# Sicherer Admin Zugang zu OpenShift (OKD) und anderen Diensten

Peter Pfläging <peter@pflaeging.net>

## Worum geht es?

In IT Organisationen gibt zwei Sicherheitsvorgaben, die sinnvoll und unbedingt einzuhalten sind, sich aber teilweise widersprechen:

- Jeder Benutzer soll nur ein einziges Mal als Identity existieren. Jegliche Doppelidentitäten sind zu vermeiden um zumindest Folgendes garantieren zu können:
  - eindeutige Identifikation jedes Benutzers und Rückführbarkeit auf EIN Benutzerprofil
  - die Möglichkeit ein Benutzer schnell außer Kraft zu setzen
  - Nachvollziehbarkeit für Audit Zwecke

- Sollte ein Benutzer mit Administrationsrechten arbeiten, so sollte diese Rolle explizit und separierbar von dem “normalen” Arbeitsprofil sein.
  - Das Arbeiten mit “Sammel-Admins” ist auf jeden Fall zu vermeiden (mangelnde Nachvollziehbarkeit, Sammelaccounts und Shared Secrets!)
  - Ein permanentes Arbeiten mit Admin Rechten kann auf der anderen Seite extrem gefährlich sein.
  - Es ist schwer festzustellen, wie Services für “normale” Benutzer aussehen, da immer mit erweiterten Berechtigungen gearbeitet wird.

## Lösungsansatz

Es werden über ein Securityportal (SAML2 oder OpenID Connect) unterschiedliche Rollen implementiert, die aber immer auf eine User Datenbank verweisen.
Dabei werden für die unterschiedlichen Rollen entweder andere Attributsätze für den gleichen Benutzer implementiert oder es wird ein Applikationsbenutzer für die Rolle generiert, der nur in diesem Kontext gilt und explizit gekennzeichnet ist (z.B. “meinusername.admin”).

## Beispiellösung

Beispielhaft wurd das oben beschriebene Konzept implementiert für OpenShift oder OKD im Zusammenspiel mit KeyCloak (SAML & OpenID Connect Portal).
Login in die OpenShift Konsole mit 2 unterschiedlichen Rollen:

- Developer: dies ist die Standardrolle. Jeder Benutzer kann einsteigen und bekommt durch die Cluster Administration Berechtigungen in Projekten zugeordnet. Standardmäßig ist kein explizites Recht vergeben (man sieht einen netten Begrüßungsschirm).
  - der Standardbenutzername “meinusername” wird automatisch angelegt, wenn er noch nicht vorhanden ist.
  - die Standard Policies und Berechtigungen sind aktiv. D.h. der Benutzer bekommt nur die Projekte zu sehen, für die er explizit berechtigt ist.

- Administrator: Dies ist der Zugang für Administratoren. Es sind zwar alle Personen berechtigt, allerdings wird der Benutzername auf meinusername.admin umgeschrieben und es wird der Benutzer / die Benutzerin nicht automatisch angelegt wie im Fall “Developer”. Die entsprechenden Berechtigungen / Benutzer / Identitäten müssen daher vorher in OpenShift definiert werden.
  - Es wird kein Benutzer automatisch angelegt.
  - Berechtigungen werden explizit im OpenShift gesetzt.
  - Gruppenzuordnungen sind im OpenShift (damit ist es nicht möglich, dass ein Benutzer, der AD Gruppen administriert, auch Zugriff auf die OpenShift Console bekommt)

- Es ist ohne weiteres möglich zusätzliche Absicherungsmassnahmen wie OTP (One Time Password) explizit nur für diese Rolle zu implementieren.