



# Braucht Stud.IP ein granulares Rechtesystem?

Stud.IP-Tagung 2021

Peter Thienel, data-quest GmbH

# Was heißt hier eigentlich granular?

- » Ein Rechtesystem verwaltet Zugriffsrecht:
  - » WER (z.B. Nutzer\*in)
  - » darf WAS (Erstellen, Lesen, Verändern, Löschen)
  - » WOFÜR (z.B. Dateiordner, Einrichtung)
  - » (in einem bestimmten Kontext)
  - » (zu einer bestimmten Zeit)
  - » usw.

# Globale Rollen

- » user, autor, tutor, dozent, admin, root
- » root darf (fast) ALLES ÜBERALL!
- » Rolle user nur sinnvoll bei Selbstregistrierung

	autor	tutor	dozent	admin	root
 Einrichtung	suchen	suchen	suchen	suchen	verwalten
 Veranstaltung	eintragen	eintragen	eintragen	suchen	verwalten
 Benutzer*in	suchen	suchen	suchen	suchen (verwalten)	verwalten
 Ankündigung	Profil	Profil	Profil	Profil	Startseite Einrichtungen Veranstaltungen Profile
 Umfrage	Profil	Profil	Profil	Profil	Startseite Einrichtungen Veranstaltungen

# Lokale Rollen

- » Lokale (objektbezogene) Rollen
  - » user, autor, tutor, dozent, admin
  - » Einrichtungen und Veranstaltungen als Rahmen
  - » root darf ALLES!
  - » root muss admins zu Einrichtungen zuordnen

	 Einrichtung	 Veranstaltung
<b>user</b>	studiert an	nur lesen
<b>autor</b>	arbeitet an, eigene Einrichtungsdaten bearbeiten	teilnehmen
<b>tutor</b>	arbeitet an (kein Unterschied zu autor), eigene Einrichtungsdaten bearbeiten	verwalten, (keine Tutor*innen/Lehrende zuordnen)
<b>dozent</b>	arbeitet an, Veranstaltung anlegen, eigene Einrichtungsdaten bearbeiten	verwalten
<b>admin</b>	verwalten	verwalten

# Rollenverwaltung (Systemrollen)

- » Verwaltung durch root
- » Zuordnung zu Systemrolle implizit durch globale Rolle (Nutzer\*innen können nicht explizit zugeordnet werden)
- » Einer Systemrolle sind oft mehrere globale Rollen zugeordnet
- » Systemrollen können nicht gelöscht oder angelegt werden
- » Plugins werden für die zugeordnete Systemrolle geladen
- » Es fehlt die Systemrolle für user

Systemrolle	Globale Nutzerrolle
Administrator(in)	admin
Lehrende(r)	dozent
Mitarbeiter(in)	admin, root
Nobody	-
Root-Administrator(in)	root
Studierende(r)	autor, tutor
Tutor(in)	tutor

# Rollenverwaltung (Pluginrollen)

- » Verwaltung durch root
- » Verwendung in Plugins (außer MVV)
- » Löschen und Anlegen über Oberfläche möglich
- » Plugins sollten ihre benötigten Rollen bei Installation anlegen
- » Keine implizite Zuordnung von Nutzer\*innen über globale Rollen
- » Explizite Zuordnung von Nutzer\*innen unabhängig von globaler Rolle
- » Berechtigungen werden ausschließlich im Plugin definiert

## Vorhandene Rollen

Name	Benutzer		Plugins
	explizit	implizit	
Administrator(in) [Systemrolle]	0	1	23
DedicatedAdmin	0	0	0 
Evaluationsteam	2	0	0 
Lehrende(r) [Systemrolle]	0	3	23
Mitarbeiter(in) [Systemrolle]	0	2	23
MVVAdmin	0	0	0 
MVVEntwickler	1	0	0 
MVVFreigabe	0	0	0 
MVVLvGruppenAdmin	0	0	0 
MVVRedakteur	0	0	0 
MVVTranslator	0	0	0 
Nobody [Systemrolle]	0	0	7
Root-Administrator(in) [Systemrolle]	0	1	23
Studierende(r) [Systemrolle]	0	4	23

# Freie Datenfelder

- » Verwaltung durch root
- » Sichtbar nur ab angegebener globaler Rolle
- » Bearbeitbar nur ab angegebener globaler Rolle
- » Eventuell nur für bestimmte globale Rollen verfügbar
- » Verfügbarkeit nach Einrichtung konfigurierbar

## Verwaltung von generischen Datenfeldern

Name	Feldtyp	Typ ⓘ	Institution	benötigter Status	
				Änderbar ⓘ	Öffentlich ⓘ
▼ Datenfelder für Veranstaltungen					
zugeordnete Planungsfarbe	textline	alle		admin	root
zugeordnete Planungsspalte	textline	alle		admin	root
▶ Datenfelder für Einrichtungen					
▼ Datenfelder für Benutzer					
Matrikelnummer	textline	user, autor, tutor		user	dozent
Datenfelder für Benutzerrollen in Einrichtungen					
▶ Datenfelder für Benutzer-Zusatzangaben in VA					
Datenfelder für Rollen in Einrichtungen					
Datenfelder für Moduldeskriptoren					
Datenfelder für Modulteildeskriptoren					
Datenfelder für Studiengänge					

# Sperrebenen

- » Verwaltung durch root
- » Konfigurierbar für Veranstaltungen, Einrichtungen und Nutzer\*innen
- » Steuern Zugriff auf einzelne Felder oder Funktionen des Objekts
- » Felder sind erst ab angegebener globaler Rolle bearbeitbar
- » Jeweils *eine* Sperrebene kann einem Objekt zugewiesen werden
- » Sperren von importierten Daten

## Grunddaten

	gesperrt	nicht gesperrt
Veranstaltungsnummer	<input type="radio"/>	<input checked="" type="radio"/>
beteiligte Einrichtungen	<input type="radio"/>	<input checked="" type="radio"/>
Name	<input type="radio"/>	<input checked="" type="radio"/>
Untertitel	<input type="radio"/>	<input checked="" type="radio"/>
Status	<input type="radio"/>	<input checked="" type="radio"/>
Beschreibung	<input type="radio"/>	<input checked="" type="radio"/>
Ort	<input type="radio"/>	<input checked="" type="radio"/>
Veranstaltungstyp	<input type="radio"/>	<input checked="" type="radio"/>
ECTS-Punkte	<input type="radio"/>	<input checked="" type="radio"/>
Teilnehmendenzahl	<input type="radio"/>	<input checked="" type="radio"/>

# Globale Konfiguration

- » Verwaltung durch root (oder Server-Admin)
- » Konfigurierbar über Oberfläche oder in Konfigurationsdateien
- » Steuern Verfügbarkeit von Funktionen oder Zugriff auf einzelne Felder
- » Können von globaler Rolle abhängen

permissions (19)			
<b>ALLOW_ADMIN_USERACCESS</b> Wenn eingeschaltet, dürfen Administratoren sensible persönliche Angaben wie z.B. Passwörter ändern.	✓	boolean	
<b>ALLOW_CHANGE_EMAIL</b> If true, users are allowed to change their email	✓	boolean	
<b>ALLOW_CHANGE_NAME</b> If true, users are allowed to change their name	✓	boolean	
<b>ALLOW_CHANGE_TITLE</b> If true, users are allowed to change their titles	✓	boolean	
<b>ALLOW_CHANGE_USERNAME</b> If true, users are allowed to change their username	✓	boolean	
<b>ALLOW_DOZENT_DELETE</b> Schaltet ein oder aus, ob ein Dozent eigene Veranstaltungen selbst löschen darf oder nicht	✗	boolean	

# Was noch?

- » Lokale Rechte an bestimmten Objekten
- » Dateiordnerberechtigungen
- » Lese-/Schreibrecht Wiki
- » Gruppenrechte an Ordnern
- » Rechte an Räumen/Ressourcen
- » Privacy-Einstellungen

 Zeitgesteuerter Ordner 

Sichtbar ab  
unbegrenzt 

Sichtbar bis  
unbegrenzt 

r - Lesen (Dateien können heruntergeladen werden)

w - Schreiben (Dateien können hochgeladen werden)

## Seiten-Einstellungen ändern

Standard Wiki-Einstellungen verwenden

### Leseberechtigung

- Alle in der Veranstaltung
- Lehrende und Tutor/innen

### Editierberechtigung

- Alle in der Veranstaltung
- Lehrende und Tutor/innen

# Rechteverwaltung in MVV

- » MVV => Modularisiertes  
Veranstaltungs-Verzeichnis  
(Modulkatalog)
- » Integration aller Objekte zur  
Verwaltung und Darstellung im  
Kern
- » Anforderungen:
  - » Planung: Module und  
Studiengänge  
(Status/Sichtbarkeit)
  - » Versionierung

Geschichte 80 CP Studiengangteil in Bachelor-  
Studiengängen

Geschichte 80 CP Studiengangteil in Bachelor-Studiengängen, 22.  
Änderungsfassung gültig ab WiSe 2017/18

Name / CP	Modul	Modulteil	Semester					
			1	2	3	4	5	6
Grundlagenmodule 27.00 CP	 04-Geschichte- BA-01 - Grundlagenmodul – Alte Geschichte, gültig ab WiSe 2013/14	LV 2: Proseminar	+	o				
		LV 1: Vorlesung	+	o				
		LV 2: Proseminar	o	+				
	 04-Geschichte- BA-02 - Grundlagenmodul – Mittelalterliche Geschichte, gültig ab WiSe 2013/14	LV 1: Vorlesung	+	o				
		LV 3: Übung	+	o				
		LV 2: Proseminar	o	+				
	 04-Geschichte- BA-03 - Grundlagenmodul – Neuere Geschichte, gültig ab WiSe 2013/14	LV 3: Übung	+	o				
		LV 1: Vorlesung	+	o				
		LV 2: Proseminar	o	+				
	 04-Geschichte- BA-04 -	LV 1: Übung			+	o		





**Vielen Dank für Ihre  
Aufmerksamkeit!**

