- **如果数据库负载过大，如何处理**
- 正常情况下，数据库本身的并发并不会很高，因为设置了主从读写分离，从库还有四层的负载均衡，前面还有redis缓存。数据库如果突然间负载过大有可能是遭到了大量突发的访问或者攻击，可能是前面的redis缓存失效了或者雪崩，宕机了。将redis恢复或者等待重新缓存。如果一直负载过大则可能是mysql语句优化不够，产生了太多的慢查询，mysql的sleep状态过多。我们可以show variables like slow query将慢查询日志打开，将记录日志标准的时间设置为1秒，然后查看慢查询日志，与相关开发人员进行沟通看看能不能优化一下出现的语句。sleep状态过多的话可以show variables like wait_time将其设置为更小的值，比如设置为30。当然，还有可能是系统出现问题，一般情况下，数据库的瓶颈会出现在磁盘io， 我们可以使用iostat命令查看io状态，如果出现问题我们应该提高磁盘io的效率，一个方面可以修改磁盘阵列，对数据库来说，raid10会是一个很好的选择，因为它是条带集镜像的，结合了raid0的快速与raid1的安全，另一个方面的话就是使用更好的磁盘来代替。
- **ping命令总是丢包，除开网络的原因，可能是哪些方面的原因？能正常访问但ping不通，是什么情况?**
- 会出现这种情况可能是iptables的规则过多，也可能是机器负载或者网络负载过大，还有可能是遭到了ddos攻击。
- 可能是防火墙设置了icmp的reject或drop规则。也有可能是内核设置了参数禁ping，将/proc/sys/net/ipv4/icmp_echo_ignore_all的值设置为了1，或者在/etc/sysctl.conf里面设置了net.ipv4.icmp_echo_ignore_all=1，然后用sysctl -p永久生效了。
- **如何查看squid的缓存命中率，如何提高命中率?**
- 使用squidclient mgr:info可以查看hits状态，60分钟的命中率应该要达到95%，不然就是不优秀。
- 提高命中率的方法有很多，首先就是提高squid可使用的内存大小cache_mem，然后我们可以设置nginx静态服务器的expire或者max_age将缓存过期时间加大，或者利用程序加大这个时间。缓存时间越长的话相应的命中率也会提高，但是这样做的话会对更新产生影响，所以需要我们指定一个合适的缓存策略。前端负载均衡轮询算法中的url_hash算法可以提高缓存的命中率，可以在代理服务器上进行设置。在其他方面，比如程序的优化，增加对静态资源的访问等等也可以做到对命中率的提高。
- **linux如何调优?**
- 首先在登录方面，我们需要删除多余的用户和组，像什么games、news等等一些不需要的系统却又自带的。使用userdel和groupdel命令进行删除。还有一些是运

行服务用到的用户，这些用户需要将其禁止登录，建议在创建的时候就将其禁止了，useradd -s /sbin/nologin,如果已经创建了就使用usermod命令。

- 在用户登录时，首先就是需要禁止root登录，因为root容易遭到暴力破解，又拥有最高权限，在Ubuntu和Debian里root是默认无法登录的。远程登录时最好使用密钥验证，而不使用密码验证，因为密码容易被暴力破解，而只要保存好本地的密钥，密钥认证就会十分安全。密钥认证设置需要修改ssh配置，将pubkey认证打开，同时指定pubkey的位置，还需要将password认证关闭，不然就无意义了，不关闭的话黑客还是能暴力破解密码进入系统。
- 说到修改ssh配置，我们还需要做一些事。将port修改为大于1024的指定端口，这样也是为了保证安全，我们甚至可以配置port knocking将ssh的端口隐藏起来，防止黑客通过ssh骇入系统；还有将DNS解析、GSSAPI认证关闭，可以解决ssh登录慢的问题。
- 除了ssh服务等必须的之外，我们应该关闭不需要的服务以保证系统的安全。过多的开启启动服务会占用系统资源，在系统因故障宕机时也会增加恢复的时间，使用chkconfig --level 35 off或者systemctl disable 禁用多余的服务。
- 使用普通用户登录，需要权限运行命令时应该配置sudo命令使用，在/etc/sudoers配置文件里面加入user all=（all）nopassword:all表示user用户使用sudo时不需要使用密码，当然，我们在配置用户的sudo权限时应该在不影响其工作的情况下尽可能地给予最小权限。
- 为了安全，应该修改系统登录信息和版本信息。删除或清空/etc/issue /etc/issue.net /etc/redhat-release /etc/motd 文件。这些文件里面都显示了登录系统或者版本的信息。
- 最坏的情况就是黑客侵入了我们的系统。这时候我们也应该有所防备，保护好history文件就是我们必须要做的。因为黑客可以在历史文件中找到我们重要资料的执行过程，然后轻松盗走资料，走之前也会毁尸灭迹，将文件删除。所以我们需要将它的默认路径更改，将.bash_history改名，同时频繁地备份这个文件。
- 最后的防线就是文件系统的安全了。我们需要锁定系统重要文件，可以通过chattr命令实现，+i 指定文件可以使该文件不能被修改或删除，+a可以使该文件只能被追加东西进去，而不能删除和修改数据。
- **请说一下你常用的linux命令**
- 使用服务的时候会经常使用ps命令查看进程，使用netstat命令查看端口和连接情况。监控系统状态会使用free/vmstat查看内存情况，使用iotop/iostat查看io情况，使用iftop/ifstat命令查看网络带宽，使用sar命令查看cpu情况，使用uptime命令查看系统负载情况。
- **计划任务每一列代表的是什么意思，需要注意些什么?**

- 计划任务的配置文件是/etc/crontab，计划任务的主要设置内容的每一列分别是分时天月周用户命令，就是第一列是多少分钟，第二列是多少小时，第三列是某个月的第多少天，第四列是第几个月，第五列是星期几，第六列是执行命令的用户，第七列是具体的执行的命令或脚本。需要注意的是脚本对用户有没有执行权限，命令需要用绝对路径，比如执行ls就需要写/usr/bin/ls，因为计划任务里的环境变量会不一样。
- **磁盘io过大的情况应该怎么办?**
- 磁盘io过大我的第一反应就是数据库，因为数据库的瓶颈一般就在磁盘io。如果是数据库这台服务器出现了这种情况，我们应该考虑一下将磁盘换成ssd固态或者高速硬盘，修改磁盘阵列为raid10也是一个好方法。当然，在数据库前面加上缓存也是一个好办法。比如redis或memcache。memcache安装比较方便，但是没有持久化，断电数据就会丢失。redis的话可以将数据持久化到硬盘中。
- 如果是其他服务的机器出现了这种情况，我们可以使用iotop命令查看哪些程序占用io过大，如果是具体有程序占用了过大的磁盘io，那么就需要与开发人员进行沟通，看看能不能优化一下程序。当然我们可以从架构的方面来解决问题，比如使用负载均衡等等。
- **如果系统/目录变成只读模式怎么解决?**
- 如果是一般目录出现这种情况就使用mount -o remount rw 重新以rw的方式挂载就行。但是根目录不能重挂，因为一直被使用。也可以用e2fsck命令对分区进行检测修复，但是想检查根需要进入单用户模式。
- 对根变成只读的话，我们需要对系统日志进行分析/var/log/message，看看是否有报错，这种情况应该会有内核的错误信息存在。如果没有的话，可能是硬件故障，查看磁盘硬件是否有黄灯报警，有的话我们需要进行热插拔将磁盘拔掉重插，然后将系统重启。
- **如何查看192.168.1.1的3306端口有没有被占用?**
- nmap -P 或者 telnet