[在此处输入文章标题]

1. **数据库规划和安装（中级）**
2. **DB2版本、客户端**

DB2 Everyplace——供移动设备使用

DB2 Personal Edition——单用户使用，支持win和linux

DB2 Express-C——免费版本，支持win和linux，不支持hadr、表分区等功能，有2C&4Gmemory限制

DB2 Express Edition——支持win和linux，有2C&4GBmemory限制

DB2 Workgroup Edition—— (WSE)入门级服务器，LUW

DB2 Enterprise Edition—— (ESE) 具有数据库分区特性，LUW

Data Enterprise Developer Edition——为开发人员提供

Runtime Client——仅提供对数据服务器的访问，不具备数据管理工具

Client——标准客户端，可管理数据库

参考《db2 training》第1章

1. **DB2安装**

使用root用户，进入安装介质目录

使用sh db2\_install –b /opt/IBM/db2/V9.1 –p ESE进行安装ESE

添加license（需要在实例用户下添加，注意确保实例用户对license文件的执行权限）

命令：使用db2licm –a <license文件名>

查看license

命令：使用db2licm –l查看

创建实例

db2icrt –u db2fenc1 db2inst1

参考《db2 training》第2、3、4章

1. **DB2启停**

db2start

db2stop force

参考《db2 training》第5章

1. **数据库建库**

**create database sales1 on /dbsales1 USING CODESET gbk TERRITORY cn**

数据库路径（Database Path）: /dbsales1

实际路径：/dbsales1/<instance\_name>/NODE0000/sales1（库名）

CODESET: 数据库字符集

1. **数据库安全性（中级）**
2. **安全机制**

**身份验证**——操作系统验证用户ID和密码

**授权**——决定用户可以执行的操作和访问的数据（SYSADM—SYSCTRL—SYSMAINT—SYSMON—DBADM—LOAD）

**特权**——基于数据库对象（表、视图、模式、表空间等）的权限

1. **身份验证类型**

Server——身份验证在服务器上进行

Server\_encrypt——身份验证在服务器上进行，密码在客户机上加密后发送到服务器

Client——身份验证在客户机上进行

Kerberos——由kerberos安全软件进行身份验证

Krb\_server\_encrypt——用kerberos进行身份验证或使用Server\_encrypt

Data\_encrypt——身份验证在服务器上，与Server\_encrypt相同，但是数据也加密

Data\_encrypt\_cmp——提供对老式客户机的兼容，同Data\_encrypt

Gssplugin——身份验证由外部的GSS-API插件决定

Gss\_server\_enceypt——身份验证由外部的GSS-API插件决定

身份验证类型的更改：

db2 update dbm cfg using authentication server\_encrypt

db2stop

db2start

1. **权限类型**

最高权限（SYSADM）：由dbm cfg文件中的SYSADM\_GROUP参数控制

最高系统控制权限（SYSCTRL）：由dbm cfg文件中的SYSCTRL\_GROUP参数控制

不能对数据库对象进行存取；不能对数据库管理器配置文件进行更改；只有SYSADM和SYSCTRL可以执行force applications命令

第二级系统控制权限（SYSMAINT）：由dbm cfg中SYSMAINT\_GROUP参数控制

不能创建或删除数据库和表空间；提供对数据库管理器实例执行维护多核实用程序操作的能力

系统监视器权限（SYSMON）：由dbm cfg中的sysmon\_group参数控制

可以运行以下命令监视数据库运行情况：

db2 get monitor switches（查看各个监视器是否在运作）

db2 get snapshot for [db|locks|applications] on <db\_name>

db2 list active databases

db2 list applications

数据库级别最高权限（DBADM）：通过GRANT命令设置，REVOKE命令撤销

load权限：允许用户将数据导入DB2：通过GRANT命令设置，REVOKE命令撤销

1. **特权类型**

control：全部权限

delete：删除表和视图

insert：在表和视图中插入

select：查看表和视图

update：修改表和视图

alter：更改对标的定义

index：在对象上创建索引

references：在表上创建和删除外键

bind：重新绑定包

execute：执行包和例程

db2 grant select on table t1 to user user1

db2 revoke all on table t1 from user user1

参考《db2 training》第11章

1. **数据库常用命令（中级）**

参考《DB2常用命令》

1. **SQL规范（中级）**

参考《开发管理规范》

1. **数据库并发性和锁（中级）**
2. **保证数据一致性机制**

事务

隔离级别

锁

1. **并行事务的四种现象**

丢失更新——两个事务同时更新一个数据时，其中一个更新丢失

脏读——读取到尚未提交（commit）的数据

不可重复的读——一个事务对同一数据的两次读，返回的结果不同

幻象读——当初在搜索条件匹配的数据行中没有的数据在稍后的读操作中出现

1. **隔离级别（4种）**

可重复的读RR——防止所有现象，锁定引用的每一行（不仅仅是正在读或修改的行）

读稳定性RS——会出现幻象读，锁定实际检索和修改的行，其他事务可执行插入

游标稳定性CS——可防止脏读，只锁定游标所在的行

未提交的读UR

在SELECT语句中指定隔离级别：

例如：SELECT语句加上WITH [RR/RS/CS/UR]子句

1. **锁**

锁转换——事务对同一资源只能持有一种锁，因此当有更严格访问模式需求时，会发生锁转换

锁升级——LOCKLIST和MAXLOCKS参数决定，将一个表内几个单独的行级锁转换成一个单一的表级锁

锁超时——由LOCKTIMEOUT参数控制，默认值为-1表示无限等待

死锁——由DLCHKTIME参数控制死锁检测时间

与锁相关的数据库参数：

LOCKLIST——在数据库上可存放锁的最大容量（记录锁的页面所占的存储空间）

MAXLOCKS——单个应用所能持有的锁占锁列表中的比例

查看锁、锁等待

db2pd –d <dbname> -locks

db2pd –d <dbname> -wlocks

参考《db2 training》第12章

1. **SQL优化（高级）**

参考《db2 training》第13章

**重点掌握：**

1. **三种主要的表连接方式**
2. **如何生成SQL、存储过程的执行计划**
3. **如何分析执行计划**
4. **如何收集表、索引的统计信息**
5. **如何查看表、索引的统计信息**
6. **数据库参数（高级）**

参考《db2 training》第14章

**重点掌握：**

1. **数据库参数(db2 get db cfg)**

DFT\_QUERYOPT

SELF\_TUNING\_MEM

DATABASE\_MEMORY

LOCKLIST

MAXLOCKS

PCKCACHESZ

SORTHEAP

DBHEAP

CATALOGCACHE\_SZ

LOGBUFSZ

UTIL\_HEAP\_SZ

STMTHEAP

STAT\_HEAP\_SZ

DLCHKTIME

LOCKTIMEOUT

CHNGPGS\_THRESH

NUM\_IOCLEANERS

NUM\_IOSERVERS

TRACKMOD

LOGFILSIZ

LOGPRIMARY

LOGSECOND

NEWLOGPATH

MIRRORLOGPATH

BLOCKNONLOGGED

MAX\_LOG

NUM\_LOG\_SPAN

SOFTMAX

LOGARCHMETH1

LOGINDEXBUILD

REC\_HIS\_RETENTN

1. **数据库管理参数(db2 get dbm cfg)**

FEDERATED

DIAGLEVEL

DIAGPATH

SYSADM\_GROUP/SYSCTRL\_GROUP/SYSMAINT\_GROUP/SYSMON\_GROUP

AUTHENTICATION

INSTANCE\_MEMORY

INTRA\_PARALLEL

1. **注册变量(db2set)**

DB2COMM

DB2CODEPAGE