

# SQL - Required RDBMS rights for packaging a database using the legacy CAST Delivery Manager Tool



The information below is valid **only those using the PL/SQL and T-SQL database extractors embedded in the CAST Delivery Manager Tool**. See [SQL - Available extensions](#) for information about SQL related extensions.

- [Introduction](#)
- [Oracle Server](#)
  - [Note about the DBA\\_USERS view and the dedicated extraction user](#)
    - [Situation](#)
    - [Action](#)
    - [Impacts](#)
  - [Note about DBA\\_MVIEW\\_COMMENTS / ALL\\_MVIEW\\_COMMENTS views and Oracle 9.x](#)
  - [Note about the DBA\\_ARGUMENTS view and the dedicated extraction user](#)
    - [Situation](#)
    - [Impacts](#)
    - [Options](#)
- [Microsoft SQL Server](#)
- [Sybase ASE](#)



**Summary:** This page describes the RDBMS rights and privileges required to package a database using the legacy 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 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. Delivery Managers must ensure that they configure their package with a user that has sufficient rights to perform an extraction, otherwise essential data may not be included. This page provides the required rights for all RDBMS systems supported by CAST for live extraction.

## Oracle Server

▼ **Where is your source code?**

Choose the type of database you want to target in the drop down list. Depending on the choice you make, the configuration section will change.

◆ Database targeted

◆ Host name

◆ Port

Set a Service name or an Oracle System ID

◆ Instance identification  Service  SID

◆ Service

◆ Credentials

◆ User name

◆ Password

Save password in package settings

◆ Remember password

In order to limit the scope of extracted schemas, you must specify the set of of schemas to extract

◆ Schemas to extract

Schema name

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
<b>Extraction user</b>	<p>CAST highly recommends using a dedicated <b>extraction user</b> with <b>specific privileges</b> in order to access the required data for extraction. When using <b>DBA_* views</b> to access the required data - these views give access to ALL objects. Please also read the section below entitled "<b>Note about the user</b>".</p> <p>To create the dedicated extraction user, please run the following script as the <b>SYS</b> user - it will create the dedicated user and then grant the required privileges (USER_FOR_EXTRACTION is the dedicated extraction user):</p> <pre> CREATE USER extraction_user IDENTIFIED BY password; GRANT SELECT ANY TABLE TO extraction_user; GRANT EXECUTE ANY PROCEDURE TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_INQ TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_EXTENSION TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N2 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N3 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N4 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N5 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N6 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N7 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N8 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N9 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N10 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N11 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N12 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N13 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N14 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N15 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N16 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N17 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N18 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N19 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N20 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N21 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N22 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N23 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N24 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N25 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N26 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N27 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N28 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N29 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N30 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N31 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N32 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N33 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N34 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N35 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N36 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N37 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N38 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N39 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N40 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N41 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N42 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N43 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N44 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N45 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N46 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N47 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N48 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N49 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N50 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N51 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N52 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N53 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N54 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N55 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N56 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N57 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N58 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N59 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N60 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N61 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N62 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N63 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N64 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N65 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N66 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N67 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N68 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N69 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N70 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N71 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N72 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N73 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N74 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N75 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N76 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N77 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N78 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N79 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N80 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N81 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N82 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N83 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N84 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N85 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N86 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N87 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N88 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N89 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N90 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N91 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N92 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N93 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N94 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N95 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N96 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N97 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N98 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N99 TO extraction_user; GRANT EXECUTE ON SYS.DBMS_EXPORT_I18N100 TO extraction_user; </pre>

```

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\_USEF** 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\_ARGI** 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 functor
- 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 EXECU' 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 visible in CAST Enlighten 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 that 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. **normal 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. The 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



The screenshot shows a configuration window for Oracle extraction. It includes a text input for 'JVM Memory Size' set to '1G', a checkbox for 'Anonymize log file', and a checkbox for 'ALL access mode' which is checked. A warning message states: 'The ALL access mode uses ALL\_\* views for the Oracle extraction. Warning: this mode may extract less information than regular mode, which uses DBA\_\* views.'

This option (**when selected**) explicitly allows the CAST Delivery Manager Tool to query the **ALL\_\* views** to access the required data - that is entitled to access. This means that CAST **cannot guarantee** that the extraction will contain all the required data. In addition, performance

By default this option is **not selected**, which automatically prevents the CAST Delivery Manager Tool from using the **ALL\_\* views** to access that you have entered into the "User Name" field above does not have sufficient rights to query the **DBA\_\* views** then the CAST Delivery Manager 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

**▼ Where is your source code?**

Choose the type of database you want to target in the drop down list. Depending on the choice you make, the configuration section will change.

◆ Database targeted

◆ Host name

Set a port or instance name

◆ Instance identification  Port  Instance name

◆ Port

Do not configure credentials if single sign on is enabled

◆ Credentials

◆ User name

◆ Password

Save password in package settings

◆ Remember password

In order to limit the scope of extracted databases, you must specify the set of of databases to extract

◆ Databases to extract

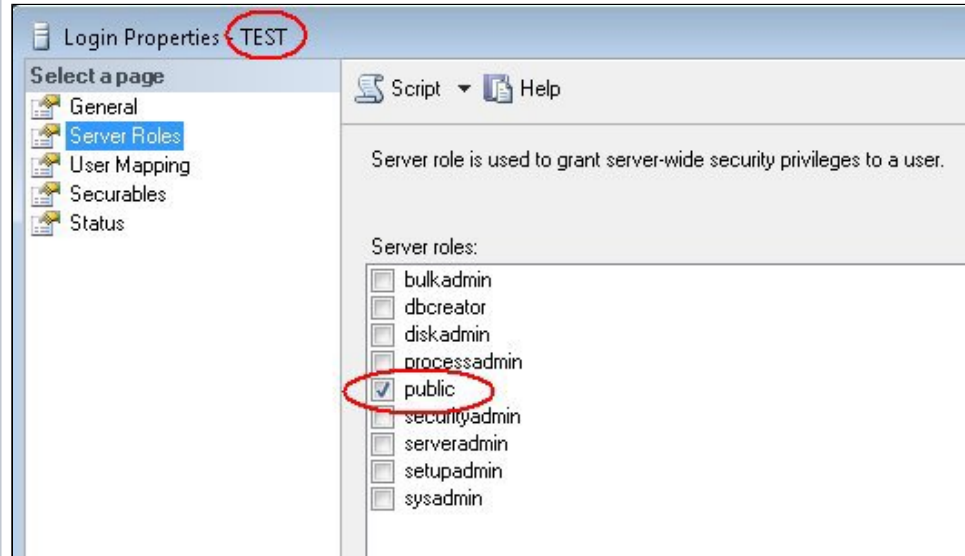
Database name

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:

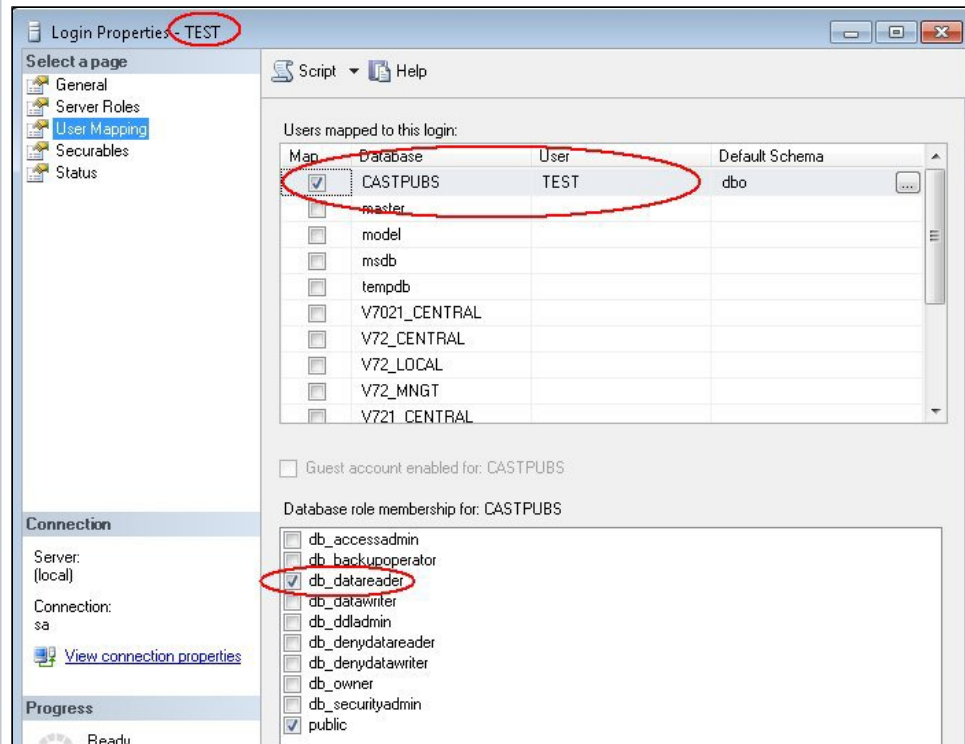
User	Required roles and permissions
Any user with the following permissions and roles	<ul style="list-style-type: none"> <li>• "public" Server Role</li> <li>• "db-datareader" Database Role on all databases that require extraction (i.e. the <b>login</b> is mapped as a <b>User</b> on the target databases and is given the "db-datareader" Database Role)</li> <li>• "View definition" + "Grant" explicit permission on all databases that require extraction (i.e. the explicit permission is given to the <b>User</b>)</li> </ul> <p>An example script to assign the required role and permissions is shown below:</p> <pre>-- Create an SQL Server login CREATE LOGIN &lt;login&gt; WITH PASSWORD = '&lt;password&gt;'; 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 &lt;database&gt; GO CREATE USER &lt;user&gt; FOR LOGIN &lt;login&gt;; GO -- Assign the db_datareader database role to the user created above for all databases that require extraction Use &lt;database&gt; GO exec sp_addrolemember 'db_datareader', &lt;user&gt; GO -- Assign your user the View definition + GRANT explicit permission on all databases that require extraction Use &lt;database&gt; GO GRANT View definition TO &lt;user&gt; GO</pre>

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

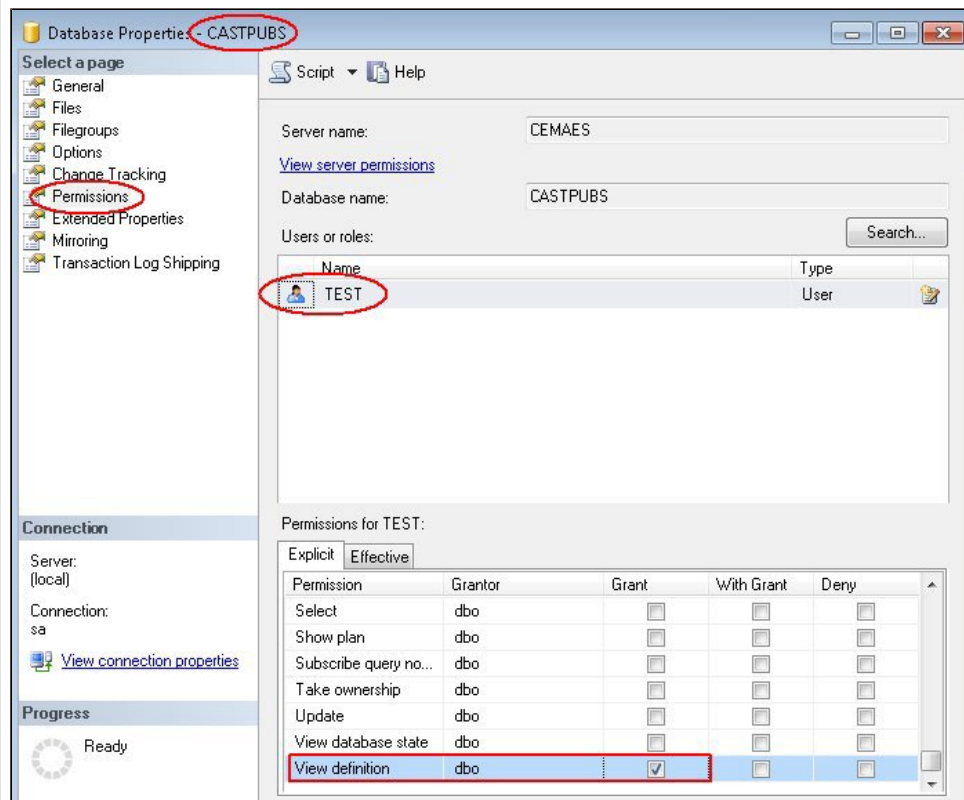
- A login (whether using Windows or SQL authentication) must be defined in the SQL Server. This login requires NO "Server Roles" at all, apart from "public" which is granted automatically when the login is created:



- 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 VIEW ANY DEFINITION 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**