玩转UbuntuLinux之加密文件系统篇 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E7_8E_A9_E8_BD_ACUbun_c103_145189.htm 本文将详细介绍利用dm-crypt来创建加密文件系统的方法。与其它创建加密文件系统的方法相比，dm-crypt系统有着无可比拟的优越性：它的速度更快，易用性更强。除此之外，它的适用面也很广，能够运行在各种块设备上，即使这些设备使用了RAID和LVM也毫无障碍。dm-crypt系统之所以具有这些优点，主要得益于该技术是建立在2.6版本内核的device-mapper特性之上的。device-mapper是设计用来为在实际的块设备之上添加虚拟层提供一种通用灵活的方法，以方便开发人员实现镜像、快照、级联和加密等处理。此外，dm-crypt使用了内核密码应用编程接口实现了透明的加密，并且兼容cryptloop系统。一、配置内核 dm-crypt利用内核的密码应用编程接口来完成密码操作。一般说来，内核通常将各种加密程序以模块的形式加载。对于256-bit AES来说，其安全强度已经非常之高，即便用来保护绝密级的数据也足够了。因此本文中我们使用256-bit AES密码，为了保证您的内核已经加载AES密码模块，请利用下列命令进行检查：$ cat /proc/crypto如果看到类似下面的输出的话，说明AES模块已经加载： name : aesmodule : aestype : cipherblocksize : 16min keysize : 16max keysize : 32否则，我们可以利用modprobe来手工加载AES模块，命令如下所示：$ sudo modprobe aes接下来安装dmsetup软件包，该软件包含有配置device-mapper所需的工具： $ sudo apt-get install dmsetup cryptsetup为检查dmsetup软件包是否已经建立了设备

映象程序，键入下列命令：$ ls -l /dev/mapper/control接下来加载dm-crypt内核模块：$ sudo modprobe dm-cryptdm-crypt加载后，它会用evice-mapper自动注册。如果再次检验的话，device-mapper已能识别dm-crypt，并且把crypt 添加为可用的对象：$ sudo dmsetup targets如果一切顺利，现在你应该看到crypt的下列输出： crypt v1.1.0striped v1.0.2linear v1.0.1error v1.0.1这说明我们的系统已经为装载加密设备做好了准备。下面，我们先来建立一个加密设备。 