# rhel7启动修复

2015年6月22日 16:07

一、RHEL7中MBR GRUB的修复（grub错误、误删）

命令：#dd if=/dev/zero of=/dev/sda bs=1 count=446

grub被损坏，此时救援模式是无法进入的，只能通过光盘或者u盘启动，选择进入trouleshooting模式，选择resuce，后面的操作跟红帽6的类似。主要命令的变化在于6里面用的是grub-install，而7里面用的是gurb2-install，其他都一样。

二、删除boot目录下的所有内容（模拟内核更新失败，或者模拟误删除内核）

此时仍然只能通过u盘或者光盘里面的resuce模式修复。修复过程和rhel6类似。

chroot /mnt/sysimage

mount /dev/cdrom /mnt

找到光盘中的内核包，用rpm -ivh --force kernel-3……命令安装内核（需要等待一段时间）

因为原来/boot/目录下的所有内容都被我们删除了，所以内核重新安装好之后，是不会在/boot目录下生成grub目录的，所以还需要安装grub。再运行一次grub2-install，安装还好grub之后和rhel6一样，里面是没有grub的配置文件，但是7里面比较方便的是，我们不需要像6一样去手动生成一个grub.cfg的文件，可以用命令grub2-mkconfig 自动生成。

三、修改、忘记root密码

- 如果rhel7中丢失root密码，需要调用一个shell去修改密码。在内核后面加上 init=/bin/sh

1. 启动时在grub界面选择启动的项目，然后按e进行编辑，找到内核，在内核后面加上参数init=/bin/sh，然后按ctrl+x启动（默认如果直接这样进入，会出现参数的回显等莫名其妙的bug。要解决这个问题，需要删除内核后面的2个参数，一个是rhgb，一个是quiet）

2. 在sh后面输入passwd是

   无法修改root密码的，因为当前的/是被只读的方式挂载的。所以我们需要以读写的方式挂载

   ```
   mount -o remount,rw / #读写方式重新挂载根分区/
   passwd
   touch /.autorelabel
   exec /sbin/init
   ```

   至此密码生效

四、grub2 加密

几乎能接触到物理机的人都能用上面的方法去修改root密码，安全性还是有点问题，我们可以通过 grub 菜单加密，进入 grub 时必须输入密码，这样就能避免上述情况发生。

1、 7.0 和 7.1方法如下

1)、执行生成加密密码的命令"grub2-mkpasswd-pbkdf2",两次输入相同密码，PBKDF2 hash of your password is 之后的部分就是加密后的密码

```
[root@CentOS-04 ~]# grub2-mkpasswd-pbkdf2
输入口令：
Reenter password:
PBKDF2 hash of your password is
grub.pbkdf2.sha512.10000.497F246861691979B9B7A6E3758A865929ED27D121E913DB7CE825BA8051A6F12C8AFA6A1A497BA87AC2AEEF2FDDC2935231 14CA
C53603B78B6BD790EEE802A7.3E1A2876C499CD9F12A8A634C7D4A18B84F8F0AF69BDB4D9C1E859A1861BB01EA5E34BBF65388CED8F4435C50051C61FBB46 0E48
9F1D1E4DA41A5B5984E43F1C
```

2)、编辑 /etc/grub.d/40_custom 文件，添加内容如下，密码为上面加密之后的密码

```
set superusers = "root"
password_pbkdf2 root
grub.pbkdf2.sha512.10000.497F246861691979B9B7A6E3758A865929ED27D121E913DB7CE825BA8051A6F12C8AFA6A1A497BA87AC2AEEF2FDDC2935231 14CA
C53603B78B6BD790EEE802A7.3E1A2876C499CD9F12A8A634C7D4A18B84F8F0AF69BDB4D9C1E859A1861BB01EA5E34BBF65388CED8F4435C50051C61FBB46 0E48
9F1D1E4DA41A5B5984E43F1C
```

文件内容如下

```
# cat /etc/grub.d/40_custom
#!/bin/sh
exec tail -n +3 $0
# This file provides an easy way to add custom menu entries.  Simply type the
# menu entries you want to add after this comment.  Be careful not to change
# the 'exec tail' line above.
set superusers = "root"
password_pbkdf2 root  grub.pbkdf2.sha512.10000.497F246861691979B9B7A6E3758A865929ED27D121E913DB7CE825BA8051A6F12C8AFA6A1A497BA87A
C2AEEF2FDDC293523114CAC53603B78B6BD790EEE802A7.3E1A2876C499CD9F12A8A634C7D4A18B84F8F0AF69BDB4D9C1E859A1861BB01EA5E34BBF65388C ED8F
4435C50051C61FBB460E489F1D1E4DA41A5B5984E43F1C
```

3)、然后执行命令"grub2-mkconfig -o /boot/grub2/grub.cfg"重新生成配置文件。

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.10.0-862.el7.x86_64
Found initrd image: /boot/initramfs-3.10.0-862.el7.x86_64.img
Found linux image: /boot/vmlinuz-0-rescue-5cd1608ab306482b8813c487489ccd84
```

Found initrd image: /boot/initramfs-0-rescue-5cd1608ab306482b8813c487489ccd84.img
done
4)、reboot 重启，进行验证

2、7.2 + 方法如下

从7.2开始，上述用于保护Grub的方法不起作用。在7.2中引入了新的实用程序“ grub2-setpassword ”

1) 执行 grub2-setpassword 命令

2）如果现在重新启动系统并尝试修改引导条目，系统将要求提供凭据，但是可以在没有凭据的情况下修改引导条目。为了阻止未经授权的修改和未经授权的启动，我们需要对 /boot/grub2/grub.cfg 文件进行更改

打开文件并使用密码搜索需要保护的启动条目，它以menuentry开头。找到条目后，从中删除 --unrestricted 参数

3) reboot 重启验证，只有当输入正确的用户名和密码时，才能进入 grub 菜单或者修改引导条目。