http://www.sqlservercentral.com/articles/Security/65170/
Printed 2008/12/18 04:11PM

Using the Service Audit Object in SQL Server 2008

By Brian Kelley, 2008/12/05

In today's age of compliance with various government regulations and laws, monitoring who is doing what with the data is extremely important. Versions of SQL Server prior to SQL Server 2008 give some great monitoring features such as DML and DDL triggers as well as server-side tracing. C2 compliance, which was introduced in SQL Server 2000, actually is a very detailed server-side trace. However, the problem with many of these solutions is that we usually end up with a lot of noise in what gets recorded. For instance, to monitor people who are viewing (not changing) data we have to monitor just about every query that goes across the server. On a busy or multi-purpose server, the effort to extract the auditing results we want may take a great effort.

Enter in the SQL Server Audit object in SQL Server 2008. This new security feature is specifically designed to track and log just about any kind of event that occurs on a SQL Server instance at a very specific level, even SELECT queries against a particular table in a database. As a result, it permits the granularity a SQL Server DBA is being asked for without the overhead, both on the server and after the fact, in the processing of the results.

One Significant Drawback - Enterprise Edition Required

Before we get too far into a discussion about the Audit object, I would be remiss in neglecting to point out what edition of SQL Server is required to use the Audit object. The SQL Server Audit object is a nice new feature that just about any organization who uses anything other than SQL Server Express can take advantage of. However, Audit is only available with SQL Server 2008 Enterprise Edition. While SQL Server clustering is now permitted with the Standard Edition of SQL Server (as of SQL Server 2005), if you want this and some of the other security related features (Transparent Data Encryption) you will have to purchase Enterprise Edition.

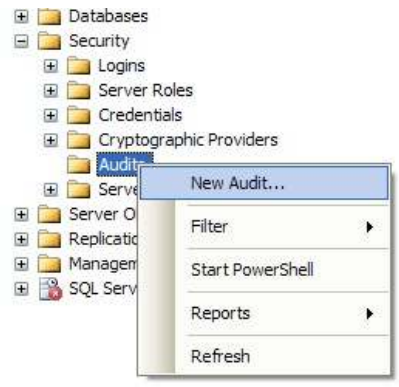
Two Levels of Audit Object Specifications

In SQL Server 2008 Enterprise Edition, while there is only one type of Audit object (called a Server Audit), there are two types of audit object specifications: server and database. These specifications correspond to the level of the events which we want to monitor. If we're looking to monitor login failures and SQL Server configuration changes, we'll use a server audit object specification. If, however, we're looking to monitor activity against a table or any events which occur within a database, we'll want to create a database audit object specification. In order to try and reduce some of the confusion, since there is a server audit specification, when I refer to the Audit object and not a specification, I'll simply use Audit or Audit object.

Creating the Initial Audit object

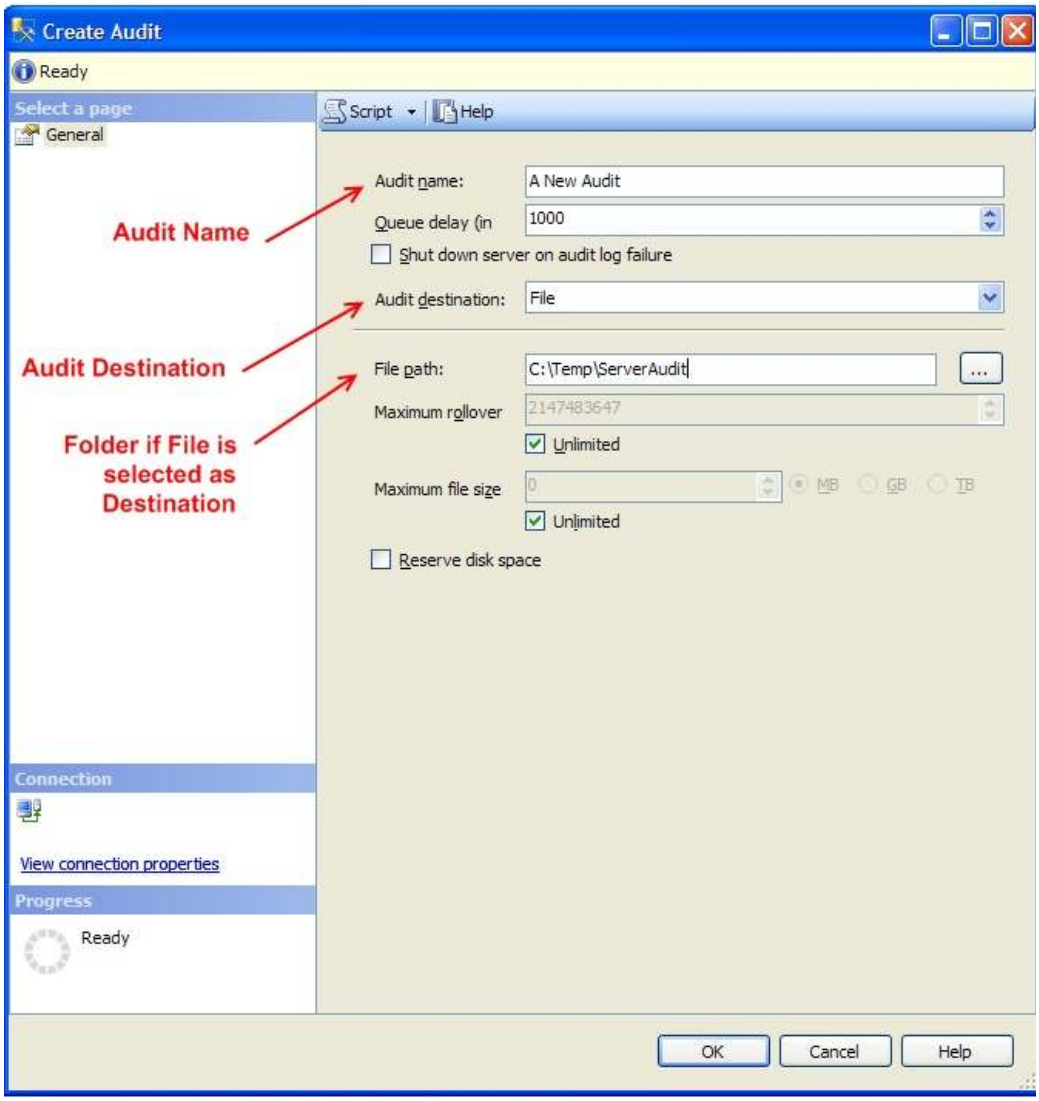
The easiest way to create an initial Audit is to use SQL Server Management Studio (SSMS). If we expand the server in Object Explorer, then expand the **Security** folder, we'll see a sub-folder called **Audits**. If we right-click on this folder, we can choose to create a **New Audit** from the pop-up menu, as shown in figure 1.

Figure 1:



A new dialog window will appear where we can specify the details of our Audit, as shown in figure 2.

Figure 2:



We'll have to give it a name and then we'll need to select a few particular settings, the most important of which is the **Audit destination** for the details on any events which are recorded. We have three choices for our destination:

- The operating system Application event log
- The operating system Security event log
- A location on the file system.

If we specify the Audit destination to be File, we'll also have to give it a folder to write to. While the dialog window uses the phrase **File path**, what is really meant is a folder. The SQL Server service will need **Modify** rights at the file system level on this folder. One catch is that you'll need to have created the folder ahead of time. While the ellipsis (…) button will allow you to select the folder location through a graphical interface, it does not give you the ability to create a new folder.

You can also configure the maximum number of rollovers for your Audit as well as how large to allow each file to grow to before performing the rollover. By default, SQL Server will configure these as unlimited unless you specify differently. It is recommended you put a maximum file size to allow the write time to be reasonable and also to ensure your audit does not run the drive out of space.

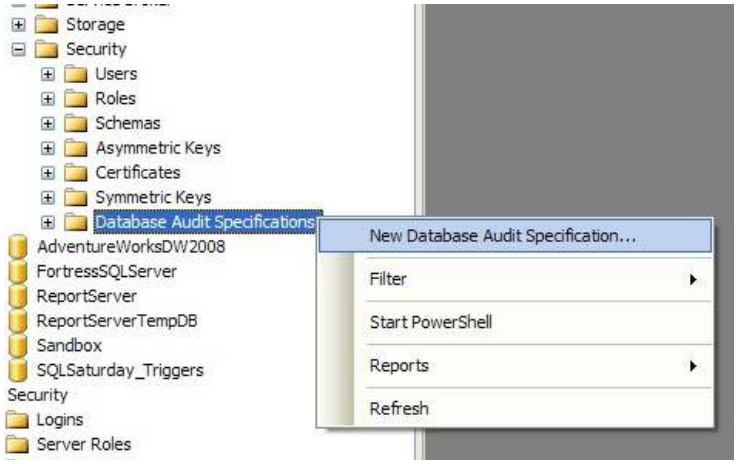
If you decide to use the Security event log, there are likely some steps you'll need to perform to enable the SQL Server service account the ability to write to the Security event log. The Books Online topic **How to: Write Server Audit Events to the Security Log** for both pre-Windows 2008/Vista systems and Windows 2008/Vista configuration as the method for doing so differs between the two classes of operating systems.

Creating an Audit Specification

If we're using SSMS, how we create the audit specification depends on the level we are looking to monitor. If we are creating a server audit specification, one which will monitor server-level events, we can right-click on the **Server Audit Specifications** folder just underneath the **Audits** folder, as shown in figure 3. If we're looking to create a database audit specification, we'll need to expand the **Security** folder in the database we're looking to monitor and right-click on the **Database Audit Specifications** folder (figure 4). From the pop-up menu we can then select the option to create a new audit specification at the appropriate level.

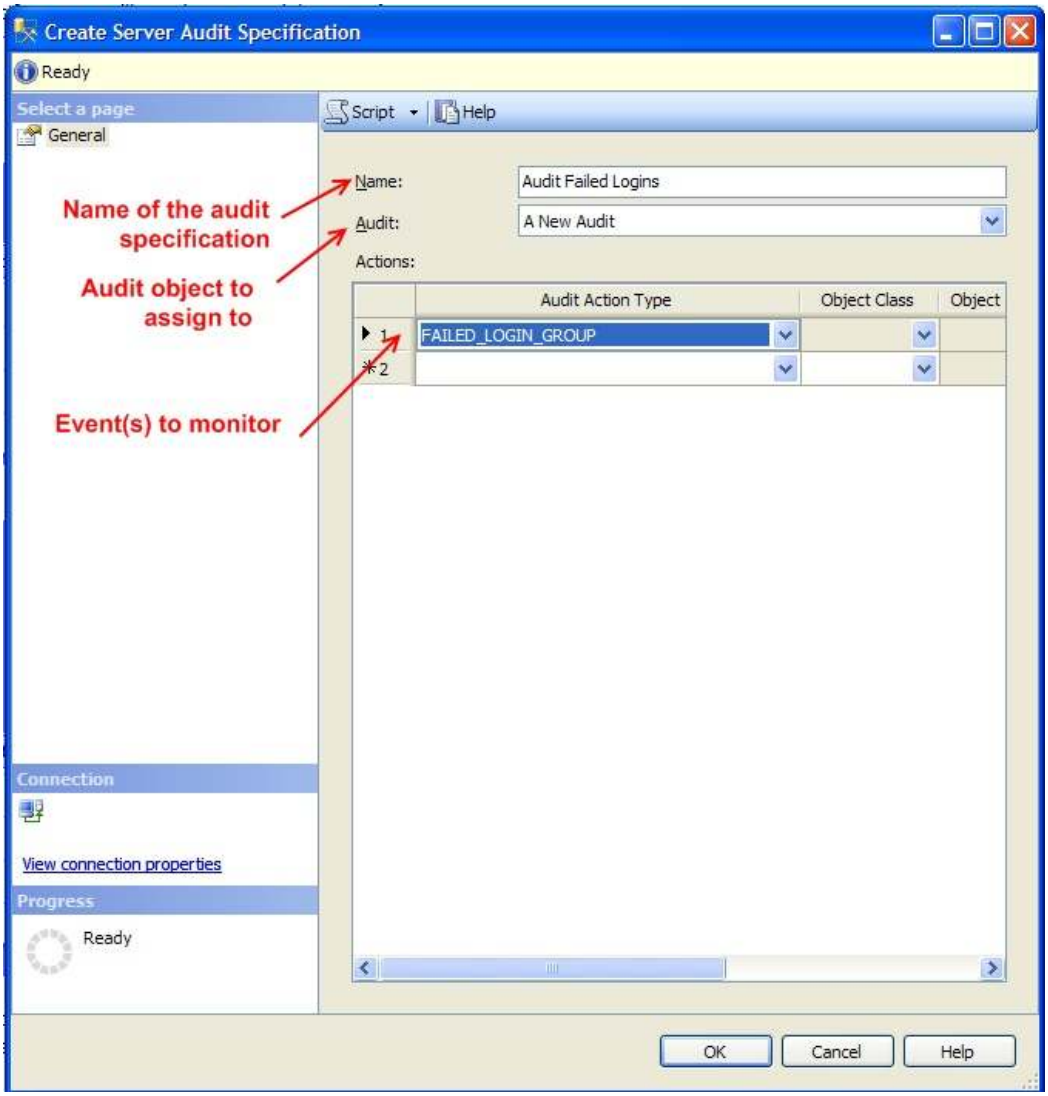
Figure 3:

Figure 4:



Once we have selected to create a new audit specification, a dialog window will appear which will give us the option to name the specification, what Audit object to assign it too, and then select what events it will monitor. In figure 5 I have specified a server audit specification, attached to an Audit object called **A New Audit**, and set it to monitor for failed login events.

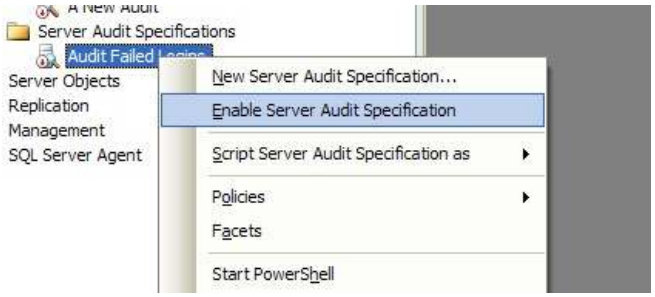
Figure 5:



Enabling the Audit Specification and Audit Object

If the Audit object or Audit specification shows a magnifying glass with a small red circle containing a red arrow pointing down, the object or specification is disabled. When a new Audit object or audit specification is created, SQL Server will create it in an initially disabled state. To enable an Audit object specification, simply right-click on the correct object and select the Enable option as appropriate. Figure 6 shows the pop-up menu for a server audit specification.

Figure 6:



Once SQL Server enables the Audit object or audit specification, a dialog window appear (similar to the one for executing a SQL Agent job) indicating that the object has been enabled (figure 7). In addition, the icon should change so that there is no longer a red circle with an arrow pointing downward.

Figure 7:

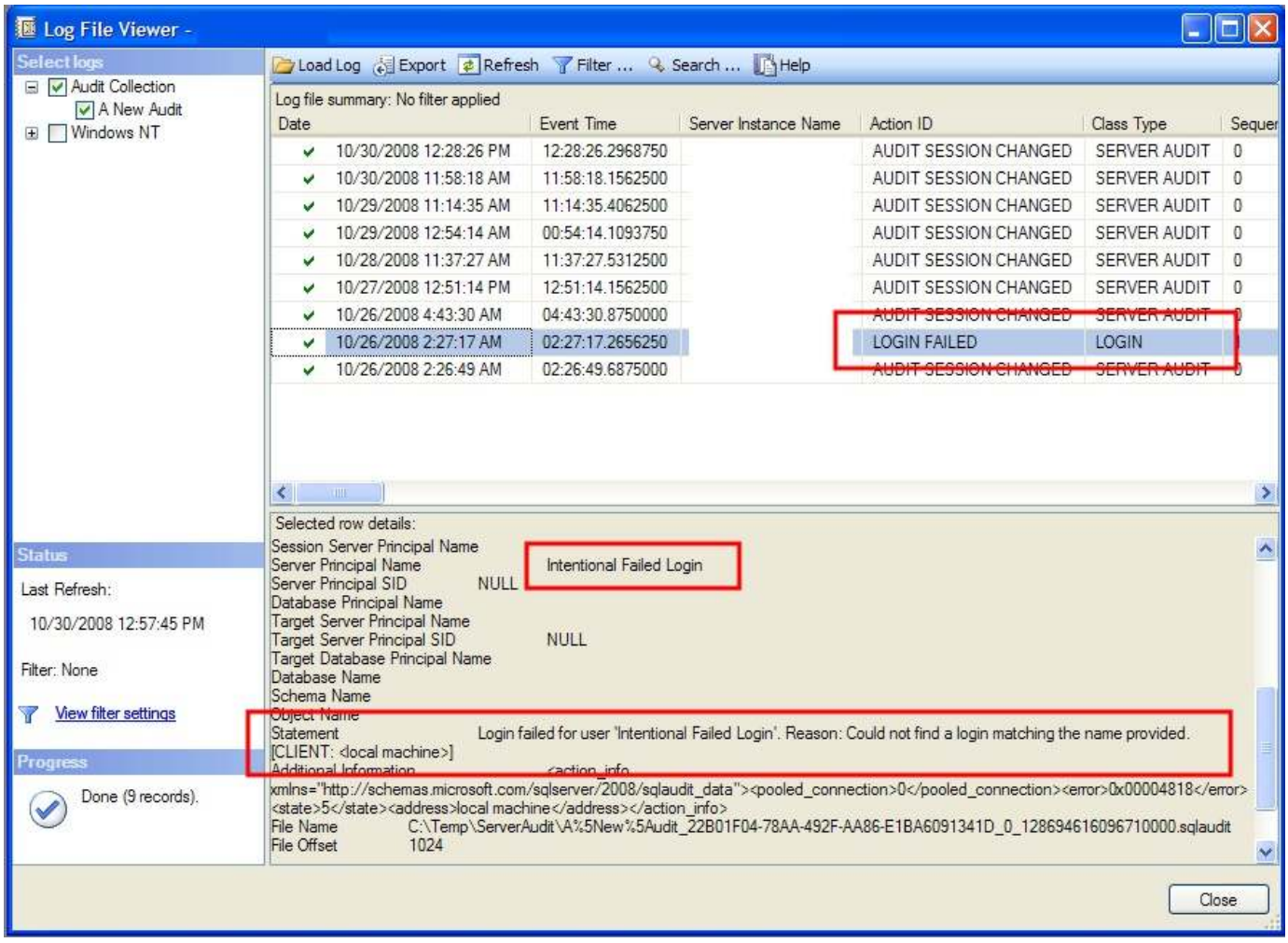
Viewing the Audit Log

We can view the log for a particular Audit object by right-clicking on the Audit object and selecting **View Audit Logs** from the pop-up menu (figure 8).

Figure 8:

This brings up all the details on any events which have been captured. Figure 9 shows where a failed login has been highlighted.

Figure 9:



The audit log will also record changes to the Audit monitoring, such as when a SQL Server is stopped or restarted or when the Audit object is manually enabled or disabled. The Action ID of **AUDIT SESSION CHANGED** is how this information can be viewed. It's always

possible that someone with enough privileges will turn off the Audit object in order to carry out an action the Audit would track (such as an Audit with a database audit specification which records whenever someone issues a SELECT query against a particular table). By examining the contents of these events, we can determine if someone turned off an audit to attempt something malicious.

Concluding Thoughts:

The Audit object in SQL Server 2008 Enterprise Edition gives us additional visibility and auditing over events which are a great addition to our security toolset. Because of the nature of the Audit object, we can ensure we monitor only the events we're concerned about, unlike Profiler or a server-side trace, thereby reducing the amount of information we have to filter through. In addition, the Audit objects are self-auditing, which allows us to see when someone turns them off. Implemented properly, and they can fill a much needed gap in our SQL Server security architectures.
