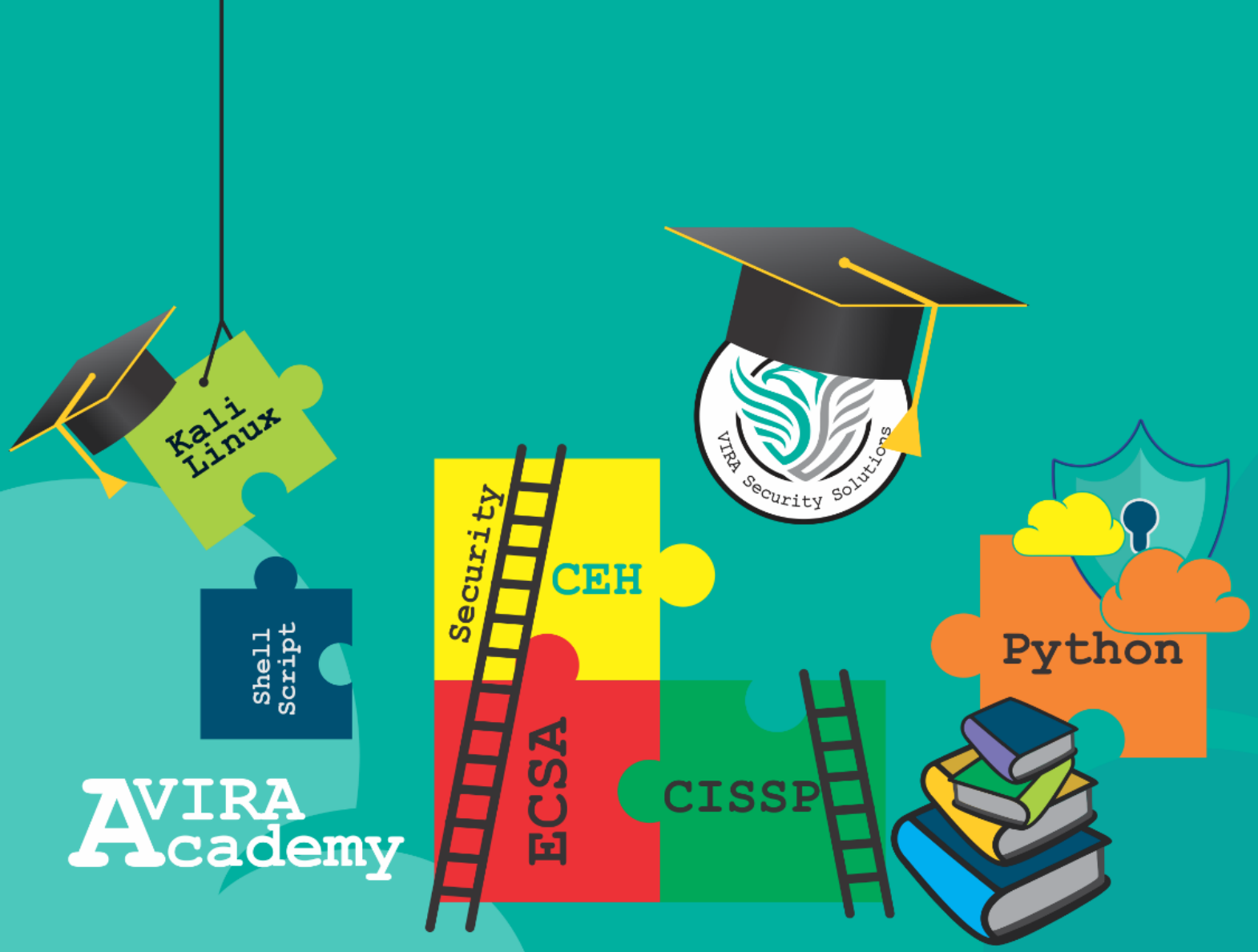
VIRA
Security
Solutions

راهکارهای امن ویرا
شماره ثبت: ۵۴۰۱۳۹
VIRA Security Solutions


Kali Linux
Shell Script
VIRA Academy
Security
CEH
ECSA
CISSP
VIRA Security Solutions
Python

DBA

SQL Server Administration

Part3

Mohammad Reza Gerami
mrgerami@aut.ac.ir
gerami@virasec.ir

Vira Security Solutions

Object Level Permissions

Vira Security Solutions

Object Level Permissions

- Access to a resource in SQL server is determined with the permissions on that resource assigned to a login, user, or role
- Different type of resources in SQL Server have different types or permissions
- The GRANT, REVOKE, DENY statements assign permissions
- Multiple permissions can be assigned to a user or role
- Multiple users can have the same permissions to resources

Vira Security Solutions

Object Level Permissions

Vira Security Solutions

- Lab Demo

```
Select * from Students

GRANT SELECT ON dbo.students TO vira

USE [vsfs_academy]
GO

INSERT INTO [dbo].[students]
        ([id]
        ,[name]
        ,[family]
        ,[mobile]
        ,[email]
        ,[fathername]
        ,[grade]
        ,[datereg]
        ,[datestart]
        ,[dateend])
    VALUES
        (1,'Mohammad Hosein','Gerami','09171500000','mh.gerami@gmail.com', ','18.5','20200110','20200201','20200520')

GO

GRANT INSERT ON dbo.students TO vira
```

System Databases

Vira Security Solutions

System Databases

SQL Server includes the following system databases.

System database	Description
master	Records all the system-level information for an instance of SQL Server.
msdb	Is used by SQL Server Agent for scheduling alerts and jobs.
model	Is used as the template for all databases created on the instance of SQL Server. Modifications made to the model database, such as database size, collation, recovery model, and other database options, are applied to any databases created afterward.
tempdb	Is a workspace for holding temporary objects or intermediate result sets.

These cannot be deleted or renamed

Vira Security Solutions

System Databases

- The master database is the main repository for information about the SQL Server instance
- The path to the master database is passed as a parameter to sqlserv.exe
- This is the default database for new logins, but should be changed
- It is a good idea to now create any objects inside of the master database
- Server level principals and security objects

Vira Security Solutions

System Databases

master database

- File Locations of the user databases
- Login accounts
- Server configuration settings
- Linked servers information
- Startup stored procedures

Vira Security Solutions

System Databases

- The msdb database is the administrative database for SQL Server

- Various **maintenance items** are stored here, such as:
  - Backup and Restore information
  - SQL Server Agent Job and results
  - SSIS packages and results
  - Log shipping information
  - Policy Based Management information

Vira Security Solutions

System Databases

- The model database is the template for all new user databases

- Any changes made to the model database, either options or objects, will be copied into all new databases created

Vira Security Solutions

System Databases

- The tempdb is a shared resource used by SQL Server all users
- Tempdb is used for temporary objects, worktables, online index operations, cursors, table variables, and the snapshot isolation version store, among other things
- It is recreated every time that the server is restarted
- As tempdb is non-permanent storage, backups and restores are not allowed for this database.

Vira Security Solutions

System Databases

- All System databases use the simple recovery model, but can be changed
- All System databases should be regularly backed up
- Tempdb should not be included in maintenance

Vira Security Solutions

User Databases

Vira Security Solutions

User Databases

- User databases are the databases created by the administrators or applications on a SQL Server instance where all user data is stored

- Each user database will have multiple files on disk that SQL Server manages and that contain the information, there are two files for each database:
  - .mdf – Primary data file
  - .ldf – Primary log file

- There can be additional, optional, files as well
  - .ldf – Additional log files
  - .ndf – Additional data files

- The file extensions are not required, but are used by convention

Vira Security Solutions

User Databases

- Lab Demo
  - Create a database and check properties and compare with model database
    - Size
    - Files
    - …

Vira Security Solutions

User Databases

Filegroup types are separated into ***Row or Primary*** , **FILESTREAM data or Memory-Optimized** filegroups.

Row filegroups contain regular data and log files.
FILESTREAM data filegroups contain FILESTREAM data files.(docs,…)
These data files **store information about how binary large object** (BLOB) **data is stored on the file system** when you are using FILESTREAM storage. The options are the same for both types of filegroups.

دسته بندی DataFileهای بانک اطلاعاتی می باشد.
FileGroup برای LogFile قابل استفاده نیست و کارایی آن صرفا مربوط به DataFileها می باشد.

Vira Security Solutions

User Databases

Data File Group

Primary File Group

پیش فرض SQL Serverبوده و برای DataFileها ایجاد می شوند.
محل قرار گیری جداول سیستمی است.
وجود آن ضروری می باشد.

برای مشاهده اشیاء سیستمی موجود در Primary File Groupمی توان از دستور زیر استفاده نمود:

```
SELECT * FROM SYS.objects S
WHERE S.type_desc IN
('SYSTEM_TABLE','INTERNAL_TABLE','SERVICE_QUEUE')
GO
```

User Defined File Group

توسط کاربر تعریف می شوند.
برای ذخیره جداول و ایندکس ها مورد استفاده قرار می گیرند.

Vira Security Solutions

User Databases

File Stream File Group

- برای ذخیره Unstructured Data خارج از پایگاه داده بکار می روند
- Documents, PDF و...

Memory Optimized Data

- مختص SQL Server 2014 می باشد.
- معماری آن شبیه به File Stream می باشد.

Vira Security Solutions

رعایت چند نکته دراستفاده از File Group

موارد زیر در استفاده از FileGroupها در یک پایگاه داده باید در نظر گرفته شود:

- پخش شدن داده ها مابین DataFileها: تمامی داده ها با کمک الگوریتم (RoundRobinنوبت گردشی) و با درصدهای مساوی بین DataFileهای موجود در یک File Groupتقسیم می شوند.
- رشد DataFileها: تا تمامی DataFileهای موجود در یک File Groupپر نشوند Growingاتفاق نمی افتد.
- امکان قرار دادن جداول در File Groupها

Vira Security Solutions

دلایل استفاده از File Groupها

۱. جدا کردن جداول از یکدیگر

به منظور کم نمودن زمان اجرای پرس و جوها و تعدیل عملیات IOبهتر است جداول مربوط به هر سیستم از یکدیگر جدا شوند.

۲. جدا کردن NonClustered Indexها

به دلیل اینکه NonClustered Indexها در فایلهای جداگانه نگهداری می شوند می توان برای بالا بردن کارایی پایگاه داده نسبت به جدا نمودن آنها اقدام نمود

Vira Security Solutions

User Databases

۳. پارتیشن بندی جداول: تقسیم بندی جداول در ساختارهای ذخیره سازی جداگانه

۴. جدا کردن جداول سیستمی از سایر جداول پایگاه داده

۵. جدا کردن داده های LOB: با جدا نمودن Large Objectها از سایر داده ها با کمک FileGroup باعث بهبود کارایی پایگاه داده خواهیم شد.

۶. ReadOnlyنمودن بخش خاصی از پایگاه داده

۷. تهیه پشتیبان از بخش خاصی از پایگاه داده

Vira Security Solutions

User Databases

ReadOnly نمودن بخش خاصی از پایگاه داده:
اینکار را با استفاده از دستور زیر می توان انجام داد:

```
ALTER DATABASE Test01 MODIFY FILEGROUP
FG_ReadOnlyData READONLY WITH ROLLBACK IMMEDIATE
GO
```

Vira Security Solutions

User Databases

تهیه پشتیبان از بخش خاصی از پایگاه داده: با اینکار هم حجم فایل پشتیبان کمتر می شود و هم مدت زمان کمتری برای گرفتن پشتیبان صرف می شود. برای اینکار کافیست دستور زیر را اجرا نمایید

```
BACKUP DATABASE DB_Name FILEGROUP = 'FG_Name'
TO  DISK = 'Destination File' WITH STATS=1
GO
```

Vira Security Solutions

Large Object (**LOB**)

Vira Security Solutions

LOBچیست؟

LOBها شامل داده هایی هستند که دارای دو ویژگی زیر می باشند:

دارای حجم زیادی هستند.

عموما غیر ساخت یافته می باشند.

به هر داده ای که ساختار باینری داشته باشد غیر ساخت یافته گفته می شود

برای مثال فیلم، عکس، pdf، فایلهای excel, word و...

Vira Security Solutions

User Databases

برای ذخیره داده های بدون ساختار در بانک اطلاعاتی اوراکل، ابتدا نوع داده LONG وLONG RAW ارائه شد که LONG برای ذخیره کاراکترهای با حجم زیاد و LONG RAW برای فایلهای باینری(صوت، تصویر و ..) استفاده می شد(و البته می شود) این نوع داده دارای محدودیتهای بسیاری بودند که شاید به همین دلیل اوراکل در نسخه i۸، نوع داده (LOB(large object را معرفی کرد که بسیاری از محدودیتهای LONG وLONG RAW را برطرف می کند

Vira Security Solutions

User Databases

از جمله این رفع محدودیتها می توان به موراد زیر اشاره کرد:

۱.گنجایش مصرفی نوع داده LOBبرابر با ۴ گیگابایت می باشد در صورتی که LONGو LONG RAWبیشتر از ۲ گیگابایت را پشتیبانی نمی کنند.

۲.در هر جدول می توان از چندین ستون با نوع داده LOBاستفاده کرد در صورتی که نوع داده ای LONG RAWو LONGنمی توانند بیشتر از یک ستون در یک جدول داشته باشند.

۳.نوع داده ای LOBدسترسی تصادفی را پشتیبانی می کند ولی نوع داده LONGتنها دسترسی ترتیبی را پشتیبانی می کند.

۴.استفاده از LONGو LONG RAWدر بسیاری از عملیات از قبیل replicationمیسور نیست در صورتی که این عملیات برای LOBها ممکن می باشد.

۵.با استفاده از نوع داده LOBکاربر می تواند نوع داده دیگری تعریف کند(.user-defined datatype)

6.امکان ذخیره LOB segmentدر خارج از جدول و حتی در tablespaceدیگر هم ممکن خواهد بود(البته LOB locatorباید در جدول اصلی ذخیره شود). در صورتی که برای نوع داد longو long rawچنین قابلیتی وجود ندارد و داده های با این نوع، باید در خود جدول ذخیره شوند.

Vira Security Solutions

User Databases

LOBو محدودیتها

صرف نظر از نوع داده LONGو LONG

RAW، نوع داده LOBهم محدودیتهایی دارد که از جمله این محدودیتها می توان به موارد زیر اشاره کرد(محدودیت نه الزاما به معنی منفی آن):

۱.این نوع از ستون نمی توانند کلید اصلی باشند.

۲.بعضی از عملیاتی که از طریق dblinkقابل انجام است، با این نوع داده ممکن نخواهد بود(البته بعضی از عملیات).

۳.نوع داده LOBتوسط جدول کلاستر(منظور objectمی باشد نه RAC)پشتیبانی نمی شود.

۴.ستون از این نوع داده را نمی توان با عبارات و توابع زیر به کار برد:

ANALYZE ،SELECT… UNIQUE ،SELECT… DISTINCT ،aggregate function ،ORDER BY ،ORDER BY

Vira Security Solutions

LOBو انواع آن

LOBها انواع مختلفی دارند که در ادامه در مورد هر یک از آنها، به اختصار مطالبی آورده شده است:

۱. CLOB : این نوع از LOBها برای ذخیره متنهای با حجم بالا به کار می روند. همچنین کاراکترست در این نوع از LOBها، همان کاراکترست پیش فرض بانک می باشد.

۲. NCLOB: همانند CLOB می باشد که برای ذخیره متن با فرمت national character set بانک، مورد استفاده قرار می گیرد.

۳. BLOB: این نوع داده، اطلاعات باینری از قبیل عکس، صوت، مستندات و .. را شامل می شود.

۴. BFILE : در هنگام استفاده از BLOB، اطلاعات در درون بانک اطلاعاتی ذخیره می شوند حال اگر بخواهیم ذخیره اطلاعات در خارج از بانک اطلاعاتی و بر روی سیستم عامل انجام شوند، می توان از این نوع داده استفاده کرد. این نوع از داده محدودیتهای بسیار زیادی را در بر دارند به طور مثال، نمی توانند در بکاپ و ریکاوری سطح بانک شرکت کنند به همین دلیل معمولا داده هایی که اصلاح و بروزرسانی در مورد آنها در موارد شاذ و نادر اتفاق می افتد، از این نوع داده بهره می گیرند.

Vira Security Solutions

Recovery Models

Vira Security Solutions

Recovery Models

عملیات بکاپ‌گیری (Backup) و بازگردانی اطلاعات (Restore)در SQL Server مطابق با نوع Recovery Model در دیتابیس مورد نظر انجام می‌پذیرد. در واقع Recovery Modelها برای کنترل نگهداری Transaction Logها طراحی شده‌اند.

یک Recovery Modelجزئی از دیتابیس است که بر موارد زیر کنترل و نظارت دارد:

- چگونگی ذخیره تراکنش‌ها بصورت Log
- چگونگی نیاز Transaction Logها به بکاپ‌گیری
- استفاده درست و به موقع از انواع عملیات بازگردانی اطلاعات (Restore)

Vira Security Solutions

Recovery Models

به طور کلی در SQL Server سه نوع Recovery Model به شرح زیر وجود دارد:

- مدل بازیابی Full
- مدل بازیابی Simple
- مدل بازیابی Bulk-Logged

Vira Security Solutions

Recovery Models

مدل بازیابی کامل یا Full Recovery Model

در این Recovery Modelتا زمانی‌که از Transaction Logها Backupگرفته نشود، SQLاقدام به حذف آنها نمی‌کند و Logها زمانی حذف خواهند شد که به یکی از روش‌های Full، Differentialو یا Transaction Logاز دیتابیس Backupتهیه گردد. در صورتی‌که Databaseدچار مشکل شود، با استفاده از Full Recovery Modelبیشترین انعطاف پذیری برای بازیابی اطلاعات در Databaseوجود دارد. از بزرگترین مزیت‌های این نوع Recovery Modelاین است که در هنگام بازیابی اطلاعات قادر خواهید بود آنها را به زمان و تاریخی که مدنظرتان است بازیابی کنید و این ویژگی به ما امکان استفاده از قابلیت نقطه زمانی بازیابی (Point In Time Recovery)را می‌دهد. مدت زمانی که طول می‌کشد SQL Serverاز Transaction Logها Backupتهیه کند در واقع تعیین کننده حجم اطلاعاتی است که در زمان بروز حادثه می‌توان بازیابی کرد.

Vira Security Solutions

Recovery Models

مدل بازیابی Bulk-Logged Recovery Model

این مدل ریکاوری شباهت بسیار زیادی به Full Recovery Modelدارد اما تفاوت اصلی بین این دو مدل در روشی است که مدل ریکاوری Bulk-loggedبرای مدیریت عملیات‌های گسترده تغییرات در اطلاعات انجام می‌دهد. در واقع این روش برای ثبت اطلاعات و عملیات ها در Transaction Logها، از روشی به نام Minimal Loggingاستفاده می‌کند. با استفاده از این روش سرعت پردازشی بسیار بالا می‌رود، زمان پردازش‌ها طبیعتاً کاهش پیدا می‌کند و میزان فضای مصرفی برای اغلب عملکردها کاهش می‌یابد. اما در این روش قابلیت استفاده از Point In Time Restoreرا نخواهید داشت. در این مدل، حجم فایل Transaction Logها نسبت به مدل ریکاوری Fullبسیار کمتر خواهد شد. در رابطه با این نوع Recoveryمایکروسافت پیشنهاد می‌کند که از Bulk-logged Recovery Modelبصورت مقطعی و موردی استفاده شود و نمی‌بایست آن را به عنوان یک راهکار دائمی در نظر گرفت. توجه داشته باشید اگر سازمان شما به گونه‌ای باشد که نیاز داشته باشید مدل ریکاوری شما از Full Loggingبه Minimal Loggingتغییر پیدا کند، باید توجه داشته باشید زمانی اقدام به انجام این عملیات کنید که کاربران در حال بروزرسانی یا ثبت اطلاعات جدید در Databaseها نباشند، زیرا در این صورت امکان از بین رفتن داده‌ها حین انجام عملیات وجود دارد.

Recovery Models

مدل بازیابی ساده یا Simple Recovery Model

هدف اصلی این روش این است که SQL Serverحداقل اندازه اطلاعات را در Transaction Logهای خود داشته باشد. در این حالت SQL Serverهرگاه که Databaseبه یک Transaction Checkpointبرسد، اطلاعات Transaction Logها را حذف می‌کند (که در اصطلاح به اینکار Truncateکردن گفته می‌شود) که در پی آن هیچ Logی برای انجام عملیات Disaster Recoveryوجود نخواهد داشت. استفاده از این مدل ریکاوری باعث می‌شود که فقط امکان بازگردانی اطلاعات از دیتابیس‌هایی وجود داشته باشد که به روش‌های Fullو Differentialبکاپ‌گیری صورت گرفته است. در حالت Simple Recovery Modelقابلیت بازیابی اطلاعات به یک نقطه زمانی خاص وجود ندارد و تنها می‌توان اطلاعات را به طور کامل با استفاده از Full Backupیا Differential Backupبه زمانی برگرداند که Backupها ایجاد شده اند. در استفاده از این حالت ریکاوری با خالی شدن Transaction Logها فضای بیشتری در هارد دیسک شما برای انجام فرآیندهای دیگر باز خواهد شد.

Vira Security Solutions