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.