DAT243x

Securing SQL Server

Lab 03 | Implementing Auditing

Estimated time to complete this lab is 60 minutes

Overview

In this lab, you need to analyze key updates in your SQL Server database. To achieve this, youy will implement auditing.

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.

- 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**.

Create a Server Audit

1. Start SQL Operations Studio on your client machine.
2. Right-click the server and click **New query**.
3. Type the following query and click **Run**:

```
USE [master]
GO
CREATE SERVER AUDIT [activity_audit]
TO FILE
(  FILEPATH = N'/tmp'
   ,MAXSIZE = 0 MB
   ,MAX_ROLLOVER_FILES = 2147483647
   ,RESERVE_DISK_SPACE = OFF
)
WITH
(  QUEUE_DELAY = 1000
   ,ON_FAILURE = CONTINUE
)
GO
```

Create a Server Audit Specification

1. Right-click the server and click **New query**.
2. Type the following query and click **Run**:

```
USE [master]
GO
CREATE SERVER AUDIT SPECIFICATION [audit_logins]
FOR SERVER AUDIT [activity_audit]
ADD (SUCCESSFUL_LOGIN_GROUP)
ALTER SERVER AUDIT SPECIFICATION [audit_logins] WITH (STATE = ON)
GO
```

Create a Database Audit Specification

1. Right-click the server and click **New query**.
2. Type the following query and click **Run**:

```
USE [AdventureWorks2016]
GO
```

```
CREATE DATABASE AUDIT SPECIFICATION [Product_Change_Audit]
FOR SERVER AUDIT [activity_audit]
ADD (INSERT ON OBJECT::[Production].[Product] BY [public]),
ADD (UPDATE ON OBJECT::[Production].[Product] BY [public])
GO
ALTER DATABASE AUDIT SPECIFICATION [Product_Change_Audit] WITH
(STATE = ON)
GO
```

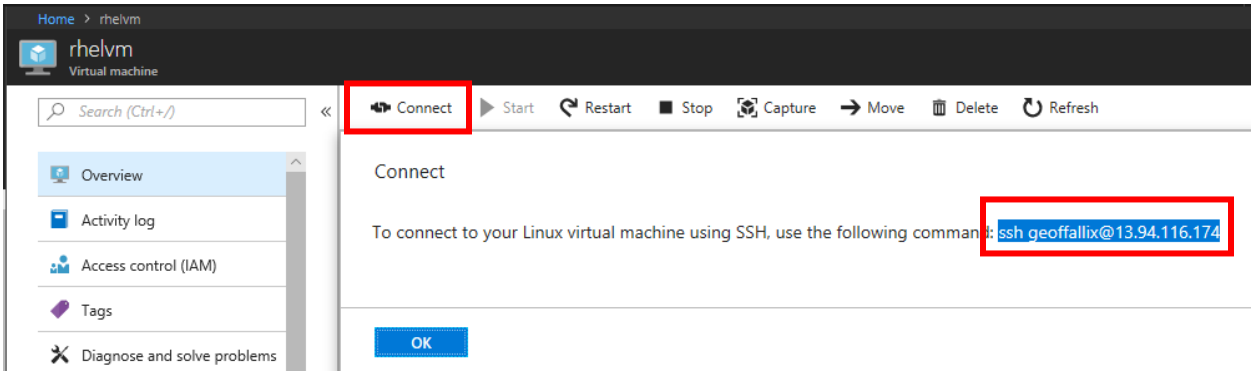
Generate Audited Activity

1. Right-click the server and click **New query**.
2. Type the following query and click **Run**:

```
USE [AdventureWorks2016]
GO
UPDATE [Production].[Product]
   SET [Color] = 'Black'
 WHERE ProductID=1
GO
```

Review Audit Data

1. Go to the Azure Portal.
2. Click on your Linux virtual machine from the dashboard and click **Connect**.
3. Copy the **ssh** command by right-clicking the **ssh** command and clicking **Copy**.



4. At the top of the portal, click **Cloud Shell**.

5. When the Cloud Shell has connected, type your password if requested and press Enter.
6. Paste the ssh command that you copied and press Enter.
7. Type your password and press Enter.
8. Type **cd /**, and press Enter.
9. Type **cd tmp**, and press Enter.

10. Type **ls** and press Enter.
11. Select the most recent file with a sqlaudit extension and copy the file name.
12. Switch to SQL Operations Studio.
13. Right-click your Linux virtual machine and click **New Query**.
14. Type the following query, edit the SQL Audit file name by pasting your file name from Step 11, and press Enter:

```
USE Master
GO
SELECT * FROM sys.fn_get_audit_file ('/tmp/Paste your SQL Audit filename here',default,default);
GO
```

15. Review the log entries and repeat Steps 11-14 for any other audit files.

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.

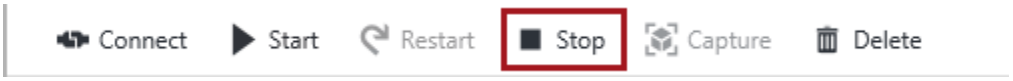
*If you are not immediately continuing with the next lab, you should complete the **Finishing Up** exercise to shut down and stop the VM.*

Finishing Up

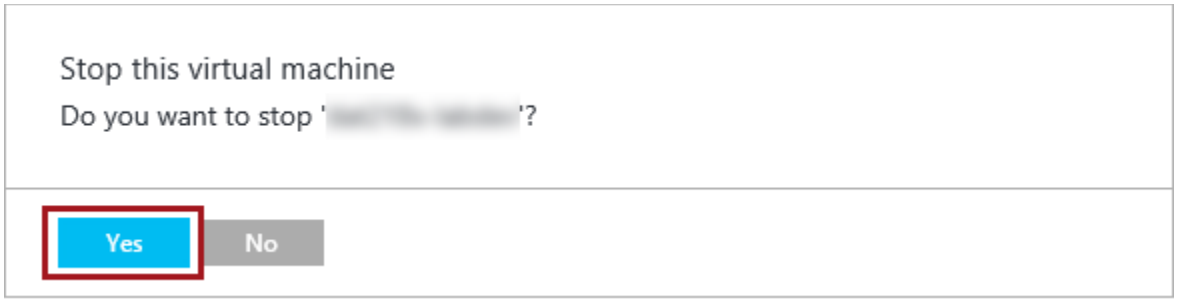
In this exercise, you will shut down and stop the VMs.

1. Deallocate the Linux VM by clicking **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.

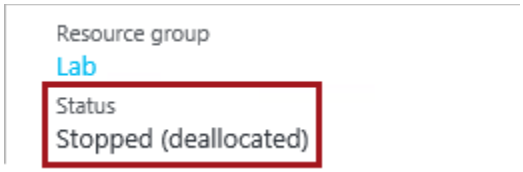


1. When prompted to stop the VM, click **Yes**.



   The deallocation can take several minutes to complete.

2. Verify that the VM status updates to **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.

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