**Lab 3 – Implement a Secure Environment**

**Estimated Time**: 60 minutes

**Prerequisites**: An Azure SQL server you created in the lab for Module 2. Azure Active Directory access in the subscription.

**Lab files**: The files for this lab are in the D:\Labfiles\Secure Environment folder.

**Lab overview**

The students will take the information gained in the lessons to configure and subsequently implement security in the Azure Portal and within the AdventureWorks database.

**Lab objectives**

After completing this lab, you will be able to:

* 1. Configure an Azure SQL Database Firewall
  2. Authorize Access to Azure SQL Database with Azure Active Directory
  3. Enable Advanced Threat Protection for Azure SQL Database
  4. Configure Data Classification for Azure SQL Database
  5. Manage access to database objects

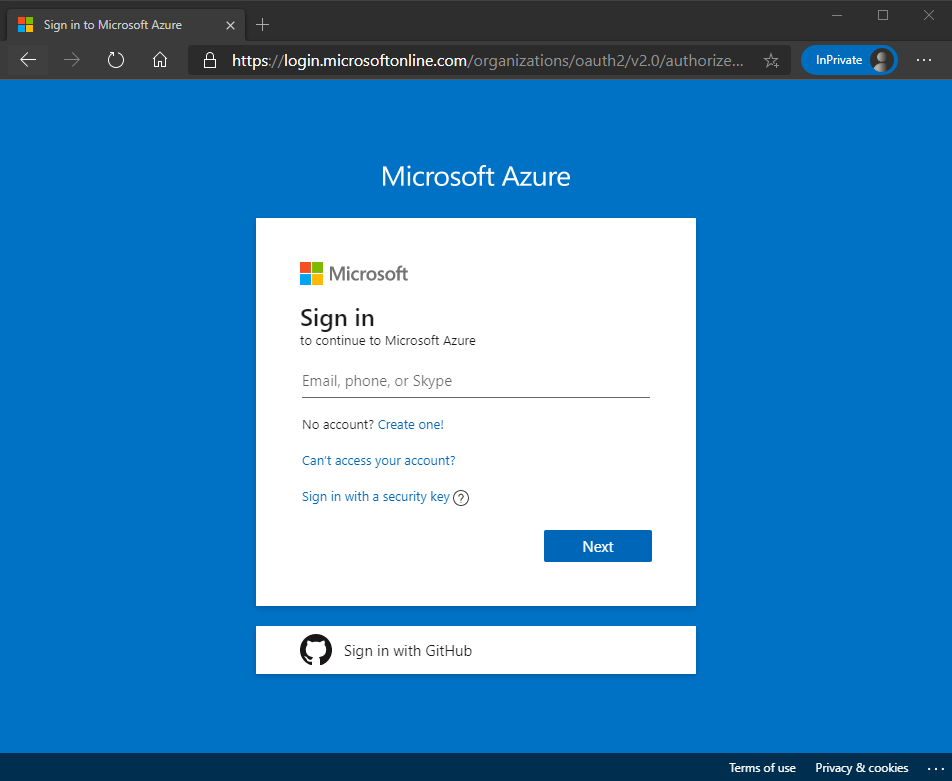
**Scenario**

You have been hired as a Senior Database Administrator help ensure the security of the database environment. These tasks will focus on Azure SQL Database.

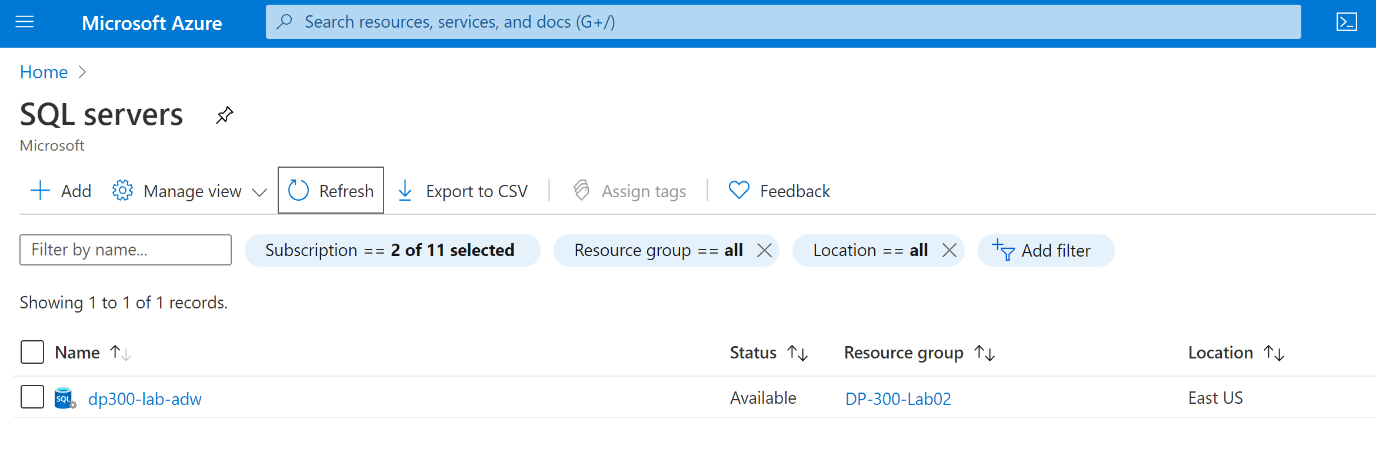
**Note:** The exercises ask you to copy and paste T-SQL code. Please verify that the code has been copied correctly, with the proper line breaks, before executing the code.

**Exercise 1: Configure an Azure SQL Database Firewall and connect to a new database**

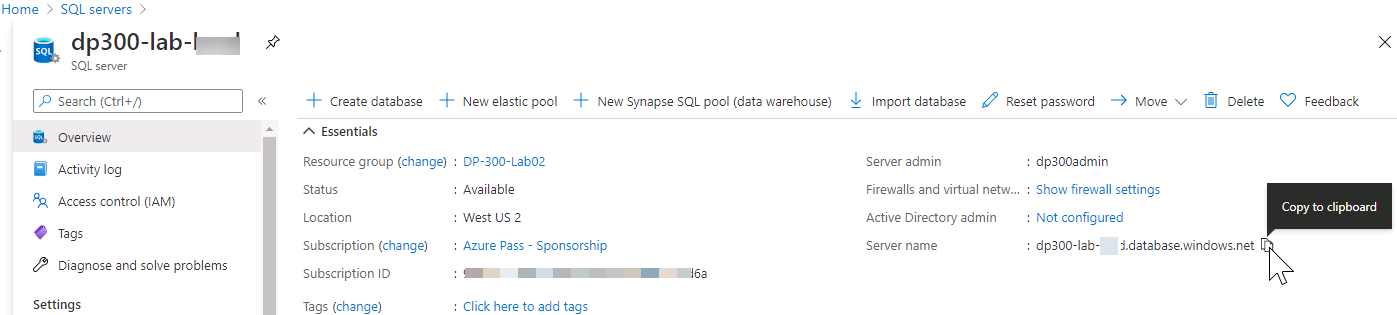
* 1. From the lab virtual machine, start a browser session and navigate to [https://portal.azure.com](https://portal.azure.com/). Provide appropriate credentials.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-01.png)

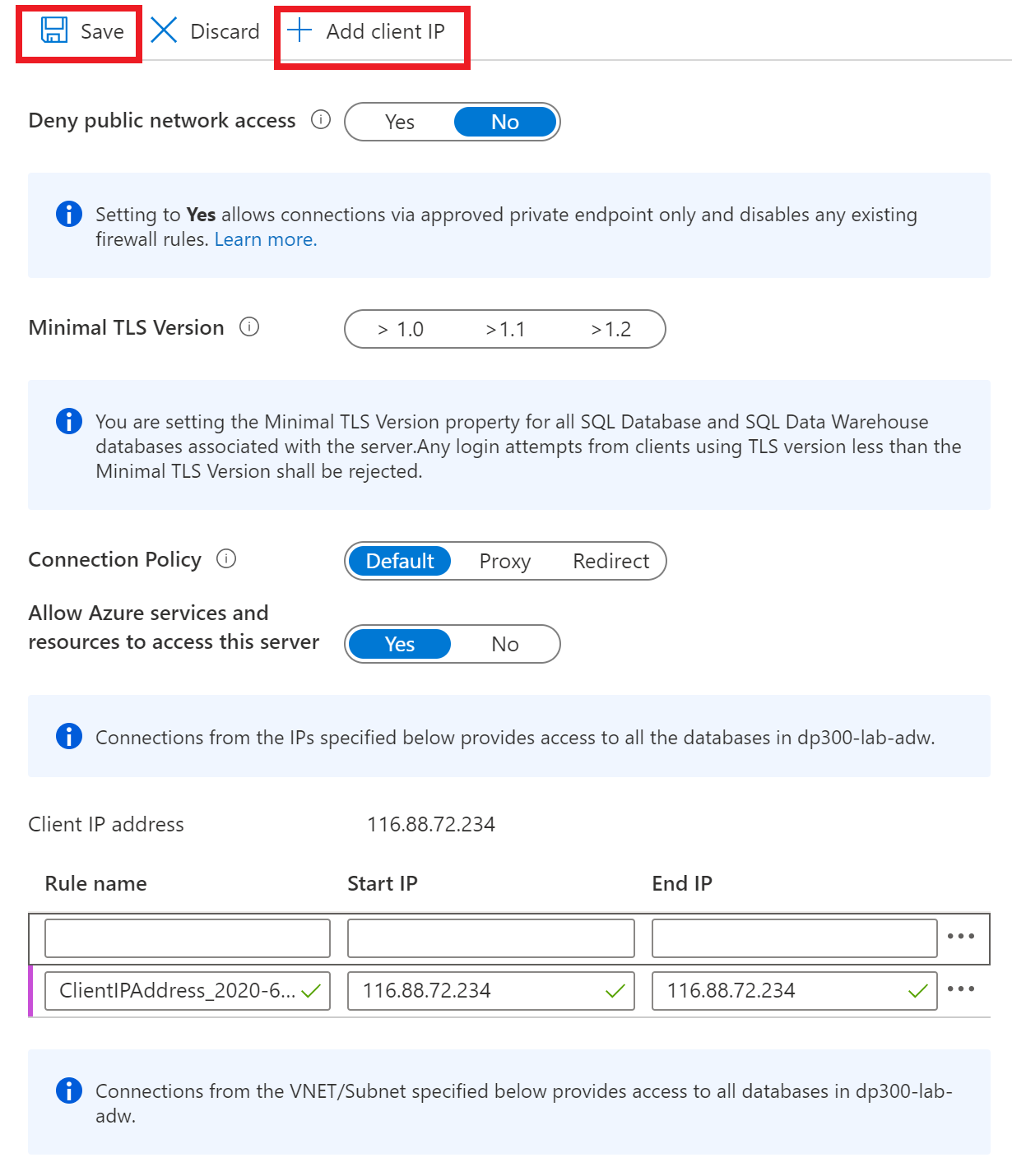
* 1. In the search bar at the top of the Azure Portal, type SQL. The SQL servers icon will appear. Click on SQL servers. Click on the server name to be taken to the detail page for the server you created in Lab 2

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-02.png)

* 1. In the detail screen for your SQL server, move your mouse to right of the server name, and click copy to clipboard button as shown below.

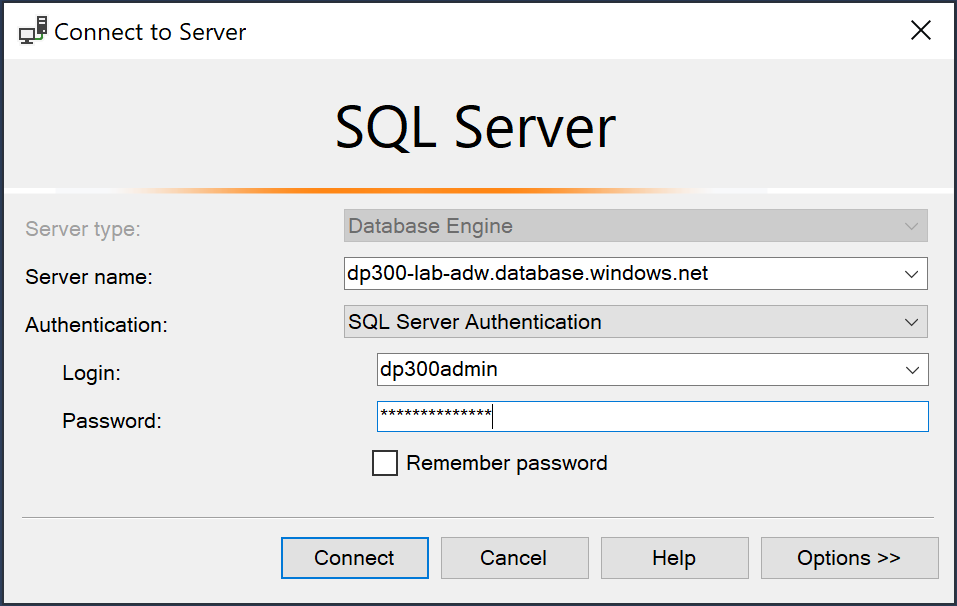
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-03.png)

* 1. Click on Show firewall settings (above the server name that you just copied). Click on + Add client IP as highlighted below and then click Save.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-04.png)

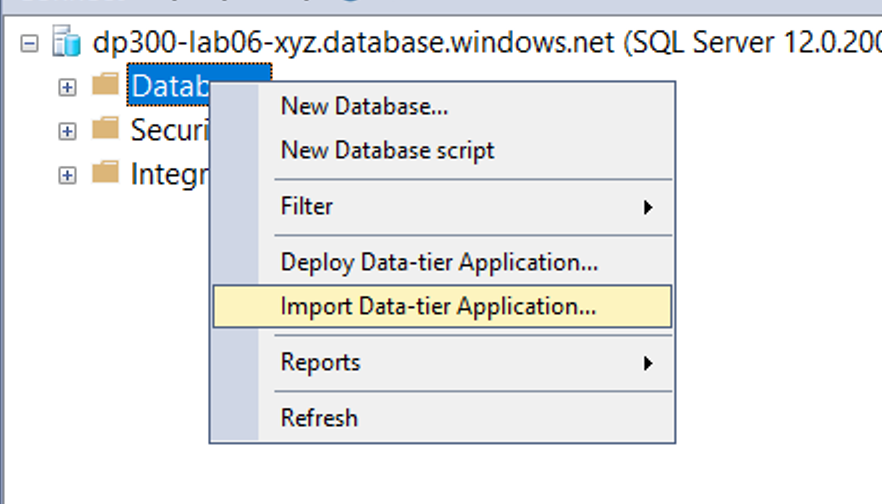
This will allow you to connect to your Azure SQL Database server using SQL Server Management Studio or any other client tools. Make note of your client IP address, you will use it later in this task.

* 1. Open SQL Server Management Studio on the lab VM, by navigating to Microsoft SQL Server Tools 18 > SQL Server Management Studio from the Start menu. Paste in the name of your Azure SQL database server and login with the credentials you created in Lab 2:
     + Server name:
     + Authentication: SQL Server Authentication
     + Server admin login: **dp300admin**
     + Password: **dp300P@ssword!**

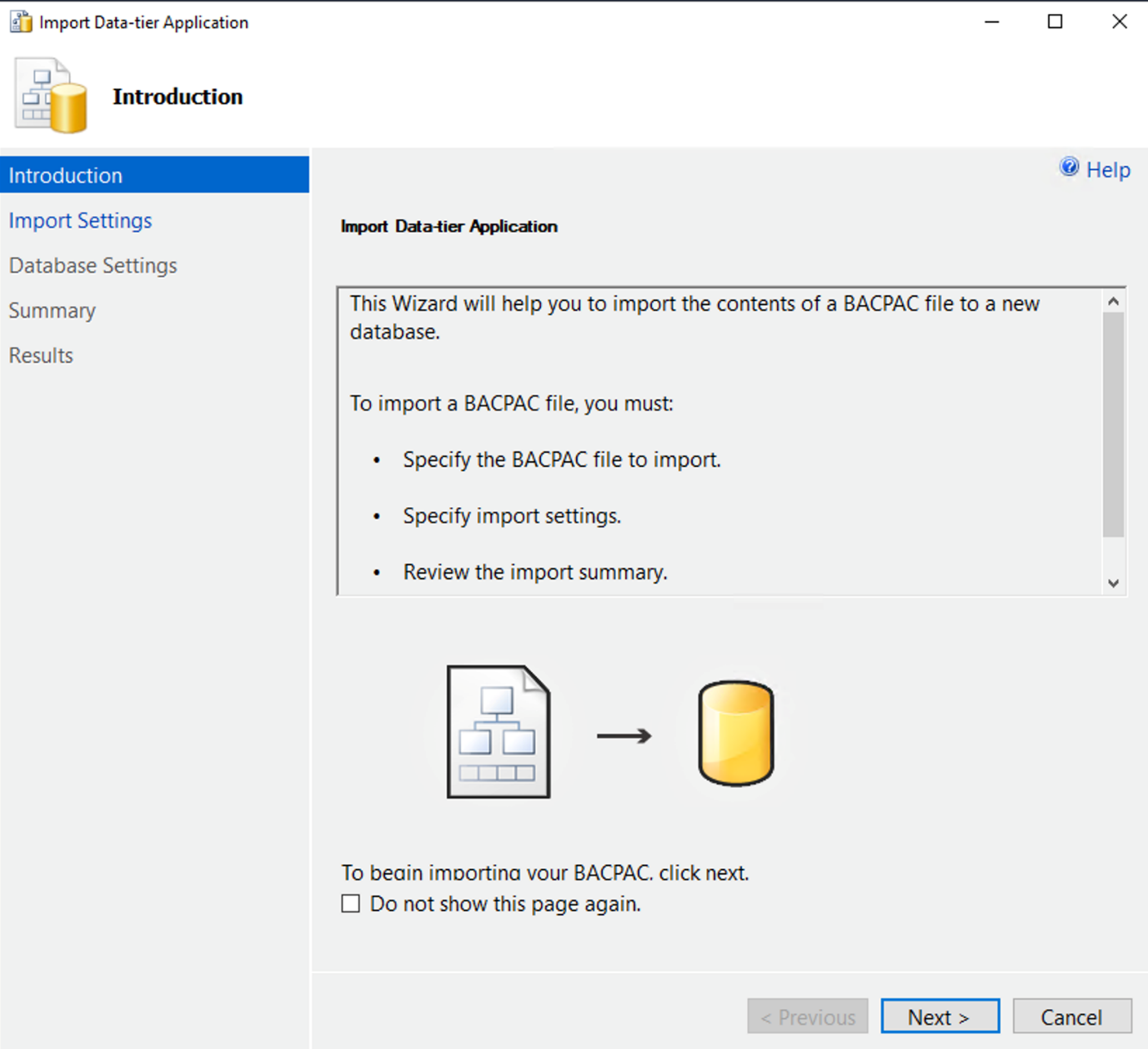
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-05.png)

Click Connect.

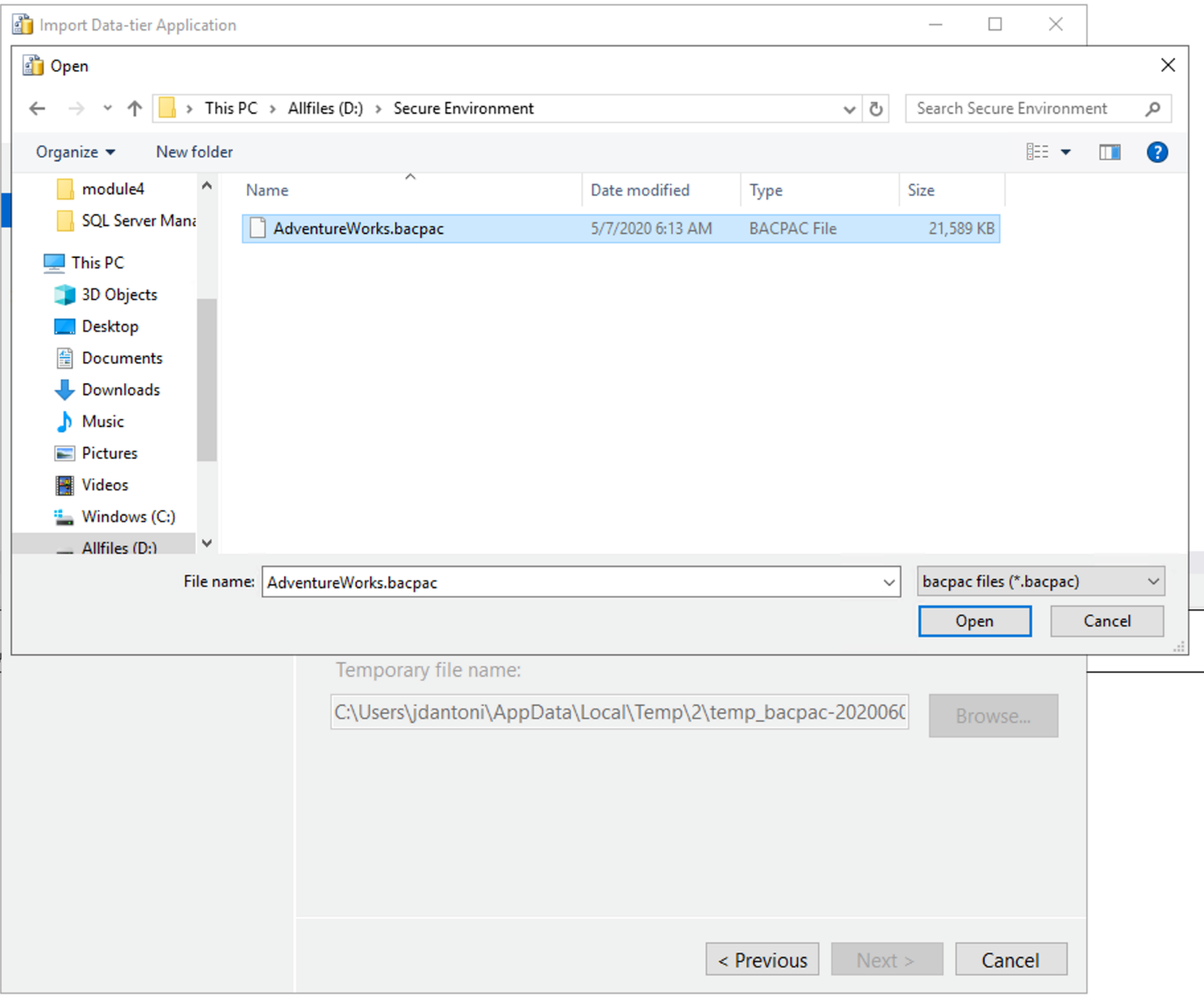
* 1. In Object Explorer expand the server node, and right click on databases. Click Import a Data-tier Application.

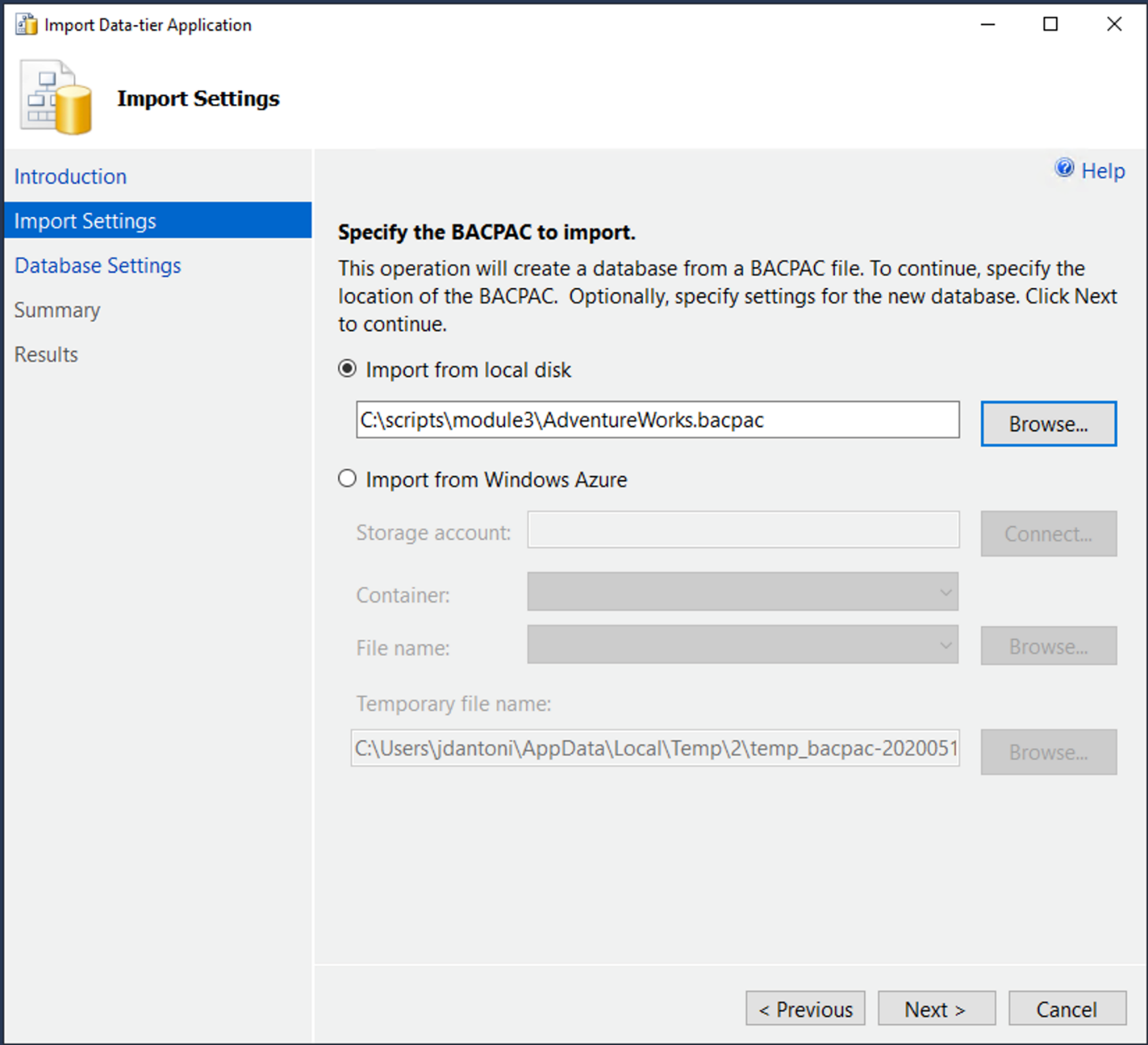
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-06.png)

* 1. In the Import Data Tier Application dialog, click Next on the first screen.

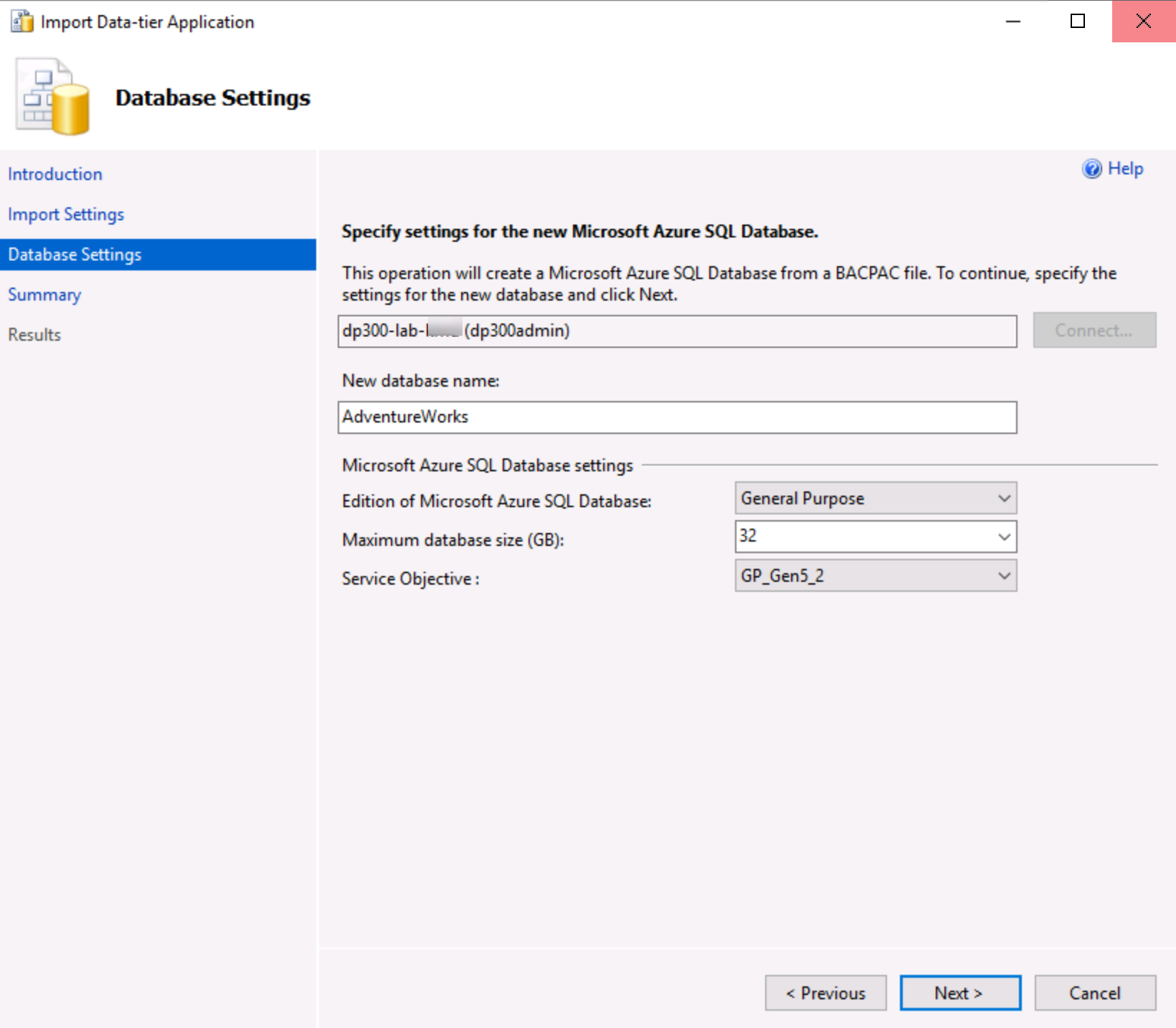
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-07.png)

* 1. In the Import Settings screen, click Browse and navigate to D:\Labfiles\Secure Environment folder and click on the AdventureWorks.bacpac file and click open. Then in the Import Data-tier application screen click **Next**.

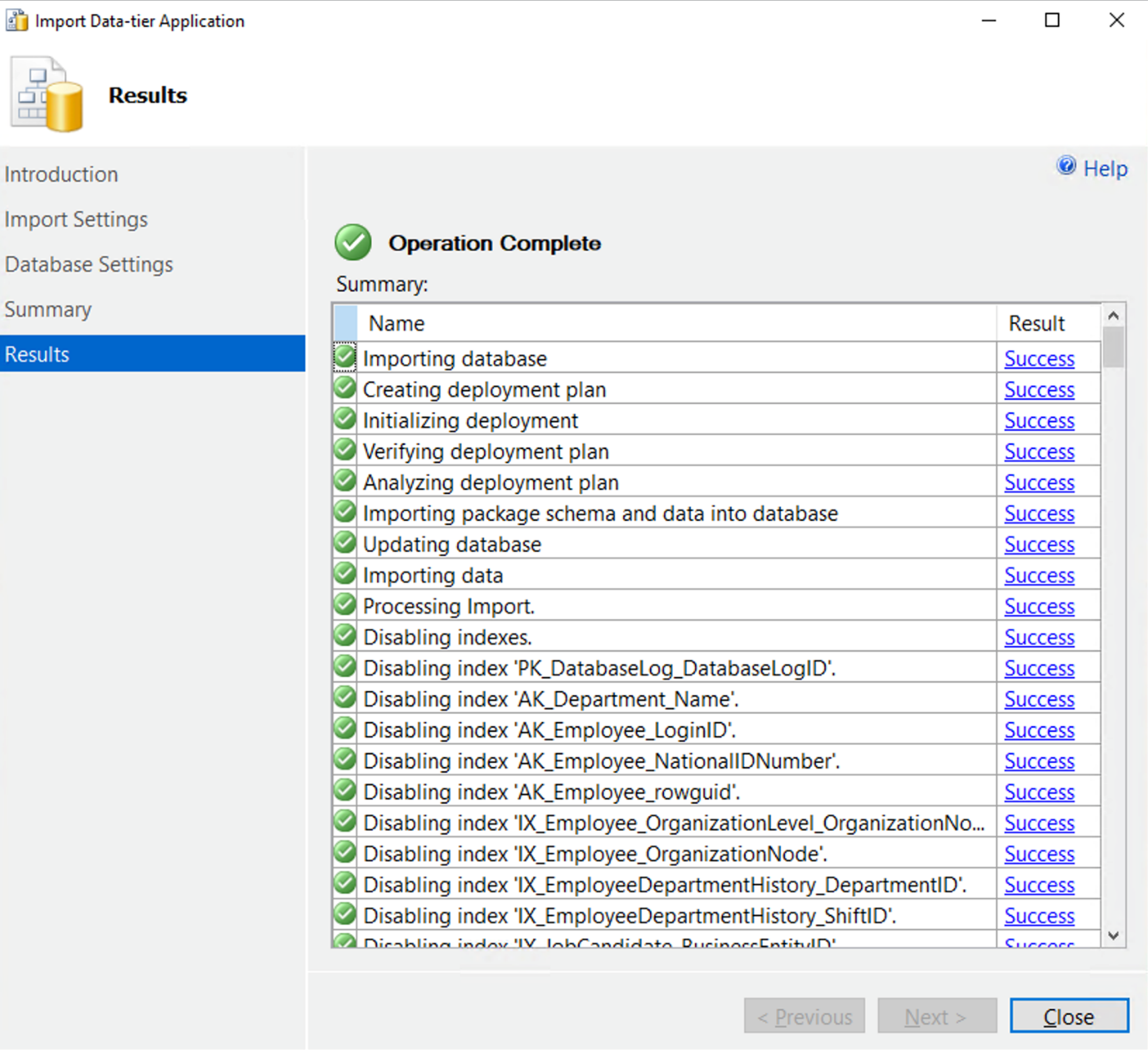
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-08.png)

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-09.png)

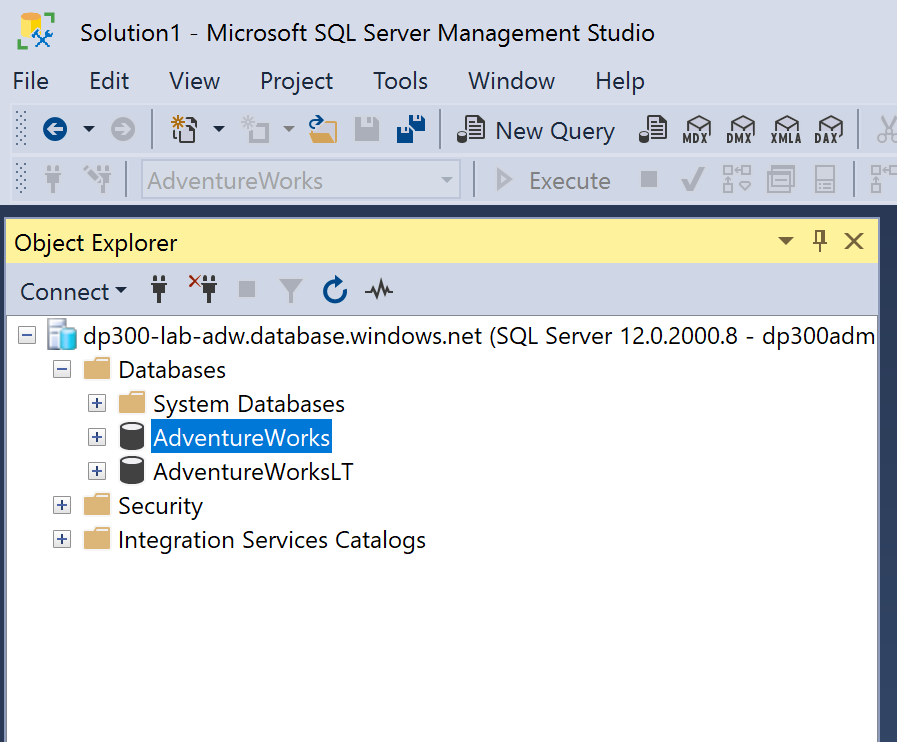
* 1. On the database settings screen, change the edition of Azure SQL Database to General Purpose. Change the Service Objective to **GP\_Gen5\_2** and click next.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-10.png)

* 1. Click **Next** and then on the Summary screen click **Finish**. When your import completes you will see the results below.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-11.png)

* 1. In Object Explorer right-click on AdventureWorks and then click on new query.

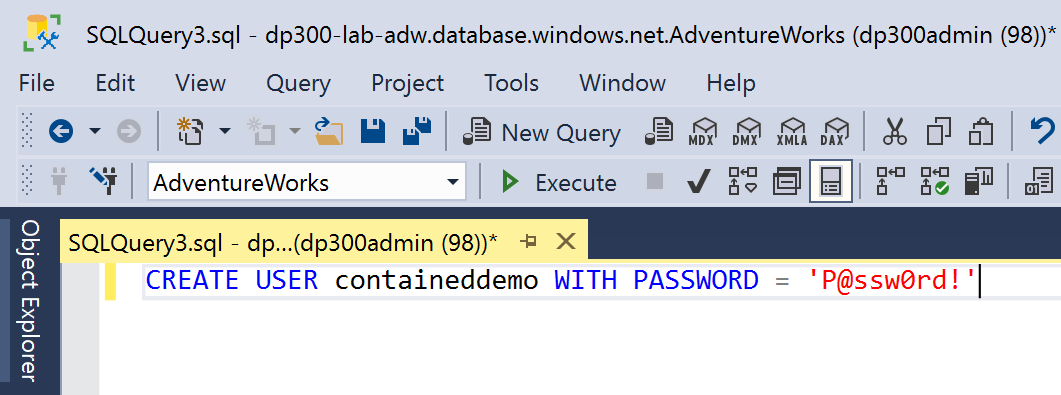
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-12.png)

* 1. Execute the following T-SQL query by pasting the text into your query window and replacing 192.168.1.1. with your client IP address from Step 4. Click execute or press F5.

Myip.com

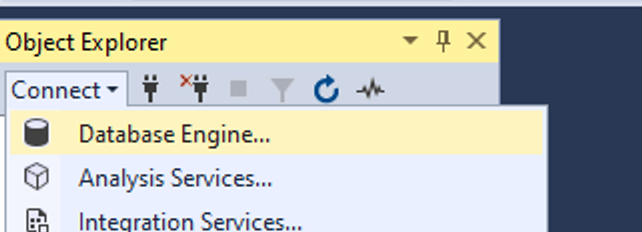
EXECUTE sp\_set\_database\_firewall\_rule @name = N'ContosoFirewallRule',@start\_ip\_address = '201.43.252.14', @end\_ip\_address = '201.43.252.14'

* 1. Next you will create a contained user in the AdventureWorks database. Click New Query and execute the following T-SQL. Ensure that you are still using the AdventureWorks database. If you see master in the database name box below, you can pull down and switch to AdventureWorks.

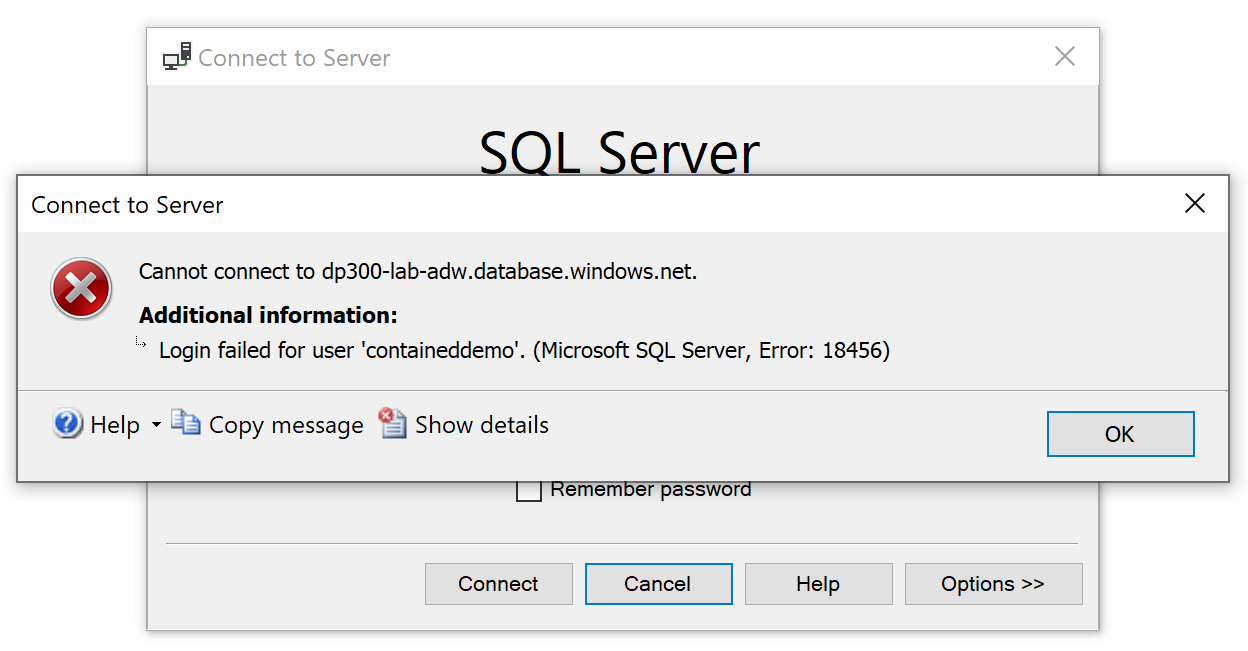
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-13.png)

Click execute to run this command. This command creates a contained user within the AdventureWorks database. You will login using the username and password in the next step.  
  
CREATE USER containeddemo WITH PASSWORD = 'P@ssw0rd!'

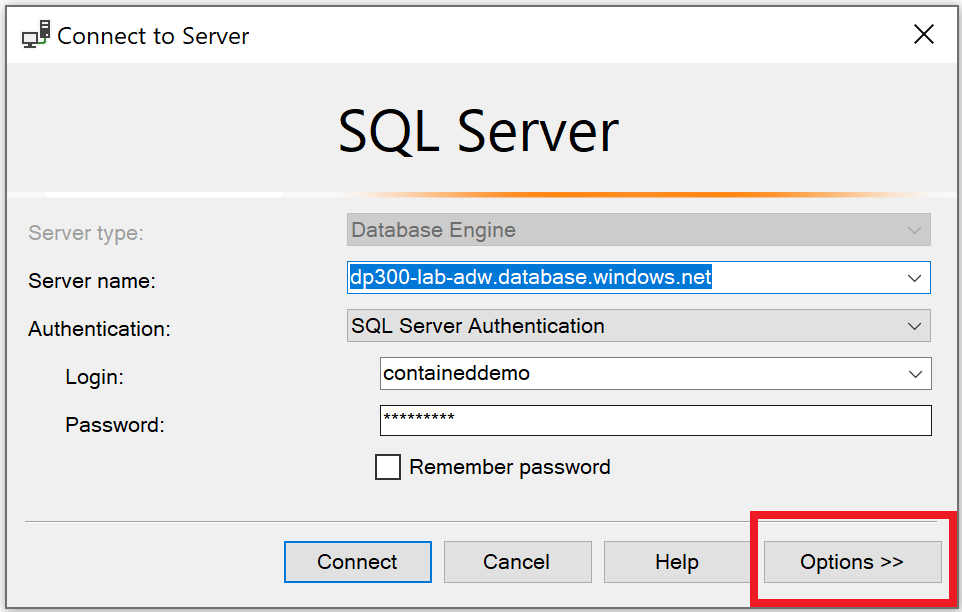
* 1. Navigate to Object Explorer in SSMS and click on connect and then Database Engine

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-14.png)

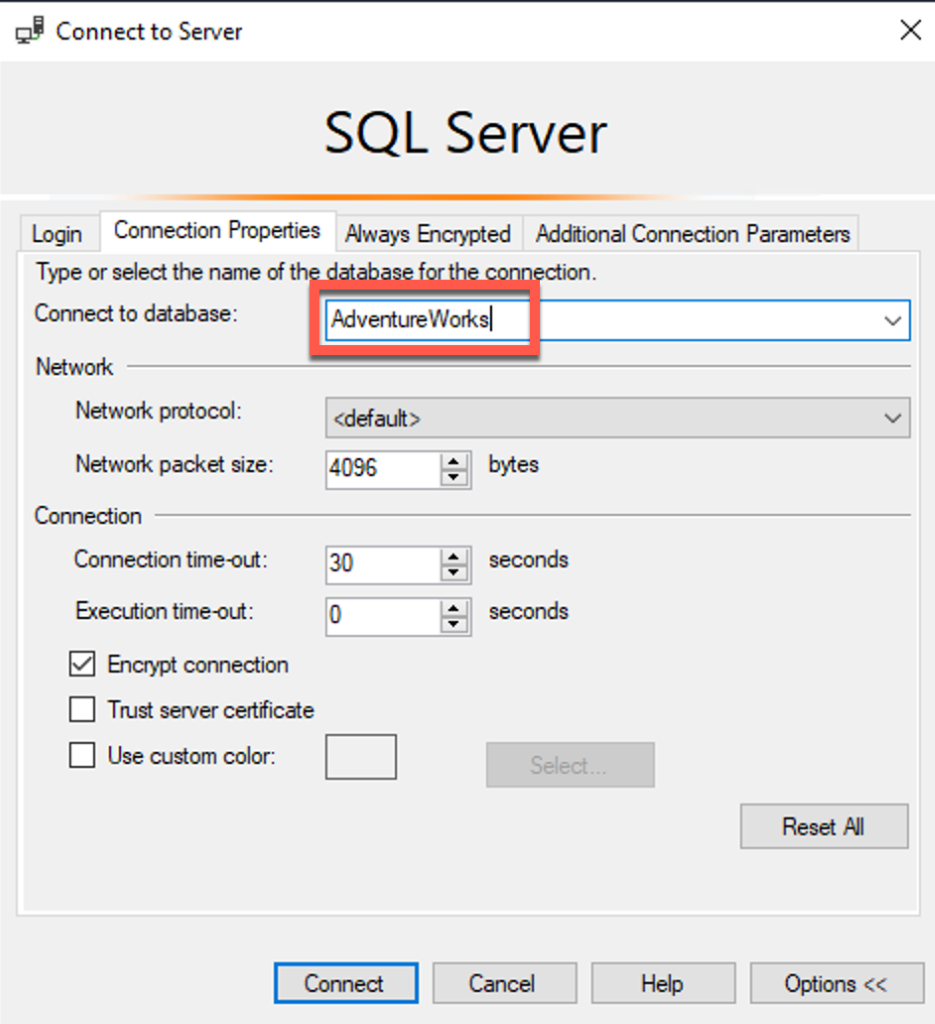
* 1. Attempt to connect with the credentials you created in step 13. You will need to use the following information:
     + **Login:** containeddemo
     + **Password:** P@ssw0rd!  
       Click Connect.  
       You will see the following error.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-15.png)

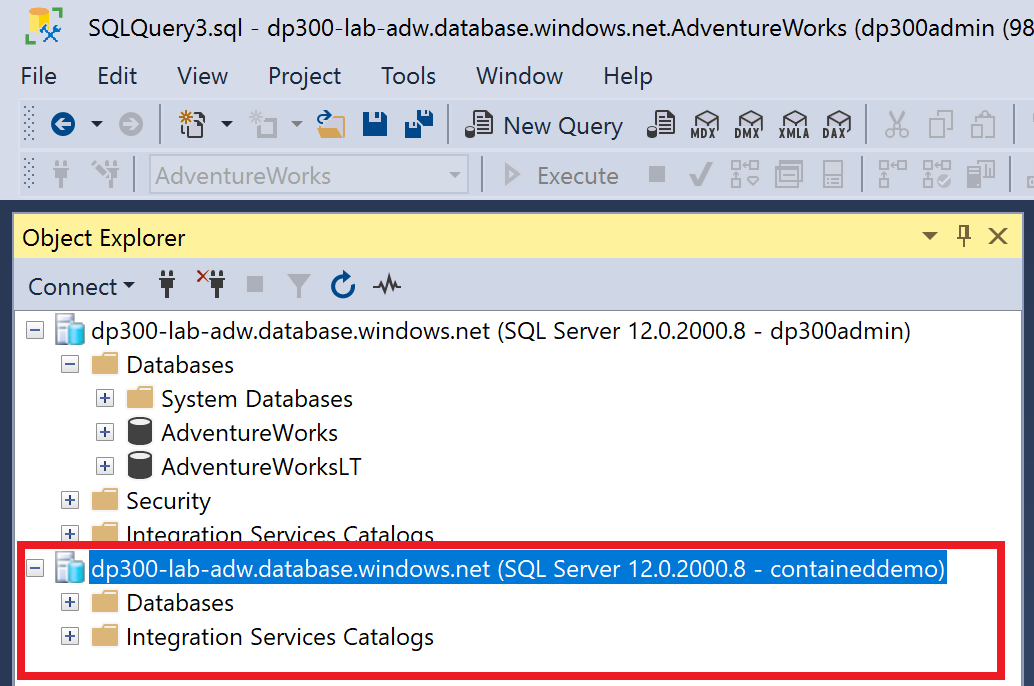
This error is generated because the connection attempted to login to the master database and not AdventureWorks where the user was created. Change the connection context by clicking OK to exit the error message and then clicking on Options >> in the Connect to Server dialog box as shown below.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-16.png)

* 1. On the connection options tab, type the database name **AdventureWorks**

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-17.png)

* 1. Click connect from that screen. This connection bypasses the master database and logs you directly into AdventureWorks, which is the only database to which the newly created user has access.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-18.png)

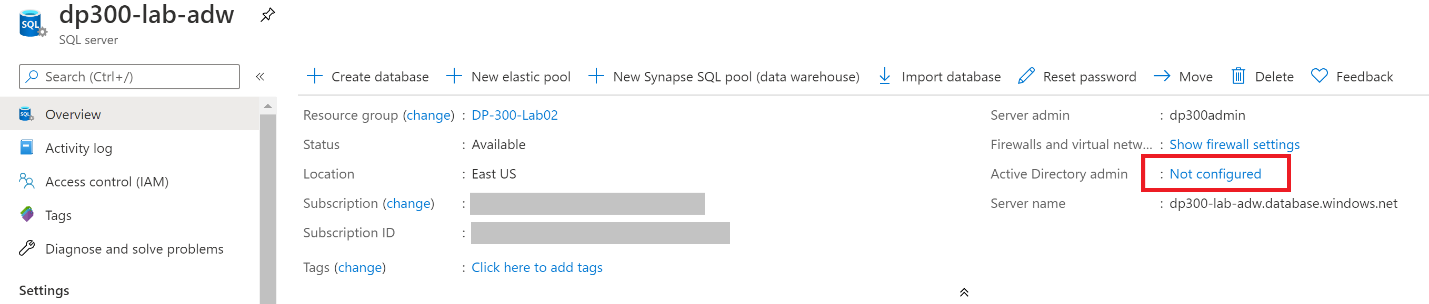
**Exercise 2: Authorize Access to Azure SQL Database with Azure Active Directory**

* 1. Navigate to the Azure Portal, and click on your user name in the top right corner of the screen.

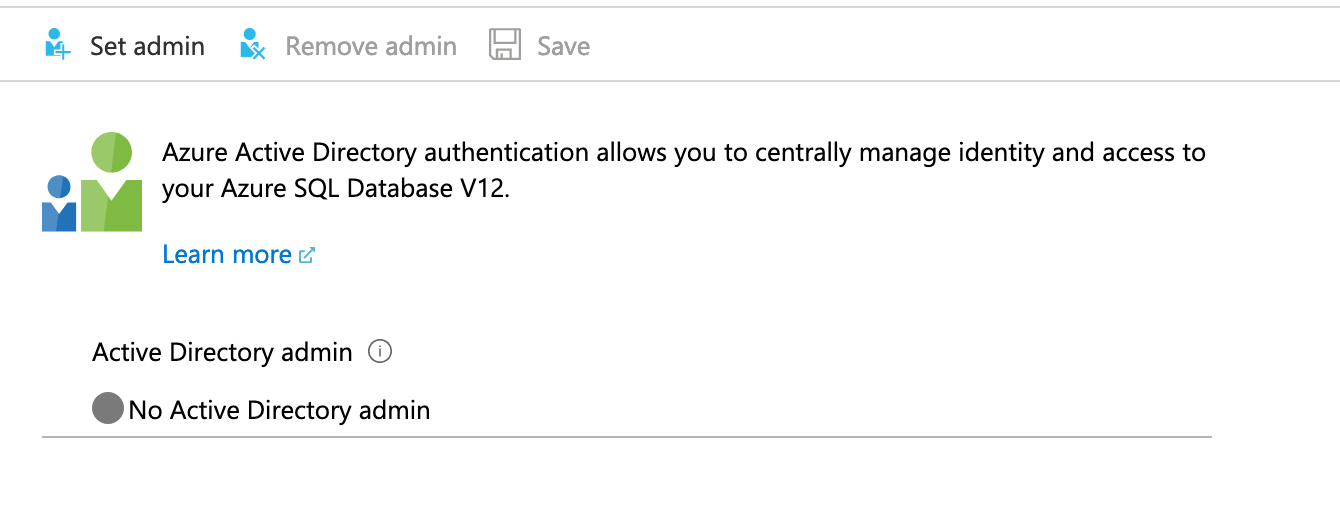
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-19.png)

Make note of the user name.  
**Note:** A Microsoft account (a user account from Outlook, Gmail, Hotmail or Yahoo, for example) is not supported for the Azure Active Directory administrator for Azure SQL Database. As a workaround, you can create an Azure Active Directory group named DBA and add your user account to it. Alternatively, you can skip Exercise 2.

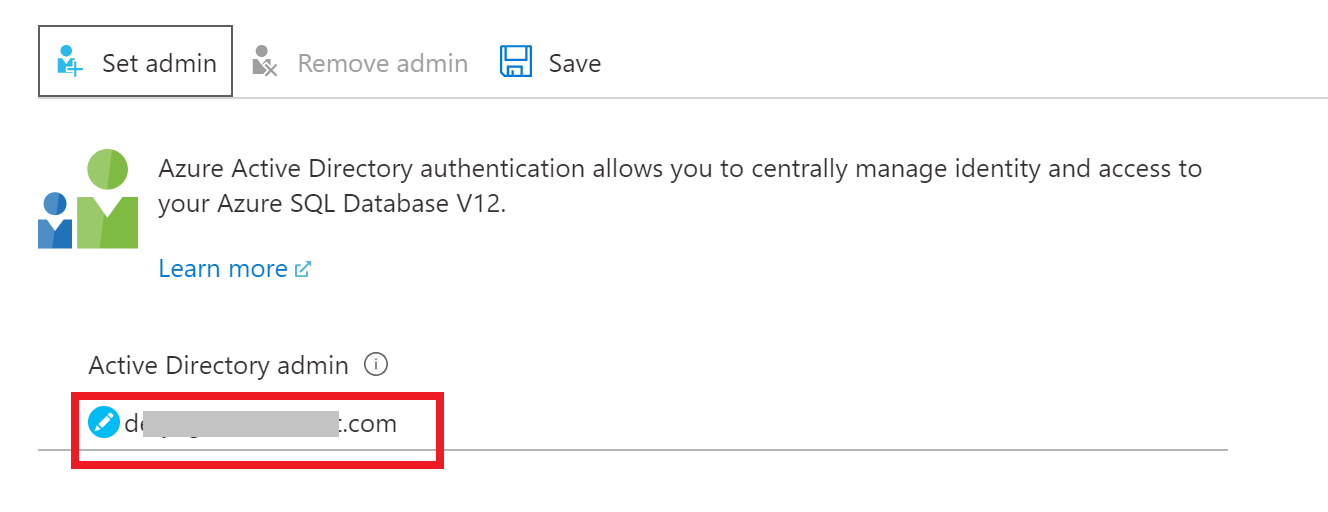
* 1. In the Azure Portal navigate to your Azure SQL Database server dp300-lab-xx and click on Not Configured next to Active Directory Admin.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-20.png)

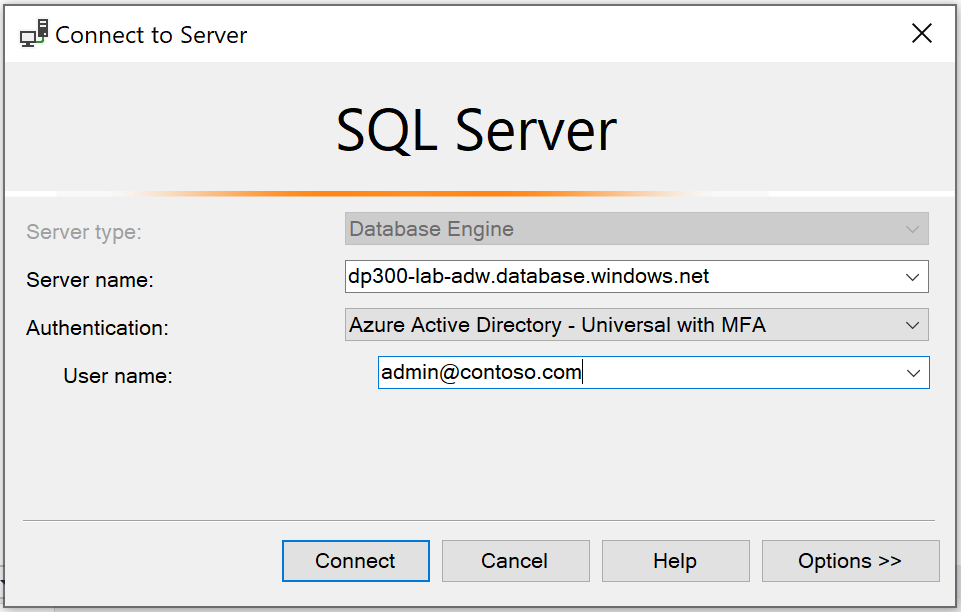
On the next screen, click set admin.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-21.png)

In the Set admin screen, search for your username. When you have found it, click on it to highlight the username, and then click Select. You will be returned to the above Active Directory Admin screen. Click save to complete the process. This will make your username the Azure Active Directory admin for the server as shown below

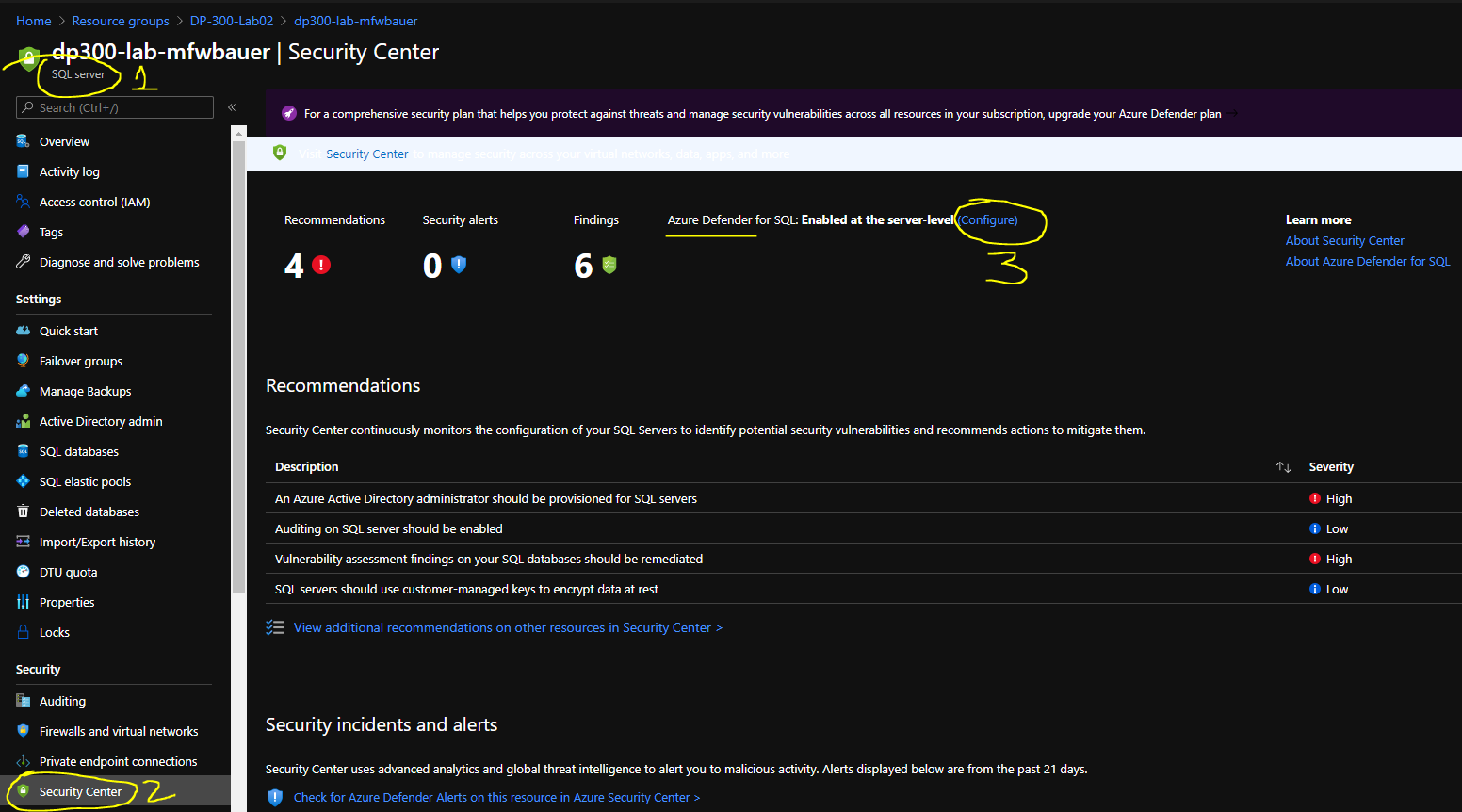
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-22.png)

* 1. Open SQL Server Management Studio and click Connect > Database Engine. In the server name enter the name of your server. Change the authentication type to Azure Active Directory Universal with MFA.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-23.png)

You will be prompted to enter your Azure Active Directory password, and will you click **Connect**, you'll be logged in to your database.

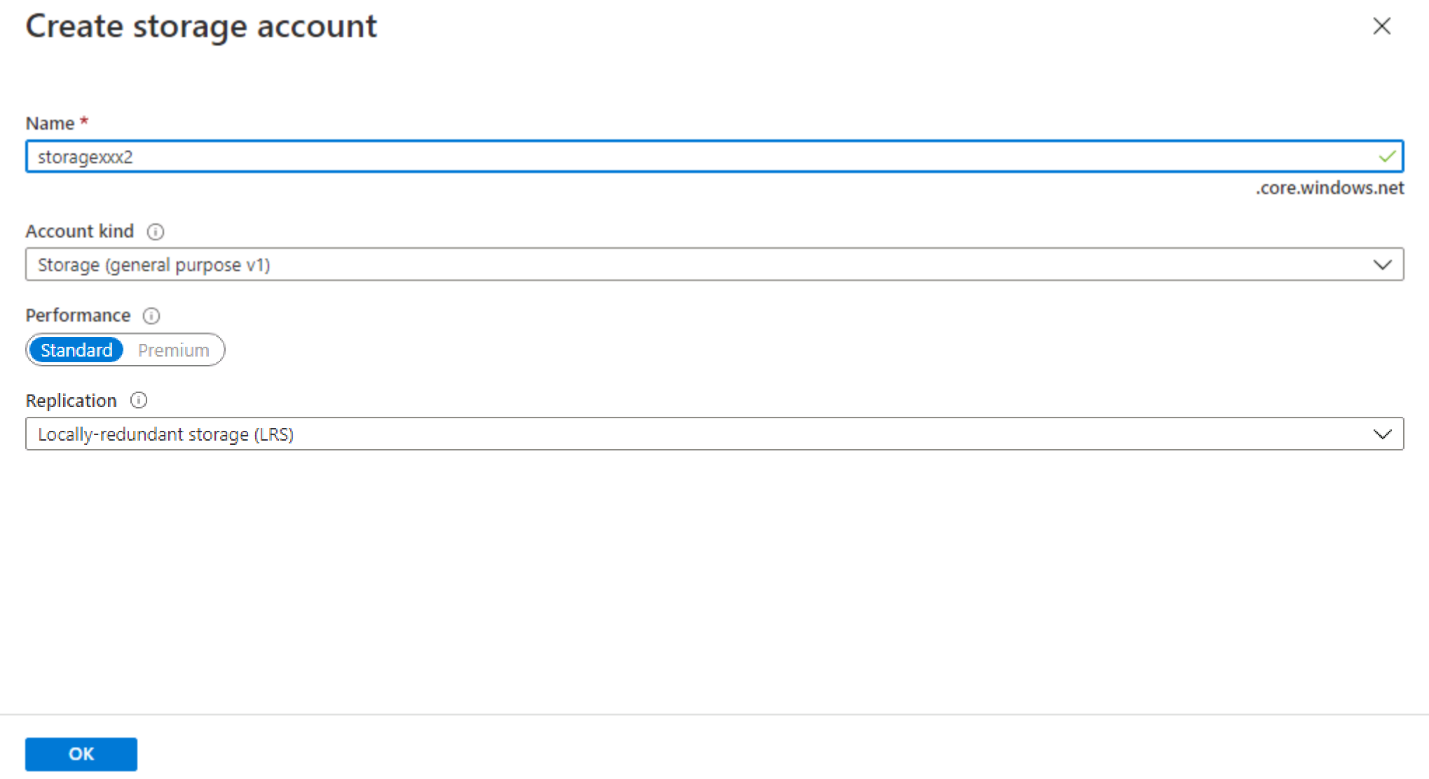
**Exercise 3: Enable Azure Defender for SQL and Data Classification**

* 1. From the main blade of your Azure SQL server navigate to the Security section and click Security Center. [Note that Azure Defender for SQL was formerly called Advanced data security, and the screenshots still reflect the former name.]
  2. 

Click the toggle switch under AZURE DEFENDER FOR SQL to ON. Click on Storage account. Toggle the switch for Periodic recurring scans to ON. Choose an email account to send scan reports and alerts to. Uncheck the box that says “Also send email notification to admins and subscription owners.”

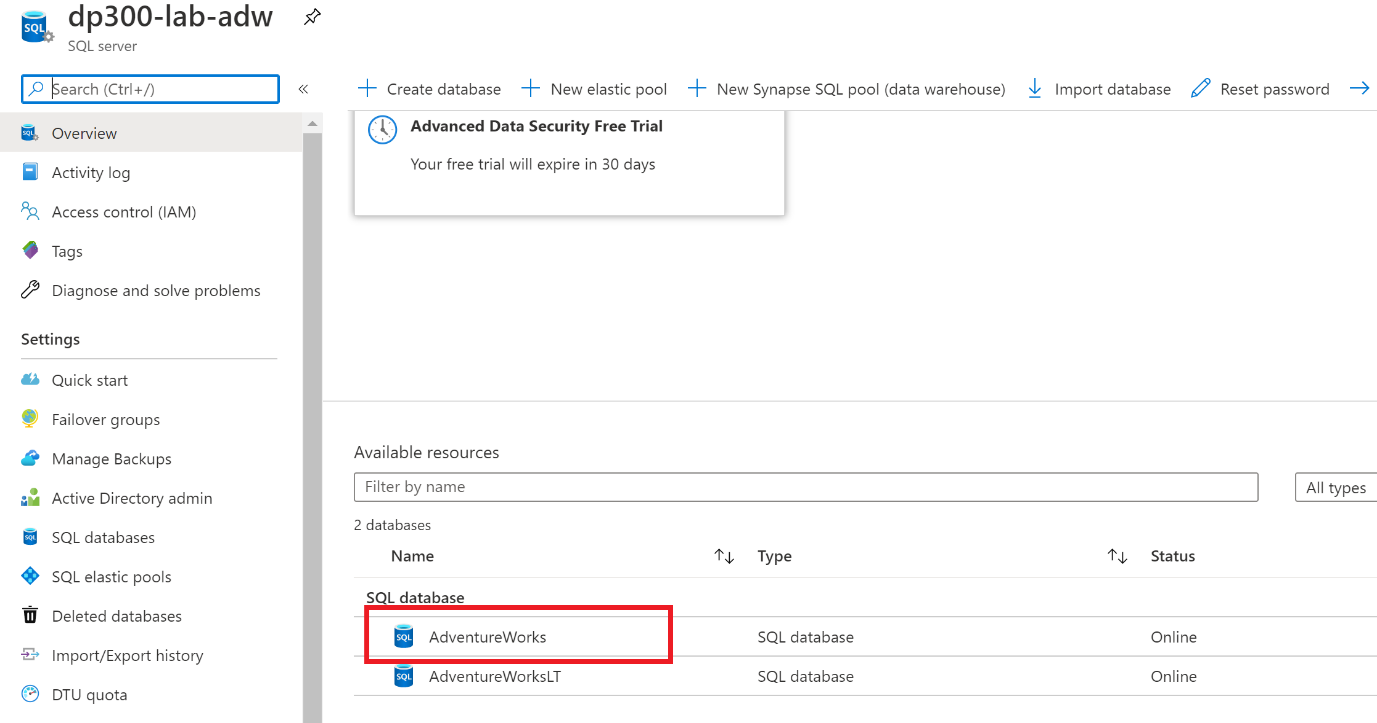
Home > Resource groups > DP-300-Lab02 > dp300-Iab-mfwbauer > 
Server settings 
d p3-m - lab f" 
Save 
AZLRE DEFENmR FOR SQL 
c ßts H 
—t We to a trial 
30 w+mt chuge. 
VULNERABILITY ASSESSMENT 
Su ption 
Azure pass — Sponsorship 
Sto rage 
pff50 
Periodic recurring scans 
Scans will be triggered automatically once a week. In most cases. it will be on the day 
Assessment has been enabled and saved. A scan result summary will be sent te 
the email addresses you provide. 
Send scan reports to 
Also send email notification to admins and subscription cwners G) 
ADVANCED THREAT PROTECTION SETTIr"S 
Send alerts to O 
Also send email notification to admins and subscription comers O 
T types 
Enable Auditir,a far better 
estiaaticm eweriem:e 

You may be prompted to create a storage account, unless there already are storage accounts for your subscription and region. You can choose an existing storage account or click + Create new. Enter a name for your storage account and click OK.

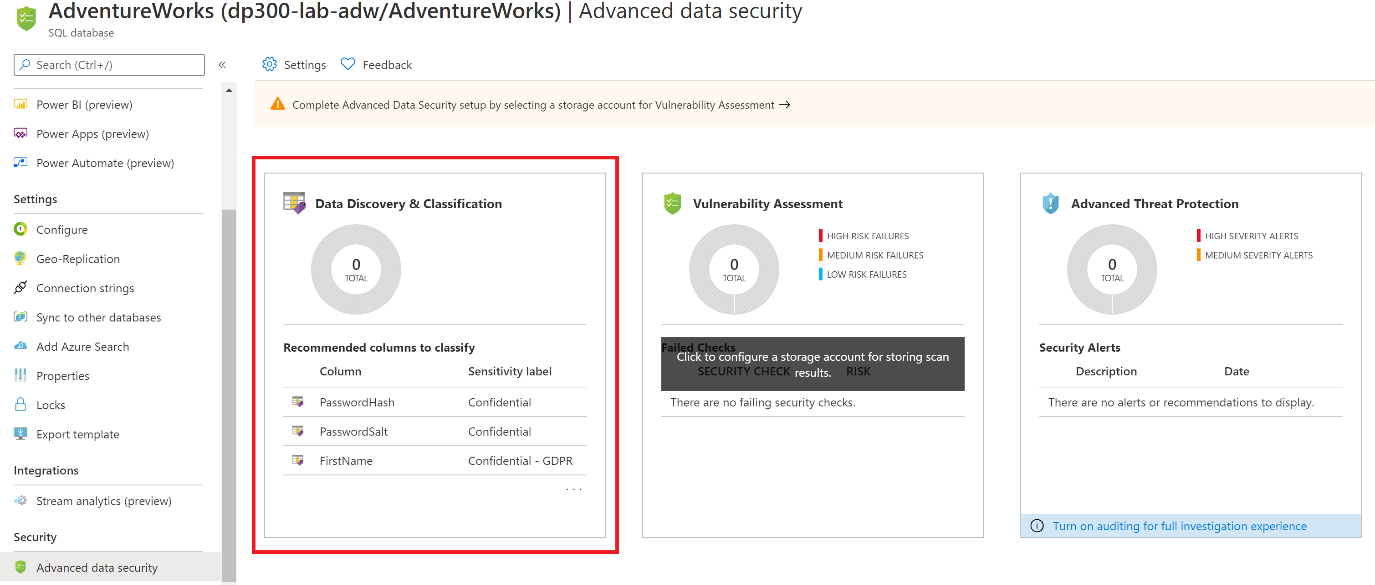
[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-90.png)

Click on Advanced Threat Protection types and review the selections. Leave all of the boxes checked and click **Save** at the top of the screen.

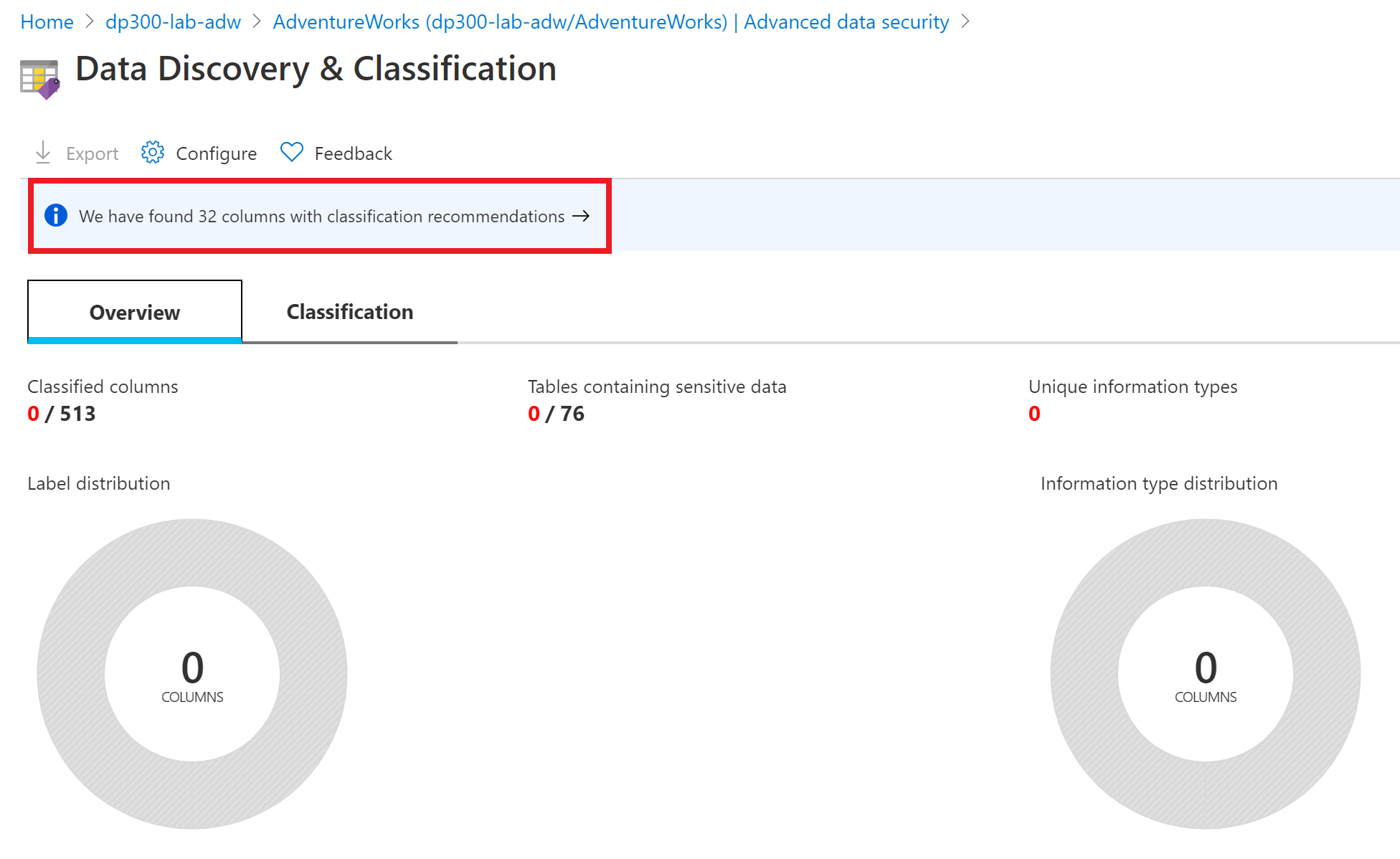
* 1. Navigate to the AdventureWorks database in the Azure portal by scrolling down in the Overview screen for Azure SQL server and clicking on the database name

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-27.png)

* 1. Navigate to the Security section of the main blade for your Azure SQL Database and click on **Data Discovery and Classification**

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-28.png)

On the next screen you will see an informational message that says “We have found 32 columns with classification recommendations”. Click on that link.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-29.png)

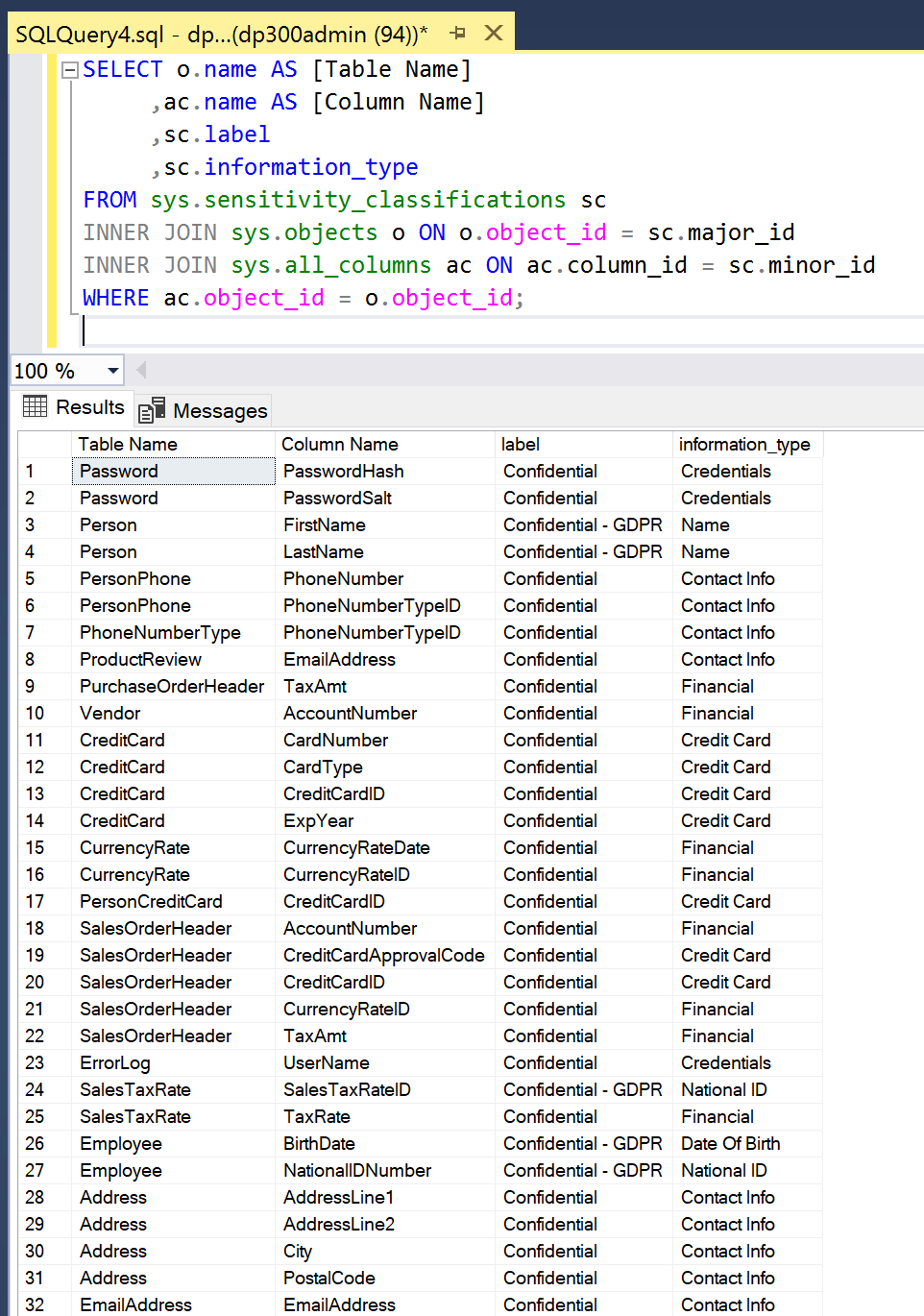
On the next screen. Click the check box next to Select all, and then click “Accepted selected recommendations”.

Click **Save** to save the classifications into the database.

* 1. Go back to SQL Server Management Studio on your VM. Launch a new query window from the AdventureWorks database and execute the following query.

SELECT o.name AS [Table Name]  
  
,ac.name AS [Column Name]  
  
,sc.label  
  
,sc.information\_type  
  
FROM sys.sensitivity\_classifications sc  
  
INNER JOIN sys.objects o ON o.object\_id = sc.major\_id  
  
INNER JOIN sys.all\_columns ac ON ac.column\_id = sc.minor\_id  
  
WHERE ac.object\_id = o.object\_id;

* 1. This query will return the results of your classified columns as shown below.

[](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/images/dp-3300-module-33-lab-31.png)

**Exercise 4: Manage access to database objects**

* 1. In this exercise, you will manage access to the database and its objects. The first thing you will do is create two users in the AdventureWorks database. Open a new query window and copy and paste the following T-SQL into it. Verify that the code has been copied correctly. Execute the query to create the two users.

CREATE USER [DP300User1] WITH PASSWORD = 'Azur3Pa$$'

GO

CREATE USER [DP300User2] WITH PASSWORD = 'Azur3Pa$$'

GO

You will note these users are created in the scope of the database. So if you were to try to login with one of these users, you would need to specify the AdventureWorks database in your connection string.

* 1. Next you will create a custom role and add the users to it. Execute the following T-SQL in the same query window as in step 1.

CREATE ROLE [SalesReader]

GO

ALTER ROLE [SalesReader] ADD MEMBER [DP300User1]

GO

ALTER ROLE [SalesReader] ADD MEMBER [DP300User2]

GO

* 1. Next you will grant permissions to the role. In this case you are assigning SELECT and EXECUTE on the Sales schema. Execute the below T-SQL to grant the permissions to the role.

GRANT SELECT, EXECUTE ON SCHEMA::Sales TO [SalesReader]

GO

* 1. Next you will create a new stored procedure in the Sales schema. You will note this procedure access a table in the Product schema. Execute the below T-SQL in your query window.

CREATE OR ALTER PROCEDURE Sales.DemoProc

AS

SELECT P.Name, Sum(SOD.LineTotal) as TotalSales ,SOH.OrderDate

FROM Production.Product P

INNER JOIN Sales.SalesOrderDetail SOD on SOD.ProductID = P.ProductID

INNER JOIN Sales.SalesOrderHeader SOH on SOH.SalesOrderID = SOD.SalesOrderID

GROUP BY P.Name, SOH.OrderDate

ORDER BY TotalSales DESC

GO

* 1. Next you will use the EXECUTE AS USER command to test out the security you just created. This allows the database engine to execute a query in the context of your user. Execute the below query in your query window.

EXECUTE AS USER = 'DP300User1'

SELECT P.Name, Sum(SOD.LineTotal) as TotalSales ,SOH.OrderDate

FROM Production.Product P

INNER JOIN Sales.SalesOrderDetail SOD on SOD.ProductID = P.ProductID

INNER JOIN Sales.SalesOrderHeader SOH on SOH.SalesOrderID = SOD.SalesOrderID

GROUP BY P.Name, SOH.OrderDate

ORDER BY TotalSales DESC

This query will fail, with an error message saying the SELECT permission was denied on the Production.Product table. The role that user DP300User1 is a member of has SELECT permission in the Sales schema, but not in the Production schema.

However, if you execute the stored procedure in that same context, the query will complete. Execute the following T-SQL.

EXECUTE AS USER = 'DP300User1'

* 1. EXECUTE Sales.DemoProc

This happens because stored procedures take advantage a feature called ownership chaining to provide data access to users who do not have direct permissions to access database objects. For all objects that have the same owner, the database engine only checks the EXECUTE permission on the procedure and not the underlying objects.

**Do not remove any of the resources created in this lab as they will be used in subsequent lab exercises.**

Go

* + © 2020 GitHub, Inc.
  + [Terms](https://github.com/site/terms)
  + [Privacy](https://github.com/site/privacy)
  + [Security](https://github.com/security)
  + [Status](https://githubstatus.com/)
  + [Help](https://docs.github.com/)
  + [Contact GitHub](https://github.com/contact)
  + [Pricing](https://github.com/pricing)
  + [API](https://docs.github.com/)
  + [Training](https://services.github.com/)
  + [Blog](https://github.blog/)
  + [About](https://github.com/about)

You can’t perform that action at this time.

You signed in with another tab or window. Reload to refresh your session. You signed out in another tab or window. Reload to refresh your session.

From <[*https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/Labs/DP-300\_03\_lab.md*](https://github.com/MicrosoftLearning/DP-300T00-Administering-Relational-Databases-on-Azure/blob/master/Instructions/Labs/DP-300_03_lab.md)>