



Supply Chain Analytics

Instructions Manual

Version 1.0

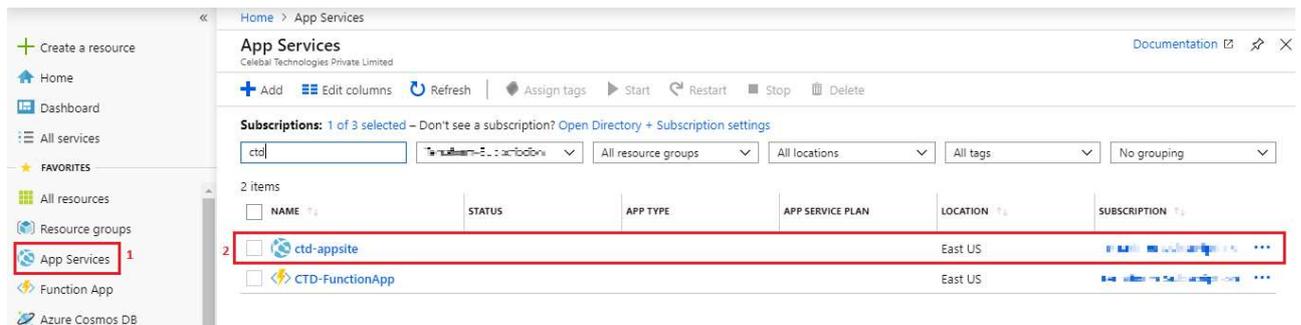
Contents

Azure App Service (URL)	3
Azure Data Factory	3
How to download and install integration runtime for Data Factory (For SAP)	5
How to add HDBODBC Driver for SAP HANA	9
Azure Storage Account (Access Keys) and (Connection String)	11
Azure SQL Server & Database (Connection Strings)	12
App Registration (Azure Active Directory)	14
Steps for generating Databricks access token	18
Power BI Embedded	20
Azure Function App (URL)	21
Key Vault Access Policy to See your Secrets in Key vault	22
Create an Azure Key Vault-backed secret scope	25
App Service Authentication & Authorization	26
Azure Active Directory	26
App Service	27
Solution Architecture	29
Components Deployed	29
Azure Data Factory	29
Azure Databricks	29
Logic Apps	30
IoT Hub	30
App Service	30
Key Vault	30
Azure Blob Storage	30
Azure SQL Database	31
Azure SQL Data warehouse	31
Azure ML Services	31
Power BI Embedded	31

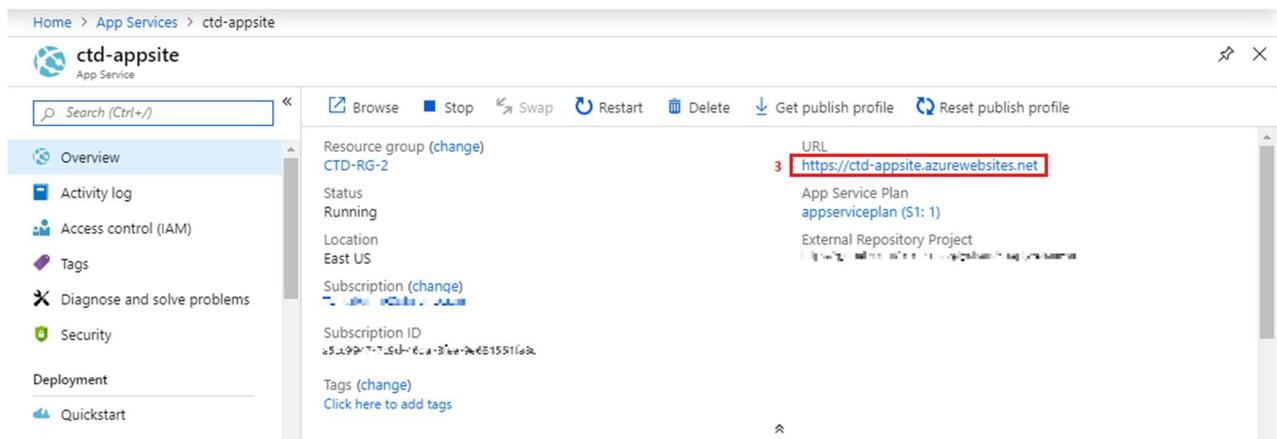
Azure App Service (URL)

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

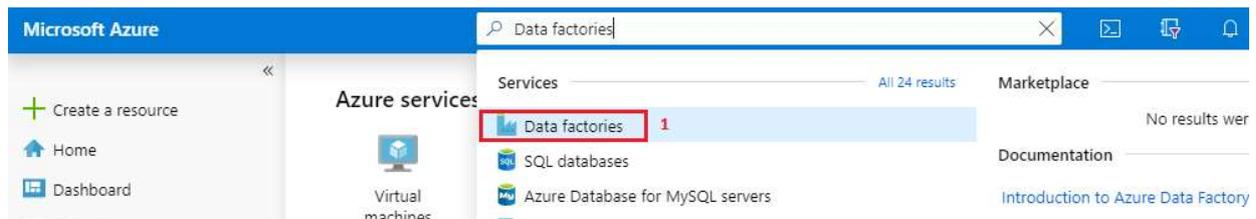


Step 3: Select the web app and copy the URL

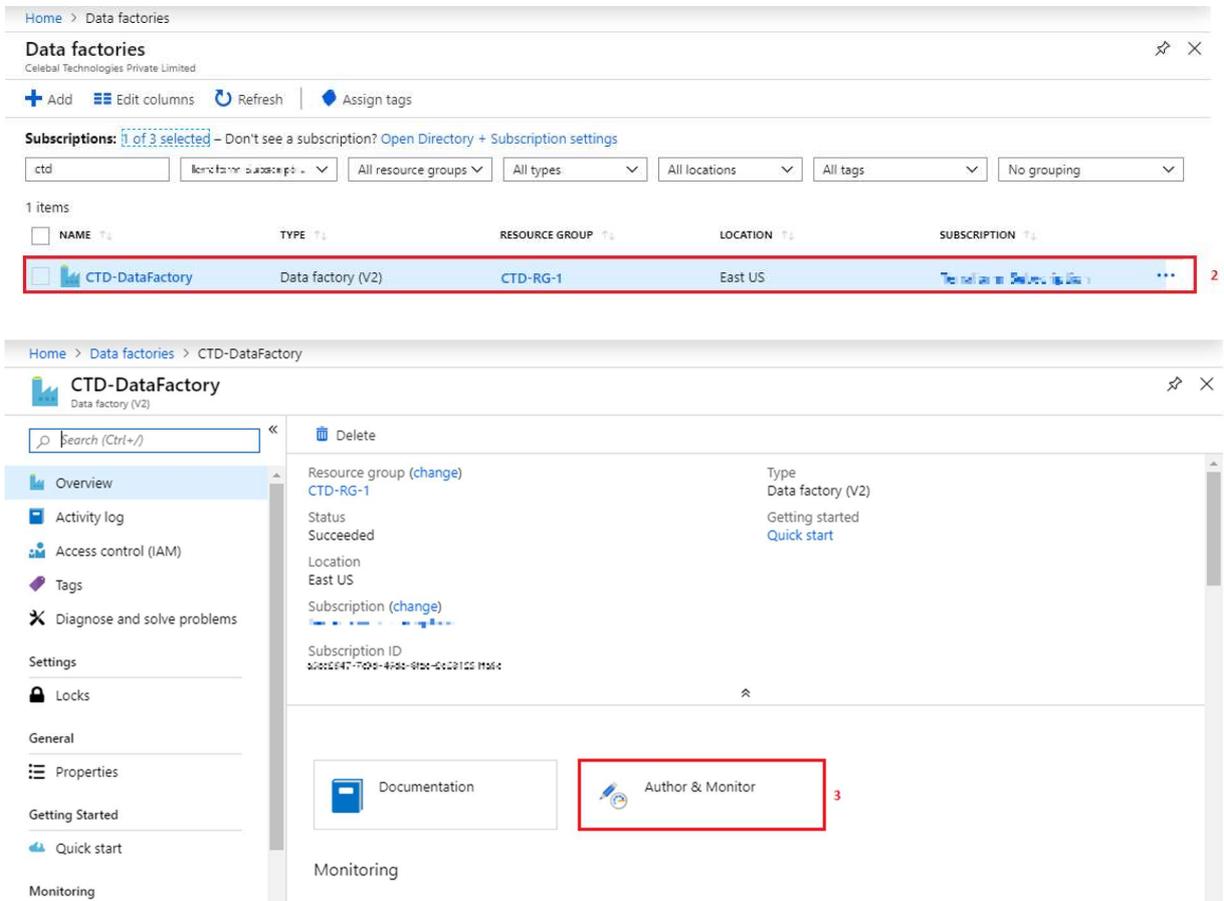


Azure Data Factory

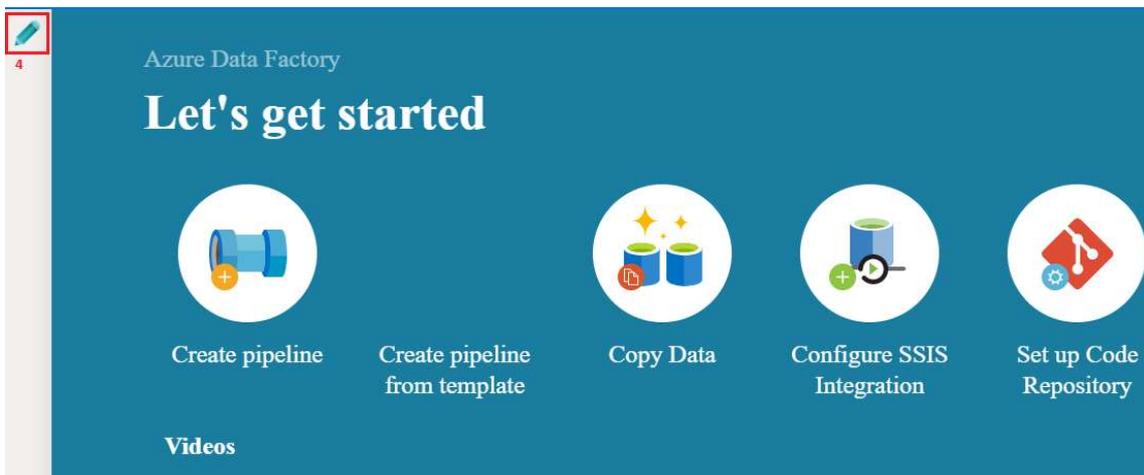
Step 1: Select **Data factories** option



Step 2: Select Data Factory and click on 'Author and Monitor'



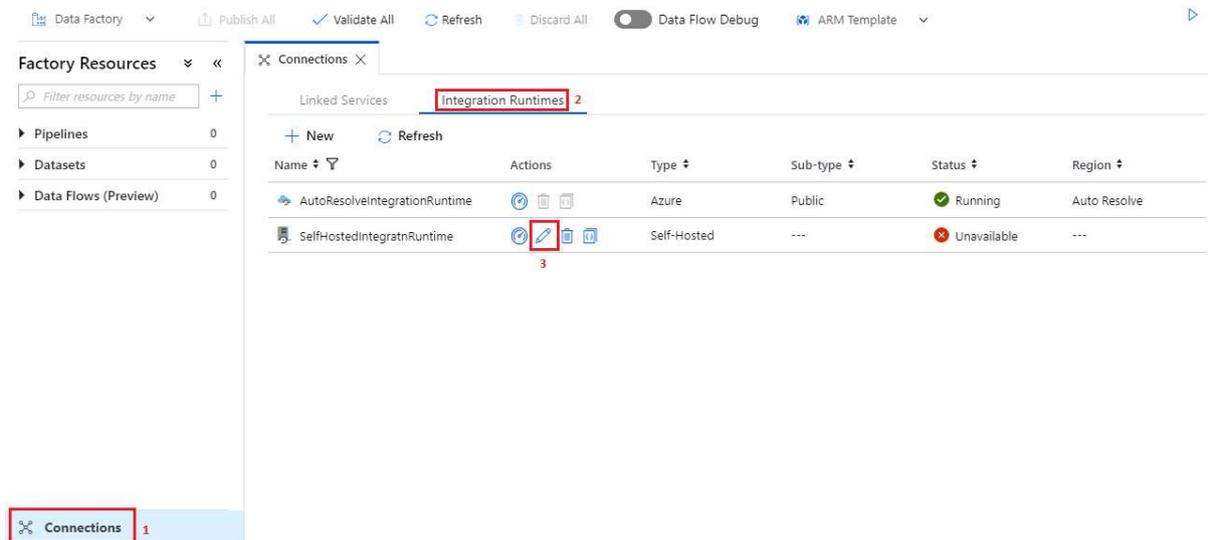
Step 3: Another blade will open, click on the pipeline symbol



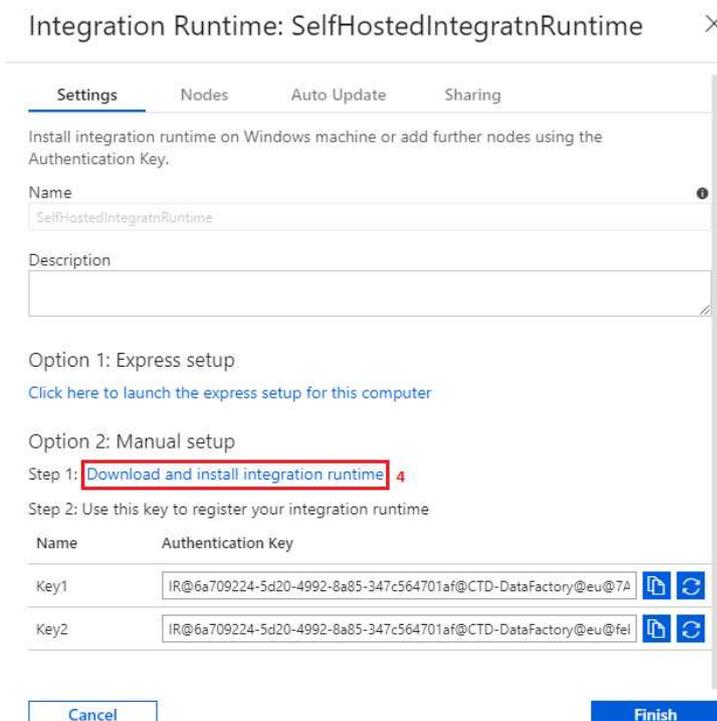
How to download and install Integration Runtimes for Data Factory (For SAP and Oracle)

Step 1: Select Connections option from the Factory Resources blade

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

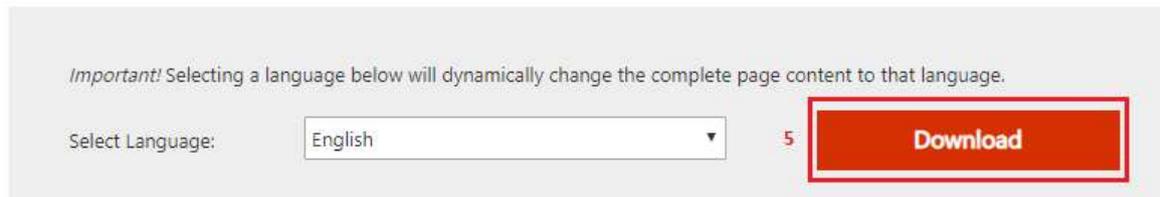


Step 3: Click on 'Download and install integration runtime' option



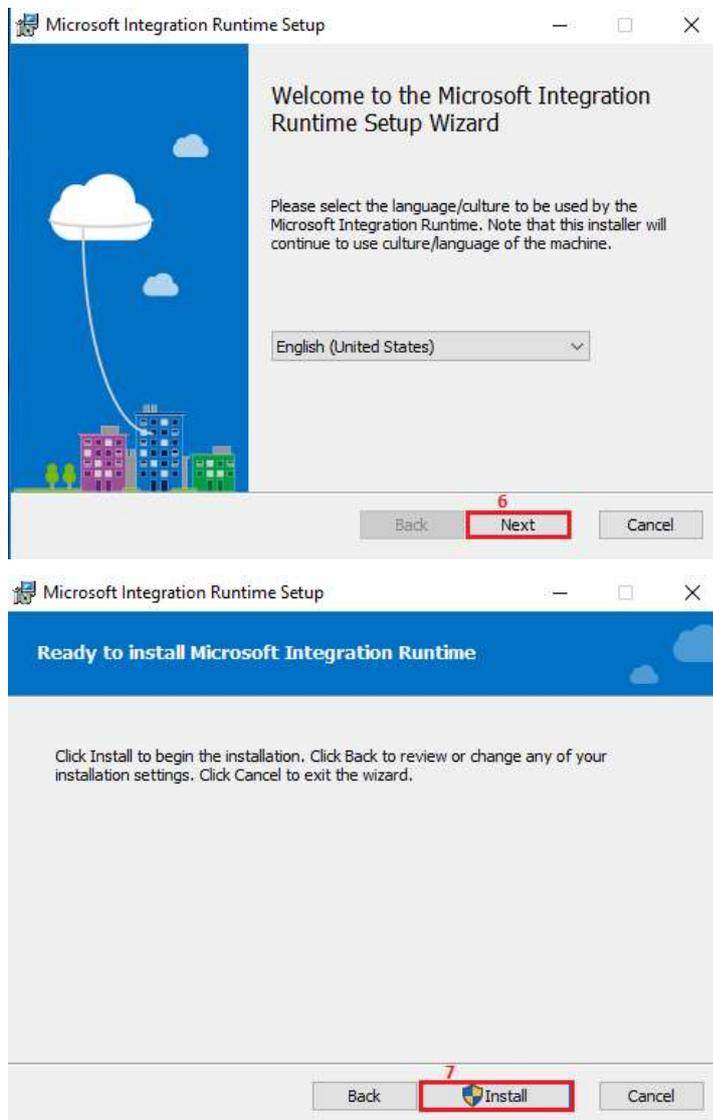
Step 4: Click on Download

Azure Data Factory Integration Runtime



The Integration Runtime is a customer managed data integration infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments. It was formerly called as Data Management Gateway.

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

Integration Runtime: SelfHostedIntegratnRuntime >

Settings Nodes Auto Update Sharing

Install integration runtime on Windows machine or add further nodes using the Authentication Key.

Name
SelfHostedIntegratrRuntime ⓘ

Description

Option 1: Express setup
[Click here to launch the express setup for this computer](#)

Option 2: Manual setup
Step 1: [Download and install integration runtime](#)
Step 2: Use this key to register your integration runtime

Name	Authentication Key
Key1	✓ Key1 Copied to your Clipboard 8 IR@6a709224-5d20-4992-8a85-347c564701af@CTD-DataFactory@eu@7A  
Key2	IR@6a709224-5d20-4992-8a85-347c564701af@CTD-DataFactory@eu@fel  

Step 7: Paste the key and click on Register

Microsoft Integration Runtime Configuration Manager

Register Integration Runtime (Self-hosted)

Welcome to Microsoft Integration Runtime Configuration Manager. Before you start, register your Integration Runtime (Self-hosted) node using a valid Authentication Key.

✓

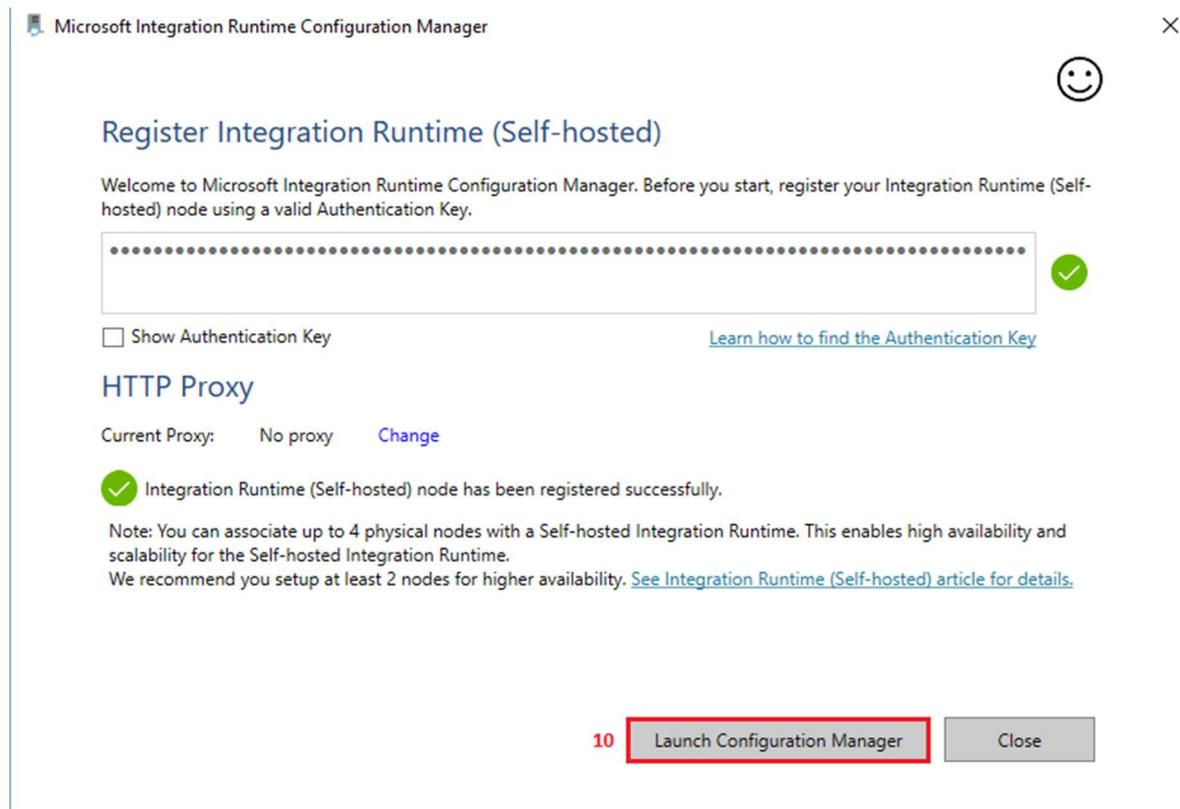
Show Authentication Key [Learn how to find the Authentication Key](#)

HTTP Proxy

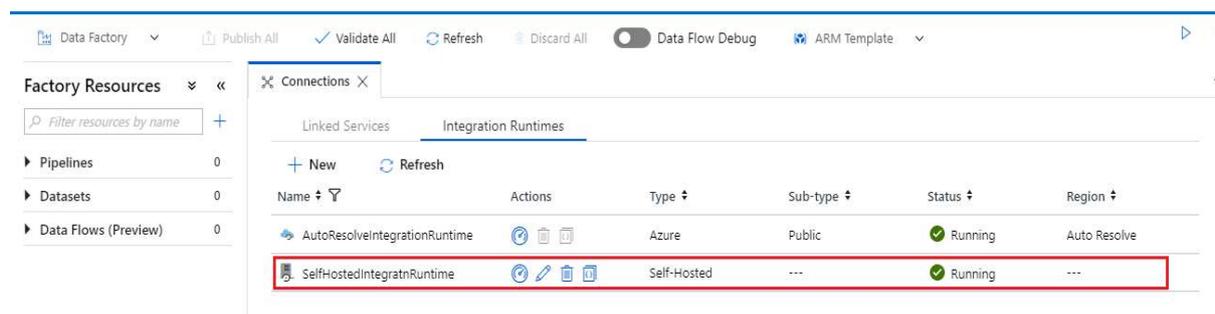
Current Proxy: No proxy [Change](#)

9

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

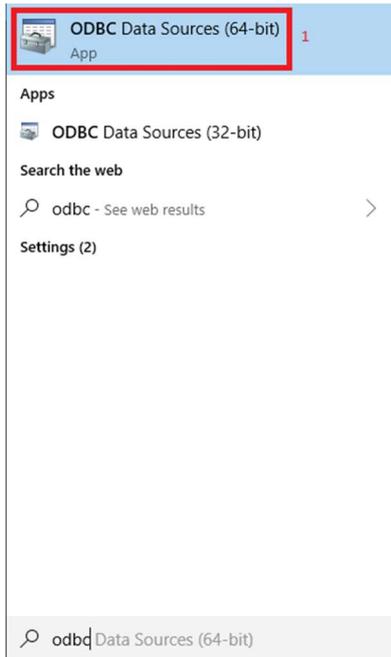


Step 9: You have successfully installed Integration Runtime for Data Factory, visit the Integration Runtimes wizard and check that the status is now running

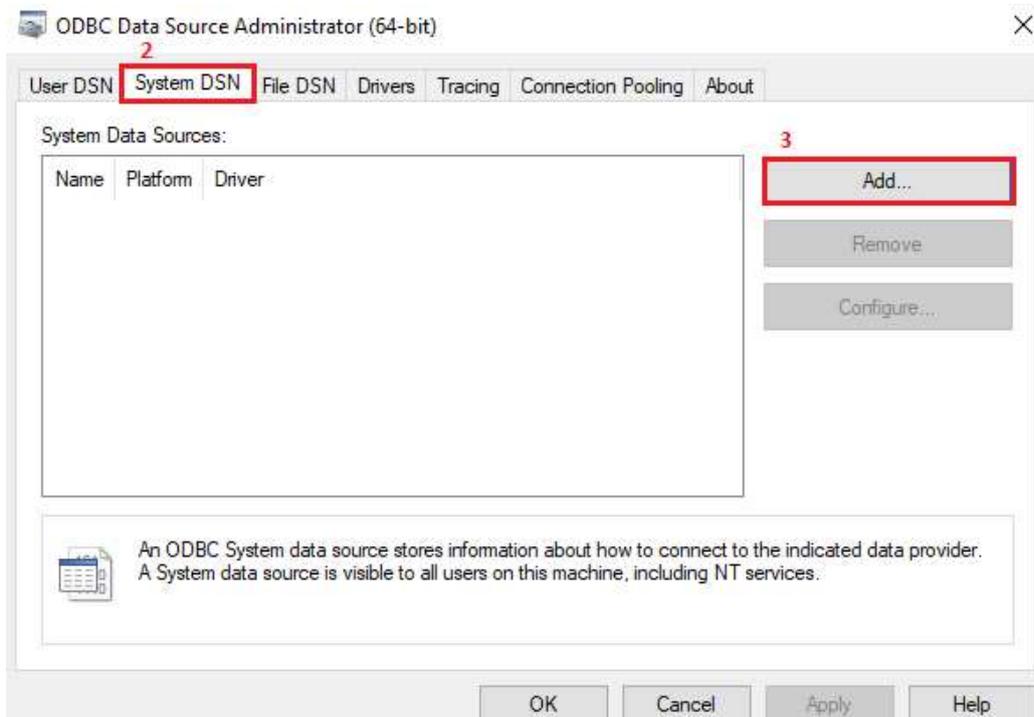


How to add HDBODBC Driver for SAP HANA

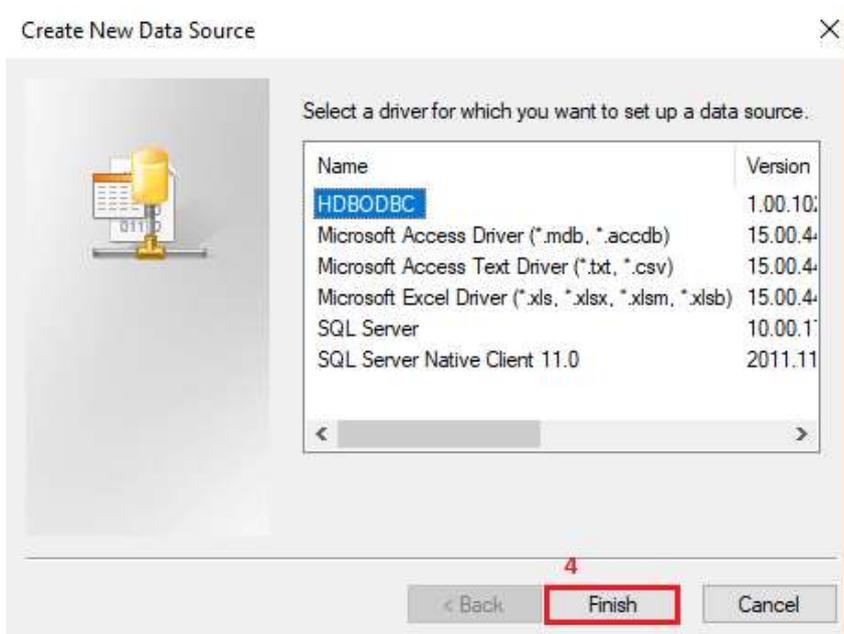
Step 1: Install SAP Client for HDBODBC Driver, open the ODBC Data Sources



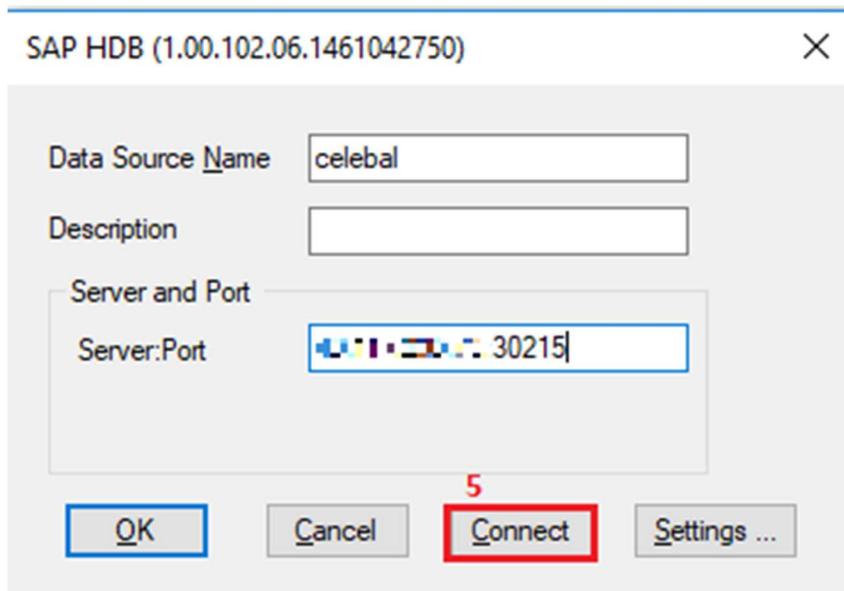
Step 2: Select 'System DSN' then click on Add



Step 3: Select HDBODBC and hit Finish



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

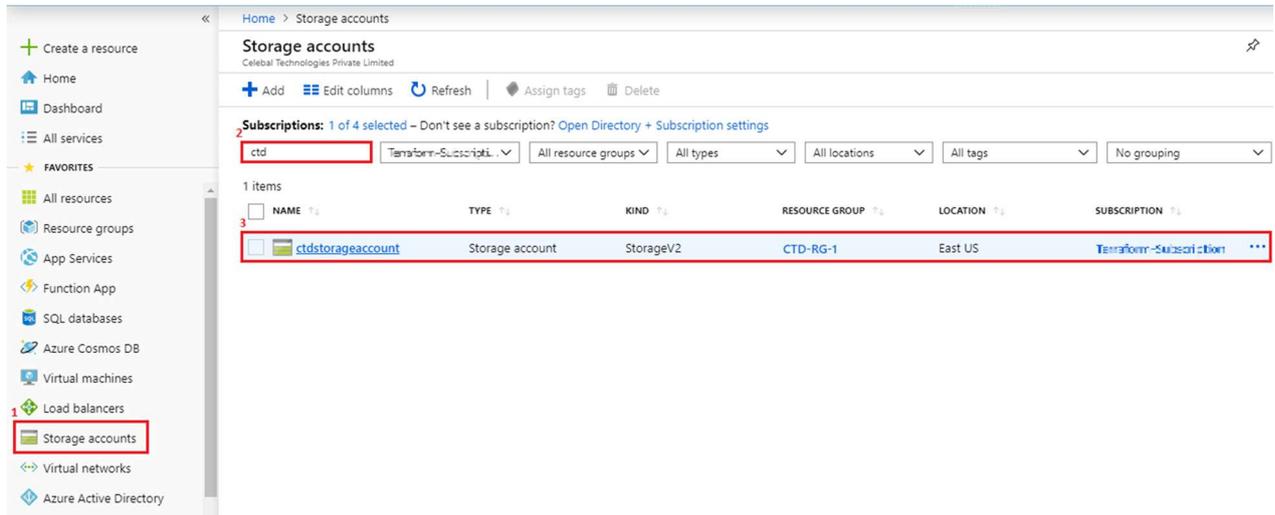


After this step another prompt will open, provide user and password then click on OK this will add HDBODBC Driver.

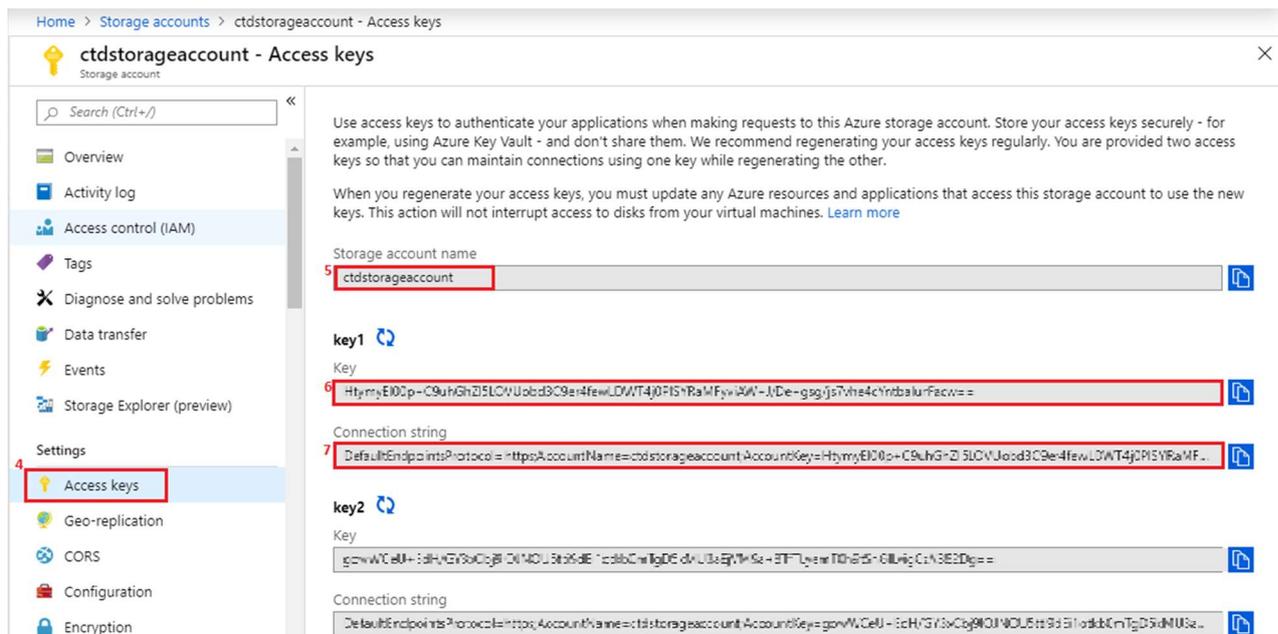
Azure Storage Account (Access Keys) and (Connection Strings)

Step 1: Log in to the Azure portal

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



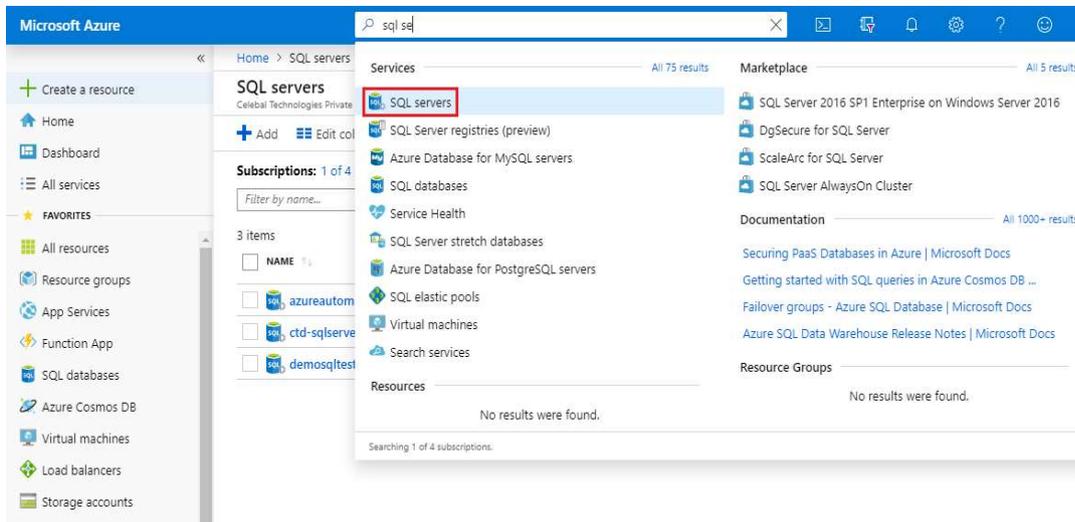
Step 3: Select **Access Keys** from blade then copy the Storage Account Name, Keys and Connection String for future reference



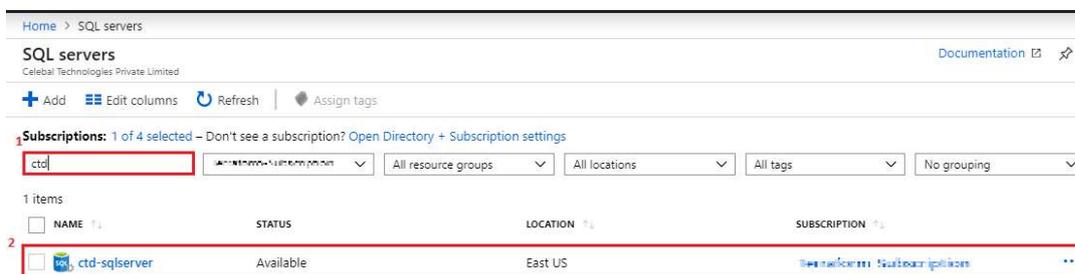
Azure SQL Server and Database (Connection Strings)

Step 1: Log in to the Azure portal

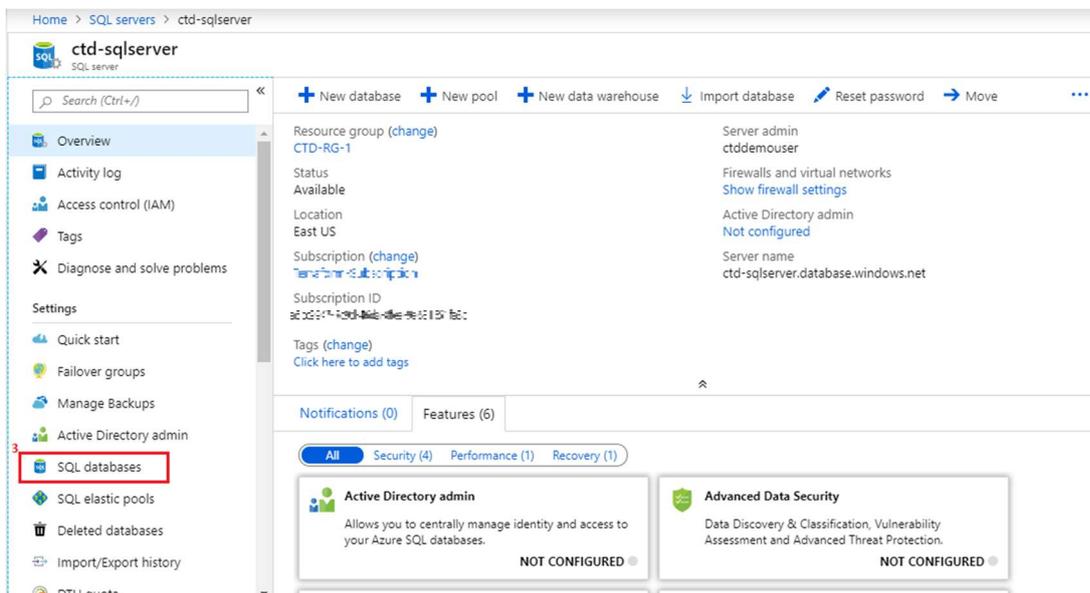
Step 2: Select **SQL Servers** from search tab



Step 3: Select the **SQL Server**



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



Step 5: Copy Database Name

The screenshot shows the 'ctd-sqlserver - SQL databases' page in the Azure portal. A table lists the databases with columns for 'DATABASE', 'STATUS', and 'PRICING TIER'. The row for 'CTD-SQL-Database' is highlighted with a red box, indicating it is the database to be copied.

DATABASE	STATUS	PRICING TIER
CTD-SQL-Database	Online	Standard S0: 10 DTUs

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

The screenshot shows the 'CTD-SQL-Database (ctd-sqlserver/CTD-SQL-Database)' details page. The 'Server name' is highlighted with a red box. Below the details, there is a 'Compute utilization' graph and a 'Show data for last' dropdown menu.

Server name: `ctd-sqlserver.database.windows.net`

Compute utilization: 100%, 90%, 80%, 70%

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

The screenshot shows the 'CTD-SQL-Database (ctd-sqlserver/CTD-SQL-Database) - Connection strings' page. The 'ADO.NET' tab is selected, and the connection string is highlighted with a red box. The connection string is: `Server=tcp:ctd-sqlserver.database.windows.net,1433;Initial Catalog=CTD-SQL-Database;Persist Security Info=False;User ID={your_username};Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;`

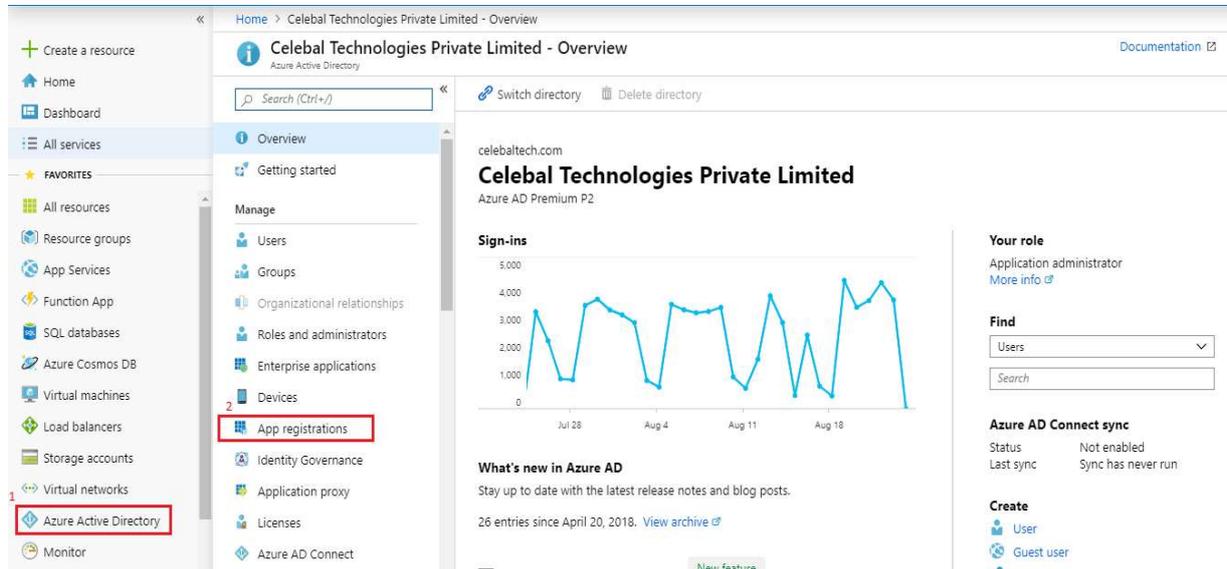
ADO.NET (SQL authentication)

Server=tcp:ctd-sqlserver.database.windows.net,1433;Initial Catalog=CTD-SQL-Database;Persist Security Info=False;User ID={your_username};Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;

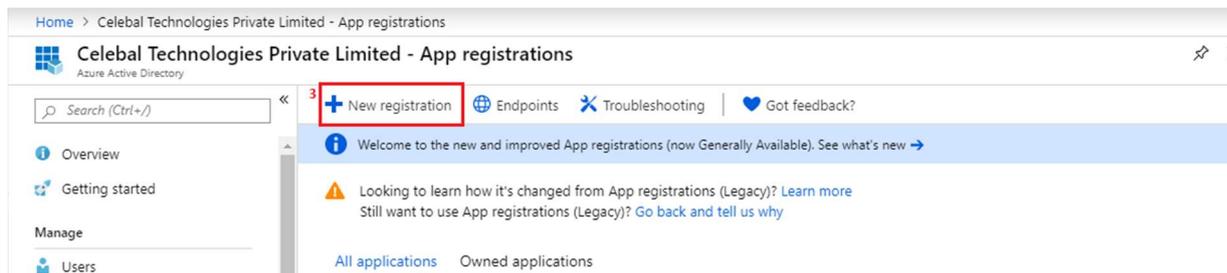
App Registrations (Azure Active Directory)

Step 1: Log in to the Azure portal.

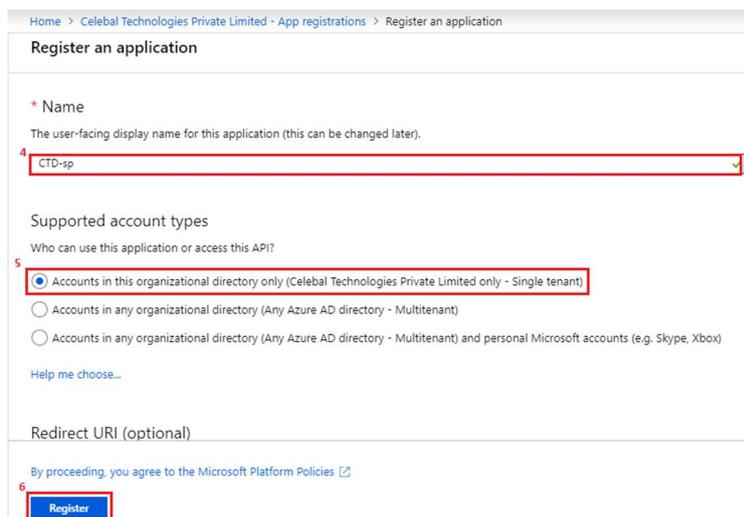
Step 2: Select **Azure Active Directory** then select 'App registrations'



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**

Home > Celebal Technologies Private Limited - App registrations > CTD-sp

CTD-sp

Search (Ctrl+/)

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? →

Display name: CTD-sp

Supported account types: My organization only

Application (client) ID: [Redacted]

Directory (tenant) ID: [Redacted]

Object ID: [Redacted]

Redirect URIs: Add a Redirect URI

Managed application in local directory: CTD-sp

Step 7: Select New client secret option

Home > Celebal Technologies Private Limited - App registrations > CTD-sp - Certificates & secrets

CTD-sp - Certificates & secrets

Search (Ctrl+/)

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Expose an API

Owners

Roles and administrators (Previ...

Manifest

Support + Troubleshooting

Troubleshooting

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

No certificates have been added for this application.

THUMBPRINT	START DATE	EXPIRES
------------	------------	---------

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

DESCRIPTION	EXPIRES	VALUE
Password uploaded on Sat Aug 24 2019	12/31/2299	-ct*****

Home > Celebal Technologies Private Limited - App registrations > CTD-sp - Certificates & secrets

CTD-sp - Certificates & secrets

Search (Ctrl+/)

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Expose an API

Owners

Roles and administrators (Previ...

Manifest

Add a client secret

Description

Expires

In 1 year

In 2 years

Never

Add Cancel

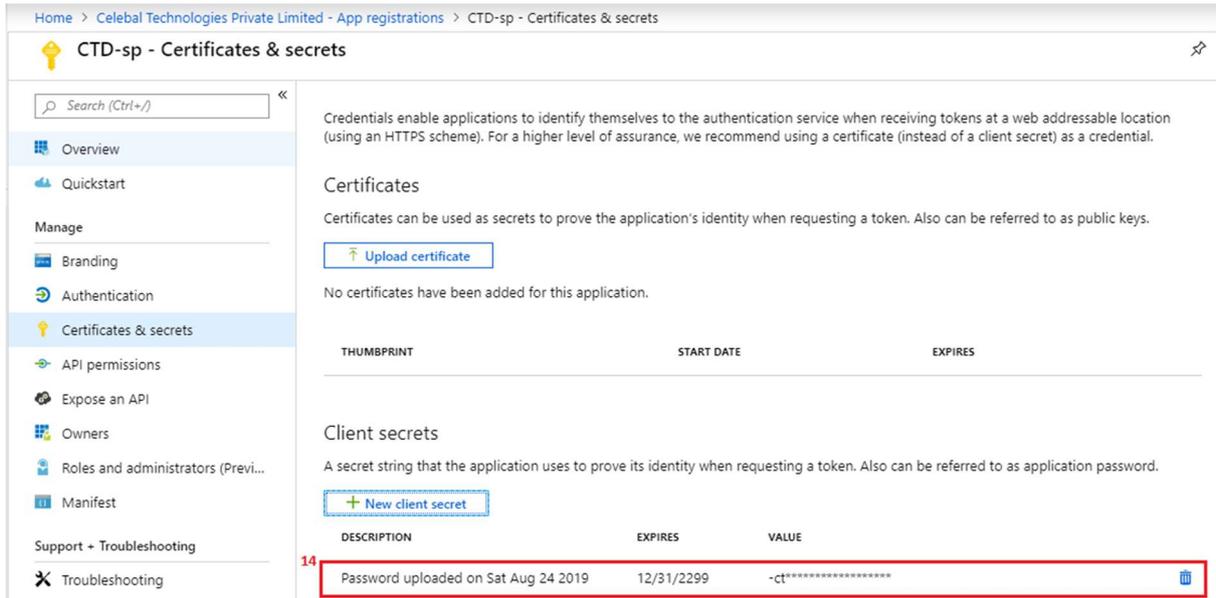
Client secrets

A secret string that the application uses to prove its identity when requesting a token.

New client secret

Step 8: Copy the client secret for future reference

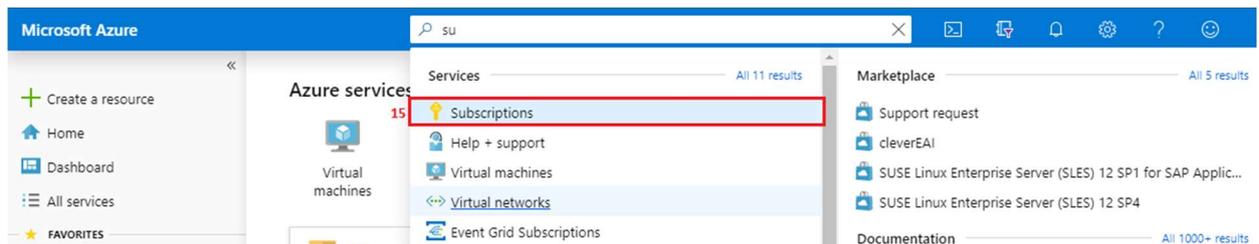
Note -: This client secret can only be seen for once so copy it for future reference or else you will have to regenerate it



The screenshot shows the 'Certificates & secrets' page in the Azure portal. The left sidebar contains navigation options like Overview, Quickstart, Manage (Branding, Authentication, Certificates & secrets), API permissions, Expose an API, Owners, Roles and administrators, Manifest, Support + Troubleshooting, and Troubleshooting. The main content area has a search bar and a description of credentials. Under 'Certificates', there is an 'Upload certificate' button and a note that no certificates have been added. Under 'Client secrets', there is a 'New client secret' button and a table with one entry:

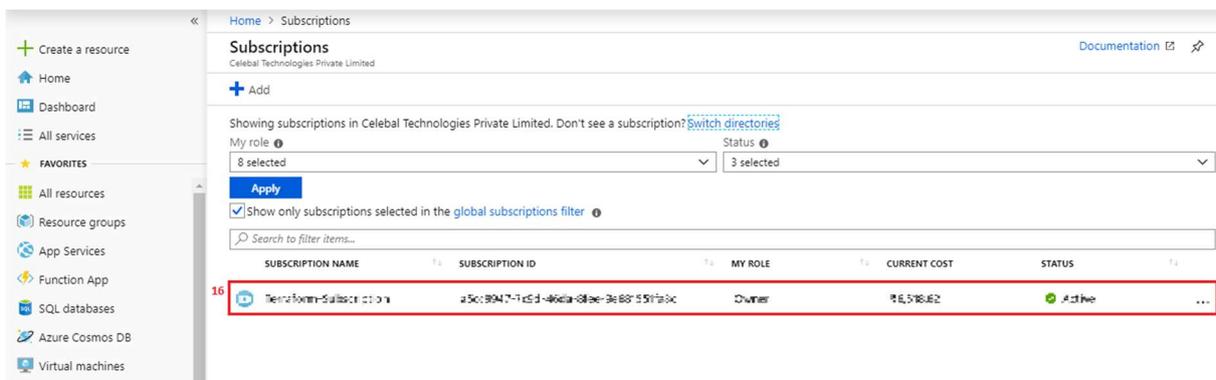
DESCRIPTION	EXPIRES	VALUE
Password uploaded on Sat Aug 24 2019	12/31/2299	-ct*****

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



The screenshot shows the Azure search results page. The search bar contains 'su'. The search results are categorized into 'Services' (11 results), 'Marketplace' (5 results), and 'Documentation' (1000+ results). Under the 'Services' category, 'Subscriptions' is highlighted with a red box. Other services listed include 'Help + support', 'Virtual machines', 'Virtual networks', and 'Event Grid Subscriptions'.

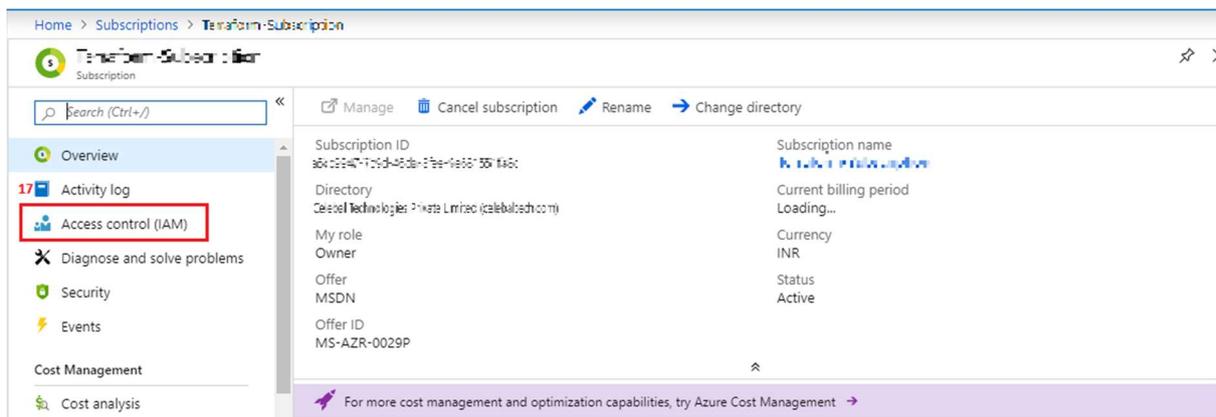
Step 10: Copy Subscription Id of your subscription



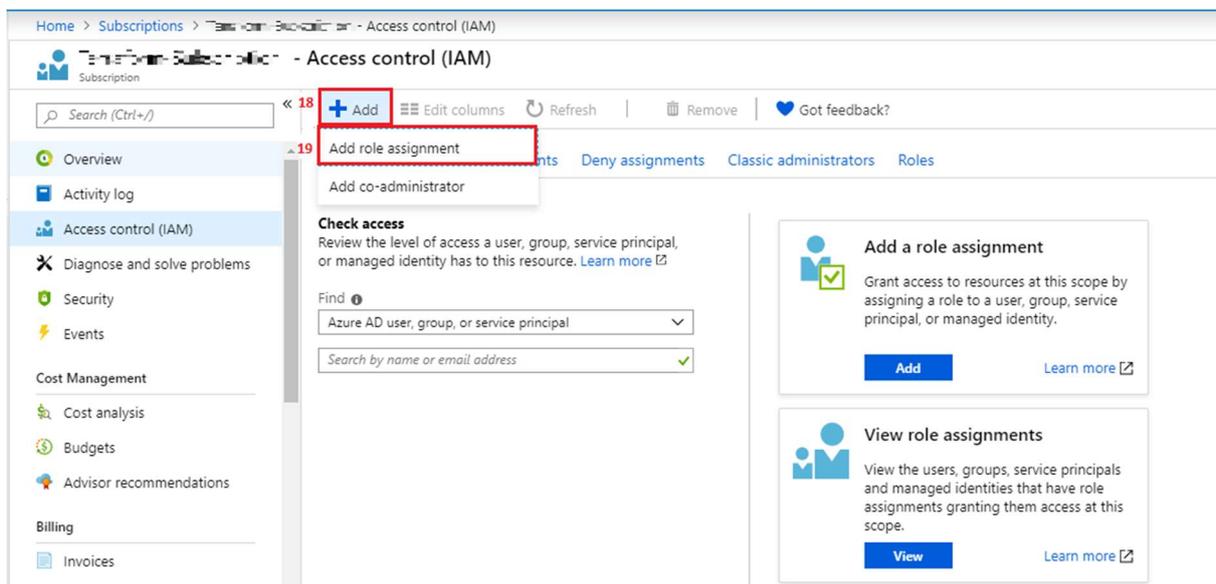
The screenshot shows the 'Subscriptions' page in the Azure portal. The left sidebar contains navigation options like Create a resource, Home, Dashboard, All services, FAVORITES, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, and Virtual machines. The main content area shows a table of subscriptions with the following columns: SUBSCRIPTION NAME, SUBSCRIPTION ID, MY ROLE, CURRENT COST, and STATUS. One subscription is highlighted with a red box:

SUBSCRIPTION NAME	SUBSCRIPTION ID	MY ROLE	CURRENT COST	STATUS
Microsoft Azure Subscription	a5c39d17-71e5-d461a-01ba-3e805517a30c	Owner	\$6,518.62	Active

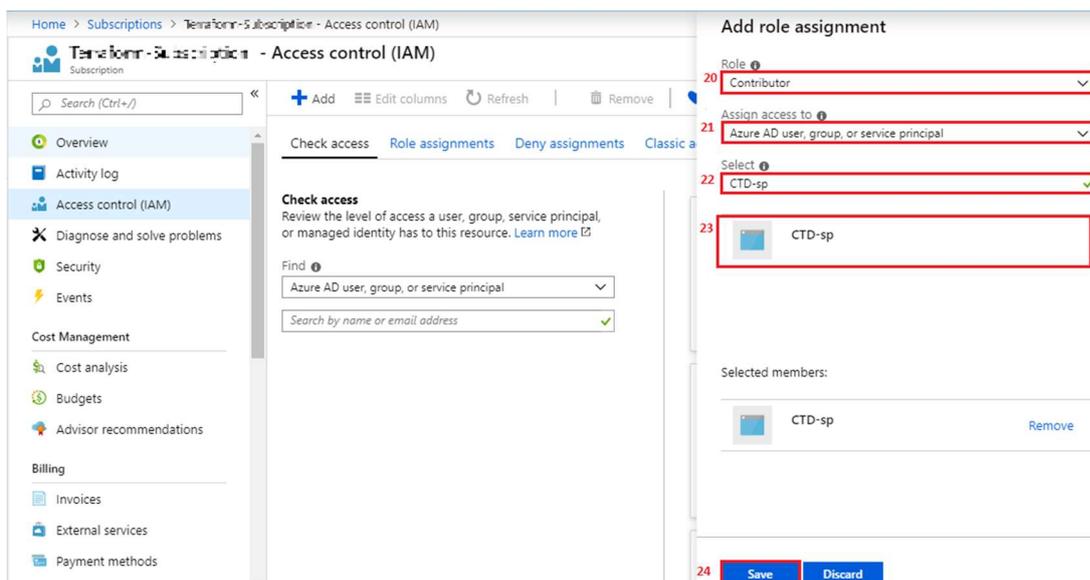
Step 11: Select Access Control (IAM) from the blade



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



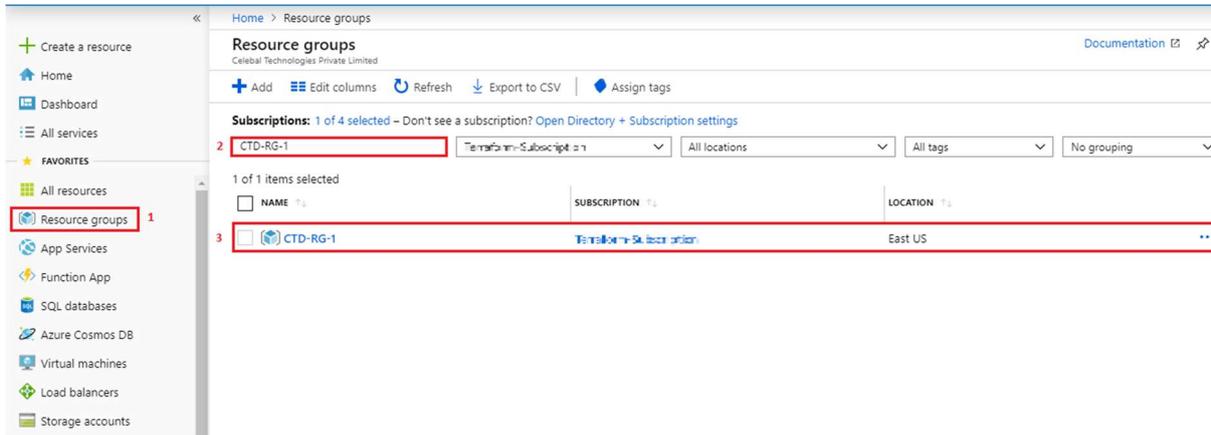
Step 13: Assign 'Contributor' role and select the registered app then click save



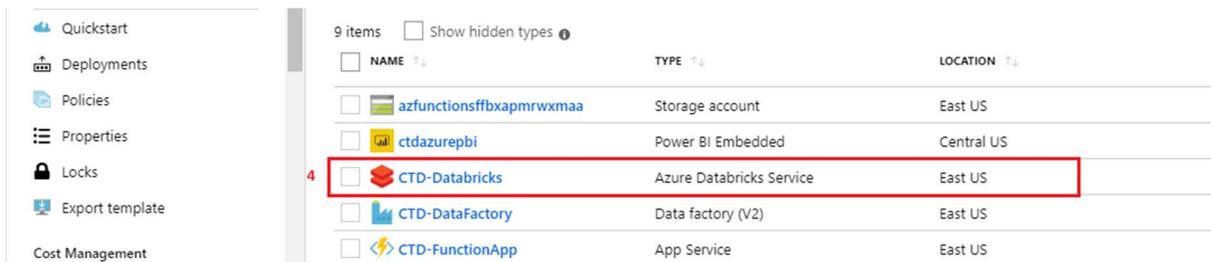
Steps for generating Databricks Access Token

Step 1: Log in to the Azure portal

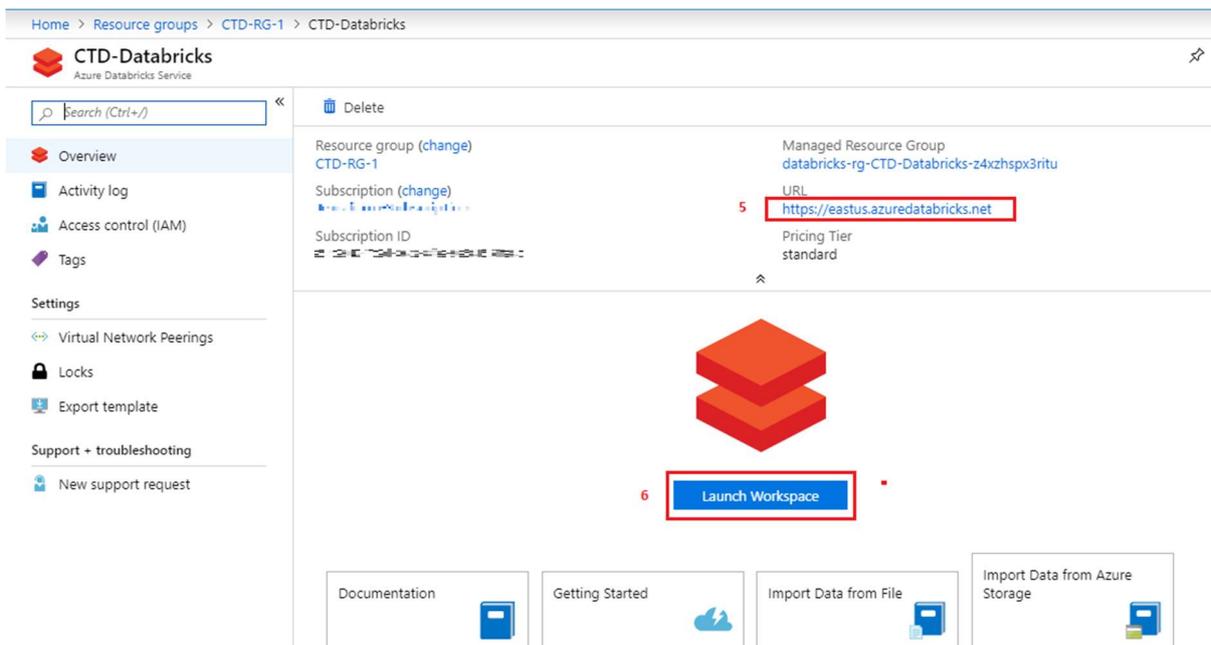
Step 2: Select **Resource groups** from Blade then select your Resource group



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

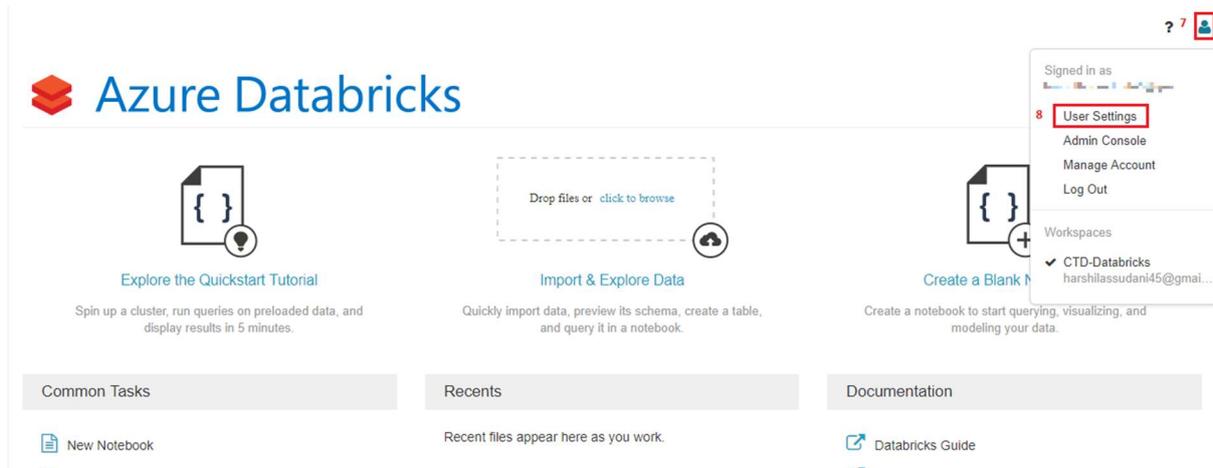


Step 4: Copy the workspace URL for future Reference then Launch Workspace



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

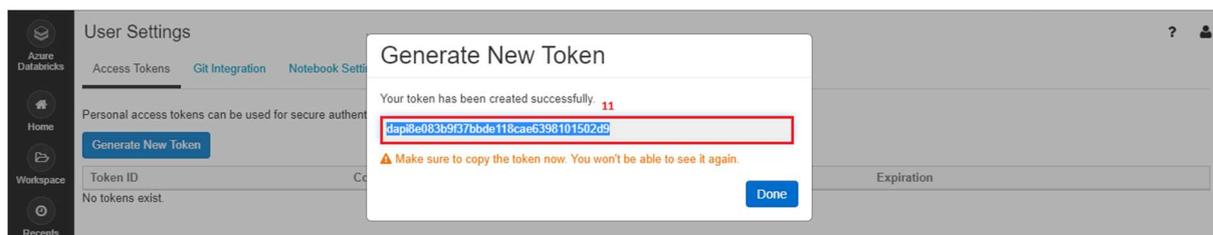
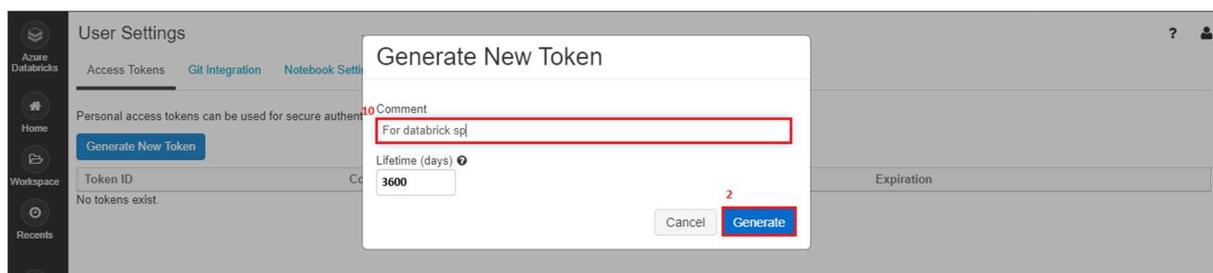
Step 6: Select **User Settings**



Step 7: Click on 'Generate New Token'



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

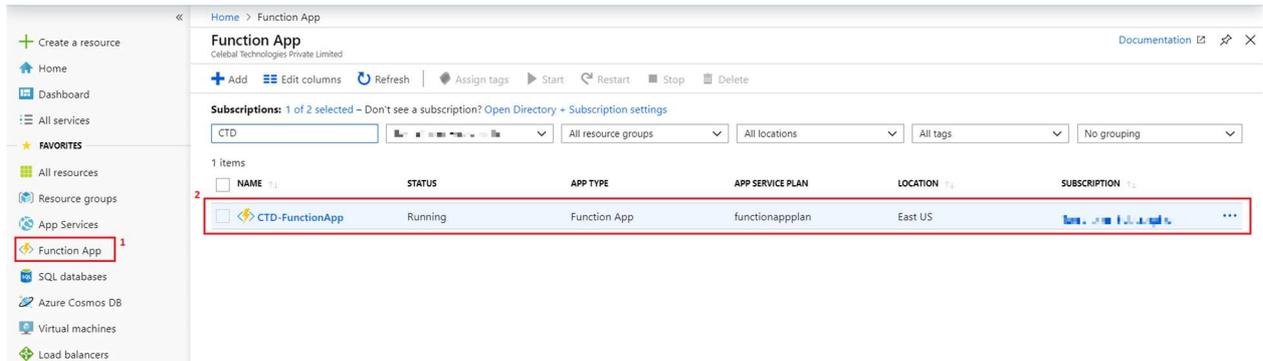


Note-: This token will be generated only once, so copy this token for future reference

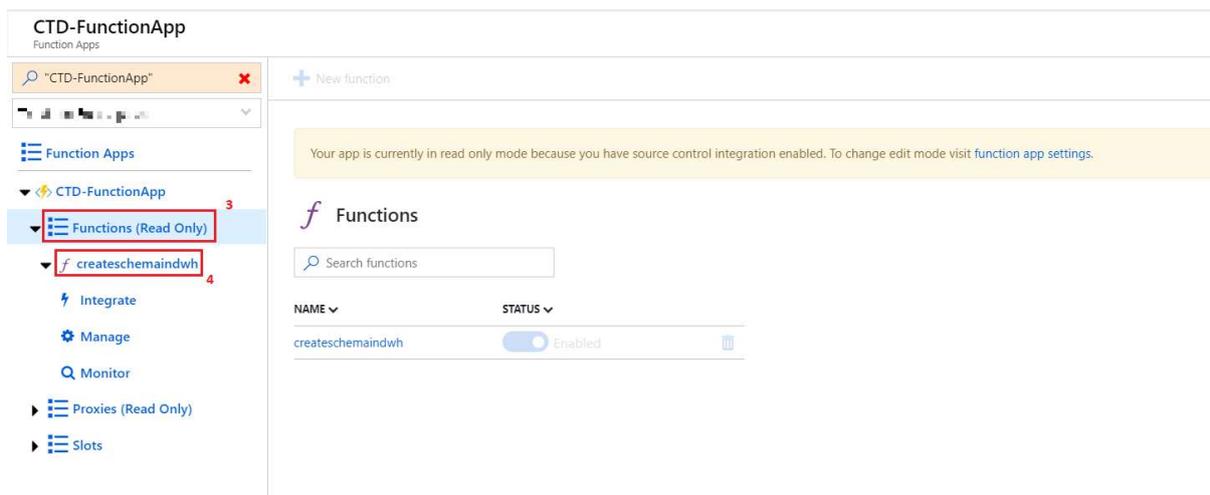
Azure Function App (URL)

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



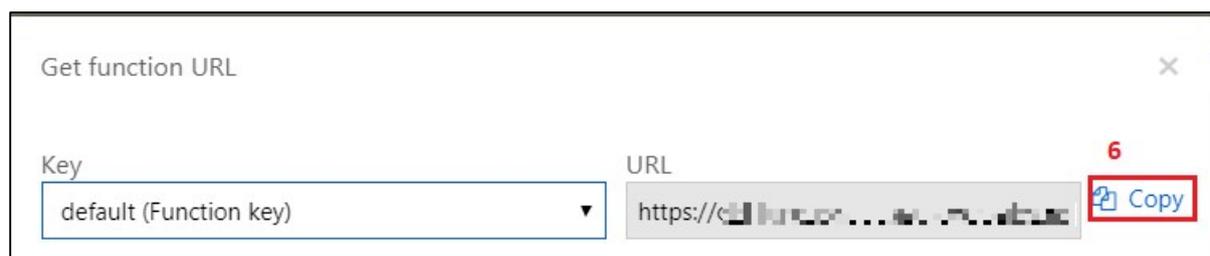
Step 3: Select the Functions from function apps blade and then select the deployed function



Step 4: Click on 'Get Function URL'

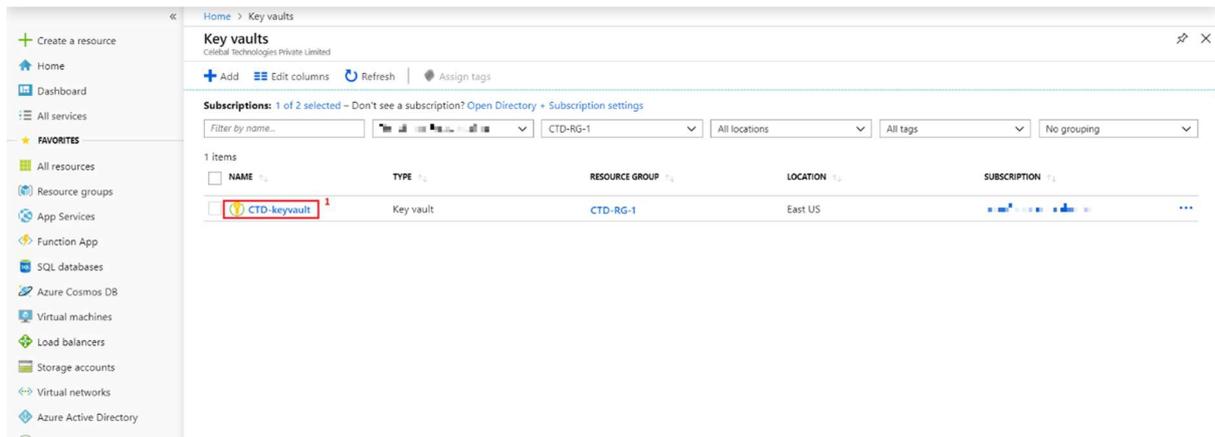


Step 5: Copy the function URL for future reference

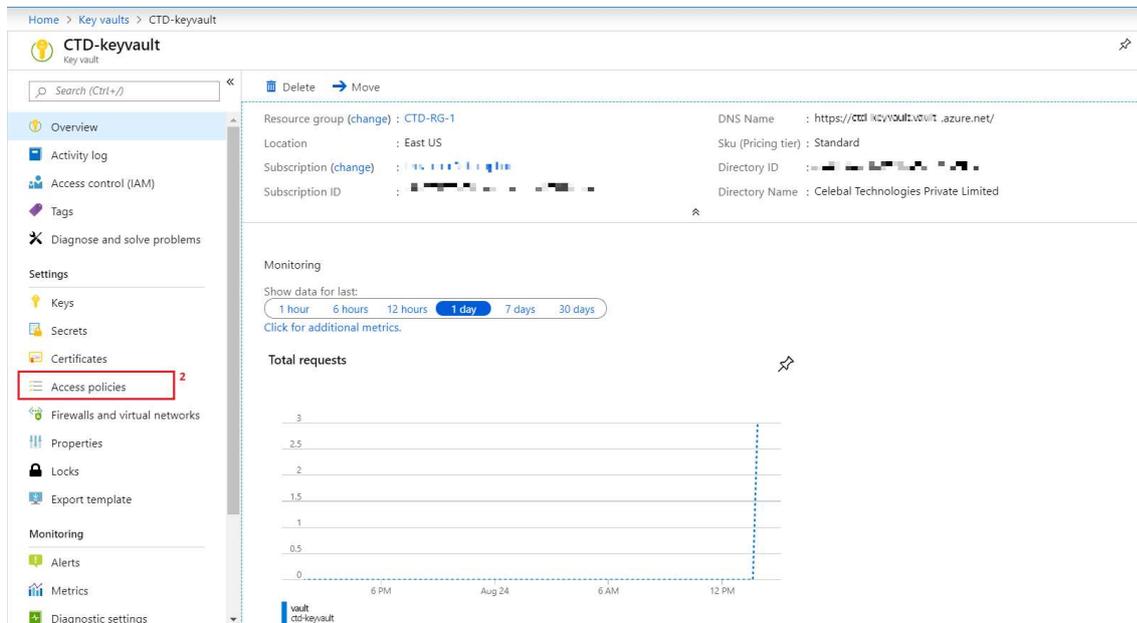


Key Vault Access Policy to see your Secrets in Key vault

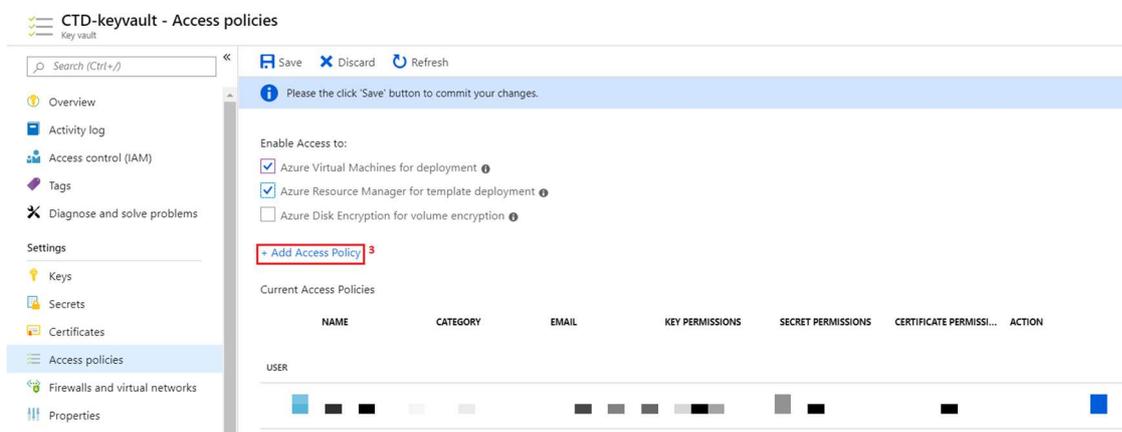
Step 1: From the Azure portal, select your Key Vault



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'

The screenshot shows the 'Add access policy' page in the Azure portal. The page has a breadcrumb trail: Home > Key vaults > CTD-keyvault - Access policies > Add access policy. The main content area includes several dropdown menus: 'Configure from template (optional)' set to 'Key, Secret, & Certificate Management' (marked with a red box and '4'), 'Key permissions' set to '9 selected', 'Secret permissions' set to '7 selected', and 'Certificate permissions' set to '15 selected'. Below these is the 'Select principal' section, which is currently empty and marked with a red box and '5'. At the bottom is an 'Add' button. A 'Principal' blade is open on the right side, titled 'Principal' with the subtitle 'Select a principal'. It has a search box containing 'abhishek' (marked with a red box and '6') and a list of members. The 'Selected member' field is empty, and the 'No member selected' message is visible. At the bottom of the blade is a 'Select' button (marked with a red box and '7').

Step 6: Now click on 'ADD'

This is a close-up screenshot of the 'Add access policy' page. The 'Select principal' field now contains the text 'abhishekvarshney.cse21' (marked with a red box and '8') and a red asterisk icon to its left. The 'Add' button at the bottom is also highlighted with a red box and '8'. All other elements, including the breadcrumb trail and the permission dropdowns, remain the same as in the previous screenshot.

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

The screenshot shows the 'Access policies' blade for a Key Vault. The left-hand navigation pane includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Keys, Secrets, Certificates), Firewalls and virtual networks, Properties, Locks, Export template, and Monitoring (Alerts). The main area displays 'Enable Access to:' with three unchecked options: 'Azure Virtual Machines for deployment', 'Azure Resource Manager for template deployment', and 'Azure Disk Encryption for volume encryption'. Below this is a '+ Add Access Policy' link. The 'Current Access Policies' section contains a table with the following data:

NAME	CATEGORY	EMAIL	KEY PERMISSIONS	SECRET PERMISSIONS	CERTIFICATE PERMISSI...	ACTION
USER						
abhishekvarshney.c...	USER	abhishekvarshney.c...	9 selected	7 selected	15 selected	Delete

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

The screenshot shows the 'Secrets' blade in Azure Key Vault. The left-hand navigation pane is the same as in the previous image, but 'Secrets' is highlighted. The main area displays a table of secrets with the following data:

NAME	TYPE	STATUS
AppServiceName		✓ Enabled
AppServiceURL		✓ Enabled
AzureFunctionURL		✓ Enabled
ClientSecret		✓ Enabled
ClientID		✓ Enabled
DatabricksName		✓ Enabled
DataBricksToken		✓ Enabled
DataBricksWorkspaceURL		✓ Enabled
DataFactoryName		✓ Enabled
PowerBIEmbeddedAdmin		✓ Enabled
PowerBIEmbeddedName		✓ Enabled
ResourceGroupLocation		✓ Enabled
ResourceGroupName		✓ Enabled
SQLConnectionString		✓ Enabled
sqlconnectionstringjdbc		✓ Enabled
SQLDatabaseName		✓ Enabled

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/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/resourcegroups/databricksg/providers/Microsoft.KeyVault/vaults/databricksKV –Resource Id

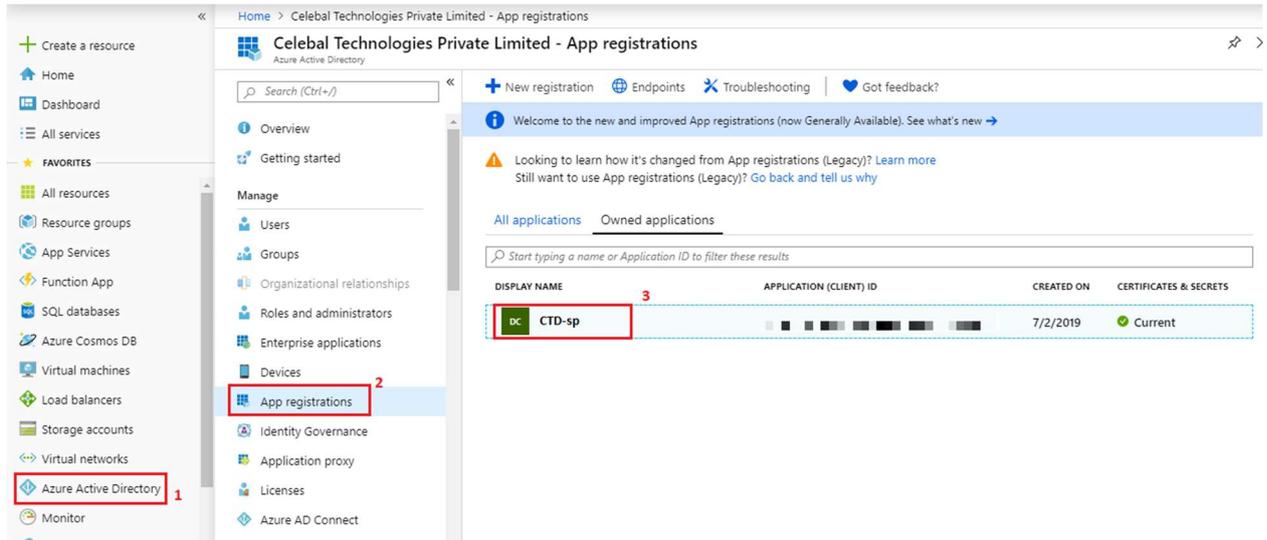
App Service Authentication & Authorization

I. Azure Active Directory

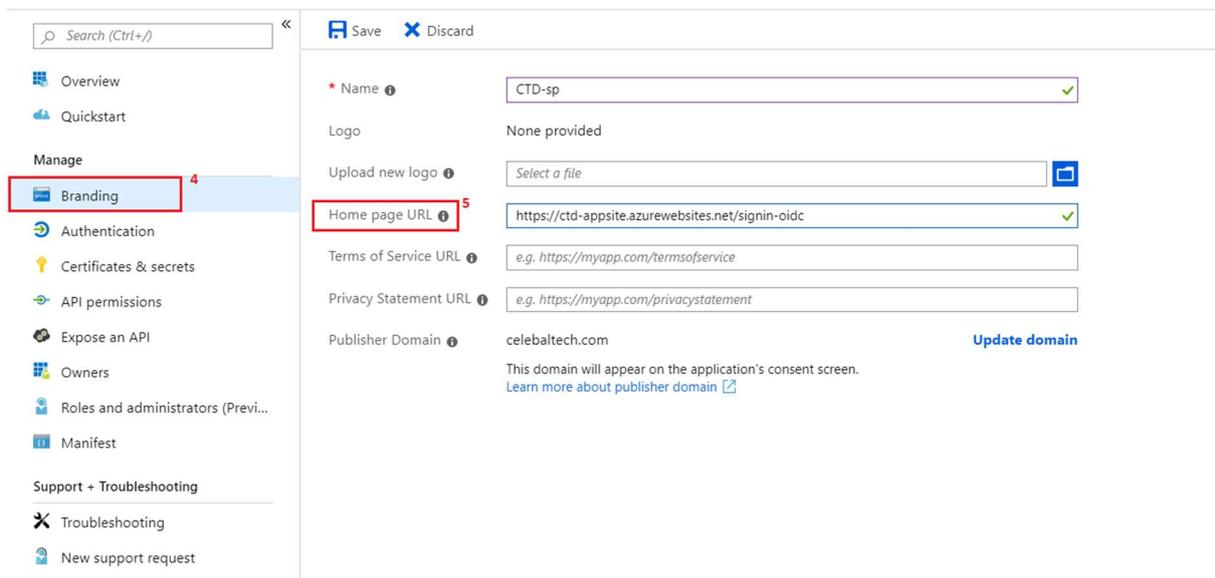
Step 1: Log in to the Azure portal

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

Step 3: Select the registered app

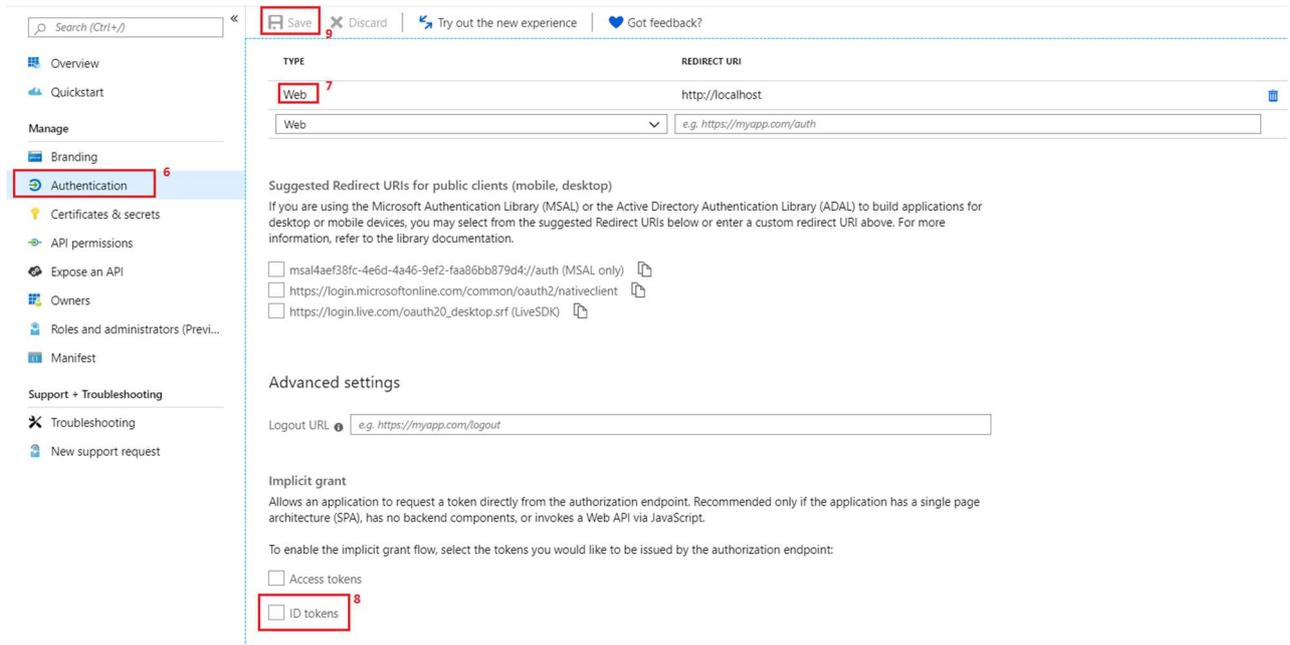


Step 4: Select **Branding** and enter the value of 'Home Page URL' and then save it



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

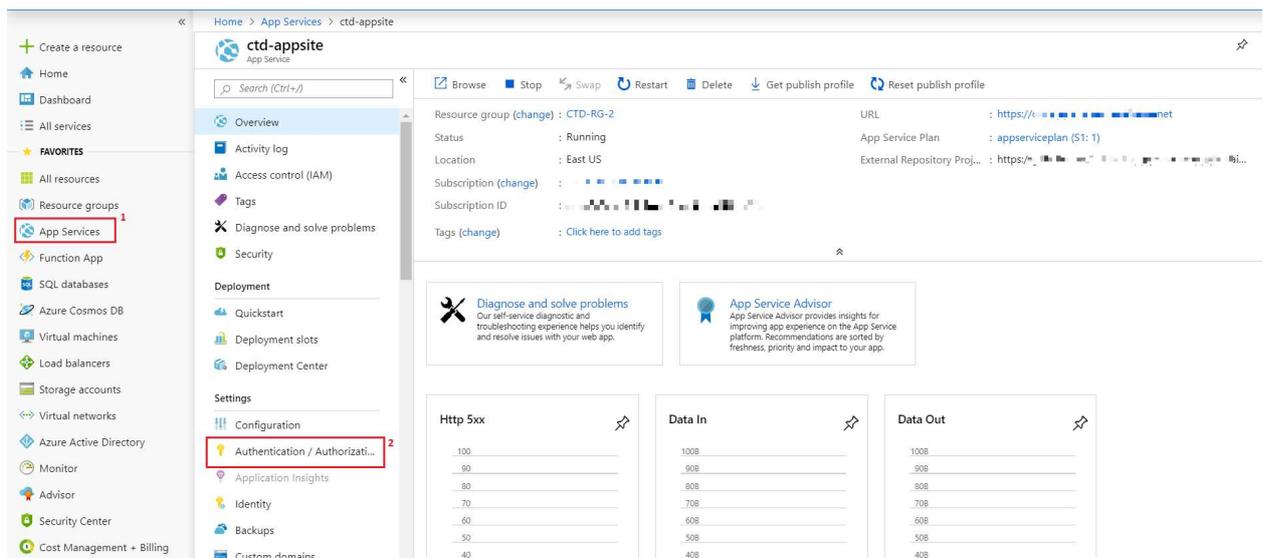
Step 5: Select **Authentication** then enter the URL then check the 'ID Token' checkbox and save it.



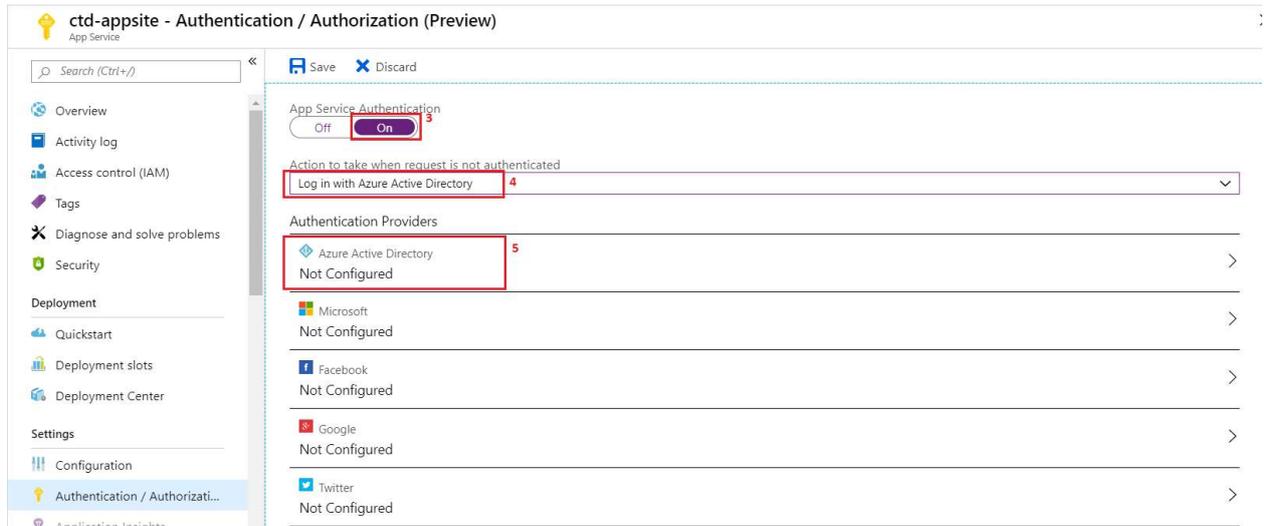
Note:- In URL mention {your App Service URL} /.auth/login/aad/callback

II. APP SERVICE

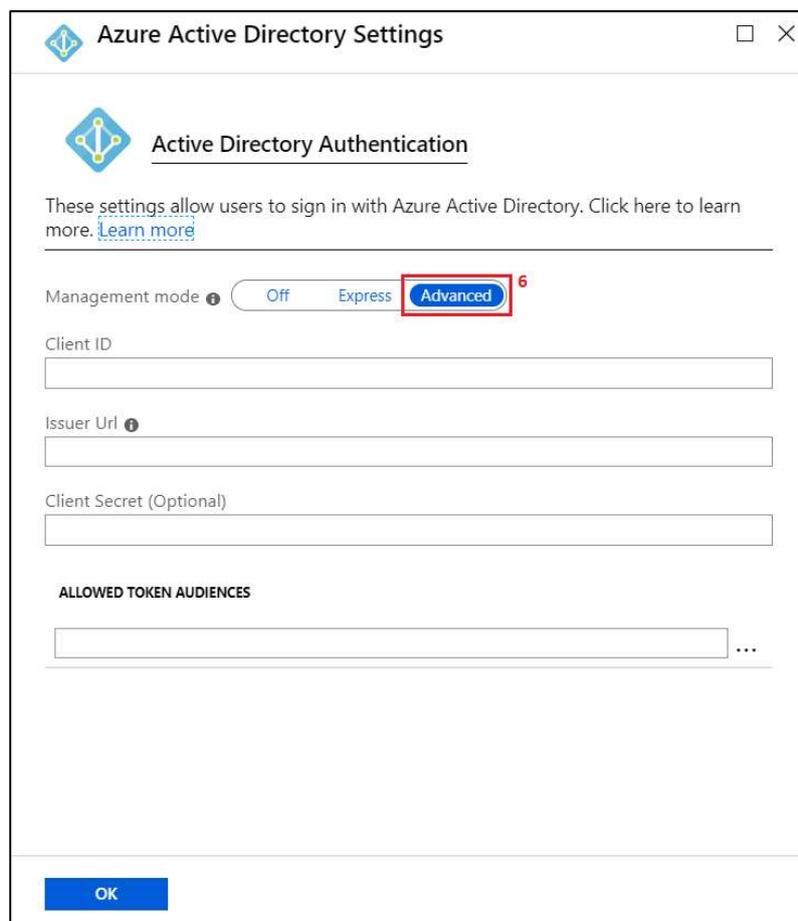
Step 1: Select **App Services** from the blade then select the Authentication/Authorization option



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

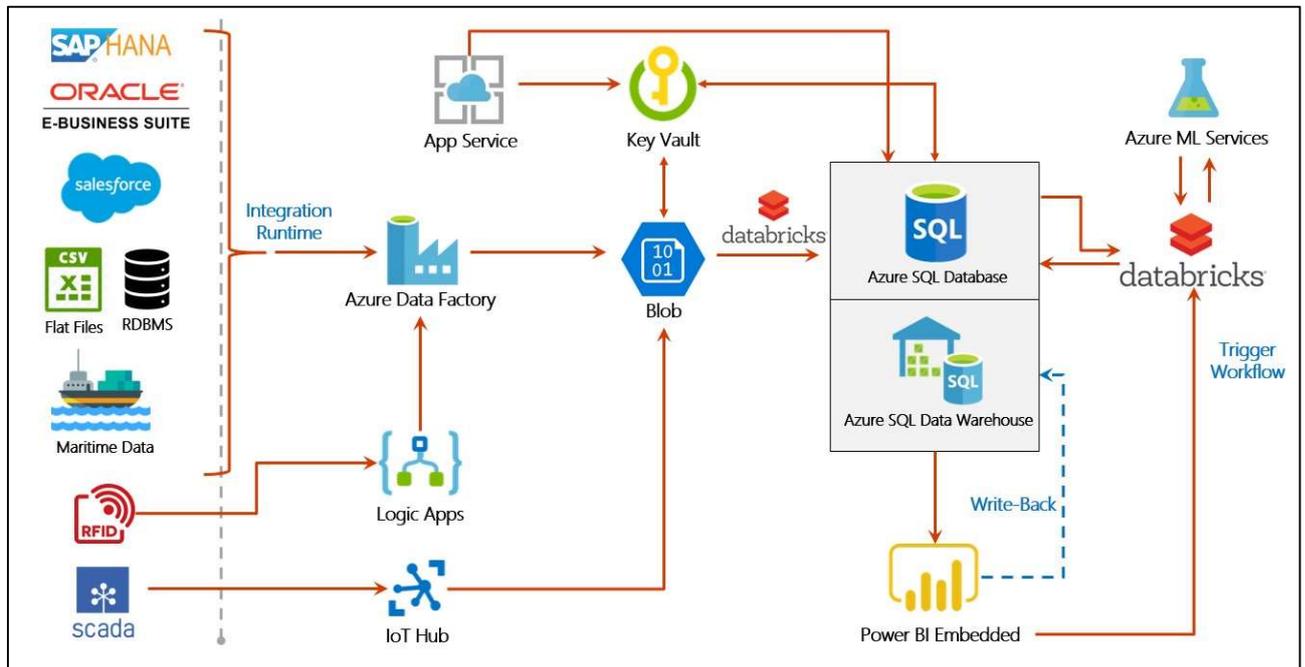


Step 3: Select the Management mode as 'Advanced', enter the Client ID and Tenant ID in Issuer URL as shown below



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.