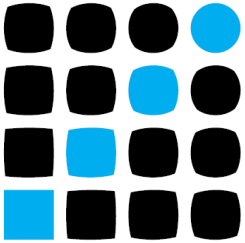


APACHE SLING & FRIENDS TECH MEETUP

BERLIN, 28-30 SEPTEMBER 2015

A case of keys – how to use ACLs effectively

Mateusz Chromiński, Cognifide

Dictionary

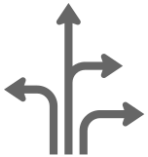
ACE ACL admin Impersonation AuthInfo
Access
Identity Principal Grant Effective Applicable
Deny
Group
Login User Permission Action JAAS

Authorization **Authentication**

System user Membership anonymous Privilege LoginModule
Subject
Allow
Permission store
Permission discovery
Policy
Restriction
Credentials
administrators

What is this talk about?

- ACLs
  - mainly…
- AEM 6.1 is the Oracle
- Examples, solutions, tools

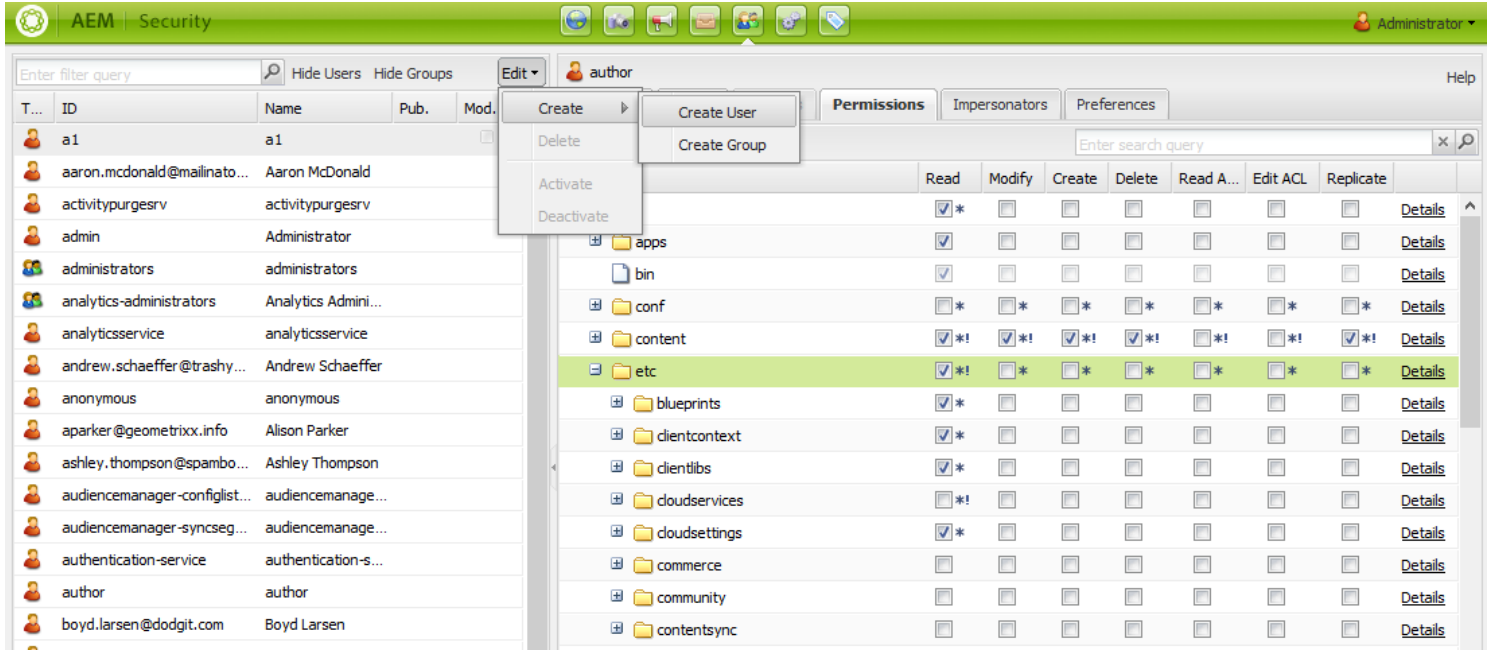


Architecture

JCR

~~Profile~~		Action
AuthenticationInfo		
AuthInfo	Authorizable	Restriction
Credentials		Privilege, Permission
Subject	Principal	Policy

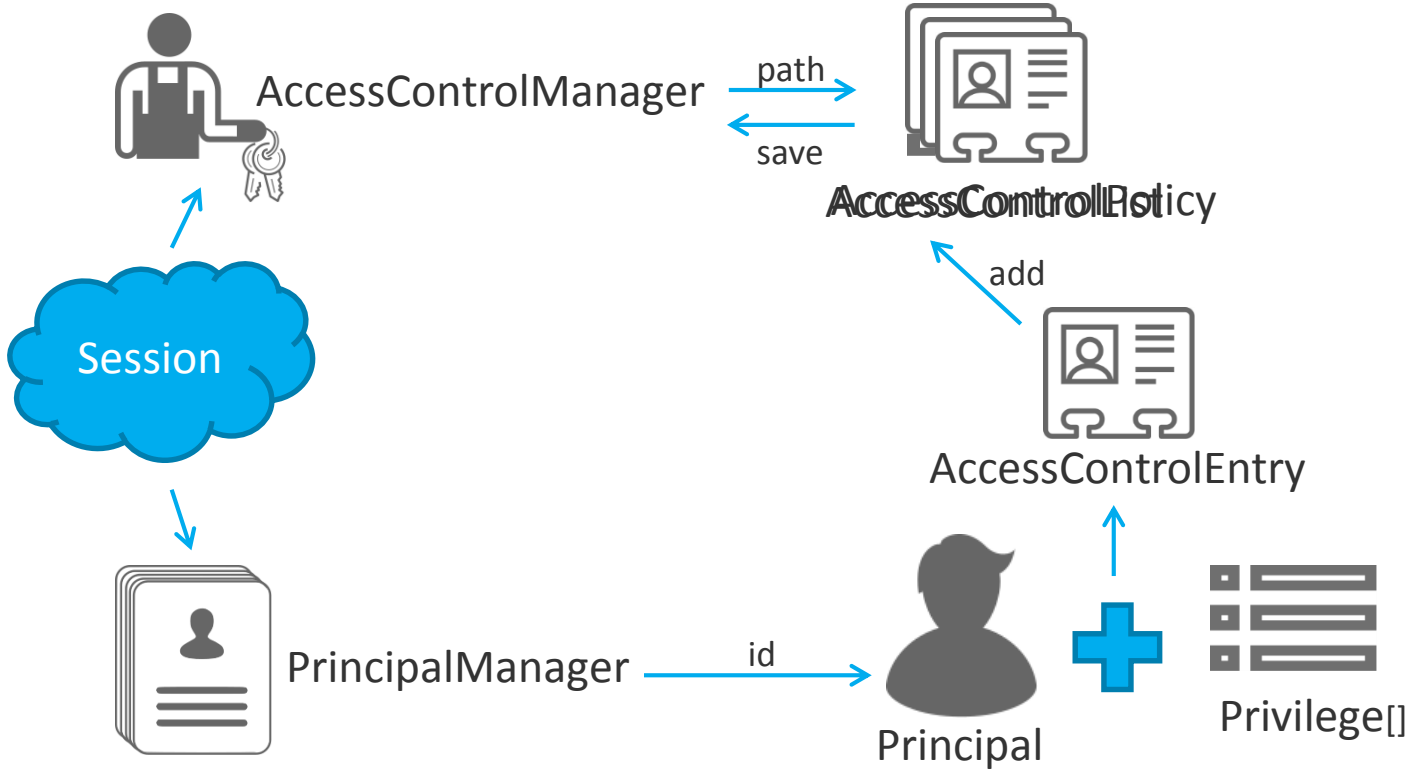
Useradmin console



Open Source tooling

- ACS AEM Commons - **ACL Packager**
  - https://adobe-consulting-services.github.io/acs-aem-commons/features/acl-packager.html
- Citytech's AEM Groovy console
  - https://github.com/Citytechinc/cq-groovy-console
- Netcentric's Access Control Management Tool
  - https://github.com/Netcentric/accesscontroltool

API objects relationship

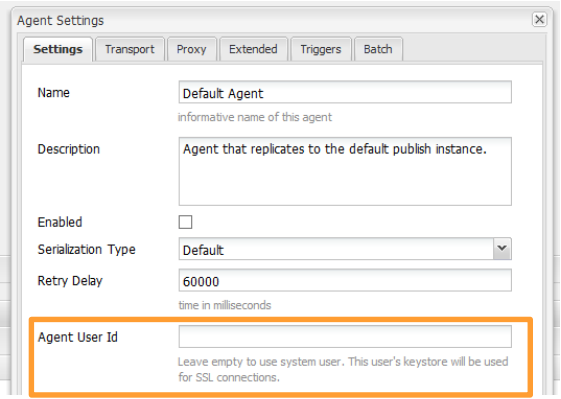


Case 1: Sharded publishes architecture

Requirements

- One author instance
- Multiple, colocated publishes
- Each publish handles a subset of sites

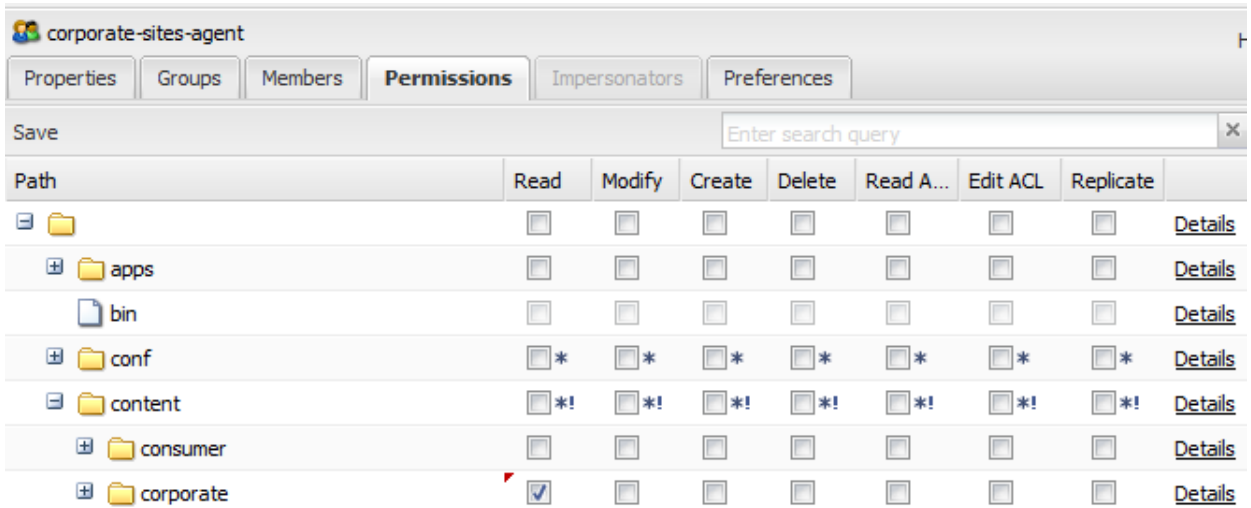
Replication agents



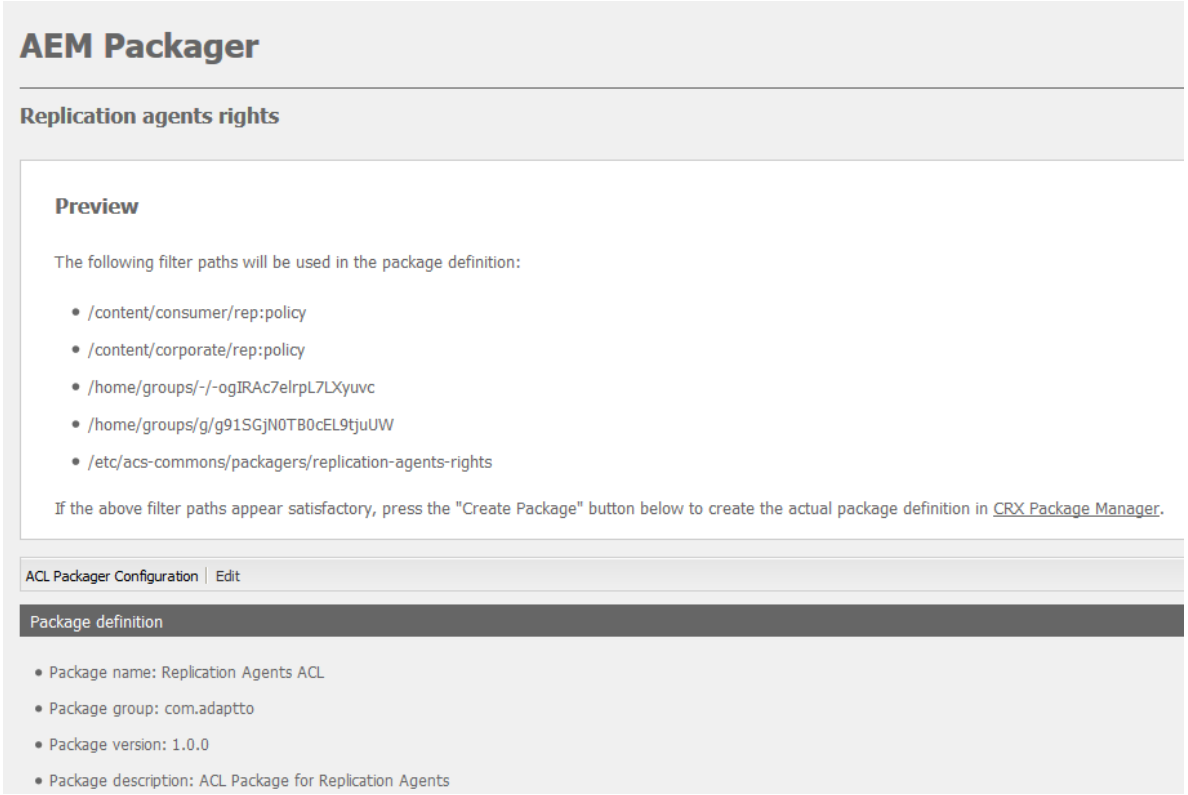
- Agent replicates content that's visible for him
- Agent User Id can be „used as a mechanism for selecting specific content for replication"
  - source: https://docs.adobe.com/docs/en/aem/6-1/deploy/configuring/replication.html

ACL inheritance

- „[…] permissions are inherited throughout the item hierarchy"
  - source: http://jackrabbit.apache.org/oak/docs/security/permission/evaluation.html



ACL Packager



Case 2: Out of AEM reviewers

Requirements

- AEM based users
- Access to documents under a page
- No authoring required
- Rather static content

Solution

```
- group_config:
   - pdf-reviewers:
     - name : Page PDF reviewers
       path : /home/groups/acme
- ace_config:
   - pdf-reviewers:
     - path: /content
       permission: allow
       actions: read
```

https://gist.github.com/mchrominski/15ad7ddcbfd9af7eb94c

Solution - refined

```
- group_config:
   - pdf-reviewers:
     - name : Page PDF reviewers
       path : /home/groups/acme
- ace_config:
   - pdf-reviewers:
     - path: '/content/*//print.pdf'
       permission: allow
       actions: read
```

Better! somehow...

https://gist.github.com/mchrominski/84e7aaa29d754e020a6a

Purging

- rep:policy nodes stored under the content tree
  - `/jcr:root/$path//rep:policy`
- ACL nodes use custom primaryType
  - `SELECT * FROM [rep:ACL] WHERE ISDESCENDANTNODE($path)`
- Permission store
  - `/jcr:system/rep:permissionStore/crx.default`

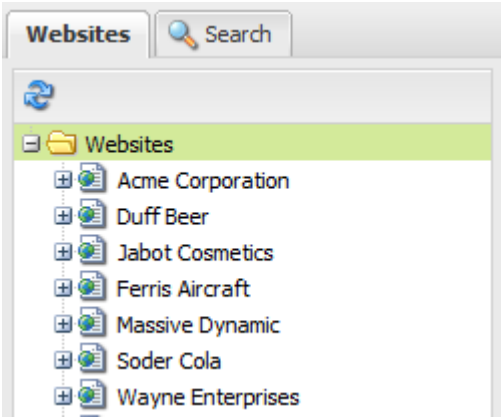
consider applying index

https://gist.github.com/mchrominski/26768994c7026bf9c850

https://gist.github.com/mchrominski/99172f8725972855a757

Case 3: Multi-tenant architecture

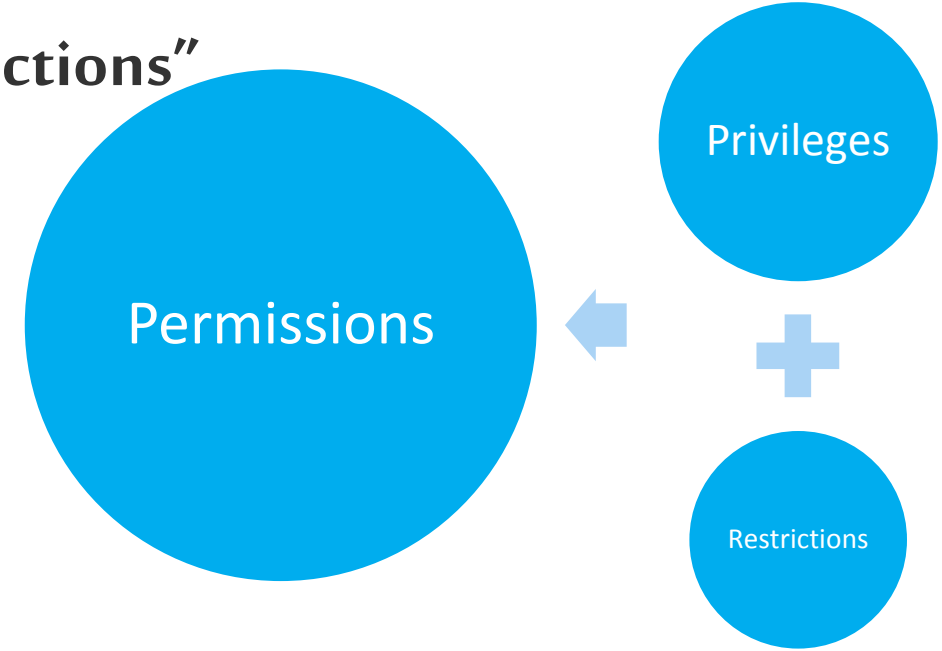
Requirements



- Single instance used by multiple brands
- Brand authors are independent and should work in isolation
- Tenants come and go

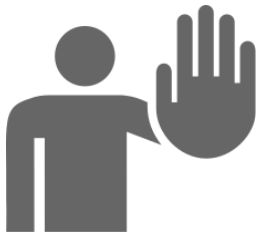
Privilege vs Permission

- „**permissions** encompass [...] **privileges**, but also [...] finer-grained access **restrictions**"
  - **Source:** JSR-283, 16.6.2



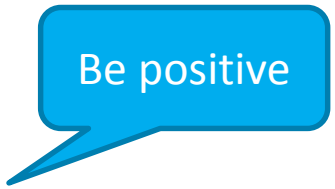
Restrictions

- „Restrictions aim to allow for custom extensions of the default access control implementation to meet project specific need"
  - source: http://jackrabbit.apache.org/oak/docs/security/accesscontrol/restriction.html
- Built-in
  - `rep:ntNames`
  - `rep:prefixes`
  - `rep:glob`



Solution

```
- ace_config:
   - massive-dynamic-authors :
     - path: /content
       permission: allow
       actions: read
     - path: /content
       permission: deny
       actions: read
       repGlob: '/*'
     - path: /content/massive-dynamic
       permission: allow
       actions: read
```



„Always **use Allow** statements to specify the group's rights (wherever possible). Avoid using a Deny statement."
Source: AEM Security Best Practices

https://gist.github.com/mchrominski/7d84e8b2d3bd57d817bc

Mixing deny and allow

- „The individual access control entries are evaluated in strict order"
  - source: http://jackrabbit.apache.org/oak/docs/security/accesscontrol.html
- ACTool does not preserve the order

```
AcHelper.getPathBasedAceMap(aceMapFromConfig, AcHelper.ACE_ORDER_DENY_ALLOW);
```

- Easy to accomplish with AEM Groovy Console

```
def globRestrictions = new HashMap<String, Value>();
globRestrictions.put("rep:glob", valueFactory.createValue("/*"));
acl.addEntry(principal, privileges, false, globRestrictions);
```

Solution - refined

```
- ace_config:
   - massive-dynamic-authors :
     - path: /content
       permission: allow
       actions: read
       repGlob: ''
     - path: /content/massive-dynamic
       permission: allow
       actions: read
       repGlob: ''
     - path: /content/massive-dynamic
       permission: allow
       actions: read
```

https://gist.github.com/mchrominski/8e8e640c185ae86af3f8

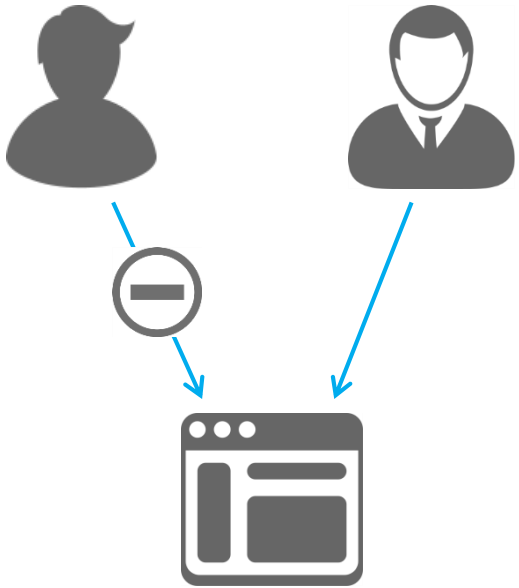
Nodetype info access issue

- Permission evaluation process calls `Node.getPrimaryType()`
- Compatibility issue wrt OAK:
  - JCR2 returned proper node type
  - OAK requires access to **jcr:primaryType** property
- Remember to maintain access to jcr:primaryType

```
path: '/path/to/node'
repGlob: '/jcr:primaryType'
```

Case 4: Limiting superuser options

Requirements

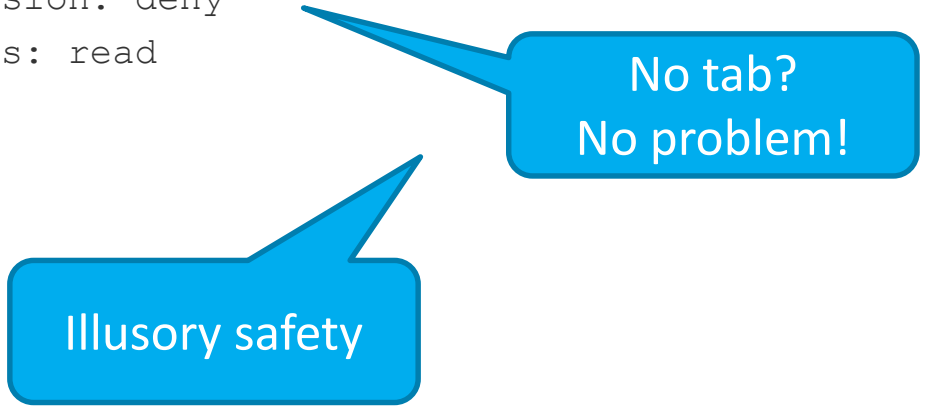


- A page dialog is customized to provide the ability to manage the HTML
- Only a superuser can edit aforementioned dialog tab

Dialog access limiting

- Limit the access to a single tab

```
- acme-corporate-authors:
  - path: /apps/acme/core/components/page/dialog/items/tabs/items/headTab
    permission: deny
    actions: read
```



Safe solution

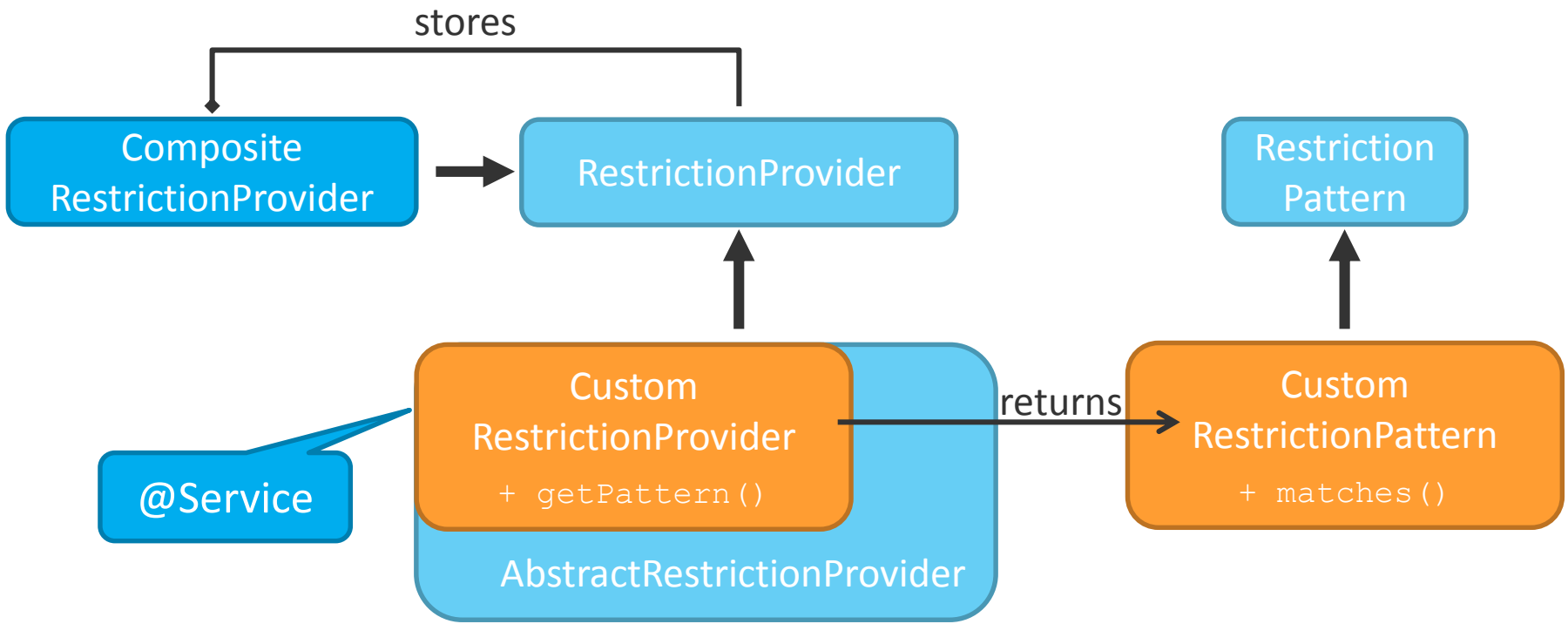
- Use prefixes restriction

```
def restrictions = new HashMap<String, Value>()
def values = new Value[1]
values[0] = session.getValueFactory().createValue("su")
restrictions.put("rep:prefixes", values)
acl.addEntry(principal, privileges, false, emptyMap, restrictions)
```

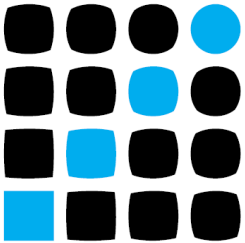
- Store data under properties with selected namespace

https://gist.github.com/mchrominski/84b887223d6d35806cd2

Custom restriction implementation



https://gist.github.com/mchrominski/8ad8975d916ac24dca25



adaptTo()

APACHE SLING & FRIENDS TECH MEETUP

BERLIN, 28-30 SEPTEMBER 2015

Thank you

mateusz.chrominski@cognifide.com