Protecting Data and Privacy

- SQL Server 2005
  - Built-in encryption functions
  - Key management in SQL Server
  - Encrypted File System (EFS)
  - Bit-Locker
  - Windows integrated authentication
- SQL Server 2008
  - Extensible Key Management (EKM)
  - Transparent Data Encryption (TDE)
  - Integrated Authentication Enhancements

4

Tracking Database Activity

- SQL Server 2005
  - SQL Trace
    - Profiler Column: SESSIONLOGINNAME
  - DDL/DML Triggers
    - Function: ORIGINAL_LOGIN()
  - Third-party tools to read transaction logs
  - No management tools support
- SQL Server 2008
  - All Actions Audited

5

Agenda

- Extensible Key Management (Enterprise Edition)
- Transparent Data Encryption (Enterprise Edition)
- Integrated Authentication Enhancements
- All Actions Audited (Enterprise Edition)

6

Extensible Key Management

8

Extensible Key Management Benefits

- Physical separation of data and keys
- Additional authorization check (separation of duties)
- Higher performance for hardware based encryption/decryption
- Store keys from across the enterprise together - easy management
- Enterprise Key Managers enable and enhance functionality not available in the SQL Server Engine:
  - Key Generation and Disposal
  - Key Storage – Keeping data separate from protection keys is best practice
  - Key Retention – Rotating keys is important to reduce the risk of one key getting compromised
  - Key Recovery
  - Key Retrieval
  - Key Distribution

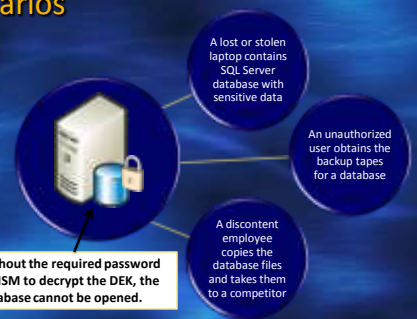
9

Module Overview

- Extensible Key Management (Enterprise Edition)
- Transparent Data Encryption (Enterprise Edition)
- Integrated Authentication Enhancements
- All Actions Audited (Enterprise Edition)

10

Transparent Data Encryption: Scenarios



11

Transparent Data Encryption

DEMO

12

Transparent Database Encryption: Benefits

- Entire database is protected
- NO application changes
- Applications do not need to explicitly encrypt/decrypt data!
- No restrictions with indexes or data types (except FILESTREAM cannot be encrypted)
- Performance cost is small
- Backups are unusable without key
- Can be used with Extensible Key Management

13

Transparent Data Encryption: Mechanism

- Very simple:
  - Database pages are encrypted before being written to disk
  - Page protection (e.g. checksums) applied *after* encryption
  - Page protection (e.g. checksums) checked *before* decryption
  - Database pages are decrypted when read into memory
- When TDE is enabled, initial encryption of existing pages happens as a background process
  - Similar mechanism for disabling TDE
  - The process can be monitored using the encryption_state column of sys.dm_database_encryption_keys
    - Encryption state 2 means the background process has not completed
    - Encryption state 3 means the database is fully encrypted

14

Transparent Data Encryption: Enabling

- Create a master key
  - CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPwdHere>';
- Create or obtain a certificate protected by the master key
  - CREATE CERTIFICATE MyDEKCert WITH SUBJECT = 'My DEK Certificate';
- Create a database encryption key and protect it by the certificate
  - CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_128 ENCRYPTION BY SERVER CERTIFICATE MyDEKCert;
- Set the database to use encryption
  - ALTER DATABASE MyDatabase SET ENCRYPTION ON;

15

Transparent Data Encryption: Backups

- A backup of a TDE encrypted database is also encrypted using the database encryption key
- To restore the backup OR attach the database, the DEK must be available!
  - There is no way around this – if you lose the DEK, you lose the ability to restore the backup (that's the point!)
  - Maintain backups of server certificates too

16

Transparent Data Encryption: Limitations

- If TDE is enabled, a database will not use instant file initialization
  - Can cause significant performance drop
  - Especially important for database restore operations during disaster recovery
- FILESTREAM data is not encrypted

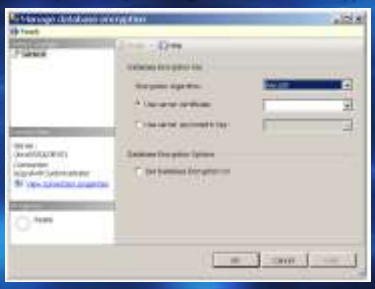
17

Transparent Data Encryption: Tools Support

18

Transparent Data Encryption: Tools Support

- Database | Tasks | Manage Database Encryption



19

Module Overview

- Extensible Key Management (Enterprise Edition)
- Transparent Data Encryption (Enterprise Edition)
- Integrated Authentication Enhancements
- All Actions Audited (Enterprise Edition)

20

Integrated Authentication Enhancements

- SQL Server 2005
  - Kerberos possible with TCP/IP connections only
  - Service Principal Name (SPN) must be registered with AD
    - An SPN is a unique identifier for a service on a network that uses Kerberos authentication.
- SQL Server 2008
  - Kerberos available with ALL protocols (TCP/IP, named pipes, shared memory)
  - SPN may be specified in connection string (OLEDB/ODBC)
  - Kerberos possible without SPN registered in AD

21

IA Enhancements: Supported SPN Formats

- Named instance
  - MSSQLSvc/FQDN:[port | instancename]
    - MSSQLSvc is the service that is being registered
    - FQDN is the fully qualified domain name of the server
    - port is the TCP port number
    - instancename is the name of the SQL Server instance
- Default instance
  - MSSQLSvc/FQDN[:port]
    - MSSQLSvc is the service that is being registered
    - FQDN is the fully qualified domain name of the server
    - port is the TCP port number
- The new format does NOT require a port number

22

Module Overview

- Extensible Key Management (Enterprise Edition)
- Transparent Data Encryption (Enterprise Edition)
- Integrated Authentication Enhancements
- All Actions Audited (Enterprise Edition)

23

All Actions Audited

- SQL Server Audit now a 1st-class server object
  - Native DDL for Audit configuration and management
  - Security support
- Create an Audit object to automatically log actions to:
  - File
  - Windows Application or Security Log
- Create an Audit Specification to include server and database actions in an audit
  - Pre-defined action groups
  - Individual action filters

24

SQL Server Audit

DEMO

25

SQL Server Audit: Audit Action Groups and Actions

- Groups of actions (*Audit Action Groups*) can be audited at various levels
  - Server level events can only be audited at the server level
    - E.g. logon, logoff, Service Broker, DBCC
  - Database level events can be audited at the per-database level or across the whole server
    - E.g. DDL, object permissions changes
- Individual actions can be audited only at the database level
  - SELECT UPDATE INSERT
  - DELETE EXECUTE RECEIVE (Service Broker)
  - When a REFERENCES permission is checked

26

SQL Server Audit: Audit Specifications

- Defined at the server and database level
  - One Server Audit Specification per instance
  - One Database Audit Specification per database per instance
- Defines what is audited at that level
- Contains audit action groups and audit actions (at the database level)
- No auditing available at the per-*column* level

27

SQL Server Audit: Targets and Audit Records

- Events are converted to *audit records*
  - Fixed schema, although not all events populate all columns
  - Schema described in BOL (search for *SQL Server Audit Records*)
- Audit records are written to the specified *target file*
  - Any binary file, Windows Application Log, Windows Security Log
  - Oversize records are chained with a sequence number
- Note: using the Security Log requires extra setup
  - Description in BOL (search for *Understanding SQL Server Audit*)
- For fine-grained permission setting on the target, use a binary file with custom permissions

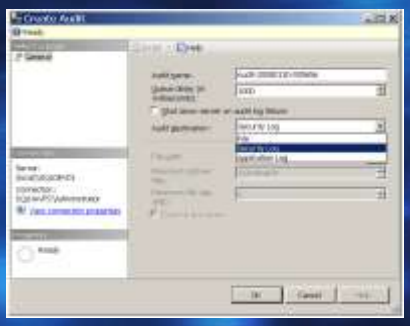
28

SQL Server Audit: Performance

- Leverages high performance Extended Events infrastructure to generate audits
- Runs within Database Engine rather than as a side/separate app
- Targeted to be faster than SQL Trace

32

SQL Server Audit: Tools Support



33

Review

- Extensible Key Management
- Transparent Data Encryption
- Integrated Authentication Enhancements
- All Actions Audited

34

Resources

- Overview Technical Webcast
  - http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventId=1032364702
- SQL Server Security Website
  - http://www.microsoft.com/sql/technologies/security/default.mspx
- SQL Server 2005 – Security and Protection
  - http://www.microsoft.com/technet/prodtechnol/sql/2005/library/security.mspx

35

Microsoft | developer & platform evangelism

36