

Collax Backup

Howto

Dieses Howto beschreibt die Einrichtung einer Datensicherung, sowie ein Bare-Metal-Recovery und eine Datenrücksicherung.

Voraussetzungen

- Collax Business Server
- Collax Platform Server
- Collax Security Gateway
- Collax V-Cube

Optional

- Modul Collax Net Backup für die Sicherung von Clients

DNS muss funktionieren. Sowohl der Collax Server, als auch die zu sichernden Clients müssen den FQDN des Collax Servers richtig auflösen können.

Zielsetzung

Erstellung einer täglichen, inkrementellen Sicherung und einer wöchentlichen Vollsicherung. Als Sicherungsziel soll eine Windowsfreigabe verwendet werden. Die Sicherung umfasst alle Daten des Collax Servers.

Mit dem Zusatzmodul Collax Net Backup soll eine Windows Arbeitsstation gesichert werden.

Einrichtung des Sicherungsplans mit Hilfe des Assistenten

Dieser Dialog befindet sich unter „Assistenten → Datensicherung“

Mit Hilfe dieses Assistenten richten Sie Sicherungspläne für Datensicherungen ein. Diese Sicherungspläne sind gleichermaßen für Sicherungen Ihres Collax Servers wie für Client-Rechner gültig und notwendig. Im Allgemeinen genügen diese generierten Sicherungspläne auch fortgeschrittenen Anwendungsfällen. Detaillierte, manuelle Modifikationen dieser Pläne sind möglich.

Ablauf

Im ersten Schritt wird die Periode für Vollsicherungen festgelegt. Es kann zwischen monatlicher, wöchentlicher oder täglicher Vollsicherung gewählt werden. Ergänzende inkrementelle Sicherungen werden zu einem späteren Zeitpunkt konfiguriert.

Assistent für Datensicherung

Mit Hilfe dieses Assistenten richten Sie Sicherungspläne für Datensicherungen ein. Diese Sicherungspläne sind gleichermaßen für Sicherungen Ihres Collax Servers wie für Client-Rechner gültig und notwendig. Im Allgemeinen genügen diese generierten Sicherungspläne auch fortgeschrittenen Anwendungsfällen. Detaillierte, manuelle Modifikationen dieser Pläne sind möglich.

Periode für Vollsicherungen

Danach wählen Sie genauere Spezifikationen Ihrer Sicherungszeitpunkte.

Assistent für Datensicherung

Wählen Sie in diesem Schritt genauere Spezifikationen Ihrer Sicherungszeitpunkte.

Wochentag für die Sicherung

Uhrzeit für die Sicherung

Im dritten Schritt fragt der Assistent nach der Backup-Strategie. Hierbei kann zwischen „Lineare Sicherung“, „Einfache Rotation“ und, abhängig von der Wahl der Periode, zwischen „Türme von Hanoi“ und „Großvater, Vater, Sohn“ gewählt werden.

Assistent für Datensicherung

Wählen Sie in diesem Schritt eine Backup-Strategie

Backup-Strategie

Führe darüber hinaus täglich inkrementelle Sicherungen durch

Führe Inkrementelle Backups durch

Benutze eigene Medien für inkrementelle Sicherung

Bei „Linearer Sicherung“ wird fortlaufend auf das jeweilige Ziel gesichert; neue Medien werden angelegt beziehungsweise angefordert, sobald das letzte Medium voll ist.

Bei „Einfacher Rotation“ werden Medien zyklisch für Sicherungen benutzt; die Zyklusdauer richtet sich nach der Periode für Vollsicherungen.

Ziel des Schemas „Türme von Hanoi“ ist es, so lange wie möglich auf alte Sicherungsdaten zurückgreifen zu können, ohne dabei zu viel Platz zu verbrauchen. Es ist aber zu beachten, dass der Platzbedarf dieses Schemas höher ist als der der anderen Schemata.

Das Schema „Großvater, Vater, Sohn“ hält drei Generationen von Sicherungen vor. Dabei wird monatlich eine Sicherung auf gesonderte Medien geschrieben, wöchentlich auf einen zweiten Satz, und täglich auf die Standardmedien. Viele Administratoren sichern die Vater- und Sohn-Generationen als differenzielle beziehungsweise inkrementelle Sicherungen. Diese Veränderung kann leicht im generierten Plan vorgenommen werden.

Bestimmen Sie im vierten Schritt, wie lange gesicherte Daten aufbewahrt werden sollen. Gemeinsam mit der Datenmenge ergibt sich daraus die benötigte Anzahl an Bändern bzw. der Gesamtplatzbedarf der Sicherung.

Assistent für Datensicherung

Bestimmen Sie in diesem Schritt, wie lange gesicherte Daten aufbewahrt werden sollen. Gemeinsam mit der Datenmenge ergibt sich daraus die benötigte Anzahl an Medien bzw. der Gesamtplatzbedarf der Sicherung.

Aufbewahrungsdauer in Tagen

Weiterhin wird eine Zuordnung erstellt, die den neuen Plan mit dem lokalen Default-Ziel und dem lokalen System verbindet. Dies geschieht nur, wenn das Default-Ziel existiert und in der vorangegangenen Maske die Checkbox „Benutze diesen Sicherungsplan für eine lokale Sicherung“ aktiviert wurde.

Assistent für Datensicherung

Sie können Ihr Backup-System mit dem nun konfigurierten Zeitplan verknüpfen. Aktivieren Sie den folgenden Schalter, um eine vollständige Sicherung Ihres Servers auf das Standard-Festplatten-Ziel durchzuführen. Sie können die dabei entstehende Zuordnung im Anschluss bearbeiten, um ein anderes Ziel zu wählen.

Benutze diesen Sicherungsplan
für eine lokale Sicherung

Im letzten Schritt wird eine Zusammenfassung der im Assistenten vorgenommenen Einstellungen angezeigt. Der Sicherungsplan wird mit einem Klick auf „Fertigstellen“ erstellt.

Assistent für Datensicherung

Ihre Konfiguration ist nun beendet. Ein neuer Sicherungsplan wird erstellt, sobald Sie auf "Fertigstellen" klicken.

Die Daten Ihres Sicherungsplans:

Zusammenfassung	Name des Sicherungsplans	linear-weekly-with-incr
	Vollsicherung:	Wöchentlich (Freitags, 23:00:00h)
	Strategie:	Lineare Sicherung (kein forcierter Medienwechsel) Zusätzliche inkrementelle Sicherungen

Grundeinstellungen

Die Grundeinstellungen für das Backup werden unter „System → Datensicherung → Grundeinstellungen“ vorgenommen.

Menü > System > Datensicherung > Grundeinstellungen

Grundeinstellungen

Grundeinstellungen | Laufzeitbeschränku... | Berechtigung...

Operator

E-Mail-Adresse des Operators
Leer: Adresse des Administrators wird verwendet

Fremder Backup-Server

Erlaube Zugriff von fremdem Backup-Server

Einstellungen

Verhalten bei Platzbedarf

Quota des lokalen Backup-Systems (GB)

Detaillierte Dateilisten nach Datenwiederherstellung

Dateilistenabgleich bei Datensicherung (Accurate mode)

Ziel für Recovery-Informationen

Kompression und Verschlüsselung

Datenkompression

Zertifikat für Datenverschlüsselung

Leer lassen, um nicht zu verschlüsseln

Master-Zertifikat

Nur sinnvoll in Net-Backup-Strukturen. Es wird empfohlen, den privaten Schlüssel auf ROM-Medien zu sichern und vom System zu entfernen.

E-Mail-Adresse des Operators Statusmeldungen der Datensicherung werden an die hier eingetragene E-Mail-Adresse gesendet.

Erlaube Zugriff von fremdem Backup-Server Übernimmt ein anderer Collax Server die Sicherung lokaler Daten muss der Zugriff hier erlaubt werden.

Verhalten bei Platzbedarf Hier wird eingestellt, ob bei einem Sicherungsvorgang mit weiterem Platzbedarf die Medien automatisch erweitert werden können, oder ob dies von Hand durchgeführt werden soll.
Quota des Backup-Systems (GB)

Größenbegrenzung für lokale Sicherung. Beschreibt den maximal zu belegenden Platz auf der Platte des lokalen Backup-Systems.

Detaillierte Dateilisten nach Datenwiederherstellung Nach einer durchgeführten Datenwiederherstellung wird eine E-Mail mit Statusinformation an den Backup-Administrator versendet. Ist diese Option gesetzt, wird zusätzlich eine Liste aller wiederhergestellten Dateien versendet. Diese Liste ist potenziell sehr lang.

Dateilistenabgleich bei Datensicherung (Accurate mode) Standardmäßig wird bei Inkrementellen Backups anhand des Änderungszeitpunktes der Datei entschieden ob eine Datei gesichert werden muss. Dadurch lässt sich nicht feststellen, welche Dateien seit dem letzten Backup gelöscht worden oder mit einem älteren Änderungsdatum hinzugefügt worden sind. Ist diese Option gesetzt, so werden auch diese Dateien mitgesichert, indem mit einer Liste aller Dateien des letzten Backups verglichen wird. Dabei ist zu beachten, dass der Ressourcenbedarf (CPU und Arbeitsspeicher) steigt.

Ziel für Recovery-Informationen Falls eine Zuordnung die für eine Wiederherstellung von Bandlaufwerken nötigen Verwaltungsdaten der Sicherungsprozesse mitsichert, lässt sich dafür mit dieser Option ein weiteres, separates Sicherungsziel festlegen. Auf dieses werden dann die Informationen über Kataloge und dergleichen gesichert, so dass Sicherungen auch nach einem Komplettausfall von einem Tapelaufwerk zurückgespielt werden können. Für diese Option stehen nur dateibasierte Sicherungsziele zur Auswahl.

Datenkompression Ist diese Option aktiviert, so werden alle Dateien mit GNU ZIP komprimiert. Dies geschieht auf Dateibasis, das heißt falls eine der Dateien unlesbar wird, so ist tatsächlich nur diese Datei betroffen und nicht alle Dateien einer Sicherung. Diese Einstellung sollte nur dann aktiviert werden, wenn das Sicherungsziel keine Hardwarekompression unterstützt.

Kompressionsstärke Daten können unterschiedlich stark komprimiert werden, was sich in Speicherbedarf und Rechenaufwand auswirkt. Bei der schnellsten Kompression (Wert 1) erhält man größere Dateien als bei einer langsamen Kompression (Wert 9). Es wird prinzipiell nicht empfohlen eine Kompressionsstärke größer als 6 zu wählen, da der Rechenaufwand unverhältnismäßig zum Platzersparnis wächst.

Zertifikat für Datenverschlüsselung Falls es gewünscht ist, dass sämtliche Daten bei Sicherungsvorgängen verschlüsselt und damit für dritte unleserlich gemacht werden, kann hier ein Zertifikat ausgewählt werden, das als Schlüssel verwendet werden soll. Beim Wiederherstellen werden die Dateisignaturen überprüft und der Vorgang bei Unstimmigkeiten unterbrochen. Metadaten einer Datei wie Pfadname und Berechtigungen werden dabei nicht mitverschlüsselt.
Master-Zertifikat

Bei der Verschlüsselung von Sicherungen gilt es zu beachten, dass diese nicht wiederherstellbar sind, wenn die Schlüssel verloren gegangen sind. Um das Risiko, Sicherungen aufgrund verloren gegangener Zertifikate nicht wieder herstellen zu können, zu minimieren, kann mit einem zweiten sogenannten Master-Zertifikat verschlüsselt werden. Im Falle von Master-Zertifikaten ist es empfehlenswert, den privaten Schlüssel nicht auf dem Server zu lagern, sondern diesen nur zu importieren, wenn tatsächlich ein Zertifikat verloren gegangen ist und Sicherungen nicht mehr anders wiederherzustellen sind.

Angabe der Laufzeitbeschränkungen

In bestimmten Fällen ist es sinnvoll, dass Sicherungs-Jobs vorzeitig automatisch abgebrochen werden. Zu den Parametern gehört die maximale Startverzögerung, die angibt wie lange sich ein Job eines geplanten Sicherungsjobs verzögern darf, weil beispielsweise noch ein vorhergehender Job läuft. Die maximale Laufzeit gibt an, wie lange ein Job aktiv sein darf. Innerhalb eines Jobs gibt die maximale Wartezeit an, wie lange ein Job unterbrochen werden darf, um zum Beispiel ein Band zu wechseln. Letztendlich gibt die maximale Dauer an, wie lange ein Job inklusive Startverzögerung, Lauf- und Wartezeit überhaupt dauern darf, damit Jobs zum Beispiel nicht während der Arbeitszeit durchgeführt werden. Jeder Parameter kann einzeln im Formular „System → Datensicherung → Grundeinstellungen“ eingestellt werden.

Erstellung des Sicherungsziels

Die Sicherung soll auf ein entferntes Ziel erfolgen. Dieser Dialog befindet sich unter „System → Datensicherung → Ziele“. In diesem Fall wird auf eine Windowsfreigabe auf dem Rechner mit der IP 172.17.0.127 gesichert. Der angegebene Benutzer benötigt Schreibberechtigung auf die Freigabe.

Nachdem das Ziel erstellt und die Konfiguration aktiviert wurde, kann das Ziel mittels „Rechtsklick → Ziel überprüfen“ getestet werden. Hierbei wird überprüft, ob schreibender Zugriff auf das Ziel möglich ist.

Zuordnungen

Im nächsten Schritt müssen Plan und Ziel miteinander verknüpft werden. Dies geschieht über die Zuordnungen. In der Zuordnung kann auch ausgewählt werden welche Daten gesichert werden sollen. Durch dieses Formular ist es möglich, sehr flexible Sicherungsabläufe zu definieren. Zuvor definierte Rechner, Ziele, Pläne und Datensätze können durch entsprechende Zuordnung auf die Anforderungen solcher Abläufe im lokalen Netzwerk angepasst werden.

Menü > System > Datensicherung > Zuordnungen > Zuordnung bearbeiten

Zuordnung bearbeiten

Grundeinstellungen

Bezeichnung:

Kommentar:

Zuordnung

Quelle/Client:

Zu sichernde Daten:

Sicherungsplan:

Ziel:

Nach der Aktivierung der noch anstehenden Änderungen ist das Backupsystem konfiguriert und wird zum eingestellten Zeitpunkt die Sicherung der eigenen Daten vornehmen.

Wichtig: Voraussetzung für einen Bare Metal Restore (eine Datenwiederherstellung nach einem Totalausfall) ist, dass in der Zuordnung entweder „Alles“ gesichert wird, oder das Häkchen bei „Sichere Zustand des Backup-Servers“ aktiviert ist.

Collax Net Backup - Sicherung von Clients

Das Collax Net Backup zeichnet sich durch die Unterstützung von unterschiedlichen Client-Betriebssystemen aus. Damit lässt sich ein Remote-Backup auch auf Apple-, Windows- und Unix-Systemen starten. Die Konfiguration der Sicherungs- und Wiederherstellungslösung erfolgt zentral über den Server, während auf den Clients lediglich ein Paket, bestehend aus der Software und der vorgefertigten Client-Konfigurationsdatei, installiert werden müssen.

Sicherung eines Windows Clients

Exemplarisch gehen wir hier auf die Sicherung eines Windows Arbeitsplatzes ein.

Inhaltslisten

Bei Sicherung von Arbeitsstationen sind zunächst Inhaltslisten zu definieren. Diese Listen geben vor, welche Dateien und Verzeichnis durch diesen Server von der Arbeitsstation gesichert werden sollen. Beachten Sie, dass bei den Pfaden der „/“, nicht der „\“ verwendet werden muss.

Menü > System > Datensicherung > Inhaltslisten > Inhaltsliste bearbeiten

Inhaltsliste bearbeiten

Kennzeichnung

Bezeichnung: Default_Windows_fileset
 Kommentar:

Inhalt

Inhaltslistentyp:

Zu sichernde Dateien:

SchlieÙe Dateien aus:

Führe vor Sicherung aus:

Führe nach Sicherung aus:

Volume Shadow Copy Support
(für Windows-Clients)

Unterstützung für MacOS
X-Clients (HFS+)

Unterstützung für erweiterte
Attribute

Clients

Unter dem Punkt *Clients* kann definiert werden, welcher Arbeitsplatz gesichert werden soll. In diesem Beispiel handelt es sich um einen Windowsclient mit der IP Adresse 172.17.0.51.

Menü > Clients > Client bearbeiten

Client bearbeiten

Identifikator:

Kommentar:

Rechnername oder Adresse:

Passwort des Clients:

Art des Backup-Clients:

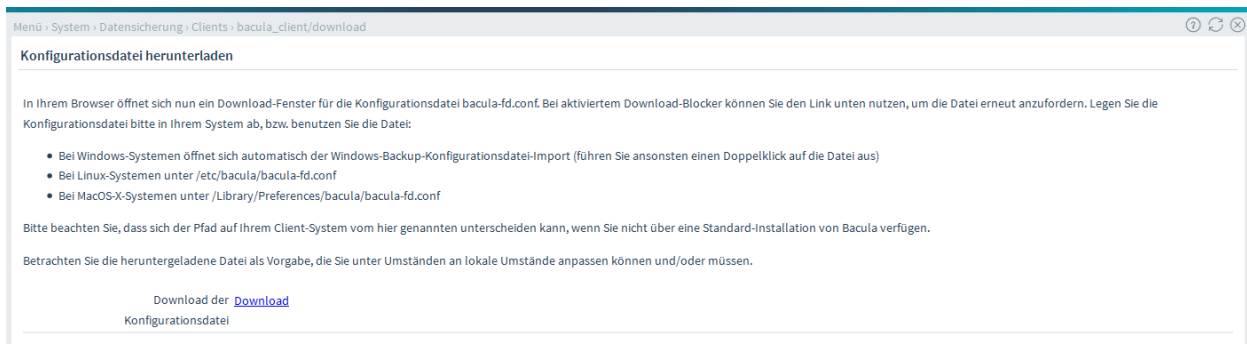
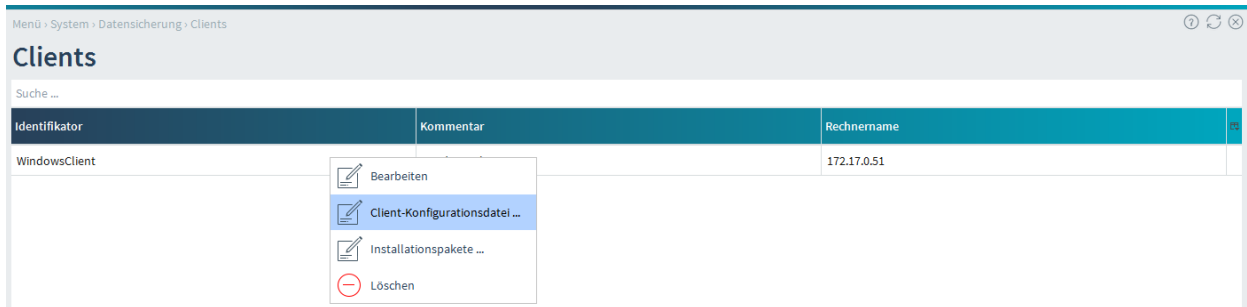
Herunterladbare
Konfigurationsdateien für

Für die einfache Konfiguration des Clients gibt es die Möglichkeit eine *Client-Konfigurationsdatei* herunterzuladen. Diese kann in der „*Client-Übersicht*“ mit einem Rechtsklick heruntergeladen werden.

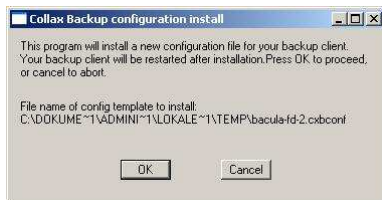
Client Konfiguration

Unter dem Menüpunkt Clients kann man auch die Software für den Windowsclient herunterladen. Klicken Sie dazu auf Installationspakete. Wenn man die Datei gleich „öffnen“ lässt, wird der Client automatisch installiert.

Hinweis: Achten Sie darauf, dass in der Windows Firewall Port 9102/tcp offen ist, damit die Sicherung funktioniert.



Die folgenden Bilder zeigen die Client-Installation:





Status und Betrieb

Eine gute Übersicht zu den Jobs und deren Verlauf finden Sie unter „System → Datensicherung → Wiederherstellung → Status und Betrieb“. Man kann sich dort einen Überblick verschaffen, ob alle Jobs erfolgreich beendet wurden, ob Fehler aufgetreten sind etc.

Bare Metal Restore

Dieser Dialog befindet sich unter „Assistenten → Bare Metal Restore“

Benutzen Sie diesen Assistenten, um Ihren Server nach einem vollständigen Systemcrash wieder in Betrieb zu nehmen (Bare Metal Restore, Disaster Recovery).

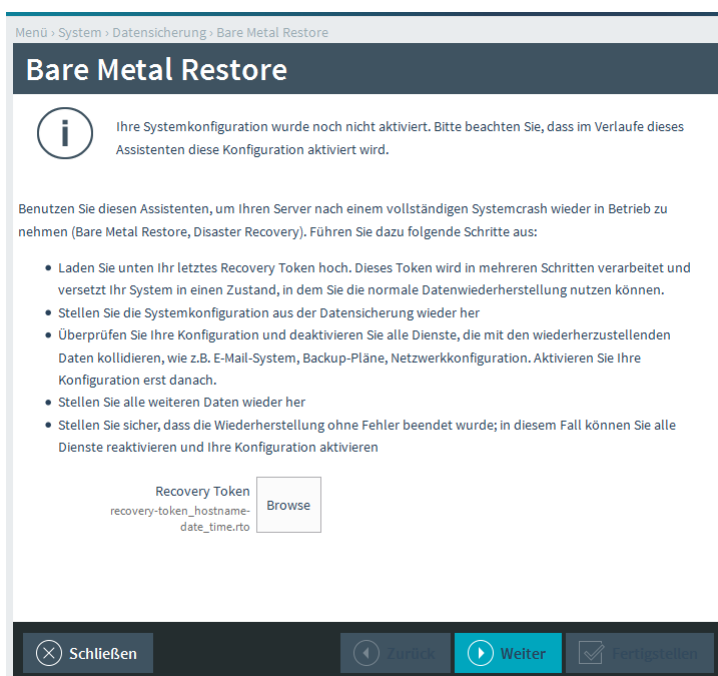
Im ersten Schritt wird eine Recovery Token-Datei (recovery-token_host_datum.rto) gewählt, welche der Administrator per E-Mail erhielt. Im nächsten Schritt werden folgende Aktionen automatisch ausgeführt:

- › Überprüfung des Recovery Token
- › Installation der Lizenz
- › Installation der lizenzierten Zusatzmodule
- › Einrichtung des Sicherungsziels und des Sicherungssystems
- › Wiederherstellung des Inhaltsverzeichnisses (Katalog) aller Sicherungsdaten

Im letzten Schritte werden Informationen zur weiteren Vorgehensweise angezeigt. Es sind alle Einstellungen vorhanden, um auf alle gesicherten Daten zuzugreifen und diese wieder herzustellen.

Es ist zu beachten, dass während einer vollständigen Datenwiederherstellung in das laufende System keine manuellen Interaktionen mit dem System oder einzelnen Diensten getätigt werden sollen.

Hinweis: Eine Freischaltung der Lizenz ist nicht nötig.



Wenn bereits ein Ersatzgerät, oder der Originalserver noch in Betrieb ist, dann achten Sie darauf, dass es keinen IP-Adressenkonflikt gibt, sowie die Dienste wie DHCP, Mailabholung und ähnliches deaktiviert sind.

Datenwiederherstellung

Ein Bare Metal Restore ist nur notwendig, wenn neu installiert wurde. Ansonsten reicht die Datenwiederherstellung aus.

Um aus einem Backup Daten wiederherzustellen, gehen Sie wie folgt vor. Wechseln Sie zum Menüpunkt „System → Datensicherung → Daten-Wiederherstellung“ und wählen Sie die rückzusichernden Daten aus.

The screenshot displays the 'Datenwiederherstellung' (Data Recovery) interface. The breadcrumb trail is 'Menü > System > Datensicherung > Datenwiederherstellung'. The main window title is 'Datenwiederherstellung'. Below the title bar, there are tabs for 'Clients', 'Wiederherstellen', and 'Optionen'. The main area is a table with columns for 'Größe', 'Datum', and 'Job-Datum'. The table lists various backup items, including 'MySQL-Datenbank test', 'MySQL-Datenbank zarafa', 'Faxdienst', 'MySQL-Verwaltungsdatenbank', 'MySQL-Datenbank phpmyadmin', 'Web-Content-Filter-Listen', 'Verzeichnis „TestSYNC“', 'Webmail-Benutzereinstellungen', 'Verzeichnis „ntopng“', 'Spamfilter-Datenbank', 'E-Mail Archiv - aktives Volume', 'Spam- und Viren-Postfächer (admin.virus, admin.spam)', 'LDAP-Verzeichnis', 'Lizenzstatus', 'Verzeichnis „freigabe“', 'E-Mail Archiv - inaktive Volumes', 'E-Mail Archiv - ISOs' (which is checked), 'Systemkonfiguration', 'Postfächer (ohne admin.virus und admin.spam)', 'Log-Dateien und Log-Auswertung', 'Zarafa-Bricklevel-Storage (Default_Zarafa_target)', 'E-Mail Archiv - grundlegende Daten', 'Verzeichnis „Backup“', 'Zarafa E-Mail Anhänge', 'Verzeichnis „porno“', and 'Heimatverzeichnisse'. A right-hand pane shows the details for the selected 'E-Mail Archiv - ISOs' item.

Nachdem die Wiederherstellung gestartet wurde kann man den Status im Menüpunkt „System → Datensicherung → Status und Betrieb → Alle Jobs / Laufende Jobs“ einsehen.