5. Aufgabenblatt

(Entwufsbeschreibung OLAT mit Fokus auf Rollen- und Rechtemanagment)

1. Allgemeines

Die Zuweisung von Zugriffsrechten innerhalb von OLAT erfolgt durch Zuordnung von Rollen an die einzelnen Benutzer. Jede Rolle bringt also entsprechende Rechte mit sich. Möglich sind innerhalb von OLAT folgende Rollen:

- Gast (anonymer Nutzer)
- Benutzer
- Autor
- Benutzerverwalter
- Gruppenverwalter
- Systemadministrator

Gast:
Jeder Nutzer von OLAT, der sich nicht registriert hat, bekommt automatisch diese Rolle zugewiesen. Ein Gast kann nur auf diejenigen Ressourcen zugreifen, die explizit für Gäste freigegeben worden sind. Die Gastrolle ist also hauptsächlich dazu gedacht, einem Besucher die Möglichkeit zu geben, einen Überblick über die Funktionsweise von OLAT zu gewinnen. Nutzen kann ein Gast diese Funktionen allerdings nicht.

Benutzer:
Wer sich bei OLAT erfolgreich registriert, bekommt automatisch die Rolle "Benutzer" zugewiesen. Die Mehrheit der Nutzer von OLAT wird diese Rolle einnehmen, sie stellt also gewissermaßen die "Basisrolle" dar. Als Benutzer steht einem der volle Umfang an Funktionen, die nur die eigene Person betreffen und die Möglichkeiten von anderen Nutzern nicht beeinflussen, zur Verfügung. Ein Gast kann z.B. seinen eigenen Terminkalender bearbeiten, Notizen erstellen, Arbeitsgruppen erstellen (mehr dazu später), Dateien in seinen persönlichen Ordner hochladen, usw. . Nutzer mit mehr Zugriffsrechten als ein normaler Benutzer müssen sich außerdem zuerst als normaler Nutzer anmelden und bekommen dann erst von einem Administrator die neue Rolle zugewiesen.

Autor:
Zusätzlich zu den Rechten eines normalen Nutzers kann ein Autor auch Lerngruppen erstellen. Der Autor kann dann Nutzer zu diesen Gruppen hinzufügen bzw. kann die Benutzer sich selbst hinzufügen lassen. Der Autor kann auch Benutzer wieder aus den Gruppen entfernen. Außerdem kann ein Autor weitere Nutzer als Betreuer für eine Gruppe festlegen. Eine typische Nutzung für eine solche Lerngruppe wären Seminargruppen, wie sie an jeder Universität existieren. Die Leiter der Seminare können dann als Betreuer für die Gruppen fungieren. Und schließlich kann ein Autor neue Lernressourcen erstellen und verwalten. Zu Lernressourcen zählen beispielsweise Kurse, Tests, Fragebögen, Wikis, Glossare, Ressourcenordner und SCORM Lerninhalte.

Benutzerverwalter:
Ein Nutzer mit der Rolle Benutzerverwalter kann nach Benutzer suchen, Einstellungen und Angaben von Benutzern einsehen und ändern, neue Benutzer erstellen und importieren und existierenden Benutzern Rechte und Rollen zuordnen.

Gruppenverwalter:
Ein Nutzer mit der Rolle Gruppenverwalter kann kursübergreifende Gruppen erstellen und verwalten und diese Gruppen mit Kursen verknüpfen. Gruppen, die nicht kursübergreifend sind, können allerdings auch ohne diese Rolle vewaltet werden.

Systemadministrator:
Ein Nutzer mit der Rolle Systemadministrator kann sämtliche verfügbaren technischen Einstellungen verändern und hat außerdem automatisch das Benutzerverwaltungs- und Gruppenverwaltungsrecht. Sie verfügen in jedem Kurs bzw jeder Lernressource die gleichen

Rechte wie die zuständigen Kursadministratoren. Außerdem haben sie teilweise erweiterte Suchformulare zur Verfügung. Hier eine Auswahl der Optionen, die dem Administrator zur Verfügung stehen:
- Auflistung aller momentan eingeloggten Benutzer
- Absenden einer Information für alle Benutzer
- detaillierte Anzeige von Fehlermeldungen (durchsucht das Logfile von OLAT)
- Einstellen der Loglevels der einzelnen Javaklassen
- Sysinfo:
- Aktuellen Memoryverbrauch der Java Virtual Machine
- Anzahl concurrent users dispatches zum Zeitpunkt der Anzeige
- Die aktuellen Java-Threads
- Java Environment Variablen
- Snoop: Anzeige aller Details einer HTTP-Anfrage
- Usersessions: technisch detaillierte Darstellung der Zustände der einzelnen Tomcat/OLAT Sessions
- Locks: Hier wird angezeigt welche Benutzer gerade einen Lock besitzen
- OLAT Systeminformation
- Anzeige aller Caches, d.h. aller Objekte, die von Hibernate aus Gründen der Performance im RAM zwischengespeichert wurden
- Quota Verwaltung
- Auflistung der erweiterten Systemproperties eines Benutzers

Ein weiteres grundlegendes Prinzip neben den Rollen in OLAT sind die Gruppen. Innerhalb von OLAT drei Typen von Gruppen (BusinessGroups):
- Arbeitsgruppen
- Lerngruppen
- Rechtegruppen

Arbeitsgruppen:
Eine Arbeitsgruppe ermöglicht die Gruppenarbeit ausserhalb eines Kurskontextes. Jeder OLAT-Benutzer kann sich eigene Gruppen mit beliebigen Personen zusammenstellen, weitere Personen dazu einladen oder Personen wieder aus seiner Gruppe ausladen. Einzige Bedingung ist, dass die jeweiligen Personen auch OLAT-Benutzer sind. Die Gruppen kann man je nach Bedarf mit verschiedenen Werkzeugen, einem Forum und/oder einem Ablageordner (Speicherplatz) ausstatten. Typische Beispiele für Arbeitsgruppen sind:
- Studiengruppe: Studierende können gemeinsam über Lerninhalte diskutieren und Dokumente austauschen
- Autorengruppe: Autoren bearbeiten gemeinsam ein Dokument und wollen erst die definitive Fassung als Lerninhalt in die Lernressourcen ablegen
- Projektgruppe: Wissenschaftliche Mitarbeiter arbeiten gemeinsam an einer Publikation

Lerngruppen:
Als Kursautor kann man in seinem Kurs Gruppen erstellen, in die sich die Studierenden einschreiben müssen oder in die man die Studierenden selbst einträgt. Diese mit einem Kurs zusammenhängenden Gruppen werden in OLAT Lerngruppen genannt. Man kann bestimmen, wann und wie viele Mitglieder die Gruppe hat und den Gruppen Betreuer zuweisen. Betreuer können die Lerngruppe administrieren d.h. Mitglieder in die Gruppe aufnehmen und weitere Betreuer ernennen. Mehrere Lerngruppen können zu einem Lernbereich zusammengefasst werden. Kursübergreifende Lerngruppen können nur von Nutzern mit der Rolle "Gruppenverwalter" erstellt und verwaltet werden.

Rechtegruppen:
Als Kursautor kann man anderen OLAT-Benutzern bestimmte Rechte an seinem Kurs erteilen indem man diese Benutzer in eine Rechtegruppe einlädt. Man kann alle OLAT-Benutzer (Autoren, Studierende) in eine Rechtegruppe aufnehmen unabhängig von deren bisherigen Rollen in OLAT. Die Rechte, die man einer Rechtegruppe zuweisen kann, sind: Das Recht Lerngruppen zu managen, das Recht einen Kurs zu editieren, das Recht Kursdaten zu archivieren und das Recht andere Kursteilnehmer zu bewerten.

Zusammenfassend kann man die Funktionalität der Gruppen in OLAT so beschreiben:
Lerngruppen werden in Kursen verwendet um Personen aus administrativen oder pädagogischen Gründen zu gruppieren, z.B. um Ihnen Lernmaterialien in einem geschützten Bereich zugänglich zu machen.
Rechtegruppen werden in Kursen verwendet um Personen gezielt spezielle Rechte innerhalb eines Kurses zuzuteilen, z.B. um das Bewertungswerkzeug zu bedienen.
Arbeitsgruppen können von allen Benutzern selbst erstellt werden um z.B. gemeinsam an einem Projekt zu arbeiten oder Dokumente auszutauschen. Sie stehen in keinem direkten Zusammenhang mit einem Kurs.

Kollaborative Werkzeuge:
Als Kursautor kann man seinen Rechtegruppen verschiedene Werkzeuge zur Verfügung stellen. Dazu zählen z.B.:
- News
- Kontaktformular
- Teilnehmerliste
- Diskussionsforum
- Ordner
- Chat
- Wiki (OLAT 5.0)
- Kalender (OLAT 5.1)

Das Rechte-Konzept von OLAT orientiert sich stark an dem Policy-Konzept von Java.
Es gibt:
- Identities (User)
- Gruppen mit Identities darin (sogenannte Securitygroups, nicht zu verwechseln mit Businessgroups)
- Rechte
- Resourcen / Objekte
- Policies

User sind in einer oder mehreren Gruppen. Eine Policy ist die Kombination von einer Gruppe, einem Recht, und einer Resource. Ein Benutzer hat dann ein gewisses Recht (z.B. lesen) auf einen gewisse Resource (z.B. RepositoryEntry), wenn er in mindestens einer Gruppe ist, die von einer Policy referenziert wird, welche das Recht „lesen“ auf die Resource hat, d.h. die Policy hat einen Fremdschlüssel auf die Gruppe, einen Fremdschlüssel auf die OLAT-Resource, und einen Text für das Recht.
Die Rechte sind additiv und positiv:
- additiv: Alle Rechte von allen möglichen Gruppen, in denen ein User ist, werden zusammengezählt, und ergeben so als Summe die Rechte dieses Benutzers
- positiv: Alle Rechte beschreiben die Erlaubnis, etwas zu tun (Im Unterschied zu negativen Rechten, die explizite Verbote beschreiben)

Die Systemrollen (also z.B. Autor) sind demzufolge nichts anderes als Gruppen mit bestimmten Rechten.

2. Grundsätzliche und spezielle Struktur- und Entwurfsprinzipien im Bezug auf das Rollen- und Rechtemanagement in OLAT

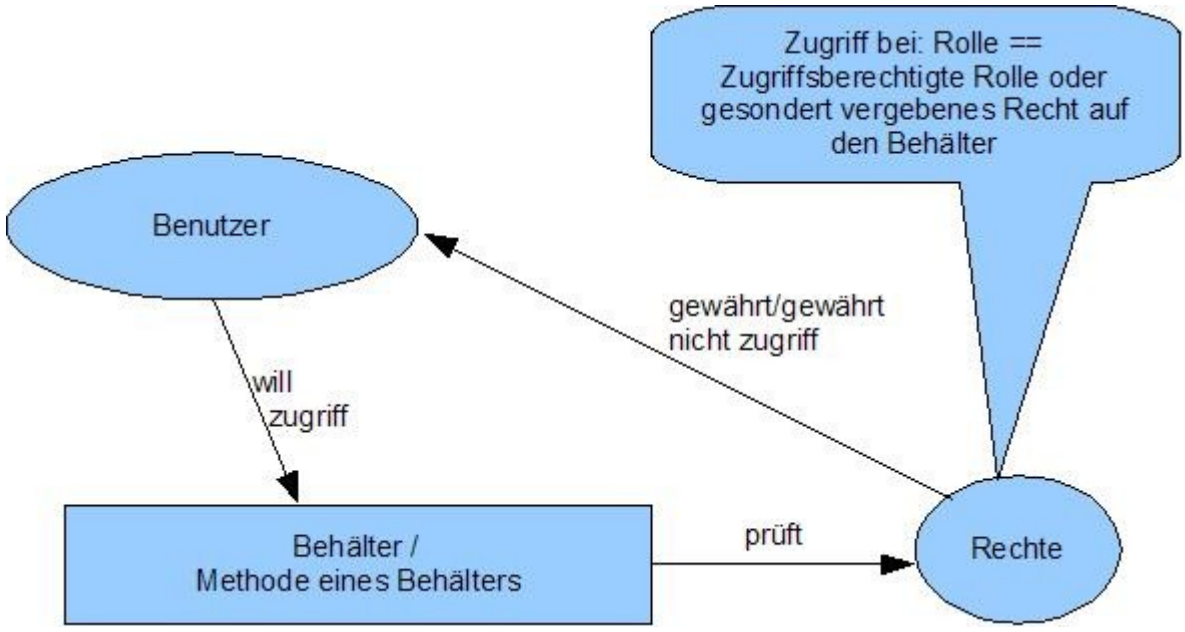
2.1. Analyse Gesamtsystem

Das Rollenmanagement in OLAT besteht in der Grundversion aus den sechs Rollen: Gast, Benutzer, Autor, Benutzerverwalter, Gruppenverwalter und Systemadministrator. Letztere fünf gehören zu den Systembenutzern. Die Rollen der Systembenutzer schließen sich gegenseitig nicht aus, so ist zum Beispiel jeder Autor auch ein Benutzer. Der Systemadministrator erhält die Rechte aller anderen Systembenutzerrollen, ist jedoch nur zur technischen Wartung von OLAT vorgesehen. Jeder authentifizierte Akteur besitzt automatisch die Rolle Benutzer, kann aber durch den Administrator (oder Benutzerverwalter) von den Systembenutzerrollen befreit werden und als anonymer Nutzer (der dann die gleichen Rechte wie ein Gast hat und dieser Rolle entspricht) eingestuft werden. Anhand der Rollen wird eine grobe Unterteilung durchgeführt, welche Seiten dem Benutzer zur Verfügung stehen. Diese sechs Rollen sind ausreichend um die Funktionalität aller OLAT spezifischen Aktionen zu kontrollieren. Bisher nicht erwähnt ist die “Login Denied”-Rolle . Sie ist im egtl. Sinne keine Rolle, sondern hindert dem registrierten Benutzer daran sich mit seinem Account einzuloggen. Solange ein Benutzer über diese Rolle verfügt ist er vom System ausgeschlossen.

Es besteht jedoch die Möglichkeit zusätzliche Rollen in den entsprechenden Tabellen zu erzeugen und in einer Extension separat abzurufen und zu nutzen, ohne das dabei die Grundfunktionen beeinflusst werden. Dem authentifizierten Akteur werden dabei die zusätzlichen Mitgliedschaften zugeordnet (zum Beispiel in einem zusätzlichen Administratrationswerkzeug).

Neben dem Rollenmanagement koexistiert das Rechtemanagement. Es wird ermöglicht, dass man einzelne Seiten oder Funktionen dem Benutzer sperrt beziehungsweise entsperrt. Dafür wird das entsprechende Zugangsrecht mit dem Behälterobjekt verknüpft.

Der Grund, warum es diese beiden Prinzipien gibt, ist, dass OLAT ein System mit vielen Anwendern innerhalb einer Instanz ist. Durch die Zweiteilung wird erreicht, dass der Datenbestand, der die Benutzerrechte repräsentiert, so gering wie möglich gehalten wird. Um gesonderte Rechte auf einen Behälter zu erhalten, muss dieses explizit erteilt werden.



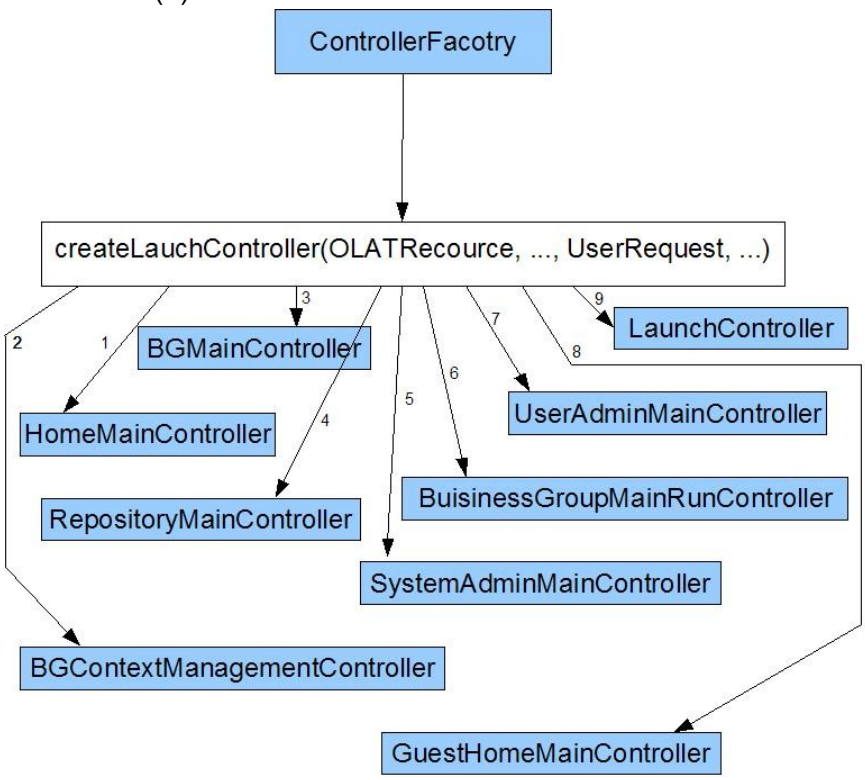
2.2. Analyse spezieller Klassen und Pakete

Das Rollen- und Rechtemanagement von OLAT ist vor allem aus den Objekten des Paketes *org.olat.basesecurity* aufgebaut. Die Klasse *Policy* enthält dabei das eigentlich Recht, was mittels der Methode *getPermission()* abgefragt wird.
Die Klasse *PersistingManager* übernimmt beim Rechtemanagement die Rolle des Controllers.

Verwendung findet das Rechtemanagement unter anderem an den folgenden Stellen bei OLAT:
Die initale Rollenunterscheidung findet in der *ControllerFactory* statt. In dieser wird entsprechend des *UserRequestes* die darzustellende Seite ermittelt.

Dabei werden die Rollen zunächst mittels *ureq.getUserSession().getRoles()* abgefragt.
Die Methode *createLaunchController(...)* kann dabei entsprechend des Benutzeranfrage folgende *Controller*-Objekte zurückgeben:

- *BusinessGroupMainRunController* (6)
- *BGMainController* (3)
- *LaunchController* (9)
- *GuestHomeMainController* (8)
- *RepositoryMainController* (4)
- *SystemAdminMainController* (5)
- *UserAdminMainController* (7)
- *BGContextManagementController* (2)
  HomeMainController (1)



- (*TestingMainController*)

Natürlich wird zuvor überprüft, ob die dem Nutzer zugewiesene Rolle auch berechtigt ist, den entsprechenden Controller aufzurufen.

Controller	**Voraussetungen (neben der Anforderung dieser Seite)**
HomeMainController	Keiner Anforderung einer bestimmten Resource
BGMainController	Man ist eingeloggt
GuestHomeMainController	Siehe *HomeMainController* und kein Login erfolgt
RepositoryMainController	Es muss der Zugriff auf diesen Behälter gewährt sein
LaunchController	Es muss der Zugriff auf diesen Behälter gewährt sein
UserAdminMainController	Benutzer ist Useradmin oder OLAT-Admin
BusinessGroupMainRunController	OLAT-Administrator oder Mitglied der angeforderten Gruppe
SystemAdminMainController	Benutzer ist OLAT-Admin

So wird zum Beispiel der Zugriff auf den *UserAdminMainController* nur gewährt, falls *roles.isUserManager()* wahr ist. Die anderen Controller werden analog überprüft. Wird im UserRequest ein Controller angefordert, auf den der Benutzer keinen Zugriff hat, so wird eine OLATSecurityException geworfen.

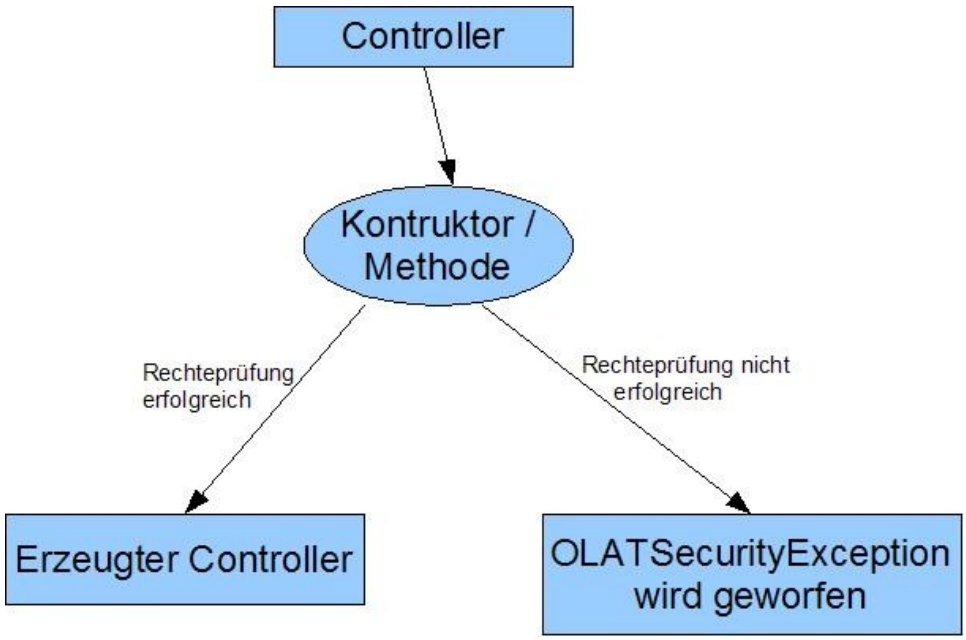
In den Oben aufgeführten Admin-Controllern (*UserAdminMainController* und *SystemAdminMainController*) erfolgt keine weitere Rollenüberprüfung.

Beim erstellen eines weiteren Controllers, wie zum Beispiel des *UserCreateController*'s, wird bei der Erzeugung eines Objektes durch folgenden Code abgefragt, ob die Vorraussetzungen erfüllt sind, um einen Benutzer zu erstellen:

```
Manager mgr = ManagerFactory.getManager();
if (!mgr.isIdentityPermittedOnResourceable(
          ureq.getIdentity(),
          Constants.PERMISSION_ACCESS,
          OresHelper.lookupType(this.getClass())
          )
   )
{
    throw new OLATSecurityException("Insufficient permissions to access UserCreateController");
}
```

Analog wird der Zugriff auf zugriffsbeschränkte Methoden überprüft.

Dies funktioniert auf allen Zugangsbeschränkten Controllern gleich:



Also gibt es eine 1:1 Verknüpfung zwischen einem Recht und einer OLAT-Resource, welche mittels der Klasse *PermissionOnResourcable* realisiert wird.
Dadurch können einzelnen OLAT-Resourcen unter Benutzern Berechtigungen zugewiesen werden. So zum Beispiel im *UserAdminMainController*.

```
if (uobject.equals("coauthors"))
{
  activatePaneInDetailView = "edit.uroles";

  // special case: use user search controller and search for all users that have author
  // rights

  PermissionOnResourceable[] permissions =
  {
     new PermissionOnResourceable(Constants.PERMISSION_HASROLE,
     Constants.ORESOURCE_AUTHOR)
  };


  UsermanagerUserSearchController myCtr = new UsermanagerUserSearchController(ureq,
  getWindowControl(),null, permissions, null, null, null);

  // now subtract users that are in the author group to get the co-authors

  Manager secMgr = ManagerFactory.getManager();
  SecurityGroup[] secGroup =
  {
    ManagerFactory.getManager().findSecurityGroupByName(Constants.GROUP_AUTHORS)
  };

  List identitiesFromAuthorGroup = secMgr.getIdentitiesByPowerSearch(null, null, null,
  null, null, null, secGroup , null, null, null, null);

  myCtr.removeIdentitiesFromSearchResult(ureq, identitiesFromAuthorGroup);
                                  contentCtr = myCtr;
                                  contentCtr.addControllerListener(this);
                                  return contentCtr.getInitialComponent();
}
```

Der Useradmin oder der OLAT-Administrator kann also auf der *UserAdminSite* (gleichnamige Klasse) für bestimmte Behälter Rechte verteilen.

Dabei hat der Autor bzw. Coautor eines Behälters natürlich die vollen Rechte auf diesen, solange sie ihm nicht entzogen werden.