

# ZDiskSnap Server — Bedienungsanleitung

Diese Anleitung beschreibt die tägliche Arbeit mit dem **ZDiskSnap Agent**, dem Programm auf Ihren Windows-Rechnern, über das Sicherung, Wiederherstellung und die Verwaltung des Sicherungsservers (**ZDiskSnap Server**) laufen. Die Einrichtung des Servers selbst übernehmen wir; sie ist nicht Teil dieser Anleitung.

Die Oberfläche des Agenten ist englisch beschriftet. Menüpunkte und Schaltflächen stehen deshalb hier so, wie sie auf dem Bildschirm erscheinen — zum Beispiel **Scheduled Backups** oder **BACKUP NOW**.

## 1. Das Prinzip in drei Sätzen

Der Agent liest die Festplatte Ihres Rechners blockweise aus — im laufenden Betrieb und über den Schattenkopie-Dienst von Windows, damit auch geöffnete Dateien und Datenbanken in sich stimmig gesichert werden. Die Daten gehen verschlüsselt über SSH an den Sicherungsserver, der sie selbst schreibt; Ihre Rechner haben dort keine Freigabe und kein Netzlaufwerk. Nach jeder Sicherung hält der Server einen **Snapshot** fest: einen unveränderlichen Stand, aus dem Sie später einzelne Dateien oder die ganze Platte zurückholen.

Ab der zweiten Sicherung werden nur noch die Blöcke übertragen, die sich geändert haben. Bricht eine Sicherung ab, etwa durch einen Neustart, setzt sie beim nächsten Lauf an der unterbrochenen Stelle fort.

## 2. Anmelden

Der Agent ist ein Werkzeug des Administrators, nicht des Anwenders. Alles, was die Sicherung verändert oder Daten zurückholt, setzt eine **Admin-Anmeldung** voraus.

- Oben rechts steht das Anmeldefeld **Admin-Password**. Das Kennwort vergeben Sie beim ersten Start im Einrichtungsassistenten.
- Das runde Symbol **A** zeigt den Zustand: blau heißt angemeldet, grau heißt nicht angemeldet.
- Ohne Anmeldung sehen Sie den Zustand der Sicherung, können aber nichts umstellen, keine Snapshots öffnen und keine Laufwerke auswählen.
- Das Kennwort ändern Sie, angemeldet, über  **Password** oben rechts.

Die Einstellungen liegen verschlüsselt auf dem Rechner. Wer ohne das Kennwort am Gerät sitzt, kann die Sicherung weder umstellen noch abschalten.

**Lizenz:** Unten links in der Seitenleiste steht der Lizenzstand. Ohne gültige Lizenz sind **BACKUP NOW** und der Zeitplan gesperrt; vorhandene Sicherungen bleiben erreichbar. Über die Schaltflächen dort wird ein Gerät aktiviert, ein Platz für den Umzug auf ein anderes Gerät freigegeben oder — bei Rechnern ohne Internet — eine Lizenzdatei ( `.token` ) eingespielt.

### 3. Die Seitenleiste im Überblick

| Menüpunkt                      | Wofür                                                         |
|--------------------------------|---------------------------------------------------------------|
| <b>Dashboard</b>               | Zustand auf einen Blick, Sicherung von Hand starten           |
| <b>Clients</b>                 | Pool-Zustand, Schlüsseldatei, Aufräumen, Übertragungsoptionen |
| <b>Registered Clients</b>      | alle Rechner, die auf diesen Server sichern                   |
| <b>Client Settings</b>         | Quelllaufwerke, Feineinstellungen, E-Mail-Berichte            |
| <b>VDEVs</b>                   | Festplatten des Servers, Prüfläufe, Plattentausch             |
| <b>Server Settings</b>         | Einstellungen für den ganzen Pool, Notfall-Schreibschutz      |
| <b>Scheduled Backups</b>       | Zeitplan und Aufbewahrung                                     |
| <b>Snapshots</b>               | alle Sicherungsstände, Löschen                                |
| <b>Restore</b>                 | einzelne Dateien aus einem Snapshot zurückholen               |
| <b>Activity Log</b>            | Protokoll der laufenden und letzten Vorgänge                  |
| <b>Replication &amp; Cloud</b> | zweite Kopie auf einem anderen Server oder in der Cloud       |
| <b>VM Backup</b>               | virtuelle Maschinen unter Hyper-V sichern                     |
| <b>Rescue Disk</b>             | Notfall-Stick für die Wiederherstellung eines ganzen Rechners |
| <b>Help</b>                    | eingebaute Kurzhilfe                                          |

Während eine Sicherung oder Replikation läuft, zeigt die Seitenleiste unten den Fortschritt — auch dann, wenn Sie gerade in einem anderen Menüpunkt sind. Prüft der Agent anschließend die Sicherung (Verify), heißt die betroffene Zeile dort wie auf dem Dashboard  **Verify** und ihr Balken läuft für die Prüfung noch einmal von 0 bis 100 %.

### 4. Erste Einrichtung: der Assistent

Beim ersten Start — solange noch kein Server eingerichtet ist — bietet das **Dashboard** den Einrichtungsassistenten an. Später erreichen Sie ihn über ► **Wizard** oben rechts. Er führt in dieser Reihenfolge:

1. **Server Connection** — einen Profilnamen vergeben und die Verbindung zum Sicherungsserver eintragen (Adresse, Port, Benutzer).  **Test Connection** prüft sie sofort.
2. **Backup Pool** — der Assistent sieht nach, ob auf dem Server schon ein Sicherungsspeicher (Pool) besteht. Wenn ja, bekommt der Rechner darin einen eigenen Bereich. Wenn nein, wird der Pool beim Registrieren aus der Festplattenvorgabe unter **VDEVs** angelegt.
3. **Server Settings (global)** — Einstellungen für den ganzen Pool, etwa Kompression. Ob der Pool verschlüsselt ist, ist bei der Einrichtung des Servers festgelegt und hier nur zu sehen.
4. **Client Settings** — die zu sichernden Laufwerke (**Source Drives**) und der Sicherungsmodus:
  -  **Incremental** (*empfohlen*): einmal vollständig, danach nur Änderungen.
  -  **Full backups only**: jedes Mal die ganze Platte. Langsamer, dafür ohne Abhängigkeit von der Kette der Änderungen.

Der Modus lässt sich nach der ersten Sicherung nicht mehr wechseln — erst wieder, wenn alle Snapshots dieses Rechners gelöscht sind.

5. **Backup Schedule** (*optional*) — der Zeitplan, siehe Abschnitt 7.

6. **Email Reports** (*optional*) — Benachrichtigung bei gescheiterter Sicherung und bei Festplattenfehlern (S.M.A.R.T.).

**Bei verschlüsseltem Pool:** Laden Sie die **Schlüsseldatei** direkt nach der Registrierung herunter und bewahren Sie sie an mindestens zwei getrennten Orten auf. **Ohne sie lassen sich die Sicherungen nicht wiederherstellen.** Abschnitt 5 beschreibt, wo Sie sie später noch einmal bekommen.

Ist der Rechner bereits registriert, weist der Assistent darauf hin (**Existing Registration Found**). Wer ihn trotzdem neu durchläuft, entfernt die Registrierung **samt allen Snapshots dieses Rechners** — das lässt sich nicht rückgängig machen. Im Zweifel **Cancel**.

## 5. Der tägliche Blick

### Dashboard

Das Dashboard zeigt Verbindung, Quelllaufwerke, Ziel-Pool mit Gesamt- und freiem Platz, den Zeitpunkt der letzten Sicherung und den Zustand des Servers mit Auslastung, Speicher, Festplatten und Temperaturen.

- **BACKUP NOW** startet eine Sicherung von Hand.
- **II PAUSE** hält eine laufende Sicherung an, **■ STOP** bricht sie ab. Eine abgebrochene Sicherung setzt beim nächsten Lauf an der unterbrochenen Stelle fort.
- Die Anzeige **Network** zeigt die tatsächliche Übertragungsrate, dazu Durchschnitt und Spitze.

### Clients

Hier steht der Zustand des Pools (**Pool Status**) mit allen wichtigen Werten. Dazu:

-  **Download Keyfile** — lädt die Schlüsseldatei eines verschlüsselten Pools herunter, solange der Pool entsperrt ist.
-  **Upload Keyfile** — spielt eine Schlüsseldatei ein und entsperrt den Pool sofort, etwa nach einem Austausch des Servers.
-  **Cleanup Restore Clones** — räumt Zwischenstände auf, die nach einer abgebrochenen Wiederherstellung Platz belegen.
-  **Clear Errors** — setzt die Fehlerzähler des Pools zurück. Das repariert nichts; es macht nur sichtbar, ob neue Fehler hinzukommen.
- Übertragungsoptionen: **Transfer-Kompression** packt die Daten mit zstd (mehrkernig) auf der Leitung – lohnt bei vollen Platten, kostet bei nicht komprimierbaren Daten kaum etwas. **Used-Blocks** liest nur belegte Bereiche. Null-Bereiche werden nie übertragen: Die Sicherung läuft als ein einziger Datenstrom, Lücken gehen nur als kurzer Vermerk über die Leitung und werden auf dem Server als Loch angelegt – dafür gibt es keine Einstellung.

### Registered Clients

Eine Liste aller Rechner, die auf diesen Server sichern — mit Pool, Gesamt- und freiem Platz, Zustand und Schutz. Von hier aus lässt sich ein Rechner abmelden (siehe Abschnitt 11).

### Activity Log

Das fortlaufende Protokoll aller Vorgänge. **Export** speichert es als Datei, etwa zum Weiterleiten an uns; **Clear** leert die Anzeige.

## 6. Einstellungen am Rechner — Client Settings

| Einstellung           | Bedeutung                                                                                                |
|-----------------------|----------------------------------------------------------------------------------------------------------|
| Source Drives         | die physischen Laufwerke, die gesichert werden. Das Systemlaufwerk ist mit <b>SYSTEM</b> markiert.       |
| KeepAlive             | hält die Verbindung während einer langen Sicherung offen; <b>Off</b> schaltet es ab                      |
| Hash-Block-Size       | Blockgröße für den Vergleich. Größer heißt schnellerer Durchlauf, aber gröbere Erkennung von Änderungen. |
| Max Snapshots / Drive | wie viele Stände je Laufwerk aufbewahrt werden; die ältesten fallen danach weg                           |
| SSH Connection        | Verbindung zum Sicherungsserver                                                                          |
| E-Mail Reporting      | Benachrichtigung bei gescheiterter Sicherung oder Festplattenfehler                                      |

Für die E-Mail-Berichte gibt es Prüfkнопfe: **Test Email** schickt eine Probemail, **Test Backup Error** und **Test SMART Error** spielen eine Fehlermeldung durch. Richten Sie die Berichte ein und probieren Sie sie einmal aus — eine Sicherung, die unbemerkt ausfällt, ist das eigentliche Risiko.

Die Grundeinstellungen sind für die meisten Betriebe passend. Ändern Sie die Blockgröße nur nach Rücksprache.

## 7. Zeitplan — Scheduled Backups

| Feld                                    | Bedeutung                                                     |
|-----------------------------------------|---------------------------------------------------------------|
| Enabled                                 | Zeitplan an oder aus                                          |
| Interval                                | <b>Hourly, Daily, Weekly</b> oder <b>Monthly</b>              |
| Time (HH:MM), Day of week, Day of month | wann genau                                                    |
| Verify Backup                           | prüft nach jedem Lauf die Unversehrtheit der Sicherung        |
| Retention (days)                        | wie lange Stände aufbewahrt werden; <b>0</b> heißt unbegrenzt |
| Only if network available               | startet nur, wenn eine Netzwerkverbindung besteht             |

Mit  **Save** speichern. Unter **Schedule Status** stehen nächste und letzte Sicherung.

Der Zeitplan läuft auch, wenn niemand angemeldet ist — der Agent arbeitet als Windows-Dienst. Ist der Server zum geplanten Zeitpunkt nicht erreichbar, versucht er es in kurzen Abständen erneut.

## 8. Snapshots und einzelne Dateien zurückholen

### Snapshots

Unter **Snapshots** stehen alle Sicherungsstände mit Datum, Art (**full** für Vollsicherung, **incr** für Änderungen) und belegtem Platz. Einzelne Stände lassen sich markieren und mit  **Delete selected** löschen.

Eine Änderungssicherung baut auf der Vollsicherung davor auf. Ist die Vollsicherung gelöscht, sind die nachfolgenden Stände verwaist; der Agent markiert sie (**Orphaned incrementals**) und schlägt vor, sie zu entfernen.

### Einzelne Dateien — Restore

1. **Restore** öffnen und den gewünschten Snapshot wählen.

2. Der Stand wird auf dem Server eingehängt; im **File Browser** erscheinen Ordner und Dateien wie in einem Explorer.
3. Dateien mit **Download** herunterladen, ganze Ordner mit  **tar.gz** als gepacktes Archiv.
4. Danach **Unmount** — damit wird der Stand wieder freigegeben.

Der Snapshot selbst bleibt dabei unverändert. Sie holen eine Kopie, Sie schreiben nicht in die Sicherung.

## 9. Ein ganzes Gerät zurückholen — Rescue Disk

Startet ein Rechner nicht mehr, oder ist die Platte getauscht, kommt er über ein **Rescue-Medium** vollständig zurück — Betriebssystem, Programme und Daten. Der Agent baut Rescue-Medien für alle Plattformen:

| Rescue-System             | für                        | Inhalt                                                                             |
|---------------------------|----------------------------|------------------------------------------------------------------------------------|
| <b>Windows (WinPE)</b>    | Windows-Rechner            | Notfall-Windows mit dem Wiederherstellungsprogramm und den Treibern Ihrer Geräte   |
| <b>Linux (x86-64)</b>     | Linux-PCs und -Server      | Rettungssystem mit dem Restore-Menü – startet auch mit eingeschaltetem Secure Boot |
| <b>Raspberry Pi 4 / 5</b> | Linux auf dem Raspberry Pi | Rettungssystem für USB-Stick oder SD-Karte                                         |

Jedes Medium stellt nur Sicherungen seiner eigenen Plattform wieder her.

### Medium erstellen (vorher, nicht erst im Ernstfall)

1. **Rescue Disk** öffnen, als Admin angemeldet.
2. Das **Rescue-System** wählen.
3. Der Agent erstellt immer eine **ISO-Datei** (Raspberry Pi: eine Image-Datei) — für virtuelle Maschinen, iLO/iDRAC-Fernkonsolen oder zum Brennen. Soll zusätzlich ein **USB-Stick** (bzw. eine SD-Karte) entstehen, **Also write to USB drive** anhängen und den Datenträger wählen (mindestens 8 GB). **Er wird vollständig gelöscht.**
4.  **Create ...**. Beim Windows-Medium sucht der Agent vorher im Netz nach erreichbaren Geräten und nimmt deren Netzwerk- und Speichertreiber mit.
5.  **Output Folder** öffnet den Ablageort (`%ProgramData%\ZDiskSnap\Rescue`, nur für Administratoren lesbar).

Server, Port und Benutzer sind bereits eingetragen; die Linux-Medien enthalten zusätzlich den SSH-Schlüssel dieses Agenten — bewahren Sie Dateien und Sticks sicher auf.

Die Netzwerk- und RAID-Treiber **aller gesicherten Windows-Rechner** kommen automatisch in jedes Windows-Medium (jeder Rechner meldet sie nach dem Backup an den Server), dazu die Treiber für virtuelle Maschinen (Proxmox/KVM) und – Option **Vendor driver packs** – die WinPE-Treiberpakete von Dell und HP für Rechner, die noch nicht gesichert werden. Im Notfall lädt das Medium nur die Treiber, die zur Hardware passen.  **Check driver coverage** zeigt je Rechner, ob Netzwerk- und RAID-Controller abgedeckt sind. Für ungewöhnliche Hardware legen Sie Treiber über  **Custom Drivers...** selbst ab.

Erstellen Sie das Medium nach jeder größeren Hardwareänderung neu und testen Sie einmal, ob ein Rechner davon startet.

## Im Ernstfall — Windows-Rechner

1. Stick einstecken (bzw. ISO einbinden) und im Bootmenü (meist **F12**, **F11** oder **Esc**) davon starten. Secure Boot kann eingeschaltet bleiben; im Menü des Mediums **ZDiskSnap Rescue** wählen (startet nach 8 Sekunden von selbst).
2. Die Notfallumgebung lädt die Treiber, verbindet sich per Netzkabel mit dem Sicherungsserver und öffnet das Wiederherstellungsprogramm. Passwort eingeben.
3. Rechner und Zeitpunkt wählen, dann die Zielplatte. Sie muss **mindestens so groß** sein wie die gesicherte.
4. Wiederherstellung starten, danach Medium entfernen und neu starten.

## Im Ernstfall — Linux-Rechner und Raspberry Pi

1. Vom Medium starten (Secure Boot kann eingeschaltet bleiben). Beim Raspberry Pi den **USB-Stick** einstecken und die alte SD-Karte entfernen — der Pi kann die Karte, von der er läuft, nicht überschreiben.
2. Das **Restore-Menü startet automatisch**. Den Linux-Rechner aus der Liste wählen, dann **4) Komplette Disk wiederherstellen** (beim Pi auf die SD-Karte bzw. NVMe).
3. Medium entfernen und neu starten.

Für die Wiederherstellung braucht der Rechner eine Netzwerkverbindung zum Server — ein Kabel ist dafür zuverlässiger als WLAN.

## 10. Die zweite Kopie — Replication & Cloud

Eine Sicherung an nur einem Ort übersteht keinen Brand und keinen Diebstahl. Dafür gibt es zwei Wege, die sich kombinieren lassen.

### ZFS Server Replication

Ein zweiter Sicherungsserver erhält nach jeder Sicherung die neuen Stände. Der Abgleich läuft zwischen den beiden Servern; Ihre Rechner müssen dafür nicht eingeschaltet sein.

- **Secondary Server Host, Port, SSH User on Secondary** eintragen.
- Einmalig  **Deploy Key** — mit dem Kennwort des zweiten Servers. Danach kommt der Abgleich ohne Kennwort aus.
- **Run automatically after each backup** einschalten,  **Save**.
- ► **Replicate Now** startet einen Abgleich von Hand.

Ist ein Abgleich gescheitert, steht das in der Ansicht. Beim nächsten Lauf prüft der Agent, ob ein vollständiger Neuabgleich nötig ist, und erledigt ihn selbst.

### Cloud Backup (rclone)

Die Stände gehen zusätzlich an einen Cloud-Speicher — unter anderem AWS S3, Cloudflare R2, Hetzner Object Storage, Azure, Backblaze B2 und Google Cloud Storage.

1. Einmalig  **Setup rclone** — installiert das Übertragungswerkzeug auf dem Sicherungsserver.
2. **Provider** wählen, Zugangsdaten und **Bucket / Container** eintragen.
3. **Encrypt before upload** einschalten: Dann sieht der Cloud-Anbieter nur verschlüsselte Daten. **Bewahren Sie das Verschlüsselungskennwort sicher auf — ohne es ist die Cloud-Kopie nicht wiederherstellbar.**

4. Speichern.  **Upload Now** startet eine Übertragung von Hand.

Replikation und Cloud laufen nacheinander, nie gleichzeitig. Die Cloud-Kopie wird auch dann übertragen, wenn die Replikation gescheitert ist.

## 11. Server und Festplatten

Diese Bereiche betreffen den Sicherungsserver als Ganzes und damit alle Rechner, die darauf sichern. **Hier wird selten etwas gebraucht — und einiges davon lässt sich nicht rückgängig machen.** Im Zweifel sprechen Sie uns vorher an.

### VDEVs

Zeigt, aus welchen Festplatten der Pool besteht, und bietet die Wartung:

- ► **Start Scrub** — liest den gesamten Bestand und prüft jeden Block. Findet sich ein Fehler, wird er aus der Spiegelkopie repariert. Einmal im Monat empfohlen.
- ⚙ **Replace Disk** — tauscht eine defekte Platte; danach stellt der Pool die Redundanz selbst wieder her (**Resilver**).
- + **Add Spare** — hinterlegt eine Ersatzplatte, die bei einem Ausfall einspringt.
- **Add to Pool** — erweitert den Pool um weitere Platten. **Das lässt sich nicht zurücknehmen**; der Agent zeigt den Befehl vorher an.

### Server Settings

Einstellungen, die für den ganzen Pool gelten, werden hier live vom Server gelesen und mit  **Save All** zurückgeschrieben.

**Emergency Immutable Mode** stellt den gesamten Pool auf **nur lesen**. Dann kann kein Rechner mehr schreiben, und kein Stand lässt sich ändern oder löschen. Gedacht für den Notfall — etwa wenn ein Angriff auf Ihr Netz läuft und Sie die Sicherungen einfrieren wollen. Solange er aktiv ist, laufen keine Sicherungen; Löschen und Einhängen von Snapshots sind gesperrt.  **Deactivate** hebt ihn wieder auf.

### Einen Rechner abmelden

Unter **Registered Clients** lässt sich ein Rechner vom Pool abmelden. Der Agent fragt danach, ob die Sicherungen erhalten bleiben (**Keep Data**) oder gelöscht werden ( **DESTROY**). Löschen ist endgültig.

## 12. Virtuelle Maschinen — VM Backup

Auf einem Hyper-V-Host sichert der Agent die virtuellen Maschinen direkt vom Host aus — ohne Software in der virtuellen Maschine. Er legt dazu einen Produktions-Prüfpunkt an, damit auch laufende Datenbanken stimmig gesichert werden.

**VM Backup** listet die Maschinen dieses Hosts;  **Backup** sichert die gewählte. Den Verlauf zeigt das **Live-Log** daneben. Auf Rechnern ohne Hyper-V meldet die Ansicht **Kein Hyper-V-Host**.

## 13. Wenn etwas nicht stimmt

| Anzeige                                   | Was zu tun ist                                                                                                                    |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Verbindung zum Server schlägt fehl        | Netzwerk prüfen, unter <b>Client Settings</b> → <b>SSH Connection</b> Adresse und Port kontrollieren, dann <b>Test Connection</b> |
| <b>BACKUP NOW</b> ist grau                | als Admin anmelden; Lizenzstand unten links prüfen; läuft gerade schon eine Sicherung?                                            |
| Sicherung endet mit Lesefehler            | Festplatte des Rechners auf Fehler prüfen — oft kündigt sich so ein Plattenschaden an                                             |
| <b>IMMUTABLE MODE ACTIVE</b>              | der Notfall-Schreibschutz ist an (Abschnitt 11). Erst aufheben, wenn der Anlass vorbei ist.                                       |
| Replikation gescheitert                   | der nächste Lauf gleicht selbst neu ab. Bleibt der Fehler, uns ansprechen.                                                        |
| Stick bootet nicht                        | <b>Secure Boot</b> im BIOS/UEFI vorübergehend ausschalten                                                                         |
| Keine Netzwerkverbindung im Notfallsystem | Netzkabel statt WLAN; fehlt ein Treiber, ihn über 📁 <b>Eigene Treiber...</b> ergänzen und den Stick neu erstellen                 |
| Schlüsseldatei verloren                   | solange der Pool entsperrt ist: <b>Clients</b> → 🔑 <b>Download Keyfile</b> . Sonst sofort bei uns melden.                         |

In allen anderen Fällen: **Activity Log** → **Export** und die Datei an uns schicken.

## Was Sie selbst im Blick behalten sollten

- **Die E-Mail-Berichte einrichten und lesen.** Eine Sicherung, deren Ausfall niemand bemerkt, schützt nicht.
- **Die Schlüsseldatei** (bei verschlüsseltem Pool) an zwei getrennten Orten aufbewahren.
- **Den Rescue-Stick** griffbereit halten und nach Hardwarewechseln neu erstellen.
- **Einmal im Quartal eine Datei zurückholen** — als Probe, dass die Wiederherstellung funktioniert, bevor sie gebraucht wird.

RB-COMPUTERSERVICE · Roman Brunetti · Elbestraße 8c, 90453 Nürnberg · 0911 6320968 · [info@rb-computerservice.de](mailto:info@rb-computerservice.de)