Berechtigungssystem II

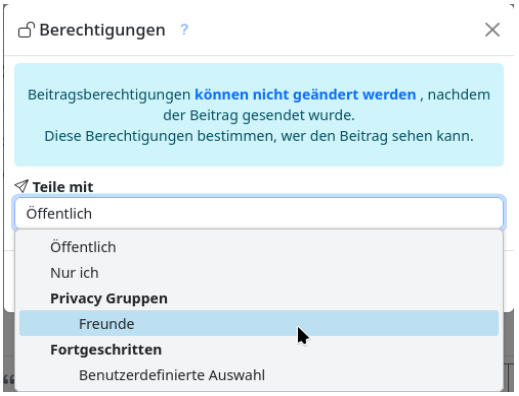
Privacy Gruppen: Helfer und Teil des Berechtigungssystems

Die Privacy Gruppen, die im ersten Teil schon mehrfach angesprochen wurden, haben eine Dreifachfunktion. Einmal kann man sie als eigenständigen Bestandteil des Berechtigungssystems sehen, dann dienen sie als Helfer für die Nutzung der Kontaktrollen und schließlich fungieren sie als Filter für den Stream.

Die App "Privacy Gruppen"

Die Funktionalität für Privacy Gruppen existiert in Hubzilla auch schon, ohne dass die App installiert ist. Wie bereits erwähnt, verfügt jeder neue Kanal über eine Privacy Gruppe mit dem Namen "Freunde".

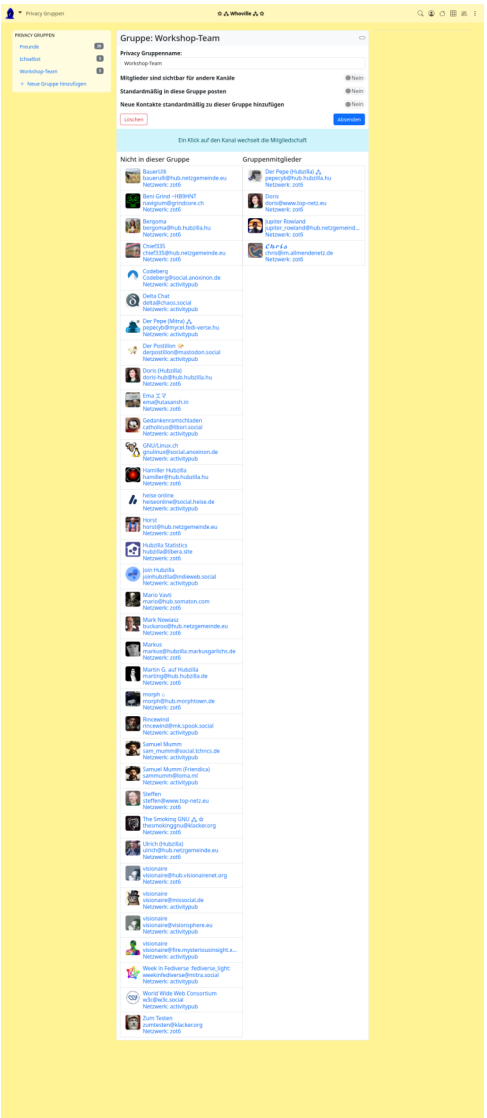
Dass dem so ist, erkennt man aber nur daran, dass eine Privacy Gruppe in den Berechtigungs-Einstellungen (🔓/🔒) zu Inhalten auftaucht: "Privacy Gruppen ⇨ Freunde".



Installiert man die App "Privacy Gruppen", so wird damit letztlich nur die App zur Verwaltung von Privacy Gruppen installiert und zugänglich gemacht. Ohne die App hat man keine Möglichkeit, die eine Gruppe "Freunde" zu betrachten oder Mitglieder hinzuzufügen (ist unerheblich, weil jede neue Verbindung von Anfang an ohnehin automatisch der Gruppe "Freunde" zugewiesen wird) bzw. zu entfernen.

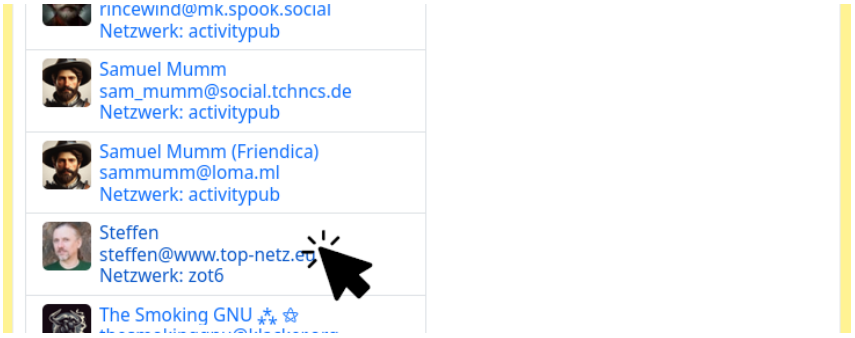
Ruft man die App nach der Installation auf, erscheint die Eingabemaske für das Erstellen einer neuen Privacy Gruppe.

In der Seitenleiste werden die existierenden Privacy Gruppen aufgelistet. Bei einem ganz neuen Kanal ist das, wie gesagt, die Gruppe "Freunde". Wählt man eine Gruppe aus, so werden die Parameter der Gruppe angezeigt und darunter die Verbindungen in zwei Spalten. In der linken Spalte alle Verbindungen, die nicht in der Gruppe enthalten sind. In der rechten Spalte alle Verbindungen, die Mitglied der Gruppe sind.



Bei einem Kanal der Rolle "Öffentlich" ist lediglich die Option "Neue Kontakte standardmäßig zu dieser Gruppe hinzufügen" bei der Standard-Gruppe "Freunde" aktiviert. Bei einem Kanal der Rolle "Persönlich" zusätzlich die Option "Standardmäßig in diese Gruppe posten". Das ist dafür verantwortlich, dass man bei einem persönlichen Kanal grundsätzlich nicht-öffentlich postet, sondern nur an alle seine Verbindungen. Möchte man mit einem persönlichen Kanal etwas öffentlich posten, muss man dies mit den Berechtigungs-Einstellungen ändern.

Um eine Verbindung, die noch nicht in der Gruppe enthalten ist, dieser hinzuzufügen, muss man lediglich auf die Verbindung in der linken Spalte klicken.



Anschließend ist die Verbindung aus der linken Spalte verschwunden

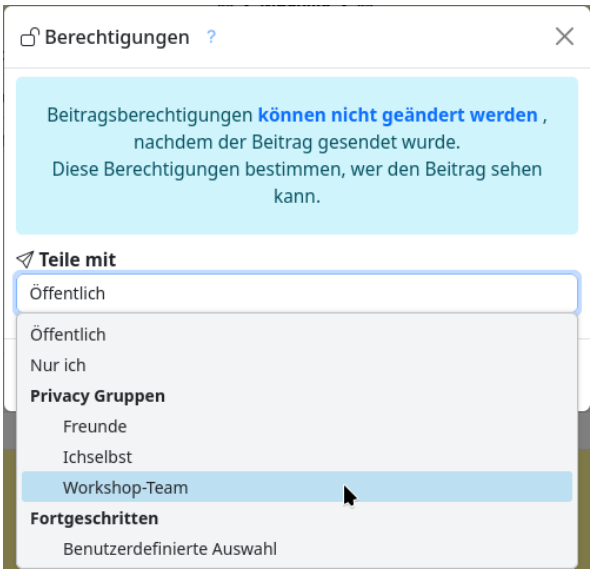
und in der rechten vorhanden

Um eine Verbindung aus einer Gruppe zu entfernen, verfährt man analog. Man klickt auf die zu entfernende Verbindung in der rechten Spalte, worauf diese dort verschwindet und wieder in der linken Spalte erscheint.

Privacy Gruppen als Bestandteil des Berechtigungssystems / Berechtigungs-Einstellungen

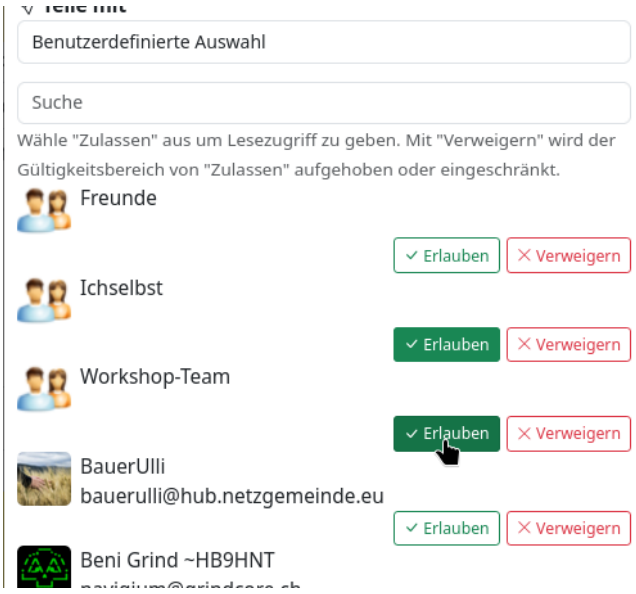
Privacy Gruppen sind Bestandteil der dritten Ebene des Berechtigungssystems, der Berechtigungs-Einstellungen. Die Berechtigungs-Einstellungen, die man bei den Editoren für Inhalte findet, ermöglichen das Teilen des Inhalts an bestimmte Kontakte, aber auch an bestimmte Privacy Gruppen.

Wählt man in den Berechtigungs-Einstellungen direkt eine Gruppe als Ziel, wird der Inhalt nur mit den Mitgliedern der Gruppe geteilt. Ein Posting wird zu einer Direktnachricht, an welcher sämtliche Mitglieder der Privacy Gruppe beteiligt sind. Die Konversation ist damit nicht-öffentlich und ein solches Posting kann auch nicht weitergesagt oder geteilt werden. Dateien sind nur durch die Verbindungen in der Privacy Gruppe verfügbar.



Möchte man an mehr als nur die Mitglieder einer einzelnen Privacy Gruppe teilen, benötigt man aber eine Mehrfach-Auswahl. Diese findet man unter "Benutzerdefinierte Auswahl". Hier tauchen alle Verbindungen auf und man kann für jede einzelne Verbindung festlegen, dass der Inhalt mit ihr geteilt wird.

Oberhalb der einzelnen Verbindungen werden außerdem auch die vorhandenen Privacy Gruppen aufgeführt. Damit kann man dann die Berechtigung für den Inhalt auf eine oder Mehrere Gruppen festlegen.

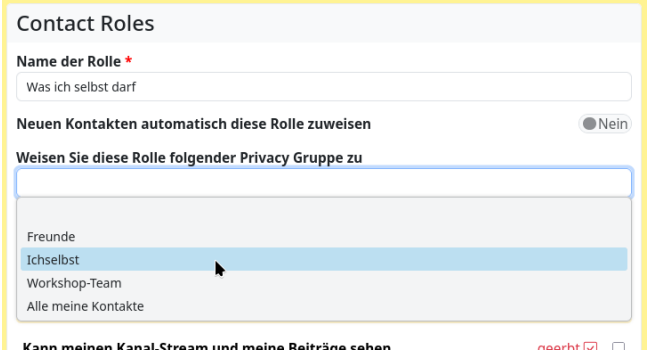


Mit den Berechtigungs-Einstellungen ist es also möglich, Inhalte mit bestimmten Verbindungen zu teilen und man kann die Privacy Gruppen für eine sinnvolle Gruppierung von berechtigten Verbindungen nutzen.

Privacy Gruppen als Helfer für die Kontaktrollen

Eine weitere Funktion von Privacy Gruppen ist die Hilfs-Funktion für die Kontaktrollen.

Hat man eine Kontaktrolle erzeugt, so kann man diese natürlich allen gewünschten Verbindungen einzeln zuweisen. Manchmal möchte man aber eine bestimmte Kontaktrolle für eine größere Anzahl von Kontakten am liebsten auf einen Rutsch zuweisen. Dafür erstellt man einfach eine entsprechende Privacy Gruppe, welche genau diese Verbindungen enthält. Nun kann man in der App "Contact Roles" die Kontaktrolle öffnen und im Auswahlfeld "Weisen Sie diese Rolle folgender Privacy Gruppe zu" einer ganzen Gruppe die Kontaktrolle zuweisen.

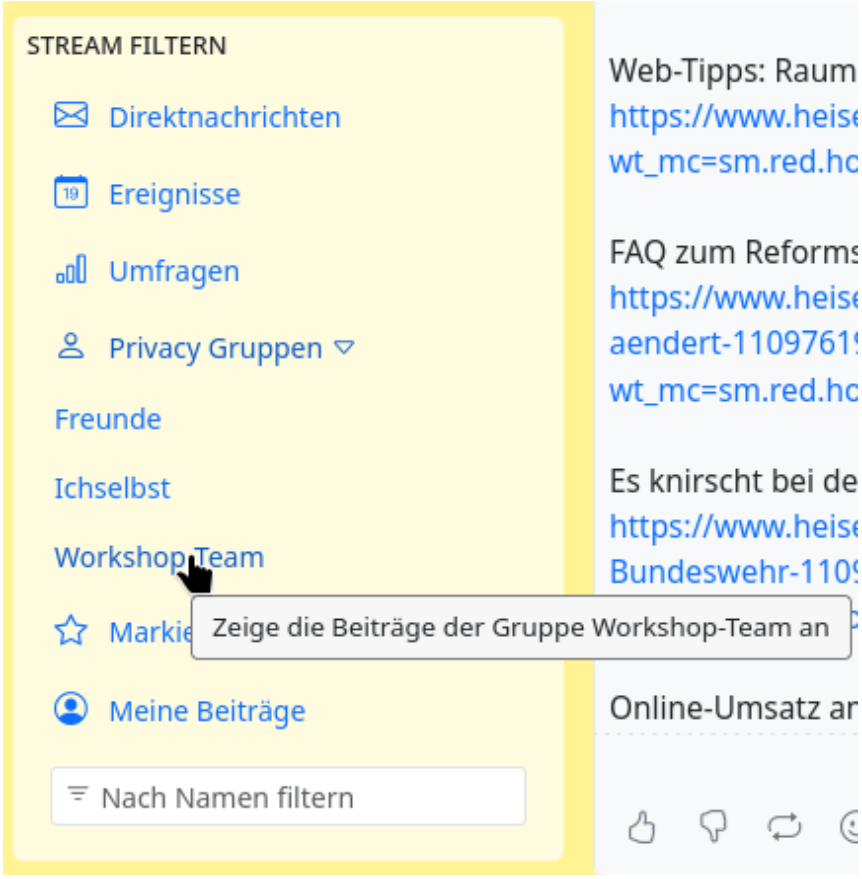


Beachte: Jeder Verbindung kann nur eine einzige Kontaktrolle zugewiesen werden. Weist man einer Verbindung über eine Privacy Gruppe eine Kontaktrolle zu, so wird diese zur aktuellen Kontaktrolle für die Verbindung. Dies gilt außerdem nicht rückwirkend. Die Kontaktrolle wird nur den Verbindungen zugewiesen, die zu diesem Zeitpunkt Mitglied der Privacy Gruppe waren. Fügt man später weitere Verbindungen zu der Gruppe hinzu, erhalten diese nicht automatisch die gerade zugewiesene Kontaktrolle, sondern diejenige, welche als Standard für neue Verbindungen eingestellt ist. Man muss also ggf. die Zuweisung, wenn mehrere Verbindungen der Privacy Gruppe zugefügt wurden, erneut durchführen, damit wieder alle auf dem selben Stand sind.

Privacy Gruppen als Filter für den Stream

Diese Funktion der Privacy Gruppen gehört streng genommen nicht zum Berechtigungssystem, weil damit lediglich die Stream-Ansicht gefiltert wird.

In der Stream-Ansicht findet man in der Seitenleiste die Karte "Stream filtern". Dort befindet sich auch ein Eintrag "Privacy Gruppen". Wählt man dort nun eine Privacy Gruppe aus, so werden ausschließlich die Inhalte der Verbindungen, welche in dieser Privacy Gruppe enthalten sind, im Stream angezeigt.



Berechtigungs-Einstellungen - die dritte Schicht des Berechtigungssystems

Die Berechtigungs-Einstellungen (🔓/🔒), welche man in den verschiedenen Inhalts-Editoren findet (meistens unmittelbar neben dem Button "Absenden" / "Bearbeiten" oder neben Datei- und Verzeichnisnamen in der Cloud), ermöglichen die Steuerung der Berechtigung für den Zugriff auf den jeweiligen Inhalt.

Wie bereits erläutert, lassen sich Zugriffs-Berechtigungen auf Inhalte mit den Berechtigungs-Einstellungen steuern. Zugriffsparameter:

- Nur ich
- Öffentlich (entsprechend der Kanalrolle)
- Privacy Gruppe
- Forum
- Benutzerdefiniert

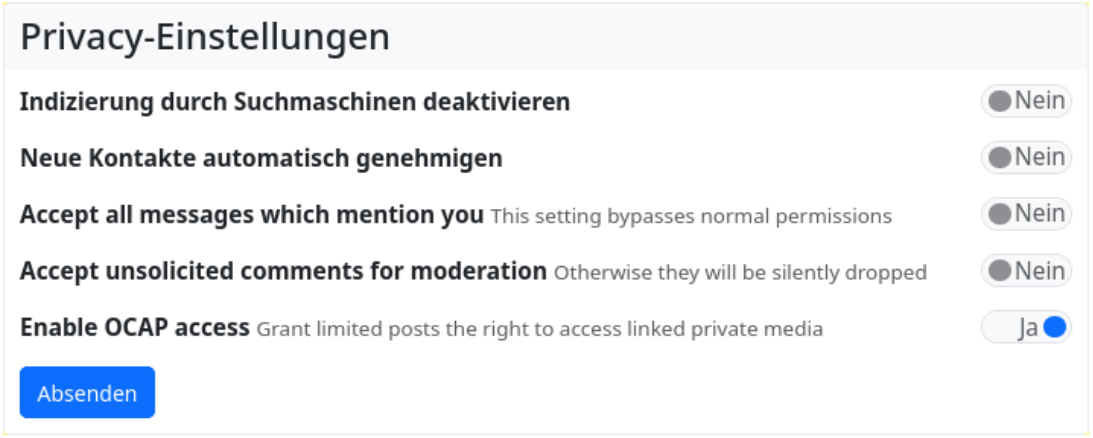
Der Zugriff kann – entsprechend der Kanalrolle – öffentlich erlaubt werden, auf einen selbst beschränkt sein oder auf eine Privacy Gruppe oder ein Community Forum beschränkt bleiben.

Die Auswahl "Benutzerdefiniert" erlaubt eine genau abgestimmte Zuteilung von Berechtigungen. Es stehen hier alle Privacy Gruppen und alle Verbindungen zur Auswahl. Im Modus "Benutzerdefiniert" ist allerdings auch eine Mehrfachauswahl möglich. So können mehrere Privacy Gruppen und mehrere Einzelverbindungen die Genehmigung erhalten, den Inhalt zu sehen und ggf. damit zu interagieren.

Zu jedem Eintrag gibt es zwei Buttons: "Erlauben" und "Verweigern". Mit dem selektieren des Buttons "Erlauben" wird der Verbindung bzw. sämtlichen Mitgliedern der Privacy Gruppe die Berechtigung erteilt. Mit dem selektieren des Buttons "Verweigern" wird der Verbindung bzw. sämtlichen Mitgliedern der Privacy Gruppe die Berechtigung entzogen. Letzteres kann dazu dienen, bestimmte Verbindungen von einem Zugriff auszuschließen, die normalerweise Zugriff auf den Inhalt hätten.

Helfer: Privacy-Einstellungen

Grundsätzliche Einstellungen zur Privatsphäre werden unter Einstellungen ⇨ Privacy-Einstellungen vorgenommen.



Es sind folgende Einstellungen möglich:

- Indizierung durch Suchmaschinen deaktivieren
- Neue Kontakte automatisch genehmigen
- Accept all messages which mention you (*This setting bypasses normal permissions*) Alle Nachrichten akzeptieren, in denen Sie erwähnt werden (*Diese Einstellung umgeht die normalen Berechtigungen.*)
- Accept unsolicited comments for moderation (*Otherwise they will be silently dropped*) Unaufgeforderte Kommentare zur Moderation akzeptieren (*Andernfalls werden sie stillschweigend verworfen.*)
- Enable OCAP access (*Grant limited posts the right to access linked private media*) OCAP-Zugriff aktivieren (*Gewährt bestimmten Beiträgen das Recht auf Zugriff auf verlinkte private Medien*)

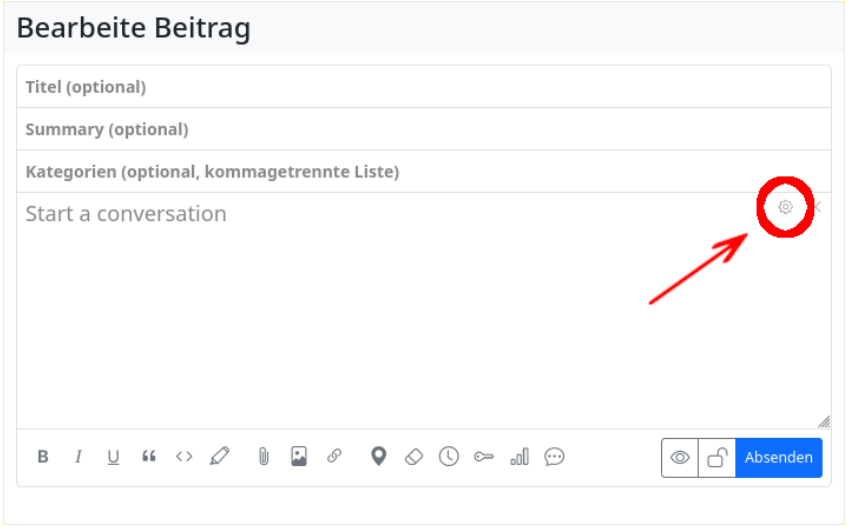
"Accept unsolicited comments for moderation" erlaubt es Nutzern, die eigentlich nicht kommentieren dürfen, einen Kommentar zu einem Beitrag abzugeben. Der Kommentar wird dem Kanalinhaber dann vorgelegt und dieser kann moderierend entscheiden, ob der Kommentar zugelassen oder er verworfen wird. Diese Option ist mit Vorsicht einzusetzen. Sie kann zu höherem Spam-Aufkommen führen. Dabei erscheinen die Kommentare zwar nicht in der Konversation, der Administrator muss aber unter Umständen sehr viele Kommentare moderieren.

Die Option “Enable OCAP access” ermöglicht den Zugriff zu verlinkten privaten Medien. OCAP steht für Object-capability model. Diese Option ist sinnvoll, insbesondere wenn man Postings in seinem Stream findet, bei welchen eingebettete Bilder nicht angezeigt werden, weil sie vom Eigentümer mit eingeschränkten Zugriffsberechtigungen veröffentlicht wurden. Dies ist insbesondere für reine ActivityPub-Dienste von Belang, weil diese keine Entsprechung zum Hubzilla-Berechtigungssystem kennen (OWA/Token).

Kommentar-Steuerung

Hat man den Beitrags-Editor entsprechend konfiguriert, kann man für einzelne Beiträge das Kommentieren verbieten oder erlauben.

Die Editor-Einstellungen erreicht man unter settings/features ⇨ Editor, oder indem man im Beitrags-Editor auf das kleine Zahnrad (⚙) oben rechts im Nachrichtenfeld klickt.



In diesen Einstellungen findet man die Option "Kommentare deaktivieren (*Ermöglicht, die Kommentarfunktion für einzelne Beiträge abzuschalten*)". Schaltet man diese Option ein, gibt es in der Toolbar des Beitrags-Editors das Symbol "💬". Die Sprechblase mit den drei Punkten signalisiert, dass Kommentare – der Kanalrolle und der Kontaktrolle folgend – grundsätzlich erlaubt sind. Klickt man auf das Symbol, verschwinden die drei Punkte (💭). Nun sind Kommentare für diesen Beitrag komplett deaktiviert.

Nicht wirklich Berechtigungssystem, aber trotzdem Privatsphäre-Features

Neben den hier aufgeführten Komponenten des Berechtigungssystems von Hubzilla gibt es noch einige weitere Funktionen, welche die Privatsphäre schützen bzw. unerwünschte Inhalte verbergen.

Inhaltsfilter auf Kanalebene

Inhaltsfilter auf Kanalebene ermöglichen es, bestimmte Inhalte aus dem eigenen Stream auszufiltern bzw. nur bestimmte Inhalte überhaupt in den Stream aufzunehmen. Konfiguriert werden diese unter Einstellungen ⇨ Kanal-Einstellungen in den Filterfeldern "Beiträge mit diesem Text nicht importieren" bzw. "Nur Beiträge mit diesem Text importieren".

Inhaltsfilter auf Kontaktebene

Inhaltsfilter auf Kontaktebene erlauben es, bestimmte Inhalte, die eine bestimmte Verbindung veröffentlicht, auszufiltern bzw. nur bestimmte Inhalte, die eine bestimmte Verbindung veröffentlicht, in den eigenen Stream aufzunehmen. Sie werden im Verbindungseditor im Reiter "Filter für den Inhalt" konfiguriert.

Weitergehende Informationen zu den Inhaltsfiltern findet Ihr in den Dokumenten und der Aufzeichnung des ersten Hubzilla-Workshops vom 17. September 2025, bei dem es um genau dieses Thema ging.

NSFW

Die App "NSFW" ist ebenfalls eine Filter-Variante für den eigenen Stream. Mit NSFW kann man bestimmte Inhalte im eigenen Stream ausblenden, also hinter einer Schaltfläche verstecken, so dass der eigentliche Inhalt erst nach Klick auf diesen Button erscheint. In der App kann man eine Reihe von Wörtern (auch reguläre Ausdrücke sind möglich und das Filtern nach Sprache des Beitrags) angeben. Tauchen diese nun in einem Beitrag auf, wird der Inhalt des Beitrags zunächst verborgen und kann durch Klick auf die entsprechende Schaltfläche angezeigt werden.

Superblock

Mit der App "Superblock" ist es möglich, auch fremde Nutzer (also Fediverse-Nutzer, zu denen man selbst keine Verbindung hat) im Stream zu blocken. Während der normale Block nur bei Verbindungen funktioniert, kann man mit Superblock auch Nutzer aus dem eigenen Stream aussperren, mit denen man nicht verbunden ist. Postings solcher Nutzer können im Stream erscheinen, wenn diese z.B. einen Kommentar zu einem Posting einer Verbindung abgegeben haben oder wenn ihre Beiträge durch eine eigene Verbindung wiederholt werden.

Im Avatarbild des Kanals gibt es ein kleines weißes Dreieck. Klickt man darauf und hat man die App Superblock installiert, gibt es im sich daraufhin öffnenden Menü den Eintrag "Vollständig blockieren", mit welchem man den Nutzer auf die Superblock-Liste bringt. Beiträge dieses Kanals erscheinen nun überhaupt nicht mehr im Stream.

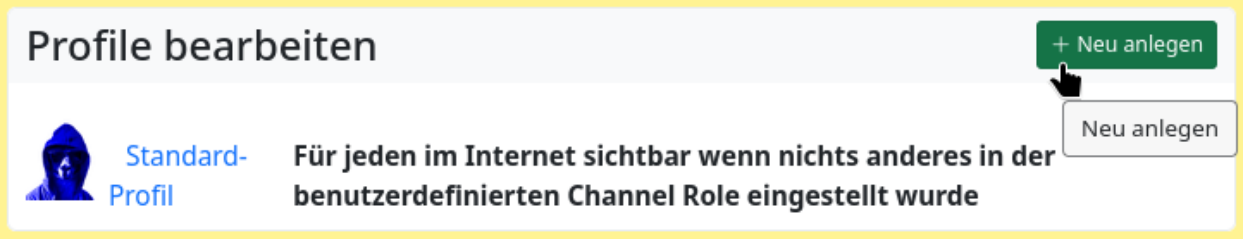
Ruft man die App selbst auf, wird die gesamte Superblock-Liste angezeigt. Hier kann man auch bei Bedarf einzelne Kanäle wieder aus der Liste entfernen und den Block damit aufheben.

Profil / Profile

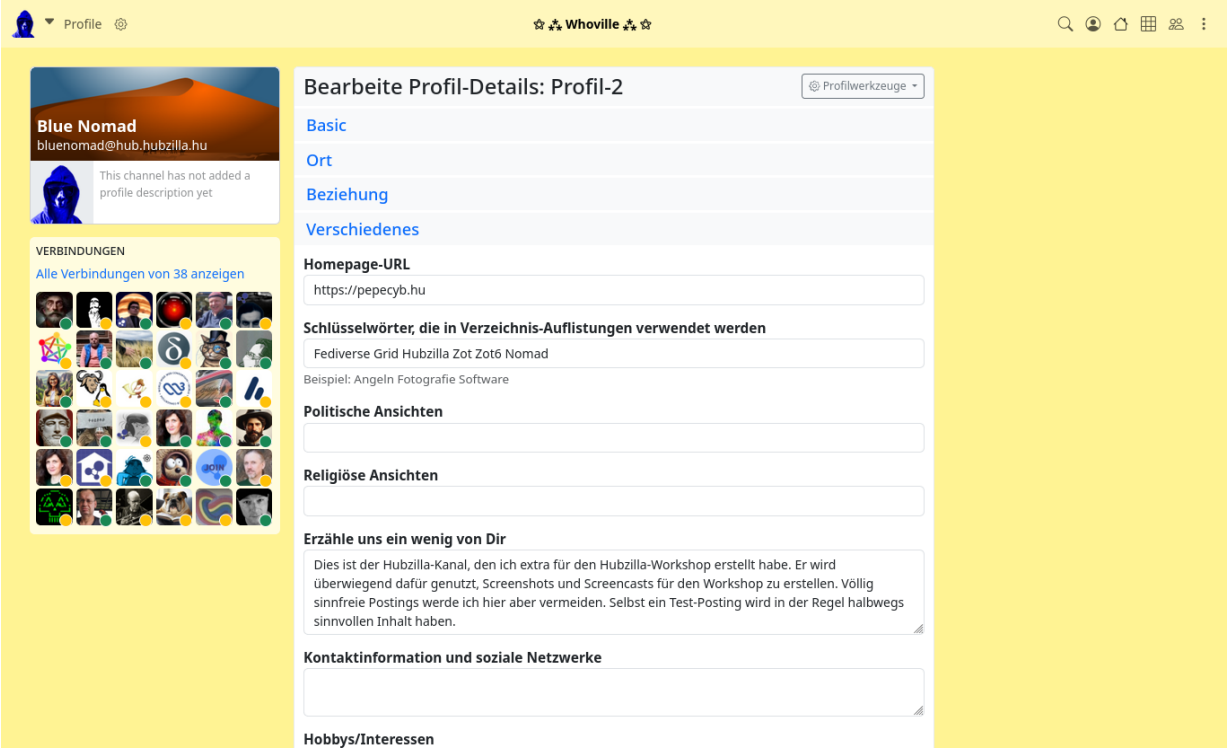
Obwohl nicht sofort offensichtlich, sind auch die Profile Teil des Berechtigungssystems. Das Profil eines Kanals ist sozusagen die Visitenkarte der Identität. Im Profil kann man Informationen zum Kanal (womöglich auch zur Person, die hinter dem Kanal steht) preisgeben. Wer auf Interaktion hofft und Verbindungen wünscht, sollte hier zumindest die Grundlegenden Informationen anbieten. Dieses Thema wurde bereits im zweiten Hubzilla Workshop besprochen (ab Minute 11:19).

Mit der Berechtigung “Kann mein Standardprofil sehen“ legen wir fest, wer dieses Profil einsehen kann und damit die Informationen erhält. Dafür können wir aus den Berechtigungen auswählen, die zur Verfügung stehen. Mit “Jeder im Internet“ machen wir unsere Profilinformationen vollkommen öffentlich. Dies ist die Voreinstellung bei allen Kanalrollen. Um dies einzuschränken, müssen wir die Kanalrolle “Benutzerdefiniert“ verwenden. Mit den Einschränkungen können wir den Kreis derer, die unser Profil sehen können, begrenzen. Hubzilla erlaubt es aber, mehrere Profile für einen Kanal zu erstellen. So kann man, wenn Bedarf besteht, weitere Profile, also quasi weitere “Visitenkarten“, erstellen, die andere oder mehr Informationen bieten, und diese dann bestimmten Verbindungen anzeigen.

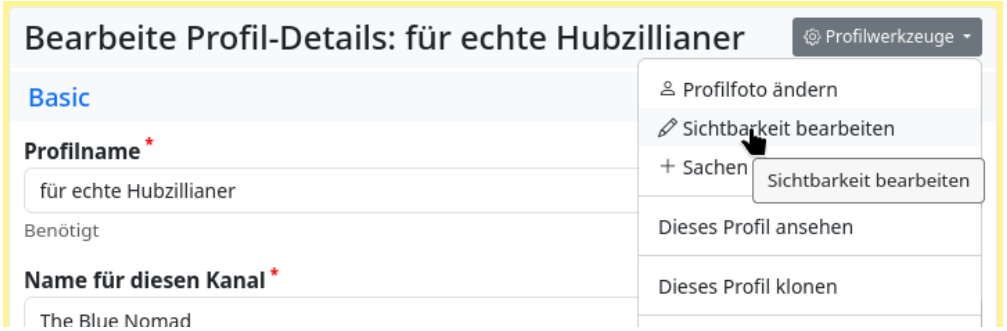
Um weitere Profile anzulegen und ihre Sichtbarkeit festzulegen, wählt man im Hauptmenü “Profile bearbeiten“. Dort werden dann alle vorhandenen Profile angezeigt (bei neuen Kanälen lediglich das Standardprofil).



Nun kann man über den Button “+ Neu anlegen“ ein neues Profil erzeugen, das man dann mit den gewünschten Informationen befüllt.



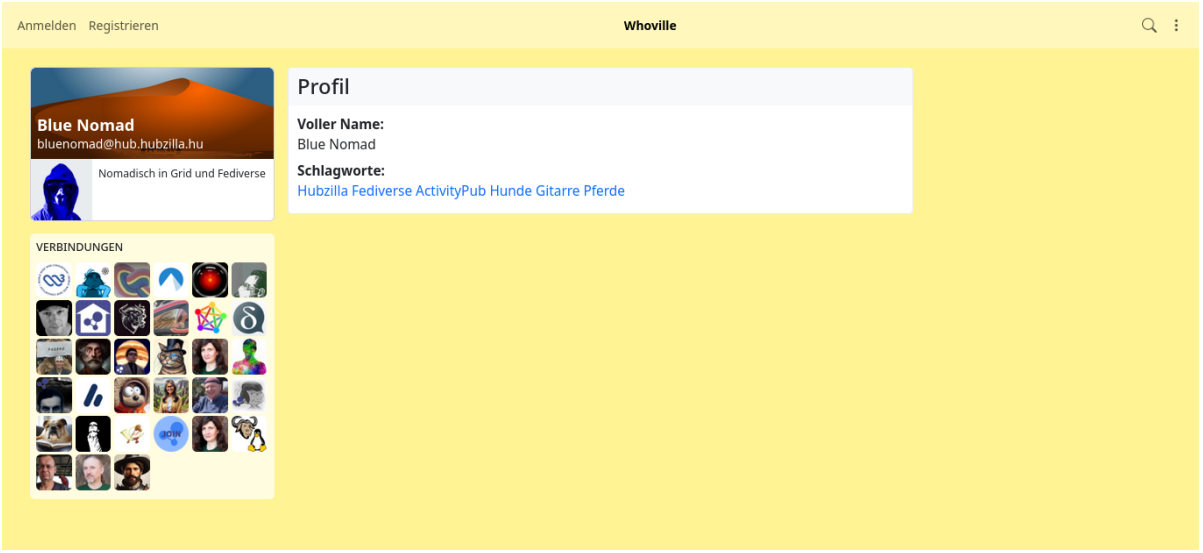
Jetzt muss man nur noch festlegen, welche Verbindungen dieses spezielle Profil präsentiert bekommen. Dies erfolgt, indem man oben rechts aus dem Menü “Profilwerkzeuge“ den Menüpunkt “Sichtbarkeit bearbeiten“ auswählt.



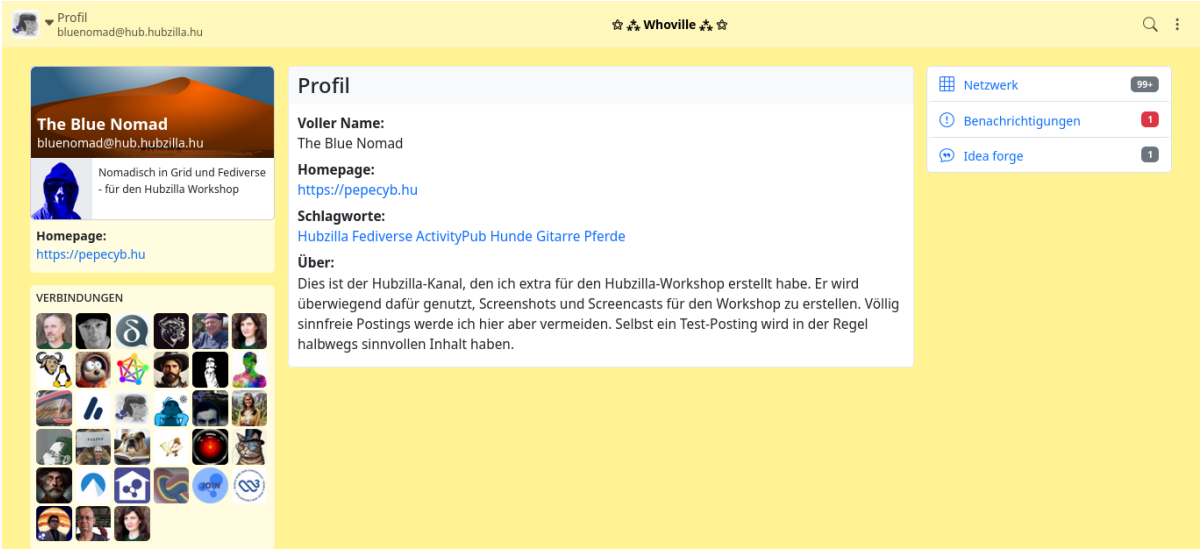
Es wird nun eine Ansicht mit zwei untereinander liegenden Blöcken von Verbdinungen geöffnet, wobei der obere Block diejenigen Verbindungen enthält, welchen das neue Profil gezeigt werden soll, und der untere alle Kontakte, die lediglich (bei entsprechender Berechtigung) das Standardprofil.

Hier kann man nun mit einem einfachen Klick auf das Profilbild der Verbindung diese zwischen beiden Blöcken hin und her schieben.

Ruft nun jemand das Profil auf, der nicht zu der speziellen Gruppe gehört, oder der (bei öffenlicher Berechtigung) gar nicht authentifiziert ist, wird diesem das Standard-profil angezeigt.



Den zugewiesenen Verbindungen hingegen wird nun das neue Profil angezeigt (sie haben die Berechtigung dafür - also ist das auch Teil des Berechtigungssystems).



Was alles möglich ist

Was kann man mit diesem Berechtigungssystem nun aber eigentlich anfangen? Die Antwort ist: ALLES!

08/15

Wenn man sich keinen Kopf über Berechtigungen machen möchte und Hubzilla einfach nur als Zugang für das Soziale Netzwerk des Fediverse verwenden möchte, kann man dies out of the box tun, indem man die Kanalrolle "Öffentlich" bei Kanalerstellung auswählt. Man muss nicht unbedingt noch an irgendetwas rühren.

Möchte man sofort oder später einige Dinge weitergehend regeln, wie z.B. die Anzeige von Medien Fremder, schaltet man OCAP Access ein und um Kommentare für bestimmte Beiträge zu sperren, muss man auch noch die entsprechende Editor-Option aktivieren. Wenn man unabhängig vom Verbindungsstatus blocken möchte, muss noch Superblock hinzukommen und zur Eigenschutz bietet sich auch noch NSFW an.

Wenn man es einfacher haben möchte, Konversationen auch an geschlossene Nutzerkreise zu steuern, installiert man Privacy Gruppen.

Mehr muss aber nicht.

4711

Wer Social Media möchte, aber etwas mehr Wert auf Privatsphäre legt, der wählt als Kanalrolle "Persönlich". Damit sind zwar einige Funktionen im Vergleich zu "Öffentlich" nicht mehr vorhanden, es sind aber solche, die man ja eben auch vielleicht einschränken möchte. Vor allem aber muss man sich im Klaren sein, dass man fortan nun nicht mehr öffentlich teilt, sondern nur an seine Verbindungen (es sei denn, man ändert dies für einzelne Inhalte explizit über die Berechtigung-Einstellungen).

Spätestens ab dieser Kanalrolle empfiehlt es sich, sowohl die Kontaktrollen-App und die Privacy-Gruppen-App zu installieren, um seine Kontakte ggf. nach unterschiedlichen Berechtigungen zu kategorisieren. Muss aber auch nicht.

foobar

Möchte man eine Gruppen-Konversation, angelehnt an ein Internet-Forum anbieten, wählt man die Kanalrolle "Community Forum". Hier gibt es die selben Berechtigungen und Einschränkungen wie bei der Kanalrolle "Persönlich". Das Wall-to-Wall Posting ist Verbindungen erlaubt, denn diese Art des Postens ermöglicht erst die forenartige Kommunikation. Die Alternative, das Posten im DN-Stil ("@!"), bewirkt bei einem Community Forum das selbe, wie das Wall-to-Wall Posten. Teilen oder Wiederholen von Postings ist hingegen nicht erlaubt, weil die Kommunikation in einem solchen Forum den Verbindungen vorbehalten ist.

Ans Eingemachte

Die Kanalrolle "Benutzerdefiniert" ist das Schweizer Taschenmesser unter den Rollen. Man kann damit die vordefinierten Kanalrollen 1:1 nachbilden, man kann die Standardrollen quasi als Vorlage nutzen und einzelne Berechtigungen schon auf Kanalebene anders regeln oder man baut sich von Grund auf eine eigene Berechtigungs-Hierarchie für seinen Kanal.

So kann man z.B. eine wirklich geschlossene Community erzeugen oder ein echtes nicht-öffentliches Forum. Grundlage jeder Konfiguration sollte sein, sich eine Liste zu erstellen, was mit dem Kanal alles möglich sein soll und wie andere mit unserem Kanal interagieren können sollen. Anhand dieser Vorgaben konfiguriert man nun die einzelnen Berechtigungen der Kanalrolle. "Jeder im Internet" ist dabei das offene Scheunentor. "Nur die, denen Du es explizit erlaubst" ist das abgeschlossene Scheunentor zu welchem man ausgewählten Kontakten mit der Kontaktrolle den Schlüssel zur Verfügung stellt. Die Verwaltung der Schlüssel zum Tor kann man zusätzlich sehr gut mit Privacy Gruppen erledigen.

Es ist übrigens auch nicht verkehrt, ein Community Forum auf diese Art und Weise zu erstellen, wenn man ein eher geschlossenes Forum erzeugen möchte.

Auch völlig nicht-öffentliche Foren sind so möglich und erlaube eine wirklich private Zusammenarbeit.

So arbeiten z.B. wir als Hubzilla-Workshop-Team mit einem solchen Forum. Und weil wir vertrauensvoll in unserem kleinen Team arbeiten, hat jedes Mitglied auch sehr weitreichende Berechtigungen.

Vorneweg: Unser Arbeitsforum existiert ausschließlich im Grid. Logisch, denn als Hubzilla-Workshop-Team verfügen wir alle ja über mindestens einen Hubzilla-Kanal. Die Beschränkung stellt sicher, dass jeder auch wirklich das im Foren-Kanal tun kann, was mit Hubzilla möglich ist.

Jetzt einmal kurz zur Konfiguration unseres Arbeitsforums:

Die Kanalrolle ist natürlich "Benutzerdefiniert". In den Privacy-Einstellungen haben wir die Indizierung durch Suchmaschinen" präventiv noch abgeschaltet, obwohl eine solche Indizierung schon aufgrund der Konfiguration der Rolle unmöglich wäre. OCAP-Access ist ebenfalls aktiviert, falls eines der Mitglieder einmal ein Bild aus der eigenen Cloud einbindet, welches ggf. nicht völlig öffentlich ist.

In den Profileinstellungen wurde die Option "Schlage mich neuen Mitgliedern als möglichen Kontakt vor" deaktiviert. In den Profil-Einstellungen wurde außerdem die Option "Mein Standardprofil im Netzwerkverzeichnis und in Followerlisten veröffentlichen" ebenfalls deaktiviert (damit taucht das Forum nicht mehr in Verzeichnissen auf). Danach wurde in den benutzerdefinierten Berechtigungen (Einstellungen Privacy-Einstellungen ⇨ Benutzerdefinierte Konfiguration der Channel Role) jede Berechtigung auf "Nur die, denen Du es explizit erlaubst" gesetzt.

Um nun den Mitgliedern des Forums (Verbindungen werden nicht automatisch angenommen) die passenden Rechte einzuräumen wurde eine Kontaktrolle angelegt, welche alle Berechtigungen bis auf "Kann meine öffentlichen Beiträge in anderen Kanälen zitieren/spiegeln" erteilt (geerbte Berechtigungen gibt es bei dieser Kanalrollen-Konfiguration ja ohnehin nicht). Wir arbeiten als Team vertrauensvoll und gleichberechtigt im Forum und dürfen damit alles im Forenkanal tun und diesen auch administrieren.

Diese Kontaktrolle haben wir dann allen Forenmitgliedern zugewiesen und hatten damit ein nicht-öffentliches Forum, welches nicht in irgendwelchen Verzeichnissen auftaucht und dessen Inhalte niemand außer uns selbst sehen oder damit interagieren kann.

Wer ein nicht-öffentliches Forum erstellen möchte, aber seinen Mitgliedern bestimmte Rechte nicht einräumen will, lässt diese in der Kanalrolle halt weg.

Auch wenn die Kanalrolle "Benutzerdefiniert" zunächst sehr speziell und kompliziert erscheint, ist sie aber eigentlich diejenige, welche das Besondere an Hubzilla ist und ich würde sie früher oder später jedem empfehlen, der von Hubzilla mehr erwartet, als nur ein 08/15-Fediverse-Dienst zu sein.