Linux上安装软件之前先验证软件包合法性Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文https://www.100test.com/kao_ti2020/555/2021_2022_Linux_E4_B8_8A_E5_AE_c103_555840.htm 以前有为Linux专家说过一句很经典的话“ 小即是美 ”。这句话一针见血的道出了Linux操作系统的设计特点。Linux操作系统跟微软操作系统不同，它都是一个个相对独立的软件所构成的一个操作系统，一个软件包完成一项单独的功能。为此Linux系统管理员平时大部分工具都在跟Linux系统软件包打交道。系统管理员要根据企业员工的需要，选择并安装恰当的软件包。故软件包直接跟Linux系统的安全与性能相关。为此为了创造一个稳定、安全的Linux操作系统环境，系统管理员最好在安装软件包之间先对软件包进行合法性验证。笔者下面就介绍几种常用的验证方法，来帮助大家识别Linux软件包的合法性。 一、检查软件包有否被篡改。 当系统工程师从网络上下载一个软件包之后，其最关心的就是这个软件包是否被篡改过。如一些非法攻击者会否在一些著名软件包中捆绑一些非法软件等等。为此系统工程师希望有工具能够帮助他来验证软件包是否被人处理过。如果为了达到这个目的，则系统工程师可以通过rpm k命令来进行验证。验证结果如图所示。为了安全起见，笔者已经把Linux服务器的主机名与账户隐去。 如果这个JDK的软件包没有被人修改过或者没有损坏，则结果就会如上图所示。Shal md5 OK这个简短的信息，就告诉系统工程师这个软件包没有被篡改过的迹象，可以放心使用。但是这个命令有一个缺陷，即只适用于rpm软件包。如果系统工程师所下载的软件包不是RPM格式的，则会提示如下的错误信息。 不过笔

者在这里也建议各位Linux系统管理员，最好通过RPM来管理软件。RPM软件包是一种开发的软件包管理系统，它简化了系统的维护工作，只需要短短的几个指令便可以完成安装软件包、删除软件包、系统验证等功能。RPM软件包有很多的特点。如通过使用RPM，系统管理员不用重新安装整个操作系统，就可以升级系统中的个别组件。RPM软件包会使用一种智能且完全自动化的方式来升级组件，而且软件包的设定文件将会在升级的过程中被保留下来。即如果对邮件客户端进行升级后，原先的帐户等设定将会被保留.如对办公软件进行升级，则原先的工具栏等用户偏爱设置也都将保留下来，用户不用在升级后进行重新设置，等等。这些措施可以大大的方便管理员的维护。如RPM可以验证软件包。如系统管理员在维护操作系统的时候，可能会担心不小心删除了某个软件包中的重要文件，则可以对这个软件包进行验证。如果这个软件包从安装到现在，相关的文件有任何改变都将被查询出来。为此系统管理员可以根据需要选择是否需要重新安装该软件包。可见RPM软件包的很多特性，都可以简化Linux系统工程师的工作。为此笔者在这里强烈建议大家通过RPM的方式来管理软件包。像上面验证软件包是否被篡改以及是否损坏也是RPM特有的功能之一。 二、检查GnuPG key信息。由于Linux软件是开源的，所以其上面的大部分软件包也是开源的。如笔者开发了一个软件包，则其他人可以在笔者软件包的基础上进行扩展与改进。但是有时候这个调整可能不是系统管理员所需要的。他们可能只需要原始版本即可。为此系统管理员希望能够在拿到软件包之后，能够该软件版本是否是原程序开发者所发布的版本。如果要实现这个目的，则

可以按如下的步骤来做。 首先这个软件包必须满足一个前提条件。即这个软件包的程序开发者对这个软件包“ 签署 ”了该程序开发者的GnuPG key。做一个形象的比喻，GnuPG key就好像是一个程序开发者的信物。大家看到这个信物之后，就可以判断这个就是程序开发者的原始作品。如果这个程序开发者在软件包中加入了这个 GnuPG key信物，那么系统工程师就可以利用rpm K命令来检查此软件包是否是原程序开发者所发布的版本。 其次先检查原帐户的信物。如果系统工程师此时得到了一个软件包，并且这个软件包中有签署GnuPG key。此时系统工程师就可以利用rpm K命令来检查这个软件包是否有问题，是否是原程序开发者所发布的。为了达到这个目的，系统工程师需要先查看原帐户的印章、签名甚至指纹等信息。通常情况下这些内容会被保存在/user/lib/rpm/gnupg目录中。系统工程师可以利用ls al命令来查看相关的GnuPG key信息。这个命令会列出系统中所有的GnuPG key信物信息。但是有时候系统管理员可能只想看一些特定的GnuPG key信物信息，则可以利用rpm qi GnuPG key名字的方式来进行查询。通常情况下，系统管理员可以先利用第一个命令查询处所有的GnuPG key信物信息。然后找到GnuPG key名字后，在利用第二个命令来查看这个信物的具体信息。另外如果信息比较多的话，则管理员可以通过rpm import命令把这些信息导出到系统管理员指定的位置。 第三步就是进行对比。当找到GnuPG key信物信息后，系统工程师就需要跟原先的便是数据来进行比较，以确定这个软件包是否是原程序开发者所发布的版本。此时系统工程师就可以利用rpm K加上软件包的命令来进行判断。注意这个功能也只适

用于RPM软件包。所以笔者在先前就强调，Linux系统工程师最好尽量采用rpm软件包。否则的话，以上这些内容将很难实现。 另外RPM软件包除了可以验证是否被篡改、是否是原版程序之外，还提供了强有力的查询选项。系统管理员可以利用数据库来查询软件包或者某些文件.还可以轻易的查询处一个文件所隶属的软件包，以及该软件包来自于何处。这主要是因为在RPM软件包中包含着特殊的二元标头数据。在这个二元标头数据中，有该软件包的信息以及相关文件，这使得系统可以更快、更容易的查询个别的软件包，节省Linux系统工程师的工作。如当系统工程师在安装后才发现这个软件有问题，需要判断这个软件包是否是原版程序。此时系统工程师就可以先通过某个文件来查询其隶属的软件包.然后再利用上面这个方法来查询这个软件包是否是原版的。甚至还可以查询处这个软件包的来源。 当系统工程师下载了原始版本的软件包之后，还可以方便的在此基础上进行改善与调整。因为RPM软件包有一个基本的设计原则，即保留该软件的原作者，发布出来的是纯净原软件程序代码。使用RPM，可拥有纯净的源代码以及曾经用过的任何程序进行修正，并加上完整的软件包建立提示。例如现在笔者从网上下载了一个新出来的软件，此时笔者并不需要从头开始对这个软件包进行编译。笔者可以先验证程序修正判断所需要做的事情。利用RPM工具可以很容易的了解编译的默认值以及这个软件所做过的变更。故当系统工程师不满意软件包的功能的话，则可以先下载一个原始版本的软件包(利用上面的方法来判断这个软件包是否是原始版本).然后再在此基础上进行一些调整与开发。开发调整过后，由于不需要从头开始编译，这就很大

程度上减轻了系统工程师开发的工作量，通过以上连个方法可以非常容易的判断出软件包是否被篡改、是否损坏以及是否是原版程序。这些信息往往是系统工程师微软软件包所必需要掌握的信息。不过比较遗憾的是，以上两种方法有一个前提条件，即必须使用的是RPM软件包。不过现在这个RPM软件包也是Linux系统上最流行的软件包。为了实现软件包验证的目的，以及出于其他的考虑，笔者建议大家还是采用RPM软件为好。 