Enable SSO for Azure Relational Connections

Contents:

You can extend the basic SSO integration between the Trifacta® platform and the Azure infrastructure to include SSO connections to Azure-based relational sources.

Supported relational connection types:

- Azure SQL Database
- SQL Datawarehouse

Pre-Requisites

- SSO integration to Azure AD must be enabled. See *Configure SSO for Azure AD*.

Limitations

1. Sharing of Azure connections is supported in the following manner:
   a. Non-SSO Azure connections: Shared normally, with or without credentials.
   b. SSO Azure connections:
      i. The connection can be shared, but the credentials cannot.
      ii. If the user who is shared the connection attempts to use it, that user's SSO principal is used. If that SSO principal has the same permissions as the original user, then the connection is fully operational. If not, then some data may not be accessible.
2. Write operations to SQL Datawarehouse are not supported for Azure SSO connections.

Configure Azure AD for Trifacta platform

Your Azure admin must enable the following:

1. Your SQL Server database must have an Active Directory Admin assigned to it.
   a. This assignment must be applied for SQL DB and SQL DW connections.
2. Each user that is creating and using SQL Server connections over SSO must have a corresponding account in the SQL Server database.
3. To the Azure AD application, the "Azure SQL Database - user impersonation" permissions must be added.

For more information, please contact your Azure administrator.

Configure Trifacta platform for Azure AD

Define scope

You can define the scope of access in either of the following ways:

1. The Azure admin can manually define access for individual databases, or:
2. You can do the following on the Trifacta node:
    a. SSH to the Trifacta node. Login as an administrator.
    b. Navigate to the following:

```
/opt/trifacta/conf/
```

    c. Open `trifacta-conf.json`.
    d. Locate the `azure.sso.scope` property. Add this value to the property:

```
"https://database.windows.net/user_impersonation"
```

    It is the second line in the following:

> **NOTE:** If there are now multiple values in the entry, a comma must be placed after every line except for the last one.

```
{
    "azure": {
        "sso": {
            "scope": [
                "https://datalake.azure.net/user_impersonation",
                "https://database.windows.net/user_impersonation"
            ]
        }

    }
}
```

    e. Save the file.

Enable SSO credential type

> **NOTE:** This configuration applies only for SQL DW connections. However, even if you are not creating these connections immediately, you should perform this configuration change.

When you create Azure SSO relational connections, you must select `azureTokenSso` for the credential type.

- For SQL DB connections, this selection is automatically enabled.
- For SQL DW connections, you must specify that this option is available by making a manual edit to a file on the Trifacta node.

Steps:

1. SSH to the Trifacta node. Login as an administrator.
2. Navigate to the following directory:

```
/opt/trifacta/service/data-service/build/conf/vendor/sqldatawarehouse
```

3. Edit `connection-metadata.json`.
4. Locate the `credentialType` property. Set the value to `azureTokenSso`.
5. Save your changes and restart the platform.

Create Connections

When you create a relational connection where Azure SSO has been enabled, select `Azure Token SSO` from the Credential Type drop-down.

> **NOTE:** The SSO principal of the user who is creating or accessing the connection is used to connect to the specified database.

- See *Create Azure SQL Database Connections*.
- See *Create SQL DW Connections*.

User Access

Users can access the connections through the Import Data page. See *Import Data Page*.