1、什么是运维？什么是游戏运维？

1）运维是指大型组织已经建立好的网络软硬件的维护，就是要保证业务的上线与运作的正常， 在他运转的过程中，对他进行维护，他集合了网络、系统、数据库、开发、安全、监控于一身的技术 运维又包括很多种，有DBA运维、网站运维、虚拟化运维、监控运维、游戏运维等等

2）游戏运维又有分工，分为开发运维、应用运维（业务运维）和系统运维 开发运维：是给应用运维开发运维工具和运维平台的 应用运维：是给业务上线、维护和做故障排除的，用开发运维开发出来的工具给业务上线、维护、做故障排查 系统运维：是给应用运维提供业务上的基础设施，比如：系统、网络、监控、硬件等等

总结：开发运维和系统运维给应用运维提供了“工具”和“基础设施”上的支撑 开发运维、应用运维和系统运维他们的工作是环环相扣的

2、在工作中，运维人员经常需要跟运营人员打交道，请问运营人员是做什么工作的？ 游戏运营要做的一个事情除了协调工作以外 还需要与各平台沟通，做好开服的时间、开服数、用户导量、活动等计划

3、现在给你三百台服务器，你怎么对他们进行管理？ 管理3百台服务器的方式： 1）设定跳板机，使用统一账号登录，便于安全与登录的考量。 2）使用salt、ansiable、puppet进行系统的统一调度与配置的统一管理。 3）建立简单的服务器的系统、配置、应用的cmdb信息管理。便于查阅每台服务器上的各种信息记录。

4、简述raid0 raid1 raid5 三种工作模式的工作原理及特点

RAID，可以把硬盘整合成一个大磁盘，还可以在大磁盘上再分区，放数据 还有一个大功能，多块盘放在一起可以有冗余（备份） RAID整合方式有很多，常用的：0 1 5 10

RAID 0，可以是一块盘和N个盘组合

其优点读写快，是RAID中最好的

缺点：没有冗余，一块坏了数据就全没有了

RAID 1，只能2块盘，盘的大小可以不一样，以小的为准

10G+10G只有10G，另一个做备份。它有100%的冗余，缺点：浪费资源，成本高

RAID 5 ，3块盘，容量计算10*（n-1）,损失一块盘

特点，读写性能一般，读还好一点，写不好

冗余从好到坏：RAID1 RAID10 RAID 5 RAID0 性能从好到坏：RAID0 RAID10 RAID5 RAID1 成本从低到高：RAID0 RAID5 RAID1 RAID10

单台服务器：很重要盘不多，系统盘，RAID1 数据库服务器：主库：RAID10 从库 RAID5\RAID0（为了维护成本，RAID10） WEB服务器，如果没有太多的数据的话，RAID5,RAID0（单盘） 有多台，监控、应用服务器，RAID0 RAID5

我们会根据数据的存储和访问的需求，去匹配对应的RAID级别

5、LVS、Nginx、HAproxy有什么区别？工作中你怎么选择？ LVS： 是基于四层的转发 HAproxy： 是基于四层和七层的转发，是专业的代理服务器 Nginx： 是WEB服务器，缓存服务器，又是反向代理服务器，可以做七层的转发

区别： LVS由于是基于四层的转发所以只能做端口的转发 而基于URL的、基于目录的这种转发LVS就做不了

工作选择：

HAproxy和Nginx由于可以做七层的转发，所以URL和目录的转发都可以做 在很大并发量的时候我们就要选择LVS，像中小型公司的话并发量没那么大 选择HAproxy或者Nginx足已，由于HAproxy由是专业的代理服务器 配置简单，所以中小型企业推荐使用HAproxy

6、Squid、Varinsh和Nginx有什么区别，工作中你怎么选择？ Squid、Varinsh和Nginx都是代理服务器

什么是代理服务器： 能当替用户去访问公网，并且能把访问到的数据缓存到服务器本地，等用户下次再访问相同的资 源的时候，代理服务器直接从本地回应给用户，当本地没有的时候，我代替你去访问公网，我接 收你的请求，我先在我自己的本地缓存找，如果我本地缓存有，我直接从我本地的缓存里回复你 如果我在我本地没有找到你要访问的缓存的数据，那么代理服务器就会代替你去访问公网

区别： 1）Nginx本来是反向代理/web服务器，用了插件可以做做这个副业

但是本身不支持特性挺多，只能缓存静态文件 2）从这些功能上。varnish和squid是专业的cache服务，而nginx这些是第三方模块完成 3）varnish本身的技术上优势要高于squid，它采用了可视化页面缓存技术

在内存的利用上，Varnish比Squid具有优势，性能要比Squid高。 还有强大的通过Varnish管理端口，可以使用正则表达式快速、批量地清除部分缓存 它是内存缓存，速度一流，但是内存缓存也限制了其容量，缓存页面和图片一般是挺好的 4）squid的优势在于完整的庞大的cache技术资料，和很多的应用生产环境

工作中选择： 要做cache服务的话，我们肯定是要选择专业的cache服务，优先选择squid或者varnish。

7、Tomcat和Resin有什么区别，工作中你怎么选择？ 区别：Tomcat用户数多，可参考文档多，Resin用户数少，可考虑文档少 最主要区别则是Tomcat是标准的java容器，不过性能方面比resin的要差一些 但稳定性和java程序的兼容性，应该是比resin的要好

工作中选择：现在大公司都是用resin，追求性能；而中小型公司都是用Tomcat，追求稳定和程序的兼容

8、什么是中间件？什么是jdk？ 中间件介绍： 中间件是一种独立的系统软件或服务程序，分布式应用软件借助这种软件在不同的技术之间共享资源 中间件位于客户机/ 服务器的操作系统之上，管理计算机资源和网络通讯 是连接两个独立应用程序或独立系统的软件。相连接的系统，即使它们具有不同的接口

但通过中间件相互之间仍能交换信息。执行中间件的一个关键途径是信息传递 通过中间件，应用程序可以工作于多平台或OS环境。

jdk：jdk是Java的开发工具包 它是一种用于构建在 Java 平台上发布的应用程序、applet 和组件的开发环境

9、讲述一下Tomcat8005、8009、8080三个端口的含义？ 8005》 关闭时使用 8009》 为AJP端口，即容器使用，如Apache能通过AJP协议访问Tomcat的8009端口 8080==》 一般应用使用

10、什么叫CDN？ - 即内容分发网络 - 其目的是通过在现有的Internet中增加一层新的网络架构，将网站的内容发布到 最接近用户的网络边缘，使用户可就近取得所需的内容，提高用户访问网站的速度

11、什么叫网站灰度发布？ 灰度发布是指在黑与白之间，能够平滑过渡的一种发布方式 AB test就是一种灰度发布方式，让一部用户继续用A，一部分用户开始用B 如果用户对B没有什么反对意见，那么逐步扩大范围，把所有用户都迁移到B上面 来 灰度发布可以保证整体系统的稳定，在初始灰度的时候就可以发现、调整问题，以保证其影响度

12、简述DNS进行域名解析的过程？ 用户要访问www.baidu.com，会先找本机的host文件，再找本地设置的DNS服务器，如果也没有的话，就去网络中找根服务器，根服务器反馈结果，说只能提供一级域名服务器.cn，就去找一级域名服务器，一级域名服务器说只能提供二级域名服务器.com.cn,就去找二级域名服务器，二级域服务器只能提供三级域名服务器.baidu.com.cn，就去找三级域名服务器，三级域名服务器正好有这个网站www.baidu.com，然后发给请求的服务器，保存一份之后，再发给客户端

13、RabbitMQ是什么东西？ RabbitMQ也就是消息队列中间件，消息中间件是在消息的传息过程中保存消息的容器消息中间件再将消息从它的源中到它的目标中标时充当中间人的作用 队列的主要目的是提供路由并保证消息的传递；如果发送消息时接收者不可用 消息队列不会保留消息，直到可以成功地传递为止，当然，消息队列保存消息也是有期限地

14、讲一下Keepalived的工作原理？ 在一个虚拟路由器中，只有作为MASTER的VRRP路由器会一直发送VRRP通告信息, BACKUP不会抢占MASTER，除非它的优先级更高。当MASTER不可用时(BACKUP收不到通告信息) 多台BACKUP中优先级最高的这台会被抢占为MASTER。这种抢占是非常快速的(<1s)，以保证服务的连续性 由于安全性考虑，VRRP包使用了加密协议进行加密。BACKUP不会发送通告信息，只会接收通告信息

15、讲述一下LVS三种模式的工作过程？ LVS 有三种负载均衡的模式，分别是VS/NAT（ nat 模式） VS/DR(路由模式) VS/TUN（隧道模式）

一、NAT模式（VS-NAT）

原理：就是把客户端发来的数据包的IP头的目的地址，在负载均衡器上换成其中一台RS的IP地址

并发至此RS来处理,RS处理完后把数据交给负载均衡器,负载均衡器再把数据包原IP地址改为自己的IP

将目的地址改为客户端IP地址即可期间,无论是进来的流量,还是出去的流量,都必须经过负载均衡器

优点：集群中的物理服务器可以使用任何支持TCP/IP操作系统，只有负载均衡器需要一个合法的IP地址

缺点：扩展性有限。当服务器节点（普通PC服务器）增长过多时,负载均衡器将成为整个系统的瓶颈

因为所有的请求包和应答包的流向都经过负载均衡器。当服务器节点过多时

大量的数据包都交汇在负载均衡器那，速度就会变慢！

二、IP隧道模式（VS-TUN）

原理：首先要知道，互联网上的大多Internet服务的请求包很短小，而应答包通常很大

那么隧道模式就是，把客户端发来的数据包，封装一个新的IP头标记(仅目的IP)发给RS

RS收到后,先把数据包的头解开,还原数据包,处理后,直接返回给客户端,不需要再经过

负载均衡器。注意,由于RS需要对负载均衡器发过来的数据包进行还原,所以说必须支持

IPTUNNEL协议，所以,在RS的内核中,必须编译支持IPTUNNEL这个选项

优点：负载均衡器只负责将请求包分发给后端节点服务器，而RS将应答包直接发给用户

所以，减少了负载均衡器的大量数据流动，负载均衡器不再是系统的瓶颈，就能处理很巨大的请求量

这种方式，一台负载均衡器能够为很多RS进行分发。而且跑在公网上就能进行不同地域的分发。

缺点：隧道模式的RS节点需要合法IP，这种方式需要所有的服务器支持"IP Tunneling"

(IP Encapsulation)协议，服务器可能只局限在部分Linux系统上

三、直接路由模式（VS-DR）

原理：负载均衡器和RS都使用同一个IP对外服务但只有DR对ARP请求进行响应

所有RS对本身这个IP的ARP请求保持静默也就是说,网关会把对这个服务IP的请求全部定向给DR

而DR收到数据包后根据调度算法,找出对应的RS,把目的MAC地址改为RS的MAC（因为IP一致）

并将请求分发给这台RS这时RS收到这个数据包,处理完成之后，由于IP一致，可以直接将数据返给客户

则等于直接从客户端收到这个数据包无异,处理后直接返回给客户端

由于负载均衡器要对二层包头进行改换,所以负载均衡器和RS之间必须在一个广播域

也可以简单的理解为在同一台交换机上

优点：和TUN（隧道模式）一样，负载均衡器也只是分发请求，应答包通过单独的路由方法返回给客户端

与VS-TUN相比，VS-DR这种实现方式不需要隧道结构，因此可以使用大多数操作系统做为物理服务器。

缺点：（不能说缺点，只能说是不足）要求负载均衡器的网卡必须与物理网卡在一个物理段上。

16、mysql的innodb如何定位锁问题，mysql如何减少主从复制延迟？

mysql的innodb如何定位锁问题: 在使用 show engine innodb status检查引擎状态时，发现了死锁问题 在5.5中，information_schema 库中增加了三个关于锁的表（MEMORY引擎）

innodb_trx ## 当前运行的所有事务

innodb_locks ## 当前出现的锁

innodb_lock_waits ## 锁等待的对应关系

mysql如何减少主从复制延迟: 如果延迟比较大，就先确认以下几个因素： \1. 从库硬件比主库差，导致复制延迟 \2. 主从复制单线程，如果主库写并发太大，来不及传送到从库

就会导致延迟。更高版本的mysql可以支持多线程复制 \3. 慢SQL语句过多 \4. 网络延迟

\5. master负载 主库读写压力大，导致复制延迟，架构的前端要加buffer及缓存层

\6. slave负载 一般的做法是，使用多台slave来分摊读请求，再从这些slave中取一台专用的服务器

只作为备份用，不进行其他任何操作.另外， 2个可以减少延迟的参数: –slave-net-timeout=seconds 单位为秒 默认设置为 3600秒

#参数含义：当slave从主数据库读取log数据失败后，等待多久重新建立连接并获取数据 –master-connect-retry=seconds 单位为秒 默认设置为 60秒

#参数含义：当重新建立主从连接时，如果连接建立失败，间隔多久后重试 通常配置以上2个参数可以减少网络问题导致的主从数据同步延迟

MySQL数据库主从同步延迟解决方案 最简单的减少slave同步延时的方案就是在架构上做优化，尽量让主库的DDL快速执行

还有就是主库是写，对数据安全性较高，比如sync_binlog=1，innodb_flush_log_at_trx_commit = 1 之类的设置，而slave则不需要这么高的数据安全，完全可以讲sync_binlog设置为0或者关闭binlog

innodb_flushlog也可以设置为0来提高sql的执行效率。另外就是使用比主库更好的硬件设备作为slave

17、如何重置mysql root密码？

一、 在已知MYSQL数据库的ROOT用户密码的情况下，修改密码的方法：

1、 在SHELL环境下，使用mysqladmin命令设置：

mysqladmin –u root –p password “新密码” 回车后要求输入旧密码

2、 在mysql>环境中,使用update命令，直接更新mysql库user表的数据：

Update mysql.user set password=password(‘新密码’) where user=’root’;

flush privileges;

注意：mysql语句要以分号”；”结束

3、 在mysql>环境中，使用grant命令，修改root用户的授权权限。

grant all on . to root@’localhost’ identified by ‘新密码’；

二、 如查忘记了mysql数据库的ROOT用户的密码，又如何做呢？方法如下：

1、 关闭当前运行的mysqld服务程序：service mysqld stop（要先将mysqld添加为系统服务）

2、 使用mysqld_safe脚本以安全模式（不加载授权表）启动mysqld 服务

/usr/local/mysql/bin/mysqld_safe --skip-grant-table &

3、 使用空密码的root用户登录数据库，重新设置ROOT用户的密码

＃mysql -u root

Mysql> Update mysql.user set password=password(‘新密码’) where user=’root’;

Mysql> flush privileges;

18、lvs/nginx/haproxy优缺点

Nginx的优点是：

1、工作在网络的7层之上，可以针对http应用做一些分流的策略，比如针对域名、目录结构

它的正则规则比HAProxy更为强大和灵活，这也是它目前广泛流行的主要原因之一

Nginx单凭这点可利用的场合就远多于LVS了。

2、Nginx对网络稳定性的依赖非常小，理论上能ping通就就能进行负载功能，这个也是它的优势之一

相反LVS对网络稳定性依赖比较大，这点本人深有体会；

3、Nginx安装和配置比较简单，测试起来比较方便，它基本能把错误用日志打印出来

LVS的配置、测试就要花比较长的时间了，LVS对网络依赖比较大。

4、可以承担高负载压力且稳定，在硬件不差的情况下一般能支撑几万次的并发量，负载度比LVS相对小些。

5、Nginx可以通过端口检测到服务器内部的故障，比如根据服务器处理网页返回的状态码、超时等等，并且会把返回错误的请求重新提交到另一个节点，不过其中缺点就是不支持url来检测。比如用户正在上传一个文件，而处理该上传的节点刚好在上传过程中出现故障，Nginx会把上传切到另一台服务器重新处理，而LVS就直接断掉了

如果是上传一个很大的文件或者很重要的文件的话，用户可能会因此而不满。

6、Nginx不仅仅是一款优秀的负载均衡器/反向代理软件，它同时也是功能强大的Web应用服务器

LNMP也是近几年非常流行的web架构，在高流量的环境中稳定性也很好。

7、Nginx现在作为Web反向加速缓存越来越成熟了，速度比传统的Squid服务器更快，可考虑用其作为反向代理加速器

8、Nginx可作为中层反向代理使用，这一层面Nginx基本上无对手，唯一可以对比Nginx的就只有lighttpd了

不过lighttpd目前还没有做到Nginx完全的功能，配置也不那么清晰易读，社区资料也远远没Nginx活跃

9、Nginx也可作为静态网页和图片服务器，这方面的性能也无对手。还有Nginx社区非常活跃，第三方模块也很多

Nginx的缺点是：

1、Nginx仅能支持http、https和Email协议，这样就在适用范围上面小些，这个是它的缺点

2、对后端服务器的健康检查，只支持通过端口来检测，不支持通过url来检测

不支持Session的直接保持，但能通过ip_hash来解决

LVS：使用Linux内核集群实现一个高性能、高可用的负载均衡服务器

它具有很好的可伸缩性（Scalability)、可靠性（Reliability)和可管理性（Manageability)

LVS的优点是：

1、抗负载能力强、是工作在网络4层之上仅作分发之用，没有流量的产生

这个特点也决定了它在负载均衡软件里的性能最强的，对内存和cpu资源消耗比较低

2、配置性比较低，这是一个缺点也是一个优点，因为没有可太多配置的东西

所以并不需要太多接触，大大减少了人为出错的几率

3、工作稳定，因为其本身抗负载能力很强，自身有完整的双机热备方案

如LVS+Keepalived，不过我们在项目实施中用得最多的还是LVS/DR+Keepalived

4、无流量，LVS只分发请求，而流量并不从它本身出去，这点保证了均衡器IO的性能不会收到大流量的影响。

5、应用范围较广，因为LVS工作在4层，所以它几乎可对所有应用做负载均衡，包括http、数据库、在线聊天室等

LVS的缺点是：

1、软件本身不支持正则表达式处理，不能做动静分离

而现在许多网站在这方面都有较强的需求，这个是Nginx/HAProxy+Keepalived的优势所在

2、如果是网站应用比较庞大的话，LVS/DR+Keepalived实施起来就比较复杂了

特别后面有Windows Server的机器的话，如果实施及配置还有维护过程就比较复杂了

相对而言，Nginx/HAProxy+Keepalived就简单多了。

HAProxy的特点是：

1、HAProxy也是支持虚拟主机的。

2、HAProxy的优点能够补充Nginx的一些缺点，比如支持Session的保持，Cookie的引导

同时支持通过获取指定的url来检测后端服务器的状态

3、HAProxy跟LVS类似，本身就只是一款负载均衡软件

单纯从效率上来讲HAProxy会比Nginx有更出色的负载均衡速度，在并发处理上也是优于Nginx的

4、HAProxy支持TCP协议的负载均衡转发，可以对MySQL读进行负载均衡

对后端的MySQL节点进行检测和负载均衡，大家可以用LVS+Keepalived对MySQL主从做负载均衡

5、HAProxy负载均衡策略非常多，HAProxy的负载均衡算法现在具体有如下8种：

①roundrobin，表示简单的轮询，这个不多说，这个是负载均衡基本都具备的；

② static-rr，表示根据权重，建议关注；

③leastconn，表示最少连接者先处理，建议关注；

④ source，表示根据请求源IP，这个跟Nginx的IP_hash机制类似

我们用其作为解决session问题的一种方法，建议关注；

⑤ri，表示根据请求的URI；

⑥rl_param，表示根据请求的URI参数'balance url_param' requires an URL parameter name；

⑦hdr(name)，表示根据HTTP请求头来锁定每一次HTTP请求；

⑧rdp-cookie(name)，表示根据据cookie(name)来锁定并哈希每一次TCP请求。

19、mysql数据备份工具

```
mysqldump工具
```

`mysqldump是mysql自带的备份工具，目录在bin目录下面：```/usr/local/mysql/bin/mysqldump```

```
支持基于innodb的热备份，但是由于是逻辑备份，所以速度不是很快，适合备份数据比较小的场景
Mysqldump完全备份+二进制日志可以实现基于时间点的恢复。
```

``

```
基于LVM快照备份
在物理备份中，有基于文件系统的物理备份（LVM的快照），也可以直接用``tar``之类的命令对整个数据库目录
进行打包备份，但是这些只能进行冷备份，不同的存储引擎备份的也不一样，myisam自动备份到表级别
而innodb不开启独立表空间的话只能备份整个数据库。
```

``

```
tar``包备份
```

``

```
percona提供的xtrabackup工具
支持innodb的物理热备份，支持完全备份，增量备份，而且速度非常快，支持innodb存储引起的数据在不同
数据库之间迁移，支持复制模式下的从机备份恢复备份恢复，为了让xtrabackup支持更多的功能扩展
可以设立独立表空间，打开 innodb_file_per_table功能，启用之后可以支持单独的表备份
```

20、keepalive的工作原理和如何做到健康检查

```
keepalived是以VRRP协议为实现基础的，VRRP全称Virtual Router Redundancy Protocol，即虚拟路由冗余
协议。
虚拟路由冗余协议，可以认为是实现路由器高可用的协议，即将N台提供相同功能的路由器组成一个路由器组
这个组里面有一个master和多个backup，master上面有一个对外提供服务的vip（该路由器所在局域网内
其他机器的默认路由为该vip），master会发组播，当backup收不到vrrp包时就认为master宕掉了
这时就需要根据VRRP的优先级来选举一个backup当master。这样就可以保证路由器的高可用了
```

``

```
keepalived主要有三个模块，分别是core、check和vrrp。core模块为keepalived的核心，负责主进程的启动、维护
及全局配置文件的加载和解析。check负责健康检查，包括常见的各种检查方式，vrrp模块是来实现VRRP协议的
```

``

```
Keepalived健康检查方式配置
HTTP_GET|SSL_GET
HTTP_GET | SSL_GET
{
url {
path /``# HTTP/SSL 检查的url可以是多个
digest <STRING> ``# HTTP/SSL 检查后的摘要信息用工具genhash生成
status_code 200``# HTTP/SSL 检查返回的状态码
}
connect_port 80 ``# 连接端口
bindto<IPADD>
connect_timeout 3 ``# 连接超时时间
nb_get_retry 3 ``# 重连次数
delay_before_retry 2 ``#连接间隔时间
}
```

21、统计ip访问情况，要求分析nginx访问日志，找出访问页面数量在前十位的ip

```
cat access.log | ``awk` `'{print $1}'` `| ``uniq` `-c | ``sort` `-rn | ``head` `-10
```

22、使用tcpdump监听主机为192.168.1.1，tcp端口为80的数据，同时将输出结果保存输出到tcpdump.log

```
tcpdump ``'host 192.168.1.1 and port 80'` `> tcpdump.log
```

23、如何将本地80 端口的请求转发到8080 端口，当前主机IP 为192.168.2.1

```
iptables -A PREROUTING -d 192.168.2.1 -p tcp -m tcp -dport 80 -j DNAT-to-destination
192.168.2.1:8080
```

24、简述raid0 raid1 raid5 三种工作模式的工作原理及特点

```
RAID 0：带区卷，连续以位或字节为单位分割数据，并行读/写于多个磁盘上，因此具有很高的数据传输率
但它没有数据冗余，``RAID 0 只是单纯地提高性能，并没有为数据的可靠性提供保证
而且其中的一个磁盘失效将影响到所有数据。因此，RAID 0 不能应用于数据安全性要求高的场合
```

```
RAID 1：镜像卷，它是通过磁盘数据镜像实现数据冗余，在成对的独立磁盘上产生互为备份的数据
不能提升写数据效率。当原始数据繁忙时，可直接从镜像拷贝中读取数据，因此RAID``1 可以提高读取性能
RAID 1 是磁盘阵列中单位成本最高的，镜像卷可用容量为总容量的1``/2``，但提供了很高的数据安全性和可用性
当一个磁盘失效时，系统可以自动切换到镜像磁盘上读写，而不需要重组失效的数据
```

```
RAID5：至少由3块硬盘组成，分布式奇偶校验的独立磁盘结构，它的奇偶校验码存在于所有磁盘上
任何一个硬盘损坏，都可以根据其它硬盘上的校验位来重建损坏的数据（最多允许1块硬盘损坏）
所以raid5可以实现数据冗余，确保数据的安全性，同时raid5也可以提升数据的读写性能
```

25、你对现在运维工程师的理解和以及对其工作的认识

```
运维工程师在公司当中责任重大，需要保证时刻为公司及客户提供最高、最快、最稳定、最安全的服务
运维工程师的一个小小的失误，很有可能会对公司及客户造成重大损失
因此运维工程师的工作需要严谨及富有创新精神
```

26、实时抓取并显示当前系统中tcp 80端口的网络数据信息，请写出完整操作命令

```
tcpdump -nn tcp port 80
```

27、服务器开不了机怎么解决一步步的排查

```
A、造成服务器故障的原因可能有以下几点：
```

1：服务器电源有问题(断电，电源线松动，人为原因)。

2：服务器系统文件丢失，硬件问题，散热不良造成蓝屏和死机。

3：服务器网络参数配置错误，物理链路原因等。

``

```
B、如何排查服务器故障的处理步骤如下：
```

1：1、先看服务器的电源指示灯是否亮，如果电源灯不亮，先检查并确认电源没问题时，试着按开机键是否能点亮服务器.如果不能点亮，和数据确认后先更换备用服务器以便快速恢复业务.

2：2 如果服务器电源灯亮，接上显示器和键盘，如果服务器系统有异常(比如蓝屏…)不能正常登录系统，先和数据确认，是否执行能重启服务器或是更换备用服务器，以便快速恢复业务.

3：3 如果正确输入用户名和密码情况下能登录系统，查看网卡指示灯是否正常，并用 ifconfig 命令查看网卡接口状态。用 ping 对 端 ip 测试网络是否连通，

4：4、如果 ping 不通，先和数据人员确认并检查网卡配置文件参数是否配置正确，是否正确配置网关(不正确则修正后)用“ifdown；ifup 网卡名“命令重启单个网卡，网卡接口(灯)状态正常后，再用 ping 命令测试，

5：5、还 ping 不通，及时排查并确保本地尾纤，模块等物理设备接入正常，收发光在规定范围内，和数据人员确认是否可以重启服务器，并确认数据方面没有网络配置和数据方面的变化。

6：6、能 ping 通则告知数据人员，并让数据人员帮忙确认链路是否正常，有没有丢包现象等，没有丢包就 OK，有丢包就继续排查尾纤，模块等，直到链路正常没有丢包，数据人员能及时的从远程登录服务器做数据配置能快速恢复业务为 OK。

7 、7、如果不能接入服务器，与数据确认是否可以重启，重启后登陆正常，继续 3.4.5.6 步骤，如果还是不行，权衡利弊，有没有必要更换新的服务器上去，恢复业务要紧。

28、Linux系统中病毒怎么解决

```
1）最简单有效的方法就是重装系统
2）要查的话就是找到病毒文件然后删除
        中毒之后一般机器cpu、内存使用率会比较高
        机器向外发包等异常情况，排查方法简单介绍下
```

```
top 命令找到cpu使用率最高的进程
```

一般病毒文件命名都比较乱，可以用 `ps aux` 找到病毒文件位置 ``

```
rm -f  命令删除病毒文件
检查计划任务、开机启动项和病毒文件目录有无其他可以文件等
```

```
3）由于即使删除病毒文件不排除有潜伏病毒，所以最好是把机器备份数据之后重装一下
```

29、发现一个病毒文件你删了他又自动创建怎么解决

```
公司的内网某台linux服务器流量莫名其妙的剧增,用iftop查看有连接外网的情况
针对这种情况一般重点查看netstat连接的外网ip和端口。
```

``

```
用lsof -p pid可以查看到具体是那些进程，哪些文件
经查勘发现/root下有相关的配置conf.n hhe两个可疑文件，rm -rf后不到一分钟就自动生成了
由此推断是某个母进程产生的这些文件。所以找到母进程就是找到罪魁祸首
```

``

```
查杀病毒最好断掉外网访问，还好是内网服务器，可以通过内网访问
断了内网，病毒就失去外联的能力，杀掉它就容易的多
怎么找到呢，找了半天也没有看到蛛丝马迹，没办法只有ps axu一个个排查
方法是查看可以的用户和和系统相似而又不是的冒牌货，果然，看到了如下进程可疑
```

``

```
看不到图片就是/usr/bin/.sshd
于是我杀掉所有.sshd相关的进程，然后直接删掉.sshd这个可执行文件
然后才删掉了文章开头提到的自动复活的文件
```

``

```
总结一下，遇到这种问题，如果不是太严重，尽量不要重装系统
一般就是先断外网，然后利用iftop,ps,netstat,chattr,lsof,pstree这些工具顺藤摸瓜
一般都能找到元凶。但是如果遇到诸如此类的问题
/boot/efi/EFI/redhat/grub.efi: Heuristics.Broken.Executable FOUND，个人觉得就要重装系统了
```

30、说说TCP/IP的七层模型

```
应用层 (Application)：
网络服务与最终用户的一个接口。
协议有：HTTP FTP TFTP SMTP SNMP DNS TELNET HTTPS POP3 DHCP
```

``

```
表示层（Presentation Layer）：
数据的表示、安全、压缩。（在五层模型里面已经合并到了应用层）
格式有，JPEG、ASCll、DECOIC、加密格式等
```

``

```
会话层（Session Layer）：
建立、管理、终止会话。（在五层模型里面已经合并到了应用层）
对应主机进程，指本地主机与远程主机正在进行的会话
```

``

```
传输层（Transport）：
定义传输数据的协议端口号，以及流控和差错校验。
协议有：TCP UDP，数据包一旦离开网卡即进入网络传输层
```

``

```
网络层（Network）：
进行逻辑地址寻址，实现不同网络之间的路径选择。
协议有：ICMP IGMP IP（IPV4 IPV6） ARP RARP
```

``

```
数据链路层（Link）：
建立逻辑连接、进行硬件地址寻址、差错校验等功能。（由底层网络定义协议）
将比特组合成字节进而组合成帧，用MAC地址访问介质，错误发现但不能纠正
```

``

```
物理层（Physical Layer）：
```

``

```
是``计算机网络`[`OSI模型`](http://baike.baidu.com/item/OSI%E6%A8%A1%E5%9E%8B)`中最低的一层
物理层规定:为传输数据所需要的物理链路创建、维持、拆除
而提供具有机械的，电子的，功能的和规范的特性
```

``

```
简单的说，物理层确保原始的``数据``可在各种物理媒体上传输。``局域网``与``广域网``皆属第1、2层
物理层是``OSI``的第一层，它虽然处于最底层，却是整个开放系统的基础
物理层为设备之间的``数据通信``提供传输媒体及互连设备，为``数据传输``提供可靠的环境
如果您想要用尽量少的词来记住这个第一层，那就是“``信号``和``介质``”
```

31、你常用的Nginx模块，用来做什么

```
rewrite模块，实现重写功能
access模块：来源控制
ssl模块：安全加密
ngx_http_gzip_module：网络传输压缩模块
ngx_http_proxy_module 模块实现代理
ngx_http_upstream_module模块实现定义后端服务器列表
ngx_cache_purge实现缓存清除功能
```

32、请列出你了解的web服务器负载架构

```
Nginx
Haproxy
Keepalived
LVS
```

33、查看http的并发请求数与其TCP连接状态

```
`netstat -n | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'
```

```
还有``ulimit` `-n 查看linux系统打开最大的文件描述符，这里默认1024
不修改这里web服务器修改再大也没用，若要用就修改很几个办法，这里说其中一个：
修改``/etc/security/limits``.conf
* soft nofile 10240
* hard nofile 10240
重启后生效
```

34、用tcpdump嗅探80端口的访问看看谁最高

```
`tcpdump -i eth0 -tnn dst port 80 -c 1000 | awk -F"." '{print $1"."$2"."$3"."$4}'| sort | uniq -c | sort -nr |head -20
```

35、写一个脚本，实现判断192.168.1.0/24网络里，当前在线的IP有哪些，能ping通则认为在线

```
#!/bin/bash
```

```
for ip ``in ``seq` `1 255
```

```
do
{
ping` `-c 1 192.168.1.$ip > ``/dev/null` `2>&1
if` `[ $? -``eq` `0 ]; ``then
echo` `192.168.1.$ip UP
else
echo` `192.168.1.$ip DOWN
fi
}&
done
wait
```

36、已知 apache 服务的访问日志按天记录在服务器本地目录/app/logs 下，由于磁盘空间紧张

现在要求只能保留最近 7 天的访问日志！请问如何解决？ 请给出解决办法或配置或处理命令

创建文件脚本：

#!/bin/bash

for n in `seq 14`

do

date -s "11/0$n/14"

touch access_www_`(date +%F)`.log

done

解决方法：

pwd/application/logs

ll

-rw-r--r--. 1 root root 0 Jan 1 00:00 access_www_2015-01-01.log -rw-r--r--. 1 root root 0 Jan 2 00:00 access_www_2015-01-02.log -rw-r--r--. 1 root root 0 Jan 3 00:00 access_www_2015-01-03.log -rw-r--r--. 1 root root 0 Jan 4 00:00 access_www_2015-01-04.log -rw-r--r--. 1 root root 0 Jan 5 00:00 access_www_2015-01-05.log -rw-r--r--. 1 root root 0 Jan 6 00:00 access_www_2015-01-06.log -rw-r--r--. 1 root root 0 Jan 7 00:00 access_www_2015-01-07.log -rw-r--r--. 1 root root 0 Jan 8 00:00 access_www_2015-01-08.log -rw-r--r--. 1 root root 0 Jan 9 00:00 access_www_2015-01-09.log -rw-r--r--. 1 root root 0 Jan 10 00:00 access_www_2015-01-10.log -rw-r--r--. 1 root root 0 Jan 11 00:00 access_www_2015-01-11.log -rw-r--r--. 1 root root 0 Jan 12 00:00 access_www_2015-01-12.log -rw-r--r--. 1 root root 0 Jan 13 00:00 access_www_2015-01-13.log

-rw-r--r--. 1 root root 0 Jan 14 00:00 access_www_2015-01-14.log

find /application/logs/ -type f -mtime +7 -name "*.log"|xargs rm –f

##也可以使用-exec rm -f {} \;进行删除

ll

-rw-r--r--. 1 root root 0 Jan 7 00:00 access_www_2015-01-07.log -rw-r--r--. 1 root root 0 Jan 8 00:00 access_www_2015-01-08.log -rw-r--r--. 1 root root 0 Jan 9 00:00 access_www_2015-01-09.log -rw-r--r--. 1 root root 0 Jan 10 00:00 access_www_2015-01-10.log -rw-r--r--. 1 root root 0 Jan 11 00:00 access_www_2015-01-11.log -rw-r--r--. 1 root root 0 Jan 12 00:00 access_www_2015-01-12.log -rw-r--r--. 1 root root 0 Jan 13 00:00 access_www_2015-01-13.log

-rw-r--r--. 1 root root 0 Jan 14 00:00 access_www_2015-01-14.log

37、如何优化 Linux系统（可以不说太具体）？

1. 不用root，添加普通用户，通过sudo授权管理
2. 更改默认的远程连接SSH服务端口及禁止root用户远程连接
3. 定时自动更新服务器时间
4. 配置国内yum源
5. 关闭selinux及iptables（iptables工作场景如果有外网IP一定要打开，高并发除外）
6. 调整文件描述符的数量
7. 精简开机启动服务（crond rsyslog network sshd）
8. 内核参数优化（/etc/sysctl.conf）
9. 更改字符集，支持中文，但建议还是用英文字符集，防止乱码
10. 锁定关键系统文件
11. 清空/etc/issue，去除系统及内核版本登录前的屏幕显示

38、请执行命令取出 linux 中 eth0 的 IP 地址(请用 cut，有能力者也可分别用 awk,sed 命令答)

cut方法1：

```
# ifconfig eth0|sed -n '2p'|cut -d ":" -f2|cut -d " " -f1 192.168.20.130
```

awk方法2：

```
# ifconfig eth0|awk 'NR==2'|awk -F ":" '{print Extra close brace or missing open brace 1}'
```

192.168.20.130

awk多分隔符方法3：

```
# ifconfig eth0|awk 'NR==2'|awk -F "[: ]+" '{print $4}'
```

192.168.20.130

sed方法4：

```
# ifconfig eth0|sed -n '/inet addr/p'|sed -r 's#^.*ddr:(.*)Bc.*$#\1#g'
```

192.168.20.130

39、请写出下面 linux SecureCRT 命令行快捷键命令的功能？

Ctrl + a

Ctrl + c

Ctrl + d

Ctrl + e

Ctrl + l

Ctrl + u

Ctrl + k

tab

Ctrl+shift+c

Ctrl+shift+v

解答：

Ctrl + a —->光标移动到行首

Ctrl + e —->光标移动到行尾

Ctrl + c —->终止当前程序

Ctrl + d —->如果光标前有字符则删除，没有则退出当前中断

Ctrl + l —->清屏

Ctrl + u —->剪切光标以前的字符

Ctrl + k —->剪切光标以后的字符

Ctrl + y —->复制u/k的内容

Ctrl + r —->查找最近用过的命令

tab —->命令或路径补全

Ctrl+shift+c —->复制

Ctrl+shift+v —->粘贴

40、每天晚上 12 点，打包站点目录/var/www/html 备份到/data 目录下（最好每次备份按时间生成不同的备份包）

cat a.sh

#/bin/bash

cd /var/www/ && /bin/tar zcf /data/html-`date +%m-%d%H`.tar.gz html/

crontab –e

00 00 * * * /bin/sh /root/a.sh

一、Linux操作系统知识

1.常见的Linux发行版本都有什么？你最擅长哪一个？它的官网网站是什么？说明你擅长哪一块？ 答： 常见的Linux发现版本有Redhat、Centos、Debian、Ubuntu、Suse 最擅长Redhat和Centos Redhat官网：www.redhat.com Centos官网：www.centos.org 我最擅长Linux基本命令操作及相关服务搭建

2.Linux开机启动流程详细步骤是什么？系统安装完，忘记密码如何破解？ 答：

开机步骤 a、首先是bios加电自检、初始化，这个过程会检测相关硬件(cpu、内存、显卡、硬盘等)

然后读取一个启动顺序，以硬盘为例，会读取硬盘中的MBR。 b、加载内核读取/boot里边的配置文件。 c、启动初始化进程，开始运行/sbin/init d、读取/etc/inittab确定运行级别 e、根据/etc/rc.d/rcN.d加载开机启动程序，rcN.d都是链接文件，都指向/etc/rc.d/init.d再运行/etc/rc.d/rc.local f、用户登录(3种方式ssh、命令行、图形化) g、进入loginshell,以命令行为例，首先读取/etc/profile这个全局配置文件

然后再针对当前用户读取家目录中的 ~/.bash_profile和~/.bash_login和~/.profile h、最后一步就是打开non-loginshell

进入图形化后手动新建一个终端，但这个shell不读取/etc/profile

忘记密码 a、重启系统，在GRUB界面，选取忘记密码的系统，按e键进入编辑模式 b、选项Kernel.....按e键进行编辑 c、在编辑界面rhgbquiet后加空格，然后输入"single"或"1"回车 d、按b启动进入单用户模式 f、进入系统后passwd 回车输入新密码(如果有selinux，先暂时关闭setenforce0)

3.企业中Linux服务器系统分区标准是什么？（硬盘为300G，内存16G） 答： /boot200M /swap16G /70G /data剩下的全部空间

4.某一天突然发现Linux系统文件只读，该怎么办呢？完整操作步骤。 答： 首先把系统关机，然后以光盘启动进入救援模式(linuxrescue)

执行"fsck.ext3-y/dev/sda2"（假如只读的分区类型为ext3，分区为/dev/sda2）

5.安装一台系统使用DVD光盘安装，如何安装50台Linux系统如何安装呢？思考一下。 答： a、可以多用几张DVD一台一台的安装。 b、可以用Kickstart批量安装(客户端从网络启动)

6.用虚拟机安装了一台Linux系统，突然想克隆一台服务器，克隆后发现无法上网，如何解决？ 答： a、编辑网卡配置文件/etc/sysconfig/network-scripts/ifcfg-eth0,将HWADDR和MAC地址这两行删除。 b、修改文件/etc/udev/rules.d/70-persistent-net.rules,删除之前eth0所在的行，将下一行eth1修改为eth0 c、reboot

7.Linux网卡配置文件路径是什么？要使服务器上外网，必须满足的条件有哪些？需要配置什么？ 答： 网卡配置文件路径：/etc/sysconfig/network-scripts/ifcfg-eth(代表数字) 要上外网需要：能够链接internet的网线(或无线)、有网卡 需要配置：IP、netmask、gateway、dns(自动或手动都ok，服务器一般自动)

8.一般可以使用什么软件远程linux服务器？通过什么上传文件和下载文件？ 答： 远程连接linux的软件：xshell、SecureCRT、putty、vnc(图形化) 上传和下载文件：lrzsz、sftp

9./mnt目录主要用于什么？/root目录跟root用户有什么关系？/根目录与/boot目录有什么联系？ 答： /mnt一般用于挂载外接设备 /root是一个目录，是root用户的家目录 /boot目录是/目录下的一个子目录

10.某一天误操作，执行了rm-rf*，会有哪些情况发生？请举例。 答： a、如果当前目录为"/tmp"，那么这个目录下的东西会全部删除(默认不包含隐藏文件) b、如果当前目录为"/"，那么系统上的数据将会丢失，且无法启动，系统崩溃(谨慎使用这个命令)

二、Linux命令及文件操作

1.在/tmp/目录下创建test.txt文件，内容为:Hello，World!,用一个命令写出来。 答： echo "Hello,World!" > /tmp/test.txt

2.给test.txt文件除所有者之外增加执行权限，最终以数字写出文件的权限。 答: 655 默认是644，可以通过"chmod 655 /tmp/test.txt"

3.用vi命令编辑test.txt，如何跳转到末行，首行，行首、行末，如何在光标行下一行插入

如何复制5行，删除10行，查找jingfeng的字符、把jingfeng替换为jfedu.net 答： 末行：G 首行：gg 行首：^（Shift+6） 行尾：$(Shift+4) 光标下插入一行:o 复制5行：5yy 删除10行：10dd 替换：:%s/jingfeng/jfedu.net/g

4.查找linux系统下以txt结尾，30天没有修改的文件大小大于20K同时具有执行权限的文件并备份到/data/backup/目录下。 答： find / -name *txt -mtime +30 -type f -size +20k -perma= x -exec cp {} /data/backup/\;

5.当前test.txt所属的用户为root，组为abc，请将test.txt使拥有者为abc，组为root，写出命令。 答： chown abc:root test.txt

6.如何修改Linux启动级别为字符模式并永久生效，如何临时、永久关闭selinux及防火墙，请分别写出操作方法。 答： 更改字符模式：修改/etc/inittab一行为id:3:initdefault: 临时关闭selinnuxsetenforce0 临时关闭防火墙 iptables-F 永久关闭selinux修改/etc/selinux/config一行为SELINUX=permissive 永久关闭防火墙 iptables -F; /etc/init.d/iptablessave

7.每次开机在/tmp目录下创建一个当天的日期文件夹(提示：当前日期表示的方法为：`date+%Y%m%d`) 答： echo "mkdir/tmp/ `date+%Y%m%d`" >> /etc/rc.d/rc.local

8.如何查看文件内容，命令有哪些？查看文件第1行到3行，查看文件最后一行。 答： 查看文件内容：vim、cat、head、tail 查看第1到行：head -3 file 查看最后一行：tail -1 file

9.查看linux服务器IP的命令，同时只显示包含ip所在的行打印出来。 答： 以eth0为例 只打印所在的行：ifconfig eth0 | grep "inetaddr:" 只打印ip：ifconfig eth0 | grep "inetaddr:" | awk -F: '{print Extra close brace or missing open brace 1}'

10.将普通用户test加入root组的命令是？ 答： usermod -G root test