MICROSOFT SQL SERVER SECURITY MANAGEMENT

Course ID : SQL-ADM-Secure

เข้าสู่เว็บไซต์

ระยะเวลา : 2 วัน
(12 ชั่วโมง) 09.00 - 16.00 น.

ราคา : Call
*ใช้เป็นค่าใช้จ่ายทางภาษีได้ 200%
*รับเฉพาะ Inhouse Training เท่านั้น

ดูตารางฝึกอบรม
www.9experttraining.com

หมวดหมู่ : Data

เรื่องของการจัดการด้านความปลอดภัยบน Microsoft SQL Server ควรครอบคลุมตั้งแต่การติดตั้ง การกำหนดสิทธิ์การเข้าถึง ไปจนถึงการควบคุมความปลอดภัยในระดับ Objects ให้สอดคล้องกับสภาพแวดล้อมการใช้งานจริง อาทิ Domain Environment อีกทั้งภายใน Microsoft SQL Server เอง ยังมีระดับชั้นที่สามารถจัดการได้ตั้งแต่ระดับ Instance ไล่ลงไป ระดับฐานข้อมูล จนถึงระดับ Schema ที่เป็นขอบเขตด้านความปลอดภัยให้แก่บรรดา Objects ในฐานข้อมูล โดยการจัดการด้านความปลอดภัยประกอบด้วยการตั้งค่าเพื่อพิสูจน์ตัวตน การกำหนดสิทธิ์การเข้าถึง การติดตามด้านความปลอดภัย ยังรวมไปถึงการใช้เทคโนโลยีการเข้ารหัสเพื่อปกป้องข้อมูลที่จำเป็น

วัตถุประสงค์

1. ผู้อบรมสามารถเลือกใช้ Service Account ที่เหมาะสมกับสภาพแวดล้อม
2. ผู้อบรมสามารถสร้างและใช้ตัวตนในแต่ละระดับชั้นได้
3. ผู้อบรมสามารถเลือกใช้เทคโนโลยีในการปกป้องข้อมูลได้อย่างเหมาะสม

หลักสูตรนี้เหมาะสำหรับ

1. ผู้ดูแล Microsoft SQL Server
2. Consultant
3. Director / Management
4. ผู้สนใจงานด้าน SQL Server Security

พื้นฐานของผู้เข้าอบรม

1. มีประสบการณ์ในการดูแล Microsoft SQL Server มาบ้าง

ความต้องการของระบบ

1. ระบบปฏิบัติการ Windows 11 / 10
2. Remote Desktop Connection (RDP)
3. Internet

หัวข้อฝึกอบรม

วันที่ 1 - ช่วงเช้า 09:00 น. – 12:00 น.

1. ความปลอดภัยของ SQL Server

- การพิสูจน์ตัวตนเพื่อเข้าใช้ MS SQL Server
  - เข้าใจทรัพยากรที่กำหนดสิทธิ์ได้ (Securable)
  - เข้าใจตัวตน (Security Principal)
  - การกำหนดสิทธิ์ (Permission)
  - ภาพรวมการรักษาความปลอดภัยของ MS SQL Server
  - การพิสูจน์ตัวตนของ MS SQL Server
- การสร้างและการจัดการ Login
  - Password Policy ผ่าน Local Security Policy หรือผ่าน Group Policy Object
- เข้าใจ Logins เชิงลึก
- การแมป Login ไปเป็น User ในฐานข้อมูล
  - การอนุญาตให้เข้าถึงฐานข้อมูล
  - จัดการกับ Database Users ชื่อ dbo และ guest
  - เบื้องลึกเกี่ยวกับ Users
  - สืบค้นสิทธิ์ของ Logins ด้วย User Tokens
  - สิทธิ์ข้ามเครื่องด้วย Linked Servers
  - ปัญหา “Double-Hop“
  - Impersonation เทียบกับ Delegation
- การจัดการกรณี SID ไม่ตรงกัน และ Orphaned Users
- รู้จักกับ Partially Contained Databases
- ข้อควรคำนึง Partially Contained Databases

วันที่ 1 - ช่วงบ่าย 13:00 น. – 16:00 น.

2. จัดการกับ Server Role และ Database Role

- การใช้งาน Server Roles
  - สิทธิ์ในระดับเซิร์ฟเวอร์
  - สิทธิ์ในระดับเซิร์ฟเวอร์โดยทั่วไป
  - รู้จักกับ Fixed Server Roles
- รู้จัก User-defined Server Roles
  - รู้จักกับ public Server Role
  - การสร้าง User-defined Server Roles

- การใช้งาน Database Roles
  - สิทธิ์ในระดับฐานข้อมูล
  - รู้จักกับ Fixed Database Roles
  - การกำหนด Database Principals ให้กับ Database Roles
  - เจ้าของฐานข้อมูล
- รู้จัก User-defined Database Roles
  - จัดการกับ User-Defined Database Roles
  - การใช้ Roles ในสถานการณ์ทั่วไป
- รู้จักกับ Application Roles
  - จัดการกับ Application Roles

วันที่ 2 - ช่วงเช้า 09:00 น. – 12:00 น.

3. การกำหนดสิทธิ์การเข้าถึง

- อนุญาตให้ผู้ใช้เข้าถึง Objects
  - ตัวตน (Security Principal)
  - ทรัพยากรที่กำหนดสิทธิ์ได้ (Securable)
  - GRANT, REVOKE, DENY
- ความปลอดภัยบน Table และ View
  - ความปลอดภัยระดับ Column
  - ความปลอดภัยระดับแถวข้อมูล
  - การได้รับสิทธิ์และมอบสิทธิ์ต่อด้วย WITH GRANT OPTION
- อนุญาตผู้ใช้เข้าถึง Execute Code
  - ความปลอดภัยของ Stored Procedures
  - ความปลอดภัยของ User-defined Functions
  - ความปลอดภัยของ User-defined TVFs
  - ความปลอดภัยของ Managed Code
- การตั้งค่าสิทธิ์ในระดับ Schema
  - ภาพรวมของ User-schema
  - วิธีการอ้างชื่อ Object
  - การให้สิทธิ์ที่ระดับ Schema

วันที่ 2 - ช่วงบ่าย 13:00 น. – 16:00 น.

4. การ Audit

- ทางเลือกในการ Audit การเข้าถึงข้อมูล
- รู้จักกับ Common Criteria Compliance
  - ตั้งค่าให้ SQL Server สนับสนุน CC Compliance
- การ Audit โดยใช้ Trigger
- การ Audit โดยใช้ Temporal Tables
- การ Audit โดยใช้ SQL Trace
- สร้าง SQL Server Audit
  - รู้จักกับ Extended Event
  - การกำหนด Server Audit
  - Audit Actions และ Action Groups
  - การสร้าง Server Audit Specifications
  - การสร้าง Database Audit Specifications
- จัดการกับ SQL Server Audit
  - การสืบค้นข้อมูลการ Audit Data
  - โครงสร้างการเก็บบันทึก Audit
  - ปัญหาที่พบได้บ่อยเกี่ยวกับการ Audit

5. การปกป้องข้อมูล

- รู้จักกับ Transparent Data Encryption (TDE)
  - การเข้ารหัสฐานข้อมูลด้วย TDE
- รู้จักกับ Always Encrypted
  - การเข้ารหัสคอลัมน์ด้วย Always Encrypted
- รู้จักกับ Dynamic Data Masking
  - การใช้งาน Dynamic Data Masking

ดาวน์โหลด PDF