

# 运维之路—linux忘记密码修改 (rd.break 方式)

## RedHat 7 rd.break方式破解root密码

### 1.开机进入grub界面， 开机按两次e键

```
Red Hat Enterprise Linux Server (3.10.0-693.el7.x86_64) 7.4 (Maipo)
Red Hat Enterprise Linux Server (0-rescue-2fca90e46a2948219df66dc81819ab→
```

[https://blog.csdn.net/qq\\_36586867](https://blog.csdn.net/qq_36586867)

### 2.找到linux16这一行，如果是物理机，添加：rd.break，如果是虚拟机，添加：rd.break console=tty0，这里末尾添加 rd.break console=tty0

```
insmod xfs
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1' b19fb207-5\
e6b-4ea7-b2f7-dd1de44492b3
else
    search --no-floppy --fs-uuid --set=root b19fb207-5e6b-4ea7-b2f7-dd1d\
e44492b3
fi
→linux16 /vmlinuz-3.10.0-693.el7.x86_64 root=/dev/mapper/rhel-root ro c\
rashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet LANG=zh_CN.\
UTF-8 rd.break console=tty0_ ←此处添加内容
initrd16 /initramfs-3.10.0-693.el7.x86_64.img
```

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to  
discard edits and return to the menu. Pressing Tab lists  
possible completions.

[https://blog.csdn.net/qq\\_36586867](https://blog.csdn.net/qq_36586867)

### 3.ctrl + x 进入switch\_root

```
[ 2.070356] sd 0:0:0:0: [sda] Assuming drive cache: write through
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.

switch_root:/#
```

← 进入switch\_root模式 [https://blog.csdn.net/qq\\_36586867](https://blog.csdn.net/qq_36586867)

#### 4. 输入命令mount，发现根为/sysroot/，并且不能写，只有ro=readonly权限

```
switch_root:/# mount
rootfs on / type rootfs (rw)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=917544k,nr_inodes=229386,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_prio,net_cls)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/mapper/rhel-root on /sysroot type xfs (ro,relatime,attr2,inode64,noquota)
switch_root:/#
```

← 根路径为/sysroot，只读 [https://blog.csdn.net/qq\\_36586867](https://blog.csdn.net/qq_36586867)

#### 5. 重新挂载已经挂载了的根文件系统（以读写权限挂载）

执行命令：mount -o remount,rw /sysroot

```
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# mount
rootfs on / type rootfs (rw)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=917544k,nr_inodes=229386,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_prio,net_cls)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/mapper/rhel-root on /sysroot type xfs (rw,relatime,attr2,inode64,noquota)
switch_root:/#
```

← 重新挂载根文件系统为rw可读可写  
← 查看是否挂载成功  
← 已具有w权限 [https://blog.csdn.net/qq\\_36586867](https://blog.csdn.net/qq_36586867)

-o <选项> 指定挂载文件系统时的选项

defaults 使用所有选项的默认值 (auto、nouser、rw、suid)

auto/noauto 允许/不允许以 -a选项进行安装

dev/nodev 对/不对文件系统上的特殊设备进行解释

exec/noexec 允许/不允许执行二进制代码

suid/nosuid 确认/不确认suid和sgid位

user/nouser 允许/不允许一般用户挂载

codepage=XXX 代码页

iocharset=XXX 字符集

ro 以只读方式挂载

rw 以读写方式挂载

remount 重新安装已经安装了的文件系统

loop 挂载“回旋设备”以及“ISO镜像文件”

**6.挂载好后将根改成sysroot。（执行命令：chroot /sysroot）并在根下创建.autorelabel文件（selinux标签验证,即允许你修改密码）,再给root设置新密码。**

```
switch_root:/# chroot /sysroot ← 修改根
sh-4.2# touch /.autorelabel
sh-4.2# echo 123456 |passwd --stdin root ← 修改root密码
      root
passwd
sh-4.2# _
```

[https://blog.csdn.net/qq\\_36586867](https://blog.csdn.net/qq_36586867)

**7.exit退出，reboot重启后新密码登录**

```
sh-4.2#
sh-4.2#
sh-4.2# exit
exit
switch_root:/# reboot _
```

[https://blog.csdn.net/qq\\_36586867](https://blog.csdn.net/qq_36586867)

方法二

如果不知道旧密码，则需要重启系统，通过如下方式修改

重启系统，在开机过程中，快速按下键盘上的方向键和。目的是告知引导程序，我们需要在引导页面选择不同的操作，以便让引导程序暂停。

按键盘 e 键，进入编辑模式，找到 linux16 的那一行。将光标一直移动到

LANG=en\_US.UTF-8 后面，空格，再追加 init=/bin/sh。这里特别注意，需要写在UTF-8后，保持再同一行，并注意空格。由于屏幕太小，会自动添加换行，这个是正常的。

二 按下Ctrl+X 进行引导启动(单用户模式启动)，成功后进入该界面。然后输入以下命令

1 挂载根目录

```
mount -o remount, rw /
```

2 选择要修改密码的用户名，这里选择root用户进行修改，可以更换为你要修改的用户

```
echo 123456 | passwd --stdin root
```

3 输入2次一样的新密码，注意输入密码的时候屏幕上不会有字符出现。

如果输入的密码太简单，会提示警告BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic) ，可以无视它，继续输入密码，不过建议还是设置比较复杂一些的密码，以保证安全性

4 更新系统信息 touch /.authorelabel

```
touch /.authorelabel
```

5 最后输入以下命令重启系统即可

```
exec /sbin/init 或exec /sbin/reboot
```