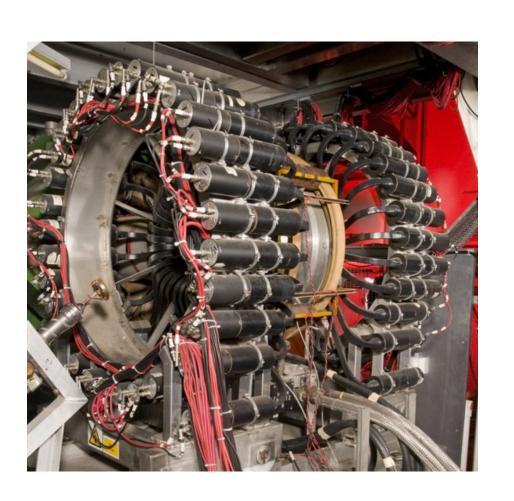
Authorisation Rules at ISIS



Tom Griffin, STFC ISIS Facility ICAT Workshop
Dublin

March 2014

tom.griffin@stfc.ac.uk



Introduction

- Implements a defined data policy
 - PaNdata policy based.
- Public Tables
- Public Steps
- Rules
- UserGroups



Background

- · Rules by default everything is closed.
- ISIS data policy requires >100 rules.....still not finished
- Are (now) sanity checked on creation
- Required at every level for direct access (see PublicSteps)
- Can be checked:

isAccessAllowed(String sessionId, EntityBaseBean bean, AccessType accessType)

Public Tables

- For read only access to open tables
- Cached
- Instrument, Application, DatasetType, InvestigationType etc
- Can be used for link tables : DataCollectionDatafile, InvestigationUser



Public Tables

```
List<String> publicTables = new ArrayList<>();
publicTables.add("Application");
publicTables.add("DatafileFormat");
publicTables.add("DatasetType");
publicTables.add("Facility");
...<cut>...
publicTables.add("DataCollectionDatafile");
publicTables.add("DataCollectionDataset");
       ...<cut>...
List<EntityBaseBean> publicRules = new ArrayList<>();
 for (String publicTableName : publicTables) {
         Rule publicRule = new Rule();
         publicRule.what = publicTableName;
         publicRule.crudFlags = "R";
        publicRules.add(publicRule);
port.createMany(sessionId, publicRules);
```



Public Steps

- Allow access to a related object (attribute)
- ONLY used in INCLUDE processing.
- Offer a significant speedup on INCLUDE
- Thing -> ThingParameter
- Investigation -> samples, publications, users, investigationInstrument etc



Public Steps

Public Steps

```
String[] publicStepsFromInvestigation = new
String[]{"samples", "publications", "shifts",
"investigationUsers", "keywords",
"investigationInstruments"};
for (String step: publicStepsFromInvestigation)
{
      PublicStep invToSomething = new PublicStep();
      invToSomething.origin = "Investigation";
      invToSomething.field = step;
      publicSteps.add(invToSomething);
```



Rule Structure

- Administrators
- Safe Admin (read all)
- · [Raw] Data Ingestor
- Instrument Scientists
- Investigators
- Disordered Materials Database
- DOI service
- Unembargoed data



Administrators

Easy

```
List<String> allTables = port.getEntityNames();
for (String table : allTables)
{
    Rule rule = new Rule();
    rule.grouping = facilityAdmins;
    rule.crudFlags = "CRUD";
    rule.what = table;
    port.create(sessionId, rule);
}
```

Other super groups

- · Safe admins same rules, no 'CUD'
- · Data Ingestors: 'CRU', fewer tables



Instrument Scientists

Defines access relative to instruments

```
JOIN i.investigationInstruments ii

JOIN ii.instrument inst

JOIN inst.instrumentScientists instSci

JOIN instSci.user u

WHERE u.name = :user

Investigation, Dataset, Datafile, Sample,
SampleType + 4x Parameters
```

SELECT i FROM Investigation i



Instrument Scientists

```
SELECT df FROM Datafile df
JOIN df.dataset d
JOIN d.investigation i
JOIN i.investigationInstruments ii
JOIN ii.instrument inst
JOIN ii.instrumentScientists instSci
JOIN inst.instrumentScientists instSci
JOIN instSci.user u
WHERE d.name='Default'
AND u.name = :user";
```



Investigators

Defines access relative to investigation role

```
DatafileParameter <-> Datafile <-> Dataset <->
Investigation <-> InvestigationUser <-> User <->
User [name = :user]
```

Investigation, Dataset, Datafile, Sample,
SampleType + 4x Parameters



Disordered Materials Database

· Write (authenticated) and open read to domain specific 'database'

```
SELECT df FROM Datafile df

JOIN df.dataset ds

JOIN ds.investigation i

JOIN i.type it

WHERE it.name Disordered Materials

Grouping = Disordered Materials Publishers

Access = CRUD
```



DOI Account

 Requires read access to generate landing pages

```
SELECT i FROM Investigation i WHERE i.doi IS NOT NULL SELECT ds FROM Dataset ds WHERE ds.doi IS NOT NULL
```

DOI creation runs as Data Ingestor



Unembargoed Data

Read for all authenticated users

```
SELECT i FROM Investigation i WHERE i.releaseDate <
CURRENT TIMESTAMP
SELECT dfp FROM DatafileParameter dfp
JOIN dfp.datafile df
JOIN df.dataset d
JOIN d.investigation i
WHERE d.name = 'Default'
AND i.releaseDate < CURRENT TIMESTAMP
Investigation, Dataset, Datafile, Sample, SampleType +
4x Parameters
```



Complications

- Lock updates when DOI <> null
- Granting permissions
 - Create a group per investigation
 - What about finer grain?
 - Adding new users
 - What is ICAT, what is User office?
- Allowing partial updates
 - Investigation.release_date only
- Performance



Questions...



