



## 第二版：Linux 70 道

### 目录

第二版：Linux 70 道	1
Linux 概述	3
什么是 Linux	4
Windows 和 Linux 的区别	4
Unix 和 Linux 有什么区别？	4
什么是 Linux 内核？	5
1. 系统内存管理	5
2. 应用程序管理	5
3. 硬件设备管理	5
4. 文件系统管理	5
Linux 的基本组件是什么？	5
Linux 的体系结构	6
BASH 和 DOS 之间的基本区别是什么？	6
Linux 开机启动过程？	7
Linux 系统缺省的运行级别？	7
Linux 使用的进程间通信方式？	8
Linux 有哪些系统日志文件？	8
Linux 系统安装多个桌面环境有帮助吗？	8
什么是交换空间？	9
什么是 root 帐户	9
什么是 LILO？	9
什么是 BASH？	9
什么是 CLI？	9
什么是 GUI？	10
开源的优势是什么？	10
GNU 项目的重要性是什么？	10
磁盘、目录、文件	11
简单 Linux 文件系统？	11



Linux 的目录结构是怎样的？	11
什么是 inode ？	13
什么是硬链接和软链接？	14
1. 可以在不同文件系统的文件间建立链接；	14
2. 只有超级用户才可以为目录创建硬链接。	14
RAID 是什么？	15
安全	15
一台 Linux 系统初始化环境后需要做一什么安全工作？	15
什么叫 CC 攻击？什么叫 DDOS 攻击？	16
什么是网站数据库注入？	16
Shell 脚本是什么？	17
实战	17
如何选择 Linux 操作系统版本？	17
如何规划一台 Linux 主机，步骤是怎样？	18
请问当用户反馈网站访问慢，你会如何处理？	18
Linux 性能调优都有哪几种方法？	20
基本命令	20
cd (change directory: 英文释义是改变目录) 切换目录	20
pwd (print working directory: 显示当前工作目录的绝对路径)	21
ls (ls: list 的缩写, 查看列表) 查看当前目录下的所有文件夹 (ls 只列出文件名或目录名)	21
ll (ll: list 的缩写, 查看列表详情) 查看当前目录下的所有详细信息和文件夹 (ll 结果是详细, 有时间, 是否可读写等信息)	21
touch (touch: 创建文件) 创建文件	21
mkdir (mkdir: 创建目录) 创建目录	21
cat (concatenate: 显示或把多个文本文件连接起来) 查看文件命令 (可以快速查看当前文件的内容) (不能快速定位到最后一页)	22
more (more: 更多的意思) 分页查看文件命令 (不能快速定位到最后一页)	22
B: 返回上一层或 Ctrl+B	22
less (lese: 较少的意思) 分页查看文件命令 (可以快速定位到最后一页)	22
tail (尾巴) 查看文件命令 (看最后多少行)	23



cp (copy 单词缩写, 复制功能)	23
mv (move 单词缩写, 移动功能, 该文件名称功能)	23
rm (remove: 移除的意思) 删除文件, 或文件夹	23
find (find: 找到的意思) 查找指定文件或目录	23
vi (VIsual: 视觉) 文本编辑器 类似 win 的记事本 (操作类似于地下的 vim 命令, 看底下 vim 的操作)	24
vim (VI IMproved: 改进版视觉) 改进版文本编辑器 (不管是文件查看还是文件编辑 按 Shift + 上或者下可以上下移动查看视角)	24
X ;向前删除 等同于 windows 系统中的删除键	24
x ;向后删除和大写 x 相反方向	24
管道命令 (把多个命令组合起来使用)	25
grep (grep : 正则表达式) 正则表达式, 用于字符串的搜索工作(模糊查询)。不懂可以先过	25
yum install -y lrzsz 命令 (实现 win 到 Linux 文件互相简单上传文件)	26
tar (解压 压缩 命令)	26
ps (process status: 进程状态, 类似于 windows 的任务管理器)	27
clear 清屏命令。(强迫症患者使用)	27
ifconfig 命令	28
ping (用于检测与目标的连通性) 语法: ping ip 地址	28
1、在 Windows 操作系统中 cmd ipconfig, 查看本机 IP 地址:	28
2、再到 Linux 系统中输入 ping ip 地址	28
free 命令 (显示系统内存)	28
top 命令	28
netstat 命令	29
file (可查看文件类型)	29
重启 linux	29
关机 linux	29
同步时间命令	29
更改为北京时间命令	29
查看时间命令:	30

微信搜一搜

搜云库技术团队



我们的网站: <https://tech.souyunku.com>

关注我们的公众号: **搜云库技术团队**, 回复以下关键字

回复: **【进群】** 邀请您进「技术架构分享群」

回复: **【内推】** 即可进: 北京, 上海, 广州, 深圳, 杭州, 成都, 武汉, 南京, 郑州, 西安, 长沙「程序员工作内推群」

回复 **【1024】** 送 4000G 最新架构师视频

回复 **【PPT】** 即可无套路获取, 以下最新整理调优 PPT!

## 46 页《JVM 深度调优, 演讲 PPT》



## 53 页《Elasticsearch 调优演讲 PPT》

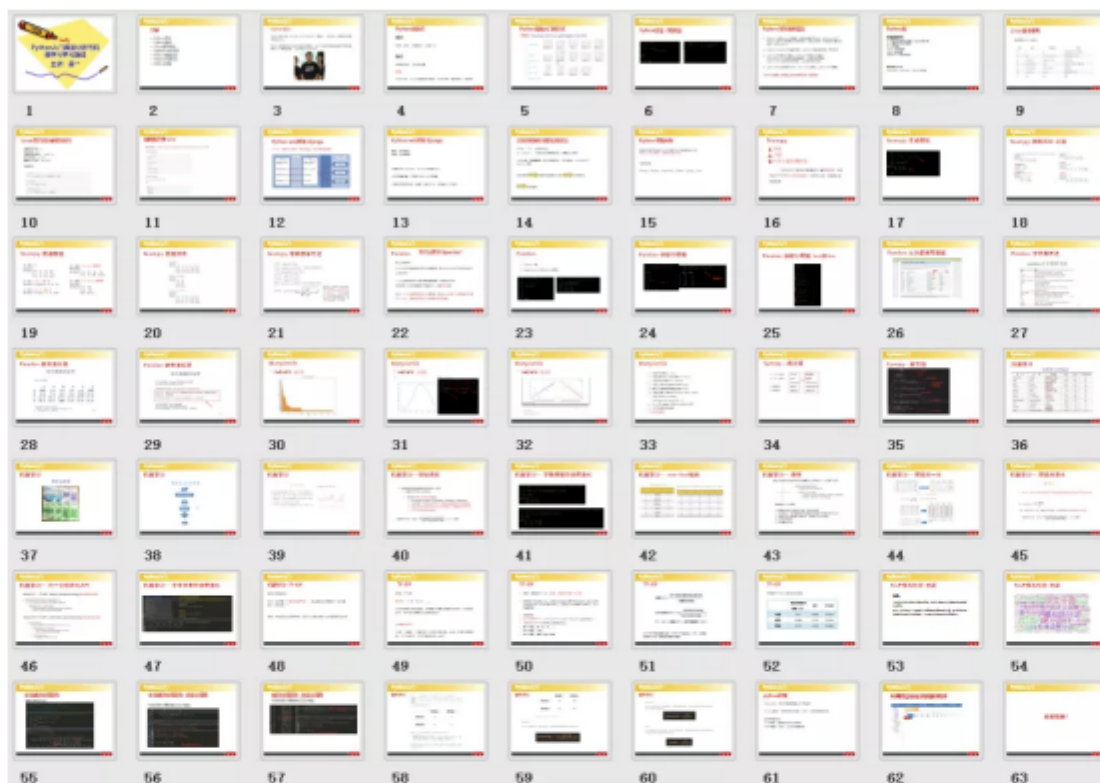


微信搜一搜

搜云库技术团队



## 63 页《Python 数据分析入门 PPT》



# 微信扫一扫

<https://tech.souyunku.com>

技术、架构、资料、工作、内推  
专注于分享最有价值的互联网技术干货文章





## Linux 概述

### 什么是 Linux

- Linux 是一套免费使用和自由传播的类似 Unix 操作系统，一般的 WEB 项目都是部署都是放在 Linux 操作系统上面。Linux 是一个基于 POSIX 和 Unix 的多用户、多任务、支持多线程和多 CPU 的操作系统。它能运行主要的 Unix 工具软件、应用程序和网络协议。它支持 32 位和 64 位硬件。Linux 继承了 Unix 以网络为核心的设计思想，是一个性能稳定的多用户网络操作系统。

### Windows 和 Linux 的区别

- Windows 是微软开发的操作系统，民用操作系统，可用于娱乐、影音、上网。Windows 操作系统具有强大的日志记录系统和强大的桌面应用。好处是它可以帮我们实现非常多绚丽多彩的效果，可以非常方便去进行娱乐、影音、上网。
- Linux 的应用相对单纯很多，没有什么绚丽多彩的效果，因此 Linux 的性能是非常出色的，可以完全针对机器的配置有针对性的优化，
- 简单来说 Windows 适合普通用户进行娱乐办公使用，Linux 适合软件开发部署

### Unix 和 Linux 有什么区别？



- Linux 和 Unix 都是功能强大的操作系统，都是应用广泛的服务器操作系统，有很多相似之处，甚至有一部分人错误地认为 Unix 和 Linux 操作系统是一样的，然而，事实并非如此，以下是两者的区别。

#### 1. 开源性

Linux 是一款开源操作系统，不需要付费，即可使用；Unix 是一款对源码实行知识产权保护的传统商业软件，使用需要付费授权使用。

#### 2. 跨平台性

Linux 操作系统具有良好的跨平台性能，可运行在多种硬件平台上；Unix 操作系统跨平台性能较弱，大多需与硬件配套使用。

#### 3. 可视化界面

Linux 除了进行命令行操作，还有窗体管理系统；Unix 只是命令行下的系统。

#### 4. 硬件环境

Linux 操作系统对硬件的要求较低，安装方法更易掌握；Unix 对硬件要求比较苛刻，按照难度较大。

#### 5. 用户群体

Linux 的用户群体很广泛，个人和企业均可使用；Unix 的用户群体比较窄，多是安全性要求高的大型企业使用，如银行、电信部门等，或者 Unix 硬件厂商使用，如 Sun 等。

相比于 Unix 操作系统，Linux 操作系统更受广大计算机爱好者的喜爱，主要原因是 Linux 操作系统具有 Unix 操作系统的全部功能，并且能够在普通 PC 计算机上实现全部的 Unix 特性，开源免费的特性，更容易普及使用！

## 什么是 Linux 内核？

- Linux 系统的核心是内核。内核控制着计算机系统上的所有硬件和软件，在必要时分配硬件，并根据需要执行软件。

#### 1. 系统内存管理



2. 应用程序管理
3. 硬件设备管理
4. 文件系统管理

## Linux 的基本组件是什么？

- 就像任何其他典型的操作系统一样，Linux 拥有所有这些组件：内核，shell 和 GUI，系统实用程序和应用程序。Linux 比其他操作系统更具优势的是每个方面都附带其他功能，所有代码都可以免费下载。

## Linux 的体系结构

- 从大的方面讲，Linux 体系结构可以分为两块：
- 用户空间(User Space)：用户空间又包括用户的应用程序(User Applications)、C 库(C Library)。
- 内核空间(Kernel Space)：内核空间又包括系统调用接口(System Call Interface)、内核(Kernel)、平台架构相关的代码(Architecture-Dependent Kernel Code)。

为什么 Linux 体系结构要分为用户空间和内核空间的原因？





- 1、现代 CPU 实现了不同的工作模式，不同模式下 CPU 可以执行的指令和访问的寄存器不同。
- 2、Linux 从 CPU 的角度出发，为了保护内核的安全，把系统分成了两部分。
- 用户空间和内核空间是程序执行的**两种不同的状态**，我们可以通过两种方式完成用户空间到内核空间的转移：
  - 系统调用；
  - 硬件中断。

## BASH 和 DOS 之间的基本区别是什么？

- BASH 和 DOS 控制台之间的主要区别在于 3 个方面：
  - BASH 命令区分大小写，而 DOS 命令则不区分；
  - 在 BASH 下，/ character 是目录分隔符，\作为转义字符。在 DOS 下，/ 用作命令参数分隔符，\是目录分隔符
  - DOS 遵循命名文件中的约定，即 8 个字符的文件名后跟一个点，扩展名为 3 个字符。BASH 没有遵循这样的惯例。

## Linux 开机启动过程？

了解即可。

- 1、主机加电自检，加载 BIOS 硬件信息。
- 2、读取 MBR 的引导文件(GRUB、LILO)。
- 3、引导 Linux 内核。
- 4、运行第一个进程 init (进程号永远为 1)。



- 5、进入相应的运行级别。
- 6、运行终端，输入用户名和密码。

## Linux 系统缺省的运行级别？

- 关机。
- 单机用户模式。
- 字符界面的多用户模式(不支持网络)。
- 字符界面的多用户模式。
- 未分配使用。
- 图形界面的多用户模式。
- 重启。

## Linux 使用的进程间通信方式？

了解即可，不需要太深入。

- 1、管道(pipe)、流管道(s\_pipe)、有名管道(FIFO)。
- 2、信号(signal)。
- 3、消息队列。
- 4、共享内存。
- 5、信号量。
- 6、套接字(socket)。

## Linux 有哪些系统日志文件？



- 比较重要的是 `/var/log/messages` 日志文件。

该日志文件是许多进程日志文件的汇总，从该文件可以看出任何入侵企图或成功的入侵。

另外，如果胖友的系统里有 ELK 日志集中收集，它也会被收集进去。

## Linux 系统安装多个桌面环境有帮助吗？

- 通常，一个桌面环境，如 KDE 或 Gnome，足以在没有问题的情况下运行。尽管系统允许从一个环境切换到另一个环境，但这对用户来说都是优先考虑的问题。有些程序在一个环境中工作而在另一个环境中无法工作，因此它也可以被视为选择使用哪个环境的一个因素。

## 什么是交换空间？

- 交换空间是 Linux 使用的一定空间，用于临时保存一些并发运行的程序。当 RAM 没有足够的内存来容纳正在执行的所有程序时，就会发生这种情况。

## 什么是 root 帐户

- root 帐户就像一个系统管理员帐户，允许你完全控制系统。你可以在此处创建和维护用户帐户，为每个帐户分配不同的权限。每次安装 Linux 时都是默认帐户。



## 什么是 LILO?

- LILO 是 Linux 的引导加载程序。它主要用于将 Linux 操作系统加载到主内存中，以便它可以开始运行。

## 什么是 BASH?

- BASH 是 Bourne Again SHell 的缩写。它由 Steve Bourne 编写，作为原始 Bourne Shell (由 / bin / sh 表示) 的替代品。它结合了原始版本的 Bourne Shell 的所有功能，以及其他功能，使其更容易使用。从那以后，它已被改编为运行 Linux 的大多数系统的默认 shell。

## 什么是 CLI?

- **命令行界面** (英语\*\*：command-line interface\*\*，缩写]：**CLI**) 是在图形用户界面得到普及之前使用最为广泛的用户界面，它通常不支持鼠标，用户通过键盘输入指令，计算机接收到指令后，予以执行。也有人称之为**字符用户界面** (CUI)。
- 通常认为，命令行界面 (CLI) 没有图形用户界面 (GUI) 那么方便用户操作。因为，命令行界面的软件通常需要用户记忆操作的命令，但是，由于其本身的特点，命令行界面要较图形用户界面节约计算机系统的资源。在熟记命令的前提下，使用命令行界面往往要较使用图形用户界面的操作速度要快。所以，图形用户界面的操作系统中，都保留着可选的命令行界面。



## 什么是 GUI?

- 图形用户界面 (Graphical User Interface, 简称 GUI, 又称图形用户接口) 是指采用图形方式显示的计算机操作用户界面。
- 图形用户界面是一种人与计算机通信的界面显示格式, 允许用户使用鼠标等输入设备操纵屏幕上的图标或菜单选项, 以选择命令、调用文件、启动程序或执行其它一些日常任务。与通过键盘输入文本或字符命令来完成例行任务的字符界面相比, 图形用户界面有许多优点。

## 开源的优势是什么?

- 开源允许你将软件 (包括源代码) 免费分发给任何感兴趣的人。然后, 人们可以添加功能, 甚至可以调试和更正源代码中的错误。它们甚至可以让它运行得更好, 然后再次自由地重新分配这些增强的源代码。这最终使社区中的每个人受益。

## GNU 项目的重要性是什么?

- 这种所谓的自由软件运动具有多种优势, 例如可以自由地运行程序以及根据你的需要自由学习和修改程序。它还允许你将软件副本重新分发给其他人, 以及自由改进软件并将其发布给公众。

## 磁盘、目录、文件





## 简单 Linux 文件系统？

在 Linux 操作系统中，所有被操作系统管理的资源，例如网络接口卡、磁盘驱动器、打印机、输入输出设备、普通文件或是目录都被看作是一个文件。

- 也就是说在 Linux 系统中有一个重要的概念\*\*：一切都是文件\*\*。其实这是 Unix 哲学的一个体现，而 Linux 是重写 Unix 而来，所以这个概念也就传承了下来。在 Unix 系统中，把一切资源都看作是文件，包括硬件设备。UNIX 系统把每个硬件都看成是一个文件，通常称为设备文件，这样用户就可以用读写文件的方式实现对硬件的访问。
- Linux 支持 5 种文件类型，如下图所示：

## Linux 的目录结构是怎样的？

这个问题，一般不会问。更多是实际使用时，需要知道。

- Linux 文件系统的结构层次鲜明，就像一棵倒立的树，最顶层是其根目录：  
常见目录说明：

目录	介绍
/bin	存放二进制可执行文件(ls,cat,mkdir 等), 常用命令一般都在这里;
/etc	存放系统管理和配置文件;
/home	存放所有用户文件的根目录, 是用户主目录



	的基点，比如用户 user 的主目录就是 /home/user，可以用~user 表示；
/usr	用于存放系统应用程序；
/opt	额外安装的可选应用程序包所放置的位置。一般情况下，我们可以把 tomcat 等都安装到这里；
/proc	虚拟文件系统目录，是系统内存的映射。可直接访问这个目录来获取系统信息；
/root	超级用户（系统管理员）的主目录（特权阶级）；
/sbin	存放二进制可执行文件，只有 root 才能访问。这里存放的是系统管理员使用的系统级别的管理命令和程序。如 ifconfig 等；
/dev	用于存放设备文件；
/mnt	系统管理员安装临时文件系统的安装点，系统提供这个目录是让用户临时挂载其他的文件系统；
/boot	存放用于系统引导时使用的各种文件；
/lib	存放着和系统运行相关的库文件；
/tmp	用于存放各种临时文件，是公用的临时文件存储点；
/var	用于存放运行时需要改变数据的文件，也是某些大文件的溢出区，比方说各种服务的日志文件（系统启动日志等。）等；
/lost+found	这个目录平时是空的，系统非正常关机而留下“无家可归”的文件（windows 下叫什



## 什么是 inode ？

一般来说，面试不会问 inode 。但是 inode 是一个重要概念，是理解 Unix/Linux 文件系统和硬盘储存的基础。

- 理解 inode，要从文件储存说起。
- 文件储存在硬盘上，硬盘的最小存储单位叫做"扇区" (Sector)。每个扇区储存 512 字节 (相当于 0.5KB)。
- 操作系统读取硬盘的时候，不会一个个扇区地读取，这样效率太低，而是一次性连续读取多个扇区，即一次性读取一个"块" (block)。这种由多个扇区组成的"块"，是文件存取的最小单位。"块"的大小，最常见的是 4KB，即连续八个 sector 组成一个 block。
- 文件数据都储存在"块"中，那么很显然，我们还必须找到一个地方储存文件的元信息，比如文件的创建者、文件的创建日期、文件的大小等等。这种储存文件元信息的区域就叫做 inode，中文译名为"索引节点"。
- 每一个文件都有对应的 inode，里面包含了与该文件有关的一些信息。

**简述 Linux 文件系统通过 i 节点把文件的逻辑结构和物理结构转换的工作过程？**

如果看的一脸懵逼，也没关系。一般来说，面试官不太会问这个题目。

- Linux 通过 inode 节点表将文件的逻辑结构和物理结构进行转换。
  - inode 节点是一个 64 字节长的表，表中包含了文件的相关信息，其中有文件的大小、文件所有者、文件的存取许可方式以及文件的类型等重要信息。



在 inode 节点表中最重要的内容是磁盘地址表。在磁盘地址表中有 13 个块号，文件将以块号在磁盘地址表中出现的顺序依次读取相应的块。

- Linux 文件系统通过把 inode 节点和文件名进行连接，当需要读取该文件时，文件系统在当前目录表中查找该文件名对应的项，由此得到该文件相对应的 inode 节点号，通过该 inode 节点的磁盘地址表把分散存放的文件物理块连接成文件的逻辑结构。

## 什么是硬链接和软链接？

- 硬链接：**由于 Linux 下的文件是通过索引节点(inode)来识别文件，硬链接可以认为是一个指针，指向文件索引节点的指针，系统并不为它重新分配 inode 。每添加一个硬链接，文件的链接数就加 1 。
  - 不足：
    1. 不可以不同文件系统的文件间建立链接；
    2. 只有超级用户才可以为目录创建硬链接。
- 软链接：**软链接克服了硬链接的不足，没有任何文件系统的限制，任何用户可以创建指向目录的符号链接。因而现在更为广泛使用，它具有更大的灵活性，甚至可以跨越不同机器、不同网络对文件进行链接。
  - 不足：因为链接文件包含有原文件的路径信息，所以当原文件从一个目录下移到其他目录中，再访问链接文件，系统就找不到了，而硬链接就没有这个缺陷，你想怎么移就怎么移；还有它要系统分配额外的空间用于建立新的索引节点和保存原文件的路径。
- 实际场景下，基本是使用软链接。总结区别如下：**
  - 硬链接不可以跨分区，软链接可以跨分区。
  - 硬链接指向一个 inode 节点，而软链接则是创建一个新的 inode 节点。



- 删除硬链接文件，不会删除原文件，删除软链接文件，会把原文件删除。

## RAID 是什么？

RAID 全称为独立磁盘冗余阵列(Redundant Array of Independent Disks)，基本思想就是把多个相对便宜的硬盘组合起来，成为一个硬盘阵列组，使性能达到甚至超过一个价格昂贵、容量巨大的硬盘。RAID 通常被用在服务器电脑上，使用完全相同的硬盘组成一个逻辑扇区，因此操作系统只会把它当做一个硬盘。

RAID 分为不同的等级，各个不同的等级均在数据可靠性及读写性能上做了不同的权衡。在实际应用中，可以依据自己的实际需求选择不同的 RAID 方案。

- 当然，因为很多公司都使用云服务，大家很难接触到 RAID 这个概念，更多的可能是普通云盘、SSD 云盘酱紫的概念。

## 安全

### 一台 Linux 系统初始化环境后需要做一些什么安全工作？

- 1、添加普通用户登陆，禁止 root 用户登陆，更改 SSH 端口号。

修改 SSH 端口不一定绝对哈。当然，如果要暴露在外网，建议改下。|

- 2、服务器使用密钥登陆，禁止密码登陆。
- 3、开启防火墙，关闭 SELinux，根据业务需求设置相应的防火墙规则。
- 4、装 fail2ban 这种防止 SSH 暴力破击的软件。
- 5、设置只允许公司办公网出口 IP 能登陆服务器(看公司实际需要)





也可以安装 VPN 等软件，只允许连接 VPN 到服务器上。

- 6、修改历史命令记录的条数为 10 条。
- 7、只允许有需要的服务器可以访问外网，其它全部禁止。
- 8、做好软件层面的防护。
  - 8.1 设置 nginx\_waf 模块防止 SQL 注入。
  - 8.2 把 Web 服务使用 www 用户启动，更改网站目录的所有者和所属组为 www 。

## 什么叫 CC 攻击？什么叫 DDOS 攻击？

- CC 攻击，主要是用来攻击页面的，模拟多个用户不停的对你的页面进行访问，从而使你的系统资源消耗殆尽。
- DDOS 攻击，中文名叫分布式拒绝服务攻击，指借助服务器技术将多个计算机联合起来作为攻击平台，来对一个或多个目标发动 DDOS 攻击。

攻击，即是通过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。

### 怎么预防 CC 攻击和 DDOS 攻击？

- 防 CC、DDOS 攻击，这些只能是用硬件防火墙做流量清洗，将攻击流量引入黑洞。

流量清洗这一块，主要是买 ISP 服务商的防攻击的服务就可以，机房一般有空余流量，我们一般是买服务，毕竟攻击不会是持续长时间。

## 什么是网站数据库注入？



- 由于程序员的水平及经验参差不齐，大部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断。
- 应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的 SQL 注入。
- SQL 注入，是从正常的 WWW 端口访问，而且表面看起来跟一般的 Web 页面访问没什么区别，如果管理员没查看日志的习惯，可能被入侵很长时间都不会发觉。

#### 如何过滤与预防？

- 数据库网页端注入这种，可以考虑使用 nginx\_waf 做过滤与预防。

### Shell 脚本是什么？

- 一个 Shell 脚本是一个文本文件，包含一个或多个命令。作为系统管理员，我们经常需要使用多个命令来完成一项任务，我们可以添加这些所有命令在一个文本文件(Shell 脚本)来完成这些日常工作任务。

## 实战

### 如何选择 Linux 操作系统版本？



一般来讲，桌面用户首选 **Ubuntu**；服务器首选 **RHEL** 或 **CentOS**，两者中首选 **CentOS**。

- 根据具体要求：
  - 安全性要求较高，则选择 **Debian** 或者 **FreeBSD**。
  - 需要使用数据库高级服务和电子邮件网络应用的用户可以选择 **SUSE**。
  - 想要新技术新功能可以选择 **Fedora**，**Fedora** 是 **RHEL** 和 **CentOS** 的一个测试版和预发布版本。
  - **【重点】**根据现有状况，绝大多数互联网公司选择 **CentOS**。现在比较常用的是 **6** 系列，现在市场占有大概一半左右。另外的原因是 **CentOS** 更侧重服务器领域，并且无版权约束。

**CentOS 7** 系列，也慢慢使用的会比较多了。

## 如何规划一台 Linux 主机，步骤是怎样？

- 1、确定机器是做什么用的，比如是做 **WEB**、**DB**、还是游戏服务器。

不同的用途，机器的配置会有所不同。

- 2、确定好之后，就要定系统需要怎么安装，默认安装哪些系统、分区怎么做。
- 3、需要优化系统的哪些参数，需要创建哪些用户等等的。

## 请问当用户反馈网站访问慢，你会如何处理？

有哪些方面的因素会导致网站访问慢？



- 1、服务器出口带宽不够用
- 本身服务器购买的出口带宽比较小。一旦并发量大的话，就会造成分给每个用户的出口带宽就小，访问速度自然就会慢。
- 跨运营商网络导致带宽缩减。例如，公司网站放在电信的网络上，那么客户这边对接是长城宽带或联通，这也可能导致带宽的缩减。

- 2、服务器负载过大，导致响应不过来

可以从两个方面入手分析：

- 分析系统负载，使用 `w` 命令或者 `uptime` 命令查看系统负载。如果负载很高，则使用 `top` 命令查看 CPU，MEM 等占用情况，要么是 CPU 繁忙，要么是内存不够。
- 如果这二者都正常，再去使用 `sar` 命令分析网卡流量，分析是不是遭到了攻击。一旦分析出问题的原因，采取对应的措施解决，如决定要不要杀死一些进程，或者禁止一些访问等。

- 3、数据库瓶颈

- 如果慢查询比较多。那么就要开发人员或 DBA 协助进行 SQL 语句的优化。
- 如果数据库响应慢，考虑可以加一个数据库缓存，如 Redis 等。然后，也可以搭建 MySQL 主从，一台 MySQL 服务器负责写，其他几台从数据库负责读。

- 4、网站开发代码没有优化好

- 例如 SQL 语句没有优化，导致数据库读写相当耗时。

针对网站访问慢，怎么去排查？



- 1、首先要确定是用户端还是服务端的问题。当接到用户反馈访问慢，那边自己立即访问网站看看，如果自己这边访问快，基本断定是用户端问题，就需要耐心跟客户解释，协助客户解决问题。

不要上来就看服务端的问题。一定要从源头开始，逐步逐步往下。

- 2、如果访问也慢，那么可以利用浏览器的调试功能，看看加载那一项数据消耗时间过多，是图片加载慢，还是某些数据加载慢。
- 3、针对服务器负载情况。查看服务器硬件(网络、CPU、内存)的消耗情况。如果是购买的云主机，比如阿里云，可以登录阿里云平台提供各方面的监控，比如CPU、内存、带宽的使用情况。
- 4、如果发现硬件资源消耗都不高，那么就需要通过查日志，比如看看 MySQL 慢查询的日志，看看是不是某条 SQL 语句查询慢，导致网站访问慢。

怎么去解决？

- 1、如果是出口带宽问题，那么久申请加大出口带宽。
- 2、如果慢查询比较多，那么就要开发人员或 DBA 协助进行 SQL 语句的优化。
- 3、如果数据库响应慢，考虑可以加一个数据库缓存，如 Redis 等等。然后也可以搭建 MySQL 主从，一台 MySQL 服务器负责写，其他几台从数据库负责读。
- 4、申请购买 CDN 服务，加载用户的访问。
- 5、如果访问还比较慢，那就需要从整体架构上进行优化咯。做到专角色专用，多台服务器提供同一个服务。

## Linux 性能调优都有哪几种方法？

- 1、Disabling daemons (关闭 daemons)。





- 2、Shutting down the GUI (关闭 GUI)。
- 3、Changing kernel parameters (改变内核参数)。
- 4、Kernel parameters (内核参数)。
- 5、Tuning the processor subsystem (处理器子系统调优)。
- 6、Tuning the memory subsystem (内存子系统调优)。
- 7、Tuning the file system (文件系统子系统调优)。
- 8、Tuning the network subsystem (网络子系统调优)。

## 基本命令

**cd (change directory: 英文释义是改变目录) 切换目录**

cd ../;跳到上级目录

cd /opt ;不管现在到那直接跳到指定的 opt 文件夹中

cd ~ ;切换当前用户的家目录。root 用户的家目录就是 root 目录。

**pwd (print working directory: 显示当前工作目录的绝对路径)**

pwd

显示当前的绝对路劲

**ls (ls: list 的缩写, 查看列表) 查看当前目录下的所有文件夹**

**(ls 只列出文件名或目录名)**



ls -a ;显示所有文件夹,隐藏文件也显示出来

ls -R ;连同子目录一起列出来

## ll (ll: list 的缩写, 查看列表详情) 查看当前目录下的所有详细信息和文件夹 (ll 结果是详细,有时间,是否可读写等信息)

ll -a ;显示所有文件,隐藏文件也显示出来

ll -R ;连同子目录内容一起列出来

ll -h ;友好展示详情信息,可以看大小

ll -al ;即能显示隐藏文件又能显示详细列表。

## touch (touch: 创建文件) 创建文件

touch test.txt ;创建 test.txt 文件

touch /opt/java/test.java ;在指定目录创建 test.java 文件

## mkdir (mkdir: 创建目录) 创建目录

mkdir 文件夹名称 ;在此目录创建文件夹

mkdir /opt/java/jdk ;在指定目录创建文件夹

## cat (concatenate: 显示或把多个文本文件连接起来) 查看文件命令 (可以快捷查看当前文件的内容) (不能快速定位到最后一页)



cat lj.log ;快捷查看文件命令

Ctrl + c ;暂停显示文件

Ctrl + d ;退出查看文件命令

## more (more: 更多的意思) 分页查看文件命令 (不能快速定位到最后一页)

回车: 向下 n 行, 需要定义, 默认为 1 行。

空格键: 向下滚动一屏或 Ctrl+F

B: 返回上一层或 Ctrl+B

q: 退出 more

## less (lese: 较少的意思) 分页查看文件命令 (可以快速定位到最后一页)

less -m 显示类似于 more 命令的百分比。

less -N 显示每行的行号。(大写的 N)

两参数一起使用如: less -mN 文件名, 如此可分页并显示行号。

空格键: 前下一页或 page down。

回车: 向下一行。

b: 后退一页 或 page up。

q: 退出。

d: 前进半页。

u: 后退半页



## tail (尾巴) 查看文件命令 (看最后多少行)

tail -10 ;文件名 看最后 10 行

## cp (copy 单词缩写, 复制功能)

cp /opt/java/java.log /opt/logs/ ;把 java.log 复制到/opt/logs/下  
cp /opt/java/java.log /opt/logs/aaa.log ;把 java.log 复制到/opt/logs/下并且改名为 aaa.log  
cp -r /opt/java /opt/logs ;把文件夹及内容复制到 logs 文件中

## mv (move 单词缩写, 移动功能, 该文件名称功能)

mv /opt/java/java.log /opt/mysql/ ;移动文件到 mysql 目录下  
mv java.log mysql.log ;把 java.log 改名为 mysql.log

## rm (remove: 移除的意思) 删除文件, 或文件夹

-f 或--force 强制删除文件或目录。删除文件不包括文件夹的文件  
-r 或-R 或--recursive 递归处理, 将指定目录下的所有文件及子目录一并删除。  
-rf 强制删除文件夹及内容

rm 文件名 ;安全删除命令 (yes 删除 no 取消)

rm -rf 强制删除文件夹及内容

rm -rf \* 删除当前目录下的所有内容。

rm -rf /\* 删除 Linux 系统根目录下所有的内容。系统将完蛋。



## find (find: 找到的意思) 查找指定文件或目录

\* 表示 0~多个任意字符。

find -name 文件名;按照指定名称查找在当前目录下查找文件

find / -name 文件名按照指定名称全局查找文件

find -name '\*文件名';任意前缀加上文件名在当前目录下查找文件

find / -name '\*文件名\*';全局进行模糊查询带文件名的文件

**vi (Visual: 视觉) 文本编辑器 类似 win 的记事本 (操作类似于地下的 vim 命令, 看底下 vim 的操作)**

**vim (VI IMproved: 改进版视觉) 改进版文本编辑器 (不管是文件查看还是文件编辑 按 Shift + 上或者下可以上下移动查看视角)**

输入" vim 文件名" 打开文件, 刚刚时是" 一般模式"。

一般模式: 可以浏览文件内容, 可以进行文本快捷操作。如单行复制, 多行复制, 单行删除, 多行删除, (退出) 等。

插入模式: 可以编辑文件内容。

底行模式: 可以进行强制退出操作, 不保存 :q!

可以进行保存并退出操作 :wq

按下" i" 或" a" 或" o" 键, 从" 一般模式", 进入" 插入模式 (编辑模式)"。





在编辑模式下按“ Esc” 即可到一般模式

在一般模式下按“ :” , 冒号进入底行模式。

在一般模式下的快捷键

dd ;删除一整行

X ;向前删除 等同于 windows 系统中的删除键

x ;向后删除和大写 x 相反方向

Ctrl + f ;向后看一页

Ctrl + b ;向前看一页

u ;撤销上一步操作

/word ;向下查找 word 关键字 输入:n 查找下一个,N 查找上一个 (不管是哪个查找都是全局查找 只不过 n 的方向相反)

?log ;向上查找 log 关键字 输入:n 查找上一个,N 查找下一个

:1,90s/redis/Redis/g ;把 1-90 行的 redis 替换为 Redis。语法 n1,n2s/原关键字/新关键字/g, n1 代表其实行,n2 代表结尾行,g 是必须要的

:0 ;光标移动到第一行

:\$ ;光标移动到最后一行

:300 ;光标移动到 300 行,输入多少数字移动到多少行

:w ;保存

:w! ;强制保存

:q ;退出

:q! ;强制退出

5dd ;删除后面 5 行,打一个参数为自己填写

5x ;删除此光标后面 5 个字符

d1G ;删除此光标之前的所有

d0 ;从光标当前位置删除到此行的第一个位置

yy ;复制

p ;在光标的下面进行粘贴

P ;在光标的上面进行粘贴



## | 管道命令 (把多个命令组合起来使用)

管道命令的语法: 命令 1 | 命令 2 | 命令 3。

**grep (grep : 正则表达式) 正则表达式, 用于字符串的搜索工作(模糊查询)。不懂可以先过**

单独使用:

grep String test.java ; 在 test.java 文件中查找 String 的位置, 返回整行  
一般此命令不会单独使用下面列几个常用的命令 (地下通过管道命令组合起来使用)

ps aux|grep java ; 查找带 java 关键字的进程

ll |grep java ; 查找带 java 关键字的文件夹及文件

**yum install -y lrzsz 命令 (实现 win 到 Linux 文件互相简单上传文件)**

# (实际上就是在 Linux 系统中下载了一个插件) 下了了此安装包后就可以实现 win 系统到 linux 之间拉文件拉文件

#等待下载完了就可以输入:

rz 从 win 系统中选择文件上传到 Linux 系统中

sz 文件名 选择 Linux 系统的文件复制到 win 系统中



## tar (解压 压缩 命令)

常用的组合命令：

-z 是否需要用 gzip 压缩。

-c 建立一个压缩文件的参数指令(create) -压缩

-x 解开一个压缩文件的参数指令(extract) -解压

-v 压缩的过程中显示文件(verbose)

-f 使用档名，在 f 之后要立即接档名(file)

常用解压参数组合：zxvf

常用压缩参数组合：zcvf

解压命令：

tar -zxvf redis-3.2.8.tar.gz ; 解压到当前文件夹

tar -zxvf redis-3.2.8.tar.gz -C /opt/java/ ; 解压到指定目录

压缩命令：（注意 语法有点反了，我反正每次都搞反）

tar -zcvf redis-3.2.8.tar.gz redis-3.2.8/ ;语法 tar -zcvf 压缩后的名称  
要压缩的文件

tar -zcvf 压缩后的文件（可指定目录） 要压缩的文件（可指定目录）

## ps (process status: 进程状态, 类似于 windows 的任务管理器)

常用组合：ps -ef 标准的格式查看系统进程

ps -aux BSD 格式查看系统进程

ps -aux|grep redis BSD 格式查看进程名称带有 redis 的系统进程（常用技巧）

//显示进程的一些属性,需要了解 (ps aux)



```
USER      //用户名
PID        //进程 ID 号,用来杀死进程的
%CPU      //进程占用的 CPU 的百分比
%MEM      //占用内存的的百分比
VSZ       //该进程使用的虚拟内存量 (KB)
RSS       //该进程占用的固定内存量 (KB)
STAT      //进程的状态
START     //该进程被触发启动时间
TIME      //该进程实际使用 CPU 运行的时间
```

## clear 清屏命令。（强迫症患者使用）

kill 命令用来中止一个进程。（要配合 ps 命令使用，配合 pid 关闭进程）

（ps 类似于打开任务管理器，kill 类似于关闭进程）

kill -5 进程的 PID ;推荐,和平关闭进程

kill -9 PID ;不推荐,强制杀死进程

## ifconfig 命令

用于查看和更改网络接口的地址和参数，包括 IP 地址、网络掩码、广播地址，使用权限是超级用户。（一般是用来查看的，很少更改）

如果此命令输入无效，先输入 yum -y install net-tools

ifconfig

## ping （用于检测与目标的连通性）语法：ping ip 地址

测试：

1、在 Windows 操作系统中⌨cmd⌨ipconfig，查看本机 IP 地址：



2、再到 Linux 系统中输入 ping ip 地址

(公司电脑, 我就不暴露 Ip 了,没图片 自己去试)

按 Ctrl + C 可以停止测试。

## free 命令 (显示系统内存)

#显示系统内存使用情况, 包括物理内存、交互区内存(swap)和内核缓冲区内内存。

-b 以 Byte 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

-g 以 gb 为单位显示内存使用情况

-s<间隔秒数> 持续显示内存

-t 显示内存使用总合

## top 命令

#显示当前系统正在执行的进程的相关信息, 包括进程 ID、内存占用率、CPU 占用率等

-c 显示完整的进程命令

-s 保密模式

-p <进程号> 指定进程显示

-n <次数> 循环显示次数

## netstat 命令

#Linux netstat 命令用于显示网络状态。

#利用 netstat 指令可让你得知整个 Linux 系统的网络情况。

#语法:





```
netstat [-acCeFghilMnNoprstuvVwx][-A<网络类型>][--ip]
```

## file（可查看文件类型）

```
file 文件名
```

## 重启 linux

```
Linux centos 重启命令：reboot
```

## 关机 linux

```
Linux centos 关机命令：halt
```

## 同步时间命令

```
ntpdate ntp1.aliyun.com
```

## 更改为北京时间命令

```
rm -rf /etc/localtime
```

```
ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime
```

## 查看时间命令：

✳ 微信搜一搜

🔍 搜云库技术团队 |



date

公众号：架构师专栏