Ordivis

MODUL · DATENSICHERUNG

Modul Datensicherung

Sicherungen planen, ihre Ausführung protokollieren und die Kontrolle nachweisen

Produktversion 2026.09.20 · Handbuch-Revision 1.0
Stand 20.09.2026 · Plattform .NET 10 / Windows Server

ID-35 Datensicherung

Modul Datensicherung

Die meisten Häuser sichern zuverlässig. Was fast keines beantworten kann, ist die Frage danach: *Wurde in den letzten dreißig Nächten tatsächlich gesichert – und wer hat das geprüft?* Die Antwort liegt üblicherweise in einem Postfach voller Berichtsmails, die niemand einzeln liest, und im Gedächtnis eines Kollegen.

Das Modul **Datensicherung** schließt genau diese Lücke.

Ordivis IT sichert nicht selbst. Es mountet nichts, spricht kein Bandlaufwerk an und schreibt in kein S3-Bucket. Es ist das Führungssystem über Ihren vorhandenen Sicherungsprodukten – Veeam, Veritas, den Bordmitteln Ihres Hypervisors oder einem Skript. Diese Produkte sichern weiterhin; Ordivis IT weiß, was sie tun sollen, hält fest, was sie getan haben, und führt die Kontrolle darüber.

Achtung – zwei Dinge heißen „Sicherung". Dieses Kapitel beschreibt die Sicherungen **Ihres Hauses**. Die Sicherung der Ordivis-Datenbank selbst ist eine Betriebsfunktion des Produkts und steht im Betriebshandbuch (ID-50).

INHALT

1 Der gefährlichste Lauf ist nicht der fehlgeschlagene
2 Die Bausteine
3 Einen Plan einrichten
4 Woher die Ergebnisse kommen
5 Die Kontrolle – und der Ein-Klick-Abschluss
5.1 Die geführte manuelle Prüfung: „Alle offenen als erfolgreich"
6 Aus einem Fehllauf einen Vorgang machen
7 Wiederherstellungstests
8 Die Regel 3-2-1-1-0
9 Bänder und Wechselmedien
10 Überblick, Kapazität und Konzept
11 Was Sie beim Umstieg erwartet
12 Rechte
13 Benachrichtigungen
Verwandte Themen

1 Der gefährlichste Lauf ist nicht der fehlgeschlagene

Ein fehlgeschlagener Sicherungslauf meldet sich. Er steht rot in der Konsole, er verschickt eine Mail, jemand sieht ihn.

Ein Sicherungsdienst, der seit elf Tagen gar nicht mehr startet, meldet **nichts**. Keine Fehlermeldung, keine Mail, keine Zeile. In jedem Werkzeug, das nur eingehende Meldungen sammelt, sieht dieser Zustand exakt so aus wie „keine Probleme".

Deshalb kennt Ordivis IT nicht nur den *gemeldeten*, sondern auch den **erwarteten** Lauf. Aus dem hinterlegten Zeitplan entsteht für jede Nacht ein Eintrag. Trifft bis zum Ende des Toleranzfensters keine Meldung ein, bekommt dieser Eintrag den Zustand **ausgeblieben** – und der lässt sich filtern, zählen, melden und quittieren. Ein fehlender Datensatz könnte das nicht.

Genau dafür ist der Zeitplan ein Baukasten und kein Textfeld: Aus „täglich 22:00, So. Vollsicherung" lässt sich keine Erwartung ableiten.

2 Die Bausteine

Baustein	Was er beschreibt
Sicherungsplan	Die Zusage: Schutzklasse, Verantwortliche und Vertretung, Soll-RPO und Soll-RTO, Prüfrhythmus, gesetzliche Aufbewahrung
Sicherungsauftrag	Was das Produkt tatsächlich tut: Name im Produkt, ausführendes Backup-System, Verfahren, Zeitplan
Quelle	Welche Configuration Items der Auftrag sichert
Stufe	Ein Glied der Kopienkette – mit eigenem Ziel, eigenem Takt und eigener Aufbewahrung
Ziel	Wohin gesichert wird: Platte, SMB, NFS, S3, Band, Cloud-Dienst oder Replikat
Lauf	Ein Ergebnis je Auftrag, Stufe und Solltermin
Prüfperiode	Der Kontrollnachweis über einen Zeitraum
Wiederherstellungstest	Der einzige Nachweis, der etwas über Wiederherstellbarkeit aussagt

3 Einen Plan einrichten

💻 **Nur im Client:** *Datensicherung ▸ Pläne & Ziele* · 🔑 `backup.manage` — Das Portal führt nur die eigenen offenen Prüfungen (*Meine Vorgänge ▸ Datensicherung prüfen*); Pläne und Ziele werden im Client eingerichtet.

🔒 **Pflichtreihenfolge** — ein Plan braucht ein Ziel. Die vier Schritte unten sind nicht als Gliederung gemeint, sondern als Reihenfolge.

1. **Ziele zuerst.** Legen Sie an, wohin gesichert wird. Bei einem verschlüsselten Ziel ist der Nachweis der Schlüsselhinterlegung ein Pflichtfeld – als *Verweis* (Abschnitt im Notfallhandbuch, Tresorfach, Schlüsselverwaltung), niemals als Schlüssel selbst.
2. **Plan anlegen.** Name, Schutzklasse, Verantwortliche und Vertretung. Prüfrhythmus und Frist für den Wiederherstellungstest sind je Schutzklasse vorbelegt und bleiben änderbar.
3. **Auftrag anlegen.** Tragen Sie den Namen ein, unter dem Ihr Sicherungsprodukt den Auftrag führt – darüber ordnet Ordivis IT später Berichtsmails und Schnittstellenmeldungen zu.
4. **Zeitplan bauen.** Wählen Sie die Wiederholung, die Startzeit, die Zeitzone, die Fensterlänge und die Toleranz. Die Schaltfläche **Nächste zehn Termine anzeigen** rechnet den Plan vor, bevor Sie speichern.

5. **Stufen anhängen.** Quelle → Platte → SMB → Band → S3, je Stufe ein Ziel und eine Aufbewahrung.

Achtung – die Quelle wird noch nicht im Client zugewiesen. Welche Configuration Items ein Auftrag sichert (Baustein *Quelle*, Abschnitt 2), lässt sich in dieser Fassung nur über die Schnittstelle oder durch den Support festlegen; die Auswahl im Client ist in Arbeit. Solange keine Quellen hinterlegt sind, bleiben drei Auskünfte leer: die Ziffer **1 extern** der Regel 3-2-1-1-0 (Abschnitt 8), die Angabe *gesichert durch* am CI-Steckbrief und die Prüfung gegen Wartungsfenster. Alles Übrige – Zeitplan, Soll-Ist-Abgleich, Prüfperioden und Wiederherstellungstests – arbeitet davon unberührt.

Tipp – die Terminvorschau ist mehr als eine Bequemlichkeit. Sie zeigt auch, was über den Sommerzeitwechsel geschieht und was aus dem „31." in einem Februar wird (nämlich der Monatsletzte). Zwei Nächte im Jahr entscheiden sich hier zwischen einem richtigen und einem falschen Ausfallalarm.

4 Woher die Ergebnisse kommen

Drei Wege, die sich beliebig mischen lassen:

Weg	Wie er funktioniert	Wofür er taugt
Von Hand	Unter *Sicherungsläufe* → **Lauf erfassen**, auch rückwirkend	Funktioniert am ersten Tag und für jedes Produkt – auch für die Bandkassette, die jemand aus dem Tresor holt
Aus der Berichtsmail	Regeln je Auftrag: Absender, Betreffmuster, Erfolgs- und Fehlermuster	Das beste Verhältnis von Nutzen zu Aufwand – praktisch jedes Produkt kann eine Berichtsmail schicken
Über die Schnittstelle	`POST /api/v1/backup/runs` als Stapel, idempotent über die Lauf-Kennung der Quelle	Der sauberste Weg, setzt aber ein Skript bei Ihnen voraus

Trifft eine Meldung im Toleranzfenster eines erwarteten Laufs ein, wird **dieser** nachgetragen. So entsteht kein zweiter Eintrag, und derselbe Zeitraum zeigt nicht gleichzeitig einen erfolgreichen und einen ausgebliebenen Lauf.

Wichtig – eine Berichtsmail, die zu keiner Regel passt, verschwindet nicht. Sie wird in einem Eingang aufbewahrt, statt still verworfen zu werden. Ein geändertes Betreffformat nach einem Produktupdate geht damit nicht verloren.

Achtung: Die Regeln und dieser Eingang sind in dieser Fassung **noch nicht im Client bedienbar**. Beides wird über die Schnittstelle (`…/backup/mail-rules` und `…/backup/mail-inbox`) oder durch den Support eingerichtet und eingesehen; die Bildschirmseite dazu ist in Arbeit. Wer die Aufnahme aus Berichtsmails nutzen möchte, richtet sie deshalb einmalig mit dem Support ein – danach läuft sie ohne weiteres Zutun.

5 Die Kontrolle – und der Ein-Klick-Abschluss

Prüfperioden entstehen **ohne Ihr Zutun** aus dem Rhythmus des Plans, mit Frist und Zuständigem. Sie finden sie unter **Datensicherung → Prüfungen**, im Portal unter *Datensicherung prüfen*.

Ist der Zeitraum lückenlos grün, genügt ein Klick auf **Zeitraum ohne Befund abschließen**.

Ist er es nicht, bleibt die Schaltfläche gesperrt – und nennt den Grund daneben. Dann führt der Weg über einen **Befund** je betroffenem Lauf: Ursache, Maßnahme, Stand. Erst wenn jeder nicht-grüne Lauf einen Befund trägt, lässt sich der Zeitraum abschließen.

Warum die Sperre, wenn es doch einfach sein soll? Beides gehört zusammen. Der Klick erledigt den Regelfall in zwei Sekunden – das ist der Grund, warum eine Kontrolle überhaupt durchgehalten wird. Eine Schaltfläche, die aber auch dann grün färbt, wenn drei Nächte fehlen, dokumentiert nicht die Kontrolle, sondern ihr Ausbleiben. Im Audit wäre sie **schlechter als gar nichts**, weil sie eine Prüfung behauptet, die nicht stattgefunden hat. Im Regelfall nimmt Ihnen die Bedingung nichts weg: Es ist alles grün, und der Klick sitzt.

Beim Abschluss wird **kein Haken** gespeichert, sondern ein **Nachweis**: Anzahl und Kennungen der Läufe, das gesicherte Volumen, Zeitpunkt und Prüfer. Ein Haken sagt „jemand hat geklickt". Der Nachweis sagt „am 03.08. bestätigte Frau X 31 von 31 erwarteten Läufen, 4,1 TB, kein Befund" – und *das* ist der Beleg nach ISO/IEC 27001 A.8.13. Eine spätere Korrektur legt eine neue Fassung daneben, statt die alte zu überschreiben.

5.1 Die geführte manuelle Prüfung: „Alle offenen als erfolgreich"

Nicht jedes Sicherungsprodukt ist angebunden. Wer die Ergebnisse **im Produkt nachsieht** und sie hier nachträgt, brauchte dafür bisher einen Lauf nach dem anderen. Dafür gibt es die Schaltfläche **Alle offenen als erfolgreich**: Sie trägt für alle noch offenen Läufe des gewählten Zeitraums ein erfolgreiches Ergebnis nach. Danach bleiben nur die Abweichungen zu bearbeiten.

Die Rückfrage nennt die Anzahl und ist bewusst deutlich formuliert:

Das ist eine **Aussage über die Wirklichkeit** – bitte nur bestätigen, wenn im Sicherungsprodukt tatsächlich nachgesehen wurde. Eine Schaltfläche, die das lautlos täte, wäre dasselbe Problem wie ein Abschluss ohne Prüfung: Sie dokumentierte eine Kontrolle, die nicht stattgefunden hat.

Der Vorgang ist **wiederholbar**: Ein zweiter Klick trägt dieselben Läufe nicht erneut ein, sondern aktualisiert sie. Läufe, die bereits ein Ergebnis tragen — auch ein schlechtes —, bleiben unberührt; angefasst wird nur, was noch offen ist.

6 Aus einem Fehllauf einen Vorgang machen

> 💻 **Nur im Client:** *Datensicherung* ▸ *Sicherungsläufe* ▸ *Vorfall erzeugen* · 🔑 `backup.manage` und `tickets.update`

1. Öffnen Sie *Datensicherung* ▸ *Sicherungsläufe*.
2. Markieren Sie den beanstandeten Lauf.
3. Klicken Sie auf *Vorfall erzeugen*.

✅ **Ergebnis:** Es entsteht ein Vorgang im Service Desk – mit dem betroffenen Configuration Item verknüpft und dem Backup-Verantwortlichen des Plans zugewiesen.

Der Betreff entsteht automatisch:

> `[Backup] VEEAM-SRV01 · Dateiserver FS-01 · 09.08.2026 22:00 · Fehlgeschlagen: VSS-Snapshot-Zeitüberschreitung`

Die vollständige Meldung des Produkts steht im Beschreibungstext, das betroffene Configuration Item ist verknüpft, und zugewiesen wird der Backup-Verantwortliche des Plans – ersatzweise die Vertretung, ersatzweise die Support-Gruppe. Steht keiner davon fest, entsteht der Vorgang trotzdem: unzugewiesen ist besser als gar nicht.

> **Wichtig.** Vierzehn Fehlnächte hintereinander erzeugen **einen** Vorgang mit vierzehn Journaleinträgen, nicht vierzehn Vorgänge. Ein geschlossener Vorgang wird bei erneutem Fehler innerhalb von vierzehn Tagen wieder aufgenommen.

7 Wiederherstellungstests

Ein Lauf mit dem Ergebnis „erfolgreich" bedeutet: *Das Sicherungsprodukt hat Erfolg gemeldet.* Er bedeutet **nicht**: *Die Daten sind wiederherstellbar.* Der Unterschied zwischen beidem ist der Wiederherstellungstest.

Erfasst werden Art (Einzeldatei, Postfach, Datenbank, vollständige VM, isolierte Testumgebung, Bare-Metal), Umfang, Ergebnis sowie die **gemessene** Wiederanlaufzeit und der **gemessene** Datenverlust.

- Ein überfälliger Test färbt die Ampel des Plans – **auch wenn jeder Lauf grün war**.
- Ist am Plan ein Wiederanlaufplan hinterlegt, erscheint der Test zugleich dort als Testergebnis (ID-30). Es gibt keinen zweiten Speicher.
- Eine Lücke zwischen gemessenem Ist und zugesagtem Soll wandert als Risiko in die Informationssicherheit (ID-28).

- Eine reine **Lesbarkeitsprüfung** eines Mediums erneuert die Testfrist bewusst nicht: Sie belegt, dass das Band lesbar ist, nicht dass sich daraus etwas wiederherstellen lässt.

8 Die Regel 3-2-1-1-0

Unter *Pläne & Ziele* zeigt **3-2-1-1-0** die Bewertung eines Plans. Sie wird **berechnet**, nicht angekreuzt – und nennt bei jeder nicht erfüllten Ziffer den Grund.

Ziffer	Woraus sie sich ergibt
3 Kopien	Produktivdaten plus Stufen mit gültiger Aufbewahrung. Ein Replikat zählt als Standort, nicht als Kopie
2 Medienarten	Verschiedene Zielarten über die Stufen hinweg
1 extern	Mindestens ein Ziel mit einem Standort, der nicht der Standort der Quelle ist. Ein Ziel ohne Standortangabe zählt nicht – unbekannt ist nicht extern
1 unveränderlich	Ein Ziel mit Object Lock, WORM oder Air-Gap
0 Fehler	Kein fehlgeschlagener oder ausgebliebener Lauf im Zeitraum **und** ein bestandener Wiederherstellungstest innerhalb der Frist

Die letzte Ziffer ist die, die fast alle Werkzeuge weglassen – und die einzige, die etwas über Wiederherstellbarkeit aussagt.

9 Bänder und Wechselmedien

Für Häuser, die Band betreiben: Medienpools mit Rotationsverfahren, Einzelmedien mit Barcode, Zustand, Schreibzyklen gegen die Herstellergrenze und Ablauf der Aufbewahrung. Auslagerung und Rückholung werden mit **Quittung** festgehalten – wer hat das Band wann wohin gebracht, wer hat es angenommen.

> **Tipp.** Ohne diese Quittung ist die „1 extern" der 3-2-1-Regel eine Absicht. Mit ihr wird sie ein Datum, das jemand bestätigt hat.

Für ein Haus mit einer NAS und einer externen Platte ist dieser Abschnitt entbehrlich – Plan, Auftrag, Läufe und Kontrolle funktionieren ohne jede Medienverwaltung.

10 Überblick, Kapazität und Konzept

- **Überblick** zeigt je Plan eine Ampel samt Begründung, Fehler- und Ausfallquote, offene und überfällige Prüfungen sowie den Verlauf.
- **Auslastung der Sicherungsziele** schreibt das Wachstum fort und meldet, wann ein Ziel voll läuft – *bevor* es voll ist. Danach meldet es das Sicherungsprodukt ohnehin selbst, und dann ist die Nacht bereits verloren.

- Das **Datensicherungskonzept** erscheint als eigenes Kapitel im IT-Betriebshandbuch (ID-50). Es entsteht bei jedem Abruf aus den gepflegten Daten: Geltungsbereich, Verfahren, Ziele und Stufen, Fristen, Verantwortliche, Prüfrhythmus und Testnachweise.

11 Was Sie beim Umstieg erwartet

Bis zu dieser Fassung standen vier Angaben als Attribute am Configuration Item der Klasse *Backup-System*: Aufbewahrung, RPO, Zeitplan und der letzte Test-Restore. Sie ziehen beim Update automatisch in dieses Modul um und werden dort künftig geführt; doppelte Pflege entfällt.

> **Achtung – der übernommene Auftrag ist zunächst stillgelegt.** Aus dem bisherigen Zeitplan-Freitext lässt sich keine Erwartung ableiten. Wäre der Auftrag sofort aktiv, liefe er mit dem Vorgabetakt (täglich 22:00) los und Sie fänden am ersten Morgen eine Liste ausgebliebener Läufe vor, die niemand versprochen hat. Der Freitext bleibt vollständig in den Notizen des Auftrags erhalten: Bauen Sie den Zeitplan im Baukasten nach und schalten Sie den Auftrag dann scharf.

12 Rechte

Recht	Wofür
`backup.read`	Pläne, Aufträge, Läufe und Nachweise sehen
`backup.manage`	Pläne, Aufträge, Stufen, Ziele und Einstellungen pflegen
`backup.run.record`	Ergebnisse von Läufen erfassen und nachtragen
`backup.verify`	Prüfperioden abschließen, Befunde und Wiederherstellungstests führen
`backup.media.manage`	Medienpools, Bänder und deren Auslagerung verwalten

Die Trennung folgt der Aufgabe, nicht dem Schema: Wer Läufe *erfasst* – etwa der Kollege, der das Band wechselt –, muss deshalb keine Pläne ändern dürfen. Und wer *prüft*, ist ein anderer als der, der die Sicherungsstrategie festlegt. Genau diese Trennung von Ausführung und Kontrolle will ein Prüfer sehen.

13 Benachrichtigungen

Sechs Ereignisse lassen sich je Benutzer für Glocke und E-Mail getrennt schalten (ID-31):

Ereignis	E-Mail voreingestellt	Warum
Sicherungslauf fehlgeschlagen	**an**	Verlangt eine Reaktion außerhalb der Anwendung
Sicherungslauf ausgeblieben	**an**	Der stille Fall – eine reine Meldung in der Anwendung bliebe wirkungslos

Ereignis	E-Mail voreingestellt	Warum
Prüfung fällig	aus	Routine
Prüfung überfällig	**an**	Eine ausgefallene Kontrolle ist der Auditbefund
Wiederherstellungstest fällig	aus	Planbar, mit Vorlauf
Ziel läuft voll	aus	Kapazitätswarnung mit Vorlauf

Verwandte Themen

- **ID-21 Modul CMDB** – die gesicherten Configuration Items und das Backup-System als CI
- **ID-30 Modul Notfall- & Wiederanlaufplanung (DR)** – dorthin schreiben die Wiederherstellungstests
- **ID-28 Modul Security (ISMS)** – Control A.8.13 und die RPO-/RTO-Lücke als Risiko
- **ID-29 Modul Business Continuity Management** – RPO und RTO aus der Business-Impact-Analyse
- **ID-20 Modul Service Desk** – die Vorgänge, die aus Fehlläufen entstehen
- **ID-31 Modul Benachrichtigungen & E-Mail-Integration** – Meldungen und die Aufnahme aus Berichtsmails
- **ID-50 Betriebshandbuch** – das erzeugte Datensicherungskonzept und die Sicherung der Ordivis-Datenbank selbst
- **ID-44 Rollen- und Rechte-Matrix** – die fünf Rechte im Gesamtbild