Auditing in SQL Server 2008

Il-Sung Lee
Senior Program Manager
Microsoft Corporation
ilsung@microsoft.com
Agenda

• What’s changed since Microsoft® SQL Server® 2005?
• Why should I use SQL Server Audit?
• What is the performance impact?
• Can I protect the audit log from the database administrator (DBA)?
• What happens if audit fails to write?
• What do I do if the server fails to start because of SQL Server Audit?
• Anything else I should know?
What’s changed since SQL Server 2005?
We now have a dedicated security auditing feature
Auditing Database Activity

- **SQL Server 2005**
  - SQL Trace
  - Data definition language (DDL)/Data modification language (DML) triggers
  - Third-party tools to read transaction logs
  - No management tools support

- **Microsoft® SQL Server® 2008**
  - SQL Server Audit
SQL Server Audit

- Audit now a first-class object
  - Native DDL for configuration and management
  - Security support
- Create an Audit object to automatically log actions to:
  - File
  - Windows® Application Log
  - Windows® Security Log
- Ability to define granular Audit actions of Users or Roles on database (DB) objects
- Multiple, independent audits may run concurrently
Audit Specifications

0..1 Server audit specification per Audit object

0..1 DB audit specification per database per Audit object

CREATE SERVER AUDIT
SPECIFICATION SvrAC
TO SERVER AUDIT PCI_Audit
ADD (FAILED_LOGIN_GROUP);

CREATE DATABASE AUDIT
SPECIFICATION AuditAC
TO SERVER AUDIT PCI_Audit
ADD (SELECT ON Customers BY public)
Why should I use SQL Server Audit?
For performance, security, flexibility, and other good reasons!
Reasons to Use SQL Server Audit

- Faster than SQL Trace
  - Leverages high performance eventing infrastructure
  - Granular auditing
  - Runs within engine
- More secure
  - More choices for audit target
  - Automatically records changes to Audit state
  - Persists state between restarts
- Parity with SQL Server 2005 Audit Generation
- Configuration and management in Microsoft® SQL Server® Management Studio (SSMS)
- Integration with Policy-Based Management
demonstration

Enabling SQL Server Audit
What is the performance impact?
Depends...
Audit Performance

• Depends upon:
  – The workload
  – What’s being audited

• Comparison of SQL Server Audit against SQL Trace for 5 different typical customer workloads…
SQL Server Audit vs. SQL Trace

Customer Workload Performance

- Base Time (min)
- SQL Trace (min)
- SQL Server Audit (min)

<table>
<thead>
<tr>
<th>Workload</th>
<th>Base Time</th>
<th>SQL Trace</th>
<th>SQL Server Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workload 1</td>
<td>13.3</td>
<td>15.9</td>
<td>14.1</td>
</tr>
<tr>
<td>Workload 2</td>
<td>5.1</td>
<td>6.3</td>
<td>5.6</td>
</tr>
<tr>
<td>Workload 3</td>
<td>3.6</td>
<td>4.78</td>
<td>4</td>
</tr>
<tr>
<td>Workload 4</td>
<td>76.6</td>
<td></td>
<td>68.13</td>
</tr>
<tr>
<td>Workload 5</td>
<td>41.3</td>
<td></td>
<td>55.9</td>
</tr>
</tbody>
</table>
Can I protect the Audit log from the DBA?
Yes.
Protecting Audit Data

Windows Security Log
- “Tamper-proof” log
- DBA cannot clear log (assuming not an Administrator)
- Microsoft® System Center Operations Manager Audit Collection Service

Copy Audit logs to secure location
- Directory or share inaccessible by service account or DBA
- Audit logs files are shared-read and cannot be tampered with while active
- Possible momentary exposure if using multiple logs

Combination of the two
- Audit “tamper” activity to Security Log, e.g., DBA modifying Audit
- All other Audit events are sent to file
What happens if Audit fails to write?
Depends again...
Audit Write Failure (shutdown)

- Shut down server on audit log failure
Audit Write Failure (non-shutdown)

Audit Events Buffered
- Audit buffer size varies but is around 4MB (equivalent to at least 170 events, depending upon statement text)

Server Blocks Activity Generating Audit Event
- Does not effect other Audits
- Blocks until buffer space freed or audit disabled

Audit Session Turned Off
- Buffered data is discarded and error written to error log
- Continue trying to write future events to Audit log
- If failure during creation of handle to file/Window log session, manual restart of Audit session required
What do I do if the server fails to start because of SQL Server Audit?
Start the server in single-user mode
Starting the Server

Option 1
- Correct source of error
- E.g., file system full

Option 2
- Single-user mode, “-m”
- Audit is active but shutdown-on-failure behavior deactivated
- Audit Admin can fix Audit configuration

Option 3
- Minimal configuration mode, “-f”
- Audit disabled but Audit DDL can still be issued
demonstration

Using SQL Server Audit with Policy-Based Management
Anything else I should know?
Just a few things
Other Things You Should Know

- Enterprise only
- Parameterized queries
- Audit Xevent Sessions may not be manipulated by Xevent DDL
- Audit logs are not encrypted
- Audit events are fired with permission checks
- Writing to files is much faster than writing to event log
Other Things You Should Know

• Both Audit and Audit Specifications have STATE parameters
  – Can only change state outside user transaction
  – All other audit changes can be done in a transaction, but with Audit or Audit Specification OFF
demonstration

Using SQL Server Audit with Policy-Based Management
Securely and Easily Track DB Activity

• Consider SQL Server Audit for all security auditing requirements
• Carefully devise a strategy for what needs to be audited and where to send the audit information based on security and performance needs
• Monitor administrator activity and prevent tampering of the logs
For More Information…

- Visit TechNet at [www.microsoft.com/technet](http://www.microsoft.com/technet)
- For additional information on books, courses, and other community resources that support this session visit
  - Understanding SQL Server Audit
  - Auditing in SQL Server 2008 white paper
  - SQL Server Security home page
Questions and Answers

• Submit text questions using the “Ask” button
• Don’t forget to fill out the survey
• For upcoming and previously live webcasts: www.microsoft.com/webcast
• Got webcast content ideas? Contact us at: http://go.microsoft.com/fwlink/?LinkId=41781
Your potential. Our passion.