

|  |
| --- |
| Microsoft SQL Server 2008 Audit Guide for Aviva Shared Service Implementation Guide |
| Version 0.1 – DRAFT |
| 16th June 2011 |

Change History

1. When using this document to create a project deliverable, it is recommended that the above statement and these instructions be deleted prior to delivering the document to the client.

The following Change History log contains a record of changes made to this document:

|  |  |  |  |
| --- | --- | --- | --- |
| Revised Date | Version # | Author (optional) | Section / Nature of Change |
| 16/06/2011 | 0.A | John Aigbokhaode |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Include links to peer review(s):

|  |  |
| --- | --- |
| Peer Review Link | Comments |
| <http://ustlsvugq001.amer.corp.eds.com/sites/Applications/PeerReview/default.aspx> |  |
|  |  |
|  |  |
|  |  |

Contents

[1 Reference documenation 1](#_Toc296330870)

[2 Introduction 1](#_Toc296330871)

[3 assumptions 2](#_Toc296330872)

[4 pre-implementation 3](#_Toc296330873)

[4.1 pre-requisites 3](#_Toc296330874)

[5 Implementation of sql audit 3](#_Toc296330875)

[5.1 Advantages of SQL Server Audit 4](#_Toc296330876)

[5.2 Limitations of SQL Server Audit 4](#_Toc296330877)

[5.3 How SQL Server Audit Works 4](#_Toc296330878)

[5.4 implementation 5](#_Toc296330879)

[5.4.1 Step by step walk through 6](#_Toc296330880)

[5.5 Deploy sql audit using tsql script to any sql server instance 24](#_Toc296330881)

[5.5.1 Script Considerations 24](#_Toc296330882)

[5.5.2 Implementing SQL Audit Script 24](#_Toc296330883)

[5.6 Delete SQL AUDIT 25](#_Toc296330884)

[6 SQL Audit operation 26](#_Toc296330885)

[7 Troubleshoot SQL AUDIT 28](#_Toc296330886)

[Appendix a 29](#_Toc296330887)

# Reference documenation

|  |  |
| --- | --- |
| Document | Description |
| Detail Design - SQL Server | Detail design of SQL Server databases |

# Introduction

The purpose of this guide is to allow an experienced Microsoft SQL Server Administrator to successfully implement SQL server 2008 Audit.

It is intended that this document is used in conjunction with the other document detailed in Section 1 supporting the SQL Server shared service within the Aviva account.

# assumptions

The assumption is that the person performing the implementation will have the following permissions and memberships:

* Membership of the AD Group VIA\SQL\_NUIT\_Access2OASQLServers or have an account with necessary SQL server rights.
* Access to Axios Assyst.
* Approved Assyst request exist
* Approved design exist
* Local computer access to Remote Desktop (MSTSC).
* It is also assumed that the person(s) using this guide will be familiar to the Windows 2008 Server and SQL Server 2008 environment.
* Audit log folder exists and the required disk space available for the audit logs.

# pre-implementation

## pre-requisites

* Define the SQL audit levels
* Collaborate with the business and conclude on the various types of audit to ensure compliance for the application.
* Create a folder with the necessary access rights for the audit to be logged.
* SQL Server Audit is only available in SQL Server 2008 or above.

# Implementation of sql audit

The auditing of a SQL server database involves tracking and logging events that occur on the system. These events provide accumulated information about changes to the database, access to the databases etc. The type of audit (tracked event) implemented depends on Aviva requirements or governing body compliances.

There are several audit (tracked actions) levels that can be implemented and they are grouped into the following categories;

* *Server-level:* These actions include server operations, such as management changes and logon and logoff operations.
* *Database-level:* These actions encompass data manipulation languages (DML) and data definition language (DDL) operations.
* *Audit-level:* These actions include actions in the auditing process.

The entire SQL database environment can be audited using these tracked actions categories.

Before implementing SQL Server 2008 auditing it is important to understand these four items and there useful use in setting up SQL auditing correctly:

1. SQL Server Audit

2. Server Audit Specification (Events to capture on the Server Instance Level)

3. Database Audit Specification (Events to capture on a specific database)

4. Target (Where would be the events be logged)

For more detail refer to:

* *See section 4.10, Detail Design - SQL Server*
* [*http://msdn.microsoft.com/en-us/library/dd392015(v=sql.100).aspx*](http://msdn.microsoft.com/en-us/library/dd392015(v=sql.100).aspx)

## Advantages of SQL Server Audit

Refer to:

* [*http://www.bradmcgehee.com/2010/03/an-introduction-to-sql-server-2008-audit/*](http://www.bradmcgehee.com/2010/03/an-introduction-to-sql-server-2008-audit/)

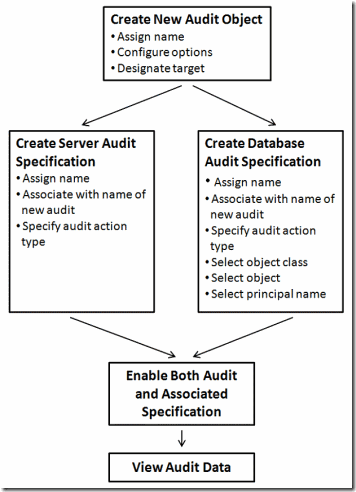
## Limitations of SQL Server Audit

Refer to:

* [*http://www.bradmcgehee.com/2010/03/an-introduction-to-sql-server-2008-audit/*](http://www.bradmcgehee.com/2010/03/an-introduction-to-sql-server-2008-audit/)

## How SQL Server Audit Works

The flow chart shown below should provide a broad overview of what’s involved in setting up auditing:

[](http://www.bradmcgehee.com/wp-content/uploads/2010/03/clip_image002.gif)

*Figure 1: A flow chart showing how to create a new SQL Server Audit*

SQL Server Audit allows for the creation of many different audits, covering most activity that occurs inside SQL Server.

The first step when creating a new audit is to create a **SQL Server Audit object**. When a new SQL Server Audit object created, assign it a name, select from several configuration options, and enter a designated a target. A target is the location where the audit data will be stored. A target can be a file on disk, the Applications Event Log, or the Security Event Log. Once these steps are completed, the new SQL Server Audit object is saved.

The second step is to create what is called an **Audit Specification**. SQL Server Audit offers two different types of Audit Specifications:

1. *Server Audit Specifications*– this is use to audit an activity that occurs at the SQL Server instance level, such as auditing login and logout activity.
2. *Database Audit Specifications*- this is use to audit an activity within a database, such as who is SELECTing data from a particular table.

Server and Database Audit Specifications are created differently so decision needs to be made on the type needed up-front. When creating either type of Audit Specification, first assign it a name, and then the Audit Specification must be associated with the SQL Server Audit object created in the first step.

*The rule is that a SQL Server Audit object can only be associated with one Audit Specification*. In other words, SQL Server Audit objects can’t be reuse when creating another Audit Specifications.

The last step to creating a Server or Database Audit Specification is to assign it an Audit Action Type. *An Audit Action Type is a predefined activity that occurs in SQL Server that can be audited.*

For more detail refer to:

* [*http://www.bradmcgehee.com/2010/03/an-introduction-to-sql-server-2008-audit/*](http://www.bradmcgehee.com/2010/03/an-introduction-to-sql-server-2008-audit/)

## implementation

To implement SQL Server Audit there are three main components that can be configured to achieve audit and they are as follows:

1. Server Audit

* *See section 4.10, Detail Design - SQL Server*
  + [*http://msdn.microsoft.com/en-us/library/dd392015(v=sql.100).aspx*](http://msdn.microsoft.com/en-us/library/dd392015(v=sql.100).aspx)

1. Server Audit Specification object

* *See section 4.10, Detail Design - SQL Server*
  + [*http://msdn.microsoft.com/en-us/library/dd392015(v=sql.100).aspx*](http://msdn.microsoft.com/en-us/library/dd392015(v=sql.100).aspx)

1. Database Audit Specification

* *See section 4.10, Detail Design - SQL Server*
  + [*http://msdn.microsoft.com/en-us/library/dd392015(v=sql.100).aspx*](http://msdn.microsoft.com/en-us/library/dd392015(v=sql.100).aspx)

**Note**: *SQL Server Audit must be configure first or exist in order to be able to configure Server or Database audit specification because of the dependencies.*

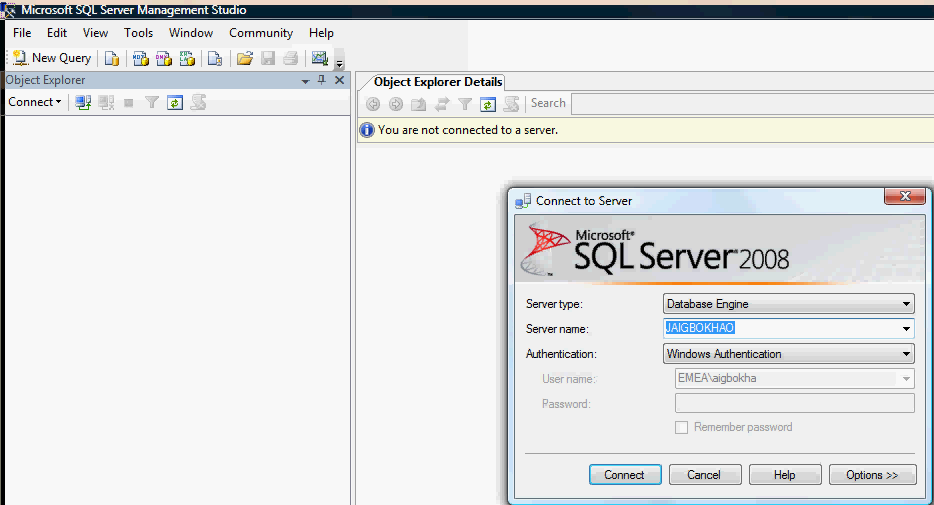
For more detail refer to:

* [*http://msdn.microsoft.com/en-us/library/dd392015.aspx*](http://msdn.microsoft.com/en-us/library/dd392015.aspx)

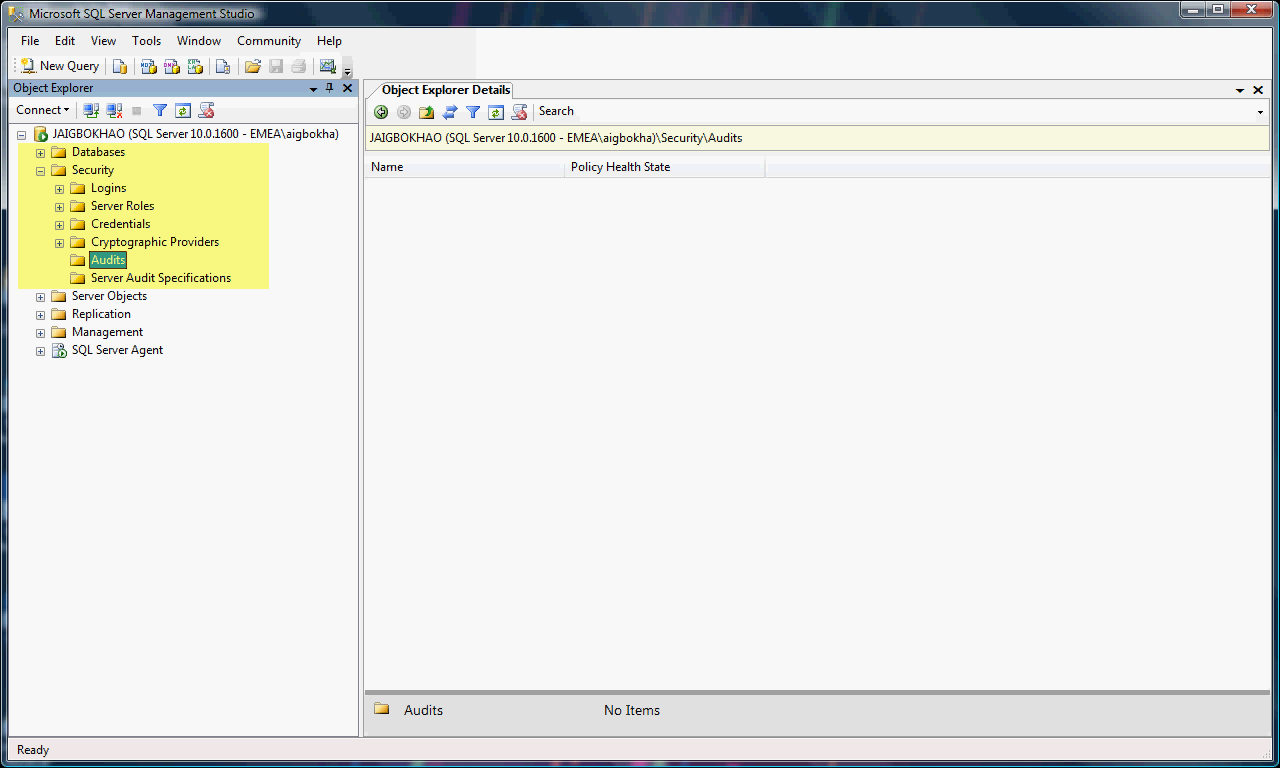
### Step by step walk through

#### Configure Server Audit

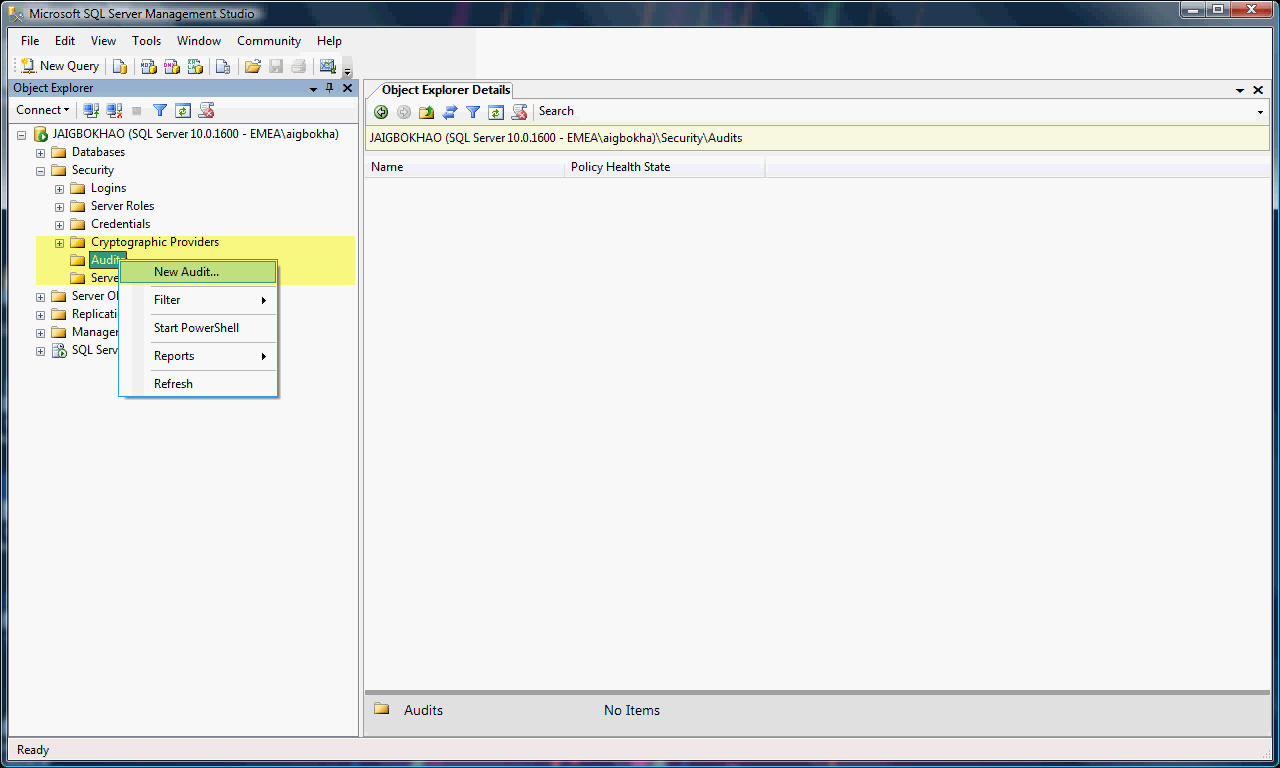
1. Click open SQL Server 2008 Management Studio and log into it.



1. In the Object Explorer, expand the Security node and select the Audit node.



1. Right click on the Audit node and select the option "New Audit" from the menu.



1. A dialog box "Create Audit" will appear with a few important fields.

Field description

*Audit name:* This is the name of the audit. There presently no naming convention for this and it is yet to be decided.

*Queue delay (in milliseconds):* This specifies the amount of time in milliseconds that can elapse before audit actions are forced to be processed.

*Shut down server on audit failure:* Forces a server shut down when the server instance writing to the target cannot write data to the audit target.

*Audit destination:* This specifies the target for auditing data.

*File path:* This specifies the location of the folder where audit data is written when the Audit destination is a file.

**Note:** This is a path name only. SQL Server automatically names the output file in the following format:

*<audit\_name>\_<audit\_GUID>\_<partition\_number>.sqlaudit*

*Maximum rollover files:* This specifies the maximum number of audit files to retain in the file system.

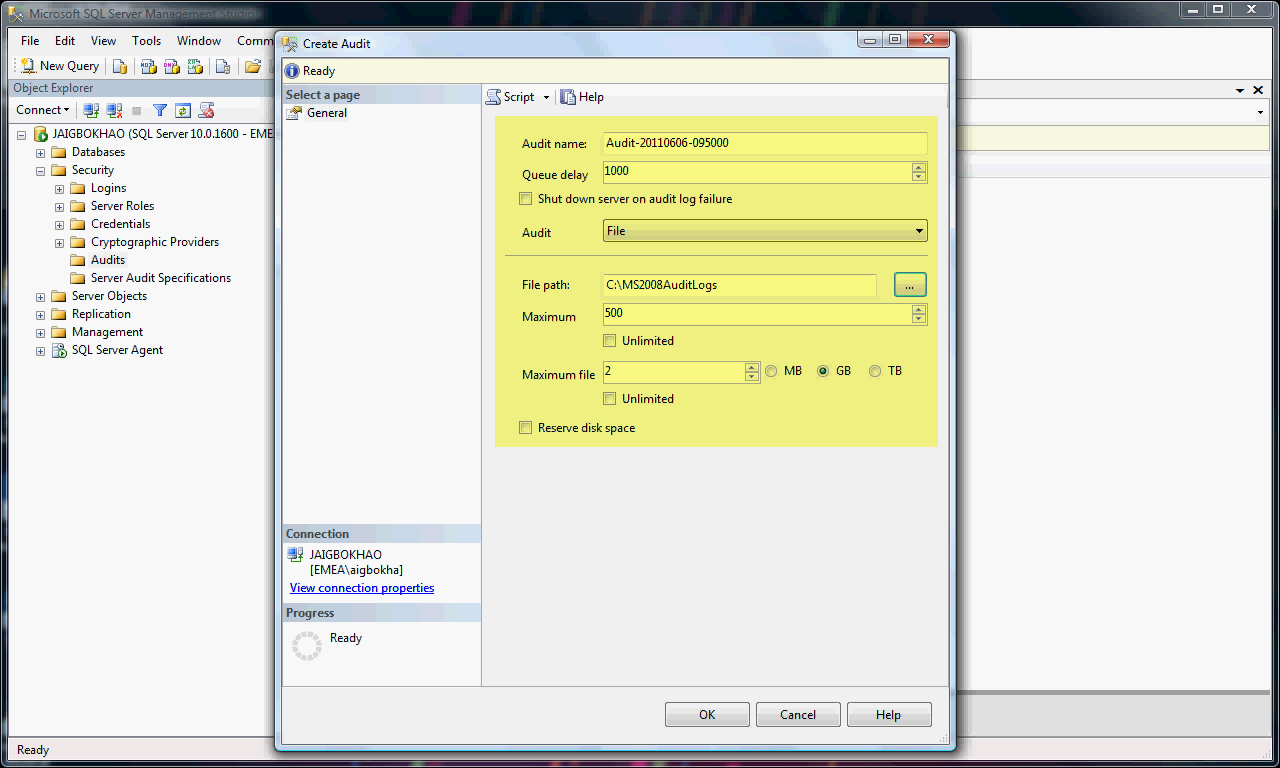
*Maximum file size (MB):* This specifies the maximum size, in megabytes (MB), for an audit file.

*Reserve disk space:* This specifies that space is pre-allocated on the disk equal to the specified maximum file size.

To understand the importance of these fields refer to:

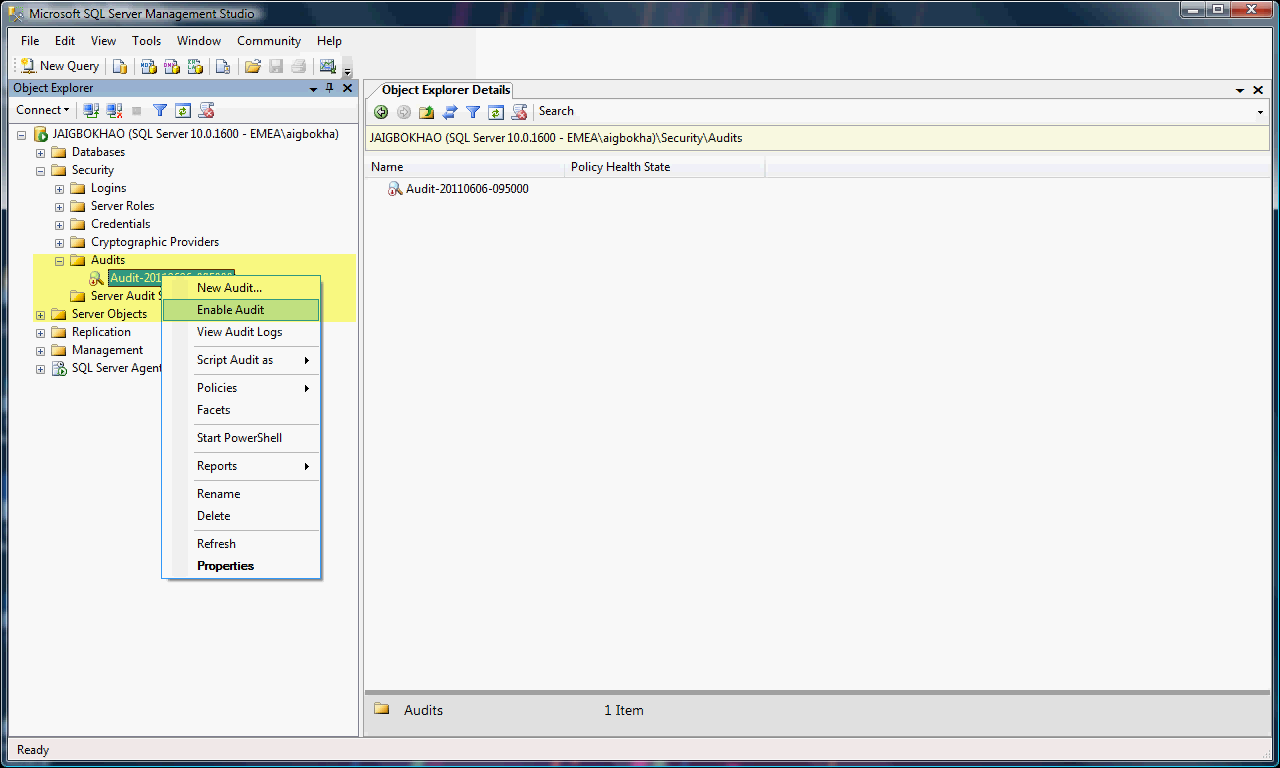
* *See section 4.10.1, Detail Design – SQL Server*
* [*http://blogs.msdn.com/b/manisblog/archive/2008/07/21/sql-server-2008-auditing.aspx*](http://blogs.msdn.com/b/manisblog/archive/2008/07/21/sql-server-2008-auditing.aspx)
* [*http://msdn.microsoft.com/en-us/library/cc280649.aspx*](http://msdn.microsoft.com/en-us/library/cc280649.aspx)

Fill the fields highlighted in yellow as shown below.

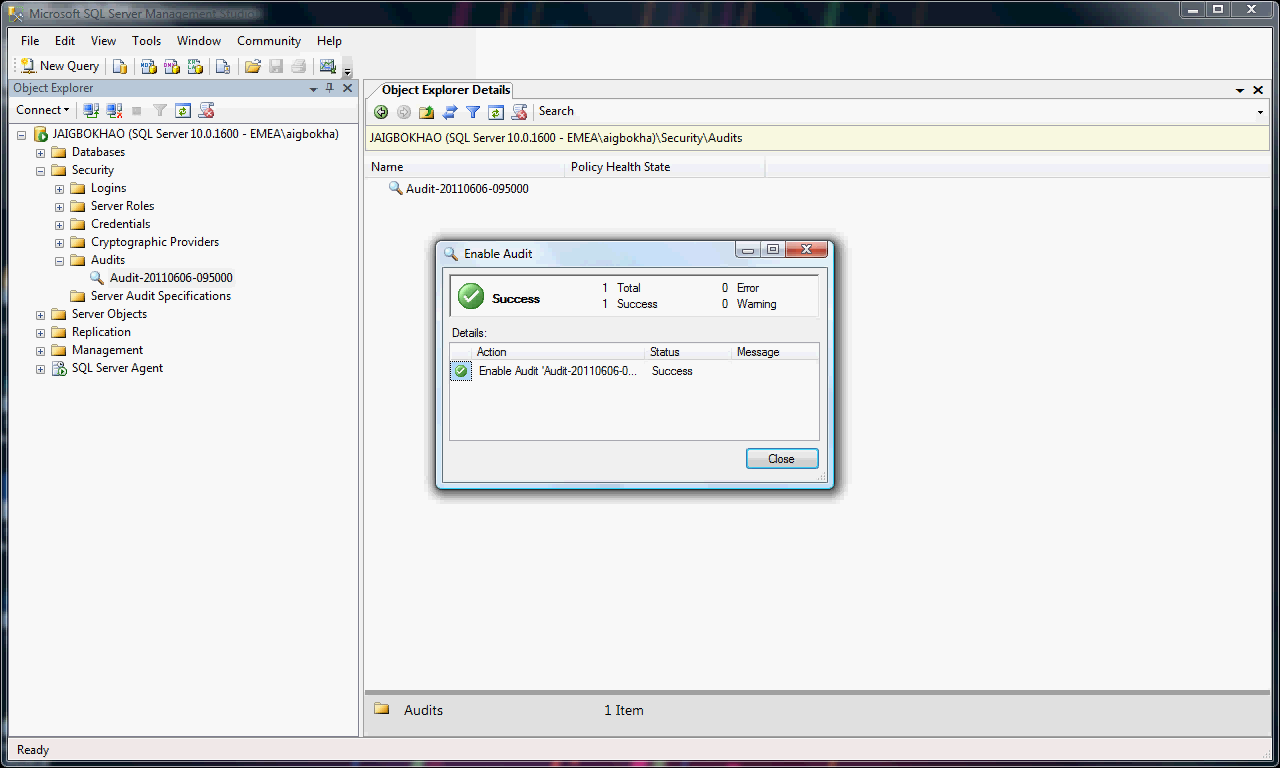


**Note**: These values above are to show how to configure audit and is to be used as a guide only. The actual values of the fields in shared service environment will depend solely on the business requirement and approved design.

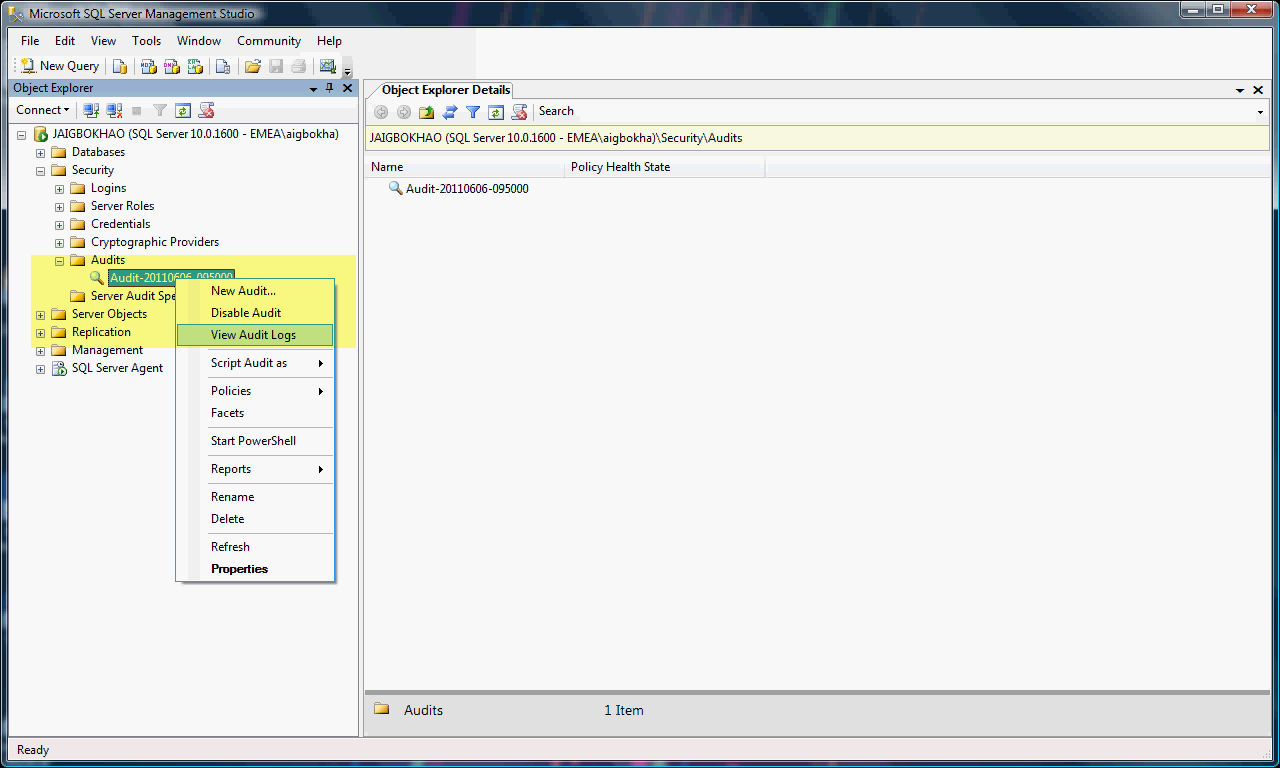
1. Once the Audit is created, it is in a disabled state and it needs to be enabled. To enable the Audit, just right click on the Server Audit that was just created and from the menu select "Enable Audit".



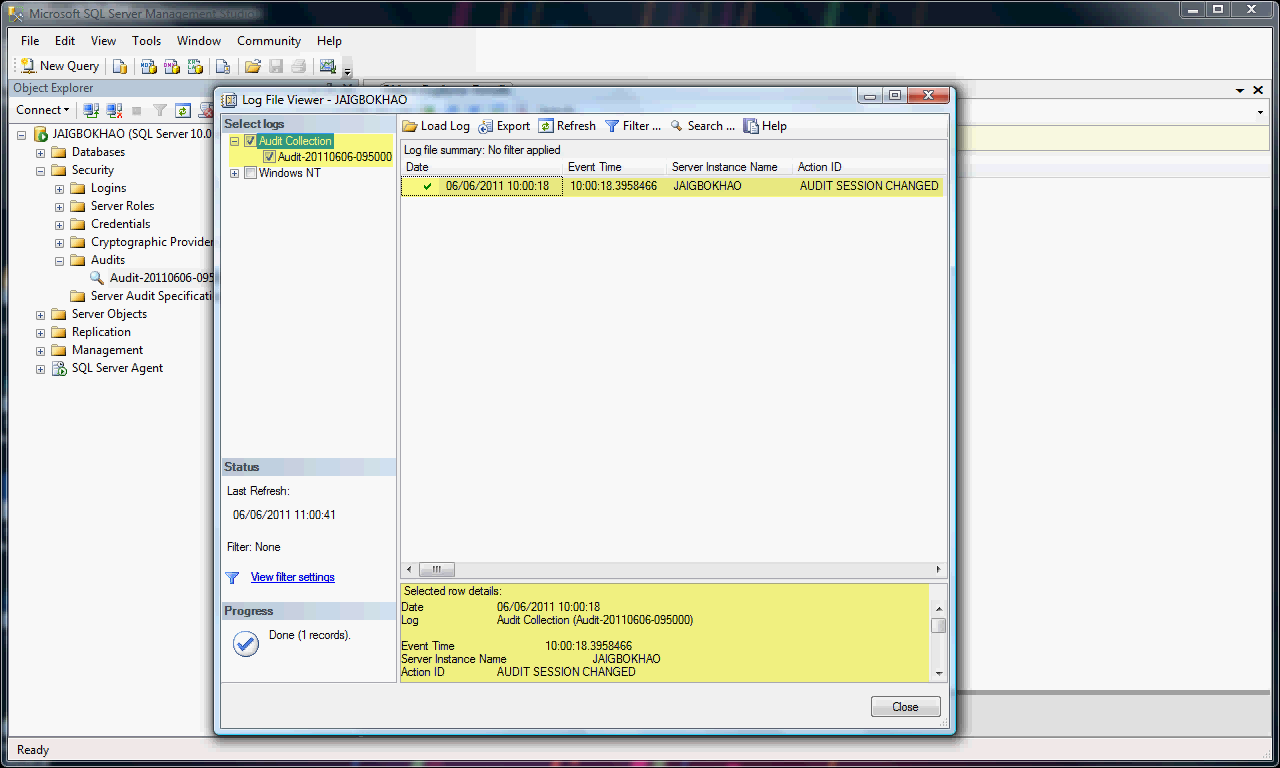
A dialog box with the success message will appear, if the operation was successful.



1. To view the Audit log of the Audit just created and select the option "View Audit Logs".



A dialog box containing the audit logs will appear.



#### Configure Server Audit Specification

Before creating server audit specification, it is very important to ensure Server Audit exist and also useful to understand the concept and detail about Server Audit specifications.

For detail about Server Audit specifications refer to:

* [*http://technet.microsoft.com/en-us/library/cc280663(SQL.100).aspx*](http://technet.microsoft.com/en-us/library/cc280663(SQL.100).aspx)

For Server Audit Specification configuration settings in FMO shared service refer to:

* *See Appendix A: Audit\_Events\_Settings.doc, Detail Design – SQL Server*

Fields description for the file in *Appendix A: Audit\_Events\_Settings.doc*:

*Audit Action description*: Shows the event captured by audit.

*Object Class Name*: The objects belogong to the SQL server object class.

*Audit action type*: Shows the Audit Action Group.

*Server Audit Level settings*: Indicates audit events that can be configured from the server audit specification.

*Database Audit Level settings*: Indicates audit events that can be configured from the database audit specification.

Once a decision is made on the type of audit events to configure, check the *Appendix A: Audit\_Events\_Settings.doc* to determine if the event can be configured from the Server or database specification level.

For example, configure Failed Login audit event.

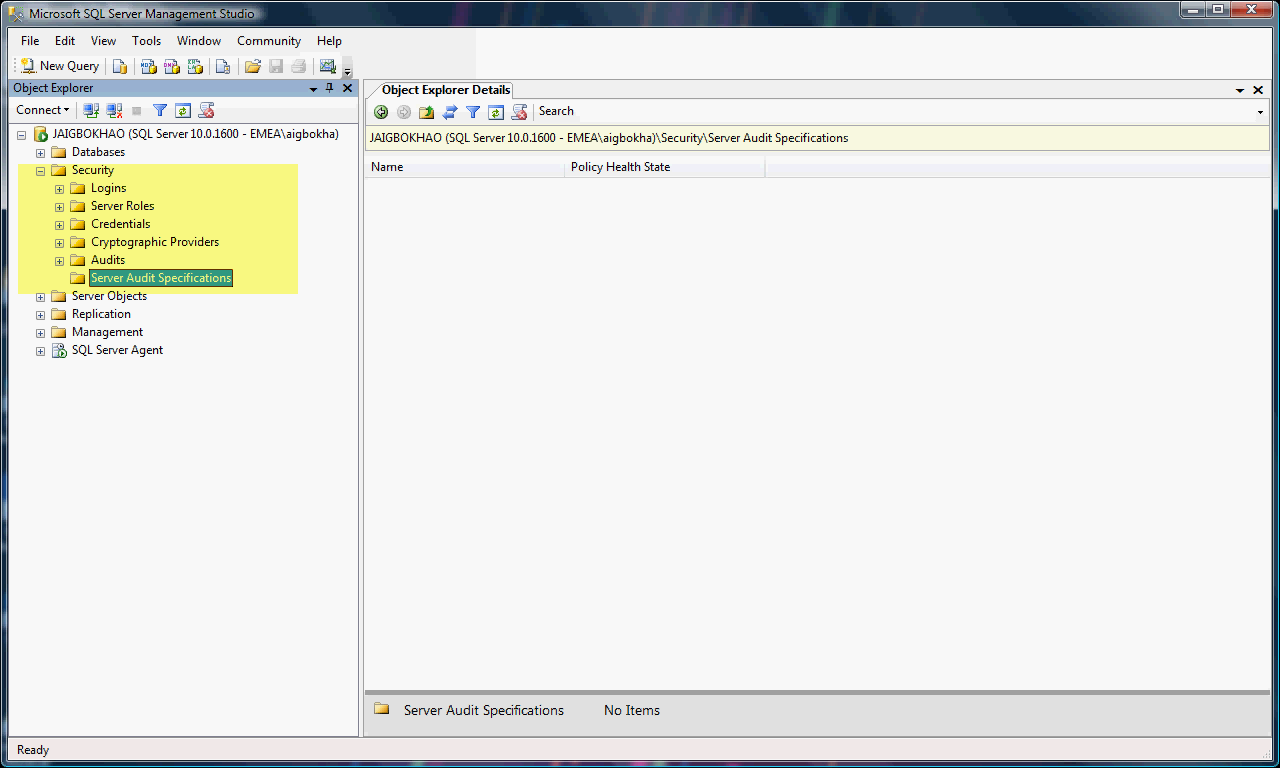
| **Audit Action Description** | **Object Class Name** | **Audit Action Type** | **Server Audit Level Settings** | **Database Audit Level Settings** |
| --- | --- | --- | --- | --- |
| **LOGIN FAILED** | LOGIN | FAILED\_LOGIN\_GROUP | SERVER AUDIT SPECIFICATION |  |

*From the Appendix A: Audit\_Events\_Settings.doc, failed login audit event can only be configured from the Server Audit Level (Server Audit specification) settings.*

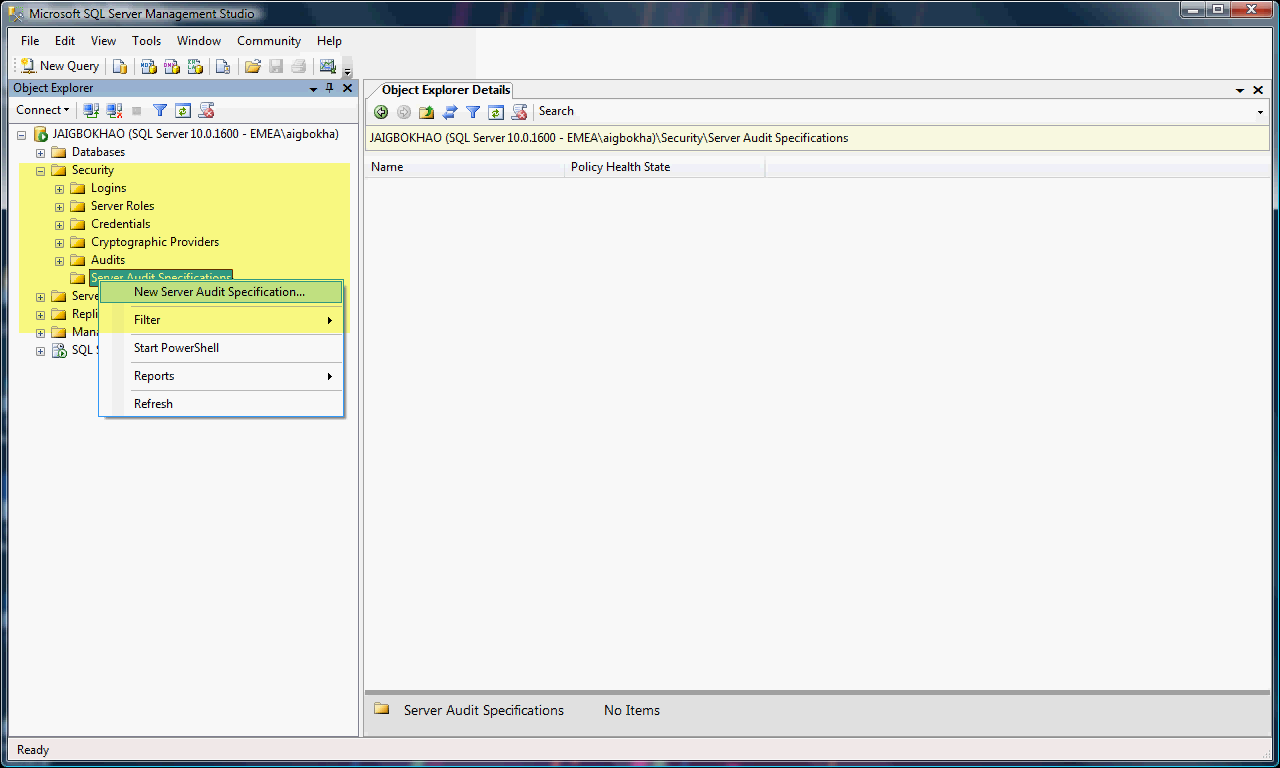
*Steps to create Server Audit Specification*

In this example, create the Server Audit Specification for failed login audit.

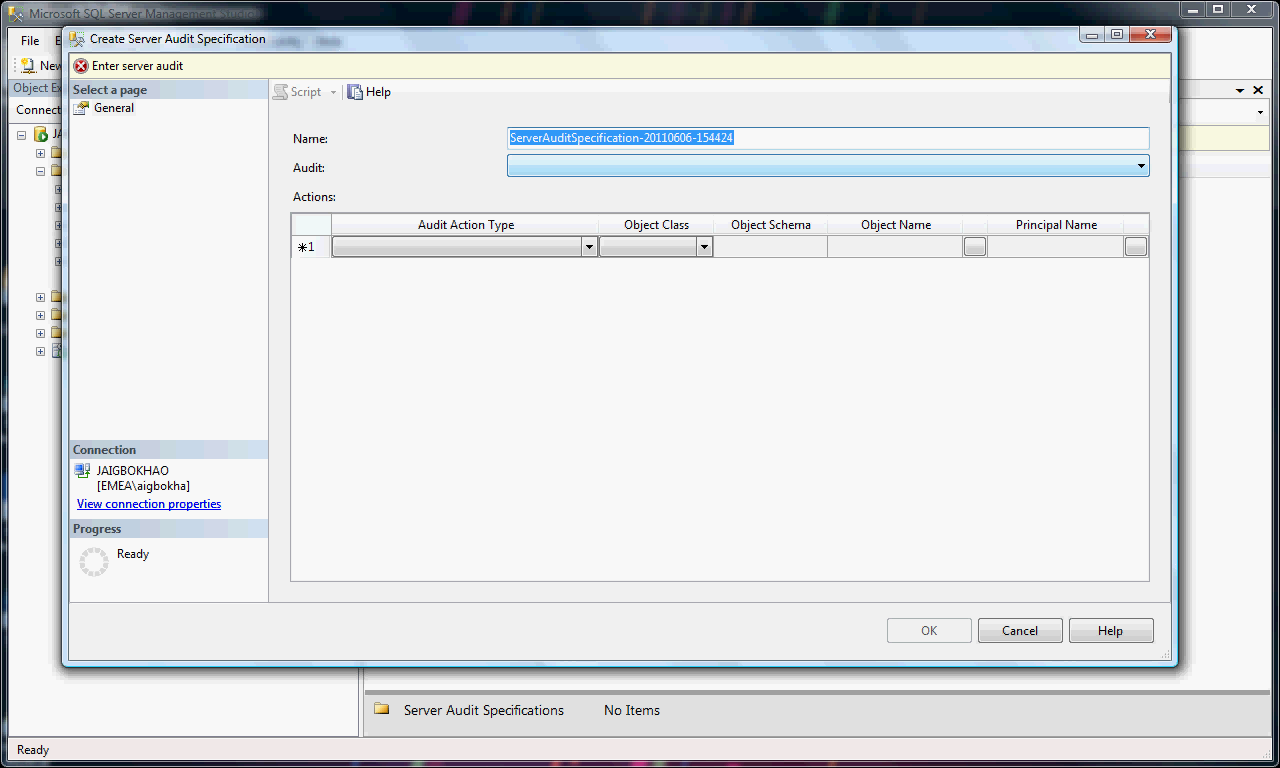
1. In Object Explorer, expand the Security node, then the Audits node and Select “Server Audit Specifications”.



1. Right click on the Server Audit Specifications and select "New Server Audit Specification".

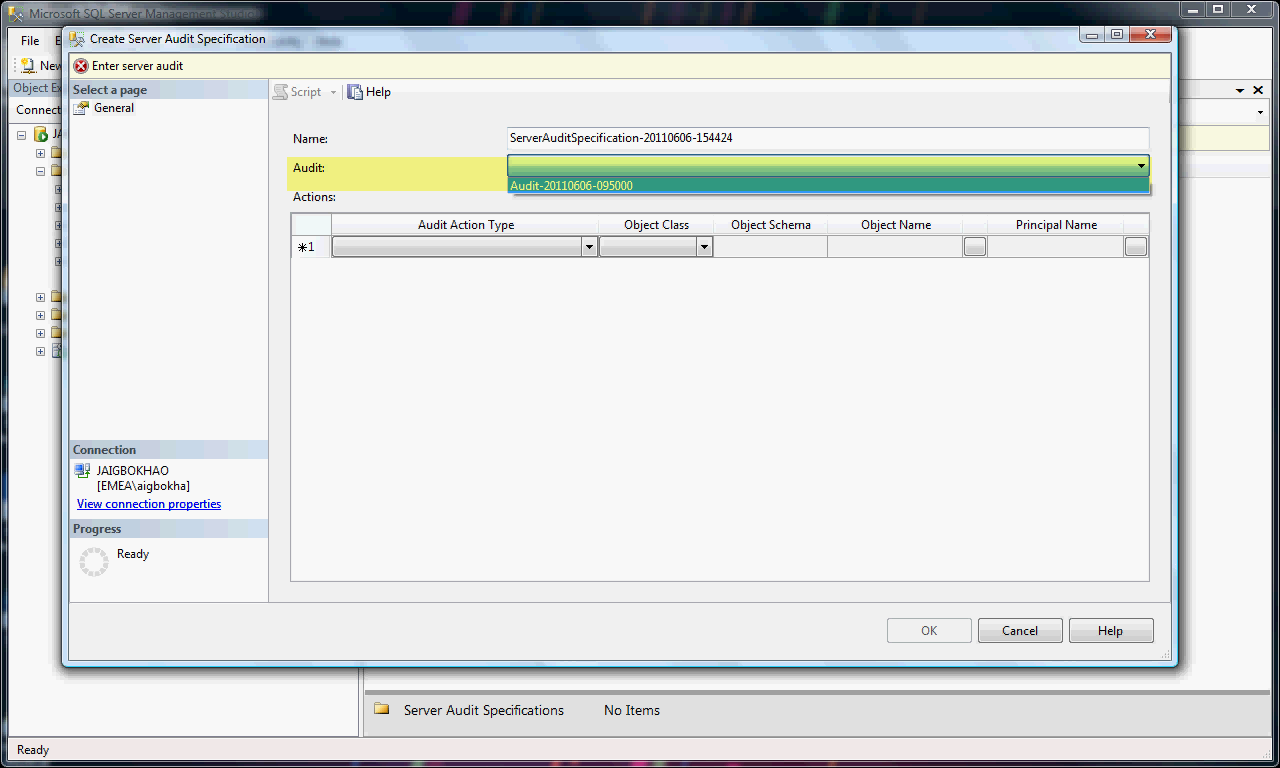


A dialog box appears in which the Server Audit Specification can be created.



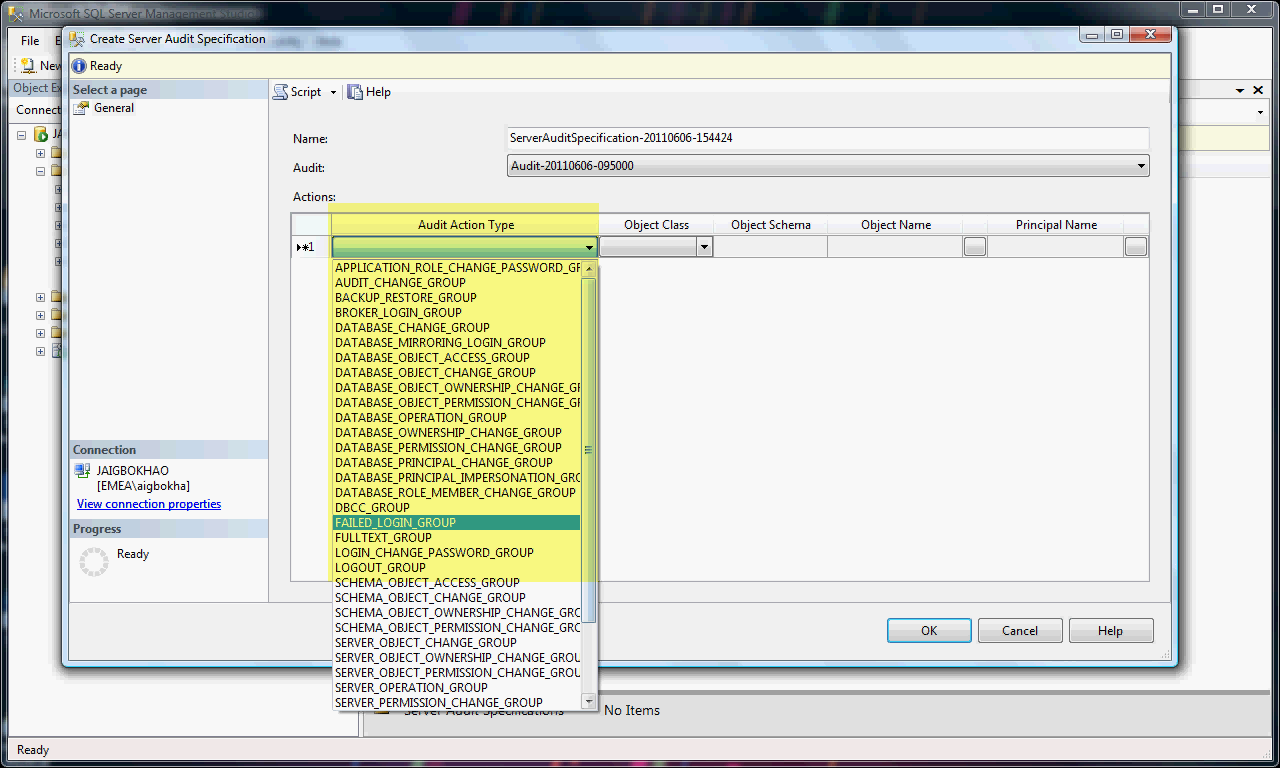
**Note**: The name for Server Audit Specification can be changed to a user friendly name. But in this example, the default name is used.

1. Select "Server Audit" created in *section 5.4.1.1*.

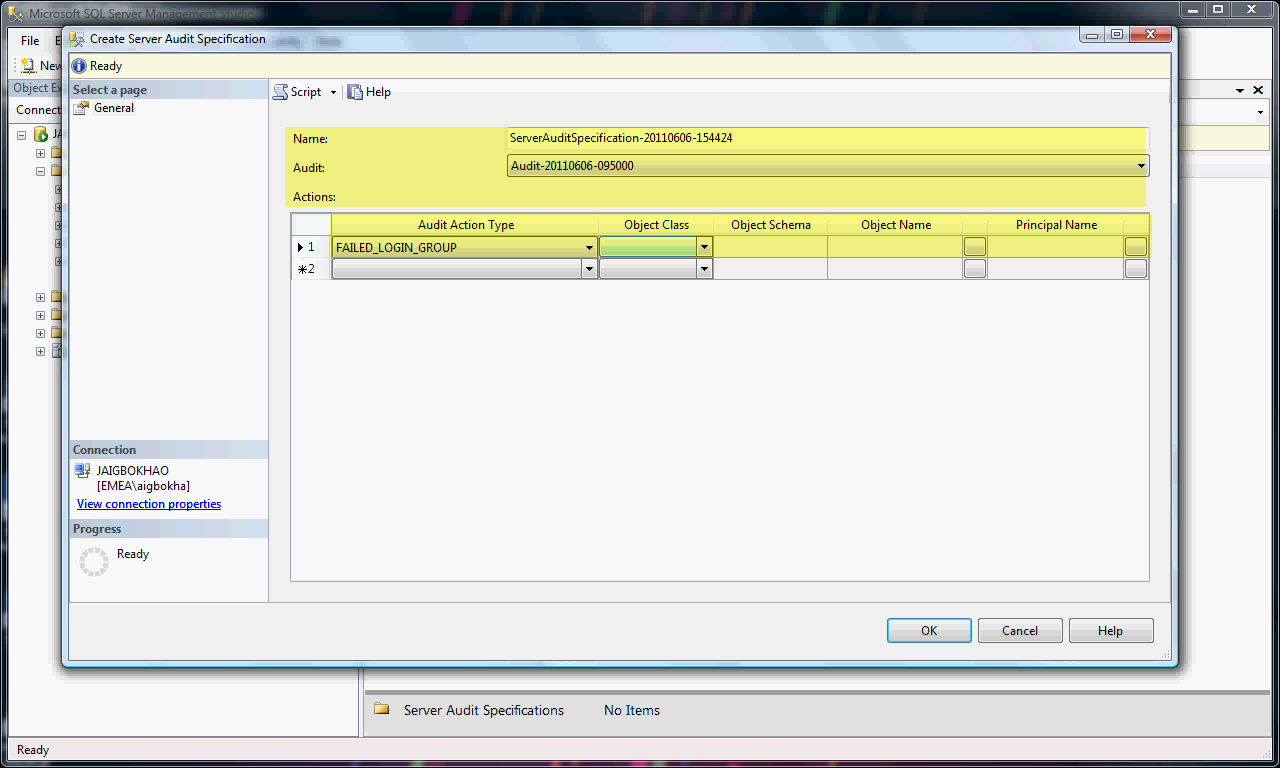


1. Select the specific the Audit Action Type (same as Audit Action Group) from the drop down list. Once all the required Audit Action Groups are selected, click OK and Audit Specification will be created for the server. In this Step the Server Audit Specification for failed login audit is created.

To do this, select the Audit Action Type "FAILED\_LOGIN\_GROUP" and click OK. Whenever a failed login occurs it will then be logged.



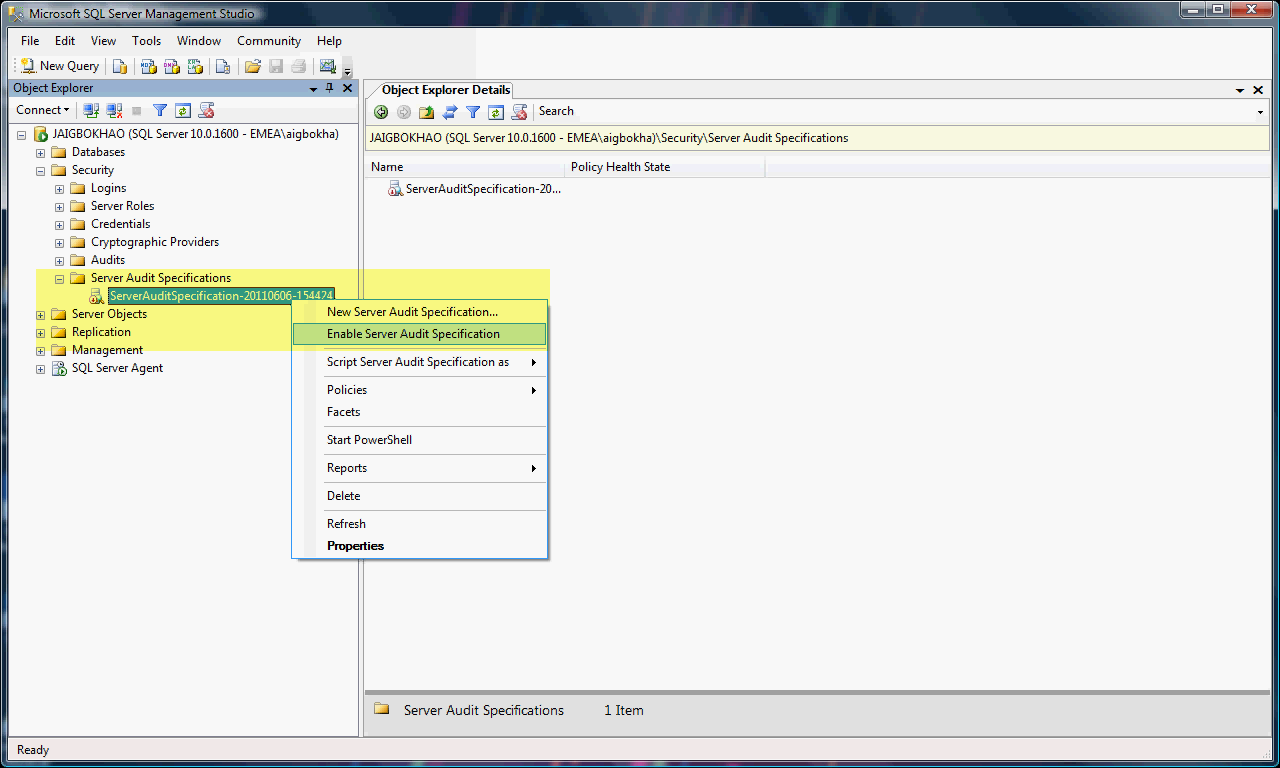
The Audit Action Group "FAILED\_LOGIN\_GROUP" selected.



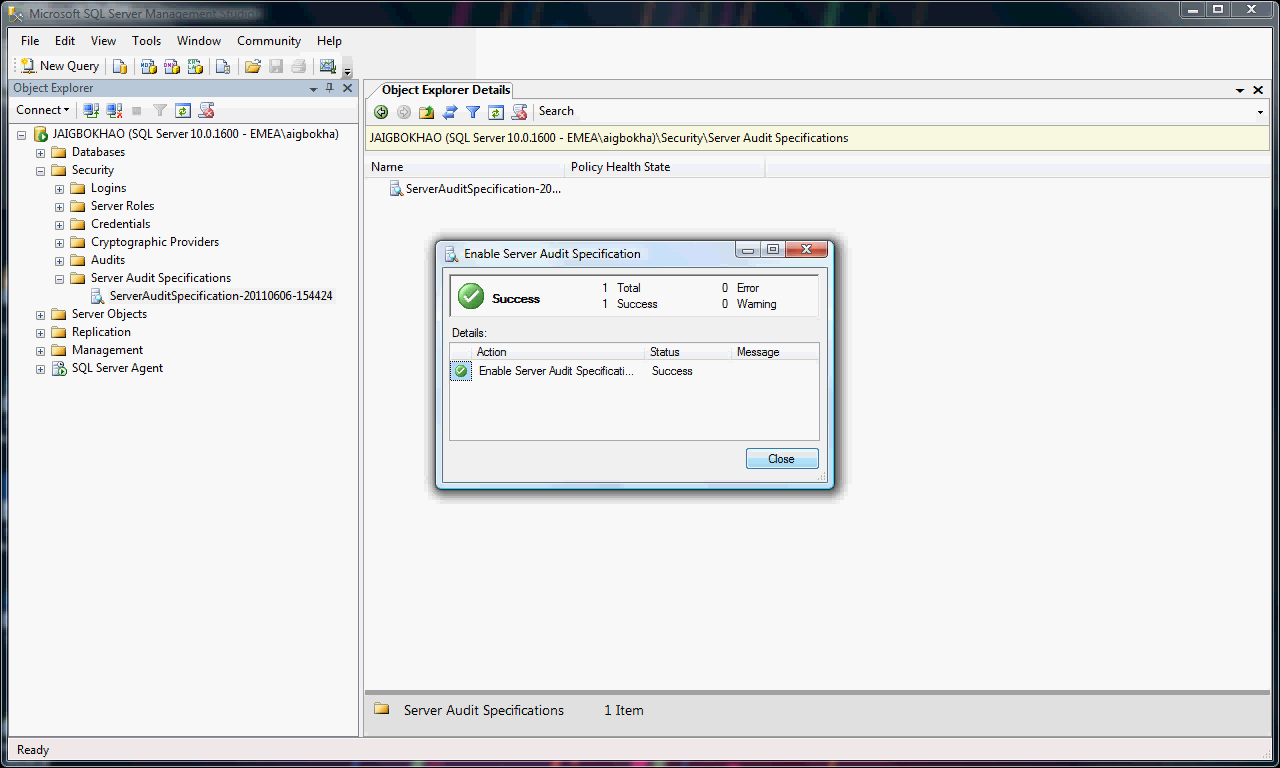
For more about Create Server Audit Specification fields refer to:

* [*http://msdn.microsoft.com/en-us/library/cc280453.aspx*](http://msdn.microsoft.com/en-us/library/cc280453.aspx)

1. Once the Server Audit Specification is created, it is in a disabled state and it needs to be enabled. To enable the Server Audit Specification, just right click on the Server Audit Specification that was just created and from the menu select "Enable Server Audit Specification".



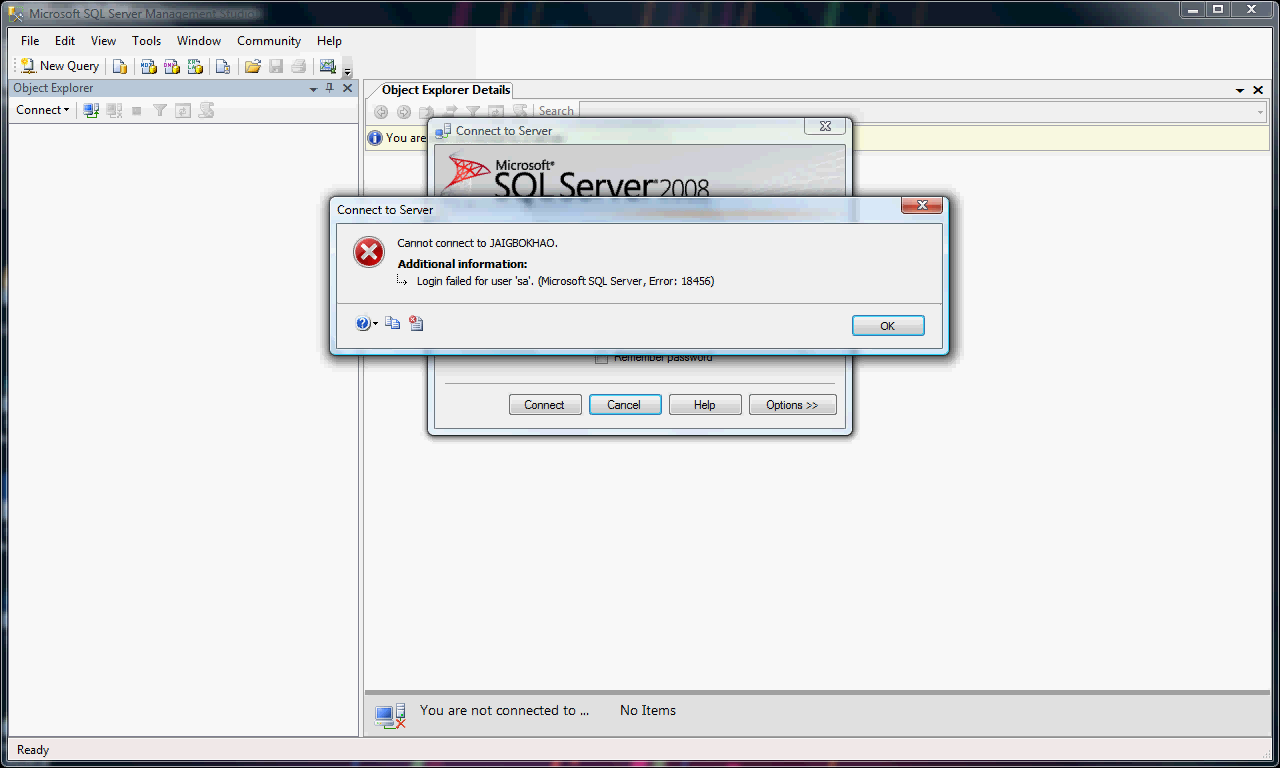
A dialog box with the success message will appear, if the operation was successful.



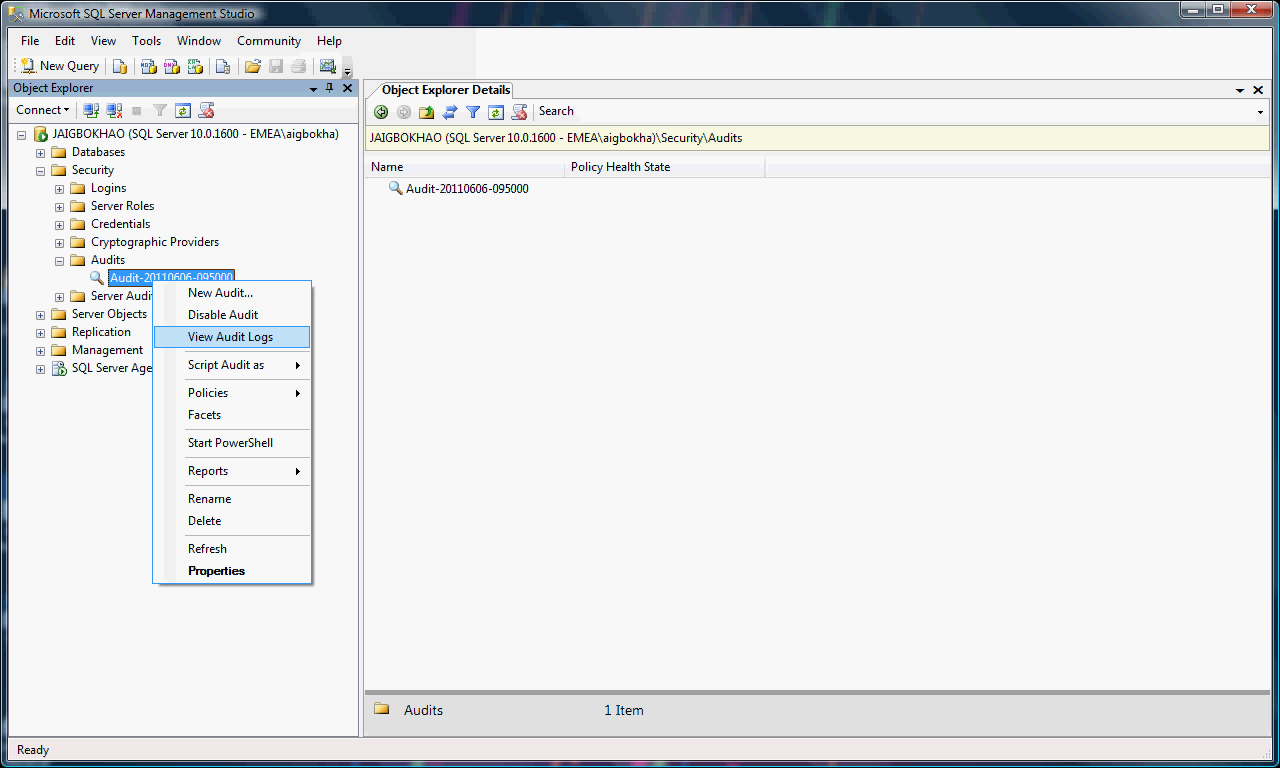
##### Test Server Audit Configure

To test the Server Audit Specification configured for login failure, logon to the server with the wrong password to force login failure. Then review the logs to assure that the Audit is working.

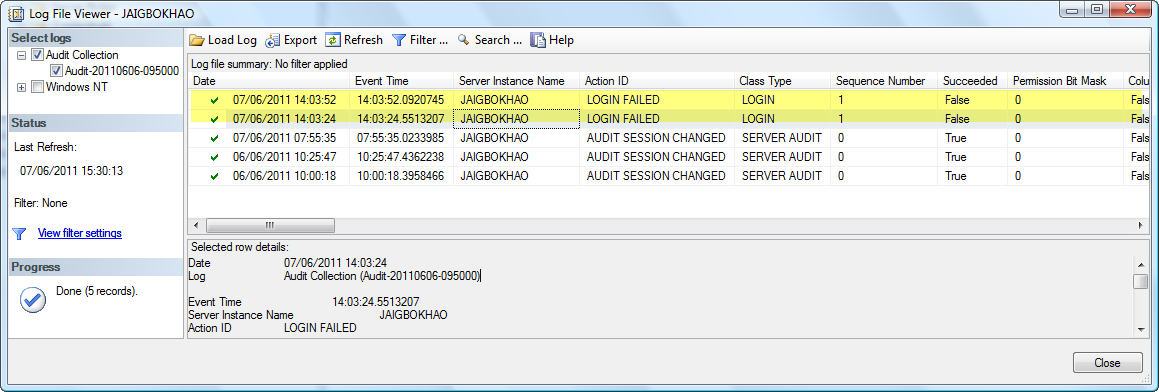
1. Logon to the server as SA with wring password. Logon failure occurred.



1. Right click on the Audit node and select the option "View Audit Logs" to view the Audit log of the Audit (*Audit-20110606-095000*).



1. This will bring up the dialog box that will show the details of the failed login event. Scroll to the right to find the details in the dialog box.



This show the audit events are been logged successfully.

#### Configure Database Audit Specification

Before creating database audit specification, it is very important to ensure Server Audit exist and also useful to understand the concept and detail about Database Audit specifications.

For detail about Database Audit specifications ("Database-Level Audit Action Groups" and "Database-Level Audit Actions") refer to:

* [*http://technet.microsoft.com/en-us/library/cc280663(SQL.100).aspx*](http://technet.microsoft.com/en-us/library/cc280663(SQL.100).aspx)

For Database Audit Specification configuration settings in FMO shared service refer to:

* *See Appendix A: Audit\_Events\_Settings.doc, Detail Design – SQL Server*

Example,

Configure Audit for create, alter, and drop operations done by any user in DemoTestDB.

*Firstly, check the Appendix A: Audit\_Events\_Settings.doc to determine if the event can be configured from the Server or database specification level.*

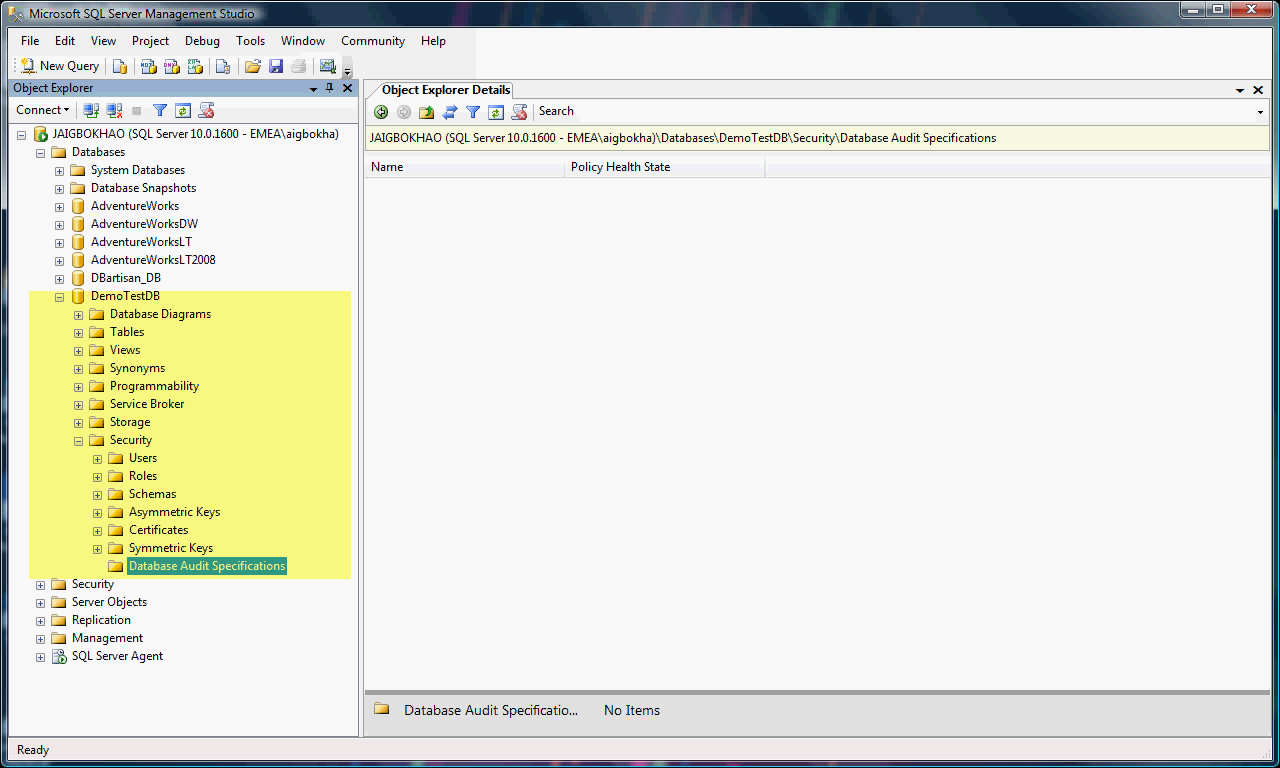
| **Audit Action Description** | **Object Class Name** | **Audit Action Type** | **Server Audit Level Settings** | **Database Audit Level Settings** |
| --- | --- | --- | --- | --- |
| **CREATE** | TABLE | DATABASE\_OBJECT\_CHANGE\_GROUP | SERVER AUDIT SPECIFICATION | DATABASE AUDIT SPECIFICATION |
| **ALTER** | TABLE | DATABASE\_OBJECT\_CHANGE\_GROUP | SERVER AUDIT SPECIFICATION | DATABASE AUDIT SPECIFICATION |
| **DROP** | TABLE | DATABASE\_OBJECT\_CHANGE\_GROUP | SERVER AUDIT SPECIFICATION | DATABASE AUDIT SPECIFICATION |
| **CREATE** | OBJECT | SCHEMA\_OBJECT\_CHANGE\_GROUP | SERVER AUDIT SPECIFICATION | DATABASE AUDIT SPECIFICATION |
| **ALTER** | OBJECT | SCHEMA\_OBJECT\_CHANGE\_GROUP | SERVER AUDIT SPECIFICATION | DATABASE AUDIT SPECIFICATION |
| **DROP** | OBJECT | SCHEMA\_OBJECT\_CHANGE\_GROUP | SERVER AUDIT SPECIFICATION | DATABASE AUDIT SPECIFICATION |

*From the Audit\_Events\_Settings.doc,* create, alter, and drop audit event can *be configured from either Server Audit Level (Server Audit specification) settings or Database Audit Level (Database Audit specification) settings.*

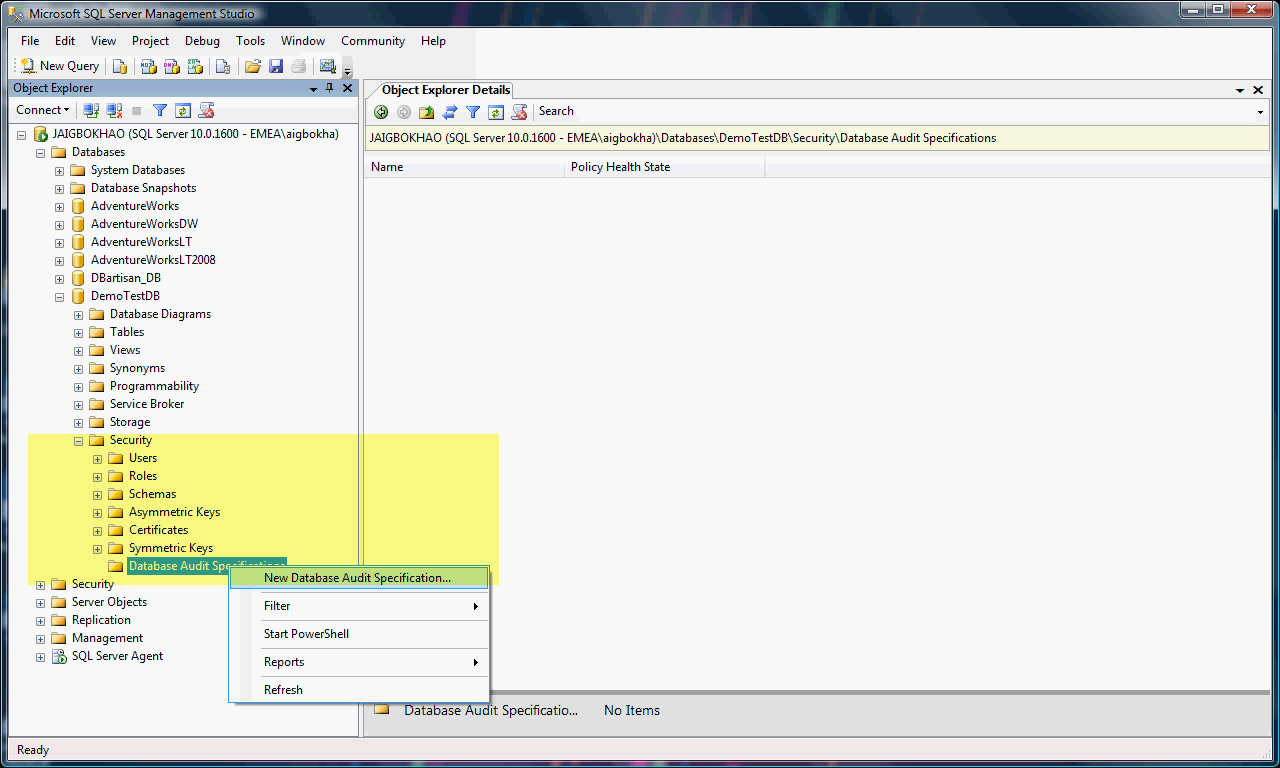
**Note**: *In order to audit CREATE/DROP of an objects, select both the SCHEMA\_OBJECT\_CHANGE\_GROUP and DATABASE\_OBJECT\_CHANGE\_GROUP. The reason for this, see* [*http://connect.microsoft.com/SQLServer/feedback/details/370103/database-object-change-group-audit-group-does-not-audit-drop-proc*](http://connect.microsoft.com/SQLServer/feedback/details/370103/database-object-change-group-audit-group-does-not-audit-drop-proc)*Steps to create Database Audit Specification*

In this example, create the Database Audit Specification for create, alter, and drop audit.

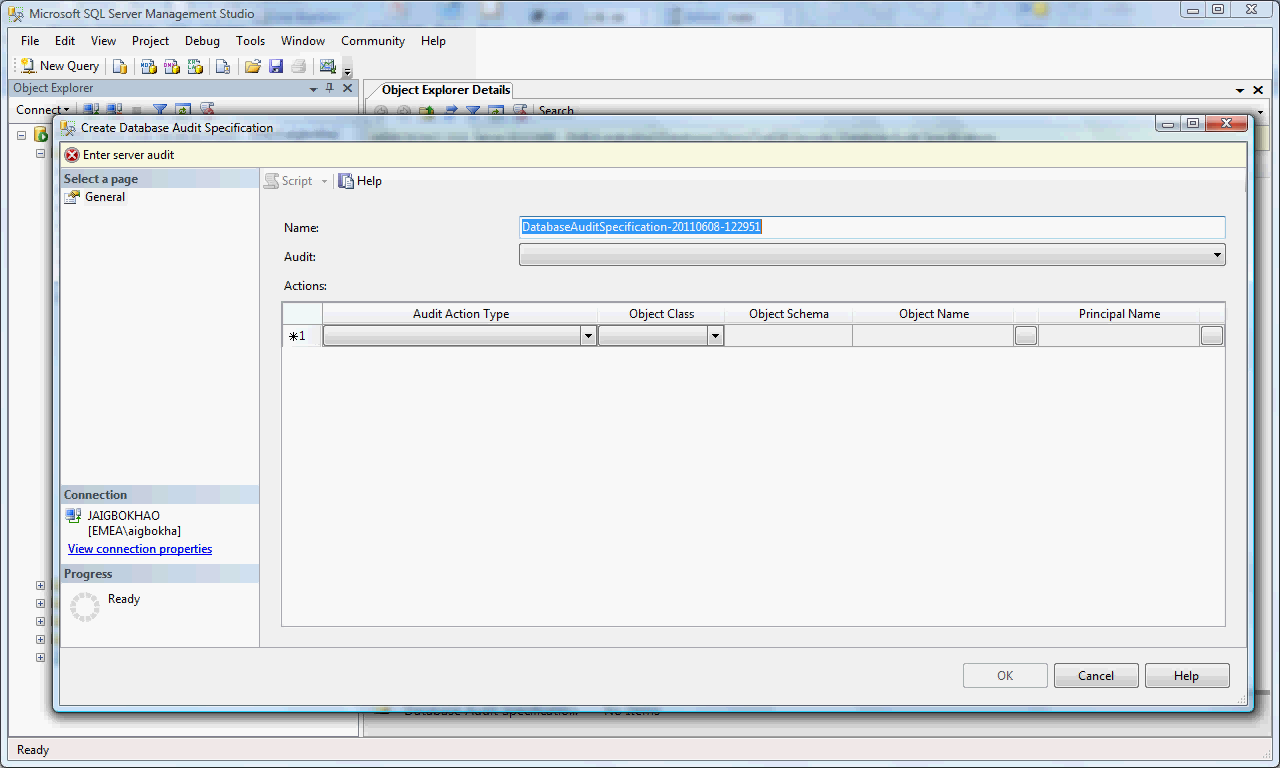
1. In Object Explorer, expand the Database node, the DemoTestDB node, then Security node and Select “Database Audit Specifications”.



1. Right click on the "Database Audit Specifications" node and select "New Database Audit Specification" from the menu.

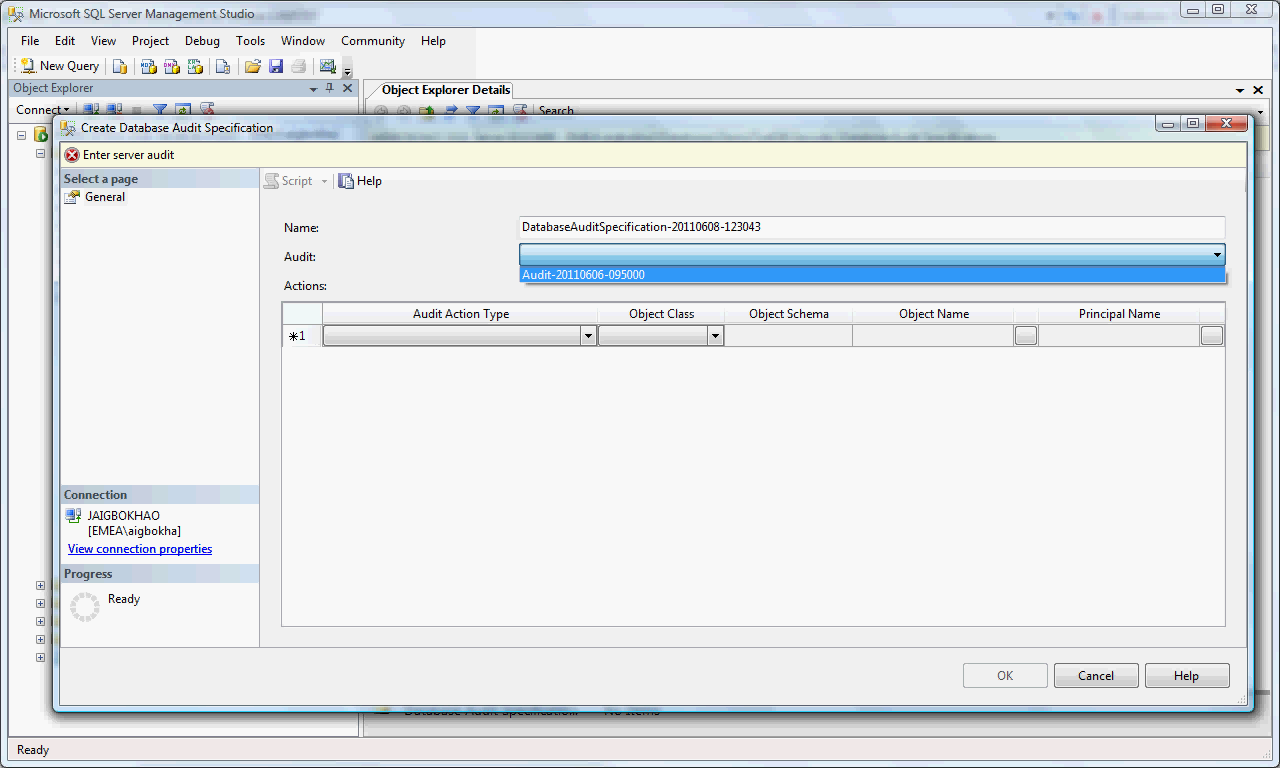


A dialog box appears to Create Database Audit Specification.



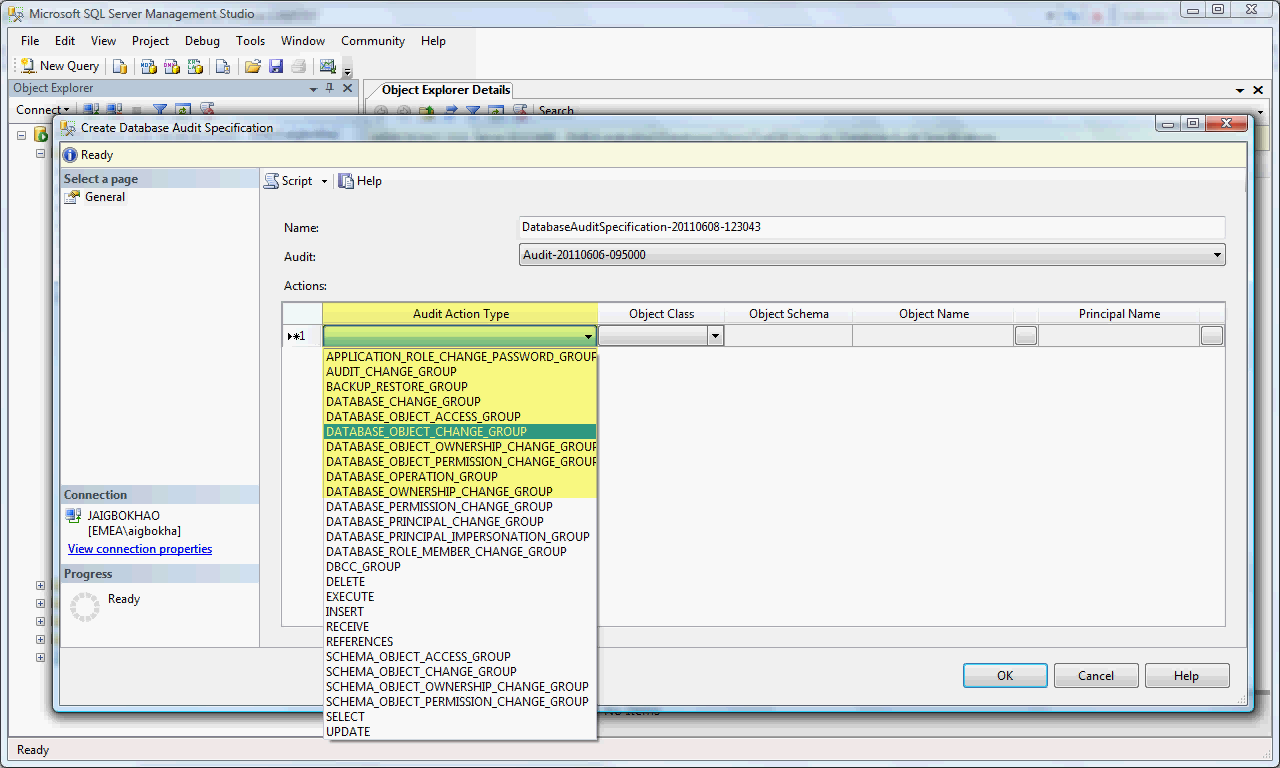
**Note**: The name for Database Audit Specification can be changed to a user friendly name. But in this example, the default name is used.

1. Select "Server Audit" created in *section 5.4.1.1.*

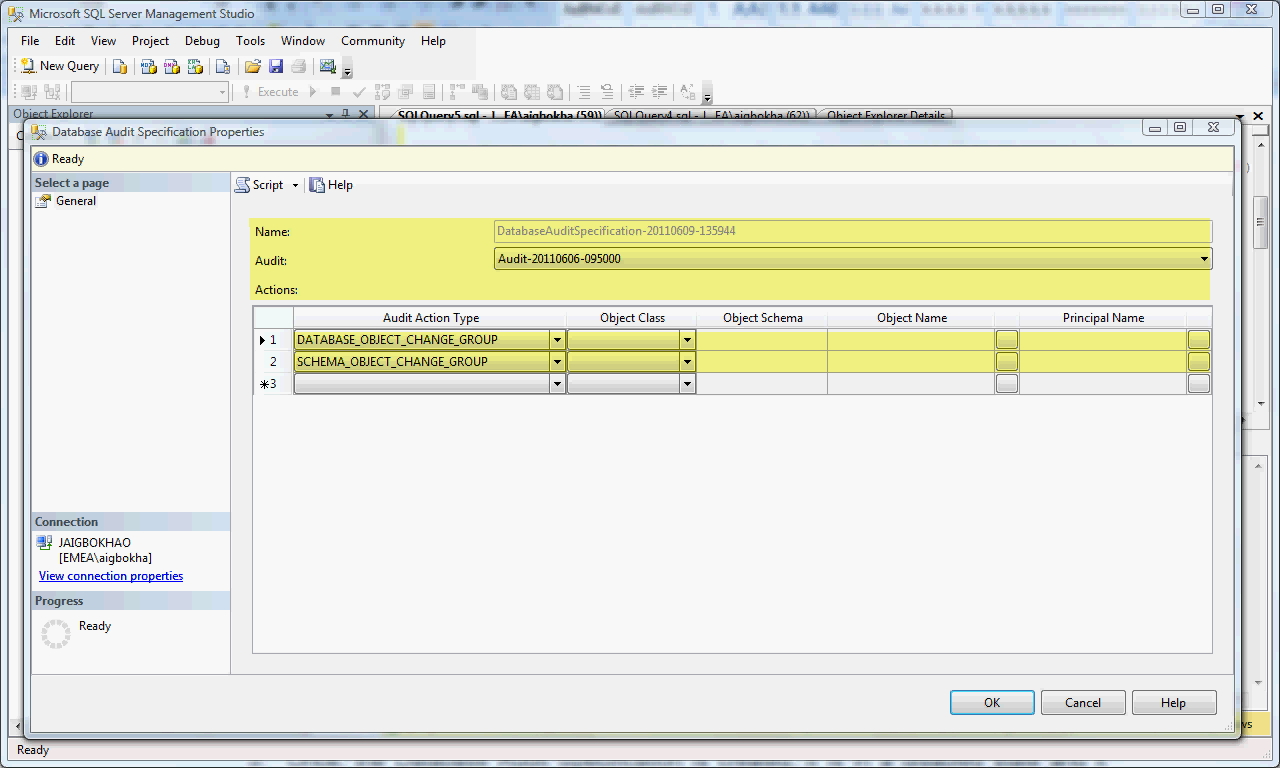


1. Select the specific the Audit Action Type (same as Audit Action Group) from the drop down list. Once all the required Audit Action Groups are selected, click OK and Database Audit Specification will be created for the server. In this Step the Database Audit Specification for create, alter, and drop audit is created.

To do this, select the Audit Action Type "DATABASE\_OBJECT\_CHANGE\_GROUP" and "SCHEMA\_OBJECT\_CHANGE\_GROUP" and click OK. These events are raised whenever any users create, alter or drop table object in the database (DemoTestDB).



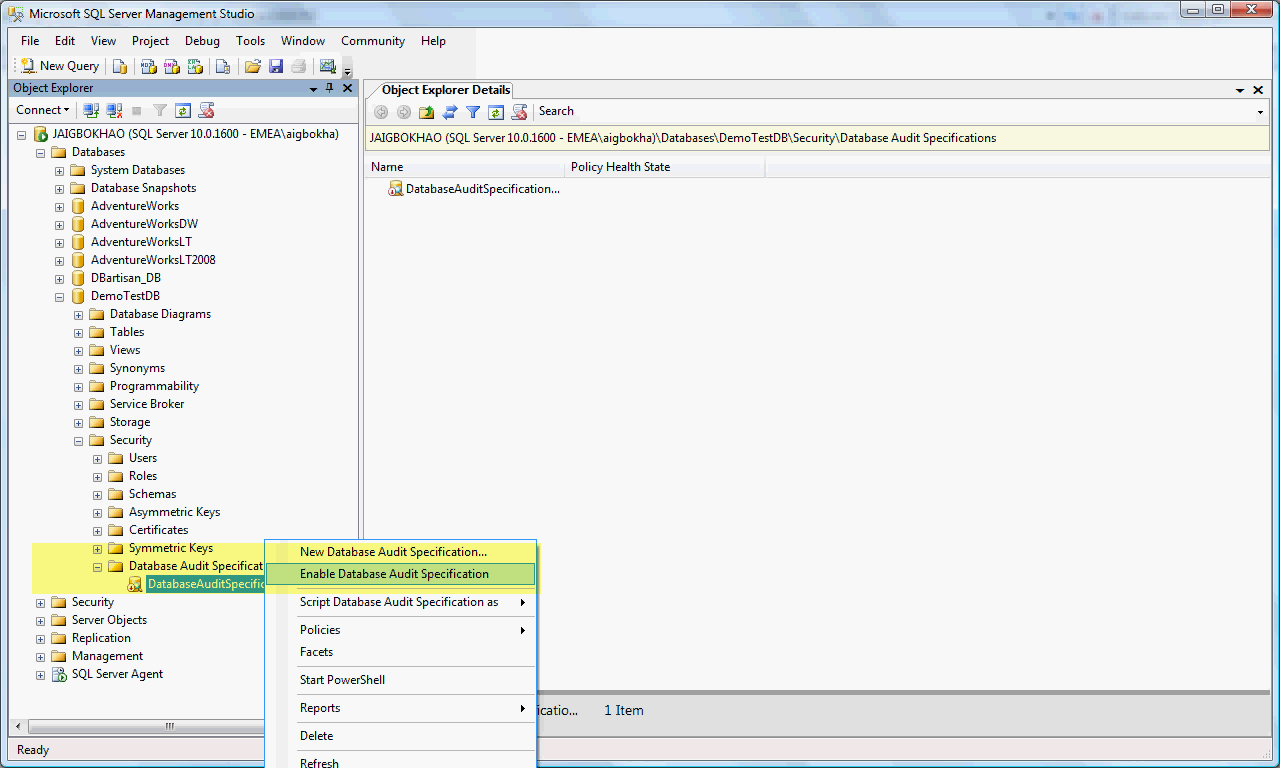
The Audit Action Types "DATABASE\_OBJECT\_CHANGE\_GROUP” and "SCHEMA\_OBJECT\_CHANGE\_GROUP" selected.



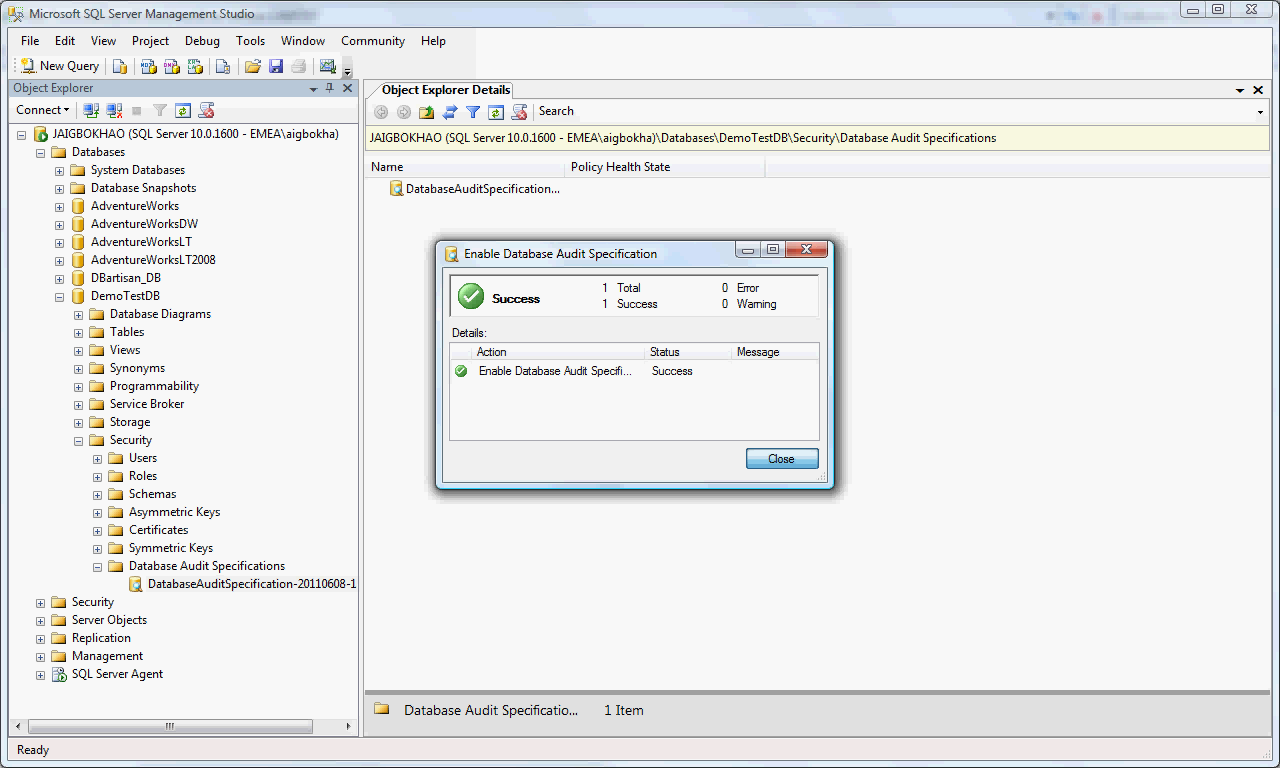
For more about Create Database Audit Specification fields refer to:

* + [*http://msdn.microsoft.com/en-us/library/cc280472.aspx*](http://msdn.microsoft.com/en-us/library/cc280472.aspx)

1. Once, the Database Audit Specification is created, it is in a disabled state and it needs to be enabled. To enable the Database Audit Specification, just right click on the Database Audit Specification that was just created and from the menu select "Enable Database Audit Specification".



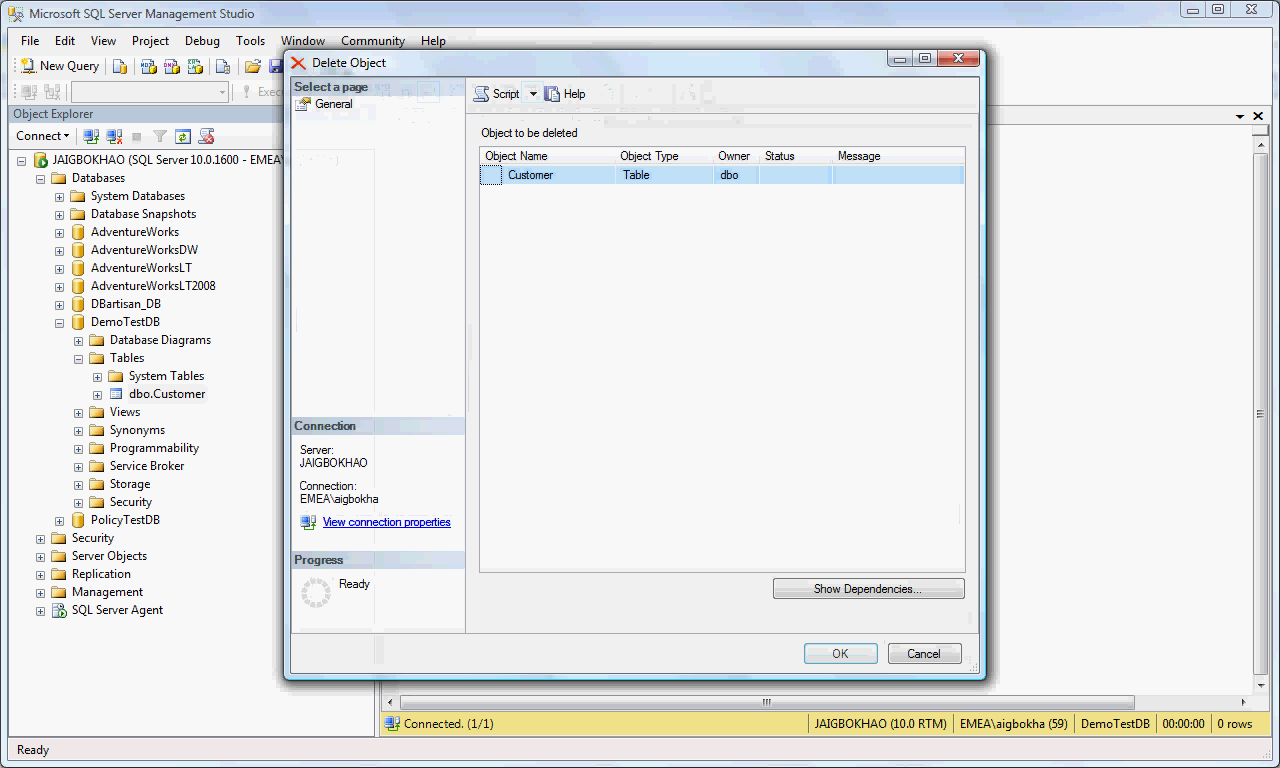
A dialog box with the success message will appear, if the operation was successful.



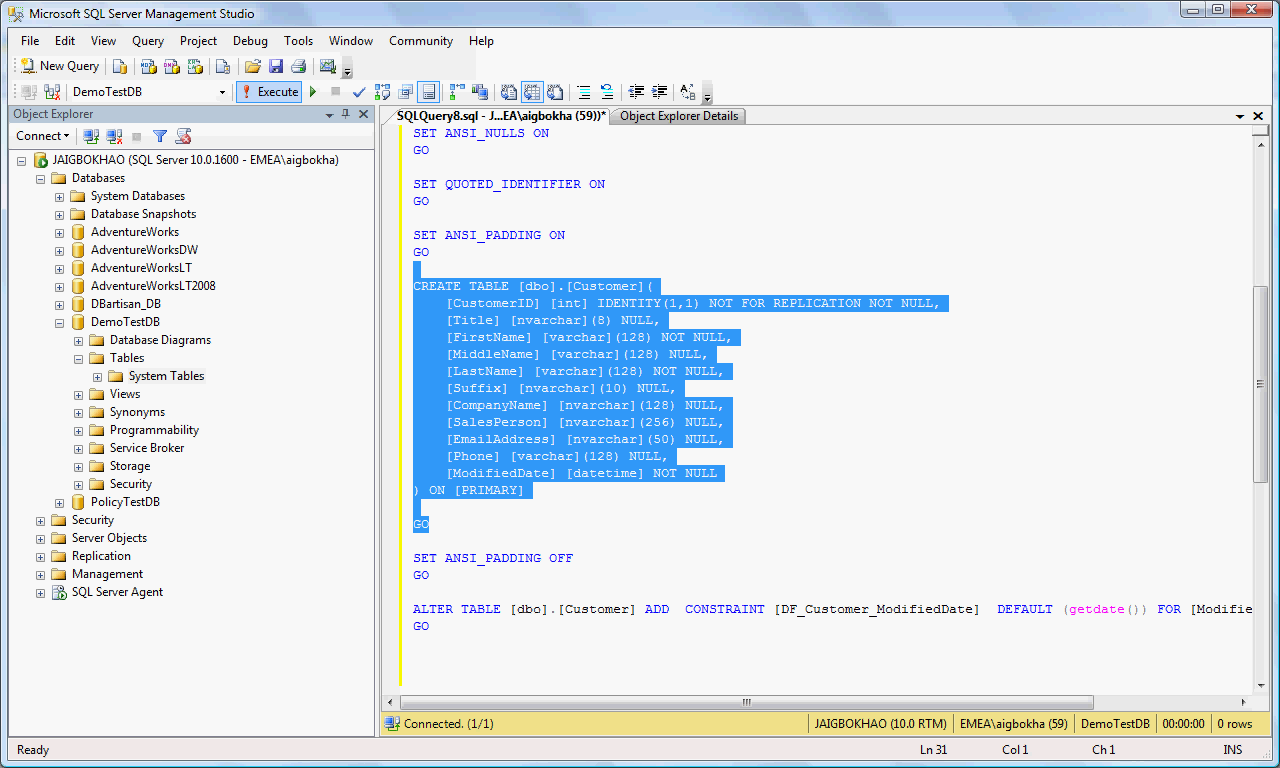
##### Test Database Audit Configure

To test the Database Audit Specification configured for create, alter and drop table, logon to the server and carryout create, alter and drop table actions. Then review the logs to assure that the Audit is working.

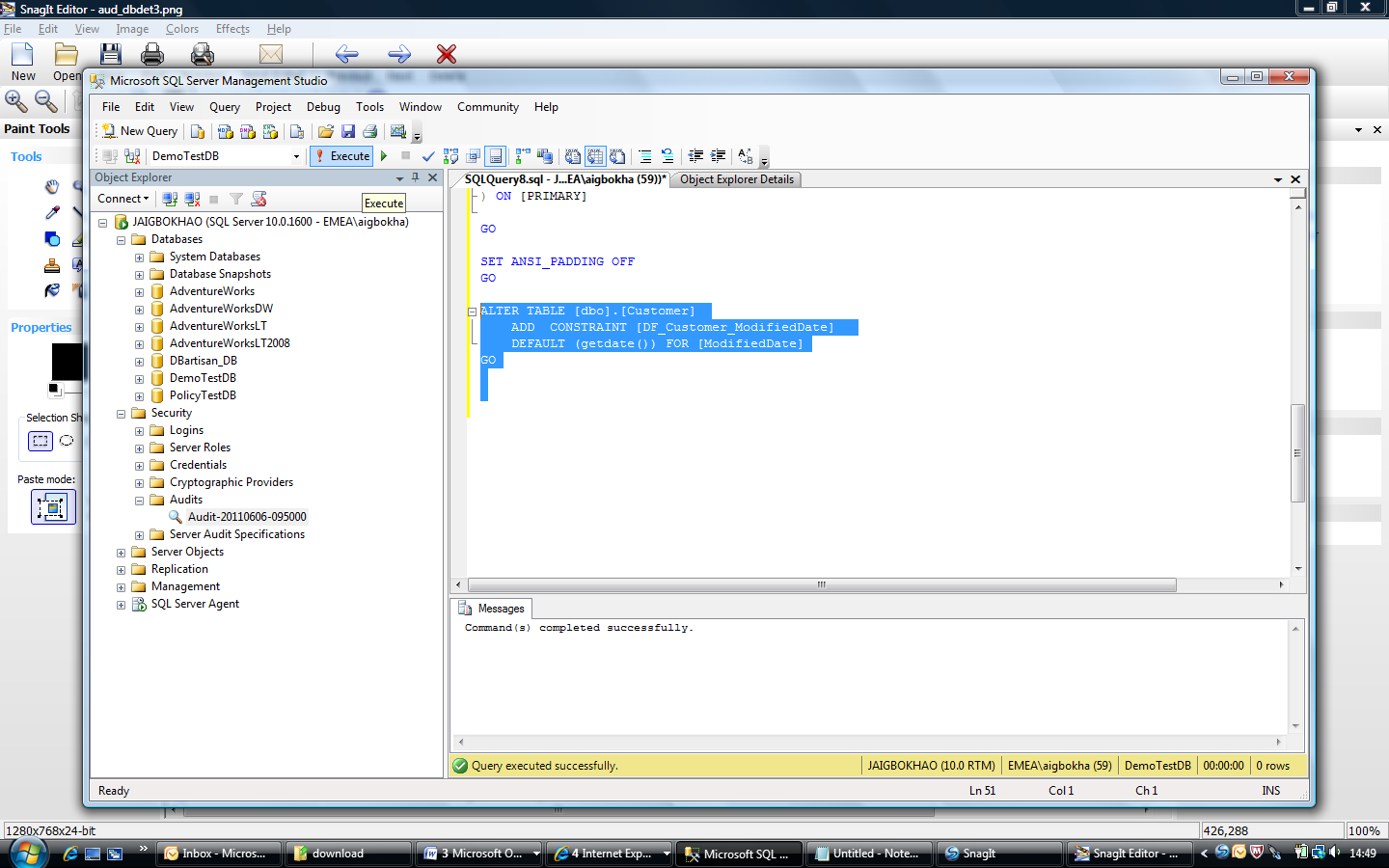
1. Logon to the server, drop, create, and alter (dbo.customer) table in DemoTestDB.
2. Drop table dbo.customer



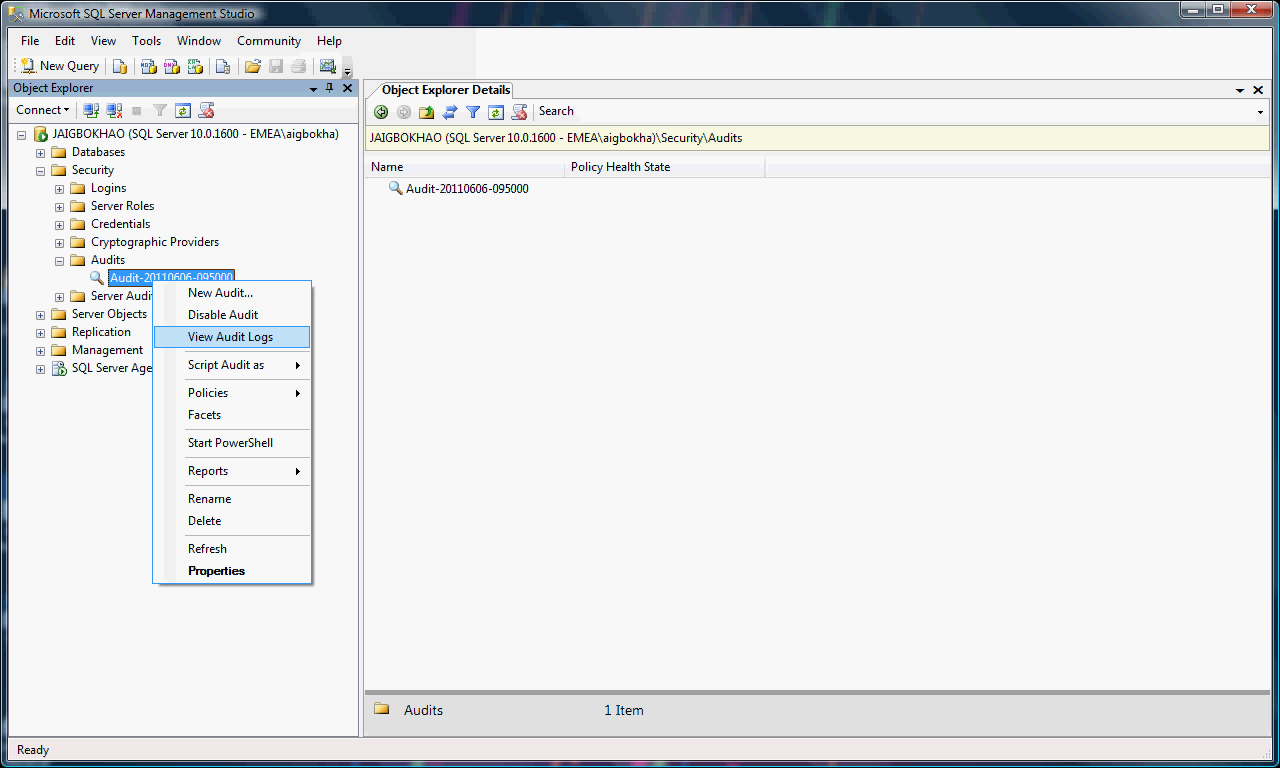
1. Create table dbo.customer



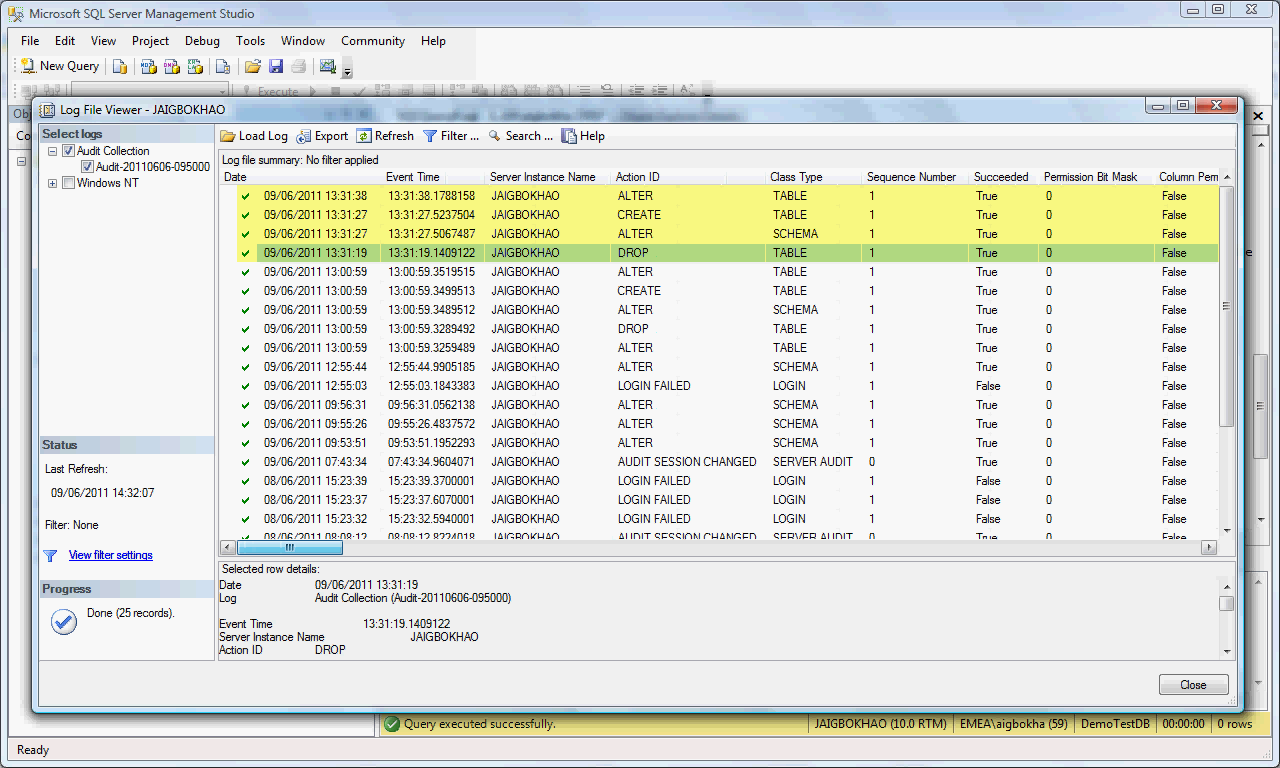
1. Alter table dbo.customer

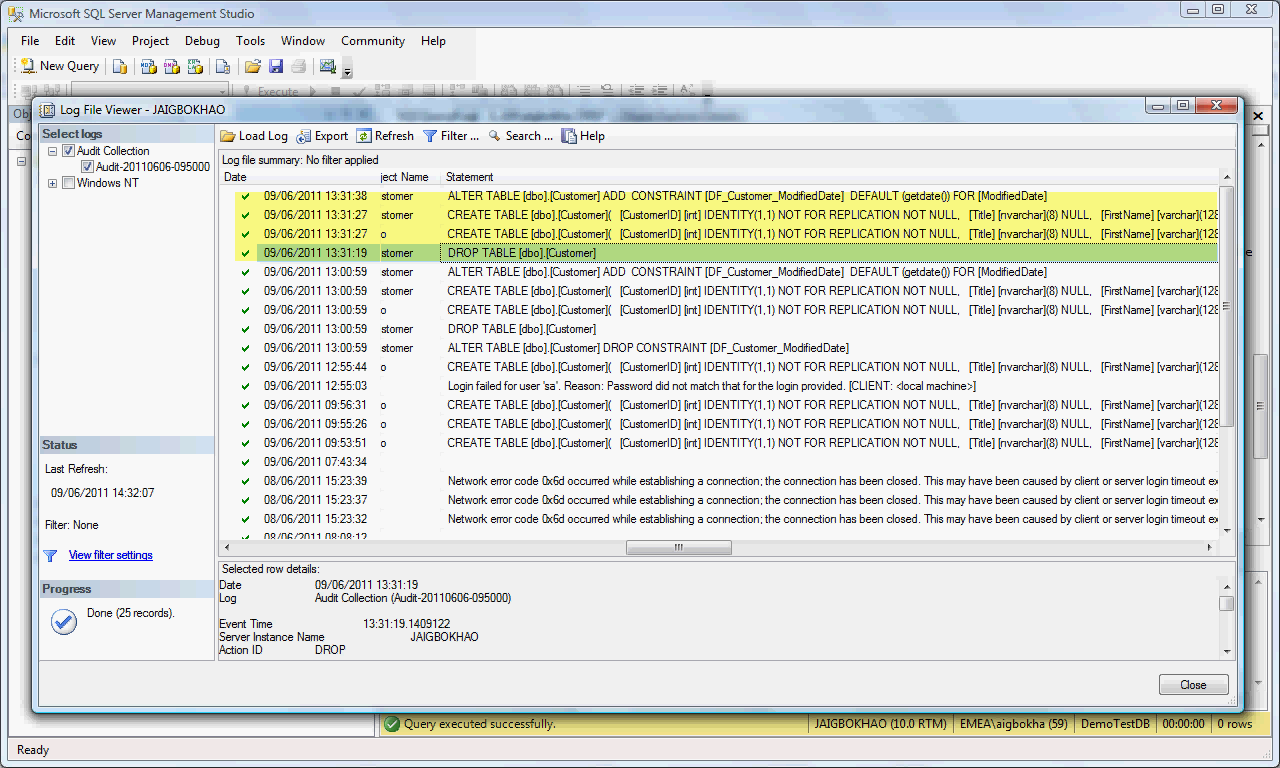


1. Right click on the Audit node and select the option "View Audit Logs" to view the Audit log of the Audit (*Audit-20110606-095000*).



1. This will bring up the dialog box that will show the details of the failed login event. Scroll to the right to find the details in the dialog box.





This show the audit events are been logged successfully.

## Deploy sql audit using tsql script to any sql server instance

### Script Considerations

1. Ensure the audit log folder exist in the SQL server instance. If not, create one.
2. Ensure the SQL server service account has the rights to read and write to audit log folder.
3. Ensure the audit logged file size and rollover file number are approved by design.
4. Every time the script is run, it replaces the existing SQL audit in the instance if any exist prior to run.

### Implementing SQL Audit Script

1. Copy the script to destination instance.
2. Modify the script.

Set the parameters in the script based on design.

*-- Set parameters*

*SET @AuditTargetFilePath= '' (Full UNC folder path.*

*Please make sure this folder exist in the instance)*

*SET @NumOfRollOverFiles= '' (number of rollover files)*

*SET @AuditFileMaxSize= (minimun file size is 2MG)*

1. Save the script as *<instance>\_sql\_audit\_<data>.sql* for future reference.
2. Copy and paste it into Query Analyzer of the instance.
3. Run the script to create SQL audit for that instance.
4. Copy the saved file to *<instance>* folder in the script Repository in the shared service.

For script, *see APPENDIX A: SQLAuditCreationSript.sql*

## Delete SQL AUDIT

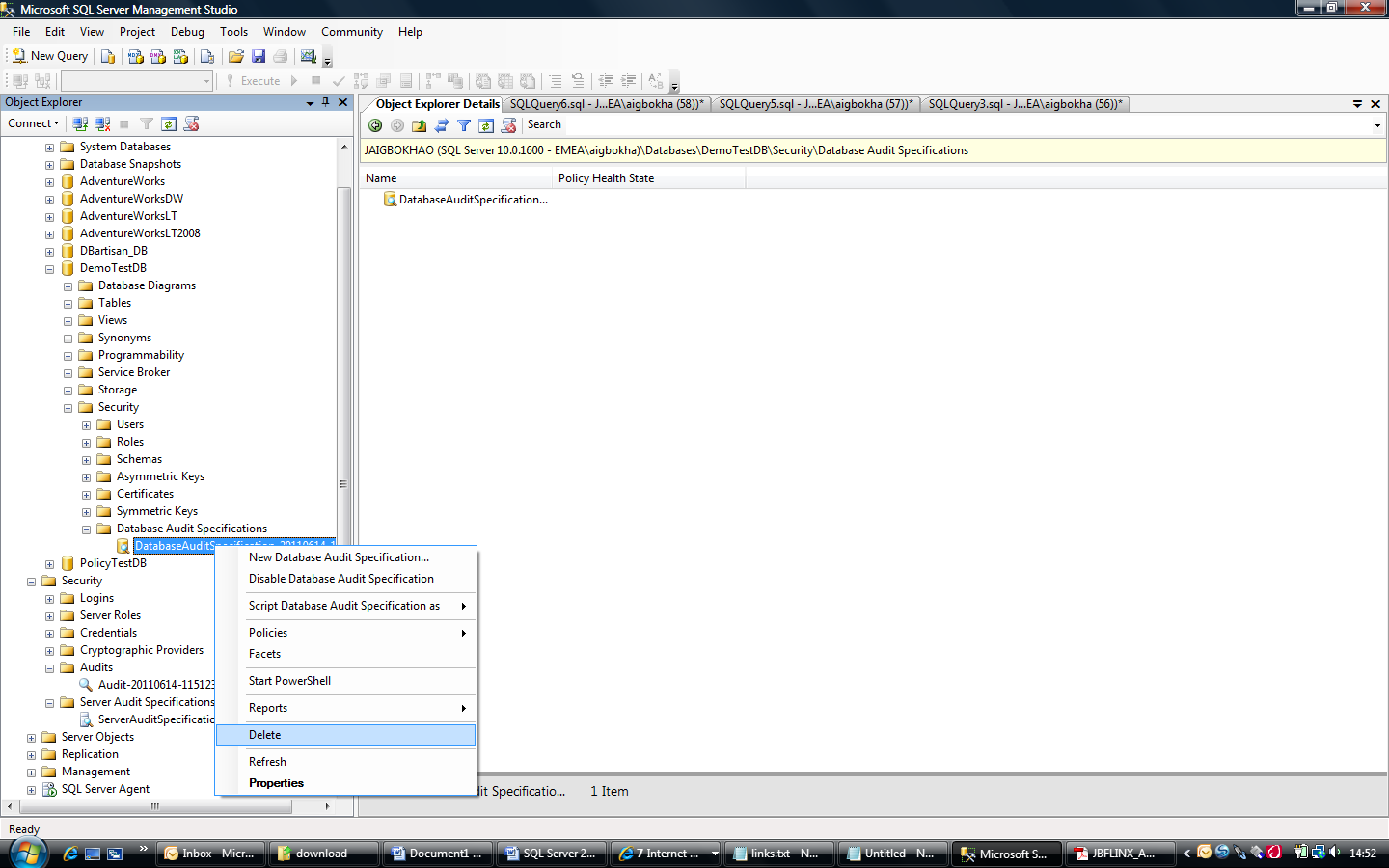
Deleting SQL Audit must be done in this order:

1. Delete or drop *Database Audit Specification* if exist.

Using TSQL:

* + [*http://msdn.microsoft.com/en-us/library/cc280479.aspx*](http://msdn.microsoft.com/en-us/library/cc280479.aspx)

Using SSMS;

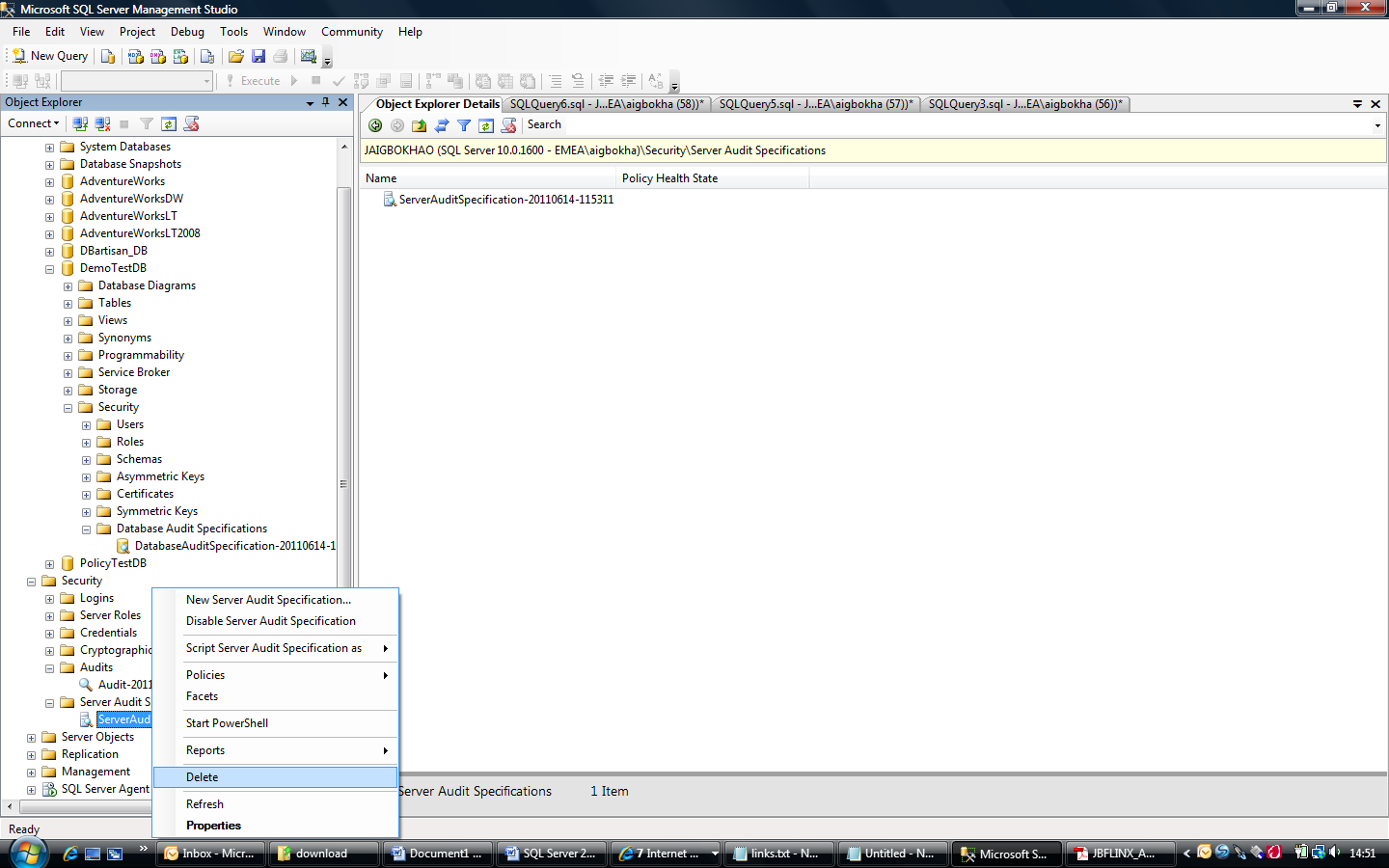


1. Delete or drop *Server Audit Specification* if exist

Using TSQL:

* + [*http://msdn.microsoft.com/en-us/library/cc280603.aspx*](http://msdn.microsoft.com/en-us/library/cc280603.aspx)

Using SSMS;

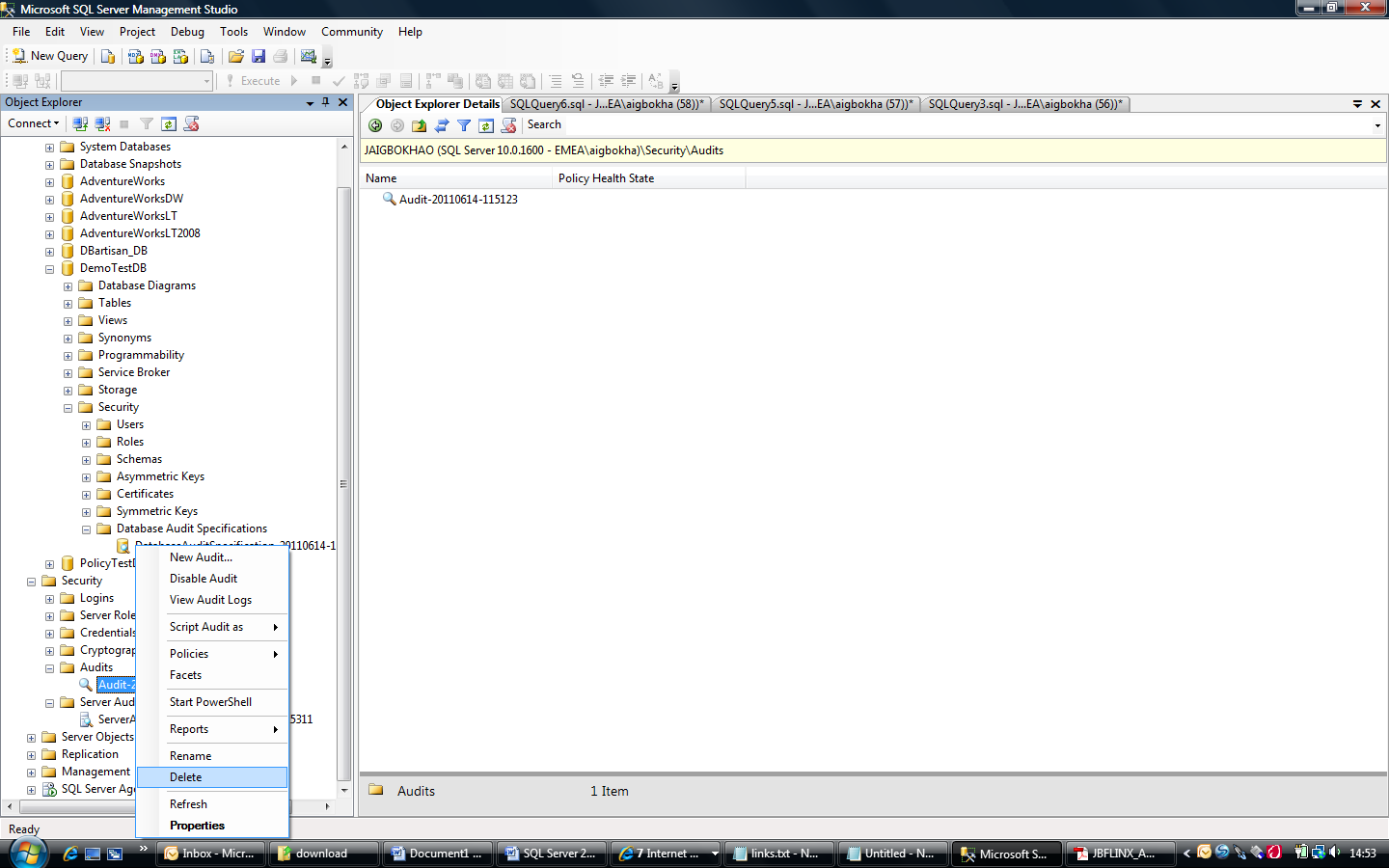


1. Lastly, Delete or drop *Server Audit.*

Using TSQL;

* + [*http://msdn.microsoft.com/en-us/library/cc280899.aspx*](http://msdn.microsoft.com/en-us/library/cc280899.aspx)

Using SSMS;

**

**Note**: Always delete the server audit last due to dependencies with both Server and Database Audit Specification.

# SQL Audit operation

The operation of SQL audit can be monitored by constant reviewing of audit logs and audit trace files. There are several methods to ensure the SQL audit is running smoothly and logging the server activities as required and expected, they as follows:

1. Reviewing SQL Audit Log Using SSMS

Refer to sections in this document;

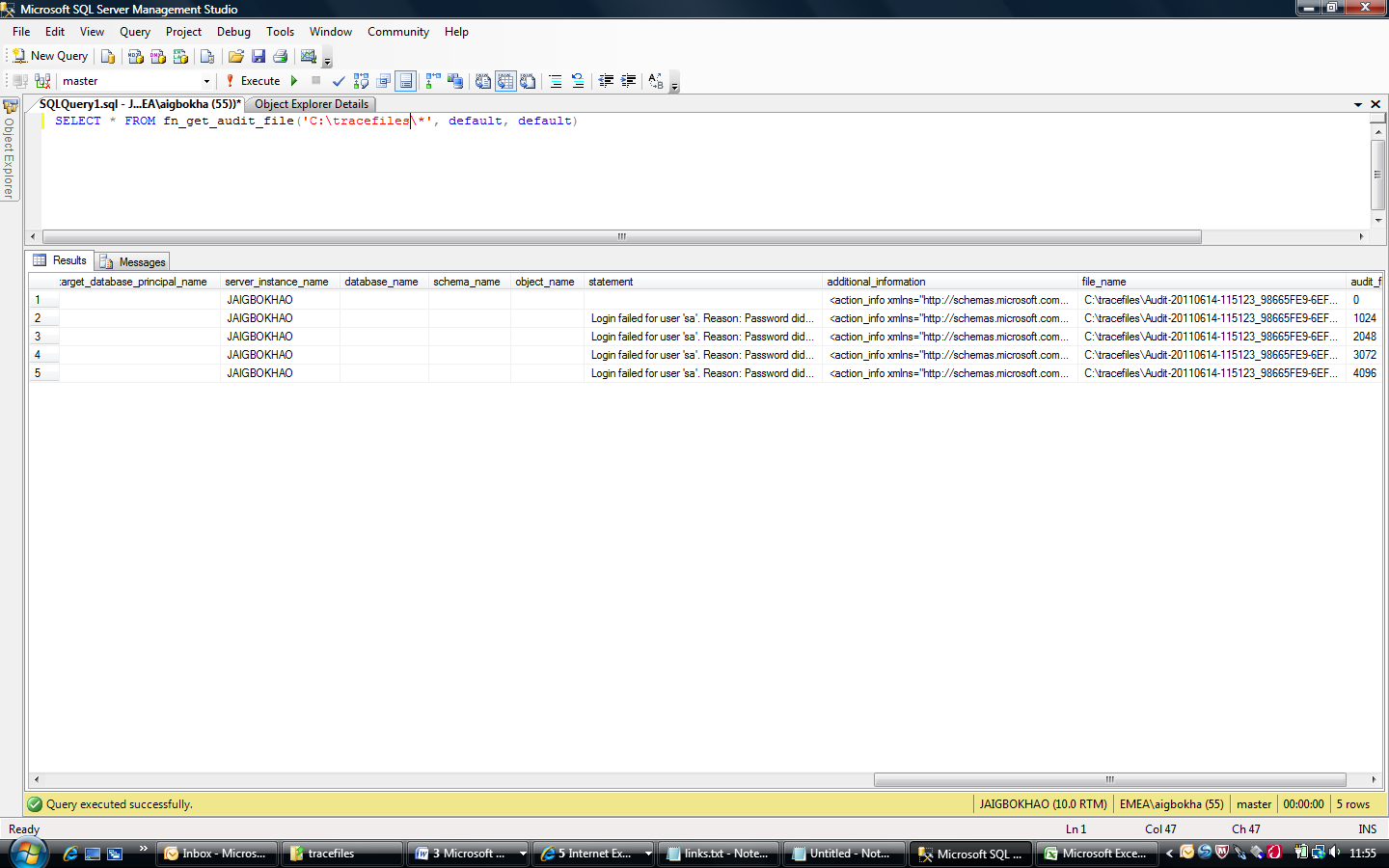
* + - * Configure Server Audit, Step 6
      * Test Server Audit Configure, step 2 and 3
      * Test Database Audit Configure, step 4 and 5
      * [*http://msdn.microsoft.com/en-us/library/cc280728.aspx*](http://msdn.microsoft.com/en-us/library/cc280728.aspx)

1. Querying SQL audit trace files

Query:

*Select \* from fn\_get\_audit\_file ('<audit folder path>', default, default)*

*<audit folder path>: e.g. 'C:\tracefiles\\*'*

**

*For more details refer to:*

* [*http://msdn.microsoft.com/en-us/library/dd392015(SQL.100).aspx*](http://msdn.microsoft.com/en-us/library/dd392015(SQL.100).aspx)
* [*http://msdn.microsoft.com/en-us/library/cc280765.aspx*](http://msdn.microsoft.com/en-us/library/cc280765.aspx)

1. SQL audit dynamic view

* To get location of the target, size and status of the audit itself.

DMV Query:

*Select name, status\_desc,*

*audit\_file\_path, audit\_file\_size*

*from sys.dm\_server\_audit\_status*

* More detailed information about the auditing with FILE as target.

DMV Query:

*Select name, on\_failure ,max\_file\_size*

*,max\_rollover\_files ,log\_file\_path*

*,log\_file\_name*

*from sys.server\_file\_audits*

* To retrieve details of a database audit specification of an individual database audit.

DMV Query:

Select \* from sys.database\_audit\_specification\_details where database\_specification\_id

in

(select

database\_specification\_id

from sys.database\_audit\_specifications where name ='<Database\_Audit\_Spec>')

* To check the extended events that are created by SQL server related to this audit.

DMV Query:

Select s.name as [session name],

se.event\_name as [event name],

p.name as [package name],

t.target\_name as [target name]

from sys.dm\_xe\_sessions s

join sys.dm\_xe\_session\_events se on

s.address = se.event\_session\_address

join sys.dm\_xe\_packages p on

se.event\_package\_guid = p.guid

join sys.dm\_xe\_session\_targets t on

s.address=t.event\_session\_address

For more detail refer to:

* [*http://www.databasejournal.com/features/mssql/article.php/3867641/SQL-Server-2008--Accessing-Audit-Details.htm*](http://www.databasejournal.com/features/mssql/article.php/3867641/SQL-Server-2008--Accessing-Audit-Details.htm)

# Troubleshoot SQL AUDIT

1. Review SQL log
2. Review Application Event log
3. Review Audit log to ensure SQL audit is logging activities. *See section 5.4.1.1. Step 6*.
4. Query SQL audit trace files to determine when the last audit event was logged. *See section 6*.
5. Use SQL audit dynamic views. *See section 6*.

# Appendix a



