Soffid XACML Conceptos

XACML Concepts

1. Policy set

Un PolicySet es un contenedor que puede contener otras Políticas o PolicySets, así como referencias a políticas que se encuentran en ubicaciones remotas.

Cada PolicySet contiene un objetivo y obligaciones, ambos pueden estar vacíos.

- Algoritmo de combinación
- Target
- Obligaciones

El objetivo contiene los sujetos, recursos, acciones y entornos en los que se aplicará el conjunto de políticas. Un target puede contener más de un sujeto, entorno, recurso o acción o ninguno de ellos.

El conjunto de políticas puede exportarse a un archivo XML pulsando el botón Exportar. El archivo contendrá el objetivo del conjunto de políticas y todos los elementos incluidos en él, como otros conjuntos de políticas, políticas o referencias.

Es posible crear una nueva versión de un PolicySet pulsando sobre 'Añadir nueva versión'. Esto copiará todos los elementos del PolicySet en el árbol con el siguiente número de versión.

Ejemplo:

- Un conjunto de políticas aplica sobre una determinada carpeta del Password Vault.
- Cuando se trata de acceder a esta carpeta del Password Vault, se ha configurado como obligación introducir un 2FA

2. Policy

Una Política representa una única política de control de acceso, expresada a través de un conjunto de Reglas.

Cada policy contiene:

- Algoritmo de combinación
- Target
- Variables
- Rules
- Obligations

Ejemplo:

- Se establecen unas reglas para
  - Permitir conectar solamente en horario laboral
  - Permitir conectar solamente en dias laborables
  - Prohibir conectar desde una IP no registrada
  - ..

3. Target

Define a qué solicitudes de acceso se aplica una política o regla. En XACML todos los atributos se clasifican en cuatro categorías principales:

- Subjects
- Resources
- Actions
- Environments

Un objetivo puede contener más de un sujeto, entorno, recurso o acción, o ninguno de ellos. El objetivo es la forma de definir el alcance de una política de autorización. El resultado será MATCHES si todos los elementos definidos coinciden.

- **Attribute Designator**: permite a la política especificar un atributo con un nombre y tipo determinados, y opcionalmente también un emisor.
- **Valor del atributo**: contiene un valor literal del atributo.

3.1. Subjects

(Sujeto) Representa la entidad que realiza una solicitud de acceso a un recurso.

Actor cuyos atributos pueden ser referenciados por un predicado.

Permite añadir uno o varios sujetos como objetivo donde se aplicará la política.

Para configurar un sujeto, en primer lugar debe seleccionar un atributo. Puede seleccionar un valor de una lista de designadores de atributos o escribir el valor del selector de atributos y seleccionar el tipo de datos.

A continuación, debe seleccionar el operador, que se utilizará para comparar o calcular atributos.

Por último, debe establecer un valor con el que se calculará o comparará el atributo. El tipo de datos del valor depende del tipo de datos del atributo.

3.2. Resources

Datos, servicio o componente del sistema.

Permite añadir uno o varios recursos como destino donde se aplicará la política.

Para configurar un recurso, en primer lugar debe seleccionar un atributo. Puede seleccionar un valor de una lista de designadores de atributos o escribir el valor del selector de atributos y seleccionar el tipo de datos.

A continuación, debe seleccionar el operador, que se utilizará para comparar o calcular atributos.

Por último, debe establecer un valor con el que se calculará o comparará el atributo. El tipo de datos del valor depende del tipo de datos del atributo.

3.3. Actions

Una operación sobre un recurso.

Permite añadir una o varias acciones como objetivo donde se aplicará la política.

Para configurar una acción, en primer lugar debe seleccionar un atributo. Puede seleccionar un valor de una lista de designadores de atributos o escribir el valor del selector de atributos y seleccionar el tipo de datos.

A continuación, debe seleccionar el operador, que se utilizará para comparar o calcular atributos.

Por último, debe establecer un valor con el que se calculará o comparará el atributo. El tipo de datos del valor depende del tipo de datos del atributo.

3.4. Environments

Conjunto de atributos que son relevantes para una decisión de autorización y son independientes de un sujeto, recurso o acción en particular.

Permite añadir uno o varios entornos como destino donde se aplicará la política.

Para configurar un entorno, en primer lugar debe seleccionar un atributo. Puede seleccionar un valor de una lista de designadores de atributos o escribir el valor del selector de atributos y seleccionar el tipo de datos. La dirección

A continuación, debe seleccionar el operador, que se utilizará para comparar o calcular atributos.

Por último, debe establecer un valor con el que se calculará o comparará el atributo. El tipo de datos del valor depende del tipo de datos del atributo.

Ejemplo:

- Target: solo aplica a usuairos con un determinado rol.
- Resources: solo aplica sobre una determinada carpeta

Rules

Una regla es la unidad más pequeña dentro de una política. Sólo puede existir de forma aislada dentro de uno de los actores principales del dominio XACML. Cada regla establece una condición específica para permitir o denegar el acceso a un recurso.

- Efecto (Permit/Deny)
- Target
- Conditions

Variables

Las variables son los elementos para definir las funciones que pueden utilizarse en toda la política.

- Expressions

Obligations

XACML define las obligaciones como acciones que deben devolverse al PEP con la respuesta XACML del PDP.

Si la evaluación del PDP se ve como un árbol de reglas, conjuntos de políticas y políticas, cada una de las cuales devuelve «Permitir» o «Denegar», entonces el conjunto de obligaciones devueltas por el PDP al PEP incluirá sólo las obligaciones asociadas con aquellas rutas en las que el efecto en cada nivel de evaluación es el mismo que el efecto devuelto por el PDP.

- Efecto (Permit/Deny)

OBLIGATION	ATTRIBUTE
urn:soffid:obligation:otp	timeout
urn:soffid:obligation:message	text
urn:soffid:obligation:bpm	process

Conditions

La condición representa una expresión booleana que refina la aplicabilidad de la regla más allá de los predicados implicados por su objetivo. Por lo tanto, puede no estar.

- Expressions

Expressions

Las Expresiones son elementos que permiten evaluar condiciones dentro de reglas y políticas para tomar decisiones de acceso.

The attributes depend on the Expression type selected.

EXPRESSION TYPE	OTHER FIELDS	DATA TYPE
Attribute value	**Value**: alfanumeric field	Available data types (*)
Resource	**Attribute designator** • URL • Soffid object • Account name • System name • Login name • Vault folder • Access level	Available data types (*)
Subject	**Attribute designator** • User • User attributes • Account • System • Role • Group • Primary Group • IP Address	Available data types (*)
Action	**Attribute designator**: • method	Available data types (*)

EXPRESSION TYPE	OTHER FIELDS	DATA TYPE
Environment	**Attribute designator**: • Country • Current Time • Current Date • Current DateTime	Available data types (*)
Attribute selector	**Attribute selector**: alphanumeric field	Available data types (*)
Variable	**Variable**: alfanumeric field	--
Function	**Function type**: • Comparison • Arithmetic • Conversions • Date conversions • Boolean Operators • String Functions • Set Functions • Bag Functions • HigherOrderBagFunctions • XPath	Available data types (*)
Function name	**Function type**: • Comparison • Arithmetic • Conversions • Date conversions • Boolean Operators • String Functions • Set Functions • Bag Functions • HigherOrderBagFunctions • XPath **Function**: the value depends on the function type selected.	Available data types (*)

Available data types

- String
- Boolean
- Integer
- Double
- Date and time
- Date
- Time

- HEX-encoded binary
- URI
- Year-month duration
- Day-time duration
- Base 64 binary
- X. 500 name
- RFC822 name

---

https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

---

Revision #6
Created 13 March 2025 14:26:35 by pgarcia@soffid.com
Updated 14 March 2025 09:50:29 by pgarcia@soffid.com