DAT243x

Securing SQL Server

Lab 03 | Implementing Auditing

Estimated time to complete this lab is 60 minutes

Overview

In this lab, you are preparing to install SQL Server 2016 for the IT department in Adventure Works Cycles. Before installing, you want to find out if the server hardware provisioned for the instance is ready.

The labs in this course are accumulative. You cannot complete the following labs if this lab has not been successfully completed.

What You'll Need

To complete this lab, you will need the following:

- High-speed and reliable internet connectivity (for remote connections to the VM)
- A second monitor is recommended (for the Remote Desktop connection)
- A Microsoft account (such as one used for outlook.com, Hotmail, or other Microsoft services)
- A Microsoft Azure subscription
- To have completed the previous labs in this course.

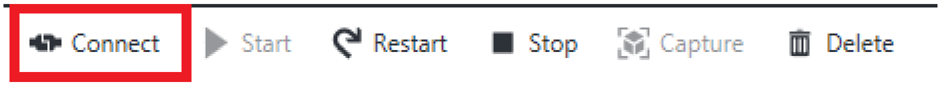
Exercise 1: Working with SQL Server Audit

In this exercise, you will create a server audit with server and database audit specifications.

Start the virtual machine

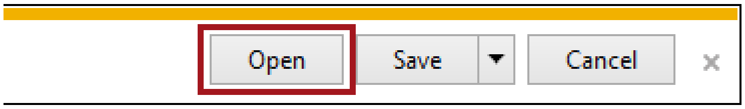
In this task, you will start the virtual machine for the lab.

1. If the virtual machine that you created in Lab 00 is not already running, open the Azure Portal, sign in, select the virtual machine, and click **Start**.
2. When the virtual machine has started, click **Connect**.

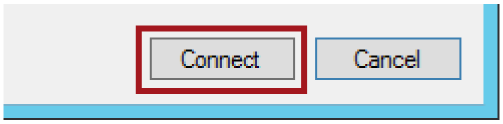


3. Click **Save**.

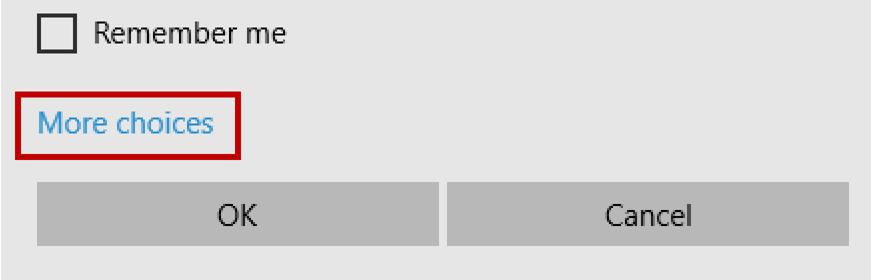
4. When prompted by the web browser to open the Remote Desktop File, click **Open**.



5. If prompted to connect to the unknown publisher, click **Connect**.



*To enter your credentials, you may need to select **More Choices**, and then select **Use a Different Account**.*



6. In the **Windows Security** window, enter the password you created for your VM, select **Remember me** and click **OK**.

7. If you have a second monitor, maximize the Remote Desktop window inside a single monitor.

Create a Server Audit

1. Start SQL Server Management Studio and connect to the **localhost** database engine using Windows authentication.
2. If Object Explorer is not visible, on the **View** menu, click **Object Explorer**.
3. Expand the **Security** node, right-click the **Audits** node, and click **New Audit**.
4. In the **Create Audit** dialog box, in the **Audit name** box, type **activity_audit**.
5. In the **Audit destination** box, select **Application Log**, and then click **OK**.
6. In Object Explorer, expand the **Audits** node, right-click the **activity_audit** node, and then click **Enable Audit**.
7. In the **Enable Audit** dialog box, click **Close**.

Create a Server Audit Specification

1. In Object Explorer, right-click the **Server Audit Specifications** node, and click **New Server Audit Specification**.
2. In the **Create Server Audit Specification** dialog box, in the **Name** box, type **audit_logins**. In the **Audit** box, select **activity_audit**.
3. In the **Actions** box, in the **Audit Action Type** list, select the **SUCCESSFUL_LOGIN_GROUP** value, and then click **OK**.

Create a Database Audit Specification

1. In Object Explorer, expand the **Databases** node, expand the **AdventureWorks2012** node, and then expand the **Security** node.
2. Right-click the **Database Audit Specifications** node, and click **New Database Audit Specification**.
3. In the **Create Database Audit Specification** dialog box, in the **Name** box, type **product_change_audit**, and in the **Audit** box, select **activity_audit**.
4. In the **Actions** box, in the **Audit Action Type** list, select the **INSERT** value. In the **Object Class** list, on the first row, select **OBJECT**.
5. In the **Object Name** column, in the first row, click the ellipsis (**…**).
6. In the **Select Objects** dialog box, in the **Enter the object names to select (examples)** box, type **Production.Product**, and then click **OK**.
7. In the **Principal Name** column, in the first row, click the ellipsis (**…**).
8. In the **Select Objects** dialog box, in the **Enter the object names to select (examples)** box, type **public**, and then click **OK**.
9. On the second row, in the **Audit Action Type** list, select the **UPDATE** value. In the **Object Class** list on the second row, select **OBJECT**.
10. In the **Object Name** column, in the second row, click the ellipsis (**…**).
11. In the **Select Objects** window, in the **Enter the object names to select (examples)** box, type **Productio.Product**, and then click **OK**.
12. In the **Principal Name** column, in the second row, click the ellipsis (**…**).

13. In the **Select Objects** window, in the **Enter the object names to select (examples)** box, type **public**, and then click **OK**.
14. In the **Create Database Audit Specification** dialog box, click **OK**.
15. In Object Explorer, expand the **Database Audit Specifications** node, right-click the **employees_change_audit** node, and click **Enable Database Audit Specification**.
16. In the **Enable Database Audit Specification** dialog box, click **Close**.

Generate Audited Activity

1. In SQL Server Management Studio, click **New Query**.
2. In the query window, type the following Transact-SQL statement:

```
USE [AdventureWorks2016]
GO

UPDATE [Production].[Product]
   SET [Color] = 'Black'
 WHERE ProductID=1

GO
```

3. Click **Execute**.

Review Audit Data in Windows

1. In SQL Server Management Studio, expand **Management**, right-click **SQL Server Logs**, click **View**, and click **SQL Server and Windows** Log.
2. Click the first row with a **Source** of **MSSQLSERVER**.
3. Expand **Audits**, and click **View Audit Logs**.

Disable the Audit

1. In SQL Operations Studio, right-click your server and click **New Query**.
2. Type the following query and press Enter:

```
USE AdventureWorks2016
GO
ALTER DATABASE AUDIT SPECIFICATION [Product_Change_Audit] WITH
(STATE = OFF)
GO
USE master
GO
ALTER SERVER AUDIT SPECIFICATION [audit_logins] WITH (STATE = OFF)
GO
```

Lab Check – *You will need these answers for the module quiz – write them down!*

Lab 03 ► Exploring the Lab Solution

What is the value for **server_principal_name**? _______________

What is the value for **schema_name**? _______________

What is the value for **Source**? _______________

You have now completed the lab.

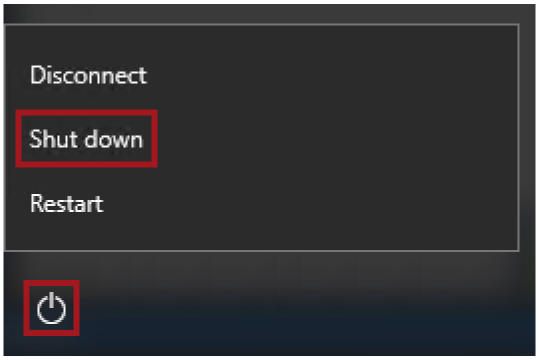
*If you are not immediately continuing with the next lab, you should complete the **Finishing Up** exercise to shut down and stop the VM.*

Finishing Up

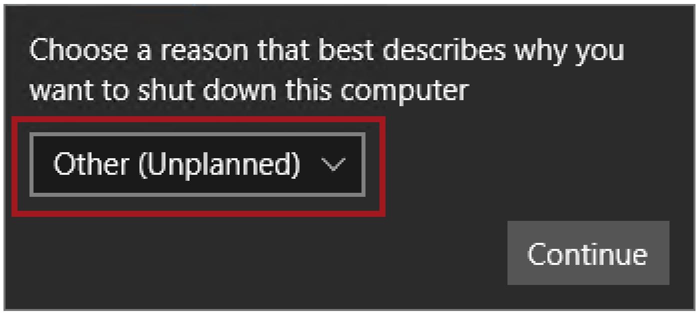
In this exercise, you will shut down and stop the VM.

1. Close all open applications.

2. Press the **Windows** key, and then in the **Start** page, located at the bottom-left, click the **Power** button, and then select **Shut Down**.



3. When prompted to choose a reason, to accept the default.

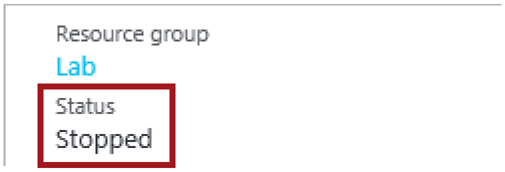


Choose a reason that best describes why you want to shut down this computer

Other (Unplanned)

4. Click **Continue**.

5. In the **Azure Portal** Web browser page, wait until the status of the VM updates to **Stopped**.



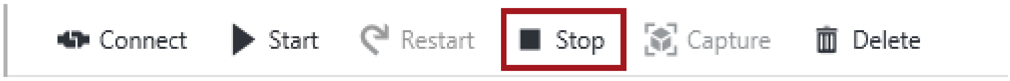
Resource group
Lab

Status
Stopped

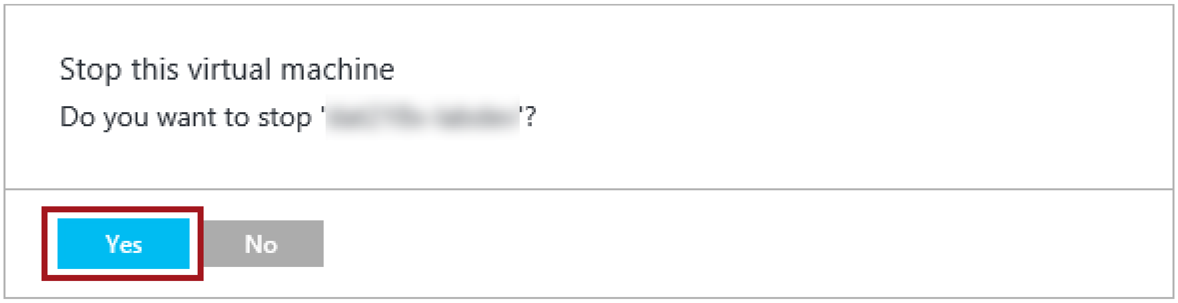
In this state, however, the VM is still billable.

6. Optionally, to deallocate the VM, click **Stop**.

   Deallocation will take some minutes to complete, and also extends the time required to restart the VM. Consider deallocating the VM if you want to reduce costs, or if you choose to complete the next lab after an extended period.

7. When prompted to stop the VM, click **Yes**.

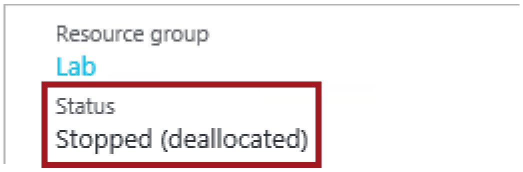
   

   Stop this virtual machine

   Do you want to stop '[redacted]'?

   The deallocation can take several minutes to complete.

8. Verify that the VM status updates to **Stopped (Deallocated)**.

   Resource group
   Lab

   Status
   Stopped (deallocated)

   In this state, the VM is now not billable—except for a relatively smaller storage cost.

   Note that a deallocated VM will likely acquire a different IP address the next time it is started.

9. Sign out of the **Azure Portal**.