



Informatica® Metadata Command Center
November 2025

Microsoft Azure Synapse Analytics Sources

© Copyright Informatica LLC 2025

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica, Informatica Cloud, Informatica Intelligent Cloud Services, PowerCenter, PowerExchange, and the Informatica logo are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at <https://www.informatica.com/trademarks.html>. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2025-11-20

Table of Contents

Preface.	4
Chapter 1: Introduction to Microsoft Azure Synapse Analytics catalog sources.	5
Extraction and view process.	6
About the Microsoft Azure Synapse Analytics catalog source.	7
Extracted metadata.	7
Compatible connectors.	12
Chapter 2: Before you begin.	13
Verify permissions.	13
Permissions for metadata extraction.	13
Permissions to run data classification.	13
Permissions to run glossary association.	13
Create a connection.	14
Admin User connection mode.	15
Service Principal connection mode.	15
Proxy properties.	15
Create endpoint catalog sources for connection assignment.	16
Chapter 3: Create catalog sources in Metadata Command Center.	17
Step 1. Register a catalog source.	17
Step 2. Configure capabilities.	19
Configure metadata extraction.	19
Configure lineage discovery.	22
Configure data classification.	23
Configure glossary associations.	24
Step 3. Associate stakeholders and asset groups.	24
Step 4. Run or schedule the job.	26
Step 5. Assign reference catalog source connections to endpoint catalog source objects.	27
Chapter 4: View results in Data Governance and Catalog.	29
View metadata extraction results.	29
View data lineage.	31
View lineage at the catalog source level.	31
View lineage at the data set level.	31
View lineage at the data element level.	32
View classified data.	33
View glossary associations.	34

Preface

Read *Microsoft Azure Synapse Analytics Sources* to learn how to register and configure Microsoft Azure Synapse Analytics sources as catalog sources in Metadata Command Center. After you configure a catalog source, you extract metadata and then view the results in Data Governance and Catalog.

CHAPTER 1

Introduction to Microsoft Azure Synapse Analytics catalog sources

You can use Metadata Command Center to extract metadata from a source system.

A source system is any system that contains data or metadata. For example, Microsoft Azure Synapse Analytics is a source system from which you can extract metadata through a Microsoft Azure Synapse Analytics catalog source. A catalog source is an object that represents and contains metadata from the source system.

Before you extract metadata from a source system, you first create and register a catalog source that represents the source system. Then you configure capabilities for the catalog source. A capability is a task that Metadata Command Center can perform, such as metadata extraction, lineage discovery, data profiling, data classification, or glossary association.

When Metadata Command Center extracts metadata, Data Governance and Catalog displays the extracted metadata and its attributes as technical assets. You can then perform tasks such as analyzing the assets, viewing lineage, and creating links between those assets and their business context.

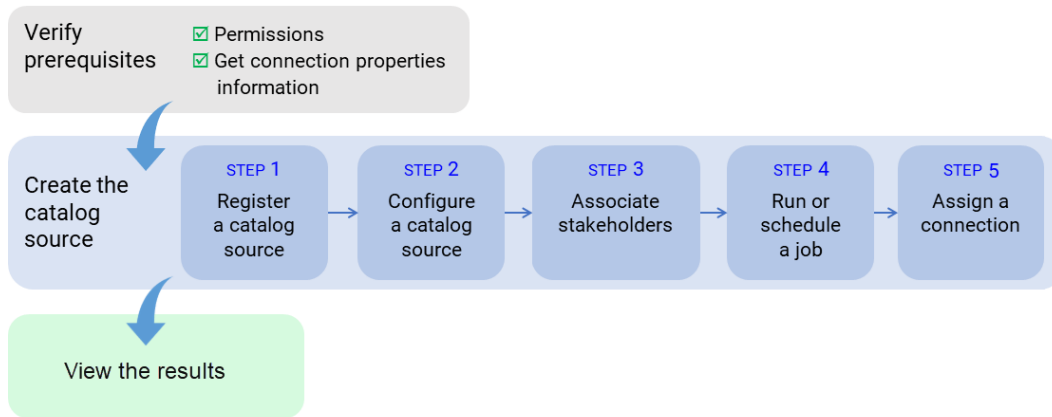
The following table describes the capabilities of the catalog source:

Capability	Description
Lineage Discovery	Builds the complete lineage of a catalog source by recommending endpoint catalog source objects to assign to reference catalog source connections. When you run the catalog source job, Metadata Command Center assigns the reference catalog source connections to CLAIRE recommended endpoint catalog source objects. You can then view the list of CLAIRE recommendations and accept or reject them.
Data Classification	Data classification is the process of identifying and organizing data into relevant categories based on the functional meaning of the data. Classifying data can help your organization manage risks, compliance, and data security.
Glossary Association	You can associate terms that are in the glossary with technical assets to provide user-friendly business names to technical assets. Glossary Association automatically associates glossary terms with technical assets or recommends glossary terms that you can manually associate with technical assets in Data Governance and Catalog.

Extraction and view process

To extract metadata from a source system, configure the catalog source and run the extraction job in Metadata Command Center. Then view the results in Data Governance and Catalog.

The following image shows the process to extract metadata from a Microsoft Azure Synapse Analytics source system:



After you verify prerequisites, perform the following tasks to extract metadata from Microsoft Azure Synapse Analytics:

1. Register a catalog source. Create a catalog source object, select Microsoft Azure Synapse Analytics, and then select and test the connection
2. Configure the catalog source. Specify the runtime environment and configure parameters for metadata extraction. Optionally, add filters to include or exclude source system assets from metadata extraction. You can also configure other capabilities such as data profiling and quality, data classification, or glossary association.
3. Optionally, associate stakeholders. Associate users with technical assets, giving the users permission to perform actions determined by their roles.
4. Run or schedule the catalog source job.
5. Optionally, if the catalog source job generates referenced asset objects, you can assign a connection to referenced source system assets.
You can view the lineage with object references without performing connection assignment. After connection assignment, you can view the objects.

Run the catalog source again after you assign connections to referenced source system assets.

After you run the catalog source job, you view the results in Data Governance and Catalog.

About the Microsoft Azure Synapse Analytics catalog source

You can use the Microsoft Azure Synapse Analytics catalog source to extract metadata from a Microsoft Azure Synapse Analytics source system.

Microsoft Azure Synapse Analytics is an enterprise analytics service that enables insight across data warehouses and big data systems.

Extracted metadata

You can use the Microsoft Azure Synapse Analytics catalog source to extract metadata from a Microsoft Azure Synapse Analytics source system.

Metadata Command Center extracts notebooks and pipelines from a Microsoft Azure Synapse Analytics source system.

Extracted notebook objects

Metadata Command Center extracts the following notebook objects from a Microsoft Azure Synapse Analytics source system:

- Calculation
- Cell
- Folder
- Notebook Definition
- Notebook Instance
- Workspace

You can extract metadata from Microsoft Azure Synapse Analytics notebooks with the following programming languages:

- Python
- SQL

You can extract metadata from Microsoft Azure Synapse Analytics notebooks with the following Python functionalities:

- Standard language constructions
- Standard built-in functions
- Partially-compatible modules:

Note: Data Governance and Catalog processes only a subset of library functions of partially-compatible modules.

- abs
- adal
- argparse
- array
- ast
- azure

- base64
- binascii
- calendar
- codecs
- collections
- concurrent
- contextlib
- contextvars
- copy
- copyreg
- csv
- dataclasses
- datetime
- decimal
- delta
- difflib
- distutils
- email
- enum
- errno
- fnmatch
- fractions
- functools
- gc
- genericpath
- gettext
- glob
- graphframes
- hashlib
- heapq
- hmac
- importlib
- inspect
- io
- itertools
- json
- keyword
- locale
- logging

- math
- matplotlib
- mssparkutils
- nt
- numbers
- numpy
- operator
- os
- pandas
- pathlib
- pickle
- pkgutil
- posix
- posixpath
- pprint
- py4j
- pyodbc
- pyspark
- pytz
- random
- re
- reprlib
- requests
- seaborn
- secrets
- shutil
- simplejson
- six
- sklearn
- smtplib
- socket
- ssl
- stat
- string
- struct
- subprocess
- sys
- teradatasql
- textwrap

- threading
- time
- traceback
- types
- typing
- urllib
- urllib3
- uuid
- warnings
- weakref
- xml
- yaml
- zipfile
- zlib

- Custom libraries

Note: Custom libraries are libraries created by a user.

If a Microsoft Azure Synapse Analytics catalog source detects an incompatible function or library, it can't process the statement. It skips the statement and continues to process the next one.

Extracted pipeline objects

Metadata Command Center extracts the following pipeline objects from a Microsoft Azure Synapse Analytics source system:

- Activity
- Activity Instance
- Calculation
- Folder
- Pipeline
- Pipeline Instance
- Workspace

The Microsoft Azure Synapse Analytics catalog source is compatible with the following Pipeline Activity and Dataset components:

Component name	Description
Copy	Pipeline activity
ExecuteDataFlow	Pipeline activity.
ExecuteSSISPackage	Pipeline activity. Supported page locations: <ul style="list-style-type: none"> - File System (Package) - Embedded Package

Component name	Description
GetMetadata	Pipeline activity
Lookup	Pipeline activity
SqlServerStoredProcedure	Pipeline activity
IfCondition	Pipeline activity
Switch	Pipeline activity
Until	Pipeline activity
ForEach	Pipeline activity
Wait	Pipeline activity
SetVariable	Pipeline activity
ExecutePipeline	Pipeline activity
WebActivity	Pipeline activity
DatabricksNotebook	Pipeline activity
Binary	Dataset
DelimitedText	Dataset
Excel	Dataset
Json	Dataset
Parquet	Dataset
FileShare	Dataset
AmazonRedshiftTable	Dataset
AzureSqlDWTTable	Dataset
AzureSqlTable	Dataset
DynamicsCrmEntity	Dataset
OracleTable	Dataset
SalesforceObject	Dataset
SnowflakeTable	Dataset
SqlServerTable	Dataset
AzureDatabricksDeltaLakeDataset	Dataset

Compatible connectors

Before you configure a Microsoft Azure Synapse Analytics catalog source, you must connect to the Microsoft Azure Synapse Analytics source system.

Use the Microsoft Azure Synapse Analytics connector to connect to the master and work repository of the Microsoft Azure Synapse Analytics source system.

For information about configuring a connection, see *Connections* in the Administrator service.

CHAPTER 2

Before you begin

Before you create a catalog source, ensure that you have the information required to connect to the source system.

Perform the following tasks:

- Assign the required permissions.
- Create a connection to the Microsoft Azure Synapse Analytics source system in Administrator.
- Create endpoint catalog sources for connection assignment.

Verify permissions

To extract metadata and to configure other capabilities that a catalog source might include, you need account access and permissions on the source system. The permissions required might vary depending on the capability.

Permissions for metadata extraction

Ensure that you have the required permissions to enable metadata extraction.

Verify that the administrator performs the following tasks:

- Grants the Synapse Monitoring Operator role in Azure Synapse Studio.
- Grants the Reader role in the Azure Synapse workspace that you use.

Permissions to run data classification

You can perform data classification with the permissions required to perform metadata extraction.

Permissions to run glossary association

You can perform glossary association with the permissions required to perform metadata extraction.

Create a connection

Before you configure the Microsoft Azure Synapse Analytics catalog source, create a connection object in Administrator.

1. In Administrator, select **Connections**.
2. Click **New Connection**.
3. Enter the following connection details:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + ; Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	Microsoft Azure Synapse Analytics
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. Note: If you're using this connection to apply data access policies through pushdown or proxy services, you cannot use the Secret Vault configuration option. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment.

4. Select the authentication type to connect to Microsoft Azure Synapse Analytics and enter the required properties.

You can use the following connection modes:

- Admin User connection mode
- Service Principal connection mode

5. Click **Test Connection**.
6. Click **Save**.

Admin User connection mode

This connection mode uses the client ID, user name, and password to connect to Microsoft Azure Synapse Analytics.

The following table describes the connection properties for the Admin User connection mode:

Subscription ID	Subscription ID of Microsoft Azure Synapse Analytics.
Client ID	The application ID or client ID of your application registered in Azure Active Directory.
User Name	Fully qualified user name to connect to Microsoft Azure Synapse Analytics instances. Contact your administrator for the user name.
Password	Password associated with the user name. Contact your administrator for the password.

Service Principal connection mode

This connection mode uses the client ID, secret ID, and tenant ID to connect to Microsoft Azure Synapse Analytics.

The following table describes the connection properties for the Service Principal connection mode:

Subscription ID	Subscription ID of Microsoft Azure Synapse Analytics.
Client ID	The application ID or client ID of your application registered in Azure Active Directory.
Tenant ID	The tenant ID of your application registered in Azure Active Directory.
Client Secret	The client secret key to connect to Microsoft Azure Synapse Analytics instances through Azure Active Directory. Contact your administrator for the client secret key.

Proxy properties

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

The following table describes Microsoft Azure Synapse Analytics connection proxy properties:

Connection property	Description
Use Proxy	Determines whether the connection uses a proxy server to connect to Microsoft Azure Synapse Analytics. Select to use a proxy server. Default is disabled.
Host	Host name of the outgoing proxy server.
Port	Port number of the outgoing proxy server.

Connection property	Description
User Name	Name of the authenticated user of the proxy server. Required if the proxy server requires authentication.
Password	Password for the authenticated user. Required if the proxy server requires authentication.

Create endpoint catalog sources for connection assignment

An endpoint catalog source represents a source system that the catalog source references. Before you perform connection assignment, create endpoint catalog sources and run the catalog source jobs.

You can then perform connection assignment to reference source systems and run connection-aware scans to view complete lineage with source system objects.

CHAPTER 3

Create catalog sources in Metadata Command Center

Use Metadata Command Center to configure a catalog source for Microsoft Azure Synapse Analytics and extract metadata.

When you configure a catalog source, you define the source system that you want to extract metadata from. Configure filters to include or exclude source system metadata before you run the job. Optionally, configure other capabilities, such as lineage discovery, data profiling and quality, data classification, relationship discovery, and glossary association.

To provide stakeholders access to technical assets, you can assign access through stakeholder roles. You can also associate technical assets extracted from the catalog source to asset groups. If your catalog source references other source systems, you can create a connection assignment to the endpoint catalog source to view complete lineage.

Step 1. Register a catalog source

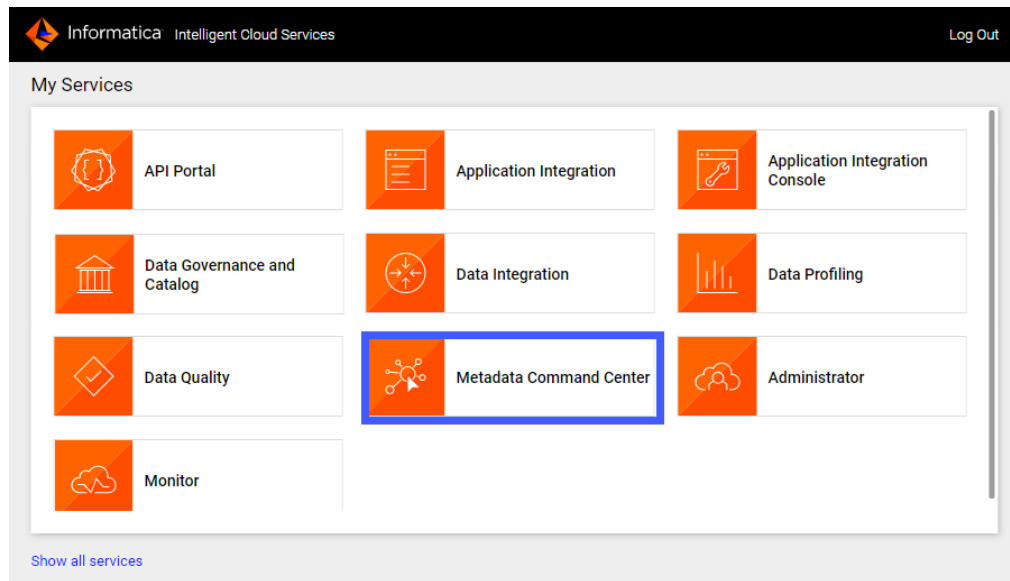
When you register a catalog source, provide general information and connection values.

1. Log in to Informatica Intelligent Cloud Services.

The **My Services** page appears.

2. Click **Metadata Command Center**.

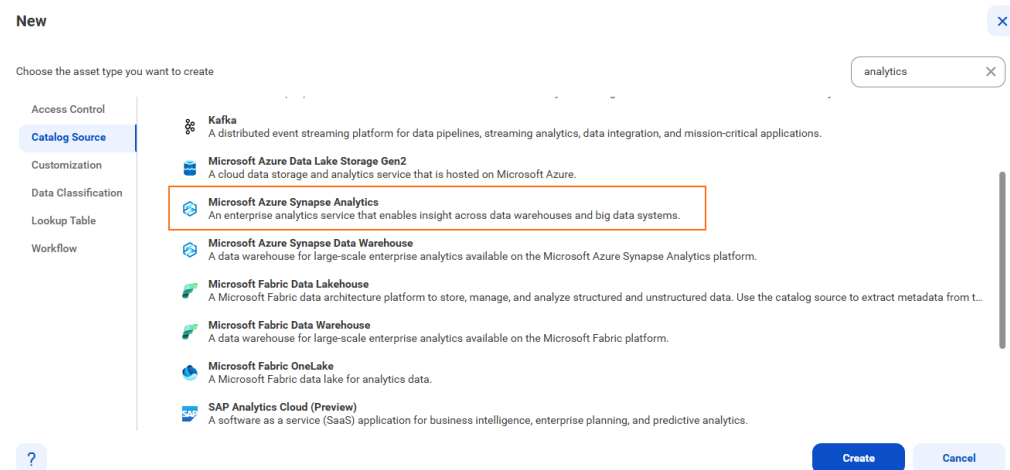
The following image shows the Metadata Command Center box on the **My Services** page:



The Metadata Command Center home page appears.

3. Click **New**.
4. Select **Catalog Source** from the list of asset types.
5. Select Microsoft Azure Synapse Analytics from the list of catalog source types.

The following image shows the Microsoft Azure Synapse Analytics catalog source type:



6. Click **Create**.

The **New Catalog Source** page opens.

The following image shows the **Registration** tab on the **New Catalog Source** page:

7. In the **General Information** section, enter a name and an optional description for the catalog source.

Note: You can rename a catalog source after you create it, but to apply the change to all associated objects you must rerun the metadata extraction job.

After you save the catalog source, you can update the description in Metadata Command Center and Data Governance and Catalog. The update appears only in the service in which you update it.

8. In the **Connection Information** area, select the connection that you created in Administrator.

Note: To create or edit a catalog source, you need permissions on the connection to the source system. Select a connection that you have access to, or ask the administrator to grant the necessary permissions to the connection that you want to use.

9. Click **Connection Properties** to expand and view the connection properties for the selected connection.
10. Click **Test Connection** to test your connection to the source system.
11. Click **Next**.

The **Configuration** page appears.

Step 2. Configure capabilities

When you configure the Microsoft Azure Synapse Analytics catalog source, you define the settings for the metadata extraction capability.

The metadata extraction capability extracts source metadata from external source systems. You can also configure other capabilities that the catalog source includes.

You can save the catalog source configuration at any point after you enter the connection information. After you save the catalog source, you can choose to run the catalog source job. To run the job once, click **Run**. To run metadata extraction and other capabilities on a recurring schedule, configure schedules on the **Schedule** tab.

Configure metadata extraction

When you configure the Microsoft Azure Synapse Analytics catalog source, you choose a runtime environment, define filters, and enter configuration parameters for metadata extraction.

1. In the **Connection and Runtime** area, choose a serverless runtime environment or the Secure Agent group where you want to run catalog source jobs.

Note: Serverless runtime environment options are available if the catalog source works with a serverless runtime environment.

2. Choose to retain, delete, or deprecate objects that are deleted from the source system in the catalog with the **Metadata Change Option**.
 - **Retain.** Retains objects that are deleted from the source system in the catalog. If you update or add a filter, the catalog retains objects extracted from the previous job and extracts additional objects that match the current filter. Objects deleted from the source system are not deleted from the catalog. Enrichments added on deleted objects and relationships are retained.
 - **Delete.** Deletes metadata from the catalog based on objects deleted from the source system and changes you make to the filter. Enrichments added on deleted objects and relationships are also permanently lost. Objects renamed in the source system are removed and recreated in the catalog.
 - **Deprecate.** The lifecycle of objects imported into the catalog moves to Obsolete based on objects deleted from the source system and changes you make to the filter. This does not impact enrichments added on deprecated objects and relationships. Objects renamed in the source system are removed and recreated in the catalog. When you run the catalog source job again for other capabilities such as data classification, relationship discovery, or glossary association, the job doesn't consider obsolete objects. Obsolete objects remain in the catalog until they are purged when you run a **Purge Obsolete Objects** job on the **Explore** page.

Note: You can also change the configured metadata change option when you run a catalog source.

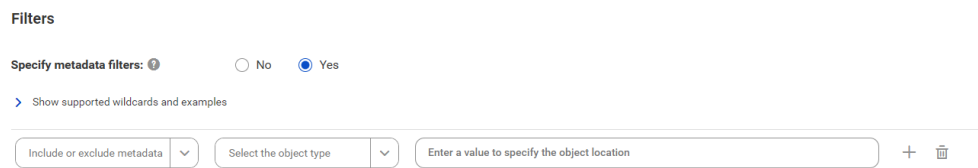
3. In the **Filters** area, define one or more filter conditions to apply for metadata extraction:
 - a. From the Include or Exclude metadata list, choose to include or exclude metadata based on the filter parameters.
 - b. From the Object type list, select **Notebook** or **Pipeline**.
 - c. Enter a value to specify the object location.

Filters can contain the following wildcards:

 - Question mark. Represents a single character.
 - Asterisk. Represents multiple characters.

To differentiate objects in workspaces and pipelines from file paths, use pipes.

The following image shows the filter condition options:



Examples:

- To include or exclude metadata from all notebooks in all folders under 'Workspace1' workspace, select **Notebook** as the object type and enter `Workspace1/*`.
- To include or exclude metadata from the notebook named 'Notebook1' in the subfolder 'Folder3', select **Notebook** as the object type and enter `Workspace1/Folder1|Folder2|Folder3|Notebook1`.
- To include or exclude metadata from all activities in all pipelines under all folders under 'Workspace1' workspace, select **Pipeline** as the object type and enter `Workspace1/*/*`.
- To include or exclude metadata from from all activities in the pipeline named 'Pipeline1' in the subfolder 'Folder3', select **Pipeline** as the object type and enter `Workspace1/Folder1|Folder2|Folder3|Pipeline1/*`.

4. In the **Configuration Parameters** area, enter properties to override default context and variable values.

Note: Click **Show Advanced** to view all configuration parameters.

The following table describes the properties that you enter for Catalog Source Configuration Options:

Property	Description
Operational Metadata Config	<p>Specifies whether to process operational metadata.</p> <p>To process operational metadata, set the Process Operational Metadata parameter to Yes.</p> <p>Configure the following parameters:</p> <ul style="list-style-type: none"> - Operational Metadata Time Range. Determines the time range from which pipeline runs are processed. - Process Latest Runs. Determines whether to process only the latest pipeline runs or all pipeline runs. <p>If you select No and run the job with the Delete Metadata Change Option selected, any metadata extracted previously through the operational metadata in the pipeline instance is deleted.</p>
Databricks Parameters	<p>Specifies the parameters for Databricks notebooks.</p> <p>Configure the following parameters:</p> <ul style="list-style-type: none"> - Notebooks Python Modules Path. The path to the directory containing custom python user modules. This path must be accessible by the Secure Agent. <p>Example value:</p> <ul style="list-style-type: none"> - On Windows: <code>Y:\etc\user_modules</code> - On Linux: <code>/opt/etc/user_modules</code> <p>This parameter appears when you click Show Advanced.</p> <ul style="list-style-type: none"> - Python Default Variables Values File. The path to the default values files for Databricks Notebook Python. This path must be accessible by the Secure Agent. <p>This parameter appears when you click Show Advanced.</p> <ul style="list-style-type: none"> - Databricks Connection. The connection details for Databricks notebooks. <p>Click Add Entry and provide the following connection details:</p> <ul style="list-style-type: none"> - Host. The Databricks host name. - Workspace path. The path to the Databricks Notebook workspace. - Connection. A Databricks Delta connection created in Administrator. - Catalog Preload Include Filter. A list of include filters to preload Databricks catalog assets. - Catalog Preload Exclude Filter. A list of exclude filters to preload Databricks catalog assets.
SecureString Entries as Key-value Pairs	<p>The SecureString key and value that Microsoft Azure Synapse Analytics uses to connect to other data sources. Contact your administrator for the key and value.</p>
SSISDB SQL Server Connection Configuration	<p>Specifies SSISDB SQL Server connections assigned to Integration Runtimes. In the Name field, enter the name of the Integration Runtime configured to run the Execute SSIS Package activity in Microsoft Azure Synapse Analytics. In the Connection field, enter the SSISDB SQL Server connection created in the Administrator service.</p> <p>Note: This parameter appears when you click Show Advanced.</p>

5. Optional. In the **Configuration Parameters** area, enter additional settings.

The following table describes the property that you enter for additional settings:

Note: The **Additional Settings** section appears when you click **Show Advanced**.

Property	Description
Expert Parameters	Enter additional configuration options to be passed at runtime. Required if you need to troubleshoot the catalog source job. Caution: Use expert parameters when it is recommended by Informatica Global Customer Support.

6. Configure additional capabilities for the catalog source by clicking on the tabs.

Configure lineage discovery

Enable the lineage discovery capability and use CLAIRE to build complete lineage by recommending endpoint catalog source objects to assign to reference catalog source connections.

1. Click the **Lineage Discovery** tab.
2. Select **Enable Lineage Discovery**.
3. In the **Filters** area, define one or more filter conditions to apply for lineage discovery.

To define filters, you can choose to select catalog source types, asset groups, or enter a catalog source name or search from a list of catalog sources.

- a. Select **Yes** to view filter options.
- b. From the Include/Exclude list, choose to include or exclude catalog sources for lineage discovery based on the filter parameters.
- c. From the filter type list, select catalog source type, catalog source name, or asset group.
- d. In the filter value field, select the required catalog source types, or click the Search button and select catalog sources or asset groups.

Filters can contain the asterisk wildcard to represent multiple characters or empty text.

The following image shows the filter condition options:

Enable Lineage Discovery: ☒

Filters

Specify lineage discovery filters: ☒ No ☒ Yes

[Show supported wildcards and examples](#)

Include	Catalog Source Type	Select Catalog Source Types	+	🗑
Exclude	Catalog Source Name	Select Catalog Sources	+	🗑
Exclude	Asset Group	Select Asset Groups	+	🗑

Examples:

- To include or exclude all Oracle catalog sources, select **Catalog Source Type** as the filter type and select `Oracle` in the filter value field.
- To include or exclude the 'Oracle_Retail' catalog source, select **Catalog Source Name** as the filter type and search for the catalog source or enter `Oracle_Retail` in the filter value field.

- To include or exclude all catalog sources with names that start with 'Oracle', select **Catalog Source Name** as the filter type and search for the catalog source or enter `Oracle*` in the filter value field.
- To include or exclude all catalog sources with names that end with 'Retail', select **Catalog Source Name** as the filter type and search for the catalog source or enter `*Retail` in the filter value field.
- To include or exclude all catalog sources with names that contain 'Ret', select **Catalog Source Name** as the filter type and search for the catalog source or enter `*Ret*` in the filter value field.
- To include or exclude all catalog sources that are part of the 'Financial Group' asset group, select **Asset Group** as the filter type and search `Financial Group` in the filter value field.

Note: You can't add more than one include or exclude filter for the same filter type.

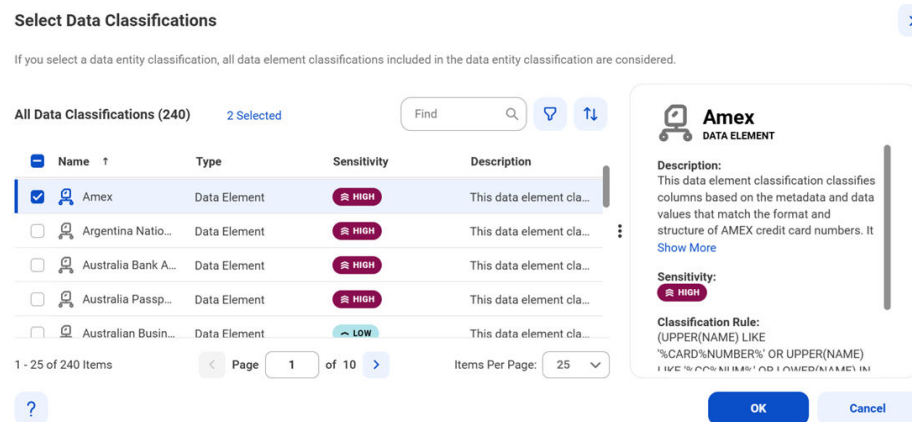
- Optionally, to define an additional filter with an AND condition, click the **Add** icon.

For more information about lineage discovery, see *Lineage discovery* in the *Administration* help.

Configure data classification

Enable the data classification capability to identify and organize data into relevant categories based on the functional meaning of the data.

- Click the **Data Classification** tab.
 - Select **Enable Data Classification**.
 - Choose one or both of the following options:
 - **Generated Data Classifications.** CLAIRE automatically generates data classifications for the data elements.
 - **Data Classification Rules.** Choose from predefined or custom data classifications.
- Click **Add Data Classification**. The following image shows the **Select Data Classifications** dialog box:



- Select the data classifications that you want to use.
- Click **OK**.

Configure glossary associations

Enable the glossary association capability to associate glossary terms with technical assets, or to get recommendations for glossary terms that you can manually associate with technical assets in Data Governance and Catalog.

Metadata Command Center considers all published business terms in the glossary while making recommendations to associate your technical assets.

1. Click the **Glossary Association** tab.
2. Select **Enable Glossary Association**.
3. Select **Enable auto-acceptance** to automatically accept glossary association recommendations.
4. Specify the **Confidence Score Threshold for Auto-Acceptance** to set a threshold limit based on which the glossary association capability automatically accepts the recommended glossary terms.
Note: Specify a percentage from 80 to 100. If the score is higher than the specified limit, the glossary association capability automatically assigns a matching glossary term to the data element.
5. Select **Enable Below-threshold Recommendations** to receive glossary association recommendations below the auto-acceptance threshold. If you enable auto-acceptance, you can enable below-threshold recommendations to receive glossary recommendations below the auto-acceptance threshold.
6. Specify the **Confidence Score Threshold for Recommendations** to set a threshold based on which the glossary association capability makes recommendations
If you enable auto-acceptance, specify a percentage from 80 to the selected auto-acceptance threshold. You can accept or reject the recommended glossary terms that fall within this range in Data Governance and Catalog.
If you disable auto-acceptance, specify a percentage from 80 to 100 inclusive.
7. Choose to automatically assign business names and descriptions to technical assets. You can then choose to retain existing assignments and only assign business names and descriptions to assets that don't have assignments, or allow overwrite of existing assignments.
By default, existing assignments are retained.
8. Optional. Choose to ignore specific parts of data elements when making recommendations. Select **Yes** and enter prefix and suffix keyword values as needed.
Click **Select** to enter a keyword. You can enter multiple unique prefix and suffix keywords. Keyword values are case insensitive.
9. Optional. Choose specific top-level business glossary assets to associate with technical assets. Selecting a top-level asset selects its child assets as well. Select **Top-level Glossary Assets** and specify the assets on the **Select Assets** page.
10. Optional. Choose to use abbreviations and synonym definitions from lookup tables for accurate glossary association. Select **Yes** to enable, and then click **Select** to upload a lookup table.
11. Click **Next**.
The **Associations** page appears.

Step 3. Associate stakeholders and asset groups

Associate users or user groups within a stakeholder role as stakeholders for technical assets in Data Governance and Catalog. Also, you can choose to assign technical assets extracted from the catalog source

to asset groups. You can then use access policies to control permissions on assets that are assigned to asset groups.

Verify that the administrator assigned users and user groups to the stakeholder role that you want to associate with technical assets.

1. To associate users or user groups as stakeholders with technical assets extracted from the catalog source, perform the following steps:

- a. On the **Associations** page, click **Stakeholders**.
- b. Select **Assign Stakeholders**.
- c. Select a stakeholder role.
- d. Click **Select** to add users and user groups from the stakeholder role as stakeholders for the technical assets.

The **Add Users & User Groups** dialog box displays a list of users and user groups assigned to the selected stakeholder role.

	Full Name	Email	User Name	Status
<input type="checkbox"/>	gov owner_09			Active

? OK Cancel

- e. Select one or more users or user groups to assign as stakeholders for the technical assets, and click **OK**.

Only the selected users and user groups belonging to the specified stakeholder role are granted the permissions to technical assets.

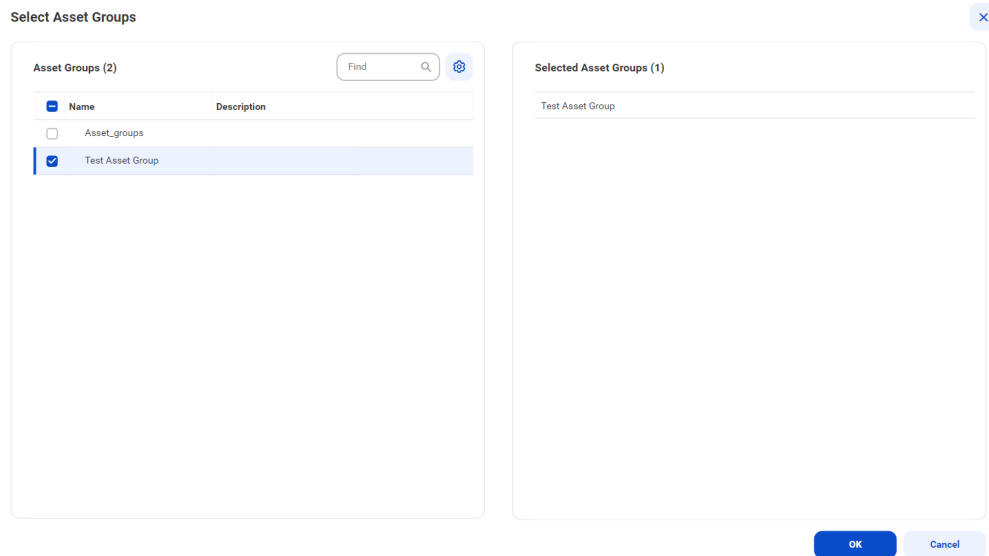
- f. To assign users or user groups from another stakeholder role, click **Add** and then repeat the steps.
2. To assign asset groups to technical assets extracted from the catalog source, perform the following steps:

- a. On the **Associations** page, click **Asset Groups**.
- b. Select **Assign Asset Groups**.
- c. Click **Select**.

The **Select Asset Groups** dialog box displays the list of asset groups.

If you enabled an access policy that includes an asset group, you can only view assets that belong to that asset group.

3. Select the asset groups to which you want to assign technical assets extracted from the catalog source, and click **OK**.



4. Choose to save and run the job or to schedule a recurring job.
 - To save and run the job, click **Save** and then **Run**.
 - To schedule a recurring job, click **Next** to open the **Schedule** page.

Step 4. Run or schedule the job

Choose to run a catalog source job manually, or configure it to run on schedule.

Note: You can't run multiple jobs simultaneously.

You can choose to perform a full or an incremental metadata extraction. A full metadata extraction extracts all objects from the source to the catalog. An incremental metadata extraction extracts only the changed and new objects since the last successful catalog source job run. Incremental metadata extraction doesn't remove deleted objects from the catalog and doesn't extract metadata of code-based objects if applicable.

When you run an incremental metadata extraction job with a filter to include metadata from objects, the job extracts only the objects that have the latest timestamp since the last successful job.

Note: The incremental extraction option appears if it is available for the catalog source.

Run the job manually

Click **Save** to save the catalog source and click **Run**. On the **Run Catalog Source Job** window, click **Run** to run the job.

You can override the capabilities that you selected while configuring your catalog source on the **Configuration** page. The first time you run the catalog source job, the metadata extraction capability is mandatory. From the second run onwards, you can choose to override the configured metadata change option. You can retain, delete, or deprecate objects that are deleted from the source in the catalog. For subsequent runs of the catalog source job, the metadata extraction capability is optional.

Note: You can choose incremental metadata extraction for subsequent runs only after one full metadata extraction job completes successfully. Incremental metadata extraction jobs run with the **Retain** metadata change option even if you set the option to **Delete** or **Deprecate** in the catalog source.

Note: To run a catalog source job, you need permissions on the connection to the source system. To run a catalog source job for catalog sources that reference other source systems, you need permissions on the connections for all the reference source systems.

Run the job on a schedule

You can choose to run metadata extraction and other capabilities on a recurring schedule. You can't choose incremental metadata extraction and full metadata extraction in the same schedule. To create a schedule for incremental metadata extraction, you must have completed at least one full metadata extraction job successfully. If not, first create a schedule for a full metadata extraction.

If an incremental metadata extraction is scheduled to run when the last run details aren't available, the job first performs a full metadata extraction, followed by incremental metadata extraction on subsequent runs.

For example, this can happen in the following scenarios:

- You create schedules for both incremental metadata extraction and full metadata extraction, but schedule the incremental extraction to run before the first full metadata extraction job.
- You create schedules for both incremental metadata extraction and full metadata extraction, but delete the full metadata extraction schedule before its first run.

1. On the **Schedule** tab, select **Run on Schedule**.
The **Schedule** configuration page opens.
2. Click the checkbox corresponding to each capability that you want to include in the schedule.
3. Enter the start date, time zone, and the interval at which you want to run the job.
4. You can manage additional schedules using the following options:
 - To create a new schedule, click the **Add** button.
 - To delete a schedule, click the **Delete** button.
 - To enable or disable a schedule, click the **Enable Schedule** toggle button.

Note: You can create a maximum of one schedule per capability that you enable. If you purged a catalog source or did not run the metadata extraction job, the catalog source job runs metadata extraction before running other scheduled capabilities.

Note: To create a schedule, you need permissions on the connection to the source system. If you lose permissions on the connection after you create a schedule, the scheduled jobs continue to run.

5. Click **Save** to save the schedule.

Monitor job status

After the job runs, you can monitor the status of the job on the **Overview** page of the job.

For more information about job monitoring, see *Administration*.

Step 5. Assign reference catalog source connections to endpoint catalog source objects

When you run the catalog source job, if the catalog source references another source system, a reference catalog source and connection get created that point to the reference source system. To view the complete lineage for your catalog source, you can perform connection assignment from the reference catalog source connection to the objects in the reference source system. A reference source system might be a data

integration platform, such as Microsoft Azure Synapse Analytics. You must first create and run an endpoint catalog source that connects to the reference source system.

Before you assign a connection, ensure that you have created and run an endpoint catalog source for each reference source system.

Note: If the source schema contains case-sensitive tables or if the reference objects contain multiple objects with the same name in different cases, perform case-sensitive connection assignment to get correct lineage.

If you enabled the lineage discovery capability for your catalog source, you can either curate the CLAIRE recommended endpoint objects on the **Related Catalog Sources** tab or assign connections manually.

For more information about related catalog sources and lineage discovery, see *Lineage discovery* in the *Administration* help.

1. On the **Configure** page, select the **Lineage** tab, and then select the **Lineage Discovery** tab. On the **Catalog Sources** panel, select the required catalog source and click the **Assign Connections** tab.

The **Assign Connections** tab displays a list of assigned and unassigned connections along with details for each connection. Use filters to view the connections based on the connection names. Click the **Add Filter** menu to add filters.

2. Select the connection to the reference source system and click **Assign**.

The connection name appears prefixed to the reference catalog source name on the **Hierarchy** tab of your catalog source in Data Governance and Catalog.

The **Assign Connection** dialog box appears with a list of recommended objects from the endpoint catalog sources. Click **All** to view all endpoint catalog source objects.

3. In the **Assign Connection** dialog box, select one or more objects from the endpoint catalog sources and click **Assign**.

You can filter the list in the **Assign Connection** dialog box by name, type, or endpoint.

You can connect to the following source systems:

- Amazon Redshift. The catalog source must belong to the Database class type.
- Amazon S3. The catalog source must belong to the AmazonS3 Bucket class type.
- File System The catalog source must belong to the File System class type.
- Microsoft Azure Blob Storage The catalog source must belong to the File System class type.
- Microsoft Azure Data Lake Storage Gen2. The catalog source must belong to the ADLS Container class type.
- Microsoft Azure SQL Server. The catalog source must belong to the Database class type.
- Microsoft Azure Synapse Data Warehouse. The catalog source must belong to the Database class type.
- Oracle. The catalog source must belong to the Database class type.
- Salesforce. The catalog source must belong to the Application class type.
- Snowflake. The catalog source must belong to the Database class type.
- SAP HANA Database. The catalog source must belong to the Database class type.

The objects must be of the Database or File System class type.

When you click **Assign**, Metadata Command Center creates links between matching objects in the connected catalog sources, and it calculates the percentage of matched and unmatched objects. The higher the percentage of matched objects, the more accurate the lineage that you view in Data Governance and Catalog.

4. Run the catalog source job again. If you configured the catalog source job to run on a regular schedule, the next scheduled run picks up the updated details. If you didn't configure a schedule, run the catalog source job again to view complete lineage.

CHAPTER 4

View results in Data Governance and Catalog

After Metadata Command Center runs a job, you can view the results in Data Governance and Catalog where the catalog source and its elements are called technical assets. You can view a catalog source as a hierarchy. Expand each technical asset to see its components.

When referenced source systems are connected to a catalog source, you can expand the hierarchy to see details about the technical asset's component elements.

You can view the data lineage of an asset contained within a catalog source to see individual elements such as data sources, calculations, and filters. When you view data lineage, you can see the individual upstream elements that contribute data or expressions to each component of a data flow or catalog source.

View metadata extraction results

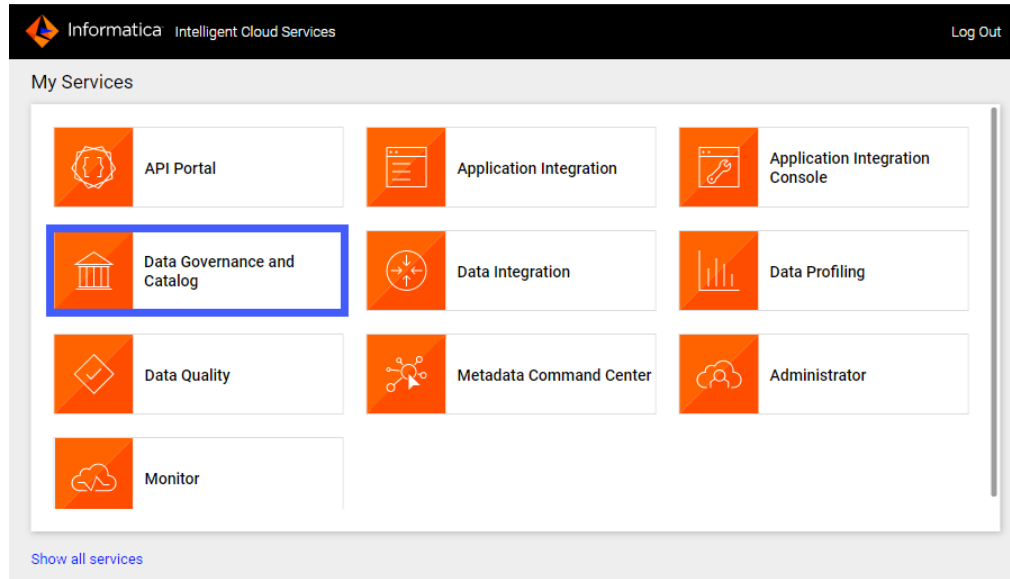
After a job runs in Metadata Command Center, view the results in Data Governance and Catalog. You can view details about source system contents in a hierarchical structure and trace data lineage.

1. Log in to Informatica Intelligent Cloud Services.

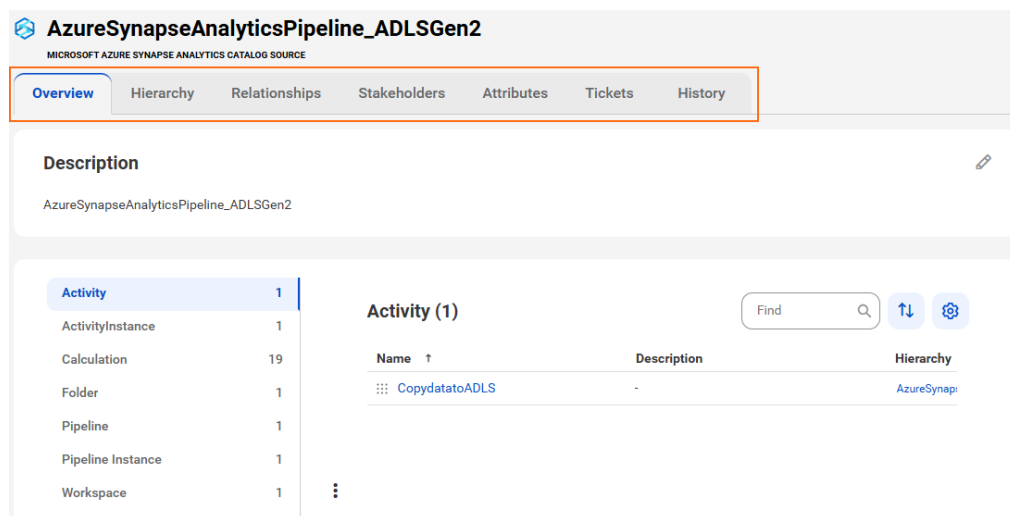
The **My Services** page appears.

2. Click Data Governance and Catalog.

The following image shows the Data Governance and Catalog box on the **My Services** page:



3. On the Data Governance and Catalog home page, click the number in the **Technical Assets** panel. The **Technical Assets** page opens.
4. Select **Catalog Source** in the **Filter** list. The list of catalog sources opens.
5. Search for the catalog source from which you extracted metadata, and click the name. The **Overview** tab of the asset opens. The following image shows a sample asset page:



6. View the asset from different perspectives by clicking on the tabs. For more information about working with assets, see *Working with Assets* in *Data Governance and Catalog* help.

View data lineage

Data lineage is a visual representation of the flow of data across the systems in your organization. Lineage depicts how the data flows from the system of its origin to the system of its destination.

Data lineage views are available for technical assets in the catalog source. You can view lineage at the catalog source, data set, or data element level.

The lineage at the catalog source level shows how data flows from one catalog source to another. The lineage at the data set and the data element levels show how other technical assets such as files or tables contribute to the selected asset.

If linking catalog sources is available for your catalog source, you can use Metadata Command Center to generate data lineage based on rules or by generating automated lineage with CLAIRE. You can choose source and target catalog sources and objects to link and generate lineage.

To determine whether linking catalog sources is available for your catalog source, navigate to the **Configuration** tab of the **Link Catalog Sources** page. The catalog source must appear in the list of source and target catalog sources.

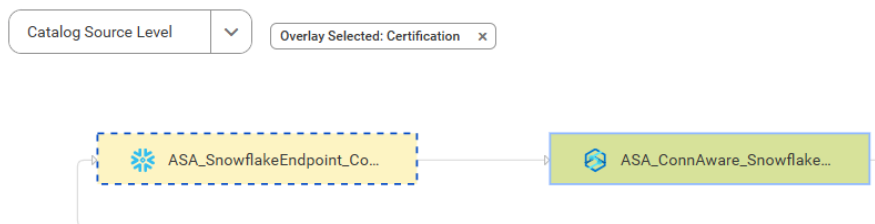
For information about linking catalog sources, see *Link catalog sources* in the Administration help.

View lineage at the catalog source level

The catalog source level shows how data flows from one catalog source to another with the lineage aggregating data from the data set and data element levels.

To view data lineage at the catalog source level, open a technical asset, click the **Lineage** tab, and then verify that the level is set to **Catalog Source Level**.

The following image shows how data flows between the ASA_ConnAware_Snowflake17 and the ASA_SnowflakeEndpoint_ConnAware catalog sources after connection assignment:



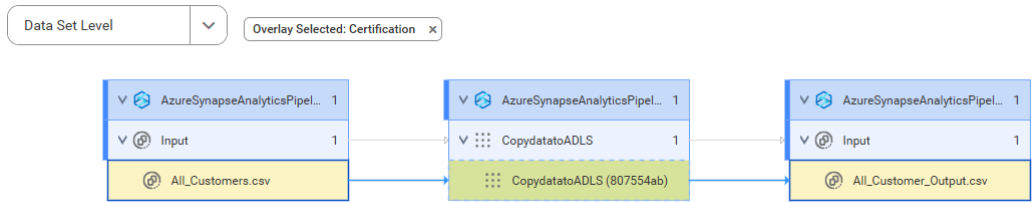
After connection assignment, the referenced object icons change to specific object icons.

View lineage at the data set level

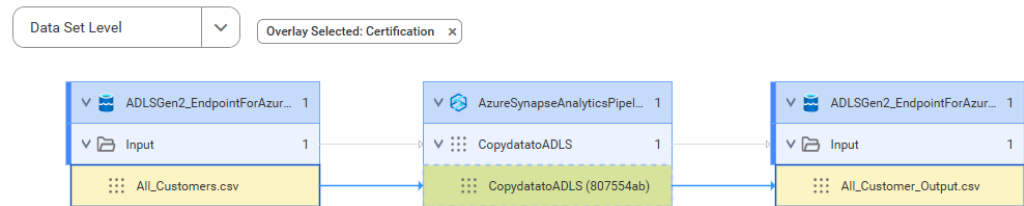
The data set level displays individual sets of data in the data flow.

To view lineage at the data set level, open a technical asset, click the **Lineage** tab, and then verify that the level is set to **Data Set Level**.

The following image shows how the target file gets data from the referenced source file before connection assignment:



The following image shows how the target file gets data from the source file after connection assignment:



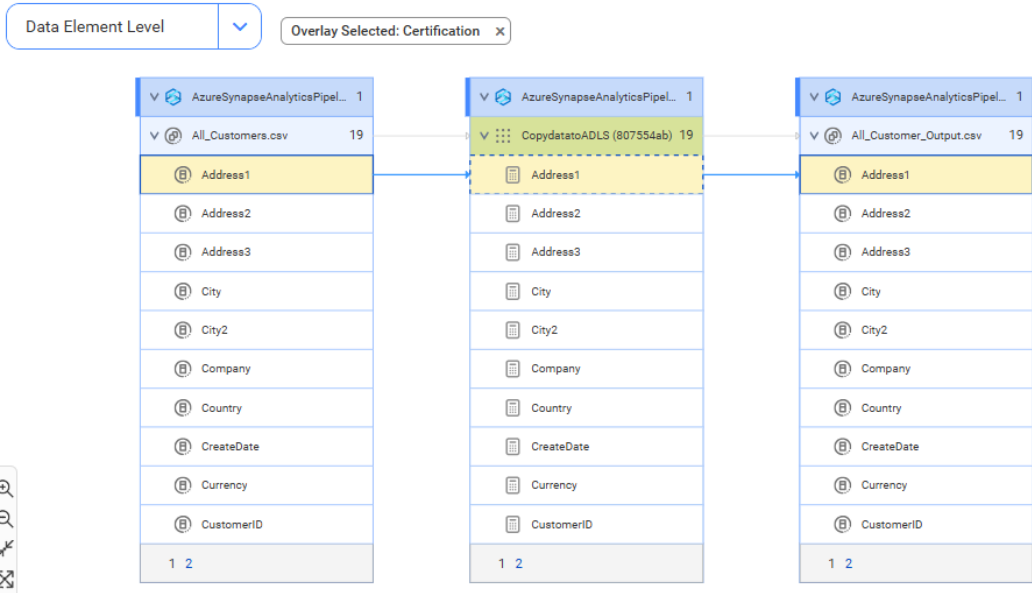
After connection assignment, the referenced object icons change to specific object icons.

View lineage at the data element level

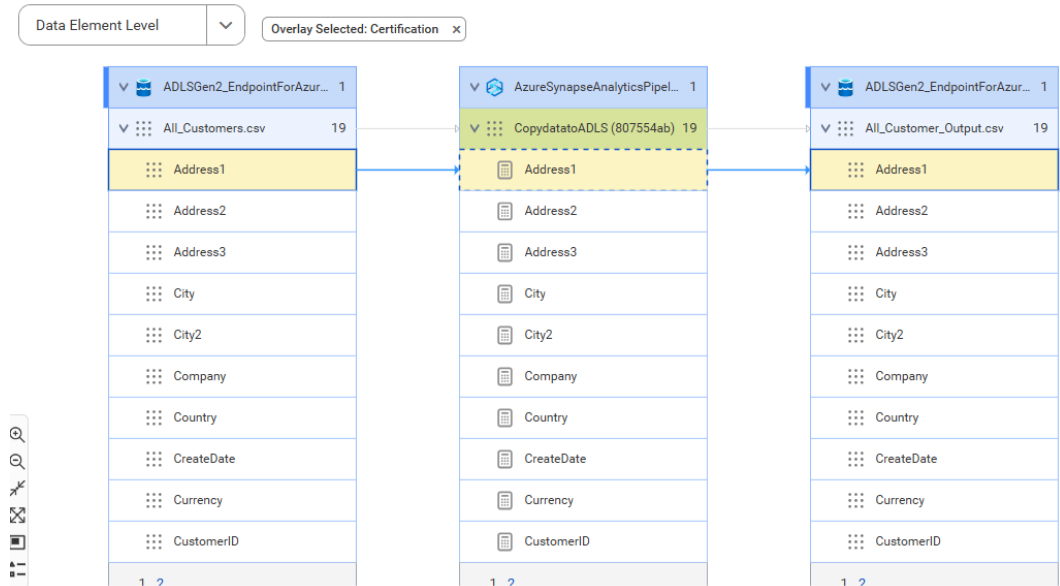
The data element level displays details of the data set level. At the data element level, you can see the input sources for expressions or commands and calculations or transformations on the data.

To view data lineage at the data element level, open a technical asset, click the **Lineage** tab, and then verify that the level is set to **Data Element Level**.

The following image shows how the target file gets data from the referenced source file before connection assignment:



The following image shows how the target file gets data from the source file after connection assignment:



After connection assignment, the referenced object icons change to specific object icons.

View classified data

When you add data classification rules to a catalog source in Metadata Command Center, the system identifies the columns and tables that match the rules and displays one or more matched data classifications on the column or table asset pages in Data Governance and Catalog.

The following image shows a column asset page with the inferred data element classifications that match the column data and metadata:

Overview
Lineage
Relationships
Data Quality
Stakeholders
Properties
Tickets
History

Catalog Source Definition

Glossaries

Accepted (0)
CLAIRE™ Recommendations (1)
Declined (0)

Click here to add Glossary assets
BEYONDWE
No declined Glossary assets.

Data Element Classifications

Accepted (1)
Declined (0)

Amex
No declined Classification assets.

For more information about data classification assets, see *Asset Details* in the Data Governance and Catalog help.

View glossary associations

When you enable the glossary association capability for a catalog source in Metadata Command Center, you can view the accepted glossary assets in Data Governance and Catalog.

The **Overview** tab for a technical asset in the catalog source displays glossary assets in the Accepted and CLAIRE Recommendations sections.

The **Glossaries** panel shows the automatically accepted and CLAIRE® recommended terms.

The following image shows a sample asset page:

