ownCloud Infinite Scale

Identity, Roles and Permissions

Agenda

1. oCIS core concepts
2. Permissions Graph
3. Grants
4. Permissions API

David Christofas
Security Engineer

oCIS Core concepts

User

Group

Role

Permission

File

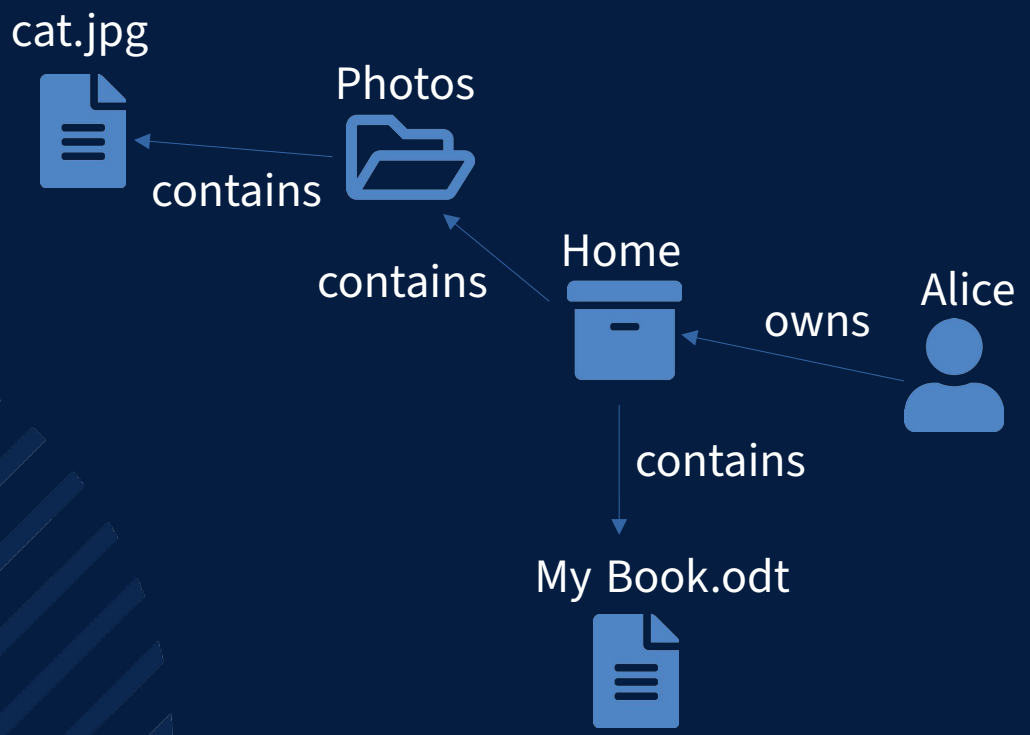
Folder

Space

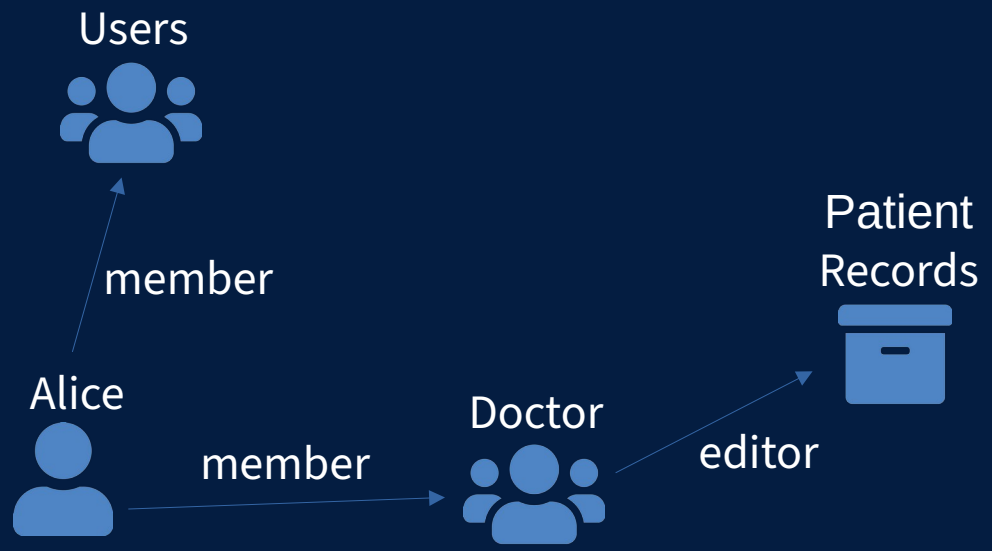
Share

Extension

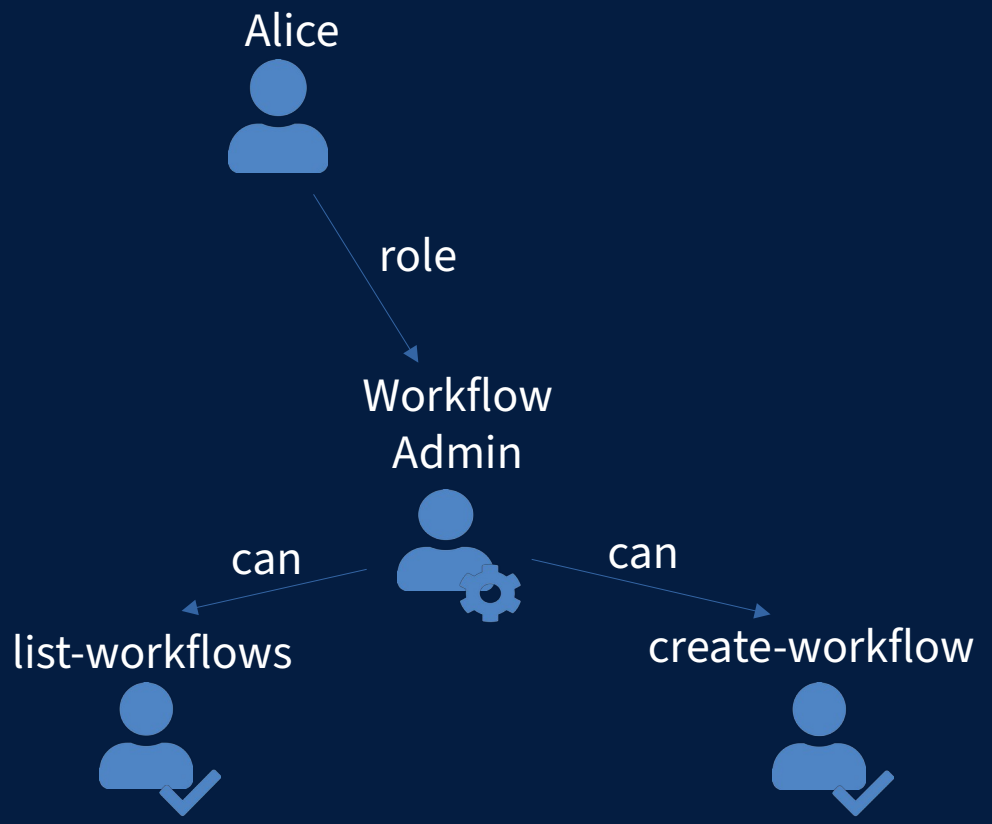
Permission Graph



Permission Graph



Permission Graph



Permission Graph

Solution: Grants

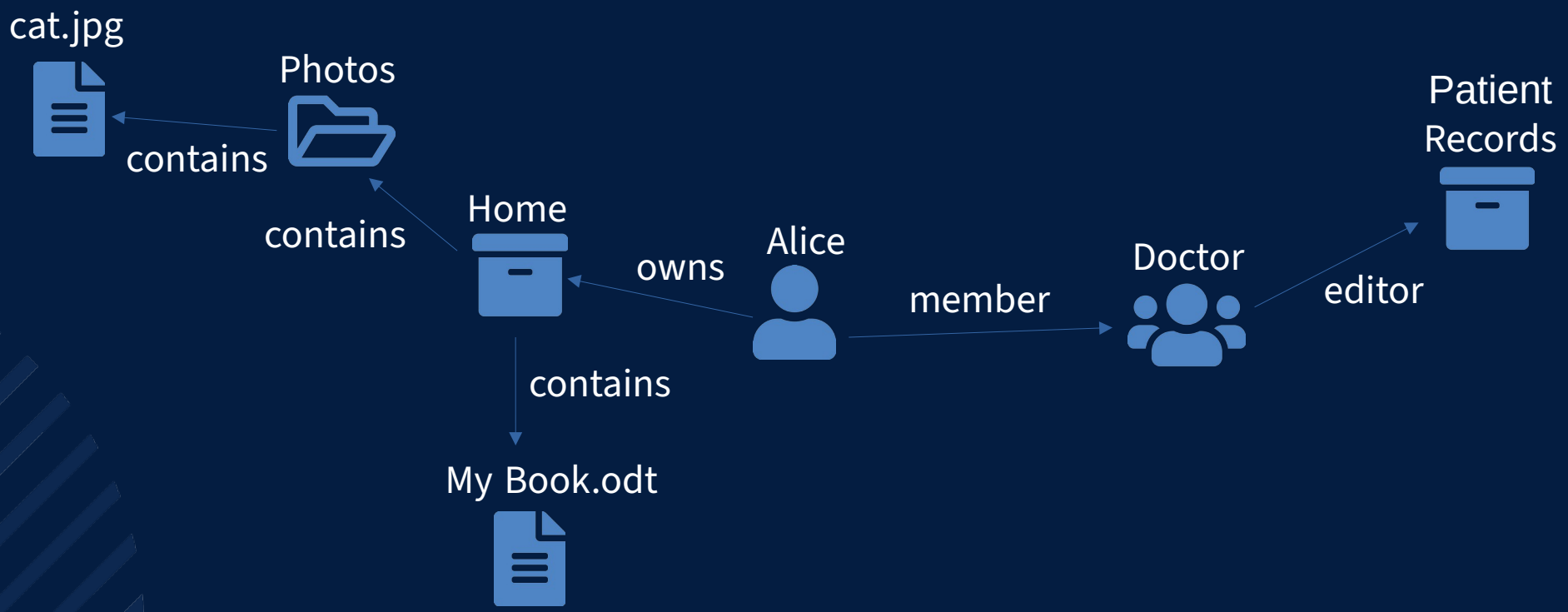
- [User|Group] can [Read|Write] Resource
- Handled by the storage
  - Closer to the files
  - Faster checks
- Limited permissions

ResourcePermissions

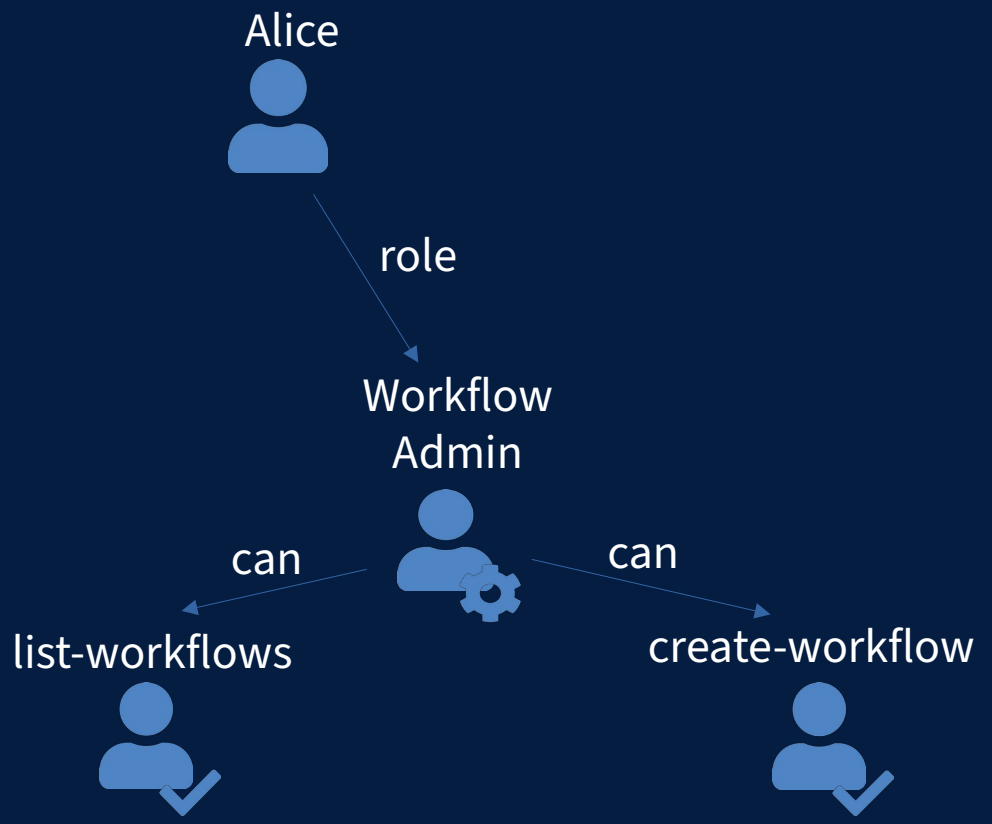
The representation of permissions attached to a resource.

Field	Type	Label
add_grant	bool	
create_container	bool	
delete	bool	
get_path	bool	
get_quota	bool	
initiate_file_download	bool	
initiate_file_upload	bool	
list_grants	bool	
list_container	bool	
list_file_versions	bool	
list_recycle	bool	
move	bool	
remove_grant	bool	
purge_recycle	bool	
restore_file_version	bool	
restore_recycle_item	bool	
stat	bool	
update_grant	bool	
deny_grant	bool	

Permission Graph

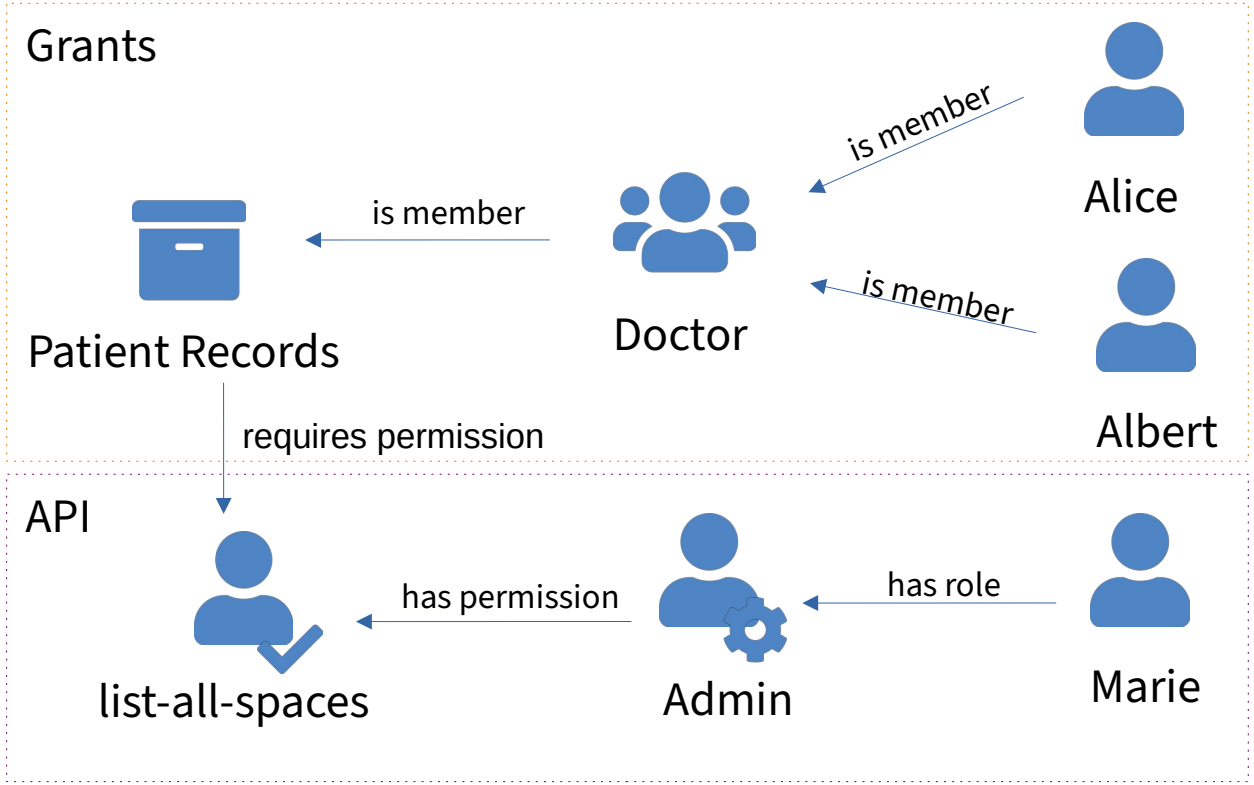


Permission Graph



Solution: Permissions API

- A permission service would:
- Store mappings
  - Permissions <–> Roles
  - Roles <-> User/Group
  - User <-> Group
- Efficiently check if a user has a certain permission



Permissions API

- 3 Primitives
  - Permission
  - Subject
  - Reference
- Eventually
  - Manage roles
  - Manage permissions
  - Namespaces

CheckPermissionRequest

CheckPermissionsRequest is used to check if a user has a certain permission.

Field	Type	Label	Description
permission	string		REQUIRED. The permission to check.
subject_ref	SubjectReference		REQUIRED. The subject holding the permission.
ref	cs3.storage.provider.v1beta1.Reference		OPTIONAL. The target resource of the permission.

[Permissions API CS3 Doc]
[Google Zanzibar Paper]
[Authzed spicedb]


ownCloud