

Auditing Solution

SQL Server 2005 and .NET CLR Triggers

John Cashwell

Battelle Centers for Public Health Research and Evaluation

What is an audit log?

- Computer files containing details of amendments to records, which may be used for system recovery or intrusion investigation.

Source: <http://www.itd.uts.edu.au/itsecurity/glossary.html>

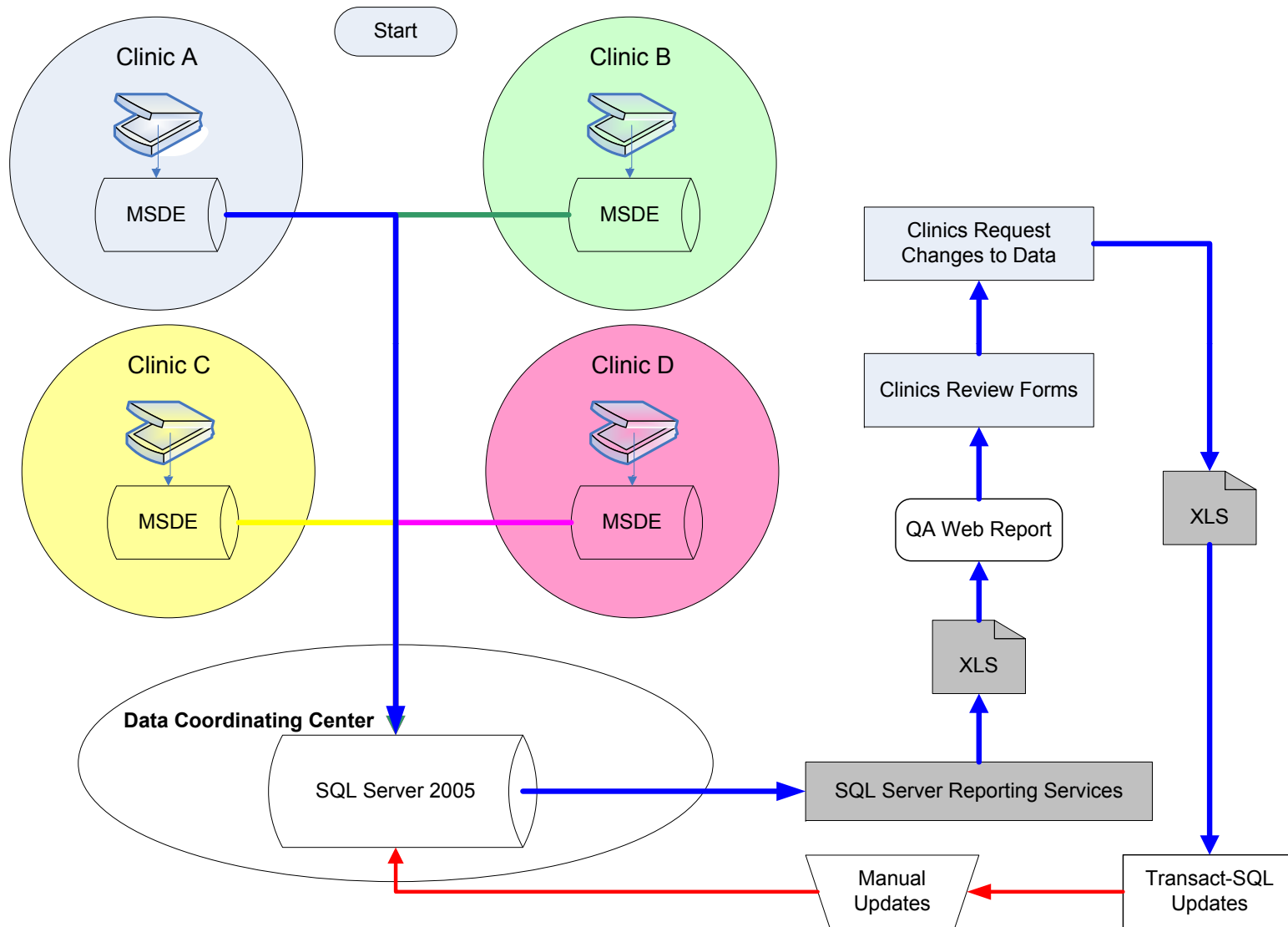
Why have an audit log?

- Accountability
- Data Reconstruction
- Intrusion Detection

Audit Log Elements

- Who
- When
- Operation
- Database Name
- Table Name
- Field Name
- Record ID
- Old Value
- New Value

Scenario



Specifications

- Audit Log
 - Updates (per variable)
 - Deleted Records
- 4 Dedicated Clinic Databases
- 28 Tables per Database

Options

- 3rd Party Tools
 - Lumigent: Log Explorer, and Audit DB
 - ApexSQL Audit
- Transact-SQL Triggers
- **.NET CLR Triggers**

What is a SQL Server Trigger?

- Procedure that runs when DML or DDL events occur
- Data Manipulation Language (DML)
 - INSERT, UPDATE, DELETE
- Data Definition Language (DDL)
 - CREATE, ALTER, DROP

.NET CLR vs T-SQL

- T-SQL
 - Best when query-based (*Select, Insert, Update, Delete*)
 - Internal SQL Server efficiencies
 - Use as much as possible
- .NET CLR
 - More extensive library of functions (VB, C#, C++, etc)
 - Complex mathematical computations
 - Intensive logic or procedural tasks

Why Selected .NET CLR

- Easier to conceptualize than Transact-SQL
- One reusable assembly for all databases
 - *Limited customization required*
 - *Transact-SQL would need customization per table*
- Future changes to table structure not a problem

.NET CLR in SQL Server 2005

- Visual Studio C# or VB.NET
- SQL Server Project Type
- Stored Procedures, Triggers, Functions, etc.
- [demo Visual Studio]

Deployment Steps

- Compile and copy assembly to server
- Copy table structures for “DeletedRows” table
- Setup assembly in SQL Server
 - Enable CLR
 - CREATE ASSEMBLY (Transact-SQL)
- Create trigger per table
 - CREATE TRIGGER (Transact-SQL)
 - AS EXTERNAL NAME

Demo

Challenges Ahead

- Cannot have BLOB fields (CLR limitation)
 - text, ntext, image, binary, varbinary
 - syscolumns table TYPE
 - Auto build field list excluding BLOB fields
- Wrapper functions required per table
 - Cannot access metadata of affected table
 - Cannot pass parameters to a Trigger

Resources

<http://sqljunkies.com/Article/4CD01686-5178-490C-A90A-5AEEF5E35915.scuk>

By David Ziffer

Published: 10/6/2005

<http://msdn.microsoft.com/en-us/library/ms131093.aspx>