- **nginx是怎么做rewrite的?**
- nginx跳转的话可以匹配域名跳转，也可以匹配url跳转。匹配域名跳转的话在server段前面需要定义server_name，然后if $host等于需要被跳转的域名，就rewrite到http需要跳往的域名。匹配url跳转跟域名的差不多，不过是if $request_uri等于需要被跳转的url，然后rewrite到需要跳往的url。还可以做到在跳转时保持url不变，在rewrite规则后面加一个break就行了。
- **是不是培训的?**
- 算吧，在大学自学了一段时间的linux，感觉学的比较散，有很多不懂的地方，就去参加了培训做了一些项目，然后感觉那家公司还不错，在那里的学长也推荐，就在那里实习了一段时间。
- **mysql内连接和外连接的区别?**
- 内连接inner join，它保证两个表里面所有的行都满足连接的条件，它会从结果表里面删除与其它所有连接表中不匹配的所有行，所以有可能会造成信息的丢失。外连接outer join，有左外连接、右外连接，全外连接。它和内连接不同的是，它会以第一张表为主，与其它表进行连接，不管能不能匹配到都会保留行。
- **将数据还原到任意时刻是怎么还原的?**
- 我之前的公司是每天凌晨4点一全备，一小时一增备。如果是还原到3：30分，就需要将前一天的全备导入还原，然后一个小时一个小时地将二进制增量备份导入还原至3点，再查看属于3点的那个binlog找到30分钟对应的position，指定--stop-position进行还原。
- **如何对两个网卡进行冗余?**
- bonding可以为网卡提供冗余的支持。把两个网卡绑定到一个ip地址，当一块网卡发生问题时，另一块网卡也能提供l
- 正常服务。bonding最常用的有0，1两种模式，0模式是将两块网卡做负载均衡，采用轮询策略。1模式是将两块网卡做主备，平时只有主工作，主发生故障了就切换备用的提供服务。
- **du df不一致，是什么原因?**
- 可能是在删除某一文件的时候该文件一直被进程占用，所以删除后空间没有释放。通过lsof命令过滤delete找到对应进程的pid，然后将其kill，就可以释放删除的空间了。
- **tcp的四次挥手，断开**
- 客户端请求完成后，会发送一个fin=1的信息给服务端表示请求断开，同时发送的会有一个seq数字，然后客户端会进入一个fin-wait-1的等待状态。服务端收到fin信息后，会返回ack=1确认信息，还有将接收的seq数字加1作为ack的数字，还有一个自己的seq数字，返回之后服务端就会进入close-wait状态。此时tcp处于半连接状

态，客户端不能发送数据给服务端，但是服务端还可以发送最后的数据给客户端，半连接状态持续时间就是close-wait的时间。客户端收到服务端的确认信息后，就会进入fin-wait-2的等待状态，接收服务端发送的最后的数据，然后等待服务端发送释放链接的信息。服务端在发送完最后的数据后，就会向客户端发送fin=1，ack=1，ack数字为之前客户端一开始发送的seq数字加1，然后还有本次的seq数字，发送后，服务端进入last-ack最后确认状态，等待客户端确认。客户端收到信息后，会发送ack=1，ack数字为seq数字加1，自己进入timewait状态，经过两个msl时间后，进入close状态，而服务器接收到信息后，直接进入close状态。

- **nginx负载均衡和keepalived高可用有什么区别?**
- keepalived高可用的话主要是用来解决单点故障的，它是通过vrrp协议来实现的，同时只会有一台机器提供服务，其它的用作备用。而nginx负载均衡的话主要是用来提高访问效率的，每一个机器都会根据调度算法提供服务，调度算法有轮询权重，iphash，urlhash等等。
- **要你学会一个和nginx功能差不多的服务，要多久的时间**
- 如果要做到能用的话，一天应该可以，如果要深入学习的话肯定要花更长的时间。
- **如果服务器遭到攻击，怎么处理?**
- 安全总是相对的，所以我们应该有预演方案。首先需要断开服务器与外界的联系，远程的话就使用iptables，除了自己能登录，其它机器都不能。如果在机房的话，就直接切断网线。
- 我们需要查找攻击源，分析系统登录日志，使用last命令，或者查看/var/log/wtmp文件，不过一般的话黑客都会将其清空。
- w命令查看连接是否有异常，如果有异常的连接的话需要将连接用户直接锁定禁止登录，使用passwd -l命令，然后根据终端直接踢下线，使用kill -9命令。查看/var/log/security安全日志是否有异常。还可以通过netstat命令查看系统打开了哪些异常的端口。ps查看系统是否运行了什么异常的进程。特别关注每个用户家目录下面的.bash_history文件，里面有history历史记录。
- 最重要的是检查包的完整性。使用rpm -Va能查看软件包里文件的改变情况，这个主要是检查命令是否被植入了rootkit后门程序，我们也可以使用专门的第三方工具来检查，比如chkrootkit。如果软件包真的出现未知的修改，我们应该使用备份覆盖过去再使用。
- 一般来说，服务器遭到最多的攻击就是DDOS和rootkit攻击。
- 被入侵了有可能是系统出现漏洞，也可能是程序本身出现漏洞被黑客抓住了。无论我们之前做了什么补救分析工作，最后的结果一定是要重装系统的。因为就算我们自信不会再有问题，也防不住黑客随意做的一些小改动，破坏总比恢复要简单得多。

我们也无法信任一台曾经被黑客光顾的系统，这也是对公司的负责。在重装之前我们需要将重要数据备份，当然是要保证没有被修改的情况下，重装后恢复服务和数据，然后再将网络恢复，开始工作。

- **首页访问不了，其它页面正常，怎么解决?**
- 如果是这样的话，那说明服务的本身是没有问题的。首页一般会进行静态化以便缓存，那么有可能是CDN缓存出现问题，需要联系一下CDN公司帮忙分析一下；还有可能是nginx对首页有特殊的设置，比如rewrite重定向，但是目标目录出现问题，还有可能是首页应用的某个程序出现了问题，比如死循环等等，这些情况需要与相关开发人员进行沟通，看看是否出现了问题。
- **几十台机器通过ssh连接到远程服务器，出现卡顿很慢的情况，怎么解决?**
- 首先需要确认是不是自己的网络出现问题，使用ping命令ping一下服务器，如果能通的话说明不是网络问题。然后在服务器上使用top查看sshd占用的资源是不是过大，然后修改ssh的配置文件，将ssh的最大连接数maxstartups减小，或者其中会有一个连接在运行特别耗费资源的任务，用ps查到耗费资源的内容。
- **如果服务器创建文件出现不能再创建的错误，但检查磁盘空间又有，是什么原因?**
- 可能是节点数不够或者是设置了配额。df -i可以查看分区的节点总数以及使用情况。repquota -a可以查看配额情况，edquota -u 可以配置用户的文件使用配额。
- **网页报502和504错误分别是什么原因导致的，怎么排错?**
- 502是bad gateway，网关收到无效响应，504是gateway timeout，网关未能及时收到响应。这两个错误一般出现在有负载均衡的情况，当代理服务器收到了无法理解的未知响应时，就会返回502错误，如果超出代理服务器自己配置的超时时间还没有收到请求，就返回504错误。排错的话需要跳过代理服务器直接指定后台的服务器，curl或者浏览器查看是具体哪台服务器出现了问题。
- **lvs访问很慢，怎么办?**
- lvs访问很慢一般会出现在DR模式中，我们先在lvs上访问realserver，看看访问是否很慢，如果慢的话真实服务器肯定有问题，有可能是lo本地没有绑定vip的地址，或者是没有抑制arp的响应。还有可能是真实服务器运行的服务没有监听vip的地址。我们可以通过tcpdump -i -nnn抓包查看具体是哪个阶段出现了问题。