省时省力在Linux系统上进行自动备份（2） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E7_9C_81_E6_97_B6_E7_9C_81_E5_c103_144479.htm 使用公钥/私钥进行安全的远程访问 在数字安全的上下文中，密钥（key）指的是用来加密或解密其他数据片断的一个数据片断。公钥私钥模式的有趣之处在于，使用公钥加密的数据，只有用相应的私钥才可以解密。您可以自由地发布一个公钥，这样别人就可以对发送给您的消息进行加密。公钥/私钥模式彻底改变了数字安全的原因之一是，发送者和接收者不必再共享一个通用的密码。除了其他方面的贡献，公钥/私钥加密使用电子商务和其他安全传输成为可能。在本文中，我们将创建并使用公钥和私钥来创建一个非常安全的分布式备份解决方案。 要进行备份过程的每台机器都必须运行 OpenSSH 安全 shell 服务（sshd），同时让 22 端口可以通过任何内部防火墙被访问。如果您访问远程的服务器，那么很有可能您正在使用安全 shell。 我们的目标将是，不需要人工提供密码就可以安全地访问机器。一些人认为最简单的办法是设置无密码的访问：不要这样做。这样做不安全。不用那样，本文中我们将使用的方法可能会占用您大约一个小时的时间，建立起一个与使用“ 无密码 ”帐号同样方便的系统 不过它是公认非常安全的。 让我们首先确保 OpenSSH 已经安装，接下来查看它的版本号。完成本文时，最新的发行的 OpenSSH 是 2004 年 2 月 24 日发布的版本 3.8。您应该考虑使用一个较新的而且稳定的发布版本，至少所用的版本应该要比版本 2.x 新。访问 OpenSSH Security 网页以获得关于特定旧版本的缺陷的细节（

请参阅本文后面的 参考资料 中的链接）。到目前为止，OpenSSH 是非常稳定的，而且已经证明不存在其他 SSH 工具所报告的很多缺陷。 在 shell 提示符中，输入 ssh 并给出重要的 V 选项来检查版本号： $ ssh -V OpenSSH_3.5p1, SSH protocols 1.5/2.0, OpenSSL 0x0090701f 如果 ssh 返回的版本号大于 2.x，则机器处于相对良好的状态。无论如何，建议您所有的软件都使用最新的稳定版本，这对于安全相关的软件来说尤其重要。 我们的第一个步骤是，使用将会有特权访问服务器 1 和 2 的帐号登录到离线存储服务器机器（见图 1）。 $ ssh accountname@somedomain.com 登录到离线存储服务器以后，使用 ssh-keygen 程序并给出 -t dsa 选项来创建一个公钥/密钥对。 -t 选项是必须的，用来指定我们要生成的密钥类型。我们将使用数字签名算法（Digital Signature Algorithm，DSA），它让我们可以使用更新的 SSH2 协议。参阅 ssh-keygen 手册以获得更多细节。 在 ssh-keygen 执行的过程中，在询问您口令（passphrase）之前，将提示您输入 ssh 密钥存储的位置。当询问在何处存储密钥时只需要按下回车键，然后 ssh-keygen 程序将创建一个名为 .ssh 的隐藏目录（如果原来不存在），以及两个文件，一个公钥文件和一个私钥文件。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com