

Michael Pietroforte

Backup-Software
Konzepte-Bewertung-Vergleich
Version 1.0

Kapitel Dantz Retrospect 6.5 Multi-Server

<http://www.pietroforte.de>

Dantz Retrospect 6.5 Multi-Server

Ausgaben

Retrospect ist in drei verschiedenen Ausgaben verfügbar: Professional, Single-Server, Multi-Server. Die Professional-Ausgabe ist nicht für die Serverversionen von Windows gedacht, sondern nur für die Arbeitsplätze. Mit der Single-Server-Ausgabe können außer dem Server auf dem Retrospect installiert ist, auch noch alle PC-Arbeitsplätze und mit der Multi-Server-Ausgabe beliebig viele Server über das Netz gesichert werden. Dem Test liegt die Multi-Server-Ausgabe zu Grunde.

Installation

Die Installation der Server- beziehungsweise Client-Software muss zunächst vor Ort durchgeführt werden, die Clients werden dann auf dem Server von Hand eingebunden. Retrospect findet dabei die Clients im lokalen Netz über Multicast, Clients in anderen Subnetzen lassen sich durch Angabe von Netzwerkadresse und Subnetzmaske mithilfe von Broadcasts auffinden. Schließlich können auch einzelne Rechner über IP-Adressen oder Rechnernamen (DNS beziehungsweise WINS) direkt angesprochen werden.

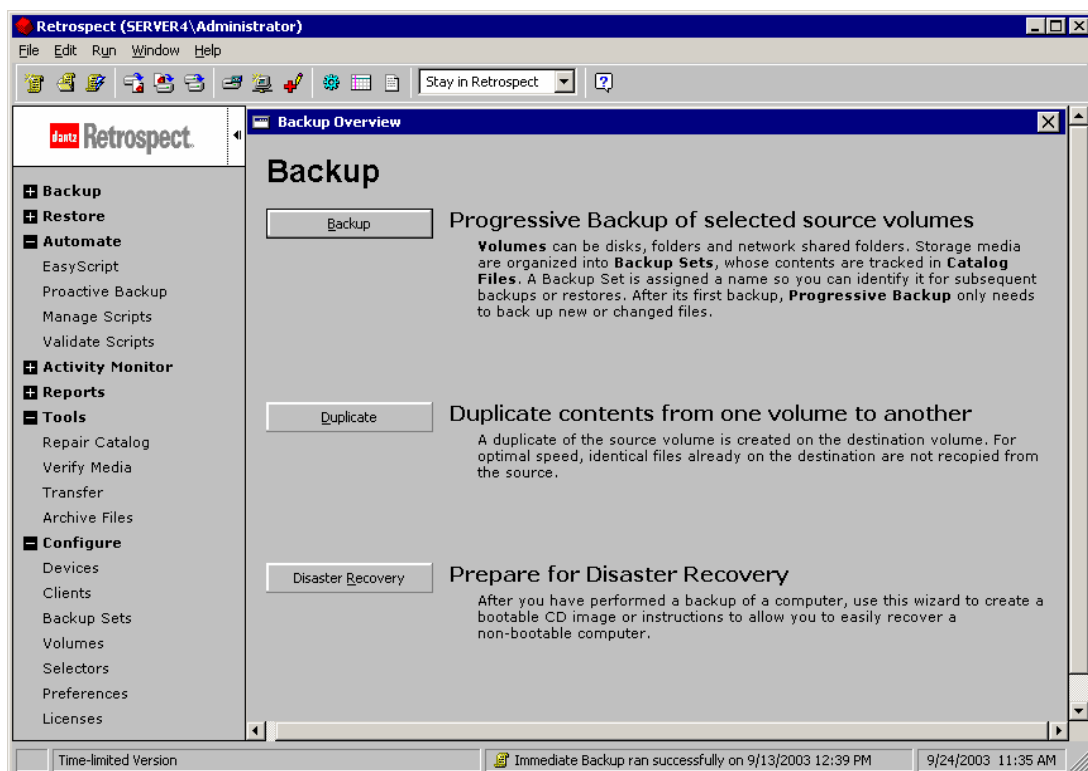


Abbildung 1: Der Startbildschirm von Retrospect

Bei der Integration in die Retrospect-Datenbank muss dann das bei der Installation des Clients gewählte Passwort angegeben werden. Fortan erscheint der Client in der „Volumes Database“ und steht damit zur Auswahl für Backup- und Restore-Jobs zur Verfügung. Positiv ist dabei,

dass die Backup-Clients klar zu unterscheiden sind von Rechnern, die lediglich über Windows-Freigaben zu sichern sind.

Außerdem werden die Rechner mit installiertem Backup-Client in die Client-Datenbank eingetragen, über die verschiedene Informationen wie die Netz-Adresse, die Volumes oder der Online-Status für die einzelnen Clients abrufbar sind. Neue Software-Versionen spielt der Administrator über das Netz ein, wobei leider nur die gerade online verfügbaren Maschinen auf den neuesten Stand gebracht werden. Maschinen, die sich nicht am Netz befinden, werden auch bei Wiederverfügbarkeit nicht aktualisiert.

Authentifikation

Die Authentifikation des Servers gegenüber den Clients geschieht mittels Passwort. Das Kennwort ist bei der Installation der Client-Software anzugeben und kann nachträglich zentral über die Server-Software verändert werden. Allerdings muss dies für jeden Client einzeln geschehen, was bei einem großen Netz recht aufwändig werden kann.

Auftragsdefinition

Die Definition von Einmalaufträgen und geplanten Aufträgen ist in zwei getrennten Bereichen untergebracht. Einmalaufträge können nicht gespeichert werden, so dass nur hin und wieder von Hand durchzuführende Jobs jedes Mal neu zu erstellen sind.

Geplante Aufträge lassen sich übersichtlich in einer hierarchischen Verzeichnisstruktur ordnen. Praktisch ist auch, dass Auftragsdefinitionen kopiert werden können. Das erspart Konfigurationsarbeit, wenn häufiger ähnliche Backup-Aufträge zu definieren sind.

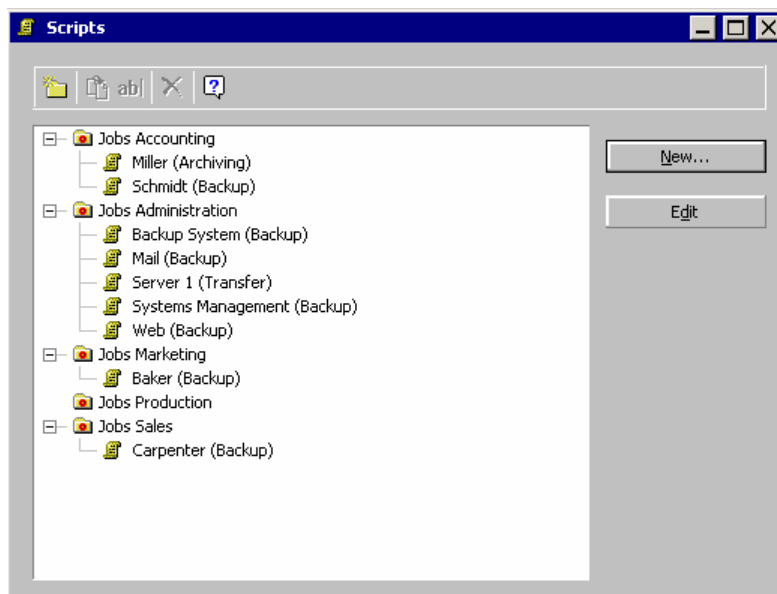


Abbildung 2: Backup-Aufträge werden in Ordner sortiert.

Datenselektion

Die Selektion der zu sichernden Daten erfolgt auf eine zunächst ungewohnte Weise. Der Volumes Database fügt man die Laufwerke beziehungsweise Unterverzeichnisse hinzu, welche sich dann innerhalb der Retrospect-Datenbank zu Gruppen zusammenfügen lassen. So können zum Beispiel verschiedene Verzeichnisse einer Abteilung, die über mehrere Server verstreut sind, zu einer virtuellen Gruppe zusammengefügt werden, die dann bei der Definition von Backup-Jobs als Backup-Quelle wählbar ist.

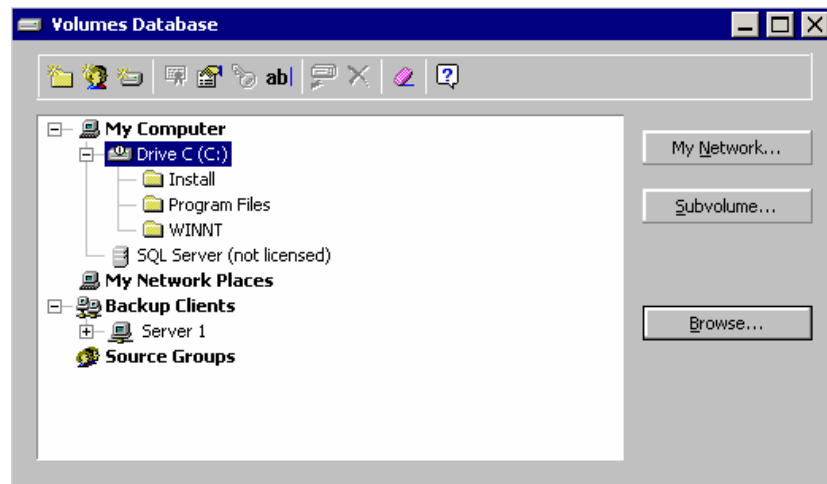


Abbildung 3: Die Volumes Database

Eine gezielte Auswahl einzelner Dateien ist nicht möglich, nur Laufwerke und Verzeichnisse können der Volumes-Datenbase hinzugefügt werden. Die Sicherung einzelner Dateien kann nur mit Einmalaufträgen erfolgen.

Medienauswahl

Das Backup-Ziel wird bei Retrospect als Backup-Satz bezeichnet. Einzelne Medien können bei der Definition des Backup-Satzes hinzugefügt werden. Falls die Kapazität des Backup-Satzes erschöpft ist, erweitert Retrospect den Backup-Satz automatisch mit dem nächsten verfügbaren leeren Medium. Dabei erfolgt die Eingrenzung auf bestimmte Backup-Geräte bei der Definition des Backup-Satzes und nicht wie sonst üblich bei der Auftragsdefinition.

Eine weitere interessante Eigenart von Retrospect ist die Möglichkeit, bei einer Auftragsdefinition mehrere Backup-Sätze als Ziel zu definieren. Welcher Backup-Satz beim Start eines Auftrags verwendet wird, ist über die Zeitplanung festzulegen.

Backup-Methoden

Andere Wege geht Retrospect auch bei der Backup-Methode. Inkrementelle oder differentielle Backups im üblichen Sinn gibt es bei Retrospect nicht, stattdessen kommt das Normal-Backup zum Einsatz. Dabei handelt es sich um die so genannte progressive Sicherungsmethode, ein Verfahren, dass man sonst eher bei Enterprise-Backup-Software findet. Es arbeitet bei der Datensi-

cherung im Prinzip wie ein inkrementelles Backup, unterscheidet sich aber in der Art und Weise, wie man bei einer Wiederherstellung der Daten vorzugehen hat.

Statt für ein Restore ein Komplet-Backup und eine Reihe inkrementeller Backups zurückzuspielen, wählt man einen Backup-Satz und das Datum an dem ein Backup-Job durchgeführt wurde. Welche Dateien an diesem Tag gesichert wurden, spielt keine Rolle, zurückgesichert wird der exakte Zustand der Backup-Quelle zum Zeitpunkt dieser Sicherung. Retrospect erzeugt bei jedem Start eines Backup-Jobs ein so genanntes Snapshot, ein Verzeichnis aller Dateien einer Backup-Quelle, mit dessen Hilfe es dann Dateien, die bei vorhergehenden Backup-Jobs gesichert wurden, im Backup-Satz ausfindig macht.

Mit dieser Methode lässt sich ein altbekanntes Problem von Inkrementell-Backups lösen. Bei der Datenwiederherstellung werden hier fälschlicherweise immer auch Dateien zurückgesichert, die im Zeitraum zwischen Komplet-Backup und den Inkrementell-Backups absichtlich gelöscht wurden. Da im Falle eines progressiven Backups, Dateien, die vor dem Zeitpunkt der Sicherung gelöscht wurden, nicht mehr im Snapshot verzeichnet sind, werden sie dann auch nicht fälschlicherweise wiederhergestellt.

Um zu erkennen, ob eine Datei sich verändert hat und damit gesichert werden muss, verwendet Retrospect nicht wie sonst üblich das Archiv-Bit, maßgebend sind vielmehr Datum beziehungsweise Uhrzeit der letzten Änderung und die Größe der Datei. Zusätzlich kann man noch den Speicherort zur Identifikation einer Datei miteinbeziehen. Macht man das nicht, werden Dateien deren Name, Größe und Erzeugungs- beziehungsweise Änderungsdatum übereinstimmen, nur einmal gesichert und zwar auch dann, wenn sie sich in verschiedenen Verzeichnissen befinden. Für den Fall, dass aus Sicherheitsgründen Kopien von wichtigen Dateien angelegt wurden, spart das Backup-Zeit und Platz auf dem Medium. Da im Snapshot verzeichnet ist, in welchen Ordnern sich die Dateien zum Zeitpunkt der Sicherung befanden, werden sie auch bei einem Restore wieder auf die richtigen Verzeichnisse verteilt.

Ein Normal-Backup verhält sich beim Sicherungs-Prozess also wie ein inkrementelles Backup, mit den Vorteilen einer kürzeren Backup-Zeit und eines geringeren Bedarfs an Speicherplatz auf dem Medium, beim Restore ist es aber wie ein Komplet-Backup zu handhaben. Natürlich speichert Retrospect ältere Snapshots, so dass immer die Möglichkeit besteht, auch Zustände vor der letzten Sicherung wiederherzustellen. Logisch gesehen befinden sich auf einem Backup-Satz also immer so viele Komplet-Backups wie Sicherungen stattgefunden haben, physikalisch wird eine Datei, die sich nie ändert, aber nur einmal gesichert. Im Vergleich zu einer Kombination von gewöhnlicher Komplettsicherung und Inkrementell- beziehungsweise Differential-Backup lassen sich so mit einem Progressiv-Backup Medienkapazitäten sparen, da mit dieser Methode viel seltener „echte“ Komplet-Backups durchgeführt werden müssen.

Ein Nachteil dieses Verfahrens ist, dass zur Erstellung des Snapshots vor dem Start der Sicherung zunächst die gesamte Backup-Quelle gescannt werden muss, was Rechnerressourcen frisst und mitunter auch eine Weile dauern kann. Ein weiteres Problem ist, dass bei Retrospect Snapshots immer einem bestimmten Backup-Satz zugeordnet sind, so dass man zur Wiederherstellung quasi die Medien kennen muss, die die Backup-Daten enthalten. Retrospect bietet zwar eine Suchfunktion, die es einem erlaubt mehrere Backup-Sätze nach einem Muster zu durchsuchen, doch muss hier bekannt sein, wie die Dateien oder Verzeichnisse heißen. Das Browsen durch eine Verzeichnisstruktur zur Auswahl der gewünschten Daten bietet diese Suchfunktion nicht. Die fehlende Abstraktion von den Backup-Medien mag etwas befremdlich wirken, wenn man jedoch die Backup-Satz-Bezeichnung sinnvoll wählt, dürfte dieser Nachteil nicht so sehr ins Gewicht fallen.

Medienrotation

Die automatische Wiederverwendung von Medien wird bei Retrospect ebenfalls anders umgesetzt als bei der Konkurrenz. Zum Einsatz kommt hier eine weitere Backup-Methode, das so genannte Recycle-Backup. Dabei handelt es sich um ein Komplett-Backup, das den Ziel-Backup-Satz überschreibt, das entsprechende Snapshot löscht und ein neues Snapshot für die entsprechende Backup-Quelle anlegt. Ein nachfolgendes Normal-Backup wird dieses Snapshot weiterverwenden und dann nur noch veränderte Dateien sichern.

Das interessante an diesem Verfahren ist die Tatsache, dass der Überschreibschutz eines Backup-Satzes zu einem genau definierten Termin aufgehoben wird. Dieses Überschreibdatum ist im Rahmen der Zeitplanung eines Backup-Auftrags zu definieren und nicht wie sonst üblich, bei der Konfiguration von Überschreibrichtlinien für die Mediensätze. Auf diese Weise ist es für den Administrator wesentlich einfacher, den Überblick zu behalten, wann und unter welchen Bedingungen Medien überschrieben werden.

Nachteilig wirkt sich bei diesem Verfahren aus, dass immer der gesamte Backup-Satz mit allen seinen enthaltenen Medien wieder in den Backup-Kreislauf eingebunden werden muss, da ja ein Snapshot dem gesamten Backup-Satz zugeordnet ist. Alle darauf befindlichen Daten gehen bei der Wiederverwendung des Backup-Satzes auf einmal verloren, also auch dann, wenn lediglich das Überschreiben eines Mediums für das Recycle-Backup notwendig wäre.

Auftragsplanung

Retrospect verfügt über zwei Typen von Backup-Jobs: Backup-Skripts und proaktive Backups. Letzteres ist nicht Bestandteil der Standardausführung und ist separat, als Add-on zu erwerben. Bei den Backup-Skripts handelt es sich nicht um Skripts im üblichen Sinn. Die Konfiguration erfolgt über eine grafische Oberfläche, ohne dass eine Zeile Programmcode einzugeben wäre.

Während die Backup-Skripts zu einem vorgegebenen Zeitpunkt starten, sind proaktive Jobs innerhalb eines definierten Zeitintervalls aktiv. In diesem Zeitraum versuchen sie möglichst viele Daten zu sichern, wobei jene Computer, die bereits länger nicht mehr gesichert wurden, eine höhere Priorität erhalten. Maschinen, die schon eine Weile nicht mehr am Netz angeschlossen waren, zum Beispiel Laptops, werden bei der Anmeldung am Netz erkannt und dann gesichert.

Einstellbar ist darüber hinaus, in welchem Zeitintervall ein Client erneut gesichert werden soll. Als Einheit stehen hier Tage oder Stunden zur Auswahl. Wenn der Administrator es erlaubt, dürfen Anwender aber schon vorher ein Backup anfordern. Dabei können sie jedoch die zu sichernden Daten nicht selbst selektieren, dies muss vorher schon vom Administrator am Server geschehen sein. Der Anwender kann lediglich über einen entsprechenden Schalter in der Client-Software dem Server mitteilen, dass zum nächstmöglichen Zeitpunkt eine Sicherung durchzuführen ist.

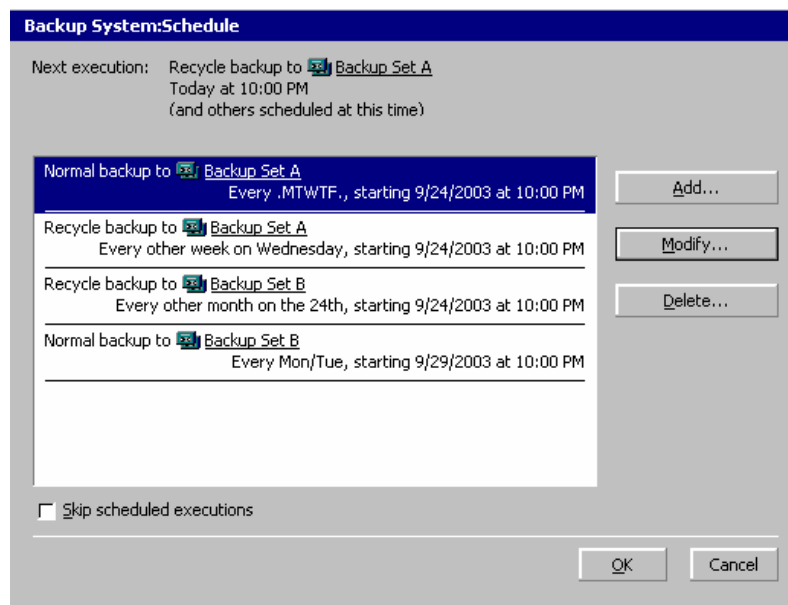


Abbildung 4: Ein Auftrag mit zwei Backup-Sätzen und jeweils zwei Zeitplänen

Die Zeitplanung der Backup-Skripts ist auf eine interessante Art und Weise organisiert. Jeder Auftragsdefinition können mehrere Zeitpläne zugeordnet werden, wobei die einzelnen Zeitpläne sich in der Backup-Methode aber auch in Bezug auf den Ziel-Backup-Satz unterscheiden dürfen. Durch die Kombination von Normal-Backup und Recycle-Backup ist so jede Rotationsstrategie umsetzbar. Als Zeitpläne werden bestimmte Termine festgelegt, oder auch Intervalle wie „alle drei Wochen“. Mit einer einzigen Auftragsdefinition kann man so auf recht einfache Weise eine komplette Rotationsstrategie für eine bestimmte Backup-Quelle konfigurieren.

Nützlich ist auch die Möglichkeit, ein geplantes Backup bis zu einem bestimmten Termin deaktivieren zu können. Finden zum Beispiel Wartungsarbeiten an einem bestimmten Backup-Gerät

statt, kann man so die entsprechenden Jobs für einen gewissen Zeitraum aussetzen, ohne sie später wieder aktivieren zu müssen.

Auftragsübersicht

Retrospects Auftragsübersicht ist vorbildlich. Proaktive Backups werden von geplanten Backup-Scripts getrennt in eigenen Registern angezeigt. Bei Letzteren ist nicht nur der kommende Auftrag zu sehen, sondern auch alle Auftragstermine für die folgenden Monate. Soll ein Auftrag an einem bestimmten Datum nicht starten, löscht man einfach den entsprechenden Eintrag in der Liste.

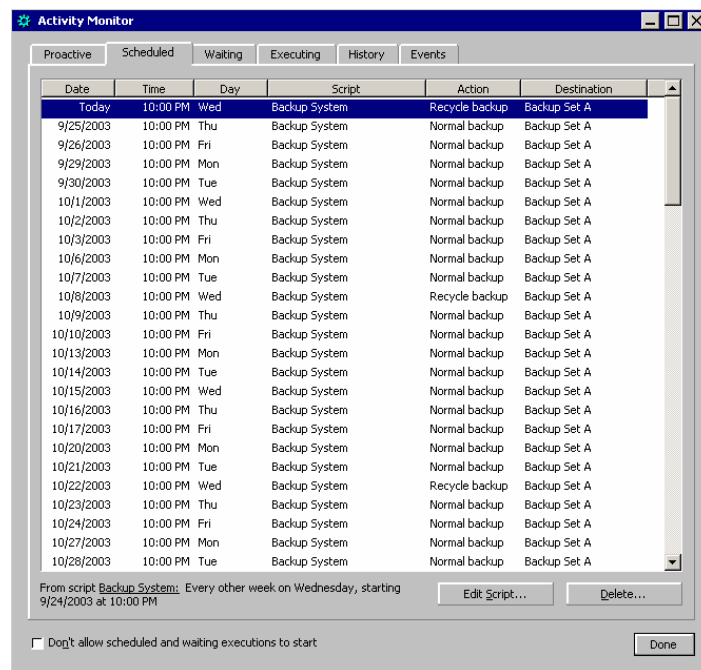


Abbildung 5: Die Auftragsübersicht

Bereits gestartete Jobs, die sich noch in der Warteschlange befinden und zum Beispiel auf ein freies Backup-Gerät warten, erhalten gleichfalls eine eigene Übersicht, ebenso wie die gerade aktiven Jobs. Zwei weitere Register beinhalten die abgearbeiteten Jobs und Ereignismeldungen.

Alerts

Meldungen über Ereignisse aller Art zeigt Retrospect unter dem Event-Register in der Auftragsübersicht an. Ein Ereignis kann zum Beispiel der Start eines proaktiven Backups sein oder ein gescheiterter Zugriffsversuch auf eine Backup-Quelle. Ansonsten sind Retrospects interne Alerting-Fähigkeiten eher bescheiden, wenn Administratoren via Netz zu informieren sind. Lediglich Fehlermeldungen, die beim Medienzugriff erzeugt wurden, können an eine E-Mail-Adresse weitergeleitet werden.

Allerdings ist das Versenden von Nachrichten mithilfe von externen Skripten in einer beliebigen Skriptsprache möglich. Über Kommandozeilenbefehle können Ereignisse aus Retrospect abge-

fragt und dann in Abhängigkeit von den Möglichkeiten der jeweiligen Skriptsprache an die Systemverwaltung weitergeleitet werden.

Protokolle

Der Zugriff auf Protokollinformationen von Aufträgen ist bei Retrospect an mehreren Stellen möglich: in der Auftragsübersicht der abgearbeiteten Jobs, in der Gesamtlogdatei und über den so genannten „Backup-Report“. Während das Logfile, das über die Auftragsübersicht zu erreichen ist, nur das Protokoll des jeweiligen Auftrags anzeigt, enthält die Gesamtlogdatei eine chronologische Abfolge der Protokolle aller Aufträge.

Reports

Der Backup-Report ist nicht das, was man sich normalerweise unter einem Report vorstellt. Es handelt sich dabei vielmehr um eine Übersicht aller Backup-Quellen mit ihrem letzten Sicherungsdatum. Die Übersicht kann man sich in eine einfache Textdatei ausgeben, welche mit jedem Editor zu öffnen ist. Interessant ist aber vor allem die Möglichkeit, direkt auf das Logfile und die Definition des Jobs zuzugreifen, der das entsprechende Verzeichnis gesichert hat.

Ein weitere Übersicht führt alle Backup-Sätze mit ihren Sicherungsaufträgen auf. Für jeden einzelnen dieser Aufträgen kann man sich die Dateien anzeigen lassen, die bei diesem Auftrag auf den Backup-Satz kopiert wurden.

Zusammenfassung

- Die Einbindung von Clients in entfernten Subnetzen ist sehr einfach möglich.
- Die Client-Server-Authentifizierung erfolgt passwortbasiert.
- Es sind zwei Typen von zeitgesteuerten Backup-Jobs verfügbar: zu einem bestimmten Zeitpunkt startende oder innerhalb eines Zeitintervalls ablaufende Aufträge.
- Die zu sichernden Server und Verzeichnisse müssen zunächst der Volumes Database hinzugefügt werden.
- Retrospect arbeitet mit progressiven statt mit inkrementellen oder differentiellen Backups.
- Anstelle des Archiv-Bits ist Dateiname, Datum und Größe ausschlaggebend bei der Auswahl der zu sichernden Daten.
- Für das Restore muss der Backup-Satz bekannt sein.
- Es gibt keine Überschreibrichtlinien für Mediensätze, stattdessen wird das Überschreiben des gesamten Backup-Satzes im Rahmen einer Auftragsdefinition geplant.