# Esta Tekton Openshift Rollenkonzept

### Openshift Rollen Berechtigungsmatrix

Für Openshift braucht es ein Rollenkonzept was für User mit welcher Rolle welche Ressourcen editieren, anlegen, löschen, einsehen können.

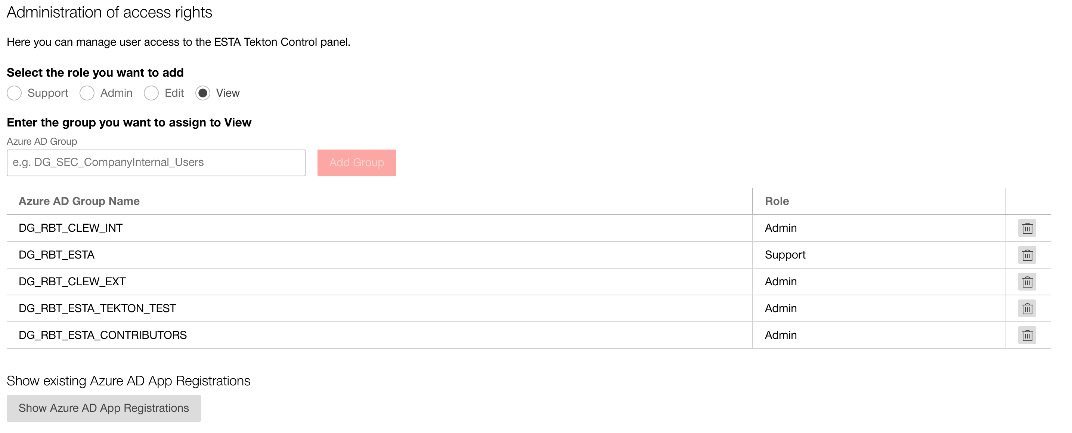
R = Read, W = Write, D = Delete

|  |  |  |  |
| --- | --- | --- | --- |
| **Ressource** | **Rolle-Admin** | **Rolle-Write** | **Rolle-View** |
| Deployment | R | R | R |
| Pod | R,W,D | R | R |
| ConfigMap | R,W,D | R | R |
| PVC | R,W,D | R | R |
| Secret | - | - | - |
| Task | R,W,D | R | R |
| TaskRun | R,W,D | R,W,D | R |
| Pipeline | R,W,D | R | R |
| PipelineRun | R,W,D | R,W,D | R |
| Template | R,W,D | R | R |
| Roles | R | R | R |
| RoleBindings | R | R | R |

Nach Absprache mit [Gerber Jürg (IT-PTR-CEN2-BDE16)](file:///C:\display\~u229412)  würden wir ~~3~~ 2 Cluster Rollen erfassen welche die entsprechenden Berechtigungen aus der Matrix oben abbilden. Für die Rolle "View" kann die existierende "view" ClusteRole verwendet werden. Die Berechtigungen sind dann Namespace Scoped.

### Mapping RBT Gruppen nach Esta-Tekton Rollen, nach Openshift Rolebindings

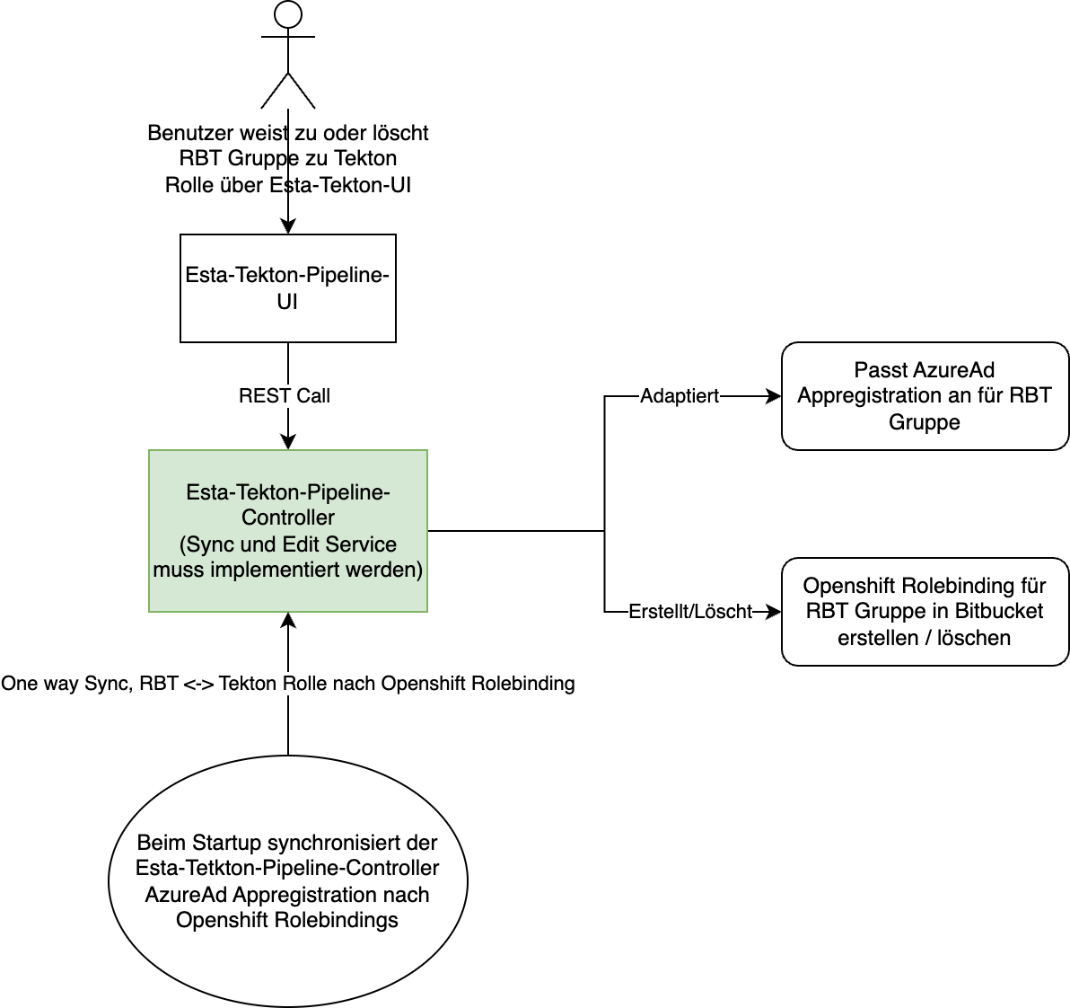
Im Esta-Tekton-UI können RBT Gruppen den verschiedenen Rollen zugewiesen werden:



Während die RBT Gruppen auf Rollen im AzureAd gemappt werden, sollen gleichzeitig durch den Controller durch einen AppRegistrationRoleBindingSyncer die RoleBindings im Bitbucket Repo angelegt werden. Worauf dann ArgoCD die Rolebindings nach Openshift synchronisiert.

Damit die Openshift Rolebindings auf RBT Gruppen gemacht werden können, muss diese Story abgeschlossen sein: [CON-7974](https://flow.sbb.ch/browse/CON-7974) - LDAP/AD Groups in OpenShift Closed

Gemäss Openshiftbug-Report: <https://access.redhat.com/support/cases/#/case/03256619> sollte der Bugfix in Openshift 4.11 geliefert werden. Das heisst sobald auf aws01t Openshift 4.11 installiert ist, kann die Lösung implementiert werden.



### RoleBindings für AD Gruppen in OpenShift anlegen

Für die 3 Tekton Rollen sind die folgenden ClusterRoles verfübgar:

* Admin: sbb-esta-tekton-admin
* Write: sbb-esta-tekton-edit
* View: view

Mit diesen können nur RoleBindings im jeweiligen Tekton Namespace für User oder Gruppe angelegt werden:

**esta-tekton-admin-dg-rbt-esta-test.yaml**

kind: RoleBinding

apiVersion: rbac.authorization.k8s.io/v1

metadata:

name: esta-tekton-admin-dg-rbt-esta-test

namespace: esta-tekton-dev

subjects:

- kind: Group

apiGroup: rbac.authorization.k8s.io

name: DG\_RBT\_ESTA\_TEKTON\_TEST

roleRef:

apiGroup: rbac.authorization.k8s.io

kind: ClusterRole

name: sbb-esta-tekton-admin

Gut zu wissen: Gruppen sind ein Konstrukt von Openshift und kein Kubernetes Feature. Man kann RoleBindings für ein Subject von kind:Group mit einem beliebigen Name erstellen, auch wenn es (noch) keine Gruppe mit diesem Namen gibt. Der AD Group Sync funktioniert so, dass beim Login eines Users alle Gruppen, in denen dieser Mitglied ist angelegt resp. aktualisiert werden.