Resistro Cloud — Kundendokumentation

Kundendokumentation v1.0 · Stand: 2026-05-16 · cloud.resistro.org

Einleitung

Resistro Cloud ist ein sicherer Backup-Service für PostgreSQL, MySQL und MariaDB — ohne komplizierten Setup, ohne Nebenkosten. Sie installieren einen kleinen Agent auf Ihrem Server, wir kümmern uns um den Rest: automatische tägliche Backups, verschlüsselte Speicherung in Europa, Wiederherstellung auf Knopfdruck. Ihre Daten bleiben in der EU, unter Ihrer Kontrolle, und Sie können jederzeit kündigen und Ihre Backups exportieren.

Erste Schritte

1. Registrierung und Plan-Auswahl

1. Besuchen Sie cloud.resistro.org
2. Klicken Sie auf Kostenlos starten oder Plan auswählen
3. Wählen Sie einen Plan, der zu Ihrer Datenbankanzahl und Retention passt (siehe Pläne & Preise weiter unten)
4. Erstellen Sie ein Kundenkonto (E-Mail, Passwort)
5. Zahlung via Paddle — Kreditkarte, Banküberweisung (ab Plan Business) oder Kauf auf Rechnung (nur Enterprise)

2. API-Key generieren

Nach dem Login:

1. Gehen Sie zu Einstellungen → API-Schlüssel
2. Klicken Sie auf Neuen API-Key generieren
3. Kopieren Sie den Key und speichern Sie ihn an einem sicheren Ort (später brauchen Sie ihn für die Agent-Installation)

3. Agent installieren

Melden Sie sich auf Ihrem Datenbankserver an und führen Sie folgende Befehle aus:

```
curl https://cloud.resistro.org/install-agent.sh | sudo sh
```

Dies installiert den [resistro-agent] und aktiviert ihn als Systemdienst. Der Agent verbindet sich danach automatisch mit Ihrem Konto.

4. API-Key konfigurieren

Öffnen Sie die Agent-Konfigurationsdatei:

```
sudo nano /etc/resistro-agent/env
```

Fügen Sie den API-Key ein:

```
RESISTRO_API_KEY=your-api-key-here
RESISTRO_ENDPOINT=https://cloud.resistro.org/api
```

Speichern (Ctrl+X, dann Y) und starten Sie den Agent neu:

```
sudo systemctl restart resistro-agent
```

5. Datenbanken hinzufügen

Im Dashboard unter Datenbanken → Neue Datenbank:

- Datenbanksystem auswählen (PostgreSQL, MySQL, MariaDB)
- Hostname/IP eingeben (z.B. [localhost] oder [db.example.com])
- Port (Standard: 5432 für PostgreSQL, 3306 für MySQL/MariaDB)
- Datenbankname
- Benutzer und Passwort
- Backup-Zeitplan festlegen (z.B. täglich 02:00 Uhr)

Der Agent beginnt dann automatisch mit den Backups nach dem nächsten Heartbeat.

Dashboard-Überblick

Nach dem Login sehen Sie:

Startseite

- Überblick: Anzahl Datenbanken, nächstes geplantes Backup, verfügbarer Speicher
- Letzte Backups: Tabelle mit Status, Größe, Datum und Uhrzeit
- Alert-Benachrichtigungen: Falls Backups fehlgeschlagen sind (mit Link zur Fehlerbeschreibung)

Datenbanken

- Liste aller hinzugefügten Datenbanken mit Status (✓ aktiv, pausiert, ✗ Fehler)
- Klick auf eine Datenbank zeigt:
- Letzte 10 Backups
- Backup-Größe und Retention (wie lange Backups aufbewahrt werden)
- Fehlerlog (falls vorhanden)

Backups

- Chronologische Übersicht aller Backups über alle Datenbanken
- Download-Button für jedes Backup

Einstellungen

- API-Schlüssel verwalten

- E-Mail-Adressen für Alert-Benachrichtigungen
- Kontoquota und verbrauchter Speicher
- Abonnement-Verwaltung

Backups verstehen

Zeitplan und Automatisierung

Jede Datenbank erhält einen Backup-Zeitplan (z.B. täglich um 02:00 Uhr). Der Agent führt das Backup durch und übermittelt das verschlüsselte Archiv an unsere Server in Nürnberg. Sie müssen nichts manuell machen — die Backups laufen vollautomatisch im Hintergrund.

Retention (Aufbewahrung)

Jeder Plan hat eine Retention-Frist:

- Starter: 7 Tage
- Business: 30 Tage
- Professional: 90 Tage
- Enterprise: 365 Tage

Ältere Backups werden automatisch gelöscht. Wenn Sie ein älteres Backup brauchen, können Sie jederzeit ein manuelles Backup erstellen oder upgraden.

Verschlüsselung und Sicherheit

Alle Backups werden AES-256-GCM verschlüsselt — das ist Military-Grade-Verschlüsselung. Wichtig: Der Verschlüsselungsschlüssel liegt ausschließlich bei Ihnen, nicht auf unseren Servern. Selbst wenn jemand einen unserer Server kompromittiert, kann er Ihre Backup-Daten nicht lesen. Sie sind die einzige Person, die Ihre Backups entschlüsseln und wiederherstellen kann.

Restore durchführen

Download aus dem Dashboard

1. Gehen Sie zu Backups
2. Finden Sie das Backup, das Sie brauchen (Datenbank, Datum, Status: ✓ erfolgreich)
3. Klicken Sie auf Download
4. Die Datei wird heruntergeladen: [backup-dbname-2026-05-16.resistro] (verschlüsselt)

Lokal wiederherstellen

Nachdem der Download abgeschlossen ist, verwenden Sie die resistro CLI (Open Source, Releases unter https://git.uuxo.net/UUXO/resistro/releases):

```
# Binary herunterladen und ausführbar machen
chmod +x resistro
sudo mv resistro /usr/local/bin/
```

Entschlüsseln und wiederherstellen:

```
resistro restore \
  --file backup-dbname-2026-05-16.resistro \
  --host localhost \
  --port 5432 \
  --database dbname \
  --user postgres
```

Die CLI liest den Verschlüsselungsschlüssel aus der Umgebungsvariable [RESISTRO_ENCRYPTION_KEY] und spielt das Backup in die Zieldatenbank ein. Der Prozess dauert je nach Größe einige Minuten.

Alternativer Weg (manuell):

```
# Entschlüsseln mit resistro CLI
resistro decrypt \
  --file backup-dbname-2026-05-16.resistro \
  --output backup-dbname-2026-05-16.sql

# Dann manuell importieren
psql -h localhost -U postgres dbname < backup-dbname-2026-05-16.sql
# oder bei MySQL/MariaDB:
mysql -h localhost -u root -p dbname < backup-dbname-2026-05-16.sql
```

Pläne & Preise

Plan	Monatspreis	Datenbanken	Retention	Speicher
Starter	7 €	1	7 Tage	5 GB
Business	29 €	5	30 Tage	50 GB
Professional	79 €	25	90 Tage	250 GB
Enterprise	149 €	unbegrenzt	365 Tage	1 TB

Abrechnung monatlich, kein Vertrag, jederzeit kündbar. Alle Preise netto zzgl. MwSt.

Zahlungsarten:

- Kreditkarte (Visa, Mastercard, American Express) — alle Pläne
- Kauf auf Rechnung — ab Plan Business
- SEPA-Banküberweisung — auf Anfrage

Datenschutz & Sicherheit

Wo sind meine Daten?

Alle Backups werden in Hetzner Object Storage in Nürnberg, Deutschland, gespeichert. Die Daten verlassen Europa nicht und unterliegen dem deutschen und europäischen Datenschutzrecht.

Verschlüsselung

- Transport: TLS 1.3 (Backup-Upload vom Agent zum Cloud)
- Speicherung: AES-256-GCM (jedes Backup wird mit Ihrem eindeutigen Schlüssel verschlüsselt)
- Schlüsselverwaltung: Ihr Verschlüsselungsschlüssel liegt ausschließlich auf Ihrem Server und wird nicht an Resistro Cloud übertragen

Resistro Cloud hat keinen Zugriff auf Ihre Backup-Inhalte — auch nicht zum Support, auch nicht zur Fehleranalyse.

DSGVO-Konformität

- ✓ Datenhaltung in der EU
- ○ Auftragsverarbeitungsvertrag (AVV) — in Vorbereitung
- ✓ Löschung Ihrer Daten auf Kündigungsantrag (und mit 30 Tagen Verzögerung für Datensicherheit)
- ✓ Keine Nutzerdaten-Weitergabe an Dritte
- ✓ Keine Tracking-Cookies, kein Analytics

Kein Vendor Lock-in

Backups sind im resistro-Format gespeichert — dem gleichen Format wie die Open-Source-Version von resistro. Sie können Ihre Daten jederzeit exportieren und mit einem anderen Tool wiederherstellen.

Support & SLA

Service Level Agreement (SLA)

- Verfügbarkeitsziel: 99% monatliche Uptime
- Incident-Reaktionszeit: < 4 Stunden während CET/CEST Geschäftszeiten (Mo–Fr 09:00–17:00)
- Planned Maintenance: Ankündigung mindestens 7 Tage vorher via E-Mail
- Datenintegrität: Backup-Deduplizierung und Checksummen-Verifizierung bei jedem Upload

Support kontaktieren

- E-Mail: support@resistro.org
- FAQ: Siehe unten
- Enterprise-Kunden: Dedizierte technische Ansprechperson nach Vertragsabschluss

---

FAQ

Fragen zur Installation und Kompatibilität

Q: Welche PostgreSQL/MySQL-Versionen werdet ihr unterstützt?

A: PostgreSQL ab 9.6, MySQL ab 5.7, MariaDB ab 10.3. Ältere Versionen können Kompatibilitätsprobleme verursachen — fragen Sie Support, wenn Sie eine ältere Version haben.

Q: Kann ich den Agent auf mehreren Servern installieren?

A: Ja. Ein API-Key funktioniert für alle Server. Jeder Agent verbindet sich eigenständig und sendet seine Backups zum selben Konto. Beachten Sie nur, dass Sie genug Speicherkontingent haben für alle Datenbanken und Retention-Fristen.

Q: Funktioniert der Agent in Docker/Kubernetes?

A: Ja. Der Agent läuft als Container in Docker-Umgebungen. Kubernetes-Deployments sind möglich; spezifische Konfigurationen auf Anfrage.

Fragen zu Backups und Restore

Q: Wie lange dauert ein Backup?

A: Das hängt von der Größe Ihrer Datenbank und Ihrer Upload-Geschwindigkeit ab. Der Agent läuft im Hintergrund ohne die Datenbank zu blockieren.

Q: Was passiert, wenn der Agent ausfällt oder der Server keinen Internet-Zugang hat?

A: Der Agent versucht das Backup erneut beim nächsten Heartbeat (alle 60 Sekunden). Falls es mehrmals fehlschlägt, erhalten Sie eine Alert-Benachrichtigung per E-Mail mit einer Fehlerbeschreibung. Der Agent puffert Backups lokal und sendet sie nach, wenn die Verbindung wiederhergestellt ist.

Q: Kann ich Backups manuell triggern, oder nur nach Zeitplan?

A: Backups laufen nach dem konfigurierten Zeitplan vollautomatisch. Für ad-hoc-Backups außerhalb des Plans wenden Sie sich bitte an den Support.

Q: Wie lange dauert ein Restore?

A: Ein Restore ist so schnell wie Ihre Netzwerkverbindung und Ihre lokale Datenbank-Import-Zeit. Der Download ist typischerweise schnell (Hetzner-Object-Storage ist gut erreichbar aus Deutschland). Das Einspielen in die Datenbank hängt von der Größe und Ihrer Hardware ab.

Fragen zu Kosten und Verträge

Q: Was kostet mich der Agent?

A: Nichts extra. Der Agent ist im Preis enthalten. Sie zahlen nur für die Resistro-Cloud-Pläne, nicht für den Agent selbst.

Q: Was passiert, wenn ich kündige? Kann ich meine Backups mitnehmen?

A: Ja. Bei Kündigung können Sie alle Ihre Backups herunterladen. Sie haben 30 Tage Zeit, um sie abzurufen. Danach werden sie gelöscht. Es gibt keine Sperrfristen oder Lock-in.

Q: Können Sie meine Backups lesen? Brauche ich mir Sorgen um die Privatsphäre zu machen?

A: Nein. Ihre Backups sind verschlüsselt. Resistro Cloud und auch Hetzner haben keinen Zugriff auf den Inhalt. Nur Sie können Ihre Backups mit Ihrem Verschlüsselungsschlüssel entschlüsseln. Das ist ein wesentlicher Vorteil unseres Ansatzes.

Q: Kann ich meinen Plan später upgraden oder downgraden?

A: Ja. Sie können jederzeit upgraden oder downgraden. Bei Upgrade wird der Preisunterschied sofort berechnet, bei Downgrade zum nächsten Abrechnungszyklus angerechnet.

Fragen zu Sicherheit

Q: Wer hat Zugriff auf meine Verschlüsselungsschlüssel?

A: Nur Sie. Der Verschlüsselungsschlüssel liegt ausschließlich auf Ihrem Server — er ist ein separater Schlüssel vom API-Key und wird nicht an unsere Server übertragen. Resistro Cloud hat keinen Zugriff darauf.

Q: Werden meine Backups redundant gespeichert?

A: Ja. Hetzner Object Storage ist auf Hochverfügbarkeit und Redundanz ausgelegt. Ihre Backups sind damit gegen Hardware-Ausfälle gesichert.

Weitere Fragen? Kontaktieren Sie uns unter support@resistro.org oder besuchen Sie unsere Dokumentation unter cloud.resistro.org/docs.