Required RDBMS rights for packaging a database

On this page:

Target audience:

CAST Administrators, Delivery Managers

Summary: This page describes the RDBMS rights and privileges required to package a database using the CAST Delivery Manager Tool. Note that these rights are also detailed in the CAST Delivery Manager Tool help.

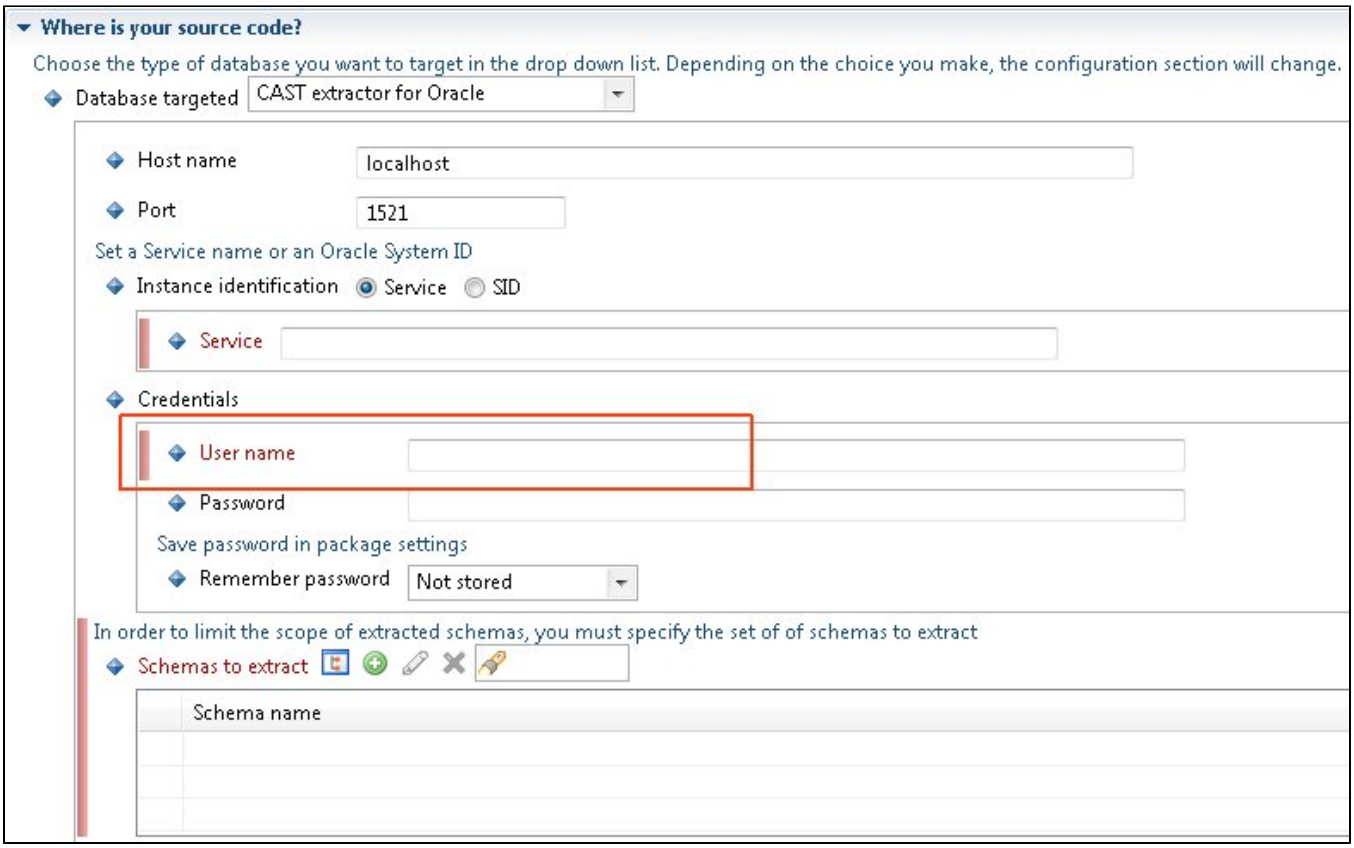
Introduction

The CAST Delivery Manager Tool provides the means for Delivery Managers to:

1. configure a connection to a live **Oracle Server/Microsoft SQL Server/Sybase ASE** and then use this connection to perform an **extraction** of the relevant schemas to file using CAST's own SQL extractor. The extraction data is then packaged for analysis in the CAST Management Studio
2. configure a connection to a live **DB2 UDB server** and then **package the connection details** ready for use in the CAST Management Studio.

For both scenarios, Delivery Managers must ensure that they configure their package with a user that has sufficient rights to perform an extraction (scenario 1) or a live analysis (scenario 2), otherwise essential data may not be included. This page provides the required rights for all RDBMS systems supported by CAST for analysis.

Oracle Server



In order to carry out an extraction of the required schemas, the person in charge of the extraction (Delivery Manager or DBA) must use one of the following Oracle users:

User	Notes
Extraction user	CAST highly recommends using a dedicated **extraction user** with **specific privileges** in order to access the required data for extraction. When u **DBA_* views** to access the required data - these views give access to ALL objects. Please also read the section below entitled "**Note about the user**". To create the dedicated extraction user, please run the following script as the **SYS** user - it will create the dedicated user and then grant the requ USER_FOR_EXTRACTION is the dedicated extraction user):

```
create user USER_FOR_EXTRACTION identified by cast
/
grant connect to USER_FOR_EXTRACTION
/
grant create session to USER_FOR_EXTRACTION
/
grant select on dba_arguments to USER_FOR_EXTRACTION
/
grant select on dba_col_comments to USER_FOR_EXTRACTION
/
grant select on dba_tab_comments to USER_FOR_EXTRACTION
/
/*
*   The view dba_mview_comments does not exist on Oracle 9.x, therefore the
*   following grant should not be executed when running the extraction on Oracle 9i.
*/
grant select on dba_mview_comments to USER_FOR_EXTRACTION
/
grant select on dba_coll_types to USER_FOR_EXTRACTION
/
grant select on dba_cons_columns to USER_FOR_EXTRACTION
/
grant select on dba_constraints to USER_FOR_EXTRACTION
/
grant select on dba_db_links to USER_FOR_EXTRACTION
/
grant select on dba_dependencies to USER_FOR_EXTRACTION
/
grant select on dba_ind_columns to USER_FOR_EXTRACTION
/
grant select on dba_ind_expressions to USER_FOR_EXTRACTION
/
grant select on dba_indexes to USER_FOR_EXTRACTION
/
grant select on dba_mviews to USER_FOR_EXTRACTION
/
grant select on dba_object_tables to USER_FOR_EXTRACTION
/
grant select on dba_objects to USER_FOR_EXTRACTION
/
grant select on dba_procedures to USER_FOR_EXTRACTION
/
grant select on dba_sequences to USER_FOR_EXTRACTION
/
grant select on dba_source to USER_FOR_EXTRACTION
/
grant select on dba_synonyms to USER_FOR_EXTRACTION
/
grant select on dba_tab_columns to USER_FOR_EXTRACTION
/
grant select on dba_tables to USER_FOR_EXTRACTION
/
grant select on dba_triggers to USER_FOR_EXTRACTION
/
grant select on dba_types to USER_FOR_EXTRACTION
/
grant select on dba_users to USER_FOR_EXTRACTION
/
grant select on dba_views to USER_FOR_EXTRACTION
/
```

Note about the DBA_USERS view and the dedicated extraction user

Situation

- If you are using the **dedicated extraction user** (as recommended and outlined above) to perform your extraction, a view called **DBA_USER** extraction
- If you do not want to grant the select right on this view for security reasons, you can change the script above to use a synonym instead of th

Action

- Comment the following lines in the above script as follows:

```
-- grant select on dba_users to USER_FOR_EXTRACTION
-- /
```

- Add two new lines to the script as follows:

```
create synonym USER_FOR_EXTRACTION.DBA_USERS for SYS.ALL_USERS
/
```

- Re-run the script as the SYS user
- Use the dedicated extraction user in any future extractions

Impacts

- There are no impacts - results when using the synonym instead of the grant select on the DBA_USERS view are identical.

Note about DBA_MVIEW_COMMENTS / ALL_MVIEW_COMMENTS views and Oracle 9.x

The views DBA_MVIEW_COMMENTS / ALL_MVIEW_COMMENTS do not exist on Oracle 9.x, therefore when running an extraction on Oracle 9 Oracle user), the extractor will use DBA_TAB_COMMENTS to extract comments on materialized views instead. Results are not impacted. This w

```
Unable to use access mode: Extracting comments on materialized views using DBA_MVIEW_COMMENTS
No access to: DBA_MVIEW_COMMENTS
Unable to use access mode: Extracting comments on materialized views using ALL_MVIEW_COMMENTS. Using ALL_M
including AFP.
No access to: ALL_MVIEW_COMMENTS
Using access mode: Extracting comments on materialized views using DBA_TAB_COMMENTS on Oracle 9i
```

Note about the DBA_ARGUMENTS view and the dedicated extraction user

Situation

- If you are using the **dedicated extraction user** (as recommended and outlined above) to perform your extraction, a view called **DBA_ARGU** extraction
- On some Oracle Servers (Oracle 10.2.0.4.0 or any earlier Oracle 10 version and all Oracle 9 versions) this view is **not present by default**, t

Impacts

The extraction will succeed, but:

- Oracle extractor log contains 'Extraction error: ORA-00942: table or view does not exist' in section 'Extracting: Oracle wrapped valid functior
- Extraction will be incomplete - i.e. the following information will be missing:
  - IN/OUT parameters will be missing for all procedures and functions outside of the user's own schema, unless the user has the EXECUT is true for the return code of functions. This will impact the analysis and Quality Rules based on datatypes of functions/procedures/para
  - IN/OUT parameters will be missing from the source code generated for wrapped procedures or functions, therefore they will not be visil Dashboard.
  - Return code will be missing from the source code generated for wrapped functions, therefore they will not be visible in CAST Enlighten

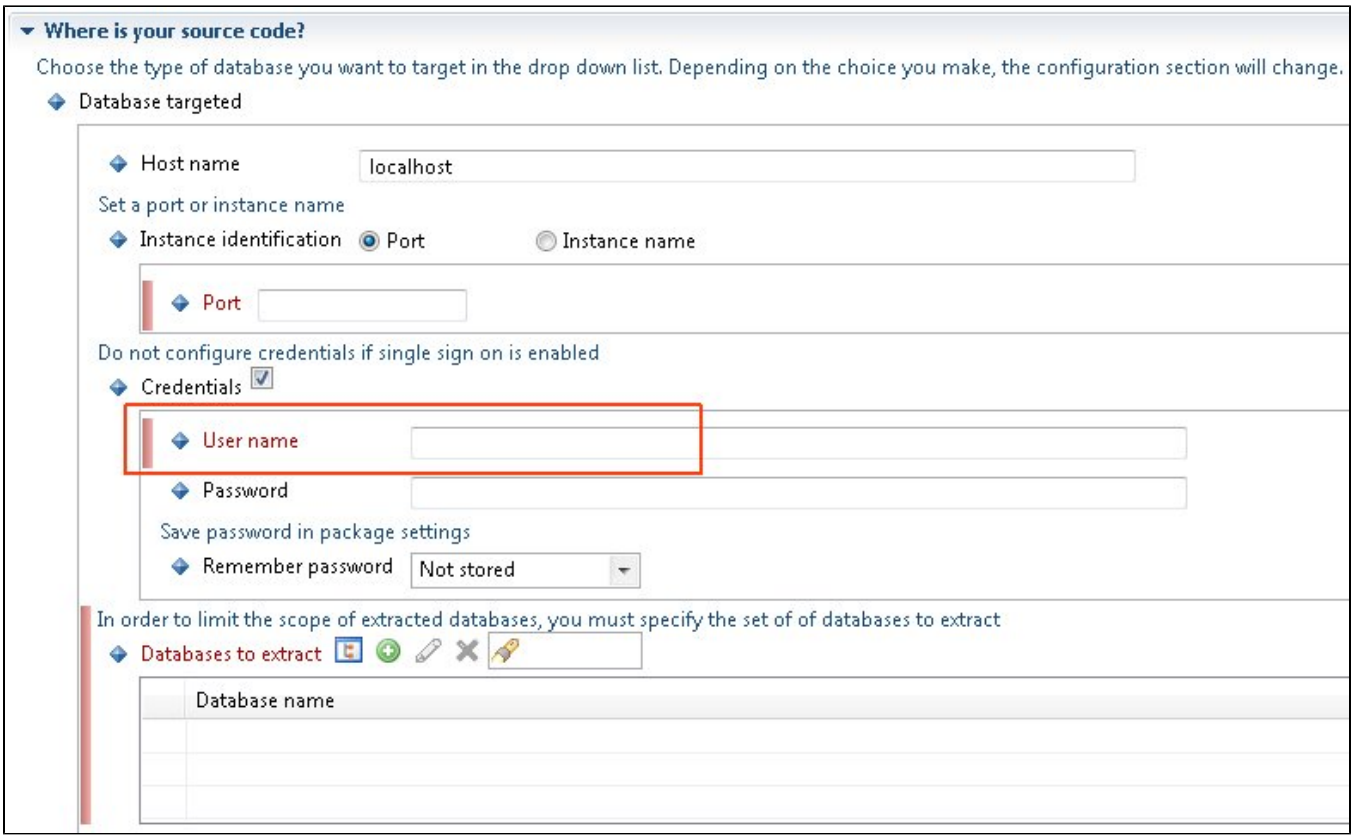
Note that there is no impact on the source code for unwrapped function/procedures because this code is not generated and is instead ex

Options

Two options exist if you find yourself in this situation:

	1. Manually create the **DBA_ARGUMENTS** view on the Oracle server prior to running the extraction. To do so, please use this script. Note tha the view has been created, you can perform an extraction and analysis results will be correct. 2. If it is not possible to create the DBA_ARGUMENTS view: a. then if the "**ALL Access**" mode is unchecked the extraction will not be possible and will fail b. then if the "**ALL Access**" mode is checked the extraction will be possible but you must accept that the extraction results will be incompl
SYSTEM	When it is not possible to use the **dedicated extraction user**, CAST recommends using the **SYSTEM** user instead. CAST will query the **DBA_*** access to ALL objects.
Other Oracle users	When it is not possible to use the **dedicated extraction user** or the **SYSTEM** user as outlined above, it is possible to use any other user (i.e. nor **ma owner user**. However, there are several drawbacks to doing this and **CAST therefore does not recommend using this type of user**: • CAST will query the **ALL_* views** to access the required data - these views only give access to objects that the user is entitled to access. T extraction will contain all the required data. • Performance of the extraction will be reduced. Note also that in order for the **ALL_* views** to be queried, the **ALL access mode** option must be explicitly selected in the CAST Delivery  This option (**when selected**) explicitly allows the CAST Delivery Manager Tool to query the **ALL_* views** to access the required data - t entitled to access. This means that CAST **cannot guarantee** that the extraction will contain all the required data. In addition, performanc By default this option is **not selected**, which automatically prevents the CAST Delivery Manager Tool from using the **ALL_* views** to acc that you have entered into the "User Name" field above does not have sufficient rights to query the **DBA_* views** then the CAST Delivery and if the **ALL access mode** option is not selected, then the extraction will fail. Please avoid using the SYS user to perform extractions. Results cannot be guaranteed.

Microsoft SQL Server



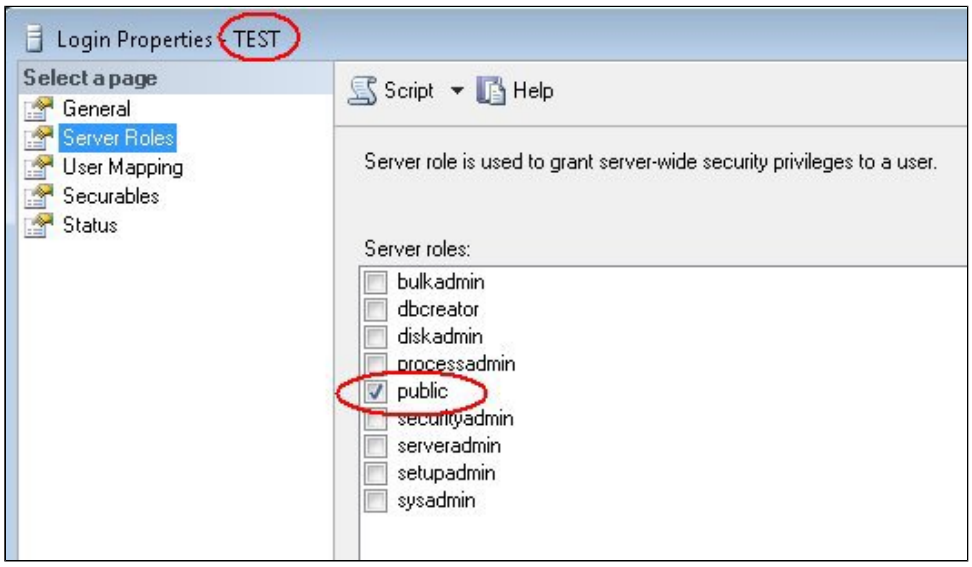
In order to carry out an extraction of the required databases, the person in charge of the extraction (Delivery Manager or DBA) must use a Microsoft SQL Server **login** (whether using Windows or SQL authentication) that has the following roles and permissions:

User	Required roles and permissions

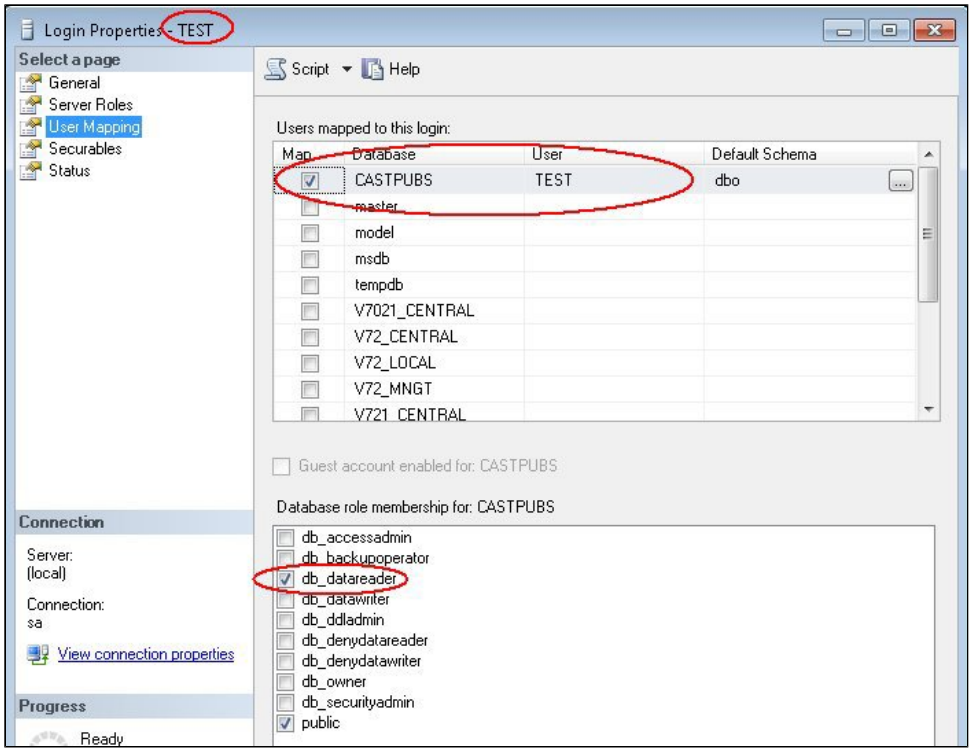
Any user with the following permissions and roles	• "**public**" Server Role
	• "**db-datareader**" Database Role on all databases that require extraction (i.e. the **login** is mapped as a **User** on the target databases and is given the "db-datareader" Database Role)
	• "**View definition**" + "**Grant**" explicit permission on all databases that require extraction (i.e. the explicit permission is given to the **User**)
	
	An example script to assign the required role and permissions is shown below:
	
	`-- Create an SQL Server login`
	`CREATE LOGIN <login> WITH PASSWORD = '<password>';`
	`GO`
	`-- Create a database user (on all databases that require extraction) for the login created above`
	`-- this will also automatically assign the CONNECT + GRANT explicit permission`
	`Use <database>`
	`GO`
	`CREATE USER <user> FOR LOGIN <login>;`
	`GO`
	`-- Assign the db_datareader database role to the user created above for all databases that require extraction`
	`Use <database>`
	`GO`
	`exec sp_addrolemember 'db_datareader', <user>`
	`GO`
	`-- Assign your user the View definition + GRANT explicit permission on all databases that require extraction`
	`Use <database>`
	`GO`
	`GRANT View definition TO <user>`
	`GO`

The following screenshots show the same changes performed in the Microsoft SQL Server GUI:

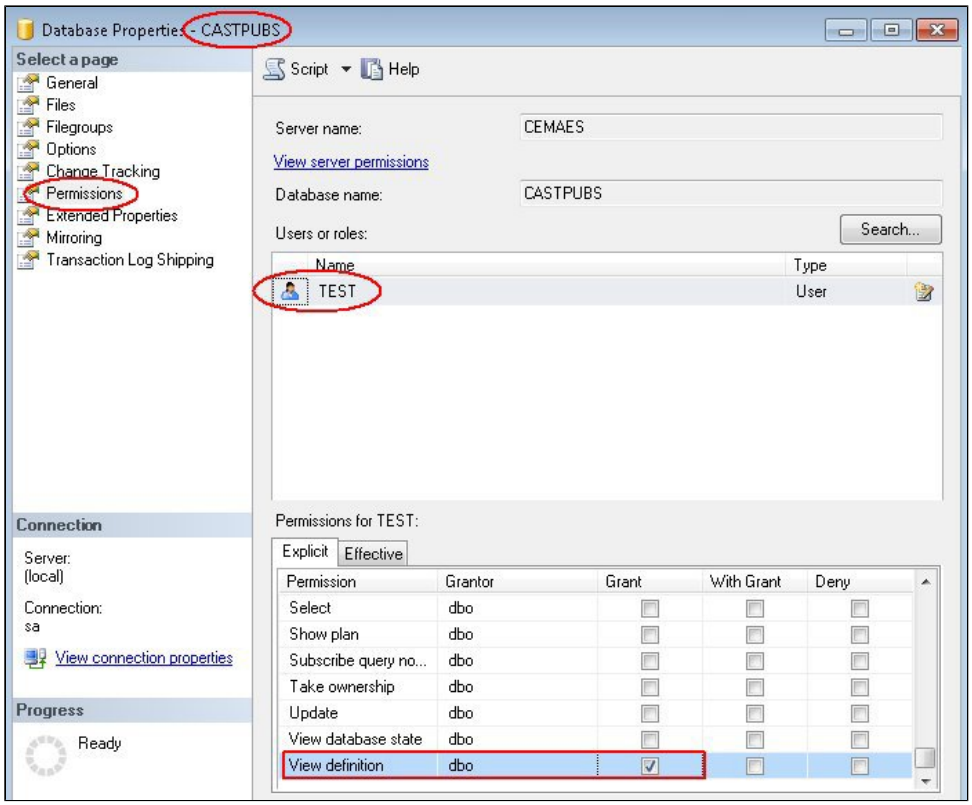
- A login (whether using Windows or SQL authentication) must be defined in the SQL Server. This login requires NO "Server Roles" at all, apart from "public" which is granted automatically when the login is created:



- Under "User Mapping" (login properties), the login must be assigned the "db_datareader" database role for for all databases that require extraction:



- Lastly in the Properties of all databases that require extraction, assign your user the "View definition" + "Grant" explicit permission:



Extraction user

When it is not possible to grant a user the "**public**" Server Role and the "**db-datareader**" Database Role as outlined above, CAST recommends using a dedicated **extraction user** with **specific privileges** in order to access the required data for extraction.

An example script to assign the required role and permissions is shown below:

```
-- Create an SQL Server login
CREATE LOGIN <login> WITH PASSWORD = '<password>';
GO

-- Create a database user (on all databases that require extraction) for the login
created above
-- this will also automatically assign the CONNECT + GRANT explicit permission
Use <database>
GO
CREATE USER <user> FOR LOGIN <login>;
GO

-- Issue grant on specific tables
GRANT SELECT ON master.dbo.sysdatabases TO <user>
GO
GRANT SELECT ON master.dbo.spt_values TO <user>
GO
GRANT SELECT ON master.dbo.syscharsets TO <user>
GO
GRANT SELECT ON master.dbo.syscurconfigs TO <user>
GO
GRANT SELECT ON sys.databases TO <user>
GO
GRANT SELECT ON sys.schemas TO <user>
GO
GRANT SELECT ON sys.columns TO <user>
GO
GRANT SELECT ON sys.types TO <user>
GO
GRANT SELECT ON sys.foreign_keys TO <user>
GO
GRANT SELECT ON sys.sysforeignkeys TO <user>
GO
GRANT SELECT ON sys.tables TO <user>
GO
GRANT SELECT ON sys.foreign_key_columns TO <user>
GO
GRANT SELECT ON sys.views TO <user>
GO
GRANT SELECT ON sys.procedures TO <user>
GO
GRANT SELECT ON sys.numbered_procedures TO <user>
GO
GRANT SELECT ON sys.objects TO <user>
GO
GRANT SELECT ON sys.trigger_events TO <user>
GO
GRANT SELECT ON sys.triggers TO <user>
GO
GRANT SELECT ON dbo.sysobjects TO <user>
GO
GRANT SELECT ON dbo.sysusers TO <user>
GO
GRANT SELECT ON dbo.systypes TO <user>
GO
GRANT SELECT ON dbo.sysforeignkeys TO <user>
GO
GRANT SELECT ON dbo.syscomments TO <user>
GO

--Issue grant select to extraction user on databases that require extraction
use <database>
GO
GRANT SELECT TO <user>
GO
```

Sybase ASE

In order to carry out an extraction of the required databases, the person in charge of the extraction (Delivery Manager or DBA) must use a Sybase ASE **login** that has the following roles and permissions:

- **CONNECT** role
- **SELECT** permission on the following tables:
  - **master.dbo.sysdatabases**
  - **master.dbo.spt_values**
  - **master.dbo.syscurconfigs**
- For **each target database** you want to extract, the **SELECT** permission is required on the following tables:
  - **[%SQLdatabase%].dbo.sysusers**
  - **[%SQLdatabase%].dbo.sysconstraints**
  - **[%SQLdatabase%].dbo.sysreferences**
  - **[%SQLdatabase%].dbo.sysobjects**
  - **[%SQLdatabase%].dbo.syscolumns**
  - **[%SQLdatabase%].dbo.sysindexes**
  - **[%SQLdatabase%].dbo.syscomments**
  - **[%SQLdatabase%].dbo.systypes**

DB2 UDB

In order to package the connection parameters for the required schemas and for subsequent analysis of these schemas, the person in charge of the configuration (Delivery Manager or DBA) must use a DB2 UDB **login** that has the following roles and permissions:

- read access to all views in the **SYSCAT schema**.
- **connect to database** permission

These rights are already available to the PUBLIC group by default.