenerate-all -f
```

This command rebuilds the initramfs images for all installed kernels and ensures the necessary drivers and LVM components are included.

## Step 3: Rebuild the GRUB Configuration

After the initramfs regeneration completes successfully, rebuild the GRUB configuration:

```
grub2-mkconfig > /boot/grub2/grub.cfg
```

This command recreates the GRUB configuration file to reflect the current system state.



### SELinux

If SELinux is used, it may also be necessary to prompt SELinux to scan and reset security context labels by creating an empty `.autorelabel` file in the root directory.

```
# touch /.autorelabel
```

## Step 4: Reboot the System

```
reboot
```

## Verification

After rebooting, verify that:

- The system boots normally without entering rescue mode.
- The root filesystem mounts successfully.
- LVM volumes are available.
- No boot-related errors appear during startup.

## Additional Notes

If the issue persists after performing the above steps, review the following logs:

- `/var/log/messages`
- `journalctl -xb`

Also review any GRUB or dracut-related error messages displayed during boot. These logs can provide additional insight into any remaining boot configuration or storage-related issues.