



Informatica® Metadata Command Center
November 2025

Snowflake Sources

© Copyright Informatica LLC 2023, 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.	5
Chapter 1: Introduction to Snowflake catalog sources.	6
Extraction and view process.	7
About the Snowflake catalog source.	8
Extracted metadata.	8
Data profiling for Snowflake objects.	9
Compatible connectors.	9
Chapter 2: Before you begin.	10
Verify permissions.	10
Permissions to extract metadata.	10
Permissions to run data profiles.	11
Permissions to perform data classification.	11
Permissions to perform relationship discovery.	11
Permissions to perform glossary association.	11
Permissions to perform writeback.	11
Create a connection.	12
Standard authentication.	12
Key pair authentication.	13
Client Credentials.	14
Import a relationship inference model.	15
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 profiling and quality.	23
Configure data classification.	25
Configure relationship discovery.	26
Configure glossary association.	27
Configure writeback.	27
Step 3. Associate stakeholders and asset groups.	28
Step 4. Run or schedule the job.	30
Step 5. Assign reference catalog source connections to endpoint catalog source objects.	31
Chapter 4: View results in Data Governance and Catalog.	33
View metadata extraction results.	33
View data lineage.	35

View lineage at the catalog source level.	35
View lineage at the data set level.	35
View lineage at the data element level.	36
View data profiling results	37
View data observability results	37
View classified data.	38
View glossary associations.	39

Preface

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

CHAPTER 1

Introduction to Snowflake 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, Snowflake is a source system from which you can extract metadata through a Snowflake 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:

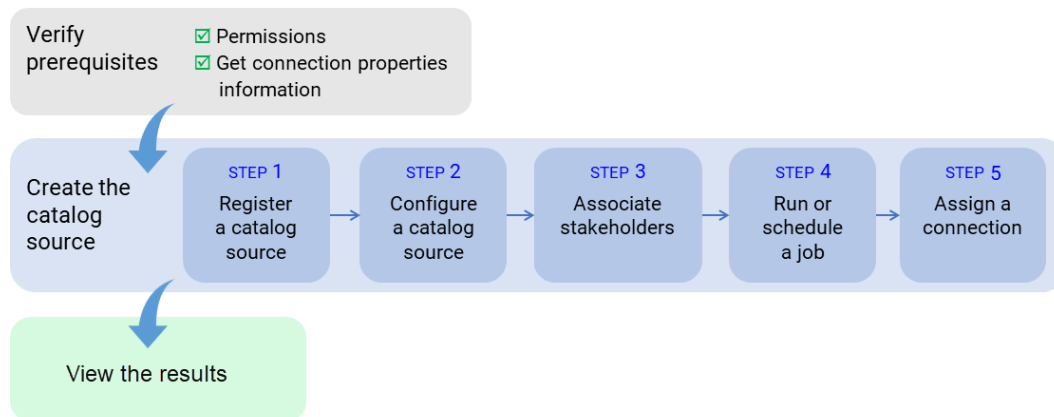
Capability	Description
Incremental metadata extraction	An incremental metadata extraction extracts only the changed and new objects since the last catalog source job run. Incremental metadata extraction doesn't remove deleted objects from the catalog and doesn't extract metadata of code-based objects if applicable.
Serverless Runtime Environment	A serverless runtime environment is an advanced serverless deployment solution that doesn't require downloading, installing, configuring, or maintaining a Secure Agent or Secure Agent group. You can use a serverless runtime environment in the same way that you use a Secure Agent when you configure a catalog source.
Advanced Programming Language Parsing	Advanced Programming Language Parsing parses the source system code in addition to extracting objects from the source system.
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 Profiling and Quality	<ul style="list-style-type: none">- Data Profiling. Assesses source metadata and analyzes the collected statistics to discover content and structure, such as value distribution, patterns, and data types.- Data Quality. Measures the reliability of the data and enables data usage.- Data Observability. Identifies anomalies in the characteristics of the data.

Capability	Description
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.
Relationship Discovery	The relationship discovery capability identifies pairs of similar columns and relationships between tables within a catalog source.
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 source system:



After you verify prerequisites, perform the following tasks to extract metadata from Snowflake:

1. Register a catalog source. Create a catalog source object, select the source system, and specify values for connection properties.
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.

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

About the Snowflake catalog source

You can use the Snowflake catalog source to extract metadata from the Snowflake source system.

Snowflake is an analytic data warehouse provided as Software-as-a-Service (SaaS). The Snowflake data warehouse uses an SQL database engine with a unique architecture designed for cloud services.

Extracted metadata

You can use the Snowflake catalog source to extract metadata from a Snowflake source system.

The metadata extraction service extracts the following objects from a Snowflake source system:

- Database
- Schema
- Tables
- Tags
- View
- Materialized View

Note: Objects of the Materialized View type appear as View in Data Governance and Catalog.

- Function
- Stored Procedure

Note: To extract Data Definition Language (DDL) statements from a stored procedure, you need owner privileges on the stored procedure. Alternatively, you can re-create the stored procedure with the `EXECUTE AS CALLER` clause.

- Pipe
- Stage
- Column

You can extract metadata from stored procedures that use the following languages:

- JavaScript
- Snowflake SQL scripting
- Snowpark Python

Note: Effective in the 2024.11.S release, extracting metadata from stored procedures that use Snowpark Python is available for preview.

Preview functionality is supported for evaluation purposes but is unwarranted and is not supported in production environments or any environment that you plan to push to production. Informatica intends to include the preview functionality in an upcoming release for production use, but might choose not to in

accordance with changing market or technical circumstances. For more information, contact Informatica Global Customer Support.

Secure Data Sharing in Snowflake allows you to share selected database assets with other Snowflake accounts without copying or transferring any actual data. To share data, providers create a share of their database, select specific objects to include, and then add consumer accounts to this share.

You can extract metadata from the following database assets shared through Snowflake Secure Data Sharing:

- Database
- Table
- External table
- Secure view
- Secure materialized view

To view the complete data lineage and all the metadata extracted for the consumer account, including shared assets, perform a connection assignment between catalog sources created for the provider and consumer Snowflake accounts.

Data profiling for Snowflake objects

Configure data profiling to run profiles on the metadata extracted from a Snowflake source system.

You can run data profiles on the following Snowflake objects:

- Table
- View

The data profiling task runs profiles on the following data types for Snowflake objects:

- NUMBER
- FLOAT
- DOUBLE
- VARCHAR
- BOOLEAN
- DATE
- TIME
- TIMESTAMP_LTZ
- TIMESTAMP_NTZ
- TIMESTAMP_TZ
- OBJECT
- ARRAY
- VARIANT

Compatible connectors

Before you configure a Snowflake catalog source, you must connect to the Snowflake source system.

Use the Snowflake Data Cloud connector to connect to the Snowflake source system. For information about configuring a connection, see *Connections* in the Administrator help.

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.
- To scan procedures and functions, set the following roles depending on permissions:
 - With administrator permission. In the JDBC connect string, use: `role=<procedure owner>`
`orrole=SYSADMIN`
Only the SYSADMIN can scan procedures or functions defined with the EXECUTE AS OWNER statement.
 - Without administrator permission. Set the USAGE privileges for all procedures and functions. Create procedures with the EXECUTE AS CALLER statement.
- Configure a connection to the Snowflake source system in Administrator.
- Optionally, if you want to identify pairs of similar columns and relationships between tables within a catalog source, import a relationship inference model.

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 to extract metadata

To extract Snowflake metadata, you need access to the Snowflake source system.

Grant read permission to the user account on all tables in the database from which you extract metadata.

Grant permissions that allow you to perform the following operations:

- select on information_schema.EXTERNAL_TABLES
- select on information_schema.FUNCTIONS
- select on information_schema.PIPES
- select on information_schema.PROCEDURES
- select on information_schema.SCHEMATA
- select on information_schema.SEQUENCES

- select on information_schema.STAGES
- select on information_schema.TABLES
- select on information_schema.VIEWS
- select on information_schema.DATABASES
- select on information_schema.COLUMNS
- show objects
- show columns
- show streams
- show primary keys
- show imported keys
- show columns
- show objects
- show materialized views
- show views
- show tasks
- show databases

Optionally, to obtain more detailed results, grant permissions that allow you to perform the following operations:

- select on SNOWFLAKE.ACCOUNT_USAGE.TAGS
- select on SNOWFLAKE.ACCOUNT_USAGE.TAG_REFERENCES

Permissions to run data profiles

Ensure that you have the required permissions to run profiles.

Grant SELECT permissions for tables and views that you want to profile.

Permissions to perform data classification

You don't need any additional permissions to run data classification.

Permissions to perform relationship discovery

You don't need any additional permissions to run relationship discovery.

Permissions to perform glossary association

You don't need any additional permissions to run glossary association.

Permissions to perform writeback

Ensure that you have the required permissions to perform writeback.

You need the following privileges to perform writeback:

- CREATE TAG privilege to create tags in a database or schema.

- APPLY TAG privilege to assign or modify tag values for objects.

Create a connection

When you configure a connection, you specify the connection properties for the connection. Connection properties enable an agent to connect to data sources.

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	Optional description of the connection. Maximum length is 4000 characters.
Type	Type of connection. Ensure that the type is Snowflake Data Cloud.

4. In the Snowflake Data Cloud Properties section, select the runtime environment where you want to run the tasks. The runtime environment is either a Secure Agent or a serverless runtime environment.
5. In the Connection section, select the authentication method.

You can use the following authentication methods to connect to Snowflake:

- **Standard.** Uses the Snowflake account user name and password credentials to connect to Snowflake.
- **KeyPair.** Uses the private key file and private key file password, along with the existing Snowflake account user name to connect to Snowflake.
- **Client Credentials.** Uses the client ID, access token URL, client secret, scope, and the access token at a minimum.

Standard authentication

This authentication method requires the Snowflake account user name and password credentials to connect to Snowflake.

The following table describes the basic connection properties for standard authentication

Property	Description
Username	The user name to connect to the Snowflake account.
Password/PAT	The password or programmatic access token (PAT) to connect to the Snowflake account. Enter the password of your Snowflake account or the PAT granted by Snowflake.

Property	Description
Account	<p>The name of the Snowflake account.</p> <p>For example, if the Snowflake URL is <code>https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#/,</code> your account name is the first segment in the URL before <code>snowflakecomputing.com</code>. Here, <code>123abc.us-east-2.aws</code> is your account name.</p> <p>If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard,</code> your account name is <code>123abc.us-east-2.aws</code>.</p> <p>Note: Ensure that the account name doesn't contain underscores. If the account name contains underscores, you need to use the alias name. To use an alias name, contact Snowflake Customer Support.</p>
Warehouse	The Snowflake warehouse name.

Property	Description
Role	The Snowflake role assigned to the user.
Additional JDBC URL Parameters	<p>The additional JDBC connection parameters.</p> <p>You can specify multiple JDBC connection parameters, separated by ampersand (&), in the following format:</p> <pre><param1>=<value>&<param2>=<value>&<param3>=<value>...</pre> <p>For example, you can pass the following database and schema values when you connect to Snowflake:</p> <pre>db=mydb&schema=public</pre> <p>When you add parameters, ensure that there is no space before and after the equal sign (=).</p>

Key pair authentication

This authentication method requires the private key file and private key file password, along with the existing Snowflake account user name to connect to Snowflake.

The following table describes the basic connection properties for key pair authentication:

Property	Description
Username	The user name to connect to the Snowflake account.
Account	<p>The name of the Snowflake account.</p> <p>For example, if the Snowflake URL is <code>https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#/,</code> your account name is the first segment in the URL before <code>snowflakecomputing.com</code>. Here, <code>123abc.us-east-2.aws</code> is your account name.</p> <p>If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard,</code> your account name is <code>123abc.us-east-2.aws</code>.</p> <p>Note: Ensure that the account name doesn't contain underscores. If the account name contains underscores, you need to use the alias name. To use an alias name, contact Snowflake Customer Support.</p>

Property	Description
Warehouse	The Snowflake warehouse name.
Private Key File	<p>Path to the private key file, including the private key file name, that the Secure Agent uses to access Snowflake.</p> <p>For example, specify the following path and key file name in the Secure Agent machine:</p> <ul style="list-style-type: none"> - On Windows: C:\Users\path_to_key_file\rsa_key.p8 - On Linux: /export/home/user/path_to_key_file/rsa_key.p8 <p>To use the serverless runtime environment, specify the following path and key file name in the serverless agent directory:</p> <p>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<Private key file name></p> <p>Note: Verify that the keystore is FIPS-certified.</p>

The following table describes the advanced connection properties for key pair authentication:

Property	Description
Additional JDBC URL Parameters	<p>The additional JDBC connection parameters.</p> <p>You can specify multiple JDBC connection parameters, separated by ampersand (&), in the following format:</p> <pre><param1>=<value>&<param2>=<value>&<param3>=<value>...</pre> <p>For example, you can pass the following database and schema values when you connect to Snowflake:</p> <pre>db=mydb&schema=public</pre> <p>When you add parameters, ensure that there is no space before and after the equal sign (=).</p>
Private Key File Password	Password for the private key file.

Client Credentials

The OAuth 2.0 client credentials authentication requires at a minimum the client ID, access token URL, client secret, scope, and the access token.

The following table describes the basic connection properties for OAuth 2.0 client credentials authentication:

Property	Description
Account	<p>The name of the Snowflake account.</p> <p>For example, if the Snowflake URL is <code>https://<123abc>.us-east-2.aws.snowflakecomputing.com/console/login#/,</code> your account name is the first segment in the URL before <code>snowflakecomputing.com</code>. Here, <code>123abc.us-east-2.aws</code> is your account name.</p> <p>If you use the Snowsight URL, for example, <code>https://app.snowflake.com/us-east-2.aws/<123abc>/dashboard,</code> your account name is <code>123abc.us-east-2.aws</code>.</p> <p>Note: Ensure that the account name doesn't contain underscores. If the account name contains underscores, you need to use the alias name. To use an alias name, contact Snowflake Customer Support.</p>
Warehouse	The Snowflake warehouse name.

Property	Description
Access Token URL	The Snowflake access token endpoint that is used to exchange the authorization code for an access token. Specify the access token URL that you get from the OAuth endpoint.
Client ID	Client ID of your application generated when you configure the application for OAuth.
Client Secret	Client secret generated for the client ID.
Scope	Determines the access control when the API endpoint has defined custom scopes. For example, specify <code>session:role:CQA_GCP</code> as the scope to override the value of the default user role. The value needs to one of the roles assigned in Security Integration. To enter multiple scope attributes, separate each scope attribute with a space.
Access Token	The access token value. Enter the populated access token value that you get from the OAuth endpoint, or click Generate Access Token to populate the access token value.

The following table describes the advanced connection properties for the OAuth 2.0 client credentials authentication:

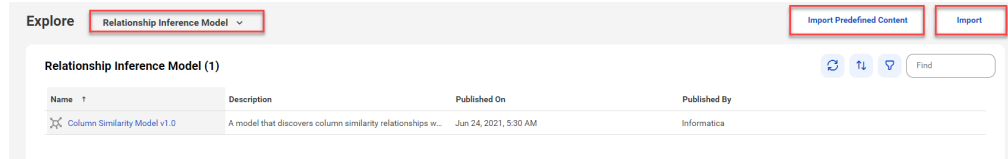
Property	Description
Additional JDBC URL Parameters	The additional JDBC connection parameters. You can specify multiple JDBC connection parameters, separated by ampersand (&), in the following format: <code><param1>=<value>&<param2>=<value>&<param3>=<value>...</code> For example, you can pass the following database and schema values when you connect to Snowflake: <code>db=mydb&schema=public</code> When you add parameters, ensure that there is no space before and after the equal sign (=). For the list of additional JDBC parameters that you can configure, see JDBC URL parameters .
Access Token Parameters	Additional parameters to use with the access token URL. Define the access token parameters in the following JSON format: <pre>[{"Name": "<Parameter name>", "Value": "<Parameter value>"}]</pre> For example, you can use the following <code>code_verifier</code> parameter when you connect to Snowflake: <pre>[{"Name": "code_verifier", "Value": "5PMddu6Zcg6Tc4sbg"}]</pre> For more information about access token parameters that you can define, see Introduction to OAuth in the Snowflake documentation.

Import a relationship inference model

Import a relationship inference model if you want to configure the relationship discovery capability. You can either import a predefined relationship inference model, or import a model file from your local machine.

1. In Metadata Command Center, click **Explore** on the navigation panel.

2. Expand the menu and select **Relationship Inference Model**. The following image shows the **Explore** page with the **Relationship Inference Model** menu:



3. Select one of the following options:
- **Import Predefined Content.** Imports a predefined relationship inference model called Column Similarity Model v1.0.
 - **Import.** Imports the predefined relationship inference model from your local machine. Select this if you previously imported predefined content into your local machine and the inference model is stored on the machine.
To import a file, click **Choose File** in the **Import Relationship Inference Model** window and navigate to the model file on your local machine. You can also drag and drop the file.

The imported models appear in the list of relationship inference models on the **Relationship Discovery** tab.

CHAPTER 3

Create catalog sources in Metadata Command Center

Use Metadata Command Center to configure a catalog source for Snowflake and run the catalog source job.

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.

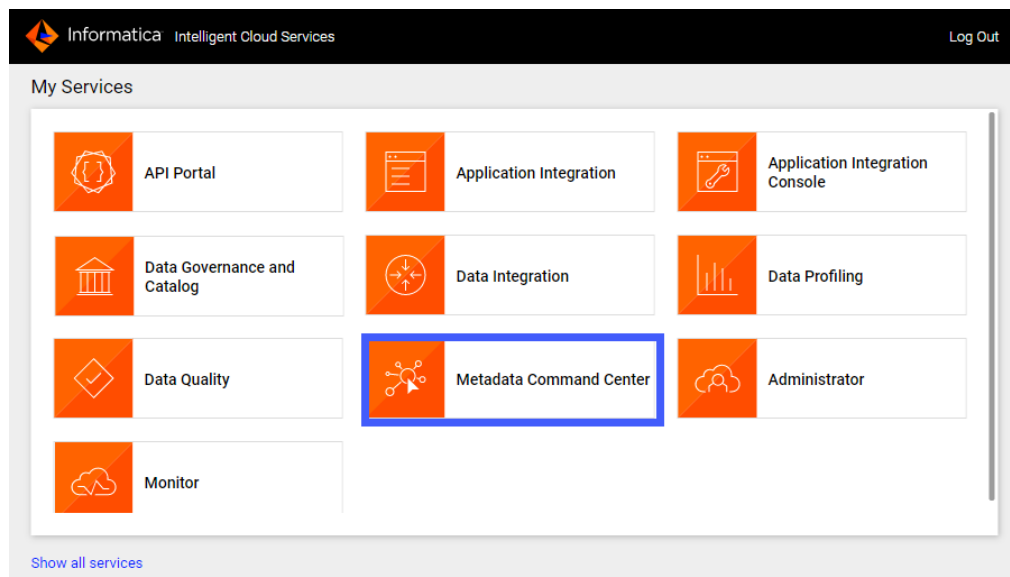
To provide stakeholders access to technical assets, you can assign access through roles. To view lineage for any system that the source system references, create a catalog source and a connection associated with the referenced source system after you run the job.

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 Snowflake from the list of source systems.

New

Choose the asset type you want to create

Find

Catalog Source

Customization

Data Classification

Lookup Table

Snowflake
A cloud-based data storage and analytics service.

Snowflake SQL Script
A set of Snowflake SQL statements stored in files that you can use to run sequential scripts.

Tableau
A business intelligence tool to connect to data and create dashboards that can be shared.

Talend Data Integration
An ETL data integration platform that you can use to gain business insights from data.

Teradata BTEQ Script
A set of BTEQ commands and Teradata SQL statements stored in files that you can use to run sequential scripts.

Teradata Database
A relational database management system (RDBMS) solution for data warehousing applications.

Create **Cancel**

6. Click **Create**.

The **New Catalog Source** page opens.

The following image shows the Snowflake catalog source:

General Information

Name: *

Description:

Connection Information

Catalog Source Type: Snowflake

Connection: *

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 Snowflake catalog source, you define the settings for the metadata extraction capability and other optional capabilities.

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 Snowflake catalog source, you choose a runtime environment, define filters, and enter configuration parameters for metadata extraction.

Before you configure metadata extraction, configure runtime environments in the Informatica Intelligent Cloud Services Administrator.

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:

Note: If the JDBC URL in the connection that you use doesn't include database details and you don't add a filter, the catalog source job extracts metadata only from the default database. If you are unsure whether the JDBC URL includes database details, add filters to ensure that the job extracts metadata from all required databases.

To define filters, you can either select an object type and enter the path to the object as the filter value, or select an object from a list of objects available in the source system.

- a. Select **Yes** to view filter options.
- b. From the Include/Exclude list, choose to include or exclude metadata based on the filter parameters.
- c. Perform one of the following steps:
 - From the Object type list, select **Tables, Views, External tables, Tags, Stored procedures, Tasks, Pipes, Dynamic tables, or All** depending on the object that you want to extract metadata from. Enter the path to the object as the filter value.
 - In the filter value field, click the Search button and select an object from a list of objects available in the source system.
The Object type field updates based on the selected object.

If you select an object type and then click the Search button, the list of objects includes all object types, but you can only select objects that match the selected object type.

You can edit the filter value after you select an object from the list.

Note: You can only search for object types that work with the search functionality. If you don't see the Search button for the selected object, enter the object path as the filter value.

Note: If the object metadata is available in Data Governance and Catalog, a check mark appears next to the object.

Note: To select an object, you need to have permissions on the connection to the source system.

Filters can contain the following wildcards:

- Question mark. Represents a single character.
- Asterisk. Represents multiple characters or empty text.

For object hierarchies, use a dot as a separator.

Filters are case-insensitive.

When you enter values for filters, enclose them in double quotes if you use a space or a dot in a single segment.

The following image shows the filter condition options:

Examples:

- To include or exclude all object types in the 'Schema1' schema in the 'dbName1' database, select **All** as the object type and enter `dbName1.Schema1` in the value field.
 - To include or exclude all tables in the 'Schema1' schema in the 'dbName1' database, select **Tables** as the object type and enter `dbName1.Schema1` in the value field.
 - To include or exclude all views in the 'dbName1' database, select **Views** as the object type and enter `dbName1` in the value field.
 - To include or exclude all tables in databases with names that start with 'dbName' followed by one additional character, select **Tables** as the object type and enter `dbName?` in the value field.
 - To include or exclude the 'Externaltable1' external table in the 'Schema1' schema in the 'dbName1' database, select **External tables** as the object type and enter `dbName1.Schema1.Externaltable1` in the value field.
 - To include or exclude stored procedures with names that start with 'abc' followed by one additional character, in schemas with names that start with 'Schema' followed by any number of characters, select **Stored procedures** as the object type and enter `Schema*.abc?` in the value field.
- d. Optionally, to define an additional filter with an OR condition, click the **Add** icon.
4. Optionally, in the **Configuration Parameters** area, enter properties to override default context values and job parameters.

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

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

Parameter	Description
Default variables values	Specify a default value for variables used in the programmable objects.
MetaTables Include Filter	<p>Advanced parameter. When you process PL/SQL statements, Metadata Command Center does not read tables or view content by default. If you want to use the content, for example, to process dynamic SQL statements, use the MetaTables Include Filter parameter. This parameter prompts the database for the required metadata. Verify that the user has SELECT permissions for metatables.</p> <p>Note: Don't use this option to specify filters for tables that you want to include or exclude for metadata extraction.</p>

The following table describes the property that you can 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.

5. 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.
- e. 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 profiling and quality

Enable the data profiling and quality capability to evaluate the quality of metadata extracted from the Snowflake source system.

1. Click the **Data Profiling and Quality** tab.
2. Expand **Data Profiling** and select **Enable Data Profiling**.

Note: Ensure that you have permissions on all the staging connections that you use in your data profiling configuration. You can't run the job if you don't have permissions on the connections that you use. Select connections that you have access to, or ask the administrator to grant the necessary permissions on the connections that you want to use.
3. In the **Connection and Runtime** area, choose the Secure Agent group where you want to run catalog source jobs.
4. Optionally, in the **Filters** area, specify additional filters in addition to metadata filters.
 - a. Select **Yes** to view filter options.
 - b. From the Include/Exclude list, choose to include or exclude metadata based on the filter parameters.
 - c. From the Object type list, select **Tables** or **Views** depending on the object that you want to profile. Select **All** to profile all objects.
 - d. Enter the path to the object as the filter value.

Filters can contain the following wildcards:

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

Examples:

 - You extracted metadata of all tables and views from a database schema and now you want to profile a specific table. Select **Tables** from the Object type list and then enter the database name and schema name followed by the table name in the input field. For example, `Database_Name.Schema_Name.TABLE_NAME`.
 - You extracted metadata from multiple database schemas and now you want to run a profile on all objects in a specific schema. Select **All** from the Object type list and then enter the database name and schema name in the input field.

To include or exclude multiple objects, click the **Add** icon to add filters with the OR condition.
5. In the **Parameters** area, select the parameters.

The following table describes the parameters that you can enter:

Parameter	Description
Modes of Run	<p>Determine the type of data that you want the data profiling task to collect. Choose one of the following options:</p> <ul style="list-style-type: none"> Keep signatures only. Collects only aggregate information such as data types, average, standard deviation and patterns. Keep signatures and values. Collects both signatures and data values.
Profiling Scope	<p>Determine whether you want to run data profiling only on the changes made to the source system or on the entire source system. Choose one of the following options:</p> <ul style="list-style-type: none"> Incremental. Includes only source metadata that is changed or updated since the last profile run. Full. Includes the entire metadata that is extracted based on the filters applied for extraction. <p>Note: You can run a profile on a maximum of 500,000 data elements. If you have more than 500,000 data elements, run profiles incrementally.</p>
Sampling Type	<p>Determine the sample rows on which you want to run the data quality task. Choose one of the following options:</p> <ul style="list-style-type: none"> All rows. Runs data profiling on all rows in the metadata. Limit N Rows. Runs data profiling on a limited number of rows. Custom Query. Provides an SQL clause to select sample rows to run the data profiling task.
No of rows to limit	Required if you select Limit N Rows in Sampling Type. Specify the number of rows that you want to run the profile on.
Mapping Submission Timeout	The maximum amount of time a mapping task stays in the queue before it times out. Enter the time in minutes.
Maximum Precision of String Fields	The maximum precision value for profiles on string data type.
Text Qualifier	<p>The character that defines string boundaries. If you select a quote character, profiling ignores delimiters within the quotes. Select a qualifier from the list.</p> <p>Note: Default is Double Quote.</p>

- Expand **Data Quality** and select **Enable Data Quality**.

Note: You can click **Use Data Profiling Parameters** to use the same parameters as in the **Data Profiling** section.

Note: Ensure that you have permissions on all the staging and flat file connections that you use in your data quality configuration. You can't run the job if you don't have permissions on the connections that you use. Select connections that you have access to, or ask the administrator to grant the necessary permissions on the connections that you want to use.

- In the **Connection and Runtime** area, choose the Secure Agent group where you want to run catalog source jobs.

8. In the **Parameters** area, select the parameters.

The following table describes the properties that you can enter:

Parameter	Description
Data Quality Rule Automation	Enable the option to automatically create or update rule occurrences for data elements in the catalog source. Choose one of the following options: <ul style="list-style-type: none">• Apply on Data Elements linked with Business Dataset. Creates rule occurrences for all data elements that are linked with business data sets in the catalog source.• Apply on all Data Elements. Creates rule occurrences for all data elements in the catalog source.
Cache Result	Specify how you want to preview the rule occurrence results. Select Agent Cache if you want to generate a cache file in the runtime environment and to preview the cached results faster in subsequent data preview runs. The results are cached for seven days by default after the first run in the runtime environment. Select No Cache if you don't want to cache the preview results and view the live results.
Run Rule Occurrence Frequency	Specify whether you want to run data quality rules based on the frequency defined for the rule occurrence in Data Governance and Catalog.
Sampling Type	Determine the sample rows on which you want to run the data quality task. Choose one of the following options: <ul style="list-style-type: none">• All rows. Runs data quality on all rows in the metadata.• Limit N Rows. Runs data quality on a limited number of rows.• Custom Query. Provide an SQL clause to select sample rows to run the data quality task.
No of rows to limit	Required if you select Limit N Rows in Sampling Type. Specify the number of rows on which you want to run data quality.
Mapping Submission Timeout	The maximum amount of time a mapping task stays in the queue before it times out. Enter the time in minutes.
Maximum Precision of String Fields	The maximum precision value for profiles on string data type.
Text Qualifier	The character that defines string boundaries. If you select a quote character, the data quality task ignores delimiters within the quotes. Select a qualifier from the list. Note: Default is Double Quote.

9. To enable the data observability capability, expand **Data Observability** and select **Enable Data Observability**.

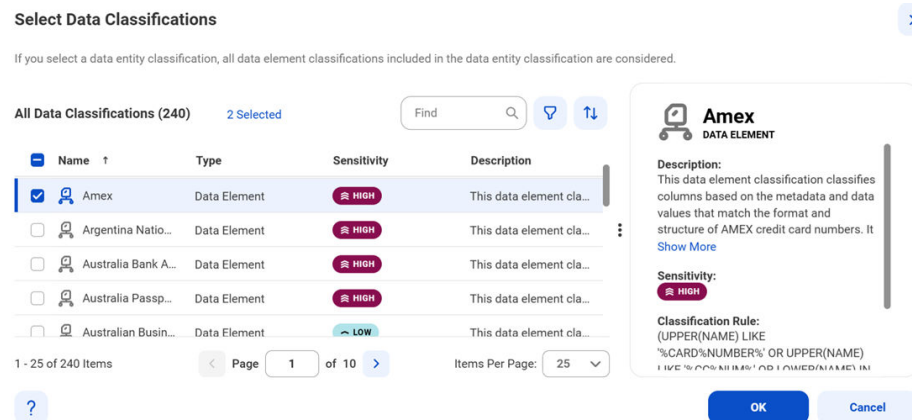
Configure data classification

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

1. Click the **Data Classification** tab.
2. Select **Enable Data Classification**.

3. Choose one 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.
 1. Click **Add Data Classification**. The following image shows the **Select Data Classifications** dialog box:



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

Configure relationship discovery

Enable the relationship discovery capability to identify pairs of similar columns and relationships between tables within a catalog source.

Before you configure relationship discovery, perform the following tasks:

- Import a relationship inference model. For more information about importing a relationship inference model, see [“Import a relationship inference model” on page 15](#).
- Enable data profiling on the **Data Profiling and Quality** tab, and select **Keep Signatures and Values** as the run mode in the **Parameters** section. These configurations enable you to retain values of the columns in the profiling results and discover relationships.

1. Click the **Relationship Discovery** tab.
2. Select **Enable Relationship Discovery**.
3. In the **Column Similarity** area, select the **Relationship Inference Model**.

Note: The relationship inference models that you imported appear in the **Relationship Inference Model** field.

4. In the **Joinable Tables Relationship** area, specify the **Containment Score Threshold** to identify joinable table relationships within the catalog source. This score is an indicator of the data overlap between any two given columns which determines whether the tables are joinable.

Note: A higher score means that the objects have more overlapping data and a lower score means lesser overlapping data between the two objects. A containment score threshold lower than 0.4 might result in a large number of false positives.

After you run the catalog source job, you can view the inferred relationships on the **Relationships** tab of the extracted assets in Data Governance and Catalog.

Configure glossary association

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.

Configure writeback

After you apply data classifications to the Snowflake metadata and data facts, you can write back the associated data classifications as tag values to the Snowflake source system.

To write back data classifications, you must have run the catalog source job at least once with data classification configured.

In Snowflake, a tag is a schema-level object that can be assigned to another Snowflake object. When you run the catalog source job on a Snowflake source system, the metadata extraction task extracts Snowflake tags by default. The writeback capability lets you enrich the Snowflake source system directly with the data classifications that you manually or automatically associate with columns. For example, if the Snowflake source includes a masking policy, the data classification capability identifies columns that contain sensitive information and the writeback capability allows users to send the data classification associated with sensitive data to Snowflake. After performing the writeback capability, the Snowflake user can use the information to mask the data.

Note: You can apply data classification only to the columns that already have Snowflake tags.

You can't configure the writeback capability to run on a schedule.

After you associate data classifications with the Snowflake metadata and data facts, perform the following tasks to write back the associated data classifications as tag values to the Snowflake source system:

1. Export the details of the associated data classifications in an Excel file.
 - a. Go to the **Explore** page and search for the Snowflake catalog source that you created.
 - b. Click the **Action** menu for the catalog source, and select **Export** to export the file. You can monitor the export job on the **Job Monitoring** page. After the export job completes successfully, you can view the statistics for the classification associations on the job details page.
 - c. Click **Download Export File** in the **Job Details** area to download the Excel file. The file contains details of the data classifications associated with the columns of the Snowflake source system.

Note: If you did not associate data classifications with the Snowflake metadata, the downloaded file contains only headers.
2. Optionally, curate the downloaded file based on business needs.
3. Import the Excel file and run the catalog source job.
 - a. Go to the **Explore** page and open the Snowflake catalog source.
 - b. Click the **Writeback** tab.
 - c. Select **Enable writeback**.
 - d. In the **Connection and Runtime** area, select an OAuth-based Snowflake connection that has permissions to manage Snowflake tags. This connection can be different from the connection that you use to connect to the Snowflake source system.
 - e. Click **Run**.
 - f. On the **Run Catalog Source Job** dialog window, upload the Excel file.
 - g. Click **Run**.
 - h. Click the **Refresh** button to view the updated status.
 - i. When the writeback job completes, you can see the results in the **Writeback Details** area.

After the catalog source job completes successfully, the catalog source job adds the data classifications as tag values to the Snowflake source system.

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.

- 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.

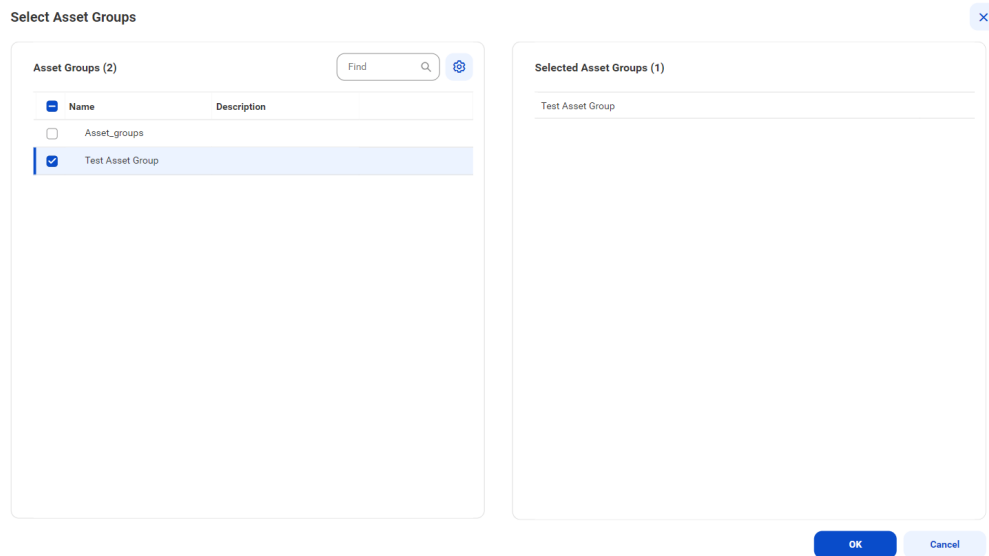
- f. To assign users or user groups from another stakeholder role, click **Add** and then repeat the steps.
2. To assign asset groups to technical assets extracted from the catalog source, perform the following steps:

- 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 database,

such as Snowflake. 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 assign a Snowflake source system as an endpoint catalog source. The objects must be of the Schema 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.

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

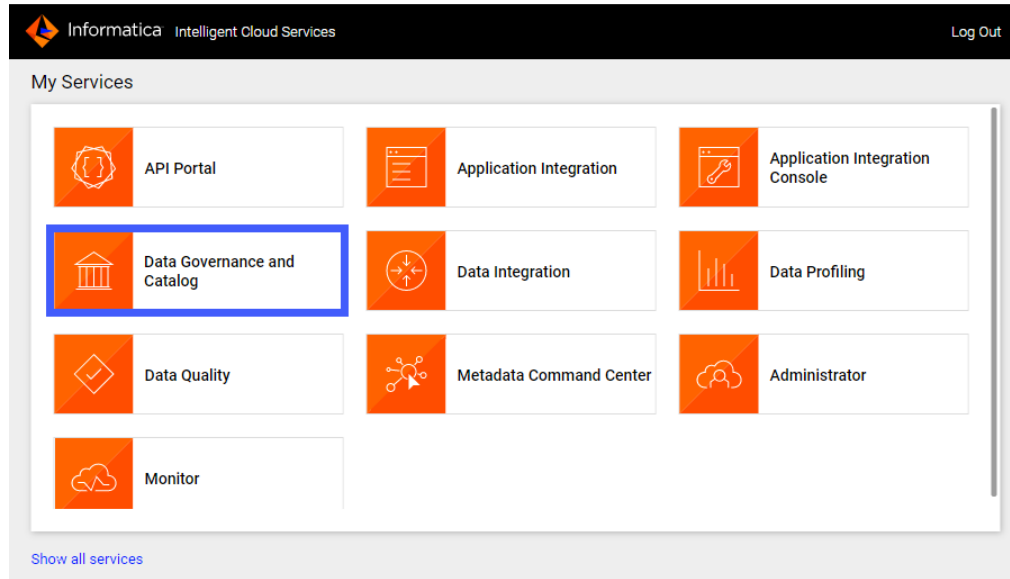
After a job runs in Metadata Command Center, view the results in Data Governance and Catalog. You can view details about source system contents as hierarchical displays and trace data lineage.

1. Log in to Informatica Intelligent Cloud Services.

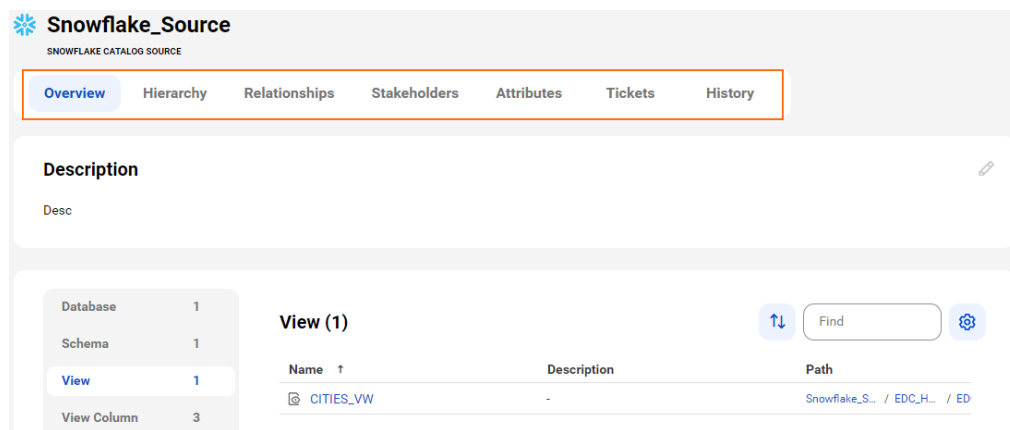
The **My Services** page appears.

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. You can view the calculation properties such as expression, control conditions, and calculation complexity in the **Overview** tab of a calculation asset.
- Note:** If a new record is added to the source system and you run an incremental metadata extraction job, no objects are extracted because the metadata has not changed. If an incremental metadata extraction job includes a view, the job extracts the corresponding tables even if the tables were extracted in previous runs.

For more information about working with assets, see *Working with Assets* in the 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.

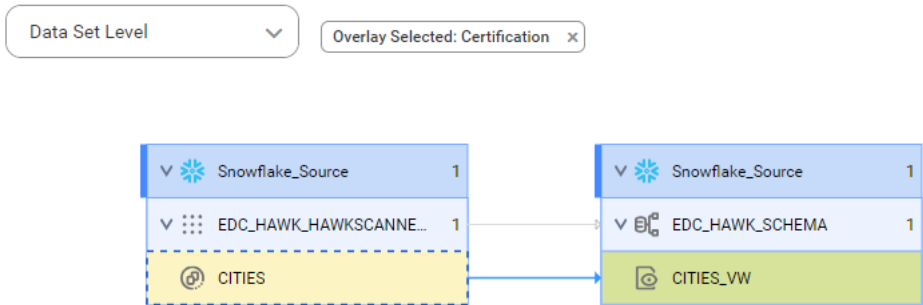
To view data lineage at the catalog source level, open a technical asset, click the **Lineage** tab, and then verify that the level is set to **Catalog Source Level**.

View lineage at the data set level

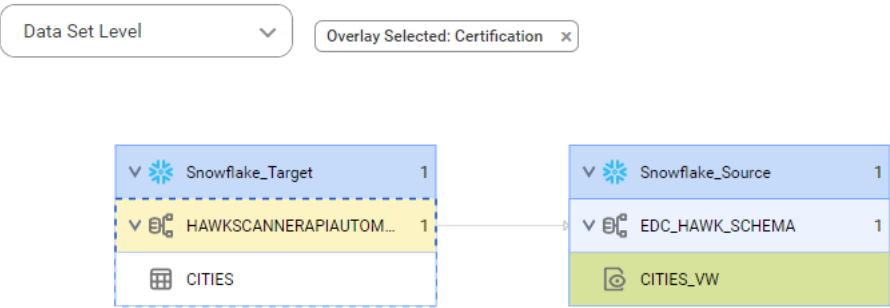
The data set level is a view that shows individual sets of data in the data flow.

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 view gets data from the referenced source table before connection assignment:



The following image shows how the target view gets data from the actual source table after connection



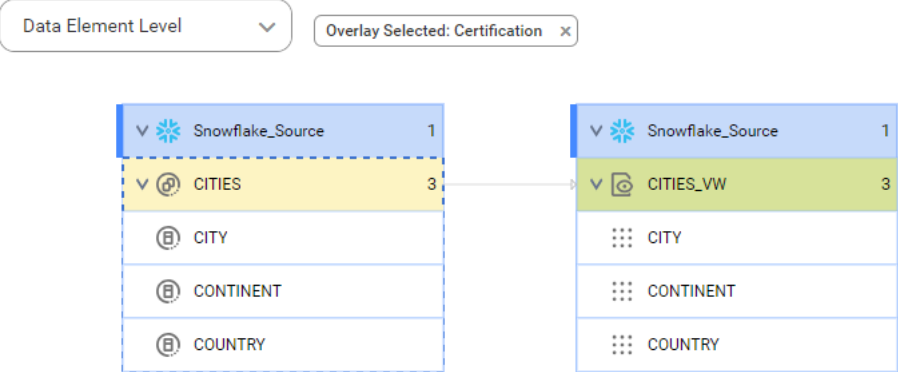
assignment:

View lineage at the data element level

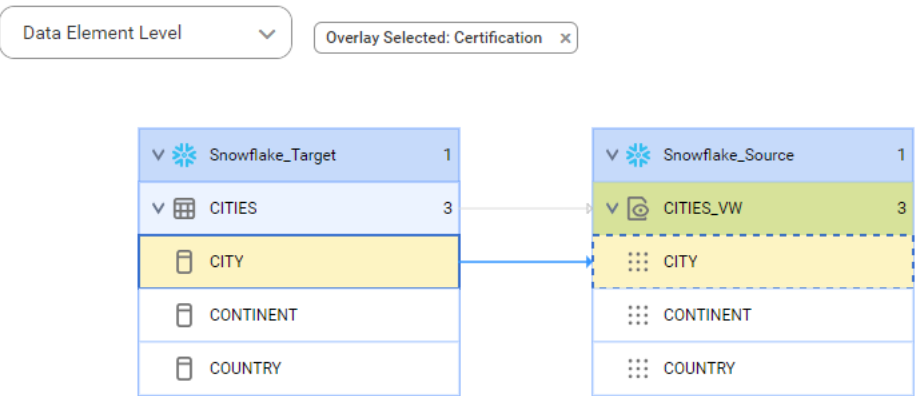
The data element level displays details of the data set level. At the data element level, you can see the input sources for expressions or commands and calculations or transformations on the data.

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 view column gets data from the one column of the referenced source table before connection assignment:



The following image shows how the target view column gets data from one column of the source table after connection assignment:

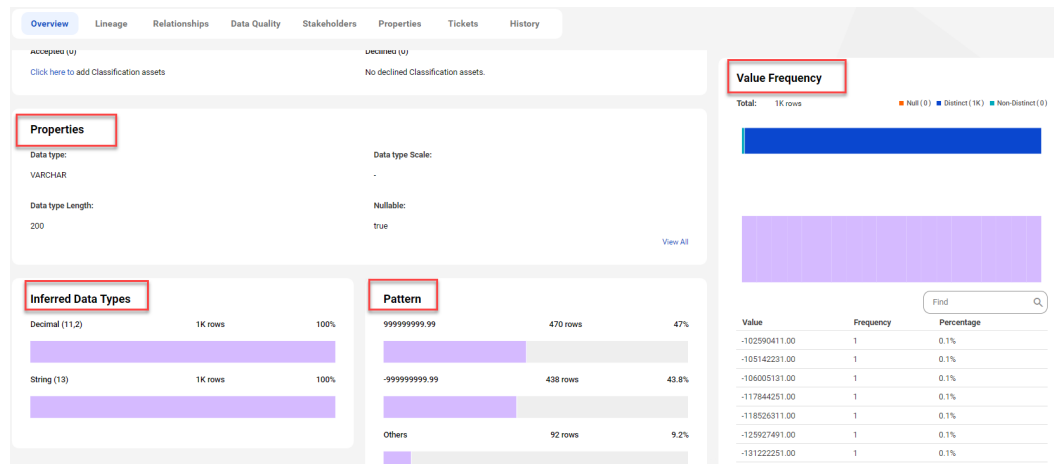


View data profiling results

When you enable the data profiling task for a catalog source in Metadata Command Center, the system runs a profile to evaluate the quality of the metadata extracted from the source system. The profiling statistics appear in Data Governance and Catalog when you open the technical assets.

The scope of profiling statistics that Data Governance and Catalog displays depends on the data profiling configuration parameters that you set when you configured the catalog source in Metadata Command Center.

The following image shows the data profiling statistics that appear on a column asset page in Data Governance and Catalog:



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

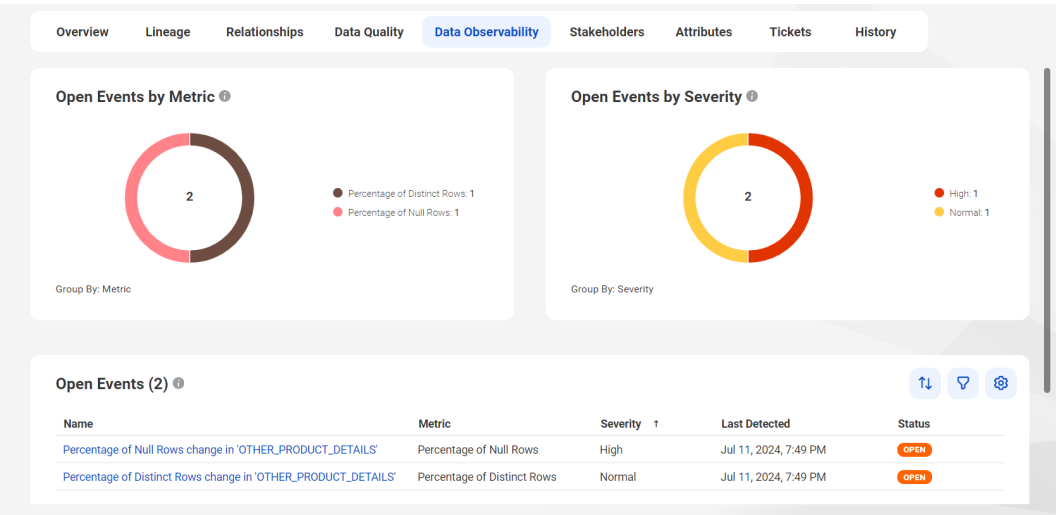
View data observability results

When you enable data observability for a catalog source in Metadata Command Center, you can view and evaluate the events that it generates in Data Governance and Catalog. These events indicate anomalies identified in the characteristics of the profiled data in your source system.

You can view the events that data observability generates for anomalies identified for catalog sources, technical data sets, and data elements. You can then take appropriate actions for the generated events.

Note: The administrator of the catalog source might have applied filters to the data to narrow down the data elements that are applicable for business users in Data Governance and Catalog. The data for which users receive anomaly notifications depend on the filters that are configured for the catalog source.

The following image shows the open events for a column asset in Data Governance and Catalog:

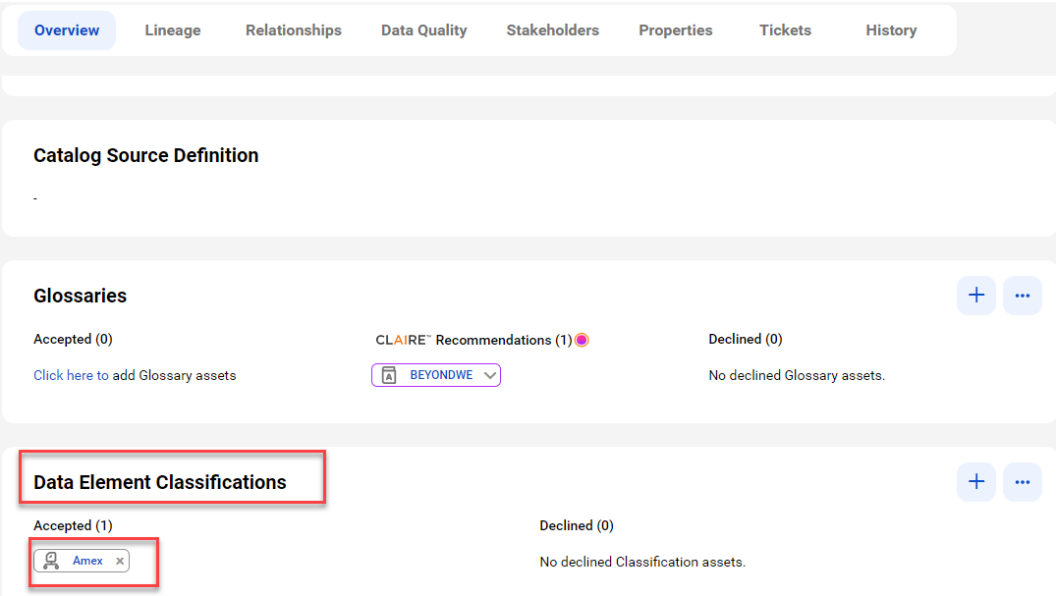


For more information about data observability results, see *Working With Assets* in the Data Governance and Catalog help.

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:



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:

