

Project Spaces Authorization

This is a live design document on how to support authorization at the level of project spaces. The primary driver of this development is the [SEAD](#) project.

The current design tries to support requirements described in this document:

? Unknown Attachment

The following notes are from a meeting on 06/09/15 attended by [Indira Gutierrez Polo](#), [Mario Felarca](#), [Winston Jansz](#), [Rob Kooper](#), [Luigi Marini](#).

Goals:















1. Meet the requirements of the above document
2. Meet the outcomes of the SEAD all hands meeting in May 2015
3. Simplify the design as much as possible to not overwhelm the user and provide a stable implementation within the current efforts
4. Accommodate other use cases

Features Needed:

The following are already available in the current implementation:

1. A dataset can be in multiple collections

The following need to be implemented:

1. A file can only exist as part of a dataset (currently it can exist in multiple or none)
 **CATS-25** - Remove ability to upload files outside of a datasets 
2. A dataset can be part of multiple spaces (currently it can exist in multiple or none)
 **CATS-26** - A dataset can be in multiple spaces 
 - a. With this design there is no "move" just assign to one or more spaces
3. A collection can be part of multiple spaces (currently it can exist in multiple or none)
 **CATS-27** - A collection can be in multiple spaces 
 - a. With this design there is no "move" just assign to one or more spaces
4. Use permissions on space, collection, dataset page to pick what is available and what is not in the GUI
 **CATS-28** - Update Dataset/Collection page based on permissions 
5. Nested collections (which are different from folders because a collection can be in multiple collections)
 **CATS-29** - Nested collections 
6. Ability to list who has access to a dataset or collection on its page
 **CATS-30** - List who has access to a dataset or a collection 
7. (Bonus) Folders in dataset to organize files *similar* to a file system
 **CATS-31** - Folders in dataset to organize files similar to a file system 

Notes:

1. Implement access control only at the level of spaces
 - a. Datasets and collections authorization is based on space
 - b. For resources in multiple spaces take the union of permissions
2. Only the owner can add a dataset/collection to a new space
3. In a world where resources can be in multiple spaces, spaces becomes a view into the data, not a simple self contained place
4. **What happens if D1 is in C1, C1 is in S1, but D1 is not in S1?**
5. Publishing a dataset or collection for public viewing will be done as a separate feature from managing permission on a space level

Permissions Cleanup:

(Note this is the list from `api.Permissions.Permission`. It's pretty low lever and it's what controller look for in the case of secured actions)

Public -> Public (will eventually be removed)
Admin -> *Keep*
CreateCollections -> CreateCollection
DeleteCollections -> DeleteCollection
EditCollection -> *Keep*
ListCollections -> *Remove* (see ViewSpace)
ShowCollection -> ViewCollection

CreateSpaces -> CreateSpace
UpdateSpaces -> EditSpace
DeleteSpaces -> DeleteSpace
EditSpace -> *Keep*
ListSpaces -> *Remove*
ShowSpace -> ViewSpace
CreateDatasets -> CreateDataset
DeleteDatasets -> DeleteDataset
ListDatasets -> *Remove* (see ViewSpace)
ShowDataset -> ViewDataset
SearchDatasets -> ViewDataset
AddDatasetsMetadata -> AddMetadata
ShowDatasetsMetadata -> ViewMetadata
CreateTagsDatasets -> AddTag
DeleteTagsDatasets -> DeleteTag
ShowTags -> ViewTags
UpdateDatasetInformation -> EditDataset
UpdateLicense -> EditLicense
CreateComments -> CreateComment
RemoveComments -> DeleteComment
EditComments -> EditComment
CreateNotes -> CreateNote
AddSections -> AddSection
GetSections -> ViewSections
CreateTagsSections -> AddTag
DeleteTagsSections -> Delete Tag
CreateFiles -> AddFile
DeleteFiles -> DeleteFile
ListFiles -> *Remove* (everyone should be able to)
ExtractMetadata -> ViewMetadata
AddFilesMetadata -> AddMetadata
ShowFilesMetadata -> ViewMetadata
ShowFile -> ViewFile
SearchFiles -> ViewFile
CreateTagsFiles -> AddTag
DeleteTagsFiles -> DeleteTag
CreateStreams -> CreateGeoTemporalStream
AddDataPoints -> CreateGeoTemporalDatapoint
SearchStreams -> ViewGeoTemporalStream
AddZoomTile -> CreatePreview
Add3DTexture -> CreatePreview
AddIndex -> CreateIndex
CreateSensors -> CreateGeoTemporalSensor
ListSensors -> ViewGeoTemporalSensor
GetSensors -> ViewGeoTemporalSensor
SearchSensor -> ViewGeoTemporalSensor
RemoveSensors -> ViewGeoTemporalSensor
AddThumbnail -> CreatePreview
DownloadFiles -> *Same*
GetUser -> ViewUser
AddProject -> EditUser
AddInstitution -> EditUser
UserAdmin -> Admin

New List:

```

val Public, // Page is public accessible, i.e. no login needed
    Admin,

    // spaces
    ViewSpace,
    CreateSpace,
    DeleteSpace,
    EditSpace,

    // datasets
    ViewDataset,
    CreateDataset,
    DeleteDataset,
    EditDataset,

    // collections
    ViewCollection,
    CreateCollection,
    DeleteCollection,
    EditCollection,

    // files
    AddFile,
    DeleteFile,
    ViewFile,
    DownloadFiles,
    EditLicense,
    CreatePreview, // Used by extractors
    MultimediaIndexDocument,
    CreateNote,

    // sections
    CreateSection,
    ViewSection,
    DeleteSection, // FIXME: Unused right now
    EditSection, // FIXME: Unused right now

    // metadata
    AddMetadata,
    ViewMetadata,
    DeleteMetadata, // FIXME: Unused right now
    EditMetadata, // FIXME: Unused right now

    // social annotation
    AddTag,
    DeleteTag,
    ViewTags,
    AddComment,
    DeleteComment,
    EditComment,

    // geostreaming api
    GSCreateStream,
    GSAddDatapoint,
    GSViewDatapoints,
    GSAddSensor,
    GSViewSensor,
    GSDeleteSensor,

    // users
    ViewUser,
    EditUser = Value

```