



Informatica® Metadata Command Center
November 2025

SAP BusinessObjects Data Services

© Copyright Informatica LLC 2025

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

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

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

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

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

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

Publication Date: 2025-11-20

Table of Contents

Preface.	4
Chapter 1: Introduction to SAP BusinessObjects Data Services catalog sources.	5
Extraction and view process.	6
About the SAP BusinessObjects Data Services catalog source.	7
Extracted metadata.	7
Compatible connectors.	7
Chapter 2: Before you begin.	8
Verify permissions.	8
Permissions to extract metadata.	8
Create a connection.	8
Microsoft SQL Server connection properties.	9
Oracle connection properties.	11
SAP HANA connection properties.	14
Create endpoint catalog sources for connection assignment.	16
Chapter 3: Create catalog sources in Metadata Command Center.	17
Step 1. Register a catalog source.	17
Step 2. Configure capabilities.	19
Configure metadata extraction.	20
Configure lineage discovery.	22
Step 3. Associate stakeholders and asset groups.	23
Step 4. Run or schedule the job.	25
Step 5. Assign reference catalog source connections to endpoint catalog source objects.	26
Chapter 4: View results in Data Governance and Catalog.	28
View metadata extraction results.	28
View data lineage.	30
View lineage at the catalog source level.	30
View lineage at the data set level.	30
View lineage at the data element level.	31

Preface

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

CHAPTER 1

Introduction to SAP BusinessObjects Data Services catalog sources

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

A source system is any system that contains data or metadata. For example, SAP BusinessObjects Data Services is a source system from which you can extract metadata through an SAP BusinessObjects Data Services catalog source. A catalog source is an object that represents and contains metadata from the source system.

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

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

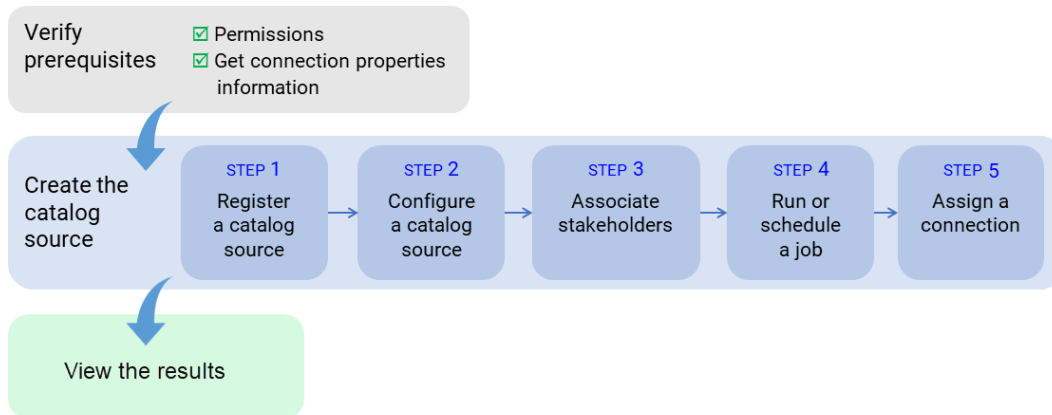
The following table describes the capabilities of the catalog source:

Capability	Description
Lineage Discovery	Builds the complete lineage of a catalog source by recommending endpoint catalog source objects to assign to reference catalog source connections. When you run the catalog source job, Metadata Command Center assigns the reference catalog source connections to CLAIRE recommended endpoint catalog source objects. You can then view the list of CLAIRE recommendations and accept or reject them.

Extraction and view process

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

The following image shows the process to extract metadata from an SAP BusinessObjects Data Services source system:



After you verify prerequisites, perform the following tasks to extract metadata from SAP BusinessObjects Data Services:

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

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

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

About the SAP BusinessObjects Data Services catalog source

You can use the SAP BusinessObjects Data Services catalog source to extract metadata from an SAP BusinessObjects Data Services source system.

SAP BusinessObjects Data Services is an ETL tool used for data integration, data quality, data profiling and data processing. It enables you to integrate and transform reliable data into a data warehouse system for analytical reporting.

Extracted metadata

You can use the SAP BusinessObjects Data Services catalog source to extract metadata from an SAP BusinessObjects Data Services source system.

Objects extracted

Metadata Command Center extracts the following metadata from an SAP BusinessObjects Data Services source system:

- Project
- Job
- Workflow
- Dataflow
- Dataflow Instance
- Script
- Script Instance
- Calculation

Compatible connectors

Before you configure an SAP BusinessObjects Data Services catalog source, you must connect to the SAP BusinessObjects Data Services source system.

You can use the following connectors to connect to the SAP BusinessObjects Data Services repository:

- Microsoft SQL Server
- Oracle
- SAP HANA

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

CHAPTER 2

Before you begin

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

Perform the following tasks:

- Assign the required permissions.
- Configure an Oracle, Microsoft SQL Server, or SAP HANA connection in Administrator to connect to the SAP BusinessObjects Data Services repository.
- If your Oracle database is SSL-enabled, specify appropriate values for the Trust Store and Key Store fields in the Oracle connection properties. Test Connection to an SSL-enabled Oracle database fails if either the truststore or keystore value is not specified in the connection properties.
- Create endpoint catalog sources for connection assignment.

Verify permissions

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

Permissions to extract metadata

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

Grant permissions that allow you to perform the following operations:

- select on CONNECTION_SCHEMA.AL_LANG
- select on CONNECTION_SCHEMA.AL_LANGXMLTEXT
- select on CONNECTION_SCHEMA.AL_PARENT_CHILD

Create a connection

Before you configure the SAP BusinessObjects Data Services catalog source, create a connection object in Administrator.

1. In Administrator, select **Connections**.

2. Click **Add Connection** and select Oracle, Microsoft SQL Server, or SAP HANA.
Note: Select the connector that corresponds to your local BusinessObjects Data Services repository type.
3. Enter the connection properties.
4. Click **Test**.
5. Click **Save**.

Microsoft SQL Server connection properties

If you use the Microsoft SQL Server connection type, configure the Microsoft SQL Server connection parameters.

- Enter properties specific to the Microsoft SQL Server connection type:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>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.</p>
Description	<p>Description of the connection. Maximum length is 4000 characters.</p>
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>Note: If you're using this connection to apply data access policies through pushdown or proxy services, you cannot use the Secret Vault configuration option.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run the tasks.</p> <p>A runtime environment is either Informatica Cloud Secure Agent or a serverless runtime environment.</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
SQL Server Version	This property is no longer used. If you select a version, it is ignored.
Authentication Mode	<p>You can configure one of the following authentication modes to connect to Microsoft SQL Server databases:</p> <ul style="list-style-type: none"> - SQL Server authentication - Windows authentication (Deprecated) - Active Directory Password authentication - Windows Authentication V2 - Kerberos authentication - Service Principal authentication <p>Select the required authentication mode and then configure the authentication-specific parameters.</p> <p>For SQL Server sources in database ingestion and replication tasks, you must select SQL Server Authentication, Windows Authentication v2, or Active Directory Password. Don't use the Kerberos or Service Principal Authentication mode.</p> <p>For SQL Server targets in application ingestion and replication tasks and database ingestion and replication tasks, you must select either SQL Server Authentication or Windows Authentication v2. Don't use any other authentication type.</p>

The following table describes the advanced connection properties:

Property	Description
Encryption Method	<p>The method that the Secure Agent uses to encrypt the data sent between the driver and the database server. You can use the encryption method to connect to Microsoft Azure SQL Database.</p> <p>Default is None.</p>
Crypto Protocol Version	Cryptographic protocols to use when you enable SSL encryption.
Validate Server Certificate	<p>When set to True, Secure Agent validates the certificate that is sent by the database server. If you specify the HostNameInCertificate parameter, Secure Agent also validates the host name in the certificate.</p> <p>When set to false, the Secure Agent doesn't validate the certificate that is sent by the database server.</p>
Trust Store	<p>The location and name of the truststore file. The truststore file contains a list of Certificate Authorities (CAs) that the driver uses for SSL server authentication.</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/ <TrustStore_filename></pre>
Trust Store Password	The password to access the contents of the truststore file.
Host Name in Certificate	Host name of the machine that hosts the secure database. If you specify a host name, the Secure Agent validates the host name included in the connection with the host name in the SSL certificate.

Property	Description
Metadata Advanced Connection Properties	<p>Additional properties for the JDBC driver to fetch the metadata.</p> <p>Enter properties in the following format:</p> <pre><parameter name>=<parameter value></pre> <p>If you enter more than one property, separate each key-value pair with a semicolon.</p> <p>For example, enter the following property to configure the connection timeout when you test a connection:</p> <pre>LoginTimeout=<value_in_seconds></pre> <p>Note: The default connection timeout is 270 seconds.</p> <p>When you use Kerberos authentication to connect to Microsoft SQL Server, you need to add the <code>KRB5_CONFIG</code>, <code>KRB5CCNAME</code>, and <code>JAASCONFIG</code> properties.</p>
Runtime Advanced Connection Properties	<p>Additional properties for the ODBC driver required at run time.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>When you use Kerberos authentication to connect to Microsoft SQL Server, you need to add the <code>KRB5_CONFIG</code> and <code>KRB5CCNAME</code> properties.</p>

Oracle connection properties

If you use the Oracle connection type, configure the Oracle connection parameters.

- Enter properties specific to the Oracle connection type:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>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.</p>
Description	Description of the connection. Maximum length is 4000 characters.
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>Note: If you're using this connection to apply data access policies through pushdown or proxy services, you cannot use the Secret Vault configuration option.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	<p>The name of the runtime environment where you want to run the tasks.</p> <p>Select a Secure Agent, Hosted Agent, or serverless runtime environment.</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
Oracle Subtype	The Oracle connection subtype that you can use to connect to Oracle on-premises or Oracle Autonomous Database. Select one of the following options: <ul style="list-style-type: none"> - Oracle ADB. Connects to Oracle Autonomous Database. - Oracle On-premise. Connects to Oracle on-premises.
Authentication Mode	You can configure one of the following authentication modes to connect to Oracle databases: <ul style="list-style-type: none"> - Oracle Database authentication - Kerberos authentication Default is Oracle Database Authentication .

The following table describes the basic connection properties for Oracle Database authentication:

Property	Description
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 1521.
Service Name	Service name or System ID (SID) that uniquely identifies the Oracle database. Specify the SID in the following format to connect to Oracle databases: SID:<ORACLE_SID>
Schema	The schema name to select tables during object selection in a mapping. If you want to select tables from multiple schemas, leave the field blank. When left blank, all schemas you have access to are displayed and you can select tables from the available schemas.
Code Page	The code page of the database server.

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

Property	Description
Host	Name of the machine that hosts the database server.
Port	Network port number used to connect to the database server. Default is 1521.
Service Name	

Property	Description
Schema	The schema name to select tables during object selection in a mapping. If you want to select tables from multiple schemas, leave the field blank. When left blank, all schemas you have access to are displayed and you can select tables from the available schemas.
Code Page	The code page of the database server.

The following table describes the advanced connection properties for Oracle Database authentication:

Property	Description
Encryption Method	The method that the Secure Agent uses to encrypt the data exchanged between the Secure Agent and the database server. Default is No Encryption. This property doesn't apply if you use the Hosted Agent.
Crypto Protocol Version	Cryptographic protocols to use when you enable SSL encryption. Not applicable when you use the Hosted Agent or the serverless runtime environment.
Validate Server Certificate	Validates the certificate that is sent by the database server. If you specify the <code>HostNameInCertificate</code> parameter, the Secure Agent also validates the host name in the certificate.
Trust Store	The location and name of the truststore file. For the serverless runtime environment, specify the following certificate path in the serverless agent directory: <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<TrustStore_filename></code>
Trust Store Password	The password to access the contents of the truststore file.
Host Name in Certificate	Host name of the machine that hosts the secure database. If you specify a host name, the Secure Agent validates the host name included in the connection with the host name in the SSL certificate.
Key Store	The location and the file name of the keystore. For the serverless runtime environment, specify the following certificate path in the serverless agent directory: <code>/home/cldagnt/SystemAgent/serverless/configurations/ssl_store/<KeyStore_filename></code>
Key Store Password	The password for the keystore file required for secure communication.
Key Password	
Connection Retry Period	

Property	Description
Metadata Advanced Connection Properties	<p>Additional properties for the JDBC driver to fetch the metadata. Enter properties in the following format:</p> <pre><parameter name>=<parameter value></pre> <p>If you enter more than one property, separate each key-value pair with a semicolon.</p> <p>For example, enter the following property to configure the connection timeout when you test a connection:</p> <pre>LoginTimeout=<value_in_seconds></pre> <p>Note: The default connection timeout is 270 seconds.</p> <p>To connect to an Oracle database enabled for advanced security, you can specify the Oracle advanced security options for the JDBC driver.</p> <p>For example, <code>EncryptionTypes=AES256;</code> <code>EncryptionLevel=accepted;DataIntegrityLevel=accepted;</code> <code>DataIntegrityTypes=SHA1</code></p>
Runtime Advanced Connection Properties	<p>Additional properties for the ODBC driver to run .</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example, <code>charset=sjis;</code> <code>readtimeout=180</code></p> <p>To connect to an Oracle database enabled for advanced security, you can specify the Oracle advanced security options for the ODBC driver.</p> <p>For example, <code>EncryptionTypes=AES256;EncryptionLevel=1;</code> <code>DataIntegrityLevel=1;DataIntegrityTypes=SHA1;</code> <code>DataIntegrityTypes=SHA1</code></p>

SAP HANA connection properties

If you use the SAP HANA connection type, configure the SAP HANA connection parameters.

- Enter properties specific to the SAP HANA connection type:

Property	Description
Connection Name	<p>Name of the connection.</p> <p>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.</p>
Description	<p>Description of the connection. Maximum length is 4000 characters.</p>

Property	Description
Use Secret Vault	<p>Stores sensitive credentials for this connection in the secrets manager that is configured for your organization.</p> <p>This property appears only if secrets manager is set up for your organization.</p> <p>When you enable the secret vault in the connection, you can select which credentials that the Secure Agent retrieves from the secrets manager. If you don't enable this option, the credentials are stored in the repository or on a local Secure Agent, depending on how your organization is configured.</p> <p>Note: If you're using this connection to apply data access policies through pushdown or proxy services, you cannot use the Secret Vault configuration option.</p> <p>For information about how to configure and use a secrets manager, see "Secrets manager configuration" in the Administrator help.</p>
Runtime Environment	The name of the runtime environment where you want to run tasks.
Host	SAP HANA server host name.
Port	SAP HANA server port number.
Database Name	Name of the SAP HANA database.
Current Schema	<p>SAP HANA database schema name.</p> <p>Specify _SYS_BIC when you use SAP HANA database modelling views.</p>
Code Page	<p>The code page of the database server defined in the connection.</p> <p>Select the UTF-8 code page.</p>
Username	User name of the SAP HANA account.
Password	<p>Password of the SAP HANA account.</p> <p>The password can contain alphanumeric characters and the following special characters: ~ ` ! @ # \$ % ^ & * () _ - + = [] : ; ' < , > . ? /</p>

The following table describes the advanced connection properties:

Property	Description
Metadata Advanced Connection Properties	<p>The optional properties for the JDBC driver to fetch the metadata.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example, you can set the connection timeout for the JDBC driver when you connect to SAP HANA.</p>
Run-time Advanced Connection Properties	<p>The optional properties for the ODBC driver to run mappings.</p> <p>If you specify more than one property, separate each key-value pair with a semicolon.</p> <p>For example,</p> <pre>charset=sjis;readtimeout=180</pre>

Create endpoint catalog sources for connection assignment

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

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

Note: When you create an Oracle endpoint catalog source, configure a different Oracle connection than the one used for the SAP BusinessObjects Data Services catalog source. If you use the same Oracle connection and run the SAP BusinessObjects Data Services catalog source again after connection assignment, you can't view the lineage of data elements.

CHAPTER 3

Create catalog sources in Metadata Command Center

Use Metadata Command Center to configure a catalog source for SAP BusinessObjects Data Services and extract metadata.

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

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

Step 1. Register a catalog source

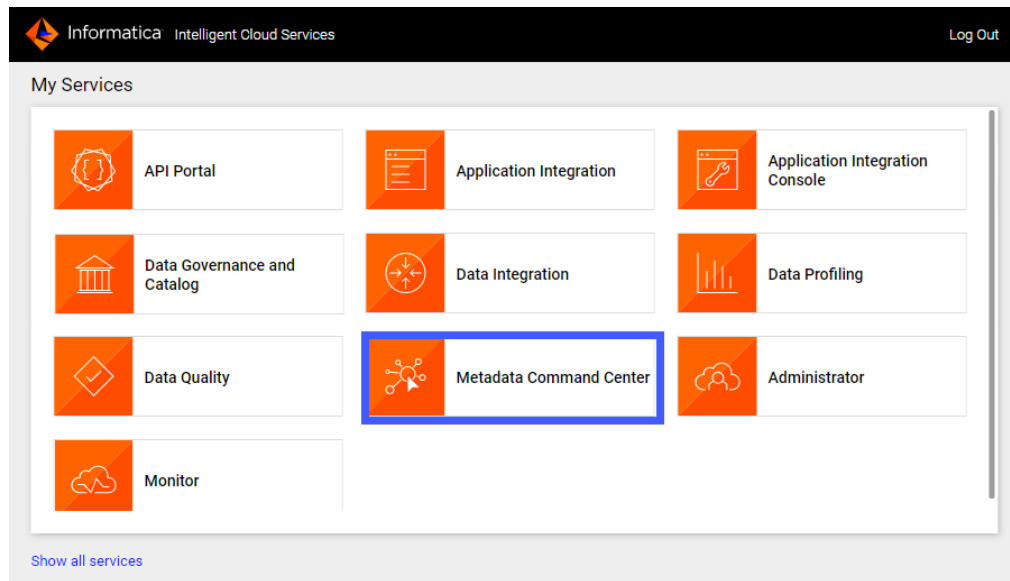
When you register a catalog source, provide general information and connection values.

1. Log in to Informatica Intelligent Cloud Services.

The **My Services** page appears.

2. Click **Metadata Command Center**.

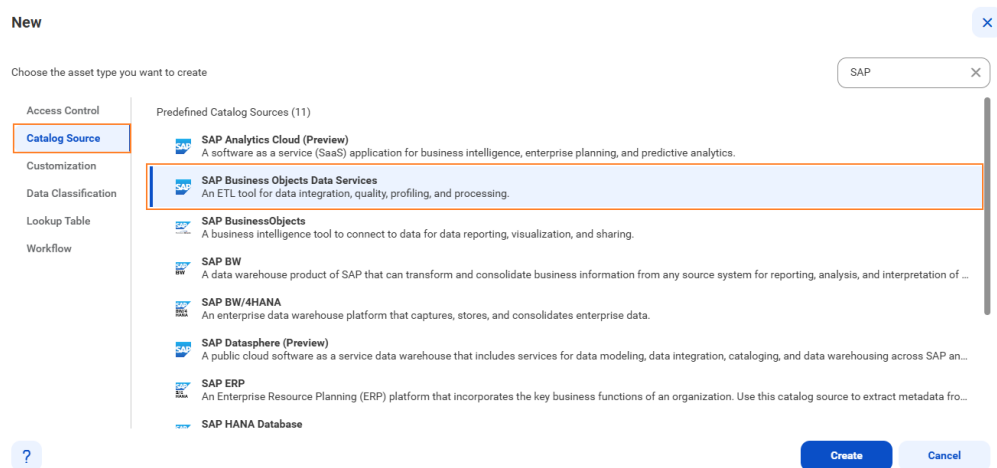
The following image shows the Metadata Command Center box on the **My Services** page:



The Metadata Command Center home page appears.

3. Click **New**.
4. Select **Catalog Source** from the list of asset types.
5. Select SAP BusinessObjects Data Services from the list of catalog source types.

The following image shows the SAP BusinessObjects Data Services catalog source type:



6. Click **Create**.

The **New Catalog Source** page opens.

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

New Catalog Source

1 Registration 2 Configuration 3 Associations 4 Schedule

General Information

Name: *

Description:

Connection Information

Catalog Source Type: SAP Business Objects Data Services

BODS Local Repository Connection: *

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

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

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

8. In the **Connection Information** area, enter the SAP BusinessObjects Data Services connection information.

The following table describes the connection property that you can specify:

Property	Description
BODS Local Repository Connection	Select the Oracle connection that you created in Administrator to connect to the BODS Local Repository.

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

The **Configuration** page appears.

Step 2. Configure capabilities

When you configure the SAP BusinessObjects Data Services catalog source, you define the settings for the metadata extraction capability.

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

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

Configure metadata extraction

When you configure the SAP BusinessObjects Data Services catalog source, you choose a runtime environment, define filters, and enter configuration parameters for metadata extraction.

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

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

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

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

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

Filters can contain the following wildcards:

 - Question mark. Represents a single character.
 - Asterisk. Represents multiple characters or empty text.
 - Double asterisk. Represents any number of segments with any number of characters.

The following image shows the filter condition options:

Filters

Specify metadata filters: ☐ No ☒ Yes

[Show supported wildcards and examples](#)

Include or exclude metadata	Select the object type	Enter a value to specify the object location	+	✕
-----------------------------	------------------------	--	---	---

For path hierarchies, use the '/' separator. When you enter values for filters, enclose them in double quotes if the value includes an asterisk or spaces before or after a string value. Filters are case-sensitive.

Use the following format when you enter values for filters: *PROJECT_NAME/JOB_NAME/WORKFLOW_NAME/DATAFLOW_NAME*

Examples:

- To include or exclude metadata from all projects named 'Project' across the BODS repository, enter `Project/**`
- To include or exclude metadata from all "DTFL4" dataflows located in workflows with names that start with 'Workflow' followed by a single character, in all projects across the BODS repository, enter `**/Workflow?/DTFL4`
- To include or exclude metadata from all projects with names that start with 'Project', across the BODS repository, enter `Project*/**`
- To include or exclude metadata from all dataflows named 'DataflowX' located in jobs named 'JobX', across the BODS repository, enter `*/JobX/**/DataflowX`

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

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

The following table describes the properties that you enter for Configuration Parameters:

Property	Description
Default Variable Values	<p>Specify default values for the variables used in programmable objects in the form of key-value pairs. Use sections in the form of [section name] before you specify a variable.</p> <p>Example:</p> <pre>[Global] "[\$\$Parameter]" = 'avg' \$IntValue = 256 get_env('wood') = 'tree' [Variables] "[\$\$Substitute]" = 'val' \$stringValue = 'text' [Functions] exec('sh', '-xd') = 1 datastore.owner.function() = 16 [JobName] \$DoubleValue = 1.84 sql('datastore', 'select * from X') = 4</pre>

You can provide default variable values for substitute parameters, global variables, or functions.

Consider the following guidelines when you specify default variable values:

- For substitute parameters, use the following syntax: `$$SubstituteParameterName`
- For global variables, use the following syntax: `$GlobalVariable`
- For functions, use the following syntax: `function_name(parameters)`
- To use a global variable or function for all jobs, define the variable or function value under the [Global] section. Place the global variable value in the [Variables] subsection and the default function value in the [Function] subsection.

- To use a variable for a specific job, define the value of the variable in the job section.
- The value of the variable must meet the standard syntax of default variables, for example:
\$GlobalVariable = 25

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

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

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

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

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

Configure lineage discovery

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

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

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

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

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

The following image shows the filter condition options:

Examples:

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

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

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

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

Step 3. Associate stakeholders and asset groups

Associate users or user groups within a stakeholder role as stakeholders for technical assets in Data Governance and Catalog. Also, you can choose to assign technical assets extracted from the catalog source to asset groups. You can then use access policies to control permissions on assets that are assigned to asset groups.

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

1. To associate users or user groups as stakeholders with technical assets extracted from the catalog source, perform the following steps:
 - a. On the **Associations** page, click **Stakeholders**.
 - b. Select **Assign Stakeholders**.
 - c. Select a stakeholder role.
 - d. Click **Select** to add users and user groups from the stakeholder role as stakeholders for the technical assets.

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

Add Users & User Groups

Users

User Groups

All Users (1)

Find

Full Name

Email

User Name ↑

Status

☐ gov owner_09

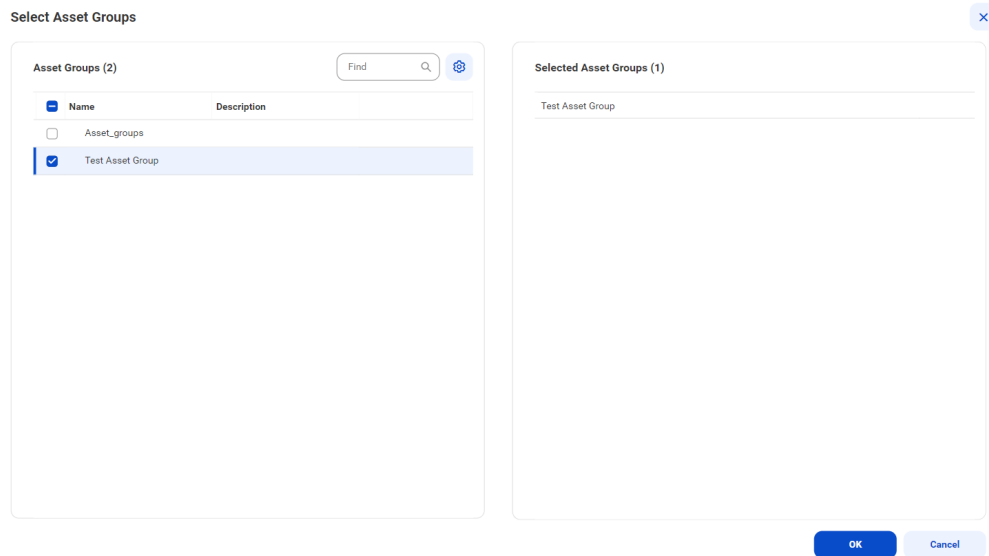
Active

?

OK

Cancel

- e. Select one or more users or user groups to assign as stakeholders for the technical assets, and click **OK**.
Only the selected users and user groups belonging to the specified stakeholder role are granted the permissions to technical assets.
- f. To assign users or user groups from another stakeholder role, click **Add** and then repeat the steps.
2. To assign asset groups to technical assets extracted from the catalog source, perform the following steps:
 - a. On the **Associations** page, click **Asset Groups**.
 - b. Select **Assign Asset Groups**.
 - c. Click **Select**.
The **Select Asset Groups** dialog box displays the list of asset groups.
If you enabled an access policy that includes an asset group, you can only view assets that belong to that asset group.
3. Select the asset groups to which you want to assign technical assets extracted from the catalog source, and click **OK**.



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

Step 4. Run or schedule the job

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

Note: You can't run multiple jobs simultaneously.

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

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

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

Run the job manually

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

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

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

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

Run the job on a schedule

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

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

For example, this can happen in the following scenarios:

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

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

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

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

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

Monitor job status

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

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

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

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

integration platform, such as SAP BusinessObjects Data Services. You must first create and run an endpoint catalog source that connects to the reference source system.

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

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

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

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

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

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

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

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

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

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

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

You can connect to the following source systems:

- Amazon S3
- File System
- Microsoft SQL Server
- Oracle
- SAP HANA Database
- SAP Business Warehouse (SAP BW)
- SAP BW/4HANA
- SAP ERP

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

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

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

CHAPTER 4

View results in Data Governance and Catalog

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

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

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

View metadata extraction results

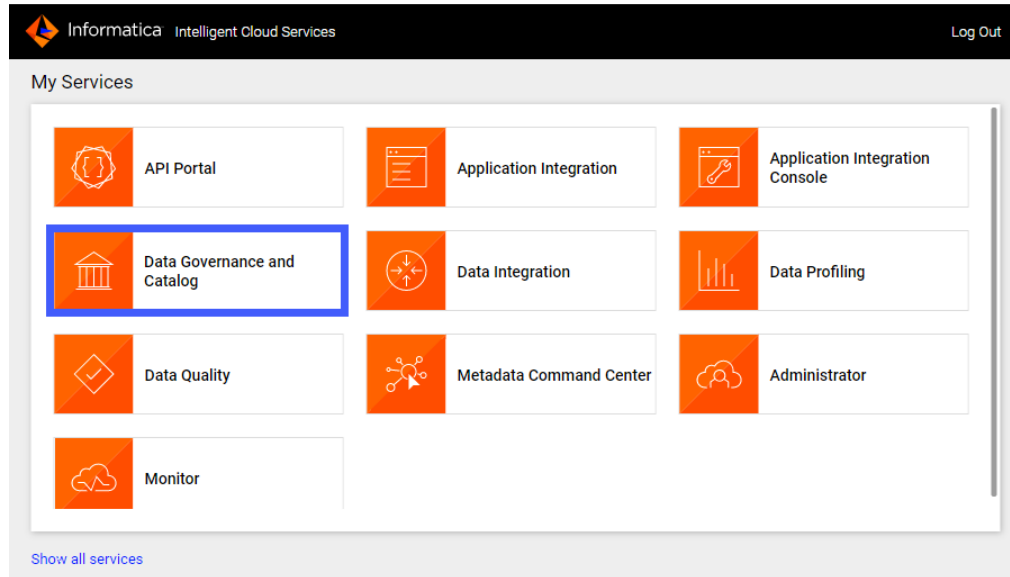
After a job runs in Metadata Command Center, view the results in Data Governance and Catalog. You can view details about source system contents in a hierarchical structure and trace data lineage.

1. Log in to Informatica Intelligent Cloud Services.

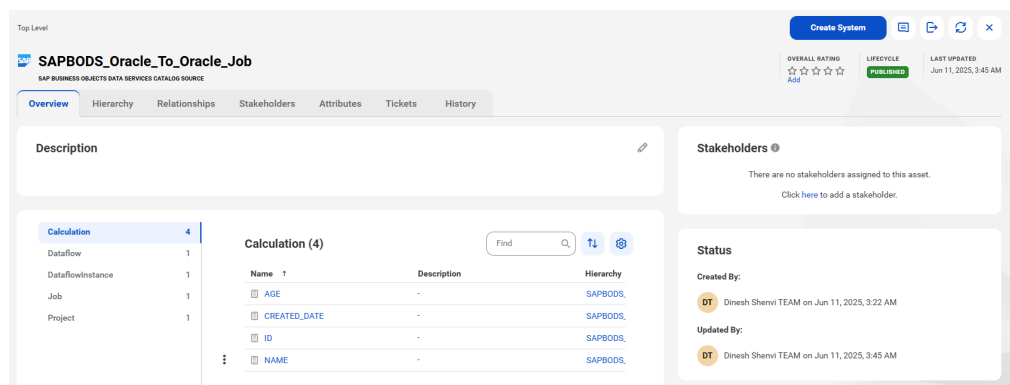
The **My Services** page appears.

2. Click Data Governance and Catalog.

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



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



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

View data lineage

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

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

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

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

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

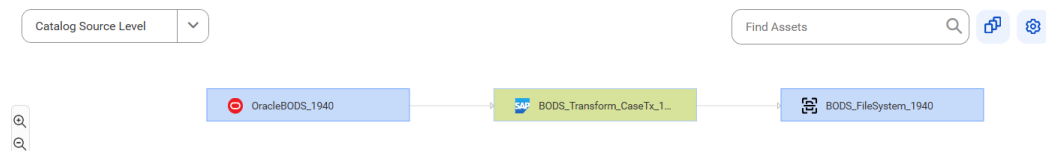
For information about linking catalog sources, see *Link catalog sources* in the Administration help.

View lineage at the catalog source level

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

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

The following image shows how the BODS_FileSystem_1940 target files of the File System source system get data from the OracleBODS_1917 source table of the Oracle source system using the BODS_Transform_CaseTx_1 model instance of the SAP BusinessObjects Data Services source system after connection assignment:

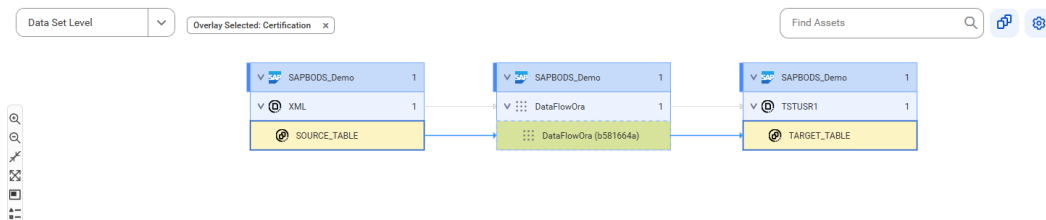


View lineage at the data set level

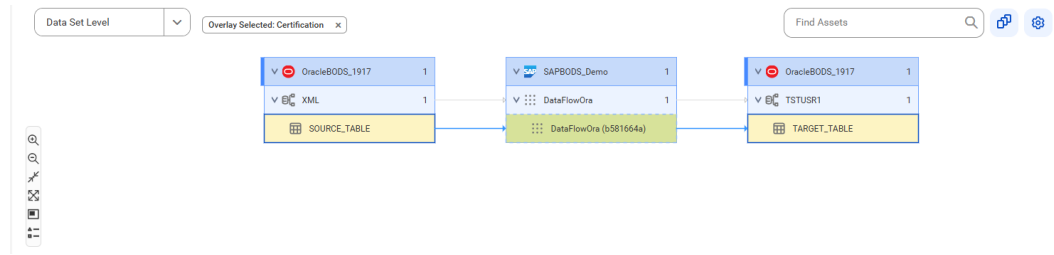
The data set level displays individual sets of data in the data flow.

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

The following image shows the data set level lineage where the TARGET_TABLE target reference data set gets data from the SOURCE_TABLE source reference data set before connection assignment:



The following image shows data set level lineage where the TARGET_TABLE target table gets data from the SOURCE_TABLE source table after connection assignment:



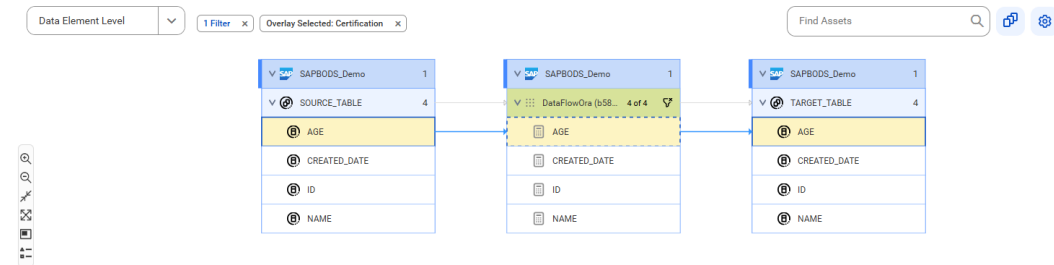
After connection assignment, the referenced object icons change to specific object icons.

View lineage at the data element level

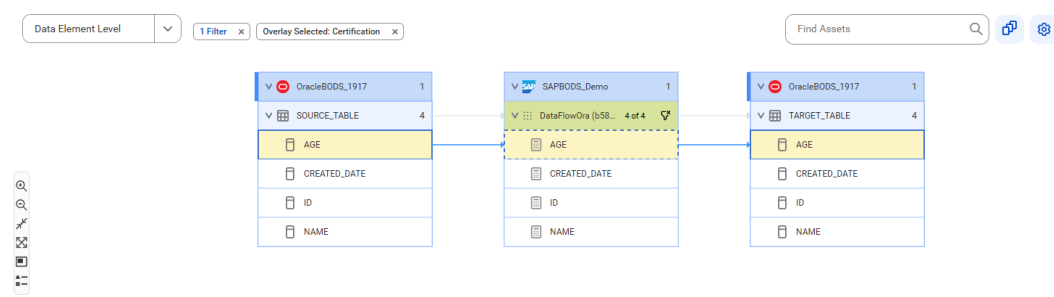
The data element level displays details of the data set level. At the data element level, you can see the input sources for expressions or commands and calculations or transformations on the data.

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

The following image shows the data element level lineage where the AGE reference data element of the TARGET_TABLE reference data set gets data from the AGE reference data element of the SOURCE_TABLE reference data set using the AGE calculation before connection assignment:



The following image shows the data element level lineage where the AGE column of the TARGET_TABLE table gets data from the AGE column of the SOURCE_TABLE table using the AGE calculation after connection assignment:



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