一、数据库管理课程模拟面试题

**1.1、谈谈你对数据库的理解。**

简单的说数据库就是按照一定的数据结构来组织、存放和管理数据的仓库。数据库的特点是共享、减少数据的冗余度、独立性、集中控制和安全可靠。

数据库技术是管理信息系统、办公自动化系统、决策支持系统等各类信息系统的核心部分，是进行科学研究和决策管理的重要技术手段。

数据库最好不用存放大文件

**1.2、数据库能存储所有类型的数据吗？一般什么样的数据适合使用数据库存储？**

不能 简单的，非图片视频等大文件的数据

**1.3、当数据库服务处理速度慢时，你认为可能是什么原因导致的？并阐述一下对应的解决办法。**

1. 系统配置不够，CPU负载过高——增加硬件配置，查看什么程序影响占用CPU并做相应的处理。
2. 数据库存储图片、视频等大文件——把这些文件放在专门的文件服务器，不要存储在数据库中。
3. 数据存储的越来越多访问量越来越大——数据库调优，提网速
4. 程序执行的SQL语句有问题——修改SQL语句
5. 写入日志太多
6. 数据库服务器节点单一，不足以满足现有义务需求——升级数据库服务器架构

**1.4、说一下什么是存储引擎，建表时如何决定表使用的存储引擎？**

[MySQL](http://www.chinabyte.com/zq/mysql/" \t "http://blog.csdn.net/stormbjm/article/details/_blank)中的数据用各种不同的技术存储在文件(或者内存)中。这些技术中的每一种技术都使用不同的存储机制、索引技巧、锁定水平并且最终提供广泛的不同的功能和能力。通过选择不同的技术，你能够获得额外的速度或者功能，从而改善你的应用的整体功能。这些技术就叫做存储引擎。

1. Hash存储引擎
2. B树存储引擎 读多
3. LSM树存储引擎 写多

**1.5、单张表过大有什么缺点？如何解决？**

**查询的效率低，风险增加——可以采用分表、分库、分区的方法进行优化。maha等软件可以实现（孟晓光）。**

**1.6、给你5台服务器，部署数据库服务，阐述一下你的拓扑结构设计思路。**

搭建mysql-mmm架构，一台monitor服务器，四台agent服务器(两台主数据库服务器，；两台从数据库服务器)

**1.7、若你是数据库管理员，阐述一下你如何给服务器添加授权用户。**

给该用户最小且满足业务需求的权限

**1.8、没有对表做备份，就把表删除了可以恢复回来吗？**

（1）从日志文件中恢复

（2）如果系统备份了，或者做快照了，将系统文件恢复

（3）到中关村系统盘恢复IMG_256

**1.9、若你是数据库管理员，阐述一下，你如何对数据做备份。**

（1）定期备份。每月一次或者每一季度一次。根据业务数据状况而定。避免数据丢失。  
（2）上限备份。可以根据数据的记录多少设置上下限。例如超出1000就进行备份。但备份程序得自定义写。  
（3）筛选备份。根据自己的需求。哪些重要信息哪些变更数据有选择的进行备份。不需要的可以不进行备份。避免不必要的空间浪费。  
（4）数据清算或者盘点备份。根据年度或者季度清算，盘点。有条件的将年度极端关联数据进行备份。  
（5）同期备份。多个服务器，某一备份，留给其它服务器同期导入和更新。  
（6）抽取和输出备份。按照需求和筛选条件将数据利用Bat程序进行呼出和转存。根据需求  
（7）保存不同格式。以备其它DB同期和输入更新。  
（8）汇总备份。针对业务数据进行合计或者汇总成电子文件数据或者报表数据进行输出。

**1.10、目前常见数据库服务软件有哪些？搭建数据库服务时，你如何选择使用那种软件？**

Mysql、mariadb、oracle、SQL server、DB2、阿里SQL、 **Acess、Sybase、PostgreySQL**

根据业务量、安全性、成本投入、操作系统等等选择

**二、Linux安全与监控课程模拟面试题**

**2.1、谈谈你对安全的理解。**

linux安全指与linux操作系统所有相关的安全技术，从系统管理到入侵检测，从程序开发到漏洞分析， 从应用层到内核无不与安全挂钩。

Linux安全很重要，近年来频频发生的安全事故（新网DNS被攻击导致大面积网瘫、淘宝数据丢失、微软代码遭泄露、病毒库的泄露导致文件勒索病毒的肆虐等）都在以生动的例子诉说的安全的重要性。

我们要从以下方面去保证服务器的安全（按照入侵的顺序，加入个人的理解）：

1. 网络安全：对网络的访问控制，防火墙规则。
2. 管理安全：各种保障性的规范、措施、方法。
3. 物理安全：各种设备、主机，机房环境。
4. 系统安全：主机或设备的操作系统。
5. 应用安全：各种网络服务、应用程序性。
6. 数据安全：信息的备份和恢复、加密解密

**2.2、谈谈你对监控的理解。**

监控是对服务器硬件（CPU、内存、硬盘等）、系统（负载、虚拟内存、用户、进程、系统日志等）、网络（Host\_Alive,Ping,端口,连接）等等的监控。

监控的目的是为了在服务器出现问题前规避问题，或者是服务器出现问题后及时发现并处理问题。

**2.3、你觉得信息在传递中有哪些风险？**

（1）电脑黑客窃取

（2）出差人员

（3）离职人员

（4）合作伙伴

（5）商业间谍

（6）高管习惯

（7）开发人员

（8）流失失控

**2.4、若你是运维工程师，说一下你如何保护一台服务器的安全？**

1. 网络安全：开启防火墙，网络访问控制
2. 用户授权:给用户最小且能完成业务需求的权限
3. 用户账号安全：设置账号的有效期，经常修改密码，伪装登录提示，改登录端口，禁root用户登录。
4. 文件系统安全：历史命令控制、程序和服务控制、文件系统规划及挂载、锁定/解锁文件
5. 物理安全：把服务器放在IDC机房
6. 系统安全：装漏洞更少、更安全的操作系统
7. 应用安全：装漏洞少、更安全的软件，打补丁，经常扫描检测漏洞，卸载没用到的软件。
8. 数据安全：给服务器备份
9. 管理安全：要从管理角度出发，利用规章制度等文字性的材料规范，约束各种针对[计算机网络](https://www.baidu.com/s?wd=%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YzuWFBnj6zPWR3PAF9PHN-0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnH64PWTYP1Dkrj03n1RLn1Rsn0" \t "https://zhidao.baidu.com/question/_blank)的行为，例如禁止员工随便下载非法程序，禁止[网络管理员](https://www.baidu.com/s?wd=%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E5%91%98&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YzuWFBnj6zPWR3PAF9PHN-0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnH64PWTYP1Dkrj03n1RLn1Rsn0" \t "https://zhidao.baidu.com/question/_blank)以外的人员进入[中心机房](https://www.baidu.com/s?wd=%E4%B8%AD%E5%BF%83%E6%9C%BA%E6%88%BF&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YzuWFBnj6zPWR3PAF9PHN-0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnH64PWTYP1Dkrj03n1RLn1Rsn0" \t "https://zhidao.baidu.com/question/_blank)，完善[网络管理员](https://www.baidu.com/s?wd=%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E5%91%98&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YzuWFBnj6zPWR3PAF9PHN-0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnH64PWTYP1Dkrj03n1RLn1Rsn0" \t "https://zhidao.baidu.com/question/_blank)的值班制度等等。
10. 购买云平台服务，做好预防

**2.5、监控一台服务器时，你觉得应该监控服务器的哪些资源呢？**

1. 服务器硬件（CPU、内存、硬盘等）
2. 系统（负载、虚拟内存、用户、进程、系统日志等）
3. 网络（Host\_Alive,Ping,端口,连接等）

**2.6、阐述一下，你如何对一台服务器做监控？**

1. 手动监控
2. 进程监控 ps top
3. 存储监控 free、swapon -s、df -h
4. 网络监控 ifconfig、netstat、ping、traceroute
5. 系统性能监控 uptime、mpstat、vmstat、iostat、netstat、sar
6. 自动监控系统
7. 安装监控软件 nagios，cacti，zabbix等
8. 添加监控项

**2.7、阐述对称加密与非对称加密的区别。**

（1）对称加密 加密和解密用同一个秘钥

（2）非对称加密 加密和解密用不同秘钥

**2.8、阐述一下CA的功能，及国家的权威CA机构有哪些。**

CA 被通信双方信任的、独立的第三方证书权威机构，他的功能是：负责证书的颁发、验证和撤销。

国内常见的CA机构：

1. 中国金融认证中心（CFCA）
2. 中国电信安全认证中心（CTCA）
3. 北京数字证书认证中心（BJCA）

**2.9、生产环境下如何获知一台主机上的网站服务是否正在运行?**

1. 客户端访问该服务器，能正常访问即正常运行
2. 查看该服务的端口号，有即正常运行
3. 查看该服务的状态，活跃即正常运行
4. 看监控，该服务正常即正常运行

**2.10、如何让系统的普通用户拥有root的权限？什么情况下需要这样做？**

1. Sudo提权
2. 修改该用户的UID为0

当普通用户需要修改一些文件或者管理服务等等时，以自己的权限是无权操作的，就需要拥有root权限