Linux 运维趋势

2010 年 10 月 第一期

本期主题：监控与报警

关键字：远程监控，top，vmstat，ps，free，Nagios，Shell 脚本

内容目录

Thomas Limoncelli 谈交流对于系统管理员的价值

编译/杨赛

人物简介：

Thomas Limoncelli（托马斯·林蒙萨林）是运维界知名的系统管理员，作者与演讲者。他从 1987 年开始从事系统运维与网络工程师的工作，在全世界多个有关系统运维与网络安全的大会上进行演讲，著有《时间管理—给系统管理员》以及《系统管理与网络管理技术实践》等书籍，同时也是 Everything Sysadmin 的博主。目前，他在 Google 纽约总部工作，职位是 System Administrator。

Tom Limoncelli 是一位经验丰富的 SA。2000 年之前，Tom 一直在 AT&T 的贝尔实验室（后来的 Lucent 贝尔实验室）工作，从系统/网络管理员逐步升职为高级网络架构师；之后的几年间，他参与过创业团队，为佛蒙特州州长的竞选者担任过 IT 技术支持，也做过咨询顾问。而除了这些工作上的经历以外，Tom 在运维界的知名度更多的是来自他在很多线上/线下社区活跃。他在很多国际运维会议上做过演讲和课程，而最具代表性的莫过于每年年底召开的 LISA 会议。

LISA 会议全称 Large Installation System Administration，意为大规模服务器环境的系统管理，由 USENIX 和 SAGE 这两个组织协办。第一届 LISA 大会在 1986 年召开，之后每年召开，到现在每届约有来自全球上千名运维人员参会交流。Tom 从 1999 年开始受邀在 LISA 大会上发表演讲，之后几乎每年都会去 LISA 大会授课。

今年的第 24 届 LISA 会议将在 11 月召开，会议的主办方于前日对 Tom Limoncelli 进行了专访，对系统管理方面的一些日常话题，以及本次大会的演讲内容进行了谈论。在讨论当中，Tom 多次提及了各种形式的交流对自己的帮助，很有借鉴的价值。笔者在这里节选编译部分有意思的内容，与大家分享。

以下，TL 是 Tom Limoncelli 的简称；LISA 会议方的采访者是来自 Purdue 大学研究系统团队的系统研究工程师 Ben Cotton，简称 BC。

BC：你看，你在“有关系统管理的一切”方面都可称得上是个专业人员了。你认为你自己算是个通才呢，还是你觉得自己在某几个领域才是真正的专家？

TL：我认为自己是一个通才。应该说，正因为我从系统管理起步，所以注定了我是一个通才（译注：原文中的 generalist 是一个中性词，除了“通才”之外也可以当做“万精油”的意思）。这年头一切都不一样了。现在，人们往往专精于特定的领域：或者存储，或者备份，或者网络，更多情况是操作系统。大家都知道《系统管理与网络管理技术实践》这本书有三位作者吧：我们

这三个臭皮匠一起，才敢说我们知道“有关系统管理的一切”。或者应该这样说：我的特长就是无论遇到什么问题，总能找到能给我一个答案的人。

BC：那真是很赞。话说你每年都来 LISA 会议，是有什么吸引你的地方吗？

TL：LISA 对我来说就像是展望未来的一个望远镜。每年在大会上介绍的东西，都是大多数系统管理员们在未来 2-3 年内还接触不到的内容。这些内容让我有更好的“全局观”。比如，我第一次了解 CFEngine，了解 Puppet 以及其他“配置管理（CM）”工具，都是在 LISA 大会上。最近人们都在讨论 CM，好像这是什么新事物一样。但很多去过 LISA 会议的人都已经享用 CM 等工具长达十多年了。

有关系统管理的各个内容中，大约九成的有趣内容都是和伸缩性（scaling）有关。更多的机器，更多的内存，更多的存储，更快的速度，更多的点击量。很多年之前，有一个演示展示了每日百万次点击的网站是如何管理的，这在当时还是一个巨大的成就。当年观看过那个演示的系统管理员们在几年后尝到了甜头，因为所有的大型网站都逐渐达到了百万级的规模。

BC：大规模伸缩性的挑战在哪里？

TL：我们所知道的一切都将改变，这是因为 SSD 来了。我本人目前所有的知识都是建立在以下前提之上：CPU 缓存比 RAM 快 10 倍；RAM 比硬盘快 10 倍；硬盘比网络快 10 倍。过去这些年一直都是如此。虽然 RAM 变快了，但硬盘也快了。然而 SSD 来了，一切都面临改变。从 SSD 这几年的价格曲线，我们不难预测到，用不了多久，我们就将告别用磁盘存储数据的日子。古老的假设前提都将烟消云散。而同一时间，那些 16 核乃至 100 多核的 CPU 们将改写其他的前提条件。从某种角度而言，情况变得更糟了。这些都是在 LISA 大会上的热门话题。

BC：作为一个资深的参会者，你对新人有哪些建议？

TL：首先，多跟人交流。在会场的时候，向你身边的人进行自我介绍。非常多的学习机会都是来自与其他参会者的交流。Sysadmin 一般会比较内向，所以一开始你会感到有些困难。有人教过我这样一个展开对话的方式，无论在什么场合都适用：向对方伸手，同时说：“你好！我是 Joe”（如果你的名字叫做 Joe 的话）。有些会议会把演讲者关在小黑屋里，不让他们随便和参会者说话；但在 Usenix 组织的会议上，你可以跟任何人交谈。我在第一次参加 Usenix 会议的时候认识了 Dennis Ritchie，他是 Unix 的创始人之一。

剩下的就是好好计划你的日程安排。看好会议日程，确认好你想要去听哪些演讲，参加哪些课程。晚上一般会有社区举办的活动。总之，提前计划好，才能有最大的收获。

文章来源：

1. LISA '10 Interview: Tom Limoncelli
2. 译文

参考阅读：

1. Tom Limoncelli 的维基页面
2. Tom Limoncelli 的个人简历页
3. Everything Sysadmin
4. 部分有关 SA 时间管理的在线视频
5. LISA'10 大会官方网站
6. Google 的系统工程师如何工作

关于这个列表，最糟糕的事情是你可能已经几个月或几年没有做这些事情了。你忽略这些事情中的任何一件，它们都会在最糟糕的时候回来作祟：比如流量高峰期，硬盘驱动器崩溃，或黑客攻击的时候。

系统管理员应该定期完成的九件事

文/Drew Ford
译/周雪峰

今天，Linux 发行版非常容易安装和入门。就算是一个缺乏经验的系统管理员，建立必须的服务通常也可以在几小时内完成。

很不幸，容易入门反而掩盖了需要做的维护工作，这些工作是保持系统稳定和使系统长期处于一个良好的工作次序中所必需的。一个单一的服务器通常可以在没有人工干预的情况下运行很长时间，但前提是所有其他的位和块必需被提前配置。

关于这个列表，最糟糕的事情是你可能已经几个月或几年没有做这些事情了。你忽略这些事情中的任何一件，它们都会在最糟糕的时候回来作祟：比如流量高峰期，硬盘驱动器崩溃，或黑客攻击的时候。

配置管理

我用配置管理来开始，是因为它和这个列表中的其余项有很大的不同。这一项对单个服务器并不重要，但是如果你有许多系统，这一项就至关重要了。Puppet 或 Chef 这样的配置管理工具允许你编写‘recipes’来定义服务器应该如何的被放置在一起。那些‘recipes’可以在每个服务器上运行产生一个一致的、容易复制的安装程序。这可以让你立即启动一个系统的新拷贝，可以给你的安装提供极大的自由度。

配置管理是做了，但是，却给服务器安装程序添加了一定的初始化复杂性，所以如果你胆子小，不用也罢。不过，即使只有两个或三个服务器，好处也是相当巨大的。

备份

大多数系统管理员都会在这方面做点工作的。如果你没有一个可靠的备份策略，你现在需要马上调整它。哪怕只等一天，后果很可能就是是灾难性的。请确保你正确的做了备份，因为备份很容易做错。Mozy，Carbonite，Backblaze 等工具的 At-home 备份已经取得了很大的进展，但是类似的 Linux 解决方案还远没有成熟。Rsync，tar 和类似的脚本工具一直很受欢迎，并且也是可行的替代方案，但是必须要小心，以适应像 MySQL 数据库那样的特殊情况。

测试你的备份

紧跟着备份计划的是测试它。这意味着定期检查备份是否一直在做，产生的文件是否是有效的并且是否没有被损坏，以及他们是否包括你需要的所有数据。一个好的经验法则是如果你的备份每 30 天一轮换，那么你应该经常的重新检查他们。这里自动化工具可以帮一些忙（自动地检查备份文件是否是最新的，是否是合理的大小并且是否有效）。尽管如此，没有任何东西可以替代人的眼睛……否则，当你发现你并没有备份那些你认为你已经备份的数据时，就只有哭的份了。

日志轮换

在最近几年，Ubuntu，RedHat 和其他主要的发行版针对他们提供的软件包的 logrotate 的运行和配置有了很大的改善。所以你的 apache 和 mysql 日志也可以被合适的轮换（默认设置是相当合理的，虽然可能并不是你希望的方式）。但是你添加的“额外”的东西，例如 Rails 应用程序，需要建立它自己的 logrotate 条目。缺少这个步骤会在最不合适的时刻引发无数的“硬盘驱动器已满”的服务器错误。当然，通常你甚至不知道你的日志引发了这个问题。针对这种情况，资源监视才是关键。

资源监视

跟踪 CPU，内存的使用情况，硬盘空间，带宽，等可以让你更好的洞察你的系统状态。当流量增加的时候，你可以比较你的增加的内存或 IO 使用情况，来提前规划你的 scaling。RRDTool / Munin，ServerDensity 和 Cloudkick 是观察这些随着时间的推移而变化的数据的很好的选择。如果你选择的工具包括对意外的变化（失控的进程，驱动器已满等）的警报功能，你将会领先任何潜在的问题一步。

进程监视

对你的网站来说，让你的 Apache，MySQL 和类似的进程一直处于运行状态至关重要。有几个很好的工具，例如 Monit 和 God，可以帮助你确保你的进程一直处于运行状态。通过检查进程的响应性，打开的端口，或进程 id 那些工具可以重新启动一个已死的服务或在一个失控的进程使你的整个系统崩溃前终止它。配置这件事的规则是个老大难问题，但是当一切都做好的时候，可以节省大量的凌晨 3 点钟的宕机时间。

安全加固（Hardening）

Hardening 包含了许多不同的操作，这些操作可以使你的 stock 系统更安全。许多简单的操作经常会被遗漏。你真的知道那些正在运行的进程中的每一个都做了什么吗？在你的系统上，哪些额外的端口和服务被打开了？有合适的 PAM 模块载入来进行安全认证吗？又一次，RedHat 和 Ubuntu 走在了时代的前列，他们提供了安全 stock 系统，并确保最常见的软件包遵守正确的安全协议。但是，这并不意味着你可以跳过这个步骤。

安全更新

在一个基于 apt 或 RPM 的系统上，安全更新是很容易执行的。为了确切知道升级包将对你的系统产生怎样的影响，拥有一台同样配置的模拟服务器是唯一的好办法。幸运的是，由安全更新引发的麻烦是十分罕见的。最后，不是每一个安全漏洞都能马上获得一个安装补丁。查看 CVE 字典上的可用警报，可以让你在补丁可用前，在保持你的系统安全性方面争取主动。

日志监视/安全扫描/入侵检测

这个列表中的所有项都是最低限度需要完成的它们很容易被忘记，直到你的系统已经被入侵为止，你可能都不会想起它们。对异常活动，黑客攻击和其他恶意行为的持续扫描，对于帮助阻止或减轻攻击来说，是十分重要的。

文章来源：

1. 9 Things You Should Be Doing With Your Server, But Probably Aren't
2. 译文

相关阅读：

1. 系统管理员不可不知的三条黄金法则

2010 年 9-10 月之间，发生了下面这些事……

八卦，趣闻与数字 2010.09 – 2010.10

收集整理/51CTO 系统频道

【Ubuntu 10.10】相对于 10.04，新版的 Ubuntu 10.10 桌面版更注重家庭及手机用户，并且在很多细节方面做了改变，比如新的主题，新的 Sound Menu 样式，软件中心作了大量改进，新的安装界面 ，新的 Ubuntu 字体，改进过的云服务 Ubuntu One ，由软件中心接管 deb 包安装过程等等。

http://os.51cto.com/art/201010/229278.htm

【Gnome 3.0】Gnome 团队于 9 月 29 日发布了 Gnome 2.32，这也意味着 Gnome 3.0 已经越来越近了。

http://os.51cto.com/art/201009/228757.htm

【OS 厂商们】Solaris 现在是市值 1400 亿美金的 Oracle 公司的一部分，同时，SLES（可能将）是市值 360 亿美金的 VMware 公司的一部分。至于 Windows，AIX 和 HP-UX，他们分别归属于市值 2200 亿美金的微软公司，市值 1660 亿美金的 IBM 公司，和市值 900 亿美金的惠普公司。相对而言，Red Hat 是比较弱小的一个，市值只有 70 亿美金。

http://os.51cto.com/art/201010/229117.htm

【Canonical】Ubuntu 团队大约有 120 人，但只有不到 5 个人长期呆在办事处工作。

http://os.51cto.com/art/201009/225966.htm

【Novell 用户】假设你是一位 Novell 用户，你现在正在使用 SUSE Linux, NetWare, Identity Manager 和 PlateSpin 产品；再假设 Oracle 从私人股本公司那里二次购得了身份和安全管理产品，CA 获得了系统和资源管理产品，而某家战略投资公司获得了 SUSE Linux Enterprise 产品家族……到那时，你不得不和三家公司续签合同，以保障能够继续使用 Novell 的产品。

http://os.51cto.com/art/201010/228977.htm

【HPC】2010 年全球高性能计算机 TOP500 排行榜在今年 6 月份公布了，今年的三甲分别是 Jaguar、曙光星云和 Roadrunner。今年让国人特别激动的是曙光的“星云”挤入第二名。可以注意到的是，这前三款超级计算机使用的都是 Linux 操作系统。

http://os.51cto.com/art/201009/228379.htm

【Linux 社区】我们 Linux 基金会去年最关注的两大主题是驱动和应用，目前来看，驱动的问题基本都已经解决了，而包括中国在内的 Linux 社区开发人员的缺乏，依然是全球 Linux 产业所面临的最主要问题。

http://os.51cto.com/art/201009/227288.htm

【虚拟机】对于那些只是想体验一下其它操作系统的初级用户，VirtualBox 无疑是最好的选择。对于那些已经熟悉虚拟化的高级用户，并且属于命令控一类的人，KVM 可能是他们的最爱。VMPlayer 对于那些制作虚拟用具的人来说，可能更有吸引力。

http://os.51cto.com/art/201009/226667.htm

【开源与安全】开源形式木马的历史可以追溯到 1999 年，当时死牛教派黑客集团发布了 Back Orifice 木马的源代码。最近，Limbo 木马的开发者也公布了其源代码，以提升骗子们的使用频率，扭转占有率下降的颓势。

http://os.51cto.com/art/201009/226488.htm

本期专题：Linux 系统监控与报警

图中文字：伊萨克·牛顿的曾曾曾曾曾曾曾曾曾孙

系统管理员解读版：牛顿发现万有引力，得益于他在无意中对苹果的运动状态进行了监控。

系统管理员解读版 2：苹果砸到头上是一种报警，提醒你不要被一台 Apple 砸到头！

图片来源：offthemarkcartoons.com

作者：Mark Parisi

使用 SecureCRT,F-Secure SSH 或是 PuTTY 等客户端工具通过 ssh 服务来实现 Windows 下管理 Linux 服务器，虽然几乎不需要什么配置，使用简单，但是它们都无法启动窗口服务的程序或进程，也无法达到远程桌面控制。

Linux 服务器远程监控与管理基础

文/李洋

Linux 系统工程师一般都是远程管理服务器，而不是天天在机房里面实地操作。远程监控与管理的好处就是随时随地管理，而且不用管理者到公司去解决问题。一方面节省了管理者的精力，另一方面也让问题在第一时间解决，避免因为路途的原因耽误企业业务开展。一般来说对于企业内部的网络故障，网络问题，应用软件问题以及一些不太严重的系统问题都可以通过远程管理来解决。也就是说凡是软件和网络的问题都可以借助远程工具来管理。

下面介绍 Linux 服务器远程监控与管理的一些基本操作方式。

SSH 远程监控及管理

SSH 的英文全称是 Secure SHell。通过使用 SSH，用户可以把所有传输的数据进行加密，这样“中间人”这种攻击方式就不可能实现了，而且也能够防止 DNS 和 IP 欺骗。还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 Telnet，又可以为 FTP、POP、甚至 PPP 提供一个安全的“通道”。

SSH 协议是建立在应用层和传输层基础上的安全协议，其主要由以下三部分组成，共同实现 SSH 的安全保密机制：

- 传输层协议。该协议提供诸如认证、信任和完整性检验等安全措施，此外还可以任意地提供数据压缩功能。通常情况下，这些传输层协议都建立在面向连接的 TCP 数据流之上。
- 用户认证协议层。用来实现服务器的跟客户端用户之间的身份认证，其运行在传输层协议之上。
- 连接协议层。分配多个加密通道至一些逻辑通道上，它运行在用户认证层协议之上。

SSH 是由客户端和服务端的软件组成的，有两个不兼容的版本分别是：1.x 和 2.x。用 SSH 2.x 的客户程序是不能连接到 SSH 1.x 的服务程序上去的。OpenSSH 2.x 同时支持 SSH 1.x 和 2.x。

在 Linux 的主流发行版本中都已经包含了与 OpenSSH 相关的软件包，目前的最新版本为 OpenSSH 5.6。

首先查询系统是否安装了上述软件包

```
#rpm -qa |grep openssh
```

如果没有安装，则需要从 OpenSSH 官网下载 rpm 包并手动安装。下载之后通过 rpm -ivh 命令安装相应的 rpm 包。

安装完成了之后，可以使用下述命令进行启动：

```
#service sshd start
```

或者命令：

```
#/etc/rc.d/initd/sshd start
```

SSH 提供了一些命令和 shell 用来登录远程服务器，在默认情况下其并不允许用户拷贝文件。但为了方便用户使用，它还是提供了一个“scp”命令，用户可以使用该命令来进行文件的远程拷贝工作。

在 Linux 客户端下使用 SSH，优点是操作更方便，无需其他软件；缺点是不太直观。下面主要介绍配置使用 Windows 环境下的 putty 工具来登录 SSH 服务器。

PuTTY 安装完毕之后，进行如下配置：

（1）打开该软件，进入配置界面。软件初始自动打开 Session 窗口。

（2）在该界面的右半区域的【Host Name（or IP address）】编辑框中输入所要远程登录的服务器地址。这里设定为：192.168.10.1，端口编辑框中输入默认的端口号 22，然后单击【Save】按钮保存输入配置。

（3）单击【Open】按钮，该软件连接服务器，显示连接结果，用户就可以进行相应的远程管理操作了。

Xmanager 进行桌面远程监控及管理

使用 SecureCRT,F-Secure SSH 或是 PuTTY 等客户端工具通过 ssh 服务来实现 Windows 下管理 Linux 服务器，虽然几乎不需要什么配置，使用简单，但是它们都无法启动窗口服务的程序或进程，也无法达到远程桌面控制。下面将介绍通过 xmanager 远程桌面控制 Linux 的方法和技巧。

X 是用在大多数 UNIX 系统中的图形支持系统。如果你在你的 Linux 机器上使用 GNOME 或者 KDE 的话，你就正在使用 X 系统。它由 X 联盟(www.X.org)定义并维护。大多数的 Linux 用户使用的都是由 XFree86 项目 (www.xfree86.org) 提供的 X Window 系统的实现。xdm 是一个显示管理器，提供了灵活的任务管理功能。然而 xdm 通常被认为是“GUI 的登陆屏幕，可以自动启动我的 X 任务”，我们会看到实际上它要更为强大。

xdm 使用 X 联盟的 X 显示管理控制协议，即 XDMCP，来和 X 服务器通信。它允许 X 服务器从运行 xdm 服务的服务器上获得会话服务。当使用 xdm 管理这些 X 任务的时候在设置上有些复杂。但设置 xdm 可以得到本地的和其他服务器上的桌面了。

本文来源：

- 做好远程监控与管理

相关链接：

1. OpenSSH 下载地址
2. PuTTY 下载地址

相关阅读：

1. Linux 系统管理员都应该熟悉的工具
2. 远程服务器管理技巧大全
3. 运维人员应该掌握哪些常用技术
4. Linux 系统全方位管理

本文介绍找出这些性能问题原因的工具。当然，这份列表只是所有监控工具当中很小的一部分。

管理员必备的 Linux 系统监控工具

文/VIVEK GITE
译/飞哥也是哥

需要监控 Linux 服务器系统性能吗？尝试下面这些系统内置或附件的工具吧。大多数 Linux 发行版本都装备了大量的监控工具，这些工具提供了能用作取得相关信息和系统活动的量度指标。你能使用这些工具发现造成性能问题可能原因，这些原因包括：

1. 找出瓶颈
2. 硬盘（存储）瓶颈
3. CPU 及内存瓶颈
4. 网络瓶颈

下面开始介绍找出这些原因的工具。当然，这份列表只是所有监控工具当中很小的一部分。

#1: top - 进程活动

top 提供一个当前运行系统实时动态的视图，也就是正在运行进程。在默认情况下，显示系统中 CPU 使用率最高的任务，并每 5 秒钟刷新一次。

#2: vmstat -系统活动、硬件及系统信息

使用 vmstat 命令可以得到关于进程、内存、内存分页、堵塞 IO、traps 及 CPU 活动的信息。

#3: w - 显示谁已登录，他们正在做什么？

w 命令显示系统当前用户及其运行进程的信息。

#4：uptime - 告诉系统已经运行了多久？

uptime 命令过去只显示系统运行多久。现在，可以显示系统运行多久、当前有多少的用户登录、在过去的 1，5，15 分钟里平均负载时多少。

#5：ps - 显示进程

ps 命令显示当前运行进程的快照。使用-A 或-e 显示所有进程。ps 与 top 非常相似，但 ps 提供更多的信息。

#6: free - 内存使用情况

free 命令显示系统中空闲的、已用的物理内存及 swap 内存,及被内核使用的 buffer。

#7: iostat - CPU 平均负载，硬盘活动

iostat 命令可报告中央处理器（CPU）的统计信息，各种设备、分区及网络文件系统输入/输出的统计信息。

#8: sar - 搜集和报告系统活动

sar 命令用来搜集、报告和储存系统活动信息。

#9:mpstat - 多处理器使用率

mpstat 命令可以显示所有可用处理器的使用情况，处理器编号从 0 开始。mpstat -P ALL 显示每个处理器的平均使用率。

#10: pmap - 进程的内存使用

pmap 命令可以显示进程的内存映射，使用这个命令可以找出造成内存瓶颈的原因。

#11：netstat - 网络相关信息

netstat 可以显示网络链接、路由表信息、接口统计信息、伪装链接和多播成员(multicast memberships)

#12：ss - 网络相关信息

ss 命令用来显示网络套接字信息，它允许显示类似 netstat 一样的信息。

#13: iptraf - 网络实时信息

iptraf 是一个可交互式的 IP 网络监控工具。它可以生成多种网络统计信息包括：TCP 信息、UDP 数量、ICMP 和 OSPF 信息、以太网负载信息、节点状态、IP 校验错误等。

#14：tcpdump：详细的网络流量分析

tcpdump 是一个简单网络流量转储工具，然而要使用好需要对 TCP/IP 协议非常熟悉。

#15:strace - 系统调用

追踪系统调用和型号，这对于调试 Web 服务器和其他服务器非常有用。了解怎样追踪进程和他功能。

#16：/proc 文件系统 - 各种内核信息

/proc 目录下文件提供了很多不同硬件设备和内核的详细信息。

#17:Nagios - 服务器及网络监控

Nagios 是一款非常流行的系统及网络监控软件。你可以轻松监控所有的主机、网络设备及服务。它能在发生故障和重新恢复后发送警讯。

#18:Cacti - 基于 Web 的监控工具

Cacti 是一套完成的网络图形化解决方案，基于 RRDTool 的资料存储和图形化功能。Cacti 提供一个快速的轮询器、进阶的图形化模板、多种数据采集方法和用户管理功能。这些功能都拥有非常友好易用的界面，确保可以部署在一个包含数百台设备的复杂网络中。它提供关于网络、CPU、内存、已登录用户、Apache、DNS 等信息。

#19:KDE System Guard

KSysguard 是在 KDE 桌面下一个网络化的系统监控工具。这个工具可以通过 SSH 会话运行。它提供很多功能，例如可以监控本机和远程主机的客户端/服务器架构，前端图形界面使用所谓传感器得到信息并展现出来。传感器返回的可以是一个简单的数值或是一组表格的信息。针对不同的信息类型，提供一个或多个显示。这些显示被组织多个工作表中，可以工作表可以独体储存和加载。所以，KSysguard 不只是一个简单的任务管理器，还是一个可以控制多台服务器的强大工具。

#20:Gnome System Monitor

System Monitor 可以显示系统基本信息、监控系统进程、系统资源及文件系统使用率。你也可以使用 System Monitor 监控和修改系统行为。尽管没有 KDE System Guard 功能强大，但其提供的基本信息对于入门用户还是非常有用的。

本文来源：

1. 20 Linux System Monitoring Tools
2. 译文

推荐阅读：

1. Linux 监控工具的展览馆
2. 十三个强大的 Linux 监控工具
3. 七大命令行工具玩转 Linux 网络配置

top -hv | -bcisS -d delay -n iterations -p pid [, pid ...]

资料篇：Linux 常用监控命令简介 - top

top 作为日常管理工作中最常用也是最重要的 Linux 系统监控工具之一，可以动态观察系统进程状况。top 命令显示的项目很多，默认值是每 5 秒更新一次，按 q 键可以退出。显示的各项目为：

指令介绍

-b : 批次模式运行。

-c : 显示执行任务的命令行。

-d : 设定延迟时间

-h : 帮助

-H : 显示线程。将显示所有进程产生的线程。

-i : 显示空闲的进程。

-n : 执行次数。一般与-b 搭配使用

-u : 监控指定用户相关进程

-U : 监控指定用户相关进程

-p : 监控指定的进程。

-s : 安全模式操作

-S : 累计时间模式

-v : 显示 top 版本，然后退出。

-M : 自动显示内存单位（k/M/G）

输出数值解读

```
15:06:57  up 129 days, 19:03,  5 users,  load average: 1.21, 1.20, 1.25
```

uptime 该项显示的是系统启动时间、已经运行的时间和三个平均负载值（最近 1 秒，5 秒，15 秒的负载值）。

```
222 processes: 219 sleeping, 2 running, 1 zombie, 0 stopped
```

processes 自最近一次刷新以来的运行进程总数。这些进程被分为正在运行的，休眠的，停止的。

```
CPU states:  cpu    user    nice  system    irq  softirq  iowait    idle
      total    0.9%    0.0%   27.4%   0.0%     0.0%    0.2%   71.2%
      cpu00    1.9%    0.0%   19.4%   0.0%     0.0%    0.0%   78.6%
      cpu01    0.0%    0.0%   33.0%   0.0%     0.0%    0.0%   66.9%
      cpu02    1.9%    0.0%   22.3%   0.0%     0.0%    0.9%   74.7%
      cpu03    0.0%    0.0%   35.2%   0.0%     0.0%    0.0%   64.7%
```

CPU states 显示用户模式，系统模式，优先级进程（只有优先级为负的列入考虑）和闲置等各种情况所占用 CPU 时间的百分比。优先级进程所消耗的时间也被列入到用户和系统的时间中，所以总的百分比将大于 100%。

```
Mem:  16214336k av, 15682832k used, 531504k free, 0k shrd, 215016k buff
                    10896844k actv, 3379680k in_d, 446432k in_c
```

Mem 内存使用情况统计，其中包括总的可用内存，空闲内存，已用内存，共享内存和缓存所占内存的情况。

```
Swap: 10482404k av,  0k used, 10482404k free                14856500k cached
```

Swap 交换空间统计，其中包括总的交换空间，可用交换空间，已用交换空间。

```
PID USER      PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM    TIME CPU COMMAND
27869 root    25   0  460M 460M  455M R    25.0  2.9 12559m   1 vmware-vmx
31819 root    16   0  6016 6016  5048 S     1.6  0.0 17573m   2 magicdev
27837 root    15 -10  460M 460M  455M S <   0.7  2.9  1328m   0 vmware-vmx
27868 root    15 -10  460M 460M  455M S <   0.3  2.9 644:35   3 vmware-vmx
```

PID 每个进程的 ID。PPID 每个进程的父进程 ID。UID 每个进程所有者的 UID 。

USER 每个进程所有者的用户名。

PRI 每个进程的优先级别。

NI 该进程的优先级值。

SIZE 该进程的代码大小加上数据大小再加上堆栈空间大小的总数。单位是 KB。

TSIZE 该进程的代码大小。对于内核进程这是一个很奇怪的值。

DSIZE 数据和堆栈的大小。

TRS 文本驻留大小。

D 被标记为“不干净”的页项目。

LIB 使用的库页的大小。对于 ELF 进程没有作用。

RES 该进程占用的物理内存的总数量，单位是 KB。

SHARE 该进程使用共享内存的数量。

STAT 该进程的状态。S=休眠；D=不可中断的休眠；R=运行；Z=僵死；T=停止或跟踪。

TIME 该进程自启动以来所占用的总 CPU 时间。如果进入的是累计模式，那么该时间还包括这个进程子进程所占用的时间。且标题会变成 CTIME。

%CPU 该进程自最近一次刷新以来所占用的 CPU 时间和总时间的百分比。

%MEM 该进程占用的物理内存占总内存的百分比。

COMMAND 该进程的命令名称，如果一行显示不下，则会进行截取。内存中的进程会有一个完整的命令行。

top 命令详解全文地址

小阅读：机房该监控些什么

有效的监控解决方案对于维护数据中心网络是至关重要的，无论管理人员是否在数据中心里面工作，他们都必须设置有效的报警装置。你无法假设某人走进数据中心去注意控制屏上显示的故障提示。没有到位的网络管理和监控解决方案，你可能只有到电话响起才知道发生了问题。

你必须监控什么？下面是一个简单的参考列表：

一、配电监测系统

二、UPS 设备

三、空调系统

四、环境温湿度系统

五、消防系统接口

六、泄漏监测系统

七、门禁管理

全文：

- 你了解机房该监控些什么吗？

资料篇：Linux 常用监控命令简介 – vmstat，ps 等

vmstat [-a] [-n] [delay [count]]

vmstat [-f] [-s] [-m]

vmstat [-S unit]

vmstat [-d]

vmstat [-p disk partition]

vmstat [-V]

指令介绍

-a：显示活跃和非活跃内存

-f：显示从系统启动至今的 fork 数量 。

-m：显示 slabinfo

-n：只在开始时显示一次各字段名称。

-s：显示内存相关统计信息及多种系统活动数。

delay：刷新时间间隔。如果不指定，只显示一条结果。

count：刷新次数。如果不指定刷新次数，但指定了刷新时间间隔，这时刷新次数为无穷。

-d：显示磁盘相关统计信息。

-p：显示指定磁盘分区统计信息

-S：使用指定单位显示。参数有 k，K, m, M, 分别代表 1000, 1024, 1000000, 1048576 字节。默认单位为 K（1024 bytes）

-V：显示 vmstat 版本信息。

方便用法推荐

每 2 秒输出一条结果

```
vmstat 2
```

显示活跃和非活跃内存

```
vmstat -a 2
```

输出数值解读

(Procs)r: 运行队列中进程数量

(Procs)b: 等待 IO 的进程数量

(Memory)swpd: 使用虚拟内存大小

(Memory)free: 可用内存大小

(Memory)buff: 用作缓冲的内存大小

(Memory)cache: 用作缓存的内存大小

(Swap)si: 每秒从交换区写到内存的大小

(Swap)so: 每秒写入交换区的内存大小

(IO)bi: 每秒读取的块数

(IO)bo: 每秒写入的块数

(System)in: 每秒中断数，包括时钟中断。

(System)cs: 每秒上下文切换数。

(CPU)us: 用户进程执行时间(user time)

(CPU)sy: 系统进程执行时间(system time)

(CPU)id: 空闲时间(包括 IO 等待时间)

(CPU)wa: 等待 IO 时间

vmstat 命令详解全文地址

ps 命令

```
ps [options]
```

指令介绍

-e 显示所有进程。

-f 全格式。

-h 不显示标题。

-l 长格式。

-w 宽输出。

a 显示终端上的所有进程，包括其他用户的

r 只显示正在运行的进程。

x 显示没有控制终端的进程。

方便用法推荐

查看使用 Vivek 用户名运行的进程

```
# ps -U vivek -u vivek u
```

只显示 Lighttpd 的进程 ID

```
# ps -C lighttpd -o pid=
```

找出消耗内存最多的前 10 名进程

```
# ps -auxf | sort -nr -k 4 | head -10
```

找出使用 CPU 最多的前 10 名进程

```
# ps -auxf | sort -nr -k 3 | head -10
```

ps 命令详解全文地址

free 命令

```
free [-b|-k|-m][-o][-s delay][-t][-V]
```

指令介绍

-b 以 Byte 为单位显示内存使用情况。

-k 以 KB 为单位显示内存使用情况。

-m 以 MB 为单位显示内存使用情况。

-o 不显示缓冲区调节列。

-s<间隔秒数> 持续观察内存使用状况。

-t 显示内存总和列。

-V 显示版本信息。

输出数值解读

```
total used free shared buffers cached
Mem: 3266180 3250004 16176 0 110652
 2668236
-/+ buffers/cache: 471116 2795064
Swap: 2048276 80160 1968116
```

total:总计物理内存的大小。

used:已使用多大。

free:可用有多少。

Shared:多个进程共享的内存总额。

Buffers/cached:磁盘缓存的大小。

used:已使用多大。

free:可用有多少。

free 命令详解全文地址

uptime 命令

```
uptime
uptime [-V]
```

输出数值解读

```
18:02:41 up 41 days, 23:42,  1 user,
 load average: 0.00, 0.00, 0.00
```

10:19:04：系统当前时间

up 257 days，18:56：主机已运行时间,时间越大，说明你的机器越稳定。

12 user：用户连接数，是总连接数而不是用户数

load average：系统平均负载，统计最近 1，5，15 分钟的系统平均负载

如果每个 CPU 内核的当前活动进程数不大于 3 的话，那么系统的性能是良好的。如果每个 CPU 内核的任务数大于 5，那么这台机器的性能有严重问题。

uptime 命令详解全文地址

监控工具可能会把用户淹没在数据的海洋中。在这些数据中，有些是有用的，有些可能并没有什么用。

服务器监控百家谈：趋势分析是关键

文/Sixto Ortiz Jr.
译/周雪峰

为了对设备做出某些调整，解决某些当前的问题，或者为了划分出修复和更新换代在预算方面的优先级，管理员们必须要对他们的设备的运行的情况进行评估。因为数据中心的设备主要由服务器组成，所以，不言而喻，对于那些需要随时关注数据中心的资产的管理员们来说，服务器监控是一个关键性的领域。

但是，监控并不只是捕获几个参数数据和当警告发生的时候做出响应那么简单。管理员们必须要确保服务器监控是有效的，并且可以提供相关的，有用的信息。这项工作的关键是尽量缓解一些可能会出现的问题，这些问题可能会干扰服务器的监控的顺利进行。

使用趋势

和服务器的监控相关的一个问题是，许多工具都提供了大量的数据，但是并没有提供太多的可用信息。没有可用的信息，管理员们不可不浪费大量的宝贵时间从一堆“杂乱无章的数据”中分离出和自己相关的一些信息。

Zenoss 社区部门副总裁 Mark Hinkle

“解决这个服务器监控的问题的关键是趋势。只通过服务器的监控工具来处理‘故障-修复’情况的管理员们，并不须要影响最终用户。监控磁盘的使用情况可以在故障发生以前看出容量存在问题。例如，一些监控解决方案提供了趋势分析的工具，你可以通过一些使用模式来预测出哪个存储容量的上限即将到达。”

LogicMonitor 创始人兼 CEO Steve Francis

“许多系统都只依靠‘基于阀值’的监控，几乎没有提供任何趋势分析的功能。被监控的每一件事情都应该被趋势化。实际上，为了提供一些帮助解决问题的信息，许多事情都应该被趋势化，而不是发出警告。如果应用程序执行的比较慢，然后触发了一个监控警告，通过这个监控警告，管理员们应该可以判断这个新版本是否导致了应用程序性能的突然降低，或者这个应用程序是否随着负载的增加而逐渐变慢。”

选择合适的监控指标/工具

管理员们和数据中心的工作人员都很清楚这样一个事实：监控工具可能会把用户淹没在数据的海洋中。在这些数据中，有些是有用的，有些可能并没有什么用。要解决这个问题，不仅仅需要趋势，还需要选择合适的监控指标。

Logicalis 公司外包业务主管 Mike Alley

“对于高效率的生产服务器管理来说，主要需要关注的事情是如何确保监控工具只报告关键性的指标，这些指标可以提供和服务器的健康程度关系最密切的一些信息。大多数的工具都会产生很多的无关事件，这会把监视控制台淹没在事件

的海洋里，这导致的直接后果是：用户很难对关键性的事件引起注意。”

“你可以从和 CPU，内存，网络和存储相关的一些性能指标开始监控，它们都是很不错的出发点。管理员们还应该监控和服务器，系统日志，系统进程相关的硬件级的管理产品探测到的一些事件。管理员们应该定期检查监控工具报告的事件，然后筛选出那些事件会对用户造成影响，哪些事件是不需要理睬的。当然，那些会对用户造成影响，但是并没有被监控工具探测到的事件也应该检查，虽然监控工具并没有探测到这个事件，但是和这个事件相关的特定的指标应该已经被监视到了。”

Uptime Software 架构师 Kenneth Cheung

“各种工具都会对很多指标进行监控，这很正常。关键是要找到这样一个监控解决方案，它可以快速地把故障和事故与相关的设备和应用程序对应起来。监控工具应该指出哪些问题需要优先处理，哪些设备设备需要优先关注。有了这样的功能，管理员们可以立即判断出哪个问题需要立刻引起注意。”

自动化

如果一个监控工具不通过自动化的方式来简化警告的处理流程，而只能通过人工的方式来处理，这会浪费很多的时间，而且还可能会由于一个故障处理的不及时让情况变得更糟。

Zenoss 社区部门副总裁 Mark Hinkle

“当一个故障发生的时候，发送一个页面或其他的警告通常会引发一系列的事件：一个管理员收到了一个页面，登陆到服务器，然后再诊断这个问题。这个过程可能会花费几分钟的时间或者更长的时间。在大多数情况下，监控工具可以启动一个进程，自动地修复这个问题。”

“例如：一个监控工具可以探测到一个服务器故障，然后使用一个自动化的工具来重新启动那个服务器，这样修复这个故障的时间会缩短很多。”

LogicMonitor 创始人兼 CEO Steve Francis

“如果你的监控系统不能自动地探测到服务器应用程序和设备的改变，那么你相当于没有做监控。原因是，在危急关头，通常会对服务器和系统会做出很多的改变，如果管理员们依靠人工的方式来处理，那么可能会遗漏掉一些关键性的变更。”

把监控和最终用户联系起来

服务器监控的最终目标是要确保关键性的业务应用程序持续正常地运行。这意味着服务器监控和最终用户的体验有很大的关系。

Uptime Software 架构师 Kenneth Cheung

“管理员们还应该监控和最终用户的应用程序相关的一些服务器和软件指标。管理员们需要监控服务器的运行情况和那些服务器上的软件的运行情况，但是最重要的事情是要把这些指标和最终用户关心的事情联系起来——那就是他们的应用程序是否在正常地运行。”

“通过以应用程序为中心的视角，可以让问题解决者把注意力集中在用户说了些什么和允许创建哪些警告上，还可以让自动化的活动更加有相关性和目的性。”

本文来源：

1. Solve Server Monitoring Problems
2. 译文

> Nagios 的功能十分强大，在我的项目里，因为我的需求不同而尽可能的简化了 nagios 而没有使用代理、更多插件等功能，在一个不超过 1000 个服务器的网络规模里，它工作得很好。

Nagios 经典入门教程——安装篇

文/田逸

作为系统管理员，我最担心那些重要的在线系统在我不知情的情况下停机或者停止网络服务，而且那些发生故障的服务或主机有时候可能要好长一段时间才知道（这种情况多发生在节假日），只要一到节假日，很多系统管理员就紧张不已。要改变这种被动局面，我在这里推荐网络监控软件 Nagios,个人认为它最大的好处是可以发故障报警短信—只要 Nagios 监控的对象发生故障，系统就会自动发送短信到手机上。下面摘录 Nagios 官方网站的描述：

Nagios 是一个用来监控主机、服务和网络的开放源码软件，很多大的公司或组织都在使用它。

在我来到现在这个机构之前，已经有一个 Netsaint(nagios 的老版本)在监控那些在线服务器，但是不完善，后来我立了一个项，部署了新的监控平台 nagios 把所有的在线服务器都监控起来了；到目前为止，监控了 413 个主机和 754 个服务。

虽然 Nagios 十分实用，但配置起来确是麻烦，根据其读音我给它取可一个中文名-难够死。基于这样的原因，我将尽可能详细地向大家讲述我用 Nagios 的过程以及心得，希望对初学者有所帮助。

（一） 安装所需软件

一、安装 Nagios

Nagios 可以运行在各种版本的 linux 及主流的 unix 环境，我试过的环境有 Redhat linux,Centos,Debian 等。在实际的运维中，我是以 centos 4 来部署 nagios 的。安装完操作系统之后，需要把多余的服务都关掉，只留 sshd 这个服务。然后用 wget 下载源码包 nagios-2.6.tar.gz 和 httpd-2.2.0.tar.gz。接下来先分别安装软件，过程如下：

1、 解压 nagios

```
tar zxvf nagios-2.6.tar.gz
```

2、配置 nagios

```
cd nagios
./configure -prefix=/usr/local/nagios
```

3、 编译 nagios

```
make all
```

4、 安装 nagios：

与别的软件安装稍有不同，nagios 的安装要好几步才能完成。第一步执行 make install 安装主要的程序、CGI 及 HTML 文件，第二步执行 make install-commandmode 给外部命令访问 nagios 配置文件的权限，第三步执行 make install-config 把配置文件的例子复制到 nagios 的安装目录。按照安装向导的提示，其实这里还有一个 make install-init 的步骤，它的作用是把 nagios 做成一个运行脚本，使 nagios 随系统开机启动，这是一个很方便的措施。但本人是一个

喜欢把问题简化的人，没有执行这样的操作。

5、 验证程序是否被正确安装：

切换目录到安装路径，我用的是

```
/usr/local/nagios
```

看是否存在 etc、bin、 sbin、 share、 var 这五个目录，如果存在则可以表明程序被正确的安装到系统了。后表是五个目录功能的简要说明：

bin

Nagios 执行程序所在目录，这个目录只有一个文件 nagios

etc

Nagios 配置文件位置，初始安装完后，只有几个*.cfg-sample 文件

sbin

Nagios Cgi 文件所在目录，也就是执行外部命令所需文件所在的目录

Share

Nagios 网页文件所在的目录

Var

Nagios 日志文件、spid 等文件所在的目录

二、安装 nagios 的插件

没有插件，nagios 将什么作用也没有，插件也是 nagios 扩展功能的强大武器，除了下载常用的插件外，我们还可以根据实际要求编写自己的插件。Nagios 的插件 nagios-plugins-1.4.5 在 www.nagios.org 上可以找到，接着我们用 wget 下载它。注意：插件与 nagios 之间的版本关联不大，不一定非得用 nagios-plugins-1.4.5 这个版本。下载完成后，安装它是很简单的：先执行配置

```
./configure -prefix=/usr/local/nagios
```

接着编译安装

```
make
make install
```

即可。这里需要说明一下的是在配置过程指定的安装路径是

```
/usr/local/nagios
```

而不是

```
/usr/local/nagios-plus
```

安装完成后，将在目录/usr/local/nagios 生成目录 libexec（里面有很多文件），这正是 nagios 所需要的。

三、安装 web 服务器 apache

Web 服务不是 nagios 所必须的，但是如果 nagios 没有 web，查看监控对象的状态将是非常费事和没有趣味的事情（只有通过查看 nagios 的日志来判断状态）。我不愿干特无聊的事，所以就花少许时间把 web 安装一下。

在 unix/linux 世界，apache 是 web 服务器的首选对象，其下载网站为 www.apache.org 。建议下载源码。因为我们不需要很复杂的 web 功能，因此简单的执行一下几个步骤就可以正确的把 apache 安装到系统：

1、 解包、配置

```
tar zxvf httpd-2.2.0.tar.gz
cd httpd-2.2.0
./configure   -prefix=/usr/local/apache
```

2、 编译安装：

```
make
make install
```

安装完成后，执行命令

```
./usr/local/apache/bin/apachectl -t
```

检查一下 apache 是否正确安装。

四、配置前的处理

最主要的工作是创建 nagios 用户及其属组，让 nagios 的运行用户为 nagios 而不是 root。再把目录/usr/local/nagios 的属主设置为 nagios，以保证系统的安全。Nagios 可以以 root 用户运行，但并不推荐这样做。用下面的步骤来完成上述过程：

1、添加系统帐户 nagios

```
useradd nagios
```

就很容易的把用户和组 nagios 添加到系统。有的类型的 linux 发行版添加用户和组要麻烦一些-需要手动添加组，然后再执行

```
useradd -g nagios nagios
```

这样的操作。在实际的运用场景，nagios 用户并没有必要作为系统用户来登录 linux 系统，因此可以不必设置 nagios 的用户密码，甚至可以把 nagios 用户的登录 shell 设置成/bin/false。

2、更改目录属组

```
chown -R nagios.nagios
 /usr/local/nagios
```

请注意，有的 unix/linux 的版本用户和属组分隔符号不是“.”,可能会是这样的形式

```
chown -R nagios:nagios
 /usr/local/nagios
```

3、sendmail

看看 sendmail 是否正常运行？我们需要使用 sendmail 来发送故障报警信息，所以这个包必须能够正常工作。Sendmail 分为服务器和客户端两部分,有 2 种发送报警邮件的方式：

（1）nagios 所在的机器通过 sendmail 客户端程序把邮件发送到专门的邮件服务器，再由邮件服务器把消息发送到用户邮箱。

（2）邮件客户端和服务器端就用 nagios 所在系统 sendmail。

第一种方式用起来非常规范，但更麻烦，例如需要做地址解析、修改邮件服务器的配置；另外还有一个问题-它还依赖别的系统，增加了故障点和复杂度。第二种方法十分简单，只需启动 sendmail 服务即可，而且它不再依赖于别的系统和服务。在我工作的实际场景，这两种方法都使用，用专门的邮件服务器会有发送延迟的情况（因为邮件服务器要处理很多其他用户邮件的收发）；而直接用 sendmail 做服务器和客户端就异常简单和方便了。非常幸运的是，几乎所有的 linux/unix 发行版都默认安装 sendmail，费了这么多笔墨，其实就做一个动作-把 sendmail 服务运行起来。

4、手机短信发送工具

……

Nagios 的功能十分强大，在我的项目里，因为我的需求不同而尽可能的简化了 nagios 而没有使用代理、更多插件等功能，在一个不超过 1000 个服务器的网络规模里，它工作得很好。如果有更多的服务器，建议使用 mysql 数据来管理监控对象。在部署 nagios 的过程中，我对很多选项作了取舍，更详细的情况请参照官方的文档。

本文为节选，全文地址：

- 看我出招之:我用 Nagios

推荐阅读：

1. Cacti 网络监控工具完全指南
2. FreeBSD 7.0 上的 nagios 安装完全攻略

> 飞信挺好的，免费、快捷，安装和使用都很方便。但是有一点使我不得不放弃他，那就是没准什么时候飞信机器人更新了，或者中国移动飞信又更新了，而这段时间里你是收不到任何短信提醒的。

教你设置 Nagios 的免费短信绑定功能

文/红昼

现在好多同行都在用飞信机器人来做 Nagios 报警短信提醒。其实我之前也一直在用，飞信挺好的，免费、快捷，安装和使用都很方便。但是有一点使我不得不放弃他，那就是没准什么时候飞信机器人更新了，或者中国移动飞信又更新了，而这段时间里你是收不到任何短信提醒的，让人很头疼。不得不让我再另想办法！

后来听朋友说让我找移动申请一个短信接口就可以了，不过我咨询了下，好像还挺麻烦。后来有个朋友说他在用 139 的手机邮箱，收到邮件后就会发通知，不过能不能看邮件内容就不清楚了。

我一想移动给自己的号段发个短信什么的应该很方便，于是就登陆移动的 139 邮箱网站，并且用自己的手机申请注册了一个（作者注： 现在 163、qq 都有短信提醒了，一样可以用）。

邮箱注册过程中可以看到左边写着这么一行字—看就明白了：

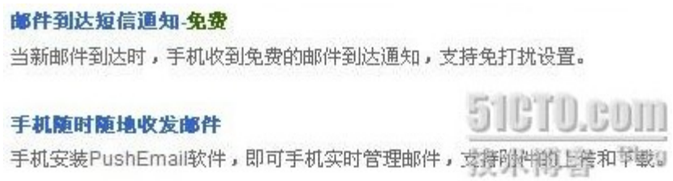

图 1: 邮箱注册提示

注册过程我就不说了吧，登录后要做一下简单的修改，好让你的邮箱能收到 sendmail 发过来的邮件。

在设置界面里选择 手机通知—邮件到达通知。

建议选择长短信，这样 NAGIOS 的提醒基本都能收到，接收时间~全天。

别忘了再设置一个白名单，这样你的 Nagios 发过来的邮件才不会被他过滤掉：

图 2: 添加白名单

好了，139 邮箱上面的设置基本就完成了，接下来再设置一下你的监控服务器 就是那台运行 Nagios 的主机。首先启动 sendmail，一般都会带。然后查看下你的 hostname 是否符合 DNS 中 A 记录的标准，比如 ime.com，如果不是，那就设置一下

```
hostname ufo.com
```

然后在 /etc/hosts 里面把 ufo.com 填进去

然后启动 sendmail 服务

```
/etc/init.d/sendmail start
```

最后让我们来测试一下

```
/bin/mail -s "`date +%Y-%m-%d` Server
 SMS TEST" nagios@139.com < /dev/null
```

几秒钟后我的手机响起，看到下面的效果

图 3: 短信接收成功

哈哈，成功。最后就是把你刚才申请的那个邮箱地址添加到你的 Nagios 的联系人文件当中就 OK 了，重启一下 Nagios 服务，看看效果吧 O(∩_∩)O~

本文来源：

- 你的 NAGIOS 还在用飞信吗？

小阅读：网站一般用什么监控工具

多数网站都会倾向于利用开源软件自行搭建监控平台。笔者一向认为，即使网站有一台服务器，也应该搭建监控工具，这是保障网站能持续改进的基石。常见的开源监控工具有 Nagios、monit 等。Nagios 也可能是当前国内最被广泛采用的监控软件了，根据官方描述，Nagios 是开源的主机、网络、服务监控程序，从这个描述能看出，Nagios 的设计目标是很庞大的。依赖其强大的扩展性，通过分布式监控模式，管理上千台甚至更多的服务器也不在话下。而对于大型集群环境，Ganglia 是个不错的选择。

另外商业化运作的比较好的开源监控工具或框架还有 Zenoss、Zabbix、Hyperic、OpenNMS 等。这几个的定位都是"企业级"监控平台。当然，功能的确不比 Nagios 差，也有的弥补了 Nagios 的一些不足之处(比如 Zenoss 增强了对 Windows 服务器的监控能力)。

来源：

- 网站运维之道

Shell 脚本分享区

下面介绍一个简单的 Shell 脚本，作用是批量生成 Linux 用户。

```
#!/bin/bash
for name in tom jerry joe jane
do
   useradd $name
   echo redhat | passwd --stdin $name
done
```

自己使用的时候，用自己需要的帐户名列表替换掉这个代码范例里的 tom jerry joe jane 等字段即可。密码都是 redhat，可以让用户之后自己更改。

本代码分享者：

抚琴煮酒

其他相关推荐

1. 几个常用的 Linux 监控脚本
2. 让你的 Nagios 记录系统监控日志

招募启事

《Linux 运维趋势》的建设需要您的加入！

您可以通过如下方式参与我们杂志的建设：

1、推荐文章

无论是您在互联网上看到的好文章，还是您自己总结/整理的资料；无论是英文还是中文；无论是入门的还是高端的，都欢迎推荐！推荐方式包括：

a）在技术圈中分享：http://g.51cto.com/linuxops

b）在邮件群中分享：linuxops-cn@googlegroups.com

c）发邮件给编辑：yangsai@51cto.com

2、投稿

如果您认为自己在 Linux 方面具有专家级别的能力，并且有与大家分享您技术经验的热诚，同时也有兴趣挣点稿费花花，那么欢迎您的投稿！

如果您在 IT 技术方面的翻译有很高的能力，能够快速、高质量的完成译文，并且也经常浏览到一些 Linux 方面的优秀外文，那么也欢迎您的投稿！

投稿信箱：yangsai@51cto.com

3、推广与意见

如果您喜欢我们的杂志，认为这本杂志对于您的工作有所帮助，请您的 Linux 好友、同事们推荐它！

如果您觉得这份杂志还有什么地方需要改进或补充，也希望您能够提出您的宝贵意见！

联系人：yangsai@51cto.com

下期预告

下期我们将谈论有关服务器可用性方面的一些内容。敬请期待！

本刊为月刊，预定每月发布日期为：

每个月的第二个星期五

您可以通过如下方式检查是否有新刊发布：

1、加入电子邮件群组：

linuxops-cn@googlegroups.com

获得邮件提醒

2、经常光顾 51CTO Linux 频道：

http://os.51cto.com/linux/

《Linux 运维趋势》是由 51CTO 系统频道策划、针对 Linux/Unix 系统运维人员的一份电子杂志，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。

《Linux 运维趋势》是开放的非盈利性电子杂志，其中所有内容均收集整理自国内外互联网（包含 51CTO 系统频道本身的内容）。对于来自国内的内容，编辑都会事先征求原作者的许可（八卦，趣闻&数字栏目例外）。如果您认为本杂志的内容侵犯到了您的版权，请发信至 yangsai@51cto.com 进行投诉。