



Informatica® Metadata Command Center  
November 2025

# Swagger API 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](mailto:infa_documentation@informatica.com).

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

Publication Date: 2025-11-20

# Table of Contents

- Preface. . . . . 4
- Chapter 1: Introduction to Swagger API sources..... 5**
  - Extraction and view process. . . . . 6
  - About the Swagger API catalog source. . . . . 6
  - Extracted metadata. . . . . 7
- Chapter 2: Before you begin..... 8**
  - Copy the required JSON files to the Secure Agent machine. . . . . 8
  - Verify permissions. . . . . 8
    - Permissions for metadata extraction. . . . . 8
- Chapter 3: Create catalog sources in Metadata Command Center..... 9**
  - Step 1. Register a catalog source. . . . . 9
  - Step 2. Configure capabilities. . . . . 10
    - Configure metadata extraction. . . . . 11
  - Step 3. Associate stakeholders and asset groups. . . . . 12
  - Step 4. Run or schedule the job. . . . . 13
- Chapter 4: View results in Data Governance and Catalog..... 15**
  - View metadata extraction results. . . . . 15
  - View relationships. . . . . 17

# Preface

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

## CHAPTER 1

# Introduction to Swagger API 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, Swagger API is a source system from which you can extract metadata through a Swagger API 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.

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 relationships, and creating links between those assets and their business context.

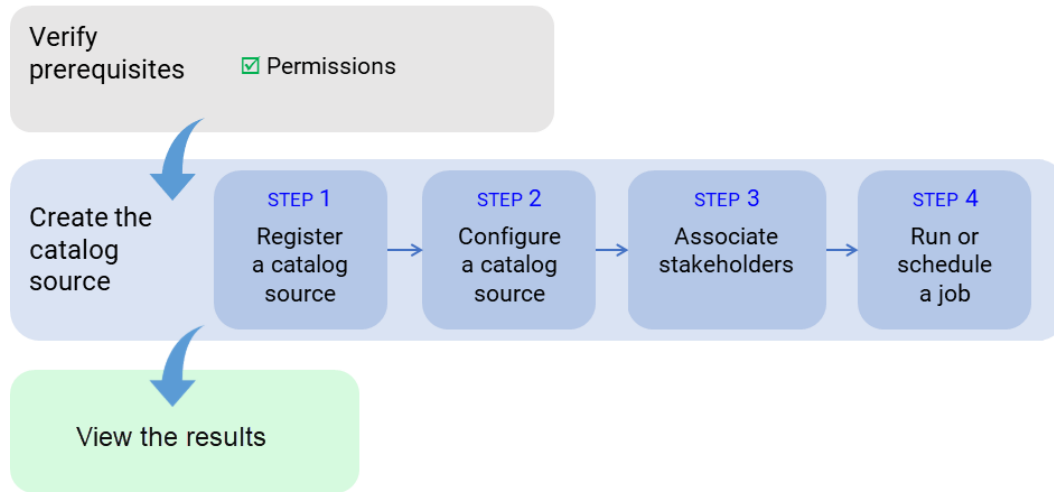
You can only extract metadata using this catalog source.

**Preview Notice:** Effective in the November 2025 release, the Swagger API catalog source 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.

# 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 Swagger API:

1. Register a catalog source. Create a catalog source object, select Swagger API, and specify values for connection properties.
2. Configure the catalog source. Specify the runtime environment, configure the metadata extraction capability, and add filters for metadata extraction.
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.

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

## About the Swagger API catalog source

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

Swagger API is a set of open-source tools built around the OpenAPI specification that help you design, build, document, and consume REST APIs.

The Swagger API catalog source works with version 3.x.x of the OpenAPI specification.

# Extracted metadata

You can extract specific metadata from a Swagger API source system with the Swagger API catalog source.

## Objects extracted

Metadata Command Center extracts the following metadata from a Swagger API source system:

- Operation
- Parameter
- Path
- Property
- RequestBody
- Response
- Schema
- Security
- SwaggerAPI
- Tag

## 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:

- Copy the JSON files to a directory on the Secure Agent machine.
- Verify permissions needed.

## Copy the required JSON files to the Secure Agent machine

The Swagger API catalog source extracts metadata by processing JSON files that conform to the OpenAPI specification. To process the files, the catalog source reads JSON content from the directory or file path that you specify when you configure the catalog source.

Perform the following tasks to ensure the Swagger API catalog source can access the JSON files:

1. Create or identify a directory on the Secure Agent machine.
2. Copy the JSON files to the directory.

When you configure the catalog source, you can specify the path to either a single JSON file or to a folder that contains multiple JSON files.

## Verify permissions

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

### Permissions for metadata extraction

To extract Swagger API metadata, you must assign specific access permissions.

The directory and the JSON files on the Secure Agent machine must have Read access permission enabled.



## CHAPTER 3

# Create catalog sources in Metadata Command Center

Use Metadata Command Center to configure a catalog source for Swagger API and extract metadata.

When you configure a catalog source, you define the source system where you want to extract metadata from. Optionally, 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 stakeholder roles. You can also associate technical assets extracted from the catalog source to asset groups.

## Step 1. Register a catalog source

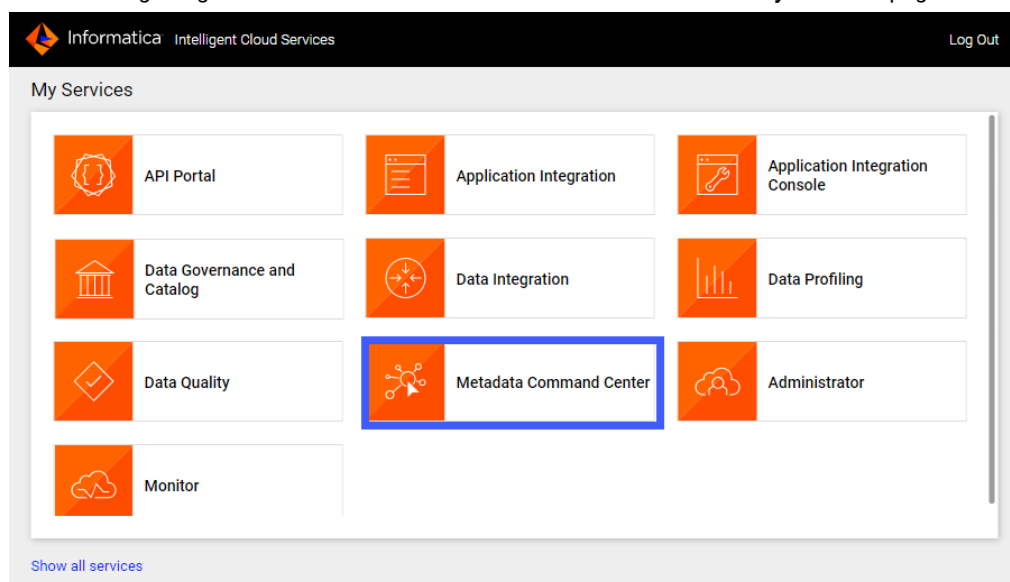
When you register a catalog source, provide general information and connection values.

1. Log in to Informatica Intelligent Cloud Services.

The **My Services** page appears.

2. Click **Metadata Command Center**.

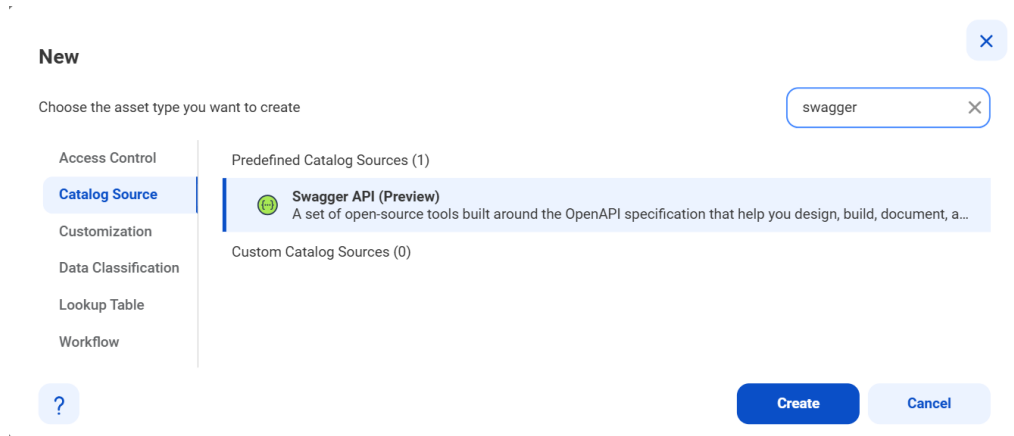
The following image shows the Metadata Command Center box on the **My Services** page:



The Metadata Command Center home page appears.

3. Click **New**.
4. Select **Catalog Source** from the list of asset types.
5. Select Swagger API from the list of catalog source types.
6. Click **Create**.

The following image shows the Swagger API catalog source type:



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, enter the path to the JSON file or directory that you created on the Secure Agent machine.
9. Click **Next**.

The **Configuration** page appears.

## Step 2. Configure capabilities

When you configure the Swagger API catalog source, you define the settings for the metadata extraction capability.

The metadata extraction capability extracts source metadata from external source systems.

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 Swagger API 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 filters for metadata extraction:

- 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. In the value field, enter the title attribute value.

Filter values can contain wildcards. Use a question mark to represent a single character and an asterisk to represent multiple characters.

For example: `*Data` includes or excludes metadata from all JSON files with title attribute values that end with 'Data.'

The following image shows the filter condition options with a sample filter value entered:

Specify metadata filters: ☐ No ☒ Yes

[Show supported wildcards and examples](#)

Include or exclude ...	Swagger API Title	*Data	+	🗑️
------------------------	-------------------	-------	---	----

To include or exclude multiple objects, click the **Add** icon to add filters with the OR condition.

4. Optional. In the **Configuration Parameters** area, enter expert parameters.

Click **Show Advanced** to view expert parameters.

**Note:** Use expert parameters when it is recommended by Informatica Global Customer Support.

5. 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

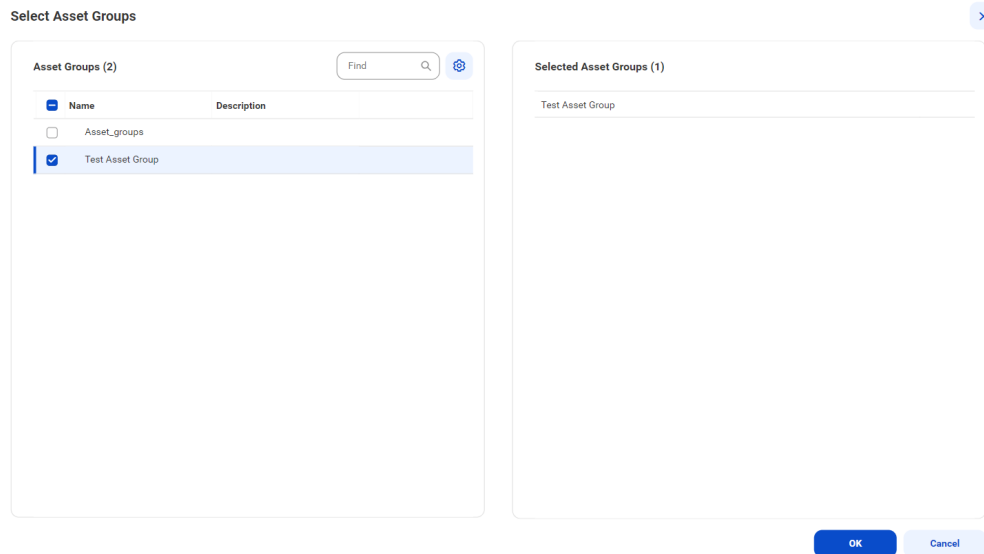
? OK Cancel

- 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**.



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*.

## 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 the catalog source and the included technical assets in a hierarchical structure.

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 relationship information of an asset in a catalog source to see individual elements such as data sources, calculations, and filters. When you view the relationship information of an asset, you can see how the assets relate to one another.

## View metadata extraction results

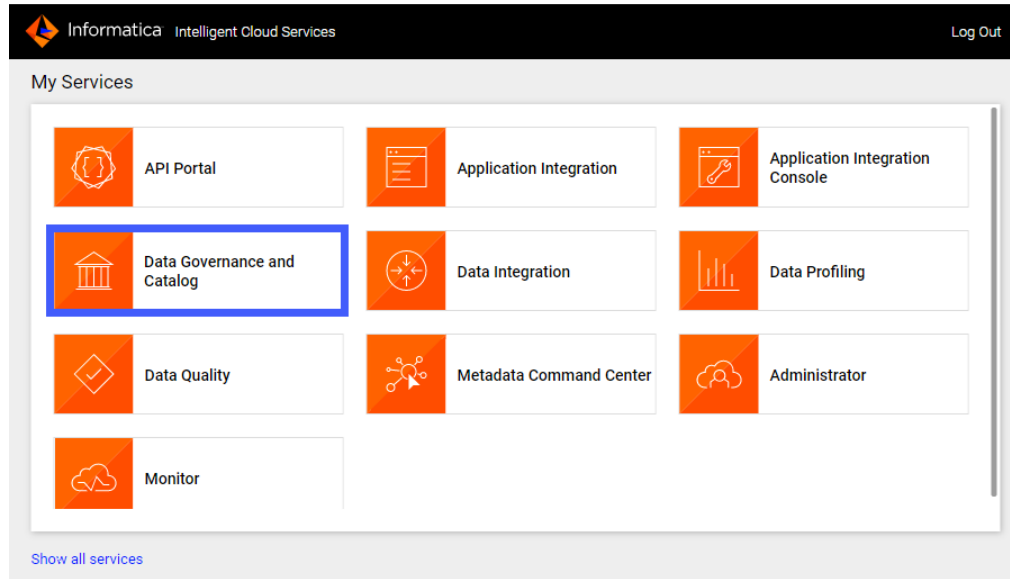
After a job runs in Metadata Command Center, view the results in Data Governance and Catalog. You can view details about source system contents in a hierarchical structure..

1. Log in to Informatica Intelligent Cloud Services.

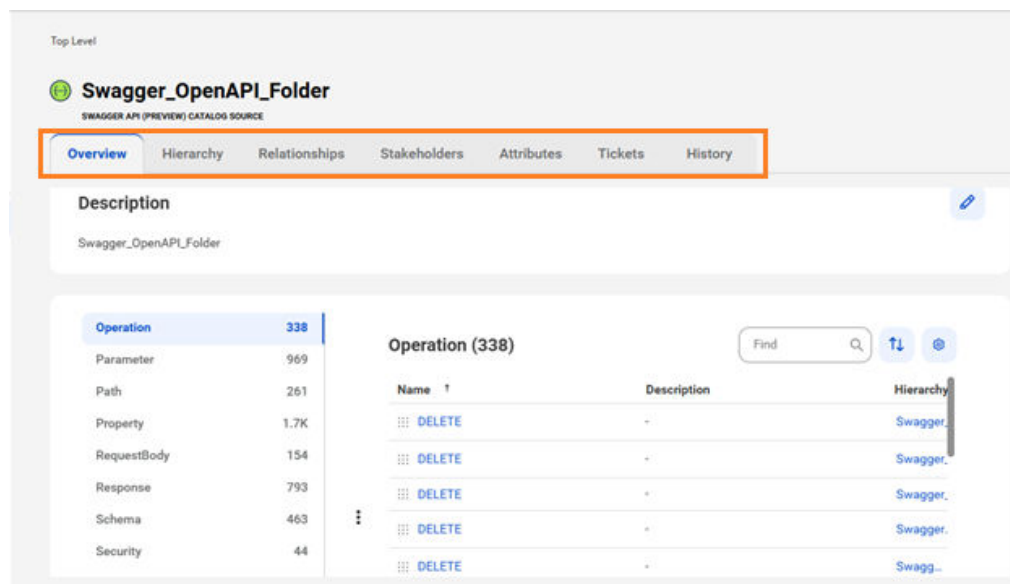
The **My Services** page appears.

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 that you extracted metadata from, and click the name. The **Overview** tab of the asset opens. The following image shows a sample asset page:



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



# View relationships

Relationship views are available for technical assets in the catalog source. You can connect assets to each other using different types of relationships.

A relationship between assets shows how the assets relate to one another. When data from a source system is ingested into the catalog, Data Governance and Catalog can automatically create relationships among the technical assets of that source system.

For more information about viewing relationships, see *Relationships* in the Data Governance and Catalog help.