Create an Azure Active Directory Group

Group names:

- DbTestReader
- DbTestOwner

1. Login to the Azure Portal:
    a. Navigate to https://portal.azure.com/ and sign in with your Azure credentials.
2. Navigate to Azure Active Directory:
    a. From the left-hand navigation pane, click on "Azure Active Directory."
3. Select Groups:
    a. Once inside Azure AD, click on "Groups" from the blade's options.
4. Create a New Group:
    a. Click the "+ New group" button located at the top of the page.
5. Fill in Group Details:
    a. Group Type: By default, this will be set to "Security" which is used for assigning access to resources.
    b. Group Name: Provide a name for the group.
    c. Group description: Optionally, you can provide a description for the group.
    d. Membership type: Determine whether members will be assigned directly or if the group will be a dynamic group where members are added based on rules.
    e. If you select "Dynamic User" or "Dynamic Device", you will need to set up rules that determine group membership. This is a powerful feature, but requires more configuration.
6. Add Members (for assigned membership groups):
    a. Click on the "Members" option and then the "Add members" button.
    b. Add one of your colleagues to the group
7. Review and Create:
    a. Once all details have been filled in and you've added any necessary members, click the "Create" button at the bottom.

Create an Azure SQL Server

1. Login to the Azure Portal:
    a. Navigate to https://portal.azure.com/ and sign in with your Azure account credentials.
2. Navigate to Create SQL Server:
    a. Click on "Create a resource" in the top left corner.
    b. In the "Search the Marketplace" box, type "SQL Server" and select "SQL Server (logical server)" from the dropdown.
    c. Click the "Create" button to start the setup process.

3. Basics Tab:
    a. Subscription: Select your Azure subscription.
    b. Resource Group: Choose an existing resource group or create a new one.
    c. Server Name: Provide a unique name for your SQL Server. This name will be used to form the full DNS name of the server in the format: <server-name>.database.windows.net.
    d. Server Admin Login: Specify the server admin username. Avoid using generic names like 'admin' as they might be disallowed for security reasons.
    e. Password: Enter a strong password for the server admin account and confirm it.
    f. Set your account as AAD admin account.
    g. Location: Choose the Azure datacenter location where the server will be hosted.
    h. Version: Typically, you'd select the latest version available, unless you have a specific need for an older version.
4. Networking:
    a. Allow Azure services and resources to access this server: You can choose to allow other Azure services to access this server.
    b. Firewall: By default, all external access to your new SQL server is blocked by the firewall. You can set firewall rules to specify which IP addresses are allowed.
5. Additional Settings:
    a. Advanced Data Security: Decide if you want to enable advanced data security features for your SQL Server.
6. Tags (Optional):
    a. You can associate tags to your resource, which are name-value pairs. They can help you categorize and manage resources in your Azure environment.
7. Review + Create:
    a. Review your server configuration details.
    b. Click the "Review + create" tab to finalize your choices. Azure will validate your configuration.
    c. Once validation passes, click the "Create" button to start the deployment process.

Create an Azure SQL Database

1. Login to the Azure Portal:
    a. Navigate to https://portal.azure.com/ and sign in with your Azure credentials.
2. Navigate to SQL Databases:
    a. Click on "Create a resource" in the top left corner.
    b. In the "Search the Marketplace" box, type "SQL Database" and select it from the dropdown.
    c. On the SQL Database page, click the "Create" button.
3. Basic Settings:
    a. Subscription: Select your Azure subscription.
    b. Resource Group: Choose an existing resource group or create a new one.

    c. Database Name: Enter a name for your SQL Database.
    d. Server: Either select an existing server or create a new one. If creating a new server, you'll need to provide server details, including server name, server admin login, password, and location.
    e. Want to use SQL elastic pool?: Decide whether you want your database to be part of an elastic pool. If yes, you can select or create an elastic pool here.
    f. Compute + storage: Configure the performance tier, data max size, and other configurations based on your requirements.
4. Additional Settings:
    a. Data Source: Choose if you want to start with an empty database, restore from a backup, or use sample data.
    b. Collation: This defines the rules that determine how data is sorted and compared. Choose the appropriate collation if you have specific requirements; otherwise, you can leave the default.
    c. Advanced Data Security: Decide if you want to enable advanced data security features for your database.
5. Review + Create:
    a. Azure will validate your configuration. Once validation passes, click the "Review + create" tab to review your database settings.
    b. After reviewing, click the "Create" button to start the deployment of your SQL Database.
6. Access and Manage:
    a. Once deployment is successful, navigate to the "SQL databases" section in the Azure Portal. You should see your newly created database listed there.
    b. Click on the database to manage, monitor, and perform other operations.
7. Set up Firewalls and Virtual Networks:
    a. To access your SQL database, you might need to configure firewall rules. This can be done from the "Firewalls and virtual networks" option in the database settings. Here you can add your client IP to allow connections.

Connect Azure Data Studio to an Azure SQL Database with AAD

1. Open Azure Data Studio:
    a. Launch Azure Data Studio on your computer.
2. Create a New Connection:
    a. Click on the New Connection icon (or you can find this option in the File menu).
3. Fill in Connection Details:
    a. Server: Enter the full name of your Azure SQL server, which typically looks like yourservername.database.windows.net.
    b. Authentication type: Choose Azure Active Directory from the dropdown. You'll see several AAD authentication methods, such as:
        i. Azure Active Directory - Universal with MFA
        ii. Azure Active Directory - Password

iii. Azure Active Directory - Integrated

c. Choose the one that best matches your requirements.
d. Username: Enter your AAD account email (for AAD Password and AAD Universal with MFA methods).
e. Password: Enter your AAD account password if you're using the AAD Password method.

4. Select Database:
    a. From the Database dropdown, select the specific Azure SQL database you want to connect to. You can also leave it as <Default> to connect to the server without selecting a specific database initially.
5. Advanced Properties (Optional):
    a. You can click on the Advanced button to configure other connection properties if necessary.
6. Initiate the Connection:
    a. Click the Connect button.
7. MFA Users:
    a. If you've chosen the Azure Active Directory - Universal with MFA option, you might be prompted to authenticate using multi-factor authentication. Follow the prompts to complete the authentication process.

Create the table

1. Runt the following query

```
CREATE TABLE Employees (
    EmployeeID INT PRIMARY KEY IDENTITY(1,1),
    FirstName NVARCHAR(50),
    LastName NVARCHAR(50),
    Position NVARCHAR(50)
);
```

2. Populate the table with dummy data:

```
INSERT INTO Employees (FirstName, LastName, Position) VALUES
('John', 'Doe', 'Manager'),
('Jane', 'Smith', 'Assistant'),
('Alice', 'Johnson', 'Engineer'),
('Bob', 'Williams', 'Developer'),
('Charlie', 'Brown', 'Designer');
```

3. View the inserted data

```
SELECT * FROM Employees;
```

Create a User in Azure SQL Database for a Service Principal

1. Open Azure Data Studio.
2. Connect to your Azure SQL Database server using your admin account.
3. Execute the following T-SQL commands in Azure Data Studio:

```
-- Use your target database
USE YourDatabaseName;
GO

-- Create a user for the service principal
CREATE USER [your-service-principal-name] FROM EXTERNAL PROVIDER;
GO
```

4. Assign Permissions to the Service Principal (Reader DB Group):

```
-- Grant the service principal read access
EXEC sp_addrolemember 'db_datareader', 'your-service-principal-name';
GO
```

Create a User in Azure SQL Database for a Service Principal using PowerShell

1. Navigate to Lab2.
    a. Open and inspect the file named addIdentityToDb.ps1.
    b. Ensure you understand the various parameters and their roles in the script.
2. Set Script Parameters:
    a. Fill in the following required parameters:
        i. tenantId: The ID of your Azure tenant.
        ii. sqlServerName: Name of your SQL Server.
        iii. sqlDatabaseName: Name of your SQL Database.
        iv. miName: Set this to the name of the owner group you created in the first exercise.
3. Authenticate to your Azure Tenant:

```
Connect-AzAccount -Tenant "your_tenantId_here"
```

   a. Note: Replace your_tenantId_here with the actual tenantId.
4. Execute the Script:
   a. In the PowerShell console, run:

```
./addIdentityToDb.ps1
```

5. Test the Configuration:
   a. Ask a colleague to connect to the database using their Azure Active Directory (AAD) account.
6. Verify that they can access the database and have the correct permissions.