Permission Concept SAP Sailing Analytics

# Introduction

This document describes the permission concept developed for the SAP Sailing Analytics (in the following just Sailing Analytics). Currently a very rough permission system based on role based access control (RBAC) is used to restrict access to among others the administration console. The system is built on the Apache Shiro (in the following just Shiro) framework. This system currently does not support unified user management (in the sense of a central user management system that manages the users for all deployments of the Sailing Analytics) and dynamic access control for all aspects of the Sailing Analytics.

However, as one medium term goal is to develop the Sailing Analytics to be usable by sailing clubs and eventually individuals as a cloud application, the user management and access control should be unified and expanded to be dynamic and provide the appropriate (the Sailing Analytics manages very personal data) security aspects.

The concept developed in this document should focus on fine grained access control with a strong focus on being able to unify and strengthen the user management and access control. Resulting in a system where multiple organizations and individuals can work on one system without unwantedly interfering in their actions and data.

A secure access control concept for the existing data model is not easily developed, because the data objects in the Sailing Analytics do not merely form static trees. Data objects can form graphs where there is no clear root for a given node. Furthermore the associations of data objects can change. These challenges have to be addressed by possible concepts by adapting them to this very specific domain.

The following requirements result from the above described (the access control system has to…):

1. Be expressive enough to support the complex associations of the Sailing Analytics
2. Support multiple organizations (clubs, events and individuals) working in one system
3. Communicate the permissions to the frontend (so only UI elements that support permitted actions are active)
4. Be reasonably complex and implementation intensive

# Access Control Concepts

The two big concepts that play together in this permission concept are access control lists (ACLs) (also used e.g. in the Linux or Windows file system) and RBAC. Furthermore, there is the concept of attribute based access control (ABAC) that is not explored in this concept document.

The concept of ACLs is based on the idea of assigning each data object that is access controlled an ACL. The ACL is a list of entries that assign a user or group of users to permissions. If e.g. read access is requested for a data object, its ACL is checked if the user or a group, the user belongs to, has an entry granting the read permission.

RBAC is based on the idea of having roles that imply certain permissions and assigning roles to users. The roles of RBAC are on a simple level equivalent to groups for ACLs. (Barkley, 1997) However, in general roles combine a set of users with a set of permissions, whereas groups represent only a set of users. According to (Sandhu, Coyne, Feinstein, & Youman, 1996) there are multiple models for RBAC. The model described above is called . Furthermore, there are , and which all include , but add additional features.

adds the concept of role hierarchies, where roles inherit the permissions granted by their parent roles. However, they do not inherit the set of users. adds constraints which restrict how and when roles and permissions can be combined with other roles or permissions. Besides mutual exclusion of roles or permissions, constraints could also require a user to have role *s* when assigned role *r* (or the same with permissions, which could be used e.g. to require to be able to view an event when a view permission for a race in the event is granted). Furthermore, the concept of constraints could also restrict the roles and permissions that a user can simultaneously have in a session (e.g. only one tenant role at a time). combines and .

In the context of RBAC (Ferraiolo, Cugini, & Kuhn) mentions the concept of subjects. A user may in one session only have a certain set of roles and permissions. This may be due to choice to reduce accidental actions with a wrong role or a constraint enforced by the system (See ). This set of roles and permissions is called a subject. A user may have any number of active subjects. However, a subject is only associated with one user.

It is to note that simple RBAC models show no difference in their ability to express access control policies than ACLs. (Barkley, 1997) More complex RBAC models are be more expressive than ACLs.

In the course of this concept document there will be no difference in meaning between roles and groups. In the existing system they are named roles, thus the term roles will be used for both roles and groups.

# Initial Idea

The initial idea was a system that fully relied on roles and tried to imply permissions over the associations of data objects. However, it was found that implying permissions poses problems when e.g. data objects are unlinked from each other (or associations are changed), in which case permissions are lost, because they can no longer be implied. Moreover, as stated above the associations between the data objects in the Sailing Analytics do not necessarily form a tree, which prevents implications to be made just along a hierarchy. We discarded this idea and developed another, described below.

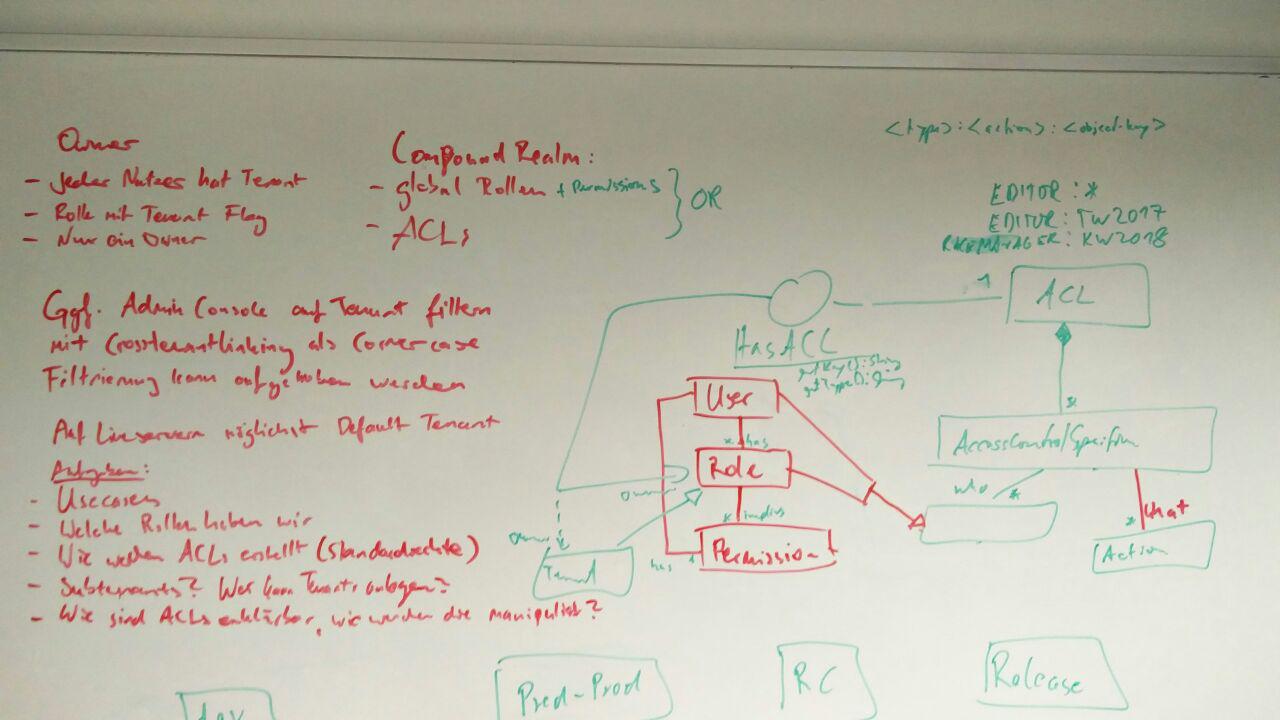


Figure 1 General concept (Walldorf 16.02.2017)

Figure 1 depicts the general initial ideas for this document that were developed after several iterations of concepts. The idea is based on the existing Shiro RBAC system that should handle global static roles and also supports directly granting permissions to a user. Furthermore, ACLs should be introduced. Those should solve the problem of “losing” implied permissions, because the access control list are directly associated with the data object. The existing Shiro authorizing realm that checks for the roles and permissions directly assigned to a user would have to be extended by the ACL concept. This will form what we call a compound realm that if a permission is checked looks for the permission in the roles and permissions of the user and in the ACL of the data object. If either the roles and permissions or the ACL grants the permission the user is allowed access.

# Ownership

It is common place in cloud applications where multiple groups of users that each belong to some kind of organization to summarize these groups of users as tenants. The tenants represent the organizations and depending on if a hierarchy is allowed the sub-organizations working on the system. In the Sailing Analytics the organizations could be sailing clubs, events like the Travemünderwoche or in the future private users.

One idea behind tenants is to encapsulate organizations so users of one organization cannot work with data objects from another organization, if they are not granted the permissions explicitly. Furthermore, tenants are used to group data objects so users can have access to all data objects of a tenant and do not have to be granted every permission explicitly. Another idea is that data objects created in the domain of the tenant are not owned by a user that can leave the tenant or be unavailable, but are owned by the tenant itself.

In the Sailing Analytics the set of roles for each tenant may, apart from certain exceptions, represent the subjects a user can adopt. A constraint could be introduced that only allows the roles for one tenant as a subject.

Tenants pose an UI problem, because it has to be clear to the user in which tenant he is currently working. Currently the best idea is to let the user select a tenant when he logs in and have default tenants for event and club servers that correspond to the event or club.

In some causes it might be necessary to transfer the ownership to another tenant/user. Thus, the owner should not be final but changeable.

## Users or Tenants as Owners

A problem with the tenant approach is that users could have no permissions to e.g. remove data objects that they have just created on accident, because the remove permission is reserved to admins of the tenant which a user that has create permissions may not be.

Three solutions come to mind. The creator of a data objects could always be granted the permission to remove the data object explicitly. Moreover, the log where the creation was logged could be crawled to find the user that created the data object and override the permission system when in a certain timespan.

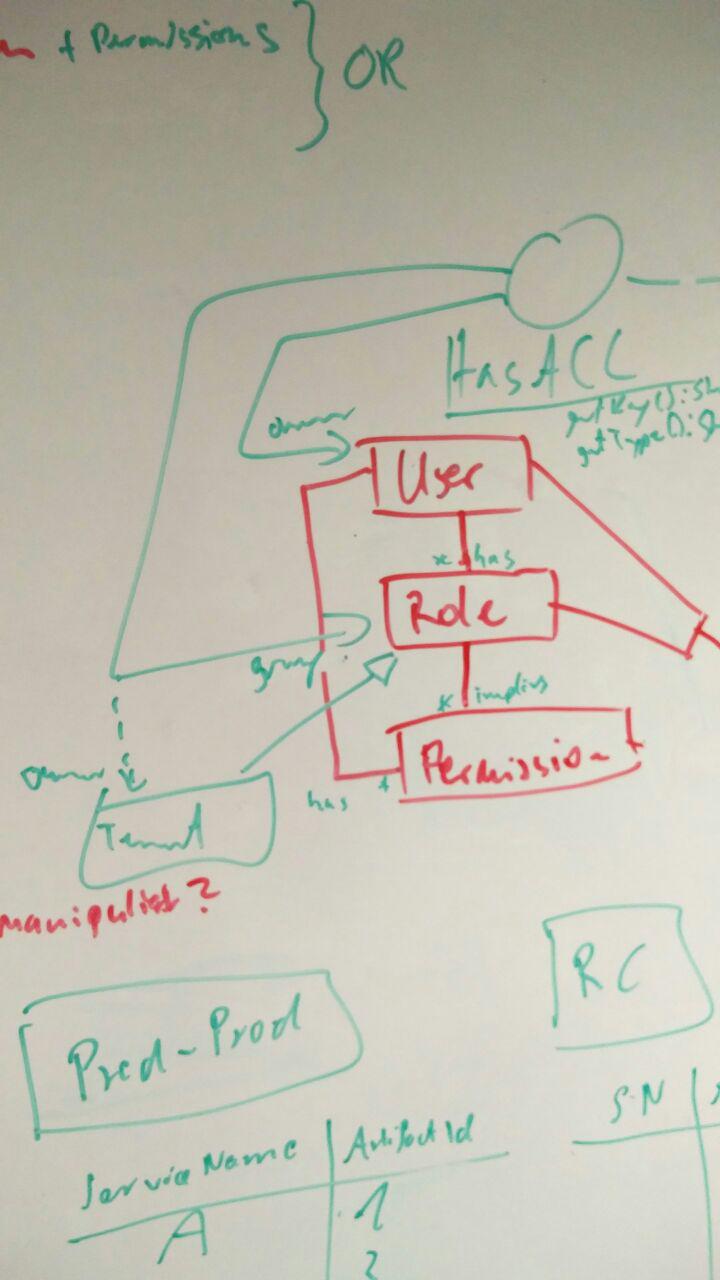


Figure 2 Alternative concept for tenants and owners (Walldorf 16.02.2017)

Figure 2 shows an alternative approach to ownership. In this approach a single user would own a data object so he can do everything with it. The tenant would then be a kind of secondary owner or group in Linux terms. This solves the problem that users could have no permissions to e.g. remove data objects that they have just created on accident. However, it also introduces a second layer of ownership.

## Subtenants

Subtenants could be a convenient way to restrict the permissions of certain users to only a part of a tenant’s domain. However, this introduces a hierarchy of tenants that brings with it its own problems. Imagine there is a tenant “tw2017” and the 49er boat class races should not be manageable by the same racer managers that can manage races of the other regattas. So “tw2017” would require a subtenant “other” and “49er” that encapsulate the 49er boat class and everything else from each other. Now if a permission is checked on an ACL, the ACL has to traverse the tenant hierarchy to find out if the user is part of a role for a parent tenant that grants the permission. However the convenience of tenant hierarchies might be stronger than the traversal problem, because the hierarchy will probably never be deeper than one or two levels.

An alternative strategy is just creating a completely new top level tenant for the 49er boat class races of “tw2017”. Only admins of a tenant could create such tenants and only they would be able to manage the newly created tenant. This would not introduce a hierarchy, but would require users that have roles for all boat classes to have their roles for both tenants instead of only the role for the parent tenant. However in this model the logical borders between the tenants hinder the permission management of the data objects.

Another challenge with subtenants is how to communicate the concept to users. Which also makes it harder to imply with which tenant or subtenant a user is currently working.

# Permissions in the Frontend (WIP)

Currently the permissions of the roles are hard coded and can thus be easily imported in the frontend. Dynamic roles that can change on runtime would require to pass the permissions implied by the roles to the frontend or the roles to be resolved before passing the set of permissions assigned to a user into the frontend.

ACLs are just delivered with the object itself. A permission on an object can then be checked in the frontend by asking the ACL delivered with the object.

A third but possibly resource hungry possibility would be to implement a service that can be called from the frontend to check single permissions. The service would implement some kind of hasPermission(permission) method.

* Rewrite this

# Administration of Authorization (WIP)

This section will discuss how it is determined if a user can grant or revoke a permission.

* We define authority as power which has been legitimately obtained (Krishnan & Zimmer, 1991)
* We regard ownership as the starting point for delegation of authority (Krishnan & Zimmer, 1991)
* However it can make sense for the creator of a data object to not be the owner
* With these two facts in mind, a data objects has to have a single user as the owner or users can deliberately lose permissions on creation. Not every user that can create data objects in a tenant should automatically be the owner of every data object of the tenant, but in return should also not lose rights e.g. for removing an accidentally created data object on creation, because the tenant is the owner. Maybe this could also be implemented with a constraint that a create permission can only be granted if a delete permission exists or the creation of an object also implies granting the delete permission to the creator.
* Centralized, Hierarchical, Cooperative, Ownership, Decentralized (Sandhu & Pierangela, Access Control: Principles and Practice, 1994)

# Creation of Access Control Lists (WIP)

ACLs could either be created when the associated data object is created or when they are used the first time, i.e. a first entry is created in the ACL. However, if the ACL is initialized with default permissions, the ACL would be created when the data object is created anyway. As data objects should only have one ACL each, the user should not be able to create the ACLs, this should instead be automated.

Especially for mass objects (GPSFixes) ACLs are only relevant when they contain entries, otherwise they are a waste of Java instances and memory space.

* Axel: Das erinnert dann ein bisschen an die sogenannten "Access Windows", die es bei Igtimi gibt. Die funktionieren so aehnlich. Man kann auf einem Track einen Zeitraum angeben und fuer den dann Rechte vergeben, z.B. mit anderen Benutzern teilen.
* This sounds like an application for attribute based access control.

There are two options for default permissions:

1. Each type of ACL has its own mask of permissions it gets assigned. This has the advantage over pure roles that if one wants to change the norm only for one instance of an object he can. The masks could even be editable for each tenant so different defaults can be set.
2. Default permissions are set in the roles and only special cases are implemented via the ACLs. This means less entries in the ACLs and less work when creating and initializing the ACLs.

* There has to be another option for default permissions. One idea is to allow per tenant editing of default permissions for data objects. However, this does not really solve the problem of implying permissions from roles or default masks

Default permissions for data objects should probably not be implied by their context they are created in. Implying permissions could lead to unwanted permissions on data objects.

# Implementation of Roles (very WIP)

* Axel: This should be framed better.
* This chapter as well as the list of roles is far from complete

Roles are currently hardcoded, however they need to be editable on runtime if they should also be used as roles in the ACLs. This implies that the UserDTO cannot obtain permissions for certain roles, only the hard coded ones. Furthermore there would be a difference between global roles and roles used in ACLs. The following roles are not necessarily global. Only the ones flagged as global are. The rest are abstract roles that every tenant should have.

* Discuss parameterized roles

1. Global Admin  
   Has permissions for everything
2. Global Moderator (Marcus Baur?)
3. Tenant (Axel: Is this a static role or is there one role of this kind for every tenant?)  
   Is owner of everything in the tenants domain
4. Tenant Admin  
   Has (almost) every permission in his tenant (Maybe only users with the tenant admin role can delete the tenant, if it is possible to delete tenants at all) (One would not want to write the tenant admin role into every ACL when he has all the permissions anyway. This is a good example when we would want to imply permissions from a role that are not global)
5. Eventmanager
6. Racemanager
7. Editor?
8. Resultservice / Competitorcleanup

## The Role of Roles (WIP)

* Frame this clearer (what does tw2017 stand for?)

Roles could either be used as a way to define global permissions for a small amount of users, like moderators and global admins. On the other hand they could also define default permissions when they are parameterized with tenant. (e.g. role “editor:tw2017” implies permissions “race:view,edit,delete:tw2017:\*”, “regatta:view,edit,delete:tw2017:\*”, …) Also see “How ACLs are created” 2. Option (Defaults).

* Who can assign these roles?

## Tenants as Roles (WIP)

On the other hand not everybody who has a role for a tenant (e.g. “editor:tw2017”) has to also have the role “tw2017”, which would make him part of the tenant. The tenant would be the owner, but people who have permissions in the domain of the tenant would not have to be part of the tenant. Thus, a small group of people would make up the tenant, thus being the owner and a larger group of people would have permissions on the data objects of the tenant.

## Role Hierarchies (WIP)

Here should be a discussion about whether to allow role hierarchies or not to allow them.

## Role Contraints (WIP)

Here should be a discussion about whether to allow role contrains or not to allow them.

# Use Cases

* Introduce Archive and club tenants that will be used in the use cases

It is always assumed that the ID of the user is “user” and the ID of its tenant is “tenant”.

1. Create Event (or probably any data object)
   1. User creates event
   2. Event is owned by tenant that user is associated with
   3. Access control list is created for the event
   4. View permission is set for all the users in the tenant   
      ACL = {“tenant”:[“read”]}
   5. Edit permission is set for all the tenant admins and event managers  
      ACL = {“tenant”:[“read”],   
      [“admin:tenant”, “eventmanager:tenant”]:[“edit”]}
   6. Remove permission is set for all the tenant admins   
      ACL = {“tenant”:[“read”],   
      [“admin:tenant”, “eventmanager:tenant”]:[“edit”],   
      ”admin:tenant”:[“remove”]}
2. Transfer ownership of event (or any other ownership transfer)
   1. User or tenant owns event  
      e.g. ACL = {“admin:tenant”:[“owns”], “user”:[“owns”]}
   2. The user is only admin of the tenant who owns the event
      1. Ownership is transferred to another tenant, but owner is left with his permissions  
         ACL = {“admin:tenant2”:[“owns”], …}
   3. The user is the owner
      1. Only the tenant level ownership is transferred
         1. ACL = {“admin:tenant2”:[“owns”], “user”:[“owns”]}
      2. The user transfers ownership to another user
         1. ACL = {“admin:tenant”:[“owns”], “user2”:[“owns”]}
3. Link RegattaLeaderboard into LeaderboardGroup
   1. If either the user, a role or a tenant, the user is part of, has the permission to edit the LeaderboardGroup (LBG) and share the RegattaLeaderboard (RL), the user can link them  
      LBG ACL = {“user”:[“edit”]}  
      RL ACL = {“user”:[“share”]}
   2. The user then has to choose who to grant view permissions for the RegattaLeaderboard. By default this will be all that can view the LeaderboardGroup
4. Unlink TrackedRace
   1. If either the user, a role or a tenant, the user is part of, has the permission to edit the Race, the user can unlink them, however if he does not have a share permission for the TrackedRace, a warning will pop up
5. Share TrackedRace
   1. If either the user, a role or a tenant, the user is part of, has the permission to share the TrackedRace, the user can grant view permissions to anybody  
      ACL = {“user”:[“share”]}
   2. The user shares the TrackedRace with “user2”  
      ACL = {“user”:[“share”], “user2”:[“read”]}
6. Grant share permission for TrackedRace
   1. If either the user, a role or a tenant, the user is part of, has the permission to share the TrackedRace, the user can grant share permissions to anybody  
      ACL = {“user”:[“share”]}
   2. The user grants share permission of TrackedRace to “user2”  
      ACL = {[“user”, “user2”]:[“share”]}
7. Create GPSFix
   1. It would only be consistent to attach a ACL to each GPSFix, however it probably never happens that a GPSFix has other permissions that a whole track, thus I propose to leave GPSFixes without ACLs
8. Masterdata import
   1. This should import all permissions as they are. A masterdata import itself is no reason to change permissions, however only data objects that the user that is importing has a “share” permission for should be importable.
9. Share event with archive/public
   1. If either the user, a role or a tenant, the user is part of, has the permission to share the data object, the user can share the event with the archive and public  
      ACL = {“user”:[“share”]}
   2. The user shares the data object  
      ACL = {“user”:[“share”], “\*”:[“view”]}
10. Clubs may only be able to create races with e.g. < 60 boats. How could this be implemented with permission checking

# Migration

With such an extensive existing system as the Sailing Analytics Suite, migration is a big concern. The existing RBAC system is easily extended to support dynamic creation of roles.

However, ACLs have to be deeply integrated into the system, because at least an interface that flags every data object that is access controlled has to be added to these objects. Furthermore at least an identifier for the ACL has to be exported to the frontend with every data object that is access controlled. It would be even better to export the ACL for every access controlled data object. This includes the roles of the user, because part of the ACL could link roles to users which would have to be resolved. If the ACLs are passed to the frontend with the data objects they belong to, the ACLs would need to be passed to their data objects on server startup when they are loaded from the database or retrieved in every service call that need to pass an ACL to the frontend, which would touch even more code.

If the solution to the above described frontend to backend interface challenge is to have a service that can be asked for the ACLs, it would be easier to implement a service that entirely checks permissions in the backend and only passes a Boolean result to the frontend. This would unify permission checking in the front- and backend and also simplify the handling of roles and ACLs.

Another challenge besides the code changes is the data migration. For every existing data object an ACL has to be created and filled with the right permissions so the users do not notice a big change.

Besides creating an ACL for every data objects that is access controlled, an owner has to be defined for each existing data object, so that in combination with the ACLs no user loses permissions they need to have.

# Bibliography

Barkley, J. (1997). Comparing Simple Role Based Access Control Models and Access Control Lists. (S. 6). http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.107.6366.