Räume moderieren (Draupnir)

Überblick

Was ist Draupnir

Draupnir ist ein Moderationswerkzeug für Matrix, das entwickelt wurde, um die Verwaltung von Räumen und Communities zu vereinheitlichen und zu erleichtern.

Es handelt sich um einen Fork des bekannten Mjolnir-Bots, jedoch mit zahlreichen Verbesserungen in Bedienung und Funktionalität.

Welche Probleme löst Draupnir konkret?

In wachsenden Matrix-Communities treten oft Spam, Trolle oder koordinierte Störungen in mehreren Räumen gleichzeitig auf. Manuelles Moderieren jedes einzelnen Raums wird schnell unübersichtlich.

Draupnir bietet hierfür eine Lösung, indem es Moderator-Aktionen synchronisiert und raumübergreifend durchsetzt. Beispielsweise kann ein einmal ausgesprochener Bann mit Draupnir auf alle geschützten Räume einer Community angewendet werden.

Zudem unterstützt Draupnir sogenannte Policy Lists (oder Banlisten), in denen vertrauenswürdige Gemeinschaften schwarze Listen von Spam- oder Abuse-Konten führen und gegenseitig abonnieren können. Durch das Abonnieren solcher gemeinschaftlicher Listen profitieren auch Ihre Räume von den Moderationsentscheidungen anderer – ein großer Vorteil im Kampf gegen weit verbreitete Spam-Wellen.

Warum läuft Draupnir als AppService auf datenba.ch?

Draupnir kann entweder als einzelner Bot oder im AppService-Modus betrieben werden. In unserem Fall läuft Draupnir als **Application Service** (AppService) auf dem Synapse-Server `datenba.ch`. Das bedeutet, dass Draupnir fest mit dem Homeserver gekoppelt ist und **mehrere Bot-Instanzen parallel für verschiedene Nutzer bereitstellen** kann.

Für Sie als Endnutzer hat das zwei Vorteile:

1. Sie müssen keinen eigenen Bot hosten oder konfigurieren – jeder Raum-Administrator kann bei Bedarf eine eigene Draupnir-Instanz erhalten, die zentral auf dem Server läuft.
2. Der Ressourcenbedarf ist geringer, da viele Bots in einer AppService-Instanz gebündelt sind

Zudem kann ein AppService erweiterte Rechte erhalten und bestimmte Homeserver-Funktionen nutzen, die einem normalen Bot eventuell verwehrt bleiben (z.B. um Einladungen serverweit zu blockieren oder Accounts zu sperren).

Zusammengefasst: Draupnir im AppService-Modus ist ein effizienter, serverseitig betriebener Moderationsdienst, der Nutzern auf `datenba.ch` ohne eigene Installation zur Verfügung steht.

Draupnir bekommen

Überblick: Draupnir-Instanz provisionieren

Um Draupnir nutzen zu können, benötigen Sie Ihre eigene Draupnir-Bot-Instanz. Auf datenba.ch kann jeder Raum-Administrator eine solche Instanz selbstständig provisionieren.

Die Bereitstellung läuft folgendermaßen ab:

Draupnir-Instanz anfordern

Laden Sie den Haupt-Draupnir-Servicebot (`@draupnir-main:datenba.ch`)in einen Ihrer Räume ein, in dem Sie Administrator sind.

Dieser Servicebot fungiert als „Verteiler“ für neue Instanzen.

Sobald Sie ihn per Matrix-Invite in einen Raum einladen, erkennt der Service Ihre Anforderung.

Automatische Bereitstellung:
Wenn Sie berechtigt sind (i.d.R. alle lokalen Admin-Nutzer, sofern vom Serverbetreiber freigegeben), wird Ihre Anfrage automatisch verarbeitet.

Der Service lehnt die Einladung zum ursprünglichen Raum ab, erstellt im Hintergrund eine neue Draupnir-Bot-Instanz für Sie und bereitet einen Verwaltungsraum vor.

Einladung in den Verwaltungsraum (Kontrollraum)

Kurz darauf erhalten Sie vom Draupnir-Service eine Einladung in einen neuen Raum, der Ihre persönliche Draupnir-Instanz repräsentiert.

Nehmen Sie diese Einladung unbedingt an.

Dieser spezielle Raum dient zugleich als Steuerungsraum und als Policy-Listen-Raum für Ihren Bot.

Sie können sich das als Ihr „Kontrollzentrum“ vorstellen, in dem Sie Befehle an Draupnir senden und wo Draupnir Informationen für Sie bereitstellt.

Voraussetzungen

Stellen Sie sicher, dass Ihr Konto die nötigen Rechte hat.

Sie sollten mindestens in einem Raum Admin sein, um dort den Servicebot einzuladen.

Zudem müssen Räume, die Sie schützen wollen, auf dem Homeserver datenba.ch liegen bzw. von einem lokalen Admin (Ihnen) verwaltet werden.

Externe Nutzer können in der Regel keine Instanz auf einem fremden Homeserver provisionieren, außer der Serverbetreiber erlaubt dies ausdrücklich.

Räume schützen: Draupnir in Räume bringen

Bot in Räume einladen:
Laden Sie Ihren persönlichen Draupnir-Bot (`@draupnir_IhrBot:datenba.ch`) in jeden Raum ein, den er moderieren soll.

Sobald Sie den Bot eingeladen haben, reagiert Draupnir im Kontrollraum mit einer Rückfrage, ob dieser Raum geschützt werden soll.

Sie können dann z.B. per Klick auf einen vorgeschlagenen Button oder Reaktion („OK“) bestätigen.

Bei Bestätigung fügt Draupnir den Raum zu seiner Schutzliste hinzu und markiert dies in der Regel mit einem grünen Häkchen im Kontrollraum.

(Hinweis: Funktioniert die automatische Abfrage nicht, prüfen Sie, ob der Bot ausreichend Berechtigungen hat und ob der Raum eventuell verschlüsselt ist.)

Manueller Befehl:
Alternativ können Sie im Kontrollraum den Befehl
`!draupnir rooms add <Raum>`
nutzen.

Dabei können Sie entweder die Raum-ID oder eine Raum-Alias-URL angeben.

Beispiel:
`!draupnir rooms add https://matrix.to/#/#meinraum:datenba.ch`

Der Bot versucht dann, dem genannten Raum beizutreten und ihn unter Schutz zu stellen.

Beachten Sie: Bei privaten Räumen müssen Sie den Bot-Benutzer zuerst manuell einladen, bevor der Befehl funktioniert, da sonst der Beitritt verweigert wird.

Kontrolle & Empfehlung zur Nutzung

Nachdem Sie alle gewünschten Räume hinzugefügt haben, können Sie mit `!draupnir rooms list` im Kontrollraum überprüfen, welche Räume aktuell geschützt sind.

Tipp:
Sie können eine Draupnir-Instanz für beliebig viele Ihrer Räume nutzen.

Es ist nicht nötig (und oft unübersichtlich), für jeden Raum eine eigene Instanz zu betreiben.

Fügen Sie lieber einen Bot mehreren Räumen hinzu, um zentrale Listen und Einstellungen zu teilen.

Installation und Konfiguration

Hintergrund

Hintergrund:
Die eigentliche Installation und der Betrieb von Draupnir erfolgen serverseitig durch die Administratoren von datenba.ch. Draupnir läuft in einem Docker-Container als AppService im Synapse-Homeserver und nutzt eine dedizierte PostgreSQL-Datenbank im Hintergrund.

Für Sie als Endnutzer bedeutet das: **Sie müssen nichts auf Ihrem eigenen Rechner installieren.**

Alles, was mit Einrichtung gemeint ist, passiert auf dem Server – Ihre Aufgabe beschränkt sich auf die oben beschriebene Provisionierung und ein paar Konfigurationsschritte in Matrix selbst.

Was passiert im Hintergrund (kurz & verständlich)

Was passiert im Hintergrund bei der Einrichtung?

Sobald Sie den Hauptbot eingeladen haben, legt der AppService eine neue Matrix-Benutzer-ID für Ihre Draupnir-Instanz an (einen virtuellen Bot-User) und erstellt den Kontrollraum.

Dieser Raum ist in der Regel nicht Ende-zu-Ende verschlüsselt, da der Bot sonst nicht richtig funktionieren könnte.

Der Kontrollraum dient als Verwaltungs- und Policy-Listen-Raum.

All dies geschieht automatisch durch das System.

Schritte für den Nutzer

Nachdem Ihre Draupnir-Instanz bereitsteht und Sie dem Kontrollraum beigetreten sind, sollten Sie folgende Dinge tun:

Kontrollraum nicht verlassen:

Bleiben Sie unbedingt Mitglied dieses Verwaltungsraums. Er ist Ihre Schnittstelle zu Draupnir. Verlieren Sie den Zugriff darauf (etwa durch Verlassen oder Löschen des Raumes), verlieren Sie die Kontrolle über Ihren Bot.

(Falls das doch passiert, wenden Sie sich an den Support, siehe Abschnitt 6.)

Befehle und Interaktion:

Sie können im Kontrollraum Befehle an Draupnir senden, die immer mit `!draupnir` beginnen.

Zum Beispiel listet `!draupnir help` alle verfügbaren Kommandos und eine Kurzbeschreibung auf.

In vielen Fällen müssen Sie jedoch gar keine komplizierten Befehle eintippen – **Draupnir ist so entwickelt, dass es intuitive interaktive Eingabeaufforderungen (Prompts) verwendet.**

Interaktive Prompts

Beispielsweise:

Wenn Sie den Bot in einen neuen Raum einladen, fragt er automatisch nach, ob er den Raum schützen soll.

Wenn Sie in einem der geschützten Räume einen Nutzer manuell über die Matrix-Oberfläche bannen, erscheint im Kontrollraum eine Nachfrage, ob dieser Bann zu Ihrer globalen Liste hinzugefügt werden soll.

Sie können dann per Klick oder kurze Antwort zustimmen, und der Bann wird raumübergreifend propagiert.

Diese Prompt-Funktion erleichtert die Bedienung enorm, da viele Standardaktionen ohne das händische Eintippen langer Befehle auskommen

Rechteverwaltung

Damit Draupnir effektiv moderieren kann, benötigt der Bot in den zu schützenden Räumen ausreichende Berechtigungen.

Insbesondere muss er in der Lage sein, Benutzer zu kicken/bannen und Raum-Einstellungen wie Sperrlisten (Server-ACLs) zu ändern. Geben Sie Ihrem Draupnir-Bot in jedem geschützten Raum am besten **Admin-Rechte**.

In Matrix erfolgt dies über die **Power-Level-Einstellungen** des Raumes – meist können Sie in Ihrem Client (z.B. Element) den Bot in der Mitgliederliste auf „Admin“ hochstufen. (Alternativ können Sie auch den Befehl `/op @draupnir_IhrBot:datenba.ch 100`
im Raum eingeben, was dasselbe bewirkt.)

Ohne Admin-Rechte wird Draupnir Sie darauf hinweisen, dass ihm Berechtigungen fehlen.

Sollten Sie dem Bot keine vollen Admin-Rechte geben wollen, achten Sie mindestens darauf, dass er **Benutzer bannen** und **Server sperren** kann.

Matrix erlaubt es z.B., das Recht „Server-ACLs ändern“ auf Moderator-Level herunterzustufen – in diesem Fall reicht es, den Bot zum Moderator zu machen.

Beachten Sie aber, dass ein Bot mit gleichem Power-Level wie Sie von Ihnen nicht mehr herabgestuft oder entfernt werden kann, da Matrix das Absenken von gleichberechtigten Admins nicht zulässt.

Es empfiehlt sich also, entweder dem Bot etwas niedrigere Rechte als sich selbst zu geben (z.B. Sie 100, Bot 90) und ggf. die Raum-ACL-Einstellungen anzupassen – **dies sind jedoch fortgeschrittene Konfigurationen**.

Für die meisten Zwecke ist es unkomplizierter, Draupnir einfach zum Admin zu machen und ihm zu vertrauen, da er nur auf Ihre Anweisung tätig wird

Weitere Grundeinrichtung:

Ihre Draupnir-Instanz besitzt von Anfang an eine eigene Policy-Liste (Banliste) – meist verkörpert durch den Kontrollraum selbst.

Sie können diesen Umstand prüfen, indem Sie `!draupnir status` im Kontrollraum ausführen; dort sollte Ihre Liste unter „**Subscribed and protected policy lists**“ aufgeführt sein.

Anfangs wird Draupnir außer Ihrer eigenen Liste keine weiteren Sperrlisten abonnieren.

Es ist jedoch empfehlenswert, gleich zu Beginn eine öffentlich verfügbare Spam-Bannliste zu abonnieren, um Schutz vor bekannten Störern zu erhalten.

Eine weit verbreitete Liste ist z.B. die Community Moderation Effort (CME) Spamliste mit dem Alias `#community-moderation-effort-bl:neko.dev`.

Um Draupnir anzuweisen, eine solche Liste zu beobachten, nutzen Sie den Befehl `!draupnir watch <AliasDerListe>`

im Kontrollraum.

Beispiel:
`!draupnir watch #community-moderation-effort-bl:neko.dev`

Ebenso existieren Listen der Matrix Foundation (z.B. `#matrix-org-coc-bl:matrix.org` für Verhaltensregeln oder `#matrix-org-hs-tos-bl:matrix.org` für Server-Sperren), die Sie bei Bedarf abonnieren können.

Jede abonnierte Liste wird vom Bot regelmäßig überwacht und durchgesetzt – d.h. Benutzer oder ganze Homeserver, die dort aufgeführt sind, werden aus Ihren Räumen ferngehalten bzw. entfernt.

Mehr dazu im Abschnitt Bedienung.

Verschlüsselung (E2EE): was geht, was nicht

Verschlüsselung beachten:

Im AppService-Modus unterstützt Draupnir aktuell keine Ende-zu-Ende-Verschlüsselung (E2EE).

Das bedeutet, dass Ihr Kontrollraum unverschlüsselt sein muss – andernfalls könnte der Bot Ihre Kommandos nicht lesen.

Auch geschützte Räume, die e2e-verschlüsselt sind, stellen eine Einschränkung dar:

Draupnir kann in solchen Räumen zwar grundsätzlich noch Benutzer anhand ihrer IDs bannen oder bekannte Spam-Server blockieren, jedoch keine Inhalte prüfen.

Funktionen, die Nachrichteninhalte analysieren (z.B. Wortfilter oder das Erkennen eines ersten Bild-Posts), greifen in E2EE-Räumen nicht zuverlässig, da Draupnir die verschlüsselten Events nicht entschlüsseln kann.

Dennoch kann Draupnir grundlegende Protektionen in verschlüsselten Räumen ausführen, solange diese keine Klartext-Inhalte benötigen.

Fazit: Für öffentliche Räume, die moderiert werden sollen, empfiehlt es sich, auf Verschlüsselung zu verzichten, oder zumindest die Limitierungen im Hinterkopf zu behalten.

Der Kontrollraum selbst sollte immer unverschlüsselt und nur für Sie (und ggf. Mit-Administratoren) zugänglich sein.

Installation: Was Nutzer wissen müssen

Installation und Konfiguration (aus Nutzersicht)

Die eigentliche Installation und der Betrieb von Draupnir erfolgen serverseitig durch die Administratoren von datenba.ch.

Draupnir läuft in einem Docker-Container als AppService im Synapse-Homeserver und nutzt eine dedizierte PostgreSQL-Datenbank im Hintergrund.

Für Sie als Endnutzer bedeutet das:
Sie müssen nichts auf Ihrem eigenen Rechner installieren.

Alles, was mit Einrichtung gemeint ist, passiert auf dem Server – Ihre Aufgabe beschränkt sich auf die Provisionierung und die Konfiguration innerhalb von Matrix selbst.

Bedienung im Alltag

Globale Sperrlisten (Policy Lists) verstehen

Wie bereits erwähnt, arbeitet Draupnir mit Banlisten-Räumen, in denen gesperrte Benutzer-IDs und Server verwaltet werden. Ihre eigene Instanz hat mindestens eine solche Liste (Standard-Banliste für Ihre Community).

Einträge in dieser Liste – z.B. `@spamuser:spam.com` oder ganze Homeserver wie `spam.com` – bedeuten, dass Draupnir alle diese Nutzer serverweit aus Ihren Räumen fernhält.

Sie können weitere eigene Listen erstellen (etwa getrennt nach Spam vs. CoC-Verstößen) mit `!draupnir list create ...`.

Wichtig ist: Jede Liste ist technisch gesehen ein Matrix-Raum mit eigener Raum-ID bzw. Alias, und Draupnir hält die Sperreinträge als Raum-State dort fest.

Dies ermöglicht es, Listen mit anderen Communities zu teilen: Andere Draupnir- oder Mjolnir-Bots können Ihre List-Räume abonnieren, und Sie können umgekehrt öffentliche List-Räume Dritter abonnieren.

Durch solches „Abonnieren“ (Watch) werden fremde Banlisten in Ihren Räumen wirksam.

Praktisch heißt das, wenn z.B. eine Nachbargemeinschaft eine Spam-Liste pflegt und Sie diese abonnieren, werden alle dort gelisteten Störenfriede auch in Ihren Räumen gebannt, ohne dass Sie jeden selbst entdecken müssen.

Diese verteilte Moderation hält das Matrix-Netzwerk sicherer.

Hinweis: Welche Listen Sie abonnieren, sollten Sie sorgfältig auswählen – achten Sie darauf, dass die Betreiber vertrauenswürdig und die Listen aktuell sind. Sie können abonnierte Listen jederzeit mit `!draupnir unwatch <Alias>` abbestellen, falls Sie doch nicht passen.

Raumregeln und Protections

Draupnir verfügt über ein Plugin-System für automatische Schutzmechanismen, sogenannte Protections. Viele davon sind standardmäßig aktiviert, um gängige Spam-Muster zu bekämpfen.

Beispiele für solche Regeln:

- **Neue-Mitglieder-Schutz (New Joiner Protection):** Erkennt, wenn viele neue Nutzer in kurzer Zeit einem Raum beitreten und Nachrichten senden, und kann automatisch Gegenmaßnahmen ergreifen.
- **Erste-Nachricht-Bild-Sperre:** Verhindert, dass neu beigetretene Nutzer als erste Nachricht direkt ein Bild oder eine Datei senden.
- **Erwähnungs-Limit (Mention Limit Protection):** Limitiert die Anzahl der Benutzer, die in einer einzelnen Nachricht erwähnt werden können.
- **Voice/Video-Message-Filter:** Kann so eingestellt werden, dass Sprachnachrichten oder bestimmte Medientypen automatisch entfernt werden.
- **Trusted Invite Blocker:** Blockiert serverweit Einladungen von Nutzern oder Homeservern, die auf Sperrlisten stehen.
- **Automatisierte Raum-Schließung (Room Takedown):** Kann im Extremfall einen Raum gezielt unzugänglich machen.

Die meisten dieser Protections lassen sich ein- oder ausschalten und oft auch konfigurieren.

Als Raum-Admin können Sie z.B. per Befehl `!draupnir protections` eine Liste aller verfügbaren Module erhalten. Mit `!draupnir enable <ProtectionName>` oder `disable` können einzelne Module gesteuert werden.

Einige erweiterte Einstellungen erfolgen über `!draupnir config ...` Befehle. Details finden Sie bei Bedarf in der offiziellen Protections-Dokumentation des Draupnir-Projekts.

Meldungen (Reports) und „Trusted Reporters“

Matrix bietet Benutzern die Möglichkeit, anstößige oder regelwidrige Inhalte über die Melden-Funktion dem Raum-Admin bzw. Server-Admin zu melden.

Draupnir kann – sofern entsprechend konfiguriert – diese Meldungen auswerten und darauf reagieren.

Insbesondere gibt es eine Protection namens **Trusted Reporters**. Hier können Sie bestimmte User Ihrer Community als „Trusted“ markieren.

Wenn dann genügend dieser vertrauenswürdigen Nutzer dieselbe Nachricht melden, kann Draupnir automatisch Maßnahmen ergreifen.

Zum Beispiel könnte ab einer Meldeschwelle von drei vertrauenswürdigen Reports die gemeldete Nachricht automatisch vom Bot redigiert werden.

Es lassen sich auch Schwellen für automatische Banns definieren.

Voraussetzung ist, dass Abuse Reporting in Ihrer Draupnir-Instanz aktiviert ist und der Bot regelmäßig neue Reports vom Server abfragt.

Im Alltag bedeutet dies: Wenn Sie Meldungen erhalten, können Sie entweder selbst tätig werden oder – falls Trusted Reporters aktiv sind – darauf vertrauen, dass Draupnir bei einer Häufung von Meldungen reagiert.

Alle eingehenden Reports aus Ihren geschützten Räumen kann Draupnir auch im Kontrollraum protokollieren (je nach Konfiguration), sodass Sie einen Überblick über gemeldete Inhalte haben.

Beachten Sie, dass diese Features meist mit erweiterten Rechten einhergehen und u.U. nicht in jeder Draupnir-Instanz auf Gemeinschaftsservern aktiviert sind.

Nutzung über den Matrix-Client (Kontrollraum und Prompts)

Die Interaktion mit Draupnir erfolgt vollständig über Matrix – es gibt keine separate Web-Oberfläche im klassischen Sinne, sondern Sie bedienen den Bot bequem in Ihrem Matrix-Client (z.B. Element Web/Desktop) durch Nachrichten und vom Bot bereitgestellte Bedienelemente im Chat.

Im Kontrollraum (Ihrer Verwaltungs- und Listenraum) können Sie Befehle eintippen. Alle Kommandos beginnen mit `!draupnir`. Eine Liste erhalten Sie mit `!draupnir help`, die Ihnen einen Überblick über mögliche Aktionen gibt.

Hier einige wichtige Basisbefehle:

`!draupnir rooms list` – listet alle Räume auf, die aktuell vom Bot geschützt werden.

`!draupnir rooms add/remove <Raum>` – fügt einen Raum dem Schutz hinzu bzw. entfernt ihn (siehe Abschnitt Provisionierung).

`!draupnir list create <Kurzname> <Alias>` – erstellt eine neue Policy-Liste (Banliste) mit einem internen Kurznamen und einem Matrix-Alias.

`!draupnir watch <Alias>` – abonniert eine externe Policy-Liste (siehe globale Sperrlisten unten).

`!draupnir ban <User> <Grund>` – bannt einen Benutzer auf allen geschützten Räumen (fügt ihn zur Banliste hinzu).

`!draupnir unban <User>` – hebt einen solchen Bann wieder auf.

Interaktive Prompts im Alltag

Die meisten dieser Aktionen können aber, wie erwähnt, komfortabler durchgeführt werden: Draupnir nutzt ein interaktives Prompt-System, das eng mit dem Matrix-Client zusammenarbeitet.

Räume schützen:
Statt `!draupnir rooms add ...` manuell einzugeben, können Sie einfach den Bot in einen Raum einladen. Der Bot postet daraufhin im Kontrollraum eine Meldung à la „Soll Raum XYZ geschützt werden?“ mit Auswahlmöglichkeiten. Bestätigen Sie mit „OK“ (z.B. als Reaktion oder Button), erledigt Draupnir den Rest für Sie.

Bann propagieren:
Wenn Sie in einem vom Bot überwachten Raum über die übliche Matrix-Funktion einen Störenfried bannen (z.B. via Kontextmenü „Nutzer entfernen“ in Element), registriert Draupnir dies. Im Kontrollraum erscheint dann eine Meldung, die sinngemäß fragt: „Benutzer @abc:example.com wurde in Raum XYZ gebannt. Soll dieser Bann der globalen Liste hinzugefügt werden?“

Wenn Sie zustimmen, wird der Nutzer zur Policy-Liste hinzugefügt und damit in allen geschützten Räumen gebannt. So müssen Sie nicht in jedem Raum einzeln tätig werden – Draupnir synchronisiert es automatisch.

Entbannung:
Ähnlich verhält es sich, wenn Sie jemanden in einem Raum entbannen. Draupnir fragt nach, ob der Eintrag auch aus der globalen Bannliste entfernt werden soll. So können Sie False Positives schnell korrigieren, ohne mühsam an vielen Stellen händisch Anpassungen vorzunehmen.

Listen abonnieren:
Auch beim Abonnieren von Sperrlisten hilft Draupnir interaktiv. Wenn Sie den Bot in einen Raum einladen, der als Policy-List eines anderen Projekts dient, erkennt Draupnir dies in der Regel und fragt, ob er diese Liste beobachten soll. (Alternativ nutzt man `!draupnir watch` wie oben erwähnt.)

Insgesamt ist die Bedienung darauf ausgelegt, möglichst viel über normale Client-Interaktionen zu steuern, sodass klassische Chat-Administratoren intuitiv mit Draupnir arbeiten können. Falls eine Aktion mal nicht über Prompts ausgelöst wird, oder Sie ein Problem per Kommando lösen müssen, steht Ihnen jederzeit `!draupnir help` zur Verfügung sowie die ausführliche Moderatorendokumentation des Draupnir-Projekts (siehe Abschnitt 6 für Links).

Praxisbeispiele

Szenario: Spam-Welle in mehreren Räumen

Stellen Sie sich vor, ein Spam-Bot-Netz postet gleichzeitig Werbung in all Ihren öffentlichen Räumen. Mit Draupnir reicht es, einen Spam-Account in einem der Räume zu bannen – der Bot fragt, ob der Bann global gelten soll, und setzt ihn anschließend in allen geschützten Räumen durch.

Szenario: eine Person eskaliert

Ein Nutzer verstößt gegen Ihre Regeln in mehreren Räumen. Mit einem einzigen !draupnir ban ... wird dieser Nutzer aus allen geschützten Räumen entfernt. Ein späterer !draupnir unban ... hebt den Bann ebenso global wieder auf.

Szenario: Regeln automatisch durchsetzen

Szenario: „Notfall“ / schwere Fälle

Support & Troubleshooting

Räume nach der Provisionierung zuweisen

Nach der Provisionierung – Zuweisung zu Räumen:
Ihre Draupnir-Instanz schützt nicht automatisch all Ihre Räume, sondern Sie müssen festlegen, welche Räume vom Bot moderiert werden sollen.

Dazu gibt es zwei Wege:

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 *verteiltem Ansatz*. **Teilen Sie Ihre Bannlisten** 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 Bannlisteintragung enthält meist einen Grund. War es Teil einer externen Liste, und Sie sind damit nicht einverstanden, **entfernen Sie den Nutzer aus Ihrer lokalen Bannliste** 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 Bannliste, 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.