SQL 2012 Admin, Part 3 of 5: Security and Resource Mgmt

Meet the expert: Chris Bell, MCITP, is an 18-year SQL Server veteran for both business intelligence and application development providing solutions for businesses, organizations, and individuals. He is the founder and CEO of WaterOx Consulting, Inc., a provider of remote SQL Server consulting and services. Chris is also the founder and current President of the Washington DC chapter of PASS and a member of the Board of Directors for CPCUG. Chris also frequently attends and presents at PASS events around the country, sharing his passion for all things SQL Server. In 2012, Chris was one of 5 finalists in the world for Red Gate’s Exceptional DBA Award.

Prerequisites: This course assumes that students have working experience with SQL Server 2005 or 2008; basic relational database concepts (e.g., tables, queries, and indexing); general knowledge of XML, Transact-SQL, and a fundamental understanding of networking and security concepts.

Runtime: 01:51:13

Course description: Security is becoming a concern of everyone. In this course we will dive into some of the features in SQL Server 2012 that relate to security. We will take a look at the encryption keys that SQL Server creates and uses, along with certificates, to protect everything from cell level data to entire databases. Then we will see how Transparent Data Encryption can help to quickly bring a database into compliance with most regulations and requirements. We will also see what exactly is required to move an encrypted database to a new server without losing any data. User defined server roles is a new SQL 2012 feature that makes administration easier when it comes to security. We will go over this and even create our own Server Role for members of the data team. Next we will look at ways to protect individual objects in your databases using security permissions and show how, as the DBA, you can test your configuration using the Execute As capabilities of SQL Server. Next we are going to look into the Resource Governor and Policy Based management. We will go through the Components of the Resource Governor and show how you can use this great feature of Enterprise edition to classify incoming connections and identify specific users or groups that are using excessive resources on the server. We will then look at the Policy Group Management feature of SQL Server. We will create policies that check and enforce naming conventions and ensure proper backups are being configured on your servers.

Course outline:

Encryption Keys
- Introduction
- Database Encryption Keys
- Managing Encryption
- Service Master Key
- Backup the SMK
- Restore the SMK
- Alter the SMK
- Create a Database Master Key
- Backup the DMK
- Restore a DMK
- Alter a DMK
- Demo: Backup Master Keys
- Demo: Alter Master Key
- Demo: Create Master Key
- Summary

Transparent Data Encryption
- Introduction
- Certificates and Database Keys
- Transparent Data Encryption
- TDE - Pros & Cons
- TDE - Restoring the Backup
- Demo: Enable TDE
- Demo: Disable Encryption
- Demo: Moving TDE
- Demo: Backup TDE
- Summary

Server Roles
- Introduction
- User Defined Server Roles
- Demo: Creating Roles
- Protecting Objects
- Grant Permissions
- Deny Permissions
- Revoke Permissions
- Execute As
- Demo: Built-In Permissions
- Demo: Testing Permissions
- Summary

Resource Governor
- Introduction
- Resource Governor
- Demo: Resource Governor
- Demo: Assigning Functions
- Demo: Performance Monitor
- Summary

Policy-Based Management
- Introduction
- Policy-Based Management
- Central Management Server
- Demo: Policy Management
- Demo: Create Policy
- Demo: Enforcing Policy
- Demo: Recovery Model
- Demo: Evaluating Policies
- Demo: Importing Policies
- Demo: Policy Violations
- Summary