



阅读新闻

背景: □ □ □ □ □ □ □ □

Linux入门教程：磁盘加密LUKS

[日期: 2014-07-20]

来源: Linux社区 作者: linux_player_c

[字体: 大 中 小]

Linux系统中有很多的磁盘设备，通常我们希望对它们进行加密，这样会更加的安全。LUKS（linux统一密钥设置）是标准的设备加密格式。LUKS可以对分区或者卷进行加密。尤其要注意的是：必须首先对加密的卷进行解密，才能挂载其中的文件系统。

下面我们来举个例子看看什么是LUKS。

RHCE认证之RHEL6打印服务、ISCSI存储、磁盘加密LUKS和grub引导 <http://www.linuxidc.com/Linux/2013-11/92269.htm>

Linux下的磁盘加密LUKS <http://www.linuxidc.com/Linux/2013-04/82569.htm>

RHEL6下磁盘加密——LUKS <http://www.linuxidc.com/Linux/2013-01/77881.htm>

RHCE_RHEL6_135_U6.1_分区加密LUKS <http://www.linuxidc.com/Linux/2012-11/74165.htm>

Linux使用LUKS对分区加密 <http://www.linuxidc.com/Linux/2013-11/93285.htm>

1. 前期准备

支持LUKS的命令是cryptsetup（默认已经安装），如果我们想要看到它所支持的命令,键入命令：

```
[root@localhost Desktop]# cryptsetup --help
luksFormat <device> [<new key file>] - formats a LUKS device
luksOpen <device> <name> - open LUKS device as mapping <name>
luksAddKey <device> [<new key file>] - add key to LUKS device
luksRemoveKey <device> [<key file>] - removes supplied key or key file from LUKS device
luksKillSlot <device> <key slot> - wipes key with number <key slot> from LUKS device
luksUUID <device> - print UUID of LUKS device
isLuks <device> - tests <device> for LUKS partition header
luksClose <name> - remove LUKS mapping
luksDump <device> - dump LUKS partition information
luksSuspend <device> - Suspend LUKS device and wipe key (all IOs are frozen).
luksResume <device> - Resume suspended LUKS device.
luksHeaderBackup <device> - Backup LUKS device header and keyslots
luksHeaderRestore <device> - Restore LUKS device header and keyslots
```

为了做这个实验，我们重新生成一个设备，生成设备的步骤如下：

```
725 fdisk -cu /dev/vda
726 partx -d /dev/vda
727 partx -a /dev/vda
728 mkfs.ext4 /dev/vda7
```

2. 初识LUKS

cryptsetup其实是一种设备的映射关系，我们用它来把一个设备映射成另外一个设备，然后对这个新的设备进行操作，并进行加密，这样就不会使我们的原设备直接被使用，从而达到一种安全的效果。使用cryptsetup对分区进行了加密后，这个分区就不再允许直接挂载。LUKS也是一种基于device mapper 机制的加密方案。如果要使用这个分区，必须对这个分区做一个映射，映射到/dev/mapper这个目录里去，我们只能挂载这个映射才能使用。然而做映射的时候是需要输入解密密码的。具体的操作如下。

（1）首先对分区进行初始化

注意：这里要大写YES！ 然后输入该设备的密码

```
[root@zhangchi@localhost Desktop]# cryptsetup luksFormat /dev/vda7
WARNING!
This will overwrite data on /dev/vda7 irrevocably.
Are you sure? (Type uppercase yes): YES
Enter LUKS passphrase:
www.linuxidc.com
```

（2）映射分区，打开LUKS

最新资讯

Linux入门教程： /var/spool/clientmqueue 占满
升级到MySQL 5.7 解决分区问题
Python连接MySQL数据库
Python在自动化运维时经常会用到的方法
MySQL基准测试工具sysbench使用
MySQL教程：Linux下搭建MySQL Cluster
MySQL查询计划key_len全知道
使用Redis作为时间序列数据库：原因及方法
MySQL 5.7 完美的分布式事务支持
jQuery 3.0 的更新内容及使用方法

本周热门

Windows 7下硬盘安装Ubuntu 14.04图文教程
Windows 7下硬盘安装Ubuntu 14.10图文教程
VMware虚拟机下安装BackTrack5(BT5)+汉化教程
Android 手机上安装并运行 Ubuntu 12.04
Ubuntu 14.04 LTS下安装Google Chrome浏览器
安装完Ubuntu 14.04要做的九件事
U盘安装CentOS 7.0图文详解教程
U盘安装Ubuntu 14.10
Android SDK Manager国内无法更新的解决方案
Windows 7下使用Ext2Fsd读取写入Linux Ext3/

这个步骤是把原设备转换成/dev/mapper下的设备，赋予了它新的名字，这个过程需要输入刚才设置的密码。而且操作完以后我们可以看到/dev/mapper这个目录里边确实多了一个disk。

```
[root@zhangchi@localhost Desktop]# cryptsetup luksOpen /dev/vda7 disk
Enter passphrase for /dev/vda7:
[root@zhangchi@localhost Desktop]# ls /dev/mapper/
control disk
```

(3) 我们确实有了一个设备，但是记住这个设备是不能被直接使用的，必须要对它进行格式化。

```
[root@zhangchi@localhost Desktop]# mkfs.ext4 /dev/mapper/disk
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
Stride=0 blocks, Stripe width=0 blocks
12288 inodes, 49152 blocks
2457 blocks (5.00%) reserved for the super user
First data block=1
Maximum filesystem blocks=50331648
6 block groups
8192 blocks per group, 8192 fragments per group
2048 inodes per group
Superblock backups stored on blocks:
    8193, 24577, 40961

Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done

The filesystem will be automatically checked every 35 mounts or
180 days if whichever comes first. Use tune2fs -c or -i to override.
```

(4) 完成之后我们对disk进行挂载，挂载是成功的。

```
[root@zhangchi@localhost Desktop]# mount /dev/mapper/disk /tmp
[root@zhangchi@localhost Desktop]# df
Filesystem            1K-blocks      Used Available Use% Mounted on
/dev/vda2              7055288    3210060    3486828   48% /
tmpfs                  510292         224     510068    1% /dev/shm
/dev/vda1             297485      33492     248633   12% /boot
/dev/vda6             6192704    3776508    2101624   65% /mnt
/mnt/rhel-server-6.4-x86_64-dvd.iso
3632776      3632776         0 100% /iso
47595        4874      40264   11% /tmp
```

(5) 之前的实验我们似乎并没有看到LUKS安全到哪里了，只是把原来的设备变了一个名字使用，接着我们关闭映射，然后把原来的设备/dev/vda7挂载上去看看有什么提示：

```
[root@zhangchi@localhost Desktop]# mount /dev/vda7 /mnt
mount: unknown filesystem type 'crypto LUKS'
```

显然是挂不上的，因为我们已经把它映射到另外一个设备disk了，这样就极大加强了设备的安全性，接着开启luks：

```
[root@zhangchi@localhost Desktop]# cryptsetup luksOpen /dev/vda7 disk
Enter passphrase for /dev/vda7:
```

刚才我们已经挂载了映射设备disk，但是却是手动的，我们想要永久的挂载，那么就必须要写入配置文件/etc/fstab中了，但是我们的挂载在开机时是需要输入密码的，显然每次都让人去输入是不合乎常理的，所以也要新建一个文件来存入luks的开启密码，并且指定该文件为密钥文件。首先演示没有进行这些操作时的情况，开机时是要输入密码的，正确的话设备会被挂载，错误的话最多设备不会被挂载，系统依然能够启动：

```
Password for /dev/vda7 (luks-396...):*****
padlock: U1A PadLock not detected.
Intel AES-NI instructions are not detected.
EXT4-fs (vda2): mounted filesystem with ordered data mode. Opts:
dracut: Mounted root filesystem /dev/vda2
dracut: Loading SELinux policy
type=1404 audit(1398228292.888:2): enforcing=1 old_enforcing=0 auid=4294967295 ses=4294967295
type=1403 audit(1398228293.655:3): policy loaded auid=4294967295 ses=4294967295
dracut:
dracut: [root@localhost ~]#
dracut: # echo 'insinsect dog' > /etc/passwd
```

更多详情请继续阅读下一页的精彩内容：<http://www.linuxidc.com/Linux/2014-07/104441p2.htm>



图片资讯



Linux操作系统入门教



Linux入门教程: 如何



Linux操作系统入门教



如何对LUKS加密的磁盘



Linux入门教程: 如何



Linux下修复 "fatal"



Linux入门教程:



Linux入门教程: DNS服

本文评论

查看全部评论 (0)

表情: 姓名: ☐ 匿名 字数 0

☒ 同意评论声明

[请登录](#)

评论声明

- 尊重网上道德,遵守中华人民共和国的各项有关法律法规
- 承担一切因您的行为而直接或间接导致的民事或刑事法律责任
- 本站管理人员有权保留或删除其管辖留言中的任意内容
- 本站有权在网站内转载或引用您的评论
- 参与本评论即表明您已经阅读并接受上述条款

Linux公社简介 - 广告服务 - 网站地图 - 帮助信息 - 联系我们

本站 (LinuxIDC) 所刊载文章不代表同意其说法或描述, 仅为提供更多信息, 也不构成任何建议。
主编: 漏网的鱼 (QQ:3165270) 联系邮箱: root@Linuxidc.net (如有版权及广告合作请联系)

本站带宽由[\[MUU.CC\]](#)友情提供

关注Linux, 关注LinuxIDC.com, [请向您的QQ好友宣传LinuxIDC.com](#), 多谢支持!
Copyright © 2006-2015 Linux公社 All rights reserved 沪ICP备15008072号-1号