



---

## Administering a SQL Database Infrastructure

### MCSA: SQL 2016 Database Administration

DURATION: 5 DAYS

COURSE CODE: M20764

FORMAT: LECTURE/LAB

---

#### WHY FIREFLY

Firefly is trusted by customers, technology vendors and channel partners around the world to deliver highly effective, immersive educational experiences. Our innovative, role-based Microsoft training covers all of the latest certifications, from Azure to Server 2016 to SQL to the modern desktop, and is designed engineers the skills they need to remain relevant in today's multcloud world.

#### WHO SHOULD ATTEND

The primary audience for this course is individuals who administer and maintain SQL Server databases. These individuals perform database administration and maintenance as their primary area of responsibility, or work in environments where databases play a key role in their primary job.

---

#### COURSE DESCRIPTION

This five-day instructor-led course provides students who administer and maintain SQL Server databases with the knowledge and skills to administer a SQL server database infrastructure. Additionally, it will be of use to individuals who develop applications that deliver content from SQL Server databases.

---

#### PREREQUISITES

Basic knowledge of the Microsoft Windows operating system and its core functionality

Working knowledge of Transact-SQL

Working knowledge of relational databases

Some experience with database design

---

#### LEARNING OBJECTIVES

Authenticate and authorize users

Assign server and database roles

Authorize users to access resources

Protect data with encryption and auditing

Describe recovery models and backup strategies

Backup SQL Server databases

Restore SQL Server databases

Automate database management

Configure security for the SQL Server agent

Manage alerts and notifications

Managing SQL Server using PowerShell

Trace access to SQL Server

Monitor a SQL Server infrastructure

Troubleshoot a SQL Server infrastructure

Import and export data

## COURSE OUTLINE

### 1. SQL Server Security

Protection of data within your Microsoft SQL Server databases is essential and requires a working knowledge of the issues and SQL Server security features. This module describes SQL Server security models, logins, users, partially contained databases, and cross-server authorization.

Authenticating Connections to SQL Server

Authorizing Logins to Connect to databases

Authorization Across Servers

Partially Contained Databases

#### Lab : Authenticating Users

Create Logins

Create Database Users

Correct Application Login Issues

Configure Security for Restored Databases

### 2. Assigning Server and Database Roles

Using roles simplifies the management of user permissions. With roles, you can control authenticated users' access to system resources based on each user's job function—rather than assigning permissions user-by-user, you can grant permissions to a role, then make users members of roles. Microsoft SQL Server includes support for security roles defined at server level and at database level.

Working with server roles

Working with Fixed Database Roles

Assigning User-Defined Database Roles

#### Lab : Assigning server and database roles

Assigning Server Roles

Assigning Fixed Database Roles

Assigning User-Defined Database Roles

Verifying Security

### 3. Authorizing Users to Access Resources

In the previous modules, you have seen how Microsoft SQL Server security is organized and how sets of permissions can be assigned at the server and database level by using fixed server roles, user-defined server roles, fixed database roles, and application roles. The final step in authorizing users to access SQL Server resources is the authorization of users and roles to access server and database objects. In this module, you will see how these object permissions are managed. In addition to access permissions on database objects, SQL Server provides the ability to determine which users are allowed to execute code, such as stored procedures and functions. In many cases, these permissions and the permissions on the database objects are best configured at the schema level rather than at the level of the individual object. Schema-based permission grants can simplify your security architecture. You will explore the granting of permissions at the schema level in the final lesson of this module.

Authorizing User Access to Objects

Authorizing Users to Execute Code

Configuring Permissions at the Schema Level

#### Lab : Authorizing users to access resources

Granting, Denying, and Revoking Permissions on Objects

Granting EXECUTE Permissions on Code

Granting Permissions at the Schema Level

### 4. Protecting Data with Encryption and Auditing

When configuring security for your Microsoft SQL Server systems, you should ensure that you meet any of your organization's compliance requirements for data protection. Organizations often need to adhere to industry-specific compliance policies, which mandate auditing of all data access. To address this requirement, SQL Server provides a range of options for implementing auditing. Another common compliance requirement is the encryption of data to protect against unauthorized access in the event that access to the database files is compromised. SQL Server supports this requirement by providing transparent data encryption (TDE). To reduce the risk of information leakage by users with administrative access to a database, columns containing sensitive data—such as credit card numbers or national identity numbers—can be encrypted using the Always Encrypted feature. This module describes the available options for auditing in SQL Server, how to use and manage the SQL Server Audit feature, and how to implement encryption.

Options for auditing data access in SQL Server

Implementing SQL Server Audit

Managing SQL Server Audit

Protecting Data with Encryption

#### Lab : Using Auditing and Encryption

Working with SQL Server Audit

Encrypt a Column as Always Encrypted

Encrypt a Database using TDE

### 5. Recovery Models and Backup Strategies

One of the most important aspects of a database administrator's role is ensuring that organizational data is reliably backed up so that, if a failure occurs, you can recover the data. Even though the computing industry has known about the need for reliable backup strategies for decades—and discussed this at great length—unfortunate stories regarding data loss are still commonplace. A further problem is that, even when the strategies in place work as they were designed, the outcomes still regularly fail to meet an organization's operational requirements. In this module, you will consider how to create a strategy that is aligned with organizational needs, based on the available backup models, and the role of the transaction logs in maintaining database consistency.

Understanding Backup Strategies

SQL Server Transaction Logs

Planning Backup Strategies

#### Lab : Understanding SQL Server recovery models

Plan a Backup Strategy

Configure Database Recovery Models

## COURSE OUTLINE

### 6. Backing Up SQL Server Databases

In the previous module, you learned how to plan a backup strategy for a SQL Server system. You can now learn how to perform SQL Server backups, including full and differential database backups, transaction log backups, and partial backups. In this module, you will learn how to apply various backup strategies.

Backing Up Databases and Transaction Logs

Managing Database Backups

Advanced Database Options

#### Lab : Backing Up Databases

Backing Up Databases

Performing Database, Differential, and Transaction Log Backups

Performing a Partial Backup

### 7. Restoring SQL Server 2016 Databases

In the previous module, you learned how to create backups of Microsoft SQL Server 2016 databases. A backup strategy might involve many different types of backup, so it is essential that you can effectively restore them. You will often be restoring a database in an urgent situation. You must, however, ensure that you have a clear plan of how to proceed and successfully recover the database to the required state. A good plan and understanding of the restore process can help avoid making the situation worse. Some database restores are related to system failure. In these cases, you will want to return the system as close as possible to the state it was in before the failure. Some failures, though, are related to human error and you might wish to recover the system to a point before that error. The point-in-time recovery features of SQL Server 2016 can help you to achieve this. Because they are typically much larger, user databases are more likely to be affected by system failures than system databases. However, system databases can be affected by failures, and special care should be taken when recovering them. In particular, you need to understand how to recover each system database because you cannot use the same process for all system databases. In this module, you will see how to restore user and system databases and how to implement point-in-time recovery.

Understanding the Restore Process

Restoring Databases

Advanced Restore Scenarios

Point-in-Time Recovery

#### Lab : Restoring SQL Server Databases

Restoring a Database Backup

Restoring Database, Differential, and Transaction Log Backups

Performing a Piecemeal Restore

### 8. Automating SQL Server Management

The tools provided by Microsoft SQL Server make administration easy when compared to some other database engines. However, even when tasks are easy to perform, it is common to have to repeat a task many times. Efficient database administrators learn to automate repetitive tasks.

This can help to avoid situations where an administrator forgets to execute a task at the required time. Perhaps more importantly, the automation of tasks helps to ensure that they are performed consistently, each time they are executed. This module describes how to use SQL Server Agent to automate jobs, how to configure security contexts for jobs, and how to implement multiserver jobs.

Automating SQL Server management

Working with SQL Server Agent

Managing SQL Server Agent Jobs

Multi-server Management

#### Lab : Automating SQL Server Management

Create a SQL Server Agent Job

Test a Job

Schedule a Job

Configure Master and Target Servers

### 9. Configuring Security for SQL Server Agent

Other modules in this course have demonstrated the need to minimize the permissions that are granted to users, following the principle of "least privilege." This means that users have only the permissions that they need to perform their tasks. The same logic applies to the granting of permissions to SQL Server Agent. Although it is easy to execute all jobs in the context of the SQL Server Agent service account, and to configure that account as an administrative account, a poor security environment would result from doing this. It is important to understand how to create a minimal privilege security environment for jobs that run in SQL Server Agent.

Understanding SQL Server Agent Security

Configuring Credentials

Configuring Proxy Accounts

#### Lab : Configuring Security for SQL Server Agent

Analyzing Problems in SQL Server Agent

Configuring a Credential

Configuring a Proxy Account

Configuring and testing the Security Context of a Job

### 10. Monitoring SQL Server with Alerts and Notifications

One key aspect of managing Microsoft SQL Server in a proactive manner is to make sure you are aware of problems and events that occur in the server, as they happen. SQL Server logs a wealth of information about issues. You can configure it to advise you automatically when these issues occur, by using alerts and notifications. The most common way that SQL Server database administrators receive details of events of interest is by email message. This module covers the configuration of Database Mail, alerts, and notifications for a SQL Server instance, and the configuration of alerts for Microsoft Azure SQL Database.

Monitoring SQL Server Errors

Configuring Database Mail

Operators, Alerts, and Notifications

Alerts in Azure SQL Database

## COURSE OUTLINE

- Lab : Monitoring SQL Server with Alerts and Notifications**  
Configuring Database Mail  
Configuring Operators  
Configuring Alerts and Notifications  
Testing Alerts and Notifications
- 11. Introduction to Managing SQL Server by using PowerShell**  
This module looks at how to use Windows PowerShell with Microsoft SQL Server. Businesses are constantly having to increase the efficiency and reliability of maintaining their IT infrastructure; with PowerShell, you can improve this efficiency and reliability by creating scripts to carry out tasks. PowerShell scripts can be tested and applied multiple times to multiple servers, saving your organization both time and money.  
Getting Started with Windows PowerShell  
Configure SQL Server using PowerShell  
Administer and Maintain SQL Server with PowerShell  
Managing Azure SQL Databases using PowerShell  
**Lab : Using PowerShell to Manage SQL Server**  
Getting Started with PowerShell  
Using PowerShell to Change SQL Server settings
- 12. Tracing Access to SQL Server with Extended events**  
Monitoring performance metrics provides a great way to assess the overall performance of a database solution. However, there are occasions when you need to perform more detailed analysis of the activity occurring within a Microsoft SQL Server instance—to troubleshoot problems and identify ways to optimize workload performance. SQL Server Extended Events is a flexible, lightweight event-handling system built into the Microsoft SQL Server Database Engine. This module focuses on the architectural concepts, troubleshooting strategies and usage scenarios of Extended Events.  
Extended Events Core Concepts  
Working with Extended Events  
**Lab : Extended Events**  
Using the System\_Health Extended Events Session  
Tracking Page Splits Using Extended Events
- 13. Monitoring SQL Server**  
The Microsoft SQL Server Database Engine can run for long periods without the need for administrative attention. However, if you regularly monitor the activity that occurs on the database server, you can deal with potential issues before they arise. SQL Server provides a number of tools that you can use to monitor current activity and record details of previous activity. You need to become familiar with what each of the tools does and how to use them. It is easy to become overwhelmed by the volume of output that monitoring tools can provide, so you also need to learn techniques for analyzing their output.  
Monitoring activity  
Capturing and Managing Performance Data  
Analyzing Collected Performance Data  
SQL Server Utility  
**Lab : Monitoring SQL Server**
- 14. Troubleshooting SQL Server**  
Database administrators working with Microsoft SQL Server need to adopt the important role of troubleshooter when issues arise—particularly if users of business-critical applications that rely on SQL Server databases are being prevented from working. It is important to have a solid methodology for resolving issues in general, and to be familiar with the most common issues that can arise when working with SQL Server systems.  
A Trouble Shooting Methodology for SQL Server  
Resolving Service Related Issues  
Resolving Connectivity and Log-in issues  
**Lab : Troubleshooting Common Issues**  
Troubleshoot and Resolve a SQL Login Issue  
Troubleshoot and Resolve a Service Issue  
Troubleshoot and Resolve a Windows Login Issue  
Troubleshoot and Resolve a Job Execution Issue  
Troubleshoot and Resolve a Performance Issue
- 15. Importing and Exporting Data**  
While a great deal of data residing in a Microsoft SQL Server system is entered directly by users who are running application programs, there is often a need to move data in other locations, to and from SQL Server. SQL Server provides a set of tools you can use to transfer data in and out. Some of these tools, such as the bcp (Bulk Copy Program) utility and SQL Server Integration Services, are external to the database engine. Other tools, such as the BULK INSERT statement and the OPENROWSET function, are implemented in the database engine. With SQL Server, you can also create data-tier applications that package all the tables, views, and instance objects associated with a user database into a single unit of deployment. In this module, you will explore these tools and techniques so that you can import and export data to and from SQL Server.  
Transferring Data to and from SQL Server  
Importing and Exporting Table Data  
Using bcp and BULK INSERT to Import Data  
Deploying and Upgrading Data-Tier Application  
**Lab : Importing and Exporting Data**  
Import and Excel Data Using the Import Wizard  
Import a Delimited Text File Using bcp  
Import a Delimited Text File using BULK INSERT  
Create and Test an SSIS Package to Extract Data  
Deploy a Data-Tier Application