LOGALI

Teoría

Políticas de Acceso Personalizadas

ABAP Cloud – Modelado con CDS

Contenido

7. Políticas de Acceso Personalizadas

7.1. Escenario empresarial

El Access Control en SAP es un sistema integral que permite definir, aplicar y gestionar políticas de seguridad para controlar el acceso a datos sensibles dentro de un entorno empresarial. Este sistema utiliza definiciones de Core Data Services (CDS) y aspectos personalizados para garantizar que solo los usuarios autorizados puedan acceder a información específica basada en sus roles y necesidades. Las políticas de Access Control pueden incluir condiciones detalladas y reglas específicas que se ajustan a los requisitos operacionales y de seguridad de la organización, proporcionando un control granular y efectivo sobre los datos sensibles. Además, permite la creación de tablas de persistencia para almacenar datos transaccionales y de usuarios, y utiliza roles y aspectos personalizados para filtrar y gestionar el acceso de manera segura y precisa.

Uso de Aspectos Personalizados:

- Se pueden definir aspectos personalizados para aplicar condiciones adicionales, como filtrar por departamento, tipo de transacción o el usuario que puede acceder a los datos.

```
@EndUserText.label: 'Access Control'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
            where CREATED_BY = 'user1';
}
```

El usuario debe se puede obtener dentro de un código abap a través de la clase **cl_abap_context_info=>get_user_technical_name( ),** para ser guardada dentro de tablas de base de datos y ser consultadas a través de entidades o vistas CDS. Y por último colocarles un control de acceso con los filtros requeridos.

7.2. Access Control – Auditoría

El Access Control en SAP es un sistema que permite definir, aplicar y gestionar políticas de seguridad para controlar el acceso a datos sensibles dentro de la organización. Estas políticas se especifican mediante Core Data Services (CDS) y pueden incluir aspectos personalizados para ajustarse a las necesidades específicas del negocio. La auditoría (auditing) complementa este sistema al proporcionar un marco para verificar y registrar las actividades de acceso y modificación de datos. En conjunto, el Access Control y la auditoría garantizan la seguridad, integridad y cumplimiento normativo de la información empresarial, permitiendo un control granular y preciso sobre quién accede a los datos y cómo lo hace.

Sintaxis:

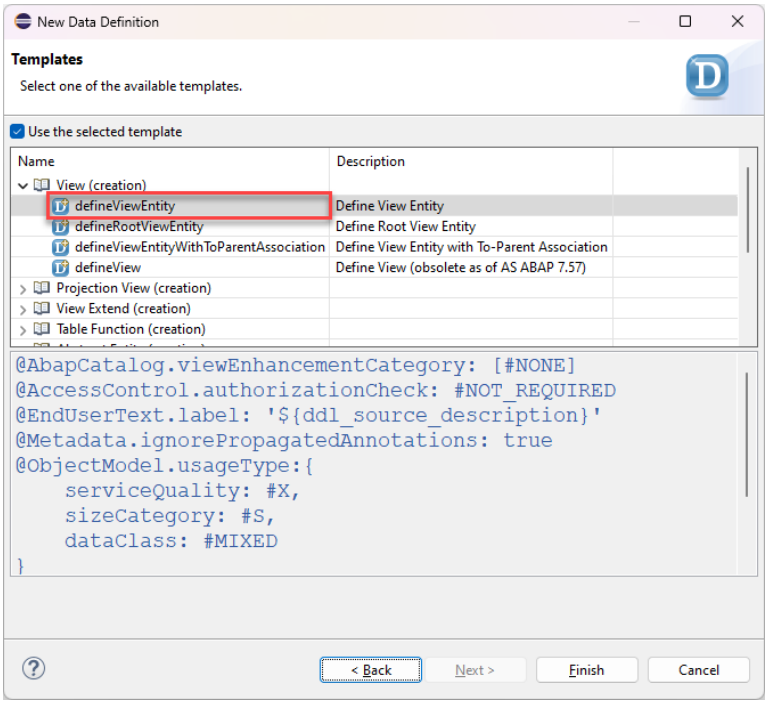
Se debe colocar dentro de las entidades CDS Luego de la anotación @AccessControl.authorizationCheck: #.

- @AccessControl.authorizationCheck: #CHECK
- @AccessControl.auditing.type: #CUSTOM
- @AccessControl.auditing.specification: 'any_word'

Aunque como cualquier anotación del mismo tipo agruparlas con el uso de "**{}**" y separando cada anotación con una coma:

```
@AccessControl: {
        authorizationCheck: #CHECK,
        auditing.type: #CUSTOM,
        auditing.specification: 'any_word'
}
```

Recordando que para crear una entidad o vista CDS, se realiza a través de la carpeta de proyecto luego New en la opción **Other ABAP Repository Object** ubicar la carpeta **Core Data Services** y luego seleccionar **Data Definition** y seleccionar la plantilla **defineViewEntity** que se encuentra en la carpeta **View (creation).**



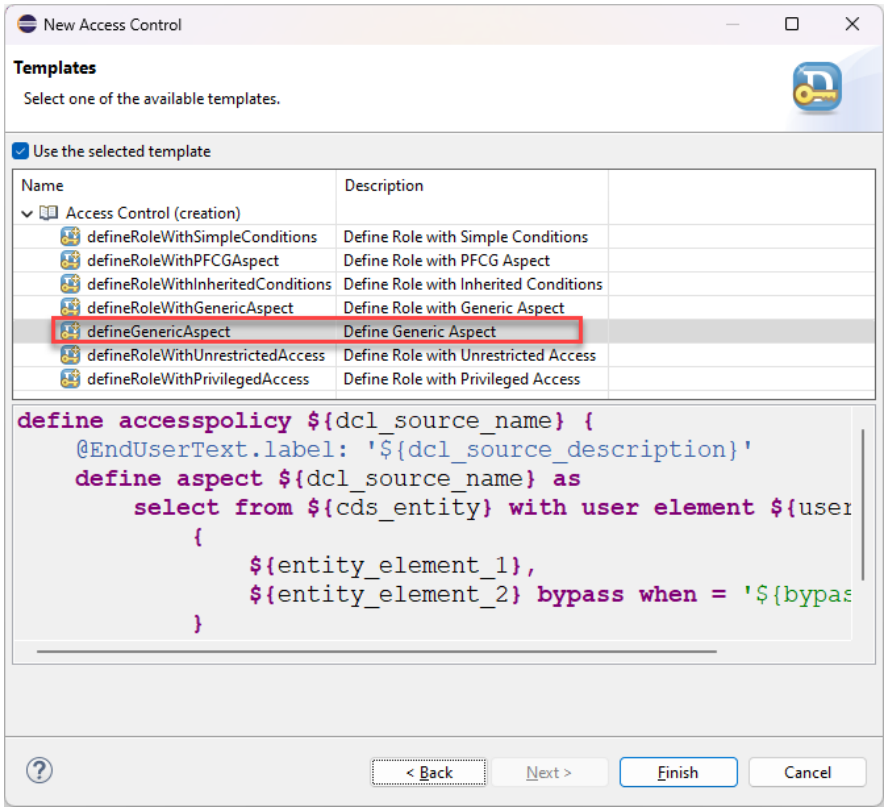
7.3. Política de Acceso – Aspecto Personalizado

Las políticas de acceso en SAP son un conjunto de reglas y directrices que determinan quién puede acceder a qué datos y bajo qué condiciones dentro del sistema SAP. Estas políticas se implementan a través de Core Data Services (CDS) y pueden personalizarse mediante aspectos específicos que se ajustan a las necesidades del negocio. Los aspectos personalizados permiten añadir condiciones y reglas adicionales no cubiertas por las políticas estándar, proporcionando un control más detallado y específico sobre los datos. La correcta definición e implementación de estas políticas son fundamentales para asegurar la seguridad e integridad de los datos empresariales, garantizando que solo los usuarios autorizados tengan acceso a información crítica.

La creación de un aspecto personalizado implica la definición de una entidad CDS y la especificación de sus propiedades de auditoría, como dentro de la anotación **@AccessControl: authorizationCheck: #CHECK**, **auditing.type: #CUSTOM** y **auditing.specification: 'any_word'**. Ya que al momento de activar la política de acceso requerirá dichas configuraciones previas en el **access control.**

La implementación de una política de acceso comienza con la creación de un nuevo control de acceso y se realiza a través de la carpeta de proyecto con clic derecho **New** o la carpeta **Core Data**

Service, luego seleccionar **Access Control** y seleccionar la plantilla **defineGenericAspect** que se encuentra en la carpeta **Access Control (creation).**



Sintaxis:

Es crucial que el nombre del aspecto coincida con el nombre de la política de acceso **access_policies_name** para evitar errores durante la implementación.

```
define accesspolicy access_policies_name {
  @EndUserText.label: 'Access Control - Access Policies'
  define aspect access_policies_name as
    select from cds_entity_name with user element user_element
      {
        entity_component,
        entity_componentN
      }

}
```

El componente o alias **user_element** en la entidad CDS se utiliza para identificar y permitir el acceso a los datos correspondientes a un usuario específico cuando se realiza una consulta. Es esencial que este componente del usuario haya sido previamente cargado en la base de datos para que pueda ser utilizado en las columnas pertinentes. De esta manera, la política de acceso puede devolver los elementos de la tabla que coincidan con el usuario seleccionado. Además, es necesario agregar al menos un componente de la entidad que devolverá los valores en la consulta **entity_component,** estos campos se conocen como **aspect fields** (campos de aspecto). Aunque es importante destacar que si se agrega más de un campo de aspecto en el caso de que se use la política de acceso en un aspecto personalizado, se deben separar los componentes con una coma.

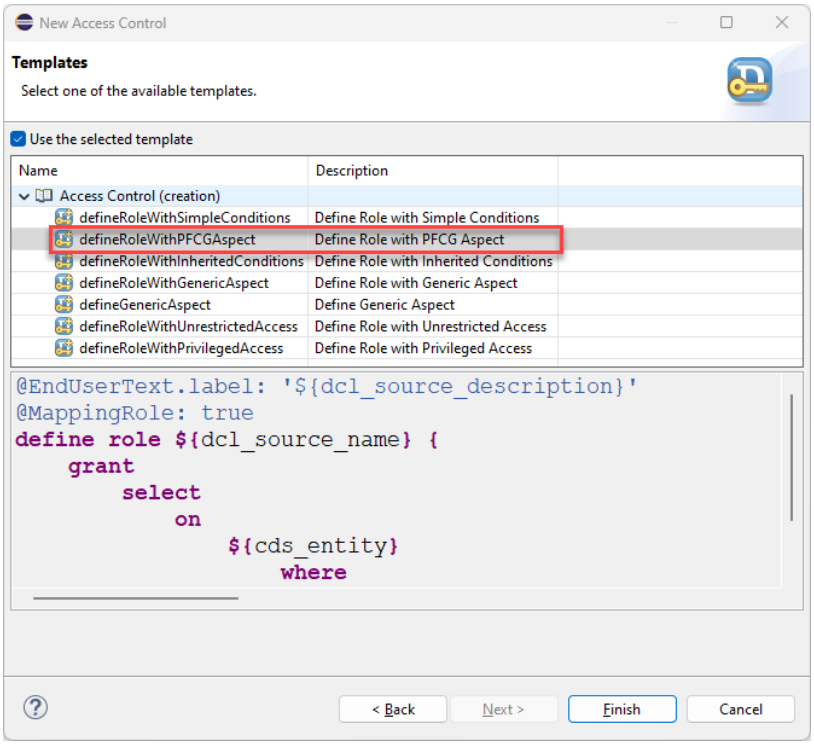
Un dato adicional es que los usuarios de sesión no se pueden usar en los controles de acceso ya que la variable que devuelve el nombre de sesión **$session.user** no se puede utilizar en los filtros dentro de los access control.

7.4. Uso de Aspecto Personalizado

El uso de aspectos personalizados en SAP permite la creación de políticas de acceso detalladas y adaptadas a las necesidades específicas del negocio, mediante la utilización de Core Data Services (CDS). Estos aspectos personalizados añaden una capa adicional de control y flexibilidad, permitiendo definir condiciones precisas sobre quién puede acceder a ciertos datos y bajo qué circunstancias. La implementación de estos aspectos incluye la creación de entidades CDS con propiedades específicas de auditoría y su integración en roles y controles de acceso. Esto asegura que las políticas de acceso sean aplicadas correctamente, permitiendo un manejo seguro y eficiente de la información sensible dentro del sistema SAP.

No se tiene una plantilla específica para el control de acceso con aspecto personalizado pero se puede usar la plantilla del aspecto PFCG. Recordando que 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).**



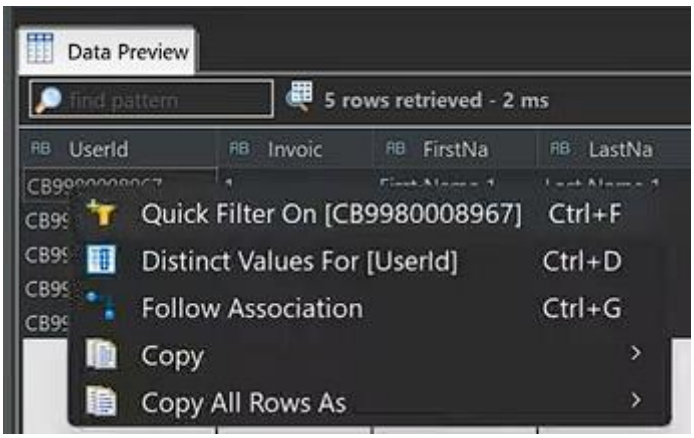
Recordando que la creación de un aspecto personalizado implica la definición de una entidad CDS y la especificación de sus propiedades de auditoría, como dentro de la anotación **@AccessControl: authorizationCheck: #CHECK, auditing.type: #CUSTOM** y **auditing.specification: 'any_word'**. Ya que al momento de activar la política de acceso requerirá dichas configuraciones previas en el **access control.**

Sintaxis:

```
@EndUserText.label: 'Access Control - Custom Aspect'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
  where (entity_component, entity_component_N) = aspect access_policies_name;
}
```

Al invocar el aspecto **access_policies_name** se va a recuperar la información de este CDs en base al usuario que se ha especificado en la política de acceso después de la instrucción **with user element** en lo que sería el usuario de sesión. Este usuario de sesión tampoco se puede confundir con el usuario **$session.user** aunque técnicamente aunque técnicamente representa lo mismo los usuarios de sesión no se pueden utilizar en los Access control, como ya se ha mencionado antes.

Una forma de simular el control de acceso personalizado por usuario en una tabla de base de datos es utilizar la herramienta **Distinct Values For** (Herramienta explicada antes en la Documentación - Access Control) dentro de la ejecución del **Data Preview** al ejecutar una tabla de base de datos o una entidad CDS. Al hacer clic derecho en alguno de los registros en un componente como por ejemplo el usuario la información mostrada en pantalla se mostrará con dicho filtro.



7.5. Aspecto con múltiples criterios

Los aspectos personalizados con múltiples criterios en SAP son configuraciones avanzadas dentro de las políticas de acceso que permiten establecer varias condiciones simultáneamente para el control del acceso a los datos. Estos aspectos se implementan mediante Core Data Services (CDS) y Access Controls, y permiten definir criterios precisos. La correcta configuración y actualización de estos aspectos personalizados garantizan que sólo los usuarios autorizados puedan acceder a los datos sensibles, proporcionando un control detallado y seguro sobre la información crítica de la empresa.

Para implementar estos criterios múltiples, los componentes deben estar en la declaración de los componentes tanto de las tablas de base de datos como en las entidades o vistas CDS para que puedan ser utilizadas dentro del aspecto personalizado. Por lo general dichos campos son los campos claves. Esto asegura que solo los datos relevantes y autorizados se devuelvan en las consultas, mejorando la precisión de las políticas de acceso. Además como los campos clave están indexados en la base de datos, esto permite un acceso más rápido y eficiente a los datos. Esto mejora el rendimiento de las consultas y asegura que las operaciones de filtrado sean más rápidas.

Sintaxis:

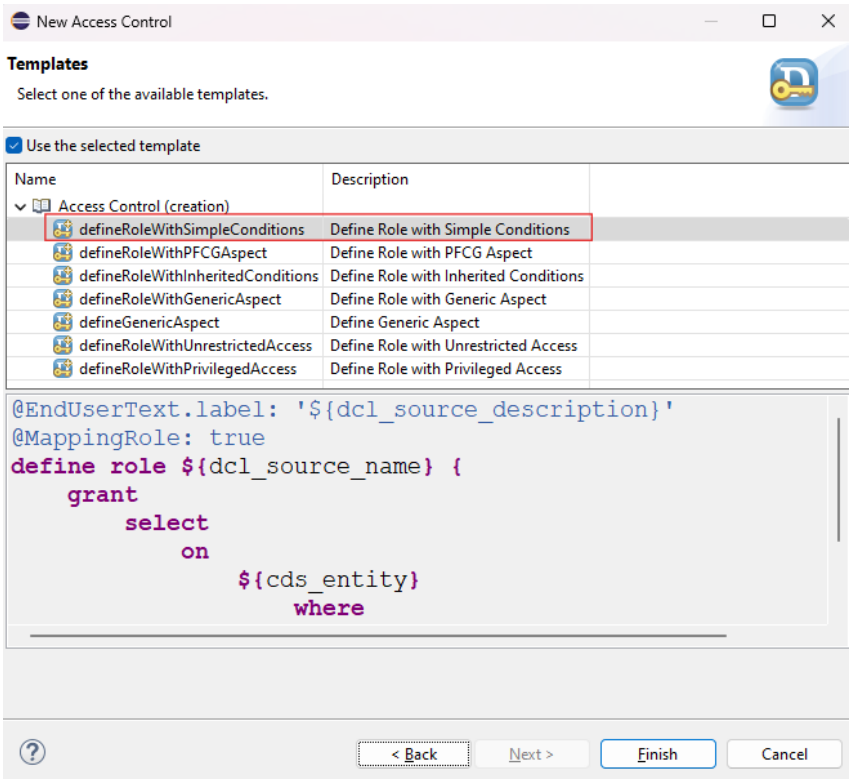
```
@EndUserText.label: 'Access Control - Custom Aspect'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
  where (entity_component_1, entity_component_N) = aspect
access_policies_name;
}
```

7.6. Aspecto de usuario

Los aspectos de usuario en SAP son funcionalidades estándar que permiten restringir el acceso a datos basados en el usuario que realiza una consulta. Estos aspectos aseguran que cada usuario solo puede acceder a la información que le corresponde. Implementados en las definiciones de roles con Access control, los aspectos de usuario comparan el identificador del usuario de sesión con los datos almacenados en los campos específicos de las entidades de datos (CDS). Esta configuración garantiza que las políticas de seguridad sean precisas y efectivas, proporcionando un acceso controlado y seguro a la información crítica de la empresa.

Es necesario crear un access control donde se defina un filtro por un componente de usuario previamente cargado en la tabla que hace referencia la entidad o vista CDS para esto usar la plantilla **defineRoleWithSimpleConditions** que se encuentra en la carpeta **Access Control (creation)**, al momento de crear el control de acceso. Para luego en el filtro utilizar la instrucción **aspect user,** el cual tiene

la misma funcionalidad de la variable de sesión de usuario **$session.user.** Un dato curioso es que, aunque no es posible utilizar la variable de sesión de usuario **$session.user** en la parte derecha del filtro, no se generan errores de sintaxis al usarla en la parte izquierda. Sin embargo, no tiene sentido utilizarla de esta manera, ya que no sería un filtro válido para las consultas.



Un aspecto interesante del **aspect user** es que ya viene incorporado por defecto en la plantilla del Access control. Esto significa que, al crear un nuevo Access control utilizando la plantilla estándar, el **aspect user** está automáticamente disponible para ser utilizado en las definiciones de roles y condiciones de acceso del filtro, lo que faltaría sería especificar o indicar el componente de la entidad que corresponderá al usuario dentro de la tabla de base de datos que hace referencia la vista o entidad CDS. Esto facilita la implementación de políticas de acceso basadas en el usuario, ya que no es necesario definir manualmente este aspecto cada vez que se crea un nuevo control de acceso.

Sintaxis:

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

Recordando que el componente o alias **entity_component1** en el control de acceso corresponde al componente en la entidad CDS se corresponde a los usuarios cuando se realiza la consulta. Es esencial que este componente del usuario haya sido previamente cargado en la base de datos para que pueda ser utilizado en las columnas pertinentes.

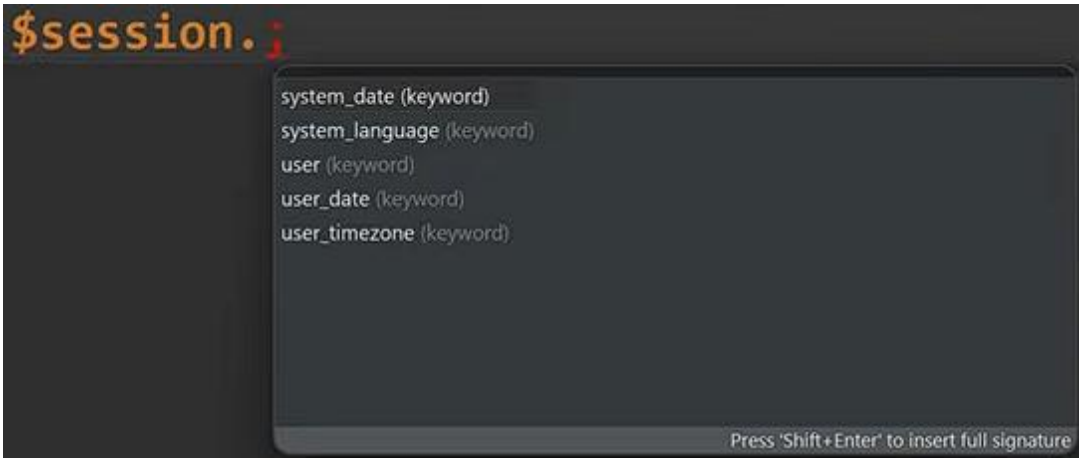
7.7. Expresiones de Host

Las expresiones de Host en SAP son componentes utilizados en la configuración de Access Control que permiten definir criterios específicos para el filtrado y autorización de datos dentro de las Core Data Services (CDS). Estas expresiones se ubican en la parte izquierda de las condiciones y pueden incluir columnas de tablas, variables de sesión, parámetros definidos en las entidades CDS y valores literales. La utilización de expresiones de Host asegura que solo los datos relevantes y autorizados sean accesibles, proporcionando un control granular y seguro sobre la información sensible de la empresa.

Puntos importantes a considerar:

- Es posible incorporar parámetros definidos en la entidad CDS dentro de las expresiones de Host. Estos parámetros permiten filtrar los datos de manera dinámica y personalizada. Para esto se puede definir un parámetro en la entidad CDS con la sentencia **with parameters** (Estudiada dentro de la Documentación - Fundamentos de Modelado de Datos) y luego utilizarlo en las expresiones de Host dentro del Access Control. Esto facilita la creación de filtros más complejos y específicos.

- Las variables de sesión **$session,** también pueden ser utilizadas en las expresiones de Host, pero solo en la parte izquierda de la condición. Estas variables proporcionan información sobre la sesión del usuario, como el idioma o el identificador del usuario, entre otras. Es importante entender que estas variables no pueden ser usadas en la parte derecha de la condición debido a restricciones de sintaxis y funcionalidad como se ha mencionado con anterioridad en los aspectos de usuario.



- Las expresiones de Host también pueden incluir comparaciones con objetos de autorización (pfcg). Pero para esto es necesario que el valor a comparar ya sea un valor literal, un componente de la entidad CDS, parámetro entro otros este dentro de los paréntesis para que cumpla con la sintaxis correcta. Esto permite definir controles de acceso basados en permisos específicos asignados a los usuarios.

Ejemplo:

```
@EndUserText.label: 'Access Control - Test PFCG'
@MappingRole: true
define role rol_name {
  grant select on cds_entity_name
  where $parameters.pParameterName  = 'filter_value_1' and/or
```

```
($parameters.pParameterName) = aspect pfcg_auth(authorization_object, authorization_field_1, authorization_field_2, filter_field_1 = 'filter_value_2') and/or

(entity_component_1, entity_coponent_2) = aspect pfcg_auth(authorization_object, authorization_field_1, authorization_field_2, filter_field_1 = 'filter_value_2') and/or

('filter_value_2') = aspect pfcg_auth(authorization_object, authorization_field_1, authorization_field_2, filter_field_1 = 'filter_value_2') and/or

$session.system_languaje = 'E' and/or

entity_component1 = 'literal_value';
```