

Best Practices und Hinweise

Die folgenden bewährten Methoden und Tipps helfen Ihnen, **Draupnir effektiv und sicher einzusetzen**:

Kontrollraum schützen

Verwalten Sie den Zugang zu Ihrem Draupnir-Kontrollraum sorgfältig. Grundsätzlich sollten nur Sie selbst (und eventuelle Co-Administratoren, denen Sie voll vertrauen) in diesem Raum sein. Jeder, der Zugriff auf den Kontrollraum hat, **kann den Bot steuern** und damit auf alle geschützten Räume Einfluss nehmen. Teilen Sie also keine Einladungen zu diesem Raum leichtfertig aus. Falls Sie in einem Team moderieren, können Sie vertrauenswürdige Kollegen in den Kontrollraum einladen, damit sie ebenfalls Befehle geben können – aber bedenken Sie die volle Rechteübertragung, die damit einhergeht.

Kontrollraum niemals verlassen

Dieser Punkt kann nicht genug betont werden. Sollte der Kontrollraum aus Versehen gelöscht werden oder Sie diesen verlassen, verlieren Sie die Kontrolle über Ihre Draupnir-Instanz. Der Bot bleibt zwar unter Umständen noch in den Räumen und setzt bestehende Listen fort, aber Sie können keine neuen Befehle mehr absetzen oder Einstellungen ändern. In so einem Fall **benachrichtigen Sie sofort den Server-Support**, damit Ihre Instanz ggf. manuell wiederhergestellt oder neu provisioniert werden kann. Am besten vermeiden Sie dieses Szenario von vornherein.

Berechtigungen richtig setzen

Wenn Draupnir meldet, dass ihm Berechtigungen fehlen, reagieren Sie umgehend. Ein häufiger Fehler ist, den Bot zwar in Räume einzuladen, aber ihm keine Admin-Rechte zu geben – dann kann er keine Server-Banns (ACLs) durchsetzen und auch keine hartnäckigen Spammer entfernen. Lesen Sie die Fehlermeldungen im Kontrollraum: Draupnir sagt meist genau, was ihm fehlt. Erteilen Sie dann im Raum die entsprechenden Rechte. Sollten Sie bewusst mit geringeren Rechten arbeiten (z.B. Bot nur Moderator), stellen Sie sicher, dass die Raumkonfiguration (Power-Level für bestimmte Aktionen) entsprechend angepasst ist.

Nicht mit dem Bot „spielen“

Draupnir ist ein mächtiges Werkzeug. Nutzen Sie es verantwortungsvoll. Versuchen Sie nicht, den Bot z.B. zum Spam-Versand zu missbrauchen oder ihn in Räume einzuladen, wo er nichts zu suchen hat. Der Betreiber des Dienstes (hier: datenba.ch) behält sich vor, Nutzer auszuschließen, die den Bot absichtlich fehlgebrauchen. So führt etwa das Versenden von Spam *über* Draupnir zum Ausschluss von der Plattform. Ebenso sollten Sie keine Befehle auf gut Glück in fremden Instanzen ausführen – bleiben Sie bei Ihrer eigenen Instanz und Ihren Räumen.

Effiziente Verwaltung mehrerer Räume

schon erwähnt, ist es sinnvoll, eine Draupnir-Instanz für alle Ihre moderierten Räume zu nutzen, damit Sie eine zentrale Bannliste und Konfiguration haben. Vermeiden Sie die parallele Nutzung mehrerer Bots für denselben Zweck – das würde nur zu Überschneidungen und Verwirrung führen. Draupnir kann hunderte Räume gleichzeitig überwachen; es gibt praktisch keine Begrenzung außer der Serverkapazität. Nutzen Sie also die Möglichkeit, **alles an einem Ort zu steuern**. Sie können thematisch unterschiedliche Banlisten innerhalb Ihrer Instanz anlegen (z.B. pro Thema eine), anstatt unterschiedliche Bots zu betreiben.

Zusammenarbeit und Teilen

Falls Sie mehrere Communities betreuen oder mit anderen Admin-Teams kooperieren, ziehen Sie Vorteile aus Draupnirs *verteiletem Ansatz*. **Teilen Sie Ihre Banlisten** mit anderen, sofern angemessen – z.B. können zwei befreundete Server gegenseitig ihre Spam-Listen abonnieren, um sich gemeinsam zu schützen. Innerhalb Ihrer Organisation können verschiedene Bereichs-Administratoren ihre Listen aufeinander abstimmen (eine zentrale CoC-Liste für alle, aber separate Spam-Listen pro Projekt etc.). Kommunikation ist hier der Schlüssel: stimmen Sie sich ab, welche Listen öffentlich sein sollen und wer was abonniert.

Umgang mit False Positives

Kein Filtersystem ist perfekt. Es kann vorkommen, dass ein harmloser Nutzer auf einer abonnierten Sperrliste landet oder dass eine Protection überreagiert (z.B. löscht Draupnir eine Nachricht, die doch regelkonform gewesen wäre). Gehen Sie folgendermaßen vor:

- **Einzelfall prüfen:** Schauen Sie im Kontrollraum oder im Listenraum nach, warum jemand gebannt wurde. Jede Banlisteintragung enthält meist einen Grund. War es Teil einer externen Liste, und Sie sind damit nicht einverstanden, **entfernen Sie den Nutzer aus Ihrer lokalen Banliste** oder heben Sie den Bann gezielt auf. Mit `!draupnir unban @user:server` können Sie in Ihrer eigenen Liste einen Bann löschen; bei einem externen Listeneintrag müssen Sie ggf. die Liste **deabonnieren**, um den Effekt loszuwerden (oder die Maintainer der Liste kontaktieren).
- **Ausnahmen handhaben:** Draupnir selbst bietet (derzeit) keine elegante "Allow-Liste", um einzelne Benutzer trotz eines Listeneintrags auszunehmen. Deshalb ist die sauberste Methode, den entsprechenden Listeneintrag aus der betroffenen Liste zu entfernen oder die Liste abzubestellen. Planen Sie Ihre Abonnements daher mit Bedacht. Abonnieren Sie nicht blind jede Banliste, sondern nur solche, deren Kriterien Sie vertrauen.
- **Protections feinjustieren:** Sollten automatische Protections zu viele False Positives erzeugen (z.B. das Mention-Limit greift zu früh), justieren Sie die Einstellungen. Viele Protections haben konfigurierbare Schwellen. Mit `!draupnir config set <Protection>.<Parameter> <Wert>` lassen sich diese anpassen (siehe Doku Ihres spezifischen Falls). Notfalls können Sie eine allzu aggressive Protection auch deaktivieren (`!draupnir disable <Name>`), bis Sie eine bessere Einstellung gefunden haben.
- **Kommunikation mit Nutzern:** Erklären Sie ggf. Ihren Raum-Mitgliedern die grundlegenden Regeln und dass ein Moderationsbot mitläuft. So stoßen plötzliche Bot-Aktionen nicht auf völliges Unverständnis. Im Fall eines False Positives entschuldigen Sie

sich transparent und stellen Sie klar, dass Sie die Regeln oder Bot-Einstellungen entsprechend anpassen.

Performance und Zuverlässigkeit

Da Draupnir als AppService zentral läuft, müssen Sie sich um Betriebsfragen kaum kümmern. Es kann aber passieren, dass der Bot **vorübergehend offline** ist (z.B. bei einem Update des Servers). In dieser Zeit reagiert er nicht auf Befehle. Behalten Sie also den Status im Blick – oft kündigen Server-Admins Wartungsfenster an. Draupnir selbst arbeitet in Echtzeit; bei extrem vielen gleichzeitigen Aktionen könnte es leichte Verzögerungen geben, aber in Tests hat sich gezeigt, dass er **sehr reaktionsschnell** ist, da er Änderungen effizient verarbeitet. Sollte Ihr Bot einmal hängen (keine Reaktion zeigt), warten Sie ein paar Minuten. Treten weiterhin Probleme auf, siehe nächster Abschnitt.

Revision #1

Created 2026-01-07 22:37:36 UTC by pacey

Updated 2026-01-07 22:44:16 UTC by pacey