



Informatica® Metadata Command Center  
November 2025

# Catalog Source Configuration

© Copyright Informatica LLC 2021, 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: 2025-12-19

# Table of Contents

Preface. . . . .	9
<b>Chapter 1: Working with catalog sources. . . . .</b>	<b>10</b>
Creating a catalog source. . . . .	10
Step 1. Register a catalog source. . . . .	11
Step 2. Configure a catalog source. . . . .	12
Step 3. Associate stakeholders and asset groups. . . . .	16
Step 4. Schedule a job. . . . .	18
Step 5. Run the catalog source job. . . . .	19
Managing catalog sources. . . . .	20
Cloning a catalog source configuration. . . . .	20
Managing configuration permissions for catalog sources. . . . .	20
Curating CLAIRE recommendations. . . . .	23
Deleting or purging a catalog source. . . . .	23
Purging obsolete objects from a catalog source. . . . .	24
Referenced catalog sources. . . . .	24
Assign connections to reference catalog sources. . . . .	25
<b>Chapter 2: Source systems. . . . .</b>	<b>26</b>
<b>Chapter 3: Amazon Athena. . . . .</b>	<b>75</b>
<b>Chapter 4: Amazon Redshift. . . . .</b>	<b>78</b>
<b>Chapter 5: Amazon S3. . . . .</b>	<b>79</b>
<b>Chapter 6: Apache Atlas. . . . .</b>	<b>80</b>
<b>Chapter 7: Apache Hive. . . . .</b>	<b>81</b>
<b>Chapter 8: Apache HiveQL Script. . . . .</b>	<b>82</b>
<b>Chapter 9: AWS Glue. . . . .</b>	<b>83</b>
<b>Chapter 10: Databricks. . . . .</b>	<b>84</b>
<b>Chapter 11: dbt. . . . .</b>	<b>85</b>
<b>Chapter 12: Denodo. . . . .</b>	<b>86</b>
<b>Chapter 13: erwin Data Modeler File. . . . .</b>	<b>87</b>

<b>Chapter 14: erwin Mart Server.....</b>	<b>88</b>
<b>Chapter 15: File System.....</b>	<b>89</b>
<b>Chapter 16: Fivetran Platform.....</b>	<b>90</b>
<b>Chapter 17: Google BigQuery.....</b>	<b>91</b>
<b>Chapter 18: Google BigQuery SQL Script.....</b>	<b>92</b>
<b>Chapter 19: Google Cloud Storage .....</b>	<b>93</b>
<b>Chapter 20: Google Looker.....</b>	<b>94</b>
<b>Chapter 21: Google Vertex AI.....</b>	<b>95</b>
<b>Chapter 22: Greenplum.....</b>	<b>96</b>
<b>Chapter 23: Hadoop Distributed File System.....</b>	<b>97</b>
<b>Chapter 24: IBM Cognos.....</b>	<b>98</b>
<b>Chapter 25: IBM Db2 for LUW.....</b>	<b>99</b>
<b>Chapter 26: IBM Db2 for LUW Script.....</b>	<b>103</b>
<b>Chapter 27: IBM Db2 for z/OS.....</b>	<b>104</b>
<b>Chapter 28: IBM InfoSphere DataStage.....</b>	<b>105</b>
<b>Chapter 29: IBM Mainframe Job Control Language (Accelerator).....</b>	<b>106</b>
Introduction to IBM Mainframe Job Control Language (Accelerator). . . . .	106
<b>Chapter 30: IBM Netezza.....</b>	<b>108</b>
<b>Chapter 31: IDERA ER/Studio Data Architect.....</b>	<b>109</b>
<b>Chapter 32: Informatica Developer.....</b>	<b>110</b>
<b>Chapter 33: Informatica Intelligent Cloud Services.....</b>	<b>111</b>
<b>Chapter 34: Informatica PowerCenter.....</b>	<b>112</b>
<b>Chapter 35: JDBC.....</b>	<b>115</b>

<b>Chapter 36: Kafka.....</b>	<b>120</b>
<b>Chapter 37: MariaDB.....</b>	<b>123</b>
<b>Chapter 38: Microsoft Azure Analysis Services.....</b>	<b>124</b>
<b>Chapter 39: Microsoft Azure Blob Storage.....</b>	<b>125</b>
<b>Chapter 40: Microsoft Azure Data Factory.....</b>	<b>126</b>
<b>Chapter 41: Microsoft Azure Data Lake Storage Gen2.....</b>	<b>127</b>
<b>Chapter 42: Microsoft Azure SQL Server.....</b>	<b>128</b>
<b>Chapter 43: Microsoft Azure SQL Server Script.....</b>	<b>129</b>
<b>Chapter 44: Microsoft Azure Synapse Analytics.....</b>	<b>130</b>
<b>Chapter 45: Microsoft Azure Synapse Data Warehouse.....</b>	<b>131</b>
<b>Chapter 46: Microsoft Azure Synapse Data Warehouse Script.....</b>	<b>141</b>
<b>Chapter 47: Microsoft Fabric Data Warehouse .....</b>	<b>142</b>
<b>Chapter 48: Microsoft Fabric Data Lakehouse.....</b>	<b>143</b>
<b>Chapter 49: Microsoft Fabric OneLake.....</b>	<b>144</b>
<b>Chapter 50: Microsoft OneDrive.....</b>	<b>145</b>
<b>Chapter 51: Microsoft Power BI.....</b>	<b>146</b>
<b>Chapter 52: Microsoft Purview.....</b>	<b>147</b>
<b>Chapter 53: Microsoft SharePoint Online.....</b>	<b>148</b>
<b>Chapter 54: Microsoft SQL Server.....</b>	<b>149</b>
<b>Chapter 55: Microsoft SQL Server Analysis Services.....</b>	<b>150</b>
<b>Chapter 56: Microsoft SQL Server Integration Services.....</b>	<b>151</b>
<b>Chapter 57: Microsoft SQL Server Reporting Services.....</b>	<b>155</b>
<b>Chapter 58: Microsoft SQL Server Script.....</b>	<b>158</b>

<b>Chapter 59: MicroStrategy.....</b>	<b>159</b>
<b>Chapter 60: MySQL.....</b>	<b>160</b>
<b>Chapter 61: Oracle.....</b>	<b>163</b>
<b>Chapter 62: Oracle Business Intelligence.....</b>	<b>164</b>
<b>Chapter 63: Oracle Cloud Infrastructure GoldenGate.....</b>	<b>165</b>
<b>Chapter 64: Oracle Cloud Object Storage.....</b>	<b>166</b>
<b>Chapter 65: Oracle Data Integrator.....</b>	<b>167</b>
<b>Chapter 66: Oracle PL/SQL Script.....</b>	<b>168</b>
<b>Chapter 67: Oracle SQL Loader.....</b>	<b>169</b>
<b>Chapter 68: PostgreSQL.....</b>	<b>170</b>
<b>Chapter 69: Qlik Sense.....</b>	<b>175</b>
<b>Chapter 70: Qlik Sense Cloud.....</b>	<b>180</b>
<b>Chapter 71: QlikView.....</b>	<b>181</b>
<b>Chapter 72: Salesforce.....</b>	<b>184</b>
<b>Chapter 73: SAP Analytics Cloud - Preview catalog source.....</b>	<b>190</b>
<b>Chapter 74: SAP BusinessObjects.....</b>	<b>191</b>
<b>Chapter 75: SAP BusinessObjects Data Services.....</b>	<b>196</b>
<b>Chapter 76: SAP Business Warehouse (SAP BW).....</b>	<b>197</b>
<b>Chapter 77: SAP BW/4HANA.....</b>	<b>205</b>
<b>Chapter 78: SAP Datasphere - Preview catalog source.....</b>	<b>216</b>
<b>Chapter 79: SAP ERP.....</b>	<b>217</b>
<b>Chapter 80: SAP HANA Database.....</b>	<b>227</b>
<b>Chapter 81: SAP PowerDesigner.....</b>	<b>230</b>

<b>Chapter 82: SAP Sales &amp; Service Cloud.....</b>	<b>231</b>
<b>Chapter 83: SAP S/4HANA Cloud - Preview catalog source.....</b>	<b>232</b>
<b>Chapter 84: SAP SuccessFactors.....</b>	<b>233</b>
<b>Chapter 85: SAS Base Libraries (Accelerator).....</b>	<b>234</b>
Introduction to SAS Base Libraries (Accelerator) sources. . . . .	234
<b>Chapter 86: SAS Base Programs (Accelerator).....</b>	<b>235</b>
<b>Chapter 87: SFTP File System.....</b>	<b>236</b>
<b>Chapter 88: Snowflake.....</b>	<b>237</b>
<b>Chapter 89: Snowflake SQL Script.....</b>	<b>238</b>
<b>Chapter 90: Strategy Cloud.....</b>	<b>239</b>
<b>Chapter 91: Swagger API - Preview catalog source.....</b>	<b>240</b>
<b>Chapter 92: Tableau.....</b>	<b>241</b>
<b>Chapter 93: Talend Data Integration.....</b>	<b>244</b>
<b>Chapter 94: Teradata BTEQ Script.....</b>	<b>245</b>
<b>Chapter 95: Teradata Database.....</b>	<b>246</b>
<b>Chapter 96: Teradata FastExport Script.....</b>	<b>249</b>
<b>Chapter 97: Teradata FastLoad Script.....</b>	<b>250</b>
<b>Chapter 98: Teradata MultiLoad Script.....</b>	<b>251</b>
<b>Chapter 99: TIBCO Spotfire.....</b>	<b>252</b>
<b>Chapter 100: Workday.....</b>	<b>253</b>
<b>Chapter 101: Custom metadata integration.....</b>	<b>254</b>
Workflow for custom metadata integration. . . . .	255
Step 1. Create a custom model. . . . .	255
Step 2. Update the custom model definition file. . . . .	256
Step 3. Import and publish the custom model. . . . .	261
Step 4. Create a custom catalog source type. . . . .	262

Step 5. Prepare the custom metadata source. . . . .	263
Step 6. Create the custom catalog source. . . . .	267
Step 7. Run the custom catalog source. . . . .	269
Example: Ingest metadata from Microsoft Access database. . . . .	270
Define the custom model. . . . .	270
Update the metadata definition files. . . . .	279
Create custom lineage. . . . .	280



# Preface

Refer to *Catalog Source Configuration* to learn how to configure various catalog sources in Metadata Command Center. Learn about the connection properties, the tasks that you can run on the catalog source, and the required permissions and prerequisites for the various catalog sources.

# CHAPTER 1

## Working with catalog sources

A catalog source is an object that represents the source system from which you can extract metadata and data facts. Amazon S3 and Oracle are examples of catalog source systems. You can create multiple instances of catalog sources for each catalog source type.

At the least, you can perform metadata extraction on a catalog source. You can also perform operations such as data profiling, data classification, relationship discovery, and glossary association on the extracted metadata and data facts. To fine-tune the data, you can apply some filters to exclude certain objects from the run or set a schedule to extract metadata at predefined intervals. You can also assign users, user groups, or roles to catalog sources to grant permissions to manage or update the catalog sources.

Data Governance and Catalog displays the extracted metadata, data facts, and the results of any other capability that was performed on the source.

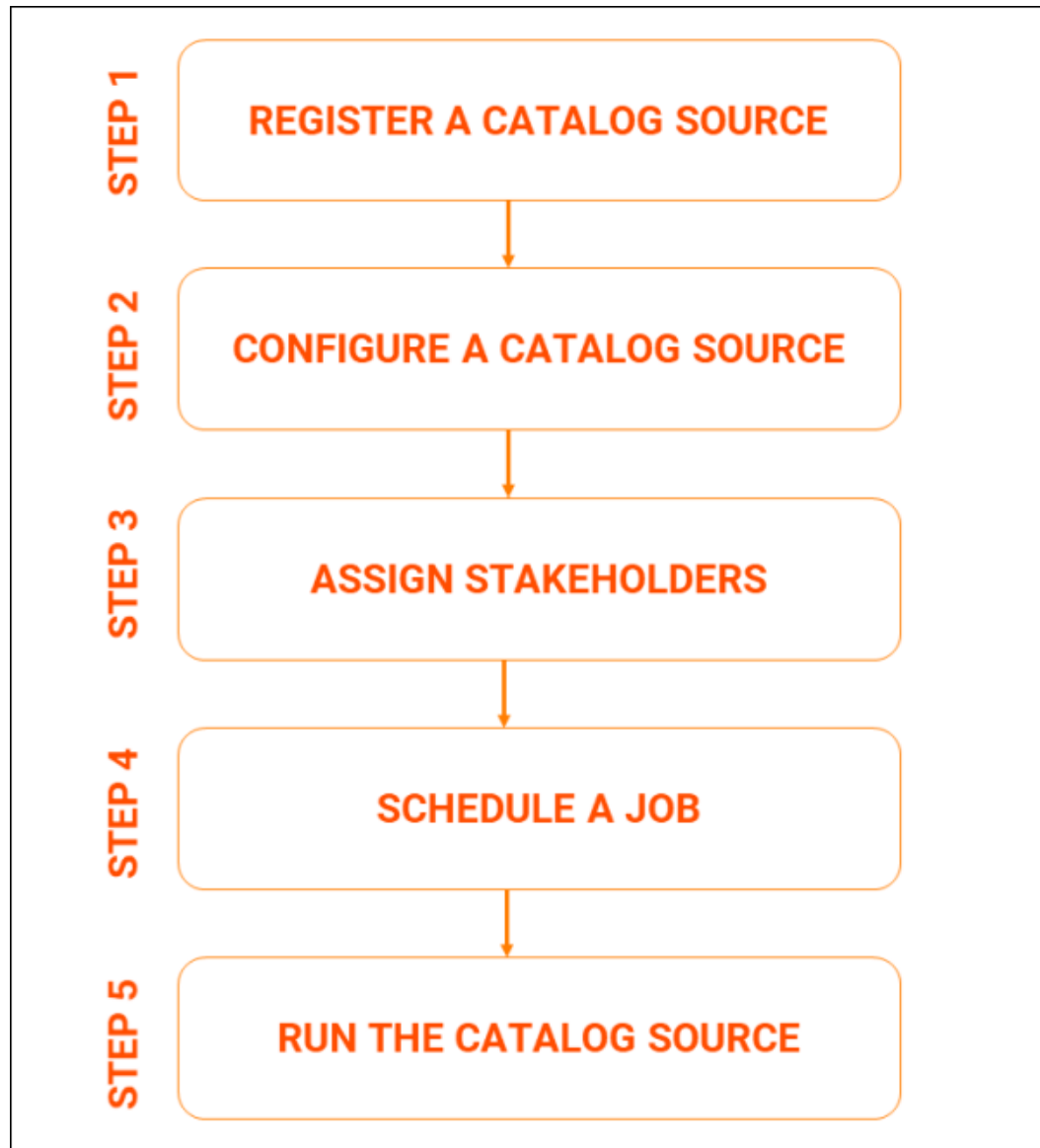
## Creating a catalog source

When you configure a catalog source, you can specify the catalog source type, perform any additional capability on the extracted metadata, and optionally specify a schedule to run your catalog source.

Before you create a catalog source in Metadata Command Center, perform the following tasks:

1. Set up a runtime environment for your organization. For information about runtime environments, see *Runtime Environments* in the Administrator help.
2. Configure a connection to your catalog source. For more information about configuring a connection, see *Connections* in the Cloud Common Services help.

After you perform the tasks, you are ready to create your first catalog source. The following image shows the steps involved in the catalog source creation process:



**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.

## Step 1. Register a catalog source

To add a catalog source to Metadata Command Center, first register the catalog service on the **Registration** page.

1. Log in to Informatica Intelligent Cloud Services and select Metadata Command Center from the My Services page.
2. Click **New**.
3. Select a source from the list of predefined source systems. For information about predefined source systems available in Metadata Command Center, see [Chapter 2, "Source systems" on page 26](#).

4. Click **Create**.
5. In the **Registration** page, enter a name and an optional description for the catalog source. The maximum allowed length for the description is 4000 characters  
**Note:** 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.
6. In the **Connection Information** area, select a connection for the catalog source from the **Connection** list. The list contains all the connections in Administrator that you have access to.  

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.

You can expand and view the connection properties for the selected connection. The connection properties differ for each catalog source type.
7. Click **Test Connection** to test your connection to the source system.  
**Note:** The **Test Connection** function is available only for some catalog sources.
8. Click **Next** to move to the **Configuration** page.

## Step 2. Configure a catalog source

Configure metadata extraction and profiling options for the catalog source.

1. On the **Configuration** page, select one or more capabilities that you want to perform on the catalog source.

The following table describes the capabilities of the catalog source:

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

Capability	Description
Data Classification	Data classification is the process of identifying and organizing data into relevant categories based on the functional meaning of the data. Classifying data can help your organization manage risks, compliance, and data security.
Relationship Discovery	The relationship discovery capability identifies pairs of similar columns and relationships between tables within a catalog source.
Glossary Association	You can associate terms that are in the glossary with technical assets to provide user-friendly business names to technical assets. Glossary Association automatically associates glossary terms with technical assets or recommends glossary terms that you can manually associate with technical assets in Data Governance and Catalog.

2. On the **Metadata Extraction** tab, select any runtime environment that is available in Informatica Intelligent Cloud Services to run the metadata extraction task.

A runtime environment is either Informatica Cloud Secure Agent or a serverless runtime environment.

3. 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.

4. You can add filter conditions to extract metadata from a specific set of objects in the source system. In the **Filters** section, select **Filter Conditions** to add filters.

The system extracts the source metadata based on the object types and conditions specified in this page.

- a. From the first list, choose to include or exclude specific metadata in an extraction run.
- b. From the second list, you can choose the type of object from which you want to include or exclude metadata.  
  
The object type can be a table, view, schema, path, file or folder depending on the catalog source type that you configure.
- c. From the third list, choose the filter condition based on the object type that you have selected.  
  
You can choose to specify the name or pattern of the path to an object that you want to include or exclude.

- d. Click **Select** to enter one or more values for the specified object type that you want to include or exclude from the extraction run.

**Note:** The Select option appears depending on the catalog source type that you configure.

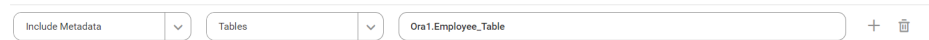
The values that you enter differ based on the catalog source types. The following table shows the different values that you can enter for different catalog source types:

Catalog Source Type	Values
Relational database-based catalog sources, such as Oracle and Azure SQL Server	Full names of tables, schemas, or views. You can use wildcard characters in the name.
ETL catalog sources, such as Azure Data Factory	Fully qualified paths to the objects. You can use wildcard characters in the pattern.
File system-based catalog sources, such as Amazon S3 and Azure Data Lake Storage	Full names of files or folders. You can use wildcard characters in the name.


- e. You can add multiple filter conditions for each catalog source to include and exclude specific metadata from the source systems. To add more filters, click the Add icon.

The following images are a few examples of filters:

- The following filter extracts metadata from a table named `Employee_Table` that belongs to the `Oral` schema in an Oracle source system:



- The following filter excludes metadata from an activity named `Activity1` located at `AzureDatafactoryName/dev_pipeline/Activity1` in a Microsoft Azure Data Factory source system:



**Note:** For File System catalog sources, if you add multiple filters with different wildcard usage for the same object type, only the last wildcard condition is considered.

Some catalog sources have additional parameters that you can configure on this tab.

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

5. On the **Lineage Discovery** tab, enable the capability to build the complete lineage of a catalog source by recommending endpoint catalog source objects to assign to reference catalog source connections.

Optionally, you can add filters to include or exclude catalog sources for lineage discovery based on filter parameters such as catalog source types, catalog source names, and asset groups.

**Note:** The **Lineage Discovery** tab appears if it is available for the catalog source.

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

6. On the **Data Profiling and Quality** tab, enable the capabilities and enter values to determine the type of data that you want the data profiling and quality task to collect, the scope of the data profile and quality run, and the sample rows on which you want to run the data profiling and quality task.

Optionally, you can add filters conditions to create subsets of metadata that you can use to run a data profiling task on a catalog source.

For more information about data profiling and data quality configuration options, see the Metadata Command Center *Administration* help.

7. On the **Data Classification** tab, enable the capability and select one or both of the following options:

Option	Description
<b>Generated Data Classifications</b>	A CLAIRE powered solution. The system automatically generates data classifications for the data elements in the catalog.
<b>Data Classification Rules</b>	Choose from predefined or custom data classifications. Click <b>Add Data Classification</b> and select the data element classification that you want to apply to the catalog source. <b>Note:</b> Data classifications that you create using the <b>New &gt; Data Classification</b> menu appear in this list.

For more information about creating data classifications, see the *Administrator* help.

8. On the **Relationship Discovery** tab, enable the capability and enter values for the following properties to determine column similarity and joinable table relationships:

The following table describes the properties:

Property	Description
Relationship Inference Model	Select the predefined relationship inference model that Metadata Command Center provides for discovering column similarity relationships within the catalog source. You can also choose a relationship inference model that you have imported.
Containment Score Threshold	Specify a score from 0 to 1 inclusive to identify joinable table relationships within the catalog source. This score is an indicator of the data overlap between the two given columns which determines whether the tables are joinable. A higher score means more similarity of data and a greater probability of the tables being joinable.

For more information about relationship discovery, see the *Administrator* help.

9. On the **Glossary Association** tab, enable the capability and configure settings for a catalog source to automatically associate or recommend glossary terms as business names for data elements in technical assets.

The following table describes the settings for a catalog source:

Property	Description
Enable auto-acceptance	When enabled, this option automatically associates glossary terms with data elements based on the threshold limit that you specify. The automatically accepted glossary terms appear as business names of data elements in Data Governance and Catalog.
Confidence Score Threshold for Auto-Acceptance	Specify a percentage from 80 to 100 inclusive to set a threshold limit. If a glossary term matches a data asset within the threshold specified, Metadata Command Center automatically assigns the matching glossary term to the data element. The name and description of the glossary term with the highest confidence score appears as the name and description of the data element asset in Data Governance and Catalog.

Property	Description
Enable below-threshold recommendations	If you enable auto-acceptance, you can select this option to receive glossary association recommendations below the auto-acceptance threshold.
Confidence score threshold for recommendations	If you enable auto-acceptance, specify a percentage between 80% and the selected confidence score threshold for auto-acceptance. If you disable auto-acceptance, specify a percentage between 80% and 100%.
Assign business names and descriptions	Choose to automatically assign business names and descriptions to technical assets.
Keep existing business names and descriptions	Applicable if you choose to assign business names and descriptions. 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.
Ignore Keywords	Choose to ignore specific parts of data elements when making recommendations. You can enter multiple unique prefix and suffix keywords. Keyword values are case insensitive.
Glossary Association Scope	Choose specific top-level business glossary assets to associate with technical assets. Selecting a top-level asset selects its child assets as well.
Use Abbreviation and Synonym Definitions	Enable this option to use a lookup table with abbreviations and synonyms to improve glossary association accuracy. To upload a lookup synonym file with the abbreviations and synonyms, select <b>Yes</b> to enable, and then click <b>Select</b> .

For more information about the glossary association settings, see the *Administrator* help.

- Click **Next** to move to the **Associations** step.

## 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.

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

- On the **Associations** page, click **Stakeholders**.
- Select **Assign Stakeholders**.
- Select a stakeholder role.
- 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. Schedule a job

Select a schedule to indicate how often you want to run the catalog source job.

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.

1. On the **Schedule** tab, select **Run on schedule** to enter a schedule for each capability that you configured for the catalog source.

The schedule determines the frequency at which the metadata extraction and other configured capabilities run for the catalog source that you create.

2. Click the checkbox corresponding to each capability that you want to include in the schedule.

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. 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 complete 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.
3. Enter the start date, time zone, and the interval at which you want to run the catalog source job.  
You can also specify options for the job to repeat daily, weekly, indefinitely, or repeat until a specified time.
  4. You can manage additional schedules using the following options:
    - a. To create a new schedule, click the **Add** button.
    - b. To delete a schedule, click the **Delete** button.
    - c. 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.

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

If you click **Run**, the catalog source job is immediately triggered.

**Note:** If the first run of the catalog source must happen on the schedule, then you need to save the catalog source and close the page.

## Step 5. Run the catalog source job

After you save the configuration details, you can run the catalog source job.

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.

1. Click **Run**.

The **Run Catalog Source Job** dialog box appears.

**Note:** If you created a schedule for the catalog source and the first run of the catalog source must happen based on the schedule, then you need not run the catalog source.

2. In the **Scope of Run** section, select or clear the capabilities that you want to include or exclude for the catalog source 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 to perform a full or an incremental metadata extraction. The incremental extraction option appears if it is available for the catalog source. 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.

3. Click **Run**.

A job is triggered to run the catalog source. You can monitor the status of the job on the **Overview** page.

**Note:** You can't trigger more than one run at a time on a catalog source simultaneously. If a job for a catalog source is in progress, wait for the existing job to complete or cancel the ongoing job before you trigger a new job.

4. Optionally, you can run your catalog source job from the **Explore** page by selecting **Run** from the Action menu for the newly created catalog source.

## Managing catalog sources

You can update, copy, delete, purge, and run a catalog source. You can also grant configuration permissions for catalog sources to different roles in your organization.

On the **Catalog Sources** page of the **Explore** page, you can select a catalog source to see its overview and related catalog sources. The **Overview** tab displays the capabilities, filters, stakeholders, asset groups, and schedules enabled for a catalog source. The **Related Catalog Sources** tab displays a list of related catalog sources that are either assigned manually using connection assignment or are curated based on CLAIRE recommendations using the lineage discovery capability. You can view related catalog sources and accept or reject CLAIRE recommendations for catalog sources that are run with the lineage discovery capability.

### Cloning a catalog source configuration

You can clone the configuration of a catalog source to create another catalog source with the same configuration.

**Note:** Cloning doesn't copy the content of the catalog source.

1. In Metadata Command Center, go to the **Explore** page.
2. Select **Catalog Sources** from the menu.
3. You can clone a catalog source in one of the following ways:
  - Hover your mouse over the catalog source that you want to clone and click **Clone** from the **Action** menu.
  - Open the catalog source that you want to clone and click **Clone**.

**Note:** By default, the cloned catalog source has the same name suffixed with **\_Clone**. You can change the name if needed.

4. If needed, modify the configuration of the catalog source by updating the parameters on each tab.

Cloning doesn't copy the content of sensitive fields. If the catalog source contains sensitive fields such as Client Secret, enter the values.

5. Click **Save**.

### Managing configuration permissions for catalog sources

As a service administrator, you can grant configuration permissions for catalog sources to different roles in your organization, and add specific users and user groups to those roles so that they can perform operational activities on a catalog source.

To manage permissions for catalog source configuration, verify that at least one role has the catalog source configuration **Set Permissions** functionality enabled for Metadata Command Center in Administrator. In Administrator, create the required roles, assign users and user groups to the roles, and specify appropriate permissions to the roles.

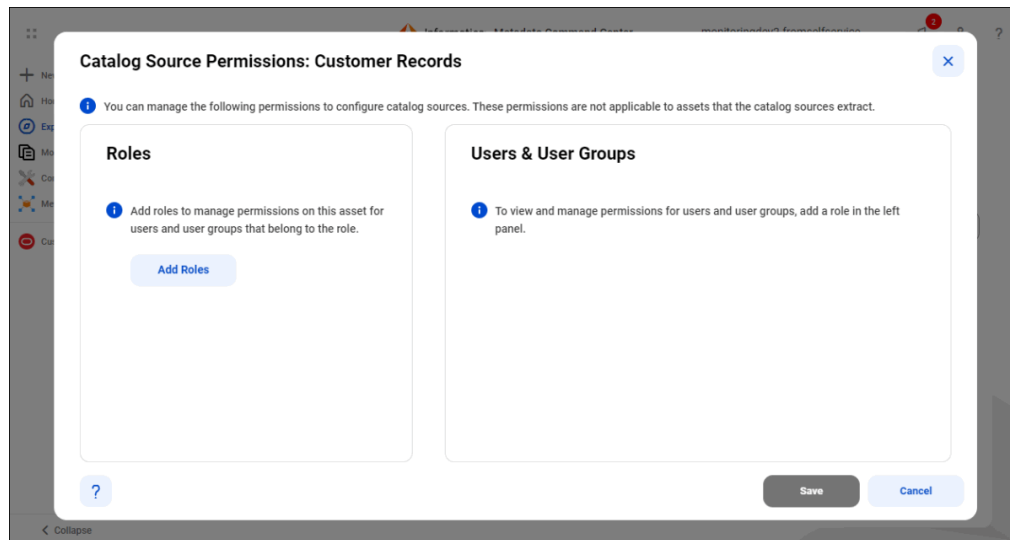
You can select roles and add specific users or user groups to those roles to grant the following levels of permission for catalog source configuration:

- Create
- Read
- Update
- Run
- Set Permissions

Based on the permissions granted to the roles, the selected users and user groups belonging to that role can perform appropriate operations for configuring catalog sources.

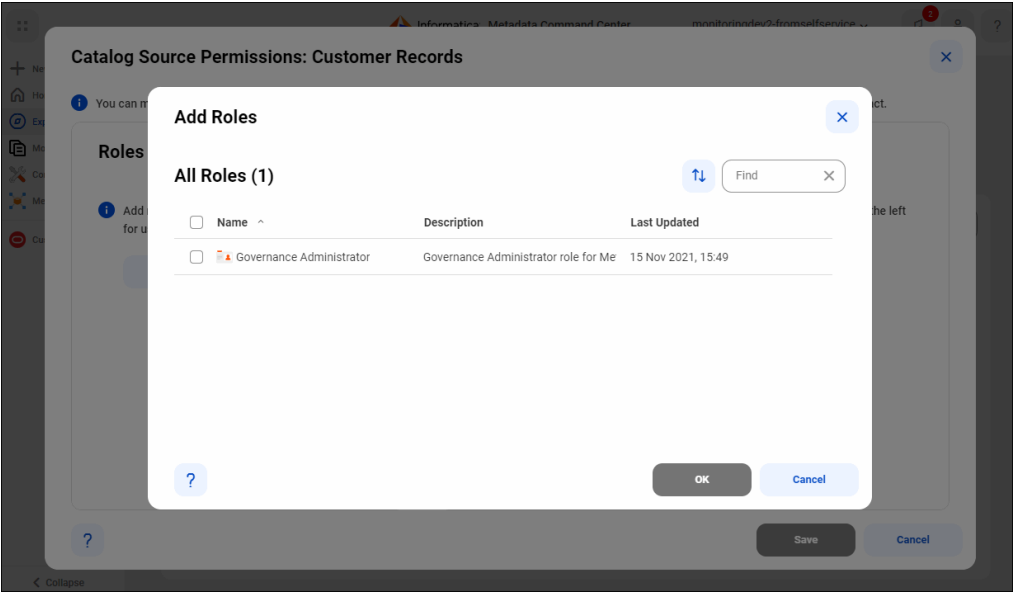
1. Go to the **Explore** page in Metadata Command Center.
2. From the list of catalog sources, search for the catalog source for which you want to manage permissions.
3. Click the **Action** menu, and select **Permissions**.

The **Catalog Source Permissions** dialog box appears. The following image shows the **Catalog Source Permissions** dialog box:



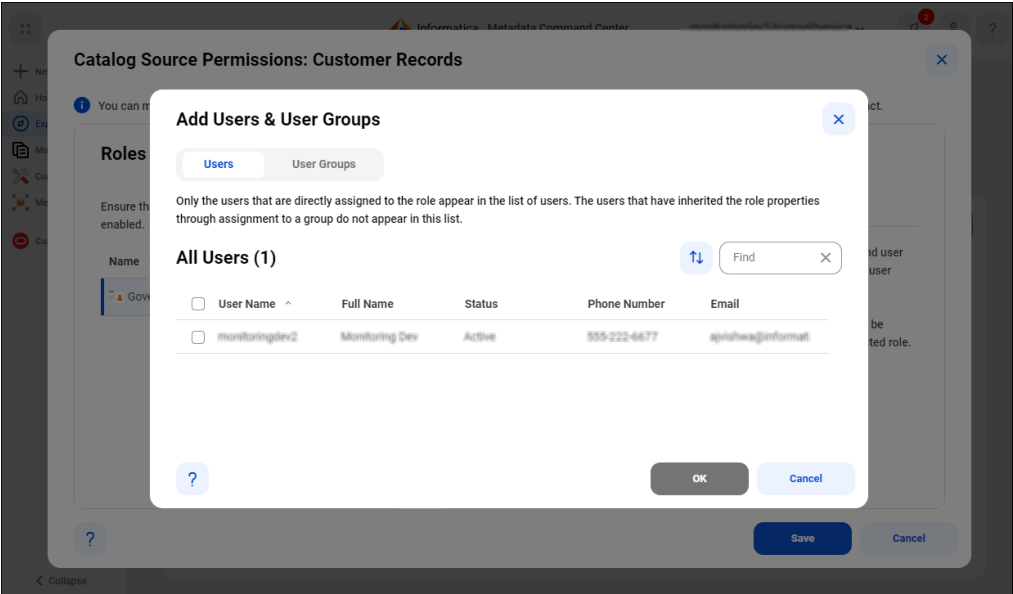
4. In the **Roles** panel, click **Add Roles**.

The **Add Roles** dialog box displays the list of roles that your organization administrator configured for Metadata Command Center. The following image shows the **Add Roles** dialog box:



5. Select one or more roles, and click **OK** to add the roles.
6. In the **Add Users & User Groups** panel, by default, all users and user groups that belong to the selected role are granted the role-defined permissions for the catalog source configuration. To assign permissions only to the selected users and user groups that belong to this role, choose **Specific Users and User Groups**.

The following image shows the **Add Users & User Groups** panel:



7. Select **Add Specific Users and User Groups**.  
The **Add Users & User Groups** dialog box displays the list of users and user groups that the administrator has assigned to the selected role.
8. Select one or more users or user groups to assign to the selected role, and click **OK**.

Only the selected users and user groups belonging to the specified role will be granted the role-defined permissions for catalog source configuration.

9. View the assigned permissions for each user and or group, and click **Save**.

## Curating CLAIRE recommendations

You can view related catalog sources and accept or reject CLAIRE recommendations for a catalog source.

1. Go to the **Explore** page in Metadata Command Center.
2. Select **Catalog Sources** from the menu.
3. From the list of catalog sources, search for the catalog source for which you want to curate CLAIRE recommendations.
4. Hover your mouse over the catalog source and click **View Lineage Discovery** from the **Action** menu.

**Note:** The **View Lineage Discovery** option is available for catalog sources that are run with the lineage discovery capability.

The **Configure** page appears with the catalog source filtered on the **Lineage Discovery** tab of the **Lineage** tab.

The **Related Catalog Sources** tab displays a list of related catalog sources.

5. Hover your mouse over a related catalog source and click **Accept** or **Reject** from the **Action** menu.

For more information about lineage discovery and curating CLAIRE recommendations, see *Lineage discovery* in the *Administration* help.

## Deleting or purging a catalog source

Delete or purge a catalog source based on your business requirements.

When you delete a catalog source, you delete all the configuration specific to that catalog source, along with all the metadata that was extracted and any enrichment made to the associated metadata. Purging a catalog source deletes all the metadata that was extracted, along with any enrichment made to the associated metadata.

**Note:** Before you delete or purge a catalog source, manually unassign the connections that are assigned to that catalog source.

1. Go to the **Explore** page in Metadata Command Center.
2. Select **Catalog Sources** from the menu.
3. From the list of catalog sources, search for the catalog source that you want to delete or purge.
4. Click the **Action** menu, and select **Delete** or **Purge**.

**Note:** You can't delete or purge a catalog source if the catalog source job is in the running state.

5. To confirm delete or purge, click **OK**.

The catalog source is triggered to delete or purge. You can monitor the status of the job on the **Monitor** page.

**Note:** If the deletion job succeeds, the catalog source disappears from Metadata Command Center. If it fails, some associated objects might still be present in Data Governance and Catalog. Such catalog sources continue to appear in the list of catalog sources in Metadata Command Center, but are marked as **Deleted**. Delete the catalog sources to remove them along with any remaining objects present in Data Governance and Catalog.

## Purging obsolete objects from a catalog source

You can purge obsolete objects from a catalog source.

When you configure or run a catalog source, you can choose to deprecate objects that are deleted from a source system. If you delete objects from the source system or make changes to the filter, the objects imported into the catalog before the change move to the Obsolete lifecycle in the catalog. You can purge obsolete objects from a catalog source. This permanently deletes all objects with the Obsolete lifecycle status, along with associated enrichments, from the catalog.

1. Go to the **Explore** page in Metadata Command Center.
2. Select **Catalog Sources** from the menu.
3. From the list of catalog sources, search for the catalog source from which you want to purge obsolete objects.
4. Click the **Action** menu, and select **Purge Obsolete Objects**.

A warning message appears on the page.

5. Click **Yes** to confirm.

A confirmation message appears on the page and the purge job starts. You can monitor the status of the job on the **Monitor** page. If the job succeeds, all obsolete objects present in the catalog source disappear from the catalog.

**Note:** If the job fails, some obsolete objects might remain in the catalog. To remove the remaining obsolete objects, run the purge job again.

## Referenced catalog sources

A referenced catalog source indicates that the catalog source that you configured includes references from other source systems. Assets from reference catalog sources are known as reference assets.

When you configure a catalog source in Metadata Command Center, it might contain lineage information and connection data from other source systems that don't exist in the catalog. Though the information about the source system does not exist in the catalog, you can still view the source system as a reference catalog source and view lineage for the assets in the configured catalog source with the reference assets from the reference catalog source.

You can configure predefined or custom catalog sources to view the lineage with reference assets from reference catalog sources. After extracting reference assets, Data Governance and Catalog displays the reference catalog source and the lineage for the asset in the catalog with the reference assets. To link the reference assets to actual objects and to view the complete lineage, assign connections between the reference catalog source and the actual catalog source that you configure in Metadata Command Center. For example, you have configured an Informatica PowerCenter catalog source that contains mappings that point to tables or columns in an Oracle database. The Oracle database is the reference catalog source and the tables and columns in the Oracle database are reference assets from the reference catalog source. To view the column details from an Oracle table referenced by the PowerCenter catalog source, configure the Oracle catalog source in Metadata Command Center and then perform connection assignments between the reference catalog source and the schema in the Oracle source system.

You can also assign glossary terms to reference assets to enrich them.



## Assign connections to reference catalog sources

Assigning a connection to reference catalog source involves assigning connections from the reference catalog source to the catalog source that represents the source system.

Assign connections for reference catalog sources to link the reference assets to actual objects in the source system and to view complete lineage. Before you assign connections, configure the catalog source for the reference source system. See [“Creating a catalog source” on page 10](#).

You can then assign connections between the reference catalog source and the configured catalog source. For information about assigning connections, refer to the *Administration* help. When you assign connections to reference catalog sources, the reference assets map to the actual objects in the configured source system.

After you assign connections to reference catalog sources, you can view the complete lineage including actual assets from the source that you configured the connection to. If you had enriched reference assets with business terms, the terms are associated with the catalog source after connection assignment.

## CHAPTER 2

# Source systems

View the source systems, the connections to configure each source in Informatica Intelligent Cloud Services Administrator, and the capabilities for each source.

The following table shows the connections and capabilities for each source system that Metadata Command Center provides by default:

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 3, "Amazon Athena" on page 75<sup>5</sup></a>	Amazon Athena	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	No
Amazon DynamoDB using <a href="#">Chapter 35, "JDBC" on page 115<sup>5</sup></a>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Pushdown to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 4, "Amazon Redshift" on page 78</a> <sup>5</sup>	Amazon Redshift V2	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	Data access control policies and data filter policies <sup>7</sup>	Yes	No
<a href="#">Chapter 5, "Amazon S3" on page 79</a> <sup>5</sup>	Amazon S3 V2	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	Yes	No	Yes	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 6, "Apache Atlas" on page 80</a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Not Applicable	No	No	No	No
Apache Cassandra using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JD BC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No
<a href="#">Chapter 7, "Apache Hive" on page 81</a>	Hive Connector	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	Yes <sup>7</sup>

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 8, "Apache Hive QL Script" on page 82</a>	Hive Connector	No	No	No	Yes	No	No	No	No	No	Yes	Not Applicable	No	No	No	Not Applicable
<a href="#">Chapter 9, "AWS Glue" on page 83</a>	Azom Athena	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Yes (PySpark)	Yes	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 10, "Data bricks Delta" on page 84</a>	Data bricks Delta	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes (Py Spark & SQL)	Yes	No	Data access control policies and data filter policies <sup>7</sup>	Yes	No
<a href="#">Chapter 12, "Denodo" on page 86</a>	Denodo	No	No	No	Yes	No	No	No	No	No	No	Yes	No	No	-	No

Source System	Connection	Incremental Metadata at Extraction	Search and Select Metadata at Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 11, "dbt" on page 85</a>	No Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	No
<a href="#">Chapter 13, "erwin Data Modeler File" on page 87</a> <sup>4</sup>	erwin Data Modeler File	No	No	No	No	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Not Applicable	No	No	No	No
<a href="#">Chapter 14, "erwin Mart Server" on page 88</a> <sup>4</sup>	erwin Data Modeler File	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Not Applicable	No	No	No	No



Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 15, "File System" on page 89</a>	No Applicable <sup>1</sup>	No	No	No	No	Yes <b>Note:</b> Available for Local File System protocol.	Yes	Yes <b>Note:</b> Available for Local File System protocol.	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes, dependent on file	No
<a href="#">Chapter 16, "Five tran Platf orm" on page 90</a>	No Applicable <sup>1</sup>	Yes	No	No	Yes	No	No	Not Applicable	No	No	No	Yes	No	No	-	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 17, "Google BigQuery" on page 91</a> <sup>5</sup>	Google BigQuery V2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	Yes	No	Yes	No
<a href="#">Chapter 18, "Google BigQuery SQL Script" on page 92</a>	Google BigQuery V2	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	No	No	Not Applicable
<a href="#">Chapter 19, "Google Cloud Storage" on page 93</a> <sup>5</sup>	Google Cloud Storage V2	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	Yes	No	Yes	No

Source System	Connection	Incremental Metadata at Extraction	Search and Select Metadata at Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 20, "Google Looker" on page 94</a>	No Not Applicable <sup>1</sup>	No	No	Yes	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	No	No	No	No	No
<a href="#">Chapter 21, "Google Vertex AI" on page 95</a>	No Not Applicable	No	No	No	Yes	No	No	No	No	No	No	No	No	No	-	No
<a href="#">Chapter 22, "Greenplum" on page 96</a>	Greenplum	No	No	No	Yes	No	No	No	Yes	Yes	Yes	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 23, "Hadoop Distributed File System" on page 97</a>	Hadoop Files V2	No	No	No	No	Yes	Yes	No	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	Not Applicable
<a href="#">Chapter 24, "IBM Cognos" on page 98<sup>4</sup></a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	No	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 25, "IBM Db2 for LUW" on page 99</a>	Db 2 for LUW Database Integration	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Not Applicable	No	No	No	No
<a href="#">Chapter 26, "IBM Db2 for LUW Script" on page 103</a>	Db 2 for LUW Database Integration	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Yes	Yes	No	No	No	Not Applicable

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 27, "IBM Db2 for z/OS" on page 104</a>	Db2 for zOS Database Integration	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Not Applicable	No	No	No	Not Applicable
IBM Db2 for z/OS using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JD BC V2	No	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 28, "IBM InfoSphere Data Stage" on page 105</a>	No t Ap pli ca bl e	No	No	No	Yes	Not App lica ble	Not Appli cabl e	Not Appli cabl e	Yes	Yes	Not Ap plic abl e	Yes	No	No	No	No
<a href="#">Chapter 29, "IBM Mainframe Job Control Language (AcceleraTor)" on page 106</a>	No t Ap pli ca bl e	No	No	No	Yes	No	No	No	No	No	Yes	Yes	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 30, "IBM Netezza" on page 108</a>	Netezza	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Not Applicable	Yes	No	Yes	No
IBM Netezza using <a href="#">Chapter 35, "JDBC" on page 115<sup>5</sup></a>	JDBC V2	No	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	No
NetSuite using <a href="#">Chapter 35, "JDBC" on page 115<sup>5</sup></a>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No



Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 31, "IDE RA/Studio Data Architect" on page 109<sup>4</sup></a>	No Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	No Not Applicable	Not Applicable	No	No	Not Applicable	Not Applicable	No	No	No	No
<a href="#">Chapter 32, "Informatica Developer" on page 110</a>	No Not Applicable <sup>1</sup>	No	No	No	Yes	No	No	No	No	No	No	Yes	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 33, "Informational Intelligent Cloud Services" on page 111</a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	Yes	No	No	No	No
<a href="#">Chapter 34, "Informational PowerCenter" on page 112</a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	Yes	No	No	No	No
<a href="#">Chapter 36, "Kafka" on page 120</a>	Kafka	No	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 37, "MariaDB" on page 123</a> <sup>5</sup>	MySQL	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	Yes <sup>7</sup>
Marketo using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	No
<a href="#">Chapter 38, "Microsoft Azure Analysis Services" on page 124</a> <sup>5</sup>	Microsoft Azure Analysis Services	No	No	No	Yes	No	No	No	No	No	Not Applicable	Yes	No	No	No	Not Applicable

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 39, "Microsoft Azure Blob Storage" on page 125</a>	Microsoft Azure Blob Storage V3	Yes	No	Yes	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes, dependent on file	No
Microsoft Azure Cosmos DB using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JD BC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 40, "Microsoft Azure Data Factory" on page 126</a>	Not Applicable <sup>1</sup>	No	No	Yes	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	Yes	No	No	No	No
<a href="#">Chapter 41, "Microsoft Azure Data Lake Storage Gen2" on page 127<sup>5</sup></a>	Microsoft Azure Data Lake Storage Gen2	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	Yes	No	Yes, dependent on file	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 42, "Microsoft Azure SQL Server" on page 128<sup>5</sup></a>	SQL Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	No	Yes	No
<a href="#">Chapter 45, "Microsoft Azure Synapse Data Warehouse" on page 131<sup>5</sup></a>	Microsoft Azure Synapse SQL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	No	Yes	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 43, "Microsoft Azure SQL Server Script" on page 129</a>	Microsoft SQL Server	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	Not Applicable
<a href="#">Chapter 44, "Microsoft Azure Synapse Analytics" on page 130</a>	Microsoft Azure Synapse Analytics	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Yes (PySpark & SQL)	Yes	Yes	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 46, "Microsoft Azure Synapse Data Warehouse Script" on page 141</a>	Microsoft Azure Synapse SQL	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	Not Applicable
Microsoft Dynamics CRM using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No



Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Pushdown to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 47, "Microsoft Fabric Data Warehouse" on page 142</a> <sup>5</sup>	Microsoft Fabric Data Warehouse	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	Yes	Data access control policies and data filter policies <sup>7</sup>	Yes	No
<a href="#">Chapter 48, "Microsoft Fabric Data Lakehouse" on page 143</a> <sup>5</sup>	Microsoft Fabric Lakehouse	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	No	No	Yes	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 49, "Microsoft Fabric OneLake" on page 144</a> <sup>5</sup>	Microsoft Fabric OneLake	No	No	No	No	Yes <b>Not</b> Available for delimited files.	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	No
<a href="#">Chapter 50, "Microsoft OneDrive" on page 145</a>	Not Applicable <sup>1</sup>	No	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Pushdown to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 51, "Microsoft Power BI" on page 146</a> <sup>5</sup>	Microsoft Power BI	No	No	Yes	Yes	Not Applicable	No Applicable	Not Applicable	Yes	Yes	Not Applicable	Yes	No	Data access control policies <sup>7</sup>	No	Not Applicable
<a href="#">Chapter 52, "Microsoft Purview" on page 147</a>	Not Applicable <sup>1</sup>	No	No	Yes	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Not Applicable	No	No	No	No
<a href="#">Chapter 53, "Microsoft SharePoint Online" on page 148</a>	Microsoft SharePoint Online	Yes	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 54, "Microsoft SQL Server" on page 149</a> <sup>5</sup>	SQL Server	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	No	Yes	Yes <sup>7</sup>
<a href="#">Chapter 55, "Microsoft SQL Server Analysis Services" on page 150</a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 56, "Microsoft SQL Server Integration Services" on page 151</a>	SQL Server	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	No
<a href="#">Chapter 57, "Microsoft SQL Server Reporting Services" on page 155</a>	Not Applicable <sup>1</sup>	No	No	No	No	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	Yes	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Pushdown to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 58, "Microsoft SQL Server Script" on page 158</a>	Microsoft SQL Server	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Yes	Yes	No	No	No	Not Applicable
<a href="#">Chapter 59, "Microsoft Strategy" on page 159<sup>4</sup></a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	No	No	No	No	No
MongoDB using <a href="#">Chapter 35, "JDBC" on page 115<sup>5</sup></a>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 60, "MySQL" on page 160</a> <sup>5</sup>	MySQL	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	Yes <sup>7</sup>
<a href="#">Chapter 61, "Oracle" on page 163</a> <sup>5</sup>	Oracle	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	No	Yes	Yes <sup>7</sup>
<a href="#">Chapter 62, "Oracle Business Intelligence" on page 164</a>	Not Applicable <sup>1</sup>	No	No	No	No	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	No	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 63, "Oracle Cloud Infrastructure GoldenGate" on page 165</a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Yes	Yes	No	No	No	No
<a href="#">Chapter 64, "Oracle Cloud Object Storage" on page 166</a>	Oracle	No	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes, dependent on file	No



Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 65, "Oracle Data Integrator" on page 167</a>	Oracle	No	No	No	Yes	No	No	No	No	No	Not Applicable	Yes	No	No	No	No
<a href="#">Chapter 66, "Oracle PL/SQL Script" on page 168</a>	Oracle	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Yes	Yes	No	No	No	Not Applicable
<a href="#">Chapter 67, "Oracle SQL Loader" on page 169</a>	Oracle	No	Not Applicable	No	Yes	No	No	No	No	No	No	Yes	No	No	-	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 68, "PostgreSQL" on page 170</a> <sup>5</sup>	PostgreSQL	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	No	Yes	Yes <sup>7</sup>
<a href="#">Chapter 69, "Qlik Sense" on page 175</a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	No	Yes	No	No	No
<a href="#">Chapter 70, "Qlik Sense Cloud" on page 180</a>	Not Applicable <sup>1</sup>	No	No	Yes	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	No	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 71, "Qlik View" on page 181<sup>4</sup></a>	No Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	No	Yes	No	No	No
<a href="#">Chapter 72, "Salesforce" on page 184</a>	Salesforce	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	Yes	No	Yes	No
<a href="#">Chapter 73, "SAP Analytics Cloud - Previous catalog source" on page 190</a>	No Not Applicable	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	No	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Pushdown to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 74, "SAP Business Objects" on page 191</a> <sup>4</sup>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	No	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 75, "SAP Business Objects Data Services" on page 196</a>	- Oracle - Microservices of tSQLServer - SAP HANA	No	No	No	Yes	No	No	No	No	No	No	Yes	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 76, "SAP Business Warehouse (SAP BW)" on page 197</a>	SAP BW	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	No
<a href="#">Chapter 77, "SAP BW/4HANA" on page 205</a>	SAP BW	Yes	No	No	Yes	Yes	Yes	No	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 78, "SAP Data sphere - Previous catalog source" on page 216</a>	SAP OD at a V4	No	No	Not Applicable	Yes	Yes	Yes	No	Yes	Yes	No	Not Applicable	No	No	No	No
<a href="#">Chapter 79, "SAP ERP" on page 217</a>	SAP Bapi SAP Table. For data profiling	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Pushdown to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 80, "SAP HANA A Database" on page 227</a>	SAP HANA	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	No
<a href="#">Chapter 81, "SAP PowerDesigner" on page 230<sup>4</sup></a>	Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Not Applicable	No	No	No	No
<a href="#">Chapter 82, "SAP Sales &amp; Service Cloud" on page 231</a>	Not Applicable	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No



Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 83, "SAP S/4HANA Cloud - Preview catalog source" on page 232</a>	Not Applicable <sup>1</sup>	No	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No
<a href="#">Chapter 84, "SAP SuccessFactors" on page 233</a>	Successful Factor on Data	No	No	No	No	Yes	No	No	No	No	No	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
SAP SuccessFactors using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No
<a href="#">Chapter 86, "SAS Base Programs (Accelerator)" on page 235</a>	Not Applicable	No	No	No	No	No	No	No	No	No	Yes	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 87, "SFTP File System" on page 236</a>	Advanced SFTP V2	No	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No
SingleStore using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 88, “Snowflake Data Cloud” on page 237</a> <sup>5</sup>	Snowflake Data Cloud	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Yes	Data access control policies and data filter policies <sup>7</sup>	Yes	No
<a href="#">Chapter 89, “Snowflake SQL Script” on page 238</a>	Snowflake Data Cloud	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	Not Applicable

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 90, "Strategy Cloud" on page 239</a>	Strategy Cloud	No	No	No	Yes	No	No	No	No	No	Not Applicable	No	No	No	-	No
<a href="#">Chapter 91, "Swagger API - Preview catalog source" on page 240</a>	Not Applicable	No	No	No	No	No	No	No	No	No	Not Applicable	No	No	No	-	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
Sybase ASE using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No
Sybase IQ using <a href="#">Chapter 35, "JDBC" on page 115</a> <sup>5</sup>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No
<a href="#">Chapter 92, "Tableau" on page 241</a>	Tableau V3	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Not Applicable	Yes	No	No	No	Not Applicable

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 93, "Tale and Data Integration" on page 244</a>	No Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	No Not Applicable
<a href="#">Chapter 94, "Teradata BTEQ Script" on page 245</a>	Teradata	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	No Not Applicable
<a href="#">Chapter 95, "Teradata Database" on page 246</a>	Teradata	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	Yes	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 96, "Tera data Fast Export Script" on page 249</a>	Tera data	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	Not Applicable
<a href="#">Chapter 97, "Tera data Fast Load Script" on page 250</a>	Tera data	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	Not Applicable
<a href="#">Chapter 98, "Tera data Multi Load Script" on page 251</a>	Tera data	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	Yes	No	No	No	Not Applicable



Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Push down to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
<a href="#">Chapter 99, "TIB CO Spotfire" on page 252</a>	No Not Applicable <sup>1</sup>	No	No	No	Yes	Not Applicable	Not Applicable	Not Applicable	No	No	Not Applicable	No	No	No	No	No
<a href="#">Chapter 100, "Workday" on page 253</a>	Workday Mass Ingestion	No	No	No	No	No	No	No	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No
Workday using <a href="#">Chapter 35, "JDBC" on page 115<sup>5</sup></a>	JDBC V2	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Not Applicable	Not Applicable	No	No	No	No

Source System	Connection	Incremental Metadata Extraction	Search and Select Metadata Filters	Serverless Runtime Environment	Lineage Discovery <sup>6</sup>	Data Profiling	DQ Automation	Data Observability	Data Classification <sup>6</sup>	Glossary Association <sup>6</sup>	Advanced Programming Language Parsing	Connection-aware scan	Relationship Discovery	Data Access Policy Pushdown to Cloud Data Providers	Data Access Policy Enforcement in Data Integration	Data Access Policy Enforcement in Data Marketplace <sup>8</sup>
---------------	------------	---------------------------------	------------------------------------	--------------------------------	--------------------------------	----------------	---------------	--------------------	----------------------------------	-----------------------------------	---------------------------------------	-----------------------	------------------------	---	--	---

<sup>1</sup> For these catalog sources, you do not need to configure a connection in the Informatica Intelligent Cloud Services Administrator.

<sup>2</sup> You can procure the source-specific JDBC drivers to perform data profiling and quality for these source systems using the JDBC catalog source. Note that JDBC drivers are not bundled as part of Informatica Intelligent Cloud Services. You can purchase the driver directly from the vendor or download it from the CData third-party website.

<sup>3</sup> Effective in the February 2023 release, the Databricks Delta Lake catalog source is deprecated. Informatica intends to drop support for the Databricks Delta Lake catalog source in a future release. If you want to extract metadata from the Databricks Delta Lake source system, Informatica recommends that you use the Databricks catalog source.

<sup>4</sup> For these catalog sources, you can only use Secure Agents installed on Windows machines.

<sup>5</sup> To connect to these source systems and run metadata extraction, data profiling, and data quality jobs, you can configure a secrets manager for your organization. Use AWS Secrets Manager or Azure Key Vault to store and retrieve sensitive credentials.

<sup>6</sup> You can enable this capability for custom catalog sources.

<sup>7</sup> For information about configuring this connection, see *Secure Agent Services* in the Administrator help.

<sup>8</sup> These are the source systems that the Data Access Management Proxy service is able to read the data from. You connect source systems to the proxy through the proxy's JDBC driver.

For information about configuring this connection, see *Secure Agent Services* in the Administrator help.

**Note:** Metadata extraction with Secure Agent is supported for all source systems.

For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.

## CHAPTER 3

# Amazon Athena

Amazon Athena is an interactive query service to query data and analyze big data in Amazon S3 using standard SQL.

### Objects extracted

Metadata Command Center extracts the following objects from an Amazon Athena source system:

- Database
- Schema
- View
- ViewColumn
- External Table
- External Column
- Calculation
- Resource

### Prerequisites for configuring an Amazon Athena catalog source

Use the Amazon Athena connector to connect to the Amazon Athena source system. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.

### Configure permissions or access to Amazon Athena

#### Permissions to extract metadata

This section addresses permissions for configuring an Amazon Athena connection. Amazon Athena uses Amazon S3 buckets to store query results.

Grant the following Identity and Access Management (IAM) permissions to the user for the INFORMATION\_SCHEMA database and all user-defined databases that you want to scan:

```
glue:GetDatabases
glue:GetDatabase
glue:GetTables
glue:GetTable
```

Grant the following IAM permissions to the user to create, manage, execute, and delete prepared statements in Amazon Athena :

```
athena:CreatePreparedStatement
athena:StartQueryExecution
athena:GetQueryResultsStream
athena:GetQueryResults
athena:GetDatabase
athena:GetDataCatalog
athena>DeletePreparedStatement
athena:GetPreparedStatement
```

```
athena:ListDatabases
athena:StopQueryExecution
athena:GetQueryExecution
athena:ListDataCatalogs
```

Grant the following IAM permissions to the user to perform operations on Amazon S3 buckets:

```
s3:PutObject
s3:GetObject
s3:GetBucketLocation
```

Grant permissions that allow you to perform the following operations:

- select on INFORMATION\_SCHEMA.SCHEMATA
- show tables

### Permissions to run data profiles

You do not need additional permissions to run data profiles.

### Data profiling for Amazon Athena

Configure data profiling to run profiles on the metadata extracted from an Amazon Athena source system. You can run data profiles on the following Amazon Athena objects:

- External tables created in the following file formats:
  - Avro
  - CSV
  - Delta
  - JSON
  - Parquet
- External columns

You can view the profiling statistics in Data Governance and Catalog. The data profiling task runs profiles on the following data types for Amazon Athena objects:

- Bigint
- Boolean
- Char
- Date
- Decimal
- Double
- Float
- Int
- Smallint
- String
- Timestamp
- Tinyint
- Varchar

### Sampling type

Determine the sample rows on which you want to run the data profiling task. You can choose one of the following sampling types for an Amazon Athena catalog source:

- All Rows
- Limit N Rows
- Custom Query. Enter the sampling method to specify a percentage of rows on which you want to run the data profiling task. For example, `TABLESAMPLE BERNOULLI(10)` or `TABLESAMPLE SYSTEM(10)`

**Note:** You can run data quality only on views and external tables that are created in Amazon Athena .

### Create a connection to Amazon Athena

When you configure a connection to the Amazon Athena source system in Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the Amazon Athena connection properties:

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: <code>_ . + -</code> , Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. <b>Note:</b> If you're using this connection to apply data access policies through pushdown or proxy services, you cannot use the Secret Vault configuration option. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, serverless, or elastic runtime environment. For more information about how to configure and use the runtime environments, see <i>Runtime Environments</i> in the Administrator help.
Authentication Type	The authentication mechanism to connect to Amazon Athena. Select Permanent IAM Credentials or EC2 instance profile. Permanent IAM credentials is the default authentication mechanism. Permanent IAM requires an access key and secret key to connect to Amazon Athena. Use the EC2 instance profile when the Secure Agent is installed on an Amazon Elastic Compute Cloud (EC2) system. This way, you can configure AWS Identity and Access Management (IAM) authentication to connect to Amazon Athena.
JDBC URL	The URL of the Amazon Athena connection. Enter the JDBC URL in the following format: <code>jdbc:awsathena:// AwsRegion=&lt;region_name&gt;;S3OutputLocation=&lt;S3_Output_Location&gt;;Workgroup=&lt;Workgroup_Name&gt;;</code> <b>Note:</b> If you use a workgroup with customer managed query results, specify at least one of the two parameters in the JDBC URL, either the S3 output location or the workgroup name. For a workgroup with Athena managed query results, specify only the workgroup name and do not include the S3 output location in the JDBC URL.

## CHAPTER 4

# Amazon Redshift

See [Amazon Redshift Sources](#) to learn how to register and configure Amazon Redshift source systems 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 5

# Amazon S3

See [Amazon S3 Sources](#) to learn how to register and configure Amazon S3 source systems 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 6

# Apache Atlas

See [Apache Atlas Sources](#) to learn how to register and configure Apache Atlas source systems 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 7

# Apache Hive

See [Apache Hive Sources](#) to learn how to register and configure Apache Hive source systems 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 8

# Apache HiveQL Script

See [Apache HiveQL Script Sources](#) to learn how to register and configure Apache Hive source systems as Apache HiveQL Script 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 9

# AWS Glue

See [AWS Glue Sources](#) to learn how to register and configure AWS Glue source systems 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 10

# Databricks

See [Databricks Sources](#) to learn how to register and configure Databricks source systems 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 11

## dbt

See [dbt Sources](#) to learn how to register and configure dbt source systems 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 12

# Denodo

See [Denodo](#) to learn how to register and configure Denodo source systems 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 13

# erwin Data Modeler File

See [erwin Data Modeler File Sources](#) to learn how to register and configure erwin Data Modeler File source systems 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 14

# erwin Mart Server

See [erwin Mart Server Sources](#) to learn how to register and configure erwin Mart Server 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 15

# File System

See [File System Sources](#) to learn how to register and configure File System source systems 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 16

# Fivetran Platform

See [Fivetran Platform Sources](#) to learn how to register and configure Fivetran Platform source systems 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 17

# Google BigQuery

See [Google BigQuery Sources](#) to learn how to register and configure Google BigQuery source systems 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 18

# Google BigQuery SQL Script

See [Google BigQuery SQL Script Sources](#) to learn how to register and configure Google BigQuery SQL Script source systems 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 19

# Google Cloud Storage

See [Google Cloud Storage](#) to learn how to register and configure Google Cloud Storage source systems 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 20

# Google Looker

See [Google Looker Sources](#) to learn how to register and configure Google Looker source systems 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 21

# Google Vertex AI

See [Google Vertex AI Sources](#) to learn how to register and configure Google Vertex AI source systems 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 22

# Greenplum

See [Greenplum Sources](#) to learn how to register and configure Greenplum source systems 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 23

# Hadoop Distributed File System

See [Hadoop Distributed File System Sources](#) to learn how to register and configure Hadoop Distributed File System source systems 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 24

# IBM Cognos

See [IBM Cognos Sources](#) to learn how to register and configure IBM Cognos source systems 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 25

# IBM Db2 for LUW

IBM Db2 for LUW is a relational database management system (RDBMS) designed by IBM to store, analyze, and retrieve data from for Windows, Linux and Unix operating systems.

Configure an IBM Db2 for LUW catalog source to extract metadata from an IBM Db2 for LUW database hosted on a dedicated server, or from an Amazon RDS for Db2 database.

### Objects extracted

The metadata extraction service extracts the following objects from an IBM Db2 for LUW source system:

- Database
- Schema
- Table
- View
- Column
- Materialized Query Table
- Stored Procedure

**Note:** To extract the following schemas, you must define include filters:

- NULLID
- SQLJ
- SYSFUN
- SYSIBMINTERNAL
- SYSIBMTS
- SYSPROC
- SYSPUBLIC
- SYSCAT
- SYSIBM
- SYSIBMADM
- SYSSTAT
- SYSTOOLS

### Prerequisites for configuring the IBM Db2 for LUW catalog source

Use the Db2 for LUW Database Ingestion connector to connect to IBM Db2 for LUW source system. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.

## Configure permissions or access to IBM Db2 for LUW

This section addresses permissions for configuring IBM Db2 for LUW connection. The following table lists the schema objects and system tables on which you configure SELECT permissions for the IBM Db2 for LUW database user account:

Schema Objects	System Tables
<ul style="list-style-type: none"><li>• Tables</li><li>• Views</li><li>• Procedures</li><li>• Functions</li><li>• Databases</li></ul>	<ul style="list-style-type: none"><li>• select on syscat.COLUMNS</li><li>• select on syscat.FUNCTIONS</li><li>• select on syscat.NICKNAMES</li><li>• select on syscat.PROCEDURES</li><li>• select on syscat.PROCPARMS</li><li>• select on syscat.TABLES</li><li>• select on syscat.VIEWS</li><li>• select on syscat.SCHEMATA</li><li>• select on syscat.TABCONST</li><li>• select on syscat.REFERENCES</li><li>• select on syscat.KEYCOLUSE</li></ul>

### Permissions to run data profiles

To perform data profiling on IBM Db2 for LUW databases, grant the Execute permission on the following objects:

- SYSCAT.ROLEAUTH table
- SYSPROC.AUTH\_LIST\_GROUPS\_FOR\_AUTHID built-in table function

## Data classification for IBM Db2 for LUW objects

Configure data classification for IBM Db2 for LUW catalog sources to classify and organize data in your organization. You can view the data classification results in Data Governance and Catalog.

## Connection properties

When you configure a connection to the IBM Db2 for LUW source system in Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the IBM Db2 for LUW connection properties:

Property	Description
Connection Name	Name of the connection.
Type	Type of connection. Select Db2 for LUW Database Ingestion from the list.
Runtime Environment	The execution platform that runs tasks. The runtime environment is either a Secure Agent or a serverless runtime environment.
User Name	The name of the user account that connects to IBM Db2 for LUW database.
Password	The password to use for connecting to IBM Db2 for LUW database.
Host	The fully qualified host name of the machine where IBM Db2 for LUW database is hosted.

Property	Description
Port	The port number for the IBM Db2 for LUW database.
Database Name	The IBM Db2 for LUW database name that is used to access metadata.
Advanced Connection Properties	<p>Advanced properties for the Progress DataDirect JDBC DB2 driver that you use to connect to the IBM Db2 for LUW source system.</p> <p>You can specify the following advanced connection properties:</p> <ul style="list-style-type: none"> <li>Specify the path to the SSL certificate. For example, <code>EncryptionMethod=SSL;TrustStore=/data/sslCertificates/DB2_ssl/mydbserverssl.jks;TrustStorePassword=Infa@123.</code></li> <li>If you enable credential protection without enabling full encryption, specify the following property: <code>AuthenticationMethod=encryptedUIDPassword</code></li> </ul> <p><b>Note:</b> If you don't specify the property, Test Connection fails.</p> <ul style="list-style-type: none"> <li>If you use an Amazon RDS for Db2 database, specify the following properties:  <code>EncryptionMethod=requestDBEncryption;AuthenticationMethod=encryptedUIDPassword</code></li> </ul> <p><b>Note:</b> If you don't specify the properties, Test Connection fails.</p>

## Referenced source systems

If the source system references another source system, create a connection assignment in Metadata Command Center to view data lineage with endpoints. To create a connection assignment, create a connection based on the referenced source system, and then assign the connection to the catalog source.

**Note:** You can view the lineage with reference objects without creating a connection assignment. After connection assignment, you can view the actual objects.

You can assign an IBM Db2 for LUW source system as a referenced source system. To create a connection assignment, the catalog source must belong to the Schema class type.

## Data Profiling for IBM Db2 for LUW

You can run data profiles and data quality tasks for IBM Db2 for LUW assets. Configure data profiling to run profiles on the metadata extracted from an IBM Db2 for LUW source system. You can view the profiling statistics in Data Governance and Catalog.

You can run data profiles on the following IBM Db2 for LUW objects:

- Tables
- Views

### Sampling type

Determine the sample rows on which you want to run the data profiling task.

You can choose one of the following sampling types for an IBM Db2 for LUW catalog source:

- All Rows
- Limit N Rows
- Custom Query

### Data types

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

- Double

- Time
- Smallint
- Real
- Float
- Char
- Varchar
- Timestamp
- Decimal
- Bigint
- Integer
- Long varchar
- Graphic
- Vargraphic
- Xml
- Decfloat

## CHAPTER 26

# IBM Db2 for LUW Script

See [IBM Db2 for LUW Script Sources](#) to learn how to register and configure IBM Db2 for LUW source systems 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 27

# IBM Db2 for z/OS

See [IBM Db2 for z/OS Sources](#) to learn how to register and configure IBM Db2 for z/OS source systems 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 28

# IBM InfoSphere DataStage

See [IBM InfoSphere DataStage Sources](#) to learn how to register and configure Amazon S3 source systems 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 29

# IBM Mainframe Job Control Language (Accelerator)

You can register and configure IBM Mainframe Job Control Language (Accelerator) source systems 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.

Job Control Language (JCL) is a scripting language used on IBM mainframe operating systems to instruct the systems on how to run a batch job or start a subsystem. The use of JCL involves the specification of job parameters through the JOB, EXEC, and DD statements to manage input, processing, and output tasks in a structured manner.

## Introduction to IBM Mainframe Job Control Language (Accelerator)

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, IBM Mainframe is a source system from which you can extract metadata through an IBM Mainframe Job Control Language (Accelerator) catalog source with Metadata Command Center.

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

**Note:** To enable and configure this catalog source, you need assistance from Informatica Professional Services. For more information, contact your account representative.

### Objects extracted

Metadata Command Center extracts the following metadata from an IBM Mainframe Job Control Language (Accelerator) source system:

- JCL Job
- JCL Step
- Calculation
- COBOL Program

- COBOL Program Instance
- JCL Procedure
- JCL Procedure Instance
- Partitioned Dataset
- Mainframe File Field
- Mainframe File Format

## CHAPTER 30

# IBM Netezza

See [IBM Netezza Sources](#) to learn how to register and configure IBM Netezza source systems 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 31

# IDERA ER/Studio Data Architect

See [IDERA ER/Studio Data Architect Sources](#) to learn how to register and configure IDERA ER/Studio Data Architect source systems 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 32

# Informatica Developer

See [Informatica Developer](#) to learn how to register and configure Informatica Developer source systems 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 33

# Informatica Intelligent Cloud Services

See [Informatica Intelligent Cloud Services](#) to learn how to register and configure Informatica Intelligent Cloud Services source systems 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 34

# Informatica PowerCenter

PowerCenter is an Informatica product that extracts data from multiple sources, transforms the data according to business logic, and loads the transformed data into different target databases. You can run connection-aware scans on PowerCenter sources.

### Objects extracted

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

- Folder
- Repository
- Workflow
- Workflow Instance
- Calculation
- Mapping
- Session
- Session Instance

### Prerequisites for configuring the PowerCenter catalog source

Perform the following tasks before you create the catalog source:

- If you installed the Secure Agent on a machine that doesn't host the Informatica domain, install the `pmrep` command line utility on the Secure Agent machine.
- Set the `INFA_HOME` variable to point to the location of the cmd utilities installed or the PowerCenter client location. The library path environment variable, `LD_LIBRARY_PATH`, should point to `$INFA_HOME/server/bin`.
- To perform a connection-aware scan, run the catalog source job. After the job completes, assign connections and run the job again. For more information about the types of connection scans and assigning connections, see *Administration*.

For more information about the prerequisites for connecting PowerCenter to Metadata Command Center, see <https://knowledge.informatica.com/s/article/What-are-the-prerequisites-for-conencting-the-PowerCenter-in-CDGC>.

### Permissions to configure the catalog source

- Configure the `Access Repository Manager` privilege for the user who accesses the PowerCenter repository.
- Configure read permission on the PowerCenter repository for the user account that you use to access the repository.
- Run the `pmrep ObjectExport` command to export the mappings from PowerCenter.



## Connection properties

On the **Registration** page in Metadata Command Center, specify values for the properties to connect to the PowerCenter repository. The following table shows the values for the properties to connect to the PowerCenter source system:

Property	Description
Pmrep path	The path to the pmrep command line program. For example, \$INFA_HOME/PowerCenter/server/bin/pmrep.
Repository name	The name of the PowerCenter repository service to connect to.
Domain host and port	The host name and port number of the Informatica domain. For example, Informatica_Domain_host>:<Port>.
Security domain	The name of the security domain to which the user belongs.
User	The name of the Informatica domain user who has access to the PowerCenter repository.
Password	The password for the Informatica domain user who has access to the PowerCenter repository.
Pmrep timeout in seconds	The timeout duration for the pmrep connect command. The default value is 600 seconds.

## Configuration parameters for metadata extraction

If a PowerCenter repository uses parameter files in sessions and workflows, you can configure Metadata Command Center to read the parameter files when you configure the PowerCenter catalog source. A parameter file contains all the parameters and variables and their associated values configured for workflows, worklets, or sessions in the PowerCenter repository. PowerCenter parameters can represent flat file sources, flat file lookups, flat file targets, relational connections, expressions at the transformation level, or objects in SQL overrides. The PowerCenter catalog source parses the parameter files and substitutes the parameter values to extract metadata for the flat file sources, flat file lookups, flat file targets, relational connections, and objects in SQL overrides.

To enable the PowerCenter catalog source to read parameter values from a parameter file, verify that the file has a .prm or .txt extension. The following example shows a sample parameters.prm file:

```
[Map_Param.WF:WF_Src_Tgt_map_param_case.ST:s_src_tgt_tbl_override_default_map_param]
$$Src_OwnName=MM_PERF6
$$Src_TblName=TBL_SAME_COL
$$Tgt_Tbl_Prefix=MM_PERF6
$$Tgt_TblName=INVENTORY_Q4_2005
[Param_lookup.WF:wf_M_LKP_schema_tble
$$LKP_SCHEMA=TEST_DATA
$$LKP_TBL=LKP_TBL_PARAM
[Param_lookup.WF:wf_M_LKP_schema_tbl_sess_param]
$Param_Lkp_Schema=TEST_DATA
$Param_Lkp_Tbl=LKP_TBL_PARAM[
Param_session.WF:wf_session_param.ST:s_session_param]
$Param_Schema_Name=CROSS_RESOURCE_LINKING_DUP
$Param_SrcTbl_Name=SRC_TBL_NAME_OVERRIDE_PARAM
$Param_TgtTbl_Name=TGT_TBL_NAME_OVERRIDE_PARAM
[Param_Sql_override.WF:wf_M_schema_table_map_parm_sql.ST:s_M_schema_table_map_parm_sql]
$$Map_Schema_Name=CROSS_RESOURCE_LINKING
$$Map_Tbl_Name=SRC_TBL_NAME_OVERRIDE_DUP
```

You can expand the **Catalog Source Configuration Options** in the **Metadata Extraction** tab of the **Configuration** page. Configure the following parameters for extracting metadata from a PowerCenter repository:

Parameter	Description
Explicit parameters	Specify additional Informatica parameters with overridden or missing definitions.
Parameter file path replacements	<p>Specify one or more Informatica file mappings to local files. The metadata extraction service uses local copies of files instead of connecting to an Informatica PowerCenter installation. This mapping is used with Informatica parameter files and with indirect source files. The values in the <b>Path</b> field are substituted by the values in the <b>Replacement</b> field in order to resolve workflow parameter file references.</p> <p>You can map the values and then copy the parameter file to the Secure Agent machine.</p> <p>For example, to map the variable file located at <code>\$PMRootDir/STG/ParamFiles/Param_File.txt</code> to the local file <code>/home/infa/Param_File.txt</code>, specify the values for the <b>Path</b> and <b>Replacement</b> fields.</p>

## Referenced source systems

If the source system references another source system, create a connection assignment in Metadata Command Center to view data lineage with endpoints. To create a connection assignment, create a connection based on the referenced source system, and then assign the connection to the catalog source.

**Note:** You can view the lineage with reference objects without creating a connection assignment. After connection assignment, you can view the actual objects.

You can connect to the following types of referenced source systems:

- Amazon Redshift. The catalog source must belong to the Database class type.
- Amazon S3. The catalog source must belong to the S3 Bucket class type.
- File System. The catalog source must belong to the File System class type.
- IBM Db2 for LUW. The catalog source must belong to the Database class type.
- Microsoft Azure Synapse Data Warehouse. The catalog source must belong to the Database class type.
- Microsoft SQL Server. The catalog source must belong to the Database class type.
- Oracle. The catalog source must belong to the Database class type.
- Snowflake. The catalog source must belong to the Database class type.
- Teradata Database. The catalog source must belong to the Database class type.

**Note:** For catalog sources that you created before the April 2023 release with connections assigned at the schema level, purge and run the catalog source again.

## CHAPTER 35

# JDBC

JDBC is a Java API to connect and interact with databases. You can use a JDBC connection to extract metadata from any source system for which a JDBC driver is available. Metadata Command Center certifies the following source systems from which you can extract metadata using the JDBC catalog source:

- Amazon DynamoDB
- Microsoft Azure Cosmos DB
- Marketo
- Microsoft Dynamics CRM
- MongoDB
- IBM Netezza
- Sybase ASE (Adaptive Server Enterprise)
- Sybase IQ (Intelligent Query)
- Workday
- Apache Cassandra
- SAP SuccessFactors
- NetSuite
- SingleStore
- IBM Db2 for z/OS

To extract metadata from these source systems, download the source-specific JDBC drivers and procure appropriate licenses. For information about using the JDBC drivers and licenses to extract metadata, see the [HOW TO: Use the JDBC drivers to extract metadata in Metadata Command Center](#) Knowledge article.

**Note:** MongoDB and Amazon DynamoDB are NoSQL databases that do not contain views and view columns.

### Objects extracted

You can use a JDBC connection to connect to any database to extract the following metadata objects:

- Database
- Schema
- View
- Table
- Column
- View Column

## Prerequisites for metadata extraction and data profiling

To use a JDBC connection to extract metadata and profile data, perform the following steps:

- Use the JDBC V2 connector to configure a connection in the Informatica Intelligent Cloud Services Administrator. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.
- Download the latest Type 4 JDBC driver version that your database supports from the third-party vendor site.  
For example, if you want to use the JDBC V2 connector to connect to Aurora MySQL, download the Aurora MySQL driver. Informatica has certified Aurora MySQL driver version 8.0.27 for JDBC V2 Connector.
- Install the Type 4 JDBC driver for the database on the Secure Agent machine and perform the following tasks:
  1. Navigate to the following directory on the Secure Agent machine:  
`<Secure Agent installation directory>/ext/connectors/thirdparty/`
  2. Create the following folder and copy the driver based on the type of source that you want to configure:  
`informatica.jdbc_v2/common`  
You can add multiple drivers for different source systems.
  3. Restart the Secure Agent.

## Configure permissions

To extract metadata and run profiles, you need account access and permissions to the JDBC source system.

### Permissions to extract metadata

Create a user account for the Informatica user to access the JDBC source system. Grant read permission to the new user account.

### Permissions to run data profiles

You do not need additional permissions to run data profiles.

## Data profiling using the JDBC V2 connection

Use the JDBC V2 connection to enable Secure Agent-based data profiling for Aurora MySQL, IBM Db2, PostgreSQL, and Oracle catalog sources. To enable Secure Agent-based data profiling for these catalog sources, download the JDBC driver from the respective third-party vendor sites and complete the prerequisite steps mentioned above.

Configure data profiling to run profiles on the metadata extracted from Aurora MySQL, IBM Db2, PostgreSQL, and Oracle catalog sources using the JDBC V2 connection. You can run data profiles on the following objects:

- Table
- View

After running the catalog source job, you can view the data profiling statistics in Data Governance and Catalog.

Amazon Aurora MySQL is a fully managed, MySQL-compatible, relational database management system (RDBMS) for the cloud offered by Amazon Web Services. The data profiling task runs profiles on the following data types for Aurora MySQL objects:

- Char
- Date

- Decimal
- Double
- Float
- Integer
- Smallint
- Bigint
- Time
- Text
- Mediumtext
- Tinytext
- Longtext
- Varchar
- Character varying

The data profiling task runs profiles on the following data types for IBM Db2 objects:

- Bigint
- Char(L)
- Date
- Decimal(P,S)
- Float
- Graphic
- Integer
- Numeric(P,S)
- Smallint
- Time
- Timestamp
- Varchar
- Vargraphic

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

- Smallint/Int2
- Int/Int4
- Bigint/int8
- Decimal
- Numeric
- Real/Float4
- Double/Float8
- Smallserial/Int2
- Serial
- Bigserial/Serial8

- Char
- Char(n)
- Varchar
- Varchar(n)
- Text
- Date
- Time
- Timestamp
- Boolean
- Ctext

#### Sampling type

Determine the sample rows on which you want to run the data profiling task. You can choose one of the following sampling types for a JDBC catalog source:

- All Rows
- Custom Query

**Note:** For Sybase ASE, you can only use the TOP clause to select sample rows to run the data profiling task. For example, SELECT TOP <N Rows>

#### Data classification for JDBC catalog sources

Configure data classification for JDBC catalog sources to classify and organize data in your organization. You can view the data classification results in Data Governance and Catalog.

#### Connection properties

When you configure a connection to JDBC in Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the JDBC connection properties for the database that you configure the connection for:

Property	Description
Connection Name	Name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	Description of the connection. Maximum length is 4000 characters.
Type	JDBC V2

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. This property is not supported by Data Ingestion and Replication.</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>For information about how to configure and use a secrets manager, see Secrets manager configuration in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent or serverless runtime environment.</p>
JDBC Driver Class Name	<p>Name of the JDBC driver class.</p> <p>For example, to connect to Aurora PostgreSQL, specify the following driver class name: <code>org.postgresql.Driver</code></p> <p>For more information about which driver class to use with specific databases, see the corresponding third-party vendor documentation.</p>
Connection String	<p>Connection string to connect to the database.</p> <p>Use the following format to specify the connection string: <code>jdbc:&lt;subprotocol&gt;:&lt;subname&gt;</code></p> <p>For example, the connection string for the Aurora PostgreSQL database type is <code>jdbc:postgresql://&lt;host&gt;:&lt;port&gt;[/dbname]</code>.</p> <p>For more information about the connection string to use with specific drivers, see the corresponding third-party vendor documentation.</p> <p>You can also connect to SSL-enabled Aurora PostgreSQL databases in mappings in advanced mode.</p>
User Name	The user name to connect to the database.
Password	The password to connect to the database.

## CHAPTER 36

# Kafka

Kafka is a distributed event streaming platform for data pipelines, streaming analytics, data integration, and mission-critical applications. Configure a Kafka catalog source to extract metadata from Apache Kafka, Confluent Platform, and Confluent Cloud source systems.

### Objects extracted

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

- Cluster
- Topic
- Field

### Supported file types

You can extract the following file types in Confluent Cloud and Apache Kafka from Kafka source system :

- Confluent Cloud. JSON, XML, CSV, and AVRO
- Apache Kafka. JSON, XML, and CSV

### Prerequisites for configuring the Kafka catalog source

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

### Connection properties

When you configure a connection to Kafka in Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

On the **Registration** page in Metadata Command Center, choose the connection and choose one of the following Kafka distributions to view the connection properties:

- Apache Kafka. A distributed event streaming platform on premises for data pipelines, streaming analytics, and data integration.
- Confluent Platform. An improved on premises distributed event streaming platform, based on Apache Kafka.
- Confluent Cloud. A fully managed streaming data service on cloud, based on Apache Kafka.



The following table describes the connection properties for the Apache Kafka and Confluent Platform distributions:

Property	Description
Runtime Environment	<p>Name of the runtime environment where you want to run tasks.</p> <p>Specify a Secure Agent, serverless, or elastic runtime environment for a mapping that runs on the advanced cluster.</p> <p>For more information about how to configure and use the runtime environments, see <i>Runtime Environments</i> in the Administrator help.</p>
Kafka Broker List	<p>Comma-separated list of the Kafka brokers.</p> <p>To list a Kafka broker, use the following format:</p> <p><code>&lt;HostName&gt;:&lt;PortNumber&gt;</code></p> <p><b>Note:</b> When you connect to a Kafka broker over SSL, you must specify the fully qualified domain name for the host name. Otherwise, the test connection fails with SSL handshake error.</p>
Retry Timeout	<p>Optional. Number of seconds after which the Secure Agent attempts to reconnect to the Kafka broker to read or write data.</p> <p>Default is 180 seconds.</p>
Kafka Broker Version	<p>Kafka message broker version. The only valid value is Apache 0.10.1.1 and above.</p>
Additional Connection Properties	<p>Optional. Comma-separated list of additional configuration properties of the Kafka producer or consumer.</p> <p>For a streaming ingestion and replication task, ensure that you set the <code>&lt;kerberos name&gt;</code> property if you configure <code>&lt;Security Protocol&gt;</code> as <code>SASL_PLAINTEXT</code> or <code>SASL_SSL</code>.</p> <p>For a database ingestion and replication task, if you want to specify a security protocol and properties, specify them here instead of in the <b>Additional Security Properties</b> property.</p> <p>For example: <code>security.protocol=SSL,ssl.truststore.location=/opt/kafka/config/kafka.truststore.jks,ssl.truststore.password=&lt;trustore_password&gt;</code>.</p>

If you choose the Confluent Cloud distribution, specify values for the following properties on the **Registration** page in Metadata Command Center:

Property	Description
Schema Registry URL	Specify a URL to access the schema registry. The URL syntax is <code>http://host1:port1</code> .
Confluent Cloud API Key	An API key to manage access and authentication to Confluent Cloud.
Confluent Cloud API Secret	An API secret for the Confluent Cloud API key.
Confluent Cloud Schema Registry API Key	An API key to interact with schema registry in Confluent Cloud.
Confluent Cloud Schema Registry API Secret	An API secret for the Confluent Cloud schema registry API key.

### Configuration parameters for metadata extraction

Expand the **Catalog Source Configuration Options** in the **Metadata Extraction** tab of the **Configuration** page. Configure the following parameters for extracting metadata from a Kafka source system:

Parameter	Description
Polling Strategy	Select one of the following polling strategies for sampling messages: <ul style="list-style-type: none"><li>- From Beginning</li><li>- From End</li></ul>

## CHAPTER 37

# MariaDB

See [MariaDB Sources](#) to learn how to register and configure MariaDB source systems 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 38

# Microsoft Azure Analysis Services

See [Microsoft Azure Analysis Services Sources](#) to learn how to register and configure Microsoft Azure Analysis Services source systems 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 39

# Microsoft Azure Blob Storage

See [Microsoft Azure Blob Storage](#) to learn how to register and configure Microsoft Azure Blob Storage source systems 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 40

# Microsoft Azure Data Factory

See [Microsoft Azure Data Factory Sources](#) to learn how to register and configure Microsoft Azure Data Factory source systems 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 41

# Microsoft Azure Data Lake Storage Gen2

See [Microsoft Azure Data Lake Storage Gen2 Sources](#) to learn how to register and configure Microsoft Azure Data Lake Storage Gen2 source systems 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 42

# Microsoft Azure SQL Server

See [Microsoft Azure SQL Server Sources](#) to learn how to register and configure Microsoft Azure SQL Server source systems 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 43

# Microsoft Azure SQL Server Script

See [Microsoft Azure SQL Server Script Sources](#) to learn how to register and configure Microsoft Azure SQL Server Script 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 44

# Microsoft Azure Synapse Analytics

See [Microsoft Azure Synapse Analytics Sources](#) to learn how to register and configure Microsoft Azure Synapse Analytics source systems 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 45

# Microsoft Azure Synapse Data Warehouse

Microsoft Azure Synapse Data Warehouse, formerly known as Azure SQL Data Warehouse, is a big data analytic service that queries and analyzes your data. Create a Microsoft Azure Synapse Data Warehouse catalog source to access data from Microsoft Azure SQL Data Warehouse.

### Objects extracted

The metadata extraction capability extracts the following objects from a Microsoft Azure Synapse Data Warehouse catalog source:

- Database
- Table
- Schema
- View
- Materialized View
- Function
- Stored Procedure
- Column
- External Table
- External Column

**Note:** If an incremental metadata extraction job includes a view, it extracts the corresponding tables even if the tables were extracted in previous runs.

**Note:** Effective in the November 2023 release, Metadata Command Center retrieves the database name from the source system instead of the Azure DW JDBC URL. If you extracted database objects before the November 2023 release, and the name of a database that you entered in the Azure DW JDBC URL uses a different case than the original database name, you might extract duplicate assets when you run the catalog source job again. To ensure that you extract the correct database structure, select **Delete** in the Metadata Change Option and rerun the catalog source job.

### Prerequisites

Use the Microsoft Azure Synapse SQL connector to connect to Microsoft Azure Synapse Data Warehouse source system. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.

## Configure permissions

Before you create a Microsoft Azure Synapse Data Warehouse catalog source, configure permissions for the Microsoft Azure SQL Server database user account that you use to connect to Microsoft Azure SQL Server. Metadata Command Center uses SQL Server authentication to connect to the Microsoft Azure SQL Server database. Verify that the user account you use to connect to Microsoft Azure SQL Server has an SQL Server login account.

### Permissions to extract metadata

Configure the VIEW DEFINITION and CONNECT permissions for the user account. These permissions allow you to view all schemas from where you can load metadata. For information about configuring permissions for the user account, see the Microsoft Azure Synapse documentation.

### Permissions to run data profiles

To perform data profiling on Microsoft Azure Synapse Data Warehouse, grant either the `db_owner` privilege or the following more granular privileges to the user to connect to Microsoft Azure SQL Data Warehouse and perform operations successfully:

- `EXEC sp_addrolemember 'db_datareader', '<user>';` // Alternately assign permission to the individual table.
- `EXEC sp_addrolemember 'db_datawriter', '<user>';` // Alternately assign permission to the individual table.
- `GRANT ALTER ANY EXTERNAL DATA SOURCE TO <user>;`
- `GRANT ALTER ANY EXTERNAL FILE FORMAT TO <user>;`
- `GRANT CONTROL TO <user>;` // To grant all permissions on the database.  
or  
`GRANT ALTER ANY SCHEMA TO <user>;` // To grant permissions only on the schema.
- `GRANT CREATE TABLE TO <user>;`

## Data profiling for Microsoft Azure Synapse Data Warehouse objects

Configure data profiling to run profiles on the metadata extracted from a Microsoft Azure Synapse Data Warehouse source system.

You can run data profiles on the following Microsoft Azure Synapse Data Warehouse objects:

- Tables
- External Tables created in the following file formats on the Microsoft Azure Serverless SQL pool:
  - Delimited text
  - Parquet
- Views

Configure the following data profiling properties in the **Data Profiling** tab of the **Configuration** page in Metadata Command Center:

Property	Description
Azure Blob Container	Name of the Blob container that is used to stage profiled data. Applies to the Azure Blob storage type.
ADLS FileSystem Name	Name of the file system that is used to stage profiled data. Applies to the ADLS Gen2 storage type.
Staging File Format	File format to use when you stage the profiled data. Select one of the following formats: <ul style="list-style-type: none"> <li>- Delimited Text. Select if the external table is created in the Delimited text file format.</li> <li>- Parquet. Select if the external table is created in the Parquet file format.</li> </ul> Applies to external tables created on the Microsoft Azure Serverless SQL pool.
Field Delimiter	Character used to separate fields in a file. Default is 0x1e. Non-printable characters must be specified as hexadecimal characters. <b>Note:</b> Use the field delimiter that you used while creating the external table in the Delimited text file format.
Quote Character	Specifies the quote character to skip when you read data from Microsoft Azure Synapse SQL. The quote character that you specify must not exist in the source table. If it exists, enter a different quote character value. Default is 0x1f. <b>Note:</b> Use the quote character that you used while creating the external table in the Delimited text file format.

You can view the profiling statistics in Data Governance and Catalog. The data profiling task runs profiles on the following data types for Microsoft Azure Synapse Data Warehouse objects:

- Bigint
- Bit
- Char
- Date
- Datetime
- Datetime2
- Decimal
- Float
- Int
- Nchar
- Nvarchar
- Real
- Smalldatetime
- Smallint
- Time
- Tinyint
- Uniqueidentifier
- Varchar

### Sampling type

Determine the sample rows on which you want to run the data profiling task. You can choose one of the following sampling types for a Microsoft Azure Synapse Data Warehouse catalog source:

- All Rows
- Limit N Rows
- Random N Rows

### Data classification for Microsoft Azure Synapse Data Warehouse objects

Configure data classification for Microsoft Azure Synapse Data Warehouse catalog sources to classify and organize data in your organization. You can view the data classification results in Data Governance and Catalog.

### Connection properties

When you configure a connection to Microsoft Azure Synapse Data Warehouse in Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the Microsoft Azure Synapse Data Warehouse connection properties:

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.
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. <b>Note:</b> If you're using this connection to apply data access policies through pushdown or proxy services, you cannot use the Secret Vault configuration option. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.

Property	Description
Runtime Environment	<p>The name of the runtime environment where you want to run tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</p> <p>Hosted Agent doesn't apply to mappings in advanced mode.</p> <p>For more information about how to configure and use the runtime environments, see <i>Runtime Environments</i> in the Administrator help.</p>

Property	Description
Azure DW JDBC URL	<p>The Microsoft Azure Synapse SQL JDBC connection string.</p> <p>Use the following string to connect to Microsoft Azure Synapse SQL:</p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;</pre> <p>You can include an authentication parameter in the connection string to specify the authentication type. You can configure the following authentication types to connect to Microsoft Azure Synapse SQL:</p> <ul style="list-style-type: none"> <li>- Microsoft SQL Server</li> <li>- Azure Active Directory</li> <li>- Managed Identity</li> <li>- Service Principal</li> </ul> <p>If you don't include an authentication parameter in the connection string, the Secure Agent uses Microsoft SQL Server authentication as the authentication type.</p> <p><b>Use the following string to connect to a serverless SQL pool in Microsoft Azure Synapse SQL:</b></p> <pre>jdbc:sqlserver://&lt;Serverless SQL endpoint&gt;:1433; database=&lt;Database&gt;;Authentication=ActiveDi rectoryMsi;</pre> <p><b>Connection string format for Microsoft SQL Server authentication</b></p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;</pre> <p><b>Connection string format for Azure Active Directory (AAD) authentication</b></p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;encrypt=true;trustServe rCertificate=false; hostNameInCertificate=*.database.windows.ne t;loginTimeout=30; Authentication=ActiveDirectoryPassword;</pre> <p><b>Connection string format for Service Principal authentication</b></p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;encrypt=true;trustServe rCertificate=false; hostNameInCertificate=*.database.windows.ne t;loginTimeout=30; Authentication= ActiveDirectoryServicePrincipal;</pre> <p><b>Connection string format for Managed Identity authentication</b></p> <pre>jdbc:sqlserver:// &lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;Authentication=ActiveDi rectoryMsi;</pre>



Property	Description
Azure DW JDBC Username	<p>User name to connect to the Microsoft Azure Synapse SQL account.</p> <ul style="list-style-type: none"> <li>- For AAD authentication, provide your AAD user name.</li> <li>- For Microsoft SQL server authentication, provide your SQL auth user name.</li> <li>- For service principal authentication, provide the application ID or client ID for your application registered in Azure Active Directory.</li> </ul> <p>This property doesn't apply to Managed Identity authentication.</p>
Azure DW JDBC Password	<p>Password to connect to the Microsoft Azure Synapse SQL account.</p> <ul style="list-style-type: none"> <li>- For AAD authentication, provide the password of the AAD user.</li> <li>- For Microsoft SQL server authentication, provide the password of SQL auth user.</li> <li>- For service principal authentication, provide the client secret for your application registered in the Azure Active Directory.</li> </ul> <p>This property doesn't apply to Managed Identity authentication.</p>
Azure DW Client ID	<p>Required if you want to use the user-assigned managed identity for Managed Identity Authentication to connect to Microsoft Azure Synapse SQL.</p> <p>The client ID of the user-assigned managed identity.</p> <p>If you use system-assigned managed identity, leave the field empty.</p>
Azure DW Schema Name	Name of the schema in Microsoft Azure Synapse SQL.

You can select Microsoft Azure Blob Storage or Microsoft Azure Data Lake Storage Gen2 as the Azure storage type to stage the data files. Default is Azure Blob. Select your preferred storage type and then configure the storage-specific parameters.

**Note:** If you connect to a serverless SQL pool, you must configure Microsoft Azure Data Lake Storage Gen2 as the storage type.

When you select Microsoft Azure Blob as the storage type, you can configure Shared Key Authentication as the authentication type to stage the files.

The following table describes the authentication type that you can configure for Microsoft Azure Blob storage:

Property	Description
Authentication Type	<p>Authentication type to connect to Microsoft Azure Blob storage to stage the files.</p> <p>You can configure Shared Key Authentication as the authentication type to stage the files.</p>

Shared Key Authentication uses the storage account name and account key to connect to Microsoft Azure Blob storage.

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

Property	Description
Azure Blob Account Name	Name of the Microsoft Azure Blob Storage account to stage the files.
Azure Blob Account Key	The Microsoft Azure Blob Storage access key to stage the files.
Container Name	The name of the container in the Azure Blob Storage account.

When you select Microsoft Azure Data Lake Storage Gen2 as the storage type, you can configure Shared Key Authentication, Service Principal Authentication, or Managed Identity Authentication as the authentication type to stage the files.

The following table describes the authentication type that you can configure for Microsoft Azure Blob storage:

Property	Description
Authentication Type	Authentication type to connect to Azure storage to stage the files. Select one of the following options: <ul style="list-style-type: none"><li>- Shared Key Authentication</li><li>- Service Principal Authentication</li><li>- Managed Identity Authentication</li></ul> For more information on how to configure the authentication types, see <a href="#">Setting up authentication to connect to Microsoft Azure Synapse SQL</a> .

Shared Key Authentication uses the storage account name and account key to connect to Microsoft Azure Data Lake Storage Gen2.

**Note:** You cannot select shared key authentication type when you connect to a serverless SQL pool.

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

Property	Description
ADLS Gen2 Storage Account Name	Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.
ADLS Gen2 Account Key	The Microsoft Azure Data Lake Storage Gen2 access key to stage the files.
File System Name	The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.

Service Principal Authentication uses the account name, client ID, client secret, and tenant ID to connect to Microsoft Azure Data Lake Storage Gen2.

The following table describes the basic connection properties for service principal authentication:

Property	Description
ADLS Gen2 Storage Account Name	Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.
Client ID	The client ID of your application. Enter the application ID or client ID for your application registered in the Azure Active Directory.
Client Secret	The client secret for your application.
Tenant ID	The directory ID or tenant ID for your application.
File System Name	The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.

Select Managed Identity Authentication to authenticate using system-assigned or user-assigned identities that are assigned to applications in Azure to access Azure resources in Microsoft Azure Data Lake Storage Gen2.

The following table describes the basic connection properties for managed identity authentication:

Property	Description
ADLS Gen2 Storage Account Name	Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.
Client ID	The client ID of your application. Enter the client ID for the user-assigned managed identity. If the managed identity is system-assigned, leave the field empty.
File System Name	The name of the file system in the Microsoft Azure Data Lake Storage Gen2 account.

### Configuration parameters for metadata extraction

Optionally, you can override default context values and job parameters on the **Configuration** tab.

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

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

Parameter	Description

Parameter	Description
Default variables values	Specify a default value for variables used in the programmable objects.
MetaTables Include Filter	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 <b>MetaTables Include Filter</b> parameter. This parameter prompts the database for the required metadata. Verify that the user has SELECT permissions for metatables. <b>Note:</b> Don't use this option to specify filters for tables that you want to include or exclude during the metadata extraction run.

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

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

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

## CHAPTER 46

# Microsoft Azure Synapse Data Warehouse Script

See [Microsoft Azure Synapse Data Warehouse Script Sources](#) to learn how to register and configure Microsoft Azure Synapse Data Warehouse Script source systems 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 47

# Microsoft Fabric Data Warehouse

See [Microsoft Fabric Data Warehouse Sources](#) to learn how to register and configure Microsoft Fabric Data Warehouse source systems 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 48

# Microsoft Fabric Data Lakehouse

See [Microsoft Fabric Data Lakehouse Sources](#) to learn how to register and configure Microsoft Fabric Data Lakehouse source systems 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 49

# Microsoft Fabric OneLake

See [Microsoft Fabric OneLake Sources](#) to learn how to register and configure Microsoft Fabric OneLake source systems 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 50

# Microsoft OneDrive

See [Microsoft OneDrive Sources](#) to learn how to register and configure Microsoft OneDrive source systems 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 51

# Microsoft Power BI

See [Microsoft Power BI Sources](#) to learn how to register and configure Microsoft Power BI source systems 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 52

# Microsoft Purview

See [Microsoft Purview Sources](#) to learn how to register and configure Microsoft Purview source systems 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 53

# Microsoft SharePoint Online

See [Microsoft SharePoint Online Sources](#) to learn how to register and configure Microsoft SharePoint Online source systems 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 54

# Microsoft SQL Server

See [Microsoft SQL Server Sources](#) to learn how to register and configure Microsoft SQL Server source systems 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 55

# Microsoft SQL Server Analysis Services

See [Microsoft SQL Server Analysis Services Sources](#) to learn how to register and configure Microsoft SQL Server Analysis Services source systems 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 56

# Microsoft SQL Server Integration Services

Microsoft SQL Server Integration Services (SSIS) is an ETL tool that extracts data from multiple sources, transforms, and loads them into different target databases. SSIS is a component of the Microsoft SQL Server database.

You can run connection-aware scans on Microsoft SQL Server Integration Services sources.

### Objects extracted

Metadata Command Center extracts the following objects from an SSIS source system:

- Calculation
- Data Task
- Database
- Folder
- Package
- Parameter
- Parameter Container
- Procedure Definition
- Procedure Instance
- Result Set
- Result Set Calculation
- Schema
- Script
- Statement

### Prerequisites for configuring the SSIS catalog source

To extract SSIS metadata using the Files mode, perform the following prerequisite tasks:

- Split input into logical applications, and then create a configuration for each logical application. For example, if you split the input into 10 logical applications based on lines of business, create 10 configurations. If a line of business comprises different areas such as treasury or accounting, create separate configurations for those areas also.

**Warning:** Jobs might run slowly or hang if you don't split input into logical applications.

- Choose one of the following options:
  - If you store the packages in a database, export the input files together with the corresponding DTSCONFIG, CONMGR, and PARAMS files. Export the input files to the Secure Agent machine using the dtutil utility. You get the utility during the Microsoft SQL Server installation.
  - If you store the package as files in the DTSX format, export the input files from the files system. You must also export the corresponding DTSCONFIG and CONMGR files.

To extract the SSIS metadata using the SSISDB mode, perform the following prerequisite tasks:

- Use the SQL Server connector to connect to Microsoft SQL Server Integration Services. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.
- If SSISDB has the packages deployed, then the catalog sources can connect to it to extract DTSX, CONMGR, and PARAMS files.
- For Windows authentication on a Linux machine, consider NTLM user authentication. The following example shows the connection string for a Microsoft SQL server database that uses NTLM authentication in a domain named informatica.com:

```
jdbc:sqlserver://
host01:1433;DatabaseName=SSISDB;integratedSecurity=true;authenticationScheme=ntlm;domain=informatica.com
```

To perform a connection-aware scan, run the catalog source job. After the job completes, assign connections and run the job again. For more information about the types of connection scans and assigning connections, see *Administration*.

## Permissions

To extract the SSIS project files from an SSISDB database in the SSISDB mode, grant permissions to perform the following operations on the SSISDB database:

- select on catalog.folders
- select on catalog.projects
- select on catalog.packages
- select on catalog.environments
- select on catalog.environment\_variables
- select on catalog.object\_parameters
- execute on catalog.get\_project procedure

To read specific folders, projects, or packages, assign one of the following roles or permissions:

- Membership to the ssis\_admin database role
- Membership to the sysadmin server role
- READ permission on the folders and projects

## Connection properties

On the **Registration** page in Metadata Command Center, you can choose to connect using the **Files** option or the **SSISDB** option.

### Files option

Use this option to extract metadata from files and directories in the file system. Specify the path to the source directory that contains the files that you want to extract. For example, `/home/ssis` may be the source directory on Linux.

### SSISDB option



To connect using the SSISDB option, configure a connection to SQL Server in the Informatica Intelligent Cloud Services Administrator. You can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the Microsoft SQL Server connection properties:

Property	Description
Runtime Environment	The execution platform that runs tasks. The runtime environment is either a Secure Agent or a serverless runtime environment.
User Name	Name of the Microsoft SQL Server user account that connects to the Microsoft SQL Server database.
Host	Host name of the machine where Microsoft SQL Server runs.
Port	Port number for the Microsoft SQL Server database engine service.
Code Page	Code page associated with the Microsoft SQL Server database.
Schema	A list of schema for which you want to extract metadata.
Database Name	Name of the Microsoft SQL Server database to connect to.

### Configuration parameters for metadata extraction

In the **Configuration Parameters** area, enter configuration parameters.

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

The following table describes the parameters that you can configure to extract metadata from an SSIS source system:

Parameter	Description
Default variables values file	Applicable for both <b>SSISDB</b> and <b>Files</b> reader module modes. Path to the file with default variables values. File format consists of [VARIABLES] and/or [FUNCTIONS] section.
External Connection Manager Files	Applicable if you connect using the <b>Files</b> reader module mode. Paths of connection manager files used by the SSIS packages. For example, enter C:\SSIS\Projects\MegaEtl\MegaDb.conmgr
DTSX Package to Project Param file mappings	Applicable if you connect using the <b>Files</b> reader module mode. If the path of a DTSX package matches the pattern specified in the <b>DTSX package pattern</b> field, then the variables that you define in the corresponding <b>Project Params file</b> field will be included. For example, enter /home/RootDir/ssis/*.dtsx=/home/RootDir/ssis/Project.params

Parameter	Description
Read parameters from SSISDB	Advanced parameter. Applicable if you connect using the <b>SSISDB</b> reader module mode. Determines whether to read parameters from SSISDB. Select one of the following options: <ul style="list-style-type: none"> <li>- Yes. Reads project and package parameters from SSISDB.</li> <li>- No. Doesn't read project and parameters from SSISDB.</li> </ul>
Expert parameter	This property appears when you click <b>Show Advanced</b> . Use expert parameters when it is recommended by Informatica Global Customer Support.

## Referenced source systems

If the source system references another source system, create a connection assignment in Metadata Command Center to view data lineage with endpoints. To create a connection assignment, create a connection based on the referenced source system, and then assign the connection to the catalog source.

**Note:** You can view the lineage with reference objects without creating a connection assignment. After connection assignment, you can view the actual objects.

You can connect to the following types of referenced source systems:

- Oracle. The catalog source must belong to the Database class type.
- Microsoft SQL Server. The catalog source must belong to the Database class type.
- File System. The catalog source must belong to the File System class type.

**Note:** For catalog sources that you created before the April 2023 release with connections assigned at the schema level, purge and run the catalog source again.

## CHAPTER 57

# Microsoft SQL Server Reporting Services

Microsoft SQL Server Reporting Services (SSRS) is a server-based report generating software system. It is part of a suite of Microsoft SQL Server services. You can use SSRS to prepare interactive and printed reports. SQL administrators can connect to SQL databases and use SSRS tools to format SQL reports.

### Objects extracted

Metadata Command Center extracts the following objects from an SSRS source system:

- Folders
- Projects
- DataSets
- Fields
- Reports
- PISql DataSet Statements
- Calculations

**Note:** If you run catalog sources created prior to the July 2023 release with Retain as the **Metadata Change Option**, duplicate calculations appear in Data Governance and Catalog. To avoid duplicate calculations and to view complete lineage information, run catalog sources created prior to the July 2023 release with Delete as the **Metadata Change Option**.

### Permissions

Get a Report Server user with permission to view and download reports and shared data sources from the SSRS administrator. Depending on the scenario, you need to get the Report Builder Role and the Publisher Role or the System User Role.

### Connection properties

On the **Registration** page, you can choose to connect with one of the following SSRS reader modes:

**Note:** When you create a new catalog source, use the Web service reader mode. Use the Files reader mode only for backward compatibility. Don't use it when you create a new catalog source.

### Web service reader mode

Use this option to extract metadata from the SSRS Report Server. Enter the following properties to connect with the Web service reader mode:

Property	Description
Web Service URL	URL of the SSRS Report Server. For example: <code>http://&lt;DomainName&gt;/ReportServer/ReportService2010.asmx</code>
Web Service Domain	Domain name of the SSRS Report Server. For example: <code>domain01</code> You don't have to prefix a Windows domain.
Web Service Username	User name of the SSRS Report Server in the following format: <code>&lt;user name&gt;</code>
Web Service Password	Password of the SSRS Report Server in the following format: <code>&lt;password&gt;</code>

### Files reader mode

Use this option to extract metadata from files and directories in the file system. Specify the path to the Report XML files that you want to extract. Verify that the Secure Agent can access files in the directory. The following example shows the path to a source directory on Linux: `/home/ssrs/*.xml`

### Configuration parameters for metadata extraction

On the **Metadata Extraction** tab of the **Configuration** page, expand **Catalog Source Configuration Options** to configure the following parameters for extracting metadata from an SSRS source system:

Parameter	Description
Default variables values file	Path to the file with default variables values. File format consists of [VARIABLES] and/or [FUNCTIONS] section.

### Data classification for Microsoft SQL Server Reporting Services objects

Configure data classification for Microsoft SQL Server Reporting Services catalog sources to classify and organize data in your organization.

You can choose one of the following options:

- **Data Classification Rules.** Choose from predefined or custom data classifications.
- **Generated Data Classifications.** CLAIRE automatically generates data classifications for the data elements.

You can view the data classification results in Data Governance and Catalog.

For more information about data classifications, see *Data classification* in the Administration help.

### Glossary association

Enable glossary association and configure settings for the catalog source to automatically associate or recommend glossary terms as business names for data elements in technical assets.

The following table describes the settings:

Property	Description
Enable auto-acceptance	When enabled, this option automatically associates glossary terms with data elements based on the threshold limit that you specify. The automatically accepted glossary terms appear as business names of data elements in Data Governance and Catalog.
Confidence Score Threshold for Auto-Acceptance	Specify a percentage from 80 to 100 inclusive to set a threshold limit. If a glossary term matches a data asset within the threshold specified, Metadata Command Center automatically assigns the matching glossary term to the data element. The name and description of the glossary term with the highest confidence score appears as the name and description of the data element asset in Data Governance and Catalog.
Enable below-threshold recommendations	If you enable auto-acceptance, you can select this option to receive glossary association recommendations below the auto-acceptance threshold.
Confidence score threshold for recommendations	If you enable auto-acceptance, specify a percentage between 80% and the selected confidence score threshold for auto-acceptance. If you disable auto-acceptance, specify a percentage between 80% and 100%.
Assign business names and descriptions	Choose to automatically assign business names and descriptions to technical assets.
Keep existing business names and descriptions	Applicable if you choose to assign business names and descriptions. 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.
Ignore Keywords	Choose to ignore specific parts of data elements when making recommendations. You can enter multiple unique prefix and suffix keywords. Keyword values are case insensitive.
Glossary Association Scope	Choose specific top-level business glossary assets to associate with technical assets. Selecting a top-level asset selects its child assets as well.
Use Abbreviation and Synonym Definitions	Enable this option to use a lookup table with abbreviations and synonyms to improve glossary association accuracy. To upload a lookup synonym file with the abbreviations and synonyms, select <b>Yes</b> to enable, and then click <b>Select</b> .

For more information about the glossary association settings, see the *Administrator* help.

## CHAPTER 58

# Microsoft SQL Server Script

See [Microsoft SQL Server Script Sources](#) to learn how to register and configure Microsoft SQL Server source systems 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 59

# MicroStrategy

See [MicroStrategy Sources](#) to learn how to register and configure MicroStrategy source systems 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 60

# MySQL

MySQL is an open-source relational database management system (RDBMS) to store and structure data.

### Objects extracted

Metadata Command Center extracts the following objects from a MySQL source system:

- Database
- Schema
- Table
- View
- Materialized view

### Prerequisites for configuring the MySQL catalog source

- Use the MySQL connector to connect to the MySQL source system in Administrator. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.
- To extract metadata from a MySQL source system, copy the MySQL JDBC driver, `mysql-connector-java-8.0.27.jar`, to the following location in your Secure Agent installation:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/ext/drivers/<MySQL driver>
```

Metadata Command Center supports the MySQL JDBC driver version 8.0.27.

- To run data profiling jobs, install the required MySQL ODBC drivers. For information about installing the drivers, see the following How-to Library article: *Configuring SSL for MySQL Connector in Cloud Data Integration*

### Configure permissions or access to MySQL

#### Permissions to extract metadata

This section addresses permissions for configuring an MySQL connection.

Grant permissions that allow you to perform the following operations:

- select on information\_schema.SCHEMATA
- select on information\_schema.TABLES
- select on information\_schema.COLUMNS
- select on information\_schema.TABLE\_CONSTRAINTS
- select on information\_schema.KEY\_COLUMN\_USAGE
- select on information\_schema.VIEWS

#### Permissions to run data profiles

To perform data profiling, grant Select permission on tables and views that you want to profile.



## Data profiling for MySQL objects

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

You can run data profiles on the following MySQL objects:

- Table
- View

### Sampling type

Determine the sample rows on which you want to run the data profiling task. You can choose one of the following sampling types for a MySQL catalog source:

- All Rows
- Limit N Rows
- Custom Query

## Data classification for MySQL objects

Configure data classification for MySQL catalog sources to classify and organize data in your organization. You can view the data classification results in Data Governance and Catalog.

## Connection properties

When you configure a connection to the MySQL source system in Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the MySQL connection properties:

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.
Type	Type of connection. Select MySQL from the list.
Runtime Environment	The execution platform that run tasks. The runtime environment is either a Secure Agent or a serverless runtime environment.
User Name	User name for the database login. The user name can't contain a semicolon.
Password	Password for the database login. The password can't contain a semicolon.
Host	Name of the machine that hosts the database server.
Port	Network port number used to connect to the database server. Default is 3306.
Database Name	Name of the MySQL database that you want to connect to.
Code Page	The code page of the database server.

Property	Description
Use SSL	<p>SSL attribute. Determines whether the Secure Agent establishes a secure connection to the MySQL database.</p> <p>When you select this option and the database server supports SSL, the Secure Agent establishes an encrypted connection. If the MySQL database server cannot configure SSL, the connection either fails or the Secure Agent establishes an unencrypted connection depending on whether you select <b>Require SSL</b>.</p> <p>If you do not select <b>Use SSL</b>, the Secure Agent attempts to establish an unencrypted connection.</p>
Verify Server Certificate	<p>SSL attribute. If you select both Use SSL and Verify Server Certificate, the client validates the server certificate that the database server sends.</p>
Require SSL	<p>SSL attribute. Applicable only if you selected <b>Use SSL</b>.</p> <p>If you select the <b>Require SSL</b> checkbox, and the MySQL database supports SSL, the Secure Agent establishes an SSL connection.</p> <p>If you select the <b>Require SSL</b> checkbox, and the MySQL database cannot configure SSL, the Secure Agent attempts to establish an SSL connection but fails.</p> <p>If you clear the <b>Require SSL</b> checkbox, and the MySQL database cannot configure SSL, the Secure Agent establishes an unencrypted connection.</p>
TLS Protocols	<p>SSL attribute. Applicable only if you selected <b>Use SSL</b>. The TLS protocols used for secure communication.</p> <p>You can select the following protocols:</p> <ul style="list-style-type: none"> <li>• TLSv1</li> <li>• TLSv1.1</li> <li>• TLSv1.2</li> </ul>
Trust Certificate Key Store	<p>JDBC attribute. The path and file name of the truststore file. You must prefix the file path with file colon (<code>file:</code>).</p> <p>For example, <code>file:C:\SSL\mysql_new\truststore</code></p>
Trust Certificate Key Store Password	<p>JDBC attribute. The password for the truststore file.</p>
Client Certificate Key Store	<p>JDBC attribute. The path and file name of the keystore file. You must prefix the file path with file colon (<code>file:</code>).</p> <p>For example, <code>file:C:\SSL\mysql_new\keystore</code></p>
Client Certificate Key Store Password	<p>JDBC attribute. The password to access the keystore file.</p>

## CHAPTER 61

# Oracle

See [Oracle Sources](#) to learn how to register and configure Oracle source systems 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 62

# Oracle Business Intelligence

See [Oracle Business Intelligence Sources](#) to learn how to register and configure Oracle Business Intelligence source systems 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 63

# Oracle Cloud Infrastructure GoldenGate

See [Oracle Cloud Infrastructure GoldenGate Sources](#) to learn how to register and configure Oracle Cloud Infrastructure GoldenGate source systems 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 64

# Oracle Cloud Object Storage

See [Oracle Cloud Object Storage Sources](#) to learn how to register and configure Oracle Cloud Object Storage source systems 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 65

# Oracle Data Integrator

See [Oracle Data Integrator Sources](#) to learn how to register and configure Oracle Data Integrator source systems 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 66

# Oracle PL/SQL Script

See [Oracle PL/SQL Script Sources](#) to learn how to register and configure Oracle PL/SQL database source systems 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 67

# Oracle SQL Loader

See [Oracle SQL Loader Sources](#) to learn how to register and configure Oracle SQL Loader source systems 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 68

# PostgreSQL

PostgreSQL is an open-source relational database management system (RDBMS) used as a data store or data warehouse for applications.

### Objects extracted

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

- Database
- Schema
- Table
- View
- Materialized View

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

- Stored Procedure

### Data profiling for PostgreSQL objects

Configure data profiling to run profiles on the metadata extracted from a PostgreSQL source system. You can run data profiles on the following PostgreSQL objects:

- Tables
- Views

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

PostgreSQL Data Type	Transformation Data Type	Description
Bigint/int8	Bigint	Precision 19, scale 0
Bigserial/Serial8	BigInt	Precision 19, scale 0
Boolean	String	Precision 6
Bytea	Binary	Precision 104857600
Char	String	Precision 1
Char(n)	String(n)	n<=10485760
Citext	Text	Precision 104857600

PostgreSQL Data Type	Transformation Data Type	Description
Date	Date/Time	Precision 29, scale 9
Decimal	Decimal	Precision 1 to 28, scale 0 to 28
Double/Float8	Double	Precision 15, scale 0
Int/Int4	Integer	Precision 10, scale 0
JSONB	String	Precision 104857600
Numeric	Decimal	Precision 1 to 28, scale 0 to 28
Real/Float4	Double	Precision 15, scale 0
Serial	Integer	Precision 10, scale 0
Smallint/Int2	Integer	Precision 10, scale 0
Smallserial/Int2	Integer	Precision 10, scale 0
Text	String	Precision 104857600
Time	Date/Time	Precision 29, scale 9
Timestamp	Date/Time	Precision 29, scale 9
Timestamp with time zone	Date/Time	Precision 29, scale 9
Timestamp without time zone	Date/Time	Precision 29, scale 9
Varchar	String	Precision 104857600
Varchar(n)	String(n)	n <=10485760

### Sampling type

Determine the sample rows on which you want to run the data profiling task. You can choose any of the following sampling types for a PostgreSQL catalog source:

- All rows
- Limit N
- Custom query

### Prerequisites for configuring the PostgreSQL catalog source

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

### Configure permissions or access to PostgreSQL

To extract metadata and run profiles, you need account access and permissions on the PostgreSQL source system.

## Permissions to extract metadata

Grant 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\_DATABASE
- 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\_MATVIEWS

To extract metadata from a table, you need to configure Select access on the table.

## Data classification for PostgreSQL objects

Configure data classification for PostgreSQL catalog sources to classify and organize data in your organization. You can view the data classification results in Data Governance and Catalog.

## Connection properties

When you configure a connection to the PostgreSQL source system in Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the PostgreSQL connection properties:

Property	Description
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, or serverless runtime environment. Select a Secure Agent, Hosted Agent, serverless, or elastic runtime environment. For more information about how to configure and use the runtime environments, see <i>Runtime Environments</i> in the Administrator help.
Host Name	Host name of the PostgreSQL server to which you want to connect.
Port	Port number for the PostgreSQL server to which you want to connect. Default is 5432.
Database Name	The PostgreSQL database name.
Schema Name	The schema name. If you don't specify the schema name, all the schemas available in the database are listed when you import the source object.

Property	Description
User Name	User name to access the PostgreSQL database.
Password	Password for the PostgreSQL database user name.
Encryption Method	<p>Determines whether the data exchanged between the Secure Agent and the PostgreSQL database server is encrypted. Select one of the following encryption methods:</p> <ul style="list-style-type: none"> <li>- noEncryption. Establishes a connection without using SSL. Data is not encrypted.</li> <li>- SSL. Establishes a connection using SSL. Data is encrypted using SSL. If the PostgreSQL database server cannot configure SSL, the connection fails.</li> <li>- requestSSL. Attempts to establish a connection using SSL. If the PostgreSQL database server cannot configure SSL, the Secure Agent establishes an unencrypted connection.</li> </ul> <p>Default is noEncryption</p>
Validate Server Certificate	<p>Determines if the Secure Agent validates the server certificate sent by the PostgreSQL database server. If you specify the Host Name In Certificate property, the Secure Agent also validates the host name in the certificate.</p> <p>Select this option to validate the server certificate.</p>
Truststore	<p>This property applies if you select the Validate Server Certificate option.</p> <p>The path and name of the truststore file, which contains the list of the Certificate Authorities (CAs) that the PostgreSQL client trusts.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;TrustStore_filename&gt;</pre>
Truststore Password	<p>This property applies if you select the Validate Server Certificate option.</p> <p>The password to access the truststore file that contains the SSL certificate.</p>
Host Name In Certificate	<p>Optional when you select the Validate Server Certificate option.</p> <p>A host name for providing additional security. The Secure Agent validates the host name included in the connection with the host name in the SSL certificate.</p>
Keystore	<p>This property applies when client authentication is enabled on the PostgreSQL database server.</p> <p>The path and the file name of the key store. The keystore file contains the certificates that the PostgreSQL client sends to the PostgreSQL server in response to the server's certificate request.</p> <p>For the serverless runtime environment, specify the following certificate path in the serverless agent directory:</p> <pre>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/ &lt;KeyStore_filename&gt;</pre>
Keystore Password	<p>This property applies when client authentication is enabled on the PostgreSQL database server.</p> <p>The password for the keystore file required for secure communication.</p>
Key Password	<p>This property applies when client authentication is enabled on the PostgreSQL database server.</p> <p>Required when individual keys in the keystore file have a different password than the keystore file.</p>

Property	Description
Additional Connection Properties	Additional connection parameters that you want to use. Provide the connection parameters as semicolon-separated key-value pairs.
Crypto Protocol Versions	Required if you select SSL or requestSSL as the encryption method. A cryptographic protocol or a list of cryptographic protocols to use with an encrypted connection. You can select from the following protocols: <ul style="list-style-type: none"> <li>- SSLv3</li> <li>- TLSv1</li> <li>- TLSv1_1</li> <li>- TLSv1_2</li> </ul>

### Configuration parameters for metadata extraction

Optionally, you can override default context values and job parameters on the **Configuration** tab.

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

The following table describes the configuration parameters 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	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 <b>MetaTables Include Filter</b> parameter. This parameter prompts the database for the required metadata. Verify that the user has SELECT permissions for metatables. <b>Note:</b> Don't use this option to specify filters for tables that you want to include or exclude during the metadata extraction run.

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

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

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

## CHAPTER 69

# Qlik Sense

Qlik Sense is a business intelligence and visual analytics platform that supports a range of use cases including centrally deployed analytic applications, dashboards, and embedded analytics within a scalable framework.

### Objects extracted

Metadata Command Center extracts the following objects from a Qlik Sense source system:

- Application
- Application Model
- Column
- Condition
- Connection
- Connection Schema
- Database Schema
- Dimension
- Dimension Attribute
- Document
- Expression
- Field
- File
- File Directory
- Folder
- Hub
- Measure
- Measure Attribute
- QVD
- QVD Model
- Source Column
- Source Table
- Story
- Stream
- System Field

- Table

## Prerequisites for configuring the Qlik Sense catalog source

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 Qlik Sense certificate to the same machine where the Secure Agent is running. You can provide the path to this certificate on the **Registration** page in Metadata Command Center.
- To access assets in the Qlik Sense source system, perform one of the following steps:
  - Assign a predefined Audit Admin role to the Qlik Sense user.
  - Create a custom role that has read access to apps, app objects, streams, and data connections and assign it to the Qlik Sense user.

For more information, see the following Knowledge Base article:

[HOW TO: Create a role and assign it to a user in Qlik Sense.](#)

## Connection properties

On the **Registration** page in Metadata Command Center, enter values for the following connection properties:

Property	Description
Engine API URL	The Qlik Sense server URL to connect to the Qlik API Engine.
User directory	User directory of the Qlik Sense server.
User	Qlik Sense user name to authenticate to the Qlik Sense server.
Certificate	Location of the client certificate required for authentication to the Qlik Sense server.
Certificate Password	Password of the Qlik Sense client certificate. Specify the password if the Qlik Sense client certificate is generated with a password.

## Configuration parameters for metadata extraction

Expand the **Catalog Source Configuration Options** in the **Metadata Extraction** tab on the **Configuration** page. Configure the following additional parameters to extract metadata from a Qlik Sense source system:

Property	Description
Incremental Import	Choose whether you want to extract the metadata that has changed since the previous run or extract complete metadata. Select one of the following options: <ul style="list-style-type: none"> <li>- True. Extracts only the changes to the metadata since the last metadata extraction job.</li> <li>- False. Extracts the complete metadata.</li> </ul>
Log Folder	<p>The path to the Qlik Sense log folder.</p> <p>Use this option if you are extracting metadata from a source system that contains dynamic information such as subroutines, loops, and variable definitions. The log files in the log folder are used to extract complete lineage.</p> <p>If the log folder on the Qlik Sense machine is accessible to the Secure Agent, you can specify the direct path to the folder. If the folder is not accessible, you can copy the files to a log folder accessible to the Secure Agent.</p> <p>To enter multiple paths, use the <code>-cluster.log.folder</code> miscellaneous option.</p>



Property	Description
QVD Folder	<p>The path to the QVD folder stored in the QVD server.</p> <p>Use this option if you are extracting metadata from a source system that contains parameterized connections.</p> <p>To enter multiple paths, use the <code>cluster.qvd.folder</code> miscellaneous option.</p>

Property	Description
Worker Threads	<p>Optional. The number of worker threads to process metadata asynchronously.</p> <p>You can enter a positive integer value.</p> <p>If you don't enter a value, Metadata Command Center computes and assigns a value between one and six based on the Java Virtual Machine (JVM) architecture and the number of available CPU cores on the Secure Agent machine.</p>
Miscellaneous Options	<p>You can specify the following additional options to pass at runtime:</p> <pre>-database.type ORACLE -log.notavailable -file.path [qlik server file path]=[agent file path] -m 4G -customXMLLocation [path to xmi files]</pre> <ul style="list-style-type: none"> <li>-m. Specify the memory size required to run the metadata extraction job. For example, enter -m 4G. The default memory size is 1GB.</li> <li>-database.type. Specify the list of connection database types as comma-separated value pairs. For example, enter -database.type ORACLE</li> </ul> <p>If databases are accessed via generic ODBC connections, then specify the exact database type in order to properly parse the database-specific SQL syntax for lineage.</p> <ul style="list-style-type: none"> <li>-log.notavailable. Specify this option if have not entered any value for the Log Folder property. If you are extracting metadata from a source system that contains dynamic metadata such as subroutines, loops, and variable definitions, then the Qlik document execution log files are required because the dynamic metadata cannot be directly extracted from the Qlik scripts. In such cases, some critical metadata for lineage are missing.</li> </ul> <p>This option lets you extract metadata even if the log folder path is not available.</p> <ul style="list-style-type: none"> <li>-cluster.log.folder. If you need to enter more than one log folder path, specify this option to enter the paths.</li> </ul> <p>For example,</p> <pre>-cluster.log.folder d:\cluster1\ -cluster.log.folder d:\cluster2\</pre> <ul style="list-style-type: none"> <li>-cluster.qvd.folder If you need to enter more than one QVD folder path, specify this option to enter the paths.</li> </ul> <p>For example, you can specify multiple paths for multiple cluster configurations:</p> <pre>-cluster.qvd.folder d:\cluster1\ -cluster.qvd.folder c:\cluster2\</pre> <ul style="list-style-type: none"> <li>-file.path. A Qlik document contains statements, such as INCLUDE, STORE, or LOAD, which operate with the file path. If the original file path is not accessible, then use this option to replace a portion of the original file path with a new one by specifying multiple file path options. For example, -file.path [qlik server file path]=[agent file path].</li> </ul> <p>The catalog source applies multiple file path options in the order in which they are specified.</p> <ul style="list-style-type: none"> <li>-directory. A Qlik document DIRECTORY statement is used to set the directory path for subsequent LOAD statements.</li> </ul> <p>If this directory is inaccessible, then use a DIRECTORY statement to redirect it to another directory. Copy the DIRECTORY statement from a Qlik document execution log, add =, and specify the path to another directory. For example, if folder c:\folder1 is redirected to folder d:\folder2, then enter -directory "c:\folder1=d:\folder2".</p> <p>When the path after the DIRECTORY statement is empty, such as -directory "[]=d:\folder2", then all DIRECTORY statements are redirected to the specified directory.</p> <ul style="list-style-type: none"> <li>-customXMLLocation. Specify this option if you want to load the XMI files that are generated when you run a metadata extraction job. Specify the location where the XMI files are stored. For example:</li> </ul> <pre>-customXMLLocation E:\Dev\apps\Metadata_Foundation_Agent\workspaces\QlikSense</pre>

Property	Description
	<ul style="list-style-type: none"> <li>- <code>-connection.map</code>. Specify this option if you want to map a source path to a destination path. You can use this option when different paths point to the same object. For example:  <code>-connection.map "M:\=C:\data" -connection.map "N:\=C:\data"</code>  Here, directory C:\data is referred to by multiple network drives like M: and N: on Windows.</li> <li>- <code>-websocket.timeout</code> Specify the time in seconds that the import bridge must wait for a websocket response. Default is 30.</li> </ul> <p>When the Qlikshare files are on a Windows machine and the Secure Agent runs on a Linux machine, you need to copy the QVD and log files from Windows to the Linux machine. To view the complete lineage in Data Governance and Catalog and for the connection assignments to work, specify the following options to pass at runtime:</p> <ul style="list-style-type: none"> <li>- <code>-file.path "&lt;location where QVD and log files are available on the Windows machine&gt;=&lt;location where QVD and log files are available on the Linux machine&gt;"</code></li> <li>- <code>-directory "&lt;all directories&gt;=&lt;location where QVD and log files are available on the Linux machine&gt;"</code></li> <li>- <code>-connection.map "&lt;location where QVD and log files are available on the Linux machine&gt;=&lt;location where QVD and log files are available on the Windows machine&gt;"</code></li> </ul> <p>For example:</p> <pre>-file.path "C:\QlikShare\=/data/qlikshare/" -directory "[]=/data/qlikshare/" -connection.map "/data/qlikshare/= C:\QlikShare\"</pre>

## Referenced source systems

If the source system references another source system, create a connection assignment in Metadata Command Center to view data lineage with endpoints. To create a connection assignment, create a connection based on the referenced source system, and then assign the connection to the catalog source.

**Note:** You can view the lineage with reference objects without creating a connection assignment. After connection assignment, you can view the actual objects.

You can assign the following source systems as endpoint catalog sources:

Source system	Object class type
Oracle	Database
Microsoft SQL Server	Database
Snowflake	Database
Amazon S3	Bucket
File System	File Path

## CHAPTER 70

# Qlik Sense Cloud

See [Qlik Sense Cloud Sources](#) to learn how to register and configure Qlik Sense Cloud source systems 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 71

## QlikView

QlikView is flexible business intelligence tool to connect to data and create reports. Create a QlikView catalog source to extract metadata from the QlikView source system.

### Objects extracted

Metadata Command Center extracts the following objects from a QlikView source system:

- Application
- Button Field
- Column
- Condition
- Connection
- Connection Model
- Connection Schema
- Database Schema
- Document
- Expression
- Field
- File
- File Directory
- Folder
- Group
- Measure
- QVD
- QVD Model
- QVW
- QVW Model
- Source Column
- Source File
- Source Table
- System Field
- System Variable
- Table

- Text Field
- Variable

### Prerequisites for configuring the QlikView catalog source

- Install the Secure Agent on a Windows machine to configure a QlikView catalog source. Ensure that you install the QlikView Desktop tool on the same machine where the Secure Agent is running. Use the same user name to install the Secure Agent and the QlikView Desktop tool. The user needs to have full access control on the machine.
- Before you run a QlikView catalog source job, close all QlikView instances and check the Task Manager on the Windows machine to confirm that there are no QlikView processes running. The QlikView catalog source job may get stuck if there are any QlikView processes running on the same machine where the Secure Agent is running.
- The user that starts the Secure Agent must have the licensed edition of QlikView Desktop. The catalog source job does not extract any metadata from the QlikView source system if you are using the QlikView Desktop Personal Edition. If you don't have a QlikView Desktop license, you must lease a license from QlikView Server to the Qlik Client. For information about leasing the QlikView Desktop License, see [Knowledge Base article 000196172](#).

### Connection properties

On the **Registration** page in Metadata Command Center, enter the path to the directory from which you want to import the QlikView documents. This directory should be present in the same machine where the Secure Agent is running.

### Configuration parameters for metadata extraction

Expand the **Catalog Source Configuration Options** in the **Metadata Extraction** tab on the **Configuration** page. Configure the following additional parameters to extract metadata from a QlikView source system:

Property	Description
Miscellaneous Options	<p>You can specify the following additional options to pass at runtime:</p> <ul style="list-style-type: none"> <li>-database.type ORACLE -log.notavailable -file.path [qlik server file path]=[agent file path] -m 4G -customXMLLocation [path to xmi files]</li> <li>-database.type. Specify the default database connection without any connection name. For example, enter -database.type ORACLE</li> </ul> <p>If specifying multiple database connections, enter each database type using the associated connection name. For example, enter -database.type MyConnectionName=ORACLE</p> <ul style="list-style-type: none"> <li>-log.notavailable. Specify this option if you are extracting metadata from a source system that contains dynamic metadata such as subroutines, loops, and variable definitions. The Qlik log files are required because the dynamic metadata cannot be directly extracted from the Qlik scripts. In such cases, some critical metadata for lineage are missing.</li> </ul> <p>This option lets you extract metadata even if the log folder path is not available.</p> <ul style="list-style-type: none"> <li>-file.path. Use this option to replace a portion of the original file path with a new one by specifying multiple file.path options. For example, enter -file.path [qlik server file path]=[agent file path]</li> <li>-m. This option lets you specify the memory size required to run the metadata extraction job. For example, enter -m 4G</li> <li>-customXMLLocation. Specify this option if you want to load the XML files that are generated when you run a metadata extraction job. Specify the location where the XML files are stored. For example: -customXMLLocation E:\Dev\apps\Metadata_Foundation_Agent\workspaces\QlikView</li> </ul>

## Referenced source systems

If the source system references another source system, create a connection assignment in Metadata Command Center to view data lineage with endpoints. To create a connection assignment, create a connection based on the referenced source system, and then assign the connection to the catalog source.

**Note:** You can view the lineage with reference objects without creating a connection assignment. After connection assignment, you can view the actual objects.

You can assign the following source systems as endpoint catalog sources:

Source system	Object class type
Microsoft SQL Server	Database
Oracle	Database

## CHAPTER 72

# Salesforce

Salesforce is a Customer Relationship Management (CRM) software solution that brings companies and customers together. It has many applications which support various features such as lead generation, lead acquisition, sales tracking, and deal closure. It is designed to manage the data of an organization around customers and sales.

Salesforce offers the following features:

- Contact management
- Opportunity management
- Customer engagement
- Lead management
- Partner management
- Email integration
- Sales forecasting

Salesforce provides version 53 of the REST API that the Salesforce catalog source uses.

### Objects extracted

The Salesforce catalog source extracts the following objects from a Salesforce source system:

- Organization
  - List View
  - List View Column
- Trigger
- Object
- Field

**Note:** If there is a duplicate global list view that is not associated with a specific object in the source system, then only one global list view is extracted.

### Prerequisites for configuring the Salesforce catalog source

- Use the Salesforce connector to connect to Salesforce source system. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.
- To extract metadata from a Salesforce source system through REST API, verify that you have access to Salesforce REST API v53.
- To set up authorization to restrict access to your organization's protected resources, use the OAuth 2.0 Refresh Token Flow for Renewed Sessions. For more information about this authorization method, see the Salesforce documentation on OAuth 2.0 Refresh Token Flow for Renewed Sessions.



## Configure permissions or access to Salesforce

Before you configure a Salesforce catalog source, configure the required permissions. Metadata Command Center uses OAuth authentication to connect to Salesforce.

### Permissions to extract metadata

To extract metadata, assign the following permissions:

- **Modify All Data.** Allows you to extract all objects. If you don't want Salesforce to modify all data, select **View All Data**.

**Note:** If you select **View All Data**, you might not extract some objects. For more information, see the [Knowledge Base article 000196069](#).

- **API Enabled.** Allows you to access the data of your organization through API requests to your Salesforce instance.

### Permissions to run data profiles

You don't need additional permissions to run data profiles. You can run data profiles with permissions used to extract metadata.

## Connection properties

When you create a connection to Salesforce in Administrator, connect using the OAuth connection type. After you configure the connection in Administrator, you can view the connection properties on the **Registration** page in Metadata Command Center.

### OAuth connection type

The following table describes the Salesforce connection properties for an OAuth connection type:

Property	Description
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent, Hosted Agent, serverless, or elastic runtime environment. Hosted Agent doesn't apply to mappings in advanced mode. For more information about how to configure and use the runtime environments, see <i>Runtime Environments</i> in the Administrator help.
OAuth Consumer Key	The consumer key to generate a refresh token.
OAuth Consumer Secret	The consumer secret to generate a refresh token.
OAuth Refresh Token	The refresh token that you generated using the SFDC OAuth 2.0 tool. For more information about how to generate the OAuth refresh token, see the <i>Before you begin</i> section.
Service URL	URL of the Salesforce service endpoint. For example: <code>https://login.salesforce.com/services/Soap/u/63.0</code> You can use any Salesforce API version up to 63.0, except the versions 58.0 and 61.0. Maximum length is 100 characters. When you edit the service URL for an existing OAuth connection, you need to re-enter the consumer key, consumer secret, and refresh token.

Property	Description
Service End Point	URL pointing to the Salesforce instance.
OAuth Access Token	Specify the token generated using the Informatica OAuth utility.

## Data profiling for Salesforce objects

Configure data profiling to run profiles on the metadata extracted from a Salesforce source system. You can run data profiles on the following Salesforce objects:

- Standard Objects
- Custom Objects

You can view the profiling statistics in Data Governance and Catalog. Data Governance and Catalog profiles only those Salesforce Standard objects that can be retrieved and queried.

**Note:** The data profiling task does not run profiles on List Views.

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

- URL
- STRING
- PHONE
- REFERENCE
- DATETIME
- BOOLEAN
- ID
- EMAIL
- DOUBLE
- TEXT AREA
- DATE
- CURRENCY
- PICKLIST
- INT
- PERCENT
- COMPLEX VALUE
- ANY TYPE
- JSON
- LONG

### Sampling type

Determine the sample rows on which you want to run the data profiling task. You can choose one of the following sampling types for a Salesforce catalog source:

- All Rows
- Limit N Rows

- Custom Query

## Data classification for Salesforce objects

Configure data classification for Salesforce catalog sources to classify and organize data in your organization.

You can choose one of the following options:

- **Data Classification Rules.** Choose from predefined or custom data classifications.
- **Generated Data Classifications.** CLAIRE automatically generates data classifications for the data elements.

**Note:** Salesforce source systems can contain ambiguous data with technical field names. To ensure that CLAIRE generates accurate data classifications, it uses the extracted **Label** attribute to generate data classifications.

You can view the data classification results in Data Governance and Catalog.

For more information about data classifications, see *Data classification* in the Administration help.

## Glossary association

Enable glossary association and configure settings for the catalog source to automatically associate or recommend glossary terms as business names for data elements in technical assets.

The following table describes the settings:

Property	Description
Enable auto-acceptance	When enabled, this option automatically associates glossary terms with data elements based on the threshold limit that you specify. The automatically accepted glossary terms appear as business names of data elements in Data Governance and Catalog.
Confidence Score Threshold for Auto-Acceptance	Specify a percentage from 80 to 100 inclusive to set a threshold limit. If a glossary term matches a data asset within the threshold specified, Metadata Command Center automatically assigns the matching glossary term to the data element. The name and description of the glossary term with the highest confidence score appears as the name and description of the data element asset in Data Governance and Catalog.
Enable below-threshold recommendations	If you enable auto-acceptance, you can select this option to receive glossary association recommendations below the auto-acceptance threshold.
Confidence score threshold for recommendations	If you enable auto-acceptance, specify a percentage between 80% and the selected confidence score threshold for auto-acceptance. If you disable auto-acceptance, specify a percentage between 80% and 100%.
Assign business names and descriptions	Choose to automatically assign business names and descriptions to technical assets.
Keep existing business names and descriptions	Applicable if you choose to assign business names and descriptions. 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.
Ignore Keywords	Choose to ignore specific parts of data elements when making recommendations. You can enter multiple unique prefix and suffix keywords. Keyword values are case insensitive.

Property	Description
Glossary Association Scope	Choose specific top-level business glossary assets to associate with technical assets. Selecting a top-level asset selects its child assets as well.
Use Abbreviation and Synonym Definitions	Enable this option to use a lookup table with abbreviations and synonyms to improve glossary association accuracy. To upload a lookup synonym file with the abbreviations and synonyms, select <b>Yes</b> to enable, and then click <b>Select</b> .

**Note:** Salesforce source systems can contain ambiguous data with technical field names. To generate accurate glossary associations, CLAIRE uses the extracted Label attribute for such technical field names.

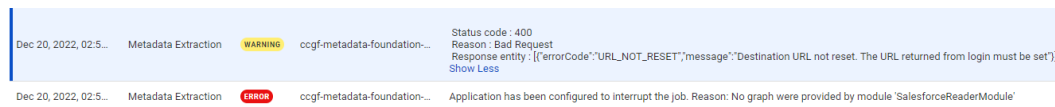
For more information about the glossary association settings, see the *Administrator* help.

### Troubleshooting the "FDC scanner fails with "Cannot retrieve the organization" in CDGC" error.

In Metadata Command Center, the Salesforce catalog source with the OAuth connection type fails during the Test connection stage with the following error:

```
Unexpected error occurred: Cannot retrieve the organization for
\"https://login.salesforce.com/services/data/v53.0/query/?
q=SELECT+Name+FROM+Organization\", no graphs created"
```

The following image shows the error on the user interface:



This issue occurs if you had provided [login.salesforce.com](https://login.salesforce.com) as the service URL in the Salesforce catalog source connection configuration. You can use the service URL such as [login.salesforce.com](https://company-abc.my.salesforce.com) for testing connections, but not for REST API calls.

To resolve this issue, use the actual service URL in the Salesforce catalog source connection configuration.

To identify the actual service URL, perform the following steps:

1. Log in to your account with the <https://login.salesforce.com/> URL.  
The service URL appears. For example, <https://company-abc.my.salesforce.com>.
2. Copy the service URL from the URL bar.  
The service URL is specific to the credentials that you use to connect to the Salesforce REST API, and based on which the standard login or OAuth keys are generated.

**Note:** The service URL configured in Administrator should have the following structure:  
<https://company-abc.my.salesforce.com/services/Soap/u/55.0>.

The following image shows a reference service URL:

## Salesforce Connection Properties

Runtime Environment: XXXXXXXXXX

Salesforce Connection Type: OAuth

OAuth Consumer Key \*\*\*\*\*

OAuth Consumer Secret \*\*\*\*\*

OAuth Refresh Token \*\*\*\*\*

Service URL: [https://\[redacted\].my.salesforce.com/services/Soap/u/55.0](https://[redacted].my.salesforce.com/services/Soap/u/55.0)

Service End Point:

OAuth Access Token:

## CHAPTER 73

# SAP Analytics Cloud - Preview catalog source

See [SAP Analytics Cloud Sources](#) to learn how to register and configure SAP Analytics Cloud source systems 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 74

# SAP BusinessObjects

SAP BusinessObjects is a business intelligence tool to connect to data for data reporting, visualization, and sharing. Configure an SAP BusinessObjects catalog source to extract metadata from SAP BusinessObjects.

### Objects extracted

Metadata Command Center extracts the following objects from an SAP BusinessObjects source system:

- Alias Column
- Alias Table
- Analytic Model
- Analytic Report
- Business Layer View
- Category
- Cell
- Class
- Column
- Connection
- Connection Classifier
- Connection Feature
- Connection Folder
- Connection Model
- Constants
- Context
- Contexts
- Crystal Report
- Crystal Report Model
- Custom Hierarchies
- Dashboard
- Data Provider
- Data Providers
- Database Connection
- Default Hierarchies
- Derived Table

- Desktop Intelligence Document
- Desktop Intelligence Model
- Detail
- Detail Result
- Detail Variable
- Dimension
- Dimension Result
- Dimension Variable
- Discovered Tables
- Enterprise Folder
- Favorite Folder
- Field
- File
- File Connection
- Filter
- Folder
- Formula Fields
- Formulas
- Group Name Fields
- Hierarchy
- Inbox
- Join
- Key
- List of Values
- Logical Column
- Measure
- Measure Result
- Measure Variable
- Merged Dimensions
- Object Package
- Olap Connection
- Olap Dimension
- Parameter
- Parameter Answer
- Parameter Prompt
- Personal Category
- Procedure Query
- Procedure Table
- Query



- Query Filter
- Report Field
- Report Filter
- Report Folder
- Repository
- Running Total Fields
- SQL Expression Fields
- SQL Query
- Schema
- Special Fields
- Summary Fields
- Table
- Universe
- Universe Connection
- Universe Folder
- Universe Model
- Universe Query
- Value
- Variables
- View
- Web Intelligence Document
- Web Intelligence Model
- XML Query

**Attention:** You must purge, run, and perform connection assignments for all SAP BusinessObjects catalog sources created prior to the November 2023 upgrade. This is required to extract additional metadata from universe objects and to view the complete lineage.

### Prerequisites for configuring the SAP BusinessObjects catalog source

To extract metadata from SAP BusinessObjects, complete the following prerequisite tasks:

- Verify that your Secure Agent is running on Microsoft Windows.
- Install the SAP BusinessObjects Client Tools for Microsoft Windows on the same machine where the Secure Agent is running.

### Permissions to configure the catalog source

Remove `write-protection` permissions from any SAP Business Object universe that you want to export. For more information about removing Business Object permissions, see the SAP Business Objects documentation.

Verify that the user who logs in to the SAP Business Objects repository belongs to the Universe Designer Users group and has read access to all the Business Objects metadata. If the Business Objects repository contains web intelligence reports in the Favorites or Personal folders, make sure that you include the user in the Administrators group. Create a custom security group and provide permission for the user to view Web intelligence reports.

## Connection properties

On the **Registration** page in Metadata Command Center, specify values for the following properties to connect to the SAP BusinessObjects source system:

Property	Description
Version	Required. Select the version of the SAP Business Objects repository.
System	Required. Name of the BusinessObjects repository used to connect.
Authentication Mode	Required. The authentication mode for the user account that logs in to the BusinessObjects repository. Select one of the following values: <ul style="list-style-type: none"><li>- Enterprise. Log in using the BusinessObjects Enterprise authentication mode.</li><li>- LDAP. Log in using LDAP authentication configured to BusinessObjects.</li><li>- Windows AD. Log in using a Windows Active Directory server.</li></ul>
User Name	Required. User name to log in to the BusinessObjects repository.
Password	Required. Password of the user account for the BusinessObjects repository.

## Configuration parameters for metadata extraction

Expand the **Catalog Source Configuration Options** in the **Metadata Extraction** tab on the **Configuration** page. Configure the following parameters to extract metadata from an SAP BusinessObjects source:

Property	Description
Incremental import	Select one of the following options to specify if you want to extract metadata that has changed since the previous run or extract complete metadata: <ul style="list-style-type: none"><li>- True. Extracts only the changes to the metadata since the last metadata extraction job.</li><li>- False. Extracts the complete metadata.</li></ul>
Add dependent objects	Select one of the following options to determine whether you want to add documents that depend on selected universes: <ul style="list-style-type: none"><li>- True. Imports the documents that depend on the specified universe. Select this option if you want to enable extraction of reference objects for the catalog source.</li><li>- False. Ignores the documents that depend on the specified universe.</li></ul>
Add specific objects	Select one of the following options to determine whether you want to add documents that do not depend on any universe: <ul style="list-style-type: none"><li>- None. Ignores all objects.</li><li>- Universe Independent Documents. Imports documents that do not depend on any universe.</li></ul>
Crystal CORBA port	Specifies the client port number on which the Crystal SDK communicates with the report application server (RAS). The RAS server uses the port to send metadata to the local client computer. If you do not specify a port, the server randomly selects a port for each execution.
Class representation	Controls how the import of the tree structure of classes and sub classes occur. Metadata Command Center imports each class containing objects as a dimension or as a tree of packages. Specify one of the following values: <ul style="list-style-type: none"><li>- As a flat structure. Creates no packages.</li><li>- As a simplified tree structure. Creates a package for each class with a sub class.</li><li>- As a full tree structure. Creates a package for each class.</li></ul>

Property	Description
Import joins	Select one of the following values to specify whether you want to import joins and contexts: <ul style="list-style-type: none"> <li>- True. Imports joins and contexts.</li> <li>- False. Does not import joins and contexts.</li> </ul>
Import hierarchies	Select one of the following options to specify whether you want to import hierarchies: <ul style="list-style-type: none"> <li>- True. Imports hierarchies.</li> <li>- False. Does not import hierarchies.</li> </ul>
Multiple threads	Number of worker threads that Metadata Command Center uses to extract metadata asynchronously. Leave blank or enter a positive integer value.  If left blank, the Secure Agent calculates the number of worker thread by using the JVM architecture and number of available CPU cores on the Secure Agent machine. If you specify a value that is not valid, the Secure Agent uses one worker thread.  Reduce the number of worker threads if the Secure Agent generates out-of-memory errors during metadata extraction. Increase the number of worker threads if the Secure Agent machine has a large amount of available memory, for example, 10 GB or more. If you specify too many worker threads, performance can decrease.
Agent Options	You can specify the following additional options to pass at runtime: <pre>-idtJre32 [path to the 32-bit JRE executable] -customXMLLocation [path to xmi files] -m 4G</pre> <ul style="list-style-type: none"> <li>- <b>-idtJre32.</b> Specify this option to configure the 32-bit JRE location and the <b>-m</b> option to specify the memory value required to run the metadata extraction job. For example:  <pre>-idtJre32 "E:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\win32_x86\\jre8\\bin\\javaw.exe\" -m 4G</pre> </li> <li>- <b>-customXMLLocation.</b> Specify this option if you want to load the XMI files that are generated when you run a metadata extraction job. Specify the location where the XMI files are stored. For example:  <pre>-customXMLLocation E:\\Dev\\apps\\Metadata_Foundation_Agent\\workspaces\\SAPBO</pre> </li> </ul>

## Referenced source systems

If the source system references another source system, create a connection assignment in Metadata Command Center to view data lineage with endpoints. To create a connection assignment, create a connection based on the referenced source system, and then assign the connection to the catalog source.

**Note:** You can view the lineage with reference objects without creating a connection assignment. After connection assignment, you can view the actual objects.

You can assign the following source systems as endpoint catalog sources:

Source system	Object class type
Microsoft SQL Server	Database
Oracle	Database
SAP HANA Database	Database

**Note:** For Web Intelligence Document, you can create a connection assignment with reference source systems at the schema level.

## CHAPTER 75

# SAP BusinessObjects Data Services

See [SAP BusinessObjects Data Services](#) to learn how to register and configure SAP BusinessObjects Data Services source systems 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 76

# SAP Business Warehouse (SAP BW)

SAP Business Warehouse (BW) is a data warehouse product of SAP that is based on the SAP NetWeaver ABAP environment. SAP BW can transform and consolidate business information from any source system for reporting, analysis, and interpretation of business data. This data is accessible through built-in reporting, business intelligence and analytics tools as well as third-party software.

### Objects extracted

The SAP BW catalog source extracts metadata from the following assets in an SAP BW source system:

- Info Area
- Data Source
- Info Objects
- Info Object Catalog
- Source System
- Info Source
- Characteristics
- Key Figures
- Dimension
- Navigational Attributes
- InfoSet
- DataStore Object (DSO)
- InfoCube
- Multi Provider
- Transformation
- Transformation Rule
- Query
- Query Element or Field
- Workbook
- Advanced DSO
- Composite Provider
- DTP

- InfoObject as InfoProvider
- CDS View  
The catalog source job extracts only CDS views that have queries.
- Open Hub Destination

**Note:** If an incremental metadata extraction job includes a view, it extracts the corresponding tables even if the tables were extracted in previous runs.

## Prerequisites

To extract metadata from SAP BW source systems, complete the following prerequisite tasks:

- **Create a connection in Administrator**

Use the SAP BW connector to connect to SAP BW. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.

- **Install the SAP BW Reader transport files**

Install the SAP BW Reader transport files on the SAP machines that you want to connect to. If you don't install the latest version of the SAP BW Reader transport files, the following message appears on the **Registration** page when you configure the catalog source: The test connection for <Connection name> failed. Unable to fetch Function Module, please validate for transport installation

For more information, see *Installing SAP BW Reader transport files* in the SAP Connector module in the Data Integration Connectors help.

- **Import SAP transports**

Import SAP transports to the SAP BW source. You can choose the transport from the dedicated Informatica namespace or the custom namespace.

Transports are available in the SAP\_Scanner\_Binaries.zip file located in the Informatica Cloud Secure Agent installation directory. The ZIP file is available in the following location:

```
<Informatica Secure Agent installation directory>/downloads/package-MFAgentCore.  
{*}/package/data/scanner/sap/SAP_Scanner_Binaries.zip
```

It is recommended that you import the latest version of the transports. If you use the scanner transports from the version preceding the current version, you see the following message in the logs: SAP Transport version is on previous Version.!!Please import latest transport!!

**Important:** Metadata extraction from SAP BW sources can fail if the transports are not valid or unavailable. For more information, see [Knowledge Base article 000202750](#).

For information about the latest transports available with the release, see [HOW TO: Import the latest transports for SAP catalog sources in Metadata Command Center](#).

- **Download the SAP JCo libraries**

Download the latest version of the 64-bit SAP JCo libraries from the SAP Service Marketplace based on the operating system on which the Secure Agent runs. Copy the files to <Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext\deploy\_to\_main\bin\rdtm-extra\tpl\sap.

The following table shows the libraries you need to download depending on your operating system:

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

**Note:** Create the `deploy_to_main\bin\rdtm-extra\tpl\sap` directory if it does not already exist.

- **Configure the `JAVA_LIBS` property**

Configure the `JAVA_LIBS` property in Informatica Intelligent Cloud Services Administrator. To do so, perform the following steps:

1. Log in to Informatica Intelligent Cloud Services Administrator.
2. Click **Runtime Environments** to access the Runtime Environments page.
3. From the menu to the left of the agent name, select **Edit Secure Agent**.
4. From the **Service** list, select **Data Integration Server**.
5. From the **Type** list, select **Tomcat JRE**.
6. Enter the `JAVA_LIBS` value based on the operating system on which the Secure Agent runs.
  - **Windows.** `../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javallib/sap/sap-adapter-common.jar`
  - **Linux.** `../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javallib/sap/sap-adapter-common.jar`
7. Click **Save**.
8. Repeat the steps on every machine where you installed the Secure Agent.
9. Restart the Secure Agent.

### Configure permissions

Before you configure an SAP BW catalog source in Metadata Command Center, configure the following permissions:

## Configure user-authorization profiles

The SAP Business Warehouse administrator creates the following product and development user authorization profiles:

Authorization Object	Description	Class	Field Values
S_RFC	Authorization check for RFC access	Cross Application Authorization Objects	ACTVT: 16 (Execute) RFC_NAME: DDIF_FIELDINFO_GET RFCPING RFC_GET_FUNCTION_INTERFACE RFC_METADATA_GET RFC_TYPE : FUGR, FUNC If you imported scanner transports from the custom namespace, use the following value: ZINFA_BW_FG If you imported scanner transports from the Informatica namespace, use the following value: /INFASCAN/BW_FG If you enabled UCON (Unified Connectivity), perform one of the following tasks: <ul style="list-style-type: none"> <li>• Disable UCON. Set the <b>ucon/rfc/active</b> profiling parameter value to 0.</li> <li>• If you can't disable UCON, whitelist the Informatica RFC function modules that start with:                ZINFA or /INFASCAN/</li> </ul>
S_RS_COMP	Business explorer components	Business Warehouse	ACTVT : 03,16 RSINFOAREA: * (Full Authorization) RSINFOCUBE: * (Full Authorization) RSZCOMPID: * (Full Authorization) RSZCOMPTP: Full Authorization
S_RS_COMP1	Business explorer components: Enhancements to the owner	Business Warehouse	ACTVT : 03,16 RSZCOMPID: * (Full Authorization) RSZOWNER: * (Full Authorization) RSZCOMPTP: * (Full Authorization)
S_RS_ISET	Data warehouse workbench InfoSet	Business Warehouse	ACTVT : 03 RSINFOAREA - * (Full Authorization) RSINFOSET - * (Full Authorization) RSISETOBJ - * (Full Authorization)
S_RS_ADMWB	Data warehouse workbench objects	Business Warehouse	ACTVT : 03 RSADMWBOBJ - * (Full Authorization)

## Connection properties

After you configure a connection to SAP BW in Informatica Intelligent Cloud Services Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.



The following table describes the SAP BW connection properties:

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.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent.
Host Name	The host name or IP address of the SAP BW server to which you want to connect. <b>Note:</b> If you select the <b>Load balancing</b> option, enter a value to continue.
System Number	The system number of the SAP BW server. Get the required system number from the SAP system to which you want to connect. <b>Note:</b> If you select the <b>Load balancing</b> option, enter a value to continue.

The following table describes the advanced connection properties:

Property	Description
Keystore location	The path and file name of the keystore file to connect to SAP. Enter both the path and file name in the following format: <Directory>/<Keystore file name>.jks
Keystore password	The password to access the keystore file.

Property	Description
Private Key password	The export password to access the .P12 file.
SAP Additional Parameters	<p>Additional SAP parameters that the Secure Agent uses to connect to the SAP system as an RFC client.</p> <p>Specify the required RFC-specific parameters and connection information to enable communication between Data Integration and SAP.</p> <p>You can specify the Secure Network Communication (SNC) parameters as additional arguments to securely connect to SAP as shown in the following format:</p> <pre>SNC_MODE=1 SNC_QOP=3 SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt; This is the SNC name of the Secure Agent machine. SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, OU=SAP Web AS, O=&lt;Organization&gt;, C=&lt;Country&gt;. This is the SNC name of the SAP system. SNC_LIB =&lt;Secure Agent installation directory&gt;/apps/Data_Integration_Server/ext/deploy_to_main/bin/&lt;libsapcrypto.so for Linux/sapcrypto.dll for Windows&gt; X509CERT=&lt;X509 certificate&gt;</pre> <p>For more information about the SNC parameters that you can configure in this field, see the How-To Library article, <a href="#">How to Configure the SAP Secure Network Communication Protocol in Informatica Cloud Data Integration</a>.</p> <p><b>Note:</b> The values of any required connection parameters override SAP additional parameter values that you have entered.</p>

**Note:** The SAP BW catalog source in Metadata Command Center supports only Secure Network Communication (SNC) with X.509 certificate. You can also use SNC with username and password.

### Configuration parameters for metadata extraction

Specify additional configuration parameters from the **Configuration Parameters** area in the **Metadata Extraction** tab of the **Configuration** page.

**Source Extraction.** Filters the metadata that you extract from an SAP BW source system.

You can choose one of the following values:

- Full. Extracts the full metadata from the source.
- Based on Query Execution Date. Extracts metadata based on the query execution date that you specify for the **Scan date** parameter in the **YYYYMMDD** format. The corresponding dependent metadata objects are also extracted.
- Based on Object Modified Date. Extracts metadata that is modified or created after the date that you specify for the **Scan date** parameter in the **YYYYMMDD** format. Perform at least one full extraction before extracting metadata based on object modified date.

**Namespace.** Specifies the namespace from which you imported the scanner transport. Select the dedicated Informatica namespace or the custom namespace based on the scanner transport that you imported.

### Referenced source systems

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

such as SAP HANA Database. You must first create and run an endpoint catalog source that connects to the reference source system.

**Note:** You can view the lineage with reference objects without performing a connection assignment. After connection assignment, you can view the actual objects.

You can assign the following source systems as endpoint catalog sources:

Source system	Endpoint
SAP HANA Database	Database
SAP ERP	SapSchema

You can perform a connection assignment from the following assets and catalog sources to SAP BW:

- From Calculation View assets of SAP HANA Database to Composite Provider assets of SAP BW
- From Table assets of SAP HANA Database to DataSource assets of SAP BW
- From View assets of SAP HANA Database to DataSource assets of SAP BW
- From CDS View assets of SAP ERP to DataSource assets of SAP BW
- From DataSource assets of SAP ERP to DataSource assets of SAP BW

### Data profiling for SAP BW objects

Configure data profiling to run profiles on the metadata extracted from an SAP BW source system. You can view the profiling statistics in Data Governance and Catalog.

You can run data profiles on the following SAP BW objects:

- InfoCube
- MultiProvider
- DataStore Object (DSO)

#### Sampling type

You can run data profiles on all rows in the metadata extracted from SAP BW source systems.

### Data classification for SAP BW objects

Configure data classification for SAP BW catalog sources to classify and organize data in your organization.

You can choose one of the following options:

- **Data Classification Rules.** Choose from predefined or custom data classifications.
- **Generated Data Classifications.** CLAIRE automatically generates data classifications for the data elements.

**Note:** SAP BW source systems can contain ambiguous data with technical field names. To ensure that CLAIRE generates accurate data classifications, it uses the extracted **Business Name** attribute to generate data classifications.

You can view the data classification results in Data Governance and Catalog.

For more information about data classifications, see *Data classification* in the Administration help.

### Glossary association

Enable glossary association and configure settings for the catalog source to automatically associate or recommend glossary terms as business names for data elements in technical assets.

The following table describes the settings:

Property	Description
Enable auto-acceptance	When enabled, this option automatically associates glossary terms with data elements based on the threshold limit that you specify. The automatically accepted glossary terms appear as business names of data elements in Data Governance and Catalog.
Confidence Score Threshold for Auto-Acceptance	Specify a percentage from 80 to 100 inclusive to set a threshold limit. If a glossary term matches a data asset within the threshold specified, Metadata Command Center automatically assigns the matching glossary term to the data element. The name and description of the glossary term with the highest confidence score appears as the name and description of the data element asset in Data Governance and Catalog.
Enable below-threshold recommendations	If you enable auto-acceptance, you can select this option to receive glossary association recommendations below the auto-acceptance threshold.
Confidence score threshold for recommendations	If you enable auto-acceptance, specify a percentage between 80% and the selected confidence score threshold for auto-acceptance. If you disable auto-acceptance, specify a percentage between 80% and 100%.
Assign business names and descriptions	Choose to automatically assign business names and descriptions to technical assets.
Keep existing business names and descriptions	Applicable if you choose to assign business names and descriptions. 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.
Ignore Keywords	Choose to ignore specific parts of data elements when making recommendations. You can enter multiple unique prefix and suffix keywords. Keyword values are case insensitive.
Glossary Association Scope	Choose specific top-level business glossary assets to associate with technical assets. Selecting a top-level asset selects its child assets as well.
Use Abbreviation and Synonym Definitions	Enable this option to use a lookup table with abbreviations and synonyms to improve glossary association accuracy. To upload a lookup synonym file with the abbreviations and synonyms, select <b>Yes</b> to enable, and then click <b>Select</b> .

**Note:** SAP BW source systems can contain ambiguous data with technical field names. To generate accurate glossary associations, CLAIRE uses the extracted Business Name attribute for such technical field names.

For more information about the glossary association settings, see the *Administrator* help.

## CHAPTER 77

# SAP BW/4HANA

SAP BW/4HANA is an enterprise data warehouse platform that captures, stores, and consolidates enterprise data.

### Objects extracted

The SAP BW/4HANA catalog source extracts metadata from the following assets in an SAP BW/4HANA source system:

- Info Area
- Data Source
- Info Objects
- Source System
- Info Source
- Characteristics
- Key Figures
- Navigational Attributes
- Transformation
- Transformation Rule
- Query
- Query Element or Field
- Advanced DSO
- Composite Provider
- DTP
- Open ODS View
- Aggregation Level
- Open Hub Destination
- InfoObject as InfoProvider

**Note:** If an incremental metadata extraction job includes a view, it extracts the corresponding tables even if the tables were extracted in previous runs.

## Prerequisites

To extract metadata from SAP BW/4HANA source systems, complete the following prerequisite tasks:

- **Create a connection in Administrator**

Use the SAP BW connector to connect to the SAP BW/4HANA source system. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.

- **Install the SAP BW Reader transport files**

Install the SAP BW Reader transport files on the SAP machines that you want to connect to. If you don't install the latest version of the SAP BW Reader transport files, the following message appears on the **Registration** page when you configure the catalog source: The test connection for <Connection name> failed. Unable to fetch Function Module, please validate for transport installation

For more information, see *Installing SAP BW Reader transport files* in the SAP Connector module in the Data Integration Connectors help.

- **Import SAP transports**

Import SAP transports to the SAP BW/4HANA source. You can choose the transport from the dedicated Informatica namespace or the custom namespace.

Transports are available in the SAP\_Scanner\_Binaries.zip file located in the Informatica Cloud Secure Agent installation directory. The ZIP file is available in the following location:

```
<Informatica Secure Agent installation directory>/downloads/package-MFAgentCore.  
{*}/package/data/scanner/sap/SAP_Scanner_Binaries.zip
```

It is recommended that you import the latest version of the transports. If you use the transports from the version preceding the current version, you see the following message in the logs: SAP Transport version is on previous Version.!!Please import latest transport!!

**Important:** Metadata extraction from SAP BW/4HANA sources can fail if the transports are not valid or unavailable. For more information, see [Knowledge Base article 000202750](#).

For information about the latest transports available with the release, see [HOW TO: Import the latest transports for SAP catalog sources in Metadata Command Center](#).

- **Download the SAP JCo libraries**

Download the latest version of the 64-bit SAP JCo libraries from the SAP Service Marketplace based on the operating system on which the Secure Agent runs and copy the files to the following location:

```
<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext  
\deploy_to_main\bin\rdtm-extra\tpl\sap
```

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

**Note:** Create the deploy\_to\_main\bin\rdtm-extra\tpl\sap directory if it does not already exist.

- **Configure the `JAVA_LIBS` property**

Configure the `JAVA_LIBS` property in Administrator. Perform the following steps:

1. Log in to Administrator.
2. Click **Runtime Environments** to access the Runtime Environments page.
3. From the menu to the left of the agent name, select **Edit Secure Agent**.
4. From the Service list, select **Data Integration Server**.
5. From the Type list, select **Tomcat JRE**.
6. Enter the `JAVA_LIBS` value based on the operating system where the Secure Agent runs.
  - **Windows.** `../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javaliib/sap/sap-adapter-common.jar`
  - **Linux.** `../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javaliib/sap/sap-adapter-common.jar`
7. Click **Save**.
8. Repeat steps on every machine where you installed the Secure Agent.
9. Restart the Secure Agent.

### Configure permissions

Before you configure an SAP BW/4HANA catalog source in Metadata Command Center, configure the following permissions:

### Configure user-authorization profiles

The SAP Business Warehouse administrator creates the following product and development user authorization profiles:

Authorization Object	Description:
S_RFC	<p>Authorization check for RFC access.</p> <p>This class uses the Cross Application Authorization Objects with the following field values:</p> <p>ACTVT: 16 (Execute)</p> <p>RFC_NAME:</p> <p>DDIF_FIELDINFO_GET</p> <p>RFCPING</p> <p>RFC_GET_FUNCTION_INTERFACE</p> <p>RFC_METADATA_GET</p> <p>RFC_TYPE : FUGR, FUNC</p> <p>If you imported scanner transports from the custom namespace, use the following value:</p> <p>ZINFA_BW4H_FG</p> <p>If you imported scanner transports from the Informatica namespace, use the following value:</p> <p>/INFASCAN/BW4H_FG</p> <p>If you enabled UCON (Unified Connectivity), perform one of the following tasks:</p> <ul style="list-style-type: none"><li>- Disable UCON. Set the <b>ucon/rfc/active</b> profiling parameter value to 0.</li><li>- If you can't disable UCON, whitelist the Informatica RFC function modules that start with:</li></ul> <p>ZINFA or /INFASCAN/</p>
S_RS_COMP	<p>Business explorer components.</p> <p>This class uses the Business Warehouse with the following field values:</p> <p>ACTVT : 03,16 RSINFOAREA: * (Full Authorization)</p> <p>RSINFOCUBE: * (Full Authorization)</p> <p>RSZCOMPID: * (Full Authorization)</p> <p>RSZCOMPTP: Full Authorization</p>
S_RS_COMP1	<p>Business explorer components: Enhancements to the owner.</p> <p>This class uses the Business Warehouse with the following field values:</p> <p>ACTVT : 03,16</p> <p>RSZCOMPID: * (Full Authorization)</p> <p>RSZOWNER: * (Full Authorization)</p> <p>RSZCOMPTP: * (Full Authorization)</p>

### Connection properties

After you configure a connection to SAP BW/4HANA in Informatica Intelligent Cloud Services Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.



The following table describes the SAP BW/4HANA connection properties:

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.
Use Secret Vault	Stores sensitive credentials for this connection in the secrets manager that is configured for your organization. This property appears only if secrets manager is set up for your organization. When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured. <b>Note:</b> If you're using this connection to apply data access policies through pushdown or proxy services, you cannot use the Secret Vault configuration option. For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent.
Username	The user name with the appropriate user authorization to connect to the SAP BW account.
Password	The password to connect to the SAP BW account.
Connection type	Required. Type of connection that you want to create. Select one of the following values: - Application. Create an application connection when you want to connect to a specific SAP BW server. - Load balancing. Create a load balancing connection when you want to use SAP load balancing. Default is Application.

The following table describes the basic connection properties for an application connection:

Property	Description
Host name	The host name or IP address of the SAP BW server to which you want to connect.
System number	The system number of the SAP BW server. Get the required system number from the SAP system to which you want to connect.
Client	The client number of the SAP BW server. Get the required client number from the SAP system to which you want to connect.
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.

The following table describes the advanced connection properties for an application connection:

Property	Description
Trace	<p>Determines whether to track the JCo calls that the SAP system makes. Enter one of the values between 0 and 8. By default, SAP doesn't store information about the JCo calls in a trace file. Default is 0. For more information about trace level values, see <a href="#">Setting up an SAP Java Connector (SAP JCo) and Related Traces</a>.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> <li>- Design time information: &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\Latest version\ICS\main\tomcat</li> <li>- Run-time information: &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\Latest version\ICS\main\bin\rdtm</li> </ul>
Additional parameters	<p>Additional JCo connection parameters that you can use when you read SAP BW data. You can enter multiple JCo connection parameters, separated by a semicolon, in the following format:</p> <pre>&lt;parameter name1&gt;=&lt;value1&gt;;&lt;parameter name2&gt;=&lt;value2&gt;;&lt;parameter name3&gt;=&lt;value3&gt;....</pre> <p>For example, if you want to create an SAP SNC connection, enter the following additional parameters:</p> <pre>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</pre>
Port Range	<p>HTTP port range. The SAP BW connection uses the specified port numbers to connect to SAP BW using the HTTP protocol. Default range is 10000-65535. Enter a range in the default range, for example, 10000-20000. When a range is outside the default range, the connection uses the default range.</p>
Use HTTPS	Select this option to enable https streaming.
Keystore location	<p>The path and file name of the keystore file to connect to SAP. Enter both the path and file name in the following format:</p> <pre>&lt;Directory&gt;/&lt;Keystore file name&gt;.jks</pre>
Keystore password	The password to access the keystore file.

Property	Description
Private Key password	The export password to access the .P12 file.
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client. Specify the required RFC-specific parameters and connection information that enable the Secure Agent to connect to SAP.</p> <p>For example, you can specify the SNC connection parameters as additional arguments listed in the following sample:</p> <pre>MSHOST= &lt;Message server hostname&gt; GROUP=PUBLIC R3NAME=SLT SNC_MODE=1 SNC_QOP=3 SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt; This is the SNC name of the Secure Agent machine. SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, OU=SAP Web AS, O=&lt;Organization&gt;, C=&lt;Country&gt;. This is the SNC name of the SAP system. SNC_LIB =&lt;Secure Agent installation directory&gt;/apps/Data_Integration_Server/ext/deploy_to_main/bin/&lt;libsapcrypto.so for Linux/sapcrypto.dll for Windows&gt; X509CERT=&lt;X509 certificate&gt;</pre> <p>For more information about SNC parameters, see <a href="#">How to configure the SAP Secure Network Communication protocol</a> Informatica How-To Library article.</p> <p>For more information about RFC-specific parameters, see the SAP documentation.</p> <p><b>Note:</b> If you specify a parameter in both the <b>SAP Additional Parameters</b> and <b>Additional parameters</b> fields, the value specified in the <b>SAP Additional Parameters</b> field takes precedence.</p>

The following table describes the basic connection properties for a load balancing connection:

Property	Description
Host name	The host name or IP address of the SAP BW server to which you want to connect.
System number	<p>The system number of the SAP BW server.</p> <p>Get the required system number from the SAP system to which you want to connect.</p>
Client	<p>The client number of the SAP BW server.</p> <p>Get the required client number from the SAP system to which you want to connect.</p>
Language	<p>Language code that corresponds to the SAP language.</p> <p>Get the required language code from the SAP system to which you want to connect.</p>

The following table describes the advanced connection properties for a load balancing connection:

Property	Description
Message host name	Required. The host name of the SAP message server to which you want to connect when you use a load balancing connection.
R3 name/SysID	Required. The system ID of the SAP message server to which you want to connect when you use a load balancing connection.
Group	Required. The name of the SAP logon group through which you want to connect when you use a load balancing connection.
Trace	<p>Determines whether to track the JCo calls that the SAP system makes. Enter one of the values between 0 and 8. By default, SAP doesn't store information about the JCo calls in a trace file. Default is 0.</p> <p>For more information about trace level values, see <a href="#">Setting up an SAP Java Connector (SAP JCo) and Related Traces</a>.</p> <p>You can access the trace files from the following directories:</p> <ul style="list-style-type: none"> <li>- Design time information: &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\tomcat</li> <li>- Run-time information: &lt;Informatica Secure Agent installation directory&gt;\apps\Data_Integration_Server\&lt;Latest version&gt;\ICS\main\bin\rdtm</li> </ul>
Additional parameters	<p>Additional JCo connection parameters that you can use when you read SAP BW data. You can enter multiple JCo connection parameters, separated by a semicolon, in the following format:</p> <pre>&lt;parameter name1&gt;=&lt;value1&gt;;&lt;parameter name2&gt;=&lt;value2&gt;;&lt;parameter name3&gt;=&lt;value3&gt;....</pre> <p>For example, if you want to create an SAP SNC connection, enter the following additional parameters:</p> <pre>SNC_MODE=1;SNC_QOP=3;SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt;;SNC_LIB=C:\SNC_11\sapcrypto.dll;TRACE=1</pre>
Port Range	<p>HTTP port range. The SAP BW connection uses the specified port numbers to connect to SAP BW using the HTTP protocol. Default range is 10000-65535.</p> <p>Enter a range in the default range, for example, 10000-20000. When a range is outside the default range, the connection uses the default range.</p>
Use HTTPS	Select this option to enable https streaming.
Keystore location	<p>The path and file name of the keystore file to connect to SAP. Enter both the path and file name in the following format:</p> <pre>&lt;Directory&gt;/&lt;Keystore file name&gt;.jks</pre>
Keystore password	The password to access the keystore file.

Property	Description
Private Key password	The export password to access the .P12 file.
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client. Specify the required RFC-specific parameters and connection information that enable the Secure Agent to connect to SAP.</p> <p>For example, you can specify the SNC connection parameters as additional arguments listed in the following sample:</p> <pre>MSHOST= &lt;Message server hostname&gt; GROUP=PUBLIC R3NAME=SLT SNC_MODE=1 SNC_QOP=3 SNC_MYNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, O=&lt;Organization&gt;, C=&lt;Country&gt; This is the SNC name of the Secure Agent machine. SNC_PARTNERNAME=p:CN=&lt;Common name&gt;, OU=&lt;Organizational unit&gt;, OU=SAP Web AS, O=&lt;Organization&gt;, C=&lt;Country&gt;. This is the SNC name of the SAP system. SNC_LIB =&lt;Secure Agent installation directory&gt;/apps/Data_Integration_Server/ext/deploy_to_main/bin/&lt;libsapcrypto.so for Linux/sapcrypto.dll for Windows&gt; X509CERT=&lt;X509 certificate&gt;</pre> <p>For more information about SNC parameters, see <a href="#">How to configure the SAP Secure Network Communication protocol</a> Informatica How-To Library article.</p> <p>For more information about RFC-specific parameters, see the SAP documentation.</p> <p><b>Note:</b> If you specify a parameter in both the <b>SAP Additional Parameters</b> and <b>Additional parameters</b> fields, the value specified in the <b>SAP Additional Parameters</b> field takes precedence.</p>

**Note:** The SAP BW catalog source in Metadata Command Center supports only Secure Network Communication (SNC) with X.509 certificate. You can also use SNC with username and password.

## Configuration parameters for metadata extraction

Specify additional configuration parameters from the **Configuration Parameters** area in the **Metadata Extraction** tab of the **Configuration** page.

**Source Extraction.** Filters the metadata that you extract from an SAP BW/4HANA source system.

You can choose one of the following values:

- Full. Extracts the full metadata from the source.
- Based on Query Execution Date. Extracts metadata based on the query execution date that you specify for the **Scan date** parameter in the YYYYMMDD format. The corresponding dependent metadata objects are also extracted.
- Based on Object Modified Date. Extracts metadata that is modified or created after the date that you specify for the **Scan date** parameter in the YYYYMMDD format. Perform at least one full extraction before extracting metadata based on object modified date.

**Namespace.** Specifies the namespace from which you imported the scanner transport. Select the dedicated Informatica namespace or the custom namespace based on the scanner transport that you imported.

## Referenced source systems

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

connection to the objects in the reference source system. A reference source system might be a database, such as SAP HANA Database. You must first create and run an endpoint catalog source that connects to the reference source system.

**Note:** You can view the lineage with reference objects without performing a connection assignment. After connection assignment, you can view the actual objects.

You can assign the following source systems as endpoint catalog sources:

Source system	Endpoint
SAP HANA Database	Database
SAP ERP	SapSchema

You can perform a connection assignment from the following assets and catalog sources to SAP BW/4HANA:

- From Calculation View assets of SAP HANA Database to Composite Provider assets of SAP BW/4HANA
- From Table assets of SAP HANA Database to DataSource assets of SAP BW/4HANA
- From View assets of SAP HANA Database to DataSource assets of SAP BW/4HANA
- From CDS View assets of SAP ERP to DataSource assets of SAP BW/4HANA
- From DataSource assets of SAP ERP to DataSource assets of SAP BW/4HANA

### Data classification for SAP BW/4HANA objects

Configure data classification for SAP BW/4HANA catalog sources to classify and organize data in your organization. You can view the data classification results in Data Governance and Catalog.

You can choose one of the following options:

- **Data Classification Rules.** Choose from predefined or custom data classifications.
- **Generated Data Classifications.** CLAIRE automatically generates data classifications for the data elements.

**Note:** SAP BW/4HANA source systems can contain ambiguous data with technical field names. To ensure that CLAIRE generates accurate data classifications, it uses the extracted **Business Name** attribute to generate data classifications.

You can view the data classification results in Data Governance and Catalog.

For more information about data classifications, see *Data classification* in the Administration help.

### Glossary association

Enable glossary association and configure settings for the catalog source to automatically associate or recommend glossary terms as business names for data elements in technical assets.

The following table describes the settings:

Property	Description
Enable auto-acceptance	When enabled, this option automatically associates glossary terms with data elements based on the threshold limit that you specify. The automatically accepted glossary terms appear as business names of data elements in Data Governance and Catalog.
Confidence Score Threshold for Auto-Acceptance	Specify a percentage from 80 to 100 inclusive to set a threshold limit. If a glossary term matches a data asset within the threshold specified, Metadata Command Center automatically assigns the matching glossary term to the data element. The name and description of the glossary term with the highest confidence score appears as the name and description of the data element asset in Data Governance and Catalog.
Enable below-threshold recommendations	If you enable auto-acceptance, you can select this option to receive glossary association recommendations below the auto-acceptance threshold.
Confidence score threshold for recommendations	If you enable auto-acceptance, specify a percentage between 80% and the selected confidence score threshold for auto-acceptance. If you disable auto-acceptance, specify a percentage between 80% and 100%.
Assign business names and descriptions	Choose to automatically assign business names and descriptions to technical assets.
Keep existing business names and descriptions	Applicable if you choose to assign business names and descriptions. 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.
Ignore Keywords	Choose to ignore specific parts of data elements when making recommendations. You can enter multiple unique prefix and suffix keywords. Keyword values are case insensitive.
Glossary Association Scope	Choose specific top-level business glossary assets to associate with technical assets. Selecting a top-level asset selects its child assets as well.
Use Abbreviation and Synonym Definitions	Enable this option to use a lookup table with abbreviations and synonyms to improve glossary association accuracy. To upload a lookup synonym file with the abbreviations and synonyms, select <b>Yes</b> to enable, and then click <b>Select</b> .

**Note:** SAP BW/4HANA source systems can contain ambiguous data with technical field names. To generate accurate glossary associations, CLAIRE uses the extracted Business Name attribute for such technical field names.

For more information about the glossary association settings, see the *Administrator* help.

## CHAPTER 78

# SAP Datasphere - Preview catalog source

See [SAP Datasphere Sources](#) to learn how to register and configure SAP Datasphere source systems 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 79

# SAP ERP

SAP Enterprise Resource Planning (ERP) is a platform that incorporates the key business functions of an organization. Use this catalog source to extract metadata from SAP ERP Central Component (ECC) or SAP S/4HANA source systems.

### Objects extracted

The SAP ERP catalog source extracts metadata from the following assets in SAP S/4HANA and SAP ECC source systems:

- Packages  
Includes subpackages and assets in subpackages.
- Classes in active state
- Data Elements in active state
- Data Sources built on tables, views and function modules
- Domains in active state
- RFC function modules and function modules used in a data source
- Executable programs in active state
- RFC Connections in active state
- Tables in active state such as transparent tables, cluster tables, and pool tables
- Fields
- Transaction codes in active state
- Views such as database views, CDS views, append views, and external views

**Note:** If an incremental metadata extraction job includes a view, it extracts the corresponding tables even if the tables were extracted in previous runs.

### Prerequisites

To extract metadata from SAP S/4HANA and SAP ECC source systems, complete the following prerequisite tasks:

- **Create a connection in the Administrator**  
Use the SAP BAPI connector to configure a connection to SAP ERP in Informatica Intelligent Cloud Services Administrator. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.
- **Import SAP transports**  
Import SAP transports to the SAP ERP source. You can choose the transport from the dedicated Informatica namespace or the custom namespace.

Transports are available in the SAP\_Scanner\_Binaries.zip file located in the Informatica Cloud Secure Agent installation directory. The ZIP file is available in the following location:

```
<Informatica Secure Agent installation directory>/downloads/package-MFAgentCore.  
{*}/package/data/scanner/sap/SAP_Scanner_Binaries.zip
```

It is recommended that you import the latest version of the transports. If you use transports from the version preceding the current version, you see the following message in the logs: SAP Transport version is on previous Version.!!Please import latest transport!!

**Important:** Metadata extraction from SAP ERP sources can fail if the transports are not valid or unavailable. For more information, see [Knowledge Base article 000202750](#).

For information about the latest transports available with the release, see [HOW TO: Import the latest transports for SAP catalog sources in Metadata Command Center](#).

- **Download the SAP JCo libraries**

Download the latest version of the 64-bit SAP JCo libraries from the SAP Service Marketplace based on the operating system on which the Secure Agent runs. Copy the files to *<Informatica Secure Agent installation directory>\apps\Data\_Integration\_Server\ext\deploy\_to\_main\bin\rdtm-extra\tpl\sap*.

The following table shows the libraries you need to download depending on your operating system:

Secure Agent System	SAP File Name
Windows	sapjco3.jar sapjco3.dll
Linux	sapjco3.jar libsapjco3.so

**Note:** Create the *deploy\_to\_main\bin\rdtm-extra\tpl\sap* directory if it does not already exist.

- **Configure the JAVA\_LIBS property**

Configure the JAVA\_LIBS property in Informatica Intelligent Cloud Services Administrator. Perform the following steps:

1. Log in to Informatica Intelligent Cloud Services Administrator.
2. Click **Runtime Environments** to access the Runtime Environments page.
3. From the menu to the left of the agent name, select **Edit Secure Agent**.
4. From the **Service** list, select **Data Integration Server**.
5. From the **Type** list, select **Tomcat JRE**.
6. Enter the JAVA\_LIBS value based on the operating system on which the Secure Agent runs.
  - **Windows.** *../bin/rdtm-extra/tpl/sap/sapjco3.jar;../bin/rdtm/javallib/sap/sap-adapter-common.jar*
  - **Linux.** *../bin/rdtm-extra/tpl/sap/sapjco3.jar:../bin/rdtm/javallib/sap/sap-adapter-common.jar*
7. Click **Save**.
8. Repeat the steps on every machine where you installed the Secure Agent.
9. Restart the Secure Agent.

## Configure permissions

To extract metadata, you need account access and permissions on the SAP S/4HANA and SAP ECC source systems.

## Configure user-authorization profiles

To access metadata from SAP ERP, the SAP ERP administrator creates the following user authorization profiles:

Authorization Object	Description	Field Values
S_RFC	Authorization check for RFC access	<p>ACTVT: 16 (Execute)</p> <p>RFC_NAME:</p> <p>DDIF_FIELDINFO_GET</p> <p>RFCPING</p> <p>RFC_GET_FUNCTION_INTERFACE</p> <p>RFC_METADATA_GET</p> <p>SEU_COMPONENT</p> <p>RFC_TYPE: FUGR, FUNC</p> <p>If you imported scanner transports from the custom namespace, use the following value:</p> <p>ZINFA_ERP</p> <p>If you imported scanner transports from the Informatica namespace, use the following value:</p> <p>/INFASCAN/ERP_META</p> <p>If you enabled UCON (Unified Connectivity), perform one of the following tasks:</p> <ul style="list-style-type: none"> <li>- Disable UCON. Set the <b>ucon/rfc/active</b> profiling parameter value to 0.</li> <li>- If you can't disable UCON, whitelist the Informatica RFC function modules that start with:</li> </ul> <p>ZINFA or /INFASCAN/</p>
ZINFA_META	Authorization check for metadata extraction	<ul style="list-style-type: none"> <li>- Classes: SRC</li> <li>- Data Elements: RQD</li> <li>- Data Sources: RQD</li> <li>- Domains: RQD</li> <li>- Function Modules: SRC</li> <li>- Keys: RQD</li> <li>- Packages: RQD</li> <li>- Programs: SRC</li> <li>- RFC: RFC</li> <li>- Tables: RQD</li> <li>- Transaction Codes: SRC</li> <li>- Views: RQD</li> <li>- Where Used Tables: WHRUSD</li> </ul> <p><b>Note:</b> Extracts metadata from the tables used in programs, classes, views, function modules, and transaction codes.</p> <ul style="list-style-type: none"> <li>- Where Used Views: WHRUSD</li> </ul> <p><b>Note:</b> Extracts metadata from views used in programs, classes, function modules, and transaction codes.</p> <p>If the mandatory value is RQD and you want to extract RFC assets along with RQD assets from the SAP ERP source system, the ZINFA_META authorization object should have the RFC value.</p> <p>If you need to extract all assets, provide the full authorization. Use an asterisk (*).</p>

**Note:** RQD is the minimum permission you need to extract metadata from SAP ERP source systems. If you have the RQD permission and run a metadata extraction job with the packages filter, the job extracts metadata from assets covered by the RQD permission. If you run a job with both the packages and classes filters but lack the SRC permission, the job extracts metadata for the RQD assets and the class package. However, the job doesn't process assets that have the Classes filter applied.

#### Permissions to run data profiles

You do not need additional permissions to run data profiles.

#### Connection properties

After you configure a connection to SAP BAPI in Informatica Intelligent Cloud Services Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the basic SAP Bapi connection properties:

Property	Description
Runtime Environment	The execution platform that runs tasks. The runtime environment is either a Secure Agent or a Serverless runtime environment.
Username	The user name with the appropriate user authorization to connect to the SAP account.
Password	The password to connect to the SAP account.
Host Name	The host name or IP address of the SAP server to which you want to connect.
Client	The client number of the SAP server. Get the required client number from the SAP system to which you want to connect.
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.
System Number	The system number of the SAP server. Get the required system number from the SAP system to which you want to connect.

The following table describes the advanced SAP Bapi connection properties:

Property	Description
SAP Additional Parameters	<p>Additional SAP properties that the Secure Agent uses to connect to the SAP system as an RFC client. See the following examples where you can use this field to configure additional parameters for the connection:</p> <ul style="list-style-type: none"> <li>- To create a load balancing connection, define the additional arguments listed in the following sample:  GROUP=interfaces MSHOST=&lt;Message server hostname&gt; R3NAME=&lt;System ID or name of SAP system&gt;  SAP infers the connection type based on the parameters that you specify. For example, if you define the GROUP, MSHOST, and R3NAME parameters, SAP infers the connection type as a load balancing connection. The GROUP parameter defines the group name of the SAP application server. The MSHOST parameter defines the host name of the SAP message server. The R3NAME parameter defines the system ID or name of the SAP system.</li> <li>- To commit data to the SAP system with each BAPI/RFC call, define the DOCOMMIT=true parameter.</li> <li>- To create a connection with the Secure Network Communication (SNC) protocol, define the required additional parameters.</li> </ul> <p>If you specify a property both in the dedicated connection field and in the <b>SAP Additional Parameters</b> field, the value specified in the <b>SAP Additional Parameters</b> field takes precedence.</p> <p>For more information about SAP parameters, see the SAP documentation.</p>
Jco Trace	<p>Select this checkbox to enable tracing for the BAPI call.</p> <p>Even if you define the Trace parameter in the <b>SAP Additional Parameters</b> field, select the Jco Trace check box to generate the trace file.</p>

After you configure a connection to SAP Table in Informatica Intelligent Cloud Services Administrator, you can view the source connection name for that connection on the **Data Profiling and Quality** tab of the **Configuration** page in Metadata Command Center.

The following table describes the basic SAP Table connection properties:

Property	Description
Runtime Environment	Required. The name of the runtime environment where you want to run the tasks. Select a Secure Agent or serverless runtime environment.
Username	The user name with the appropriate user authorization to connect to the SAP account.
Password	The password to connect to the SAP account.
Client	The client number of the SAP application server. Get the required client number from the SAP system to which you want to connect.
Language	Language code that corresponds to the SAP language. Get the required language code from the SAP system to which you want to connect.

The following table describes the advanced SAP Table connection properties:

Property	Description
Saprfc.ini Path	Required. Local directory to the <code>sapnwrfc.ini</code> file. To write to SAP tables, use the following directory: <Informatica Secure Agent installation directory>/apps/ Data_Integration_Server/ext/deploy_to_main/bin/rdtm
Destination	DEST entry that you specified in the <code>sapnwrfc.ini</code> file for the SAP application server. Use all uppercase letters for the destination. This property is required if you create the connection to write to SAP tables. If you enter the DEST entry in this field, do not enter the host name or IP address, and system number of the SAP application server in the <b>Application Server</b> and <b>System Number</b> fields.
Port Range	HTTP port range. The SAP Table connection uses the specified port numbers to connect to SAP tables using the HTTP protocol. Default range is 10000-65535. Enter a range in the default range, for example, 10000-20000. When a range is outside the default range, the connection uses the default range.
Test Streaming	Tests the connection. When selected, tests the connection using both RFC and HTTP protocol. When not selected, tests connection using RFC protocol.
Https Connection	When selected, connects to SAP through HTTPS protocol. To successfully connect to SAP through HTTPS, verify that an administrator has configured the machines that host the Secure Agent and the SAP system.
Keystore Location	Absolute path and file name of the keystore file to connect to SAP. Specify both the path and file name in the following format: <Directory>/<Keystore file name>.jks
Keystore Password	The destination password to access the keystore file.
Private Key Password	The export password to access the .P12 file.

## Configuration parameters for metadata extraction

Specify additional configuration parameters from the **Configuration Parameters** area in the **Metadata Extraction** tab of the **Configuration** page.

**Namespace.** Specifies the namespace from which you imported the scanner transport. Select the dedicated Informatica namespace or the custom namespace based on the scanner transport that you imported.

## Data profiling for SAP ERP objects

### Prerequisites

- Use the SAP Table connector to run data profiles and data quality tasks on SAP ERP objects. Create an SAP Table connection in Informatica Intelligent Cloud Services Administrator.
- To read data from SAP tables, install the SAP Table connection transport files from the Secure Agent directory to the SAP system.

For information about configuring SAP Table connection in Administrator and installing transport files to read from SAP tables, see *SAP Connector* in the Data Integration Connectors help.

Configure data profiling to run profiles on metadata extracted from SAP S/4HANA and SAP ECC source systems. You can run data profiles on the following SAP ERP objects:

- Table
- View

**Note:** You can run data profiles on database views and CDS views.

After running the catalog source job, you can view the profiling statistics in Data Governance and Catalog. The data profiling task runs profiles on the following data types for SAP ERP objects:

- ACCP
- CHAR
- CLNT
- CUKY
- CURR
- DATS
- DEC
- D16D
- D16R
- D34D
- D34R
- FLTP
- INT2
- INT4
- LANG
- LCHR
- LRAW
- NUMC
- QUAN
- SSTRING
- STRING
- STRU
- TIMS
- UNIT
- RAW
- RAWSTRING

For information about rules and guidelines for SSTRING, STRING, and RAWSTRING data types, see *SAP Connector* in the Data Integration-Free and PayGo help.

#### **Sampling type**

Determine the sample rows on which you want to run a data profiling task.

You can choose one of the following sampling types:

- All Rows



- Limit N Rows

## Data classification for SAP ERP objects

Configure data classification for SAP ERP catalog sources to classify and organize data in your organization.

You can choose one of the following options:

- **Data Classification Rules.** Choose from predefined or custom data classifications.
- **Generated Data Classifications.** CLAIRE automatically generates data classifications for the data elements.  
**Note:** SAP ERP source systems can contain ambiguous data with technical field names. To ensure that CLAIRE generates accurate data classifications, it uses the extracted **Business Name** attribute to generate data classifications.

You can view the data classification results in Data Governance and Catalog.

For more information about data classifications, see *Data classification* in the Administration help.

## Referenced source systems

If the source system references another source system, create a connection assignment in Metadata Command Center to view data lineage with endpoints. To create a connection assignment, create a connection based on the referenced source system, and then assign the connection to the catalog source.

**Note:** You can view the lineage with reference objects without creating a connection assignment. After connection assignment, you can view the actual objects.

You can perform connection assignment on the following source systems:

- From SAP ERP Central Component (ECC) data source to SAP BusinessObjects Data Services data source
- From SAP ECC data source to SAP BW data source
- From SAP ECC data source to SAP BW/4HANA data source
- From SAP S/4HANA data source to SAP BusinessObjects Data Services data source
- From SAP S/4HANA data source to SAP BW data source
- From SAP S/4HANA data source to SAP BW/4HANA data source

## Glossary association

Enable glossary association and configure settings for the catalog source to automatically associate or recommend glossary terms as business names for data elements in technical assets.

The following table describes the settings:

Property	Description
Enable auto-acceptance	When enabled, this option automatically associates glossary terms with data elements based on the threshold limit that you specify. The automatically accepted glossary terms appear as business names of data elements in Data Governance and Catalog.
Confidence Score Threshold for Auto-Acceptance	Specify a percentage from 80 to 100 inclusive to set a threshold limit. If a glossary term matches a data asset within the threshold specified, Metadata Command Center automatically assigns the matching glossary term to the data element. The name and description of the glossary term with the highest confidence score appears as the name and description of the data element asset in Data Governance and Catalog.

Property	Description
Enable below-threshold recommendations	If you enable auto-acceptance, you can select this option to receive glossary association recommendations below the auto-acceptance threshold.
Confidence score threshold for recommendations	If you enable auto-acceptance, specify a percentage between 80% and the selected confidence score threshold for auto-acceptance. If you disable auto-acceptance, specify a percentage between 80% and 100%.
Assign business names and descriptions	Choose to automatically assign business names and descriptions to technical assets.
Keep existing business names and descriptions	Applicable if you choose to assign business names and descriptions. 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.
Ignore Keywords	Choose to ignore specific parts of data elements when making recommendations. You can enter multiple unique prefix and suffix keywords. Keyword values are case insensitive.
Glossary Association Scope	Choose specific top-level business glossary assets to associate with technical assets. Selecting a top-level asset selects its child assets as well.
Use Abbreviation and Synonym Definitions	Enable this option to use a lookup table with abbreviations and synonyms to improve glossary association accuracy. To upload a lookup synonym file with the abbreviations and synonyms, select <b>Yes</b> to enable, and then click <b>Select</b> .

**Note:** SAP ERP source systems can contain ambiguous data with technical field names. To generate accurate glossary associations, CLAIRE uses the extracted Business Name attribute for such technical field names.

For more information about the glossary association settings, see the *Administrator* help.

## CHAPTER 80

# SAP HANA Database

SAP HANA is a multi-model database system that stores data in its memory and performs high-speed processing and analytics of data. Configure an SAP HANA catalog source to extract metadata from an SAP HANA database.

### Objects extracted

Metadata Command Center extracts the following objects from an SAP HANA database source system:

- Table
- Column
- Plain SQL Database Views (Views created using the CREATE VIEW syntax)
- View Column
- Schema
- Calculation View  
Includes calculation views created in the HANA Deployment Infrastructure (HDI).
- Attribute
- Constraints (Primary Key and Foreign Key)
- Sequence

### Configure permissions or access to SAP HANA Database

To extract metadata and run profiles, you need account access and permissions on the SAP HANA Database source system.

#### Permissions to extract metadata

Grant permissions that allow you to perform the following operations:

- select on SYS.FUNCTIONS
- select on SYS.FUNCTION\_PARAMETERS
- select on SYS.PROCEDURES
- select on SYS.PROCEDURE\_PARAMETERS
- select on SYS.SYNONYMS
- select on SYS.SCHEMAS
- select on SYS.TABLES
- select on SYS.VIEWS
- select on SYS.TABLE\_COLUMNS
- select on SYS.VIEW\_COLUMNS

- select on SYS.M\_TABLES
- select on SYS.CONSTRAINTS
- select on SYS.REFERENTIAL\_CONSTRAINTS
- select on \_SYS\_REPO.ACTIVE\_OBJECT

Verify that you configure the following permissions for the username that you use to connect to the database:

- SELECT METADATA on the schemas for which you want to import metadata.
- SELECT on the \_SYS\_BI and \_SYS\_BIC system schemas.

To extract metadata from calculation views created in the HANA Deployment Infrastructure (HDI), verify that you have the following permissions:

- SELECT on \_SYS\_BI.BIMC\_SOURCES
- READ permission on the HDI Container schema database

### Permissions to run data profiles

Ensure that you have the required permissions to run profiles.

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

### Data classification for SAP HANA objects

Configure data classification for SAP HANA catalog sources to classify and organize data in your organization. You can view the data classification results in Data Governance and Catalog.

### Connection Properties

After you configure a connection to SAP HANA in Informatica Intelligent Cloud Services Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the SAP HANA connection properties:

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.
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent or serverless runtime environment.
Host	SAP HANA server host name.
Port	SAP HANA server port number.
Database Name	Name of the SAP HANA database.
Current Schema	SAP HANA database schema name.

Property	Description
Code Page	The code page of the database server defined in the connection. Select the UTF-8 code page.
Username	User name of the SAP HANA account.
Password	Password of the SAP HANA account. The password can contain alphanumeric characters and the following special characters: ~ ` ! @ # \$ % ^ & * ( ) _ - + = [ ]   : ; ' < , > . ? /

The following table describes the advanced connection properties:

Property	Description
Metadata Advanced Connection Properties	Not applicable for extracting metadata in Metadata Command Center.
Run-time Advanced Connection Properties	Not applicable for extracting metadata in Metadata Command Center.

## Data Profiling for SAP HANA objects

You can run data profiles and data quality tasks for SAP HANA database assets. Configure data profiling to run profiles on the metadata extracted from an SAP HANA database source system. You can view the profiling statistics in Data Governance and Catalog.

You can run data profiles on the following SAP HANA database objects:

- Tables
- Views
- Calculation Views

**Note:** Set the Input Parameter Default Value to 1000001 when you configure the source system.

### Sampling type

Determine the sample rows on which you want to run the data profiling task.

You can choose one of the following sampling types for an SAP HANA database catalog source:

- All Rows
- Limit N Rows
- Custom Query

## CHAPTER 81

# SAP PowerDesigner

See [SAP PowerDesigner Sources](#) to learn how to register and configure SAP PowerDesigner source systems 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 82

# SAP Sales & Service Cloud

See [SAP Sales & Service Cloud](#) to learn how to register and configure SAP Sales & Service Cloud source systems 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 83

# SAP S/4HANA Cloud - Preview catalog source

See [SAP S/4HANA Cloud Sources](#) to learn how to register and configure SAP S/4HANA Cloud source systems 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 84

# SAP SuccessFactors

See [SAP SuccessFactors Sources](#) to learn how to register and configure SAP SuccessFactors source systems 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 85

# SAS Base Libraries (Accelerator)

You can register and configure SAS Base Libraries (Accelerator) source systems 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.

## Introduction to SAS Base Libraries (Accelerator) 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, Base SAS is a source system from which you can extract metadata through an SAS Base Libraries (Accelerator) catalog source with Metadata Command Center.

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

**Note:** To enable and configure this catalog source, you need assistance from Informatica Professional Services. For more information, contact your account representative.

## CHAPTER 86

# SAS Base Programs (Accelerator)

See [SAS Base Programs \(Accelerator\) Sources](#) Sources to learn how to register and configure SAS Base Programs (Accelerator) source systems 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 87

# SFTP File System

See [SFTP File System Sources](#) to learn how to register and configure SFTP File System source systems 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 88

# Snowflake

See [Snowflake Sources](#) to learn how to register and configure Snowflake source systems 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 89

# Snowflake SQL Script

See [Snowflake SQL Script Sources](#) to learn how to register and configure Snowflake database source systems 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 90

# Strategy Cloud

See [Strategy Cloud Sources](#) to learn how to register and configure Strategy Cloud source systems 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 91

# Swagger API - Preview catalog source

See [Swagger API Sources](#) to learn how to register and configure Swagger API source systems 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 92

# Tableau

Tableau is a business intelligence tool that connects to data and create dashboards that can be shared.

### Objects extracted

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

- Calculation
- Data Source
- Dashboard
- Workbook
- Worksheet
  - Measure Names
- Project
- Server
- Site
- Stored Procedure

### Prerequisites for configuring the Tableau catalog source

Use the Tableau V3 connector to connect to the Tableau source system. For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.

To use the personal access token authentication type in a Tableau V3 connection, create a personal access token (PAT) on the Tableau Server. The personal access token allows you to sign in to Tableau REST API without requiring hard-coded credentials or interactive sign in.

### Configure permissions or access to Tableau

To connect to a Tableau Server, Metadata Command Center uses the credentials of a user created on the Tableau Server. Configure the user account with the Interactor license level and have the view and download permissions for all projects, workbooks, and catalog sources for which you want to extract metadata

### Connection properties

When you configure a connection to the Tableau source system in Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the Tableau connection properties:

Property	Description
Runtime Environment	The execution platform that run tasks. The runtime environment is either a Secure Agent or a serverless runtime environment.
Tableau Product	The type of Tableau component that is used for the metadata extraction. You can select Tableau Server or Tableau Online.
Authentication Method	The authentication method to connect to the Tableau source system. Select one of the following methods: <ul style="list-style-type: none"><li>• Username &amp; Password. Uses your Tableau account user name and password to connect to Tableau Server.</li><li>• Personal Access Token. Uses the personal access token and token secret from your Tableau account to connect to Tableau Server or Tableau Cloud.</li></ul>
Connection URL	URL to connect to the Tableau Server or Tableau Cloud account.
User Name	The user name to connect to the Tableau Server account.
Password	The password associated with the user name.
Personal Access Token Name	The personal access token to connect to the Tableau Server or Tableau Cloud account.
Token Secret	The token secret associated with the personal access token to connect to the Tableau Server or Tableau Cloud account.
Site ID	The site name that points to a specific site on Tableau Server or Tableau Cloud where you want to publish the data extract file.

## Referenced source systems

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. You must first create and run an endpoint catalog source that connects to the reference source system.

**Note:** You can view the lineage with reference objects without creating a connection assignment. After connection assignment, run the catalog source job again to view the actual objects.

You can assign the following source systems as endpoint catalog sources:

Source system	Object class type
File System	File System
Amazon Redshift	Database
Apache Hive	Database
Dremio	Database

Source system	Object class type
Generic ODBC	Database
Google BigQuery	Database
IBM Db2 for LUW	Database
IBM Netezza	Database
Microsoft SQL Server	Database
Oracle	Database
PostgreSQL	Database
SAP HANA Database	Database
SAP Business Warehouse (SAP BW)	Application
SAP BW4/HANA	Application
Snowflake	Database
Teradata Database	Database
Databricks	Database

### Configuration parameters for metadata extraction

Optionally, you can override default context values and job parameters on the **Configuration** tab.

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

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

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

## CHAPTER 93

# Talend Data Integration

See [Talend Data Integration Sources](#) to learn how to register and configure Talend Data Integration source systems 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 94

# Teradata BTEQ Script

See [Teradata BTEQ Script Sources](#) to learn how to register and configure Teradata database source systems 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.

# Teradata Database

Teradata Database is a Relational Database Management System (RDBMS) solution for data warehousing applications.

### Objects extracted

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

- Database
- Schema. The service extracts schemas along with descriptions.
- Table
- View
- Column
- Stored Procedure

### Prerequisites for configuring the Teradata Database catalog source

- Use the Teradata connector to connect to the Teradata Database source system.  
For information about configuring a connection in Administrator, see *Connections* in the Cloud Common Services help.
- To extract metadata from a Teradata source system, copy the Teradata drivers to the following location in your Secure Agent installation:
  - On Windows: `<agent_installation_location>\ext\connectors\thirdparty\teradata`
  - On Linux: `<agent_installation_location>/ext/connectors/thirdparty/teradata`

**Note:** For Teradata Database versions lower than 16.20, copy the `terajdbc.jar` and `tdgssconfig.jar` drivers to the Secure Agent location. For versions higher than 16.20, copy only the `terajdbc.jar` driver to the Secure Agent location.

### Configure permissions

To extract metadata and run profiles, you need account access and permissions for the Teradata database user account that you use to connect to the Teradata database.

### Permissions to extract metadata

The following table lists the schema objects and system tables on which configure SELECT permissions for the Teradata database user account:

Schema Objects	System Tables
<ul style="list-style-type: none"><li>- Tables</li><li>- Views</li><li>- Functions</li><li>- Database</li></ul>	<ul style="list-style-type: none"><li>- select on dbc.COLUMNSV</li><li>- select on dbc.TABLESV</li><li>- select on dbc.DATABASESV</li><li>- select on dbc.TABLETEXTV</li><li>- select on dbc.INDICESV</li><li>- select on dbc.ALL_RI_CHILDRENV</li></ul> <p>You need permission on System tables to execute the help macro on the database for offline catalog purposes only.</p>

### Permissions to run data profiles

To perform data profiling, grant the **SELECT** permission to read data from the Teradata database.

### Data profiling for Teradata objects

Configure data profiling to run profiles on the metadata extracted from a Teradata source system. You can view the profiling statistics in Data Governance and Catalog.

The data profiling task runs profiles on the following objects:

- Tables
- Views

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

- Bigint
- Byte
- Byteint
- Char
- Date
- Decimal
- Float
- Integer
- Smallint
- Time
- Timestamp
- Varbyte
- Varchar

### Sampling type

Determine the sample rows on which you want to run the data profiling task.

You can choose one of the following sampling types for a Teradata Database catalog source:

- All Rows. Runs the profile on all rows in the metadata.

- **Limit N Rows.** Runs the profile on a limited number of rows. You can specify the number of rows to run the profile on.
- **Custom Query.** Enter a custom SQL clause to select sample rows to run the data profiling task on. For example, **SAMPLE 100** or **WHERE ID = 90**. Verify that the syntax of the SQL clause matches the syntax of the database.

## Data classification for Teradata objects

Configure data classification for Teradata catalog sources to classify and organize data in your organization. You can view the data classification results in Data Governance and Catalog.

## Connection properties

After you configure a connection to Teradata Database in Informatica Intelligent Cloud Services Administrator, you can view the connection properties for that connection on the **Registration** page in Metadata Command Center.

The following table describes the Teradata connection properties:

Property	Description
Runtime Environment	A runtime environment is either Informatica Cloud Secure Agent or a serverless runtime environment.
TDPID	Teradata Director Program Identifier (TDPID) specifies the host name or IP address of the Teradata database to which you connect.
Database Name	The Teradata database name. If you do not enter a database name, Teradata PT API uses the default login database name.
Authentication Type	Select one of the following methods of authentication that verify the identity of a user connecting to Teradata database: <ul style="list-style-type: none"> <li>- Native. Default authentication type.</li> <li>- LDAP authentication.</li> <li>- KRB5. Kerberos authentication.</li> </ul>
Metadata Advanced Connection Properties	Optional. Use to configure advanced behavior and performance of the Teradata Metadata Services (MDS) component of the Teradata database. Default is tmode=ANSI. Separate multiple options with an ampersand as in the following example: key1=value1&key2=value2
User Name	Name of the user account that connects to the Teradata database.
Password	Password for the user account that connects to the Teradata database.



## CHAPTER 96

# Teradata FastExport Script

See [Teradata FastExport Script Sources](#) to learn how to register and configure Teradata database source systems 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 97

# Teradata FastLoad Script

See [Teradata FastLoad Script Sources](#) to learn how to register and configure Teradata database source systems 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 98

# Teradata MultiLoad Script

See [Teradata MultiLoad Script Sources](#) to learn how to register and configure Teradata database source systems 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 99

# TIBCO Spotfire

See [TIBCO Spotfire Sources](#) to learn how to register and configure TIBCO Spotfire source systems 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 100

# Workday

See [Workday](#) Sources to learn how to register and configure Workday source systems 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.

# Custom metadata integration

Custom metadata is metadata that you define for a source system for which Metadata Command Center does not provide connectors by default. Custom metadata integration is ingesting custom metadata from any source system into the catalog. Such source systems are called custom source systems.

You can configure a custom catalog source to load metadata into the catalog using the following sources:

- Metadata definition files
- Cloud Data Integration
- Java SDK

**Preview Notice:** Effective in the July 2023 release, loading metadata into the catalog from Cloud Data Integration and Java SDK are 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.

To learn how to load metadata into the catalog from Cloud Data Integration, refer to the following tutorial: [Load custom metadata using Data Integration in Metadata Command Center](#)

To learn how to load metadata into the catalog using Java SDK, refer to the following tutorial: [Load custom metadata using Java SDK in Metadata Command Center](#)

To ingest custom metadata from a source system, perform the following high-level tasks:

### Create a custom model or reuse a system model

A model defines the structure of metadata stored in the catalog. It contains classes, associations, and attributes of the metadata. By default, Metadata Command Center provides models for multiple source systems from which you can extract metadata. These models are called system models. However, to ingest metadata from source systems for which Metadata Command Center doesn't provide a system model, you need to first define a custom model.

Use a custom model to load metadata from any source system into the catalog to meet your business requirements. For example, you are a data analyst in your organization and you need to prepare a report on the annual sales on your e-commerce website. The data that is required to prepare the report is stored in Microsoft Access Database and you are expected to ingest the data from Microsoft Access Database into Data Governance and Catalog. Since Metadata Command Center does not provide a model for Microsoft Access Database, you can create a custom model to ingest metadata from this specific source system into the catalog.

### Create a custom catalog source type

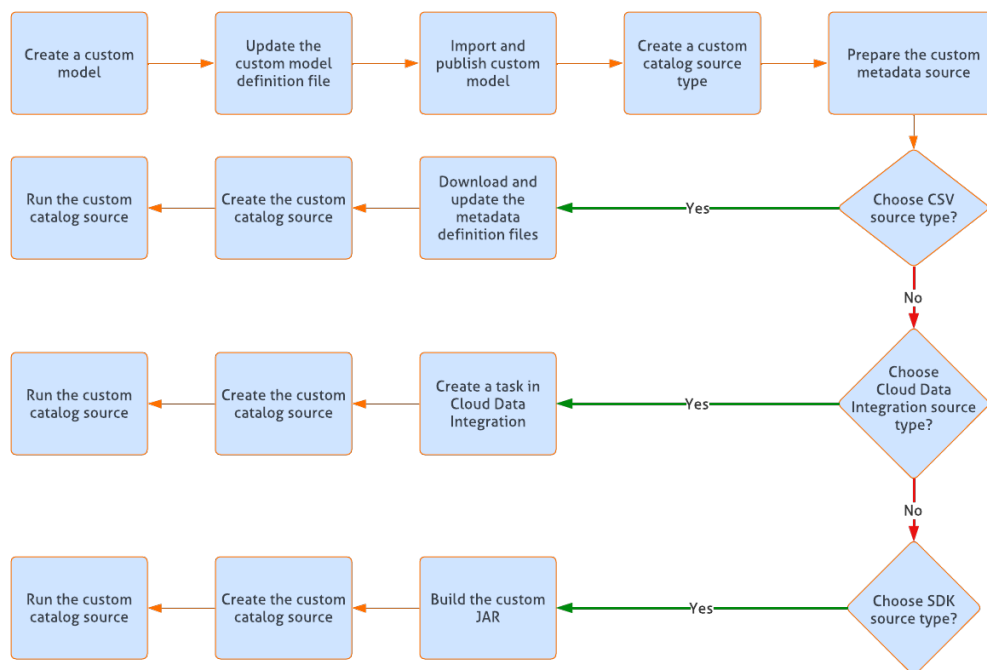
A custom catalog source type represents the type of custom source system from which you want to ingest the metadata. After you define the custom model or reuse a system model, create a custom catalog source type.

## Create a custom catalog source

Based on the custom catalog source type, create a custom catalog source. When you create the custom catalog source, provide the details of the metadata that you want to ingest from the source system into the catalog.

# Workflow for custom metadata integration

To ingest metadata from a source system, verify whether you can reuse a system model. For example, to ingest metadata from any relational source system, you can use the relational system model included in Metadata Command Center. If you cannot reuse a system model available in Metadata Command Center, perform the following steps to integrate custom metadata into the catalog.



## Step 1. Create a custom model

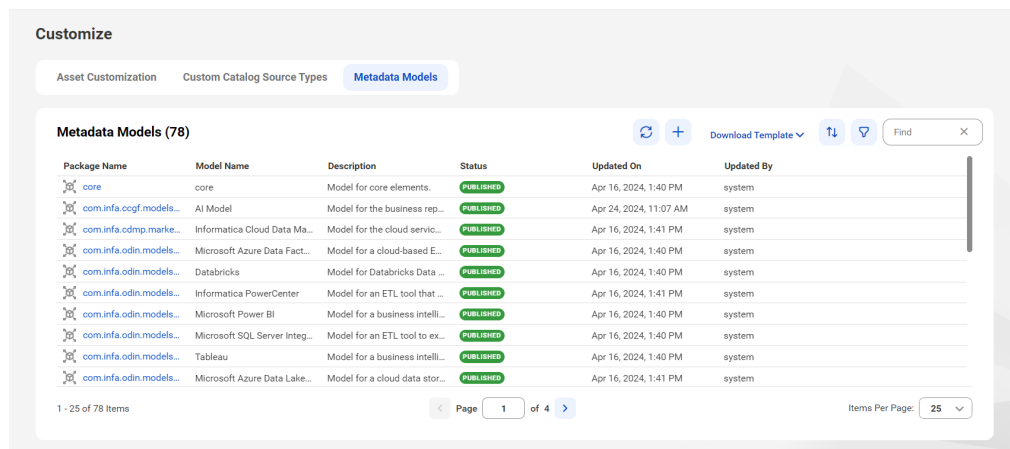
When you create a custom model for custom metadata integration, you configure the metadata that you want to ingest in the catalog. You can also configure options to search, filter, and sort the custom metadata ingested into the catalog.

Create a custom model in one of the following ways:

- Reuse a system model and update the model definition to create and define a custom model. For example, to create a custom model for a relational source system, you can use the `com.infa.odin.models.relational` model included in Metadata Command Center.
- Create a model on your own by using the template model definition file that is available for download in Metadata Command Center.

To create a custom model, perform the following steps:

1. On the **Customize** page, go to the **Metadata Models** tab.



2. To use an existing model that Metadata Command Center provides by default, hover your mouse on the model of your choice and click the **Download Model** icon on the far right.

The model definition file in the JSON format is downloaded to your machine. The file contains the package name, properties, classes, attributes, and associations of the objects in the source system.

3. Alternatively, click the **Download Template** menu and choose **Model**.

The sample model file, `sample.json`, is downloaded to you machine. This file contains sample classes, attributes, and associations that you want to extract from the custom source system.

After downloading the sample model or an existing model, update the details of the metadata following the template structure. Then, import the custom model and publish it in Metadata Command Center.

## Step 2. Update the custom model definition file

In the model definition JSON file, update the package details, parent classes, subclasses, attributes and associations of the objects in the custom source system based on your business requirements.

Open the JSON file in a text editor of your choice and update the following components of the model file:

### Package

The name of the custom model. For example, `com.example.accessdb`. The package represents a container for the classes in the model. Verify that the package name does not contain `com.infa.odin`, `com.informatica` or `infa`. These keywords are reserved for system models.

### Required Packages

A comma-separated list of required or reused package names. Use the fully-qualified package names if you are reusing any components such as classes, attributes, or associations from other packages. Verify that you define the name of the package as `core` if you are reusing other packages. For example, `core`.

### Classes

A class describes a group of objects that share the same characteristics. Each class has a set of attributes, those that belongs to itself or from its super classes. It represents the metadata objects that you want to extract from the custom source system. For example, `AccessSchema` is the root class for a model that you define for the Microsoft Access Database source system. `AccessTable` and `AccessView` are the child classes of the `AccessSchema` class. For information about the class properties that you need to define in the model, see ["Add class properties" on page 257](#).



## Attributes

An attribute describes the characteristics of an object. Define the model attributes and how they apply to classes and relationship by creating `attributeClass` entries and `attributeRelationship` entries. For information about the attribute properties that you need to define in the model, see [“Add attribute properties” on page 258](#).

## Associations

An association represents the relationship between two objects in the catalog. You can create associations between the objects within the custom catalog source and to objects already synced to the catalog. For example, for a model that you define for the Microsoft Access Database source system, the columns in the `AccessTable` schema has an association with columns in an Oracle database. For information about the association properties that you need to define in the model, see [“Add association properties” on page 259](#).

## Data Type

The data type defines the types of values possible for an attribute. For example, string and integer. For information about the data types that you need to define in the model, see [“Add data types” on page 260](#).

## Add class properties

Define the following class properties in the `classes` component of the custom model JSON file.

Property	Description
name	The name of the class.
label	The text displayed to the user to describe this entity.
externalLabel	Not in use.*
description	The description of the class displayed to the user.
isFirstClass	Use this property to prioritize the class in search. Set to true or false. If set to true, Metadata Command Center displays the object count of the classes after you run the catalog source.
IsAbstract	Use this property to specify whether the class is abstract or not. Set to true or false.
cdc	Use this property to specify if the class participates in change data capture. Change data capture is used to record the applied changes for audit purposes. Set to true or false.
superClasses	The list of classes with which the class has a semantic relationship.
deprecated	Use this property to specify whether the class is deprecated. Set to true or false.
indexType	Use this property to specify whether the class can be indexed or not. Specify any of the following values: <ul style="list-style-type: none"><li>- FULL. Indexed in both the elastic and graph stores.</li><li>- FULL_TEXT. Indexed in elastic, but not in the graph store.</li><li>- NONE. Not indexed.</li></ul>
appendOnly	Not in use.*
extensions	Indicates extension classes. Extension classes are classes that are linked to other classes. Multiple classes can have the same extension class. It contains common attributes linked to different master classes.

Property	Description
softDeleted	Not in use.*
system	Classes indicated as system do not inherit any property from the IClass abstract class. System classes are organized at the same level as IClass.
* The properties that are not in use can be ignored.	

## Add attribute properties

Define the following attribute properties in the `attributes` component of the custom model JSON file.

Property	Description
name	The name of the attribute.
label	The text displayed to the user to describe this attribute.
dataType	The data type of the attribute.
description	The description of the attribute displayed to the user.
multivalued	Use this property to specify if the attribute can have multiple values. Set to true or false.
deprecated	Use this property to specify whether the attribute is deprecated or not. Set to true or false.
derived	Use this property to specify if this attribute is derived from an existing attribute.
data	Use this property to specify whether its metadata is derived from Data. This property is used to handle sensitive attributes like value frequencies or data patterns. Set to true or false.
custom	Use this property to specify if the class should be marked as searchable. Set to true or false.
reference	The reference attribute references a registered association and its target class as a native data type of the source class. Use this property to specify the association type to relate the class from which the attribute needs to be projected based on the projectionCondition attribute value.
referencedAssociationAttributes	Not in use.*
referencedAttributes	Use this property to specify projected attributes.
projectionType	Use this property to specify the attribute type to be projected to other classes. Specify any of the following values: - PRIMITIVE. Project a single attribute - NESTED. Project a nested attribute Define the projected attribute in referencedAttributes.
projectionExpressions	The condition to be applied to project an attribute.

Property	Description
defaultValues	The value to be applied if the user does not provide values for ingestion.
isSystem	Use this property to specify whether system attributes should be added for every object or association that is ingested. Set to true or false.
embedded	Use this property to specify whether the reference data type is embedded into the same class as a struct or created as an extension table. Set to true or false.
searchConfiguration	<p>Use this property to specify the search configuration for indexing before data is ingested.</p> <p>Specify any of the following values:</p> <ul style="list-style-type: none"> <li>- <b>AttributeType</b>. Indicates if the attribute is searchable or viewable. Only searchable attributes are indexed and can be searched.</li> </ul> <p><b>Note:</b> You can change the attribute type from VIEWABLE to SEARCHABLE.</p> <ul style="list-style-type: none"> <li>- <b>FieldMappingTemplate</b>. Elasticsearch uses dynamic mapping to infer the data type of each field and assigns a field type to store each field. Use this property to map attributes in the field mapping template and assign a type to each field.</li> <li>- <b>Suggestable</b>. Suggests similar looking terms based on the provided text.</li> <li>- <b>Aggregatable</b>. Enables aggregate functions on search operations.</li> <li>- <b>Sortable</b>. Enables sorting on search results.</li> </ul>
projectionCondition	The condition to project the attribute. You can define conditions in the projectionExpressions and expressionContext attributes.
customizations	Indicates whether you can customize the attribute or not.
deleted	Indicates if the attribute is deleted. You can't use deleted attributes. Use this property to track deleted attributes.
* The properties that are not in use can be ignored.	

## Add association properties

Define the following association properties in the `associations` component of the custom model JSON file.

Property	Description
name	The name of the association.
label	The text displayed to the user to describe the association.
description	The description of the association displayed to the user.
fromClass	The source class of the association.
toLabel	The text that describes the relationship to the target class.
fromLabel	The text that describes the relationship from the source class.
toClass	The target class of the association.

Property	Description
associationKinds	The type of relationship or association between objects in the source system.
deprecated	Use this property to specify whether the association is deprecated or not. Set to true or false.
cdc	Use this property to specify if the association participates in change data capture. Change data capture is used to record the applied changes for audit purposes. Set to true or false.
unidirectional	Indicates if the association is only valid for one direction. Set to true or false.
aggregate	Not in use.*
cardinality	Use this property to specify the cardinality. The value can be OneToOne and OneToMany.
index	Use this property to specify the index type for the association. Set to COLLECTION to configure a single elastic document as a collection for classes that are not prioritized using the isFirstClass property.
customizable	Indicates whether you can customize the association or not. Set to true or false.
custom	Indicates whether the association is customized at least once or not. Set to true or false.
deleted	Indicates if the association is deleted. You can't use deleted associations. Use this property to track deleted associations.
* The properties that are not in use can be ignored.	

## Add data types

You can define the data types in a custom model using the following list of core types available in Metadata Command Center:

- STRING
- BOOLEAN
- DATE
- DECIMAL
- RICHTEXT
- INTEGER
- PAIR
- LONG
- Reference Class
- DOUBLE
- DATETIME
- MAP<STRING,CORETYPE>

In the following example, the data type, `curationStatusEnum`, is defined using the core type, `STRING`. Similarly, you can define any data type in a model using the available core types.

```
{
  "name": "curationStatusEnum",
  "constraint": {
    "constraintType": "LIST_OF_VALUES",
```

```

"values": [
  "AUTO_ACCEPTED",
  "ACCEPTED",
  "REJECTED",
  "NONE"
],
"coreType": "STRING",
"deprecated": false
}

```

## Step 3. Import and publish the custom model

After you have created and defined the model for the custom metadata in the JSON file, you can import and publish the custom model. Based on the custom model, Metadata Command Center organizes the storage of the custom metadata that is ingested. To import and publish the custom model, perform the following steps:

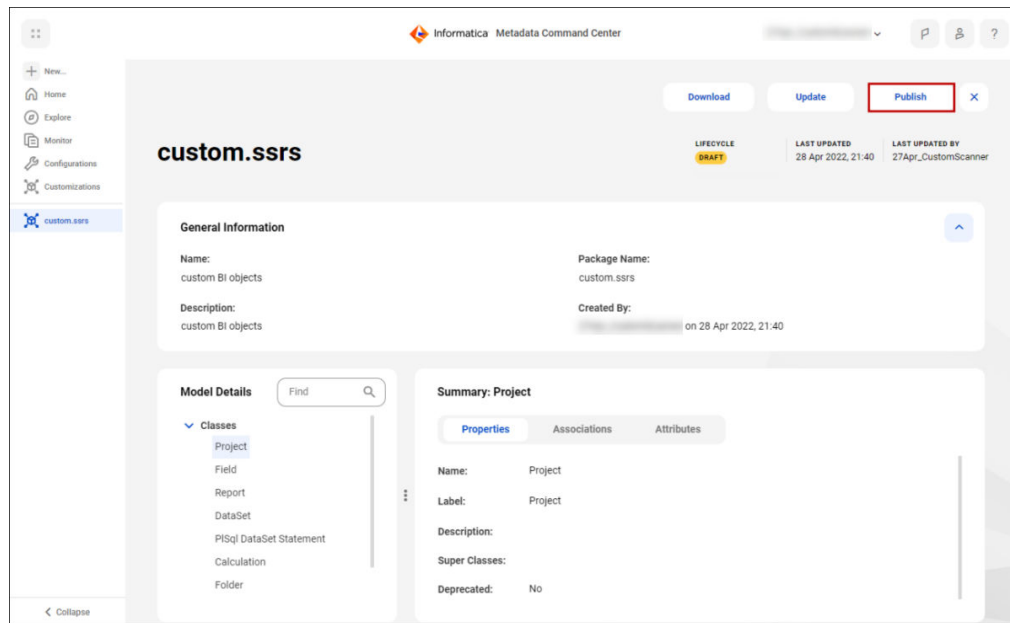
1. Click **New** in the left navigation panel.
2. In the **New** dialog box, select **Customization** from the list in the left pane, and click **Metadata Model** on the right pane.

You can also click the plus icon on the **Metadata Models** page to create a new model.

3. In the **New Model** window, click **Choose File** to upload a JSON-based model definition file that you have created for the custom metadata.
4. Enter a package name for the model.  
Verify that the package name is the same as defined in the model definition JSON file.
5. Click **Create**.

This creates a draft version of the model that appears on the **Metadata Models** page.

- From the **Metadata Models** page, select the model that you imported. You can view the model details including the classes, attributes, and associations that you defined in the model.



- Verify that your model appears as you expected. To make any updates to the model, modify the JSON file on your machine and click **Update** to import the latest version of the model file.

**Note:** You cannot modify the package name once you have imported the model.

- To publish the model, click **Publish**.

The Model Publish job is triggered. You can click **View Status** to monitor the exact status of the job on the Job Monitoring Overview page of that job. After the publishing is successful, the lifecycle of the model changes from Draft to Published. Note that you cannot import an updated model while the model publish job is in progress.

Note the following points about the lifecycle of a model:

- If you update a custom model after it is published, the lifecycle of the model changes to **Published with Draft Available**. You can publish the model again or switch the lifecycle of the model from **Draft** to **Published** to access the published version. By default, the **Draft** version of the model is displayed.
- You cannot discard a model if the lifecycle of the model is in the published state. You can discard only the draft version of the model.
- You cannot modify or delete system models.

## Step 4. Create a custom catalog source type

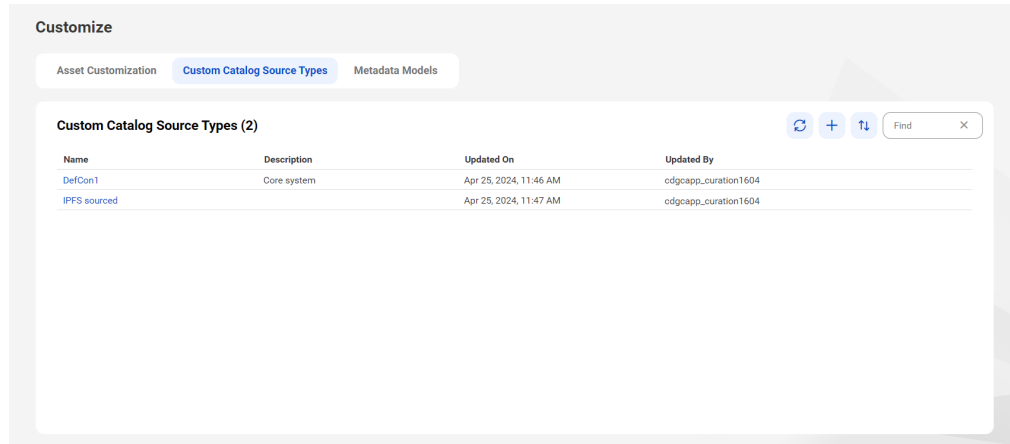
The custom catalog source type represents the custom source system from which you want to ingest the metadata. By default, Metadata Command Center provides connections for a variety of source systems. To ingest metadata from source systems for which there are no predefined catalog source types available in Metadata Command Center, create a custom catalog source type based on which you can then create a custom catalog source.

To create a custom catalog source type, define appropriate roles and assign the Create, Read, Update, and Delete permissions for the **Custom Catalog Source Type** asset for that role in Administrator. For more information about asset permissions that the organization administrator can configure for user roles, see *Asset permissions* in the Administrator help.

To create a custom catalog source type, perform the following steps:

1. Click **New** in the left navigation panel.
2. In the **New** dialog box, select **Customization** from the list of asset types in the left pane, and click **Custom Catalog Source Type** on the right pane.
3. Enter a name that describes the source system from which you want to extract metadata.
4. Optionally, enter a description of the source system and click **Save**.

The new custom catalog source type appears in the list of custom catalog sources types on the **Customize** page.



5. To modify the name or description of the catalog source type, click the name of the catalog source type, update the name or description of the catalog source type and click **Save**.

You're now ready to create a custom catalog source based on the custom catalog source type.

## Step 5. Prepare the custom metadata source

To load metadata from a custom source system, prepare the custom metadata source based on the metadata source type. You can choose to load metadata into the catalog using CSV files, Cloud Data Integration, or Java SDK.

If you choose to use CSV files as the custom metadata source, download and update the metadata definition files.

If you choose to use Cloud Data Integration as the custom metadata source, create and run a mapping task or a linear taskflow in Cloud Data Integration. CSV files that contain metadata are generated from a mapping task or a linear taskflow in Cloud Data Integration.

If you choose to use Java SDK as the custom metadata source, build a custom JAR, and copy it to any location on the Secure Agent machine.

**Preview Notice:** Effective in the July 2023 release, loading metadata into the catalog using Cloud Data Integration and Java SDK are 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.

### Load metadata into the catalog using CSV files

Before you create the custom catalog source, download the metadata definition files and enter the details of the metadata that you want to ingest from the custom source system into the metadata files.

Download and update the metadata files template. In the file, add the object details of the specific classes that you defined in the custom model for this source system. Metadata Command Center uses the details entered in the metadata files to load metadata from the custom source system into the catalog.

1. Go to the **Customization** page and click the **Metadata Models** tab.
2. Click the custom model that you created in [“Step 1. Create a custom model” on page 255](#).
3. Click **Download Template > Metadata**.  
This downloads the metadata template in the ZIP format to your machine. The ZIP file might contain multiple CSV files for the metadata that you have defined in the custom model.
4. Extract the CSV files included in the ZIP file.  
The ZIP file contains the following CSV files:
  - Object files. The ZIP file might contain multiple object files depending on the number of classes defined in the custom model. The object files are in the following format: `<package name>.<class name>`. You can map each object file to its class in the custom model. Use these files to enter details of objects in the custom source system.
  - links.csv file. This file contains association details between the objects in the source systems. You can associate objects within the source system and define relationships to objects in external source systems. Verify that the metadata file template contains only one links.csv file.

Open the CSV files in a text editor and enter the objects, association, and lineage details.

5. Enter the details of each object in separate CSV files. Each object corresponds to a specific class that you define in the custom model.  
The following table lists the details that you need to enter in the CSV file for each object of the source system:

Header Field	Description
core.externalId	Required. Unique identity of the object. The ID cannot contain a comma.
core.reference	Optional. Set to true if you want to use this object as a reference asset. Reference assets are used in place of actual assets to view the data lineage among one or more sources that don't exist in the catalog. For more information about using reference assets for custom lineage, see <a href="#">“Referenced catalog sources” on page 24</a> and <a href="#">“Create custom lineage” on page 280</a> .
core.assignable	Optional. Set to true if you want this object to be available for connection assignment. If set to true, you can assign connections to this object to view the complete lineage.
core.name	Required. Name of the object.
core.description	Optional. Description of the object.
core.businessName	Optional. Specify the name of the business term that you want to associate with this object.
core.businessDescription	Optional. Specify the description of the business term that you want to associate with this object.

6. Define associations between the objects in source system in the links.csv file that is included in the template. Define all associations between the objects or classes that you defined in the custom model for this source system. The type of associations that you specify depends on the type of associations defined in the `associationKinds` property in the custom model. Create each entry on a separate line.



The following table lists the association details that you need to enter in the `links.csv` file:

Header Fields	
Source	<p>Required. Unique external ID of the source object in the association. Specify the ID of the object in a parent-child format and verify that the ID of the object matches the external ID of the object provided in the objects CSV file.</p> <p>For example, if the source object is a view, then the identity has the full path to the view, that is, <code>Schema/Table/Column/View</code>.</p> <p><b>Note:</b> <code>\$resource</code> represents the catalog source. For this source object, the target object is the root class that is defined in the model. This creates a parent-child association between the specified catalog source and the root class or object in the source system.</p>
Target	<p>Required. Unique external ID of the target object in the association. Specify the ID of the object in a parent-child format and verify that the ID of the object matches the external ID of the object provided in the objects CSV file.</p> <p>For example, if the target object is a table, then the identity has a full path to the table, that is, <code>Schema/Table</code>.</p>
Association	<p>Required. The name of the association in the source system. Specify the association for objects in the <code>&lt;package name&gt;.&lt;association name&gt;</code> format.</p>

7. Include all the CSV files and create a ZIP file.

### Load metadata into the catalog using Cloud Data Integration

To load metadata from Cloud Data Integration, create a mapping task in Cloud Data Integration, run the task, and verify that the mappings generate CSV files.

Verify that the name of the CSV file contains the package name of the metadata model and the component class in the following format: `<Package name>.<Class name>.csv`. For example, the CSV file generated from a metadata model with the package name `com.infa.model.relational` for the class `Table` is `com.infa.model.relational.Table.csv`.

**Note:** The header fields in the CSV files can contain an underscore (`_`).

### Load metadata into the catalog using Java SDK

To load metadata into the catalog using Java SDK, build a custom JAR, and copy it to any location on the Secure Agent machine. Informatica provides an Oracle, a Swagger, and a Denodo sample project to help you build custom JARs.

To build a custom JAR, perform the following steps:

1. Download a sample project ZIP file from the following location: `<Informatica Secure Agent installation directory>/apps/Metadata_Foundation_Agent/<version>/data/scanner/custom/`

**Note:** Informatica provides several sample project ZIP files. Choose the ZIP file that is most suitable for your use case.

  - For the Oracle sample project, use the `sample-custom-sdk-scanner-oracle-xxxx.zip` file.
  - For the Swagger sample project, use the `sample-custom-sdk-scanner-swagger-xxxx.zip` file.
  - For the Denodo sample project, use the `sample-custom-sdk-scanner-denodo-xxxx.zip` file.

Here, `xxxx` represents the bundle version.
2. Copy and extract the ZIP file to a machine that has an integrated development environment (IDE).

3. Import the sample project to a suitable IDE.  
To build the custom JAR with the Denodo sample project, copy the `denodo-vdp-jdbcdriver.jar` to the `lib` folder of the extracted ZIP file. The Denodo JAR is available in the following location: `<Denodo installation directory>/tools/client-drivers/jdbc/`
4. Run the `gradle clean build` command.  
**Note:** If you want to use a build tool other than Gradle, use the `custom-scanner-sdk-contract-xxxx.jar` file present in the `lib` folder of the extracted ZIP file. Add the `custom-scanner-sdk-contract-xxxx.jar` file to the project class path.
5. To build the custom JAR with a sample project, use the Java file located in the `src` folder of the extracted ZIP file.  
To build the custom JAR with the Oracle sample project, use the `CustomOracleScanner.java` file located in the `src` folder of the extracted ZIP file.  
To build the custom JAR with the Swagger sample project, use the `CustomSwaggerScanner.java` file located in the `src` folder of the extracted ZIP file.  
To build the custom JAR with the Denodo sample project, use the `CustomDenodoScanner.java` file located in the `src` folder of the extracted ZIP file.
6. Implement the code in Java to ingest metadata from the custom source system.
7. Build the JAR based on your requirements.  
You must specify the main class to be executed in the JAR. You can either include all the dependent classes in the JAR and build a fat JAR, or specify class paths in the manifest file to include any external libraries provided outside of the main JAR.  
**Note:** Use Java Standard Edition version 17, 11, or 8 to build JARs. Newer Java versions will be supported in future releases.  
**Important:** Informatica is not responsible for any security vulnerabilities that might be associated with the custom JAR.
8. Copy the JAR to any location on the Secure Agent machine.

Consider the following points when you build custom JARs using the Swagger sample project:

- The Swagger model file is provided as part of the Swagger sample project and is available in the following location:  
`sample-custom-sdk-scanner-swagger\src\main\resources\swagger.api.json`
- You must import and publish the Swagger model file in the **Metadata Models** page.
- When you create a custom catalog source for a custom JAR, the name of the configuration parameter must be "Swagger Path". The custom catalog source can extract metadata from multiple JSON files placed in different folders. The value can be the path to a Swagger parent folder that contains the JSON Swagger files or to a JSON Swagger file on the Secure Agent machine.
- You can build custom JARs only from JSON Swagger files.
- The Swagger sample project uses the `swagger-parser-2.0.33` library validated on the OpenAPI 3.0 version. You can also update the Swagger parser library version and build custom JARs with newer OpenAPI versions.

#### Guidelines and best practices to build custom JARs

Consider the following rules and guidelines when you build custom JARs:

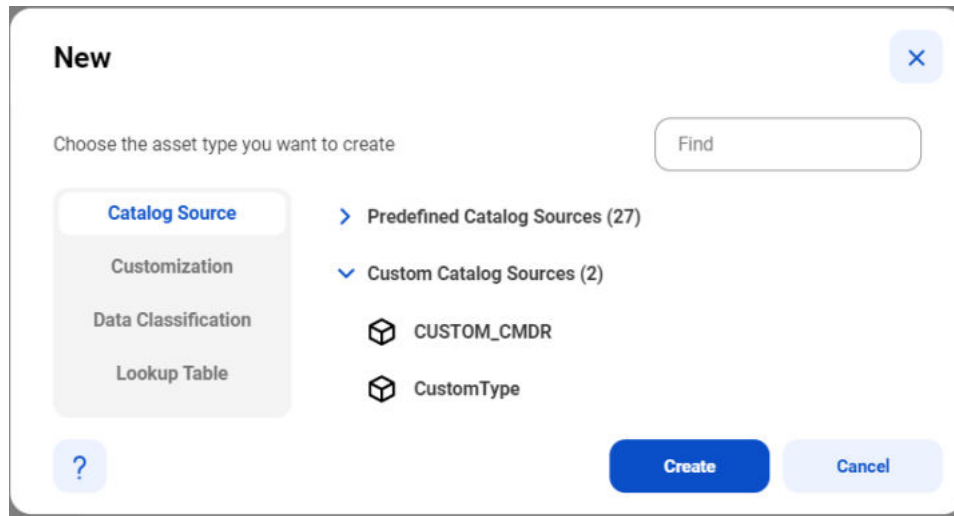
- Use Gradle build tool version 6.8.1.
- Use only the `yyyy-MM-dd'T'HH:mm:ss` date format in the Java file to extract and view metadata of system attributes in Data Governance and Catalog.

## Step 6. Create the custom catalog source

After you import and publish a custom model and define the details of your metadata in the metadata files, create a custom catalog source based on the source type.

To create a custom catalog source, define appropriate roles and assign the Create, Read, Update, and Delete permissions for the **Custom Catalog Source Type** asset for that role in Informatica Intelligent Cloud Services Administrator. For more information about asset permissions that the organization administrator can configure for user roles, see *Asset permissions* in the *Administration* help.

1. Click **New** in the left navigation panel and select **Catalog Source** from the list of asset types in the left pane.
2. Expand **Custom Catalog Source Type** on the right pane and select the custom catalog source type that you created for your source system.



3. Click **Create**.
4. On the **Registration** page, enter a name and an optional description for the custom catalog source.
5. In the **Connection Information** area, configure the following options:
  - **Metadata Source Type.** Choose **CSV Files** if you want to load metadata using the metadata ZIP file that contains the CSV files. Choose **CDI Task** if you want to load metadata using Cloud Data Integration. Choose **Java SDK** if you want to load metadata using custom JAR files.
  - If you selected **CSV Files** as the metadata source, configure the following options:

Parameter	Description
Source Type	Choose <b>Upload</b> if you want to upload the metadata ZIP file from your machine or choose <b>Provide a Local Path</b> to provide the path to the ZIP file located in your runtime environment.
File Details	Applicable if you chose to upload the ZIP file. Click <b>Browse</b> to select the ZIP file that you created for the custom metadata. Alternatively, you can drag and drop the file in the file box. <b>Note:</b> You can't upload a ZIP file that has dots in the file name. The dot that separates the file name from the extension is allowed.

Parameter	Description
Runtime Environment	Applicable if you chose the <b>Provide a Local Path</b> option. From the list, select the name of the runtime environment where the metadata file is located.
Secure Agent	Applicable if you chose the <b>Provide a Local Path</b> option. Specify the name of the Secure Agent that contains the metadata file.
Path	Applicable if you chose the <b>Provide a Local Path</b> option. Specify the absolute path to the ZIP file in the Secure Agent.

- If you selected **CDI Task** as the metadata source, configure the following options:

Parameter	Description
Task	Click <b>Browse</b> to select a Cloud Data Integration mapping task or a linear taskflow within a project and folder.
Runtime Environment	Choose the runtime environment that contains the Secure Agent where the metadata file is located.
Secure Agent	Choose the Secure Agent machine that stores the metadata files generated by Cloud Data Integration.
Path	Enter the path to the CSV files on the machine that hosts the Secure Agent. Use the path that you specified when you created the Cloud Data Integration task. <b>Note:</b> If you intend to use the same path for subsequent mapping tasks, ensure that you delete the files in the directory.

- If you selected **Java SDK** as the metadata source, configure the following options:

Parameter	Description
Runtime Environment	Choose the runtime environment that contains the Secure Agent where the JAR is located.
Secure Agent	Choose the Secure Agent machine that stores the JAR files.
Executable JAR Path	Enter the absolute path to the executable JAR on the Secure Agent machine.

6. Click **Next** to go to the **Configuration** page.

On the **Configuration** page, the Metadata Extraction capability is enabled by default.

If you selected **Java SDK** as the metadata source and want to pass parameters for your custom JAR, add configuration parameters on the **Metadata Extraction** tab. For example, you can add driver class, URL, username, and password as configuration parameters to connect to an Oracle database.

To pass parameters for a custom JAR built using the Swagger sample project, configure the following options in the **Configuration Parameters** area:

Parameter	Description
Name	Enter the name as "Swagger Path".
Value	Enter the path to a Swagger parent folder that contains the JSON Swagger files or to a JSON Swagger file on the Secure Agent machine. The custom catalog source can extract metadata from multiple JSON files placed in different folders.

To pass parameters for a custom JAR built using the Denodo sample project, configure the following options in the **Configuration Parameters** area:

Name	Value
Enter the name as "url".	Enter the URL to access the Denodo source system. Example: jdbc:denodo://<host name>:<port number>/admin By default, the port number is 9999.
Enter the name as "userName".	Enter the username to log in to the Denodo server.
Enter the name as "password".	Enter the password associated with the username.
Enter the name as "schema".	Enter the schema to connect to the Denodo server.

You can enable lineage discovery, data classification, and glossary association for the custom catalog source. For more information about enabling these capabilities, see [“Step 2. Configure a catalog source” on page 12](#).

7. Click **Next** to go to the **Associations** page.

Assign permissions to users to access this custom catalog source. For more information about assigning roles and users to technical assets, see [“Step 3. Associate stakeholders and asset groups” on page 16](#).

8. Click **Next** to go to the Schedule page.

Optionally, select schedules to run the catalog source job.

9. Click **Save**.

After you save the custom catalog source, it appears in the list of catalog sources on the **Explore** page on the left navigation tab.

## Step 7. Run the custom catalog source

When the catalog source runs, Metadata Command Center processes the metadata from the CSV files and ingests the metadata from the source system into the catalog.

You can run the custom catalog source in one of the following ways:

- Click **Run** on the custom catalog source creation wizard and click **Run** again on the **Run Catalog Source Job** dialog box.
- Optionally, select **Run** from the Action menu on the **Explore** page for the custom catalog source.

A job is triggered to run the catalog source. You can monitor the status of the job on the **Overview** page for that catalog source job.

When the catalog source job is successful, you can search for the custom catalog source in Data Governance and Catalog and view the ingested assets from the custom source system.

## Example: Ingest metadata from Microsoft Access database

You are a data analyst in your organization and you need to prepare a report on the annual sales on your e-commerce website. The data that is required to prepare the report is stored in Microsoft Access database and you are expected to ingest the data from Microsoft Access database into Data Governance and Catalog. Since Metadata Command Center does not provide a predefined source system for Microsoft Access database, you can create a custom catalog source to ingest metadata from this specific source system into the catalog.

In this example, let's define a custom model and update the metadata definition files to ingest metadata from Microsoft Access database. For the complete workflow of ingesting metadata from a custom source system, see [“Workflow for custom metadata integration” on page 255](#).

### Define the custom model

To create a custom model, you can either reuse a system model or download the template model definition file. See [“Step 1. Create a custom model” on page 255](#).

In the custom model JSON file for Microsoft Access database, define the appropriate classes, attributes, and associations.

#### Classes

Define the following classes in the custom model for Microsoft Access database:

Class	Type
AccessSchema	Schema
AccessTable	Table
AccessTableColumn	Column
AccessView	View
AccessViewColumn	View column

#### Attributes

Define the following attributes in the custom model for Microsoft Access database:

Attribute	Data Type
Name	String

Attribute	Data Type
Abbreviation	String
Business Usage	String
DateCreated	String
Datatype	String
Length	String

## Associations

Define the following attributes in the custom model for Microsoft Access database:

Association	Association Type
AccessSchemaAccessTable	Parent-child
AccessTableAccessTableColumn	Parent-child
AccessSchemaAccessView	Parent-child
AccessViewAccessViewColumn	Parent-child

## Sample custom model JSON file

The following JSON file is the sample custom model for Microsoft Access database. It defines classes, attributes, and associations for the Microsoft Access database from which you want to extract metadata:

```
{
  "packageName": "relational.accessdb",
  "packageLabel": "Access DB Objects",
  "packageDescription": "Model for Access DB Objects",
  "deprecated": false,
  "attributes": [{
    "name": "Name",
    "label": "Name1",
    "dataType": "core.String",
    "description": "",
    "multivalued": false,
    "deprecated": false,
    "derived": false,
    "data": false,
    "isCustom": false,
    "defaultValues": [],
    "isSystem": false,
    "embedded": false,
    "searchConfiguration": {
      "suggestable": false,
      "aggregatable": false,
      "sortable": false,
      "attributeType": "VIEWABLE"
    }
  }],
  {
    "name": "Abbreviation",
    "label": "Abbreviation",
    "dataType": "core.String",
    "description": "",
    "multivalued": false,
```

```

    "deprecated": false,
    "derived": false,
    "data": false,
    "isCustom": false,
    "defaultValues": [],
    "isSystem": false,
    "embedded": false,
    "searchConfiguration": {
        "suggestable": false,
        "aggregatable": false,
        "sortable": false,
        "attributeType": "VIEWABLE"
    }
},
{
    "name": "BusinessUsage",
    "label": "Business Usage",
    "dataType": "core.String",
    "description": "",
    "multivalued": false,
    "deprecated": false,
    "derived": false,
    "data": false,
    "isCustom": false,
    "defaultValues": [],
    "isSystem": false,
    "embedded": false,
    "searchConfiguration": {
        "suggestable": false,
        "aggregatable": false,
        "sortable": false,
        "attributeType": "VIEWABLE"
    }
},
{
    "name": "DateCreated",
    "label": "Date Created",
    "dataType": "core.String",
    "description": "",
    "multivalued": false,
    "deprecated": false,
    "derived": false,
    "data": false,
    "isCustom": false,
    "defaultValues": [],
    "isSystem": false,
    "embedded": false,
    "searchConfiguration": {
        "suggestable": false,
        "aggregatable": false,
        "sortable": false,
        "attributeType": "VIEWABLE"
    }
},
{
    "name": "Datatype",
    "label": "Datatype",
    "dataType": "core.String",
    "description": "",
    "multivalued": false,
    "deprecated": false,
    "derived": false,
    "data": false,
    "isCustom": false,
    "defaultValues": [],
    "isSystem": false,
    "embedded": false,
    "searchConfiguration": {
        "suggestable": false,
        "aggregatable": false,
        "sortable": false,

```



```

        "attributeType": "VIEWABLE"
    }
},
{
    "name": "Length",
    "label": "Length",
    "dataType": "core.String",
    "description": "",
    "multivalued": false,
    "deprecated": false,
    "derived": false,
    "data": false,
    "isCustom": false,
    "defaultValues": [],
    "isSystem": false,
    "embedded": false,
    "searchConfiguration": {
        "suggestable": false,
        "aggregatable": false,
        "sortable": false,
        "attributeType": "VIEWABLE"
    }
}
},
"associationAttributes": [],
"associationKinds": [],
"referenceAttributes": [],
"version": 1,
"modifiedBy": "",
"referenceDataTypes": [],
"requiredPackages": [],
"classes": [{
    "name": "AccessSchema",
    "label": "Access Schema",
    "description": "",
    "isFirstClass": true,
    "isAbstract": false,
    "superClasses": [
        "core.DataSource"
    ],
    "deprecated": false,
    "indexType": "FULL",
    "appendOnly": true
},
{
    "name": "AccessTable",
    "label": "Access Table",
    "description": "",
    "isFirstClass": true,
    "isAbstract": false,
    "superClasses": [
        "core.DataSet"
    ],
    "deprecated": false,
    "indexType": "FULL",
    "appendOnly": true
},
{
    "name": "AccessTableColumn",
    "label": "Access Table Column",
    "description": "",
    "isFirstClass": true,
    "isAbstract": false,
    "superClasses": [
        "core.DataElement"
    ],
    "deprecated": false,
    "indexType": "FULL",
    "appendOnly": true
}
],
{

```

```

        "name": "AccessView",
        "label": "Access View",
        "description": "",
        "isFirstClass": true,
        "isAbstract": false,
        "superClasses": [
            "core.DataSet"
        ],
        "deprecated": false,
        "indexType": "FULL",
        "appendOnly": true
    },
    {
        "name": "AccessViewColumn",
        "label": "Access View Column",
        "description": "",
        "isFirstClass": true,
        "isAbstract": false,
        "superClasses": [
            "core.DataElement"
        ],
        "deprecated": false,
        "indexType": "FULL",
        "appendOnly": true
    }
],
"classAttributes": [
    {
        "className": "relational.accessdb.AccessSchema",
        "attributeName": "relational.accessdb.Name",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessSchema",
        "attributeName": "relational.accessdb.Abbreviation",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessSchema",
        "attributeName": "relational.accessdb.BusinessUsage",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessSchema",
        "attributeName": "relational.accessdb.DateCreated",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessSchema",
        "attributeName": "relational.accessdb.Datatype",
        "isRequired": false,
        "isCuratable": false,

```

```

    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessSchema",
    "attributeName": "relational.accessdb.Length",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTable",
    "attributeName": "relational.accessdb.Name",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTable",
    "attributeName": "relational.accessdb.Abbreviation",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTable",
    "attributeName": "relational.accessdb.BusinessUsage",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTable",
    "attributeName": "relational.accessdb.DateCreated",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTable",
    "attributeName": "relational.accessdb.Datatype",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTable",
    "attributeName": "relational.accessdb.Length",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,

```

```

    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTableColumn",
    "attributeName": "relational.accessdb.Name",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTableColumn",
    "attributeName": "relational.accessdb.Abbreviation",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTableColumn",
    "attributeName": "relational.accessdb.BusinessUsage",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTableColumn",
    "attributeName": "relational.accessdb.DateCreated",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTableColumn",
    "attributeName": "relational.accessdb.Datatype",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessTableColumn",
    "attributeName": "relational.accessdb.Length",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],
    "isHidden": false,
    "cdc": false
  },
  {
    "className": "relational.accessdb.AccessView",
    "attributeName": "relational.accessdb.Name",
    "isRequired": false,
    "isCuratable": false,
    "deprecated": false,
    "followers": [],

```

```

        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessView",
        "attributeName": "relational.accessdb.Abbreviation",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessView",
        "attributeName": "relational.accessdb.BusinessUsage",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessView",
        "attributeName": "relational.accessdb.DateCreated",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessView",
        "attributeName": "relational.accessdb.Datatype",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessView",
        "attributeName": "relational.accessdb.Length",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessViewColumn",
        "attributeName": "relational.accessdb.Name",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessViewColumn",
        "attributeName": "relational.accessdb.Abbreviation",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,

```

```

        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessViewColumn",
        "attributeName": "relational.accessdb.BusinessUsage",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessViewColumn",
        "attributeName": "relational.accessdb.DateCreated",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessViewColumn",
        "attributeName": "relational.accessdb.Datatype",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    },
    {
        "className": "relational.accessdb.AccessViewColumn",
        "attributeName": "relational.accessdb.Length",
        "isRequired": false,
        "isCuratable": false,
        "deprecated": false,
        "followers": [],
        "isHidden": false,
        "cdc": false
    }
],
"associations": [{
    "name": "AccessSchemaAccessTable",
    "label": "AccessSchemaAccessTable",
    "description": "",
    "fromClass": "relational.accessdb.AccessSchema",
    "toClass": "relational.accessdb.AccessTable",
    "fromLabel": "AccessSchema",
    "toLabel": "AccessTable",
    "associationKinds": [
        "core.ParentChild"
    ],
    "deprecated": false,
    "unidirectional": false,
    "aggregate": false
},
{
    "name": "AccessTableAccessTableColumn",
    "label": "AccessTableAccessTableColumn",
    "description": "",
    "fromClass": "relational.accessdb.AccessTable",
    "toClass": "relational.accessdb.AccessTableColumn",
    "fromLabel": "AccessTable",
    "toLabel": "AccessTableColumn",
    "associationKinds": [
        "core.ParentChild"
    ],
    "deprecated": false,

```

```

        "unidirectional": false,
        "aggregate": false
    },
    {
        "name": "AccessSchemaAccessView",
        "label": "AccessSchemaAccessView",
        "description": "",
        "fromClass": "relational.accessdb.AccessSchema",
        "toClass": "relational.accessdb.AccessView",
        "fromLabel": "AccessSchema",
        "toLabel": "AccessView",
        "associationKinds": [
            "core.ParentChild"
        ],
        "deprecated": false,
        "unidirectional": false,
        "aggregate": false
    },
    {
        "name": "AccessViewAccessViewColumn",
        "label": "AccessViewAccessViewColumn",
        "description": "",
        "fromClass": "relational.accessdb.AccessView",
        "toClass": "relational.accessdb.AccessViewColumn",
        "fromLabel": "AccessView",
        "toLabel": "AccessViewColumn",
        "associationKinds": [
            "core.ParentChild"
        ],
        "deprecated": false,
        "unidirectional": false,
        "aggregate": false
    }
]
}

```

## Update the metadata definition files

Before you create the custom catalog source for Microsoft Access database, update the metadata definition files and enter the details of the metadata that you want to ingest from Microsoft Access database. To begin creating the metadata definition files, download and use the metadata files template. See [“Step 5. Prepare the custom metadata source” on page 263](#).

### Enter object details

The metadata template ZIP file for Microsoft Access database contains multiple object files in the CSV format. These object files represent the classes that you defined in the custom model. The object file names are in the format *<package name>.<class name>*. For example, *relational.accessdb.AccessSchema*.

Open each CSV file in any text editor, enter the following details for each class, and save the file:

Note that the `core.externalId` and `core.name` are mandatory fields in each file.

Object file	core.externalId	core.name	core.description	relational.accessdb.Name	rela
relational.accessdb.AccessSchema	HERMES	HERMES	This is a schema	HERMES	HRM
relational.accessdb.AccessTable	HERMES/ CUSTOMER	CUSTOMER	This is a table	CUSTOMER	CUS

Object file	core.externalId	core.name	core.description	relational.accessdb.Name	rela
relational.accessdb.AccessTableColumn	HERMES/ CUSTOMER/ CUSTOMER_ID	CUSTOMER_ID	This is a table column	CUSTOMER_ID	ID
relational.accessdb.AccessView	HERMES/ V_CUSTOMER	V_CUSTOMER	This is a view	V_CUSTOMER	V_C
relational.accessdb.AccessViewColumn	HERMES/ V_CUSTOMER/ V_CUSTOMER_ID	V_CUSTOMER_ID	This is a view column	V_CUSTOMER_ID	V_C

### Enter association details

Open the `links.csv` file in any text editor. Enter the association details for the objects in Microsoft Access database as shown in the following table, and save the `links.csv` file:

Source	Target	Association
HERMES	HERMES/CUSTOMER	relational.accessdb.AccessSchemaAccessTable
HERMES	HERMES/V_CUSTOMER	relational.accessdb.AccessSchemaAccessView
HERMES/CUSTOMER	HERMES/CUSTOMER/ CUSTOMER_ID	relational.accessdb.AccessTableAccessTableColumn
HERMES/CUSTOMER	HERMES/CUSTOMER/ CUSTOMER_NAME	relational.accessdb.AccessTableAccessTableColumn
HERMES/V_CUSTOMER	HERMES/V_CUSTOMER/ V_CUSTOMER_ID	relational.accessdb.AccessViewAccessViewColumn
\$resource	HERMES	core.ResourceParentChild
HERMES/CUSTOMER	HERMES/V_CUSTOMER	core.DataSetDataFlow
HERMES/CUSTOMER/ CUSTOMER_ID	HERMES/V_CUSTOMER/ V_CUSTOMER_ID	core.DirectionaDataFlow

After updating the files, add all the object CSV files and the `links.csv` file in a ZIP file and provide the ZIP file when you create the custom catalog source.

## Create custom lineage

Lineage defines the data flow across systems in your organization. You can create custom lineage to view the data lineage information for the assets in your organization. You can do this either by using the `links.csv` file or using reference assets that are derived from reference catalog sources.

**Note:** When you create a custom catalog source without the `core.externalId` for an object, the custom catalog source job generates an external ID. This ID appears in the **Reference ID** field on the **System Attributes** tab of the asset in Data Governance and Catalog. You can use this external ID to create custom lineage.



## Using the links.csv file

To create custom lineage using the `links.csv` file, define associations between any two existing objects in the catalog. Verify that the `links.csv` file contains the following details for defining associations between objects:

Header Fields	Description
Source	Required. Unique Reference ID of the object in the catalog source that has been synced. You can find the reference ID of the catalog source object in the <b>Properties</b> tab in Data Governance and Catalog.
Target	Required. Unique Reference ID of the object in the catalog source that has been synced. You can find the reference ID of the catalog source object in the <b>Properties</b> tab in Data Governance and Catalog.
Association	Required. Indicates the type of association. Specify values based on the type of source and target object that you want to link. You can define the following types of associations: <ul style="list-style-type: none"><li>- <code>core.ResourceParentChild</code>. To link a parent object to a top-level child object. For example, catalog source to schema.</li><li>- <code>core.DataSourceParentChild</code>. To link a source system to a data set. For example, schema to table object.</li><li>- <code>core.DataSetToDataElementParentship</code>. To link a data set to a data element. For example, table to column.</li><li>- <code>core.DataSetDataFlow</code>. To link source and target objects at the data set level. This association creates data set-level lineage. For example, table to view.</li><li>- <code>core.DirectionaDataFlow</code>. To link source and target objects at the data element level. This association creates data element-level lineage. For example, table column to view column.</li></ul>

### Sample custom lineage file

The following sample shows a `links.csv` file to define lineage between relational objects:

```
Source,Target,Association
06089733190270f1f3938de0b181382c://SQLDB/dbo/
customer_master~com.infa.odin.models.relational.Table,06089733190270f1f3938de0b181382c://
SQLDB/dbo/CUSTOMERS~com.infa.odin.models.relational.Table,core.DataSetDataFlow
06089733190270f1f3938de0b181382c://SQLDB/dbo/customer_master/
custid~com.infa.odin.models.relational.Column,06089733190270f1f3938de0b181382c://
SQLDB/dbo/CUSTOMERS/
CustomerID~com.infa.odin.models.relational.Column,core.DirectionaDataFlow
```

## Using reference assets

You can configure predefined or custom catalog sources to view lineage with reference assets from referenced catalog sources. For information about referenced catalog sources and reference assets, see [“Referenced catalog sources” on page 24](#).

When you configure a custom catalog source, set the `core.reference` and `core.assignable` header fields to true in the metadata CSV file for each object of the source system. See [“Step 6. Create the custom catalog source” on page 267](#). The source system objects are treated as reference assets and you can assign connections to the custom catalog source in order to define lineage.

After creating the custom catalog source and running the catalog source job, the ingested objects from the referenced catalog source appear as reference assets and Data Governance and Catalog displays the lineage with the reference assets. You can also see the reference catalog source listed on the **Connection Assignment** page in Metadata Command Center. To link the reference assets to actual objects and to view the complete lineage, assign a connection for the reference catalog source. See [“Assign connections to reference catalog sources” on page 25](#).