



adaptTo()

APACHE SLING & FRIENDS TECH MEETUP

BERLIN, 28-30 SEPTEMBER 2015

A case of keys – how to use ACLs effectively
Mateusz Chromiński, Cognifide



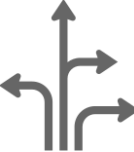
ACE ACL admin Impersonation AuthInfo
Identity Principal Grant Access Effective Applicable
Login User Group Deny Permission Action JAAS

Authorization

Authentication

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

What is this talk about?

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



	Profile	Action
--	---------	--------



AuthenticationInfo		
--------------------	--	--



AuthInfo	Authorizable	Restriction
----------	--------------	-------------

JCR

Credentials		Privilege, Permission
-------------	--	-----------------------



Subject	Principal	Policy
---------	-----------	--------



AEM | Security Administrator

Enter filter query Hide Users Hide Groups Edit author

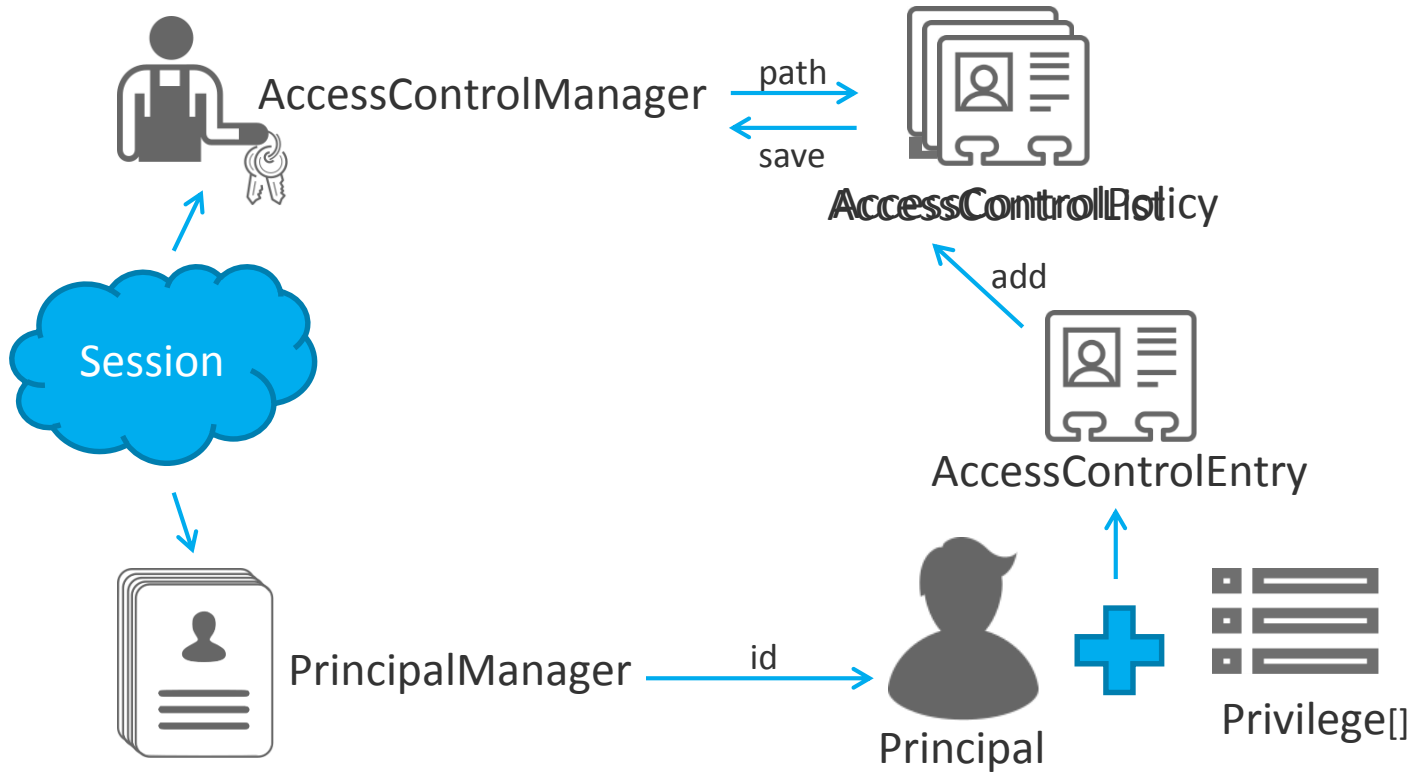
Create User Create Group

T...	ID	Name	Pub.	Mod.	Permissions	Impersonators	Preferences	Help
	a1	a1						
	aaron.mcdonald@mailinato...	Aaron McDonald						
	activitypursesrv	activitypursesrv			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	admin	Administrator			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	administrators	administrators			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	analytics-administrators	Analytics Admini...			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	analyticsservice	analyticsservice			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	andrew.schaeffer@trashy...	Andrew Schaeffer			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	anonymous	anonymous			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	aparker@geometrix.info	Alison Parker			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	ashley.thompson@spambo...	Ashley Thompson			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	audiencemanager-configlist...	audiencemange...			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	audiencemanager-syncseg...	audiencemange...			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	authentication-service	authentication-s...			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	author	author			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	boyd.larsen@dodgit.com	Boyd Larsen			<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Read	Modify	Create	Delete	Read A...	Edit ACL	Replicate	Details
apps	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
bin	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
conf	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	Details
content	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	<input type="checkbox"/> *!	<input type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	Details
etc	<input checked="" type="checkbox"/> *!	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	<input type="checkbox"/> *	Details
blueprints	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
clientcontext	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
clientlibs	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
cloudservices	<input type="checkbox"/> *!	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
cloudsettings	<input checked="" type="checkbox"/> *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
commerce	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
community	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
contentsync	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details

- **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>

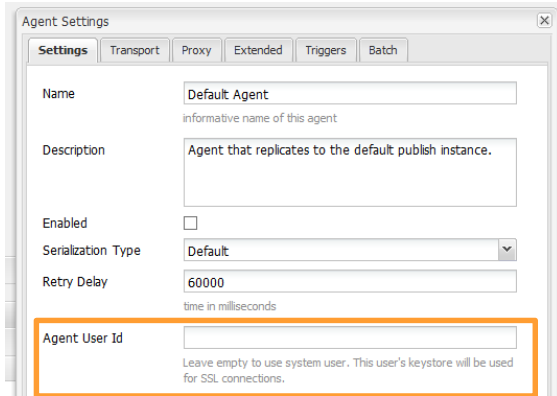
API objects relationship



Case 1: Sharded publishes architecture



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



Agent Settings

Settings Transport Proxy Extended Triggers Batch

Name: Default Agent
informative name of this agent

Description: Agent that replicates to the default publish instance.

Enabled:

Serialization Type: Default

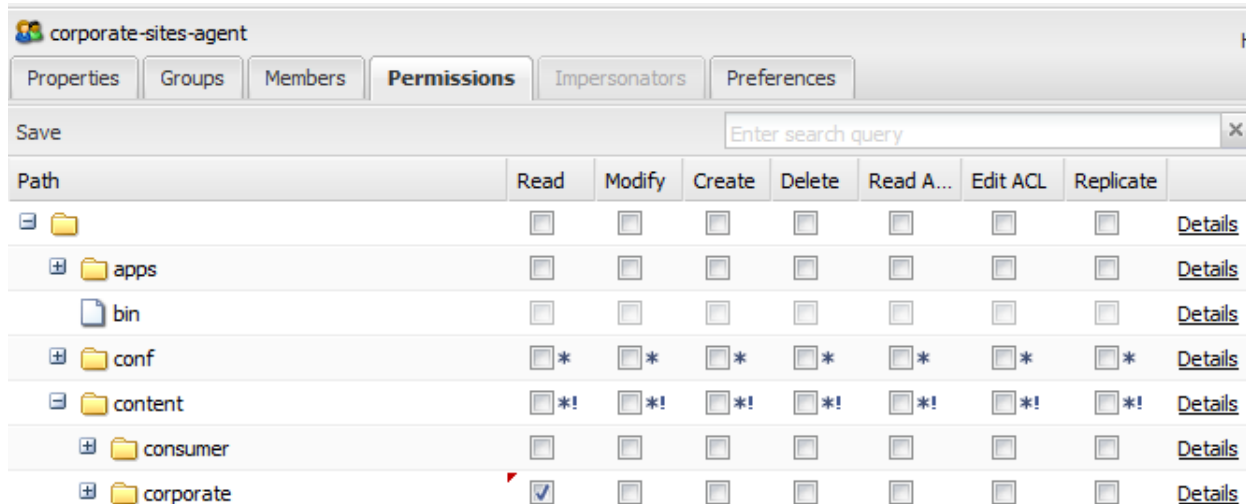
Retry Delay: 60000
time in milliseconds

Agent User Id:
Leave empty to use system user. This user's keystore will be used for SSL connections.



- 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>

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



Path	Read	Modify	Create	Delete	Read A...	Edit ACL	Replicate	
📁	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
📁 apps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
📄 bin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
📁 conf	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	<input checked="" type="checkbox"/> *	Details
📁 content	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	<input checked="" type="checkbox"/> *!	Details
📁 consumer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details
📁 corporate	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Details

AEM Packager

Replication agents rights

Preview

The following filter paths will be used in the package definition:

- /content/consumer/rep:policy
- /content/corporate/rep:policy
- /home/groups/-/-ogIRAc7elrpL7LYyuv
- /home/groups/g/g91SGjN0TB0cEL9tjuUW
- /etc/acs-commons/packagers/replication-agents-rights

If the above filter paths appear satisfactory, press the "Create Package" button below to create the actual package definition in [CRX Package Manager](#).

ACL Packager Configuration | Edit

Package definition

- Package name: Replication Agents ACL
- Package group: com.adaptto
- Package version: 1.0.0
- Package description: ACL Package for Replication Agents

Case 2: Out of AEM reviewers



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

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

A blue speech bubble with a white border and a tail pointing to the left. Inside the bubble, the word "YAML" is written in white, uppercase, sans-serif font.

YAML

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

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

A blue speech bubble with a white border and a tail pointing to the left, containing the text "Better! somehow...".

Better!
somehow...

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

- rep:policy nodes stored under the content tree

- `/jcr:root/$path//rep:policy`

consider applying
index

- ACL nodes use custom primaryType

- `SELECT * FROM [rep:ACL] WHERE ISDESCENDANTNODE($path)`

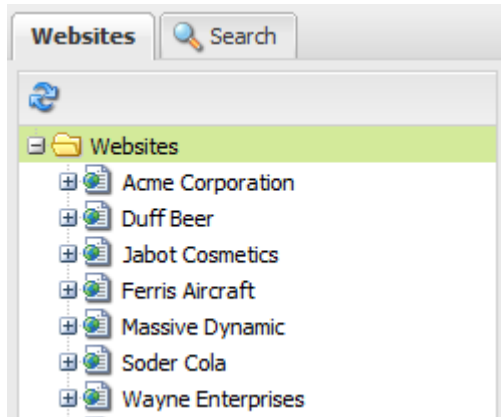
- Permission store

- `/jcr:system/rep:permissionStore/crx.default`

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

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

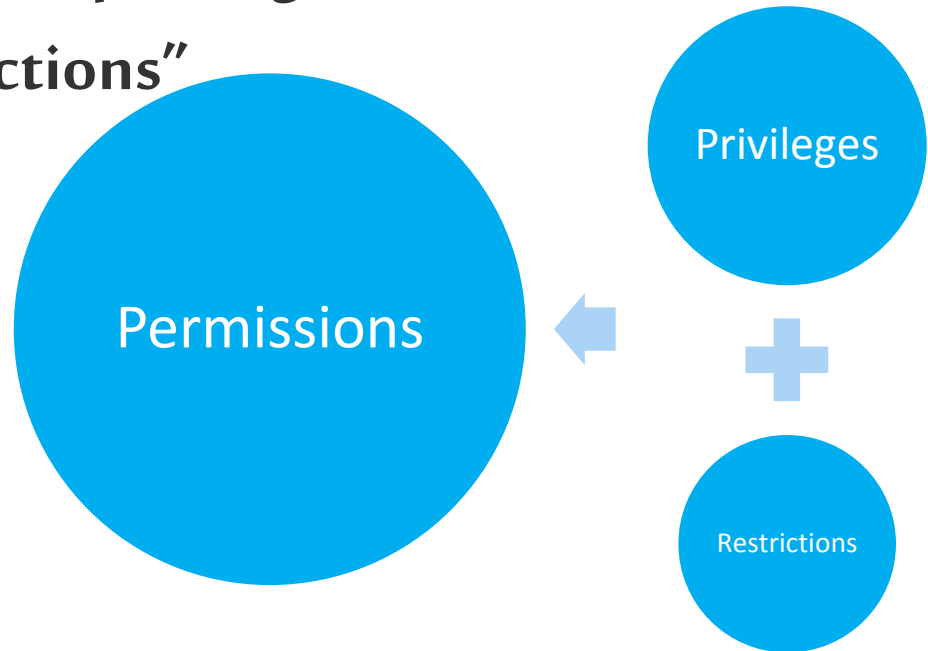
Case 3: Multi-tenant architecture



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

- „**permissions** encompass [...] **privileges**, but also [...] finer-grained access **restrictions**”

- Source: JSR-283, 16.6.2

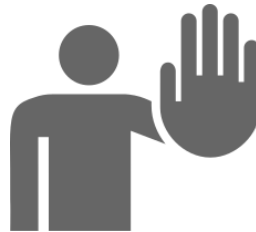


- „Restrictions aim to allow for custom extensions of the default access control implementation to meet project specific need“

- source: <http://jackrabbit.apache.org/oak/docs/security/accesscontrol/restriction.html>

- ## Built-in

- `rep:ntNames`
- `rep:prefixes`
- `rep:glob`



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

A blue speech bubble with a white border and a tail pointing towards the 'deny' permission in the code block above.

Be positive

„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>

- „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);
```

- 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

A blue speech bubble with a white border and a tail pointing towards the 'repGlob: ''' line in the code. The text inside the bubble is 'STRICT repGlob' in white, bold, sans-serif font.

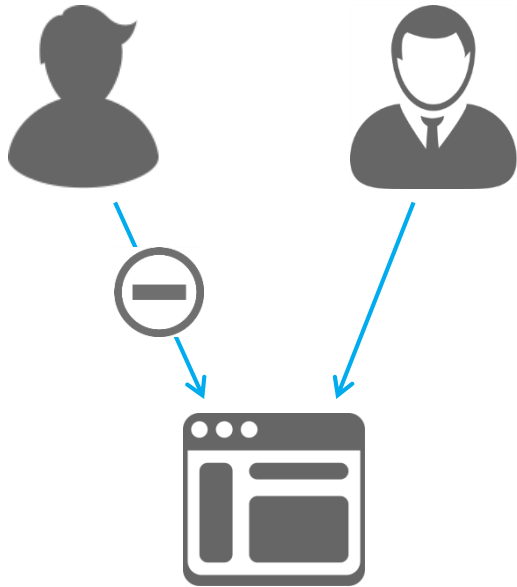
STRICT repGlob

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

- 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



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

- 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

Illusory safety

No tab?
No problem!

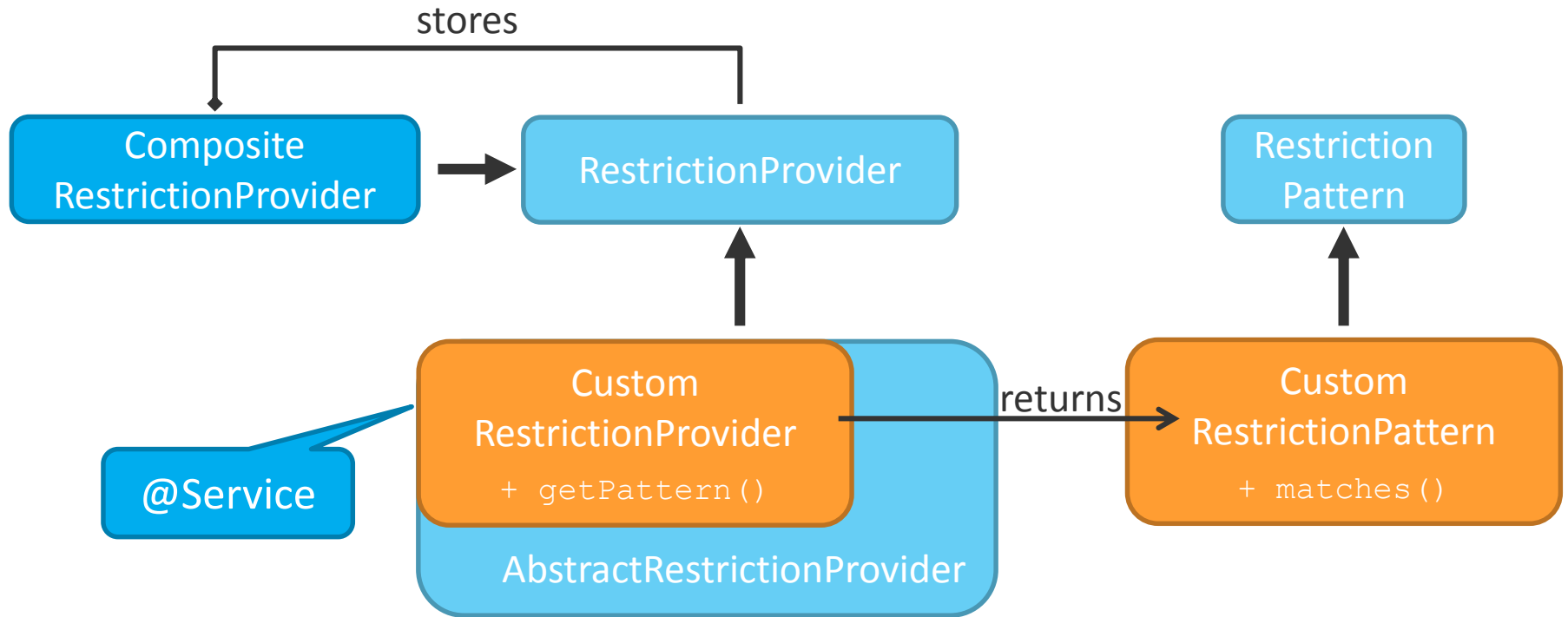
- Use prefixes restriction

```
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)
```

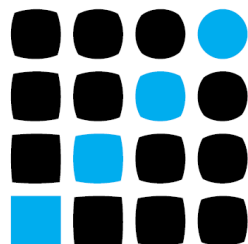
- Store data under properties with selected namespace

<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