



Informatica® Metadata Command Center
November 2025

Amazon Redshift 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 Amazon Redshift catalog sources.....	6
Extraction and view process.	7
About the Amazon Redshift catalog source.	8
Extracted metadata.	8
Data profiling for Amazon Redshift objects.	8
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.	12
Create a connection.	12
Default authentication.	13
Redshift IAM AssumeRole authentication.	18
Create endpoint catalog sources for connection assignment.	19
Import a relationship inference model.	20
Chapter 3: Create catalog sources in Metadata Command Center.....	21
Step 1. Register a catalog source.	21
Step 2. Configure capabilities.	23
Configure metadata extraction.	23
Configure lineage discovery.	25
Configure data profiling and quality.	26
Configure data classification.	30
Configure relationship discovery.	30
Configure glossary associations.	31
Step 3. Associate stakeholders and asset groups.	32
Step 4. Run or schedule the job.	33
Step 5. Assign reference catalog source connections to endpoint catalog source objects.	35
Chapter 4: View results in Data Governance and Catalog.....	36
View metadata extraction results.	36
View data lineage.	38
View lineage at the catalog source level.	39
View lineage at the data set level.	39

View lineage at the data element level.	39
View data profiling results	40
View data observability results	41
View classified data.	42
View glossary associations.	42

Preface

Read *Amazon Redshift Sources* to learn how to register and configure Amazon Redshift 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 Amazon Redshift 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, Amazon Redshift is a source system from which you can extract metadata through an Amazon Redshift 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:

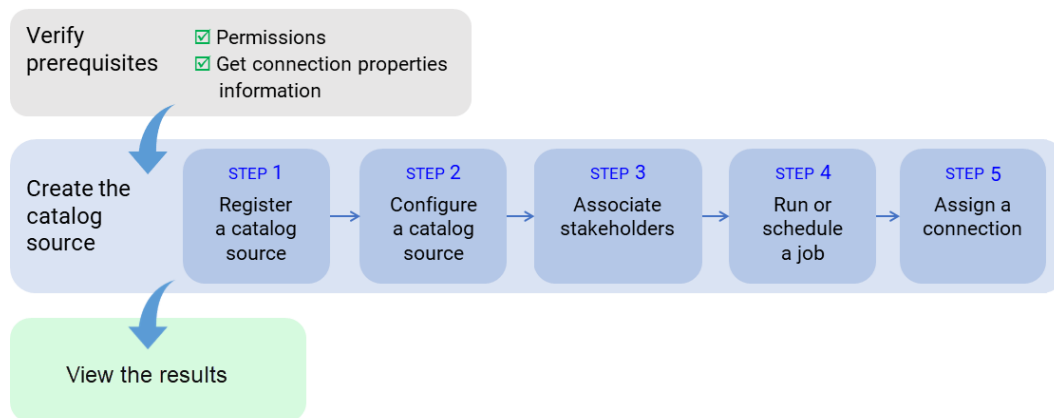
Capability	Description
Serverless Runtime Environment	A serverless runtime environment is an advanced serverless deployment solution that doesn't require downloading, installing, configuring, or maintaining a Secure Agent or Secure Agent group. You can use a serverless runtime environment in the same 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.
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.

Capability	Description
Relationship Discovery	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.
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 Amazon Redshift:

1. Register a catalog source. Create a catalog source object, select Amazon Redshift, 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.

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

About the Amazon Redshift catalog source

You can use the Amazon Redshift catalog source to extract metadata from an Amazon Redshift source system.

Amazon Redshift is a cloud-based data warehousing service that you can use to analyze and store data.

Extracted metadata

You can use the Amazon Redshift catalog source to extract metadata from an Amazon Redshift source system.

Metadata Command Center extracts the following metadata from an Amazon Redshift source system:

- Database
- Schema
- External Schema
- Table
- External Table
- View
- Materialized View
- **Note:** Objects of the Materialized View type appear as View in Data Governance and Catalog.
- Function
- Procedure
- Column

Data profiling for Amazon Redshift objects

Configure data profiling to run profiles on the metadata extracted from an Amazon Redshift source system.

You can run data profiles on the following objects:

- Table
- View
- Spectrum External Table

You can run profiles on Spectrum external tables that are created using the following file formats:

- PARQUET
- AVRO
- TEXT
- RC
- SEQUENCE
- ORC

Note: If the Spectrum external tables include columns with string data types, those columns are skipped and are not considered for data profiling and data quality.

The data profiling task runs profiles on the following data types:

- SMALLINT
- INTEGER
- BIGINT
- DECIMAL
- REAL
- DOUBLE PRECISION
- BOOLEAN
- CHAR
- VARCHAR
- DATE
- TIMESTAMP
- STRING
- SUPER

Compatible connectors

Before you configure an Amazon Redshift catalog source, you must connect to the Amazon Redshift source system.

Use the Amazon Redshift V2 connector to connect to the Amazon Redshift 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.
- Configure authentication.
- Configure a connection to the Amazon Redshift source system in Administrator.
- Create endpoint catalog sources for connection assignment.
- 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

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

Configure the following permissions:

- Read permission on the Amazon Redshift external source.
- Permissions that allow you to perform the following operations:
 - select on pg_catalog.PG_ATTRIBUTE
 - select on pg_catalog.PG_CLASS
 - select on pg_catalog.PG_CONSTRAINT
 - select on pg_catalog.PG_DESCRIPTION
 - select on pg_catalog.PG_LANGUAGE
 - select on pg_catalog.PG_NAMESPACE
 - select on pg_catalog.PG_PROC
 - select on pg_catalog.PG_TYPE

- select on pg_catalog.PG_VIEWS
- select on information_schema.COLUMNS
- select on information_schema.TABLES
- select on pg_catalog.PG_TABLES
- select on pg_catalog.PG_CLASS_INFO
- select on pg_catalog.PG_PROC_INFO
- select on pg_catalog.SVV_EXTERNAL_TABLES
- select on pg_catalog.SVV_EXTERNAL_COLUMNS
- select on pg_get_late_binding_view_cols() cols(view_schema name, view_name name, col_name name, col_type varchar, col_num int)
- Permissions to run the SHOW EXTERNAL TABLE operation on the tables that you want to process.
- Permissions to access tables from a specific schema:

GRANT USAGE ON SCHEMA <Schema name> to <User>;

GRANT SELECT ON ALL TABLES IN SCHEMA <Schema name> TO <User>;

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

- select on pg_catalog.PG_DATABASE

Permissions to run data profiles

Ensure that you have the required permissions to run profiles.

To perform data profiling, you need to unload data to the Amazon Redshift source system.

To unload data, configure the following connector permissions:

- ListBucket. Required to view objects from Amazon S3 buckets.
- GetBucketPolicy. Required to get the IAM policy information for access privilege details on Amazon S3 buckets or folders.
- GetObject. Required to read objects from Amazon S3 buckets.
- PutObject. Required to process staging data for Avro and Parquet files.
- DeleteObject. Required to delete staging data of Avro and Parquet files.

Grant permissions to perform the following operations:

- Usage permission on the schemas to profile.
GRANT USAGE ON SCHEMA <Schema name> TO <User name>;
- Select permission on all tables or specific tables in the schema.
GRANT SELECT ON ALL TABLES IN SCHEMA <Schema name> TO <User name>;
GRANT SELECT ON <Table name> TO <User name>;

Permissions to perform data classification

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

Permissions to perform relationship discovery

You can perform relationship discovery with the permissions required to perform metadata extraction.

Permissions to perform glossary association

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

Create a connection

Create an Amazon Redshift connection object in Administrator with the connection details of the Amazon Redshift source system.

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

Connection 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.

4. Select the Amazon Redshift V2 connection type.

5. Enter properties specific to the Amazon Redshift connection:

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>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.</p> <p>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.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>Name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p>
JDBC URL	<p>The JDBC URL to connect to the Amazon Redshift cluster.</p> <p>You can get the JDBC URL from your Amazon AWS Redshift cluster configuration page.</p> <p>Enter the JDBC URL in the following format:</p> <p><code>jdbc:redshift://<cluster_endpoint>:<port_number>/<database_name></code>, where the endpoint includes the Redshift cluster name and region.</p> <p>For example, <code>jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb</code></p> <p>In the example,</p> <ul style="list-style-type: none">- <code>infa-rs-qa-cluster</code> is the name of the Redshift cluster.- <code>us-west-2.redshift.amazonaws.com</code> is the Redshift cluster endpoint, which is the US West (Oregon) region.- <code>5439</code> is the port number for the Redshift cluster.- <code>rsdb</code> is the specific database instance in the Redshift cluster to which you want to connect.

6. Select the authentication type to connect to Amazon Redshift and enter the required properties.
- You can use the following authentication types:
- Default
 - Redshift IAM Authentication via AssumeRole
7. Click **Test Connection**.
8. Click **Save**.

Default authentication

Default authentication uses the user name and password to connect to Amazon Redshift.

The following table describes the basic connection properties for default authentication:

Properties	Description
JDBC URL	<p>The JDBC URL to connect to the Amazon Redshift cluster.</p> <p>You can get the JDBC URL from your Amazon AWS Redshift cluster configuration page.</p> <p>Enter the JDBC URL in the following format:</p> <p><code>jdbc:redshift://<cluster_endpoint>:<port_number>/<database_name></code>, where the endpoint includes the Redshift cluster name and region.</p> <p>For example, <code>jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb</code></p> <p>In the example,</p> <ul style="list-style-type: none">- <code>infa-rs-qa-cluster</code> is the name of the Redshift cluster.- <code>us-west-2.redshift.amazonaws.com</code> is the Redshift cluster endpoint, which is the US West (Oregon) region.- <code>5439</code> is the port number for the Redshift cluster.- <code>rsdb</code> is the specific database instance in the Redshift cluster to which you want to connect.
Username	User name of your database instance in the Amazon Redshift cluster.
Password	Password of the Amazon Redshift database user.
Use EC2 Role to Assume Role	<p>Enables the EC2 instance that assumes an S3 IAM role to access the S3 resources to stage data using the temporary security credentials.</p> <p>The EC2 role must have a policy attached with permissions to assume an S3 IAM role. The S3 IAM role and the EC2 instance can be in the same or different AWS account.</p> <p>Select the check box to enable the EC2 role to assume an S3 IAM role specified in the S3 IAM Role ARN option to access the S3 resources for staging data.</p>
S3 IAM Role ARN	<p>The Amazon Resource Number (ARN) of the IAM role assumed by the IAM user or EC2 to use the dynamically generated temporary security credentials to stage data in Amazon S3.</p> <p>This property applies when you want to generate temporary security credentials to access the S3 staging buckets by using either the EC2 instance or the IAM user who assumes the S3 IAM role.</p> <p>Specify the S3 IAM role name to use the temporary security credentials to access the Amazon S3 staging bucket.</p> <p>For more information about how to get the ARN of the S3 IAM role, see the AWS documentation.</p>

Advanced settings

The following table describes the advanced connection properties for default authentication:

Properties	Description
S3 Access Key ID	<p>Access key ID of the IAM user to access the Amazon S3 staging bucket.</p> <p>Enter the access key ID when you use the following methods for S3 staging:</p> <ul style="list-style-type: none">- When the IAM user has access to S3 staging.- When the IAM user who assumes the S3 IAM role uses the temporary security credentials to access S3. <p>The S3 access key ID is only validated at runtime, so verify its accuracy before saving the connection to prevent runtime errors.</p> <p>You do not need to enter the S3 access key ID if you use IAM authentication or the assume role for EC2 to access S3.</p> <p>Note: If you use the connection for application ingestion and replication or database ingestion and replication tasks that use key-based authentication, provide the access key value.</p>
S3 Secret Access Key	<p>Secret access key to access the Amazon S3 staging bucket.</p> <p>The secret access key is associated with the access key ID and uniquely identifies the account.</p> <p>Enter the secret access key value when you use following methods for S3 staging:</p> <ul style="list-style-type: none">- When the IAM user has access to S3 staging.- When the IAM user who assumes the S3 IAM role uses the temporary security credentials to access S3. <p>The S3 secret access key is only validated at runtime, so verify its accuracy before saving the connection to prevent runtime errors.</p> <p>You do not need to enter the S3 secret access key if you use IAM authentication or the assume role for EC2 to access S3.</p>
S3 VPC Endpoint Type	<p>The type of Amazon Virtual Private Cloud endpoint for Amazon S3.</p> <p>You can use a VPC endpoint to enable private communication with Amazon S3.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none">- Default. Select if you do not want to use a VPC endpoint.- Interface Endpoint. Select to establish private communication with Amazon S3 through an interface endpoint which uses a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to an AWS service.
Endpoint DNS Name for Amazon S3	<p>The DNS name for the Amazon S3 interface endpoint.</p> <p>Replace the asterisk symbol with the bucket keyword in the DNS name.</p> <p>Enter the DNS name in the following format:</p> <p><code>bucket.<DNS name of the interface endpoint></code></p> <p>For example, <code>bucket.vpce-s3.us-west-2.vpce.amazonaws.com</code></p>
STS VPC Endpoint Type	<p>The type of Amazon Virtual Private Cloud endpoint for AWS Security Token Service.</p> <p>You can use a VPC endpoint to enable private communication with Amazon Security Token Service.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none">- Default. Select if you do not want to use a VPC endpoint.- Interface Endpoint. Select to establish private communication with Amazon Security Token Service through an interface endpoint which uses a private IP address from the IP address range of your subnet.
Endpoint DNS Name for AWS STS	<p>The DNS name for the AWS STS interface endpoint.</p> <p>For example, <code>vpce-01f22cc14558c241f-s8039x4c.sts.us-west-2.vpce.amazonaws.com</code></p>

Properties	Description
KMS VPC Endpoint Type	<p>The type of Amazon Virtual Private Cloud endpoint for AWS Key Management Service. You can use a VPC endpoint to enable private communication with Amazon Key Management Service.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> - Default. Select if you do not want to use a VPC endpoint. - Interface Endpoint. Select to establish private communication with Amazon Key Management Service through an interface endpoint which uses a private IP address from the IP address range of your subnet.
Endpoint DNS Name for AWS KMS	<p>The DNS name for the AWS KMS interface endpoint.</p> <p>For example, <code>vpce-0e722f5c721e19232-g2pkm2r7.kms.us-west-2.vpce.amazonaws.com</code></p>
External ID	<p>The external ID associated with the IAM role.</p> <p>You can specify the external ID if you want to provide a more secure access to the Amazon S3 bucket. The Amazon S3 staging bucket and the IAM role can be in the same or different AWS accounts.</p> <p>If required, you also have the option to specify the external ID in the AssumeRole request to the AWS Security Token Service (STS) using an external ID condition in the assumed IAM role's trust policy.</p> <p>For more information about using an external ID, see External ID when granting access to your AWS resources.</p>

Properties	Description
Cluster Region	<p>The AWS cluster region in which the Redshift cluster resides.</p> <p>Select the cluster region from the list if you choose to provide a custom JDBC URL with a different cluster region from that specified in the JDBC URL field property. To continue to use the cluster region name specified in the JDBC URL field property, select None as the cluster region in this property.</p> <p>You can only read data from or write data to the cluster regions supported by the AWS SDK.</p> <p>Select one of the following cluster regions:</p> <p>None</p> <p>Asia Pacific(Mumbai)</p> <p>Asia Pacific(Seoul)</p> <p>Asia Pacific(Singapore)</p> <p>Asia Pacific(Sydney)</p> <p>Asia Pacific(Tokyo)</p> <p>Asia Pacific(Hong Kong)</p> <p>AWS GovCloud (US)</p> <p>AWS GovCloud (US-East)</p> <p>Canada(Central)</p> <p>China(Beijing)</p> <p>China(Ningxia)</p> <p>EU(Ireland)</p> <p>EU(Frankfurt)</p> <p>EU(Paris)</p> <p>EU(Stockholm)</p> <p>South America(Sao Paulo)</p> <p>Middle East(Bahrain)</p> <p>US East(N. Virginia)</p> <p>US East(Ohio)</p> <p>US West(N. California)</p> <p>US West(Oregon)</p> <p>Default is None.</p>
Connection Environment SQL	<p>The SQL statement to set up the database environment that applies for the entire session.</p> <p>Separate multiple values with a semicolon (;).</p> <p>Specify only the configurations for the database environment in the SQL statement. Do not specify any DDL or DML commands in the SQL statement.</p>
Master Symmetric Key	<p>You cannot use client-side encryption type for Amazon Redshift V2 Connector. Hence, if you specify the master symmetric key, it is ignored.</p>
Customer Master Key ID	<p>The customer master key ID generated by AWS Key Management Service (AWS KMS) or the ARN of your custom key for cross-account access when you stage data in Amazon S3. The customer master key serves to encrypt your data at the destination before they are saved in Amazon S3.</p> <p>You can either enter the customer-generated customer master key ID or the default customer master key ID.</p>

Redshift IAM AssumeRole authentication

The Redshift AssumeRole authentication enables the user to assume an IAM role or define an EC2 role configured with required trust policies to generate temporary security credentials to access Amazon Redshift.

The following table describes the basic connection properties for Redshift IAM AssumeRole authentication:

Properties	Description
JDBC URL	<p>The JDBC URL to connect to the Amazon Redshift cluster.</p> <p>You can get the JDBC URL from your Amazon AWS Redshift cluster configuration page.</p> <p>Enter the JDBC URL in the following format:</p> <p><code>jdbc:redshift://<cluster_endpoint>:<port_number>/<database_name></code>, where the endpoint includes the Redshift cluster name and region.</p> <p>For example, <code>jdbc:redshift://infa-rs-cluster.abc.us-west-2.redshift.amazonaws.com:5439/rsdb</code></p> <p>In the example,</p> <ul style="list-style-type: none">- <code>infa-rs-qa-cluster</code> is the name of the Redshift cluster.- <code>us-west-2.redshift.amazonaws.com</code> is the Redshift cluster endpoint, which is the US West (Oregon) region.- <code>5439</code> is the port number for the Redshift cluster.- <code>rsdb</code> is the specific database instance in the Redshift cluster to which you want to connect.
Username	User name of your database instance in the Amazon Redshift cluster.
Cluster Identifier	<p>The unique identifier of the cluster that hosts Amazon Redshift.</p> <p>Specify the Amazon Redshift cluster name.</p>
Database Name	Name of the Amazon Redshift database where the tables that you want to access are stored.
Redshift IAM Role ARN	<p>The Amazon Resource Number (ARN) of the IAM role assumed by EC2 to use the dynamically generated temporary security credentials to access Amazon Redshift.</p> <p>Enter the Redshift IAM role ARN to access the Amazon Redshift cluster.</p>

Properties	Description
Use EC2 Role to Assume Role	<p>Enables the EC2 role to assume an IAM role, either to connect to Redshift or to stage data using the temporary security credentials:</p> <p>Connect to Redshift with IAM authentication using the EC2 role</p> <p>Select the check box to enable the EC2 role that assumes a Redshift IAM role specified in the Redshift IAM Role ARN field to access Amazon Redshift.</p> <p>The EC2 role must have a policy attached with permissions to assume a Redshift IAM role from the same or different account.</p> <p>Access S3 resources to stage data</p> <p>Select the check box to enable the EC2 role to assume an S3 IAM role specified in the S3 IAM Role ARN field and dynamically generate the temporary security credentials to access the S3 staging buckets.</p> <p>The EC2 role must have a policy attached with permissions to assume an S3 IAM role from the same or different AWS account.</p>
S3 IAM Role ARN	<p>The Amazon Resource Number (ARN) of the S3 IAM role assumed by the IAM user or EC2 to use the dynamically generated temporary security credentials to stage data in Amazon S3.</p> <p>This property applies when you want to generate the temporary security credentials to access the S3 staging buckets by using either the EC2 instance or the IAM user who assumes the S3 IAM role.</p> <p>Specify the S3 IAM role name to use the temporary security credentials to access the Amazon S3 staging bucket.</p> <p>For more information about how to get the ARN of the IAM role, see the AWS documentation.</p>

Advanced settings

The following table describes the advanced connection properties for Redshift IAM AssumeRole authentication:

Properties	Description
Redshift Access Key ID	<p>The access key of the IAM user that has permissions to assume the Redshift IAM AssumeRole ARN.</p> <p>This property doesn't apply to Amazon Redshift AssumeRole authentication with EC2 role.</p>
Redshift Secret Access Key	<p>The secret access key of the IAM user that has permissions to assume the Redshift IAM Assume Role ARN.</p> <p>This property doesn't apply to Amazon Redshift AssumeRole authentication with EC2 role.</p>

Create endpoint catalog sources for connection assignment

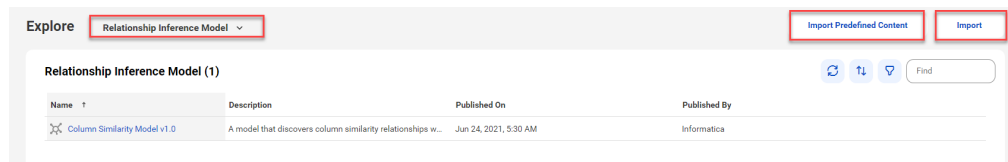
An endpoint catalog source represents a source system that the catalog source references. Before you perform connection assignment, create endpoint catalog sources and run the catalog source jobs.

You can then perform connection assignment to reference source systems to view complete lineage with source system objects.

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 Amazon Redshift 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. 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

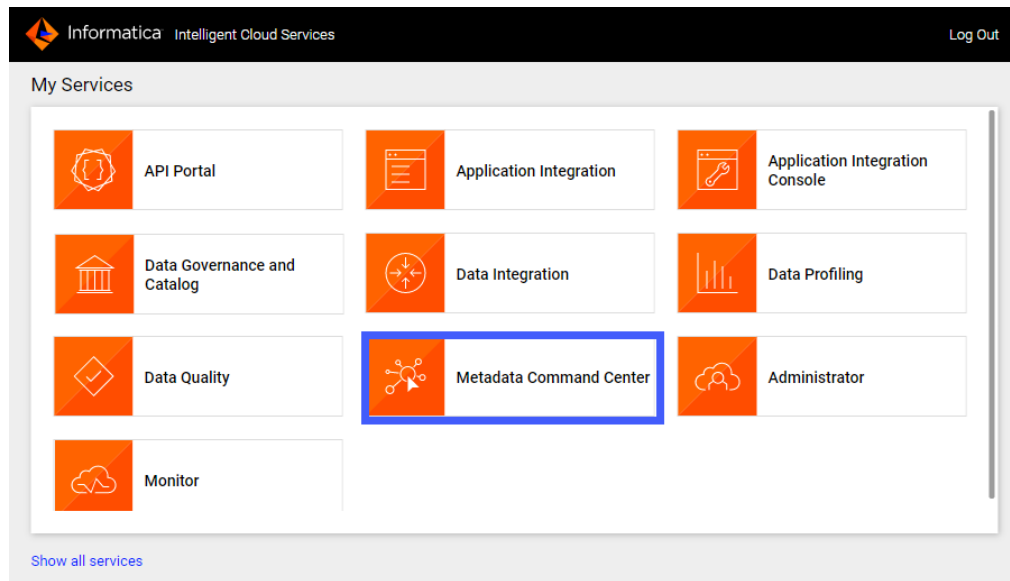
When you register a catalog source, provide general information and connection values.

1. Log in to Informatica Intelligent Cloud Services.

The **My Services** page appears.

2. Click **Metadata Command Center**.

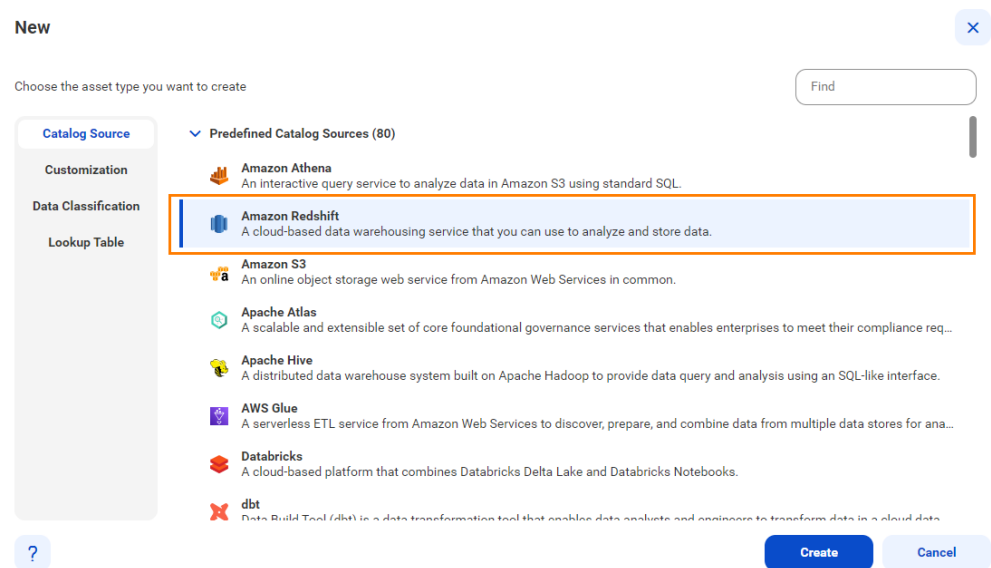
The following image shows the Metadata Command Center box on the **My Services** page:



The Metadata Command Center home page appears.

3. Click **New**.
4. Select **Catalog Source** from the list of asset types.
5. Select Amazon Redshift from the list of catalog source types.

The following image shows the Amazon Redshift catalog source:



6. Click **Create**.
7. The **New Catalog Source** page opens.
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 Amazon Redshift 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 Amazon Redshift 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:

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 an object type or select **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.

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

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. 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:

Specify metadata filters: ⓘ

> Show supported wildcards and examples

Include Metadata	Tables	Enter or select a value to specify the object location.
Exclude Metadata	External tables	Enter or select a value to specify the object location.

4. To define an additional filter with an OR condition, click the **Add** icon.

The following image shows a filter that includes metadata from all objects in schemas with names that start with Schema and excludes metadata from all tables with names that start with table followed by one additional character in the Schema1 schema.

Specify metadata filters:
☐ No
☒ Yes

[Show supported wildcards and examples](#)

Include Metadata	All	Schema*
Exclude Metadata	Tables	Schema1.table?

- Optional. In the **Configuration Parameters** area, enter properties to override default content values and job parameters. Click **Show Advanced** to view all configuration parameters.

The following table describes the properties that you 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 during the metadata extraction run.</p>

- 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	<p>Enter additional configuration options to be passed at runtime. Required if you need to troubleshoot the catalog source job.</p> <p>Caution: Use expert parameters when it is recommended by Informatica Global Customer Support.</p>

- 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.

- Click the **Lineage Discovery** tab.
- Select **Enable Lineage Discovery**.
- 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:

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 capability to evaluate the quality of metadata extracted from the Amazon Redshift 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, specify data profiling filters to run the profile on a subset of the metadata that you extract.
 - a. Select **Yes** to view filter options.
 - b. From the Include/Exclude list, choose to include or exclude metadata.
 - c. From the Object type list, select **Tables**, **Views**, or **External Tables** depending on the object that you want to profile. Select **All** to profile all objects.
 - d. Enter a value to specify the object location.

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 schema and now you want to run a profile on a specific table from the schema. Select **Tables** from the Object type list and then enter the schema name followed by the table name in the input field. For example,
`Schema_Name.TABLE_NAME`
- You extracted metadata from multiple 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 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, configure the parameters.

The following table describes the parameters that you can enter:

Parameter	Description
Modes of Run	Determine the type of data that you want the data profiling task to collect. Choose one of the following options: <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	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: <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.

Parameter	Description
Sampling Type	Determine the sample rows on which you want to run the data profiling task. Choose one of the following options: <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. • Random N Rows. Runs data quality on the selected number of random rows.
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 profiling.
No of random rows to limit	Required if you select Random N Rows in Sampling Type. Specify the number of random rows on which you want to run data profiling.
S3 Bucket Name	The path to the Amazon S3 bucket that is used to store staging data.
Maximum Precision of String Fields	The maximum precision value for profiles on string data type. You can set a maximum precision value of 255 characters. Default is 50.
Text Qualifier	The character that defines string boundaries. If you select a quote character, profiling ignores delimiters within the quotes. Select a qualifier from the list. Default is Double Quote.

- 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.
- In the **Parameters** area, configure 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.

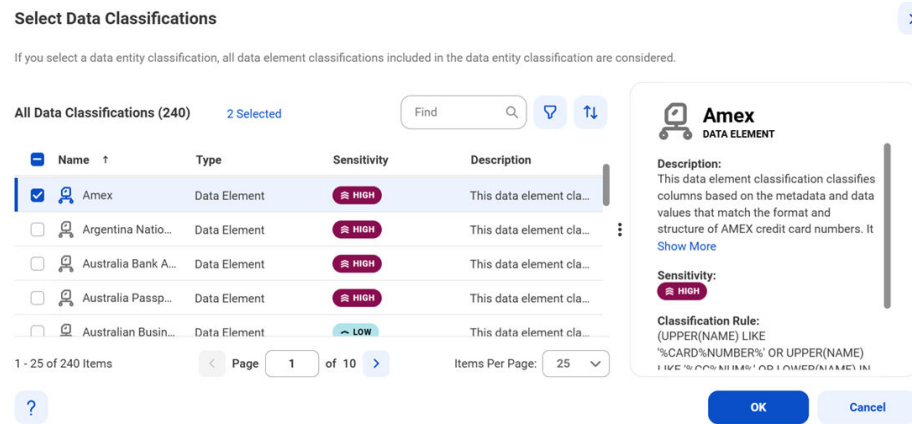
Parameter	Description
Data Quality Remediation	<p>Enable the option to specify a flat file connection to store the list of failed rows so that users can remediate poor data quality scores.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • No. Doesn't enable the Create Data Quality Failure Ticket option. • Yes. Shows a list of flat file connections where you write failed rows to customer-managed locations.
Data Quality Failure Ticket	<p>Specify whether you want to create data quality failure tickets for poor data quality scores based on the threshold defined for the rule occurrence in Data Governance and Catalog.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • No. Doesn't automatically create data quality failure tickets when the data quality scores are poor. • Yes. Automatically creates data quality failure tickets based on the data quality threshold values you define in Data Governance and Catalog, and notifies you when a data quality score is below the threshold. <p>Note: You must configure a workflow event for the data quality failure and enable the event in Metadata Command Center.</p>
Cache Result	<p>Specify how you want to preview 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.</p>
Run Rule Occurrence Frequency	<p>Specify whether you want to run data quality rules based on the frequency defined for the rule occurrence in Data Governance and Catalog.</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 quality on all rows in the metadata. • Limit N Rows. Runs data quality on a limited number of rows. • Random N Rows. Runs data quality on the selected number of random rows.
No of rows to limit	<p>Required if you select Limit N Rows in Sampling Type. Specify the number of rows on which you want to run data quality.</p>
No of random rows to limit	<p>Required if you select Random N Rows in Sampling Type. Specify the number of random rows on which you want to run data quality.</p>
S3 Bucket Name	<p>The path to the Amazon S3 bucket that is used to store staging data.</p>
Maximum Precision of String Fields	<p>The maximum precision value for profiles on string data type. You can set a maximum precision value of 255 characters. Default is 50.</p>
Text Qualifier	<p>The character that defines string boundaries. If you select a quote character, data quality ignores delimiters within the quotes. Select a qualifier from the list. Default is Double Quote.</p>

- 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 the data.

1. Click the **Data Classification** tab.
2. Select **Enable Data Classification**.
3. 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.
 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 20](#).
 - 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 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.

Add Users & User Groups

Users User Groups

All Users (1)

Find

<input type="checkbox"/>	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**.

Select Asset Groups

Asset Groups (2)

Find

Name	Description
<input type="checkbox"/> Asset_groups	
<input checked="" type="checkbox"/> Test Asset Group	

Selected Asset Groups (1)

Test Asset Group

OK Cancel

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 cloud service, such as Informatica Intelligent Cloud Services. 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. Select one or more objects from the endpoint catalog sources and click **Assign**.

You can connect to the following referenced source systems:

- Informatica Intelligent Cloud Services.
- dbt
- AWS Glue
- Informatica PowerCenter

The referenced catalog source must belong to the Database 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

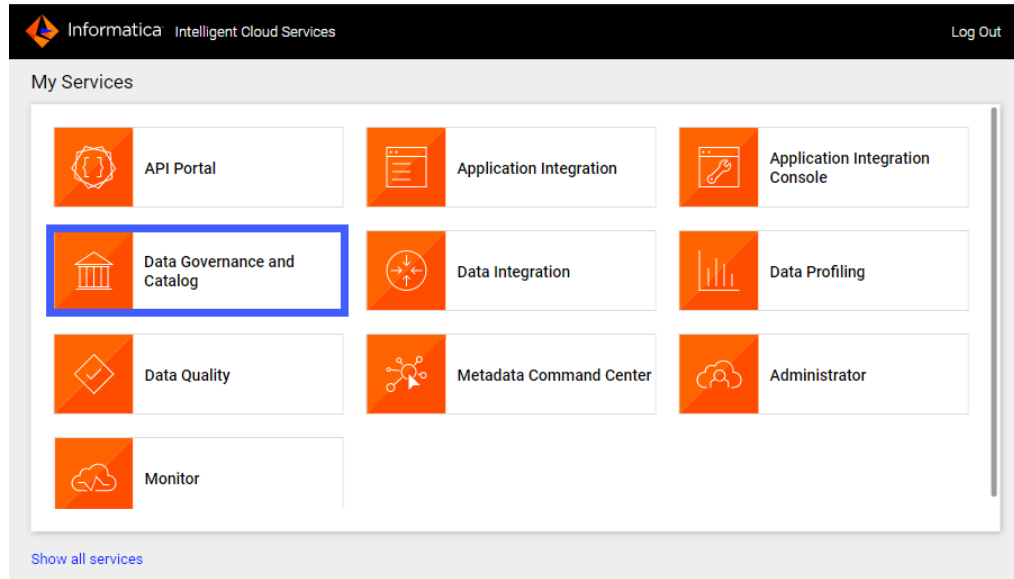
After a job runs in Metadata Command Center, view the results in Data Governance and Catalog. You can view details about source system contents in a hierarchical structure and trace data lineage.

1. Log in to Informatica Intelligent Cloud Services.

The **My Services** page appears.

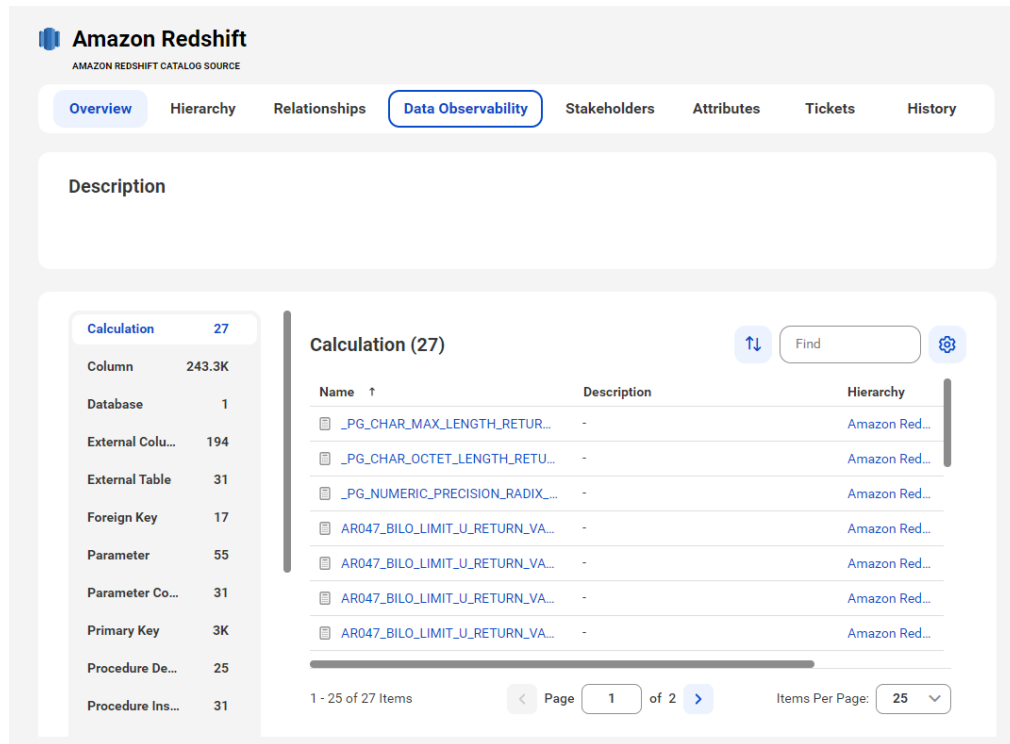
2. Click Data Governance and Catalog.

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 Amazon Redshift catalog source 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.

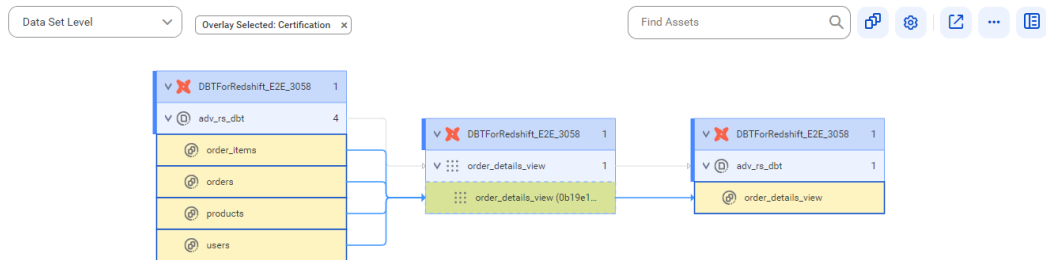
To view data lineage at the catalog source level, open a technical asset, click the **Lineage** tab, and then verify that the level is set to **Catalog Source Level**.

View lineage at the data set level

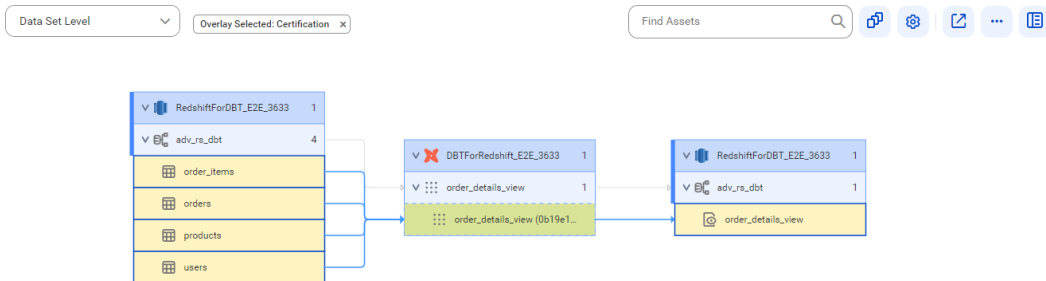
The data set level displays individual sets of data in the data flow.

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 data set level lineage where the order_details_view target reference data set gets data from the order_items, orders, products, and users source reference data sets using the order_details_view model instance before connection assignment:



The following image shows data set level lineage where the order_details_view target view gets data from the order_items, orders, products, and users source tables using the order_details_view model instance after connection assignment:



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

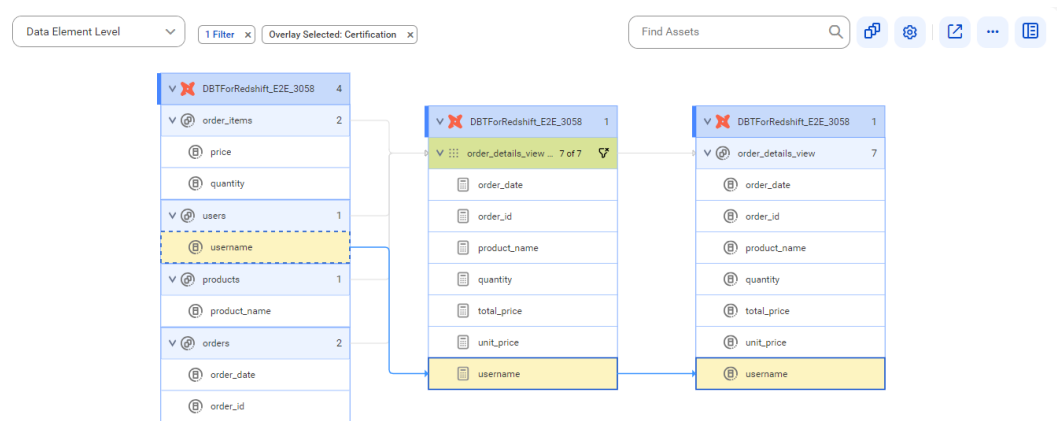
View lineage at the data element level

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.

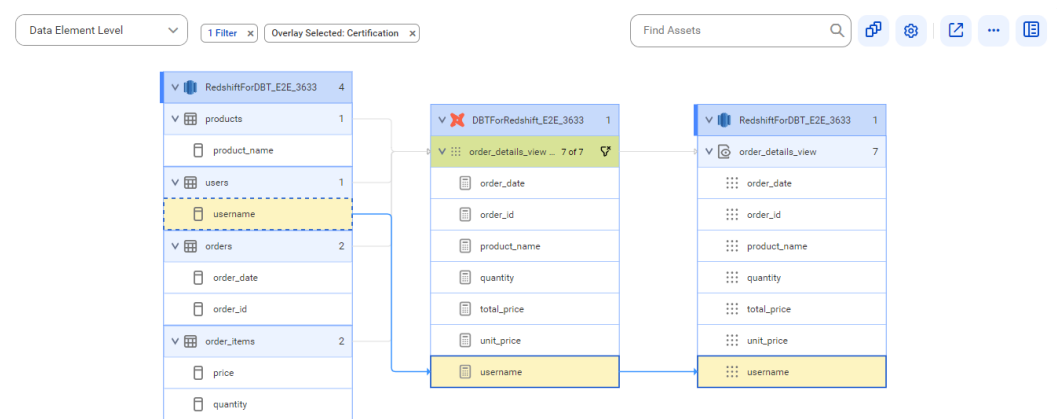
To view data lineage at the data element level, open a technical asset, click the **Lineage** tab, and then verify that the level is set to **Data Element Level**.

The following image shows data element level lineage where the username reference data element of the order_details_view reference data set gets data from the username reference data element of the users

reference data set using the username calculation of the order_details_view model instance before connection assignment:



The following image shows data element level lineage where the username view column of the order_details_view view gets data from the username column of the users table using the username calculation of the order_details_view model instance after connection assignment:



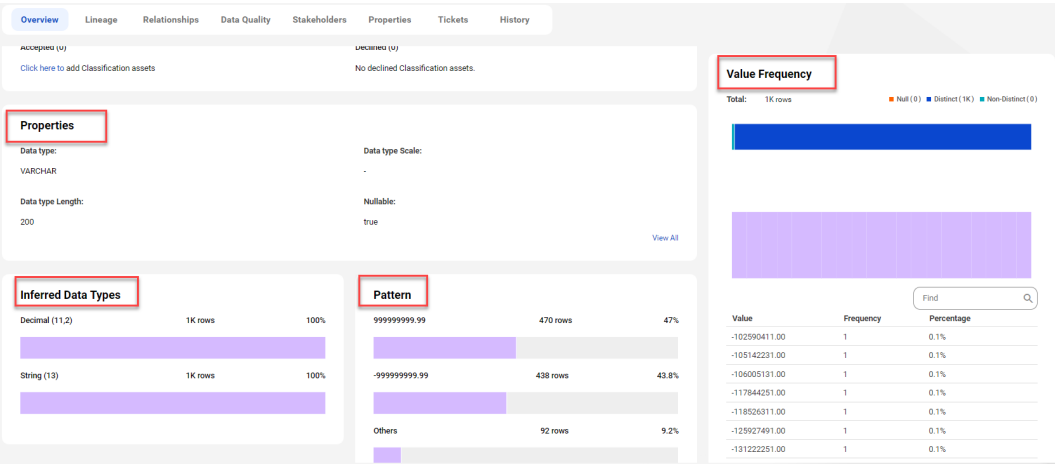
After connection assignment, the referenced object icons change to specific object icons.

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.

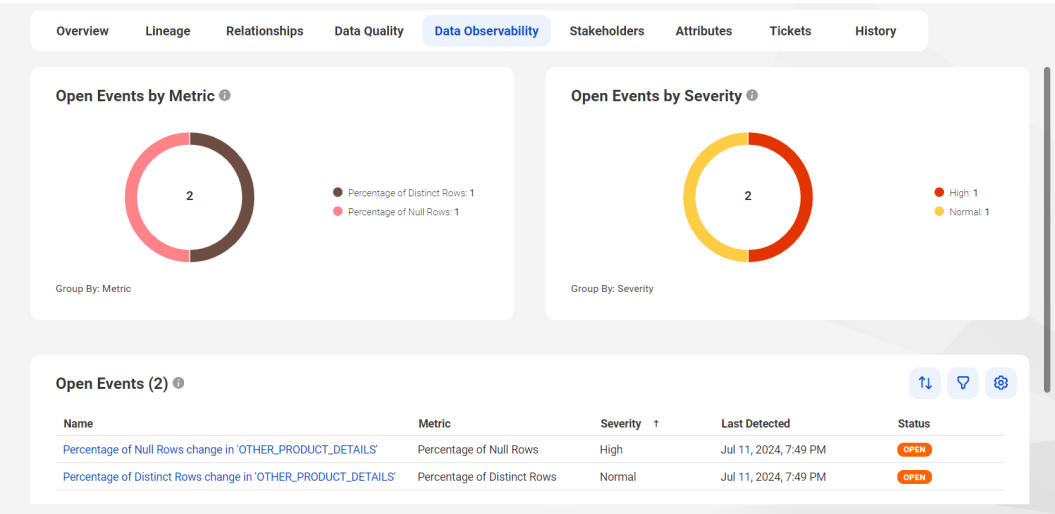
View data observability results

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:

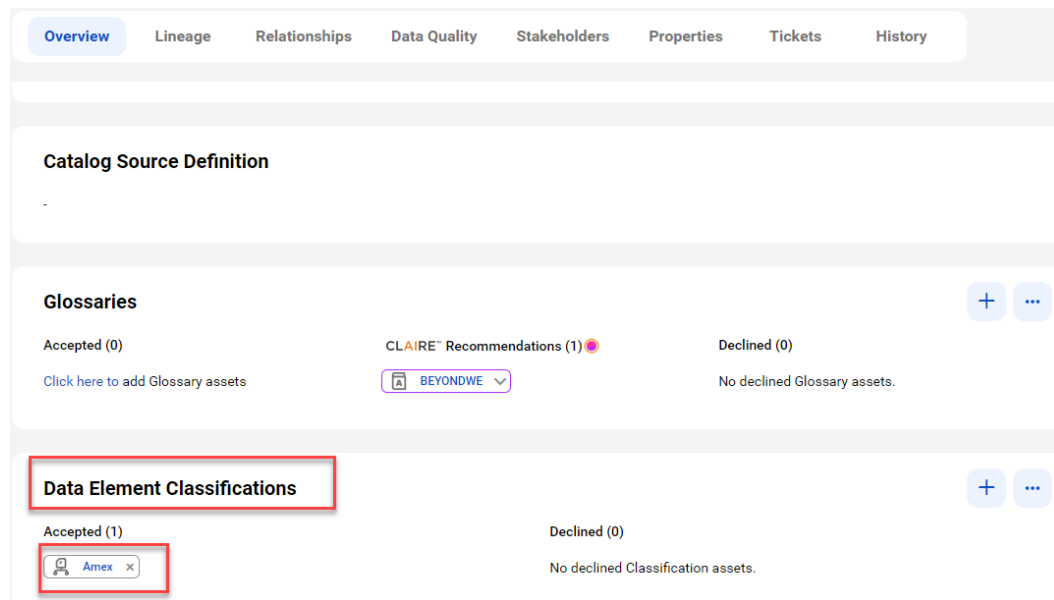


For more information about data observability results, see *Working With Assets* in the Data Governance and Catalog help.

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:

