Supply Chain Analytics

Instructions Manual

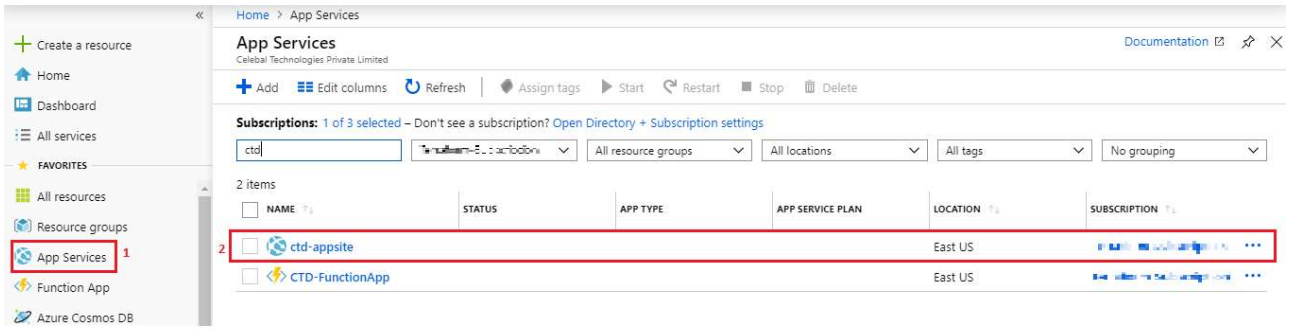
Version 1.0

Contents

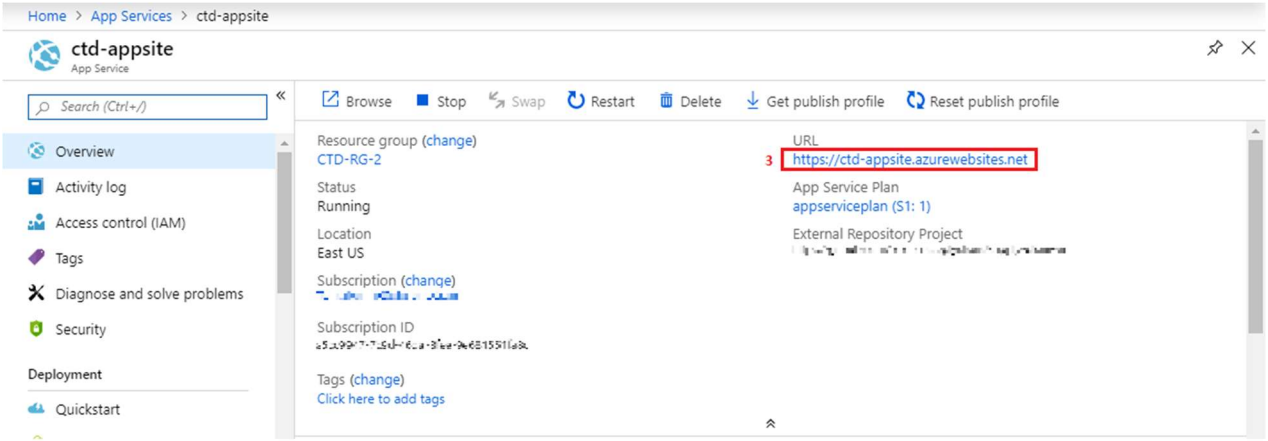
Azure App Service (URL)

Step 1: Log in to the Azure portal

Step 2: From the blade, select **App Services** then select the web app that was deployed from Azure Marketplace

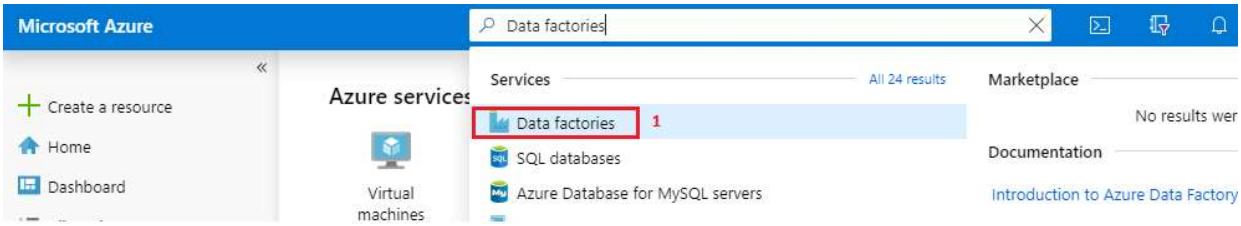


Step 3: Select the web app and copy the URL

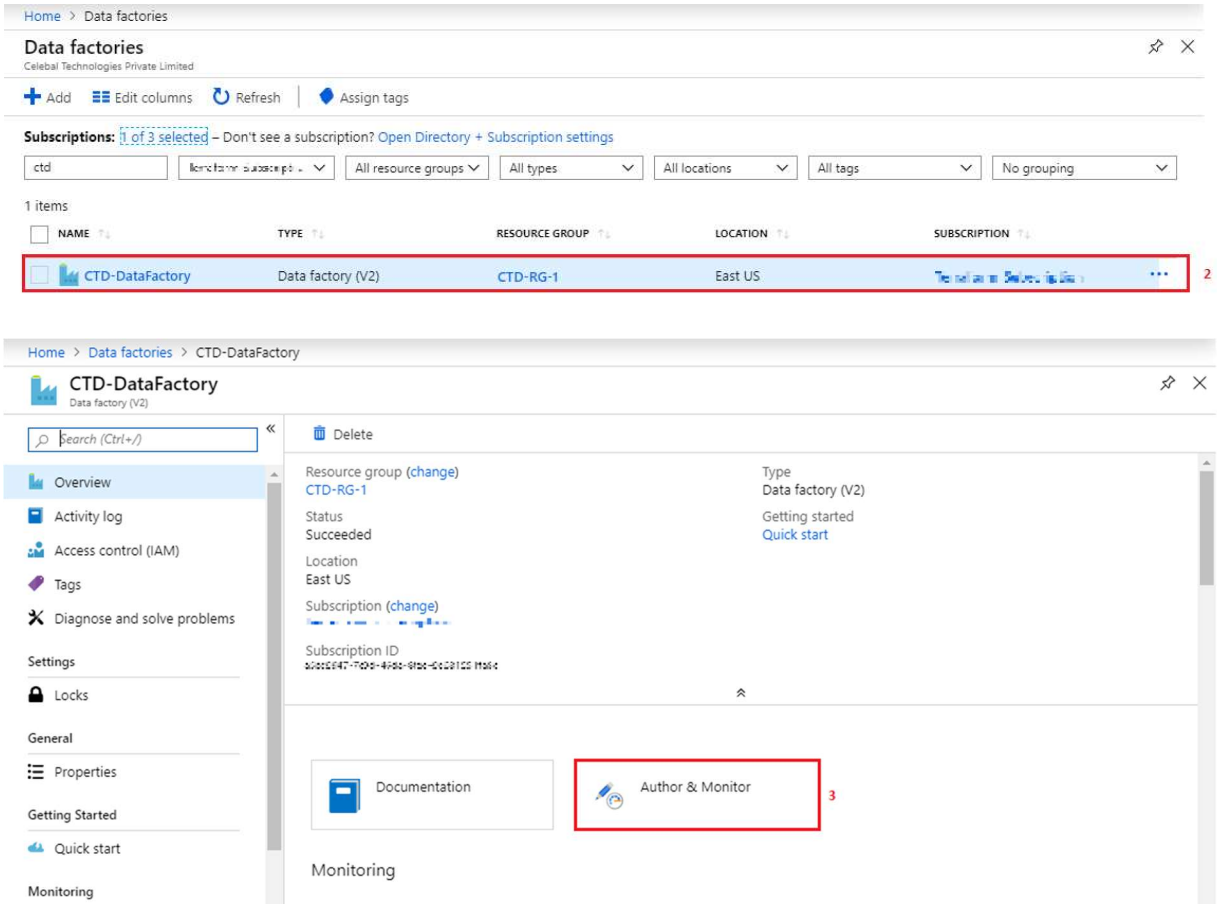


Azure Data Factory

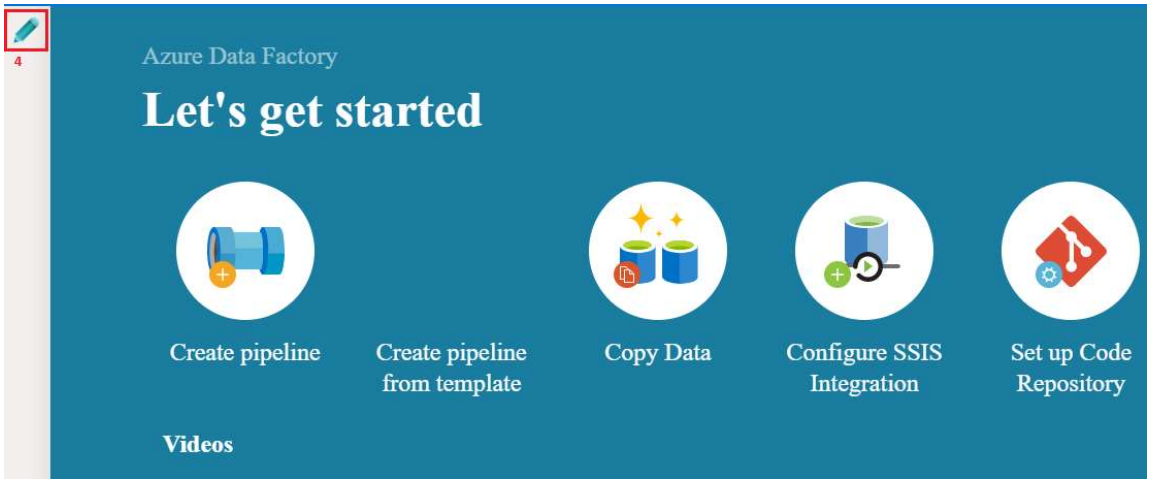
Step 1: Select **Data factories** option



Step 2: Select Data Factory and click on ‘Author and Monitor’



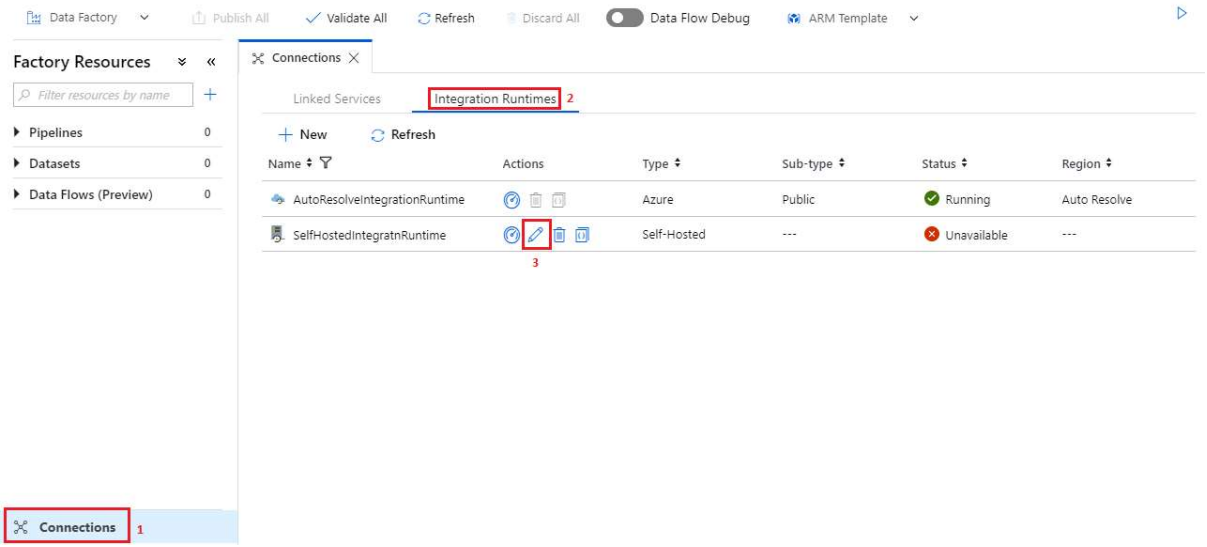
Step 3: Another blade will open, click on the pipeline symbol



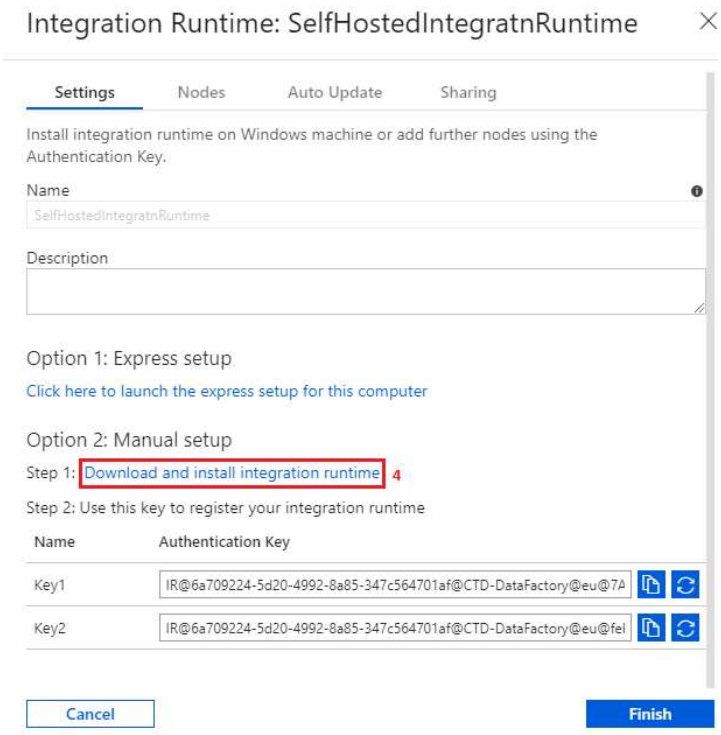
How to download and install Integration Runtimes for Data Factory (For SAP and Oracle)

Step 1: Select Connections option from the Factory Resources blade

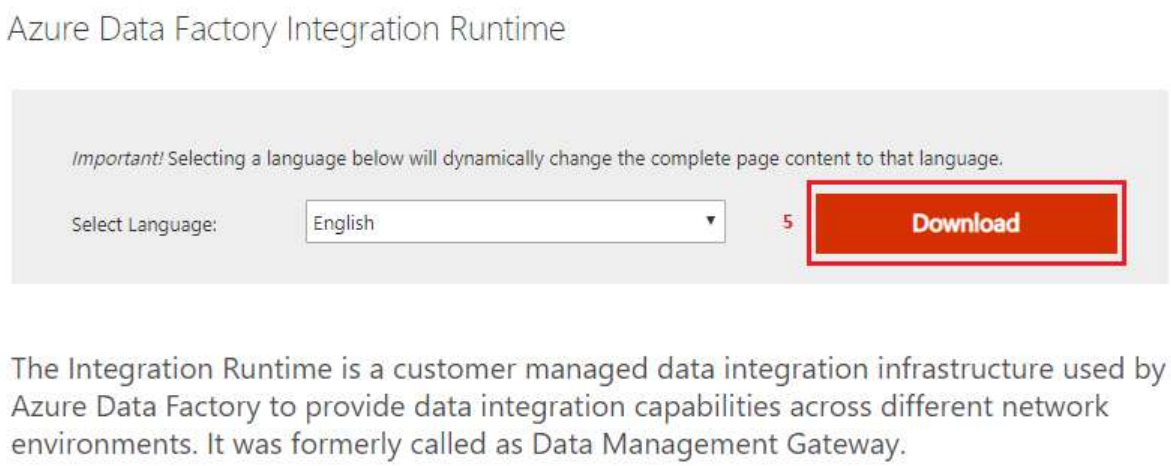
Step 2: Select Integration Runtimes, edit the one which is unavailable



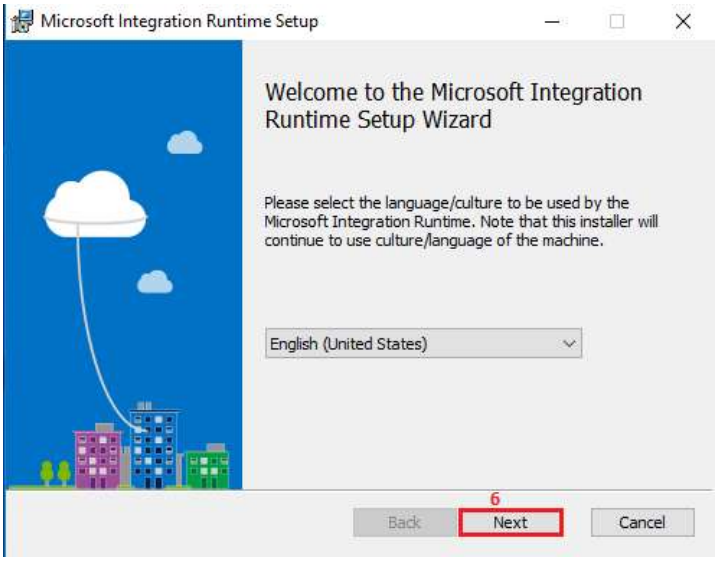
Step 3: Click on 'Download and install integration runtime' option

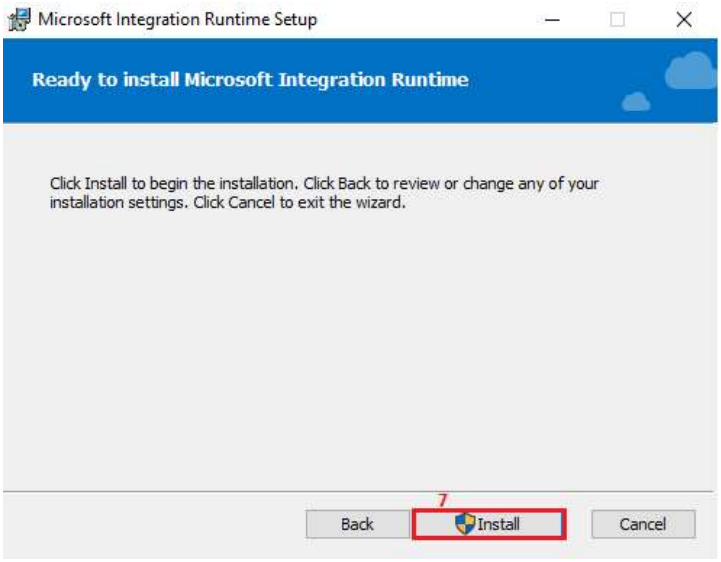


Step 4: Click on Download

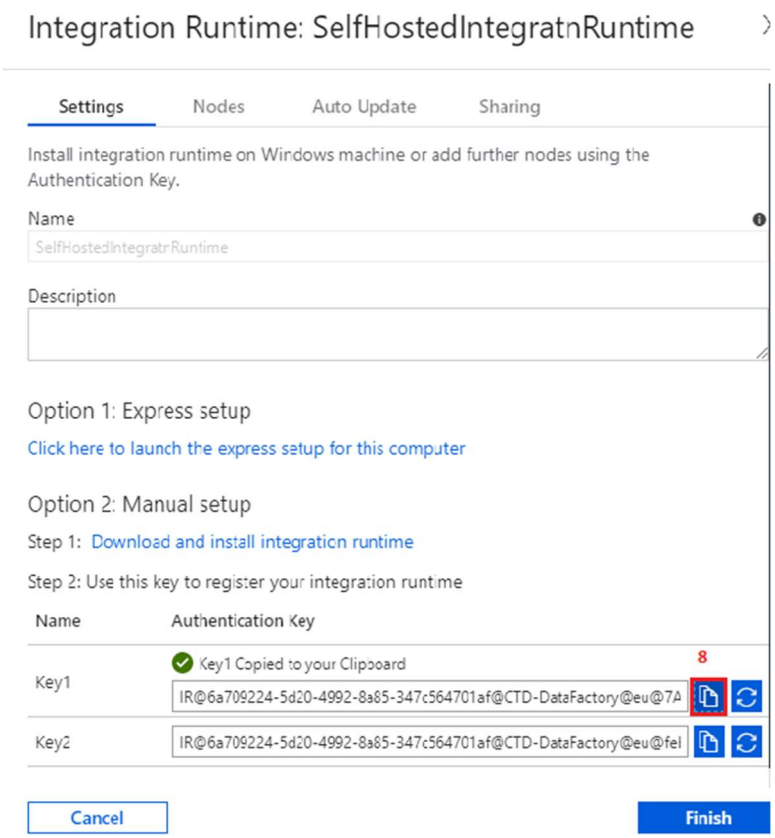


Step 5: Once it gets download, open the setup and install Integration Runtime

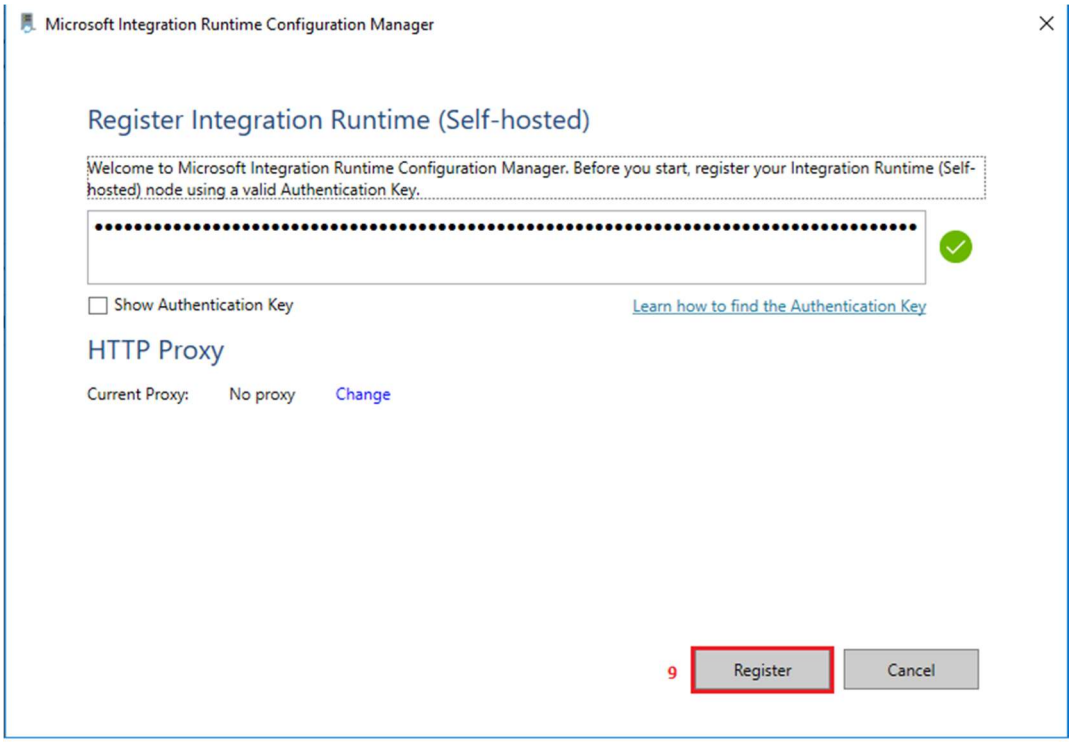




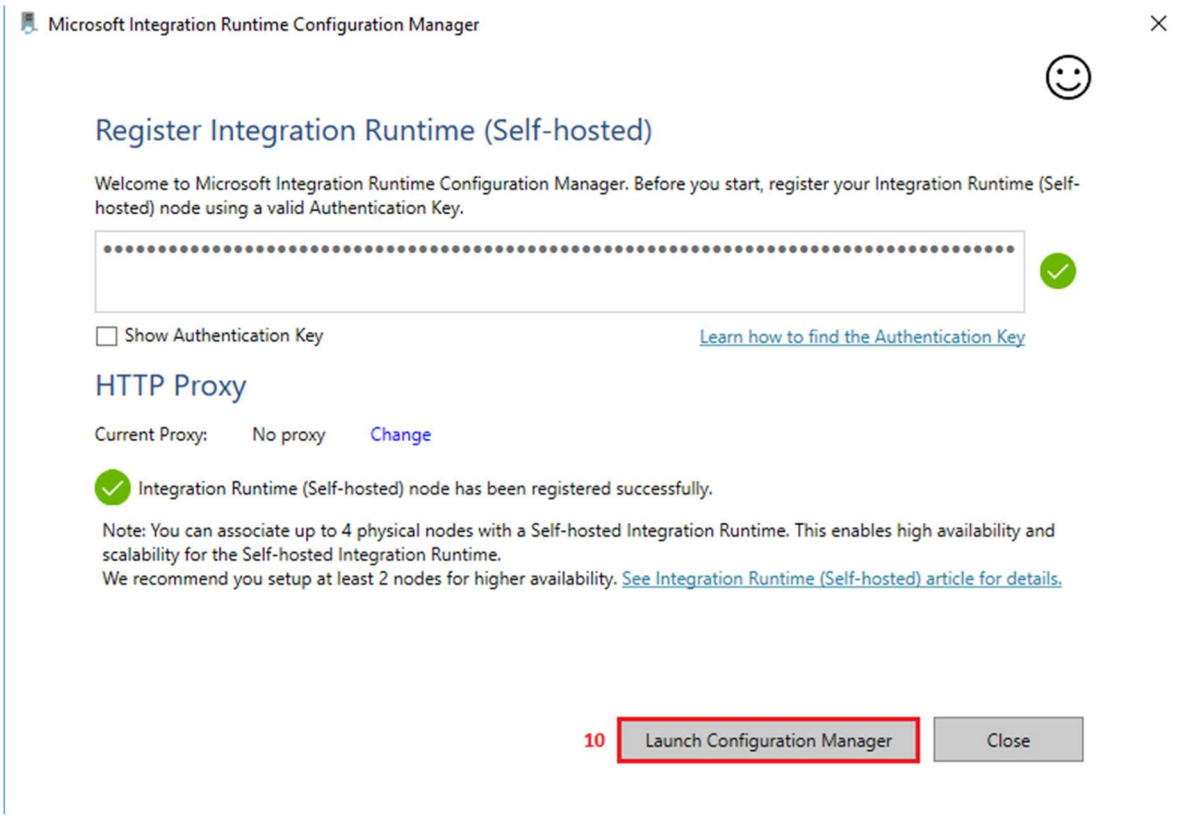
Step 6: Once setup gets installed, copy the 'Authentication Key' from Integration Runtime wizard shown above



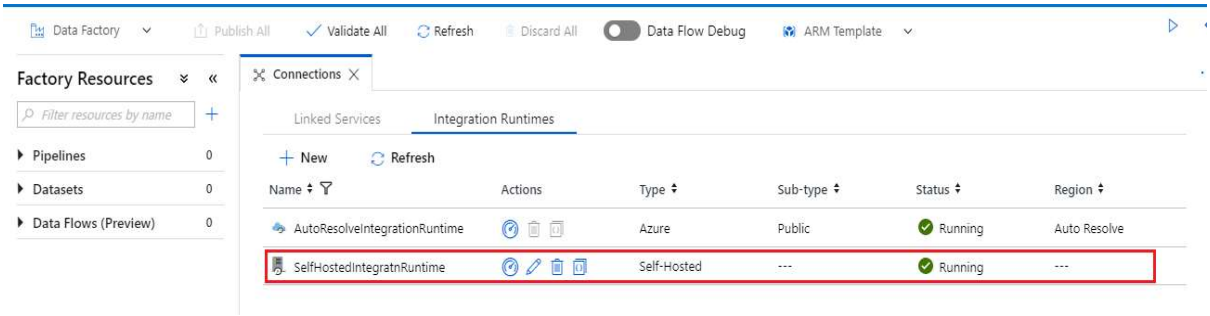
Step 7: Paste the key and click on Register



Step 8: It will detect the Integration Runtime environment, click on 'launch configuration manager'

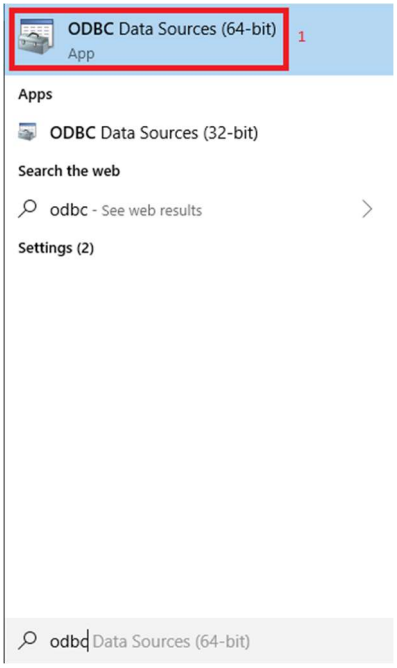


Step 9: You have successfully installed Integration Runtime for Data Factory, visit the Integration Runtimes wizard and check that the status is now running

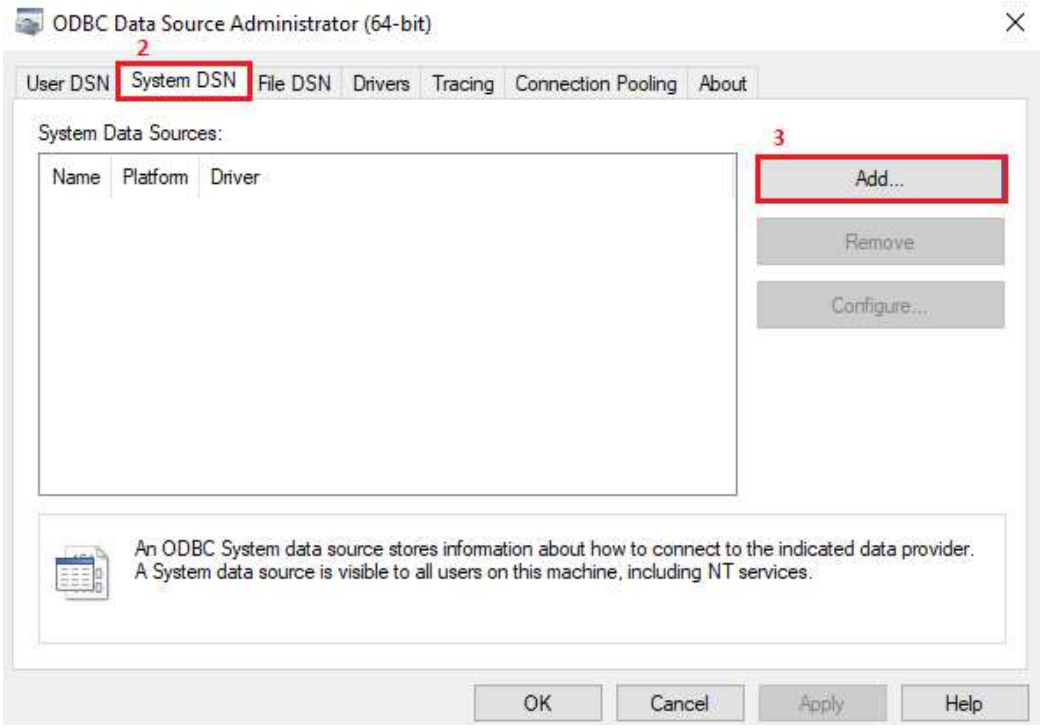


How to add HDBODBC Driver for SAP HANA

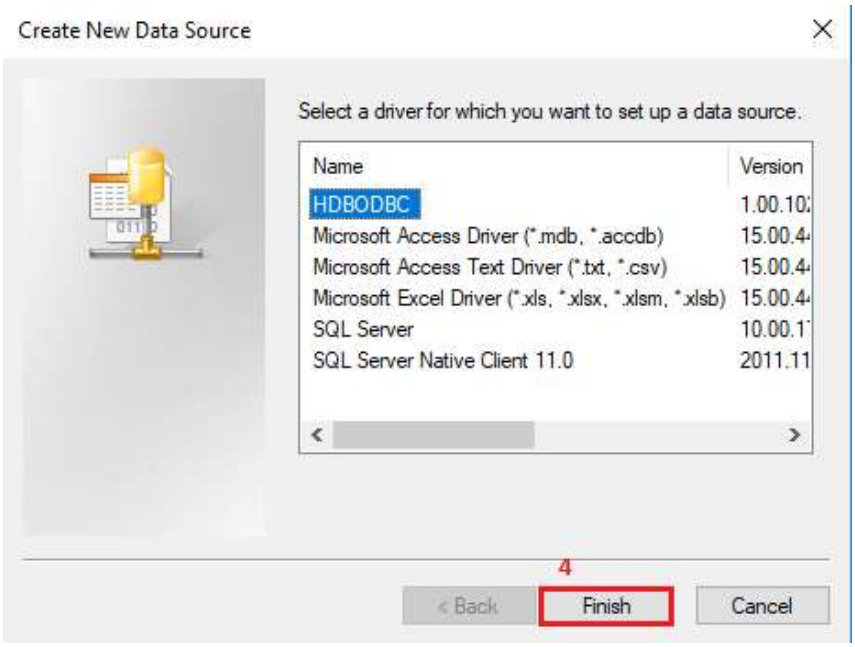
Step 1: Install SAP Client for HDBODBC Driver, open the ODBC Data Sources



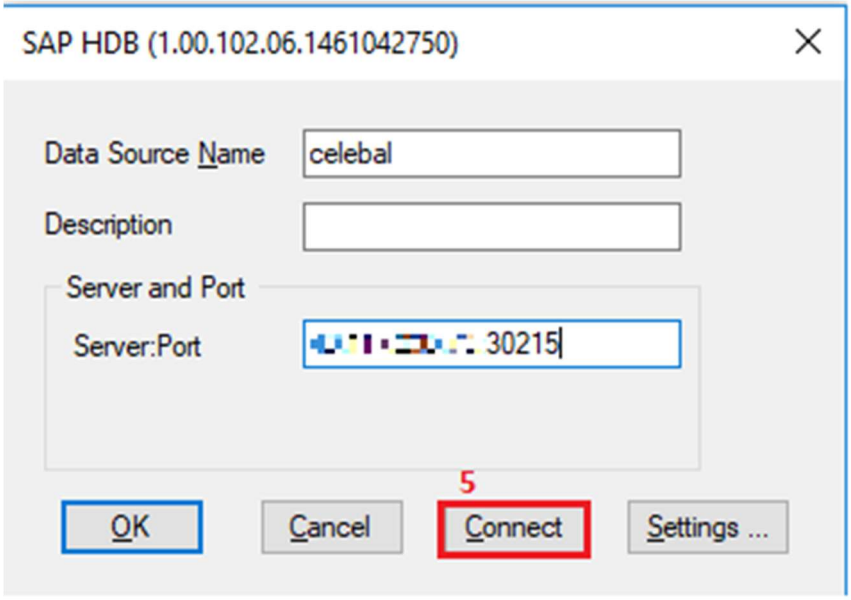
Step 2: Select 'System DSN' then click on Add



Step 3: Select HDBODBC and hit Finish



Step 4: Provide the Data Source Name and Server: port then click on connect

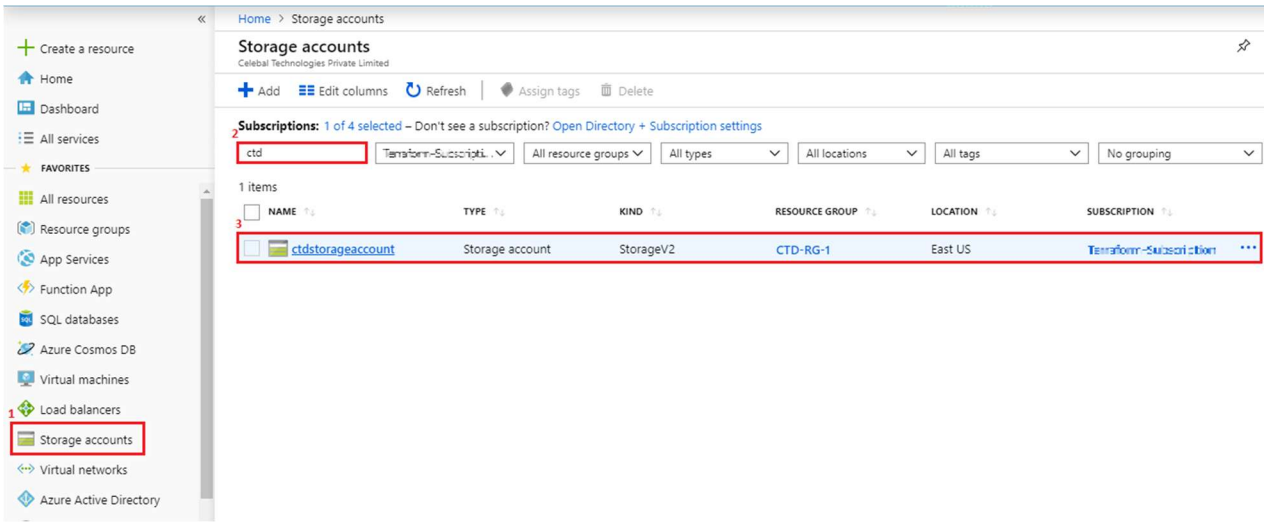


After this step another prompt will open, provide user and password then click on OK this will add HDBODBC Driver.

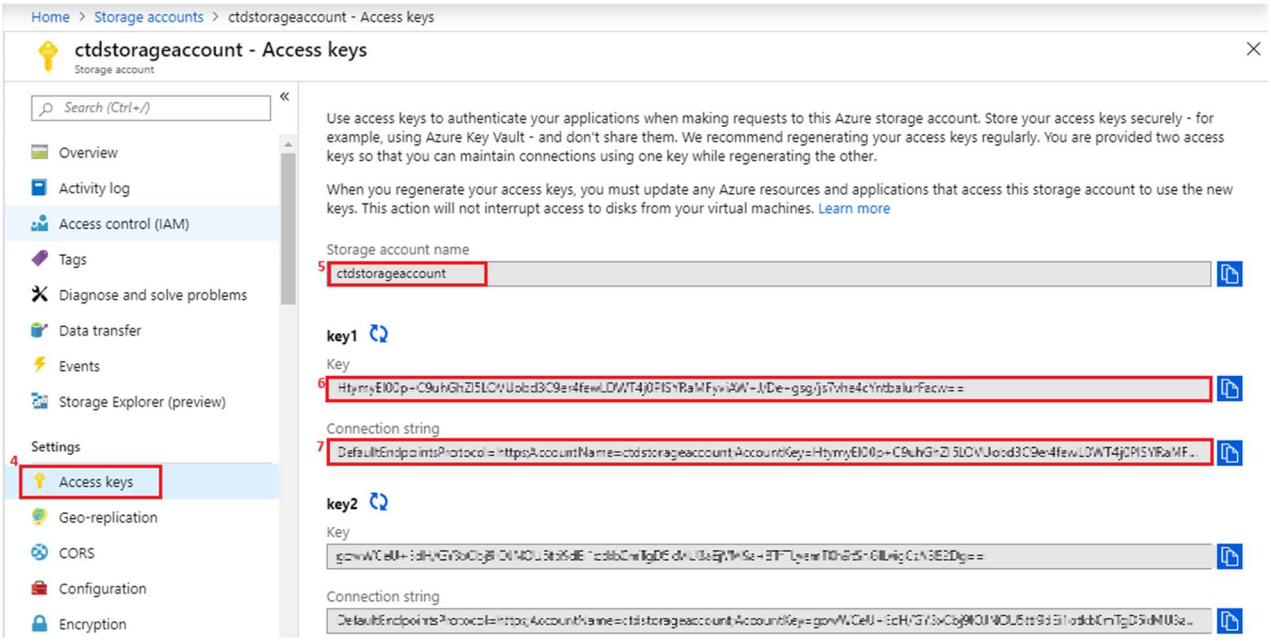
Azure Storage Account (Access Keys) and (Connection Strings)

Step 1: Log in to the Azure portal

Step 2: Select **Storage Accounts** from Blade, then select the Deployed Storage Account



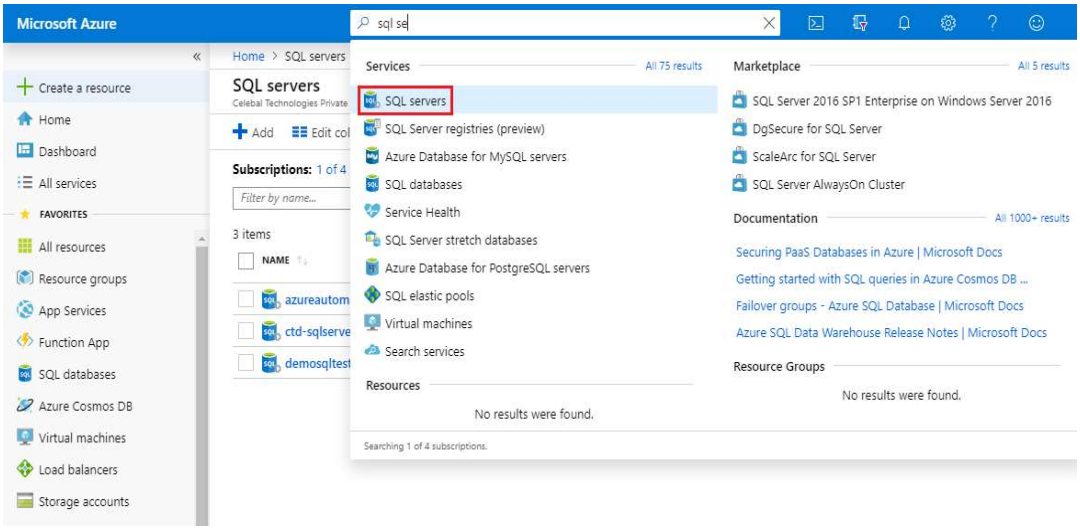
Step 3: Select **Access Keys** from blade then copy the Storage Account Name, Keys and Connection String for future reference



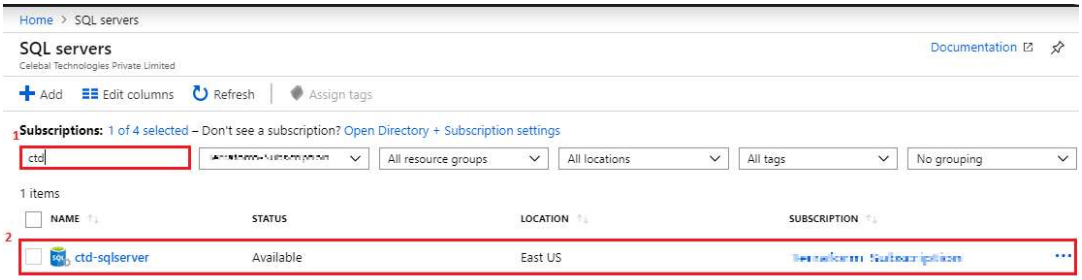
Azure SQL Server and Database (Connection Strings)

Step 1: Log in to the Azure portal

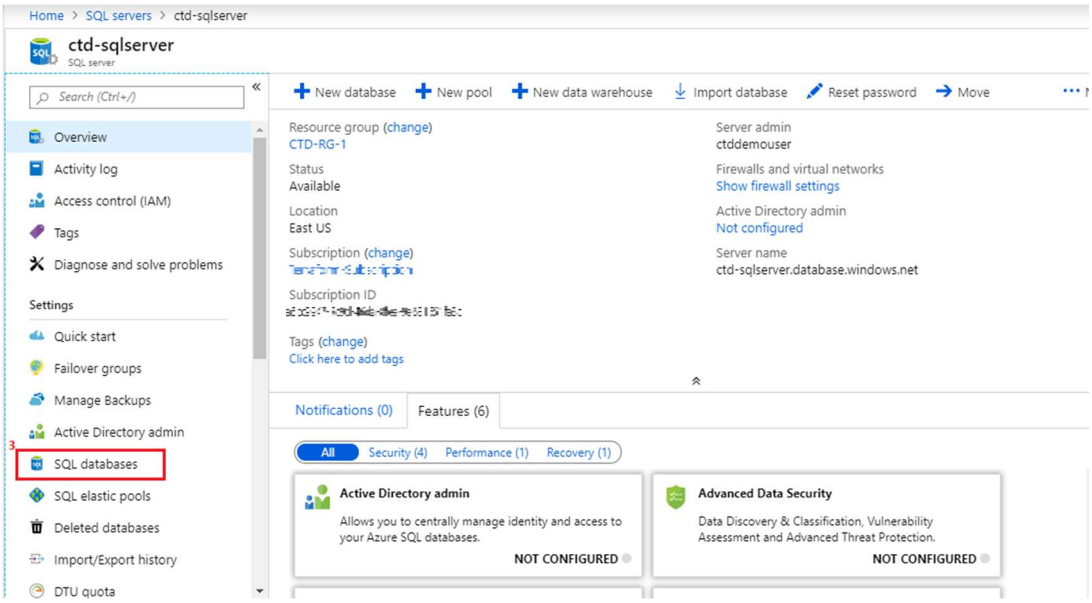
Step 2: Select **SQL Servers** from search tab



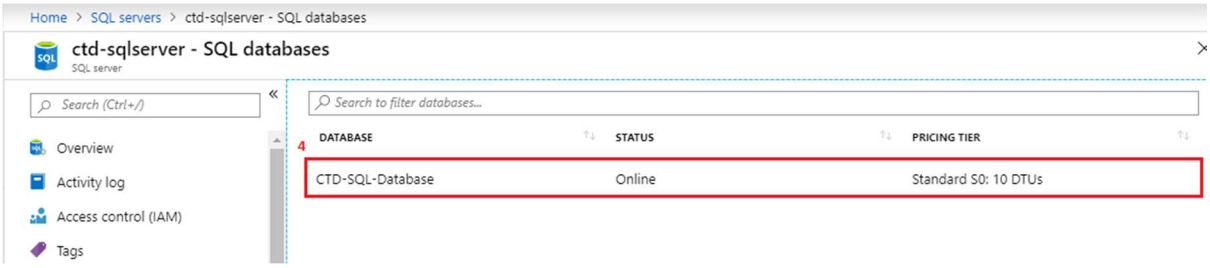
Step 3: Select the **SQL Server**



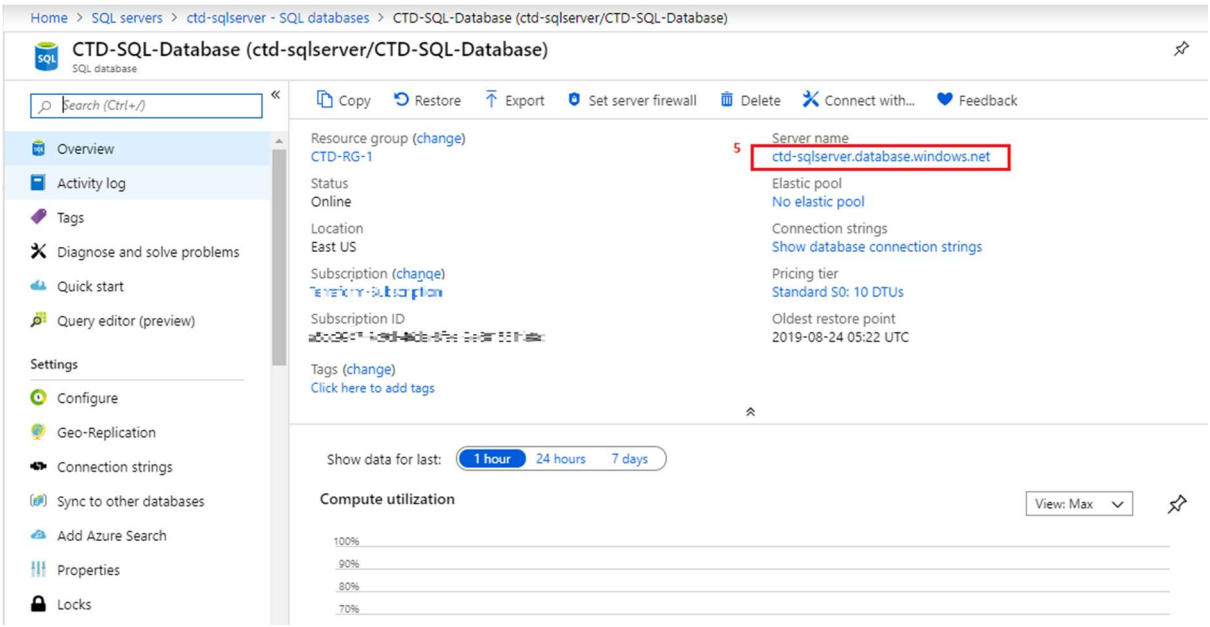
Step 4: Select **SQL Database** from the blade



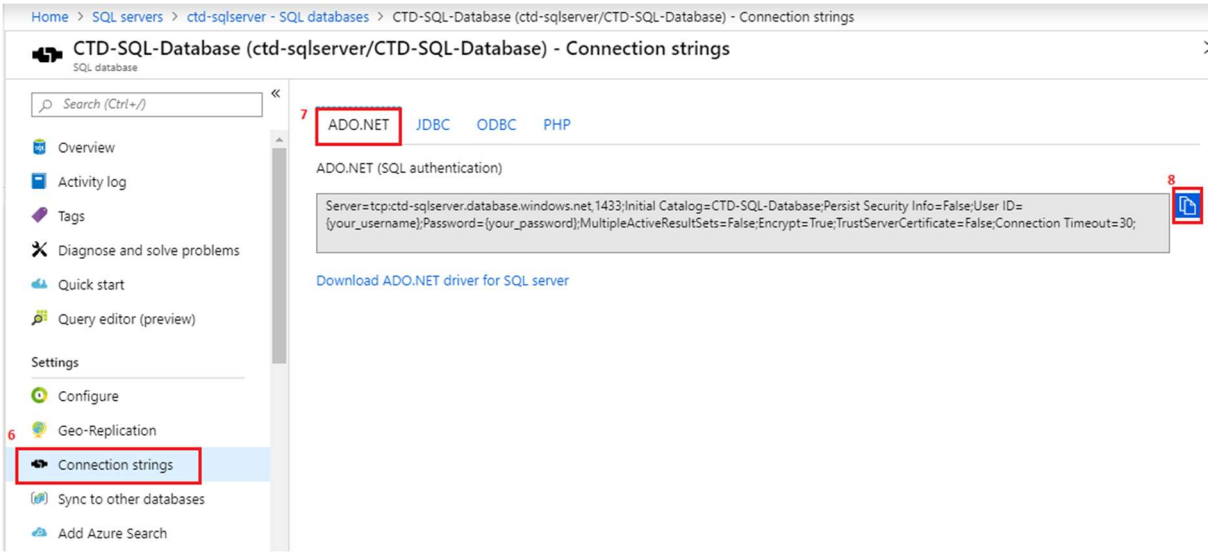
Step 5: Copy **Database Name**



Step 6: Copy Server name for future reference then Select **Connection Strings** s



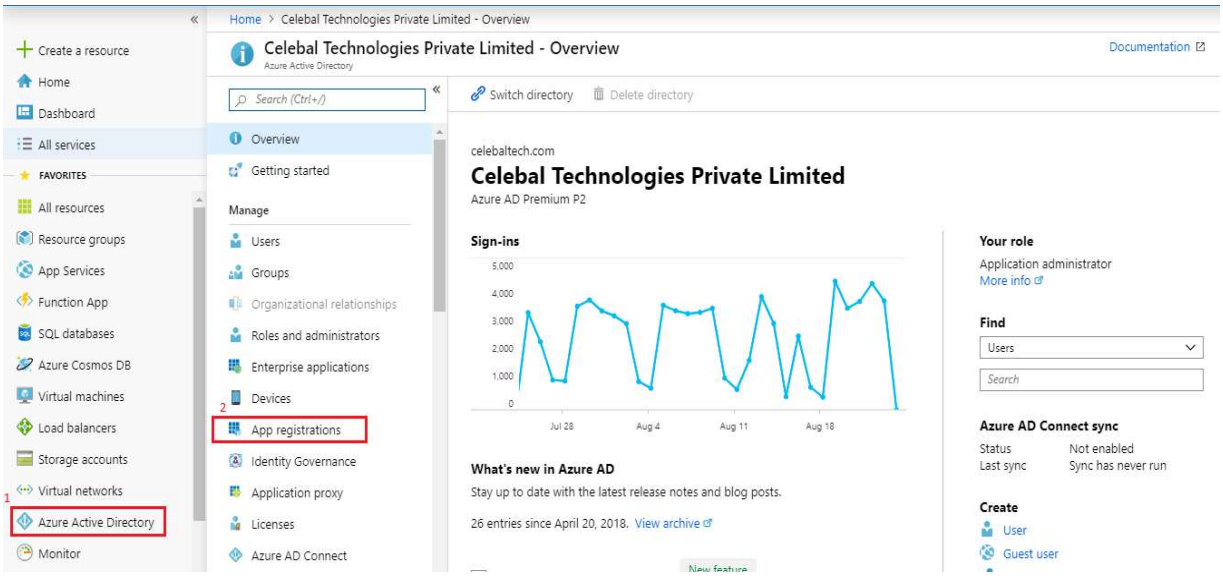
Step 7: Copy Connection String, then provide username in place of {your username} and password in place of {your password}



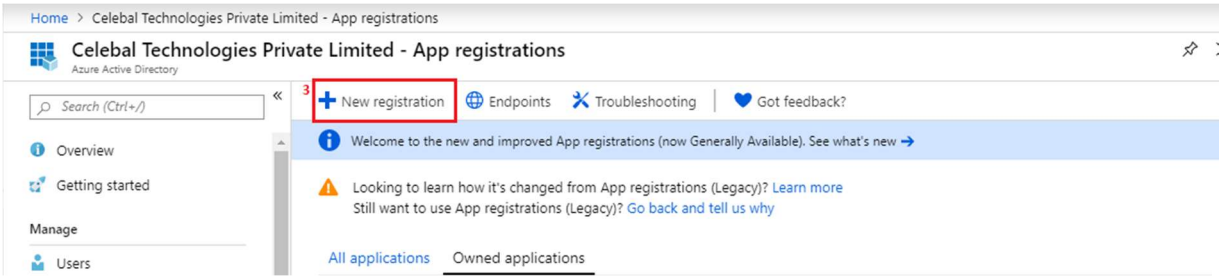
App Registrations (Azure Active Directory)

Step 1: Log in to the Azure portal.

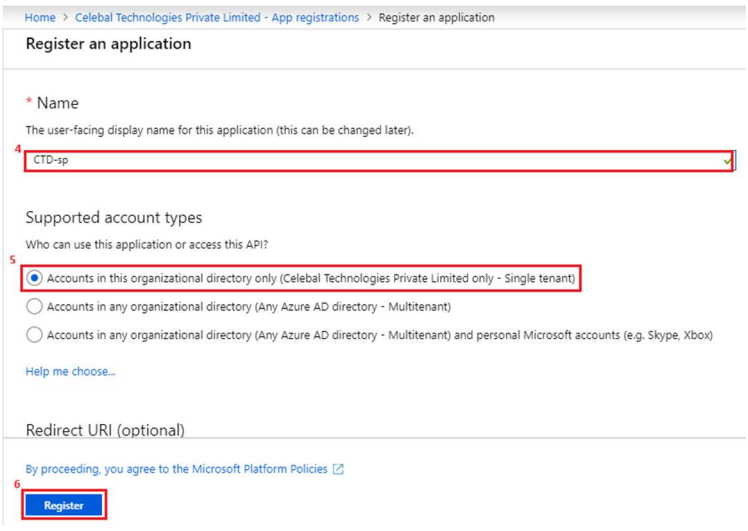
Step 2: Select **Azure Active Directory** then select 'App registrations'



Step 3: Register a new Application by clicking on **New Registration**

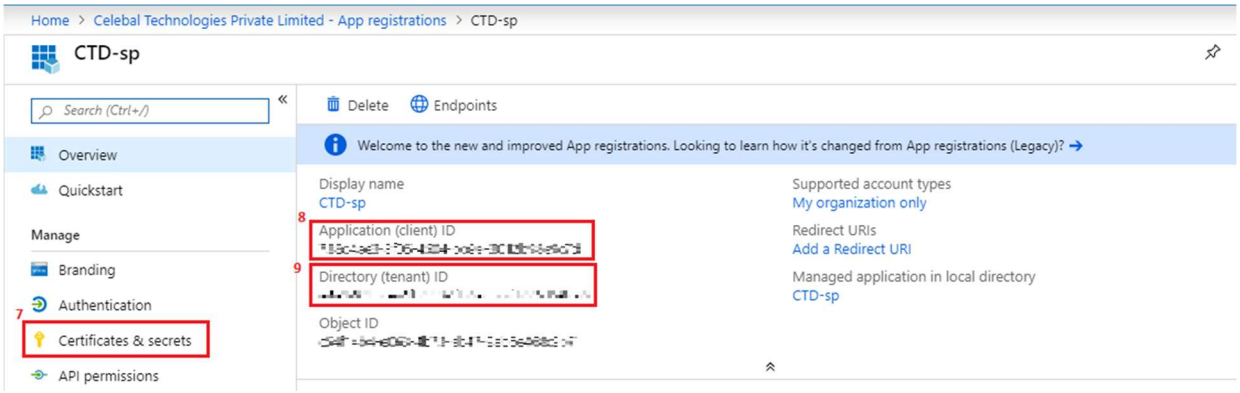


Step 4: Enter Application Name and **register** the Application.

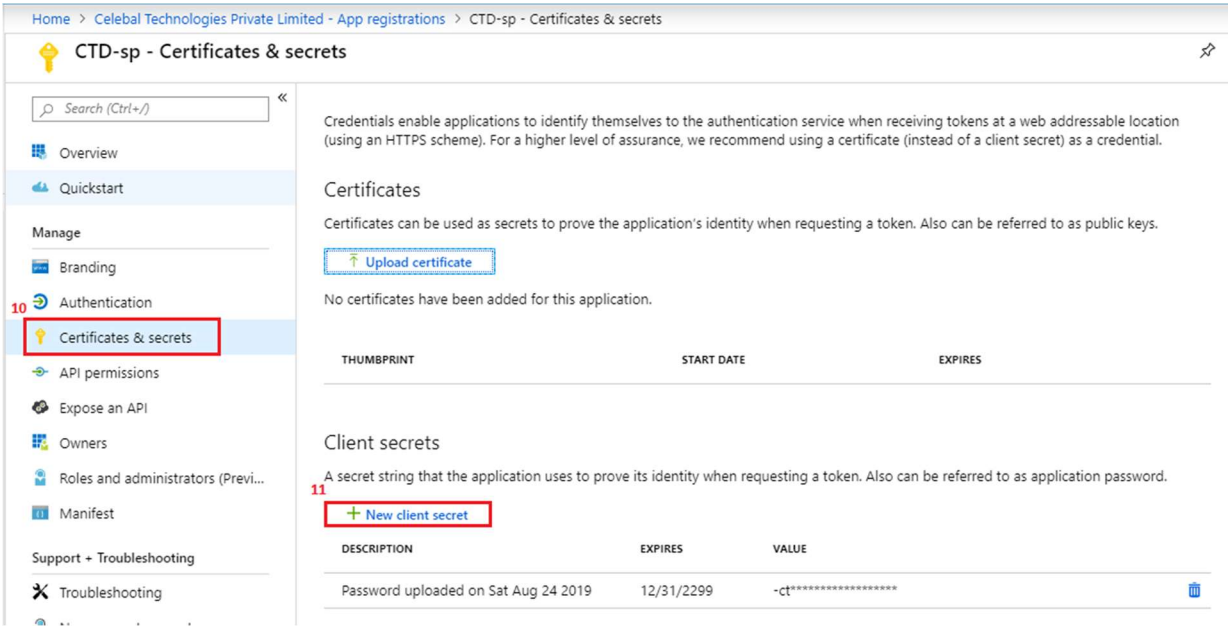


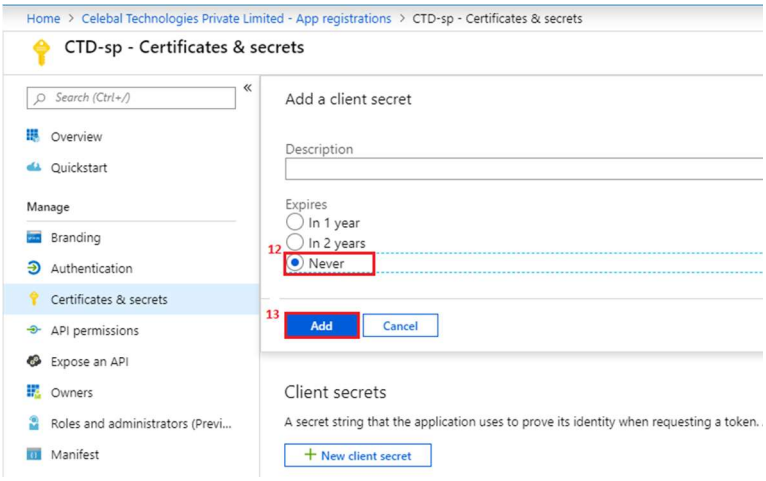
Step 5: New application is registered successfully, copy **Client ID** and **Tenant ID**.

Step 6: To fetch client secret Select **Certificates & Secrets**



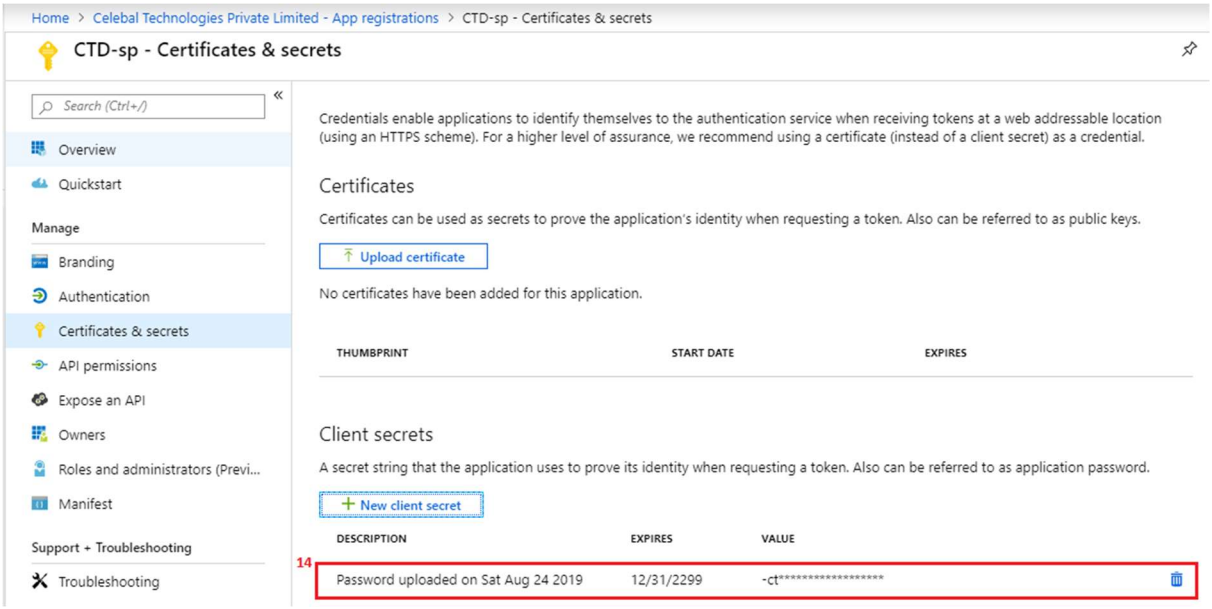
Step 7: Select New client secret option



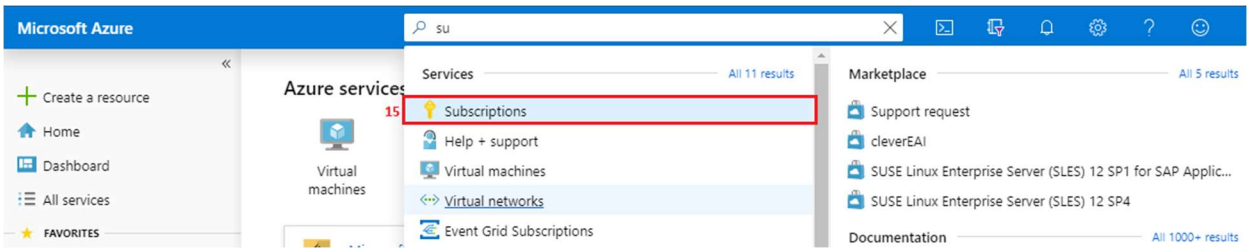


Step 8: Copy the client secret for future reference

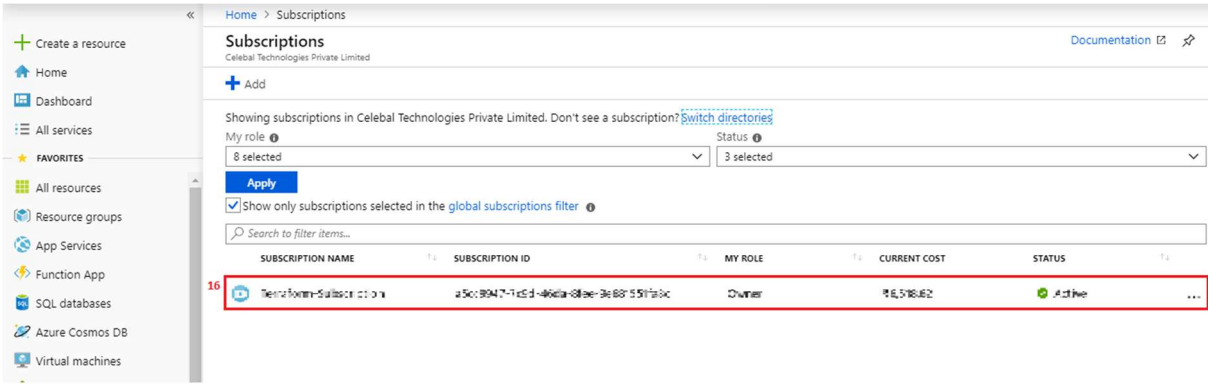
Note -: This client secret can only be seen for once so copy it for future reference or else you will have to regenerate it



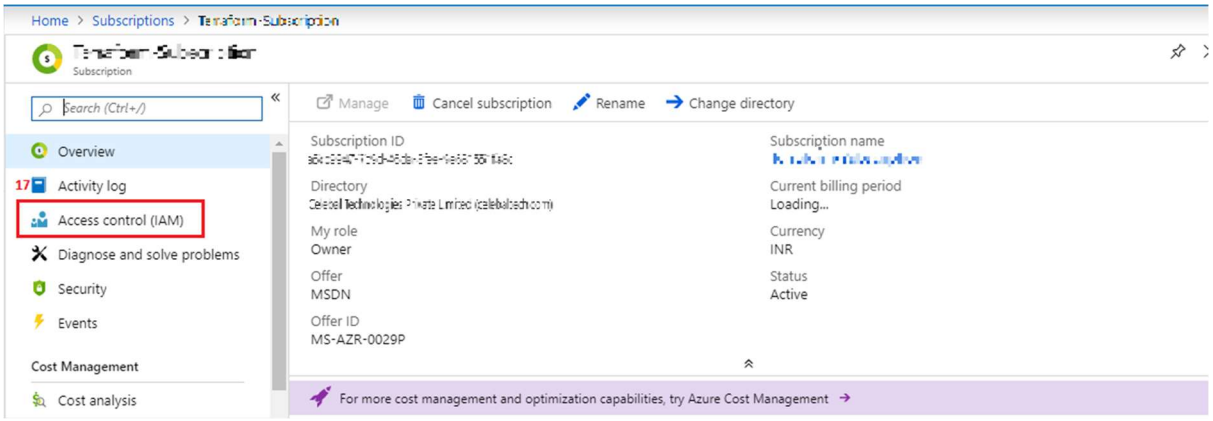
Step 9: To fetch Subscription ID, select the **Subscriptions** from Search tab



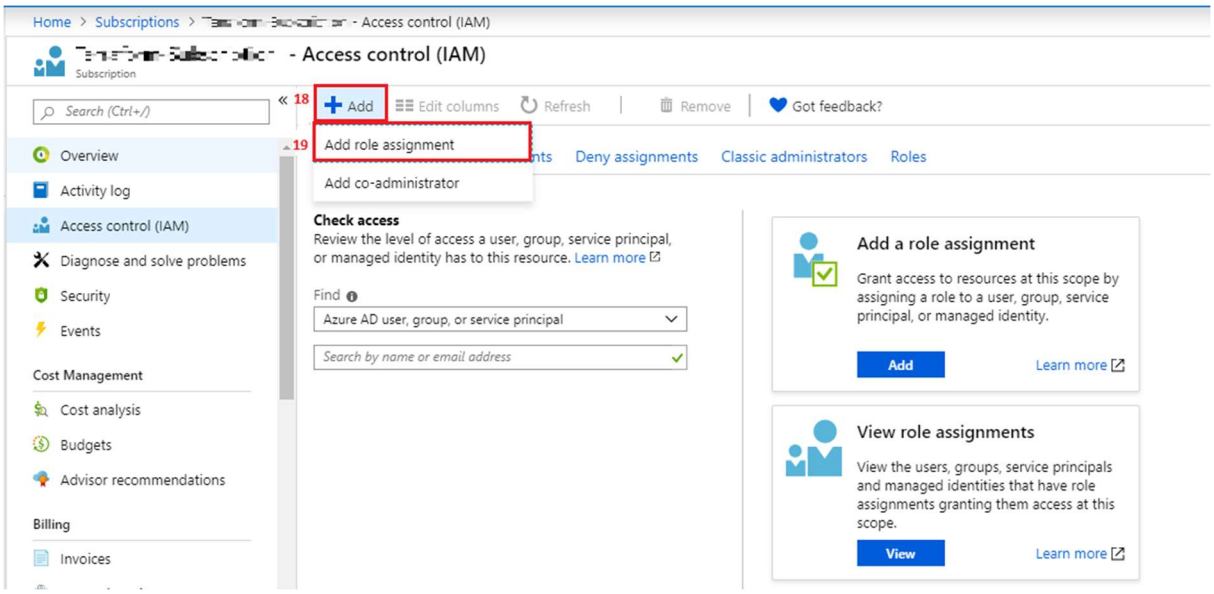
Step 10: Copy **Subscription Id** of your subscription



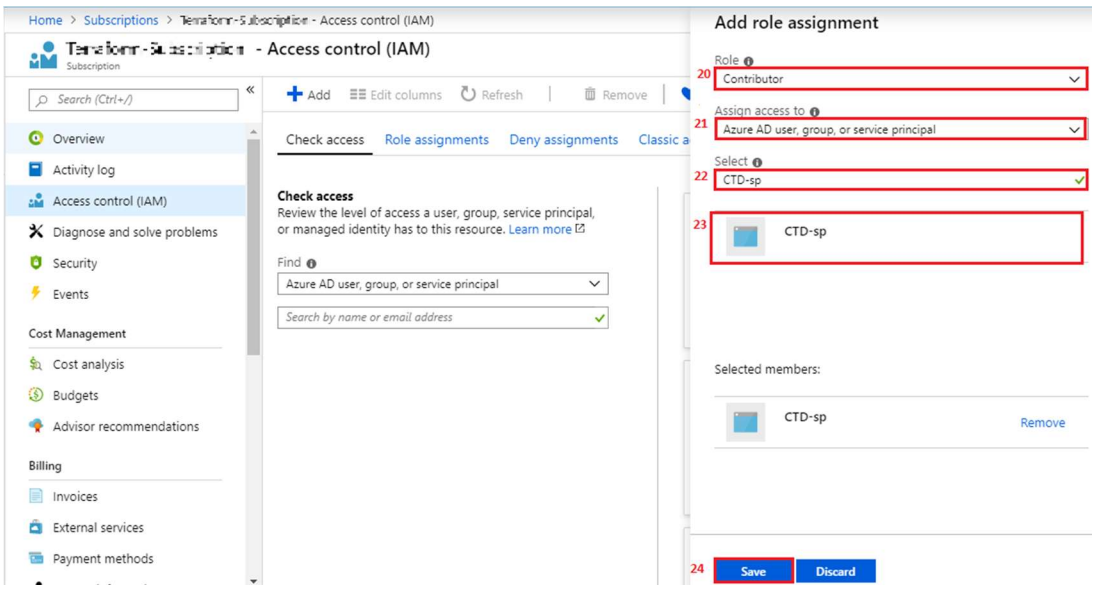
Step 11: Select **Access Control (IAM)** from the blade



Step 12: Select Add Button then choose 'Add role assignment' option



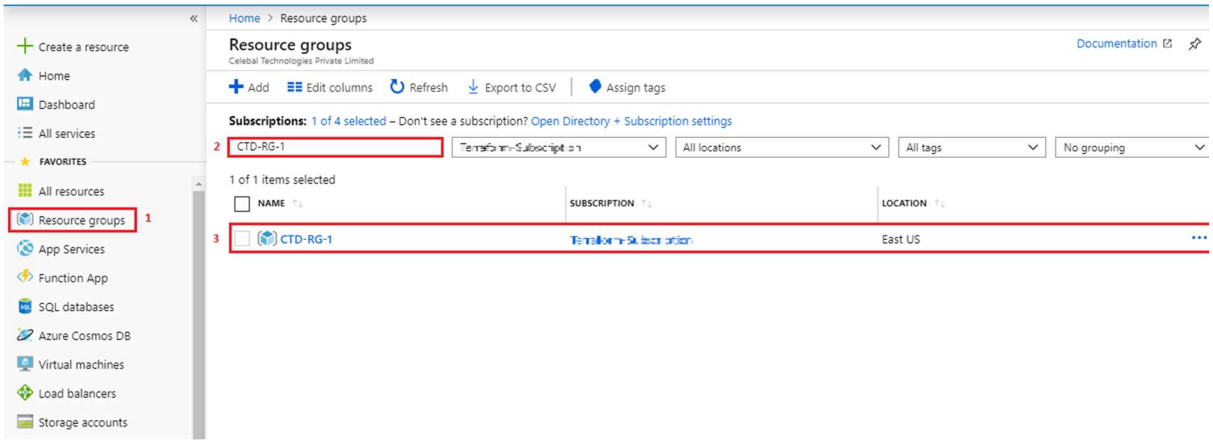
Step 13: Assign 'Contributor' role and select the registered app then click save



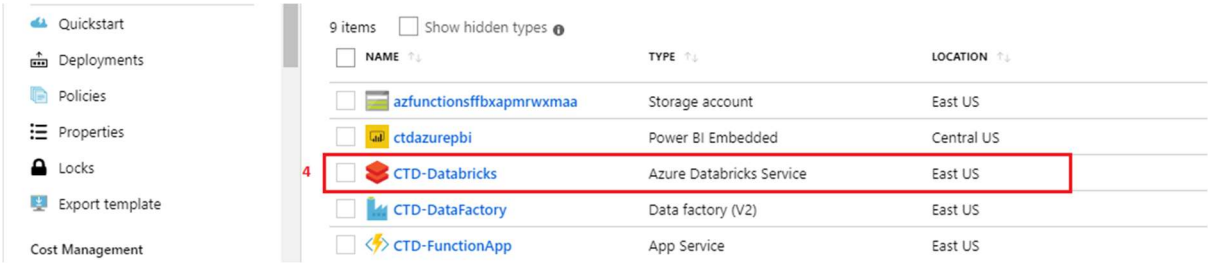
Steps for generating Databricks Access Token

Step 1: Log in to the Azure portal

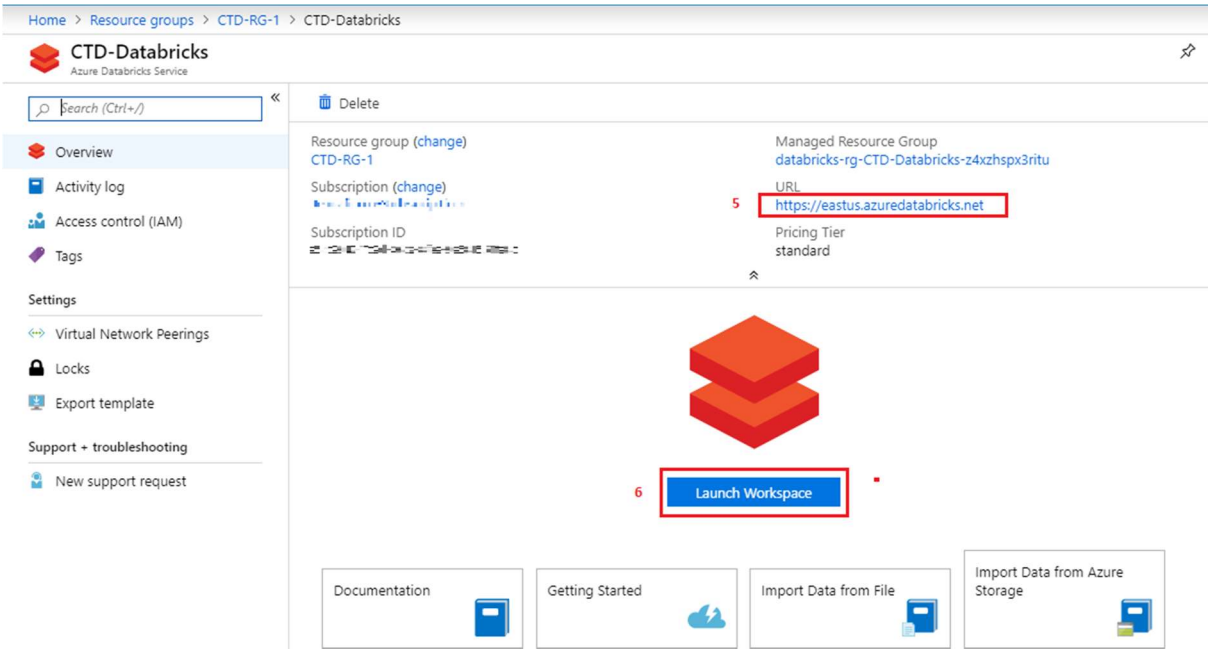
Step 2: Select **Resource groups** from Blade then select your Resource group



Step 3: In your Resource Group panel, select Databricks service

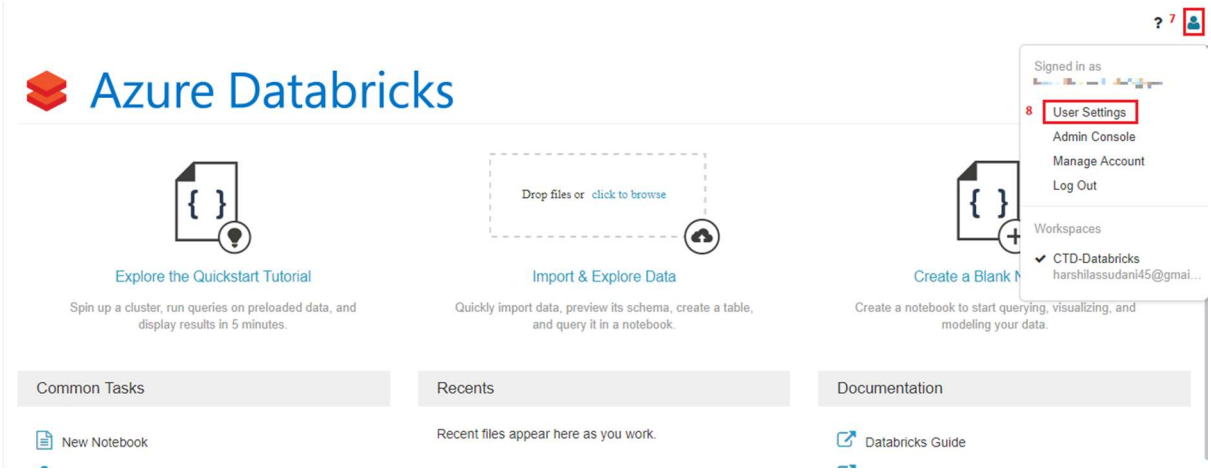


Step 4: Copy the workspace URL for future Reference then Launch Workspace

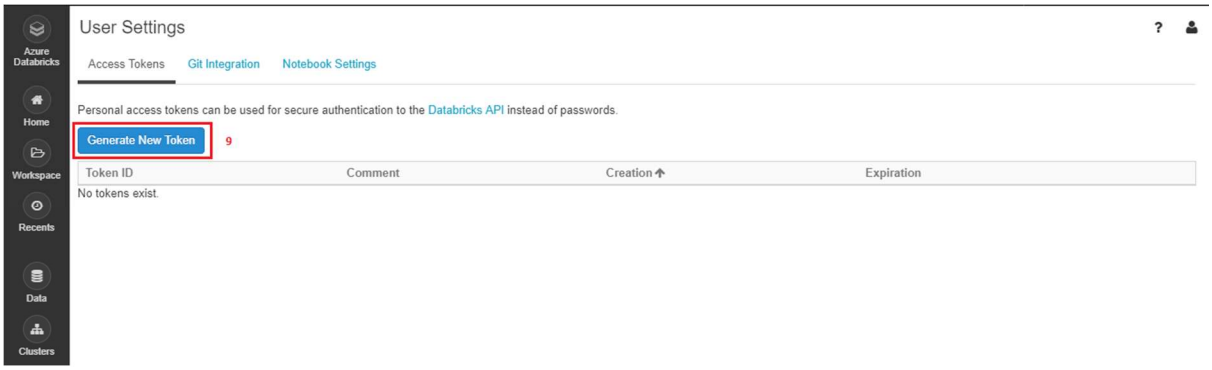


Step 5: In the top right corner, click on the **User** icon

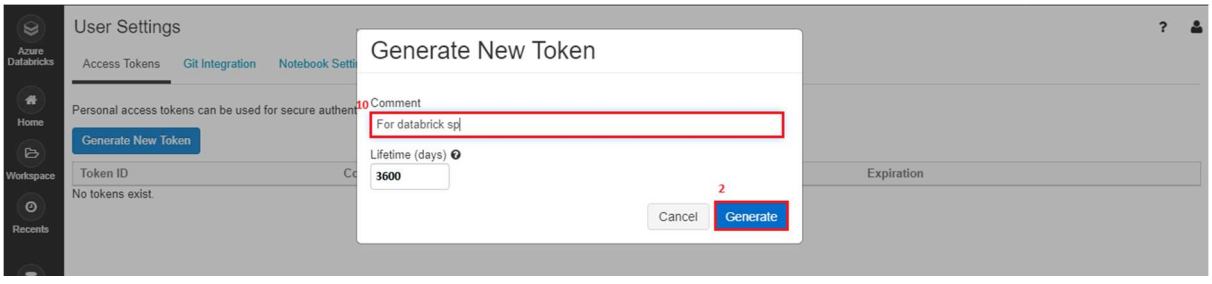
Step 6: Select **User Settings**

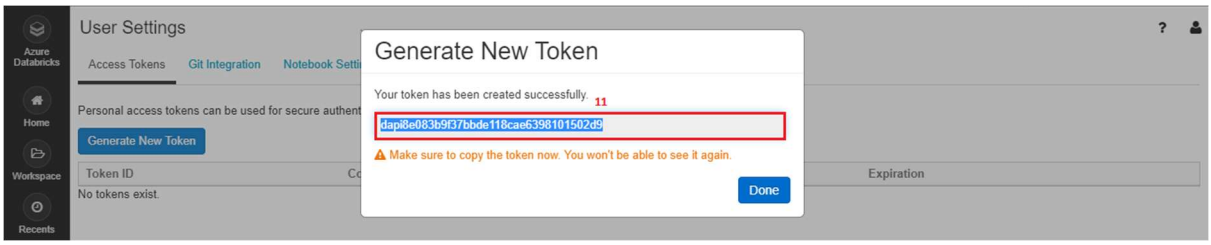


Step 7: Click on 'Generate New Token'



Step 8: This will prompt a window, add a comment and click 'Generate'

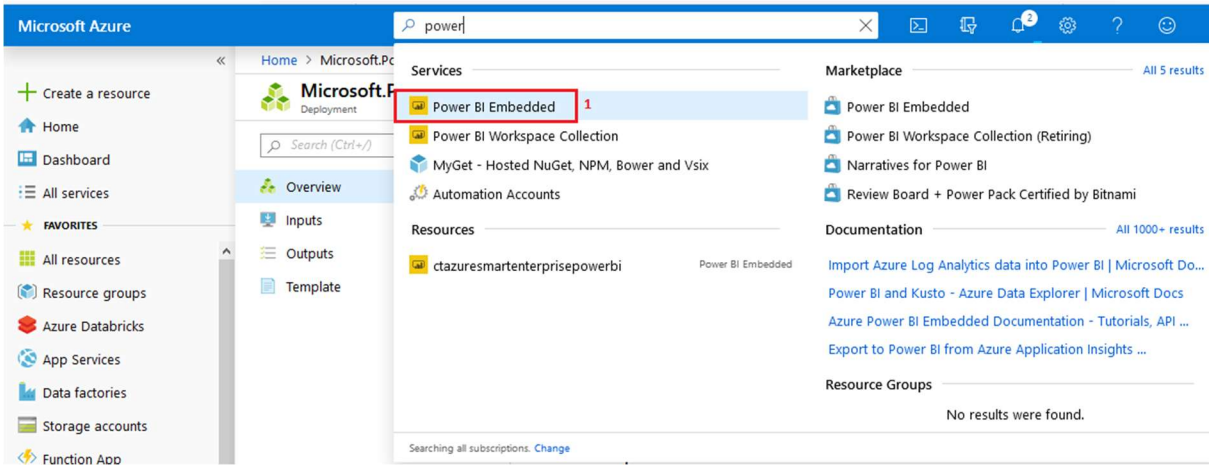




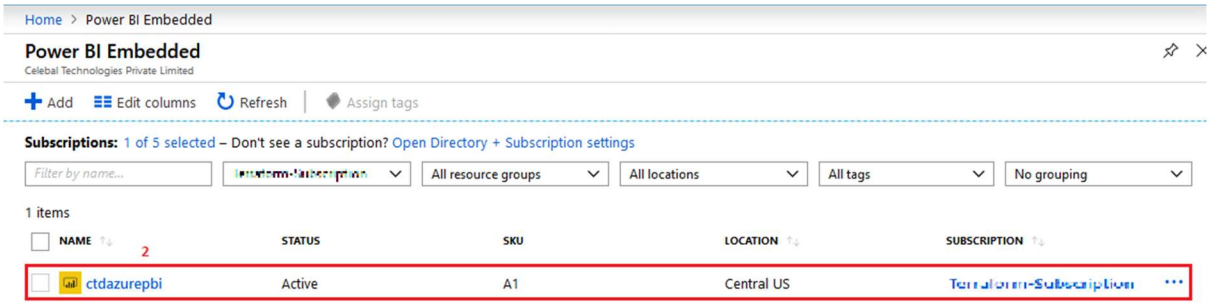
Note-: This token will be generated only once, so copy this token for future reference

Power BI Embedded

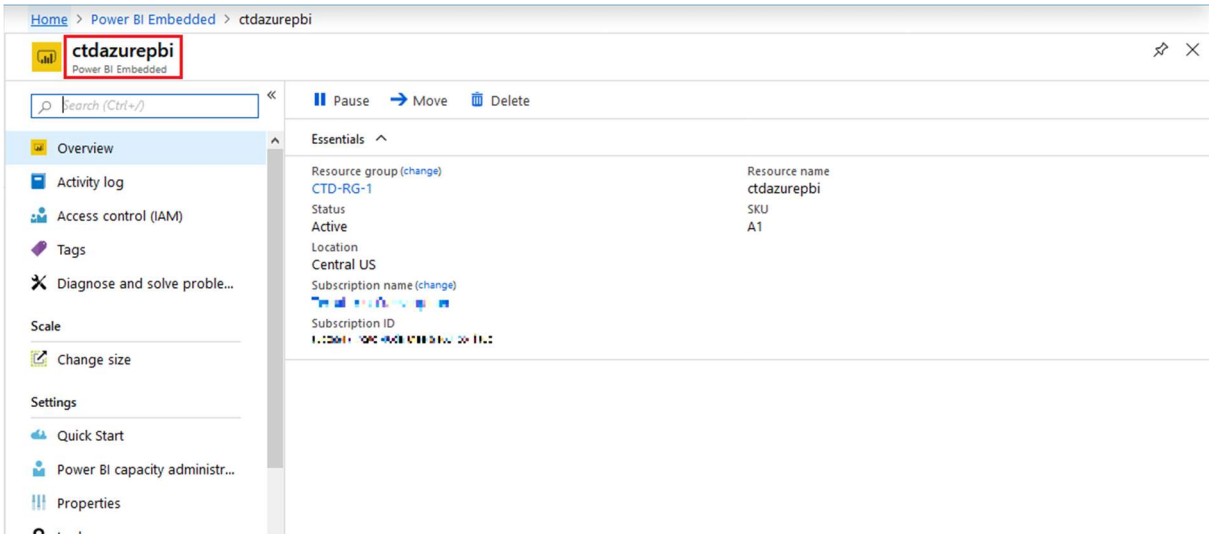
Step1: Select **Power BI Embedded** from Azure Portal



Step 2: Select your Power BI Embedded service



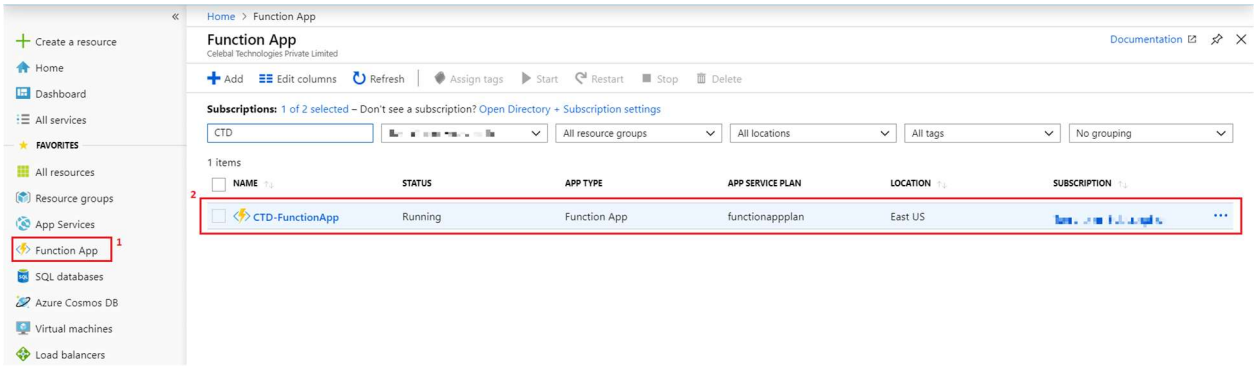
Step 3: Copy Power BI Embedded name, copy Power BI Admin name which is your Azure Portal Id for future reference



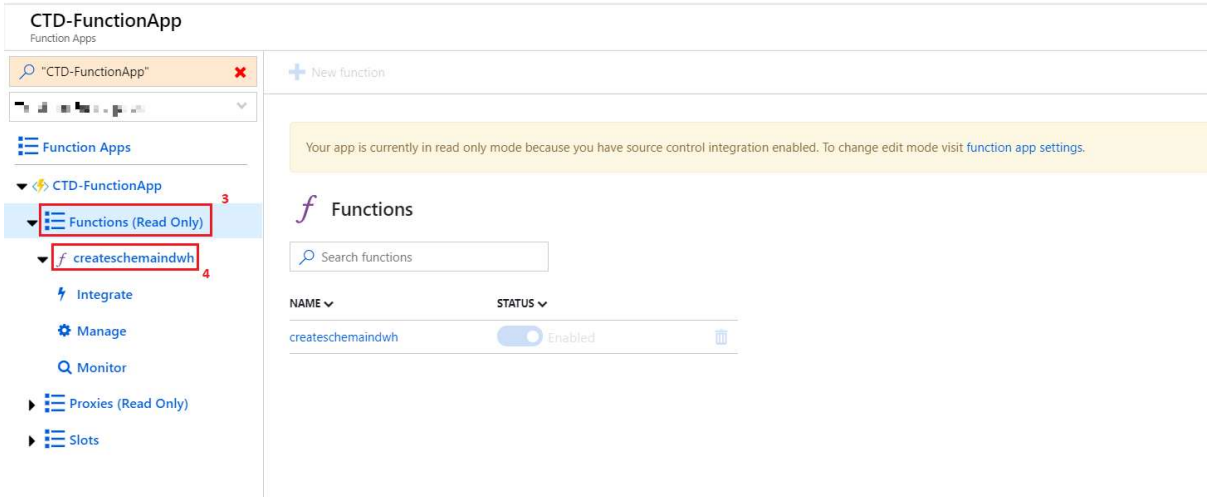
Azure Function App (URL)

Step 1: Log in to the Azure portal

Step 2: Select **Function App** from the blade then select the deployed function app from the list



Step 3: Select the Functions from function apps blade and then select the deployed function

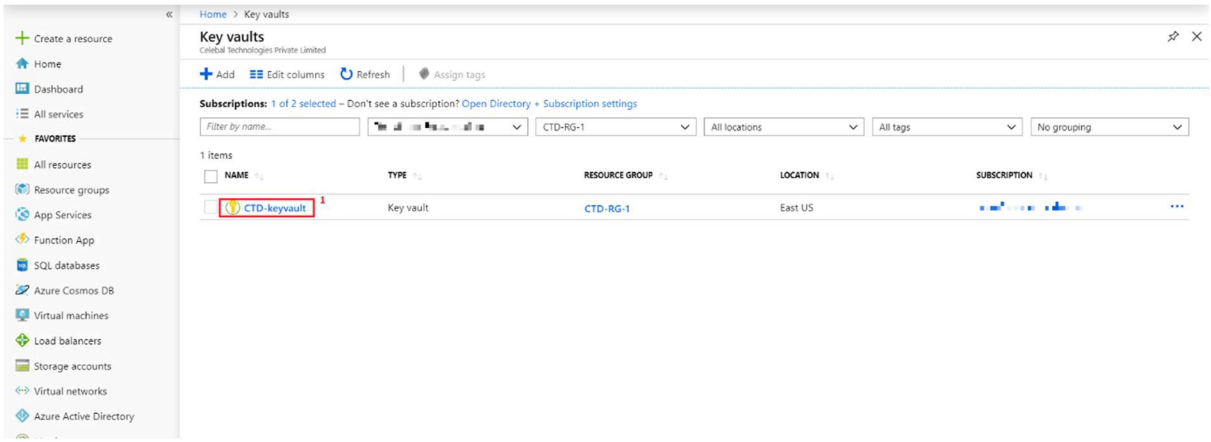


Step 4: Click on 'Get Function URL'

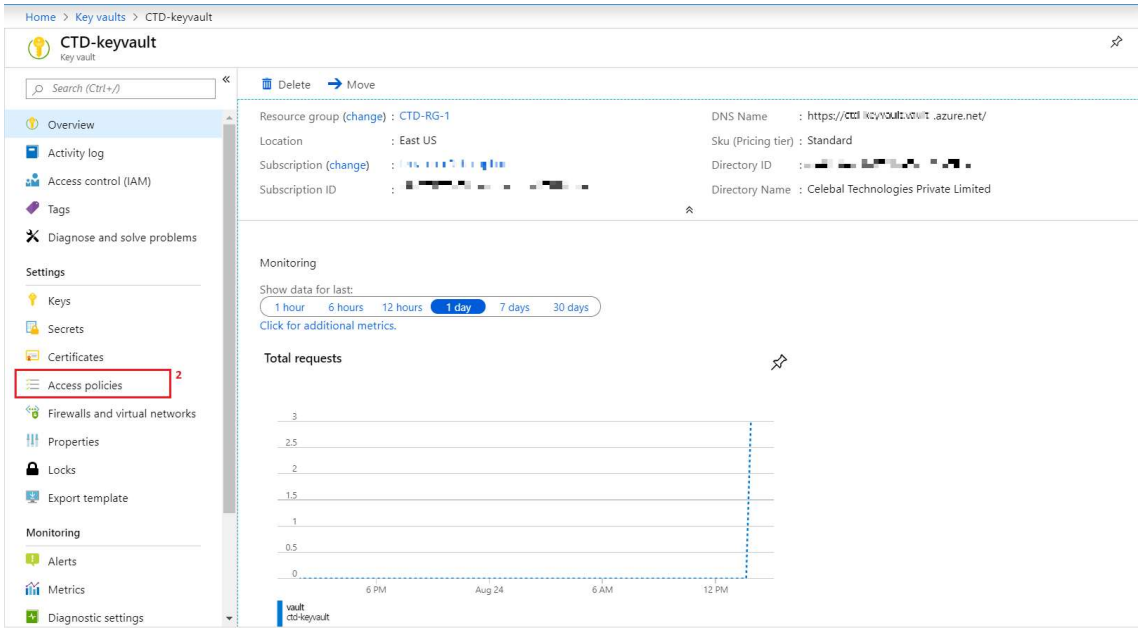
Step 5: Copy the function URL for future reference

Key Vault Access Policy to see your Secrets in Key vault

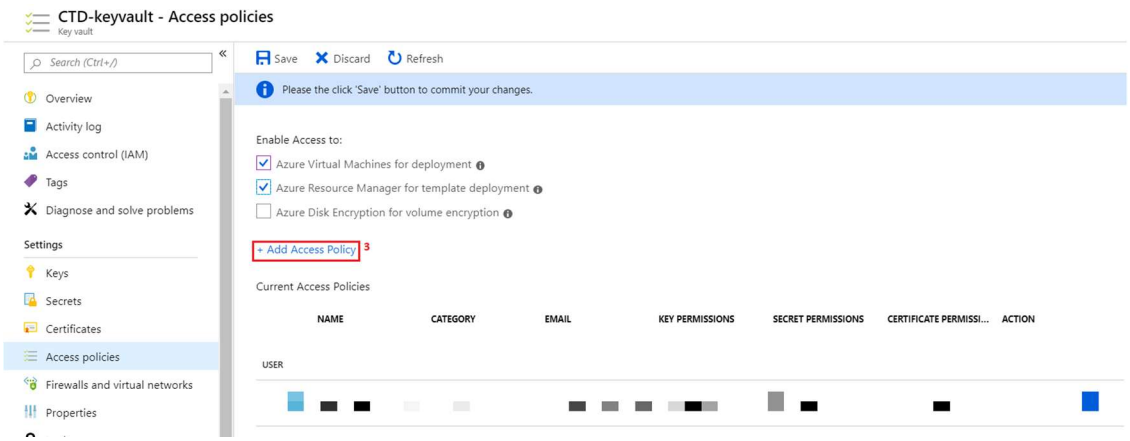
Step 1: From the Azure portal, select your **Key Vault**



Step 2: Click on the 'Access policies' in the key vault blade

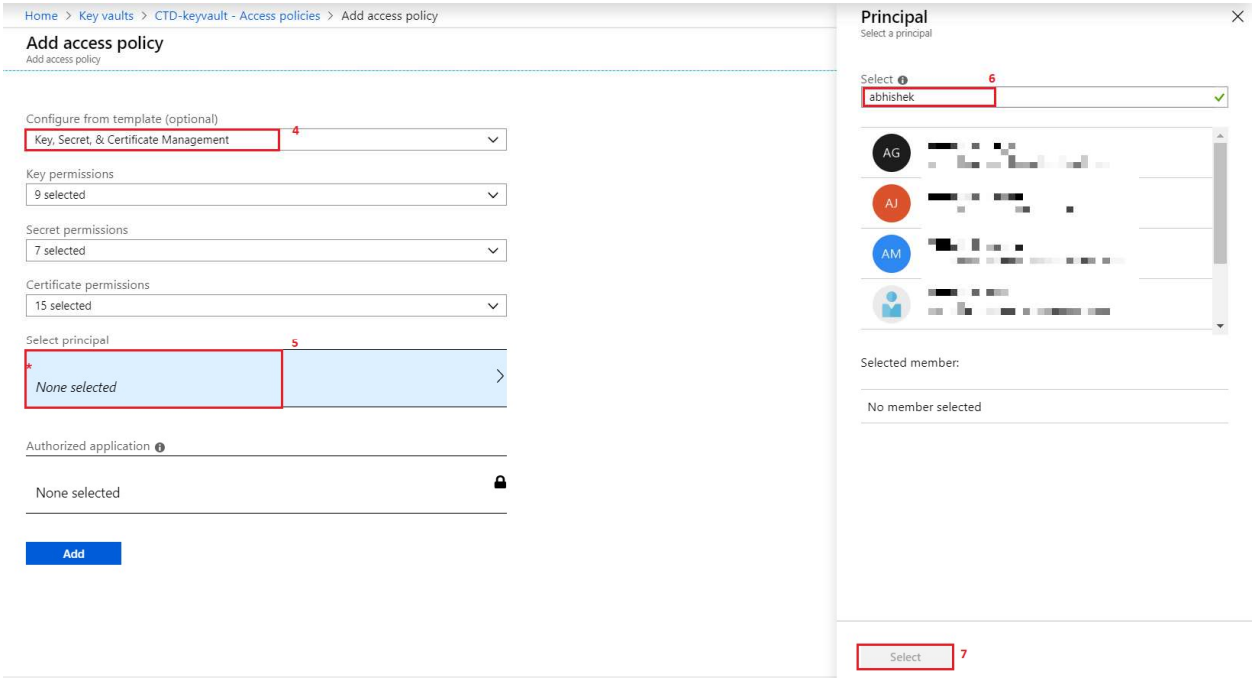


Step 3: Select Add Access Policy

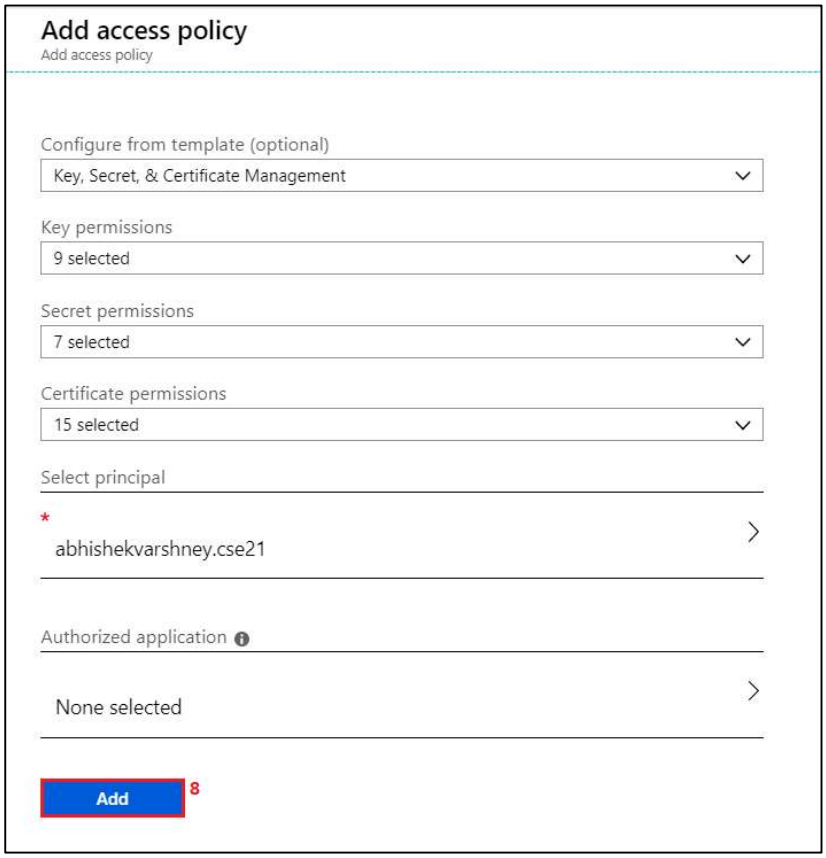


Step 4: After selecting the Add Access Policy, select the Key permissions, Secret permissions and Certificate permissions

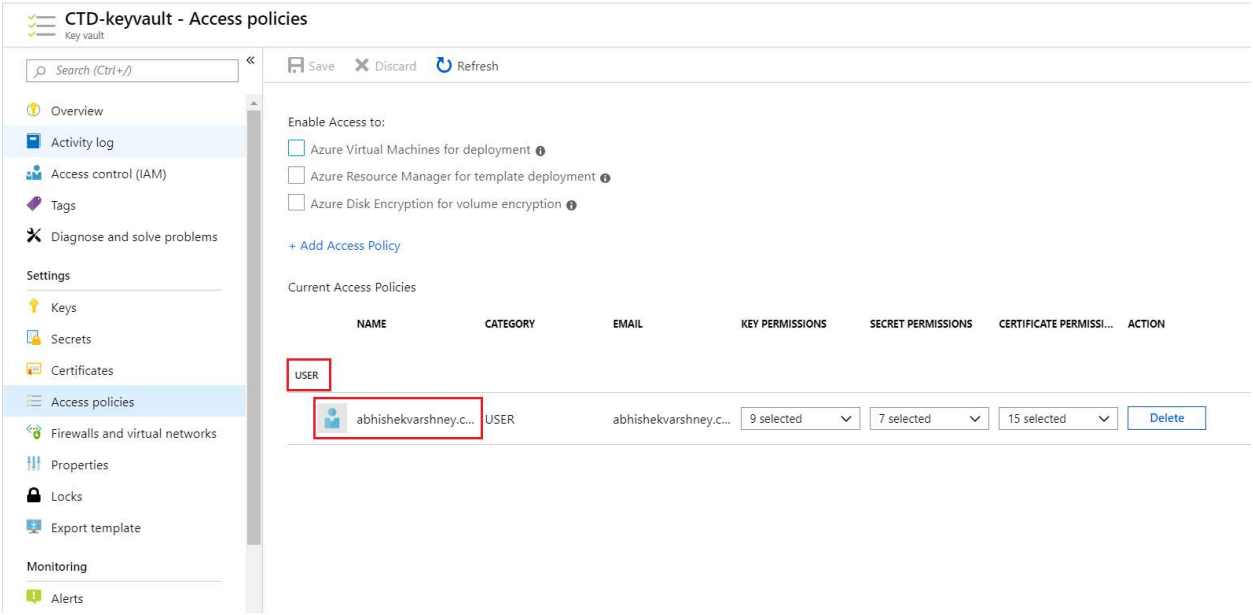
Step 5: After selecting all 3 permissions, now select Principal. A blade will open, write your name as given in image and click on 'Select'



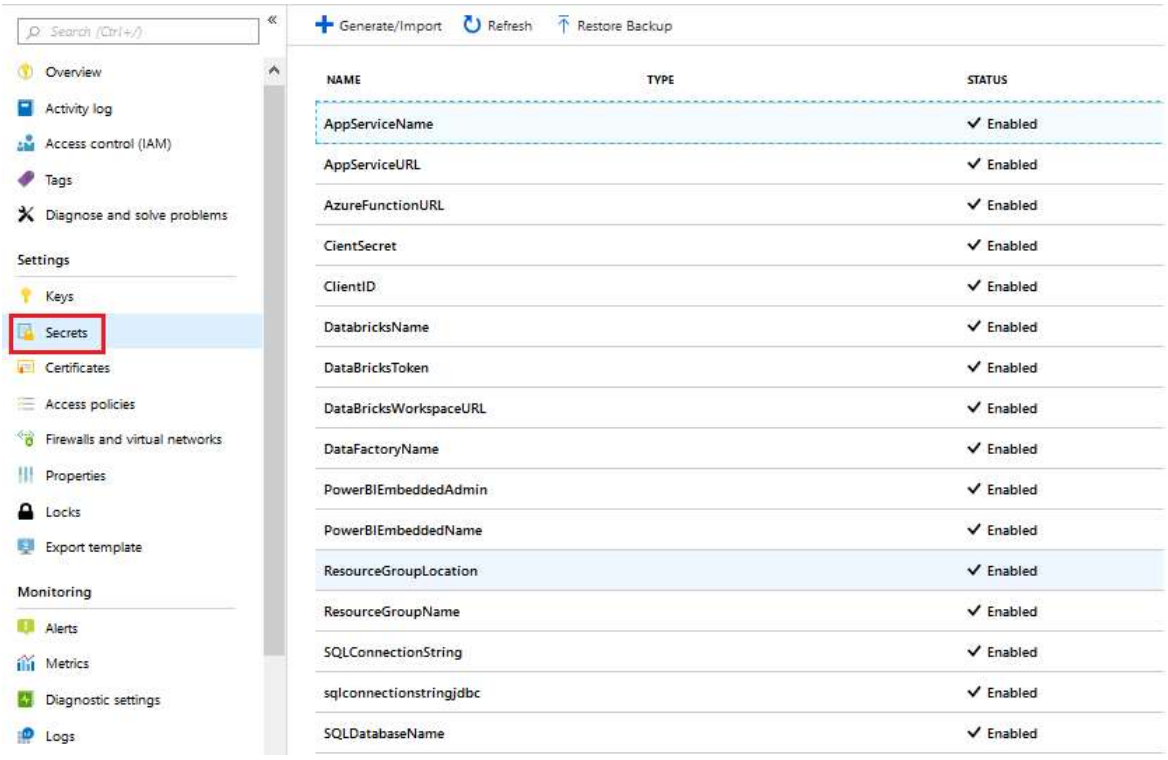
Step 6: Now click on 'ADD'



Note: Now you can see your name listed in the users



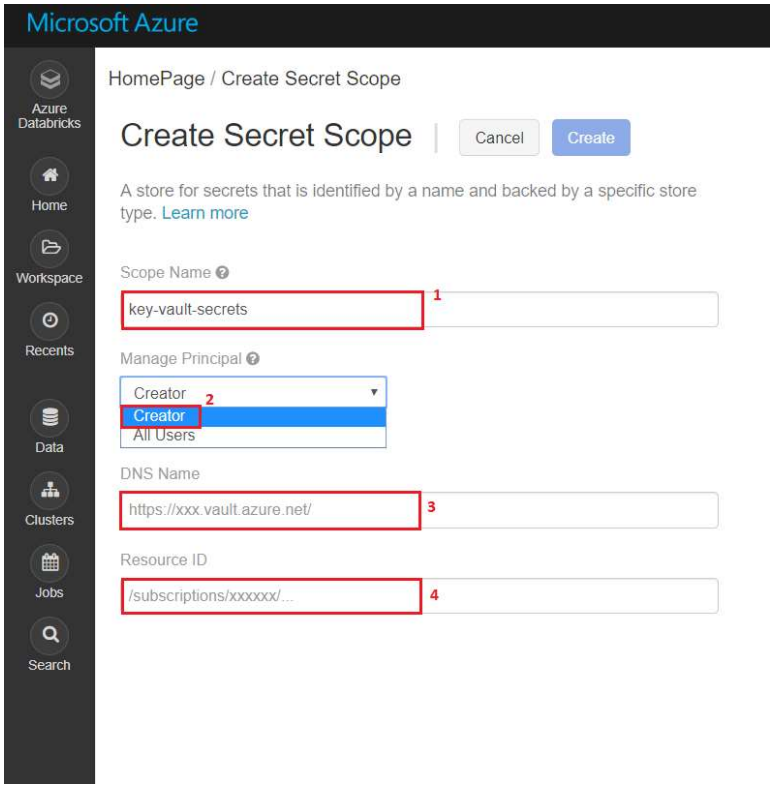
Step 8: Select **Secrets** in the blade and you can see all the credentials in stored in the Key Vault



Create an Azure Key Vault-backed secret scope

Step 1: Verify whether you have Owner permission on the Azure Key Vault instance that you want to use to back the secret scope.

Step 2: Go to https://<your_azure_databricks_url>#secrets/createScope (for example, *https://westus.azuredatabricks.net#secrets/createScope).*



Step 3: Enter the name of the secret scope.
Step 4: Use the *Manage Principal* drop-down to specify whether 'All *Users'* have MANAGE permission for this secret scope or only the 'Creator' of the secret scope

- Your account must have the Azure Databricks Premium Plan for you to be able to select '*Creator*'.
- If your account has the Standard Plan, you must set the MANAGE permission to the 'All Users' group. If you select Creator here, you will see an error message when you try to save the scope.

Step 5: Enter the DNS Name and Resource Id and click on create

Note-: Example https://databrickskv.vault.azure.net/ --DNS Name
Example
/subscriptions/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/resourcegroups/databricksrg/providers/Microsoft.KeyVault/vaults/databricksKV –Resource Id

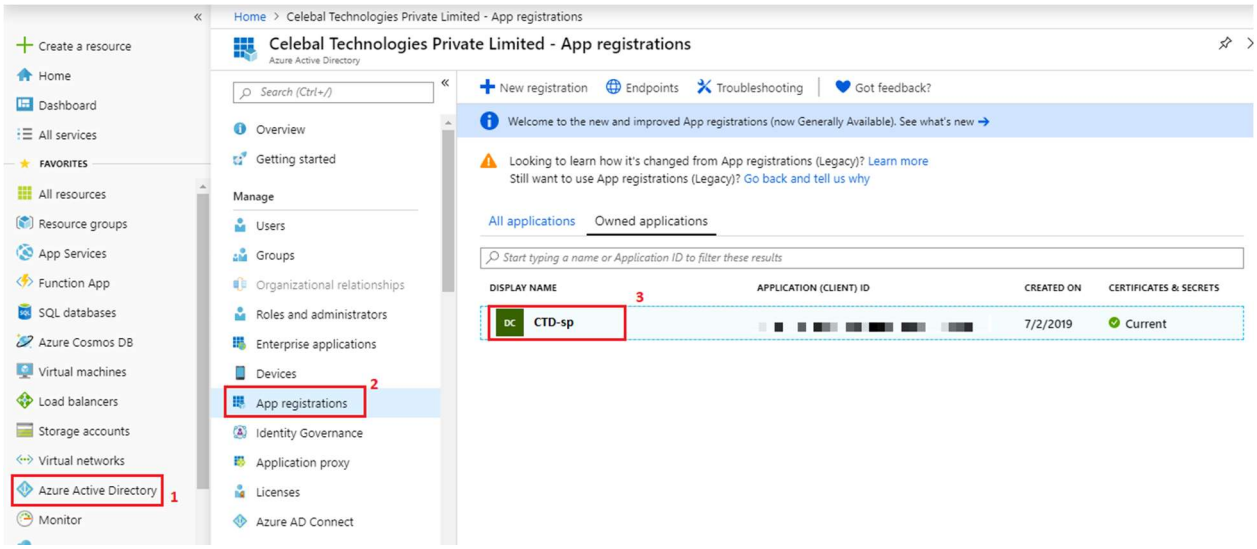
App Service Authentication & Authorization

I. Azure Active Directory

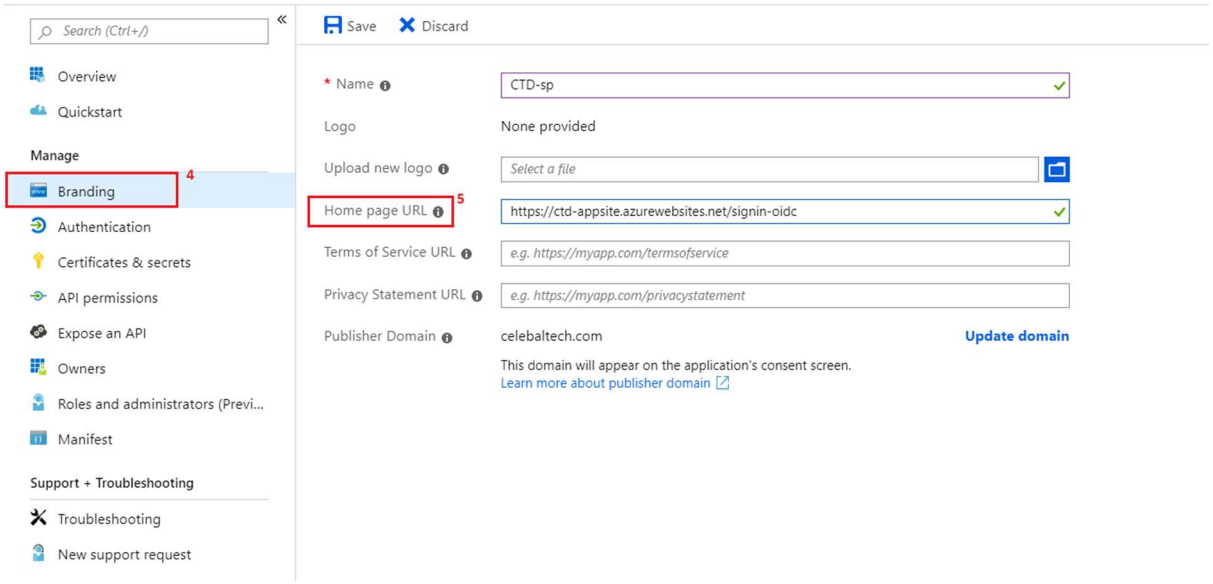
Step 1: Log in to the Azure portal

Step 2: Select **Azure Active Directory** from the blade then select **App registrations**

Step 3: Select the registered app

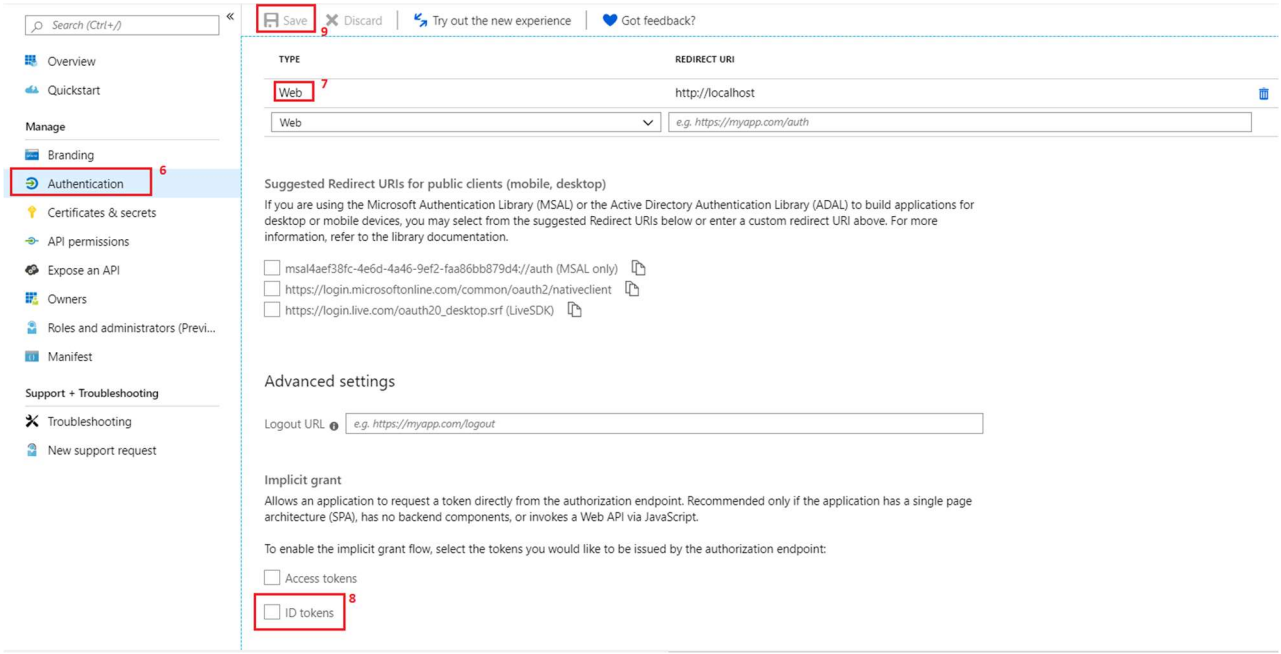


Step 4: Select **Branding** and enter the value of 'Home Page URL' and then save it



Note-: Enter {your App Service URL}/signin-oidc to the URL.

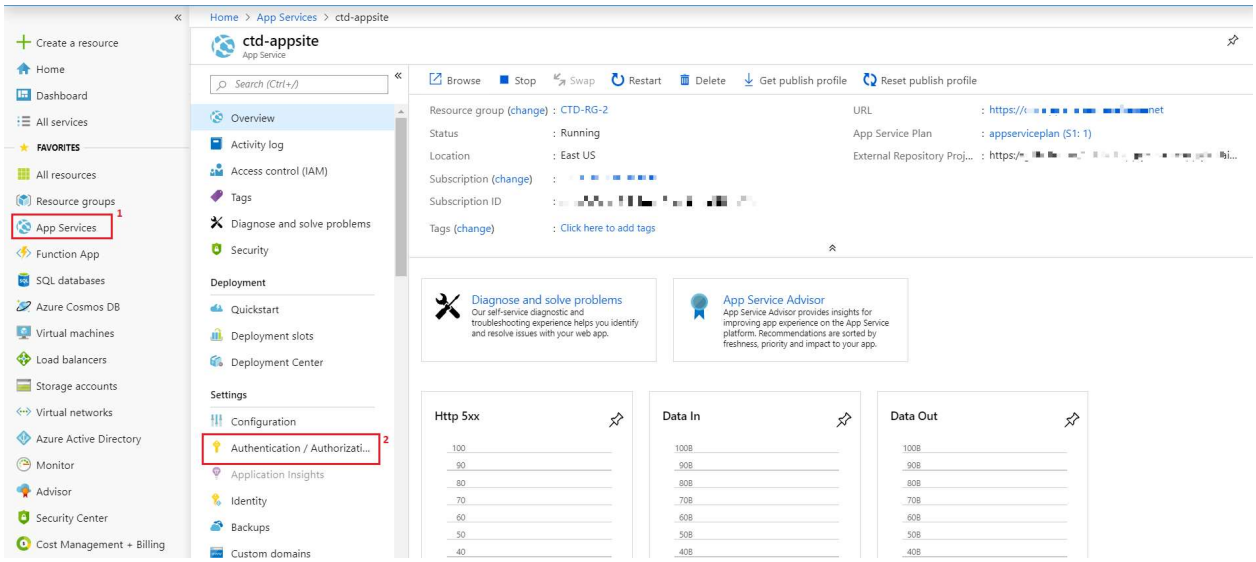
Step 5: Select **Authentication** then enter the URL then check the 'ID Token' checkbox and save it.



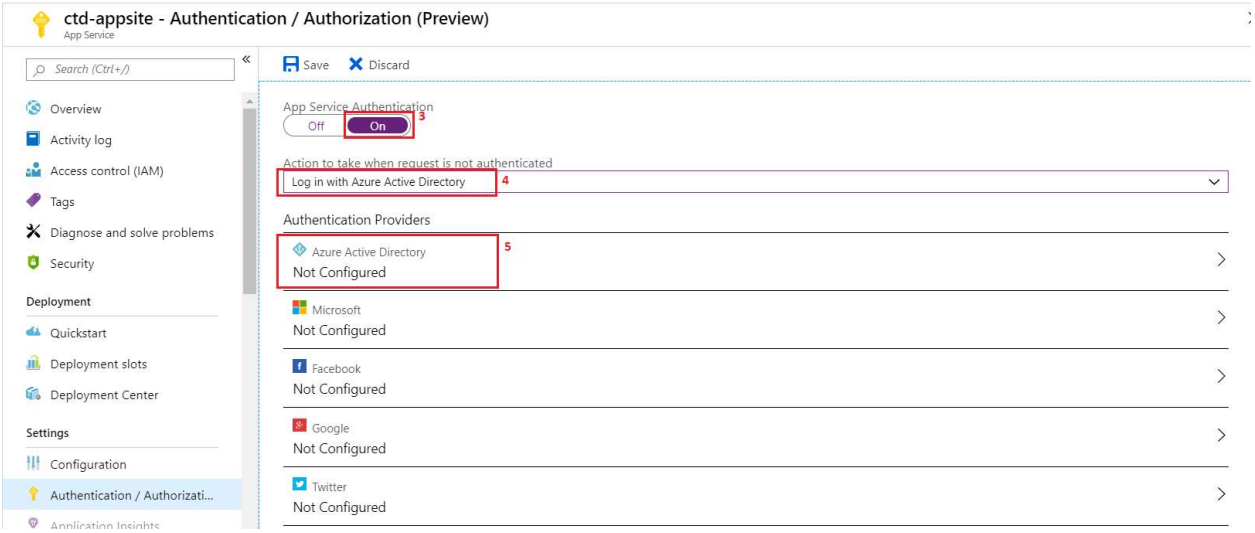
Note-: In URL mention {your App Service URL} /.auth/login/aad/callback

II. APP SERVICE

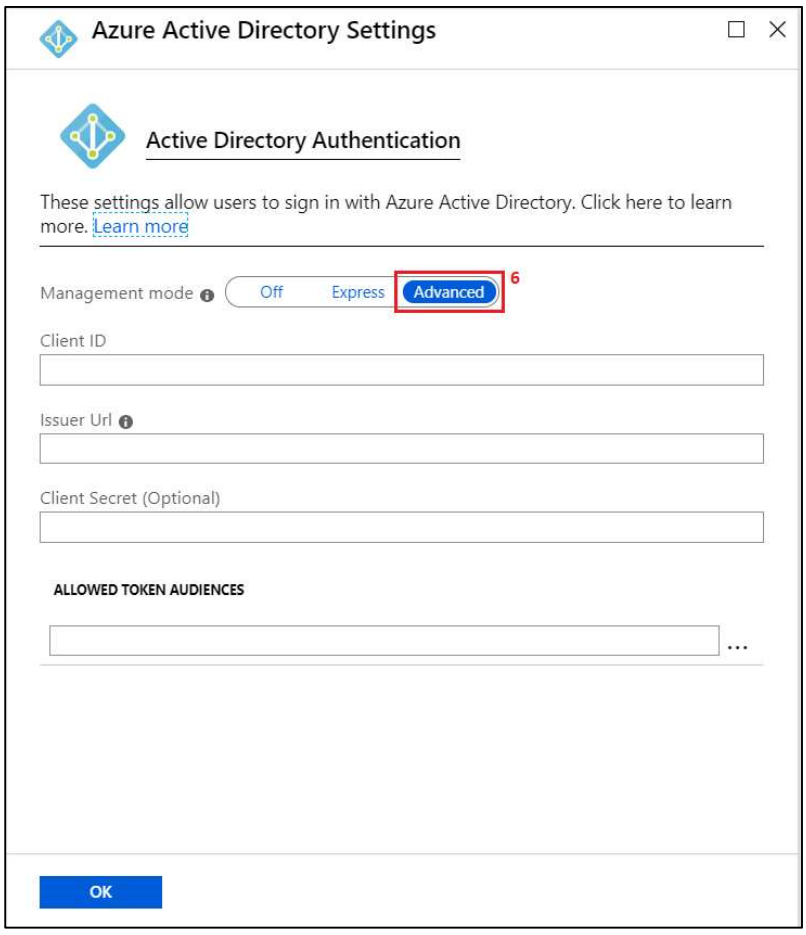
Step 1: Select **App Services** from the blade then select the Authentication/Authorization option



Step 2: Select the 'Log in with Azure Active Directory' option from the list box then configure Azure Active Directory as an Authentication Provider

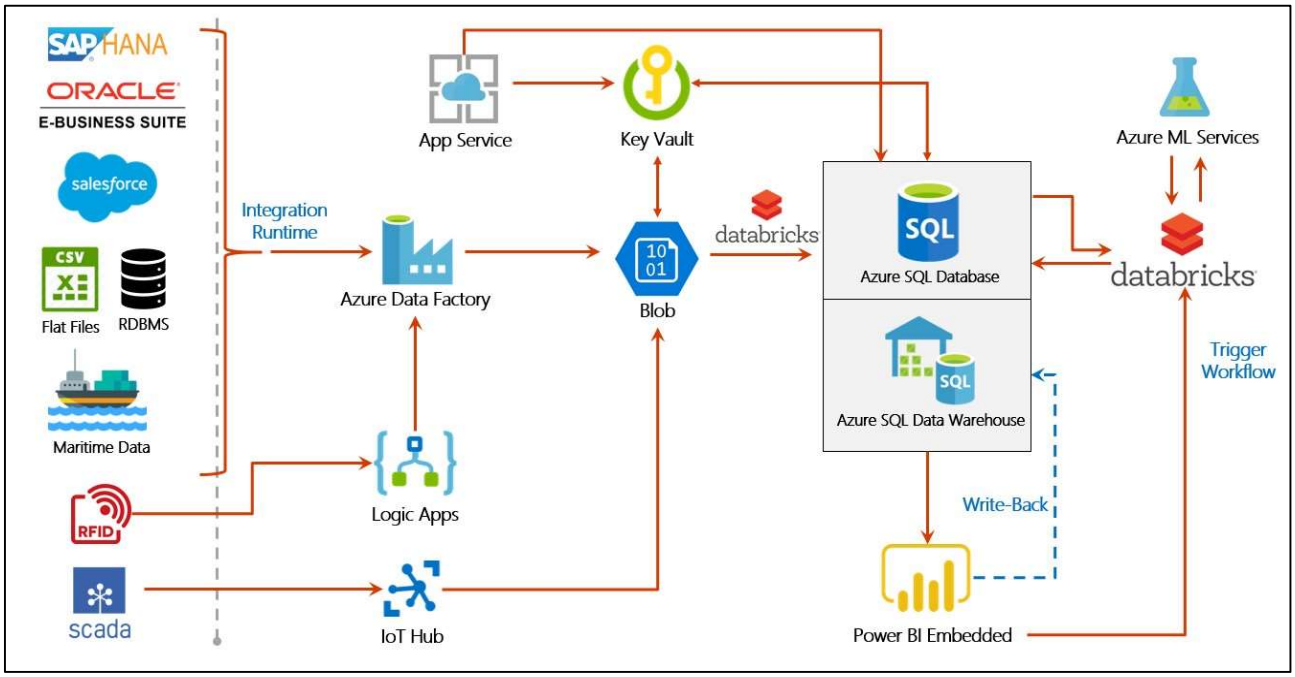


Step 3: Select the Management mode as 'Advanced', enter the Client ID and Tenant ID in Issuer URL as shown below



Note-: Add Tenant ID after the Issuer URL https://sts.windows.net/{your Tenant Id}

Solution Architecture



Architecture Description

Components Deployed-:

Azure Data Factory

- Form pipelines to ingest data from various sources

Azure Databricks

- It provides a series of performance enhancements on top of regular Apache Spark which include caching, indexing and advanced query optimizations.
- Runs simulations to identify right inventory levels & demand pricing
- Simulator for optimization and analysing different scenarios during planning.
- Run predictive models for demand and supply forecasts. The planning of different domestic sources (notification, planning documents) and demand on macro / micro level can be captured and analysed to predict the supply and helping sourcing strategy.
- Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV, MS Excel, SQL and RDBMS

- Analytics engine should provide capability to check analysis with multiple predictive & optimization algorithms
- It should have central data lake concept to manage different data sources in single platform.

Logic Apps

- It helps to schedule, automate, and orchestrate tasks, business processes, and workflows when there is a need to integrate apps, data, systems, and services across enterprises or organizations.
- It enables to design and build scalable solutions for app integration, data integration, system integration, enterprise application integration (EAI), and business-to-business (B2B) communication, whether in the cloud, on premises, or both.

- The Logic apps make use of typical VETER pipeline which involves AS2 connector, X12 connector, Transformation, Encoding and HTTP connectors

IoT Hub

- Acts as a central message hub for bi-directional communication between IoT application and the devices it manages.
- It can be leveraged to collect data from multiple sensors installed on vehicles for scheduling and tracking.

App Service

- Platform-as-a-service that runs web, mobile, API and business logic applications and automatically manages the resources required by those apps.

Key Vault

- Secret management: Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
- Key management: Create and control encryption keys that encrypt your data.
- Certificate management: Provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with Azure and your internal connected resources.
- Store secrets backed by HSMs: Use either software or FIPS 140-2 Level 2 validated HSMs to help protect secrets and keys

Azure Blob Storage

- Store large amounts of unstructured object data, such as text or binary data

Azure SQL Database

- SQL Database is a high-performance, reliable, and secure cloud database that you can use to build data-driven applications and websites in the programming language of your choice, without needing to manage infrastructure

Azure SQL Data Warehouse

- Combines SQL relational databases with massively parallel processing to design, load, manage, and analyse data

Azure ML Services

- Provides SDKs and services to quickly prep data, train, and deploy machine learning models.
- Improve productivity and costs with auto scaling compute & pipelines

Power BI Embedded

- Provide interactive visualizations and business intelligence capabilities with an interface simple enough for end users to create their own reports and dashboards
- Helps create efficient supply chain operations environment, with real-time insights on Temperature threshold, Driver performance & Customer behaviour; thereby maximizing operational efficiency.
- Enables intelligent decision making; by utilizing the power of intuitive rich visuals and reports generated from staggering number of customers, inventory and workforce data.
- Provides consolidated view of the data fetched from multiple sources; in the form of interactive dashboards.
- Delivers critical insights into various activities, to determine the areas of improvement and boost their efficiency.