Ajith's Documentum Security Notes

Content Server supports a set of **user privileges**, **object level permissions** and **table permits**, which determine what operations a user can perform on a particular object

User privileges are always enforced whether repository security is turned on or not. **Object-level permissions and table permits are only enforced when repository security is on**. Repository security is controlled by the security_mode attribute in the docbase config object. The attribute is set to ACL, which turns on security, when a repository is created.

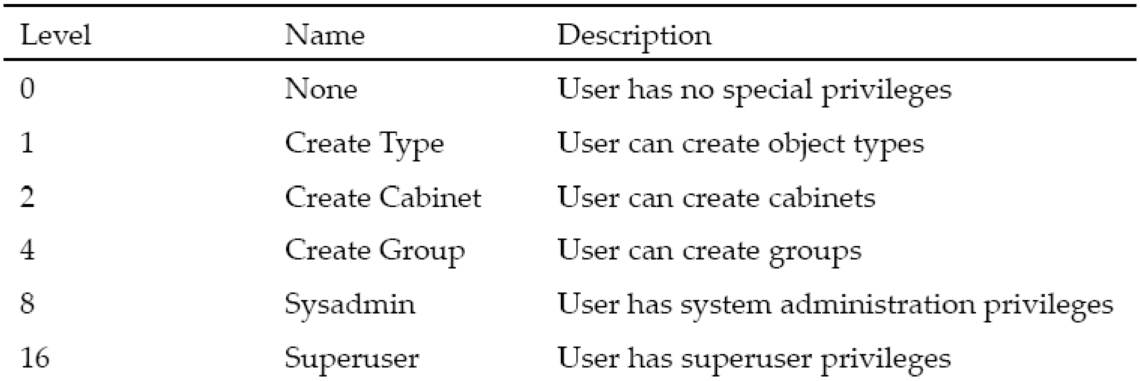
Consequently, unless you have explicitly turned security off by setting security_mode to none, object-level permissions and table permits are always enforced.

User Privileges

There are two types of user privileges: basic and extended. The **basic privileges define the Operations that a user can perform on SysObjects in the repository**. The **extended privileges define the security-related operations the user can perform**.

Basic privileges

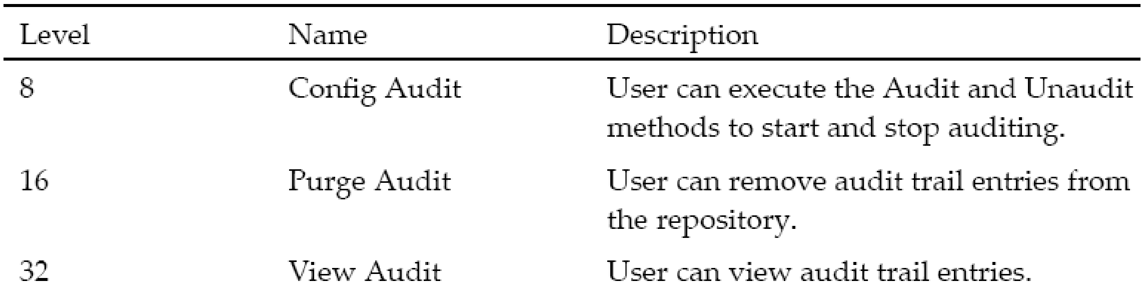
Basic privileges are Additive and not hierarchical
For example, granting Create Group to a user does not give the user Create Cabinet or Create Type privileges. If you want a user to have both privileges, you must explicitly give them both privileges.



Level	Name	Description
0	None	User has no special privileges
1	Create Type	User can create object types
2	Create Cabinet	User can create cabinets
4	Create Group	User can create groups
8	Sysadmin	User has system administration privileges
16	Superuser	User has superuser privileges

User privileges do **not override object-level permissions** when repository security is turned on. However, a **superuser always has at least Read permission on any object and can change the object-level permissions assigned to any object**.

Extended User Privileges



Level	Name	Description
8	Config Audit	User can execute the Audit and Unaudit methods to start and stop auditing.
16	Purge Audit	User can remove audit trail entries from the repository.
32	View Audit	User can view audit trail entries.

The extended user privileges are not hierarchical. For example, granting a user Purge Audit privilege does not confer Config Audit privilege also.

Repository owners, superusers, and users with the View Audit permission can view all audit trail entries. Other users in a repository can view only those audit trail entries that record information about objects other than ACLs, groups, and users.
Only repository owners and Superusers may grant and revoke extended user privileges, but they may not grant or revoke these privileges for themselves.

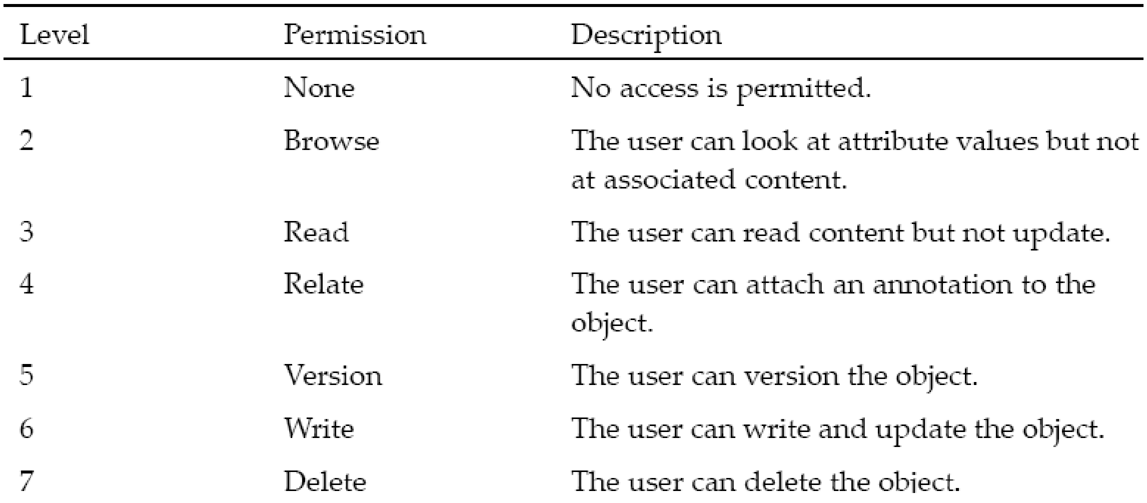
Object –Level Permissions

Object-level permissions are **access permissions assigned to every SysObject** (and SysObject subtype) in the repository. **Object-level permissions are defined as entries in ACL objects**. Each SysObject (or SysObject subtype) object has an associated ACL. The entries in the ACL identify users and groups and define their object-level permissions to the object with which the ACL is associated

There are two kinds of object-level permissions: base permissions and extended permissions.

Base Object- Level Permissions

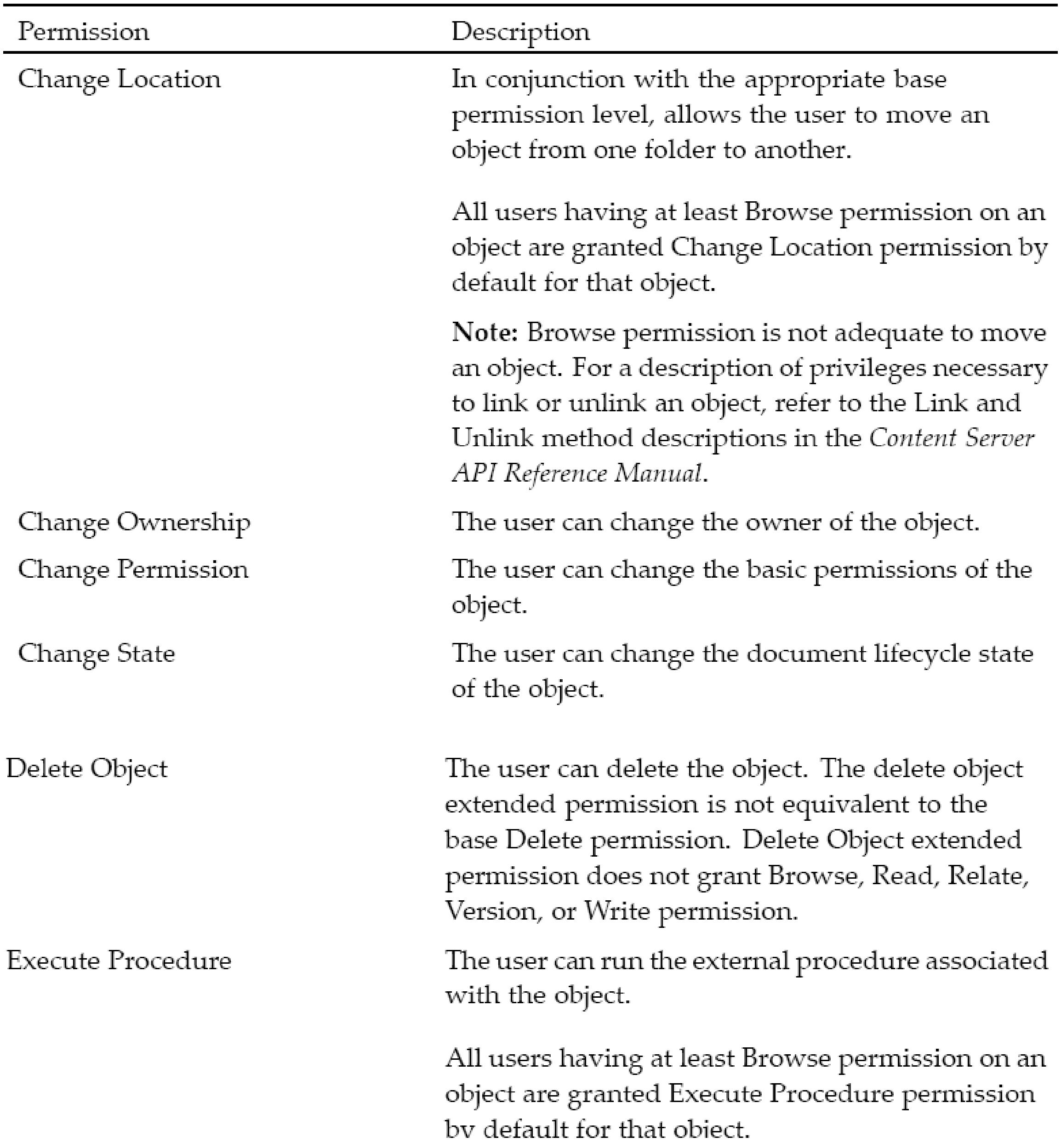
These permissions are hierarchical. For example, a user with Version permission also has the access accompanying Read and Browse permissions. Or, a user with Write permission also has the access accompanying Version permission.



Level	Permission	Description
1	None	No access is permitted.
2	Browse	The user can look at attribute values but not at associated content.
3	Read	The user can read content but not update.
4	Relate	The user can attach an annotation to the object.
5	Version	The user can version the object.
6	Write	The user can write and update the object.
7	Delete	The user can delete the obiect.

Extended Object –Level Permissions

The extended permissions **are not hierarchical**. You must **assign each explicitly**



Permission	Description
Change Location	In conjunction with the appropriate base permission level, allows the user to move an object from one folder to another. All users having at least Browse permission on an object are granted Change Location permission by default for that object. **Note:** Browse permission is not adequate to move an object. For a description of privileges necessary to link or unlink an object, refer to the Link and Unlink method descriptions in the *Content Server API Reference Manual*.
Change Ownership	The user can change the owner of the object.
Change Permission	The user can change the basic permissions of the object.
Change State	The user can change the document lifecycle state of the object.
Delete Object	The user can delete the object. The delete object extended permission is not equivalent to the base Delete permission. Delete Object extended permission does not grant Browse, Read, Relate, Version, or Write permission.
Execute Procedure	The user can run the external procedure associated with the object. All users having at least Browse permission on an object are granted Execute Procedure permission bv default for that obiect.

Object owners have Delete permission on the objects they own by default, also have Change Location and Execute Procedure permissions on those objects also.

Superusers have Read permission and all extended permissions except Delete Object by default on any object.

Table permits

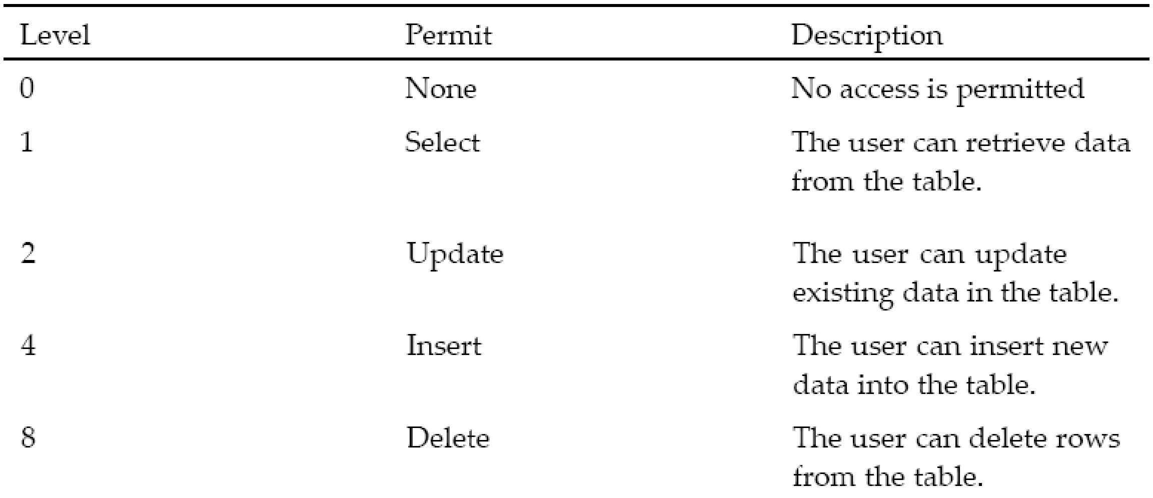
The table permits control access to the RDBMS tables represented by registered tables in the repository.
To access an RDBMS table using DQL, you must have:

At least Browse access for the dm_registered object representing the RDBMS table

The appropriate table permit for the operation that you want to perform

Superusers can access all RDBMS tables in the database using a SELECT statement regardless of whether the table is registered or not.

The permits are not hierarchical. For example, assigning the permit to insert does not confer the permit to update. **To assign more than one permit, you add together the integers representing the permits you want to assign and set the appropriate attribute to the total.**



Level	Permit	Description
0	None	No access is permitted
1	Select	The user can retrieve data from the table.
2	Update	The user can update existing data in the table.
4	Insert	The user can insert new data into the table.
8	Delete	The user can delete rows from the table.

Roles and Privileges

Sysadmin

Create, alter, and drop users and groups
Create, modify, and delete system-level ACLs
Grant and revoke Create Type, Create Cabinet, and Create Group privileges
Create types, cabinets, and printers
Manipulate workflows or work items, regardless ofownership
Manage any object’s lifecycle
Set the a_full_text attribute

Note*: The Sysadmin privilege does not override object-level permissions*

Super User

Perform all the functions of a user with Sysadmin privileges
Unlock objects in the repository
Modify or drop another user’s user-defined object type
Create subtypes that have no supertype
Register and unregister another user’s tables
Select from any underlying RDBMS table regardless of whether it is registered or not
Modify or remove another user’s groups or private ACLs
Create, modify, or remove system ACLs
Grant and revoke Superuser and Sysadmin privileges
Grant and revoke extended privileges
View audit trail entries