Security & Access Control

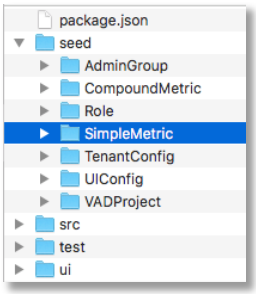
CAPSTONE PROJECT | FINAL ASSIGNMENT

In this portion of the capstone project we will define user roles, permissions, and action conditions to control access to data based on user groups.

1. GENERAL ANALYST

In this section, we are going to create a role for a *general analyst* that allows the user in this role to read all data. Like metrics, role and group configurations reside in the `/seed` folder and are json files.

Create an `/AdminGroup` and `/Role` folder to store your groups and roles respectively:



`seed` folder structure.

We can configure the `GeneralAnalystRole`, with read-only permissions in the following way:

```
{
  "id": "GeneralAnalystRole",
  "name": "GeneralAnalystRole",
  "permissions": [
      "allow:*:read:"
  ]
}
```

Now, we can create the `GeneralAnalystGroup` to which this role will be applied, and add the `GeneralAnalystRole` to the group:

```
{
  "id" : "GeneralAnalystGroup",
  "name" : "GeneralAnalystGroup",
  "roles" : [
    {
      "id": "GeneralAnalystRole"
    }
  ]
}
```

Save these files as `GeneralAnalystRole.json` and `GeneralAnalystGroup.json` in the `/Role` and `/AdminGroup` folders respectively.

2. BUILDING FETCH ONLY ANALYST

Now, we are going to create a role for a *building fetch analyst* that allows the user in this role to fetch data for buildings, and nothing else. Use the following information to create a `BuildingFetchOnlyAnalystRole`:

```
{
  "id": "BuildingFetchOnlyAnalystRole",
  "name": "BuildingFetchOnlyAnalystRole",
  "permissions": [
      "allow:Building::fetch"
  ]
}
```

Now, we can create the `BuildingFetchOnlyGroup` to which this role will be applied, and add the `BuildingFetchOnlyAnalystRole` to the group:

```
{
  "id" : "BuildingFetchOnlyGroup",
  "name" : "BuildingFetchOnlyGroup",
  "roles" : [
    {
      "id": "BuildingFetchOnlyAnalystRole"
    }
  ]
}
```

Save these files as `BuildingFetchOnlyAnalystRole.json` and `BuildingFetchOnlyGroup.json` in the `/Role` and `/AdminGroup` folders respectively.

3. EXPORT DATA PULL

Now, we are going to create a role for a user that will be allowed to *export/pull data*. Use the following information to create an `ExportDataPullRole`:

```
{
  "id": "ExportDataPullRole",
  "name": "ExportDataPullRole",
  "permissions": [
    "deny:Export::remove",
    "deny:Export::removeAll",
    "allow:Export::*",
    "allow:BatchExportSpec::make",
    "allow:OAuth::token",
    "allow:S3File::*",
    "allow:File::writeEncodedStream"
  ]
}
```

Save this file as `ExportDataPullRole.json` in the `/Role` folder.

4. BUILDING 1 ANALYST

Now, we are going to create a role for a user that will be allowed to *only read data related to Building 1*. Use the following information to create `Building1AnalystRole`:

```
{
  "id": "Building1AnalystRole",
  "name": "Building1AnalystRole",
  "permissions": [
    "allow:*:read:",
    "deny:SmartBulbMeasurement::fetch"
  ],
  "actionConditions": [
    "Building:read::(intersects(id,['bld1']))",
    "Apartment:read::(intersects(building.id, ['bld1']))",
    "Fixture:read::(intersects(apartment.building.id,['bld1']))",
```

```
"SmartBulbToFixtureRelation:read::(intersects(to.apartment.building.id,['bld1
']))",

"SmartBulb:read::(intersects(fixtureHistory.to.apartment.building.id,['bld1']
))",

"SmartBulbMeasurementSeries:read::(intersects(smartBulb.fixtureHistory.to.apa
rtment.building.id,['bld1']))"
  ]
}
```

Now, we can create the `Building1AnalystGroup` to which we will add the `Building1AnalystRole`:

```
{
  "id" : "Building1AnalystGroup",
  "name" : "Building1AnalystGroup",
  "roles" : [
    {
      "id": "Building1AnalystRole"
    }
  ]
}
```

Save these files as `Building1AnalystRole.json` and `Building1AnalystGroup.json` in the `/Role` and `/AdminGroup` folders respectively.

5. ADDING EXPORT/PULL PRIVILEGE

Finally, we want to give all groups the ability to export/pull data. For that purpose, we need to add the `ExportDataPullRole` to all the groups that we have previously created:

- `GeneralAnalystGroup`
- `BuildingFetchOnlyGroup`
- `Building1AnalystGroup`

An example of how to add the `ExportDataPullRole` is shown below in green:

```
{
  "id" : "GeneralAnalystGroup",
  "name" : "GeneralAnalystGroup",
  "roles" : [
    {
      "id": "GeneralAnalystRole"
    },
    {
      "id": "ExportDataPullRole"
    }
  ]
}
```

Congratulations, you have finished the capstone project!!!