

# Grouper - Gruppenverwaltung für die Universität Ulm

Als Erweiterung des IDM bietet Grouper allen Eigentümern einer Organisationseinheit die Möglichkeit, eigenständig eigene Gruppen anzulegen und zu verwalten. Diese Gruppen stehen dann zur individuellen Rechtevergabe in diversen Zielsystemen zur Verfügung.

Den Login-Link finden Sie hier: [Anmeldung](#)

In der Zentralen Universitätsverwaltung wird Grouper für das Management der Berechtigungen der Gruppenlaufwerke O: und S: verwendet.

## Ausgangssituation

Bisher wurden auf dem Fileserver der Zentralen Universitätsverwaltung (o: und s: Laufwerk) die Zugriffsberechtigungen über Gruppenmitgliedschaften und individuellen Benutzerrechten realisiert. Die Gruppen wurden vom kiz gepflegt, die individuellen Berechtigungen von den Beschäftigten der ZUV.














## Neue Situation

Mit der Einführung von Grouper haben die Beschäftigten der ZUV selbst die Möglichkeit Gruppenmitgliedschaften zu pflegen. Zugriffsberechtigungen auf Ordner werden ausschließlich über Gruppen geregelt. Individuelle Benutzerrechte werden abgeschafft.

- Initial werden die Dezernats- und Abteilungsleitenden aus dem IDM übernommen. Alle anderen Beschäftigten müssen explizit in die Gruppen aufgenommen werden.
- Die Verwaltung der Gruppen kann an Beschäftigte der ZUV delegiert werden.
- Für jede Abteilung gibt es Ansprechpartner, die Beschäftigte in die gewünschte Gruppe aufnehmen können. Die Ansprechpartner stehen in der Datei **Berechtigungen.txt**, die auf dem File-Server auf der Ebene der Abteilungsordnern oder in den Abteilungsordnern steht.
- Für jeden dieser Ordner steht eine Gruppe in Grouper zur Verfügung.
- Neue Ordner und die dazugehörigen Gruppen können bei Bedarf über ein Ticket angefordert werden. Dazu sind Dezernats- und Abteilungsleitenden berechtigt.
- In allen Ordnern, in denen eine Datei **Berechtigungen.txt** steht, gibt es nur Lese-Rechte. Nur Administratoren dürfen schreiben.
- In den Abteilungsordnern haben i.d.R die Mitglieder der Berechtigten Gruppe Schreib-Lese-Rechte. Ausnahmen, wie **o:\zuv\Allgemein\bilder**, stehen in der Datei **Berechtigungen.txt**. In diesem Fall dürfen alle lesen.
- Ordner, deren Inhalt von allen gelesen werden kann, enthalten die Datei **hier-kann-JEDER-lesen.txt**.
- Die Verwaltenden einer Gruppe sind dafür verantwortlich, dass Mitglieder, die keinen Ordner-Zugriff mehr haben dürfen, aus den entsprechenden Gruppen entfernt werden.
- Nach dem Verlassen der Universität wird ein Benutzer nach einer gewissen Zeit automatisch gelöscht. Damit erlöschen auch seine Gruppenberechtigungen.
- Bei einem Arbeitsplatzwechsel innerhalb der Universität bleibt die Gruppenmitgliedschaft erhalten! Hier muss manuell eingegriffen werden.
- Gruppenmitgliedschaften können zeitlich befristet vergeben werden. Das bietet sich bei Auszubildenden und Studentischen Hilfskräften an.

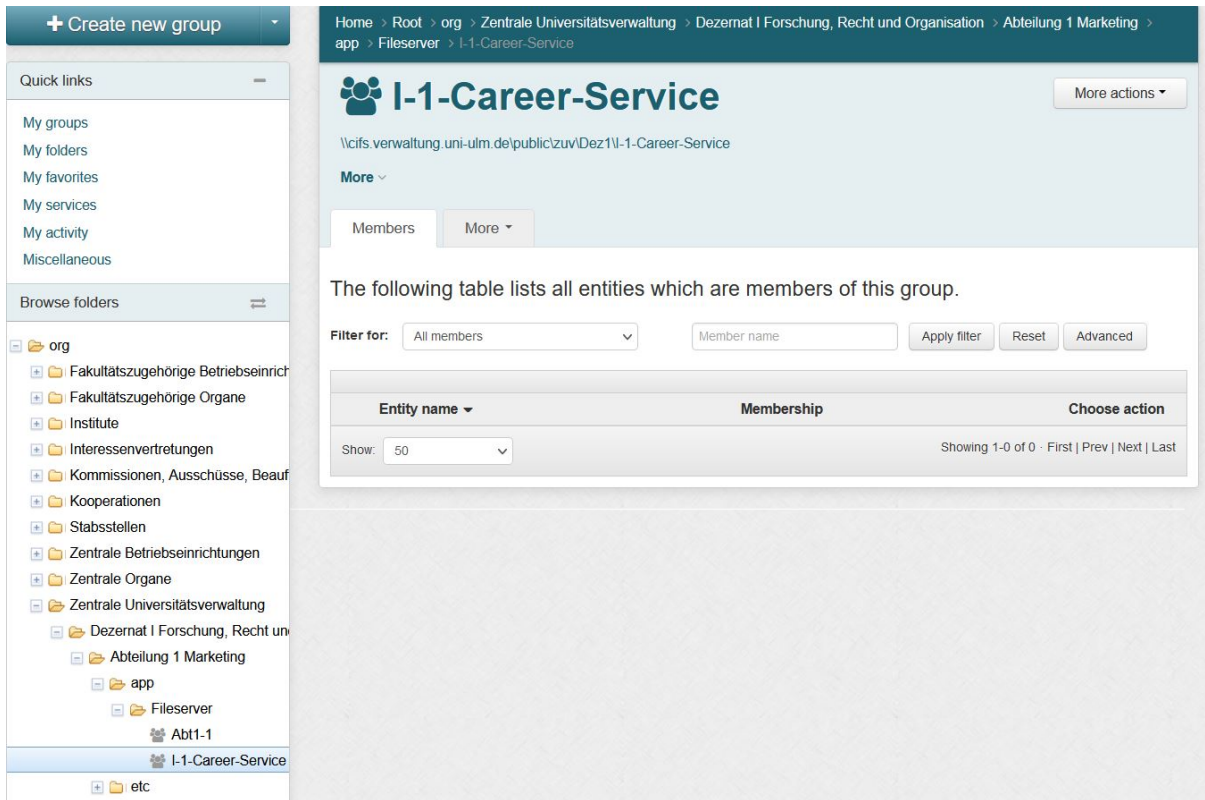
## Berechtigungen für den File-Server vergeben

Um auf die Inhalte der Ordner unterhalb der Ebene **o:\zuv\DezX\** zugreifen zu können, ist eine Mitgliedschaft in der entsprechenden Gruppe notwendig. Nachfolgend wird beschrieben, wie Beschäftigte in Gruppen aufgenommen werden und wie die Einrichtungsleitenden (i.d.R. Dezentertinnen und Dezenternenten) die Gruppenverwaltung delegieren können.

Name	Änderungsdatum	Typ
 Abt1-1	08.11.2022 07:40	Dateiordner
 Abt1-2	14.10.2022 11:17	Dateiordner
 Abt1-3	01.09.2022 14:55	Dateiordner
 Abt1-4	20.10.2022 12:11	Dateiordner
 Dez1-allgemein	02.09.2022 08:01	Dateiordner
 Dez1-Leitung	24.10.2022 13:40	Dateiordner
 Hausmeister	27.02.2019 15:11	Dateiordner
 I-1-Career-Service	27.08.2021 14:09	Dateiordner
 Team-Datenschutz	17.10.2022 15:27	Dateiordner
 Team-Erfindungen-Technologietransfer	08.09.2022 17:09	Dateiordner
 Team-Wahlen	14.04.2021 08:00	Dateiordner
 Team-Stiftungen	21.09.2022 12:26	Verknüpfung
 <b>Berechtigungen.txt</b>	12.11.2022 01:16	Textdokument

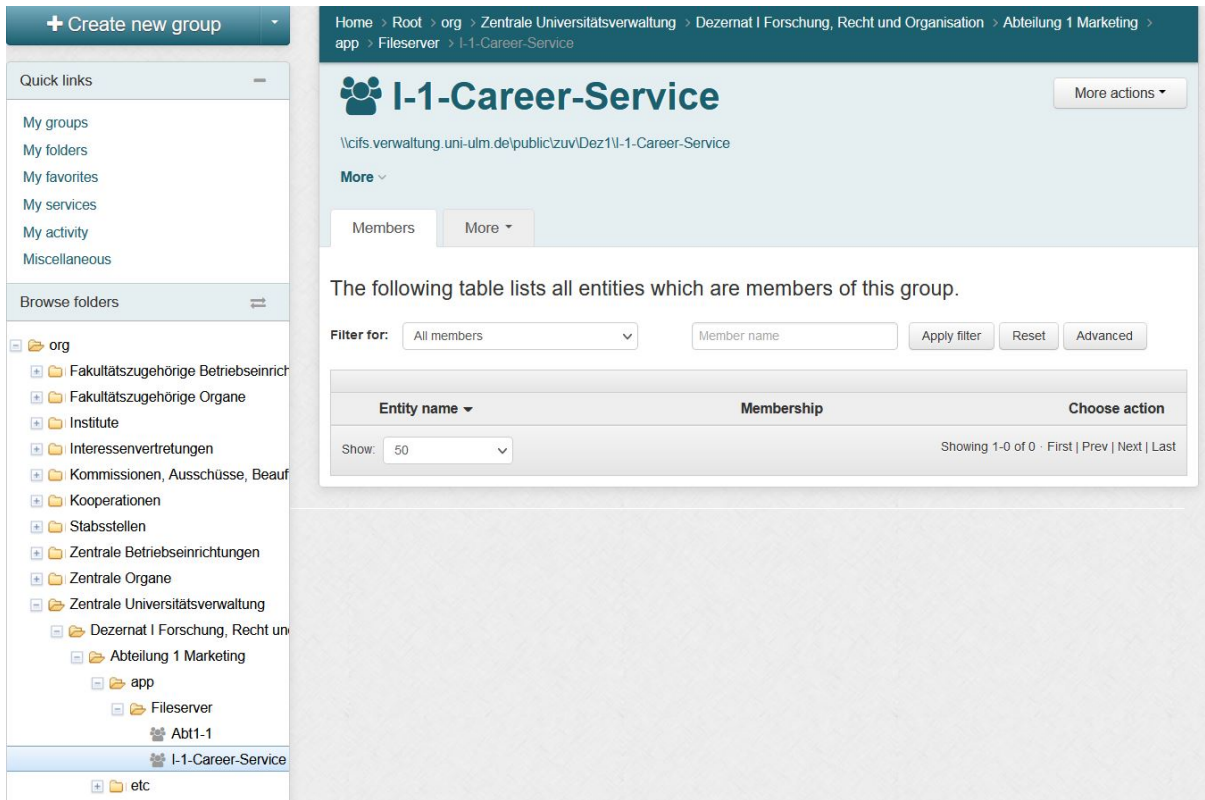
## Beschäftigte in eine Gruppe aufnehmen

Die zur Verfügung stehenden Gruppen sind in Grouper im linken Bereich unter **org → Zentrale Universitätsverwaltung → Dezernat... → Abteilung... → app → Fileserver** zu finden. Die Organisationsstruktur in Grouper kann von der Ordnerstruktur auf dem File-Server abweichen. Wählen Sie Ihre Organisationseinheit und Ihre Abteilung. Hier ein Beispiel aus Dezernat I.



Für die Abteilung 1 des Dezernats I gibt es die Gruppen **Abt1-1** und **I-1-Career-Service**. Für alle Ordner mit beschränktem Zugriff, gibt es eine korrespondierende Gruppe in Grouper. Im Beispiel oben wäre das die Gruppe **I-1-Career-Service** die dem Ordner `\\cifs.verwaltung.uni-ulm.de\public\zuv\Dez1\I-1-Career-Service` zugeordnet ist (`\\cifs.verwaltung.uni-ulm.de\public` wird auf dem Arbeitsplatzrechners durch `o:` substituiert). Der Gruppe **Abt1-1** ist der Ordner `\\cifs.verwaltung.uni-ulm.de\public\zuv\Dez1\Abt1-1` zugeordnet. Alle darunterliegenden Ordner um Dateien erben die Berechtigungen.

Klicken Sie auf die gewünschte Gruppe z.B. **I-1-Career-Service**



Um neue Mitglieder in eine Gruppe aufzunehmen, klicken Sie auf die Schaltfläche **+Add members** . Geben Sie hinter **Member name or ID** Name oder den kiz Benutzernamen an. Eventuell werden mehrere Namen angezeigt. Es kann von Vorteil sein den kiz Benutzernamen anzugeben, da dieser eindeutig ist. Mit der Schaltfläche **Add** fügen Sie das Mitglied der Gruppe hinzu und schließen den Vorgang ab.

arack-wms

**+ Add members**

Group actions ▾

Member name or ID:   
Enter an entity name or ID, or [search for an entity](#).

Assign these privileges:  Default privileges  Custom privileges

Start date:   
The optional date on which this entity's membership begins. Expected timezone is CET/CEST.

End date:   
The optional date on which this entity's membership expires. Expected timezone is CET/CEST.

**Add** or [import a list of members](#) .

Der Name des ausgewählten Mitglieds wird in der Spalte **Entity name** angezeigt.

<input type="checkbox"/> Entity name ▾	Membership	Choose action
<input type="checkbox"/> <a href="#">Kizbenutzername (kizbenutzername)</a>	Direct	<b>Actions</b> ▾

Show:  ▾ Showing 1-1 of 1 · [First](#) | [Prev](#) | [Next](#) | [Last](#)

Soll die Mitgliedschaft zeitlich befristet sein, kann ein Zeitraum angegeben werden. Klicken Sie auf **Actions** und **Edit membership and privileges**.

The following table lists all entities which are members of this group.

Filter for:  ▾

<input type="checkbox"/> Entity name ▾	Membership	Choose action
<input type="checkbox"/> <a href="#">Kizbenutzername (kizbenutzername)</a>	Direct	<b>Actions</b> ▾

Show:  ▾ Showing 1-1 of 1 · [First](#) | [Prev](#) | [Next](#) | [Last](#)

**Edit membership and privileges**

Revoke membership

Geben Sie **Start date** und **End date** im Datumsformat **JJJJ/MM/TT** an.

[User] is a direct member of the arack-vms group

[User] is not an indirect member of the arack-vms group

**Start date:**   
The date on which this entity's membership begins. Expected timezone is CET/CEST.

**End date:**   
The date on which this entity's membership expires.

**Direct group privileges:**  ADMIN  READ  UPDATE  OPTIN  OPTOUT  ATTRIBUTE\_READ  ATTRIBUTE\_UPDATE  VIEW

**Indirect group privileges:**  ADMIN  READ  UPDATE  OPTIN  OPTOUT  ATTRIBUTE\_READ  ATTRIBUTE\_UPDATE  VIEW

Mit **Save** werden die Angaben übernommen. In der Standardeinstellung werden nur aktive Gruppenmitglieder angezeigt. Sollte das **Start date** in der Zukunft liegen, verschwindet der Eintrag aus der Liste, taucht aber beim Erreichen des Datums wieder auf.

Mit einer speziellen Einstellung können auch inaktive Gruppenmitglieder eingeblendet werden. Klicken Sie dazu auf **Advanced**.

The following table lists all entities which are members of this group.

**Filter for:**

<input type="checkbox"/> Entity name	Membership	Choose action
Showing 1-0 of 0 · <a href="#">First</a>   <a href="#">Prev</a>   <a href="#">Next</a>   <a href="#">Last</a>		

Wählen Sie dann die Einstellung **Enable /disable status**. Mit **Apply filter** wird die Einstellung übernommen und es werden auch inaktive Mitglieder angezeigt.

**Enabled / disabled:**   
By default, only memberships that are currently active are shown. To view all memberships including disabled memberships due to enabled/disabled dates, select the "Enabled / disabled status" option.

**Point in time audit:**   
By default, only current memberships are shown. You can choose to show historical memberships based on audit data.

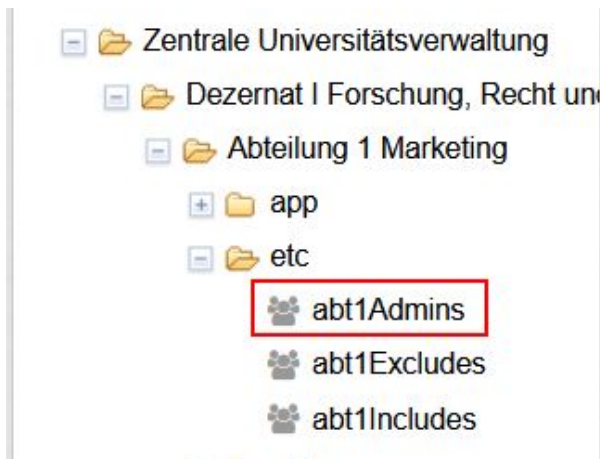
Es erscheint das Anfangs- und Endedatum der Gruppenmitgliedschaft. Diese Anzeigeeinstellung ist nicht dauerhaft.

<input type="checkbox"/> Entity name	Status	Enabled date	Disabled date	Membership	Choose action
<input type="checkbox"/> [User]	Enabled	2022/11/11 00:00:00	2022/11/30 00:00:00	Direct	<input type="button" value="Actions"/>
Showing 1-1 of 1 · <a href="#">First</a>   <a href="#">Prev</a>   <a href="#">Next</a>   <a href="#">Last</a>					

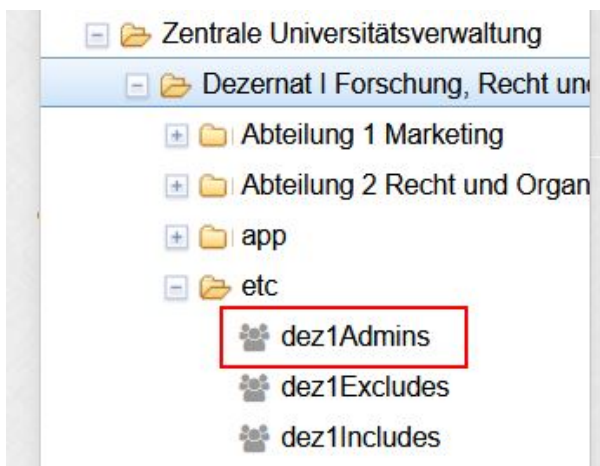


## Hinzufügen von Gruppenverwaltenden

Initial werden nur die Dezernats- und Abteilungsleitenden aus dem IDM übernommen. Die Dezernatsleitenden können weitere Gruppenverwaltende bestimmen. Dazu müssen die Dezernatsleitenden die dafür bestimmten Beschäftigten, wie oben beschrieben, in die Gruppe **abtXAdmins** aufnehmen. **X** steht für die Abteilung des Dezernats.



Sollen Gruppenverwaltende für alle Gruppen eines Dezernats zuständig sein, müssen die Verwaltenden auf Dezernatsebene in die Gruppe **dezXAdmins** aufgenommen werden.



Es ist auch möglich Gruppenverwaltende nur für eine bestimmte Gruppe zu bestimmen. Dazu muss die Gruppe ausgewählt werden und auf die Schaltfläche **Privileges** geklickt werden. Dann **+Add members**. Geben Sie hinter **Member name or ID:** Name oder den kiz Benutzernamen an, der die Gruppe verwalten soll. Es kann auch eine Gruppe angegeben werden.

**Member name or ID:**  Enter an entity name or ID, or [search for an entity](#).

**Assign these privileges:**  MEMBER  ADMIN  UPDATE  READ  VIEW  OPTIN  
 OPTOUT  ATTRIBUTE READ  ATTRIBUTE UPDATE

**Add** or import a list of members .

**More** ▾

Members **Privileges** More ▾

The following table lists all entities with privileges on this group.

**Filter for:**

**Update:**

<input type="checkbox"/> Entity name ▾	Admin	Read	Update	OptIn	OptOut	Attribute read	Attribute update	View	Choose action
<input type="checkbox"/> [blurred]	✓	✓	✓	✓	✓	✓	✓	✓	Actions ▾
<input type="checkbox"/> [blurred]	✓	✓	✓	✓	✓	✓	✓	✓	Actions ▾

Hinter **Assign these privileges:** können die Berechtigungen ausgewählt werden. Normalerweise reichen **UPDATE** und **READ**.

**Member name or ID:**  Enter an entity name or ID, or [search for an entity](#).

**Assign these privileges:**  MEMBER  ADMIN  UPDATE  READ  VIEW  OPTIN  
 OPTOUT  ATTRIBUTE READ  ATTRIBUTE UPDATE

**Add** or import a list of members .

Mit **Add** werden die Einstellungen übernommen.

### Mitglieder aus einer Gruppe entfernen

Setzen Sie dazu den Haken vor dem Namen des Mitglieds und klicken Sie **Remove selected members**.

Remove selected members

<input type="checkbox"/>	Entity name ▾	Membership	Choose action
<input checked="" type="checkbox"/>	[redacted]	Direct	Actions ▾

Show: 50 ▾ Showing 1-1 of 1 · First | Prev | Next | Last

## Anlegen von zusätzlichen Gruppen

Zuerst müssen Sie im linken Bereich unter **Browse folders** den Folder öffnen, unter dem Sie die neue Gruppe anlegen möchten. Klicken Sie dann **More actions** und **Create new Group**.

Home > Root > app > Fileserver > zuv > [redacted]

Show details ▾

Folder contents Privileges More ▾

Filter for: Folder, group, or attribute name Apply filter Reset

Name ▾

Up one folder

Show: 50 ▾

Edit folder

Folder actions ▾

- Quick links
- Add to my favorites
- Visualization
- Templates
- New template
- Manage
- Copy folder
- Create new attribute definition
- Create new attribute name
- Create new folder
- Create new group**
- Create new local entity
- Edit folder
- Move folder
- Administration
- Attestation
- Attribute assignments

Geben Sie hinter **Group name** den Namen der neuen Gruppe an. Hinter **Description** kann eine Beschreibung der Gruppe eingetragen werden.

+ Create new group ▾

Home > New group

## New group

Create in this folder: app:Fileserver:zuv: [redacted]  
Enter a folder name or [search for a folder where you are allowed to create new groups](#)

**Group name:** meine-neue-gruppe  
Name is the label that identifies this group, and might change.

**Group ID:** meine-neue-gruppe  Edit the ID  
ID is the unique identifier for this group. It should be short and simple, and might have character restrictions. The ID should rarely change, if ever.

**Description:** Beschreibung der Gruppe  
Description contains notes about the group, which could include: what the group represents, why it was created, etc.

Show advanced properties ▾

Save Cancel

Mit **Save** wird der Vorgang abgeschlossen.



## FAQs

*Kann eine Gruppe in eine Andere aufgenommen werden?*

Ja, das geht. Man könnte die Gruppe **DezX-Leitung** in alle anderen Gruppen des Dezernats X aufnehmen. Dann haben alle Mitglieder von **DezX-Leitung** die Berechtigungen, die die Gruppen haben, in denen **DezX-Leitung** Mitglied ist. Damit kann man vermeiden, dass neue Mitglieder die umfassenden Zugriff benötigen, in alle relevanten Gruppen einzeln aufgenommen werden müssen.

*Kann man die Gruppen, die unter **app** → **Fileserver** erscheinen, auch für andere Services wie z.B. Cloudstore verwenden?*

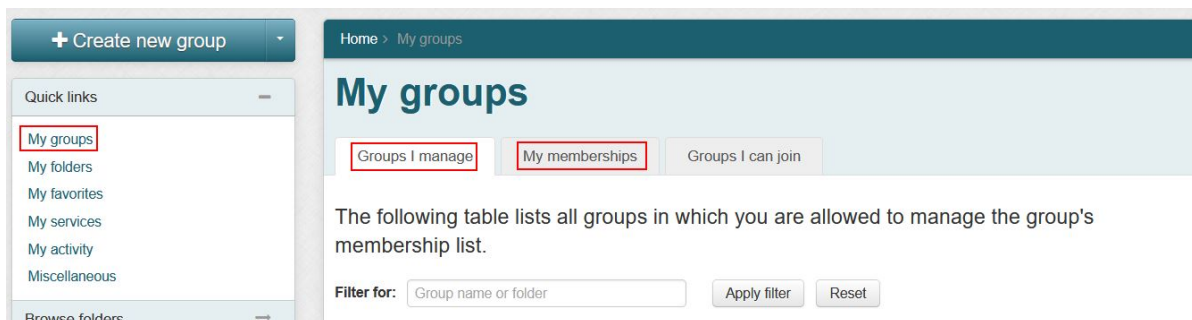
Nein, diese Gruppen können nur für den Fileserver verwendet werden.

*Was ist der Unterschied zwischen **direct** und **indirect** Member?*

Mitglieder einer Gruppe können Personen aber auch andere Gruppen sein! Ein **direct Member** ist eine Person, die Mitglied der aktuellen Gruppe ist. Ein **indirect Member** ist eine Person, die Mitglied einer anderen Gruppe ist, welche wiederum Mitglied der aktuellen Gruppe ist.

*Wie kann ich sehen, in welchen Gruppen ich Mitglied bin und welche Gruppen ich verwalten darf?*

Klicken Sie dazu links oben unter **Quick links** auf **My Groups**. Sie erhalten dann rechts die Schaltflächen **Groups I manage** und **My memberships**. Klicken Sie auf diese Schaltflächen um zu sehen, in welchen Gruppen Sie Mitglied sind bzw. welche Gruppen Sie verwalten dürfen.



*Wie kann ich sehen, in welchen Foldern und Gruppen ein Mitarbeitender Mitglied ist?*

Geben Sie dazu rechts oben im Suchfeld den Namen oder besser den kiz-Benutzernamen der betreffenden Person ein und betätigen Sie anschließend die **Enter-Taste**. Sie erhalten eine Liste mit den Namen, die dem Suchkriterium entsprechen. Klicken Sie dann auf den gewünschten Namen. Es werden die relevanten Folder und Gruppen angezeigt. Hier werden auch Folder und Gruppen angezeigt, die nichts mit dem Fileserver zu tun haben. Gruppen, die auf den Fileserver bezogen sind, enthalten im zugehörigem Folderpfad **Fileserver**. Um das zu erkennen, bewegen Sie die Maus auf die gewünschte Gruppe. Es erscheint eine Messagebox mit dem Folderpfad.

From:  
<https://help.rz.uni-ulm.de/published/> - kiz Infrastruktur - Hilfe Wiki

Permanent link:  
<https://help.rz.uni-ulm.de/published/doku.php?id=allgemein:berechtigung&rev=1682664064>

Last update: **2023/04/28 08:41**

