|  |
| --- |
|  |
| IS 637 Group Project |
|  |
| Aditya Venkatesh Annavarapu  OlubukunmiAbiodun Ajayi  Sai Bhargav Kompalli  Department of Computer Information Systems  Eastern Michigan University  Information Systems Audit  Dr. Huei Lee  April 10, 2020 |

**Abstract**

Auditing an instance of the SQL Server Database Engine or an individual database involves tracking and logging events that occur on the Database Engine. SQL Server audit lets you create server audits, which can contain server audit specifications for server level events, and database audit specifications for database level events. Audited events can be written to the event logs or to audit files.

SQL Server auditing is a new feature which makes use of extended events to allow you to audit everything that happens in your server, from server setting changes all the way down to who modified a value in a specific table in the database. This information is then written to windows security log, the windows application log or to a flat file.

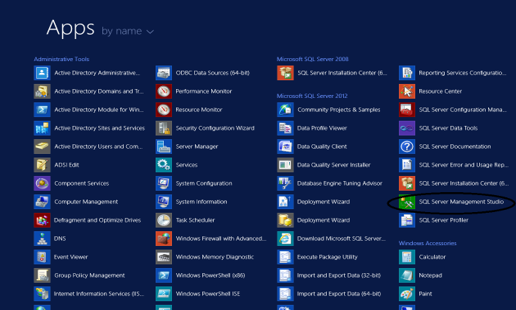
In SQL Server 2008, Auditing was an enterprise only feature. In SQL server 2012, server auditing has now been made available to all editions, however database auditing remains for use by enterprise customers only.

We will be creating and setting up the server audit and review using SQL Server Management Studio 2012 as part of this project.

**Setting up and creating Audit**

To perform the Audit, first you have to launch Server Management Studio

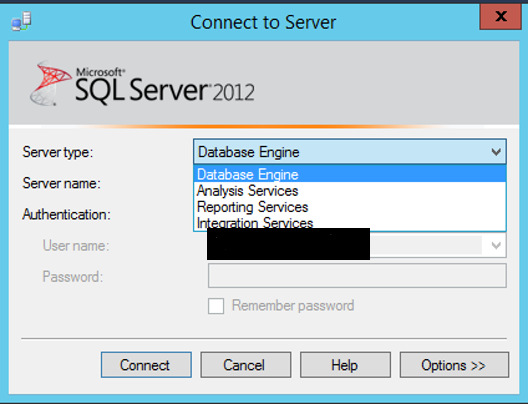
1. Go to Microsoft SQL Server Management Studio from all Apps on Windows 10



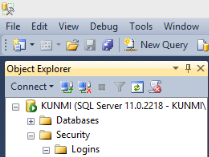
1. SQL Server Management Studio 2012 launch tab will be displayed



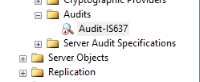
1. Select the Server type as Database Engine from the list of Server types: Database Engine, Analysis services, Reporting services, Integration services
2. Choose the Server name which is the system name in our case
3. Select the Authentication, either Windows/SQL server Authentication
4. Click on Connect



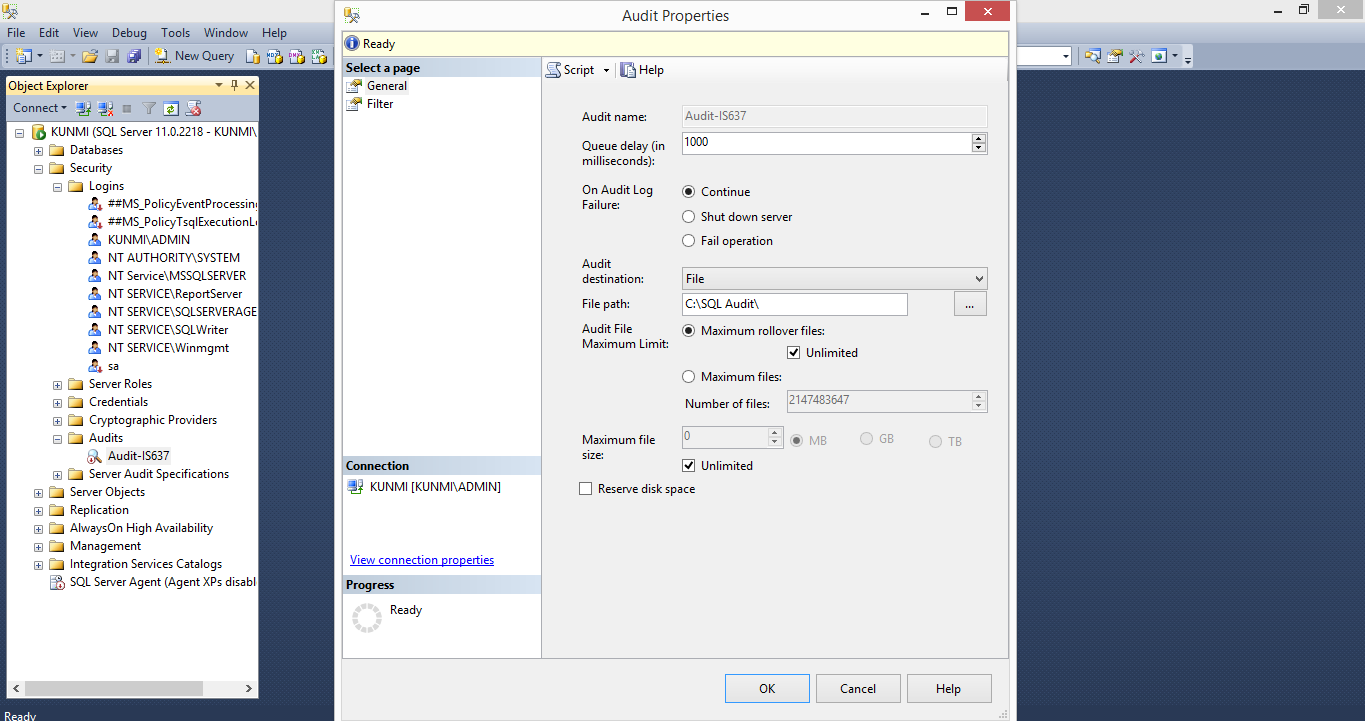
Now you are logged into SQL Server Management Studio



Here, we are connected to the server KUNMI which can be seen in the object explorer. Now, we are going to create a server audit with the name Audit-IS637



Navigate to Security -> Audits -> New Audit.



After specifying the audit name, the next step is to set the Queue delay. It is recommended to set it at least more than one second. If this is set to zero, audit will be delivered synchronously which is not recommended as it will increase the transaction duration. Auditing is highly unlikely to be needed for synchronous delivery. Hence, we set the Queue delay to 1000.

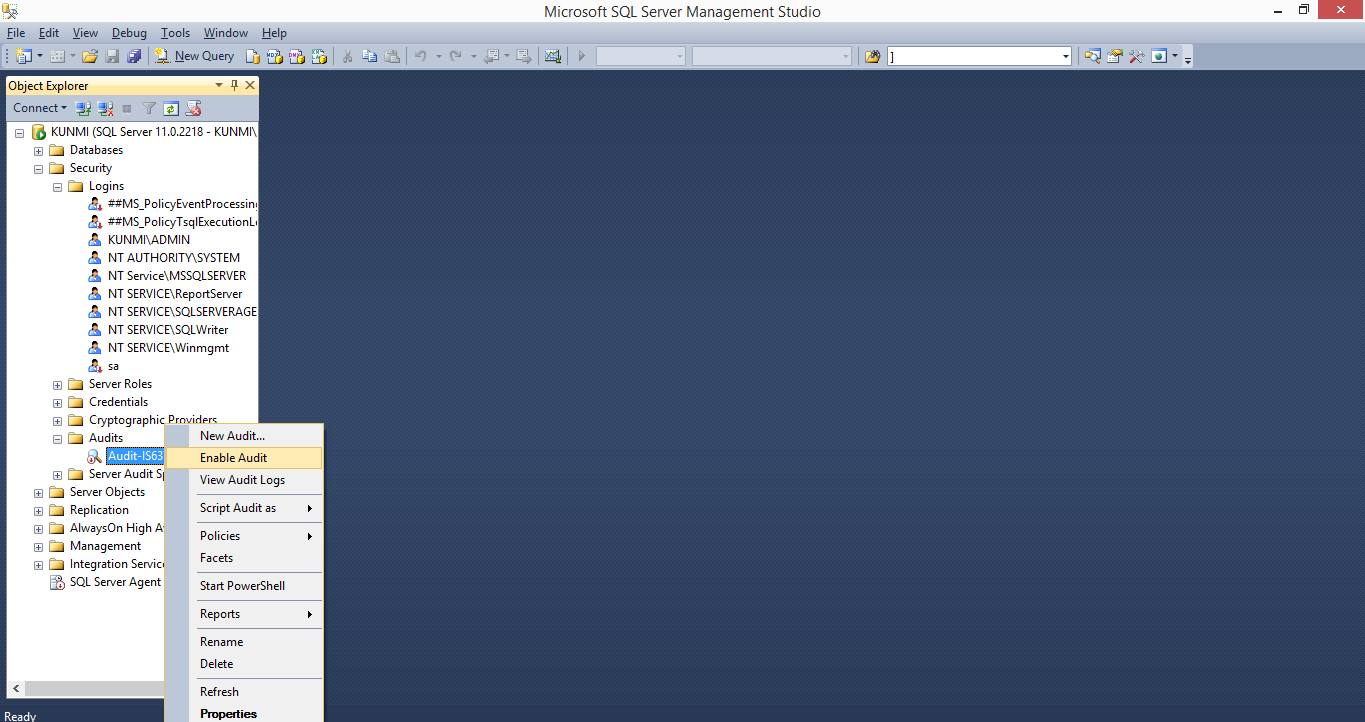
Next is a new feature introduced in SQL Server 2012. It will decide what would happen when there is a failure in the audit log. In some compliance standards, the system should shut down when a failure occurs in the Audit which means auditing is a high priority. We are selecting Continue to keep the work going.

The Audit destination defines the audit target type. The default option is File where audit records are written to a File. The other options include Application and Security logs. These options are available so that standard tools can be utilized when they are available at the event viewer. We chose File path as C:\SQL Audit\ with maximum rollover files as unlimited and click on OK to create the audit.

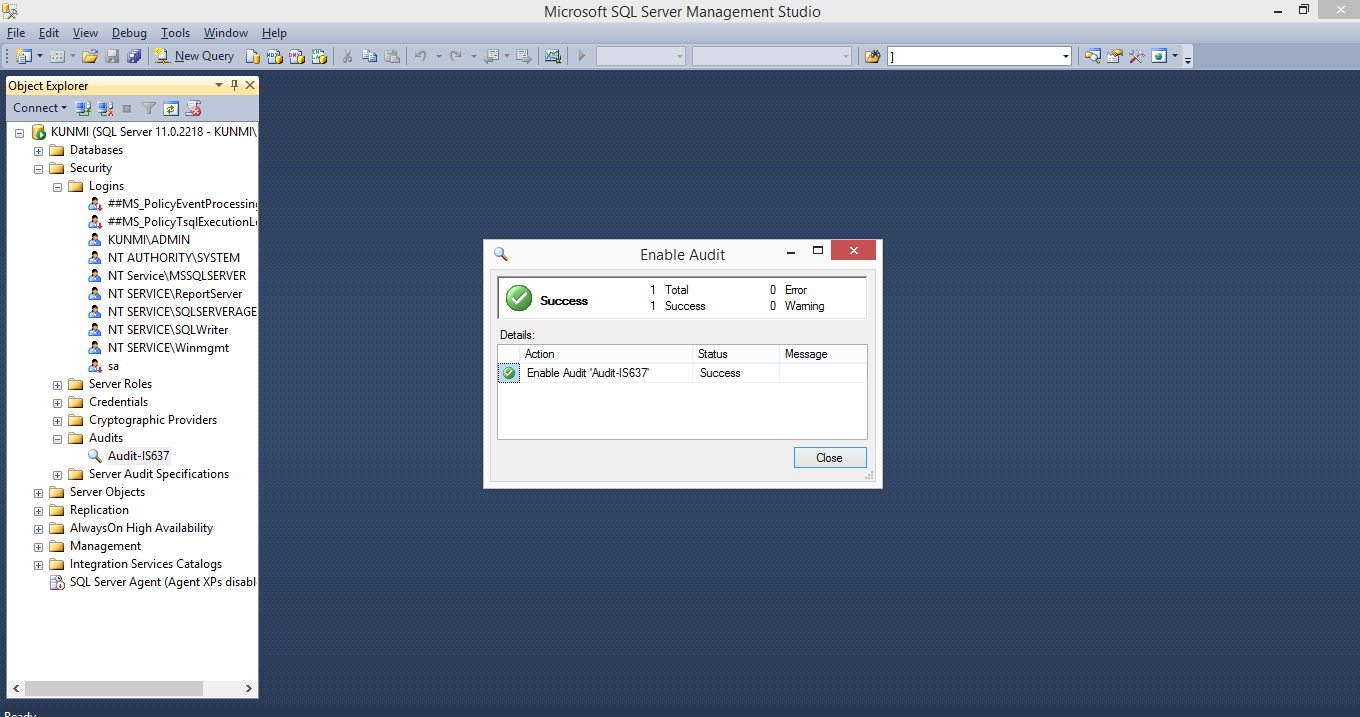
By default, auditing is disabled. This means that just because you create the audit specification it will not be active. It will be active only when you enable it after creating it. After creating an Audit, it automatically disables it.

**Enabling the Audit created:**

Select the audit you just created, right-click and select Enable Audit

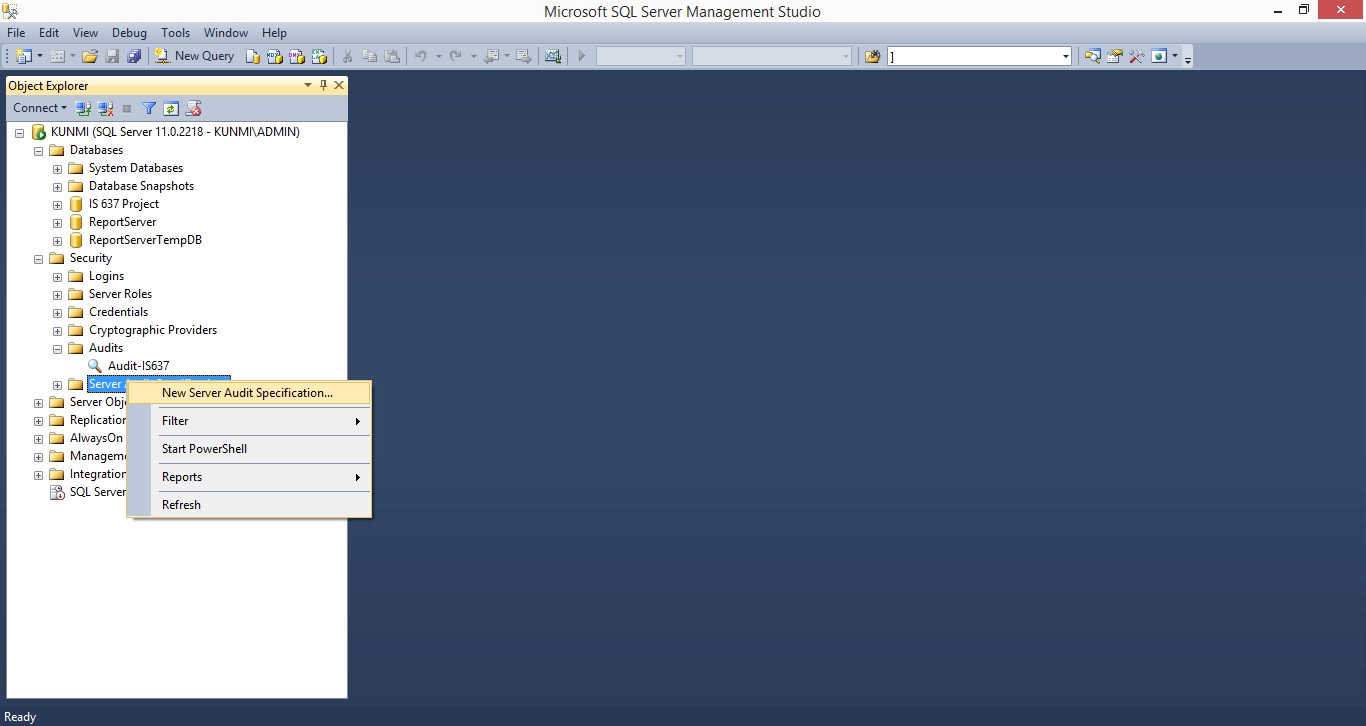


Enable Audit success for Audit-IS637 as it shown below:



**Creating New Server Audit Specification for the Audit**: Go to Server Audit Specification, right click then you can New Server Audit Specification.

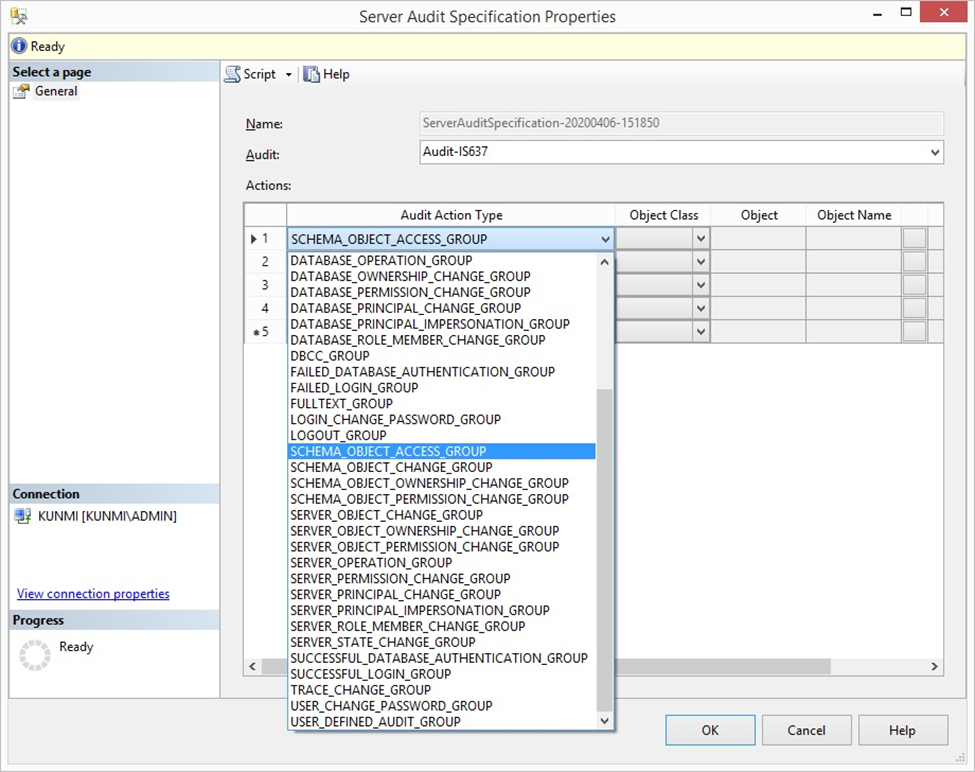
The Server Audit Specification which is available in all editions of SQL Server, is used to define what needs to be audited at a server level. For the Server Specification, all events are grouped into Audit Action Groups. Below you can see creating the server Audit specification



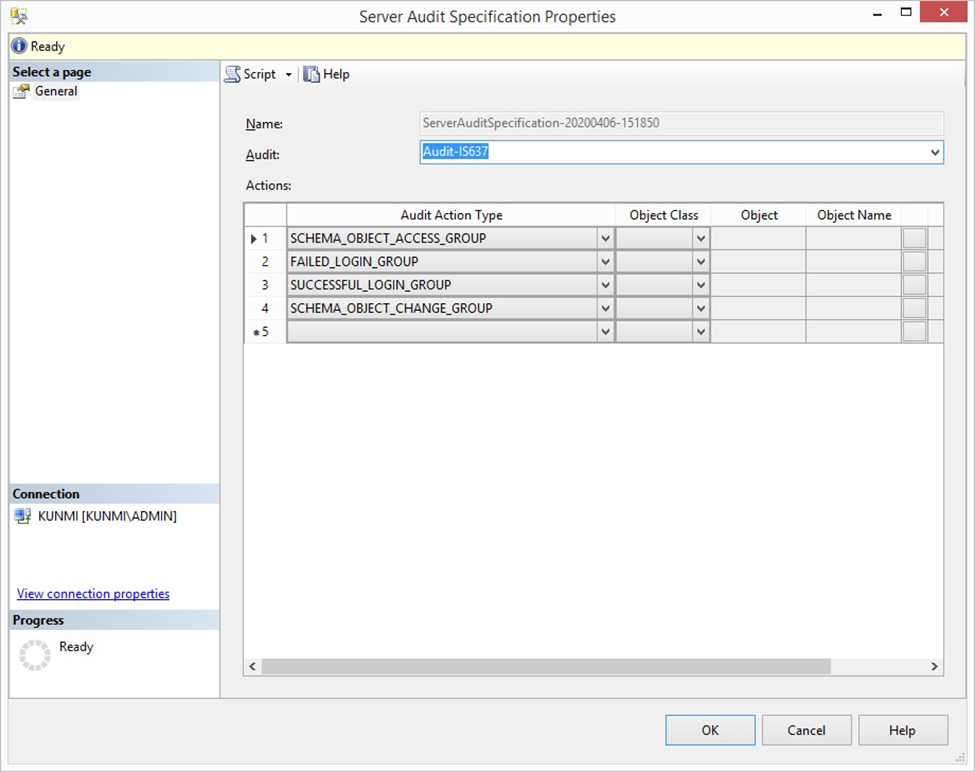
**Server Audit Specification Properties Audit Action Groups:**

SQL Server groups auditable actions into convenient categories called Audit Action Groups. You can enable action groups for auditing on a [specific database](https://www.ultimatewindowssecurity.com/sqlserver/auditpolicy/databaseauditspecification.aspx) or across the [entire server](https://www.ultimatewindowssecurity.com/sqlserver/auditpolicy/serverauditspecification.aspx). Action groups cover all auditable actions except a few Transact-SQL commands called [audit actions](https://www.ultimatewindowssecurity.com/sqlserver/auditpolicy/auditactiongroups/Database-level_audit_actions.aspx). Some action groups comprise only server level operations (e.g. create database, drop server role) and so are only available in [server audit specifications](https://www.ultimatewindowssecurity.com/sqlserver/auditpolicy/serverauditspecification.aspx). Other action groups are applicable at the database level but can be included in a server audit specification so that those actions are audited on all databases - even new ones created the future. This is indicated in the Database and Server columns below. With SQL Server 2012 and 2016, Microsoft introduced some new audit action groups also indicated in the table below. Also, some action groups that were formerly server-level only, became available at the database level and are indicated by the footnote.

The following are examples of Level Audit action groups: SUCCESSFUL\_LOGIN\_GROUP, FAILED\_LOGIN\_GROUP, DATABASE\_OPERATION\_GROUP

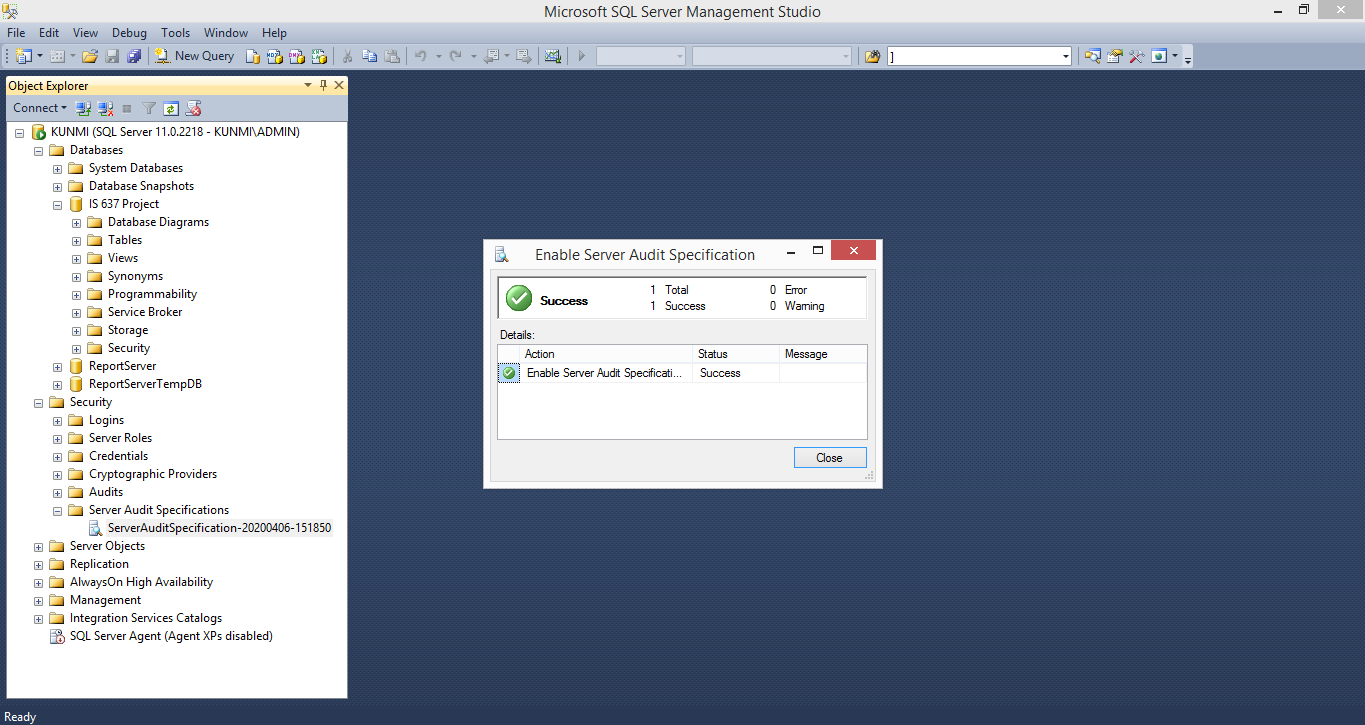


Here we have selected some audit action types that are required in the Audit-IS637 and there’s a unique id given for every ServerAuditSpecification-20200406-151850 as shown in the figure below



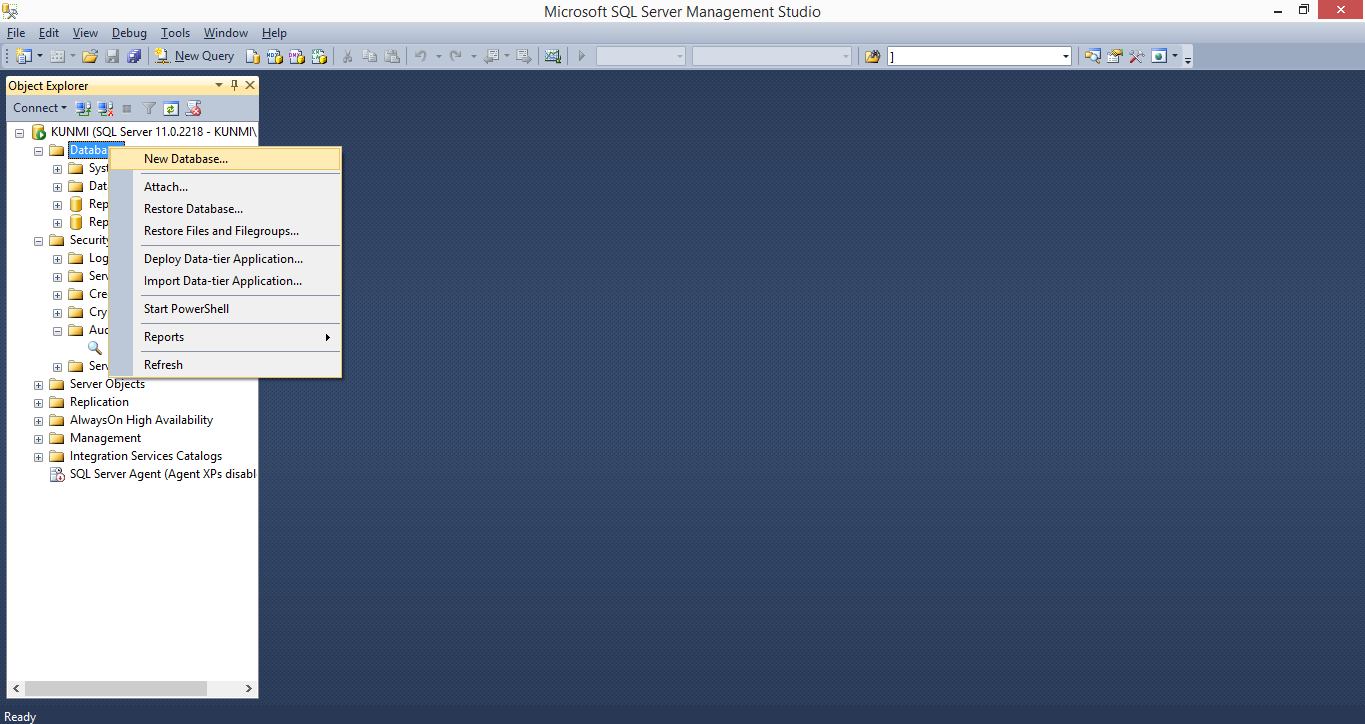
**Enabling Server Audit Specification:**

Enable Server Audit Specification by right clicking and selecting Enable Server Audit Specification under Security -> Server Audit Specifications -> Server Audit Specification you just created

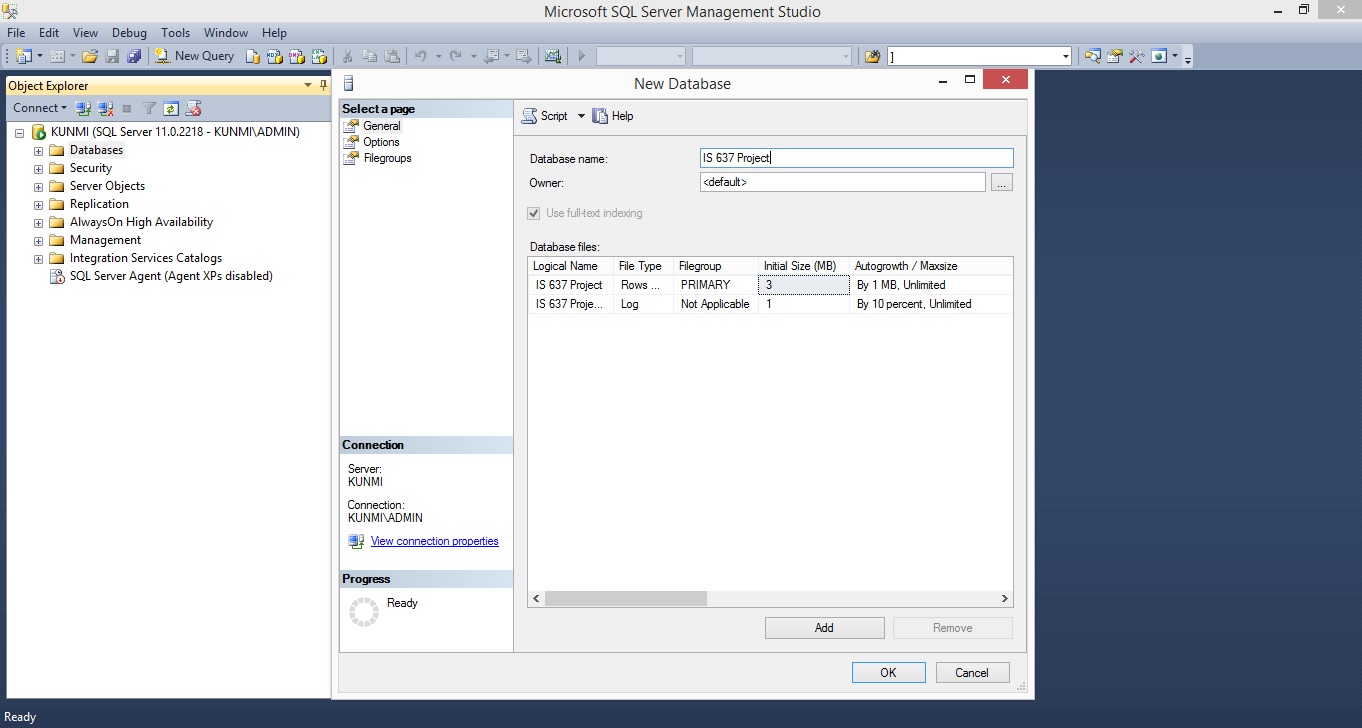


Now, in order to verify the Audit that we just created, we will further create a new database, tables and insert values to view the audit files created accordingly.

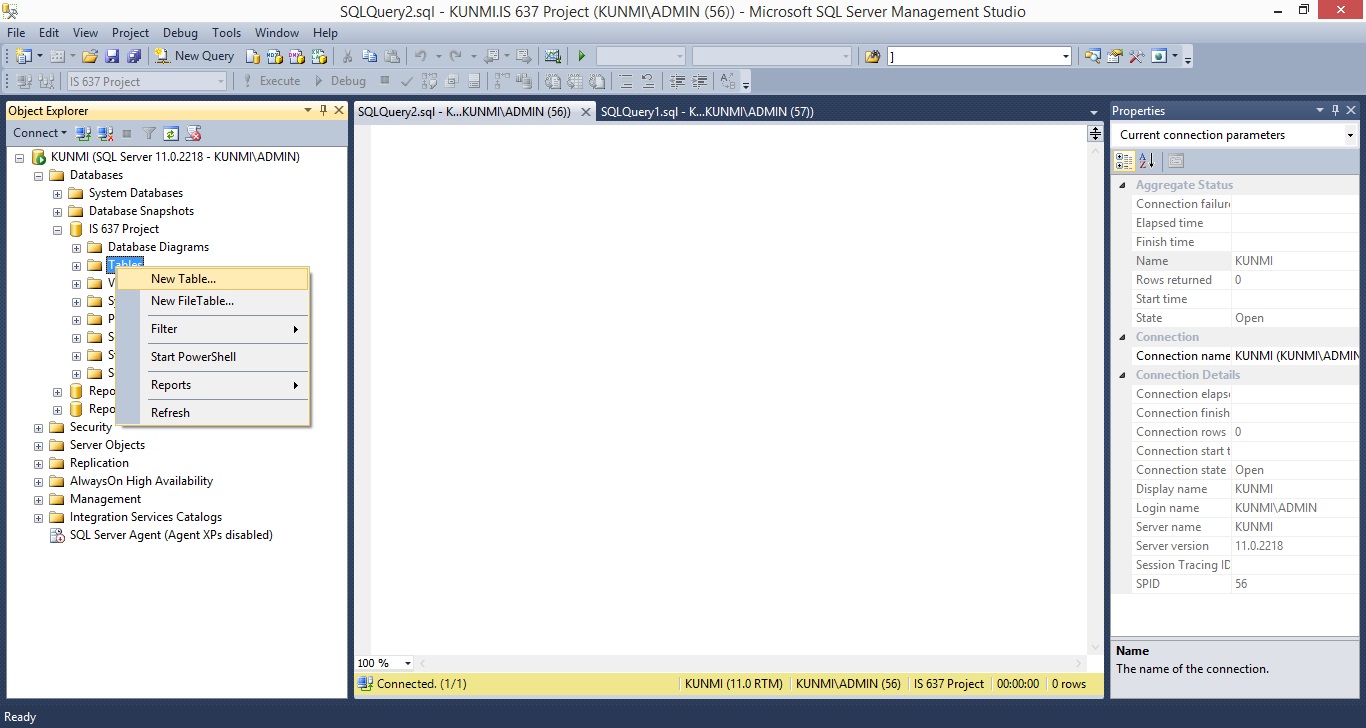
**Creating New Database:**



IS 637 Project Database is created as shown below. You can also use query in the script statement “CREATE DATABASE IS 637 Project, then click execute or press F5, database will be created.



**Creation of Tables:** Go to Tables under Database and right click to create a new table



**Creation of table for Employees**:

CREATE TABLE Employees (

EMPLOYEE\_ID int,

FIRST\_NAME varchar(255),

LAST\_NAME varchar(255),

EMAIL varchar(255),

MANAGER\_ID int,

JOB\_ID varchar(255)

);

Click execute or press F5, table will be created.

**Creating Job table:**

CREATE TABLE Jobs (

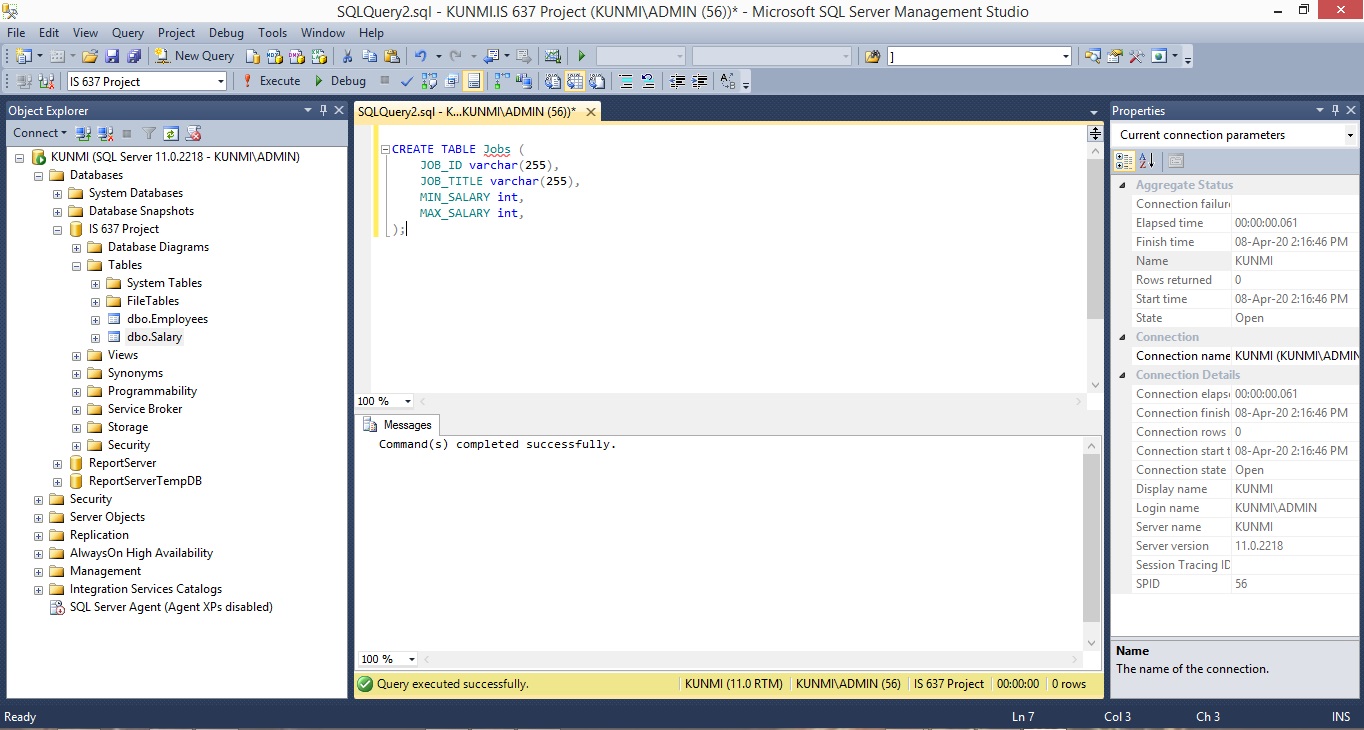
JOB\_ID varchar(255),

JOB\_TITLE varchar(255),

MIN\_SALARY int,

MAX\_SALARY int,

);

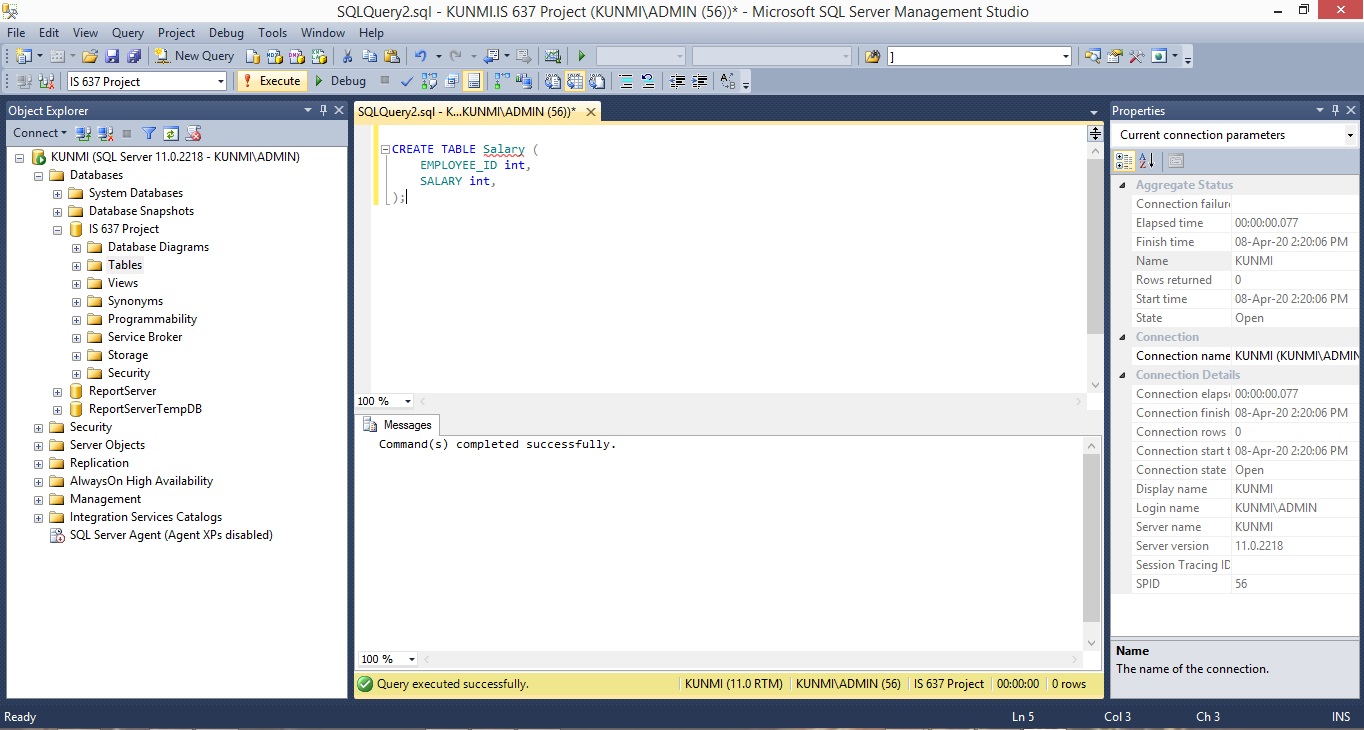


**Creating Salary table:**

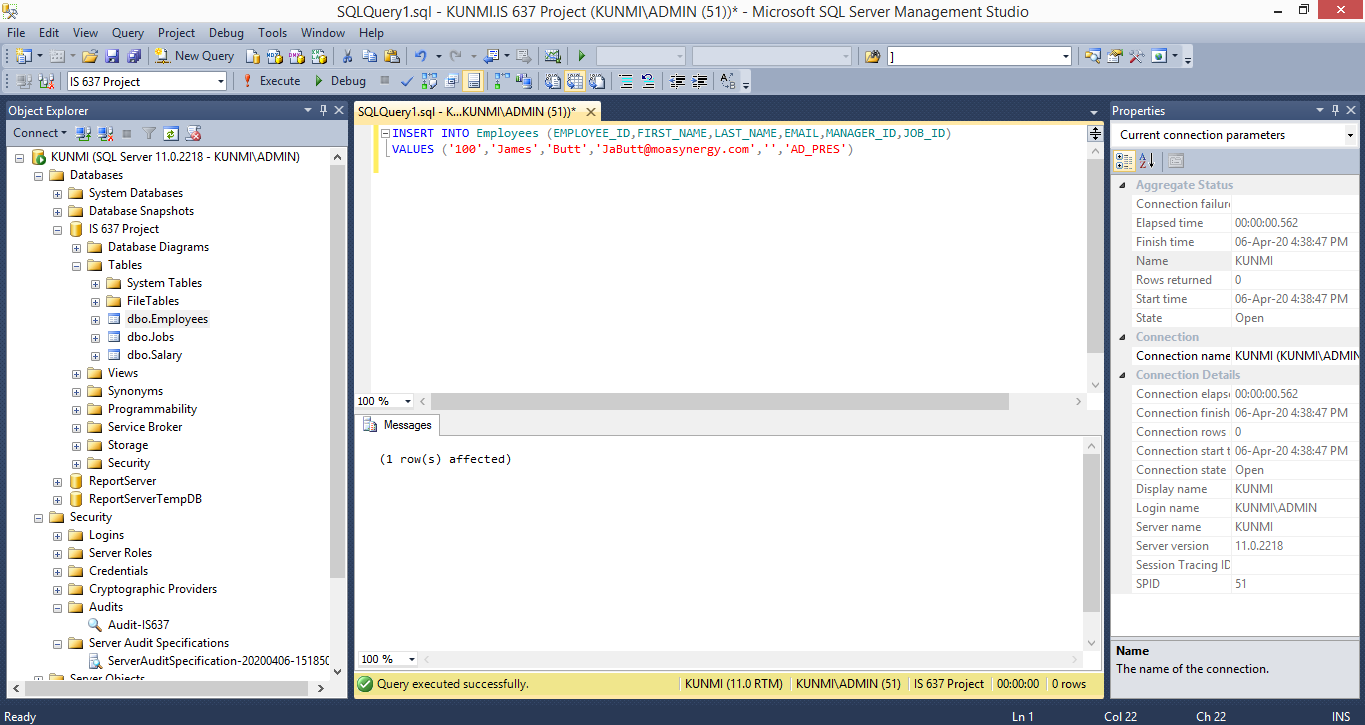
CREATE TABLE Salary (

EMPLOYEE\_ID int,

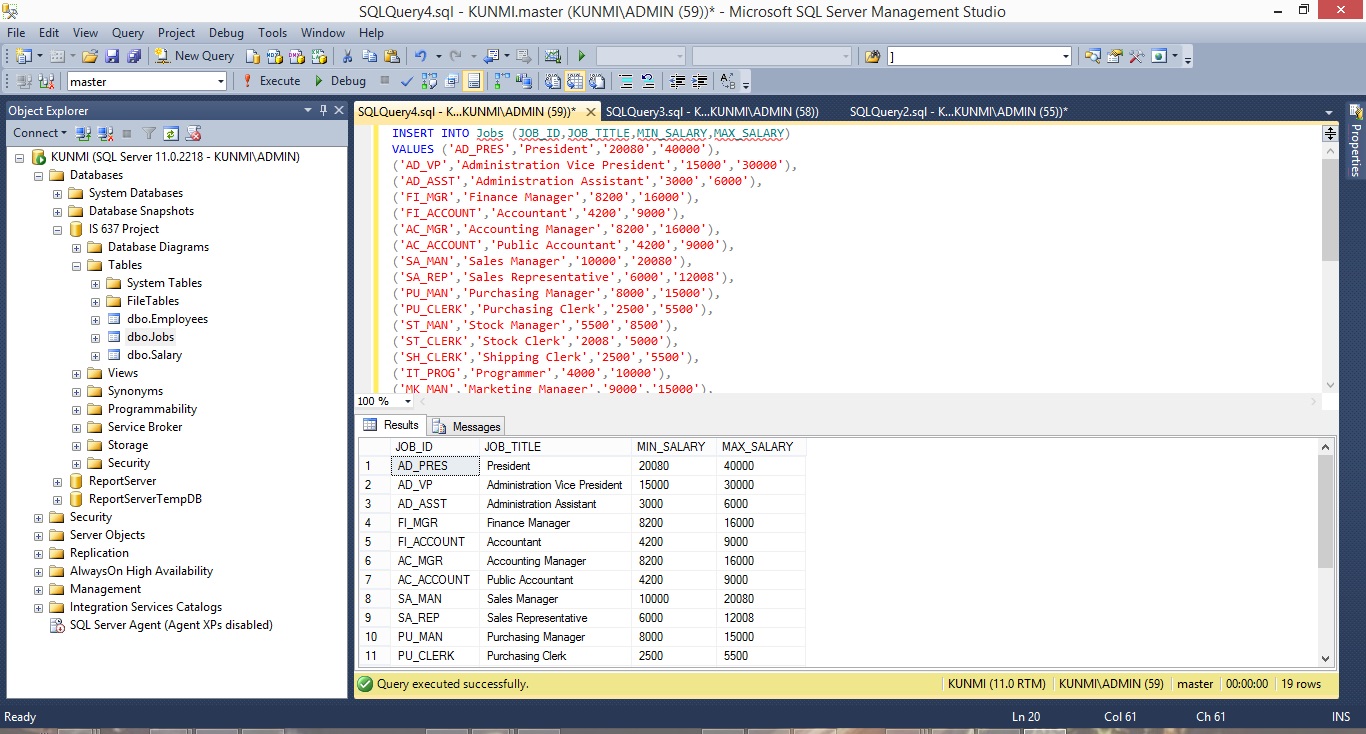
SALARY int, );



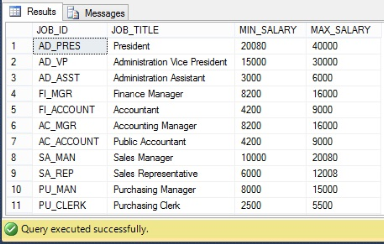
**Inserting values into Employees table:**



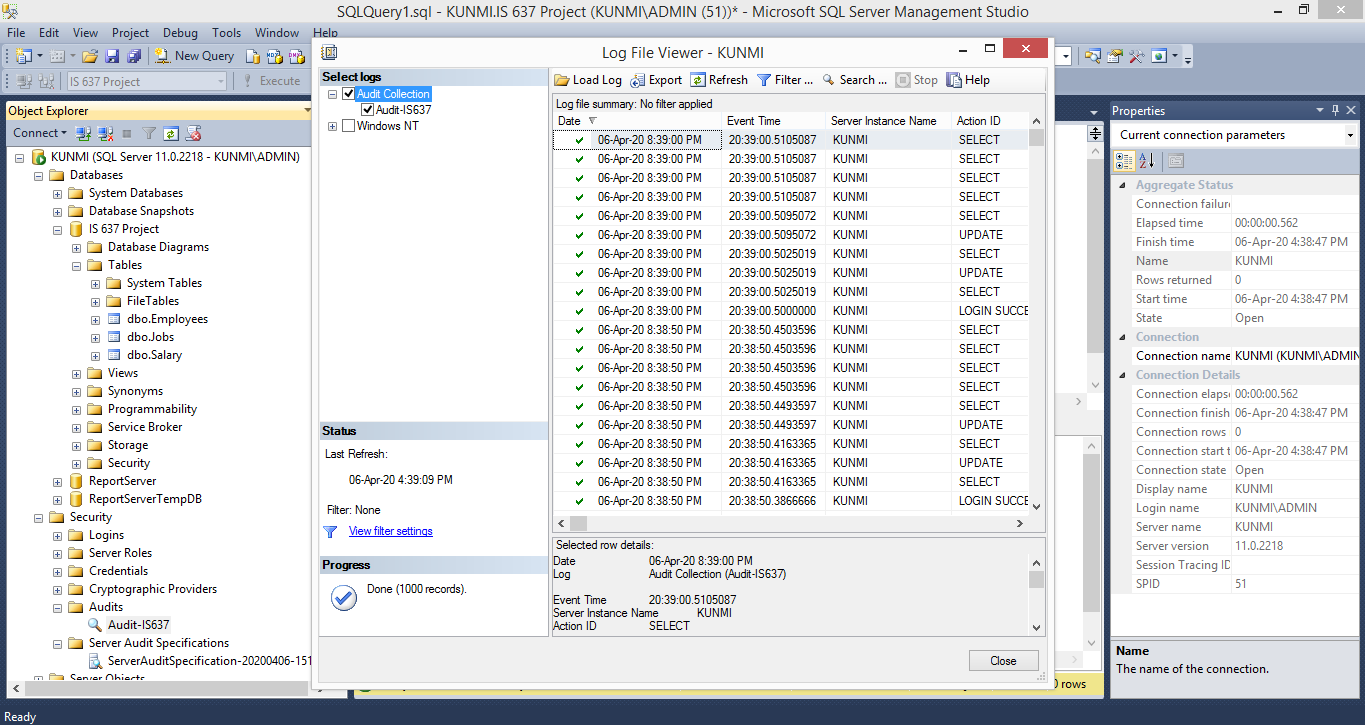
**Inserting values into the Jobs tables:**

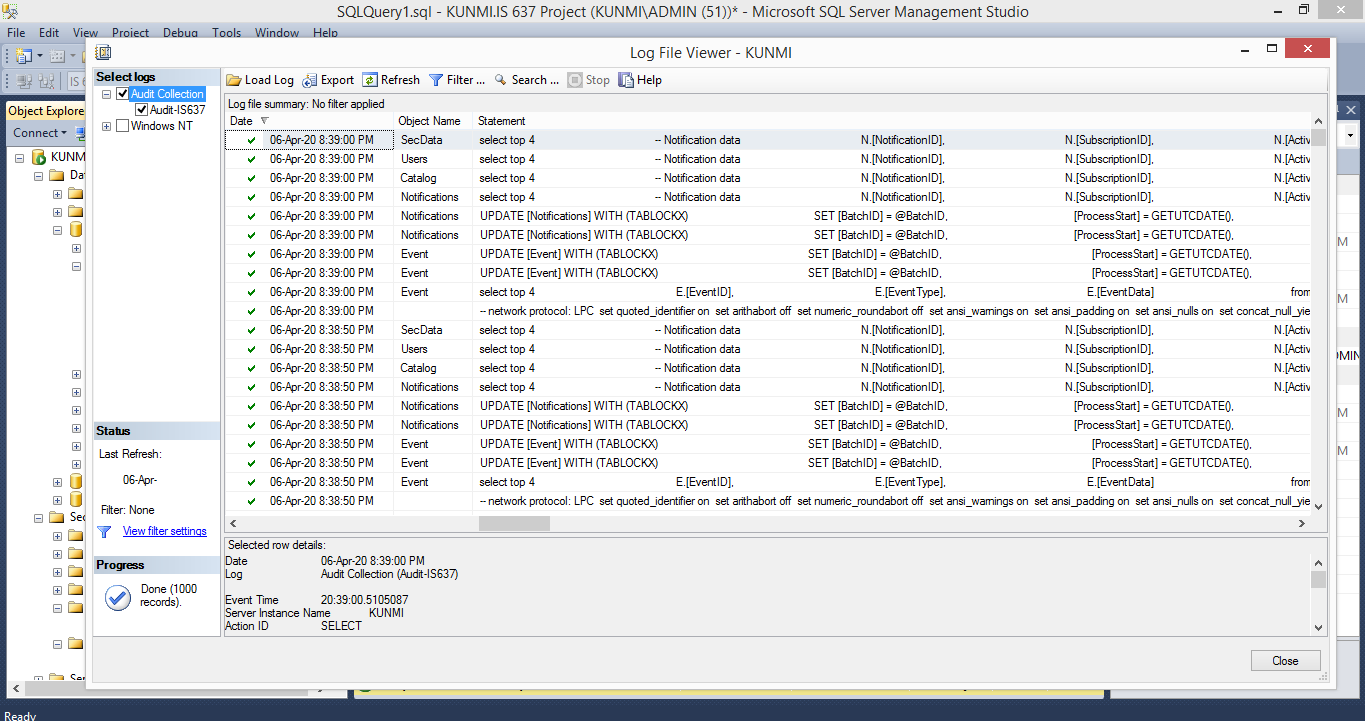


**Output:**



**Audit log:** We have successfully created the Server Audit, database and tables. Now, the audit log document must have recorded all [event](https://searchapparchitecture.techtarget.com/definition/event)s that we have just attempted. Also, when a change is applied to the system, it correlates with a change in the system’s behaviour and every such change will be documented in the audit log. We have run login, update and select statements to verify if the audit has been recorded for such events. In order to view the logs, Log File Viewer can be accessed from Security -> Audits -> View Audit Logs.



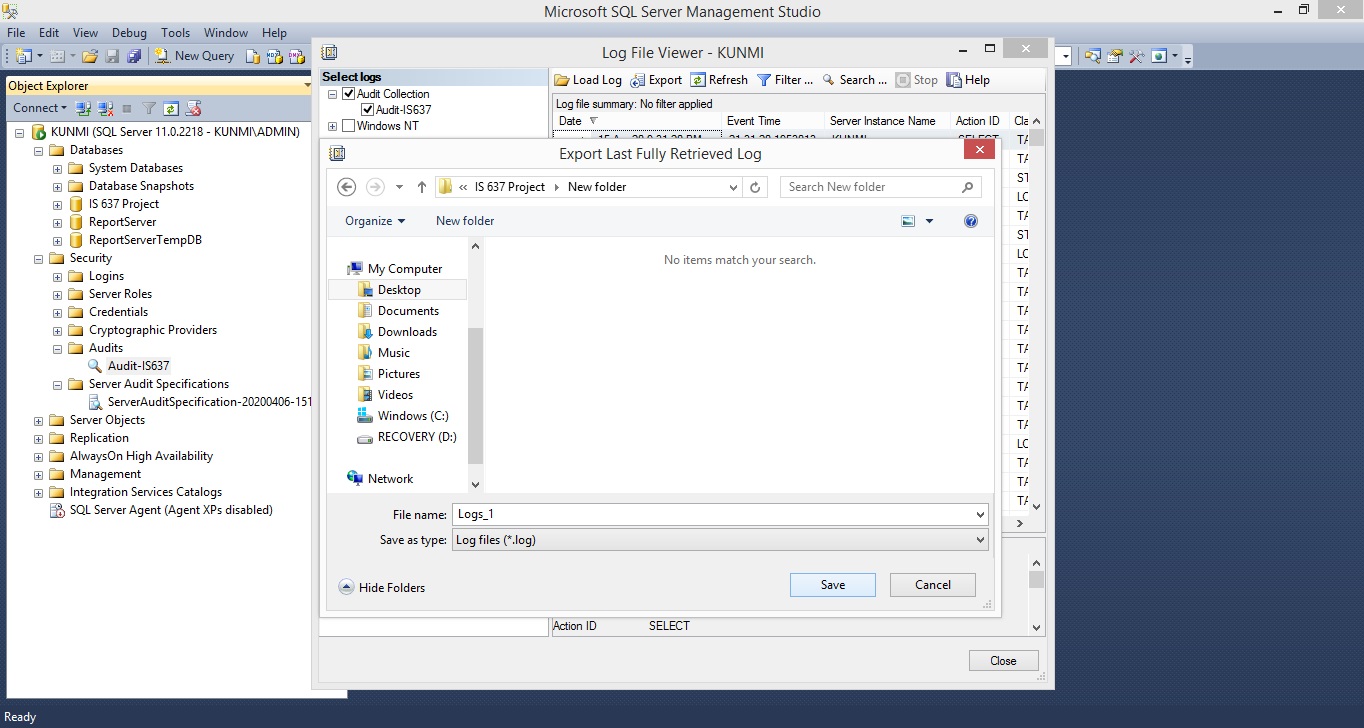


**Exporting of the Log file.**

The log file might not be easy to manipulate in the SQL management Studio, so it can be exported as a file if requested probably for report, analysis or investigation.

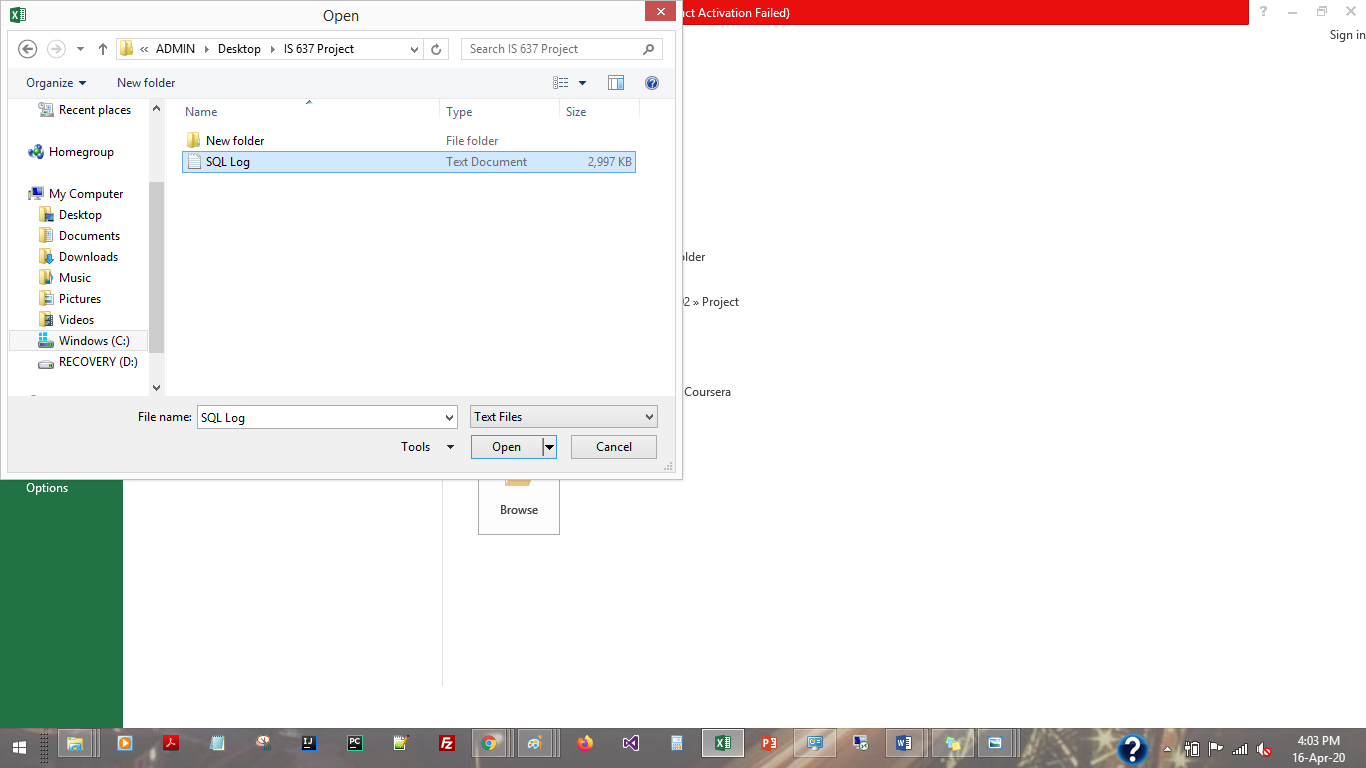
Click on Export and the image below shows.

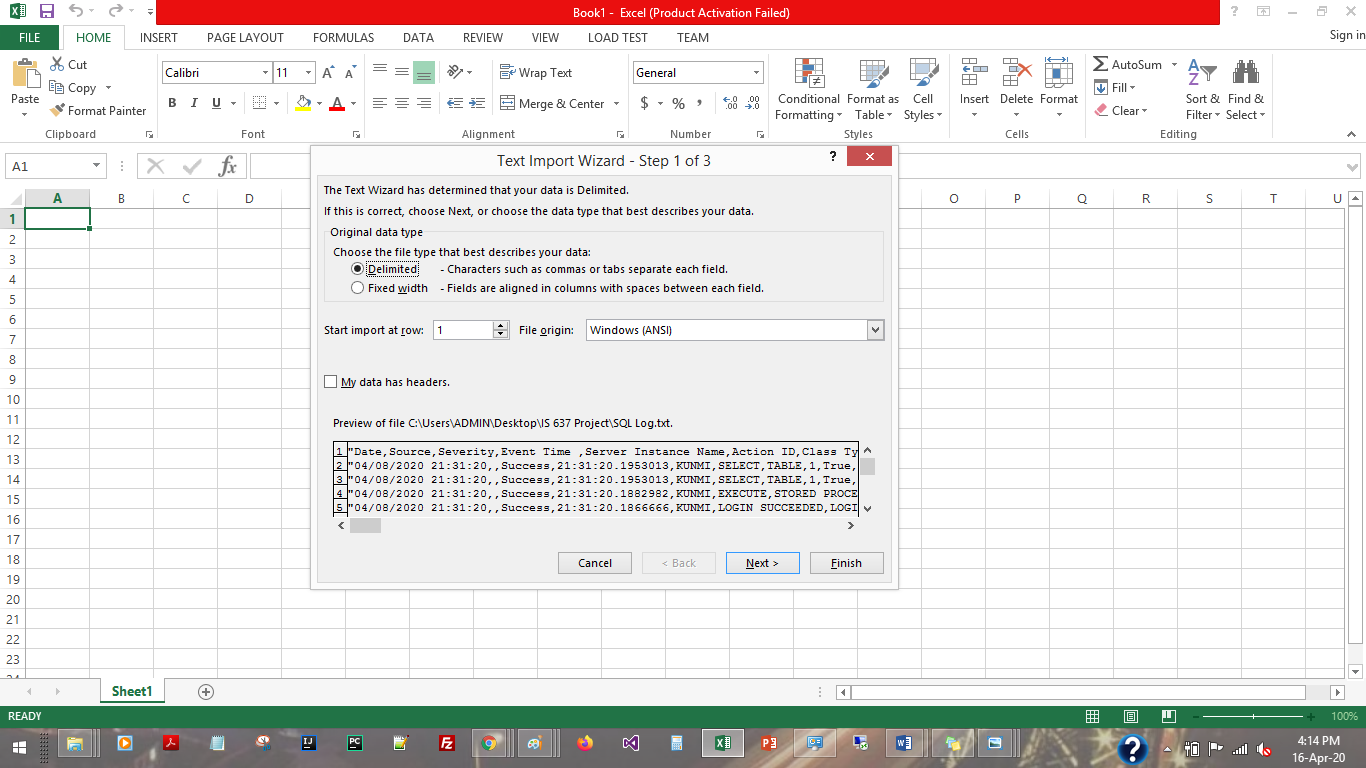
And the file is saved as a .txt file.

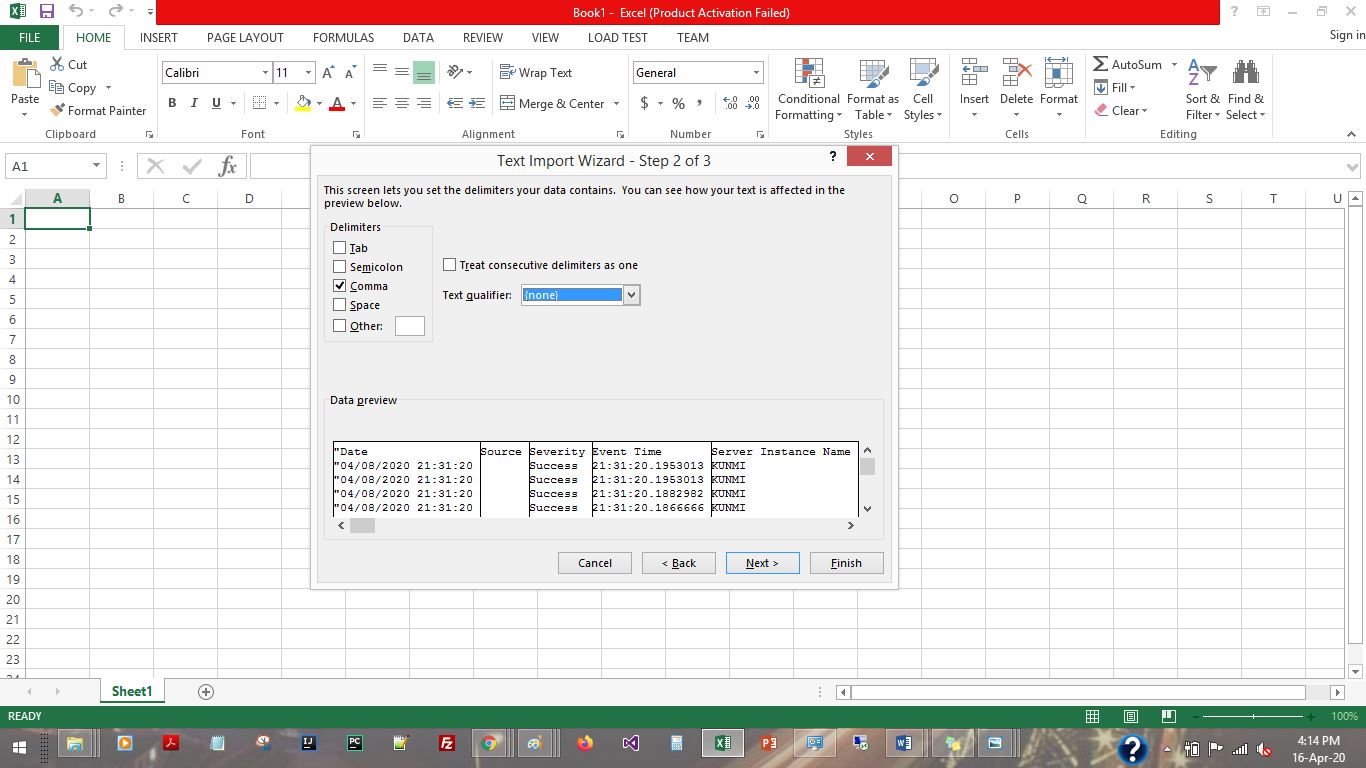


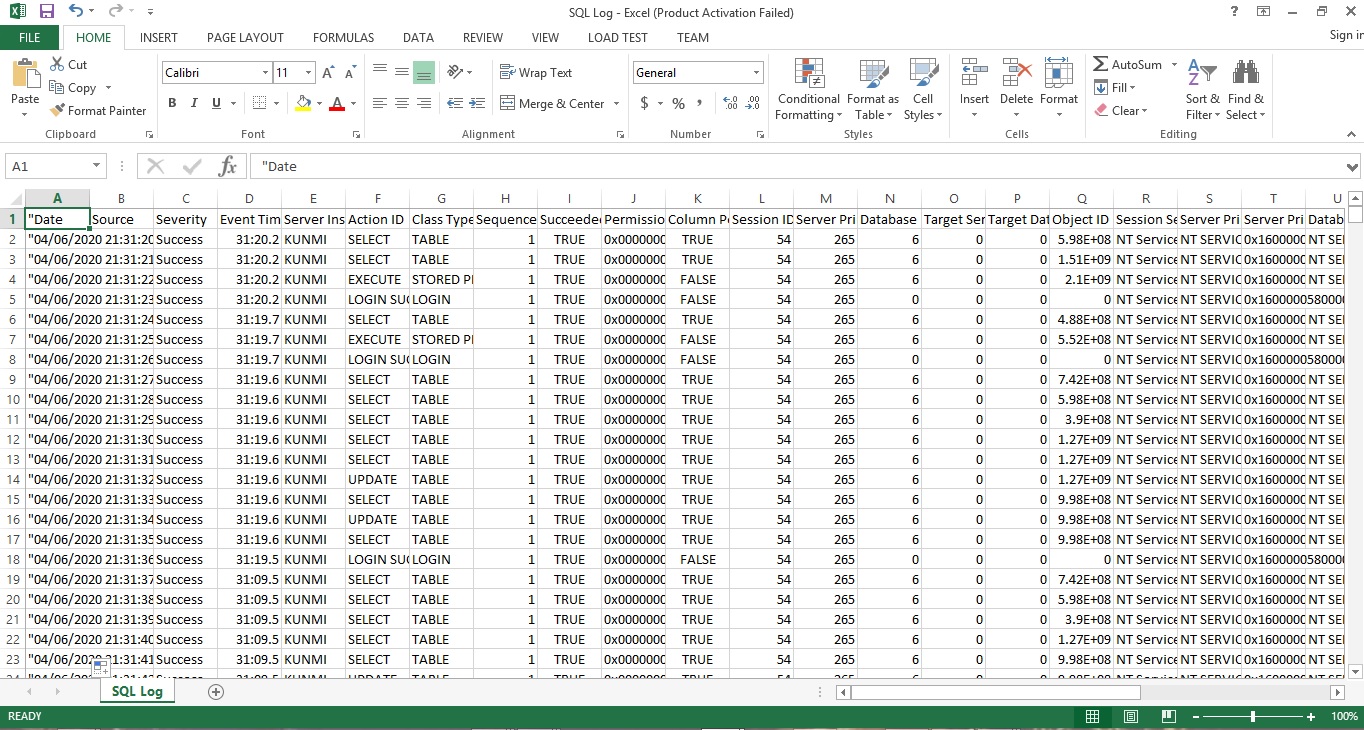
**Analysis of the Log file.**

The exported file is saved in a .txt file format and separated by commas. This can be further analyzed using Excel by following the following steps.









Here’s the Log file for the Audit

**References:**

Asanka, D. (2019, November 28). SQL Server auditing with Server and Database audit specifications. Retrieved April 12, 2020, from <https://www.sqlshack.com/sql-server-auditing-server-database-audit-specifications/>

How to set up and use SQL Server Audit. (2018, September 19). Retrieved April 12, 2020, from <https://solutioncenter.apexsql.com/how-to-setup-and-use-sql-server-audit-feature/>