文档01用户管理

1. UID-用户ID

UserID，每个用户的唯一识别ID，SuperUser：UID=0，SystemUser：UID=1-499，

一般（常规）用户：UID=500-60000.

1. GID-组ID

GroupID-每个组的唯一识别ID，没有SuperGroup，SystemGroup：GID=0-499，

一般（常规）用户：GID=500-60000.

1. cat /etc/passwd（命令，Linux里）

root:x:0:0:root:/root:/bin/bash

第一字段root:用户名；

第二字段x：密码；

第三字段0：UID；

第四字段0：primary group’s GID

第五字段root：说明；

第六字段/root:根目录

第七字段/bin/bash:Login shell

1. cat /etc/shadow命令（Linxu里）

/etc/shadow不安全；

/etc/shadow支持SHA-256及SHA-512密码哈希；

密码哈希中存储三种信息（哈希算法、用于加密哈希的salt、已加密的哈希）

1. cat /etc/group

开放给全部用户可以存取的权限

root:x:0:root

第一字段root：组名称；

第二字段x:组密码；

第三字段0：GID；

第四字段root:加入该组的用户；

1. 图形管理工具 –system-config-users

一种方式：用root登入，执行system-config-users

另一种：选单【系统】--【管理】--【用户和组群】

1. 命令行
2. 管理本地用户

useradd创建用户

useradd username:创建本地用户

useradd：默认情况下，不设置密码，用户无法登入

userdel删除用户

userdel username：默认情况下，主目录保持不变

userdel –r username:一起删除用户主目录

id:显示用户信息

id username:显示username的用户信息

psaawd:设置密码

passwd username:设置或更改用户密码

linxu下root就是superuser,UID=0;

文档02管道和IO重定向

1. Linux中命令行最强大的两个效果：管道与I/O重定向

I/O重定向可将命令行的执行的输出或错误消息重定向至文件，方便当下保存或稍后进行分析；

1. 程序执行的重定向运算符号

>:将STDOUT（标准输出）重定向到文件

文件内容会被覆盖；

举例：/etc>/root/backup/config-file-lists

>>:将STDOUT重定向到文件

文件内容会被添加，举例：（date;who -l）>>/root/monitor/who-online

<:重定向STDIN

将键盘输入改由读文件提供

举例：mail –s “Warning” root</root/mail-record/alert-notify

1. 管道使用

（1）运算符管道

|：将一个命令的STDOUT发送到另一个命令的STDIN

举例：#grep pattern /var/log/messages | mail –s “lssus notify” root

1. 命令行T管道

tee:将上一个命令的STDOUT通过T管道重定向到文件，再发送到另一个命令的STDIN；

举例：#ifconfig eth0 | grep pattern | tee /root/interface-info | cut-f2 –d: | cut –f1 –d” ”

1. 管道与重定向

比较管道与重定向

标准的命令用法：grep root/etc/passwd

重定向：grep root</etc/passwd

管道：cat /etc/passwd | grep root

三种完全不同架构，却得到相同结果

03安装与管理软件

1. 软件管理
2. 源码

Tar ball文档，源码打包，自行编程，门槛高，不易出错，不好管理

1. RPM

将源码先编程成RPM软件包，安装时只需要解开软件包复制到适当位置不用再编程，容易管理，方便更新、移除

1. RHEL软件命名规则

A-B-C.D.E

A:软件名，可用-

B:版本

C:发行次数，RHEL习惯加上el#字样，#代表RHELv#

D:搭配规格，有noarch

E:有.rpm与.src.rpm两种

1. 管理系统软件方法

安装；更新；删除

查询：软件信息，软件安装清单，软件说明文件，软件配置文件；

审核：安装前软件审核，比对数字指纹

安装软件后审核，检查是否有配置异常改动

1. 使用rpm与yum的不同方法管理软件
2. RPM软件包有些不能单独安装，必须先安装别的RPM软件包才能安装—RPM软件包相依性

rpm命令安装时不检查相依性问题

yum命令安装时，自动解决相依性问题

命令举例：rpm –ivh mod\_ssl-2.2.15-5.el6.x86\_64.rpm

1. rpm与yum的不同方法管理软件

yum命令行使用前提：有正确的.repo

使用yum前，先正确设置软件库

软件库：repository

设定路径：/etc/yum.repos.d

.conf:可任意文件名

[rhel6] name=描述 baseurl=ftp://F.Q.D.N/path/to/repodata

gpgcheck=0

1. 安装

rpm：#rpm –ivh /path/to/.rpm

#rpm - -force –ivh /path/to.rpm

#rpm - -aid –ivh path/to/.rpm

yum:#yum –y install 软件名

#yum –y reinstall 软件名

#yum –y localinstall /path/to/.rpm

1. 更新

rpm:

#rpm –Uvh /path/to/.rpm

#rpm –Fvh /path/to/.rpm

更新kernel软件应注意事项

yum:

#yum –y update 软件名

#yum –y update

不指定软件名，会更新全部

1. 删除

rpm: #rpm –e 软件名

yum:#yum –y remove 软件名

1. 查询

rpm:#rpm –q 软件名

#rpm –ql 软件名

#rpm –qi 软件名

yum:#yum –y list 软件名

#yum –y provides “/path/to/file”

#yum –y info 软件名

1. 审核

rpm:#rpm –import /etc/pki/rpm/RedHat-release-key-file

#rpm –K /path/to/.rpm

yum:#yum –y install |update 软件名

/etc/yum.repos.d/\*.conf:可任意文件名

gpgkey=file://path/to/.rpm-sign-gpg-key

该key文件可以是Red Hat或第三方签署

安装软件后：rpm:#rpm –V 软件名

yum:#yum verify-rpm 软件名

04 使用逻辑卷管理器灵活管理存储

1. LVM v1不能在线加大分区，LVM v2可以在线扩大分区更有弹性

2. LVM定义及术语

LV:逻辑卷，从卷组划分的虚拟分区，并对其格式化

VG:卷组，一个或多个物理卷的集合

PV:物理卷，标记为LVM可用的空间

通常是分区类型0x8e标记，例如/dev/sda5

也可以是一个未分区的硬盘，例如/dev/sda

RAID,例如/dev/md0

3.LVM与传统分区

传统分区----没有容错；大小固定，没有弹性

LVM----支持容错；建议搭配RAID做容错；可以弹性在线增大逻辑卷

4.分区类型

82：swap 83:ext3/ext4分区 8e:LVM分区 fd:RAID分区

5.创建及管理逻辑卷

（1）创建物理卷

需要创建0x8e的分区（fdisk,partx）

pvcreate:创建物理卷

pvs:查看物理卷

pvdisplay:查看物理卷

(2)创建卷组VG

vgcreate vgname/dev/sdaN

vgname:卷组名称

/dev/sdaN:要加入卷的物理卷

vgs:查看卷组

vgdisplay：查看卷组

(3)创建逻辑卷

lvcreate –n lvname –L 2G vgname

lvname:逻辑卷名称

-L 2G逻辑卷大小

vgname:从卷组分配空间给逻辑卷

lvs:查看逻辑卷

lvdispaly:查看逻辑卷

(4)格式化并挂载

mkfs –t ext4/dev/vgname/lvname

在逻辑卷上创建ext4文件系统

跟传统物理分区类似

mkdir /data

创建文件夹

mount /dev/vgname/lvname

手动挂载

(5)扩展卷组

可在线扩展卷组

不一定可以缩减卷组

vgextend vgname /dev/sdaN

将物理卷/dev/sdaN,加到vgname

vgs:查看卷组

vgdisplay:查看卷组

必须要有未使用的物理卷

必须先有未使用的分区或硬盘

(6)扩展逻辑卷和文件系统

卷组必须要有足够空间

lvextend –l +128 /dev/vgname/lvname

再加大128个L.E

lvextend –l+128M /dev/vgname/lvname

再加大128MB

resize2fs –p /dev/vgname/lvname

扩展文件系统

-p显示操作间的进度

(6)减小文件系统和逻辑卷

umont /data

解除挂载要缩小的文件系统

fsck –f /dev/vgname/lvname

检查文件系统

resize2fs –p /dev/vgname/lvname 512M ----文件系统调整为512M

lvreduce –L 512M /dev/vgname/lvname----逻辑卷减小到512M

mount/data:重新挂载

 LVM是逻辑盘卷管理（Logical Volume Manager）的简称，它是Linux环境下对磁盘分区进行管理的一种机制，LVM是建立在硬盘和分区之上的一个逻辑层，来提高磁盘分区管理的灵活性。LVM是在磁盘分区和文件系统之间添加的一个逻辑层，来为文件系统屏蔽下层磁盘分区布局，提供一个抽象的盘卷，在盘卷上建立文件系统。物理卷（physical volume）物理卷就是指硬盘分区或从逻辑上与磁盘分区具有同样功能的设备（如RAID），是LVM的基本存储逻辑块，但和基本的物理存储介质（如分区、磁盘等）比较，却包含有与LVM相关的管理参数。

要建立LVM，首先需要为LVM准备磁盘或者分区。如果使用磁盘分区作为物理卷的话，需要将分区标识为“Linux LVM”，其分区ID为“0x8e”

扩容顺序：

    创建新的PV---将新的PV加入到当前VG---扩容现有LV----扩容文件系统

    下图划分出一个分区，大小5G，分区标识号：83，我需要修改成8E，继续下面配置，如果想知道分区标识号有哪些，可以查看帮助。

创建新PV并将新的PV加入到现有的VG：

命令：pvcreate （创建PV，如果是创建VG前面修改成VG即可，只是语法稍有区别）

命令：vgextend （对VG进行扩容）

语法：vgextend 现有的VG + PV绝对路径

语法：pvcreate 分区1 + 分区2 + 分区3 + …

语法：vgcreate –s pe vgname pv + + + （这里的参数-S表示在创建VG的时候修改PE块的大小）

进行LV的扩容和文件系统的扩容：

命令：lvresize 或者lvextend

语法：lvresize -L size 需要扩容的LV绝对路径

文档05管理进程

1. 进程是程序运行的实例，每个进程都在内存中有属于自己的地址空间与特征

Linux的内核会依照进程的ID编号（PID）来跟踪及对进程进行控制

1. 认识进程管理监控的执行要点
2. 认识niceness值与调整方法

Linux进程调度是将CPU时间分为时间段，每个进程将依次在逻辑处理单元上运行，优先级较高的进程先执行

用户可通过设置进程的niceness值来影响优先级

niceness值范围：-20到+19，数字越小，优先级越高

root可调进程优先级到-20；非root用户只能往+19调

调整niceness值得命令：

执行命令指定niceness值----nice –n #command

对已执行命令指定niceness值----renice # <process’s PID>

1. 进程管理监控方法
2. 图形工具

应用程序----系统工具----系统监视器

进程----点击任一进程----查看----所有进程

1. 命令行

一次列出进程：ps

ps对应BSD的参数：ps aux

ps对应UNIX的参数：ps –lef

即时监控：top

热键：P----按处理使用率排列进程

M----按内存使用率排列进程

d----控制即时显示秒差

h----显示更多热键的用法

q----离开top

1. 可执行进程的终止和管理

可终止进程的指令

（a）top 热键：k->PID->signal-number

（b） kill kill –l:signal-number一览

正常结束进程：kill -15 PID

强制结束进程：kill -9 PID

数字是信号（1-64没有32、33），PID是进程号

可以忽略，默认和自定义信号（不理解32、33实时信号的意思）

1. 其他科终止信号的指令：killall;pkill
2. 管理定期任务
3. 安装默认启动后台程序：crond

每分钟唤醒一次，可运行计划中任务

1. 观察定期任务log文件

/var/log/cron

1. 设定定期任务

单一用户配置搭配命令：crontab（默认编辑器vi）

编辑文件：crontab –e

列出文件：crontab -l

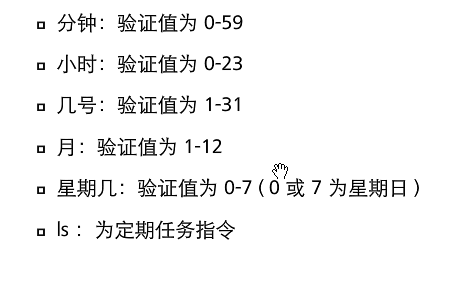
删除文件：crontab –r

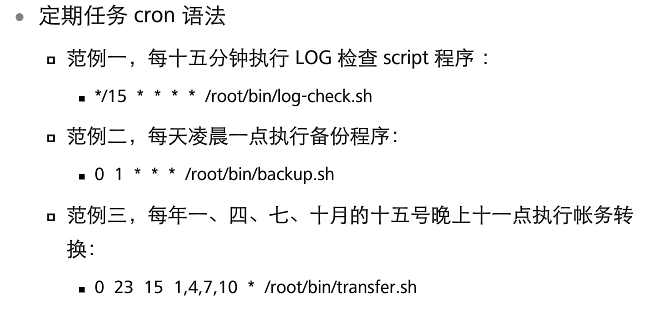
1. 定期任务cron语法

范例：每分钟执行ls----\* \* \* \* \* ls

分钟 小时 几号 月 星期几 ls

1. 定期任务cron语法





文档06网络监控和高级网络配置

对于服务器而言，确定网络服务在哪个端口运行很重要，额外多开端口将会为攻击者提供攻击的途径

IP别名，同一块物理网卡，相同的MAC Address，配置不同的Layer 3 –IP地址，适用于Web托管、HA容错、路由等机制。

1. 检测开放端口
2. 检测本地端口

命令：netstart –tupln | grep:25

t----TCP，仅显示TCP相关选项

u----UDP，仅显示UDP相关选项

p----Procedure，显示建立相关连接的服务状态

l----List，仅列出正在Listen（监听）的服务状态

n----拒绝显示别名，能显示数字的全部转化为数字

1. 检测远程服务

nmap软件包

1. 可以单独检测服务器

例如：namp 192.168.0.101

1. 可以检测整个class C

例如：nmap 192.168.0.0/24

不支持255.255.255.0的语法

1. 如果没有防火墙干扰，应该和netstar结果一致
2. 通过wireshark捕获/分析网络封包

软件包wireshark;跟tcpdump使用相同格式

1. 网络端口配置-IP别名
2. IP别名

在相同的Layer1【网卡】及Layer2【MAC Address】，指定不同的Layer3 –IP地址

命名原则：

eth0

eth0:0

eth0:1

1. 哪些不支持IP别名

DHCP不支持别名

NetworkManager不支持别名（NetworkManager也不支持网卡绑定；

service NetworkManager stop

chconfig NetworkManager off）

1. 配置IP别名

命令行：ifconfig eth0:0 192.168.1.101 netmask 255.255.255.0

网络服务重启，或服务器重启后失效

方便测试

配置文档：/etc/sysconfig/network-scripts/ifcfg-eth0:0

网络服务重启，或服务器重启后依然有效

语法跟一般网卡配置相同

1. 静态路由配置
2. 开启路由

启用数据包从一块网卡进，一块网卡出的功能

默认是关闭

启动路由、NAT，必须要先开启路由

命令：cat /proc/sys/net/ipv4/ip\_forward

echo “1” >/proc/sys/net/ipv4/ip\_forwarrd

cat /proc/sys/net/ipv4/ip\_forward

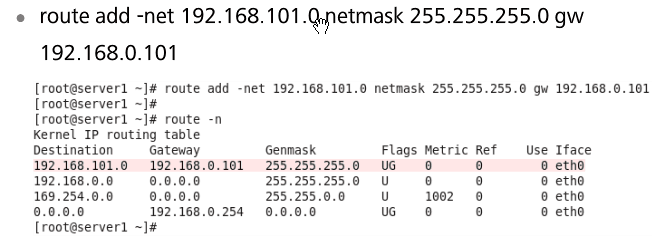
net.ipv4.ip\_forward=1

sysctl –p /etc/sysctl.conf:立刻生效

/etc/rc.d/rc.sysctl 执行sysctl –p /etc/sysctl.conf

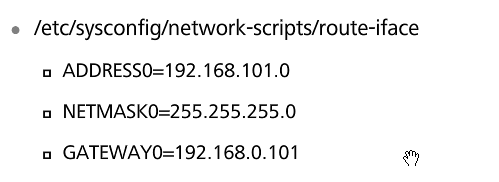
1. 添加静态路由(命令行方式)

route add –net 192.168.101.0 netmask 255.255.255.0 gw 192.168.0.101

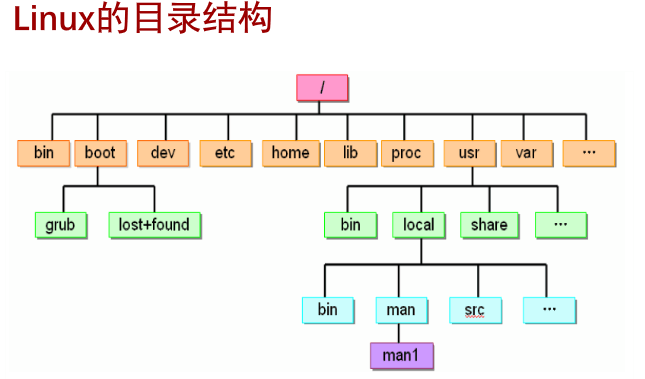


1. 添加静态路由（配置文件方式）

/etc/sysconfig/network-scripts/route-iface



文档07 Linux文件系统层次架构



1. 绝对路径

描述一律从/开始

例如：/home/student/file.txt

特征：路径的描述第一个字符一定是【/】

1. 相对路径

第一个字符不是【/】

描述路径的相对关系

1. 常用文件夹

/etc----配置文件；大部分是\*.conf

/etc/passwd /etc/group /etc/shadowa例外

/home----用户主目录

/root----root用户的主目录

/bin----引导时会使用的一般命令或可执行文件

/sbin----引导时会使用的系统命令或可执行文件

/usr/bin----引导时不使用的一般命令或可执行文件

/usr/sbin----引导时不使用的系统命令或可执行文件

/usr/local//bin----自行安装的一般命令或可执行文件

/usr/local/sbin----自行安装的系统命令或可执行文件

/tmp----临时文件区

/var/tmp----临时文件区

/boot----Boot filesystem;启动加载器；内核及initial ram disk

/dev----设备文件；/dev/sda是硬盘；dev/sda1是分区；

/media----本机硬盘以外的存储设备 例如：/medai/CDROM（光盘）

/mnt----本机以外的存储设备 RedHat习惯将手动挂载放在这里

1. 命令行文件管理

cp 来源 目的

cp /etc/passwd /tmp/passwd

cp /etc/passwd/tmp/.-------[.]相同文件名称

mkdir –p /dirA/dirB--------创建层级的文件夹

rmdir:rmdir /dir1(空文件才可以)；rm –rf /dirA---------删除整个文件夹

1. mv

mv /tmp/passwd /tmp/abc-------更改文件名称

mv /tmp/passwd /var/tmp/passwd---------移动文件，名称不变

mv /tmp/passwd /var/tmp/abc----------移动文件并变更文件名称

01服务器定义及发展史

1. 服务器的概念  
   服务器也是一种计算机，但是运行更快，负载更高，价格更贵。  
   2.服务器的客户机  
   客户机可以时我们直接用的PC机，手机，其他的服务器，ATM机，火车飞机等  
   3.服务器的特性  
   通常不会直接接触，而是通过网络来为我们提供服务  
   高速度的CPU运算能力  
   长时间的可靠运行  
   强大的I/O外部数据吞吐能力  
   更好的可扩展性  
   4.服务器的应用业务  
   银行、企业等核心数据库，关键业务应用系统、基础IT服务业务  
   5.服务器的基础服务业务  
   Email及即时通讯、web服务、虚拟化、文件打印等基础IT服务业务  
   6.工业4.0

信息技术、大数据、物联网成为工业4.0的关键  
第一台电子计算机 1946年  
1964年，IBM推出的第一台大型机system 360，业界第一台服务器，成为真正意义上的服务器。阿波罗11号数据库  
1965年，DEC公司开发了一款小型机PDP-8（不同于现在的小型机）掀起了一场小型机的革命；  
90年代，Unix服务器新概念小型机；通常采用RISC CPU和Unix操作系统；unix server。  
1989年，Inter公司，康柏公司生产了第一台X86服务器（现在成为市场主流，出货量占比98%，销售额占比80%）；  
核心部件CPU一直在遵循摩尔定律进行快速的演进和创新。

02服务器类型

1. 服务器按照外形分类  
   塔式服务器  
   机架式服务器  
   刀片式服务器  
   高密度服务器  
   2.服务器按照CPU数量分类  
   这种分类方法也最常体现到不同厂家服务器类型的分类上，华为的RH2288为两路服务器，RH5885为四路服务器，RH8100为八路服务器  
   一路服务器  
   双路服务器  
   四路服务器  
   多路服务器  
   有的Unix不采用CPU的数量进行分类，而是采用CPU的内核数量进行分类，早期的CPU仅有一个内核，后来的新技术可以将多个内核封装在一个CPU芯片内，性能得到了数倍的提升。  
   3.服务器按照指令集分类  
   RISC精简指令集和CISC复杂指令集CPU  
   采用RISC CPU的服务器通常用于Unix操作系统，国际通常称为Unix服务器，国内称为小型机；  
   X86 CPU则采用的是CISC指令集，采用X86CPU的服务器称为X86服务器   
   4.服务器按照应用分类  
   数据库服务器  
   应用服务器  
   Web服务器  
   接入服务器  
   文件服务器  
   5.服务器发展变化  
   随着服务器的不断地发展，服务器的性能不断的提升，服务器的外形也不断发生着变化，体积不断的缩小，更加的节能省电。从塔式服务器发展为更小的机架式服务器，后来又推出了高密、节能、管理优化的刀片式服务器，性能也增加了许多  
   6. 服务器的硬件组件构成  
   主要包含CPU，内存、硬盘三大组件（成本占服务器的成本的2/3）  
   另外还配置有主板、机箱、电源、风扇等基础的硬件  
   以及RAID卡、网卡等可选用的部件  
   7.主流的服务器的供应商  
   处理IBM、Oracle等厂商的大小型机以外，各厂商的X86服务器都是跟着Intel的产品开发节奏走的。  
   三大件的通用化导致各厂商的服务器在原理上看大体差不多，当然也是各有差异：主要体现在产品的工业化、模块化的设计、RAS特性、可扩展、可管理性差异，以及品牌的服务能力等等。

03服务器技术和架构

1. 服务器技术架构的三大发展趋势  
   Scale-up纵向扩展架构  
   Scale-out横向扩展架构  
   Hyper-converged超融合架构  
   Scale-up纵向扩展架构  
   主要是提升单台服务器的计算性能，主要包括高可靠性、高可用性、高扩展性  
   主要应用于：高性能的交易类业务，如：企业核心交易数据库、关键应用系统以及HPC高性能计算等业务。  
   Scale-up纵向扩展架构应用领域：  
   Scale-up纵向扩展架构被广泛应用于金融交易、电信计费、科学研究、气象分析等领域  
   Scale-out横向扩展架构  
   Scale-out横向扩展架构对单台服务器的要求不高，主要通过更多的服务器来协同完成任务。（以数量取胜）  
   Scale-out横向扩展架构的特点：  
   有高并发性能、低成本、高密度、节能低碳、统一管理  
   应用场所：  
   超大规模型数据中心、大数据扽西、公有云、web应用集群等业务场景。  
   Hyper-converged超融合架构  
   这种架构的理念是将计算、存储、网络和统一管理放在一个盒子里，可以做到开箱即用，一同一个整体的计算解决方案。  
   Hyper-converged超融合架构的特性：  
   高速的整体融合、简单易用、性能优化、消除了系统瓶颈，实现更好的整体的系统效能；（整体优势）  
   应用场合：高性能的数据分析、数据库整合、云计算资源池平台、一体化数据中心  
   2.业务应用和服务器的部署  
   早期是单机应用：在一台服务器上部署了所有的应用软件，为一个或者几个用户提供计算或者业务服务，这种单机系统通常也被称为工作站。  
   C/S应用部署架构：  
   通常有一个集中共享的应用数据库，在使用者的PC机上安装相同或者不同的应用程序。这些应用程序能够操作或者共享应用的数据库，以便实现业务数据的协同操作、应用共享和统一保存。  
   C/S架构的缺点：配置应用和维护比较复杂，软件升级也需要每台客户端逐一的进行升级，你利于应用的灵活部署，不利于大规模的客户应用和推广。  
   B/S架构：即Browse/Server三层模式的应用架构（客户端浏览器、应用服务器，数据库）  
   B/S架构的优点：  
   B/S架构的web客户端使用简单，免维护  
   业务应用软件、数据库系统则可以集中维护、统一部署、统一维护  
   非常适用于大规模的应用系统的部署于服务  
      
   3.服务器互联网应用部署架构  
   互联网业务是典型的B/S架构  
   如今百度等大企业普遍采用大规模分布式的数据库、Hadoop大数据集群、高密Scale-up水平扩展应用、搜索web集群接入的部署架构模式。

04服务器上层软件架构

1.服务器的系统安装和业务部署

服务器之上首先要做安装OS操作系统

Unix服务器操作系统系统有AIX、Solaris、和HP-un11

X86服务器的操作系统主要有Linux和windows操作系统

云计算平台通常要安装：VMvare、FusionSphere、或者KVM等虚拟化系统，虚拟化系统可以将一个物理服务器模拟成多台小的虚拟化服务器来使用。通过服务器的虚拟化能够提供更好的资源使用效率，自动部署和简化管理

1. 主要的服务器数据库

在操作系统上可以按照不同的数据库、中间件、应用业务软件等。

Oracle、IBM DB2、Mysql（开源）、SQL server、SYBASE、以及国产的人大金仓和达梦数据库等

3.主要的服务器的中间件

以java中间件为主，比如webLogical和WebSphere，Tuxedo、东方通等

开源的中间件有：Tomcat、JBoss等

中间件的作用：中间件可以为上层的应用软件提供运行和开发环境，提供预制可复用的业务功能模块，API接口等，帮助用户灵活的、高效的开发和集成复杂的应用系统。

4.主要服务器业务应用

业务应用层软件是面向客户的应用逻辑层软件，如ERP、CRM、HR等应用软件；

业务应用软件通常是基于数据库、中间件等基础结构平台之上。根据客户的需求进行定制开发，最终满足客户业务需求的软件系统。

5.与云计算服务架构对应关系

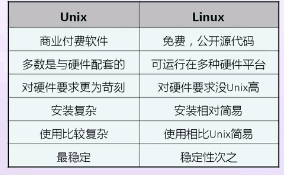
通常来讲包括服务器、存储、网络等硬件基础设施，对应的IaaS云服务层（硬件及服务）。

数据库、中间件通常会对应PaaS云服务层（平台即服务）

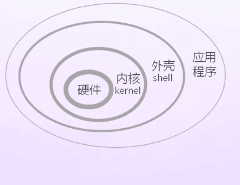
业务应用层软件则会面向SaaS层服务（软件即服务）

05Linux概述

Linux系统概述  
1 Linux的发展：离不开它的前身Unix  
  Unix的发展：  
    1970年，Ken Thompson研发出Unix内核；Unix元年  
    1973年，Ritchie用C语言编写了Unix内核，Unix正式诞生；  
    1974年，Unix对外公布，开始广泛流行。  
  Linux的产生和发展：  
    1986年，Tanenbaum研发出MINIX，并于次年发布；  
    1991年，Linus研发出Linux内核雏形；  
    1994年，Linux 1.0内核发布；  
    1995年以后，各种不同的Linux发行版（red hat）本相继出现。  
  Linux发行版本（内核是一样的）：  
     Redhat 、SUSE Entprise、CentOS：侧重于网络服务，企业管理  
     Debian、Stackware：侧重于服务器及其稳定性  
     Ubuntu、Fedora、Open SUSE：侧重于用户体验  
  Unix和Linux的区别：



2 Linux的结构：



  应用程序：  
  外壳（shell）：用户和内核之间的命令解释器，可以根据自己的需求更换shell。  
     Linux中的shell：Bourne shell（sh）最初使用的，编程号，用户交互做的没有其他的好；C shell（csh）、Korn shell（ksh）  
 内核（kernel）：Linux操作系统的核心,指挥调度Linux的运行，直接控制计算机的资源，保护用户程序不受错综复杂的硬件细节的影响  
  硬件：  
3 Linux的特点：  
  （1）多任务，多用户：CPU时间分片，分给不同的进程；允许多个用户同时登陆使用。  
  （2）管道，功能强大的shell：  管道-前一个程序的输出作为后一个程序的输入，shell是一种解释型高级语言。  
  （3）安全保护机制，稳定性好：防止系统及其数据未经许可而被非法访问；

稳定性Unix好于Linux，Linux好于Windows。  
  （4）用户界面，强大的网络支持：常用命令行的方式，同时提供图形界面；TCP/IP协议就是Linux的缺省网络协议。  
  （5）移植性好：源代码用C语言写成，便于移植到其它计算机上。

06 Linux用户和用户管理组

1.在Linux操作系统中，Linux用户会归属于用户组，那么归属于同一用户组的不同用户，它对一些公共文件具有相同的访问权限，每个用户对它所归属的文件具有其适用的访问权限。

2 Linux通过UID和GID来管理用户和用户组。



UID（User ID）：用户ID，通过配置文件/etc/passwd储存的。

/etc/passwd文件结构：记录的是单个用户的登陆信息。

root:x:0:0:root:/root:/bin/bash 被冒号分成七个字段，分别为用户名、密码、UID、GID、用户描述、用户家目录、用户的shell类型

GID（Group ID）：用户组ID，通过配置文件/etc/group储存的。

/etc/group文件结构：记录GID和用户组组名的对应关系。

root:x:0: root用户组的GID是0

smc:!:1001: smc用户组的GID是1001

3用户管理的常用命令

用户查询命令：

(1) id：查询当前登陆用户的GID和UID。

(2)finger：查询当前用户的属性信息，包含家目录和shell类型。

(3)新增用户：useradd

实例：useradd –d /home/ipcc –m –u 2000 –g mms –s /bin/csh ipcc

Useradd [参数] [用户名]

-d:设置用户家目录

-m：设置的家目录不存在时自动创建

-u：设置用户的UID

-g:设置出事GID或组名

-s:指定用户的shell，如/bin/csh

如果在新增用户时没有指定参数信息，系统就会去读取/etc/default/useradd配置文件，规定了默认的初始用户组和shell等。

如果需要查询基本的设置，通过useradd –D读取默认的配置。

(4)删除userdel ipcc

删除用户：userdel 加上-r，会将用户的家目录一起删除。

(5)设置和修改用户密码：passwd

passwd [用户名]

(6)修改用户属性：usermod

-d修改用户家目录 -g修改初始用户组

4用户组管理常用命令

(1)新增用户组：groupadd

-g指定组ID

例如：groupadd ipcc

groupadd –g 2000 iptv

(2)删除用户组：groupdel

(3)修改用户组：groupmod

-g修改组ID -n修改组名

例如：groupmod –g 2500 –n ipcc1 ipcc

07 Linux文件和目录管理

1 Linux的文件结构类似于倒树形结构。  
根目录下的子目录以及存放的内容：  
绝对路径：由根目录（/）开始写起的文件名或者目录名。  
相当路径：基于当前路径的的文件名或者目录名写法，.代表当前目录  ..代表上一级目录。  
2 文件和目录的基本操作  
  显示当前的工作目录：pwd  
  变更工作目录：cd  cd后面不跟任何路径，则是回到当前目录的家目录。  
  新增目录：mkdir  -m指定存取模式  -p建立目录时建立其所有不存在的父目录。

例如：mkdir temp

mkdir –m 777 temp/abc  
  删除目录：rmdir 删除空目录，如果删除非空目录，rm即可， –p删除目录及父目录  
 复制文件或目录 ：cp+源文件或目录+目的文件或目录  
 移动文件或目录：mv +源文件或目录+目的文件或目录  
 删除文件或目录：rm+文件或目录

rm –i:系统会提示是否执行删除操作  
 查找文件或目录：find +路径+参数   -name以指定字符串开头的文件名  -user 查找指定用户所拥有的文件。  
 查看文件内容：  
  cat：直接查阅文件内容，不能翻页  
  more：翻页查看文件内容  
  less：翻页阅读，和more类似。但操作按键比more更加丰富。  
  head：查看文档的前面几行内容，默认为10行 可以-+数字看特定行数  
  tail：查看文件的后面几行内容，默认为10行

08 文件系统管理

1文件系统的概念：操作系统用于明确存储和组织计算机数据的方法。使得对数据的查找和访问变得更加容易。

2存储在介质中数据的三个因素

文件名：定位存储的位置

数据：文件的具体内容

元数据meta-data：文件有关的信息。例如文件的权限、所有者、文件的修改时间等。

Linux支持的文件系统类型可查看/etc/filesystems

3文件系统的分类

是否有日志？

传统型文件系统：写入文件内容的时候，先写数据，再写元数据。ext2文件系统（默认的）

日志型文件系统：写入文件内容的时候，先写日志记录文件（更安全）。 ext3=ext2+日志功能

ReiserFS基于平衡树，搜索快、节约空间

如何查找数据？

索引式文件系统：文件属性数据和实际内容放在不同的区块，例如Linux中默认的ext2中，文件属性数据存放在inode（类似于指针），实际内容放在block。

非索引式文件系统：只有block，数据需要一个block接一个block读取（下一个block位置存放在上一个block中），效率低。 FAT

碎片整理：就是写入的数据的block太过分散，此时读取的效率会很低。磁盘整理的目的就是将这些分散的block尽量的集中起来。

默认文件系统ext2的结构：在格式化的时候是区分了多个群组的，每个群组有独立的inode和data block和super block，一开始就将inode和data block规划好了

4配置文件系统分区

（1）创建分区：fdisk+设备名，输入完该命令之后，可以通过参数m查看按键操作说明，通过参数p可以得到本磁盘的相关信息，输入n命令可以新建一个分区。使用完n之后，新建分区的步骤如下：

选择分区类型

选择分区开始的磁柱

决定分区的大小

保存新建的分区 w

通过重启服务器或使用partprobe命令通知内核，更改

（2）创建文件系统：mkfs 参数 设备名

-t指定文件系统类型 如ext3;-b指定block大小，单位bytes，ext2和ext3仅支持1024/2048/4096三种。

（3）挂载文件系统：挂载的过程就是将文件系统和目录树上的某一个目录结合。mount+设备名+挂载点

-t指定文件系统类型 如ext3;-b指定block大小，单位bytes，

5管理Linux文件系统  
（1）查看分区使用情况：  
 df：查看文件系统的磁盘空间占用情况

–h以容易理解的格式打印出文件系统大小

–i显示inode信息而非块使用量。

du：查看文件或目录的磁盘使用空间

–a显示目录下的每个文件所占的磁盘空间

–s只显示大小的总和

-h以容易理解的格式输出文件大小值  
（2）查看系统打开的文件：lsof  
   lsof filename显示打开指定文件的所有进程  
   lsof –c string显示以指定字符开头的进程所有打开的文件  
   lsof –u username显示所属user相关进程打开的文件  
（3）修复文件系统：  
   fsck检查文件系统并尝试修复错误。

执行fsck时，必须将要修复的设备进行umount后，再执行fsck命令。

语法：fsck [参数] [设备名称]，例如：fsck –f /dev/sda6 (用于修复磁盘的逻辑错误)  
   e2fsck：检查和修复ext2和ext3文件系统

文件系统的损坏可能是由于superblock的损坏导致的

通过dumpe2fs查看superblock备份的位置，看到备份位置之后，就可以通过备份的superblock来恢复数据

dumpe2fs /dev/sdb 1 |grep superblock

e2fsck –f –b 32768 /dev/sda6

09 Linux LVM配置

1. LVM原理

Logical volume manager，是建立在硬盘和分区之间的一个逻辑层，用来提高磁盘分区管理的灵活性。

在传统的存储模型中，文件系统是直接构建在物理分区之上的，物理分区的大小决定了其上文件系统的存储容量，调整文件系统的存储容量变得比较繁琐。

LVM设计的主要目标是实现文件系统存储容量可扩展性，使对容量的调整更简易

1. LVM架构

物理分区：pp-physical partition，可以是硬盘的分区或者是read分区

物理卷：PV-physical volume,是pp的LVM抽象，维护了pp的结构信息，是组成VG的基本逻辑单元，一般一个PV对应一个pp

物理扩展单元：PE-physical extends，每个PV都会以pe为基本单元划分，是lvm的最小存储单元；

卷组：vg-volume group,由一个或者数个PV组成，可以看做LVM组合起来的大磁盘

逻辑扩展单元：LE-logical extends，组成LV的基本单元，一个LE对应一个pe

逻辑卷：LV-logical volume，建立在VG之上，文件系统之下，由若干个LE组成，文件系统是基于逻辑卷的。

1. VG、LV、PE的关系

LVM是通过交换pe来达到弹性变更文件系统的大小；

想扩增VG的容量则可以通过增加PV的方式；

一般LVM默认的pe的大小是4M，最多有65534个pe，所以LVM的VG最大为256G；

LV和磁盘的dev/sda2分区类似，是用来格式化的单位。当对LV进行写入操作时LVM定位相应的LE，通过PV头部的映射表将数据写入到相应的PE上。

LV实现的关键在于PE和LE之间建立的映射关系，不同的映射规则决定了不同的LVM存储模型。

1. LVM优点

文件系统可以跨多个磁盘

动态地扩展文件系统大小

增加新磁盘到LVM的存储池中

1. 使用LVM的要点

按需分配文献系统的大小

把不同的数据放在不同的卷组中

1. LVM的配置流程

首先通过fdisk将systernID修改为LVM标记，再通过pvcreat将Linux分区处理成物理卷pv，接下来通过vgcreate将创建好的物理卷处理成卷组vg，再通过lvcreate将卷组分成若干个逻辑卷LV，再通过mkfs工具将LV格式化，最后挂载格式化后的LV到文件系统

1. 物理卷管理

pvcreate创建物理卷

将普通的分区加上pv属性

例如将分区/dev/sda6创建为物理卷：pvcreate /dev/sda6

pvremove删除物理卷(语法和pvcreat一致)

pvscan查看物理卷信息

pvdisplay查看各个物理卷的详细参数

1. 卷组管理命令

vgcreate 创建卷组

vgscan 查看卷组信息

vgdisplay 查看卷组的详细参数

vgreduce 缩小卷组，把物理卷从卷组中删除

vgextend 扩展卷组，把某个物理卷添加到卷组中

vgremove 删除卷组

1. 逻辑卷管理

lvcreate创建逻辑卷

lvscan 查看逻辑卷的信息

lvdisplay查看逻辑卷的具体参数

lvextend增大逻辑卷的大小

lvreduce减小逻辑卷的大小

lvremove 删除逻辑卷

1. 管理文献系统空间

增大文件系统空间步骤：

先卸载逻辑卷

然后通过vgentend,lvextend等命令增大lv的空间

再使用resize2fs将逻辑卷容量增加

最后将逻辑卷挂载到目录树

缩小文件系统空间步骤：

先卸载逻辑卷

使用resize2fs将逻辑卷容量减小

然后通过vgreduce,lvreduce等命令减小lv的空间

最后将逻辑卷挂载到目录树

10 Linux网络管理

1. 查询和配置网口

（1） 查看网口的配置

ifconfig [网口]

查看IP地址、广播地址和掩码

（2） 修改网口配置

ifconfig 网口 [参数]

设置网口的参数，如IP、广播地址、掩码

重启网络服务或操作系统后失效

例如：ifconfig eth3 192.168.100.128 broadcast 192.168.100.255 netmask 255.255.255.0

（3）使配置长期有效（修改配置文件）

/etc/sysconfig/network/ifcg-[网口]

编辑配置文件配置网口

使用ifup命令，启动网口

例如：vi ifcfg-eth4

ifup ifcfg-eth4

2. 查询和配置路由

（1）查询路由表

route

用于查询本机路由表

8个字段 ：

Destination:目的的网关或者目的的主机（default表示是默认路由）Geteway:网关； Genmask：网段的掩码； Flags:标记（U表示路由是可用的，若是G则表示是一个getway需要网关转发，若是H-host代表目的地只是一个主机）；iface表示该路由的出口。

（2）新增路由

route add [-net|-host] [netmaskNm] [gw Gw] [[dev] if]

新增路由数据保存在内存中，系统重启失效

例如：route add –net 192.168.101.0 netmask 255.255.255.0 gw 192.168.0.101

route add –net 192.168.101.0 netmask 255.255.255.0 dev eth3

使配置长期有效（修改配置文件/etc/sysconfig/network/routes）需要重启网络服务才能生效

3. 网络侦测

（1）ping

检测对端网络是否可达，或者网络连接速度

ping [参数] 目的地址

-c：后接执行ping的次数

例如：ping –c 5 10.77.215.5

（2）traceroute

侦测数据包从源到目的所经过的路由

traceroute<地址或主机名>

4. 配置常用网络服务

（1）配置FTP服务FTP 是File Transfer Protocol（文件传输协议）的英文简称 yast命令？

（a）检查安装vsftpd软件

使用命令#rpm -qa |grep vsftpd可以检测出是否安装了vsftpd软件，

如果没有安装，使用yum命令进行安装:yum install vsftpd –y

（b）启动服务

使用vsftpd软件，主要包括如下几个命令：

启动ftp命令#service vsftpd start

停止ftp命令#service vsftpd stop

重启ftp命令#service vsftpd restart

（c）vsftpd的配置

ftp的配置文件主要有三个，位于/etc/vsftpd/目录下，分别是：

ftpusers    该文件用来指定那些用户不能访问ftp服务器。

user\_list   该文件用来指示的默认账户在默认情况下也不能访问ftp

vsftpd.conf   vsftpd的主配置文件

（d）以匿名用户为例，我们去掉配置文件vsftpd.conf 里面以下

anon\_upload\_enable=YES

anon\_mkdir\_write\_enable=YES

两项前面的#号，就可以完成匿名用户的配置，此时匿名用户既可以登录上传、下载文件，修改配置文件后需要重启服务。

（2）配置telnet服务

（a）安装telnet服务

#  rpm -ivh telnet-server-0.17-47.el6\_3.1.x86\_64.rpm

安装完成后会在/etc/xinetd.d/文件夹下生成一个telnet文件

（b）编辑设置 /etc/xinetd.d/telnet

将disable= yes设置成disable= no

（c）启动telnet服务

# service  xinetd restart

（d）设置telnet服务自启动

# chkconfig  telnet on

（e）设置root用户远程登录telnet服务。

# echo  'pts/0'  >>/etc/securetty

# echo 'pts/1' >>/etc/securetty

完成后重启telnet服务

# service  xinetd  restart

（f）修改防火墙设置，开放23端口通过。

编辑/etc/sysconfig/iptables文件，添加如下一行内容

-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT。

（h）重启防火墙

# service iptables restart

11进程和任务管理

1. 进程管理

程序：文件中保存的一系列可执行命令

进程：加载内存中的程序，由CPU运行

守护进程：常驻内存，与终端无关的系统进程

用户进程：用户通过终端加载的进程。

系统中的每一个进程都有一个进程号---pid;pid=1的进程是init进程，是系统启动的第一个进程。

查看进程

（a）ps静态查看某一时间点进程信息

常用参数 a显示现行终端机下的所有程序

x显示所有程序，不以终端机来区分

u以用户为主的格式显示程序状况

f用ASCII字符显示树状结构

（b）top连续观察进程动态

默认3秒刷新一次，并按照CPU使用率的高到低排序

（c）pstree用ASCII字符显示树状结构，清楚表达进程间的相互关系

-p显示进程ID

-u显示用户名称

结束进程

（a）kill

结束进程和进程号PID，系统可能忽略

kill -9 PID 强制终止进程

（b）killall

终止同一进程组内的所有进程

kill httpd

2. 任务管理

任务：登陆系统取得shell后，在单一终端接口下启动的进程

前台：在终端接口上，可以出现提示符让用户操作的环境

后台：不显示终端接口的环境

任务管理意义是多项任务并行执行

相关命令（a）&

直接将程序放入后台处理

如 find /-name smcapp &

（b）jobs

查看当前shell的后台任务

（c）ctrl+z

将正在运行的任务放入后台暂停

（d）fg %[jobID]

将任务放入前台执行

（e）bg %[jobID]

将任务放入后台执行，不加jobID表示对当前任务

周期任务管理

crontab [-u usre] [-e | -l| -r ]

-u：指定用户

-e:编辑crontab的内容

-l:查询crontab的内容

-r：移除所有的crontab任务内容

使用crontab –e编辑时，程序会直接调用vi接口，程序路径是/use/sbin/cron；

系统计划任务保存在/etc/crontab中；

/var/spood/crontab/tabs下面有对应用户名的crontab，对应用户级别的任务配置；

/var/crontab对应系统级别的任务配置；

管理定时任务

at安排一个任务在未来执行，必须先启动atd进程

通过ps -1f | grep atd查看进程是否启动

at –l:相当于atq，列出当前at任务

at-d [jobID]：相当于atrm，删除一个at任务

at-c [jobID]：查看任务的具体内容

at使用方法：

at HH:MM ----今天的HH：MM执行

at HH：MM YYYY-MM-DO----指定具体的执行日期和时间

at now +number [minutes |hours |days |weeks]----当前时间往后多久执行

at HH:MM + number[minutes |hours |days |weeks]----某个时间点+分钟|小时|天|星期执行

例如：at 14:32 2015-10-01

再加上ctrl D来保存，出现EOT说明任务保存成功

12 Linux系统监控

1. 系统是否正常启动

未显示的信息会保存在Kernel Ring Buffer中，可以用dmesg显示存在里面的开机信息，可利用dmesg|less查看；当系统完成启动后启动信息会被写入/var/log/boot.msg里

2. 监控系统硬件信息

（1）cat /proc/…

系统硬件信息保存在/proc下的文件中

/proc/cpuinfo:cpu的信息

/proc/devices:已经加载的设备信息

/proc/bus:系统总线信息

/proc/scsi :scsi设备信息

/proc/net：网卡设备信息

（2）hwinfo显示所有硬件相关信息

--disk显示磁盘信息

--cpu显示CPU信息

--memory显示内存信息

--network显示网卡信息

--short显示硬件的摘要信息

例如：hwinfo --disk

（3）fdisk查看硬盘信息

-l查看服务器所挂载硬盘个数及分区情况

（4）iostat查询CPU和磁盘IO的统计信息

-c仅显示CPU统计信息

-d仅显示磁盘统计信息

-k以k为单位显示每秒的磁盘请求数

（5）lspci列出所有PCI设备

-v显示PCI接口装置的详细信息

-vv比-v更详细的信息

3. 监控系统和进程

（1）ps显示当前进程的状态（静态）-ef

（2）top显示进程的动态（正在使用的CPU内存信息）

（3）uptime查看系统已经开机的时间以及系统平均负载

显示依次是： 现在时间、系统已经开机时间、目前有多少登陆用户、系统在过去的1分钟、5分钟、15分钟的平均负载

（4）uname系统版本相关信息

-a详细信息

（5）netstat检验本机网络端口

4. 监控用户登陆信息

（1）who查看当前登陆的用户

-H显示各栏位的标题信息列

-m效果同who am i，显示出自己在系统的用户名，登陆终端，登陆时间

（2）w [参数] [用户]

查看当前登陆的用户及用户当前的工作，比who详细

-u后接user，查看具体用户信息

（3）finger [参数] [用户]

查看用户详细信息

-s短格式显示用户信息

-l长格式显示用户信息

（4）last [参数]

查看曾经登陆过系统的用户

-n num:设置列出名单的显示列数

-F 显示登陆和登出的详细信息

（5）lastlog [参数] [用户]

查看用户前一次登陆的信息

-t days:查看距今n天内登陆了系统的用户的最近一次登陆信息

-u 显示登陆和登出的详细信息

系统负载如何；系统是否有非法用户登陆