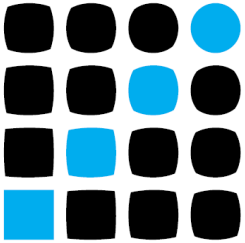


adaptTo()

APACHE SLING & FRIENDS TECH MEETUP

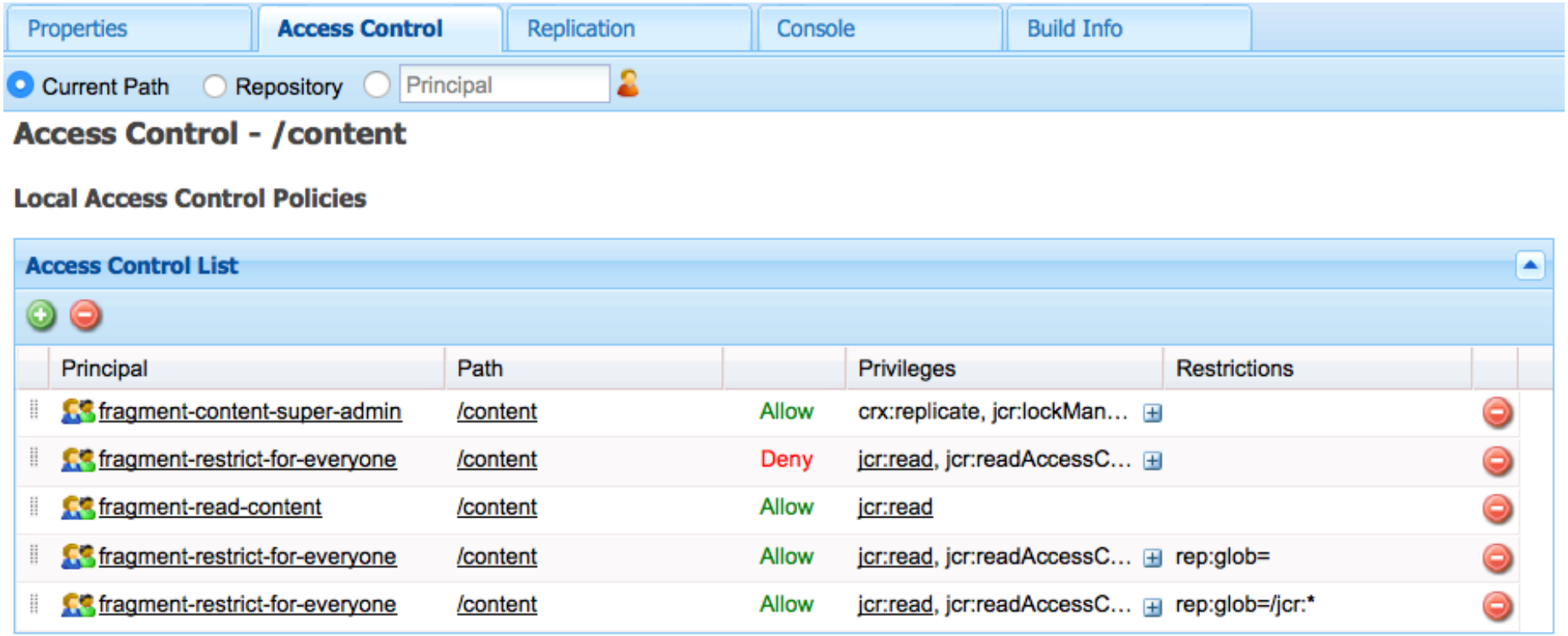
BERLIN, 26-28 SEPTEMBER 2016

AC Tool – Simplified Rights & Roles Rollout

R. Gruber, J. Koschorke, Netcentric

What are ACLs?

What Are ACLs Used For?



Why to use a tool for ACL rollout?

Why Use a Tool for AC Rules?

- Tend to be complex
- Need to be understandable
- Must be consistent
- Need to be portable between stages
- Need automation

Why a New Tool?

Aspect	Content Package	ACL Setup Service	AC Tool

Why a New Tool?

Aspect	Content Package	ACL Setup Service	AC Tool
Readability	 hard to read	 readable for small setups	 human readable files

Why a New Tool?

Aspect	Content Package	ACL Setup Service	AC Tool
Readability	✗ hard to read	⚠ readable for small setups	✓ human readable files
Run mode support	✗	✓	✓

Why a New Tool?

Aspect	Content Package	ACL Setup Service	AC Tool
Readability	✗ hard to read	⚠ readable for small setups	✓ human readable files
Run mode support	✗	✓	✓
Consistency	✗ old entries stay	✗ old entries stay	✓ deletes old ACLs

Why a New Tool?

Aspect	Content Package	ACL Setup Service	AC Tool
Readability	✗ hard to read	⚠ readable for small setups	✓ human readable files
Run mode support	✗	✓	✓
Consistency	✗ old entries stay	✗ old entries stay	✓ deletes old ACLs
Export	⚠ ACL Packager	✗	✓

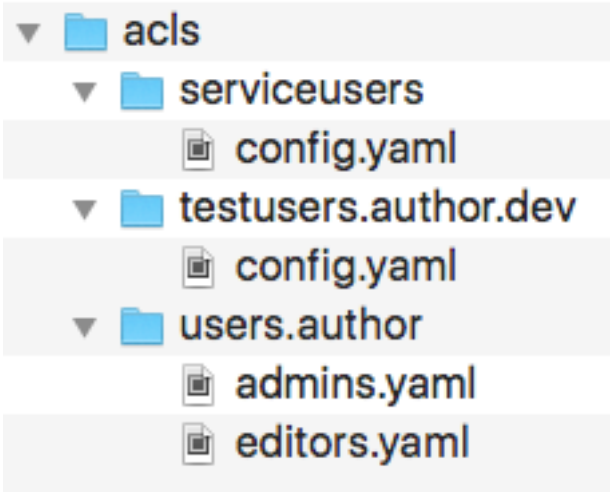
Why a New Tool?

Aspect	Content Package	ACL Setup Service	AC Tool
Readability	✗ hard to read	⚠ readable for small setups	✓ human readable files
Run mode support	✗	✓	✓
Consistency	✗ old entries stay	✗ old entries stay	✓ deletes old ACLs
Export	⚠ ACL Packager	✗	✓
Maintenance	✗ complex	⚠ one OSGI configuration	✓ multiple files

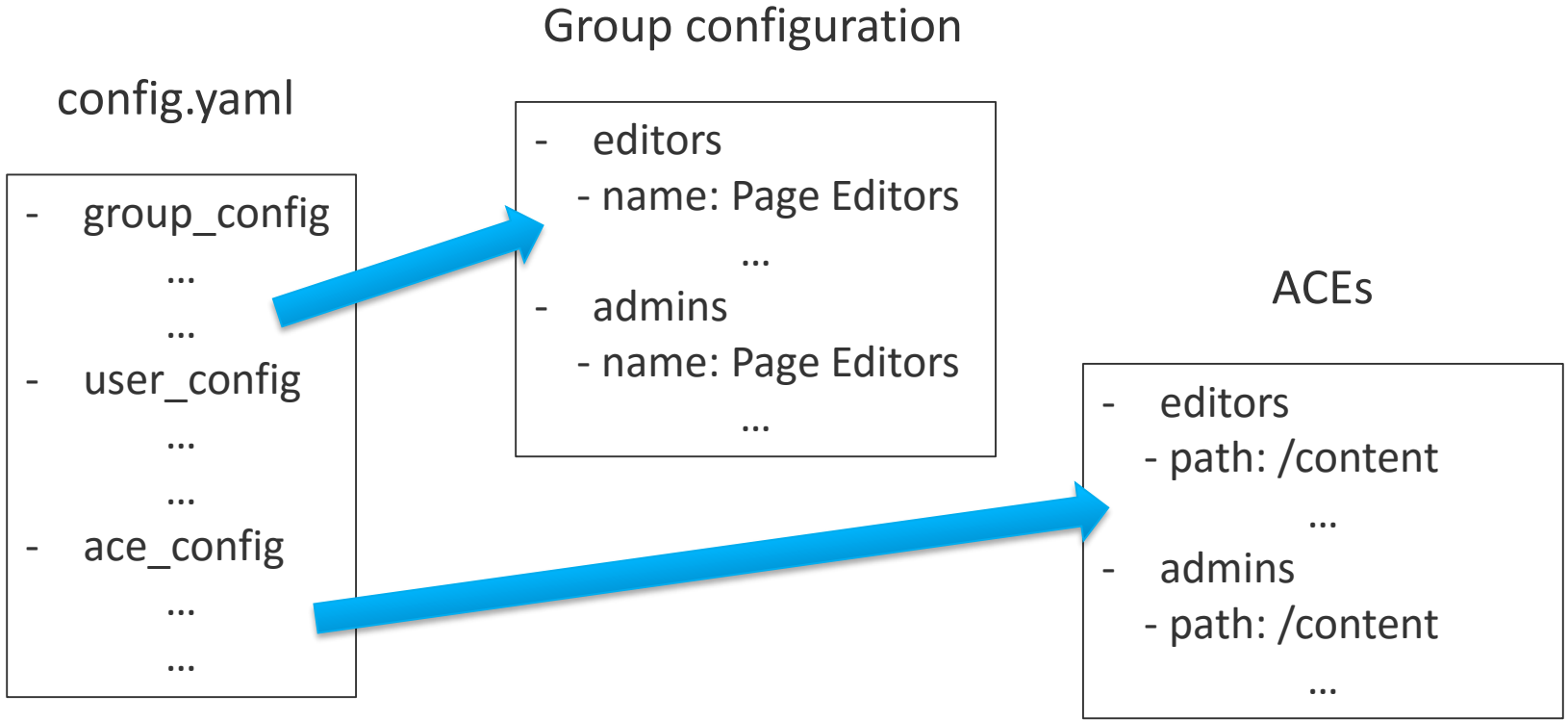
How does AC Tool work?

File Structure

- Yaml format
- Multiple files per folder
- Run mode in folder name



Sections


Group configuration
config.yaml
- group_config
…
…
- user_config
…
…
- ace_config
…
…
- editors
- name: Page Editors
…
- admins
- name: Page Editors
…
ACEs
- editors
- path: /content
…
- admins
- path: /content
…

Group Definitions

```
- group_config:
  - editors:
    - name: Page Editors
      isMemberOf: staff
      members: joe
      description: All page editors
      path: myproject
```

Assign ACEs to Groups

Simple ACE

```
- ace_config:
  - editors:
    - path: /content
      permission: allow
      privileges: jcr:read,rep:write
```

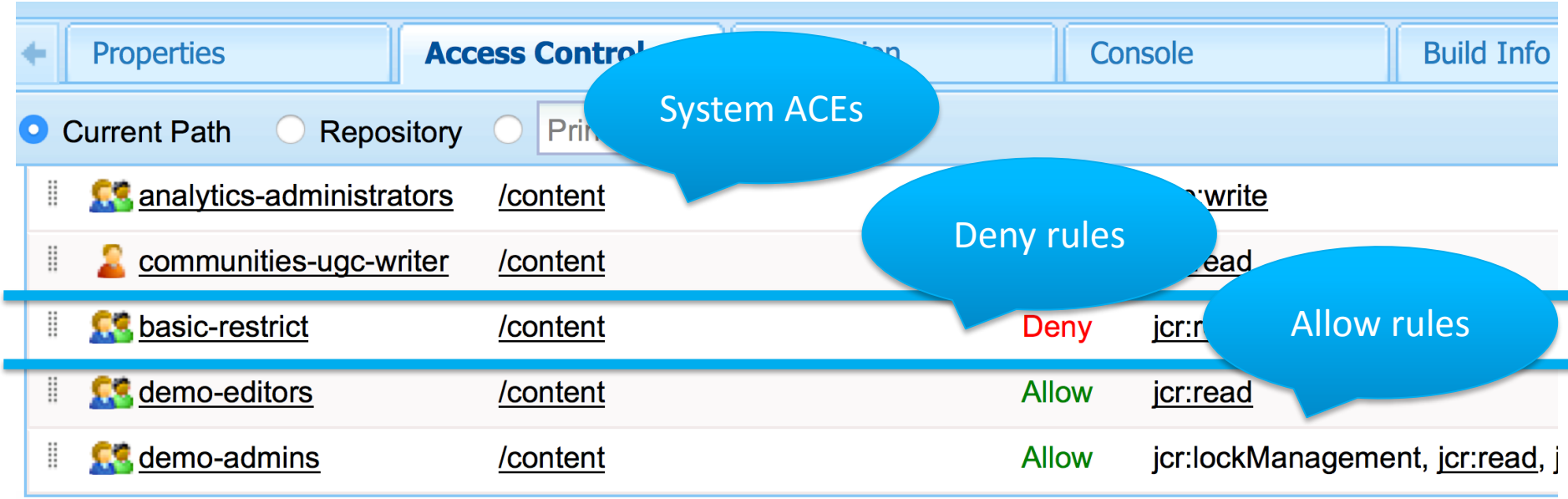
Assign ACEs to Groups

Using restrictions

```
- ace_config:
  - editors:
    - path: /content
      permission: allow
      privileges: jcr:read
      restrictions:
        rep:glob: /jcr:*
```

ACE ordering

Consistent order of ACEs



User Creation

adaptTo()

User Creation: user_config

- Primarily for test users and
- System users
- Profile content creation
- Preferences content creation

User Creation: Examples

```
- poweruser

  - name: PowerUserTestUser
    isMemberOf: powerusers
    password: secret
    path: myproject
    profileContent: <jcr:root
           jcr:primaryType="nt:unstructured"
           email="poweruser@example.com"/>

- system_reader:

  - name: system-reader
    isMemberOf: system-read
    path: myproject
    isSystemUser: true
```

Installation of ACEs

Installation: JMX

- JMX
- Curl
- JCR Listener
- Install Hook

Attributes

Attribute Name	Attribute Value
ReadyToStart	true
Executing	false
ConfigurationFiles	/var/actool/isp/config1.yaml /var/actool/shared/config2.yaml
SavedLogs	1. /var/statistics/achistory/history_1395063827706 (Mon Mar 17 14:43:45 CE

Operations

Return Type	Name
java.lang.String	execute() executes the installation of the ACE configuration(s)
java.lang.String	purgeACL(java.lang.String path) purges the AccessControlList of the given path, if existing
java.lang.String	purgeACLs(java.lang.String path) purges all AccessControlLists under the given path and its subpaths, if existing
java.lang.String	purgeAuthorizables(java.lang.String authorizableIds) purges authorizable(s) and respective ACEs from the system. Several authorizable
java.lang.String	pathBasedDump() returns a configuration dump containing all groups and all ACLs ordered by path

Installation: JMX

- JMX
- Curl
- JCR Listener
- Install Hook

Attributes

Attribute Name	Attribute Value
ReadyToStart	true
Executing	false
ConfigurationFiles	/var/actool/isp/config1.yaml /var/actool/shared/config2.yaml
SavedLogs	1. /var/statistics/achistory/history_1395063827706 (Mon Mar 17 1

Operations

Return Type	Name
java.lang.String	execute() executes the installation of the ACE configuration(s)
java.lang.String	purgeACL(java.lang.String path) purges the AccessControlList of the given path, if existing
java.lang.String	purgeACLs(java.lang.String path) purges all AccessControlLists under the given path and its subpaths, if existing
java.lang.String	purgeAuthorizables(java.lang.String authorizableIds) purges authorizable(s) and respective ACEs from the system. Several authorizable
java.lang.String	pathBasedDump() returns a configuration dump containing all groups and all ACLs ordered by path

status informations

Installation: JMX

- JMX
- Curl
- JCR Listener
- Install Hook

Attributes

Attribute Name	Attribute Value
ReadyToStart	true
Executing	false
ConfigurationFiles	/var/actool/isp/config1.yaml /var/actool/shared/config2.yaml
SavedLogs	1. /var/statistics/achistory/history_1395063827706 (Mon Mar 17 1

Operations

Return Type	Name
java.lang.String	execute() executes the installation of the ACE configuration(s)
java.lang.String	purgeACL(java.lang.String path) purges the AccessControlList of the given path, if existing
java.lang.String	purgeACLs(java.lang.String path) purges all AccessControlLists under the given path and its subpaths, if existing
java.lang.String	purgeAuthorizables(java.lang.String authorizableIds) purges authorizable(s) and respective ACEs from the system. Several authorizable
java.lang.String	pathBasedDump() returns a configuration dump containing all groups and all ACLs ordered by path

execute

Installation: JMX

- JMX
- Curl
- JCR Listener
- Install Hook

Attributes

Attribute Name	Attribute Value
ReadyToStart	true
Executing	false
ConfigurationFiles	/var/actool/isp/config1.yaml /var/actool/shared/config2.yaml
SavedLogs	1. /var/statistics/achistory/history_1395063827706 (Mon Mar 17 14:43:45 CE

Operations

Return Type	Name
java.lang.String	execute() executes the installation of the ACE configuration(s)
java.lang.String	purgeACL(java.lang.String path) purges the AccessControlList of the given path, if existing
java.lang.String	purgeACLs(java.lang.String path) purges all AccessControlLists under the given path and its subpaths, if existing
java.lang.String	purgeAuthorizables(java.lang.String authorizableIds) purges authorizable(s) and respective ACEs from the system. Several authorizable
java.lang.String	pathBasedDump() returns a configuration dump containing all groups and all ACLs ordered by path

purge permissions

Installation: JMX

- JMX
- Curl
- JCR Listener
- Install Hook

Attributes

Attribute Name	Attribute Value
ReadyToStart	true
Executing	false
ConfigurationFiles	/var/actool/isp/config1.yaml /var/actool/shared/config2.yaml
SavedLogs	1. /var/statistics/achistory/history_1395063827706 (Mon Mar 17 14:43:45 CE

Operations

Return Type	Name
java.lang.String	execute() executes the installation of the ACE configuration(s)
java.lang.String	purgeACL(java.lang.String path) purges the AccessControlList of the given path, if existing
java.lang.String	purgeACLs(java.lang.String path) purges all AccessControlLists under the given path and its subpaths, if ex
java.lang.String	purgeAuthorizables(java.lang.String authorizableIds) purges authorizable(s) and respective ACEs from the system. Sev uthorizable
java.lang.String	pathBasedDump() returns a configuration dump containing all groups and all ACLs ordered by path

create exports

Installation: Curl

- JMX
- Curl
- JCR Listener
- Install Hook

```
curl -sS --retry 1 -u admin:admin -X POST
"http://localhost:4502/system/console/jmx/biz.netcentric
cq.tools.actool:id='ac+installation'/op/execute/"
```

Installation: JCR Listener

JMX

Curl

JCR Listener

Install Hook

- Event based trigger:
- On new upload
- On change in deployed config
- Can be disabled

Installation: Install Hook

- JMX
- Curl
- JCR Listener
- Install Hook

```
<plugin>
  <groupId>com.day.jcr.vault</groupId>
  <artifactId>content-package-maven-plugin</artifactId>
    <configuration>
       <properties>
        <installhook.actool.class>
         biz.netcentric.cq.tools.actool.installhook.AcToolInstallHook
        </installhook.actool.class>
    </properties>
  </configuration>
</plugin>
```

Live Demo

Best Practices

adaptTo()

Best Practises: Some General Hints

- Avoid deny ACEs whenever possible
- Split configuration files by project/topic
- Create demo users with test content
- Keep it simple

adaptTo()

Best Practises: Fragments

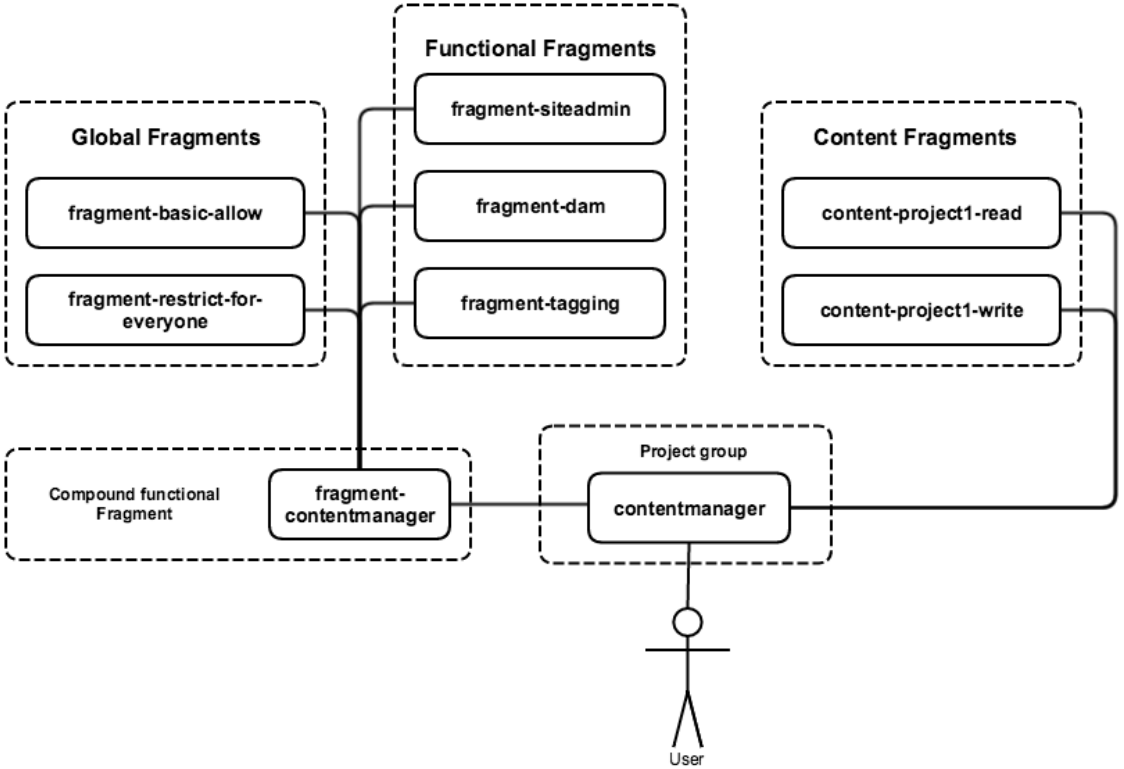
- Dogma: **separation of functional aspects and content**
- Permission specific groups: *fragments*
- Functional fragments
- Content fragments

In addition:

- One fragment-basic-restrict-for-everyone
- One fragment-basic-allow

Best Practises: Fragments

- Desired group permissions through combination of fragments



adaptTo()

Best Practises: Fragments

PROs

- Separation of allow and denies, no mix
- Decreased length of ACLs
- Reusability
- Transparency

CONs

- Increased number of total groups

Links

Links

AC Tool homepage:

https://github.com/Netcentric/accesscontroltool

Netcentric:

https://github.com/Netcentric

http://www.netcentric.biz/

Thank you