1. **How to connect Azure Databricks to ADLS using service principle**

Go to Microsoft Entra ID (previously ActiveDirectory or AzureActiveDirectory)

Go to Manage->App Registrations->NewRegistrations

A screenshot of a computer

AI-generated content may be incorrect.

Provide name and save it. Now open that ID

A screenshot of a computer application

AI-generated content may be incorrect.

Copy App Id and Tenant ID.

A close-up of a flag

AI-generated content may be incorrect.

Go to certificated and secrets, create one

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Quickly Copy the value

A yellow circle with black text

AI-generated content may be incorrect.

Go to your datalake->IAM

Add role assignment, choose Storage Blob Data Contributor and assign it to Service Principle that you created.

A screenshot of a computer

AI-generated content may be incorrect.

Go to Databricks notebook, copy the below python code and replace 3 keys which had copied earlier.

.**{config['storage\_account'**]}= Storage name

**dbutils.secrets.get(scope="sslscope", key="ssl-client-id")**)= clientid

/**{dbutils.secrets.get(scope='sslscope', key='ssl-tenant-id')}**= tenanted

**dbutils.secrets.get(scope="sslscope", key="ssl-client-secret")**)= secret

-----------------------------------------------------------------------------------------------------------

spark.conf.set(f"fs.azure.account.auth.type.**{config['storage\_account']}**.dfs.core.windows.net", "OAuth")

spark.conf.set(f"fs.azure.account.oauth.provider.type.**{config['storage\_account']}**.dfs.core.windows.net", "org.apache.hadoop.fs.azurebfs.oauth2.ClientCredsTokenProvider")

spark.conf.set(f"fs.azure.account.oauth2.client.id.**{config['storage\_account']}**.dfs.core.windows.net", **dbutils.secrets.get(scope="sslscope", key="ssl-client-id")**)

spark.conf.set(f"fs.azure.account.oauth2.client.secret.**{config['storage\_account']}**.dfs.core.windows.net", **dbutils.secrets.get(scope="sslscope", key="ssl-client-secret")**)

spark.conf.set(f"fs.azure.account.oauth2.client.endpoint.**{config['storage\_account']}**.dfs.core.windows.net", f"https://login.microsoftonline.com/**{dbutils.secrets.get(scope='sslscope', key='ssl-tenant-id')}**/oauth2/token")

A close-up of a computer screen

AI-generated content may be incorrect.

Check using dbutils



1. **How to use Azure Key Vault in Azure Databricks**

Create Key vault.

Go to Key vault IAM->Add role assignment.

Click Key vault Admininstrator and assign it to your email ID to create secrets.

A screenshot of a computer

AI-generated content may be incorrect.

Go to Secrets and add your key values.

A screenshot of a computer

AI-generated content may be incorrect.

Now to link your databricks account to your secrets by creating secret scope

Go to databricks home page and copy its URL

A screenshot of a computer

AI-generated content may be incorrect.

Paste in web and extend it

[https://adb-519392701677842.2.azuredatabricks.net**#secrets/createScope**](https://adb-519392701677842.2.azuredatabricks.net#secrets/createScope)

A screenshot of a computer

AI-generated content may be incorrect.

Enter scope name and go to key vault->properties, copy paste below and create.

Vault URL is DNS Name

Resource ID is Resource ID

A screenshot of a computer

AI-generated content may be incorrect.

Now, go to Databricks and access those secrets.

A close-up of a computer screen

AI-generated content may be incorrect.

1. **How to connect Synapse with ADLS .**

By default, Synapse has System-assigned managed identity so just assign Storage Blob Contributor Role to that Identity.

Go to ADLS->IAM

Add assign Storage Blob Contributor Role to the system created Managed Identity.

A white background with black text

AI-generated content may be incorrect.