Abstract
This article lists the permissions that you must configure for data sources before you configure resources in Enterprise Data Catalog. The article also lists the types of object metadata that the resources extract from the data sources.

Supported Versions
- Enterprise Data Catalog 10.2.1

Table of Contents
Overview. .......................................................... 3
Relational Data Sources. ........................................... 3
  Overview. .............................................................. 3
  Amazon Redshift. .................................................... 3
  Azure Microsoft SQL. ............................................... 3
  Oracle. ................................................................. 4
  Microsoft SQL Server. ............................................. 5
  Sybase. ................................................................. 6
  IBM DB2 for z/OS. ................................................... 7
  IBM DB2. .............................................................. 8
  JDBC with MySQL. .................................................. 9
  JDBC with AS400. .................................................. 10
  IBM Netezza. .......................................................... 10
  Teradata. .............................................................. 11
Business Intelligence Sources. ................................... 12
  Overview. .............................................................. 12
  IBM Cognos. ........................................................... 12
  MicroStrategy. ........................................................ 15
  Oracle Business Intelligence. ...................................... 16
  SAP Business Objects. ............................................. 18
  Tableau Server. ...................................................... 20
Data Integration Sources. ......................................... 23
  Overview. .............................................................. 23
  Business Glossary. .................................................. 24
  Informatica Axon. ................................................... 24
  Informatica PowerCenter. ......................................... 24
  Informatica Platform. .............................................. 24
File System Sources. ............................................. 24
  Overview. .............................................................. 24
  Amazon S3. ............................................................ 25
  Azure WASB. .......................................................... 25
Overview

Before you configure resources in Enterprise Information Catalog to extract metadata from data sources, you must configure permissions for data sources to extract metadata about specific objects in the data source.

Relational Data Sources

Overview

The permissions that you must configure on the relational data sources and the metadata extracted for these sources are included in the following sections:

Amazon Redshift

Objects Extracted
- Tables
- Views

Permissions

If you create a new user, ensure that you configure read permission on the Amazon Redshift data source for the user account.

Azure Microsoft SQL

Objects Extracted
- Tables
- Views
• Extended stored procedure
• Table (user-defined)
• Synonym
• UNIQUE constraint
• Triggers
• Procedures
• Index
• SQL table-valued-function
• Users
• Partition Scheme
• Partition Function
• XML Schema Collections
• User defined Data type
• Rules
• Defaults
• Constraints
• SQL_INLINE_TABLE_VALUED_FUNCTION
• SQL_SCALAR_FUNCTION
• SEQUENCE

Permissions

Before you create an Azure Microsoft SQL resource, configure the permissions for the Azure Microsoft SQL Server database user account that you use to connect to Azure Microsoft SQL Server. Enterprise Data Catalog uses SQL Server authentication to connect to the Azure Microsoft SQL Server database. The user account that you use to connect to Azure Microsoft SQL Server must be an SQL Server login account. Configure the VIEW DEFINITION permission for the user account. Configuring this permission lists all the schemas from where the user can load metadata.

Oracle

Objects Extracted

Enterprise Information Catalog extracts metadata of the following schema objects from an Oracle data source:
• Table
• Synonym
• View
• Different datatypes
• Precision and scale information for all data types
• Comments
• Trigger
• Function
• Procedure
• Condition
• Integrity constraints
• Index-organized table
• Materialized View

Permissions

You must configure the CONNECT and SELECT_CATALOG_ROLE permissions for the database user account that you use to access the Oracle database.

Microsoft SQL Server

Objects Extracted

Enterprise Information Catalog extracts metadata of the following schema objects from a Microsoft SQL Server data source:

• Tables
• Views
• Extended stored procedure
• Table (user-defined)
• Synonym
• UNIQUE constraint
• Triggers
• Procedures
• Index
• SQL table-valued-function
• Users
• Partition Scheme
• Partition Function
• XML Schema Collections
• User defined Data type
• Rules
• Defaults
• Constraints
• SQL_INLINE_TABLE_VALUED_FUNCTION
• SQL_SCALAR_FUNCTION
• SEQUENCE

Permissions

Before you create a Microsoft SQL Server resource, configure the permissions for the Microsoft SQL Server database user account that you use to connect to Microsoft SQL Server. Enterprise Information Catalog uses SQL Server authentication to connect to the Microsoft SQL Server database. The user account that you use to connect to Microsoft SQL Server must be an SQL Server login account. Configure the VIEW DEFINITION permission for the user account. Configuring this permission lists all the schemas from where the user can load metadata. You must also configure the SELECT permission for the sys.sql_expression_dependencies for the database.
**Sybase**

**Objects Extracted**

Enterprise Information Catalog extracts metadata of the following schema objects from a Sybase data source:

- Table
- View
- Clustered Index
- Procedure
- Trigger
- Rule
- Unique Index
- Non Clustered Index
- Index
- Function
- User defined data type

**Permissions**

Before you create a Sybase resource, configure the permissions for the Sybase ASE database user account that you use to connect to the Sybase ASE database.

Configure SELECT permissions on the following schema objects:

- Tables
- Views
- Columns
- Procedures

Configure SELECT permissions on the following system tables:

- sysobjects
- syscomments
- sysdepends
- syscolumns
- sysindexes
- sysconstraints
- sysreferences
- sysusers
- systypes
- master.dbo.sysservers
- master.dbo.sysconfigures
- @@*+servername
IBM DB2 for z/OS

Objects Extracted

Enterprise Information Catalog extracts metadata of the following schema objects from an IBM DB2 for z/OS data source:

- Store Procedure
- Function
- Synonym
- Trigger

Permissions

When you load an IBM DB2 for z/OS resource, Enterprise Information Catalog extracts metadata from the IBM DB2 for z/OS subsystem. Enterprise Information Catalog selects the metadata from the DB2 catalog tables.

Configure SELECT privileges on the following system tables in the IBM DB2 for z/OS user account that you use to connect to the IBM DB2 for z/OS data source:

<table>
<thead>
<tr>
<th>System Tables</th>
<th>Metadata Extracted</th>
</tr>
</thead>
</table>
| - SYSIBM.SYSSYNONYMS  
- SYSIBM.SYSTABLES  
- SYSIBM.SYSROUTINES  
- SYSIBM.SYSEQUENCES  
- SYSIBM.SYSDATATYPES | Schemas |
| - SYSIBM.SYSTABLES  
- SYSIBM.SYSTABLESPACE | - Tables  
- Views |
| - SYSIBM.SYSVIEWSS  
- SYSIBM.SYSTABLESPACE | - Alias |
| - SYSIBM.SYSKEYS  
- SYSIBM.SYSINDEXES | Columns |
| - SYSIBM.SYSRELS  
- SYSIBM.SYSFOREIGNKEYS  
- SYSIBM.SYSINDEXES | Primary keys |
| - SYSIBM.SYSCHECKS  
- SYSIBM.SYSCHECKDEP | Column constraints |
| - SYSIBM.SYSINDEXES  
- SYSIBM.SYSKEYS | Indexes |
| - SYSIBM.SYSSYNONYMS  
- SYSIBM.SYSTABLES | Synonyms |
| SYSIBM.SYSTRIGGERS | Triggers |
| SYSIBM.SYSTRIGGERS | Stored procedures |
| SYSIBM.SYSROUTINES | Functions |
System Tables | Metadata Extracted
--- | ---
SYSIBM.SYSSEQUENCES | Sequences
- SYSIBM.SYSSEQUENCESDEP
- SYSIBM.SYSSEQUENCES | Identity
SYSIBM.SYSDATATYPES | User-defined types

**IBM DB2**

Objects Extracted

Enterprise Information Catalog extracts metadata of the following schema objects from an IBM DB2 data source:

- Tables
- Partitioned Table
- Range Clustered Table
- Multidimensional Clustering Table
- Constraints (NOT NULL, UNIQUE, CHECK, PRIMARY KEY, FOREIGN KEY, DEFAULT)
- Alias
- Sequences
- Views
- Triggers
- Function
- Procedure
- Index
- Materialized Query Table
Permissions

The following table lists the schema objects and system tables on which you must configure SELECT permissions for the IBM DB2 database user account:

<table>
<thead>
<tr>
<th>Schema Objects</th>
<th>System Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Tables</td>
<td>- SYSCAT.SCHEMA DATA</td>
</tr>
<tr>
<td>- Views</td>
<td>- SYSCAT.TRIGGERS</td>
</tr>
<tr>
<td>- Indexes</td>
<td>- SYSCAT.REFERENCES</td>
</tr>
<tr>
<td>- Packages</td>
<td>- SYSCAT.INDEXES</td>
</tr>
<tr>
<td>- Procedures</td>
<td>- SYSCAT.INDEXCOLUSE</td>
</tr>
<tr>
<td>- Functions</td>
<td>- SYSCAT.REFERENCES</td>
</tr>
<tr>
<td>- Sequences</td>
<td>- SYSCAT.KEYCOLUSE</td>
</tr>
<tr>
<td>- Triggers</td>
<td>- SYSCAT.CHECKS</td>
</tr>
<tr>
<td>- Synonyms</td>
<td>- SYSCAT.VIEWS</td>
</tr>
<tr>
<td></td>
<td>- SYSCAT.PACKAGES</td>
</tr>
<tr>
<td></td>
<td>- SYSCAT.FUNCDEP</td>
</tr>
<tr>
<td></td>
<td>- SYSCAT.TRIGDEP</td>
</tr>
<tr>
<td></td>
<td>- SYSCAT.VIEWDEP</td>
</tr>
</tbody>
</table>

In addition, make sure that you the database user account has CREATEIN, DROPIN, and ALTERIN privileges on the required schema.

**JDBC with MySQL**

**Objects Extracted**

Enterprise Information Catalog extracts metadata of the following schema objects from a MySQL database that uses JDBC for connectivity:

- Tables
- Constraints (NOT NULL, UNIQUE, CHECK, PRIMARY KEY, FOREIGN KEY, DEFAULT)
- Clone Table
- Indexes
- Views
- Triggers
- Function
- Procedure
- Materialized View
- MV Trigger

**Permissions**

You must configure the CONNECT and SELECT_CATALOG_ROLE permissions for the database user account that you use to access the MySQL database.
**JDBC with AS400**

**Objects Extracted**

Enterprise Information Catalog extracts metadata of the following schema objects from an AS400 database that uses JDBC for connectivity:

- Tables
- Constraints (NOT NULL, UNIQUE, CHECK, PRIMARY KEY, FOREIGN KEY, DEFAULT)
- Alias
- Duplicate Table
- Sequences
- Views
- Triggers
- Function
- Procedure
- Index
- User defined data types

**Permissions**

You must configure the CONNECT and SELECT_CATALOG_ROLE permissions for the database user account that you use to access the AS400 database.

**IBM Netezza**

**Objects Extracted**

Enterprise Information Catalog extracts metadata of the following objects from an IBM Netezza data source:

- Column
- Data type
- Distribution key
- Distribution key column
- Expression
- External table
- Foreign key
- Materialized view
- Primary key
- Schema
- Sequence
- Synonym
- Table
- Unique key constraint
- View
Permissions

Configure the LIST privilege for the Netezza user to extract metadata from a Netezza database. The LIST privilege grants the Netezza user access to all database objects in the Netezza database through Enterprise Information Catalog. If required, you can assign database permissions to limit access to individual database objects.

Configure SELECT permissions for the Netezza user account on the following system views:

- `_V_TABLE_DIST_MAP`
- `_V_TABLE`
- `_V_DATABASE`
- `_v_relation_keydata`
- `_v_relation_column`
- `_v_view`
- `_v_synonym`
- `_v_datatype`
- `_v_sequence`

Teradata

Objects Extracted

- User
- Table
- Column
- Datatype
- View
- Index
- IndexColumn
- PrimaryKeyConstraint
- ForeignKey
- UniqueConstraint
- CheckConstraint
- Procedure
- TableTrigger
- Macro

Permissions

Configure the permissions for the Teradata database user account that you use to connect to the Teradata database.
The following table lists the schema objects and system tables on which you must configure SELECT permissions for the Teradata database user account:

<table>
<thead>
<tr>
<th>Schema Objects</th>
<th>System Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tables</td>
<td>DBC.DBCINFO</td>
</tr>
<tr>
<td>Views</td>
<td>DBC.TABLETEXT</td>
</tr>
<tr>
<td>Indexes</td>
<td>DBC.HOSTSINFO</td>
</tr>
<tr>
<td>Packages</td>
<td>DBC.DATABASES</td>
</tr>
<tr>
<td>Procedures</td>
<td>DBC.TABLES</td>
</tr>
<tr>
<td>Functions</td>
<td>DBC.COLUMNS</td>
</tr>
<tr>
<td>Sequences</td>
<td>DBC.ALL_RI_CHILDREN</td>
</tr>
<tr>
<td>Triggers</td>
<td>DBC.INDICES</td>
</tr>
<tr>
<td>Synonyms</td>
<td>DBC.TRIGGERS</td>
</tr>
<tr>
<td></td>
<td>DBC.SHOWTBLCHECKS</td>
</tr>
</tbody>
</table>

**Business Intelligence Sources**

**Overview**

The permissions that you must configure on the business intelligence sources and the metadata extracted for these sources are included in the following sections:

**IBM Cognos**

**Objects Extracted**

Enterprise Information Catalog extracts metadata of the following schema objects from an IBM Cognos Business Intelligence Suite data source:

- Axis
- Body
- Crosstab
- Crosstab Columns
- Crosstab Node
- Crosstab Node Member
- Data Sources
- DataAttribute
- Database Query
- Dimension
- Field
- Filter
- Folder
- Footer
- Header
- Hierarchy
- Namespace
Permissions

Before you create an IBM Cognos resource, you must configure the permissions for the user account that you use to connect to IBM Cognos.
You must configure the read, execute, and traverse permissions for all objects for which Enterprise Information Catalog extracts metadata. For example, reports, queries, analysis, packages, and connections.

**MicroStrategy**

**Objects Extracted**

Enterprise Information Catalog extracts metadata of the following schema objects from a MicroStrategy Business Intelligence data source:

- (Report) Metric
- (Report) Subtotal
- Attribute
- Attribute Form
- Calculated Report Field
- Column
- Consolidation
- Consolidation Element
- Custom Group
- Database Instance
- Document
- Document Report
- Expression
- Filter
- Folder
- Hierarchy
- Metrics
- Project Folder
- Project Source
- Prompt
- Prompt Answer
- Report
- Report Axis
- Report Field
- Report Graph
- Report Grid
- Report Metric
- Report Page
- Report Page Body
- Report Page Footer
- Report Page Header
- Report Rectangle
- Report
Permissions

Ensure that you configure the Bypass All Object Security Access Checks administration privilege for the MicroStrategy project user account for which you provide the user name and password. You can configure the privilege in the Microstrategy Desktop client tool.

Oracle Business Intelligence

Objects Extracted

Enterprise Information Catalog extracts metadata of the following schema objects from an Oracle Business Intelligence data source:

- Alias Colum
- AliasPhysicalTable
- AnswersReport
- Axis
- BusinessModel
- Business Model and Mapping
- Catalog
- Condition
- Criteria
- Data Attribute Column
- Database
- Derived Presentation Column
- Design Package Subject Area
- Dimension Logical Column
- DynamicVariable
- FactLogicalTable
- Field
- Folder
- Gauge
- Graphic Chart
- Hierarchy
Permissions

Enterprise Information Catalog connects to the OBIEE Presentation Server to extract report metadata. Ensure that the OBIEE user account for which you provide the user name and password has read permission on the metadata that Enterprise Information Catalog extracts from OBIEE.

SAP Business Objects

Objects Extracted

Enterprise Information Catalog extracts metadata of the following schema objects from an SAP Business Objects data source:

- Body
- Cell
- Class
- Context
- Crystal Report
- Crystal Report Model
- Custom Hierarchies Folder
- Data Providers
- Derived Table
- EnterpriseFolder
- Field
- Filter
- Folder
- Footer
- Header
- Hierarchy
- Join
- Key
- Measure
- Page
- Query
- Rectangle
- Report Chart
- Schema
- Universe Query
- UniverseFolder
- Web Intelligence Document
- Web Intelligence Model
- Dimension
- Dimension Result
• Rectangle
• Dimension variable
• alias column
• section
• report field
• Text
• Measure result
• Business Object Table
• Report page
• Axis
• Report Table
• Formulas
• Special field
• Group Name Fields
• Alias table
• Report folder
• Summary fields
• Logical column
• Query filter
• Connection folder
• Connection model
• Database connection
• Business layer view
• Context
• Contexts
• Default hierarchies
• Detail
• Repository
• View
• Queries
• Connection Model
• Connection Package Data Source
• Crosstab
• Package
• Page
• Crosstab Columns
• Crosstab Corner
• Crosstab Node
• Crosstab Node Member
You must 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.

Make sure 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. You must create a custom security group and provide permission for the user to view Web intelligence reports.

**Tableau Server**

**Objects Extracted**

Enterprise Information Catalog extracts metadata of the following schema objects from a Tableau Server data source:

- Bins
- Columns
- Data sources
- Joins
• Marks
• Parameters
• Rows
• Mark
• Filter
• Field
• Dimension
• Marks
• Measure
• Row
• Shared Filter
• Unpublished Worksheet
• Calculation Measure
• Tableau Column
• Rows
• Columns
• Fact Table
• Parameter Measure
• Set
• Calculation Dimension
• Data Source
• Dashboard
• File
• Page
• Worksheet
• Group
• Connection
• Workbook
• Namespace
• Parameters
• Dimension Table
• Project
• Tableau Server
• Resource
• Alias Column
• Alias Table
• Axis
• Body
• Business Layer View
- Cell
- Class
- BusinessObjects Column
- ConnectionFolder
- Connection Model
- Context
- Contexts
- Crystal Report
- Crystal Report Model
- Custom Hierarchies
- Data Provider
- Database Connection
- Default Hierarchies
- Derived Table
- Data Source
- Dimension
- Dimension Result
- Dimension Variable
- EnterpriseFolder
- Field
- Filter
- Folder
- Footer
- Formulas
- Group Name Fields
- Header
- Hierarchy
- Join
- Key
- Logical Column
- Measure
- Measure Result
- Query
- Query Filter
- Rectangle
- Report Chart
- Report Field
- Report Folder
- Report Page
Permissions

To connect to Tableau Server, Enterprise Information Catalog uses the credentials of a user created on the Tableau Server. Make sure that you configure the user account with the following license levels and permissions:

- Interactor license level.
- View and Download permissions for all projects, workbooks, and data sources for which you want to extract metadata.

Data Integration Sources

Overview

The permissions that you must configure on the data integration sources and the metadata extracted for these sources are included in the following sections:
**Business Glossary**

**Objects Extracted**
- Category
- Term
- Glossary
- Policy

**Permissions**
None

**Informatica Axon**

**Objects Extracted**
Glossary

**Permissions**
None

**Informatica PowerCenter**

**Objects Extracted**
Mapping

**Permissions**
- Make sure that you configure the Access Repository Manager privilege for the user who accesses the PowerCenter repository.
- Configure read permission on the PowerCenter data source for the user account that you use to access the PowerCenter data source.
- Ensure that you run the `pmrep ObjectExport` command to export the mappings in PowerCenter.

**Informatica Platform**

**Objects Extracted**
Mapping

**Permissions**
None

**File System Sources**

**Overview**

The permissions that you must configure on the file system sources and the metadata extracted for these sources are included in the following sections:
**Amazon S3**

**Objects Extracted**
- File Permissions

Configure read permission on the Amazon S3 data source for the user account that you use to access the data source. Configure access permission for the user account if you use a user account that is different from the user account used to create the Amazon S3 data source.

**Azure WASB**

**Objects Extracted**
- File Permissions

Configure read permission on the Azure WASB data source for the user account that you use to access the data source.

**Filesystem**

**Objects Extracted**
- File Permissions

Configure read permission on the Filesystem data source for the user account that you use to access the data source.

**HDFS**

**Objects Extracted**
- File Permissions

Configure read permission on the HDFS data source for the user account that you use to access the data source.

**Azure Data Lake Store**

**Objects Extracted**
- File Permissions

If you create a new user, ensure that you configure read permission on the data source for the new user account.

**Microsoft Azure Blob Storage**

**Objects Extracted**
- File
Permissions
Configure read permission on the Microsoft Azure Blob Storage data source for the user account that you use to access the data source.

Microsoft SharePoint
Objects Extracted
• File
Permissions
Configure read permission on the Microsoft SharePoint data source for the user account that you use to access the data source.

Microsoft OneDrive
Objects Extracted
• File
Permissions
Configure read permission on the Microsoft OneDrive data source for the user account that you use to access the data source.

Application Data Sources

Overview
The permissions that you must configure on the application data sources and the metadata extracted for these sources are included in the following sections:

Salesforce
Objects Extracted
• Table
Permissions
None required.

SAP R/3
Objects Extracted
• Application components
• Packages
• Tables
• Columns
• Primary and foreign keys
Permissions
To configure SAP R/3, complete the following tasks:
1. Install PowerCenter transports.
2. Configure a user-authorization profile.
3. Install SAP SDK libraries (already present in the existing guide).

Installing PowerCenter Transports
To extract metadata from SAP R/3, you must install the PowerCenter transports that Enterprise Data Catalog uses to extract metadata from SAP R/3. The transports are located in the following folder in the location where you downloaded PowerCenter:

<download location>\saptrans\mySAP

For more information about installing the transports, see the PowerExchange for SAP NetWeaver Transport Versions Installation Notice.

Configuring a User-authorization Profile
The SAP R/3 administrator needs to create the product and development user authorization profile. The following table describes the user authorization profile:

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Description</th>
<th>Class</th>
<th>Field Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>Authorization check for RFC access.</td>
<td>Cross Application Authorization objects</td>
<td>Activity: 16 (Execute) Name of RFC to be protected: *. Type of RFC object to be protected: FUGR</td>
</tr>
</tbody>
</table>

Hadoop Data Sources

Overview
The permissions that you must configure on the hadoop data sources and the metadata extracted for these sources are included in the following sections:

Cloudera Navigator

Objects Extracted
- HDFS files, directories, and datasets
- Hive tables, query templates, and query executions
- Impala query templates and executions
- MapReduce job templates and executions
- Oozie job templates and executions
- Pig tables, job templates, and job executions
- Sqoop job templates and executions
- YARN job templates and executions
Permissions

Before you create a Cloudera Navigator resource, you must configure the Java heap size for the Cloudera Navigator server and the maximum heap size for Catalog Service. If you do not correctly configure the heap sizes, the metadata load can fail.

Configure the following heap sizes:

- Java heap size for the Navigator server. Before you create a Cloudera Navigator resource, set the Java heap size for the Cloudera Navigator Server to at least 2 GB. If the heap size is not sufficient, the resource load fails with a connection refused error.

- Maximum heap size for the Catalog Service. Before you create a Cloudera Navigator resource, open the Administrator tool and check the value of the Max Heap Size property for the Catalog Service. Set the maximum heap size to at least 4096 MB (4 GB).

If you perform simultaneous resource loads, increase the maximum heap size by at least 1024 MB (1 GB) for each resource load. For example, to load two Cloudera Navigator resources simultaneously, increase the maximum heap size by 2048 MB (2 GB). Therefore, you would set Max Heap Size to at least 6144 MB.

Note: Some Cloudera distributions might require a maximum heap size larger than 4 GB. If the metadata load fails with an out of memory error, increase the maximum heap size.

Apache Atlas

Objects Extracted

Data object links from the following data sources:

- Relational databases
- Hive
- HDFS.

Note: Ensure that you configure resources in Enterprise Data Catalog for the data sources from which you want to extract data object links.

Permissions

None required.

Hive

Objects Extracted

- Table
- View

Permissions

Configure read permission on the Hive data source for the user account that you use to access the data source.

Author

Suraj Jayan

Acknowledgements
The author would like to acknowledge Gaurav Pathak, Abdullah Rao, Sudhanshu Kumar Singh, Bharadwaja Subramanya, Krishnamoorthy Gurramkonda, Rashmi Mani, and Aseem Srivastava for their contributions to this article.