

数据库安全-MSSQL

一、Sql-Server 简介

Sql server 是由微软公司开发设计的一个关系型数据库，具有使用方便，可伸缩性好，相关软件集成度高等优势。

- 1. 可伸缩性：具有高度可扩展性，可以通过增加服务器来提高处理速度。
- 2. 易用性：内置数据库管理工具，提供了丰富的图形化操作。
- 3. 可集成性高：可与微软其他产品无缝集成。（.net 开发者平台）
- 4. 安全性：有多层安全机制，包括 Windows 身份验证和默认强密码策略。
- 5. 恢复性：提供 always on availability groups 和故障转移集群。

二、Sql-Server 安装



Analysis Services 是一个分析数据引擎，用于决策支持和业务分析。 它为商业智能 (BI) 、数据分析和报表应用程序（如 Fabric/Power BI、Excel、Reporting Services 和其他数据可视化工具）提供企业级语义数据模型功能。

Reporting Services 用于创建、部署和管理分页报表。

SQL server 代理，是指对数据库的自动化操作，与 Windows 中的计划任务类似。

SQL server Browser 如果一个物理服务器上面有多个 SQL Server 实例，那么为了确保客

户端能访问到正确的实例，browser 为每一个数据库实例提供实例名称和版本号。

系统数据库中

Master: 记录了 SQL server 实例的所有系统级消息，包括实例范围的元数据（如登录账号）、端点、链接服务器和系统配置设置

msdb: 供 SQL SERVER 代理服务调度报警和作业以及记录操作员的使用，保存关于调度报警、作业、操作员等信息。

model: SQL SERVER 实例上创建的所有数据库的模板。

tempdb: 临时数据库，用于保存临时对象或中间结果集，为数据库的排列等操作提供一个临时工作空间。（每次启动都会重新创建）

Resource: 一个只读数据库，包含了 SQL SERVER 的所有系统对象。（隐藏的数据库）

三、SQL Server 基础语句

3.1 sql 语句分类

DDL-数据定义语句（CREATE , ALTER , DROP）

DML-数据操作语句（SELECT , DELETE , UPDATE , INSERT）

DCL-数据控制语言（GRANT , REVOKE , COMMIT , ROLLBACK）

3.2 建立、删除数据（库/表）

3.2.1 建立数据库

① CREATE DATABASE 数据库名称

② CREATE DATABASE 数据库名称 ON 数据文件类型（primary/secondary）

（NAME = ‘数据库文件逻辑名’，

FILENAME = ‘文件逻辑地址’，

SIZE = 数据库初始容量大小，

MAXSIZE = 数据库最大容量，

FILEGROWTH = 数据溢出，文件单次增长量）

LOG ON

(NAME = ‘数据库文件逻辑名’,

FILENAME = ‘文件逻辑地址’,

SIZE = 日志文件容量大小,

MAXSIZE = 日志文件容量,

FILEGROWTH = 数据溢出, 文件单次增长量)

-数据库文件类型

1.主要数据文件 (*.mdf)

主要数据文件包含数据库的启动信息, 并指向数据库中的其他文件, 存储部分或全部的数据。用户数据和对象可存储在此文件中, 也可以存储在次要数据文件中。

2.次要数据文件 (*.ndf)

次要数据文件是可选的, 由用户定义并存储用户数据, 用于存储主数据文件未能存储的剩余数据和一些数据库对象。

通过将每个文件放在不同的磁盘驱动器上, 次要文件可用于将数据分散到多个磁盘上。

如果数据库超过了单个 Windows 文件的最大大小, 可以使用次要数据文件, 这样数据库就能继续增长。

3.事务日志 (*.ldf)

事务日志文件保存用于恢复数据库的事务日志信息。数据库的插入、删除、更新等操作都会记录在日志文件中, 而查询不会记录在日志文件中。整个的数据库有且仅有一个日志文件。

-练习

用方法①创建数据库 test

用方法②创建数据库 grade, 数据库文件和日志文件要求初始容量为 3mb, 单次增长量为 20%。

3.2.2 建立数据表

CREATE TABLE 表名

(列名 数据类型 约束条件)

--约束条件包括:

1.主键约束 (PRIMARY KEY): 主键用于标识表中的每一条记录, 具有唯一性且不可为空 (NOT NULL), 可以定义一列或多列为主键。

2.唯一性约束 (UNIQUE): 唯一性约束用来限制非主键列的数据唯一性。

3.默认值 (DEFAULT): 为某一字段设置默认值

4.范围约束 (CHECK): 对某一字段的范围进行限制。

--练习

1.建立数据表 student:

姓名	性别	生日	年龄	地址	电话	邮件

2.建立学科表 course:

3.建立成绩表 grade:

3.2.3 获取元数据

--获取当前数据库名称

SELECT db_name();

--获取当前数据库所有表名称

Select name from sysobjects where XTYPE='u' order by name; (XTYPE='U': 表示所有用户表; XTYPE='S': 表示所有系统表。)

--获取所有数据库名称

select name from master..sysdatabases order by name;

--获取所有字段名称

select * from syscolumns where id=object_id('表名')

--查询数据库版本

Select @VERSION;

3.2.4 删除数据库/表

--删除数据库

Drop database 数据库名称 (批量删除, 名称用逗号隔开)

--删除数据表

DROP table 表名称

--练习

删除数据库 test, 新建表 test1,test2 并删除。

3.2.5 处理数据表

--增加字段

alter table 表名

add 字段名 1 数据类型 1 约束条件 1 (增加多个字段, 用逗号隔开)

--修改字段属性

alter table 表名

alter column 字段名 (数据类型) (约束条件)

--删除列

alter table 表名

drop column 字段名

--删除字段约束条件

Alter table 表名

Drop constraint 约束条件编号

--练习

1.增加婚否列和备注列

2.修改备注列的字段长度

3.删除婚否列、备注列、邮箱、地址列

3.3. 处理数据

3.3.1 插入数据

--插入单组数据

insert into 表名 (字段 1, 字段 2...) values (数据 1, 数据 2...)

-数据与字段一一对应;

-如果数据组中包含所有字段的数据且为默认顺序, 则字段可省略不写

--插入多组数据

insert into 表名 select 数据组 1 union

select 数据组 2 union

select 数据组 3...

3.3.2 修改数据

update 表名 set 字段名='字段值' where 特征字段='字段值'

3.3.3 删除数据

delete 表名 set 字段名='字段值' where 特征字段='字段值'

delete from 表名 where 特征字段='字段值'

--练习

1.在表 student 中插入数据

姓名	性别	生日	年龄	电话
Messi	man	1987-6-24		
Neymar	man	1992-2-5		123456789
Suarez	Man	1987-1-24		987456321
Yamal	man	2007-7-13		654123987
Lew	man	1988-8-21		321654987
Nico	man	2002-7-12		741852963

2.修改 messi 的电话号码为 963852741

3.删除关于 Lew、Neymar、suarez 的数据

4.在表 course 中插入数据 “math、Eng、Chinese、phy”

5.在表 grade 中随机插入数据

3.3.4 查询数据

--count，返回在集合中找到的项目数

Select count() from

--MAX ()、MIN ()、AVG ()

Select max() from

--排序后查询 order by

Select from 表名 order by 字段

默认升序，降序末尾添加 desc

--对查询结果分组 group by

select 字段名 1, count() from 表名 group by 字段名 1

--条件查询 where 和 having

where 用于查询结果产生之前，having 是用于查询结果产生之后。

--练习

- 1.查询 student 表中有多少人
- 2.用两种办法找出最高分
- 3.查询每科最高分
- 4.查询年龄大于 25 的人
- 5.查询平均成绩低于 80 分的学生
- 6.用两种方法查询男生有多少人
- 7.用两种方法查询至少有一门课程不及格的学生