



SQL SERVER SECURITY MANAGEMENT

Course ID : SQL-ADM-Secure



Scan for Details
on Our [Website](#)



Duration: 2 Days

(12 Hours) 09:00 AM – 04:00 PM



Price: Call (Inhouse training only)

* (excluding VAT 7%)

* Eligible for 200% tax deduction



Training Schedule

www.9experttraining.com

Category: Data

Security management in Microsoft SQL Server must be addressed from installation through to the object level. This course covers SQL Server security from the initial installation, ensuring compatibility with the operational environment (such as domain environments). Microsoft SQL Server provides multiple layers of security management, from the instance level down to the database and schema levels, which serve as security boundaries for database objects. Security management includes authentication configuration,

assignment of access rights, security auditing, and the use of encryption technologies to protect sensitive data.

Objectives

1. Participants will be able to select appropriate service accounts for their environment.
2. Participants will be able to create and manage identities at various levels.
3. Participants will be able to choose appropriate technologies for data protection.

Target Audience

1. Microsoft SQL Server administrators
2. Consultants
3. Directors and management personnel
4. Individuals interested in SQL Server security

Prerequisites

Some experience in administering Microsoft SQL Server

System Requirements

1. Windows 11 or Windows 10
2. CPU : 1.6 GHz or faster
3. RAM : 8 GB or higher
4. Remote Desktop Connection
5. Stable Internet access

TRAINING TOPICS

 DAY 1 Morning Session

9:00 AM – 12:00 PM

1. SQL Server Security

- Authentication methods for accessing Microsoft SQL Server
- Understanding securable resources
- Understanding security principals
- Permission management
- Overview of Microsoft SQL Server security
- Creating and managing logins
- Configuring password policies via Local Security Policy or Group Policy Object
- Mapping logins to database users
- Granting database access
- Managing database users, including dbo and guest
- Querying login permissions using user tokens
- Cross-server permissions with linked servers
- The "Double-Hop" issue
- Impersonation versus delegation
- Handling SID mismatches and resolving orphaned users
- Introduction to partially contained databases
- Key considerations for partially contained databases

2. Managing Server Roles and Database Roles

- Using server roles
- Understanding fixed server roles
- Understanding user-defined server roles
- Understanding the public server role
- Using database roles
- Understanding fixed database roles
- Assigning database principals to appropriate database roles
- Database ownership
- Understanding user-defined database roles
- Using roles in common administrative scenarios
- Understanding application roles

3. Access Permission Management

- Granting users access to objects
- GRANT, REVOKE, DENY statements
- Table and view security
- Column-level security
- Row-level security
- WITH GRANT OPTION
- Security for stored procedures
- Security for user-defined functions

- Security for user-defined table-valued functions (TVFs)
- Security considerations for managed code
- Schema-level permission configuration
- Overview of user–schema relationships
- Object naming conventions
- Granting permissions at the schema level effectively

4. Auditing

- Options for auditing data access
- Understanding Common Criteria Compliance
- Auditing with triggers
- Auditing with temporal tables
- Auditing using SQL Trace
- Creating SQL Server audits
- Introduction to extended events
- Configuring server-level audits
- Audit actions and action groups
- Creating server audit specifications
- Creating database audit specifications
- Querying audit data
- Understanding audit log structure
- Common issues related to auditing

5. Data Protection

- Introduction to Transparent Data Encryption (TDE)
- Implementing database encryption with TDE
- Introduction to Always Encrypted
- Implementing column encryption with Always Encrypted
- Introduction to Dynamic Data Masking
- Applying Dynamic Data Masking



 Download [PDF](#)