



Auditoría

Control de versiones	3
Introducción	4
Auditoría interna	4
Auditoría externa	4
Esquema de la colección audit_logs	5
Ejemplos	6
Obtención del formulario de un dataset	6
Creación de una entidad	6
Lanzamiento de workflow de validación de una entidad	6
Aprobación de un workflow de una relación	7
Indexar manualmente auditoría	7

Control de versiones

Versión	Fecha de modificación	Responsable	Aprobador	Resumen de cambios
1.0	28/10/2022	Anjana Producto	Anjana Producto	Creación del documento

Introducción

Anjana almacena en la colección `audit_logs` de Solr la auditoría tanto interna como externa. Este documento presenta información acerca de la colección y ejemplos del formato de los campos.

Auditoría interna

En Anjana toda la actividad de los usuarios queda registrada, lo que permite conocer quién y cuándo ha llevado a cabo una acción concreta sobre algún elemento. Esta auditoría proporciona la trazabilidad completa de los objetos en la aplicación.

Auditoría externa

La actividad generada por los usuarios produciendo o consumiendo datos en las estructuras desde las plataformas de datos queda también incorporada a Anjana con el objetivo de dotar de linaje dinámico y auditoría a la herramienta.

Esquema de la colección audit_logs

Field	Description	Mandatory	Type
action	Action	Yes	String
action_description	Detail of the action	No	String
api_version	Version of API for the endpoint	No	String
cluster	Identifier cluster where action is executed	No	String
end_time	Time when the action ends	No	Date
host	Machine where was launch	No	String
ip	Ip from machine	No	String
log_origin	If log was generated by Anjana, Heimdal or other module	Yes	String
object_id	Id of the entity or relation	Yes	Int
object_name	Name of the entity or relation	No	String
object_sub_type	Subtype of the object associated to log	Yes	String
object_type	Type of the object associated to log	Yes	String
process_id	Process identifier (or class to execute)	No	String
related_entities	List of entities associated to the action	No	String
result	Success/error in the action or approval/rejection in a validation	Yes	String
search_action	Flag that indicates if action is search	No	Boolean
snapshot-id	Id of snapshot generated with the action	No	String
start_time	Time when the action begins	No	Date
timestamp	Time of event on UTC	Yes	Date
user_name	Nominal name of user	Yes	String
version	Version of the object	No	Int

Ejemplos

Obtención del formulario de un dataset

```
{
  "process_id": "-1",
  "object_type": "ENTITY",
  "user_name": "maria.gonzalez",
  "ip": "10.20.0.8",
  "end_time": "2021-02-12T12:06:39.712Z",
  "api_version": "v2",
  "object_id": 659,
  "result": "OK",
  "start_time": "2021-02-12T12:06:39.712Z",
  "SNAPSHOT_ID": ["d49e142b-7e73-46ff-981b-4585d19404c8"],
  "object_sub_type": "DSA",
  "search_action": true,
  "log_origin": "anjana",
  "object_name": "mi_dsa",
  "action": "SEARCH_DYNAMIC-CATALOG",
  "timestamp": "2021-02-12T12:06:39.712Z",
  "id": "3e32e759-350d-4a9b-a6e4-06b64199fd75",
  "_version_": 1719304349006430208}
}
```

Creación de una entidad

*Se otorga versión a la entidad cuando se aprueba el workflow, por eso no lleva versión

```
{
  "process_id": "-1",
  "object_type": "ENTITY",
  "user_name": "maria.gonzalez",
  "ip": "10.20.0.8",
  "end_time": "2021-02-12T12:06:29.741Z",
  "api_version": "v2",
  "object_id": 659,
  "result": "OK",
  "start_time": "2021-02-12T12:06:29.741Z",
  "SNAPSHOT_ID": ["b9f09409-e673-4f00-9aaa-50da37751e91"],
  "object_sub_type": "DSA",
  "search_action": false,
  "log_origin": "anjana",
  "action_description": "User maria.gonzalez created the entity mi_dsa with
subtype dsa",
  "object_name": "mi_dsa",
  "action": "CREATE",
  "timestamp": "2021-02-12T12:06:29.741Z",
  "id": "9611ec10-60a9-4d2c-b480-4e7c206c50dd",
  "_version_": 1719304338554224640}
}
```

Lanzamiento de workflow de validación de una entidad

```
{
  "process_id": "-1",
  "object_type": "ENTITY",
  "user_name": "maria.gonzalez",
  "ip": "10.20.0.8",
  "end_time": "2021-02-12T12:06:45.225Z",
  "api_version": "v2",
  "object_id": 659,
  "result": "OK",
  "start_time": "2021-02-12T12:06:45.225Z",
  "SNAPSHOT_ID": ["d49e142b-7e73-46ff-981b-4585d19404c8"],
}
```

```

"object_sub_type": "DSA",
"search_action": false,
"log_origin": "anjana",
"action_description": "User maria.gonzalez submitted the entity mi_dsa with
subtype dsa",
"object_name": "mi_dsa",
"action": "SUBMIT",
"timestamp": "2021-02-12T12:06:45.225Z",
"id": "66de54c8-cdd5-463c-be0b-69993af94acd",
"_version_": 1719304354798764032}

```

Aprobación de un workflow de una relación

```

{
  "process_id": "-1",
  "object_type": "RELATIONSHIP",
  "user_name": "ana.diez",
  "ip": "10.60.0.4",
  "end_time": "2021-02-12T17:51:35.231Z",
  "api_version": "N/A",
  "object_id": 642,
  "result": "OK",
  "start_time": "2021-02-12T17:51:35.231Z",
  "SNAPSHOT_ID": ["e98225cc-40ce-4551-a38d-12977dfb9aa6"],
  "object_sub_type": "RELATED_REPORTS",
  "search_action": false,
  "log_origin": "anjana",
  "action_description": "User ana.diez approved the create workflow of the
related_reports mi_relacion with the reason 'This task was automatically validated
because the user ana.diez who started the workflow or a previous validator is a
candidate to approve this task step'",
  "object_name": "mi_relacion",
  "action": "VALIDATE",
  "timestamp": "2021-02-12T17:51:35.231Z",
  "id": "f1b639dd-be4b-426c-b6fa-97a6ff15ecfa",
  "_version_": 1719326049839349760}

```

Indexar manualmente auditoría

Para indexar en SolR con un proceso creado por cliente se tendrá que cumplimentar el siguiente JSON con la información requerida:

```

{
  "object_type": "<Tipo de objeto>",
  "user_name": "<usuario>",
  "ip": "<ip>",
  "start_time": "<Fecha UTC cuando empezó la acción auditada>",
  "end_time": "<Fecha UTC cuando acabó la acción auditada>",
  "timestamp": "<Fecha UTC cuando se auditó la acción auditada>",
  "object_id": <id del objeto/ -1 si no aplica>,
  "version": <version del objeto/ -1 si no aplica>,
  "result": "<resultado de la acción: OK/KO>",
  "object_sub_type": "<Subtipo del objeto>",
  "search_action": false,

```

```
"log_origin": "<origen de la auditoría, no puede ser 'anjana'>",  
"action_description": "<clave de traducción de la descripción o la descripción>",  
"action": "<clave de traducción de la acción o la acción>"  
}
```

Después se deberá hacer una petición REST directamente a SolR, ejemplo de un curl hecho en Bash:

```
curl  
'http://{hostname}:{SolR_port}/soudit_logslr/a/update?commitWithin=1000&  
overwrite=true&wt=json' -H 'Content-type: application/json' --data-raw  
$'[{JSON_MODIFICADO}]' --compressed --insecure
```

Donde:

- hostname: nombre de la máquina que aloja SolR
- SolR_port: puerto en el que se encuentra SolR
- JSON_MODIFICADO: el JSON que se menciona más arriba, puede ser un único JSON o varios JSON separados por comas.