LOGALI

Teoría

Access Control

ABAP Cloud – Modelado con CDS

Contenido

6. Access Control

6.1. Acceso Literal

Es un artefacto utilizado para gestionar y controlar el acceso a los datos en sistemas de datos compartidos (CDS). Se implementa utilizando el Data Control Language (DCL), que permite definir permisos y restricciones específicas para el acceso a los datos, mediante la definición de roles y filtros literales. La correcta implementación de estas políticas asegura que solo los usuarios autorizados puedan acceder a los datos, bajo condiciones predefinidas.

Sintaxis:

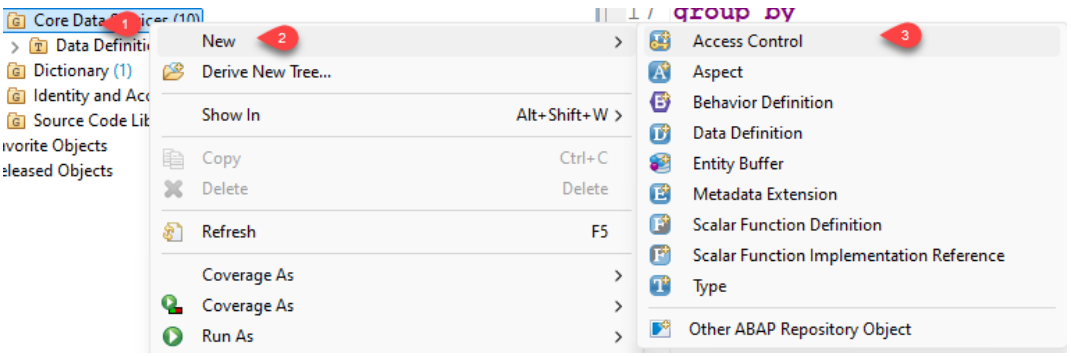
```
@AccessControl.authorizationCheck: #control_name
```

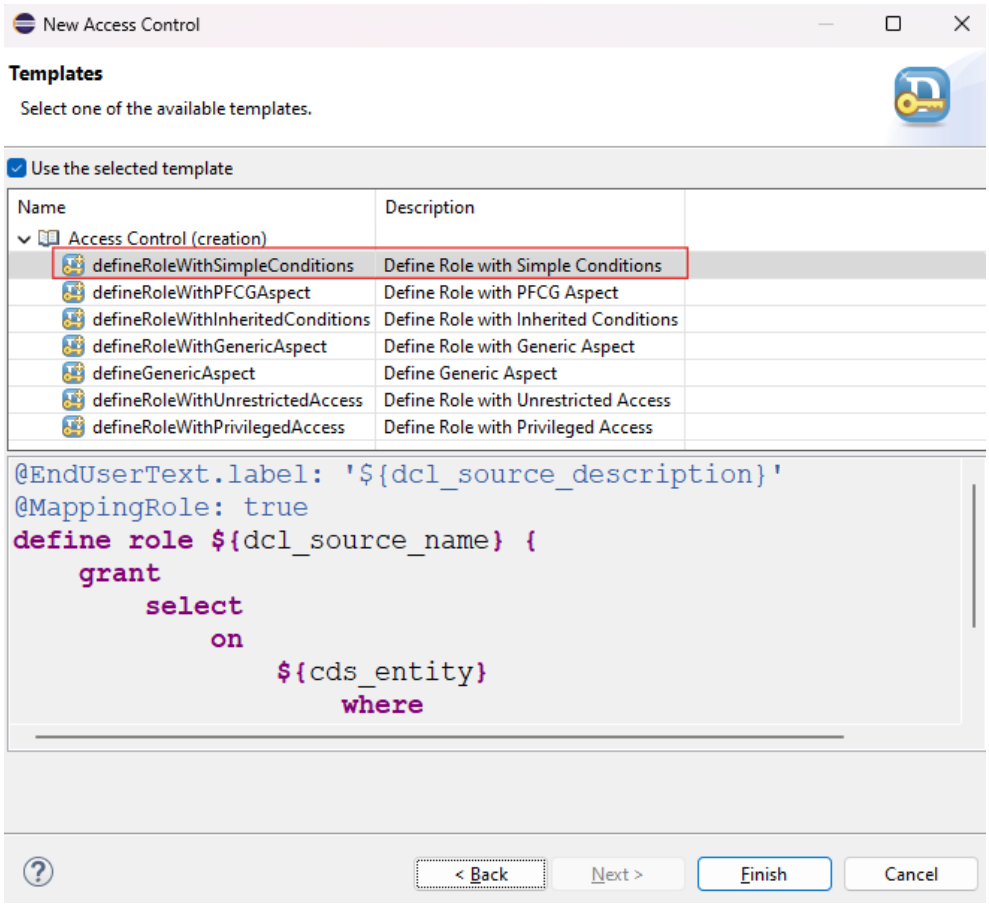
Esta anotación se agrega por defecto en la vista CDS al seleccionar la plantilla **defineViewEntity** con el valor por defecto **#NOT_REQUIRED.**

Tipos de Control de Acceso:

Existen dos tipos principales de control de acceso:

- **#NOT_REQUIRED (No Requerido):** Este tipo de control implica que no se verifican activamente las condiciones antes de permitir el acceso a los datos, proporcionando un acceso más abierto y sin restricciones.
- **#CHECK (Chequeo):** Este tipo de control verifica activamente que se cumplen las condiciones de acceso antes de permitir el acceso a los datos. Al colocar este tipo de acceso es necesario crear un control de acceso (Access control) donde se establezcan las condiciones de acceso. El control de acceso (access control), se crea de la siguiente manera: se realiza a través de la carpeta de proyecto con **New** o la carpeta **Core Data Service,** luego seleccionar **Access Control** y seleccionar la plantilla **defineRoleWithSimpleConditions** que se encuentra en la carpeta **Access Control (creation).**





Sintaxis:

```
@EndUserText.label: 'Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
            where entity_component1 = 'literal_value';
}
```

Mediante el rol o condiciones de acceso se pueden controlar los datos que las entidades CDS devuelven mediante la sentencia **where**

y es posible agregar más condiciones o filtros con las instrucciones **and** y **or** dependiendo de lo requerido. El acceso a los datos se filtra mediante un lenguaje específico llamado **Data Control Language (DCL)**, y no debe confundirse con otros tipos de filtros como los filtros SQL.

6.2. Otorgamiento múltiple

El control de acceso múltiple es una estrategia utilizada en la gestión y consulta de datos que permite definir y aplicar reglas específicas para regular el acceso a diversas entidades de datos. Este enfoque se basa en la definición de filtros literales y el uso de modelos de datos que aceleran el proceso de autorización y control semántico. A través de múltiples consultas (**grant select on**) y controles de acceso, es posible aplicar condiciones específicas a distintos conjuntos de datos, garantizando que solo los registros que cumplan con estas condiciones sean accesibles. La implementación ordenada y coherente de estos controles facilita el mantenimiento y la gestión de datos, permitiendo una integración efectiva de múltiples fuentes de datos y escenarios de filtrado.

Puntos Importantes a considerar:

- Se puede realizar una query específica para filtrar registros según condiciones predefinidas.
- Es posible crear múltiples controles de acceso que pueden aplicar diferentes condiciones a una misma entidad.
- Es recomendable trabajar para un único CDS tener múltiples **grant selects on** y no tener múltiples **access controls** utilizando a la misma CDS. Aunque es posible crearlos solo que al tener varios aplicarían los resultados con los accesos más permisivos.

Sintaxis:

```
@EndUserText.label: 'Access Control Test'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
            where entity1_component1 = 'literal_value';
  grant select on cds_entity_name_2
```

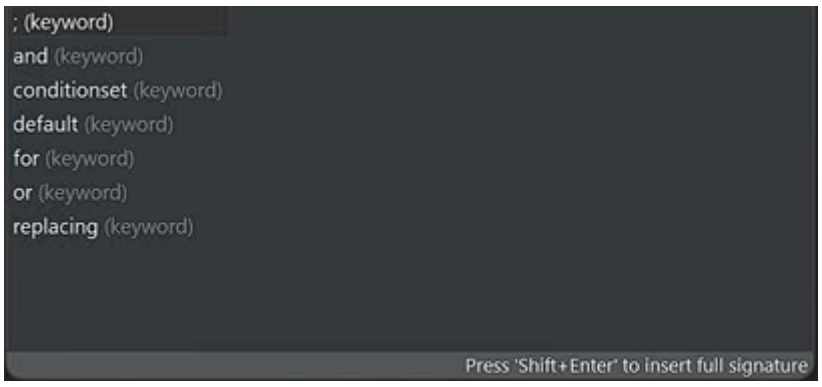
```
        where entity2_component1 = 'literal_value';
}
```

6.3. Herencia

Mediante la aplicación de herencia, es posible reutilizar y extender reglas y restricciones existentes para nuevas entidades de datos. Esto facilita la administración y actualización de las políticas de acceso, asegurando que los datos sensibles estén protegidos y solo sean accesibles por usuarios autorizados. La herencia permite definir condiciones específicas para distintas entidades o controles de acceso, optimizando así la gestión de consultas y mantenimiento del sistema de datos.

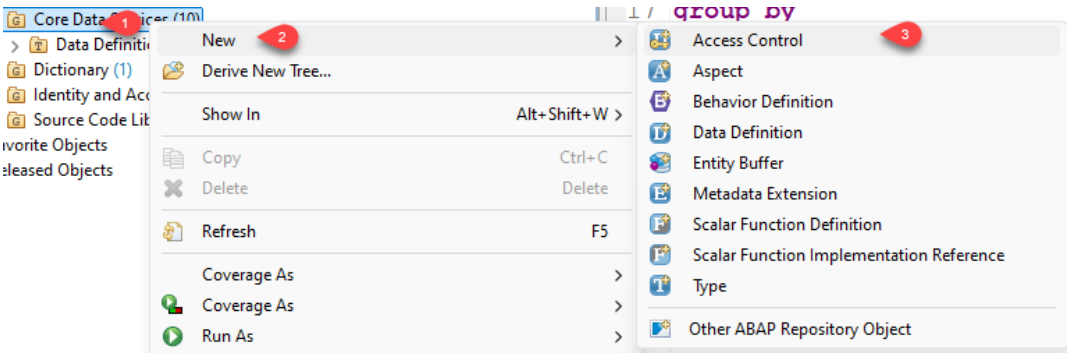
Puntos Importantes a considerar:

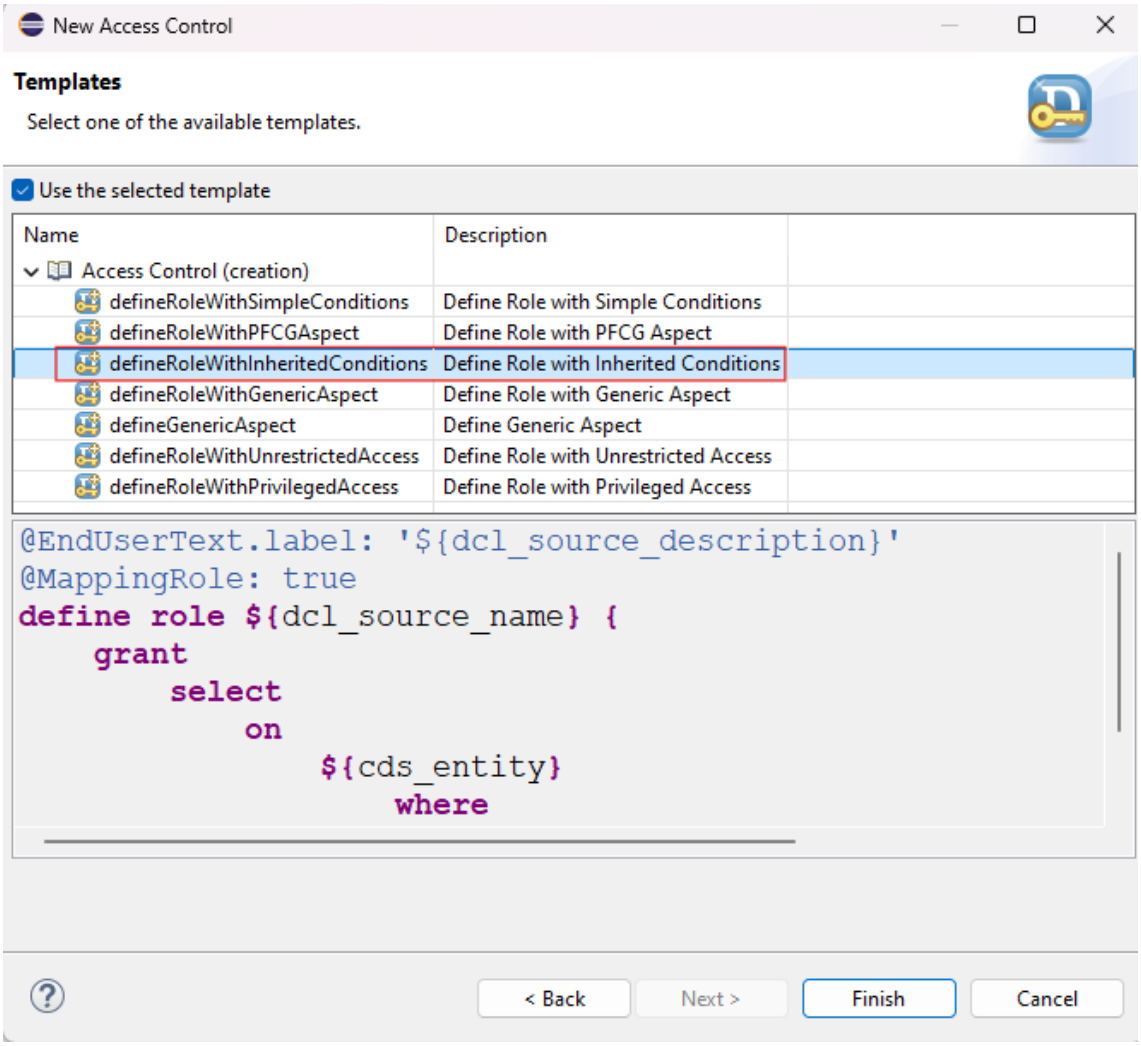
- La entidad CDS con el control de acceso que establezca la herencia de otra CDS hereda las restricciones del control de acceso de dicha entidad CDS. Si esta última tiene un control de acceso creado con anterioridad.
- Es posible modificar o ampliar las restricciones del control de acceso heredadas a través de los operadores **and, or, default, entre otros**. A continuación se muestra una lista de los operandos permitidos:



- Se pueden agregar condiciones adicionales a las entidades heredadas para aplicar filtros más específicos. A través de la instrucción **where** antes de la instrucción **inheriting conditions from entity**.

El control de acceso (access control) heredado, se crea de la siguiente manera: se realiza a través de la carpeta de proyecto con **New** o la carpeta **Core Data Service,** luego seleccionar **Access Control** y seleccionar la plantilla **defineRoleWithInheritedConditions** que se encuentra en la carpeta **Access Control (creation).**





Sintaxis:

```
@EndUserText.label: 'Inherited Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
inheriting conditions from entity cds_name_with_access_control
and/or  inherited_entity_component = 'literal_value';
}
```

Ejemplo agregando más condiciones de las heredadas:

```
@EndUserText.label: 'Inherited Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name_1
        where entity_component1 = 'literal_value' and
inheriting conditions from entity cds_name_2_with_access_control
and/or  inherited_entity_component = 'literal_value';
}
```

6.4. Autorización – Campo y Objeto

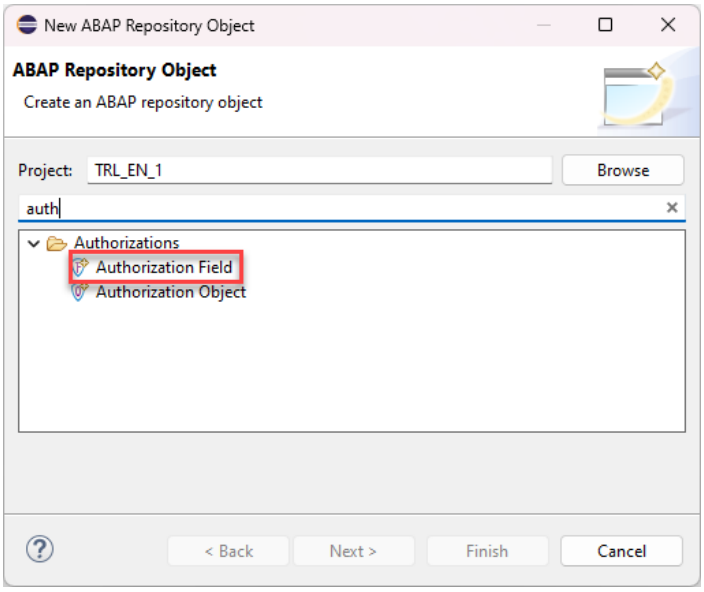
La autorización de campo y objeto en sistemas de datos es una técnica que permite controlar el acceso a la información mediante la creación y configuración de objetos de autorización. Estos objetos definen restricciones específicas para los datos, asegurando que solo los usuarios autorizados puedan ver o modificar la información. La vinculación dinámica de valores y la configuración basada en roles permiten una gestión flexible y segura de los permisos de acceso, facilitando la administración y mantenimiento de los controles de acceso en el sistema.

Campos de Autorización (Authorization Fields):

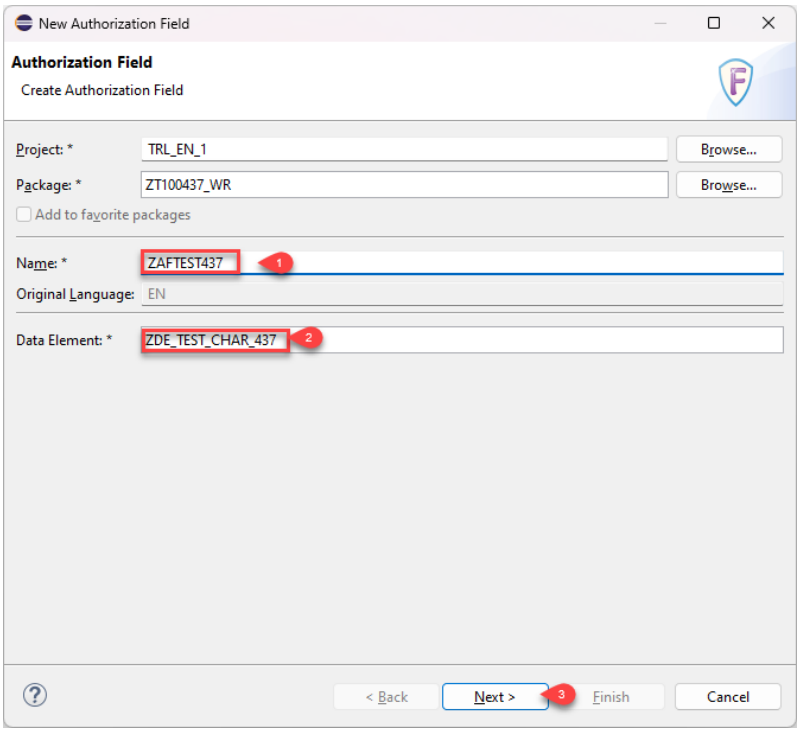
Los campos de autorización son componentes básicos utilizados dentro de los objetos de autorización. Estos campos representan atributos específicos sobre los cuales se pueden establecer restricciones de acceso. Por ejemplo, un campo de autorización podría ser el identificador de una compañía aérea (carrier ID) que se

utiliza para verificar si un usuario tiene permiso para acceder a los datos relacionados con esa compañía.

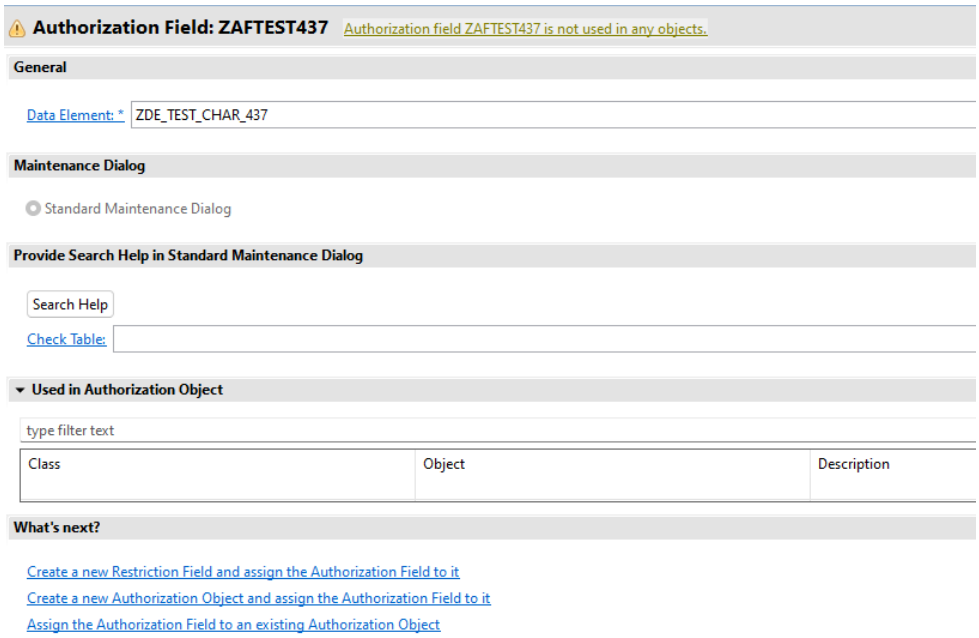
Para crear un campo de autorización se realiza a través de la carpeta de proyecto con **New** o la carpeta **Authorizations,** luego seleccionar **Authorization Field**.



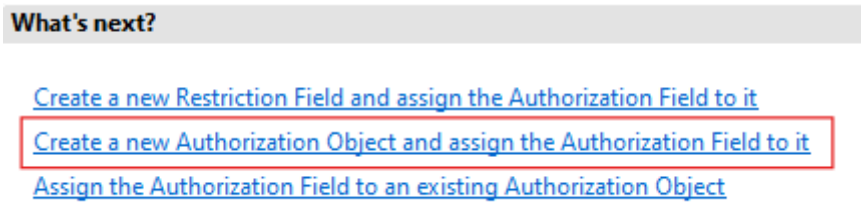
Se debe colocar un nombre para el campo de autorización no mayor de 10 caracteres y una descripción. Además es requerido de forma obligatoria colocar un elemento de datos.



Y de esta forma se ha creado exitosamente un campo de autorización.



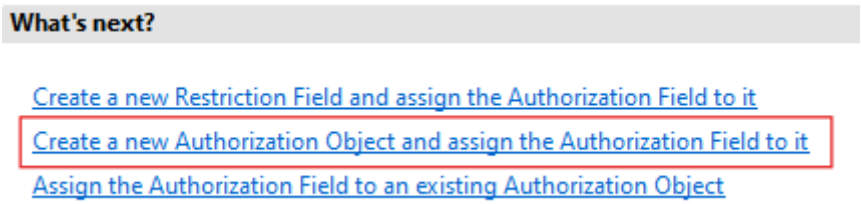
En la sección de **What 's Next** se puede asignar directamente el campo de autorización a un objeto de autorización creado anteriormente o crear uno nuevo.



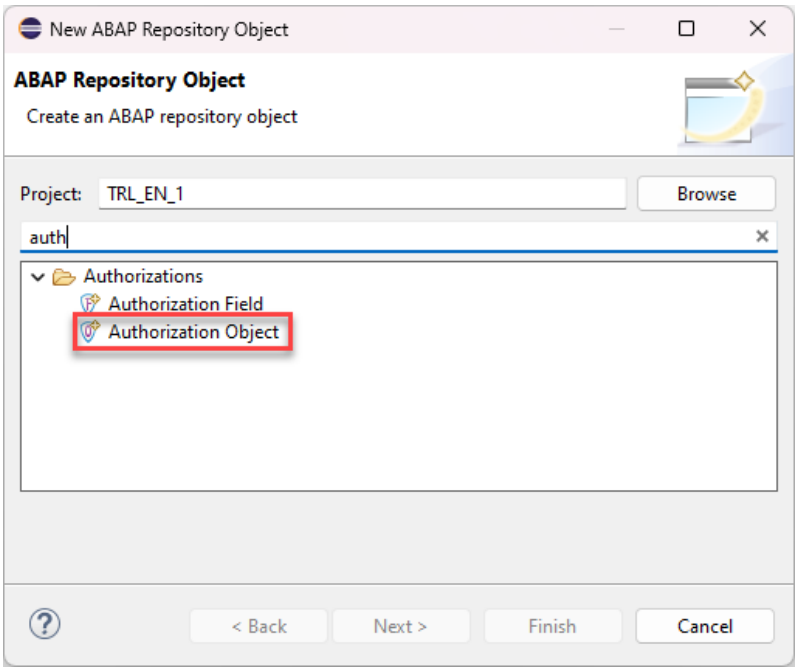
Objetos de Autorización (Authorization Objects):

Los objetos de autorización son conjuntos que agrupan uno o más campos de autorización. Estos objetos definen las reglas y restricciones que determinan el acceso a los datos. Un objeto de autorización contiene campos de autorización a elementos de datos, y define qué acciones (leer, escribir, modificar) puede realizar un usuario sobre los datos asociados. Los objetos de autorización permiten crear controles de acceso detallados y personalizados.

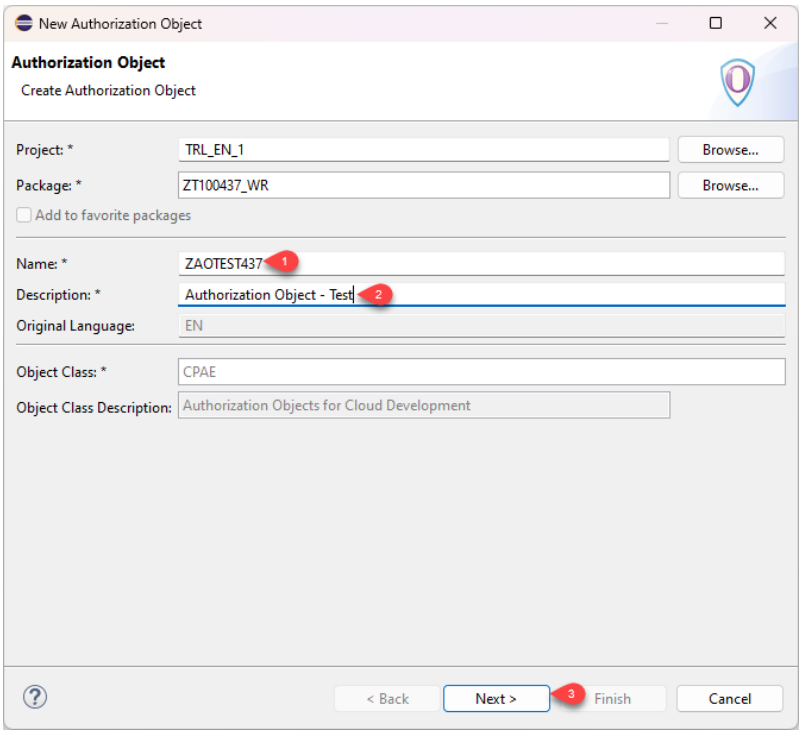
Se pueden crear a través del apartado **What's Next** dentro de los campos de autorización.



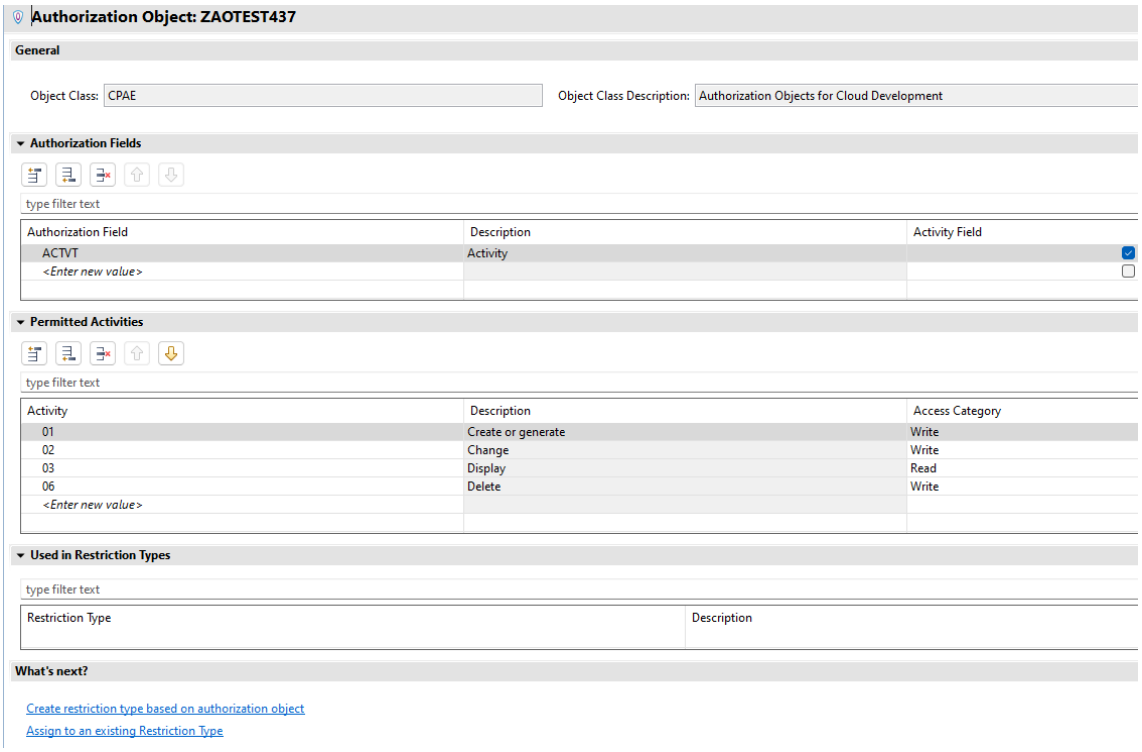
Ó a través de la carpeta de proyecto con **New** o la carpeta **Authorizations,** luego seleccionar **Authorization Object**.



De igual forma que los campos de autorización, se debe colocar un nombre para el objeto de autorización no mayor de 10 caracteres y una descripción.



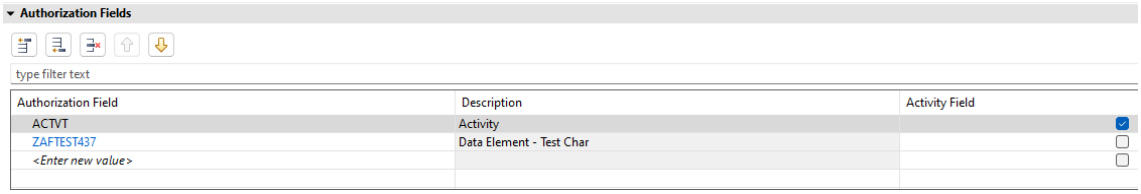
Y de esta forma se ha creado exitosamente un objeto de autorización.



Secciones del objeto de autorización:

Entre las secciones dentro el objeto de autorización que veremos en este apartado tenemos:

- **Campos de Autorización (Authorization Fields):** la cual permite asignar los campos de autorización previamente creados que sean necesarios y estos son los atributos específicos que forman parte de un objeto de autorización. Cada campo de autorización representa un aspecto particular sobre el cual se aplicarán las restricciones de acceso. Estos campos definen los criterios específicos que deben cumplirse para que se permita o deniegue el acceso a los datos.

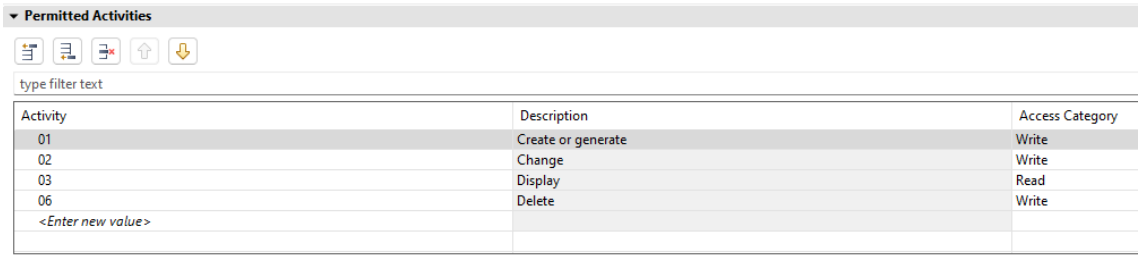


- **Actividades Permitidas (Permitted Activities):** son las acciones específicas que los usuarios pueden realizar sobre los datos protegidos por el objeto de autorización. Estas actividades definen qué operaciones están permitidas (o no) para un usuario sobre un conjunto de datos determinado.

  Las actividades que se crean por defecto son:

  - **Create or generate (Crear):** Permite al usuario agregar nuevos registros o datos.
  - **Change (Modificar):** Permite al usuario modificar los datos existentes.
  - **Display (Mostrar):** Permite al usuario ver los datos sin modificarlos.
  - **Delete (Eliminar):** Permite al usuario borrar datos.

  En el contexto de un objeto de autorización, las actividades permitidas se configuran de acuerdo con las necesidades de seguridad y operacionales de la organización. Por ejemplo, un objeto de autorización para datos de empleados podría permitir a los gerentes leer y actualizar la información de sus subordinados, pero no eliminar registros.



Objetos de Autorización Estándar:

Los objetos de autorización estándar son aquellos predefinidos dentro del sistema y que están disponibles para ser utilizados en la configuración de permisos. Estos objetos suelen cubrir escenarios comunes y proporcionar una base sólida para la gestión de acceso sin necesidad de crear nuevos objetos desde cero. Sin embargo, en algunas situaciones, puede ser necesario crear objetos de autorización personalizados para cumplir con requisitos específicos de seguridad y acceso.

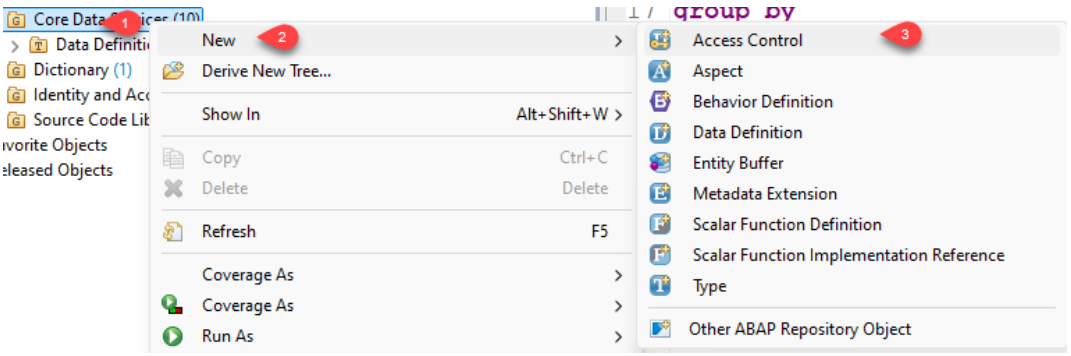
Puntos Importantes a considerar:

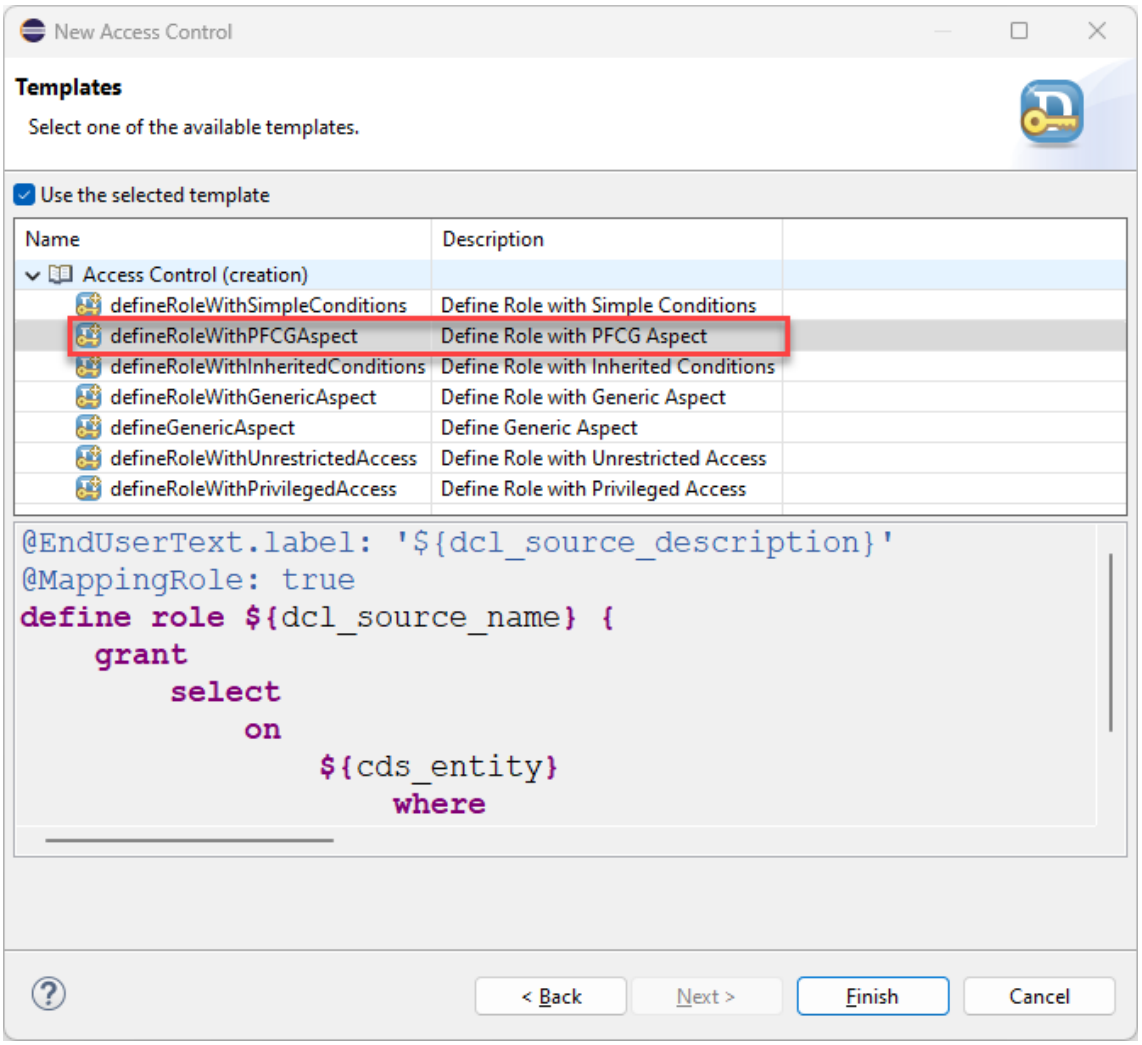
- **El equipo Basis en un entorno SAP:** por lo general se encarga de la administración técnica y el mantenimiento del sistema. Uno de sus roles clave es la gestión de permisos y roles de usuario, lo que incluye la configuración de objetos de autorización y la implementación de controles de acceso. El equipo Basis asegura que las políticas de seguridad estén correctamente aplicadas y que los usuarios tengan los permisos adecuados según sus roles y responsabilidades.
- **Hard Code:** Una de las ventajas de utilizar objetos de autorización y campos de autorización es la posibilidad de evitar valores "hard code". En lugar de especificar valores fijos o literales en los controles de acceso. Los objetos de autorización permiten definir valores de manera dinámica y configurable. Esto significa que los permisos y restricciones pueden ajustarse fácilmente sin necesidad de modificar el código fuente. Los valores se pueden gestionar a través de roles y perfiles de usuario, lo que proporciona una mayor flexibilidad y seguridad en la administración del acceso a los datos.

6.5. Aspecto PFCG

El aspecto PFCG (Profile Generator) en sistemas de datos permite la gestión y asignación de permisos y roles a los usuarios mediante el uso de objetos de autorización. Estos objetos definen restricciones específicas para el acceso a los datos en las entidades CDS (Core Data Services). La vinculación de campos de autorización y actividades permitidas asegura que solo los usuarios autorizados puedan realizar ciertas acciones sobre los datos. El equipo Basis es responsable de la administración y configuración de estos permisos, garantizando la seguridad y protección de los datos. La flexibilidad de los objetos de autorización permite ajustar los valores de manera dinámica, evitando la necesidad de valores hardcodeados y facilitando el mantenimiento y la modularización de los controles de acceso.

El control de acceso PFCG, se crea de la siguiente manera: se realiza a través de la carpeta de proyecto con **New** o la carpeta **Core Data Service,** luego seleccionar **Access Control** y seleccionar la plantilla **defineRoleWithPFCGAspect** que se encuentra en la carpeta **Access Control (creation).**





Sintaxis:

```
@EndUserText.label: 'Access Control - Test PFCG'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
  where (entity_component_1, entity_coponent_2) = aspect pfcg_auth(authorization_object, authorization_field_1, authorization_field_2, filter_field_1 = 'filter_value_1') and/or entity_component1 = 'literal_value';
}
```

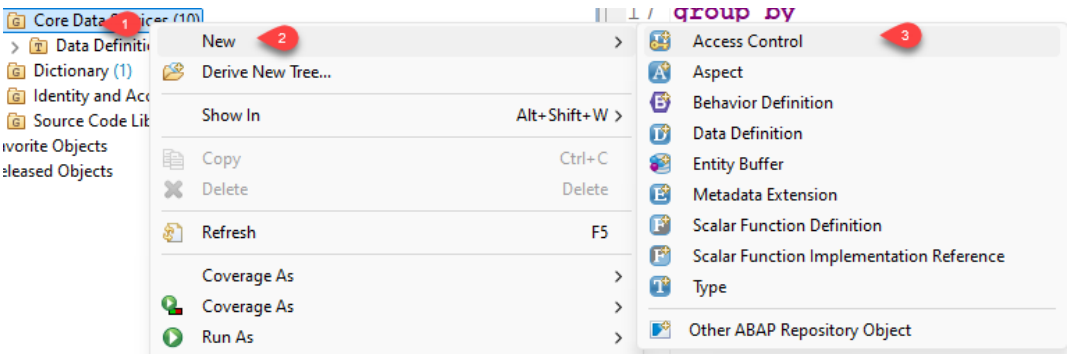
Es importante mencionar que se pueden especificar varios componentes de una entidad o vista CDS en el filtro y asociarlos a través de la instrucción aspect **pfcg_auth()** con un objeto de autorización, que esté a su vez tenga campos de autorización asociados a los elementos de datos de los componentes

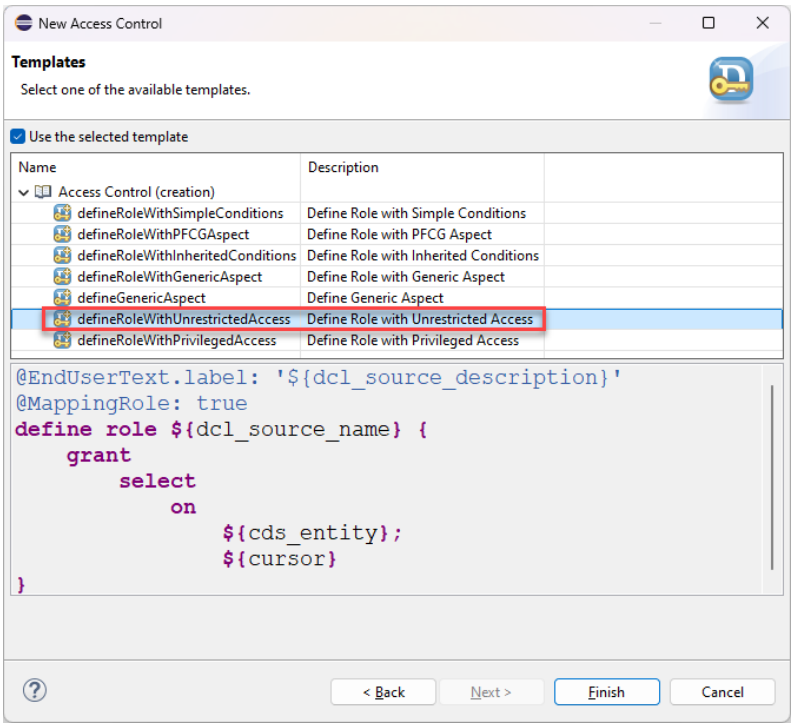
especificados. Además de colocar la actividad permitida que tendrán todos seguidos de coma donde el orden sería objeto de autorización, los diferentes campos de autorización, y la actividad con el valor literal de la actividad que se podrá realizar al utilizar la vista CDS que se haya configurado previamente en el objeto de autorización.

6.6. Full Access

"Full Access" en sistemas de datos se refiere a una situación donde no existen restricciones sobre el acceso a los datos. Este comportamiento predeterminado ocurre cuando una entidad CDS está configurada para aplicar restricciones pero no tiene ningún control de acceso creado, o cuando se crea un control de acceso sin ninguna restricción. Esto resulta en acceso total a los datos, eliminando cualquier otra condición o restricción previamente aplicada. Para gestionar adecuadamente el acceso y proteger la seguridad de los datos, es crucial definir y aplicar controles de acceso específicos.

El control de acceso Full Access, se crea de la siguiente manera: se realiza a través de la carpeta de proyecto con **New** o la carpeta **Core Data Service,** luego seleccionar **Access Control** y seleccionar la plantilla **defineRoleWithUnrestrictedAccess** que se encuentra en la carpeta **Access Control (creation).**





Sintaxis:

```
@EndUserText.label: 'Full Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name;
}
```

Un control de acceso con la condición menos restrictiva se define como "full access" porque no establece limitaciones sobre el acceso a los datos, permitiendo un acceso completo y abierto. Esto se alinea con el comportamiento predeterminado del sistema y facilita la gestión de permisos de manera eficiente y flexible.

Puntos importantes a considerar:

- Crear un nuevo control de acceso sin ninguna restricción puede eliminar todas las restricciones aplicadas por otros controles de acceso existentes. Esto es útil en situaciones donde se necesita revertir restricciones aplicadas anteriormente sin modificar o eliminar los controles de acceso existentes.

- Cuando una entidad CDS se activa con el valor de control "check" pero no tiene ningún control de acceso creado, el sistema permite un "full access" por defecto.
- Este comportamiento se manifiesta como acceso total a los datos sin restricciones, lo que se conoce como "full action".
- Para evitar el "full access", es necesario crear controles de acceso que definan restricciones específicas sobre los datos.
- El "full access" puede representar un riesgo de seguridad si no se gestiona adecuadamente, ya que permite acceso sin restricciones a los datos.

Mejores Prácticas:

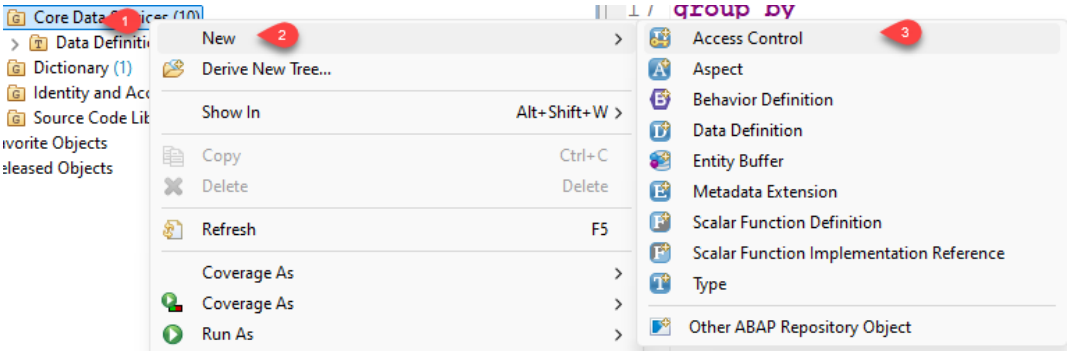
- Es posible tener múltiples controles de acceso para la misma entidad, aunque no es recomendable. Lo ideal es utilizar un único control de acceso por entidad para evitar conflictos y simplificar la gestión. Utilizar un único control de acceso por entidad para simplificar la gestión y evitar conflictos.
- Definir condiciones claras y específicas en los controles de acceso para asegurar una adecuada protección de los datos.
- Realizar pruebas y validaciones regulares para asegurar que los controles de acceso funcionen según lo esperado.

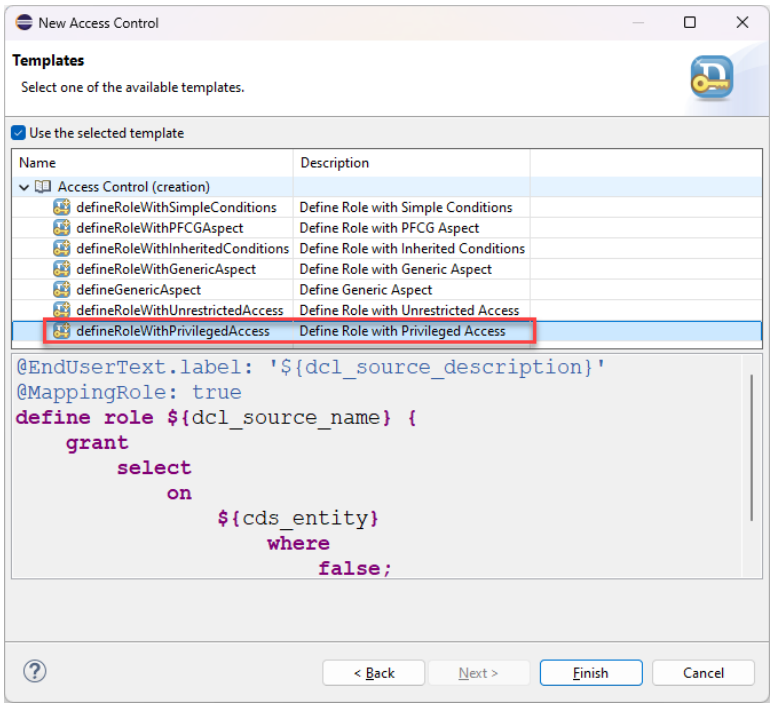
6.7. Impedir Acceso

"Impedir Acceso" en sistemas de datos se refiere a la aplicación de restricciones totales que evitan que cualquier usuario pueda acceder a los datos. Esto se logra mediante la configuración de controles de acceso con condiciones que siempre evalúan como falsas. A diferencia del "full access", que permite un acceso sin restricciones, "impedir acceso" asegura que ningún registro de datos sea accesible, proporcionando una protección completa de la información sensible o confidencial.

Para crear un control de acceso restrictivo, se crea de la siguiente manera: se realiza a través de la carpeta de proyecto con **New** o la carpeta **Core Data Service,** luego seleccionar **Access Control** y seleccionar la plantilla utilizada para el tipo de acceso privilegiado

defineRoleWithPrivilegedAccess que se encuentra en la carpeta **Access Control (creation).**





Sintaxis:

Una opción sería, colocar una condición en un campo clave no nulo como vacío. De tal forma que impida el acceso a los datos por el filtro, ya que no sería posible devolver algún valor con dicha condición.

```
@EndUserText.label: 'Restricted Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
            where entity_component1 = '';
}
```

La otra forma sería colocar después de la instrucción **where** el valor booleano false para que la evaluación de la condición después del **where** siempre sea falsa y ya que no sería posible devolver algún valor con dicha condición.

```
@EndUserText.label: 'Restricted Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
            where false;
}
```

Impedir un control de acceso sólo es posible si la entidad o vista CDS no tiene asociado ningún otro control de acceso con una condición menos restrictiva o un control de acceso de "acceso total" (full access).

6.8. Acceso Privilegiado

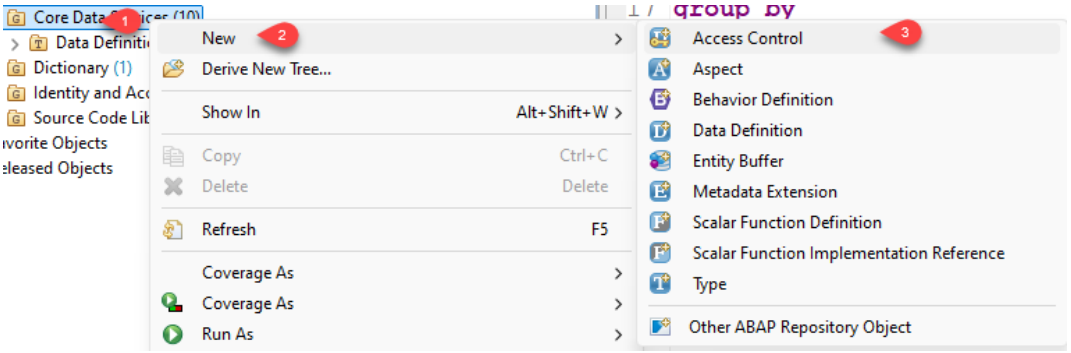
El "acceso privilegiado" en sistemas de datos se refiere a la capacidad de permitir a ciertos usuarios autorizados acceder a información sensible o protegida que normalmente estaría restringida para otros usuarios. Esto se logra mediante la configuración de controles de acceso específicos y la ejecución de consultas en un contexto de privilegios elevados, utilizando la anotación **#PRIVILEGED_ONLY** en la entidad CDS. Este tipo de acceso es esencial para proteger datos críticos y garantizar que solo los usuarios con permisos especiales puedan acceder a ellos, saltándose las restricciones normales aplicadas por los controles de acceso

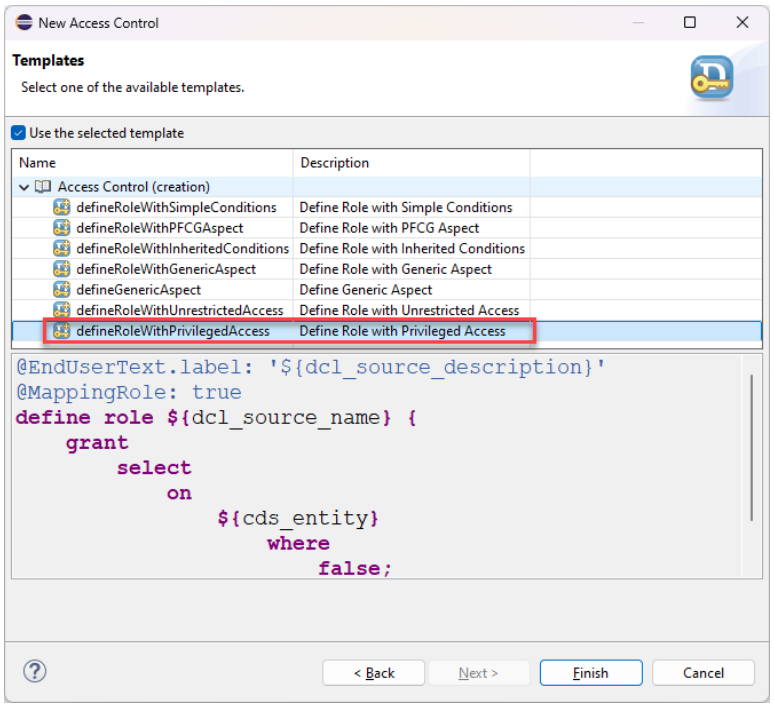
Anotación dentro de la entidad o vista CDS:

```
@AccessControl.authorizationCheck: #PRIVILEGED_ONLY
```

Para crear un control de acceso privilegiado, se crea de la misma manera que se realiza para impedir un acceso: se realiza a través de la carpeta de proyecto con **New** o la carpeta **Core Data Service,** luego seleccionar **Access Control** y seleccionar la plantilla utilizada para el

tipo de acceso privilegiado **defineRoleWithPrivilegedAccess** que se encuentra en la carpeta **Access Control (creation).**





Sintaxis:

La declaración es igual a la que se utiliza para impedir el acceso total de una tabla.

```
@EndUserText.label: 'Restricted Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
            where false;
}
```

La diferencia es que además que se pueden colocar otras condiciones con valores literales después de la instrucción **where.**

```
@EndUserText.label: 'Restricted Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
            where entity_component1 = 'literal_value';
}
```

Por medio de la instrucción **with privileged access** dentro de las consultas **select** dentro de código abap se puede dar el acceso total a las entidades CDS.

Ejemplo dentro de una clase ABAP:

```
CLASS class_name DEFINITION
 PUBLIC
 FINAL
 CREATE PUBLIC .
 PUBLIC SECTION.
  INTERFACES if_oo_adt_classrun.
 PROTECTED SECTION.
 PRIVATE SECTION.
ENDCLASS.
CLASS class_name IMPLEMENTATION.
 METHOD if_oo_adt_classrun~main.
  IF sy-uname EQ 'ADMIN'.
   SELECT FROM cds_entity_name WITH PRIVILEGED ACCESS
    FIELDS *
     INTO TABLE @DATA(lt_results)
     UP TO 1 ROWS.
   IF sy-subrc EQ 0.
    out->write( lt_results ).
   ENDIF.
  ELSE.
   out->write( 'No data' ).
  ENDIF.
 ENDMETHOD.
ENDCLASS.
```

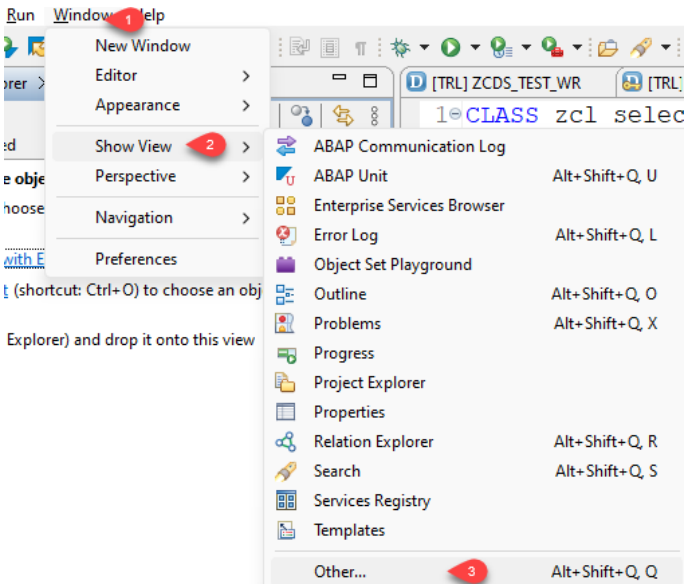
Casos de Uso Empresariales:

- El acceso privilegiado es útil en situaciones empresariales donde se necesita proteger información crítica, como nóminas de empleados o datos de contratos sensibles.
- Permite que usuarios con roles especiales puedan ver o modificar datos que están restringidos para otros usuarios

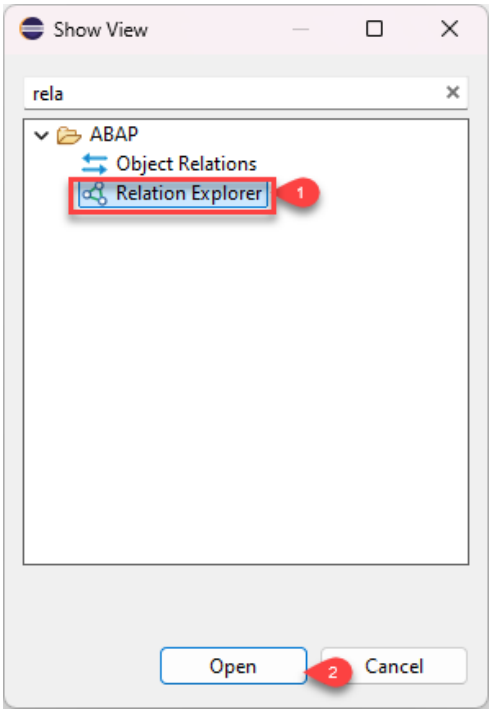
6.9. Explorador de relaciones

El "Explorador de Relaciones" es una herramienta de desarrollo integrada en Eclipse con ADT (ABAP Development Tools) que permite a los desarrolladores visualizar y analizar las relaciones entre las entidades CDS (Core Data Services) y otros objetos de datos. Proporciona una visión clara de cómo están interconectados los diferentes objetos, lo cual es esencial para comprender la estructura y el flujo de datos en un proyecto empresarial. Esta herramienta facilita la identificación de dependencias y relaciones, mejorando la eficiencia en la investigación y el análisis durante el desarrollo de sistemas complejos.

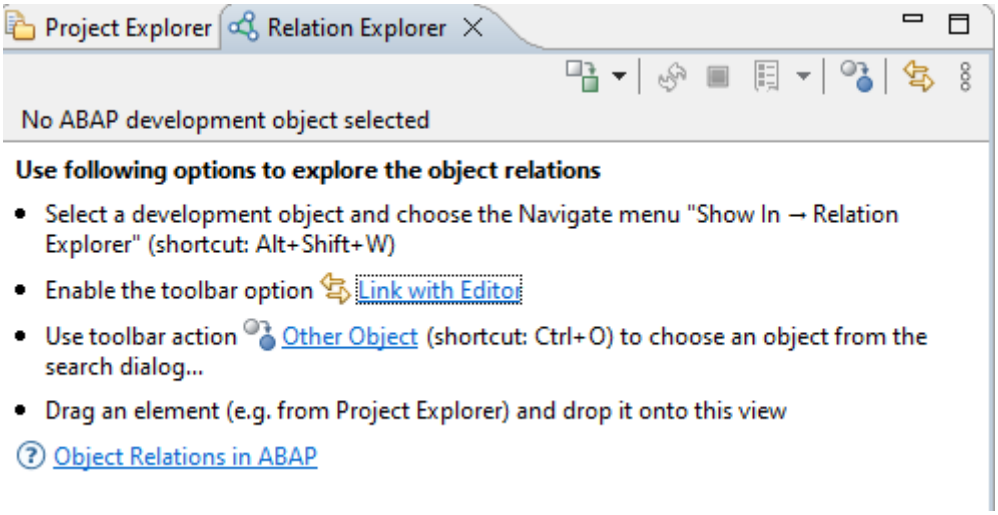
Para explorar las relaciones de una entidad CDS por primera vez es necesario mostrar la vista **Relation Explorer**, se utiliza la opción **Windows > Show View > Other.**



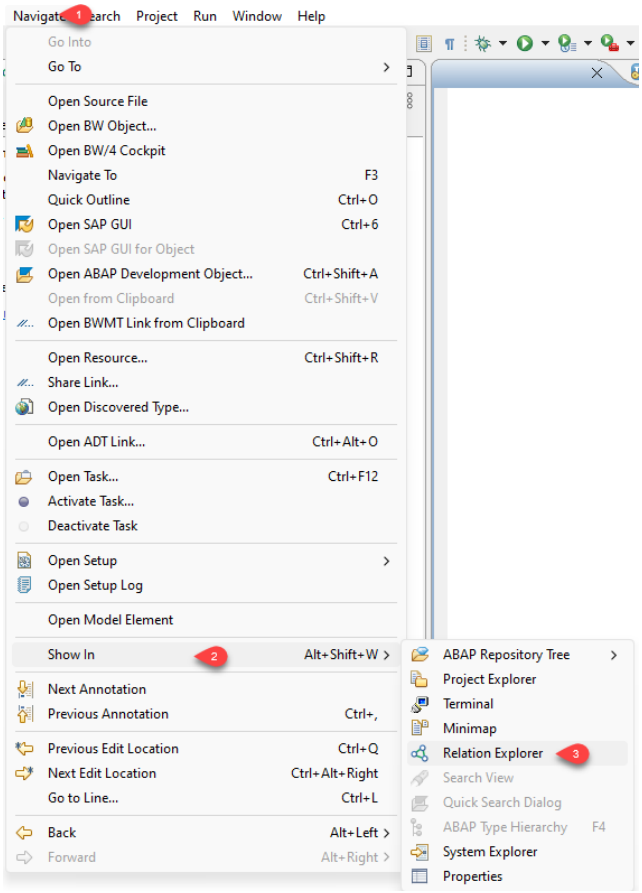
Luego ubicar la Carpeta ABAP o en el campo de búsqueda Colocar relation explorer.



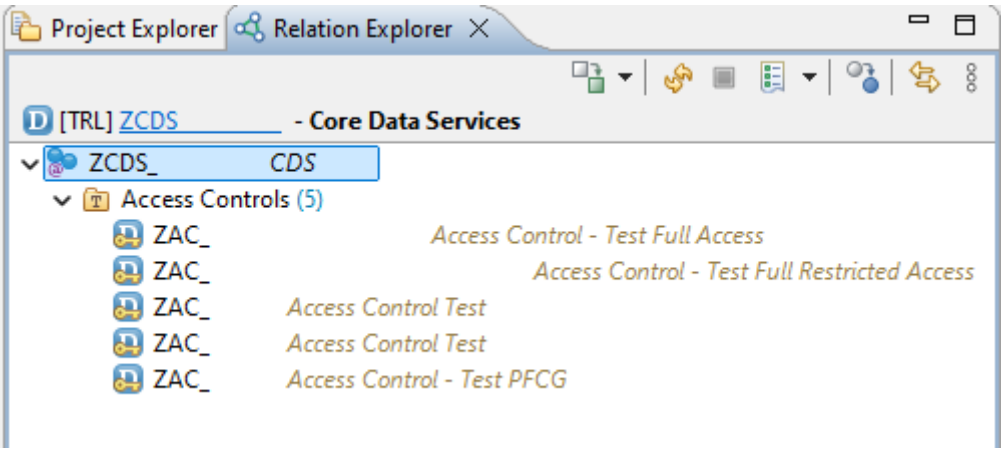
Después al abrir cualquier vista CDS posicionarse en la pestaña Relation Explorer.



Para explorar las relaciones, se utiliza la opción **Navigate > Show In > Relation Explorer.**



Esto carga las dependencias y relaciones de la entidad seleccionada, mostrando cómo está relacionada con otros objetos en el sistema.



6.10. Condiciones Literales Complejas

Son reglas avanzadas que permiten definir criterios específicos para restringir el acceso a datos en entidades CDS (Core Data Services). Utilizando una variedad de operadores lógicos y comparaciones,

estas condiciones proporcionan una flexibilidad significativa en la protección de datos. Al aplicar estos filtros, se puede asegurar que solo los usuarios autorizados tengan acceso a la información necesaria, permitiendo un control granular y preciso del acceso a los datos.}

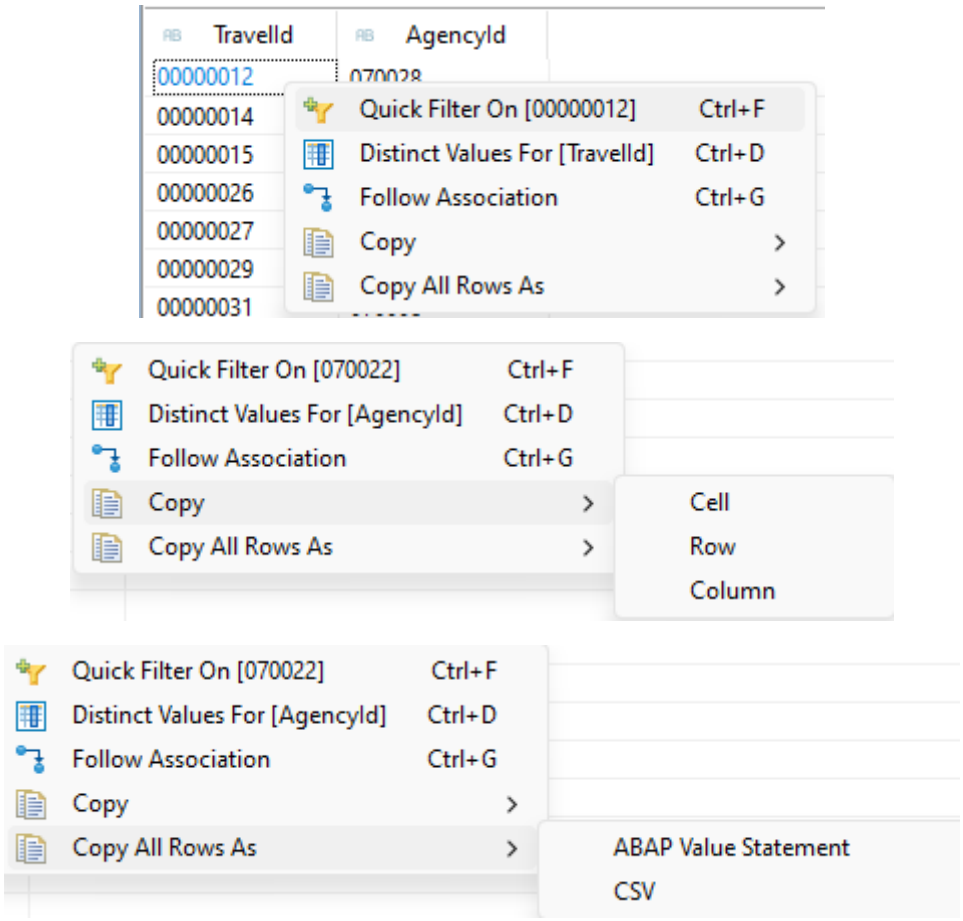
Operadores Lógicos:

Operador	Descripción
=	Igual a
!=	Diferente de
>	Mayor que
<	Menor que
>=	Mayor o igual que
<=	Menor o igual que
AND	Y lógico (combina condiciones y ambas deben ser verdaderas)
OR	O lógico (combina condiciones y al menos una debe ser verdadera)
NOT	Negación lógica (invierte el resultado de una condición)

Operadores Especiales:

Operador	Descripción
BETWEEN	Entre un rango de valores
NOT BETWEEN	Fuera de un rango de valores
LIKE '%pattern%'	Busca patrones específicos
IS NULL	Es nulo (sin valor)
IS NOT NULL	No es nulo (tiene valor)
?=	Igual a y considera valores iniciales
NOT INITIAL	Excluye valores iniciales

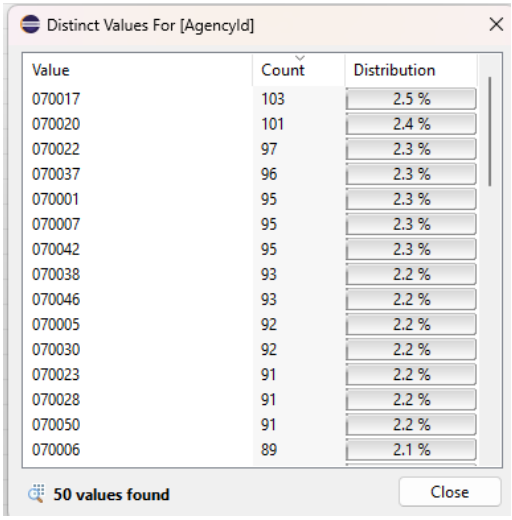
Al hacer clic derecho en alguno de los registros dentro de la tabla hay algunas opciones interesantes que se pueden seleccionar dentro de la herramienta **Data Preview.**



Las cuales son las siguientes:

Opción	Descripción
Quick Filter On	Aplica filtros rápidos y específicos a los datos devueltos en una tabla o vista CDS.
Distinct Values For	Muestra una lista de todos los valores únicos en una columna específica. Con un porcentaje de repetición dentro de la columna o componente seleccionado.
Follow Association	Navega a entidades relacionadas según las asociaciones definidas en el modelo de datos.
Copy Cell, Copy Row, Copy Column	Copia el contenido de una celda, fila o columna específica al portapapeles.
Copy All Rows As	Copia todas las filas de la tabla en formatos como declaración de valor ABAP o archivo CSV.

Ejemplo de la opción Distinct Values For:



6.11. Acceso Obligatorio

Es una medida de seguridad que impone la verificación de autorización mediante un Access control antes de permitir consultas sobre los datos. Esto significa que las consultas solo se pueden ejecutar si existe una vinculación con un objeto de tipo Access control. Si no se dispone de este objeto, cualquier intento de consulta resultará en un error, asegurando así que solo los usuarios autorizados puedan acceder a la información. Esta práctica garantiza un control riguroso sobre el acceso a los datos y protege la confidencialidad de la información.

Sintaxis:

Es importante para establecer un acceso obligatorio en una entidad o vista CDS colocar en la anotación del access control el valor **#MANDATORY.** De esta forma se asegura que las consultas solo se ejecuten si existe un control de acceso previamente creado.

Si no se dispone de este objeto de control, cualquier intento de invocar una consulta resultará en un error, impidiendo el acceso a los datos.

@AccessControl.authorizationCheck: #MANDATORY

Beneficios de la Verificación de Autorización Obligatoria:

- Aumenta la seguridad y control sobre el acceso a los datos.
- Garantiza que solo usuarios con la debida autorización puedan ejecutar consultas sobre la entidad.
- Permite definir reglas precisas y detalladas para el acceso a la información.