Acronis
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.DE

Acronis® Backup & Recovery ™ 10 Server für Linux

Update 5

Benutzerhandbuch

Inhaltsverzeichnis

1 Einführung in Acronis® Backup & Recovery™ 10

1.1 Acronis Backup & Recovery 10 – Überblick

Basierend auf der patentierten Disk Imaging- und Bare Metal Restore-Technologie ist Acronis Backup & Recovery 10 der Nachfolger von Acronis True Image Echo – und somit die nächste Generation unserer Desaster Recovery-Lösungen.

Acronis Backup & Recovery 10 Server für Linux bewahrt die Vorteile der Acronis True Image Echo-Produktfamilie:

- Backup kompletter Laufwerke bzw. Volumes, einschließlich des Betriebssystems, aller Anwendungen und Daten
- Wiederherstellung auch auf fabrikneuen Computern mit jeder Hardware
- Backup und Wiederherstellung von Dateien und Ordnern

Acronis Backup & Recovery 10 Server für Linux unterstützt Sie noch besser, um der Anforderung nach kurzen Wiederherstellungszeiten bei gleichzeitig reduzierten Kosten für Anlagen bzw. Geräte und Software-Wartung gerecht zu werden.

- **Nutzung vorhandener IT-Infrastruktur**

  Abwärtskompatibilität mit und einfaches Upgrade von Acronis True Image Echo
- **Hochautomatisierte Datensicherung**

  Allseitige Planung für den Schutz Ihrer Daten (Backup, Bewahrung und Validierung von Sicherungen) über Backup-Richtlinien

  Integration der Backup-Schemata „Türme von Hanoi“ und „Großvater-Vater-Sohn“ mit anpassbaren Parametern

  Sie können aus einer Vielzahl von Ereignissen und Bedingungen wählen, um Backups auszulösen.
- **Neu gestaltete Benutzeroberfläche (GUI)**

  Dashboard (Anzeigetafel) für schnelle operative Entscheidungen

  Überblick aller konfigurierten und laufenden Aktionen mit Farbkodierung für erfolgreiche und fehlgeschlagene Aktionen
- **Zusätzliche Möglichkeiten bei bootfähigen Medien**

  Auf bootfähigen Medien sind die Befehlszeilen-Werkzeuge von Linux und Acronis verfügbar, um vor Start einer Wiederherstellung logische Laufwerksstrukturen erstellen zu können.

1.2 Erste Schritte

Direkte Verwaltung

1. Installieren Sie die Acronis Backup & Recovery 10 Management Console und den Acronis Backup & Recovery 10-Agenten.
2. Starten Sie die Konsole.

Linux

Melden Sie sich als „root“ an oder melden Sie sich als normaler Benutzer an und wechseln falls benötigt den Benutzer. Starten Sie die Konsole mit dem Befehl

```
/usr/sbin/acronis_console
```

3. Verbinden Sie die Konsole mit der Maschine, auf der der Agent installiert ist.

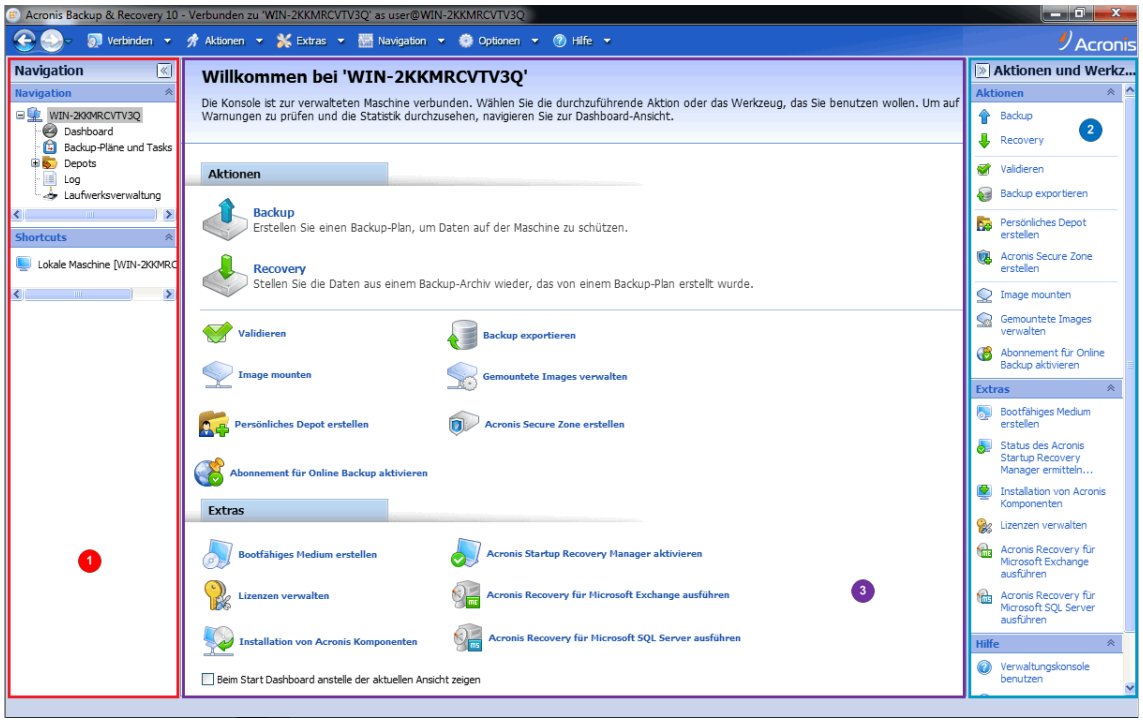
Wie es weitergeht

Informationen zu den folgenden Schritten finden Sie unter „Grundlegende Konzepte (S. 17)“.

Informationen zu den Elementen der grafischen Benutzeroberfläche finden Sie unter „Management Konsole verwenden (S. 7)“.

1.2.1 Verwaltungskonsole benutzen

Sobald die Konsole mit einer verwalteten Maschine (S. 197) oder einem Management Server (S. 193) verbunden ist, werden die entsprechenden Elemente in der gesamten Arbeitsumgebung der Konsole angezeigt (im Menü, im Hauptfenster mit dem Fenster **Willkommen**, im Fensterbereich **Navigation**, im Fensterbereich **Aktionen und Werkzeuge**), wodurch Ihnen ermöglicht wird, agenten- oder serverspezifische Aktionen auszuführen.



Acronis Backup & Recovery 10 Management Console – Startseite

Wichtige Elemente der Arbeitsumgebung der Konsole

	Name	Beschreibung
1	Fensterbereich **Navigation**	Enthält den **Navigationsbaum** sowie den Bereich **Shortcuts** und ermöglicht Ihnen, zwischen den einzelnen Ansichten zu wechseln (siehe Abschnitt Navigations-Seitenleiste (S. 8)).
2	Seitenleiste **Aktionen und Werkzeuge**	Enthält Zusammenstellungen von ausführbaren Aktionen und Werkzeugen (siehe Abschnitt Seitenleiste „Aktionen und Werkzeuge“ (S. 9)).

3	**Hauptfenster**	Die zentrale Arbeitsfläche, in der Sie Backup-Pläne, Richtlinien und Tasks erstellen, bearbeiten und verwalten sowie andere Aktionen ausführen. Zeigt verschiedene Ansichten und Aktionsseiten (S. 11) in Abhängigkeit von den Elementen an, die im Menü, **Navigationsbaum** oder in der Seitenleiste **Aktionen und Werkzeuge** ausgewählt wurden.
4	**Menüleiste**	Verläuft quer über den oberen Bereich des Programmfensters und ermöglicht Ihnen, alle in beiden Seitenleisten verfügbaren Aktionen auszuführen. Die Element des Menüs ändern sich dynamisch.

Um bequem mit der Verwaltungskonsole arbeiten zu können, ist eine Anzeigeauflösung von 1024x768 oder höher erforderlich.

Fensterbereich „Navigation“

Die Seitenleiste Navigation enthält einen **Navigationsbaum** und den Bereich **Shortcuts**.

Verzeichnisbaum „Navigation“

Mit Hilfe des Verzeichnisbaums **Navigation** können Sie sich durch die Programm-Ansichten bewegen. Welche Ansichten verfügbar sind, hängt davon ab, ob die Konsole mit einer verwalteten Maschine oder mit dem Management Server verbunden ist.

Ansichten für eine verwaltete Maschine

Wenn die Konsole mit einer verwalteten Maschine verbunden ist, sind die folgenden Ansichten im Navigationsbaum verfügbar.

- **[Name der Maschine]**. Die oberste Ebene des Baums (root) wird auch **Willkommens-Ansicht** genannt. Hier wird der Name der Maschine angezeigt, mit der die Konsole momentan verbunden ist. Verwenden Sie diese Ansicht, um schnell auf wichtige Aktionen zuzugreifen, die auf der verwalteten Maschine verfügbar sind.
  - **Dashboard**. Verwenden Sie diese Ansicht, um auf einen Blick einschätzen zu können, ob die Daten auf der verwalteten Maschine erfolgreich gesichert sind.
  - **Backup-Pläne und Tasks**. Verwenden Sie diese Ansicht, um Backup-Pläne und Tasks auf der verwalteten Maschine zu verwalten: Sie können hier Pläne und Tasks ausführen, bearbeiten, stoppen und löschen, ihre Stadien und Zustände anzeigen und Pläne überwachen.
  - **Depots**. Verwenden Sie diese Ansicht, um persönliche Depots und darin gespeicherte Archive zu verwalten, neue Depots hinzuzufügen, bestehende Depots umzubenennen oder zu löschen, Depots zu validieren, Backup-Inhalte zu untersuchen, Backups als virtuelle Geräte zu mounten usw.
  - **Log**. Verwenden Sie diese Ansicht, um Informationen zu solchen Aktionen zu überprüfen, die vom Programm auf der verwalteten Maschine ausgeführt werden.

Seitenleistenbereich „Shortcuts“

Der Bereich **Shortcuts** wird unterhalb des Navigationsbaums angezeigt. Ermöglicht Ihnen, in einfacher und bequemer Weise eine Verbindung mit oft benötigten Maschinen herzustellen, indem Sie diese als Shortcuts hinzufügen.

So weisen Sie einer Maschine einen Shortcut zu

1. Verbinden Sie die Konsole mit einer verwalteten Maschine.
2. Klicken Sie im Verzeichnisbaum „Navigation“ mit der rechten Maustaste auf den Namen der Maschine (Root-Element des Verzeichnisbaums „Navigation“) und wählen Sie **Shortcut erstellen**.

Wenn die Konsole und der Agent auf derselben Maschine installiert sind, wird der Shortcut auf diese Maschine automatisch als **Lokale Maschine [Name der Maschine]** zum Shortcuts-Bereich hinzugefügt.

Bereich „Aktionen und Werkzeuge“

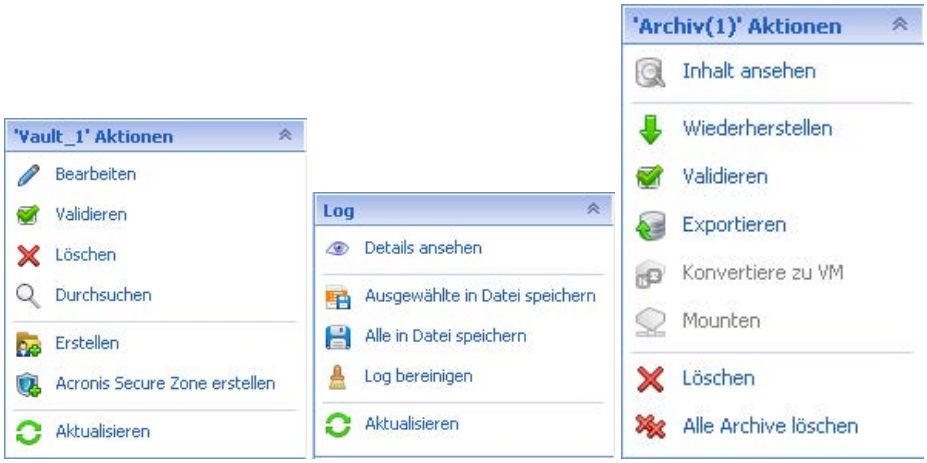
Im Bereich **Aktionen und Werkzeuge** können Sie in einfacher und effizienter Weise mit Acronis Backup & Recovery 10 arbeiten. Die Bereiche der Seitenleisten bieten einen schnellen Zugriff auf die Aktionen und Werkzeuge des Programms. Alle Elemente des Bereichs **Aktionen und Werkzeuge** sind außerdem im Programm-Menü verfügbar.

Seitenleistenbereiche

Aktionen für „[Name des Elements]“

Enthält eine Zusammenstellung von Aktionen, die in einer beliebigen Navigationsansicht auf ausgewählte Elementen angewendet werden können. Wenn Sie auf die Aktion klicken, wird die entsprechende Aktionsseite (S. 12) geöffnet. Elemente aus unterschiedlichen Navigationsansichten haben jeweils eigene Zusammenstellungen von Aktionen. Der Name des Seitenleistenbereiches ändert sich in Abhängigkeit davon, welches Element Sie ausgewählt haben. Wenn Sie beispielsweise in der Ansicht **Backup-Pläne und Tasks** den Backup-Plan mit dem Namen *System-Backup* auswählen, erhält der Aktionsbereich die Bezeichnung **Aktionen für System-Backup** und erhält eine Zusammenstellung von Aktionen, die typisch für Backup-Pläne sind.

Auf alle Aktionen kann auch über das entsprechende Menü zugegriffen werden. Wenn Sie ein Element in einer beliebigen Navigationsansicht auswählen, wird ein Element in der Menüleiste angezeigt.



Beispiele für Seitenleistenbereiche mit der Bezeichnung „Aktionen für [Name des Elements]“

Aktionen

Enthält eine Liste üblicher Aktionen, die auf einer verwalteten Maschine oder auf einem Management Server ausgeführt werden können. Diese ist für alle Ansichten gleich. Wenn Sie auf die Aktion klicken, wird die entsprechende Aktionsseite geöffnet (siehe Abschnitt Aktionsseiten (S. 12)).

Auf alle Aktionen kann auch über das Menü **Aktionen** zugegriffen werden.

Seitenleistenbereich „Aktionen“ auf einer verwalteten Maschine und auf einem Management Server

Werkzeuge

Enthält eine Liste der Werkzeuge von Acronis. Diese ist in allen Programmansichten gleich.

Auf alle Werkzeuge kann auch über das Menü **Extras** zugegriffen werden.

Seitenleistenbereich „Werkzeuge“

Hilfe

Enthält eine Liste von Hilfethemen. Es gibt unterschiedliche Ansichten und Aktionsseiten in Acronis Backup & Recovery 10 mit entsprechenden Listen von Hilfethemen.

Aktionen mit Seitenleisten

So erweitern/minimieren Sie die Seitenleisten

In der Standardeinstellung ist der Fensterbereich **Navigation** erweitert und der Fensterbereich **Aktionen und Werkzeuge** minimiert. Möglicherweise müssen Sie die Seitenleisten minimieren, um sich zusätzliche freie Arbeitsfläche zu verschaffen. Zur Umsetzung klicken Sie auf das Chevron-Symbol (« – für den Fensterbereich **Navigation**; » – für den Fensterbereich **Aktionen und Werkzeuge**). Die Seitenleiste wird daraufhin minimiert und das Chevron-Symbol ändert seine Ausrichtung. Klicken Sie ein weiteres Mal auf das Chevron-Symbol, um die Seitenleiste zu erweitern.

So ändern Sie die Begrenzungen der Seitenleiste

1. Zeigen Sie auf die Begrenzungslinie der Seitenleiste
2. Wenn der Zeiger als Pfeil mit zwei Spitzen angezeigt wird, dann ziehen Sie, um den Rand zu verschieben.

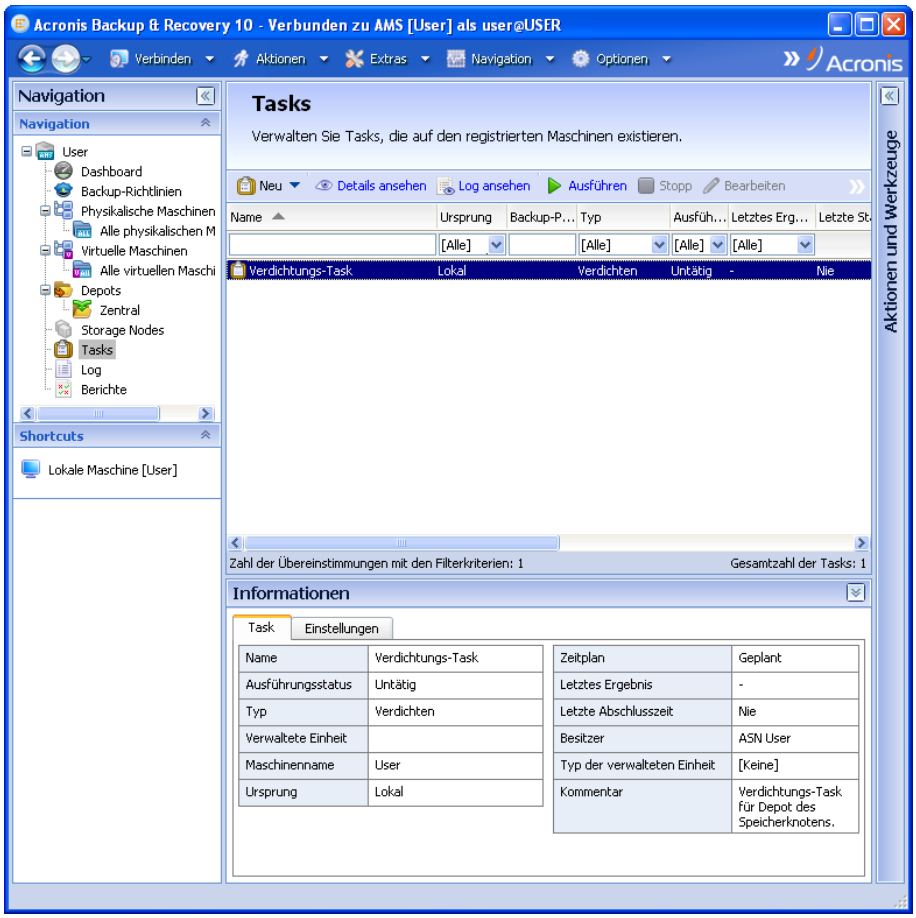
Die Verwaltungskonsole „merkt sich“, wie die Begrenzungslinien der Seitenleisten eingestellt sind. Wenn Sie die Verwaltungskonsole das nächste Mal starten, befinden sich alle Begrenzungslinien der Seitenleiste an der zuvor eingestellten Position.

Hauptfenster, Ansichten und Aktionsseiten

Das Hauptfenster ist der zentrale Bereich, in dem Sie mit der Konsole arbeiten. Sie können Backup-Pläne, Richtlinien und Tasks erstellen, bearbeiten und verwalten sowie andere Aktionen ausführen. Das Hauptfenster zeigt verschiedene Ansichten und Aktionsseiten in Abhängigkeit von den Elementen, die im Menü, **Navigationsbaum** oder in der Seitenleiste **Aktionen und Werkzeuge** ausgewählt wurden.

Ansichten

Wenn Sie auf ein beliebiges Element im **Navigationsbaum** der Seitenleiste Navigation (S. 8) klicken, wird eine entsprechende Ansicht angezeigt.



Ansicht „Tasks“

Übliche Arbeitsweise mit Ansichten

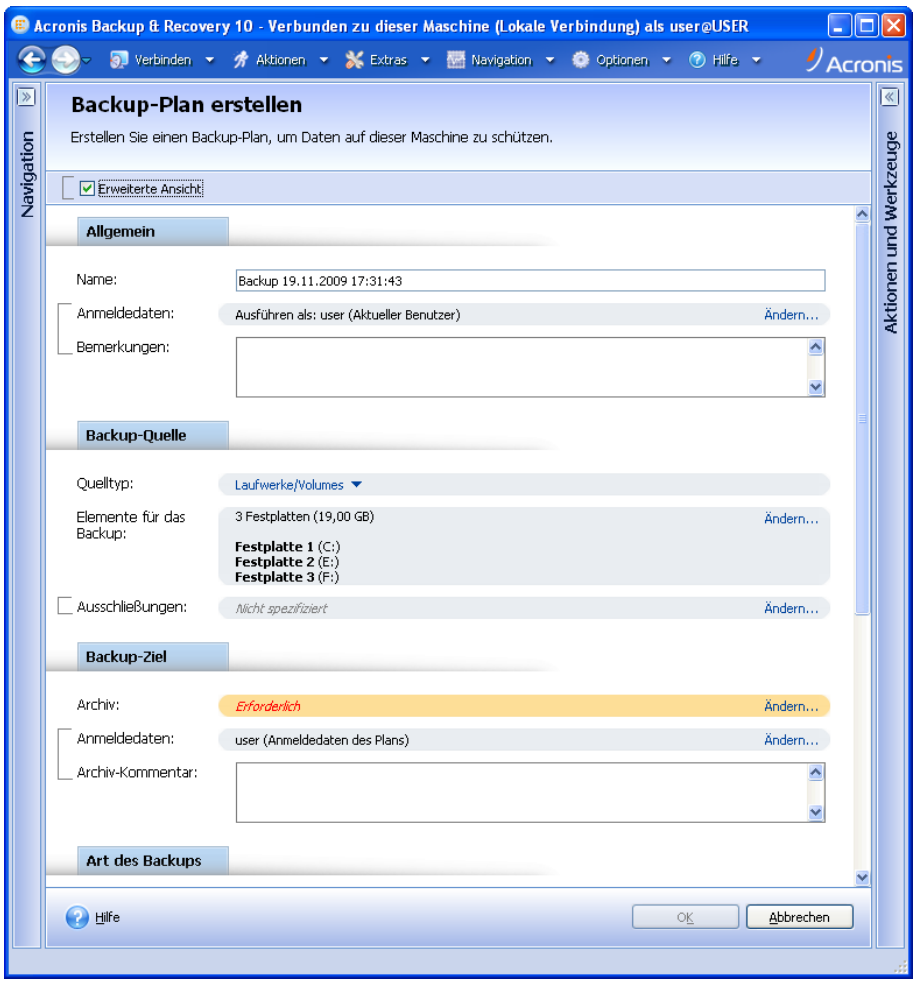
In der Regel enthält jede Ansicht eine Tabelle mit Elementen, eine Symbolleiste mit Schaltflächen für die Tabelle sowie den unteren Fensterbereich **Informationen**.

- Verwenden Sie die Filter- und Sortierfunktionen, um die Tabelle nach dem gewünschten Element zu durchsuchen
- Wählen Sie in der Tabelle das gewünschte Element aus
- Sehen Sie sich im Fensterbereich **Informationen** (standardmäßig eingeklappt) die Details des Elements an

- Führen Sie die entsprechenden Aktionen mit dem ausgewählten Element aus. Es gibt verschiedene Möglichkeiten, wie Sie ein und dieselbe Aktion mit ausgewählten Elementen ausführen können:
  - Indem Sie auf die Schaltflächen in der Symbolleiste der Tabelle klicken;
  - Indem Sie auf die Befehle in Bereich **Aktionen für [Name des Elements]** (in der Seitenleiste **Aktionen und Werkzeuge**) klicken;
  - Indem Sie die Befehle im Menü **Aktionen** auswählen;
  - Indem Sie mit der rechten Maustaste auf das Element klicken und die Aktion im Kontextmenü auswählen.

Aktionsseiten

Eine Aktionsseite wird im Hauptfenster angezeigt, wenn Sie auf ein Aktionselement im Menü **Aktionen** oder im Bereich **Aktionen** der Seitenleiste **Aktionen und Werkzeuge** klicken. Diese enthält Schritte, die Sie ausführen müssen, um einen beliebigen Task oder einen Backup-Plan oder eine Backup-Richtlinie zu erstellen und zu starten.



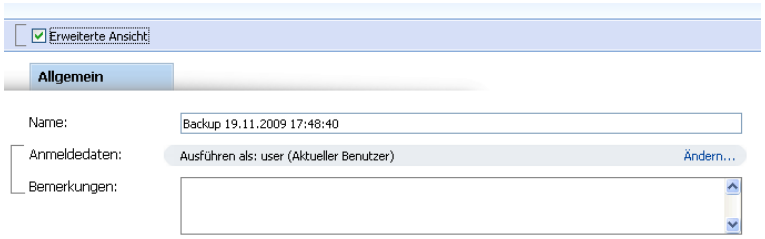
Aktionsseite – Backup-Plan erstellen

Steuerelemente verwenden und Einstellungen festlegen

Aktionsseiten können auf zwei verschiedene Weisen dargestellt werden: Einfach und erweitert. Bei der einfachen Darstellung werden bestimmte Felder ausgeblendet, wie z.B. Anmeldeinformationen, Kommentare usw. Wenn die erweiterte Darstellung aktiviert ist, dann werden alle verfügbaren

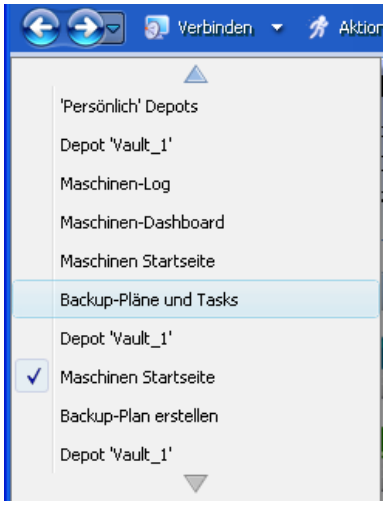
Felder angezeigt. Sie können zwischen den Ansichten umschalten, indem Sie das Kontrollkästchen **Erweiterte Ansicht** im oberen Bereich der Aktionsseite aktivieren bzw. deaktivieren.

Die meisten Einstellungen werden konfiguriert, indem Sie auf den entsprechenden Link **Ändern…** rechts neben der Einstellung klicken. Andere Einstellungen werden aus einem Listenfeld ausgewählt oder manuell in die Felder auf der Seite eingegeben.



Aktionsseite – Steuerelemente

Acronis Backup & Recovery 10 merkt sich die Änderungen, die Sie auf den Aktionsseiten vornehmen. Wenn Sie z.B. begonnen haben, einen Backup-Plan zu erstellen und dann aus irgendeinem Grund zu einer anderen Ansicht gewechselt sind, ohne die Plan-Erstellung abzuschließen, können Sie die Navigationsschaltfläche **Zurück** im Menü anklicken. Oder wenn Sie mehrere Schritte forwärts gegangen sind, klicken Sie den Pfeil **Nach unten** und wählen die Seite, auf der Sie die Plan-Erstellung aus der Liste gestartet haben. Auf diese Weise können Sie die verbleibenden Schritte ausführen und die Erstellung des Backup-Plans abschließen.



Navigationsschaltflächen

1.3 Acronis Backup & Recovery 10-Komponenten

Dieser Abschnitt enthält eine Liste der Acronis Backup & Recovery 10-Komponenten mit einer kurzen Beschreibung ihrer Funktion.

Komponenten für eine verwaltete Maschine (Agenten)

Dies sind Anwendungen zur Durchführung von Backups, Wiederherstellungen und anderen Aktionen auf Maschinen, die mit Acronis Backup & Recovery 10 verwaltet werden. Die Agenten benötigen je eine Lizenz zur Durchführung von Aktionen mit verwalteten Maschinen. Agenten haben mehrere Features (Add-ons), die zusätzliche Funktionen ermöglichen und daher möglicherweise weitere Lizenzen erfordern.

Konsole

Die Konsole stellt eine grafische Benutzerschnittstelle und Remote-Verbindung zu den Agenten zur Verfügung. Zur Verwendung der Konsole wird keine Lizenz benötigt.

Bootable Media Builder

Mit Bootable Media Buildern können Sie bootfähige Medien erstellen, damit Sie die Agenten und andere Rettungswerkzeuge in einer autonome Notfallversion verwenden können. Die Verfügbarkeit der Add-ons für die Agenten in der autonome Notfallversion hängt davon ab, welche Add-ons auf der Maschine installiert sind, auf der der Media Builder arbeitet.

1.3.1 Agent für Linux

Dieser Agent ermöglicht unter Linux eine Datensicherung auf Festplatten- und Datei-Ebene.

Disk-Backup

Dabei basiert die Datensicherung auf Festplatten-Ebene auf der Sicherung des gesamten Dateisystems auf einer Festplatte bzw. einer Partition, einschließlich aller zum Booten des Betriebssystems notwendigen Informationen; oder – bei einem Sektor-für-Sektor-Ansatz – auf der Sicherung der einzelnen Sektoren (raw-Modus). Ein Backup, das die Kopie einer Festplatte oder Partition in gepackter Form enthält, wird auch Disk-Backup (Partition-Backup, Volume-Backup) oder Disk-Image (Partition-Image, Volume-Image) genannt. Aus solchen Backups können Festplatten oder Partitionen in ihrer Gesamtheit wiederhergestellt werden, es können aber auch einzelne Dateien oder Ordner wiederhergestellt werden.

Datei-Backup

Die Datensicherung auf Datei-Ebene basiert auf der Sicherung von Dateien und Verzeichnissen, die sich auf der Maschine, auf der der Agent installiert ist oder auf einem freigegebenen Netzlaufwerk befinden, auf das über das SMB- oder das NFS-Protokoll zugegriffen wird. Dateien können an ihren ursprünglichen oder einen anderen Speicherort wiederhergestellt werden. Es ist möglich, alle gesicherten Dateien und Verzeichnisse wiederherzustellen. Sie können aber auch auswählen, welche Dateien und Verzeichnisse wiederhergestellt werden sollen.

1.3.2 Management Console

Acronis Backup & Recovery 10 Management Console ist ein administratives Werkzeug für den lokalen Zugriff auf Acronis Backup & Recovery 10 Agent für Linux. Eine Remote-Verbindung mit dem Agenten ist nicht möglich.

1.3.3 Bootable Media Builder

Acronis Bootable Media Builder ist ein spezielles Werkzeug zur Erstellung von bootfähigen Medien (S. 188). Der unter Linux installierte Media Builder erstellt bootfähige Medien, die auf dem Linux-Kernel basieren.

1.4 Unterstützte Dateisysteme

Acronis Backup & Recovery 10 kann Backups und Wiederherstellungen der folgenden Dateisysteme mit den angegebenen Einschränkungen ausführen:

- FAT16/32
- NTFS
- Ext2/Ext3/Ext4
- ReiserFS3 – aus Laufwerk-Backups, die sich auf dem Acronis Backup & Recovery 10 Storage Node befinden, können keine einzelnen Dateien wiederhergestellt werden
- ReiserFS4 – Volume-Wiederherstellung ohne Größenanpassung des Volumes; aus Laufwerk-Backups, die sich auf dem Storage Node in Acronis Backup & Recovery 10 befinden, können keine einzelnen Dateien wiederhergestellt werden
- XFS – Volume-Wiederherstellung ohne Größenanpassung des Volumes; aus Disk-Backups, die sich auf dem Storage Node in Acronis Backup & Recovery 10 befinden, können keine einzelnen Dateien wiederhergestellt werden
- JFS – aus Laufwerk-Backups, die sich auf dem Acronis Backup & Recovery 10 Storage Node befinden, können keine einzelnen Dateien wiederhergestellt werden
- Linux SWAP

Acronis Backup & Recovery 10 kann unter Verwendung eines Sektor-für-Sektor-Ansatzes Backups und Wiederherstellungen bei beschädigten oder nicht unterstützten Dateisystemen ausführen.

1.5 Unterstützte Betriebssysteme

Acronis Backup & Recovery 10 Management Console, Acronis Backup & Recovery 10 Agent für Linux

- Linux mit Kernel 2.4.18 oder später (einschließlich 2.6.x-Kernels) und glibc 2.3.2 oder später
- Diverse 32-Bit- und 64-Bit-Linux-Distributionen, einschließlich:
  - Red Hat Enterprise Linux 4.x und 5.x
  - Red Hat Enterprise Linux 6
  - Ubuntu 9.04 (Jaunty Jackalope), 9.10 (Karmic Koala) und 10.04 (Lucid Lynx)
  - Fedora 11 und 12
  - SUSE Linux Enterprise Server 10 und 11
  - Debian 4 (Lenny) und 5 (Etch)
  - CentOS 5
- Der Agent für Linux ist eine 32-Bit-Anwendung. Zur Authentifizierung verwendet der Agent Systembibliotheken, deren 32-Bit-Versionen nicht immer standardmäßig in 64-Bit-Distributionen installiert sind. Wenn Sie den Agenten auf einer 64-Bit-Distribution mit RedHat-Basis verwenden (etwa RHEL, CentOS, Fedora) oder auf einer 64-Bit-SUSE-Distribution, dann stellen Sie sicher, dass folgende 32-Bit-Pakete im System installiert sind:

  pam.i386

  libselinux.i386

  libsepol.i386

  Diese Pakete sollten im Repository der Linux-Distribution verfügbar sein.
- Bevor Sie das Produkt auf einem System installieren, das keinen RPM-Paketmanager verwendet (wie etwa ein Ubuntu-System), müssen Sie diesen Manager manuell installieren – beispielsweise durch Ausführung folgenden Befehls (als Benutzer 'root'):

```
apt-get install rpm
```

1.6 Systemanforderungen

Unter Linux installierte Komponenten

Edition	Speicher (zusätz. zu dem für OS und akt. Programme)	Erforderlicher Festplattenplatz während Installation oder Update	Durch Komponenten belegter Platz	Erweitert
Server für Linux	120 MB	400 MB	240 MB	Bildschirmauflösung 1024*768 Pixel oder höher
Bootable Media Builder (Linux)	70 MB	240 MB	140 MB	

Bootfähiges Medium

Medientyp	Arbeitsspeicher	ISO-Image-Größe	Erweitert
Linux-basiert	256 MB	130 MB	

1.7 Technischer Support

Maintenance- und Support-Programm

Wenn Sie Unterstützung für Ihr Acronis-Produkt benötigen, besuchen Sie http://www.acronis.de/support/.

Produkt-Updates

Sie können für all Ihre registrierten Acronis-Software-Produkte jederzeit Updates von unserer Website herunterladen, nachdem Sie sich unter **Mein Konto** (https://www.acronis.de/my) eingeloggt und Ihr Programm registriert haben. Weitere Informationen auch in den (englischsprachigen) Artikel unter **Registering Acronis Products at the Website** (http://kb.acronis.com/content/4834) und **Acronis Website User Guide** (http://kb.acronis.com/content/8128).

2 Acronis Backup & Recovery 10 verstehen

Dieser Abschnitt bemüht sich, den Lesern ein klareres, vertieftes Verständnis des Produktes zu vermitteln, damit es sich auch ohne Schritt-für-Schritt-Anleitungen unter den unterschiedlichsten Umständen erfolgreich einsetzen lässt.

2.1 Grundlegende Konzepte

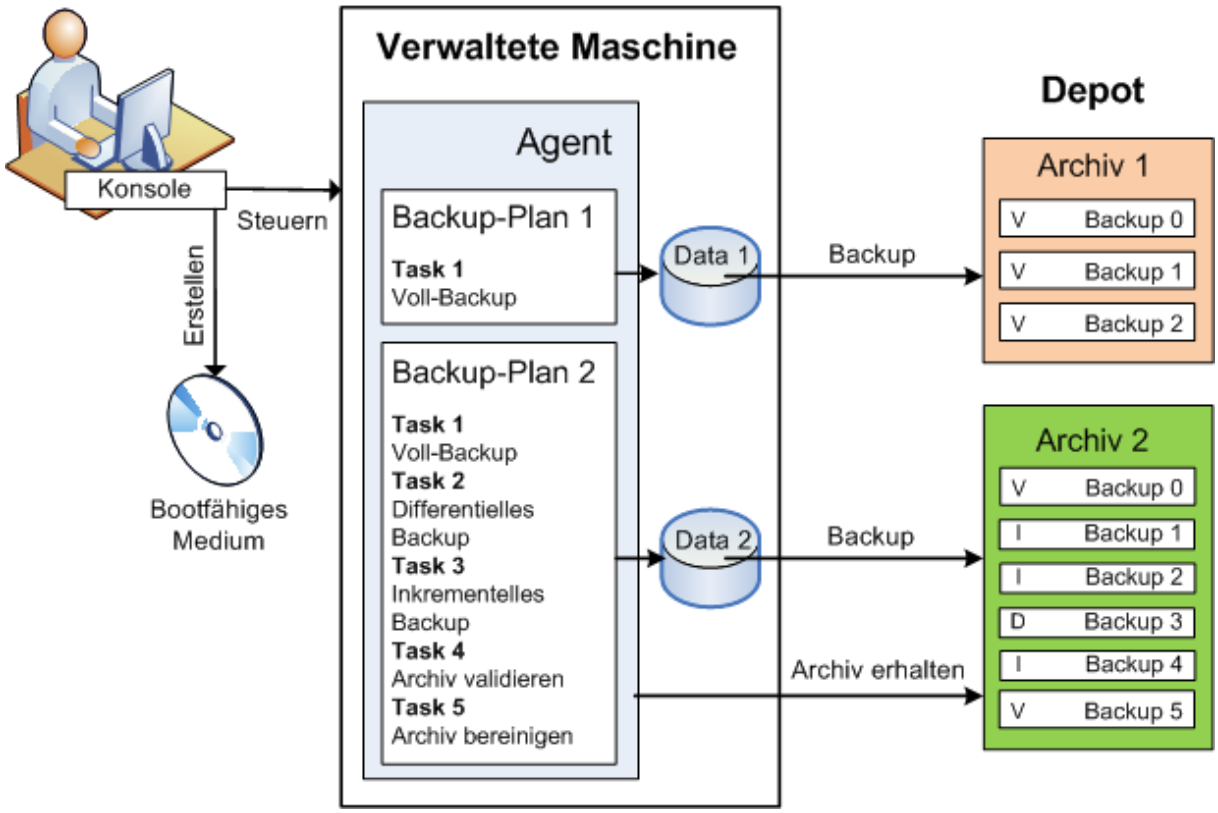
Machen Sie sich mit den grundlegenden Begriffen in der Benutzeroberfläche und Dokumentation von Acronis Backup & Recovery 10 vertraut. Fortgeschrittene Anwender können diesen Abschnitt auch als eine Schnellanleitung verwenden. Entsprechende Details können zudem in der kontextsensitiven Hilfe gefunden werden.

Backup unter einem Betriebssystem

1. Um die Daten einer Maschine zu schützen, installieren Sie auf dieser den Acronis Backup & Recovery 10 Agent (S. 185), wodurch die Maschine von diesem Zeitpunkt an zu einer verwalteten Maschine (S. 197) wird.
2. Um die Maschine mit einer grafischen Benutzeroberfläche zu managen, installieren Sie die Acronis Backup & Recovery 10 Management Console (S. 192) auf derselben oder jeder anderen Maschine, von der aus Sie operieren wollen. Sollten Sie die Standalone-Ausgabe des Produktes haben, so können Sie diesen Schritt überspringen, da in Ihrem Fall die Konsole zusammen mit dem Agenten installiert wird.
3. Die Konsole ausführen. Damit Sie für den Fall, dass das Betriebssystem nicht mehr startet, in der Lage sind, die betreffende Maschine wiederherzustellen, erstellen Sie ein bootfähiges Medium (S. 188).
4. Verbinden Sie die Konsole mit der verwalteten Maschine.
5. Einen Backup-Plan (S. 186) erstellen.

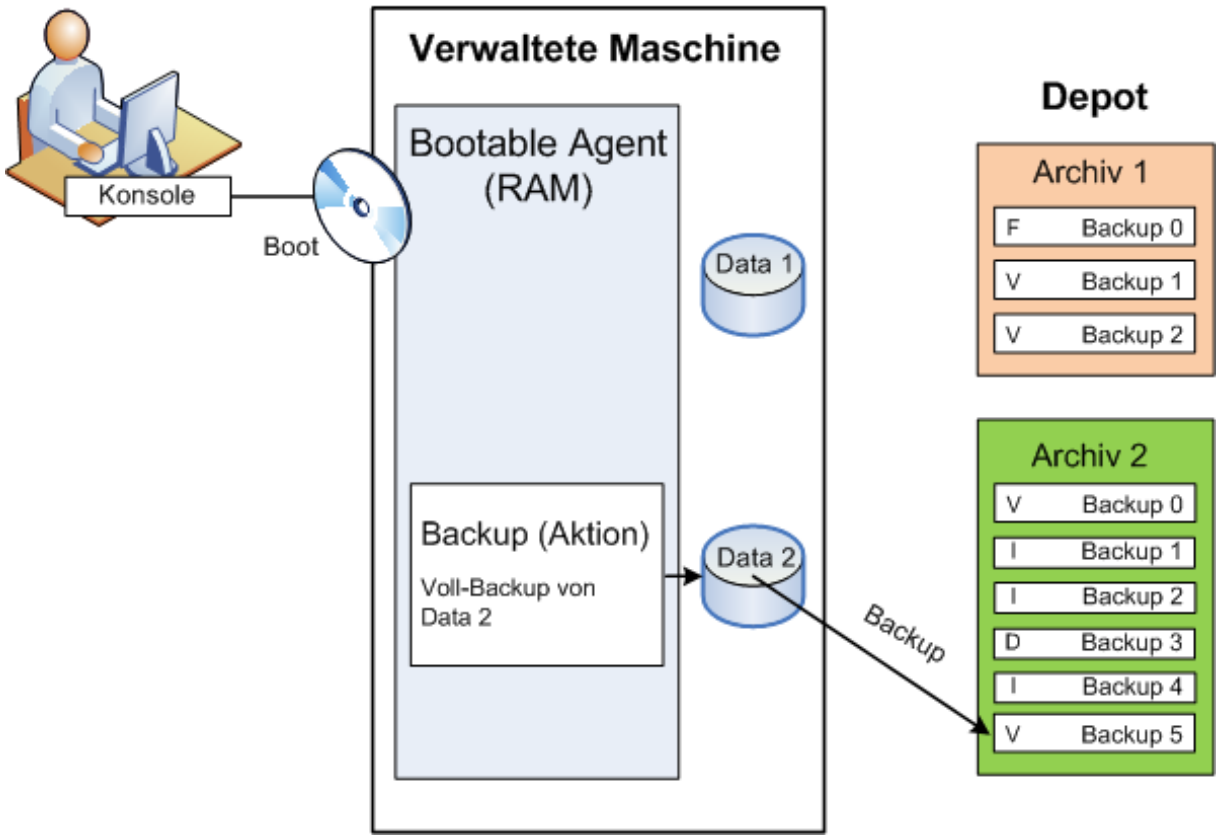
   Zur Umsetzung müssen Sie im Minimum die zu sichernden Daten sowie den Zielort spezifizieren, wo das erstellte Backup (S. 185) gespeichert wird. Das erstellt eine minimale, aus einem Task (S. 195) bestehende Backup-Aufgabe, die ein vollständiges Backup (S. 185) Ihrer Daten immer dann erstellt, wenn der Task manuell ausgeführt wird. Ein komplexer Backup-Plan kann dagegen aus mehreren, per Ereignis oder Zeitsteuerung geplanten Tasks bestehen, die vollständige, inkrementelle oder differentielle Backups (S. 21) erstellen, Wartungsaktionen wie Backup-Validierung (S. 196) durchführen oder veraltete Backups löschen (Säuberung (S. 187)). Sie können Backup-Aktionen mit Hilfe verschiedener Optionen anpassen, z.B. Vor-/Nach-Befehle, Begrenzung der Netzwerkbandbreite, Fehlerreaktionen oder einstellbare Ereignismeldungen.
6. Siehe **Backup-Pläne und -Tasks**, um mehr Informationen zu dieser Thematik zu erhalten. Siehe **Logs**, um die Ereignismeldungen der Aktion einzusehen.
7. Der Ort, an dem Sie Ihre Backup-Dateien speichern, wird Depot (S. 189) genannt. Wechseln Sie zur Seite **Depots**, um mehr Informationen zu dieser Thematik zu erhalten. Indem Sie dann zu einem speziellen Depot wechseln, können Sie weitere Informationen über hinterlegte Backups einsehen und mit diesen Aktionen ausführen (anschließen, validieren, löschen, Inhalte einsehen). Zudem können Sie ein Backup auch auswählen, um in ihm gespeicherte Daten wiederherzustellen.

Das folgende Diagramm illustriert die zuvor erläuterten Begriffe. Weitere Definitionen finden Sie im Glossar.



Backups mit bootfähigen Medien durchführen

Sie können eine Maschine unter Verwendung eines bootfähigen Mediums starten, eine Backup-Aktion wie einen einfachen Backup-Plan konfigurieren und die Aktion ausführen. Das hilft Ihnen, Dateien und logische Volumes von einem System mit Bootschwierigkeiten zu extrahieren, ein Abbild des Offline-Systems zu erstellen oder ein nicht unterstütztes Dateisystem per Sektor-für-Sektor-Backup zu sichern.



Recovery unter einem Betriebssystem

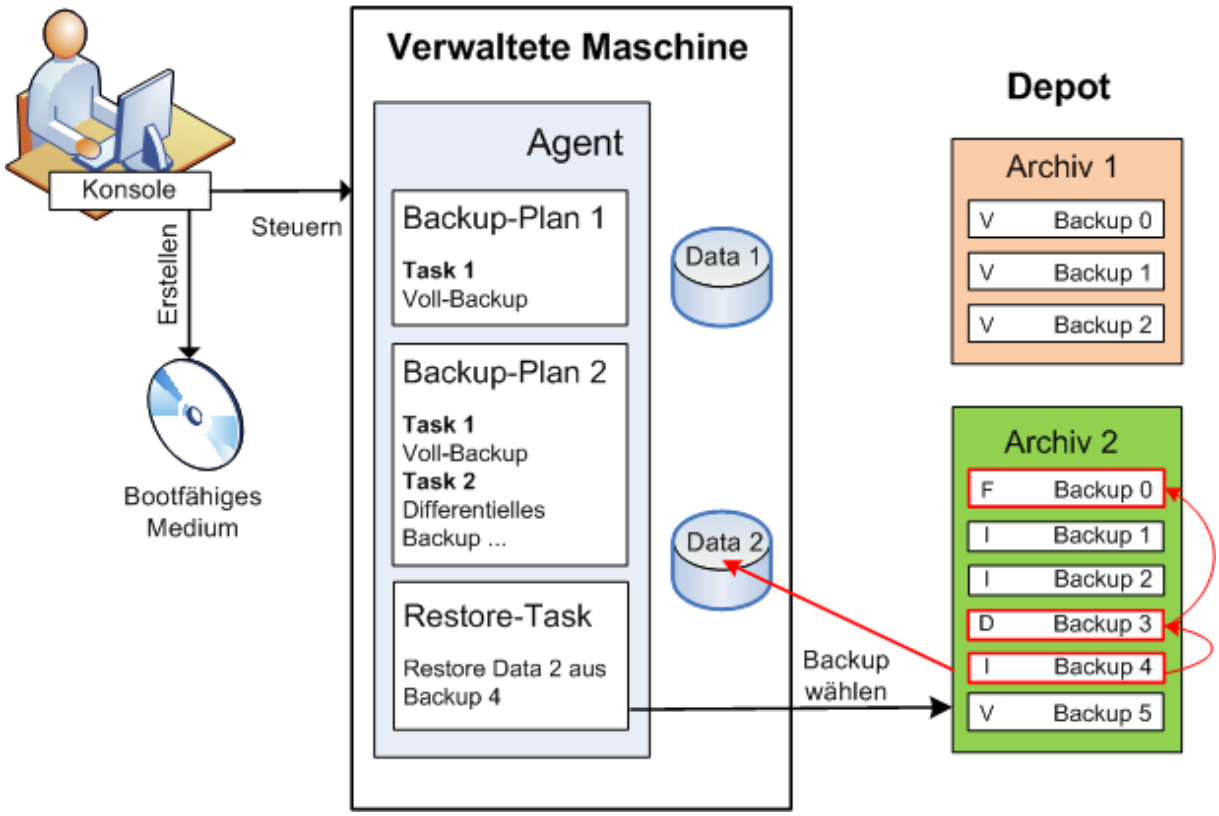
Wenn eine Wiederherstellung von Daten ansteht, so erstellen Sie auf der verwalteten Maschine einen Recovery-Task. Sie spezifizieren dafür zuerst das Depot und bestimmen dann das passende Backup anhand von Tag und Zeitpunkt, zu dem die ursprüngliche Sicherung gestartet wurde. In den meisten Fällen werden die Daten dann genau auf den Zustand dieses Zeitpunktes zurückgesetzt.

Beispiele für Ausnahmen von dieser Regel:
Die Wiederherstellung einer Datenbank aus einem Backup, das das Transaktions-Log enthält (ein einzelnes Backup enthält multiple Wiederherstellungspunkte, wodurch Sie eine zusätzliche Auswahlmöglichkeit haben).
Die Wiederherstellung multipler Dateien aus einem Backup, das ohne Snapshots erstellt wurde (jede Datei wird auf den Moment zurückgesetzt, zu dem sie in das Backup kopiert wurde).

Sie spezifizieren außerdem den Zielort, wohin die Daten wiederhergestellt werden sollen. Sie können die Wiederherstellungsaktion durch Verwendung entsprechender Recovery-Optionen anpassen, z.B. durch Vor-/Nach-Befehle, die Definition von Fehlerreaktionen oder Benachrichtigungsoptionen.

Das nachfolgende Diagramm illustriert die Datenwiederherstellung unter einem Betriebssystem (online). Während die Wiederherstellung auf der Maschine abläuft, kann keine Backup-Aktion stattfinden. Falls benötigt, können Sie die Konsole mit einer anderen Maschine verbinden und auf dieser dann eine Wiederherstellungsaktion konfigurieren. Diese Fähigkeit zur parallelen Remote-

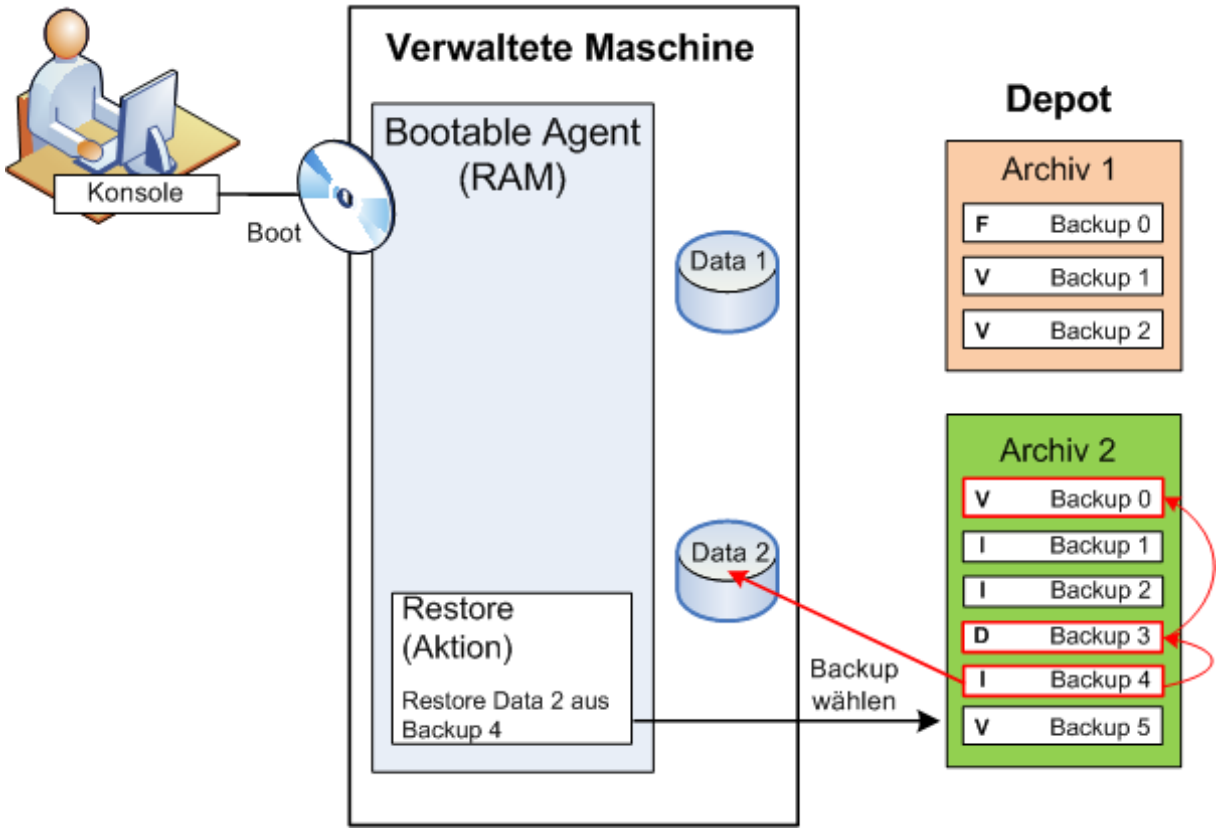
Wiederherstellung wurde erstmals mit Acronis Backup & Recovery 10 eingeführt; vorherige Acronis-Produkte verfügen nicht darüber.



Recovery unter Verwendung bootfähiger Medien

Die Wiederherstellung eines von einem Betriebssystem blockierten Laufwerkes (wie etwa das Laufwerk des Betriebssystems selbst) benötigt einen Neustart in eine bootfähige Umgebung, die Teil des Agenten ist. Nach dem Abschluss der Wiederherstellung geht das wiederhergestellte Betriebssystem automatisch online.

Sollte das Booten auf der Maschine scheitern oder sollten Sie Daten auf eine fabrikneue Maschine wiederherstellen müssen, so booten Sie die Maschine mit einem bootfähigen Medium und konfigurieren dort die Wiederherstellungsaktion auf die gleiche Art wie den Recovery-Task. Das folgende Diagramm illustriert die Wiederherstellung unter Verwendung eines bootfähigen Mediums.



2.2 Vollständige, inkrementelle und differentielle Backups

Acronis Backup & Recovery 10 ermöglicht Ihnen, gängige Backup-Schemata (z.B. Großvater-Vater-Sohn oder „Türme von Hanoi“) wie auch selbst erstellte Schemata zu verwenden. Alle Backup-Schemata basieren auf vollständigen, inkrementellen und differentiellen Backup-Methoden. Genau genommen kennzeichnet der Begriff „Schemata“ den Algorithmus zur Anwendung dieser Methoden plus dem Algorithmus zur Backup-Bereinigung.

Backup-Methoden miteinander zu vergleichen macht nicht viel Sinn, da die Methoden als Team in einem Backup-Schema arbeiten. Jede Methode sollte abhängig von ihren Vorteilen ihre spezifische Rolle spielen. Ein sachgerechtes Backup-Schema profitiert von den Vorteilen und vermindert die Unzulänglichkeiten aller Backup-Methoden. So erleichtert z.B. ein wöchentliches differentielles Backup eine Archiv-Bereinigung, da es zusammen mit einem wöchentlichen Set täglicher, von ihm abhängender inkrementeller Backups mühelos gelöscht werden kann.

Mit vollständigen, inkrementellen oder differentiellen Backup-Methoden durchgeführte Sicherungen resultieren in Backups (S. 185) des jeweils entsprechenden Typs.

Voll-Backup

Ein vollständiges Backup speichert alle für ein Backup ausgewählten Daten. Ein Voll-Backup liegt jedem Archiv zugrunde und bildet die Basis für inkrementelle und differentielle Backups. Ein Archiv

kann mehrere Voll-Backups enthalten oder nur aus Voll-Backups bestehen. Ein Voll-Backup ist autark – Sie benötigen also keinen Zugriff auf irgendein anderes Backup, um Daten aus diesem Voll-Backup wiederherzustellen.

Es ist weitgehend akzeptiert, dass ein Voll-Backup bei der Erstellung am langsamsten, aber bei der Wiederherstellung am schnellsten ist. Eine Wiederherstellung aus einem inkrementellen Backup ist dank Acronis-Technologien jedoch nicht langsamer als aus einem vollständigen Backup.

Ein Voll-Backup ist am nützlichsten, wenn:

- Sie ein System auf seinen Ausgangszustand zurückbringen wollen
- dieser Ausgangszustand sich nicht häufig ändert, so dass es keine Notwendigkeit für reguläre Backups gibt.

Beispiel: Ein Internet-Cafe, eine Schule oder ein Universitätslabor, wo der Administrator durch Studenten oder Gäste bewirkte Änderungen rückgängig macht, aber nur selten das Referenz-Backup aktualisiert (tatsächlich nur nach Installation neuer Software). In diesem Fall ist der Backup-Zeitpunkt nicht entscheidend, während die zur Wiederherstellung aus dem Voll-Backup benötigte Zeit minimal ist. Zur Erreichung einer zusätzlichen Ausfallsicherheit kann der Administrator mehrere Kopien des Voll-Backups haben.

Inkrementelles Backup

Ein inkrementelles Backup speichert die Veränderungen der Daten in Bezug auf das **letzte Backup**. Sie benötigen Zugriff auf die anderen Backups des gleichen Archivs, um Daten aus einem inkrementellen Backup wiederherzustellen.

Ein inkrementelles Backup ist am nützlichsten, wenn:

- es möglich sein muss, die Daten zu jedem der multiplen, gespeicherten Zustände zurückzusetzen.
- die Veränderung der Daten im Vergleich zur Gesamtdatenmenge klein ist.

Es ist weitgehend akzeptiert, dass inkrementelle Backups weniger zuverlässig als Voll-Backups sind, da bei Beschädigung eines Backups innerhalb der „Kette“ auch die nachfolgenden nicht mehr verwendet werden können. Dennoch ist das Speichern mehrerer Voll-Backups keine Option, wenn Sie multiple frühere Versionen Ihrer Daten benötigen, da die Verlässlichkeit eines übergroßen Archivs noch fragwürdiger ist.

Beispiel: Das Backup eines Datenbank-Transaktions-Logs.

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum **letzten Voll-Backup**. Sie benötigen den Zugriff auf das entsprechende Voll-Backup, um die Daten aus einem differentiellen Backup wiederherzustellen. Ein differentielles Backup ist am nützlichsten, wenn:

- Sie daran interessiert sind, nur den neusten Datenzustand zu speichern.
- die Veränderung der Daten im Vergleich zur Gesamtdatenmenge klein ist.

Die typische Schlussfolgerung ist: Differentielle Backups sind langsamer bei Erstellung, aber schneller bei Wiederherstellung, während inkrementelle schneller zu erstellen, aber langsamer wiederherzustellen sind. Tatsächlich gibt es keinen physikalischen Unterschied zwischen einem an ein Voll-Backup angefügten, inkrementellen Backup und einem differentiellen Backup, welches demselben Voll-Backup zum gleichen Zeitpunkt angehängt wird. Der weiter oben erwähnte Unterschied setzt die Erstellung eines differentiellen Backups nach (oder statt) Erstellung multipler differentieller Backups voraus.

Ein nach Defragmentierung einer Festplatte erstelltes inkrementelles oder differentielles Backup kann beträchtlich größer als üblich sein, weil die Defragmentierung die Speicherposition von Dateien auf der Platte verändert und die Backups genau diese Veränderungen reflektieren. Es wird daher empfohlen, dass Sie nach einer Festplatten-Defragmentierung erneut ein Voll-Backup erstellen.

Die nachfolgende Tabelle fasst die allgemein bekannten Vorteile und Schwächen jedes Backup-Typs zusammen. Unter realen Bedingungen hängen diese Parameter von zahlreichen Faktoren ab, wie Menge, Größe und Muster der Datenveränderungen, Art der Daten, den physikalischen Spezifikationen der Geräte, den von Ihnen eingestellten Backup- bzw. Recovery-Optionen und einigen mehr. Praxis ist der beste Leitfaden für die Wahl des optimalen Backup-Schemas.

Parameter	Voll-Backup	Differentielles Backup	Inkrementelles Backup
Speicherplatz	Maximal	Medium	Minimal
Erstellungszeit	Maximal	Medium	Minimal
Wiederherstellungszeit	Minimal	Medium	Maximal

2.3 Benutzerrechte auf einer verwalteten Maschine

Bei Verwaltung einer unter Linux laufenden Maschine hat oder erhält der Benutzer Root-Privilegien und kann daher:

- beliebige Daten oder die komplette Maschine sichern und wiederherstellen, mit voller Kontrolle über alle Aktionen des Acronis Backup & Recovery 10-Agenten und der Log-Dateien auf der Maschine.
- lokale Backup-Pläne und Tasks verwalten, die jedem beliebigen, im Betriebssystem registrierten Anwender gehören.

Zur Vermeidung eines routinemäßigen Einloggens in das System als Root kann sich der Root-Benutzer mit seinen gewöhnlichen Benutzer-Anmeldedaten einloggen und dann den Benutzer bei Bedarf wechseln.

2.4 Besitzer und Anmeldedaten

Dieser Abschnitt erläutert das Konzept von Besitzern und die Bedeutung von Anmeldedaten für Backup-Pläne oder Backup-Tasks.

Plan- oder Task-Besitzer

Ein lokaler Backup-Plan-Besitzer ist derjenige Benutzer, der den Plan erstellt oder als letzter verändert hat.

Ein zentraler Backup-Plan-Besitzer ist derjenige Management Server-Administrator, der die zentrale Richtlinie erstellt oder als letzter modifiziert hat, die den Plan hervorgebracht hat.

Tasks, die Bestandteil eines Backup-Plans sind (entweder lokal oder zentral), gehören einem Backup-Plan-Besitzer.

Tasks, die kein Bestandteil eines Backup-Plans sind (wie z.B. Recovery-Tasks), gehören dem Benutzer, der den Task erstellt oder als letzter modifiziert hat.

Einen Plan (Task) verwalten, der einem anderen Benutzer gehört

Ein Benutzer, der auf einer Maschine Administrator-Rechte hat, kann die Tasks und lokalen Backup-Pläne eines jeden Benutzers, der im Betriebssystem registriert ist, verändern.

Wenn ein Benutzer einen Plan oder Task, der einem anderen Benutzer gehört, zur Bearbeitung öffnet, werden alle in diesem Task gesetzten Passwörter gelöscht. Das verhindert ein Vorgehen „verändere die Einstellungen, behalte Passwörter“. Das Programm reagiert jedes Mal mit einer Warnung, wenn Sie versuchen, einen Plan (Task) zu editieren, den zuletzt ein anderer Benutzer modifiziert hat. Wenn Sie die Warnung sehen, haben Sie zwei Möglichkeiten:

- Klicken Sie auf **Abbrechen** und erstellen Sie einen eigenen Plan oder Task. Der ursprüngliche Task bleibt dabei intakt.
- Fahren Sie mit der Editierung fort. In dem Fall müssen Sie alle zur Ausführung des Plans oder Tasks benötigten Anmeldedaten eingeben.

Archiv-Besitzer

Ein Archiv-Besitzer ist der Benutzer, der das Archiv am Zielort gespeichert hat. Präziser gesagt ist es derjenige Anwender, dessen Konto bei Erstellung des Backup-Plans im Schritt **Backup-Ziel festlegen** angegeben wurde. Standardmäßig werden die Anmeldedaten des Backup-Plans verwendet.

Anmeldedaten für Backup-Pläne und Tasks

Jeder Task, der auf einer Maschine läuft, läuft im Namen eines bestimmten Benutzers. Beim Erstellen eines Plans oder Tasks haben Sie die Möglichkeit, explizit ein Konto anzugeben, unter dem der Plan oder Task laufen wird. Ihre Wahl hängt davon ab, ob die Ausführung des Plans bzw. Tasks manuell oder zeit- bzw. ereignisgesteuert erfolgen soll.

Manueller Start

Sie können den Schritt zu den **Plan (Task)-Anmeldedaten** überspringen. Jedes Mal, wenn Sie einen Task starten, wird er mit den Anmeldedaten ausgeführt, mit denen Sie zu der Zeit am System angemeldet sind. Außerdem kann der Task auch von jeder Person, die auf der Maschine über administrative Rechte verfügt, gestartet werden. Der Task wird dann unter den Anmeldedaten dieser Person ausgeführt.

Für den Fall, dass Sie die Anmeldedaten für einen Task explizit spezifizieren, wird er auch immer mit genau diesen ausgeführt, unabhängig davon, welcher Anwender den Task dann tatsächlich startet. So gehen Sie auf der Seite zur Plan (Task)-Erstellung vor:

1. Aktivieren Sie das Kontrollkästchen **Erweiterte Ansicht**.
2. Wählen Sie **Allgemein –> Plan (Task)-Anmeldedaten –> Ändern**.
3. Geben Sie die Anmeldedaten ein, unter denen der Plan (Task) laufen soll.

Zeit-/ereignisgesteuerter oder verschobener Start

Plan (Task)-Anmeldedaten sind zwingend. Falls Sie diese Anmeldedaten überspringen, werden Sie zur Eingabe derselben noch nach Abschluss der Plan (Task)-Erstellung aufgefordert.

Warum verlangt das Programm von mir, Anmeldedaten zu spezifizieren?

Ein zeit-/ereignisgesteuerter oder verschobener Task muss auf jeden Fall ausgeführt werden, unabhängig davon, ob ein Benutzer überhaupt eingeloggt ist (z.B. weil das System sich in der Begrüßungsanzeige befindet) oder ein anderer Benutzer als der Task-Besitzer angemeldet ist. Es ist ausreichend, dass die Maschine zum für den Task-Start geplanten Zeitpunkt angeschaltet ist (aber

nicht in Standby oder im Ruhezustand). Das ist der Grund, warum der Acronis-Scheduler die explizit spezifizierten Anmeldedaten benötigt, um den Task starten zu können.

2.5 GVS-Backup-Schema

Dieser Abschnitt behandelt die Umsetzung des Großvater-Vater-Sohn (GVS) Backup-Schemas in Acronis Backup & Recovery 10.

Dieses Backup-Schema erlaubt Ihnen nicht, ein Backup mehr als einmal am Tag auszuführen. Dieses Schema ermöglicht Ihnen tägliche, wöchentliche und monatliche Zyklen innerhalb Ihrer Backup-Zeitplanungen abzugrenzen und Aufbewahrungsfristen für die täglichen, wöchentlichen und monatlichen Backups zu bestimmen. Die täglichen Backups werden als „Söhne“ zugeordnet, wöchentliche als „Väter“ und die am längsten lebenden monatlichen Backups werden „Großväter“ genannt.

GVS als Rotationsschema für Bänder (Tapes)

GVS wurde ursprünglich als Band-Rotationsschema erstellt und wird daher häufig darauf bezogen. Band-Rotationschemata als solche bieten jedoch keinen Automatismus. Sie legen lediglich fest:

- wie viele Bänder Sie zur Ermöglichung einer Wiederherstellung bei einer gewünschten Auflösung benötigen (Zeitintervall zwischen zwei Wiederherstellungspunkten) und die Roll-Back Periode
- welche Bänder Sie mit dem nachfolgenden Backup überschreiben sollen.

Band-Rotationsschemata ermöglichen Ihnen mit einer minimalen Zahl von Bandkassetten auszukommen ohne unter benutzten Bändern begraben zu werden. Etliche Internetquellen beschreiben Variationen des GVS-Band-Rotationsschemas. Es steht Ihnen frei, jede dieser Variationen zu verwenden, wenn Sie Backups auf ein lokal angeschlossenes Bandgerät erstellen.

GVS mit Acronis

Es ist einfach, mit Acronis Backup & Recovery 10 einen Backup-Plan aufzusetzen, der gemäß des GVS-Schemas Daten regelmäßig sichert und die resultierenden Archive bereinigt.

Erstellen Sie den Backup-Plan wie gewohnt. Wählen Sie als Backup-Ziel irgendein Speichergerät, auf dem eine automatische Bereinigung durchgeführt werden kann, z.B. ein Festplatten-basiertes Gerät oder eine Roboter-Bandbibliothek. (Da auf Bändern freigegebener Speicherplatz solange nicht verwendet werden kann, bis ein Band komplett freigegeben wurde, sollten Sie dies bei Verwendung von GVS auf Bandbibliotheken zusätzlich berücksichtigen.)

Nachfolgend eine Erläuterung der Einstellungen, die typisch für das GVS-Backup-Schema sind.

GVS-bezogene Einstellungen eines Backup-Plans

Backup starten:

Sichern:

Dieser Schritt erstellt die komplette Backup-Planung, definiert also all die Tage, an denen Sie ein Backup durchführen müssen.

Angenommen, Sie bestimmen, dass ein Backup um 20:00 Uhr werktags durchgeführt wird. Das ist der komplette Zeitplan, den Sie definiert haben.

„B“ steht für „Backup“

Der gesamte Zeitplan.
Zeitplan: Werktags um 20:00 Uhr

Wöchentlich/monatlich:

Dieser Schritt gestaltet die täglichen, wöchentlichen und monatlichen Zyklen im Zeitplan.

Bestimmen Sie einen Wochentag aus den im vorherigen Schritt gewählten Tagen. Jedes erste, zweite und dritte Backup, das an diesem Wochentag erstellt wurde, wird als wöchentliches Backup betrachtet. Jedes vierte Backup, das an diesem Wochentag erstellt wurde, wird als monatliches Backup betrachtet. An den anderen Tagen erstellte Backups werden als tägliche Backups betrachtet.

Angenommen, Sie wählen Freitag als wöchentliches/monatliches Backup. Hier ist der komplette Zeitplan, gekennzeichnet in Bezug auf die getroffene Auswahl.

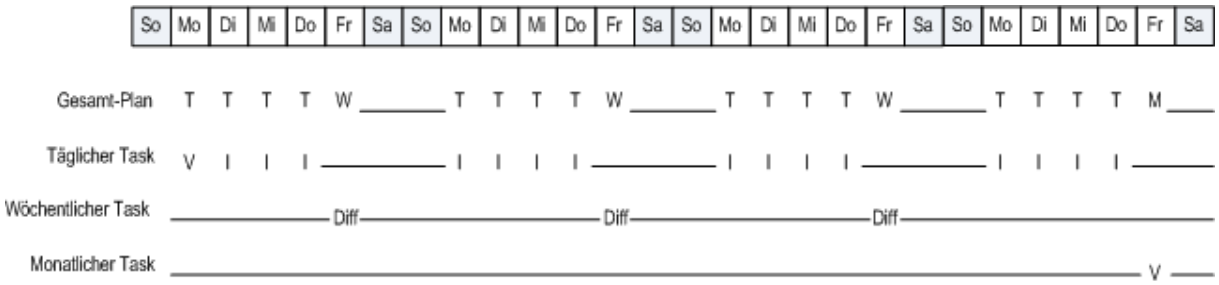
„T“ steht für das als täglich betrachtete Backup. „W“ steht für das als wöchentlich betrachtete Backup. „M“ steht für das als monatlich betrachtete Backup.

Der bezogen auf das GVS-Schema gekennzeichnete Zeitplan.
Zeitplan: Wochentags um 20:00 Uhr
Wöchentlich/monatlich: Freitag

Acronis verwendet inkrementelle und differentielle Backups, die helfen, Speicherplatz zu sparen und eine Bereinigung zu optimieren, so dass keine Konsolidierung notwendig ist. Hinsichtlich der Backup-Methoden ist das wöchentliche Backup differentiell (Diff), das monatliche Backup vollständig (V) und das tägliche Backup inkrementell (I). Das erste Backup ist immer vollständig.

Die Wöchentlich/monatlich-Parameter teilen den kompletten Zeitplan in tägliche, wöchentliche und monatliche Zeitpläne.

Angenommen, Sie wählen Freitag als wöchentliches/monatliches Backup. Hier ist der tatsächliche Zeitplan der Backup-Tasks, die erstellt werden.



Backup-Tasks bezogen auf das GVS-Schema – erstellt durch Acronis Backup & Recovery 10.
Zeitplan: Wochentags um 20:00 Uhr
Wöchentlich/monatlich: Freitag

Backups aufbewahren: Täglich

Dieser Schritt definiert die Aufbewahrungsregel für tägliche Backups. Der Bereinigungs-Task wird nach jedem täglichen Backup ausgeführt und löscht alle täglichen Backups, die älter als von Ihnen spezifiziert sind.

Backups aufbewahren: Wöchentlich

Dieser Schritt definiert die Aufbewahrungsregel für wöchentliche Backups. Der Bereinigungs-Task wird nach jedem wöchentlichen Backup ausgeführt und löscht alle wöchentlichen Backups, die älter als von Ihnen spezifiziert sind. Die Aufbewahrungsdauer für wöchentliche Backups kann nicht kleiner als die für tägliche Backups sein. Üblicherweise wird sie um ein Mehrfaches länger festgelegt.

Backups aufbewahren: Monatlich

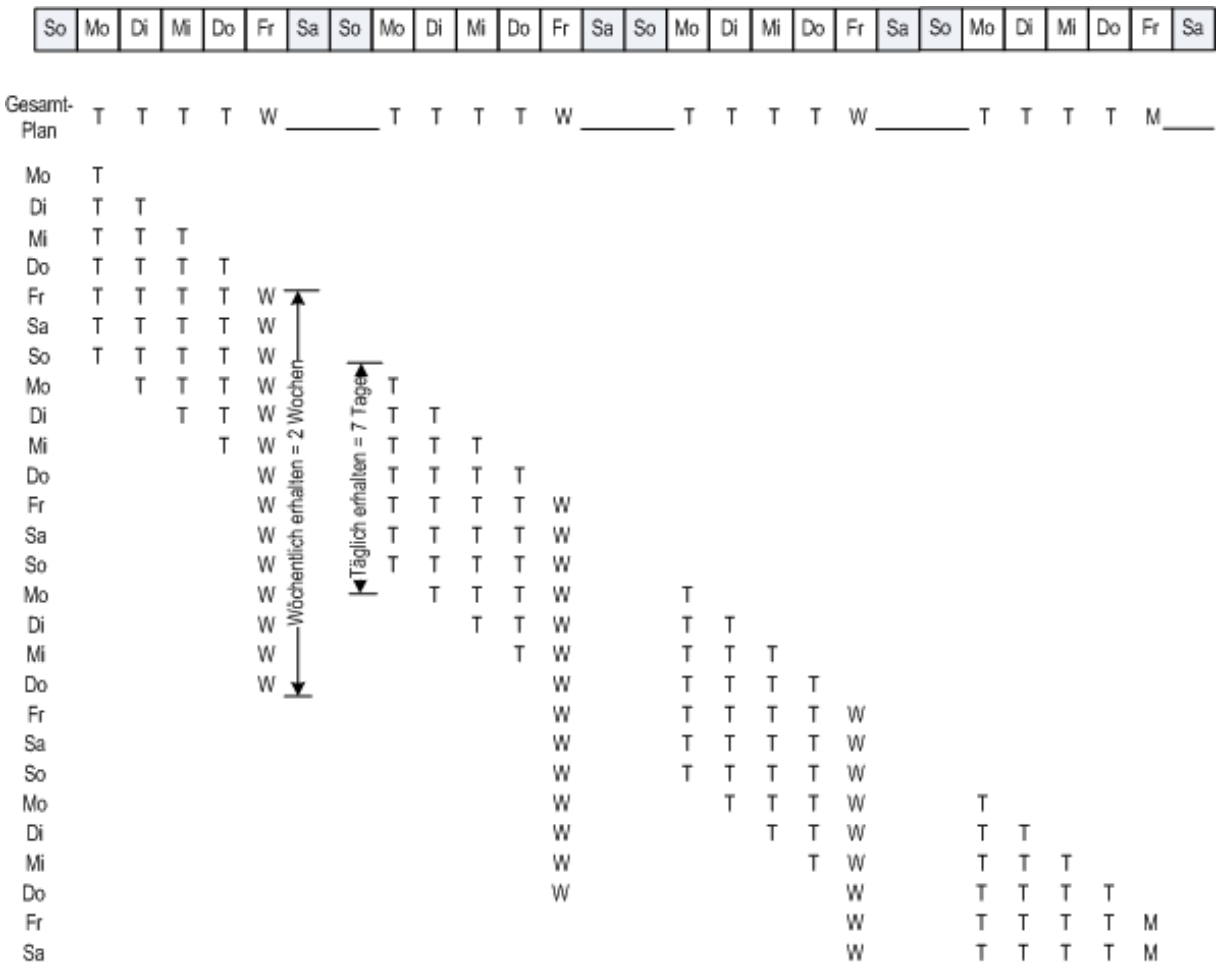
Dieser Schritt definiert die Aufbewahrungsregel für monatliche Backups. Der Bereinigungs-Task wird nach jedem monatlichen Backup ausgeführt und löscht alle monatlichen Backups. die älter als von Ihnen spezifiziert sind. Die monatliche Backup-Aufbewahrungsperiode kann nicht kleiner als die wöchentliche Backup-Aufbewahrungsperiode sein. Üblicherweise wird sie um ein Mehrfaches länger festgelegt. Sie haben die Möglichkeit, die monatlichen Backups unbegrenzt zu behalten.

Das resultierende Archiv: Ideal

Angenommen Sie wählen, tägliche Backups für 7 Tage, wöchentliche für 2 Wochen und monatliche für 6 Monate aufzubewahren. Und so würde Ihr Archiv aussehen, nachdem der Backup-Plan gestartet wurde, falls alle Backups vollständig sind und daher gelöscht werden können, sobald es das Schema verlangt.

Die linke Spalte zeigt die Wochentage. Für jeden Wochentag wird der Archivinhalt nach dem regulären Backup und darauf folgender Bereinigung gezeigt.

„T“ steht für das als täglich betrachtete Backup. „W“ steht für das als wöchentlich betrachtete Backup. „M“ steht für das als monatlich betrachtete Backup.



Ein ideales, bezogen auf das GVS-Schema erstelltes Archiv.
Zeitplan: Wochentags um 20:00 Uhr
Wöchentlich/monatlich: Freitag
Behalte tägliche Backups: 7 Tage
Behalte wöchentliche Backups: 2 Wochen
Behalte monatliche Backups: 6 Monate

Beginnend von der dritten Woche werden wöchentliche Backups regelmäßig gelöscht. Nach 6 Monaten wird begonnen, monatliche Backups zu löschen. Das Diagramm für wöchentliche und monatliche Backups wird bezogen auf die wöchentliche Zeitskala ähnlich aussehen.

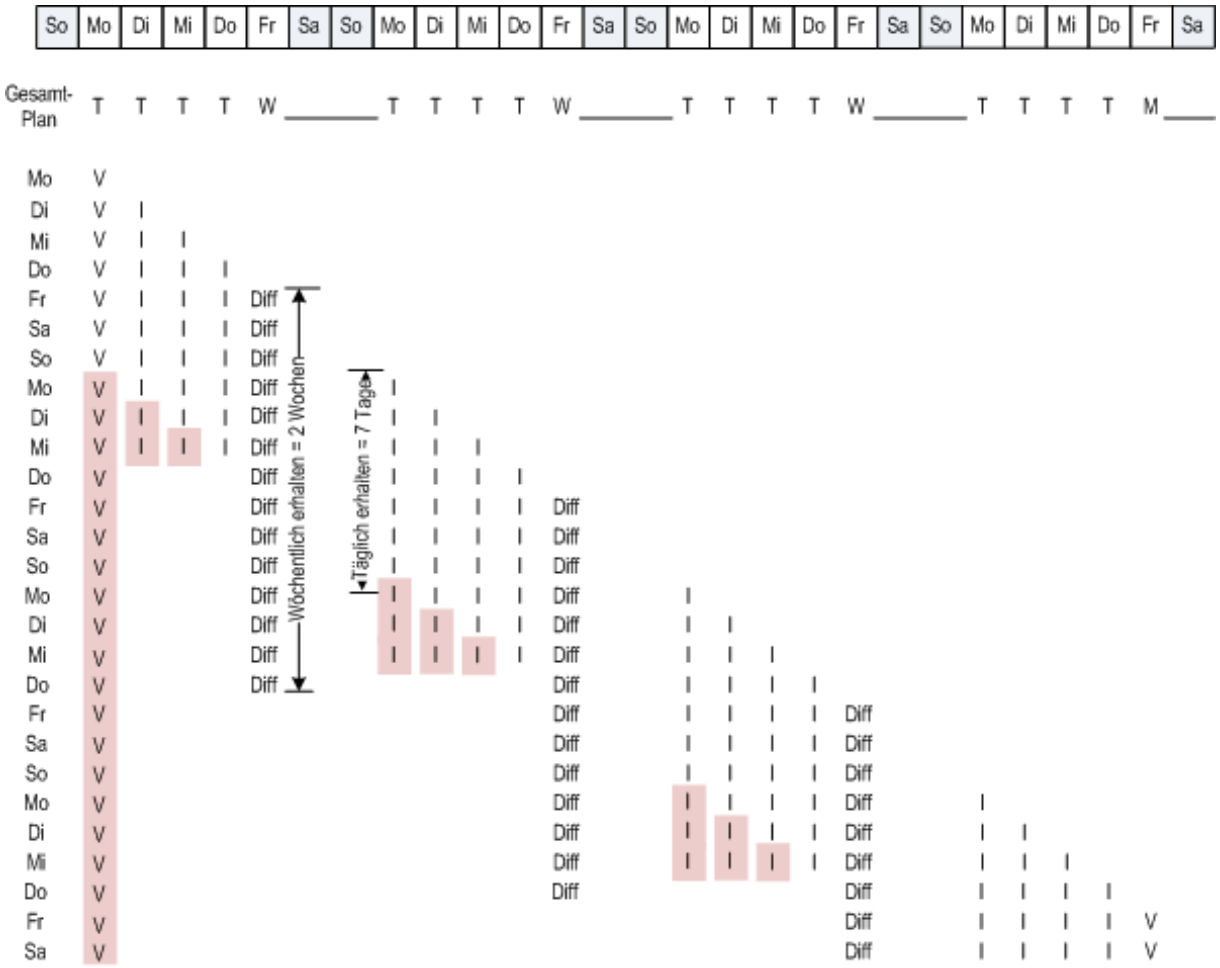
Das resultierende Archiv: Real

Unter realistischen Umständen wird der Archivinhalt etwas vom idealen Schema abweichen.

Bei Verwendung der inkrementellen und differentiellen Backup-Methoden können Sie Backups nicht unmittelbar nach Anforderung des Schemas löschen, wenn nachfolgende Backups noch auf diesem Backup beruhen. Eine reguläre Konsolidierung ist hier unzumutbar, weil sie zu viele System-Ressourcen benötigt. Das Programm muss solange warten, bis das Schema die Löschung aller abhängigen Backups erfordert und dann die vollständige Kette löscht.

Und so wird der erste Monat Ihres Backup-Plans unter realen Bedingungen aussehen. „V“ steht für Voll-Backup. „Diff“ steht für differentielles Backup. „I“ steht für inkrementelles Backup.

Backups, die aufgrund von Abhängigkeiten ihre nominelle Lebenszeit überleben, sind pink gekennzeichnet. Das ursprüngliche Voll-Backup wird gelöscht, sobald alle auf ihm beruhenden differentiellen und inkrementellen Backups gelöscht wurden.



Ein Archiv, bezogen auf das GVS-Schema – erstellt durch Acronis Backup & Recovery 10.
Zeitplan: Wochentags um 20:00 Uhr
Wöchentlich/monatlich: Freitag
Behalte tägliche Backups: 7 Tage
Behalte wöchentliche Backups: 2 Wochen
Behalte monatliche Backups: 6 Monate

2.6 Das Backup-Schema „Türme von Hanoi“

Die Anforderung nach häufigen Backups steht immer im Konflikt mit den Kosten, diese Backups für längere Zeit aufzubewahren. Das Backup-Schema „Türme von Hanoi“ (TvH) ist dafür ein brauchbarer Kompromiss.

Türme von Hanoi im Überblick

Das Türme von Hanoi-Schema basiert auf einem mathematischen Knobel- und Geduldsspiel mit selbem Namen. In dem Spiel wird eine Serie von Ringen der Größe nach auf einem von drei Pflöcken übereinander gestapelt, wobei der größte Ring unten liegt. Ziel des Spiels ist es, den Stapel der Ringe auf den dritten Pflock zu verschieben. Dabei dürfen Sie nur je einen Ring auf einmal bewegen und es ist verboten, einen größeren über einen kleineren Ring zu legen. Die Lösung besteht darin, den ersten Ring bei jedem zweiten Zug zu verlagern (Bewegung 1, 3, 5, 7, 9, 11...), den zweiten Ring mit

Abständen von je vier Zügen (Bewegung 2, 6, 10...), den dritten Ring mit Abständen von je acht Zügen (Bewegung 4, 12...) und so weiter.

Ein Beispiel: wenn fünf mit A, B, C, D und E gekennzeichnete Ringe im Spiel sind, so besteht die Lösung in dieser Bewegungsabfolge:

Ring \ Zug	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	A		A		A		A		A		A		A		A		A		A		A		A		A		A		A		A
2		B				B				B				B				B				B				B				B	
3				C								C								C								C			
4								D																D							
5																E															

Das TvH-Backup-Schema basiert auf denselben Mustern. Es arbeitet mit **Sitzungen** anstatt **Spielzügen** und mit **Backup-Ebenen** anstatt **Ringen**. Das Muster eines Backup-Schemas mit „N“ Ebenen enthält gemeinhin (2 hoch „N“) Sitzungen (N = Zahl der Ebenen bzw. Ringe).

Daher durchläuft ein TvH-Backup-Schema mit 5 Ebenen ein Muster, das aus 16 Sitzungen besteht (Spielzüge von 1 bis 16 in der oberen Abbildung).

Die Tabelle zeigt das Muster für das Backup-Schema mit fünf Ebenen. Das Muster besteht aus 16 Sitzungen.

Backup-Level \ Sitzung	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	A		A		A		A		A		A		A		A	
2		B				B				B				B		
3				C								C				
4								D								
5																E

Das TvH-Backup-Schema setzt voraus, dass nur ein Backup pro Ebene erhalten bleibt. Alle veralteten Backups müssen gelöscht werden. Daher ermöglicht das Schema eine effiziente Datenspeicherung, wobei sich mehr Backups zur gegenwärtigen Zeit hin ansammeln. Mit vier Backups können Sie die Daten von heute, gestern, vor einer halben oder einer ganzen Woche wiederherstellen. Mit einem Fünf-Ebenen-Schema können Sie außerdem Daten wiederherstellen, die vor zwei Wochen gesichert wurden. Jede zusätzliche Backup-Ebene verdoppelt also die maximale Roll-Back Periode für Ihre Daten.

Türme von Hanoi mit Hilfe von Acronis

Das TvH-Backup-Schema ist normalerweise zu komplex, um das nächste zu benutzende Medium im Kopf zu berechnen. Acronis Backup & Recovery 10 unterstützt Sie jedoch mit einer Automatisierung zur Anwendung des Schemas. Sie können das Backup-Schema während der Erstellung eines Backup-Plans anlegen.

Die Acronis-Umsetzung des Schemas hat folgende Eigenschaften:

- Bis zu 16 Backup-Ebenen

- Inkrementelle Backups auf der ersten Ebene (A) – um Zeit- und Speicherersparnisse für die häufigsten Backup-Aktionen zu gewinnen; wobei die Datenwiederherstellung hier jedoch länger braucht, da allgemein ein Zugriff auf drei Backups notwendig ist
- Voll-Backup auf der letzten Ebene (E im Fünf-Ebenen-Muster) – die seltensten Backups im Schema, benötigen mehr Zeit und belegen mehr Speicherplatz
- Differentielle Backups auf allen Zwischen-Ebenen (B, C und D im Fünf-Ebenen-Muster)
- Die Folge startet mit einem Voll-Backup, weil das allererste Backup kein inkrementelles sein kann
- Das Schema zwingt jede Ebene nur das je jüngste Backup zu behalten, andere Backups dieser Ebene müssen gelöscht werden – die Löschung wird jedoch verschoben, wenn das Backup als Basis für ein anderes inkrementelles oder differentielles dient.
- Ein altes Backup einer Ebene wird solange aufbewahrt, bis ein neues Backup dieser Ebene erfolgreich erstellt wurde.

Die Tabelle zeigt das Muster für das Backup-Schema mit fünf Ebenen. Das Muster besteht aus 16 Sitzungen.

Backup-Level \ Sitzung	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1 (Inkrementell)		A		A		A		A		A		A		A		A
2 (Differentiell)			B				B				B				B	
3 (Differentiell)					C								C			
4 (Differentiell)									D							
5 (Voll)	E															

Durch Verwendung inkrementeller und differentieller Backups kann die Situation entstehen, dass die Löschung eines alten Backups aufgeschoben werden muss, weil es noch als Basis für andere Backups dient. Die untere Tabelle verdeutlich diesen Fall, wenn die Löschung des Voll-Backups (E) – erstellt in Sitzung 1 – bei Sitzung 17 bis zu Sitzung 25 aufgeschoben wird, weil das differentielle Backup (D) – erstellt bei Sitzung 9 – immer noch aktuell ist. In der Tabelle sind alle Zellen mit gelöschten Backups ausgegraut:

Backup-Level \ Sitzung	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1 (Inkrementell)		A		A		A		A		A		A		A		A		A		A		A		A	
2 (Differentiell)			B				B				B				B				B				B		
3 (Differentiell)					C								C								C				
4 (Differentiell)									D																D
5 (Voll)	E																E								

Das differentielle Backup (D) – erstellt bei Sitzung 9 – wird bei Sitzung 25 gelöscht, nachdem die Erstellung eines neuen differentiellen Backups abgeschlossen wurde. Daher beinhaltet ein Backup-Archiv, das mit Acronis gemäß dem TvH-Schema erstellt wurde, manchmal bis zu zwei Backups mehr, als es der klassischen Umsetzung des Schemas entspricht.

Informationen über die Nutzung des Türme von Hanoi-Schemas mit Bandbibliotheken siehe Türme von Hanoi-Bandrotationsschema verwenden.

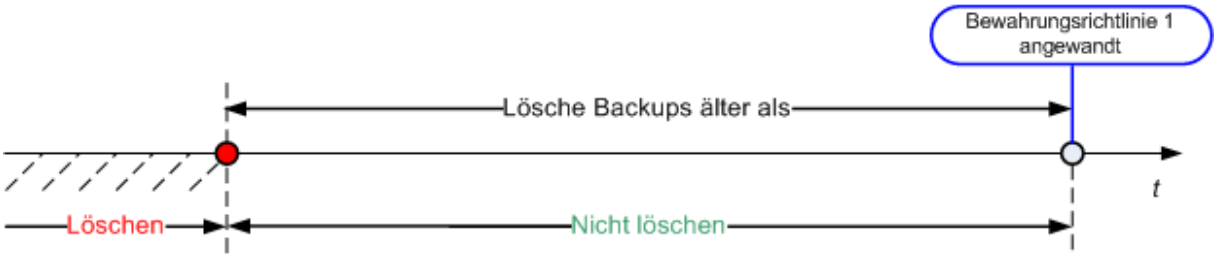
2.7 Aufbewahrungsregeln

Durch einen Backup-Plan erstellte Backups bilden ein Archiv. Die zwei in diesem Abschnitt beschriebenen Aufbewahrungsregeln ermöglichen Ihnen, Archivgröße und Lebenszeit (Aufbewahrungsperiode) von Backups zu definieren.

Die Aufbewahrungsregeln sind wirksam, wenn das Archiv mehr als ein Backup enthält. Das bedeutet, dass das letzte Backup im Archiv erhalten bleibt, selbst wenn dabei die Verletzung einer Aufbewahrungsregel entdeckt wird. Versuchen Sie nicht, das einzige Ihnen verfügbare Backup zu löschen, indem Sie die Aufbewahrungsregeln *vor* dem Backup anwenden. Dies wird nicht funktionieren. Verwenden Sie die alternative Einstellung **Archiv bereinigen –> Wenn nicht ausreichend Speicherplatz während des Backups vorhanden ist** (S. 133); beachten Sie dabei aber das Risiko, möglicherweise das letzte Backup verlieren zu können.

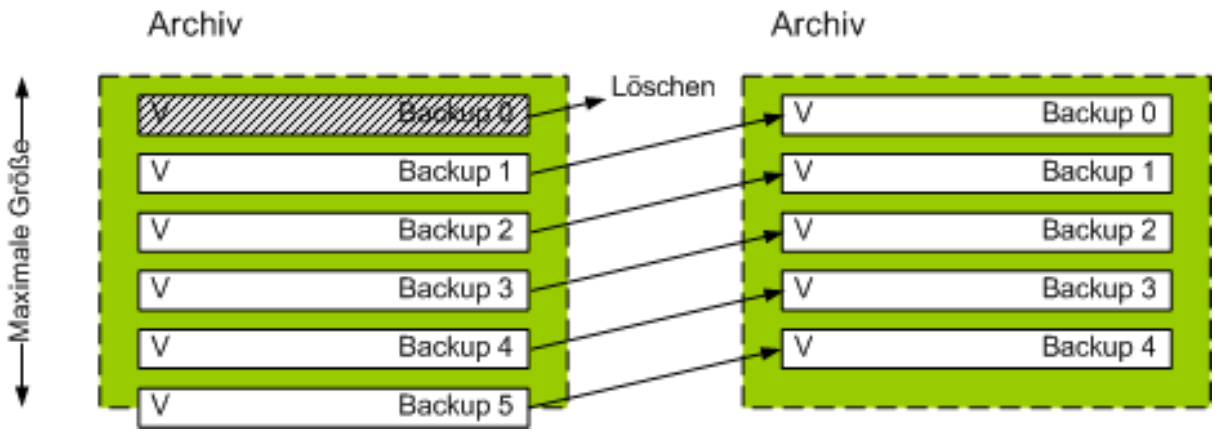
1. Lösche Backups älter als

Dies ist ein Zeitintervall, das von dem Augenblick zurückgezählt wird, an dem die Aufbewahrungsregeln angewendet werden. Jedes Mal, wenn eine Aufbewahrungsregel angewendet wird, ermittelt das Programm den zu diesem Intervall korrespondierenden, zurückliegenden Zeitpunkt und löscht dann alle Backups, die vor diesem erstellt wurden. Von nach diesem Zeitpunkt erstellten Backups wird dagegen keines gelöscht.



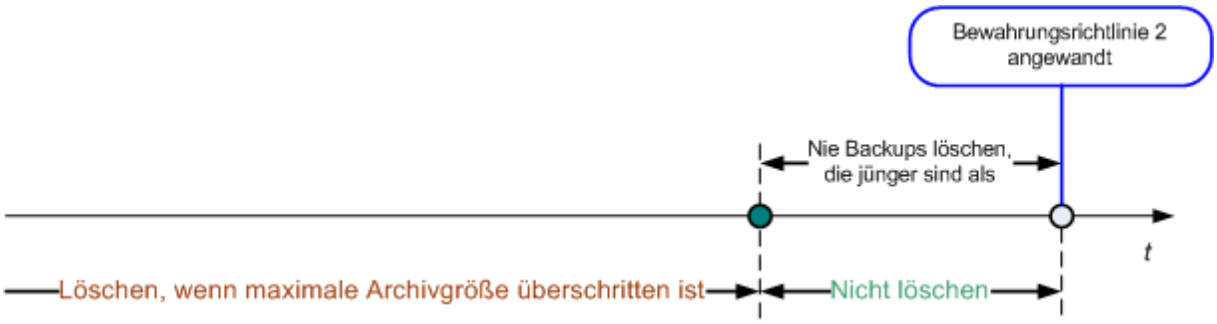
2. Halte die Archivgröße innerhalb

Dies ist die maximale Größe für das Archiv. Jedes Mal, wenn eine Aufbewahrungsregel angewendet wird, vergleicht das Programm die aktuelle Archivgröße mit dem von Ihnen gesetzten Grenzwert und löscht die ältesten Backups, um die Archivgröße innerhalb dieses Wertes zu halten. Das untere Diagramm zeigt den Archivinhalt vor und nach der Löschung.



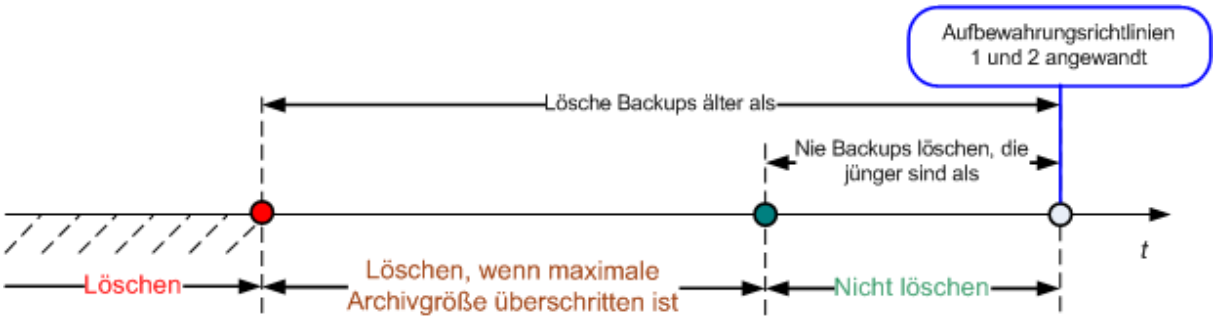
Es gibt ein gewisses Risiko, dass bis auf eines alle Backups gelöscht werden, wenn die maximale Archivgröße unpassend (zu klein) gesetzt wurde oder ein reguläres Backup sich als zu groß erweist. Um die jüngsten Backups vor einer Löschung zu schützen, aktivieren Sie das Kontrollkästchen **Lösche**

keine Backups jünger als und spezifizieren das maximale Alter von Backups, die bewahrt werden müssen. Das untere Diagramm illustriert die sich daraus ergebende Regel.



Kombination der Regeln 1 und 2

Sie können sowohl die Lebenszeit als auch die Archivgröße von Backups limitieren. Das untere Diagramm illustriert die sich daraus ergebende Regel.



Beispiel

Lösche Backups älter als = 3 Monate

Halte die Archivgröße innerhalb = 200 GB

Lösche niemals Backups jünger als = 10 Tage

- Jedes Mal, wenn eine Aufbewahrungsregel angewendet wird, löscht das Programm alle Backups, die vor mehr als 3 Monaten (exakt 90 Tagen) erstellt wurden.
- Sollte nach der Löschung die Archivgröße über 200 GB liegen und das älteste Backup älter als 10 Tage sein, so wird das Programm dieses Backup löschen.
- Dann wird, falls notwendig, das nachfolgend älteste Backup gelöscht, bis die Archivgröße auf den voreingestellten Grenzwert reduziert wurde oder das Alter des ältesten Backups 10 Tage erreicht.

Löschen von Backups mit Abhängigkeiten

Beide Aufbewahrungsregeln setzen das Löschen einiger Backups und die Bewahrung anderer voraus. Aber was, wenn das Archiv inkrementelle und differentielle Backups enthält, die von einander und dem Voll-Backup abhängen, auf dem diese basieren? Sie können kein veraltetes Voll-Backup löschen und sozusagen seine inkrementellen „Kinder“ behalten.

Wenn das Löschen eines Backups andere Backups beeinflusst, wird eine der folgenden Regeln angewendet:

- **Backup bewahren, bis alle abhängigen Backups gelöscht werden.**

  Das veraltete Backup wird solange bewahrt, bis alle auf ihm beruhenden Backups ebenfalls überaltert sind. Dann wird die gesamte Kette während der regulären Bereinigung gleichzeitig gelöscht. Dieser Modus hilft, die potentiell zeitaufwendige Konsolidierung zu vermeiden, benötigt aber extra Speicherplatz für von der Löschung zurückgestellte Backups. Die Archivgröße oder auch das Backup-Alter kann daher die von Ihnen spezifizierten Werte überschreiten.

- **Das Backup konsolidieren**

  Das Programm wird das Backup, das einer Löschung unterworfen ist, mit dem nächsten abhängigen Backup konsolidieren. Zum Beispiel erfordern die Aufbewahrungsregeln, ein Voll-Backup zu löschen, das nachfolgende inkrementelle Backup aber zu bewahren. Die Backups werden zu einem einzelnen Voll-Backup kombiniert, welches das Datum des inkrementellen Backups erhält. Wenn ein inkrementelles oder differentielles Backup aus der Mitte einer Kette gelöscht wird, wird der resultierende Backup-Typ inkrementell.

  Dieser Modus stellt sicher, dass nach jeder Bereinigung die Archivgröße und das Backup-Alter innerhalb der spezifizierten Grenzen liegen. Die Konsolidierung kann jedoch viel Zeit und Systemressourcen in Anspruch nehmen. Und Sie benötigen einigen zusätzlichen Platz im Depot für während der Konsolidierung erstellte temporäre Dateien.

  Das sollten Sie über Konsolidierung wissen

  Machen Sie sich bewusst, dass Konsolidierung nur eine Methode und keine Alternative zur Löschung ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup enthalten, im bewahrten inkrementellen oder differentiellen Backup jedoch abwesend waren.

  Aus einer Konsolidierung resultierende Backups sind immer maximal komprimiert. Das bedeutet, dass alle in einem Archiv enthaltenen Backups als Resultat wiederholter Bereinigung durch Konsolidierung eine maximale Kompression erlangen können.

Optimale Vorgehensweisen

Bewahren Sie die Balance zwischen der Kapazität des Speichergerätes, den restriktiven, von Ihnen bestimmten Parametern und der Bereinigungsfrequenz. Die Logik der Aufbewahrungsregeln setzt voraus, dass die Kapazität des Speichergerätes deutlich über der durchschnittlichen Backup-Größe liegt und sich die maximale Archivgröße nicht der physikalischen Speicherkapazität nähert, sondern eine angemessene Reserve verbleibt. Aufgrund dessen bleibt ein Überschreiten der Archivgröße, was zwischen den Abläufen der Bereinigungs-Tasks vorkommen kann, unkritisch für den Geschäftsprozess. Je seltener die Bereinigung abläuft, desto mehr Platz benötigen Sie zum Speichern von Backups, die ihre Lebenszeit überschreiten.

Die Seite „Depots (S. 77)“ versorgt Sie mit Informationen zu dem in jedem Depot verfügbaren Speicherplatz. Überprüfen Sie diese Seite von Zeit zu Zeit. Wenn sich der freie Platz (der freie Platz des Speichergeräts) Null nähert, so müssen Sie eventuell die Beschränkungen für einige oder alle Archive im Depot verschärfen.

2.8 Backup von LVM-Volumes und MD-Geräten (Linux)

Dieser Abschnitt erläutert, wie Sie durch den Linux 'Logical Volume Manager' (LVM) verwaltete Volumes (logische Volumes genannt) sowie Multiple-Disk- bzw. MD-Geräte (Linux Software RAID genannt) per Backup sichern und wiederherstellen können.

2.8.1 Backup von logischen Volumes

Der Acronis Backup & Recovery 10 Agent für Linux kann auf solche Laufwerke zugreifen, sie sichern und wiederherstellen, wenn er unter Linux mit 2.6-Kernel oder einem Linux-basierten Boot-Medium ausgeführt wird.

Backup (Benutzeroberfläche)

Logische Volumes erscheinen in der Benutzeroberfläche von Acronis Backup & Recovery 10 unter **Dynamische & GPT-Volumes**, am Ende der Liste aller zum Backup verfügbarer Volumes.

Um alle verfügbaren Laufwerke zu sichern, spezifizieren Sie alle logischen Volumes und zusätzlich alle nicht zu diesen gehörenden Basis-Volumes. Das ist die vorgegebene Wahl, wenn Sie die Seite **Backup-Plan erstellen** öffnen.

In logischen Laufwerken enthaltene Basis-Volumes werden innerhalb der Liste mit der Kennzeichnung **Kein** in der Spalte **Dateisystem** angezeigt. Wenn Sie solche Volumes auswählen, sichert das Programm diese mit einem Sektor-für-Sektor-Backup. Normalerweise ist dies nicht notwendig.

Recovery

Bei der Wiederherstellung logischer Volumes haben Sie zwei Optionen:

- **Nur Volume-Inhalt wiederherstellen**. Der Typ oder andere Eigenschaften des Ziel-Volumes werden nicht verändert.

  Diese Option ist sowohl im Betriebssystem wie auch unter einem bootfähigen Medium verfügbar.

  Die Option ist in folgenden Fällen nützlich:

  - Wenn auf dem Volume einige Daten verloren gegangen sind, aber keine Laufwerke ersetzt wurden.
  - Wenn Sie ein logisches Volume über ein Basis-(MBR)-Laufwerk bzw. Volume wiederherstellen. Sie können in diesem Fall die Größe des resultierenden Volumes anpassen.

    Ein System, bei dem das Backup eines logischen Volumes auf einem Basis-MBR-Laufwerk wiederhergestellt wurde, ist nicht bootfähig, da sein Kernel versucht, das Root-Dateisystem beim logischen Volume zu mounten. Um das System zu booten, ändern Sie die Konfiguration des Loaders und von '/etc/fstab' (so dass LVM nicht verwendet wird) und reaktivieren Sie Ihren Boot-Loader (S. 149).

  - Bei Wiederherstellung eines Basis-Volumes oder logischen Volumes zu einem zuvor erstellten logischen Volume. Das ist der Fall, wenn Sie die Struktur logischer Volumes manuell unter Verwendung des Utilities **lvm** erstellen.
- **Die Struktur logischer Volumes und ihre Inhalte wiederherstellen**.

  Das ist der Fall, wenn Sie auf fabrikneue Geräte wiederherstellen oder auf eine Maschine mit anderer Volume-Struktur. Die Struktur logischer Volumes kann während der Recovery-Aktion automatisch erstellt werden, sofern diese im Backup gespeichert wurde (S. 36).

  Diese Option ist nur verfügbar, wenn Sie unter einem Boot-Medium arbeiten.

Zu weiteren Informationen über die Wiederherstellung logischer Volumes siehe Wiederherstellung von MD-Geräten und logischen Volumes (S. 179).

Hilfreicher Link (in Englisch):

- http://tldp.org/HOWTO/LVM-HOWTO/.

2.8.2 Backup von MD-Geräten

MD-Geräte kombinieren mehrere Volumes und erstellen quasi 'Geräte aus einem Guss' (/dev/md0, /dev/md1, ..., /dev/md31). Die Informationen über MD-Geräte sind in 'etc/raidtab' oder in bestimmen Bereichen dieser Volumes gespeichert.

Sie können aktive (gemountete) MD-Geräte auf dieselbe Art wie logische Volumes per Backup sichern. Die MD-Geräte erscheinen am Ende der für Backups verfügbaren Laufwerksliste.

Wenn ein MD-Gerät gemountet ist, macht es keinen Sinn, die im MD-Gerät enthaltenen Volumes per Backup zu sichern, weil es nämlich nicht möglich ist, diese auch wiederherzustellen.

Wenn Sie MD-Geräte von einem bootfähigen Medium ausgehend wiederherstellen, kann die Struktur der MD-Geräte automatisch erstellt werden, sofern sie ebenfalls per Backup gespeichert wurde (S. 36). Zu weiteren Informationen über die Wiederherstellung von MD-Geräten, ausgehend von einem bootfähigen Medium, siehe MD-Geräte und logische Volumes wiederherstellen (S. 179).

Zu weiteren Informationen über die Erstellung von MD-Geräten bei Recovery-Aktionen unter Linux siehe MD-Geräte für eine Wiederherstellung zusammenstellen (Linux) (S. 147).

2.8.3 Die Volume-Strukturinformation sichern

Damit bei einer Recovery-Aktion die Struktur von MD-Geräten und logischen Volumes automatisch erstellt werden kann, müssen Sie die Volume-Strukturinformation auf eine der folgenden Arten sichern:

- Gehen Sie bei Erstellung eines Backup-Plans für ein Laufwerk-Backup zu **Backup-Optionen –> Erweiterte Einstellungen** und aktivieren Sie dort das Kontrollkästchen **Software-RAID- und LVM-Metadaten gemeinsam mit Backups speichern**. (Ist standardmäßig aktiviert.)
- Starten Sie folgenden Befehl, bevor Sie auf einer Quellmaschine das erste Laufwerk-Backup ausführen:

  ```
  trueimagecmd --dumpraidinfo
  ```

Jede Aktion speichert die logische Volume-Struktur der Maschine in das Verzeichnis /etc/Acronis. Stellen Sie sicher, dass das Volume mit diesem Verzeichnis ebenfalls zum Backup ausgewählt ist.

2.8.4 Logische Volumes und MD-Geräte per Befehlszeile auswählen

Angenommen, ein System verfügt über vier physikalische Laufwerke (Disks): Disk 1, Disk 2, Disk 3 und Disk 4.

- Ein RAID-1-Volume ist auf zwei Basis-Volumes konfiguriert: sdb1, sdd1
- Ein logisches Volume ist auf zwei Basis-Volumes konfiguriert: sdb2, sdd2
- Disk 1 enthält die Acronis Secure Zone, die normalerweise nicht in ein Backup aufgenommen wird.

Eine Liste der Volumes kann mit folgendem Befehl eingeholt werden:

```
trueimagecmd --list
```

```
Num  Partition             Flags       Start      Size       Type
---- -------------------- ----------- ---------- ---------- -----------
Disk 1 (sda):
1-1  sda1                 Pri,Act     63         208813     Ext2
1-2  sda2                 Pri         417690     12289725   ReiserFS
1-3  sda3                 Pri         24997140   1052257    Linux Swap
     Unallocated                      27101655   2698920    Unallocated
1-4  Acronis Secure Zone  Pri         32499495   522112     FAT32
     Unallocated                      33543720   5356       Unallocated
Disk 2 (sdb):
2-1  sdb1                 Pri         62         124969     Ext2
2-2  sdb2                 Pri         250001     125000     None
     Unallocated                      500001     8138607    Unallocated
Disk 3 (sdc):
     Table                            0                     Table
     Unallocated                      1          1048575    Unallocated
Disk 4 (sdd):
4-1  sdd1                 Pri         62         124969     Ext2
4-2  sdd2                 Pri         250001     125000     None
     Unallocated                      500001     798575     Unallocated
Dynamic & GPT Volumes:
DYN1  VolGroup00-LogVol00                        245760     Ext3
                          Disk: 3     250385     245760
                          Disk: 5     250385     245760
DYN2  md0                                        124864     Ext2
                          Disk: 5     62         249728
                          Disk: 3     62         249728
```

Das logische Volume, DYN1, belegt die Basis-Volumes 2-2 und 4-2. Das RAID-1-Volume, DYN2, belegt die Basis-Volumes 2-1 und 4-1.

Führen Sie folgenden Befehl aus, um das logische Volume DYN1 zu sichern (als Backup-Name wird '/home/backup.tib' angenommen):

```
trueimagecmd --partition:dyn1 --filename:/home/backup.tib --create
```

Führen Sie folgenden Befehl aus, um das RAID-1-Volume DYN2 zu sichern:

```
trueimagecmd --partition:dyn2 --filename:/home/backup.tib --create
```

Wählen Sie die Volumes 1-1, 1-2, DYN1 und DYN2, um alle drei Laufwerke mit Ihren Volumes zu sichern:

```
trueimagecmd --partition:1-1,1-2,1-3,dyn1,dyn2 --filename:/home/backup.tib --
create
```

Wenn Sie Laufwerk 3 (Volume 2-1 oder Volume 2-2) wählen, so erstellt das Programm ein RAW-Backup (Sektor-für-Sektor-Sicherung).

2.9 Backup von Hardware-RAID-Arrays (Linux)

Hardware-RAID-Arrays unter Linux kombinieren mehrere physikalische Laufwerke, um ein als Einheit partitionierbares Laufwerk zu erstellen. Die spezielle, auf ein Hardware-RAID-Array bezogene Datei befindet sich üblicherweise unter /dev/ataraid. Sie können Hardware-RAID-Arrays auf dieselbe Art wie gewöhnliche Festplatten per Backup sichern.

Physikalische Laufwerke, die Teil eines Hardware-RAID-Arrays sind, können neben anderen Laufwerken so aufgelistet sein, als ob sie eine beschädigte oder überhaupt keine Partitionstabelle

haben würden. Solche Laufwerke per Backup zu sichern macht keinen Sinn, wie es auch nicht möglich ist, sie wiederherzustellen.

2.10 Band-Unterstützung

Acronis Backup & Recovery 10 unterstützt Bandbibliotheken, Autoloader sowie SCSI- und USB-Bandlaufwerke als Speichergeräte. Ein Bandgerät kann lokal an eine verwaltete Maschine angeschlossen sein (in diesem Fall schreibt und liest der Acronis Backup & Recovery 10 Agent die Bänder) oder der Zugriff erfolgt über den Acronis Backup & Recovery 10 Storage Node. Storage Node gewährleisten einen vollautomatischen Betrieb von Bandbibliotheken und Autoloadern.

Backup-Archive, die durch unterschiedliche Zugriffsarten auf die Bänder erstellt wurden, haben unterschiedliche Formate: Ein per Storage Node beschriebenes Band kann nicht von einem Agenten gelesen werden.

Linux- und PE-basierte Boot-Medien erlauben für Backup und Wiederherstellung gleichermaßen einen lokalen wie auch per Storage Node erfolgenden Zugriff. Durch Verwendung von Boot-Medien erstellte Backups können mit dem im Betriebssystem laufenden Acronis Backup & Recovery 10 Agenten wiederhergestellt werden.

2.10.1 Kompatibilitätstabelle für Bänder

Die nachfolgende Tabelle fasst die Lesbarkeit von Bändern in Acronis Backup & Recovery 10 zusammen, die durch Acronis True Image Echo und die Acronis True Image 9.1 Produktfamilie beschrieben wurden. Die Tabelle illustriert außerdem die Kompatibilität von Bändern, die durch verschiedene Komponenten von Acronis Backup & Recovery 10 beschrieben wurden.

			... ist lesbar auf einem Bandgerät, angeschlossen an eine Maschine mit...			
			ABR10 Bootfähige Medien	ABR10 Agent für Windows	ABR10 Agent für Linux	ABR10 Storage Node
Band, beschrieben auf einem lokal angeschlossenen Bandgerät (Bandlaufwerk oder -bibliothek) durch...	Bootfähige Medien	ATIE 9.1	+	+	+	+
		ATIE 9.5	+	+	+	+
		ATIE 9.7	+	+	+	+
		ABR10	+	+	+	+
	Agent für Windows	ATIE 9.1	+	+	+	+
		ATIE 9.5	-	-	-	+
		ATIE 9.7	-	-	-	+
		ABR10	+	+	+	+
	Agent für Linux	ATIE 9.1	+	+	+	+
		ATIE 9.5	+	+	+	+
		ATIE 9.7	+	+	+	+
		ABR10	+	+	+	+

Band, beschrieben auf einem Bandgerät durch...	Backup Server	ATIE 9.1	+	+	+	+
		ATIE 9.5	-	-	-	+
		ATIE 9.7	-	-	-	+
	Storage Node	ABR10	-	-	-	+

2.10.2 Verwendung eines einzelnen Bandlaufwerkes

Ein lokal an eine verwaltete Maschine angeschlossenes Bandlaufwerk kann durch lokale Backup-Pläne als Speichergerät verwendet werden. Die Funktionalität eines lokal angebundenen Autoloaders oder einer Bandbibliothek ist auf die eines gewöhnlichen Bandlaufwerkes limitiert. Das bedeutet, dass das Programm nur mit dem gerade angeschlossenen Band arbeiten kann und Sie Bänder manuell anschließen müssen.

Backup auf ein lokal angeschlossenes Bandgerät

Sie können ein lokal angebundenes Bandgerät bei Erstellung eines Backup-Plans als Backup-Ziel auswählen. Ein Archivname muss beim Backup auf Band jedoch nicht angegeben werden.

Ein Archiv kann sich über mehrere Bänder aufspannen, enthält dabei aber nur je ein Voll-Backup, während die Zahl von inkrementellen Backups unbegrenzt sein kann. Jedes Mal, wenn Sie ein neues Voll-Backup erstellen, starten Sie mit einem neuen Band und erstellen ein neues Archiv. Sobald das Band voll ist, erscheint ein Dialogfenster mit einer Aufforderung, ein neues Band einzulegen.

Der Inhalt eines nicht-leeren Bands wird auf Aufforderung hin überschrieben. Sie haben aber die Option, diese Eingabeaufforderungen zu deaktivieren, siehe Zusätzliche Einstellungen (S. 66).

Problemumgehung

Für den Fall, dass Sie mehr als ein Archiv auf einem Band behalten wollen (z.B. ein getrenntes Backup von Laufwerk C und D), wählen Sie bei Erstellung des ersten, einleitenden Backups für das zweite Laufwerk den Backup-Modus „voll“ statt „inkrementell“. Inkrementelle Backups werden sonst, in anderen Situationen verwendet, um Veränderungen an ein zuvor erstelltes Archiv anzuhängen.

Es kann sein, dass Sie kurze Pausen erleben, die benötigt werden, um das Band zurückzuspulen. Außerdem können alte Bänder und solche von niedriger Qualität, genauso wie ein verschmutzter Magnetkopf, Pausen von bis zu einigen Minuten bewirken.

Einschränkungen

1. Multiple Voll-Backups innerhalb eines Archives werden nicht unterstützt.
2. Aus einem Festplatten-Backup können keine individuellen Dateien wiederhergestellt werden.
3. Backups können nicht von einem Band gelöscht werden, weder manuell noch durch automatische Bereinigung. In der Benutzeroberfläche werden Aufbewahrungsregeln und Backup-Schemata, die automatische Bereinigung verwenden (GVS, Türme von Hanoi), beim Backup auf ein lokal angeschlossenes Band deaktiviert.
4. Auf einem Bandgerät können keine persönlichen Depots erstellt werden.
5. Da die Anwesenheit eines Betriebssystems in einem Backup, das auf einem Band gespeichert ist, nicht festgestellt werden kann, wird die Verwendung von Acronis Universal Restore (S. 196) bei jeder Wiederherstellung eine Festplatte oder Partition vorgeschlagen, selbst wenn es sich um ein Linux- oder Nicht-System-Windows-Laufwerk handelt.

6. Acronis Active Restore (S. 184) ist bei Wiederherstellung von einem Band nicht verfügbar.

Wiederherstellung von einem lokal angebundenen Bandgerät

Bevor Sie einen Recovery-Task einrichten, sollten Sie das Band, welches das für die Wiederherstellung benötigte Backup enthält, einlegen bzw. anschließen. Wählen Sie das Bandgeräte von der Liste der verfügbaren Speicherorte, wenn Sie einen Recovery-Task erstellen und bestimmen Sie danach das entsprechende Backup. Nachdem die Wiederherstellung gestartet ist, werden von Ihnen weitere Bänder angefordert, sofern diese für die Wiederherstellung benötigt werden.

2.11 Unterstützung für SNMP

SNMP-Objekte

Acronis Backup & Recovery 10 stellt die folgenden Simple Network Management Protocol (SNMP)-Objekte für SNMP-Verwaltungsanwendungen zur Verfügung:

- Typ des Ereignisses

  Objekt-Identifier (OID): 1.3.6.1.4.1.24769.100.200.1.0

  Syntax: OctetString

  Der Wert kann „Information“, „Warnung“, „Fehler“ und „Unbekannt“ sein. „Unbekannt“ wird nur in der Testnachricht gesendet.
- Textbeschreibung des Ereignisses

  Objekt-Identifier (OID): 1.3.6.1.4.1.24769.100.200.2.0

  Syntax: OctetString

  Der Wert enthält die Textbeschreibung des Ereignisses (identische Darstellung wie in den Meldungen der Ereignisanzeige von Acronis Backup & Recovery 10).

Beispiele für Varbind-Werte:

1.3.6.1.4.1.24769.100.200.1.0:Information

1.3.6.1.4.1.24769.100.200.2.0:I0064000B

Unterstützte Aktionen

Acronis Backup & Recovery 10 **unterstützt nur TRAP-Aktionen**. Es ist nicht möglich, Acronis Backup & Recovery 10 unter Verwendung von GET- und SET-Anforderungen zu verwalten. Das bedeutet, dass Sie einen SNMP-TRAP-Receiver verwenden müssen, um TRAP-Meldungen zu empfangen.

Über die Management Information Base (MIB)

Die MIB-Datei **acronis-abr.mib** befindet sich im Installationsverzeichnis von Acronis Backup & Recovery 10. Standardmäßig: %ProgramFiles%\Acronis\BackupAndRecovery unter Windows und /usr/lib/Acronis/BackupAndRecovery unter Linux.

Diese Datei kann von einem MIB-Browser oder einem einfachen Texteditor (wie Notepad oder vi) gelesen werden.

Über die Testnachricht

Sie können bei der Konfiguration von SNMP-Benachrichtigungen eine Testnachricht versenden, um zu überprüfen, ob Ihre Einstellungen richtig sind.

Die Parameter der Testnachricht lauten folgendermaßen:

- Typ des Ereignisses
  OID: 1.3.6.1.4.1.24769.100.200.1.0
  Wert: „Unbekannt“
- Textbeschreibung des Ereignisses
  OID: 1.3.6.1.4.1.24769.100.200.2.0
  Wert: "?00000000"

2.12 Proprietäre Acronis-Technologien

Dieser Abschnitt beschreibt diejenigen proprietären Technologien, die Acronis Backup & Recovery 10 von Acronis True Image Echo und der Acronis True Image 9.1-Produkt-Familie übernommen hat.

2.12.1 Acronis Secure Zone

Die Acronis Secure Zone ist eine sichere Partition auf dem Festplattenplatz einer verwalteten Maschine, in der Backup-Archive gespeichert werden können, so dass die Wiederherstellung einer Festplatte auf der gleichen Festplatte erfolgen kann, auf der sich auch die Backups selbst befinden.

Verschiedene Windows-Anwendungen, wie z.B. die Acronis Disk Management-Tools, können auf die Zone zugreifen.

Sollte die Festplatte jedoch einen physikalischen Fehler erleben, so gehen die Zone und alle dort aufbewahrten Archive verloren. Das ist der Grund, warum die Acronis Secure Zone nicht der einzige Ort sein sollte, wo Backups gespeichert werden. In Unternehmensumgebungen kann die Acronis Secure Zone als Zwischenspeicher für Backups betrachtet werden, wenn der üblicherweise verwendete Speicherort temporär nicht verfügbar ist oder über einen langsamen bzw. ausgelasteten Kanal angebunden ist.

Vorteile

Acronis Secure Zone:

- Ermöglicht die Wiederherstellung einer Festplatte auf die Festplatte, auf der auch die Backups der Festplatte selbst abgelegt sind.
- Bietet eine kosteneffektive und handliche Methode für den Schutz der Daten vor Softwarefehlern, Virusangriffen, Bedienerfehlern u.a.
- Ist ein interner Archiv-Speicher und beseitigt die Notwendigkeit, in jedem Fall für Backup oder Wiederherstellung ein separates Medium oder eine Netzwerkverbindung bereitstellen zu müssen. Diese Funktion ist besonders nützlich für mobile Benutzer.
- Kann bei Verwendung von Dual Destination (S. 63)-Backup als primäres Ziel dienen.

Einschränkungen

- Die Zone kann nicht auf einem dynamischem Laufwerk oder einem Laufwerk eingerichtet werden, das das GPT-Partitionsschema verwendet.

Die Acronis Secure Zone verwalten

Die Acronis Secure Zone wird als persönliches Depot (S. 189) betrachtet. Einmal auf einer verwalteten Maschine erstellt, ist die Zone stets in der Liste **Persönliche Depots** präsent. Zentrale Backup-Pläne (S. 198) können die Acronis Secure Zone ebenso benutzen wie lokale Pläne (S. 193).

Sollten Sie die Acronis Secure Zone schon früher verwendet haben, so werden Sie einen radikalen Wechsel in ihrer Funktionalität feststellen. Die Zone führt von allein keine automatischen Bereinigungen, also das Löschen alter Archive, mehr aus. Nutzen Sie stattdessen zum Sichern in die Zone Backup-Schemata mit automatischer Bereinigung oder löschen Sie veraltete Backups manuell unter Verwendung von Archiv-Verwaltungsfunktionen.

Durch das neue Verhalten der Acronis Secure Zone erhalten Sie die Fähigkeit:

- in der Zone lokalisierte Archive und in ihnen enthaltene Backups aufzulisten
- den Inhalt eines Backups zu untersuchen
- ein Laufwerk-Backup zu mounten, um Dateien aus dem Backup auf eine physikalische Platte zu kopieren
- Archive und Backups aus Archiven sicher zu löschen.

Weitere Informationen zu den für die Acronis Secure Zone verfügbaren Aktionen finden Sie im Abschnitt 'Persönliche Depots (S. 78)'.

Upgrade von Acronis True Image Echo

Beim Upgrade von Acronis True Image Echo auf Acronis Backup & Recovery 10 werden die mit Echo erstellten Archive in der Acronis Secure Zone bewahrt. Die Zone wird in der Liste der persönlichen Depots angezeigt und die alten Archive sind weiterhin für Wiederherstellungen verfügbar.

2.12.2 Acronis Startup Recovery Manager

Eine Modifikation des bootfähigen Agenten (S. 188) kann auf einem Systemlaufwerk platziert und so konfiguriert werden, dass er beim Bootens durch Drücken der Taste F11 gestartet werden kann. Dies bietet eine Alternative zum Einsatz von Rettungsmedien oder zu einer Netzwerkverbindung für den Start der bootfähigen Rettungsumgebung. Diese Funktion hat den geschützten Markennamen „Acronis Startup Recovery Manager“.

Der Acronis Startup Recovery Manager ist besonders für mobile Anwender nützlich. Wenn ein Fehler auftritt, bootet der Benutzer die Maschine neu, drückt die F11-Taste, sobald die Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers…“ erscheint, und stellt dann die Daten auf die gleiche Weise wie mit den gewöhnlichen bootfähigen Medien wieder her. Anwender können außerdem auch Backups mit dem Acronis Startup Recovery Manager erstellen, wenn sie unterwegs sind.

Auf Maschinen, die einen GRUB Boot-Loader installiert haben, wählt der Benutzer den Acronis Startup Recovery Manager aus dem Boot-Menü, statt F11 zu drücken.

Aktivierung und Deaktivierung des Acronis Startup Recovery Manager

Die Aktion, die die Verwendung des Acronis Startup Recovery Manager ermöglicht, wird „Aktivierung“ genannt. Um den Acronis Startup Recovery Manager zu aktivieren, wählen Sie im Programm-Menü **Aktionen > Acronis Startup Recovery Manager aktivieren**.

Sie können den Acronis Startup Recovery Manager jederzeit über das Menü **Extras** aktivieren oder deaktivieren. Die Deaktivierung schaltet die Boot-Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Manager“ aus (oder entfernt den entsprechenden Eintrag aus dem Boot-Menü von GRUB). Dies bedeutet, dass Sie im Fall eines Boot-Fehlers des Systems ein bootfähiges Medium benötigen.

Einschränkungen

Der Acronis Startup Recovery Manager benötigt nach seiner Aktivierung bei Anwesenheit von Dritthersteller-Boot-Loadern deren Reaktivierung.

Upgrade von Acronis True Image Echo

Nach einem Upgrade von Acronis True Image Echo auf Acronis Backup & Recovery 10 wird der Acronis Startup Recovery Manager unabhängig von seinem Status vor dem Upgrade als deaktiviert angezeigt. Sie können den Acronis Startup Recovery Manager jederzeit wieder aktivieren.

3 Optionen

Dieser Abschnitt beschreibt die Optionen von Acronis Backup & Recovery 10, die mit Hilfe der grafischen Benutzeroberfläche konfiguriert werden können. Der Inhalt dieses Abschnitts gilt für autonome und erweiterte Editionen (Advanced Editions) von Acronis Backup & Recovery 10.

3.1 Konsolen-Optionen

Die Konsolenoptionen legen fest, wie die Informationen in der grafischen Benutzeroberfläche von Acronis Backup & Recovery 10 erscheinen.

Um auf die Konsolenoptionen zuzugreifen, wählen Sie **Optionen -> Konsolenoptionen** im Menü.

3.1.1 Startseite

Diese Option definiert, ob das Fenster **Willkommen** oder das **Dashboard** bei einer Verbindung von der Konsole zu einer verwalteten Maschine oder zum Management Server angezeigt wird.

Voreinstellung ist: das Fenster **Willkommen**.

Um eine Auswahl zu treffen, benutzen Sie das Kontrollkästchen **Bei Verbindung der Konsole zu einer Maschine Dashboard zeigen**.

Diese Option kann auch auf dem Fenster **Willkommen** gesetzt werden. Wenn Sie das Kontrollkästchen für **Beim Start Dashboard anstelle der aktuellen Ansicht zeigen** auf dem Fenster **Willkommen** aktivieren, dann erreichen Sie den gleichen Effekt.

3.1.2 Pop-Up-Meldungen

Über Tasks, bei denen eine Interaktion erforderlich ist

Diese Option ist wirksam, wenn die Konsole zu einer verwalteten Maschine oder zum Management Server verbunden ist.

Die Option legt fest, ob das Pop-Up-Fenster erscheint, wenn ein oder mehrere Tasks eine Interaktion erfordern. Dieses Fenster ermöglicht Ihnen, für alle Tasks am selben Platz eine Entscheidung zu treffen, wie z.B. einen Neustart zu bestätigen oder einen Neuversuch nach Freigabe von Festplattenplatz zu erlauben. So lange wenigstens ein Task eine Interaktion erfordert, können Sie dieses Fenster jederzeit vom **Dashboard** der verwalteten Maschine öffnen. Alternativ können Sie den Status der Task-Ausführung in der Ansicht **Tasks** überprüfen und Ihre Entscheidung für jeden Task im Bereich **Information** treffen.

Voreinstellung ist: **Aktiviert.**

Um eine Auswahl zu treffen, benutzen Sie das Kontrollkästchen **Fenster „Task erfordert Interaktion“ anzeigen**.

Über Ergebnisse der Task-Ausführung

Diese Option ist nur wirksam, wenn die Konsole zu einer verwalteten Maschine verbunden ist.

Die Option legt fest, ob die Pop-Up-Meldungen über Ergebnisse der Task-Ausführung erscheinen: Erfolgreiche Vollendung, Fehlschlagen oder erfolgreicher Abschluss mit Warnungen. Wenn die Anzeige der Pop-Up-Meldungen deaktiviert ist, können Sie den Status der Task-Ausführung und die Ergebnisse in der Ansicht **Tasks** überprüfen.

Voreinstellung ist: **Aktiviert** für alle Ergebnisse.

Um eine Einstellung für jedes Ergebnis (Erfolgreiche Vollendung, Fehlschlagen oder erfolgreicher Abschluss mit Warnungen) einzeln festzulegen, benutzen Sie das zugehörige Kontrollkästchen.

3.1.3 Zeit-basierte Warnungen

Letztes Backup

Diese Option ist wirksam, wenn die Konsole zu einer verwalteten Maschine (S. 197) oder zum Management Server (S. 193) verbunden ist.

Die Option legt fest, ob eine Warnung erscheint, wenn auf der gegebenen Maschine nach Ablauf einer Zeitspanne kein Backup durchgeführt wurde. Sie können die Zeitspanne einrichten, die Sie als kritisch für Ihr Geschäftsumfeld betrachten.

Voreinstellung ist: Warnen, wenn die letzte erfolgreiche Sicherung auf einer Maschine vor mehr als **5 Tagen** vollendet wurde.

Der Alarm erscheint im Abschnitt **Warnungen** des **Dashboards**. Wenn die Konsole zum Management Server verbunden ist, wird diese Einstellung auch das Farbschema der Spalte **Letztes Backup** für jede Maschine steuern und wird auch .

Letzte Verbindung

Diese Option ist wirksam, wenn die Konsole zu einer verwalteten Maschine (S. 194) oder zum Management Server verbunden ist.

Die Option legt fest, ob eine Warnung erscheint, wenn innerhalb einer eingerichteten Zeitspanne keine Verbindung zwischen einer verwalteten Maschine und dem Management Server hergestellt wurde, die Maschine also möglicherweise nicht zentral verwaltet wurde (z.B. bei einem Ausfall der Netzverbindung zu dieser Maschine). Sie können die Zeitspanne festlegen, die als kritisch erachtet wird.

Voreinstellung ist: Warnen, wenn die letzte Verbindung der Maschine zum Management Server vor mehr als **5 Tagen** war.

Der Alarm erscheint im Abschnitt **Warnungen** des **Dashboards**. Wenn die Konsole zum Management Server verbunden ist, wird diese Einstellung auch das Farbschema der Spalte **Letzte Verbindung** für jede Maschine steuern und wird auch .

3.1.4 Zahl der Tasks

Diese Option ist nur wirksam, wenn die Konsole zum Management Server verbunden ist.

Die Option legt fest, wie viele Tasks auf einmal in der Ansicht **Tasks** dargestellt werden. Sie können auch Filter benutzen, die in der Ansicht **Tasks** verfügbar sind, um die Anzahl angezeigter Tasks zu begrenzen.

Voreinstellung ist: **400**. Der Einstellungsbereich ist: **20 bis 500**.

Um eine Auswahl zu treffen, wählen Sie den gewünschten Wert im Listenfeld **Zahl der Tasks**.

3.1.5 Schriftarten

Diese Option ist wirksam, wenn die Konsole zu einer verwalteten Maschine oder zum Management Server verbunden ist.

Die Option legt fest, welche Schriftarten in der grafischen Benutzeroberfläche von Acronis Backup & Recovery 10 erscheinen. Die Einstellung **Menü** beeinflusst die Dropdown- und die Kontextmenüs. Die Einstellung **Anwendung** beeinflusst die anderen GUI-Elemente.

Voreinstellung ist: **Systemstandardschriftart** sowohl für die Menüs als für die Schnittstellenelemente der Anwendung.

Um eine Auswahl zu treffen, wählen Sie die Schriftart im jeweiligen Listenfeld und stellen die Schrifteigenschaften ein. Sie können die Erscheinung der Schriftart durch Klicken auf die rechts angeordnete Schaltfläche in einer Vorschau sehen.

3.2 Maschinen-Optionen

Die Maschinenoptionen definieren das allgemeine Verhalten von allen Acronis Backup & Recovery 10-Agenten, die auf der verwalteten Maschine operieren und werden daher als spezifisch für die Maschine betrachtet.

Um auf die Maschinenoptionen zuzugreifen, verbinden Sie die Konsole zur verwalteten Maschine und wählen dann **Optionen > Maschinenoptionen** im Menü.

3.2.1 Ereignisverfolgung

Es ist möglich, die von auf der verwalteten Maschine agierenden Agenten erstellten Logs an spezifizierte SNMP-Manager zu senden. Wenn Sie die Optionen zur Ereignisverfolgung an keiner anderen Stelle außer dieser verändern, werden die Einstellungen für jeden lokalen Backup-Plan und jeden erstellten Task auf der Maschine wirksam.

Sie können die Einstellungen in den Standardoptionen für Backup und Recovery (S. 48) exklusiv für die Ereignisse überschreiben, die während eines Backups oder einer Wiederherstellung auftreten. In diesem Fall werden die hier vorgenommenen Einstellungen auch wirksam für andere Tasks, z.B. für die Validierung von Archiven oder die Bereinigung.

Sie können die als Standard gesetzten Optionen auch überschreiben, wenn Sie einen Backup-Plan oder einen Recovery-Task einrichten. Diese so vorgenommenen Einstellungen werden plan-spezifisch oder task-spezifisch verwendet.

SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Sie können die Einstellungen in den Standardoptionen für Backup und Recovery (S. 48) exklusiv für die Ereignisse überschreiben, die während eines Backups oder einer Wiederherstellung auftreten. In diesem Fall werden die hier vorgenommenen Einstellungen auch wirksam für andere Tasks, z.B. für die Validierung von Archiven oder die Bereinigung.

Sie können die als Standard gesetzten Optionen auch überschreiben, wenn Sie einen Backup-Plan oder einen Recovery-Task einrichten. Diese so vorgenommenen Einstellungen werden plan-spezifisch oder task-spezifisch verwendet.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup & Recovery 10 siehe „Unterstützung für SNMP (S. 40)“.

Voreinstellung ist: **Ausgeschaltet**.

Versenden von SNMP-Benachrichtigungen einrichten

1. Aktivieren Sie das Kontrollkästchen **Meldungen an den SNMP-Server schicken**.
2. Spezifizieren Sie die passenden Optionen wie folgt:
   - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
   - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.
   - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist „public“.

   Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

Um die Funktion auszuschalten, deaktivieren Sie das Kontrollkästchen **Meldungen an den SNMP-Server schicken**.

Die Nachrichten werden über UDP verschickt.

Der nächste Abschnitt enthält zusätzliche Informationen über das Einstellen der SNMP-Dienste auf den empfangenden Maschinen (S. 47).

Einstellen der SNMP-Dienste auf der empfangenden Maschine

Windows

So installieren Sie den SNMP-Dienst auf einer Windows-Maschine:

1. **Start -> Systemsteuerung -> Software -> Windows-Komponenten hinzufügen/entfernen**
2. Wählen Sie **Verwaltungs- und Überwachungsprogramme.**
3. Klicken Sie auf **Details**.
4. Aktivieren Sie das Kontrollkästchen bei **SNMP (Simple Network Management Protocol)**.
5. Klicken Sie auf **OK**.

Sie sollten dann nach der Datei lmmib2.dll gefragt werden, die sich auf dem Installationsmedium des Betriebssystems befindet.

Linux

Um SNMP-Nachrichten auf einer Linux-Maschine zu empfangen, muss das Paket net-snmp (für RHEL und SUSE) oder das Paket snmpd (für Debian) installiert werden.

SNMP kann mit dem Befehl **snmpconf** konfiguriert werden. Die Standardkonfigurationsdateien befinden sich im Verzeichnis /usw/snmp:

- /etc/snmp/snmpd.conf – Konfigurationsdatei für den Net-SNMP Agenten
- /etc/snmp/snmpd.conf – Konfigurationsdatei für den Net-SNMP Trap Daemon.

3.2.2 Log-Bereinigungsregeln

Diese Option spezifiziert, wie das Log des Acronis Backup & Recovery 10 Agenten bereinigt wird.

Die Option definiert die maximale Größe des Ordners für den Agenten-Log (unter Windows XP/2003 Server, %ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\LogEvents).

Voreinstellung ist: **Maximale Log-Größe: 1 GB**. **Bei Bereinigung, behalte 95% der maximalen Loggröße bei**.

Wenn diese Option aktiviert ist, vergleicht das Programm nach jeweils 100 Log-Einträgen die tatsächliche Log-Größe mit der maximalen Größe. Sobald die maximale Log-Größe überschritten ist, löscht das Programm die ältesten Log-Einträge. Sie können bestimmen, wie viele Log-Einträge beibehalten werden sollen. Mit der Standardeinstellung '95%' wird ein Großteil des Logs beibehalten. Mit der Minimaleinstellung '1%' wird das Log fast vollständig geleert.

Diesen Parameter können Sie auch im Acronis Administrative Template setzen.

3.3 Standardoptionen für Backup und Recovery

3.3.1 Standard-Backup-Optionen

Jeder Acronis Agent hat eigene Standardoptionen für Backups. Sobald ein Agent installiert ist, haben die Standardoptionen vordefinierte Werte, die in der Dokumentation als **Voreinstellungen** bezeichnet werden. Bei Erstellung eines Backup-Plans können Sie entweder eine Standardoption verwenden oder diese mit einem benutzerdefinierten Wert überschreiben, der nur für diesen Plan gültig ist.

Sie können außerdem auch eine Standardoption konfigurieren, indem Sie den vordefinierten Wert verändern. Der neue Wert wird dann als Standard für alle nachfolgend auf dieser Maschine erstellten Backup-Pläne verwendet.

Um die Standardoptionen für Backups einzusehen und zu verändern, verbinden Sie die Konsole mit der verwalteten Maschine und wählen dort aus dem Hauptmenü **Optionen –>Standardoptionen für Backup und Recovery –> Backup-Standardoptionen**.

Verfügbarkeit der Backup-Optionen

Art und Umfang der verfügbaren Backup-Optionen sind abhängig von:

- der Umgebung, in der der Agent arbeitet (Linux, bootfähige Medien)
- dem Datentyp, der gesichert wird (Laufwerke, Dateien)
- Dem Backup-Ziel (Netzwerkpfad oder lokales Laufwerk)
- Dem Backup-Schema (sofortige Sicherung oder nach Zeitplan)

Die nachfolgende Tabelle fasst die Verfügbarkeit der Backup-Optionen zusammen:

	Agent für Linux		Bootfähiges Medium (Linux-basiert)	
	Laufwerk-Backup	**Datei-Backup**	**Laufwerk-Backup**	**Datei-Backup**
Schutz des Archivs (S. 50) (Kennwort und Verschlüsselung)	+	+	+	+
Ausschluss von Quelldateien (S. 51)	+	+	+	+
Vor-/Nach-Befehle für das Backup (S. 52)	+	+	-	-
Befehle vor/nach der Datenerfassung (S. 54)	+	+	-	-
Snapshot für Backup auf Dateiebene (S. 56)	-	+	-	-
Komprimierungsrate (S. 56)	+	+	+	+
Backup-Performance:				
Backup-Priorität (S. 57)	+	+	-	-
Schreibgeschwindigkeit auf Laufwerk (S. 57)	Ziel: HDD	Ziel: HDD	Ziel: HDD	Ziel: HDD
Datendurchsatz im Netzwerk (S. 58)	Ziel: Netzlaufwerk	Ziel: Netzlaufwerk	Ziel: Netzlaufwerk	Ziel: Netzlaufwerk
Beschleunigtes inkrementelles und differentielles Backup (S. 61)	+	-	+	-
Backup-Aufteilung (S. 61)	+	+	+	+
Medienkomponenten	Ziel: Wechselmedien	Ziel: Wechselmedien	-	-
Fehlerbehandlung (S. 62):				
Während der Durchführung keine Meldungen bzw. Dialoge zeigen (stiller Modus)	+	+	+	+
Bei Fehler neu versuchen	+	+	+	+
Fehlerhafte Sektoren ignorieren	+	+	+	+
Dual-Destination (S. 63)	Ziel: lokal	Ziel: lokal	-	-
Task-Startbedingungen (S. 64)	+	+	-	-
Task-Fehlerbehandlung (S. 65)	+	+	-	-
Erweiterte Einstellungen (S. 66):				
Überschreiben der Daten auf einem Band, ohne den Benutzer zur Bestätigung aufzufordern	Ziel: Band	Ziel: Band	Ziel: Band	Ziel: Band

Medien trennen, nachdem das Backup beendet ist	Ziel: Wechselmedien	Ziel: Wechselmedien	Ziel: Wechselmedien	Ziel: Wechselmedien
Beim Backup auf ein entfernbares Medium nach dem ersten Medium fragen	Ziel: Wechselmedien	Ziel: Wechselmedien	Ziel: Wechselmedien	Ziel: Wechselmedien
Nach Abschluss des Backups die Maschine automatisch neu starten	-	-	+	+
Software-RAID- und LVM-Metadaten gemeinsam mit Backups speichern	+	-	-	-
Benachrichtigungen:				
E-Mail (S. 58)	+	+	-	-
Win Pop-up (S. 59)	+	+	-	-
Ereignisverfolgung:				
SNMP (S. 60)	+	+	-	-

Schutz des Archivs

Diese Option ist für Windows-, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist wirksam für Disk-Backups und Backups auf Dateiebene.

Voreinstellung ist: **Deaktiviert.**

So schützen Sie ein Archiv vor unberechtigtem Zugriff

1. Aktivieren Sie das Kontrollkästchen **Kennwort für das Archiv einrichten**.
2. Tragen Sie im Eingabefeld **Kennwort** ein Kennwort ein.
3. Tragen Sie das Kennwort im Eingabefeld **Kennwortbestätigung** erneut ein.
4. Wählen Sie eine der nachfolgenden Varianten:
   - **Nicht verschlüsseln** – das Archiv wird nur mit dem Kennwort geschützt.
   - **AES 128** – das Archiv wird mit Hilfe des Advanced Encryption Standard-Verfahrens (AES) und 128-Bit verschlüsselt.
   - **AES 192** – das Archiv wird mit Hilfe von Advanced Standard Encryption (AES) und einem 192-Bit-Schlüssel verschlüsselt.
   - **AES 256** – das Archiv wird mit Hilfe von Advanced Standard Encryption (AES) und einem 256-Bit-Schlüssel verschlüsselt.
5. Klicken Sie auf **OK**.

Der kryptografische Algorithmus AES arbeitet im Cipher Block Chaining Mode (CBC) und benutzt einen zufällig erstellten Schlüssel mit der benutzerdefinierten Größe von 128, 192 oder 256 Bit. Je größer die Schlüsselgröße, desto länger wird das Programm für die Verschlüsselung brauchen, aber desto sicherer sind auch die Daten.

Der Kodierungsschlüssel ist dann mit AES-256 unter Benutzung eines SHA-256-Hash-Werts des angegebenen Kennworts verschlüsselt. Das Kennwort selbst wird nirgendwo auf der Festplatte oder in der Backup-Datei gespeichert, es wird nur der Kennwort-Hash-Wert für Bestätigungszwecke benutzt. Mit dieser zweistufigen Methode sind die gesicherten Daten vor jedem unberechtigten Zugriff geschützt, aber ein verlorenes Kennwort kann unmöglich wiederhergestellt werden.

Ausschluss von Quelldateien

Diese Option ist für Windows-, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist nur für Disk-Backups mit NTFS- und FAT-Dateisystemen wirksam. Diese Option ist bei Backups auf Dateiebene für alle unterstützten Dateisysteme wirksam.

Diese Option definiert, welche Dateien und Ordner während des Backup-Prozesses übersprungen und so von der Liste der gesicherten Elemente ausgeschlossen werden.

Voreinstellung ist: **Dateien ausschließen, die folgende Kriterien erfüllen: *.tmp, *.~, *.bak.**

Dateien und Verzeichnisse zum Ausschließen spezifizieren:

Verwenden Sie einen der nachfolgenden Parameter:

- **Ausschluss aller Systemdateien und Systemordner**

  Diese Option ist nur für Dateisysteme wirksam, die von Windows unterstützt werden. Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner mit dem Attribut **Versteckt** zu überspringen. Bei Ordnern mit dem Attribut **Versteckt** wird der gesamte Inhalt ausgeschlossen – einschließlich solcher Dateien, die nicht **versteckt** sind.
- **Ausschluss aller Systemdateien und Systemordner**

  Diese Option ist nur für Dateisysteme wirksam, die von Windows unterstützt werden. Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner mit dem Attribut **System** zu überspringen. Bei Ordnern mit dem Attribut **System** wird der gesamte Inhalt ausgeschlossen – einschließlich solcher Dateien, die nicht mit **System** gekennzeichnet sind.

*Sie können die Attribute von Dateien oder Ordnern über ihre Datei-/Ordner-Eigenschaften einsehen oder durch Verwendung des Kommandozeilenbefehls **attrib**. Weitere Informationen finden Sie im Hilfe und Support-Center von Windows.*

- **Dateien ausschließen, die folgenden Kriterien entsprechen**

  Aktivieren Sie dieses Kontrollkästchen, um Dateien und Ordner zu überspringen, deren Bezeichnungen mit einem der Kriterien in der Liste übereinstimmen (Dateimaske genannt) – verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Alle entfernen**, um die Liste der Dateimasken zu erstellen.

  Sie können ein oder mehrere Wildcard-Zeichen (* und ?) in einer Datei-Maske verwenden:

  Das Asterisk (*) steht für Null oder mehrere Zeichen im Dateinamen; so ergibt z.B. die Datei-Maske Doc*.txt Dateien wie Doc.txt und Document.txt.

  Das Fragezeichen (?) steht für exakt ein Zeichen in einem Dateinamen, so ergibt z.B. die Datei-Maske Doc?.txt Dateien wie Doc1.txt und Docs.txt – aber nicht Doc.txt oder Doc11.txt.

Fügen Sie einem als Kriterium angegebenen Ordnernamen ein Backslash (\) hinzu, um einen Ordner zu spezifizieren, dessen Pfad einen Laufwerksbuchstaben enthält, beispielsweise: C:\Finanzen\

Beispiele für Ausschließungen

Kriterium	Beispiel	Beschreibung
Windows und Linux		
Per Name	F.log F	Schließt alle Dateien namens „F.log“ aus Schließt alle Ordner namens „F“ aus

Per Maske (*)	*.log F*	Schließt alle Dateien mit der Erweiterung „.log“ aus Schließt alle Dateien und Ordner aus, deren Namen mit „F“ beginnen (etwa die Ordner F, F1 und die Dateien F.log, F1.log)
Per Maske (?)	F???.log	Schließt alle .log-Dateien aus, deren Namen am Ende vier Zeichen enthalten und mit „F“ beginnen
Windows		
Per Dateipfad	C:\Finanzen\F.log	Schließt die Datei aus, die „F.log“ heißt und im Ordner „C:\Finanzen“ vorliegt
Per Ordnerpfad	C:\Finanzen\F\	Schließt den Ordner „C:\Finanzen\F“ aus (stellen Sie sicher, dass Sie den vollständigen Pfade angeben, beginnend mit einem Laufwerksbuchstaben)
Linux		
Per Dateipfad	/home/user/Finanzen/F.log	Schließt die Datei aus, die „F.log“ heißt und im Ordner „/home/user/Finanzen“ vorliegt
Per Ordnerpfad	/home/user/Finanzen/	Schließt den Ordner „/home/user/Finanzen“ aus

Die genannten Einstellungen sind nicht für Dateien oder Ordner wirksam, die ausdrücklich zum Backup ausgewählt wurden. Ein Beispiel: Angenommen, Sie haben das Verzeichnis „MeinOrdner“ sowie die (außerhalb dieses Ordners liegende) Datei MeineDatei.tmp gewählt – und festgelegt, dass alle .tmp-Dateien übersprungen werden sollen. In diesem Fall werden alle .tmp-Dateien in „MeinOrdner“ während der Backup-Prozedur übersprungen, jedoch nicht die Datei „MeineDatei.tmp“.

Vor-/Nach-Befehle

Diese Option ist für Windows-, Linux-Betriebssysteme und das PE-Boot-Medium wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach einem Backup durchgeführt werden.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

So benutzen Sie diese Vor- bzw. Nach-Befehle:

- Löschen temporärer Dateien von der Festplatte vor dem Start des Backups
- Konfiguration des Antivirenprodukts eines Drittanbieters, so dass es jedes Mal vor dem Backup startet
- Kopieren des Archivs zu einem anderen Ort nach Abschluss des Backups.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern, wie z.B. „pause“.

So spezifizieren Sie Vor-/Nach-Befehle

1. Sie aktivieren Vor-/Nach-Befehle mit Hilfe der folgenden Optionen:
   - **Vor Backup ausführen**
   - **Nach Backup ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.

- Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.

3. Klicken Sie auf **OK**.

Befehl vor Backup

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start des Backups ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	**Auswahl**			
Task scheitern lassen, wenn die Ausführung der Befehle fehlschlägt	Ausgewählt	Abgewählt	Ausgewählt	Abgewählt
Kein Backup, bis die Befehlsausführung vollständig ist	Ausgewählt	Ausgewählt	Abgewählt	Abgewählt
Ergebnis				
	Voreinstellung Backup nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Task scheitern lassen, wenn die Ausführung der Befehle fehlschlägt.	Ausführen des Backups nach Ausführung des Befehls unabhängig von Erfolg oder Misserfolg der Ausführung.	N/A	Ausführen des Backups gleichzeitig mit der Befehlsausführung und unabhängig vom Ergebnis der Ausführung des Befehls.

Befehl nach Backup

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn das Backup vollständig ist

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei.
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wenn die erfolgreiche Ausführung des Befehls für die Backup-Strategie kritisch ist, dann aktivieren Sie das Kontrollkästchen **Task scheitern lassen, wenn die Ausführung der Befehle**

fehlschlägt. Falls die Befehlsausführung versagt, wird das Programm die entstehende tib-Datei und temporäre Dateien entfernen, falls das möglich ist, und der Task wird fehlschlagen.

Wenn das Kontrollkästchen nicht ausgewählt ist, dann hat das Ergebnis der Befehlsausführung keinen Einfluss auf Erfolg oder Misserfolg des Tasks. Sie können das Ergebnis der Befehlsausführung durch Ansicht des Logs oder der Fehler und Warnungen verfolgen, die auf dem **Dashboard** dargestellt werden.

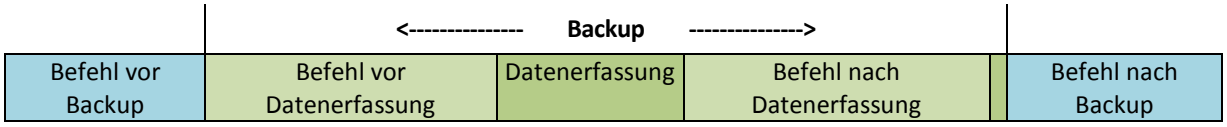
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Befehle vor/nach der Datenerfassung

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenerfassung (also Erstellung des Daten-Snapshots) durchgeführt werden. Die Datenerfassung wird von Acronis Backup & Recovery 10 zu Beginn der Backup-Prozedur durchgeführt.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.



Wenn die Option Volume Shadow Copy Service aktiviert ist, werden die Ausführung der Befehle und die Aktionen von Microsofts VSS folgendermaßen eingeordnet:

Befehle „vor Datenerfassung“ -> VSS Suspend -> Datenerfassung -> VSS Resume -> Befehle „nach Datenerfassung“.

Mit Hilfe der Befehle vor bzw. nach der Datenerfassung können Sie Datenbanken, die nicht mit VSS kompatibel sind, vor der Datenerfassung suspendieren und nach der Datenerfassung wieder anlaufen lassen. Im Gegensatz zu den Vor-/Nach-Befehlen (S. 52) werden die Befehle vor/nach der Datenerfassung direkt vor bzw. nach dem Datenerfassungsprozess durchgeführt. Das benötigt einige Sekunden. Die komplette Backup-Prozedur kann in Abhängigkeit von der zu sichernden Datenmenge entsprechend deutlich länger dauern. Daher werden die Datenbanken oder die Anwendungen nur kurze Zeit pausieren.

So spezifizieren Sie Befehle vor/nach der Datenerfassung

1. Sie aktivieren Befehle vor/nach der Datenerfassung mit Hilfe der folgenden Optionen:
   - **Vor der Datenerfassung ausführen**
   - **Nach der Datenerfassung ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.
   - Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.
3. Klicken Sie auf **OK**.

Befehl vor Datenerfassung

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor der Datenerfassung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	**Auswahl**			
Backup-Task scheitern lassen, wenn die Ausführung der Befehle fehlschlägt	Ausgewählt	Abgewählt	Ausgewählt	Abgewählt
Keine Datenerfassung, bis die Befehlsausführung vollständig ist	Ausgewählt	Ausgewählt	Abgewählt	Abgewählt
Ergebnis				
	Voreinstellung Datenerfassung nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Task scheitern lassen, wenn die Ausführung der Befehle fehlschlägt.	Ausführen der Datenerfassung nach Ausführung des Befehls unabhängig von Erfolg oder Misserfolg der Ausführung.	N/A	Ausführen der Datenerfassung gleichzeitig mit der Befehlsausführung und unabhängig vom Ergebnis der Ausführung des Befehls.

Befehl nach Datenerfassung

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die nach der Datenerfassung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	Auswahl			
Task scheitern lassen, wenn die Ausführung der Befehle fehlschlägt	Ausgewählt	Abgewählt	Ausgewählt	Abgewählt
Kein Backup, bis die Befehlsausführung vollständig ist	Ausgewählt	Ausgewählt	Abgewählt	Abgewählt
Ergebnis				
	Voreinstellung Backup nur fortsetzen, nachdem der Befehl erfolgreich durchgeführt wurde. Löschen der tib-Datei und der temporären Dateien und Task fehlschlagen, wenn die Befehlsausführung versagt.	Fortsetzen des Backups nach Ausführung des Befehls unabhängig von Erfolg oder Misserfolg der Ausführung.	N/A	Fortsetzen des Backups gleichzeitig mit der Befehlsausführung und unabhängig vom Ergebnis der Ausführung des Befehls.

Snapshot für Backup auf Dateiebene

Diese Option ist nur für Backups auf Dateiebene wirksam in Windows- und Linux-Betriebssystemen.

Diese Option definiert, ob Dateien eine nach der anderen gesichert werden oder auf Basis eines sofortigen Snapshots der Daten.

Beachten Sie: *Dateien von Netzlaufwerken werden immer eine nach der anderen gesichert.*

Voreinstellung ist: **Snapshot erstellen, wenn es möglich ist.**

Wählen Sie eine der nachfolgenden Varianten:

- **Immer einen Snapshot erstellen**

  Ein Snapshot ermöglicht das Backup aller Dateien einschließlich solcher, die für den exklusiven Zugriff geöffnet sind. Die Dateien werden zum gleichen Zeitpunkt gesichert. Wählen Sie diese Einstellung nur, wenn diese Faktoren kritisch sind, d.h. ein Backup der Dateien ohne den vorhergehenden Snapshot keinen Sinn macht. Um einen Snapshot zu benutzen, muss der Backup-Plan mit einem Administrator-Konto oder den Rechten eines Backup-Operators ausgeführt werden. Wenn kein Snapshot erstellt werden kann, wird das Backup fehlschlagen.
- **Snapshot erstellen, wenn es möglich ist**

  Dateien direkt sichern, wenn kein Snapshot möglich ist.
- **Keinen Snapshot erstellen**

  Dateien immer direkt sichern. Administratorrechte oder Rechte eines Backup-Operators sind nicht erforderlich. Der Versuch zum Sichern von Dateien, die für exklusiven Zugriff geöffnet sind, wird in einem Fehler resultieren. Außerdem ist die Backup-Zeit der Dateien nicht gleich.

Komprimierungsrate

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Die Option definiert den Grad der Komprimierung für die zu sichernden Daten.

Voreinstellung ist: **Normal.**

Der ideale Grad für die Datenkomprimierung hängt von der Art der Daten ab, die gesichert werden sollen. So wird z.B. eine maximale Komprimierung die Größe einer Archivdatei nicht wesentlich beeinflussen, wenn bereits stark komprimierte Dateien im Archiv erfasst werden wie jpg-, pdf- oder mp3-Dateien. Andere Typen, wie z.B. doc- oder xls-Dateien, werden gut komprimiert.

So spezifizieren Sie den Komprimierungsgrad

Wählen Sie eine der nachfolgenden Varianten:

- **Keine** – die Daten werden so gesichert, wie sie sind, ohne dabei komprimiert zu werden. Die entstehende Größe des Backup-Archivs wird maximal sein.
- **Normal** – in den meisten Fällen empfohlen.
- **Hoch** – die Größe des entstehenden Backups ist üblicherweise kleiner als die bei der Einstellung **Normal**.
- **Maximum** – die Daten werden so sehr komprimiert, wie es geht. Die Dauer eines solchen Backups wird maximal sein. Sie könnten beim Backup auf Wechselmedien die maximale Komprimierung auswählen, um die Zahl der erforderlichen Medien zu verringern.

Backup-Performance

Benutzen Sie diese Gruppe der Optionen, um die Nutzung der Netzwerk- und der System-Ressourcen zu steuern.

Die Optionen zur Steuerung der Performance haben mehr oder weniger spürbare Auswirkungen auf die Geschwindigkeit des Backups. Die Wirkung hängt von den Systemkonfigurationen und den physikalischen Eigenschaften der Geräte ab, die beim Backup als Quelle oder Ziel benutzt werden.

Backup-Priorität

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Die Priorität eines jeden Prozesses, der in einem System läuft, hängt vom Grad der CPU-Benutzung und der Systemressourcen ab, die dem Prozess zugeordnet werden. Das Herabsetzen der Backup-Priorität wird mehr Ressourcen für andere Anwendungen freisetzen. Das Heraufsetzen der Backup-Priorität kann den Backup-Prozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren wie der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk.

Voreinstellung ist: **Niedrig.**

So spezifizieren Sie die Priorität des Backup-Prozesses

Wählen Sie eine der nachfolgenden Varianten:

- **Niedrig** – minimiert die durch den Backup-Prozess verwendeten Ressourcen und belässt mehr Ressourcen für andere Prozesse, die auf der Maschine laufen.
- **Normal** – führt den Backup-Prozess mit normaler Geschwindigkeit aus und teilt die verfügbaren Ressourcen mit anderen Prozessen.
- **Hoch** – maximiert die Geschwindigkeit des Backup-Prozesses und zieht Ressourcen von anderen Prozessen ab.

Schreibgeschwindigkeit der Festplatte

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option steht zur Verfügung, wenn eine interne (feste) Festplatte der Maschine als Backup-Ziel für das laufende Backup gewählt wurde.

Ein laufendes Backup auf einer internen Festplatte (z.B. in der Acronis Secure Zone) kann die Performance anderer Programme beeinträchtigen, weil eine große Datenmenge auf die Festplatte geschrieben werden muss. Sie können den Festplattengebrauch durch das Backup-Verfahren auf einen gewünschten Grad begrenzen.

Voreinstellung ist: **Maximum.**

So stellen Sie die gewünschte Schreibgeschwindigkeit für das Backup ein

Wählen Sie aus den nachfolgenden Varianten:

- Klicken Sie auf **Schreibgeschwindigkeit in Prozent bezogen auf die maximale Geschwindigkeit der Zielfestplatte** und verändern Sie dann mit dem Schieber den Prozentwert.
- Klicken Sie auf **Schreibgeschwindigkeit in Kilobytes pro Sekunde** und tragen Sie dann den gewünschten Wert in Kilobytes pro Sekunde ein.

Datendurchsatz im Netzwerk

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option steht zur Verfügung, wenn ein Speicherort im Netzwerk (freigegebenes Netzlaufwerk, verwaltetes Depot oder FTP-/SFTP-Server) als Ziel für das Backup gewählt ist.

Die Option definiert den Betrag der Bandbreite für die Netzwerkverbindung, die zum Übertragen der gesicherten Daten zugeteilt wird.

Als Standard ist dieser Wert auf das Maximum gesetzt, d.h. die Software benutzt die gesamte Netzwerkbandbreite zum Übertragen der gesicherten Daten, die sie erhalten kann. Benutzen Sie diese Option, um einen Teil der Netzwerkbandbreite für andere Aktivitäten im Netzwerk zu reservieren.

Voreinstellung ist: **Maximum.**

So stellen Sie den Datendurchsatz im Netzwerk ein

Wählen Sie aus den nachfolgenden Varianten:

- Klicken Sie auf **Datendurchsatz in Prozent bezogen auf die geschätzte maximale Bandbreite der Netzverbindung** und verändern Sie dann mit dem Schieber den Prozentwert.
- Klicken Sie auf **Datendurchsatz in Kilobytes pro Sekunde** und tragen Sie dann den gewünschten Wert in Kilobytes pro Sekunde ein.

Benachrichtigungen

Acronis Backup & Recovery 10 kann Sie über den Abschluss eines Backups per E-Mail oder Windows Nachrichtendienst (WinPopup, nur bei Windows XP) benachrichtigen.

E-Mail

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Die Option ermöglicht Ihnen den Erhalt von E-Mail-Benachrichtigungen zusammen mit dem vollständigen Log des Tasks über die erfolgreiche Vollendung von Backup-Tasks, über Fehler oder über erforderliche Interaktion.

Voreinstellung ist: **Ausgeschaltet**.

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung schicken**, um die entsprechende Funktion zu aktivieren.
2. Geben Sie in das Feld **E-Mail-Adresse** die E-Mail-Adresse an, zu der die Benachrichtigung geschickt wird. Sie können auch durch Semikolons abgetrennt mehrere Adressen eingeben.
3. Aktivieren Sie unter **Benachrichtigungen senden** die Kontrollkästchen folgendermaßen:
   - **Wenn Backup erfolgreich vollendet ist** – Benachrichtigung wird gesendet, wenn das Backup erfolgreich abgeschlossen wurde.
   - **Wenn Backup fehlgeschlagen ist** – Benachrichtigung wird gesendet, wenn das Erstellen des Backups nicht erfolgreich war.

   Das Kontrollkästchen **Wenn eine Benutzeraktion erforderlich ist** ist immer aktiviert.
4. Aktivieren Sie das Kontrollkästchen **Vollständiges Log zur Benachrichtigung hinzufügen**, damit die E-Mail-Nachricht zum Backup gehörende Log-Einträge mit beinhalten wird.
5. Klicken Sie auf **Erweiterte E-Mail-Parameter**, um die nachfolgend erläuterten E-Mail-Parameter zu konfigurieren und klicken Sie dann auf **OK**:
   - **Von** – geben Sie die E-Mail-Adresse des Benutzers ein, von dem die Nachricht verschickt wird. Wenn Sie dieses Feld leer lassen, werden die Nachrichten werden so konstruiert, als stammten sie von der Zieladresse.
   - **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.
   - Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:
     - **Posteingangssever (POP3)** – geben Sie den Namen des POP3-Servers an.
     - **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf 110 gesetzt.
     - **Benutzername** – geben Sie den Benutzernamen ein
     - **Kennwort** – geben Sie das Kennwort ein.
   - Aktivieren Sie das Kontrollkästchen **Spezifizierten Postausgangsserver benutzen**, um einen SMTP-Server zu aktivieren und seine Einstellungen einzurichten:
     - **Postausgangsserver (SMTP)** – geben Sie den Namen des SMTP-Servers an.
     - **Port** – bestimmt den Port des SMTP-Servers. Standardmäßig ist der Port auf 25 gesetzt.
     - **Benutzername** – geben Sie den Benutzernamen ein.
     - **Kennwort** – geben Sie das Kennwort ein.
6. Klicken Sie auf **Test-Mail senden**, um die Richtigkeit der Einstellungen zu überprüfen.

Nachrichtendienst (WinPopup)

Diese Option ist wirksam für Windows und Linux-Betriebssysteme auf der sendenden Maschine und für Windows-Systeme auf der empfangenden Maschine.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Die Option ermöglicht Ihnen den Erhalt von WinPopup-Benachrichtigungen über die erfolgreiche Vollendung von Backup-Tasks, über Fehler oder über erforderliche Handlungen.

Voreinstellung ist: **Ausgeschaltet.**
Vor Konfiguration der WinPopup-Benachrichtung sollten Sie sicherstellen, dass der Nachrichtendienst von Windows XP auf beiden Maschinen (die Task ausführende und die Nachrichten empfangende Maschine) gestartet ist.

In der Microsoft Windows Server 2003-Familie ist der Nachrichtendienst standardmäßig ausgeschaltet. Wechseln Sie den Startmodus des Dienstes auf Automatisch und starten Sie ihn dann.

So konfigurieren Sie WinPopup-Benachrichtigungen:

1. Aktivieren Sie das Kontrollkästchen **WinPopup-Benachrichtigung schicken**.
2. Geben Sie in das Feld **Maschinenname** den Namen der Maschine ein, an die die Benachrichtigungen verschickt werden. Multiple Namen werden nicht unterstützt.

Aktivieren Sie unter **Benachrichtigungen senden** die Kontrollkästchen folgendermaßen:

- **Wenn Backup erfolgreich vollendet ist** – Benachrichtigung wird gesendet, wenn das Backup erfolgreich abgeschlossen wurde.
- **Wenn Backup fehlgeschlagen ist** – Benachrichtigung wird gesendet, wenn das Erstellen des Backups nicht erfolgreich war.

Das Kontrollkästchen **Wenn eine Benutzeraktion erforderlich ist** – Benachrichtigung wird gesendet, wenn während der Aktion das Eingreifen des Benutzers erforderlich ist – ist immer ausgewählt.

Klicken Sie auf **WinPopup-Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

Ereignisverfolgung

Es ist möglich, Ereignis-Logs von Backup-Aktionen, die auf der verwalteten Maschine ausgeführt werden, an spezifizierte SNMP-Manager zu senden.

SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse von Backup-Aktionen zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup & Recovery 10 siehe „Unterstützung für SNMP (S. 40)“.

Voreinstellung ist: **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind.**

So wählen Sie, ob Ereignisse von Backup-Aktionen an SNMP-Manager geschickt werden:

Wählen Sie eine der folgenden Optionen:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen bei Optionen der Maschine (S. 46).

- **SNMP-Benachrichtigungen für Ereignisse bei Backup-Aktionen einzeln senden** – für das Senden von SNMP-Benachrichtigungen mit den Ereignissen bei Backup-Aktionen an spezifizierte SNMP-Manager.
  - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
  - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.
  - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist „public“.

  Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.
- **Keine SNMP-Benachrichtigungen senden** – Einstellung, um das Versenden von Ereignissen über Backup-Aktionen an SNMP-Manager unwirksam zu machen.

Beschleunigtes inkrementelles und differentielles Backup

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist wirksam für inkrementelle und differentielle Backups auf Dateiebene.

Diese Option definiert, ob für die Ermittlung einer Dateiänderung die Dateigröße und der Zeitstempel benutzt werden oder dafür der Dateiinhalt mit den im Archiv gespeicherten Dateien verglichen wird.

Voreinstellung ist: **Aktiviert.**

Inkrementelle oder differentielle Backups erfassen nur die geänderten Daten. Um das Backup-Verfahren zu beschleunigen, entscheidet das Programm darüber, ob eine Datei geändert wurde oder nicht, anhand von Dateigröße und Zeitstempel der letzten Änderung. Das Ausschalten dieser Funktion wird dazu führen, dass das Programm immer den Inhalt einer Datei mit dem Inhalt der Datei vergleicht, die in einem Archiv gespeichert ist.

Aufteilung von Backups

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Die Option definiert, wie ein Backup aufgeteilt werden kann.

Voreinstellung ist: **Automatisch.**

Es stehen die folgenden Einstellungen zur Verfügung.

Automatisch

Mit dieser Einstellung wird Acronis Backup & Recovery 10 wie folgt arbeiten.

- **Beim Backup einer Festplatte:**

  Es wird eine einzige Backup-Datei erstellt werden, wenn das Dateisystem des Ziels die geschätzte Dateigröße erlaubt.

  Das Backup wird automatisch in mehrere Dateien aufgeteilt, wenn das Dateisystem des Ziels die geschätzte Dateigröße erlaubt. Das ist z.B. der Fall, wenn als Ziel des Backups ein FAT16- oder FAT32-Dateisystem gewählt ist, die eine 4GB-Grenze für die Dateigröße haben.

  Wenn die Zielfestplatte während des Backups voll läuft, wechselt der Task in den Zustand **Interaktion erforderlich**. Sie haben dann die Möglichkeit, zusätzlichen Speicherplatz frei zu machen und die Aktion zu wiederholen. In diesem Fall wird das resultierende Backup in zwei Teile gesplittet, die vor bzw. nach der Wiederholung erstellt wurden.

- **Beim Backup auf Wechselmedien** (CD, DVD oder ein Bandgerät, das lokal mit der verwalteten Maschine verbunden ist):

  Der Task wird in den Status **Interaktion erforderlich** wechseln und nach einem neuen Medium fragen, wenn das vorhergehende voll ist.

Feste Größe

Tragen Sie die gewünschte Dateigröße ein oder wählen Sie diese aus dem Listenfeld. Das Backup wird in mehrere Dateien der angegebenen Größe gesplittet werden. Das ist praktisch, wenn Sie ein Backup mit der Absicht erstellen, dieses nachträglich auf eine CD oder DVD zu brennen. Sie müssen auch die Backups aufteilen, die zu einem FTP-Server geschickt werden, da die Wiederherstellung der Daten direkt von einem FTP-Server erfordert, dass die Backups in Dateien nicht größer als 2 GB aufgeteilt sind.

Medienkomponenten

Diese Option ist für Windows- und Linux-Betriebssysteme wirksam, wenn das Ziel des Backups ein Wechselmedium ist.

Wenn Sie ein Backup auf ein Wechselmedium speichern, dann können Sie dieses Medium auf Linux-Basis zu einem bootfähigen Medium (S. 188) machen, indem Sie zusätzliche Komponenten darauf speichern. Demzufolge benötigen Sie kein separates Notfallmedium.

Voreinstellung ist: **Nichts ausgewählt.**

Aktivieren Sie die Kontrollkästchen der Komponenten, die Sie auf das bootfähige Medium platzieren wollen:

- **One-Click Restore** ist eine kleine Ergänzung zu einem Disk-Backup, das auf einem Wechselmedium gespeichert ist, welche auf einen einzelnen Klick hin eine Wiederherstellung dieses Backups ermöglicht. Wenn Sie eine Maschine mit einem bootfähigen Medium starten und auf den Befehl **Acronis One-Click Restore ausführen** klicken, werden alle Daten sofort und ohne weitere Nachfrage zu ihrem ursprünglichen Speicherort wiederhergestellt.

  Achtung: *Weil diese Art der Wiederherstellung keine Interaktionaktionsmöglichkeit für den Benutzers bietet, wie z.B. die Auswahl der wiederherzustellenden Volumes, stellt Acronis One-Click Restore immer das komplette Laufwerk wieder her. Falls das Laufwerk also mehrere Volumes enthält und Sie den Einsatz von Acronis One-Click Restore planen, dann müssen Sie alle Volumes in das Backup aufnehmen. Ansonsten gehen beim Einsatz dieser Funktion die Volumes verloren, die nicht im Backup enthalten sind.*

- Der **Bootable Agent** ist ein bootfähiges, auf einem Linux-Kernel basierendes Notfallmedium, das die meisten Funktionen von Acronis Backup & Recovery 10 Agent enthält. Platzieren Sie diese Komponente auf dem Medium, wenn Sie größere Funktionalität während der Wiederherstellung wünschen. Sie können die Wiederherstellung auf die gleiche Weise wie von einem regulären Boot-Medium konfigurieren und Active Restore oder Universal Restore verwenden. Wenn das Medium in Windows erstellt wird, stehen auch die Funktionen zur Laufwerksverwaltung zur Verfügung.

Fehlerbehandlung

Diese Optionen sind für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Optionen ermöglichen Ihnen vorzugeben, wie auftretende Fehler beim Backup behandelt werden.

Meldungen und Dialogboxen während der Aktion nicht zeigen (stiller Modus)

Voreinstellung ist: **Ausgeschaltet**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die eine Benutzeraktion erfordern (außer der Behandlung von fehlerhaften Sektoren, die mit einer eigenen Option gesteuert wird). Wenn eine Aktion ohne einen Benutzereingriff nicht fortsetzen kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

Bei Fehler neu versuchen

Voreinstellung ist: **Aktiviert**. **Zahl der Versuche: 5. Abstand zwischen Versuchen: 30 Sekunden.**

Wenn ein regenerierbarer Fehler auftritt, versucht das Programm erneut, die erfolglose Aktion durchzuführen. Sie können den Zeitabstand und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

Wenn der Speicherort des Backups im Netzwerk nicht verfügbar oder erreichbar ist, wird die Anwendung versuchen, den Ort alle 30 Sekunden erneut zu erreichen, aber nur fünf Mal. Die Versuche werden aufgegeben, wenn entweder die Verbindung gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

Fehlerhafte Sektoren ignorieren

Voreinstellung ist: **Ausgeschaltet**.

Wenn die Option unwirksam gemacht ist, wird das Programm jedes Mal ein Pop-up-Fenster zeigen, wenn es auf einen fehlerhaften Sektor stößt, und um eine Entscheidung bitten, ob das Backup fortgesetzt oder abgebrochen werden soll. Wenn Sie z.B. vorhaben, die Informationen von einer „sterbenden“ Festplatte zu retten, aktivieren Sie diese Funktion. Die restlichen Daten werden in diesem Fall noch gesichert und Sie werden das entstandene Festplatten-Backup mounten und die noch gültigen Daten auf eine andere Festplatte kopieren können.

Dual-Destination

Diese Option ist für Windows und Linux-Betriebssysteme wirksam, wenn das primäre Backup-Ziel ein *lokaler Ordner oder die Acronis Secure Zone* ist und das sekundäre Ziel ein *anderer lokaler oder Netzwerk-Ordner*. Verwaltete Depots und FTP-Server werden als sekundäre Ziel-Speicherorte nicht unterstützt.

Voreinstellung ist: **Ausgeschaltet.**

Nach dem Einschalten dieser Funktion wird der Agent automatisch bei jedem Backup auf einen lokalen Speicherort eine Kopie auf einem zweiten Zielspeicherort erstellen, z.B. einem Netzlaufwerk. Sobald das Backup zum primären Ziel vollendet ist, vergleicht der Agent den aktualisierten Archivinhalt mit dem sekundären Archivinhalt und kopiert dann zusammen mit dem neuen Backup alle möglicherweise fehlenden anderen Backups an das sekundäre Ziel.

Die Funktion bietet ein schnelles Backup der Maschine auf ein internes Laufwerk als Zwischenschritt, bevor das fertige Backup über das Netzwerk übertragen wird. Das ist besonders praktisch bei langsamen oder stark beschäftigten Netzwerken und bei besonders zeitaufwändigen Backup-Verfahren. Im Gegensatz zu einem direkten Backup auf einen Remote-Speicherort wird ein Verbindungsabbruch während des Kopierens den Backup-Prozess selbst nicht beeinflussen.

Andere Vorteile:

- Die Replizierung erhöht die Zuverlässigkeit des Archivs.

- Diese Funktion ist besonders für Geschäftsreisende mit tragbaren Computern interessant, die Backups unterwegs in der Acronis Secure Zone sichern. Sobald dann der tragbare Computer wieder mit dem Netzwerk des Unternehmens verbunden ist, werden alle Änderungen, die zwischenzeitlich zum Archiv übertragen wurden, beim nächsten Backup mit auf die stationäre Kopie übertragen.

Wenn Sie eine durch ein Kennwort geschützte Acronis Secure Zone als primären Speicherort verwenden, dann bedenken Sie, dass das Archiv im sekundären Speicherort nicht durch ein Kennwort geschützt wird.

So benutzen Sie Dual-Destination:

1. Aktivieren Sie das Kontrollkästchen **Dual-Destination benutzen**.
2. Wählen Sie den sekundären Zielspeicherort oder tragen Sie den vollen Pfad dahin manuell ein.
3. Klicken Sie auf **OK**.

Sie müssen möglicherweise die Anmeldedaten für den Zugriff auf den sekundären Speicherort angeben. Tragen Sie die Anmeldeinformation nach Aufforderung ein.

Task-Startbedingungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option bestimmt das Programmverhalten, falls ein Backup-Task starten will (die eingestellte Zeit ist gekommen oder das spezifizierte Ereignis ist eingetreten), aber die Bedingung (oder eine der Bedingungen) nicht erfüllt ist. Weitere Informationen über Bedingungen finden Sie unter Planen (S. 85) und Bedingungen (S. 92).

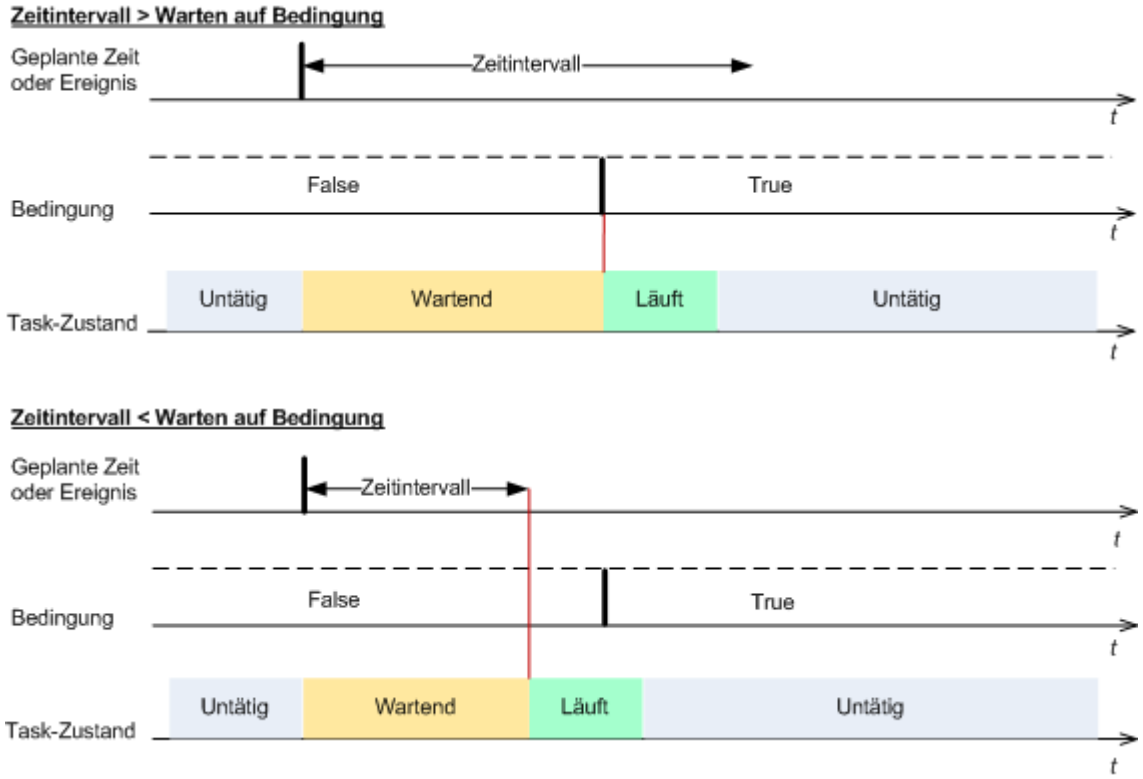
Voreinstellung ist: **Warten, bis die Bedingungen erfüllt sind.**

Warten, bis die Bedingungen erfüllt sind

Mit dieser Einstellung beginnt der Scheduler mit dem Überwachen der Bedingungen und schließt die Aufgabe ab, sobald die Bedingungen erfüllt sind. Wenn die Bedingungen nie erfüllt sind, wird der Task nie starten.

Um zu reagieren, wenn die Bedingungen für zu lange Zeit nicht erfüllt wurden und ein weiteres Verschieben des Backups zu riskant erscheint, können Sie einen Zeitabstand einstellen, nach dessen Ablauf der Task unabhängig von der Erfüllung der Bedingungen starten wird. Aktivieren Sie das Kontrollkästchen **Task trotzdem ausführen nach** und geben Sie dann den Zeitabstand an. Der Task wird starten, sobald die Bedingungen erfüllt sind ODER die Zeitspanne abgelaufen ist, je nachdem, was als Erstes eintritt.

Zeit-Diagramm: Warten, bis die Bedingungen erfüllt sind



Ausführung des Tasks übergehen

Das Verschieben eines Backups könnte nicht akzeptabel sein, wenn Sie z.B. ein Backup unbedingt zu einer angegebenen Zeit ausführen müssen. Dann macht es eher Sinn, das Backup zu übergehen, anstatt auf die Erfüllung der Bedingungen zu warten, besonders wenn die Ereignisse verhältnismäßig oft stattfinden.

Task-Fehlerbehandlung

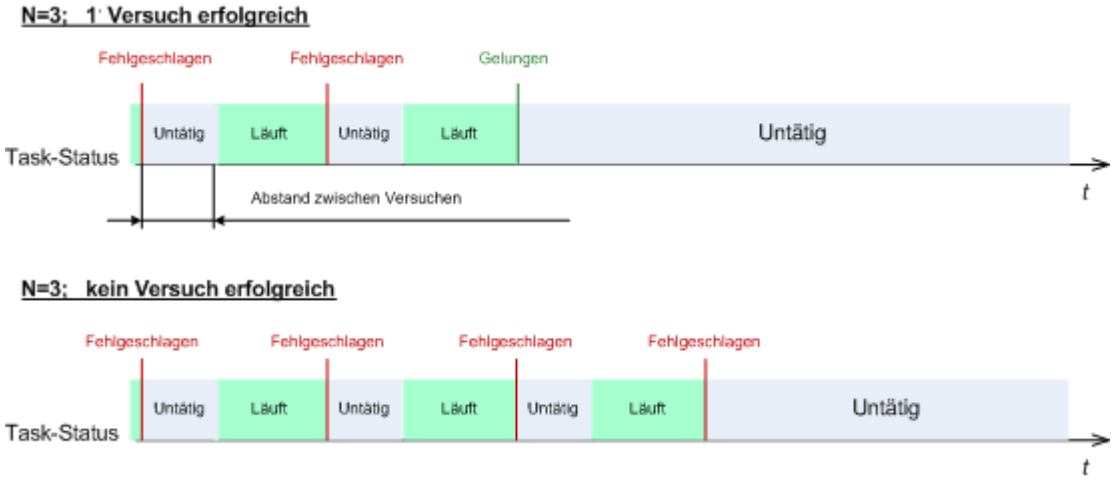
Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option bestimmt das Programmverhalten, wenn irgendein Task eines Backup-Plans versagt.

Die Voreinstellung ist **Fehlgeschlagenen Task nicht erneut starten.**

Wenn Sie das Kontrollkästchen **Fehlgeschlagenen Task erneut starten** aktivieren und die Anzahl der Versuche sowie den Zeitabstand zwischen den Versuchen angeben, versucht das Programm, den fehlgeschlagenen Task erneut zu starten. Die Versuche werden aufgegeben, wenn entweder die Aktion gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.



Wenn ein Task aufgrund eines Fehlers im Backup-Plan fehlgeschlagen ist, können Sie den Plan bearbeiten, während der Task untätig ist. Während der Task dagegen läuft, müssen Sie ihn stoppen, bevor Sie den Backup-Plan bearbeiten können.

Erweiterte Einstellungen

Spezifizieren Sie die zusätzlichen Einstellungen für das Backup durch Aktivieren oder Deaktivieren der folgenden Kontrollkästchen.

Überschreiben der Daten auf einem Band, ohne den Benutzer zur Bestätigung aufzufordern

Diese Option ist nur beim Backup auf ein Bandgerät wirksam.

Voreinstellung ist: **Ausgeschaltet**.

Wenn Sie ein Backup auf ein nicht leeres Band in einem lokal angeschlossenen Bandgerät starten, dann wird das Programm warnen, dass die Daten auf dem Band verloren gehen. Um diese Warnung unwirksam zu machen, aktivieren Sie dieses Kontrollkästchen.

Medien trennen, nachdem das Backup beendet ist

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option wirksam bei einem Backup auf Wechselmedien (CD, DVD, Band oder Diskette).

Voreinstellung ist: **Ausgeschaltet.**

Die Ziel-CD/DVD kann ausgeworfen oder das Band ausgehängt werden, nachdem das Backup abgeschlossen ist.

Beim Backup auf ein entfernbares Medium nach dem ersten Medium fragen

Diese Option ist nur beim Backup auf Wechselmedien wirksam.

Diese Option definiert, ob die Meldung **Legen Sie das erste Medium ein** erscheint, wenn Sie ein Wechselmedium zum Backup benutzen.

Voreinstellung ist: **Aktiviert**.

Bei eingeschalteter Option ist es unmöglich, ein Backup auf ein Wechselmedium auszuführen, wenn der Benutzer nicht anwesend ist, weil das Programm auf eine Bestätigung dieser Meldung wartet. Deshalb sollten Sie diese Meldung ausschalten, wenn ein geplanter Task eine Sicherung auf ein Wechselmedium vorsieht. Mit dieser Einstellung kann der Task unbeaufsichtigt erfolgen, wenn ein Wechselmedium beim Start gefunden wird (z.B. eine CD-R/W).

Archivattribut zurücksetzen

Diese Option ist nur für Backups auf Dateiebene unter Windows-Betriebssystemen und beim Arbeiten nach dem Start vom Boot-Medium wirksam.

Voreinstellung ist: **Ausgeschaltet**.

Im Betriebssystem Windows hat jede Datei ein Attribut **Datei kann archiviert werden**, das über **Datei** -> **Eigenschaften** -> **Allgemein** -> **Erweitert** -> **Archiv- und Indexattribute**verfügbar wird. Dieses Attribut, auch Archiv-Bit genannt, wird durch das Betriebssystem jedes Mal gesetzt, wenn die Datei verändert wurde, und kann durch Backup-Anwendungen zurückgesetzt werden, wenn die Datei in ein Backup auf Dateiebene eingeschlossen wird. Archiv-Bits werden durch viele Anwendungen benutzt, z.B. Datenbanken.

Wenn das Kontrollkästchen **Archivattribut zurücksetzen** aktiviert ist, wird Acronis Backup & Recovery 10 das Archivattribut aller im Backup enthaltenen Dateien zurückzusetzen. Acronis Backup & Recovery 10 selbst nutzt das Archiv-Bit aber nicht. Bei Ausführung eines inkrementellen oder differentiellen Backups wird die Änderung einer Datei anhand der Änderung der Dateigröße und von Tag bzw. Zeitpunkt der letzten Speicherung ermittelt.

Nach Abschluss des Backups die Maschine automatisch neu starten

Diese Option ist nur verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Voreinstellung ist: **Ausgeschaltet**.

Wenn die Option eingeschaltet ist, wird Acronis Backup & Recovery 10 die Maschine neu starten, nachdem der Backup-Prozess vollendet ist.

Wenn die Maschine standardmäßig z.B. von einer Festplatte bootet und Sie dieses Kontrollkästchen aktivieren, wird unmittelbar nach Abschluss eines Backups durch den bootfähigen Agenten die Maschine neu gestartet werden und das Betriebssystem booten.

Backup nur nach dem Übertragen zum Depot deduplizieren (keine Deduplizierung an der Quelle)

Diese Option ist nur in den Advanced Editions von Acronis Backup & Recovery 10 verfügbar.

Diese Option ist für Windows und Linux-Betriebssysteme und beim Arbeiten nach dem Start vom Boot-Medium wirksam, wenn das Ziel des Backups ein deduplizierendes Depot ist.

Voreinstellung ist: **Ausgeschaltet**.

Das Aktivieren dieser Option schaltet die Deduplizierung der Backups an der Quelle aus, d.h. die Deduplizierung erfolgt durch den Acronis Backup & Recovery 10 Strorage Node, nachdem das Backup im Depot abgelegt ist (auch Deduplizierung am Ziel genannt).

Das Abschalten der Deduplizierung an der Quelle führt zu einem schnelleren Backup-Prozess, aber auch zu größerem Datenverkehr über das Netzwerk und schwererer Last auf dem Storage Node. Die

resultierende Größe des Backups im Depot ist unabhängig davon, ob die Deduplizierung an der Quelle eingeschaltet ist oder nicht.

Die Funktionen Deduplizierung an der Quelle und Deduplizierung am Ziel sind beschrieben unter Deduplizierung – Überblick.

RAID- und LVM-Metadaten für Software zusammen mit Backups speichern

Diese Option ist nur wirksam für Disk-Backups von Maschinen, die unter Linux laufen.

Voreinstellung ist: **Aktiviert.**

Wenn diese Option aktiviert ist, speichert Acronis Backup & Recovery 10 vor Erstellen des Backups im Verzeichnis **/etc/Acronis** Informationen über die Struktur der logischen Volumes (so genannter LVM-Volumes) und der Linux RAID-Geräte (so genannter MD-Geräte).

Bei der Wiederherstellung von MD-Geräten und LVM-Volumes unter Verwendung von bootfähigen Medien kann anhand dieser Informationen die Volume-Struktur automatisch wiederhergestellt werden. Eine Anleitung finden Sie unter MD-Geräte und logische Volumes wiederherstellen (S. 179).

Vergewissern Sie sich bei Verwendung dieser Option, dass das Volume mit dem Verzeichnis **/etc/Acronis** beim Volume-Backup mit gesichert wird.

FTP im Modus 'Aktiv' verwenden

Voreinstellung ist: **Ausgeschaltet**.

Aktivieren Sie diese Option, wenn der FTP-Server den Modus 'Aktiv' unterstützt und Sie möchten, dass dieser Modus zur Dateiübertragung verwendet wird.

3.3.2 Standardoptionen für Recovery

Jeder Acronis Agent hat eigene Standardoptionen für Recovery. Sobald ein Agent installiert ist, haben die Standardoptionen vordefinierte Werte, die in der Dokumentation als **Voreinstellungen** bezeichnet werden. Bei Erstellung eines Recovery-Tasks können Sie entweder eine Standardoption verwenden oder diese mit einem benutzerdefinierten Wert überschreiben, der nur für diesen Task gültig ist.

Sie können außerdem auch eine Standardoption konfigurieren, indem Sie den vordefinierten Wert verändern. Der neue Wert wird dann als Standard für alle nachfolgend auf dieser Maschine erstellten Recovery-Tasks verwendet.

Um die Standardoptionen für Recovery einzusehen und zu verändern, verbinden Sie die Konsole mit der verwalteten Maschine und wählen dort aus dem Hauptmenü **Optionen –>Standardoptionen für Backup und Recovery –> Recovery-Standardoptionen**.

Verfügbarkeit der Recovery-Optionen

Art und Umfang der verfügbaren Recovery-Optionen sind abhängig von:

- der Umgebung, in der der Agent arbeitet (Linux, bootfähige Medien)
- dem Daten-Typ, der gesichert wird (Laufwerke, Dateien)
- Das Betriebssystem, das aus dem Disk-Backup wiederhergestellt wird

Die nachfolgende Tabelle fasst die Verfügbarkeit der Recovery-Optionen zusammen:

	Agent für Linux		Bootfähiges Medium (Linux-basiert oder PE-basiert)	
	Disk-Recovery	**Wiederherstellung von Dateien (auch aus Disk-Backup)**	**Disk-Recovery**	**Wiederherstellung von Dateien (auch aus Disk-Backup)**
Vor-/Nach-Befehle für Wiederherstellung (S. 69)	+	+	nur PE	nur PE
Recovery-Priorität (S. 71)	+	+	-	-
Sicherheit auf Dateiebene (S. 72):				
Dateien mit ihren Sicherheitseinstellungen wiederherstellen	-	+	-	+
Fehlerbehandlung (S. 74):				
Meldungen und Dialogboxen während der Aktion nicht zeigen (stiller Modus)	+	+	+	+
Neu versuchen, wenn ein Fehler auftritt	+	+	+	+
Erweiterte Einstellungen (S. 75):				
Aktuelles Datum und Zeit für wiederhergestellte Dateien verwenden	-	+	-	+
Backup-Archiv vor Wiederherstellung prüfen	+	+	+	+
Dateisystem nach Wiederherstellung prüfen	+	-	+	-
Maschine automatisch neu starten, wenn das für die Wiederherstellung erforderlich ist	+	+	-	-
SID nach Wiederherstellung ändern	Windows-Recovery	-	Windows-Recovery	-
Benachrichtigungen:				
E-Mail (S. 72)	+	+	-	-
Win Pop-up (S. 73)	+	+	-	-
Ereignisverfolgung:				
SNMP (S. 74)	+	+	-	-

Vor-/Nach-Befehle

Diese Option ist für Windows-, Linux-Betriebssysteme und das PE-Boot-Medium wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenwiederherstellung durchgeführt werden.

So benutzen Sie diese Vor- bzw. Nach-Befehle:

- Ausführen von `Checkdisk` für das Suchen und Beheben logischer Fehler im Dateisystem, physikalischer Fehler oder fehlerhafter Sektoren vor dem Start der Wiederherstellung oder nach deren Ende.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).

Ein Befehl wird nach der Wiederherstellung nicht ausgeführt, wenn die Wiederherstellung einen Neustart ausführt.

So spezifizieren Sie Vor-/Nach-Befehle

1. Sie aktivieren Vor-/Nach-Befehle mit Hilfe der folgenden Optionen:
   - **Vor Recovery ausführen**
   - **Nach Recovery ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.
   - Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.
3. Klicken Sie auf **OK**.

Befehl vor Recovery

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start der Wiederherstellung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	**Auswahl**			
Task scheitern lassen, wenn die Ausführung der Befehle fehlschlägt	Ausgewählt	Abgewählt	Ausgewählt	Abgewählt
Keine Wiederherstellung, bis die Befehlsausführung vollständig ist	Ausgewählt	Ausgewählt	Abgewählt	Abgewählt

Ergebnis				
	Voreinstellung Recovery nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Task scheitern lassen, wenn die Ausführung der Befehle fehlschlägt.	Recovery nach Ausführung des Befehls ausführen, unabhängig von Erfolg oder Misserfolg der Ausführung.	N/A	Recovery gleichzeitig mit der Befehlsausführung und unabhängig vom Ergebnis der Ausführung des Befehls ausführen.

Befehl nach Recovery

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn die Wiederherstellung vollständig ist

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei.
2. Spezifizieren Sie im Eingabeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wenn die erfolgreiche Ausführung des Befehls für Sie kritisch ist, dann aktivieren Sie das Kotrollkästchen **Task scheitern lassen, wenn die Ausführung der Befehle fehlschlägt**. Falls die Befehlsausführung fehlschlägt, wird das auch das Ergebnis der Ausführung des Tasks auf Fehlgeschlagen gesetzt.

   Wenn das Kontrollkästchen nicht ausgewählt ist, dann hat das Ergebnis der Befehlsausführung keinen Einfluss auf Erfolg oder Misserfolg des Tasks. Sie können das Ergebnis der Befehlsausführung durch Ansicht des Logs oder der Fehler und Warnungen verfolgen, die auf dem **Dashboard** dargestellt werden.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Ein Befehl wird nach der Wiederherstellung nicht ausgeführt, wenn die Wiederherstellung einen Neustart ausführt.

Recovery-Priorität

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Die Priorität eines jeden Prozesses, der in einem System läuft, hängt vom Grad der CPU-Benutzung und der Systemressourcen ab, die dem Prozess zugeordnet werden. Das Herabsetzen der Recovery-Priorität wird mehr Ressourcen für andere Anwendungen freisetzen. Das Heraufsetzen der Recovery-Priorität kann den Wiederherstellungsprozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren wie der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk.

Voreinstellung ist: **Normal.**

So spezifizieren Sie die Priorität des Recovery-Prozesses

Wählen Sie eine der nachfolgenden Varianten:

- **Niedrig** – minimiert die durch den Recovery-Prozess verwendeten Ressourcen und belässt mehr Ressourcen für andere Prozesse, die auf der Maschine laufen.
- **Normal** – führt den Recovery-Prozess mit normaler Geschwindigkeit aus und teilt die verfügbaren Ressourcen mit anderen Prozessen.
- **Hoch** – maximiert die Geschwindigkeit des Recovery-Prozesses und zieht Ressourcen von anderen Prozessen ab.

Sicherheit auf Dateiebene

Diese Option ist nur für Wiederherstellungen von Windows-Dateien auf Dateiebene wirksam.

Diese Option definiert, ob die NTFS-Zugriffsrechte für Dateien zusammen mit den Dateien wiederhergestellt werden.

Voreinstellung ist: **Dateien mit ihren Sicherheitseinstellungen wiederherstellen**.

Wenn die NTFS-Zugriffsrechte auf die Dateien während des Backups erhalten wurden, können Sie wählen, ob Sie die Zugriffsrechte wiederherstellen oder ob Sie die Erlaubnis erteilen, dass die Dateien die NTFS-Zugriffsrechte vom Ordner erben, in den sie wiederhergestellt werden.

Benachrichtigungen

Acronis Backup & Recovery 10 kann Sie über den Abschluss eines Backups per E-Mail oder Windows Nachrichtendienst (WinPopup, nur bei Windows XP) benachrichtigen.

E-Mail

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Die Option ermöglicht Ihnen den Erhalt von E-Mail-Benachrichtigungen zusammen mit dem vollständigen Log des Tasks über die erfolgreiche Vollendung von Recovery-Tasks, über Fehler oder über erforderliche Handlungen.

Voreinstellung ist: **Ausgeschaltet**.

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung schicken**, um die entsprechende Funktion zu aktivieren.
2. Geben Sie in das Feld **E-Mail-Adresse** die E-Mail-Adresse an, zu der die Benachrichtigung geschickt wird. Sie können auch durch Semikolons abgetrennt mehrere Adressen eingeben.
3. Aktivieren Sie unter **Benachrichtigungen senden** die Kontrollkästchen folgendermaßen:
   - **Wenn Backup erfolgreich vollendet ist** – Benachrichtigung wird gesendet, wenn das Backup erfolgreich abgeschlossen wurde.
   - **Wenn Backup fehlgeschlagen ist** – Benachrichtigung wird gesendet, wenn das Erstellen des Backups nicht erfolgreich war.

   Das Kontrollkästchen **Wenn eine Benutzeraktion erforderlich ist** ist immer aktiviert.
4. Aktivieren Sie das Kontrollkästchen **Vollständiges Log zur Benachrichtigung hinzufügen**, damit die E-Mail-Nachricht zum Backup gehörende Log-Einträge mit beinhalten wird.
5. Klicken Sie auf **Erweiterte E-Mail-Parameter**, um die nachfolgend erläuterten E-Mail-Parameter zu konfigurieren und klicken Sie dann auf **OK**:

- **Von** – geben Sie die E-Mail-Adresse des Benutzers ein, von dem die Nachricht verschickt wird. Wenn Sie dieses Feld leer lassen, werden die Nachrichten werden so konstruiert, als stammten sie von der Zieladresse.
- **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.
- Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:
  - **Posteingangssever (POP3)** – geben Sie den Namen des POP3-Servers an.
  - **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf 110 gesetzt.
  - **Benutzername** – geben Sie den Benutzernamen ein
  - **Kennwort** – geben Sie das Kennwort ein.
- Aktivieren Sie das Kontrollkästchen **Spezifizierten Postausgangsserver benutzen**, um einen SMTP-Server zu aktivieren und seine Einstellungen einzurichten:
  - **Postausgangsserver (SMTP)** – geben Sie den Namen des SMTP-Servers an.
  - **Port** – bestimmt den Port des SMTP-Servers. Standardmäßig ist der Port auf 25 gesetzt.
  - **Benutzername** – geben Sie den Benutzernamen ein.
  - **Kennwort** – geben Sie das Kennwort ein.

Klicken Sie auf **Test-Mail senden**, um die Richtigkeit der Einstellungen zu überprüfen.

Nachrichtendienst (WinPopup)

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Die Option ermöglicht Ihnen den Erhalt von WinPopup-Benachrichtigungen über die erfolgreiche Vollendung von Recovery-Tasks, über Fehler oder über erforderliche Handlungen.

Voreinstellung ist: **Ausgeschaltet.**

Vor Konfiguration der WinPopup-Benachrichtung sollten Sie sicherstellen, dass der Nachrichtendienst von Windows XP auf beiden Maschinen (die Task ausführende und die Nachrichten empfangende Maschine) gestartet ist.

In der Microsoft Windows Server 2003-Familie ist der Nachrichtendienst standardmäßig ausgeschaltet. Wechseln Sie den Startmodus des Dienstes auf Automatisch und starten Sie ihn dann.

So konfigurieren Sie WinPopup-Benachrichtigungen:

1. Aktivieren Sie das Kontrollkästchen **WinPopup-Benachrichtigung schicken**.
2. Geben Sie in das Feld **Maschinenname** den Namen der Maschine ein, an die die Benachrichtigungen verschickt werden. Multiple Namen werden nicht unterstützt.
3. Aktivieren Sie unter **Benachrichtigungen senden** die Kontrollkästchen folgendermaßen:
   - **Wenn Recovery erfolgreich vollendet ist** – Benachrichtigung wird gesendet, wenn der Recovery-Task erfolgreich abgeschlossen wurde.
   - **Wenn Recovery fehlgeschlagen ist** – Benachrichtigung wird gesendet, wenn die Wiederherstellung nicht erfolgreich war.

Das Kontrollkästchen **Wenn eine Benutzeraktion erforderlich ist** – Benachrichtigung wird gesendet, wenn während der Aktion das Eingreifen des Benutzers erforderlich ist – ist immer ausgewählt.

4. Klicken Sie auf **WinPopup-Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

Ereignisverfolgung

Es ist möglich, Ereignis-Logs von Recovery-Aktionen, die auf der verwalteten Maschine ausgeführt werden, an spezifizierte SNMP-Manager zu senden.

SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse von Recovery-Aktionen zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup & Recovery 10 siehe „Unterstützung für SNMP (S. 40)“.

Voreinstellung ist: **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind.**

So wählen Sie, ob Ereignisse von Recovery-Aktionen an SNMP-Manager geschickt werden:

Wählen Sie eine der folgenden Optionen:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen bei Optionen der Maschine (S. 46).
- **SNMP-Benachrichtigungen für Ereignisse bei Recovery-Aktionen einzeln senden** – für das Senden von SNMP-Benachrichtigungen mit den Ereignissen bei Recovery-Aktionen an spezifizierte SNMP-Manager.
  - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
  - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.
  - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist „public“.

  Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

Keine SNMP-Benachrichtigungen senden – Einstellung, um das Versenden von Ereignissen über Recovery-Aktionen an SNMP-Manager unwirksam zu machen.

Fehlerbehandlung

Diese Optionen sind für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Optionen ermöglichen Ihnen vorzugeben, wie auftretende Fehler beim Recovery behandelt werden.

Meldungen und Dialogboxen während der Aktion nicht zeigen (stiller Modus)

Voreinstellung ist: **Ausgeschaltet**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die eine Benutzeraktion erfordern, falls das möglich ist. Wenn eine Aktion ohne einen Benutzereingriff nicht fortsetzen kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

Bei Fehler neu versuchen

Voreinstellung ist: **Aktiviert**. **Zahl der Versuche: 5. Abstand zwischen Versuchen: 30 Sekunden.**

Wenn ein regenerierbarer Fehler auftritt, versucht das Programm erneut, die erfolglose Aktion durchzuführen. Sie können den Zeitabstand und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

Wenn der Speicherort im Netzwerk nicht verfügbar oder erreichbar ist, wird die Anwendung versuchen, den Ort alle 30 Sekunden erneut zu erreichen, aber nur fünf Mal. Die Versuche werden aufgegeben, wenn entweder die Verbindung gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

Erweiterte Einstellungen

Spezifizieren Sie die zusätzlichen Einstellungen für das Recovery durch Aktivieren oder Deaktivieren der folgenden Kontrollkästchen.

Aktuelles Datum und Zeit für wiederhergestellte Dateien verwenden

Diese Option ist nur wirksam, wenn Dateien wiederhergestellt werden.

Voreinstellung ist: **Aktiviert**.

Diese Option definiert, ob der Zeitstempel der wiederhergestellten Dateien aus dem Archiv übernommen wird oder ob den Dateien das aktuelle Datum und die aktuelle Zeit zugewiesen werden.

Backup vor Wiederherstellung validieren

Voreinstellung ist: **Ausgeschaltet**.

Diese Option definiert, ob ein Backup vor der Wiederherstellung der darin enthaltenen Daten zu validieren ist, um sicherzustellen, dass das Backup nicht beschädigt ist.

Dateisystem nach Wiederherstellung prüfen

Diese Option ist nur wirksam, wenn Festplatten oder Partitionen wiederhergestellt werden.

Diese Option ist beim Arbeiten nach dem Start vom Boot-Medium nicht für das NTFS-Dateisystem wirksam.

Voreinstellung ist: **Ausgeschaltet**.

Diese Option definiert, ob nach der Wiederherstellung einer Festplatte oder Partition die Integrität des wiederhergestellten Dateisystems geprüft wird.

Maschine automatisch neu starten, wenn für Wiederherstellung erforderlich

Diese Option ist wirksam, wenn die Wiederherstellung auf einer Maschine mit laufendem Betriebssystem erfolgt.

Voreinstellung ist: **Ausgeschaltet**.

Die Option definiert, ob die Maschine automatisch neu gestartet wird, wenn das für die Wiederherstellung erforderlich ist. Das dürfte der Fall sein, wenn eine Partition wiederhergestellt werden muss, die vom Betriebssystem gesperrt ist.

Maschine nach Wiederherstellung neu starten

Diese Option ist wirksam, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Voreinstellung ist: **Ausgeschaltet**.

Diese Option ermöglicht den Neustart der Maschine in das wiederhergestellte Betriebssystem ohne weitere Aktion eines Benutzers.

SID ändern, nachdem die Wiederherstellung abgeschlossen ist

Diese Option ist nicht wirksam, wenn die Wiederherstellung zu einer virtuellen Maschine mit dem Acronis Backup & Recovery 10 Agenten für ESX/ESXi oder dem Acronis Backup & Recovery 10 Agenten für Hyper-V durchgeführt wird.

Voreinstellung ist: **Ausgeschaltet**.

Acronis Backup & Recovery 10 kann für das wiederhergestellte System einen eindeutigen Security Identifier (SID) generieren. Sie benötigen keinen neuen SID, wenn Sie das System auf der gleichen Maschine wiederherstellen, von der das Image erstellt wurde, oder wenn Sie ein Duplikat erstellen, das das alte System ablöst. Generieren Sie einen neuen SID, wenn das originale und das wiederhergestellte System gleichzeitig in einer Arbeitsgruppe oder Domain arbeiten werden.

FTP im Modus 'Aktiv' verwenden

Voreinstellung ist: **Ausgeschaltet**.

Aktivieren Sie diese Option, wenn der FTP-Server den Modus 'Aktiv' unterstützt und Sie möchten, dass dieser Modus zur Dateiübertragung verwendet wird.

4 Depots

Ein Depot ist ein Ort zum Speichern von Backup-Archiven. Zur leichteren Nutzung und Administration ist ein Depot mit den Metadaten der Archive assoziiert. Auf diese Metadaten Bezug zu nehmen, macht Aktionen mit Archiven bzw. im Depot gespeicherten Backups schneller und bequemer.

Ein Depot kann auf einem lokalen oder einem Netzlaufwerk organisiert sein, wie auch auf einem abtrennbaren Medium oder einem Bandgerät, das an den Acronis Backup & Recovery 10 Storage Node angeschlossen ist.

Es gibt keine Limits für die Größe eines Depots oder die Zahl der Backups in einem Depot. Sie können die Größe jedes Archivs durch Bereinigung begrenzen, aber die Gesamtgröße aller Archive in einem Depot wird nur durch die Größe des Speichers selbst begrenzt.

Warum sollten Sie ein Depot erstellen?

Es wird empfohlen, dass Sie ein Depot an jedem Zielort erstellen, wo Sie Backup-Archive speichern werden. Das erleichtert Ihre Arbeit auf folgende Weise.

Schneller Zugriff auf ein Depot

Sie müssen sich niemals Pfade zu Ordnern merken, in denen die Archive gespeichert werden. Beim Erstellen eines Backup-Plans oder eines Tasks, der die Wahl eines Archivs bzw. eines Archiv-Zielortes benötigt, ist die Depot-Liste zum schnellen Zugriff verfügbar, damit Sie den Verzeichnisbaum nicht durchsuchen müssen.

Leichte Verwaltung der Archive

Sie können auf ein Depot aus dem Fensterbereich **Navigation** zugreifen. Wenn Sie ein Depot ausgewählt haben, können Sie die dort gespeicherten Archive durchsuchen und mit ihnen die folgenden Verwaltungsaktionen durchführen:

- eine Liste der in jedem Archiv enthaltenen Backups einsehen
- Daten aus einem Archiv wiederherstellen
- den Inhalt eines Backups zu untersuchen
- alle oder bestimmte Archive bzw. Backups in dem Depot validieren
- ein Partitions-Backup zu mounten, um Dateien aus dem Backup auf eine physikalische Platte zu kopieren
- Archive und Backups aus Archiven sicher zu löschen.

Die Erstellung von Depots ist zwar sehr empfehlenswert, aber nicht obligatorisch. Sie können auf die Verwendung von Shortcuts verzichten und stattdessen immer den vollständigen Pfad zum Archiv-Depot angeben. Alle oben beschriebenen Aktionen, mit Ausnahme der Löschung von Archiven und Backups, können auch ohne die Erstellung von Depots durchgeführt werden.

Das Erstellen eines Depots resultiert schließlich darin, dass sein Name zum Abschnitt **Depots** im Fensterbereich **Navigation** hinzugefügt wird.

Arbeitsmöglichkeiten mit der Ansicht „Depot“

 **Depots** (im Fensterbereich „Navigation“) – oberstes Element des Verzeichnisbaums „Depots“. Klicken Sie auf dieses Element, um die Gruppen zentraler und persönlicher Depots zu sehen.

Persönlich. Diese Gruppe ist verfügbar, wenn die Konsole mit einer verwalteten Maschine verbunden ist. Erweitern Sie diese Gruppe, damit eine Liste persönlicher, auf der verwalteten Maschine erstellter Depots angezeigt wird.

Klicken Sie auf ein persönliches Depot im Depot-Verzeichnisbaum, um eine Detailansicht dieses Depots (S. 78) zu öffnen und führen Sie dann Aktionen mit dem Depot (S. 80) bzw. den dort gespeicherten Archiven (S. 81) und Backups (S. 82) aus.

4.1 Persönliche Depots

Ein Depot wird als persönlich bezeichnet, wenn es durch direkte Verbindung der Konsole zu einer verwalteten Maschine erstellt wurde. Persönliche Depots sind spezifisch für jede verwaltete Maschine. Persönliche Depots sind für jeden Benutzer sichtbar, der sich am System anmelden kann. Die Berechtigungen eines Benutzers, Backups zu einem persönlichen Depot durchzuführen, werden über die Zugriffsrechte definiert, die dieser Benutzer für den Ordner bzw. das Gerät hat, wo das Depot gespeichert ist.

Ein persönliches Depot kann auf Netzwerkfreigaben, FTP-Servern, Wechselmedien, dem Acronis Online Backup Storage, Bandgeräten oder auf einem für die Maschine lokalen Laufwerk organisiert werden. Die Acronis Secure Zone wird als persönliches Depot betrachtet, das für alle Benutzer verfügbar ist, die sich am System anmelden können. Persönliche Depots werden automatisch erstellt, wenn Sie Backups zu einem der oberen Speicherorte durchführen.

Persönliche Depots können von lokalen Backup-Plänen bzw. Tasks verwendet werden. Zentrale Backup-Pläne können, mit Ausnahme der Acronis Secure Zone, keine persönlichen Depots verwenden.

Persönliche Depots erstellen

Mehrere Maschinen können sich auf denselben physikalischen Speicherort beziehen, beispielsweise auf denselben freigegebenen Ordern. Jede dieser Maschinen hat im Verzeichnisbaum **Depots** jedoch ihre eigene Verknüpfung. Benutzer, die ein Backup zu einem gemeinsam genutzten Ordner durchführen, können die Archive anderer Benutzer sehen und verwalten, abhängig von ihren Zugriffsberechtigungen für diesen Ordner. Um die Identifikation von Archiven zu erleichtern, hat die Ansicht **Persönliches Depot** die Spalte **Besitzer**, die den Besitzer eines jeden Archivs zeigt. Um mehr über das Konzept der Besitzer zu erfahren, siehe Besitzer und Anmeldedaten (S. 23).

Metadaten

In jedem persönlichen Depot wird bei Backup-Durchführung ein Ordner namens **.meta** erstellt. Dieser Ordner enthält zusätzliche Informationen über die im Depot gespeicherten Archive und Backups, wie z.B. die Besitzer der Archive oder den Maschinen-Namen. Sollten Sie den .meta-Ordner einmal versehentlich löschen, dann wird er automatisch neu erstellt, sobald Sie das nächste Mal auf das Depot zugreifen. Einige Informationen, wie Besitzer- oder Maschinen-Namen, können jedoch verloren gehen.

4.1.1 Mit der Ansicht „Persönliches Depot“ arbeiten

Dieser Abschnitt beschreibt kurz die Hauptelemente der Ansicht **Persönliches Depot** und macht Vorschläge, wie Sie damit arbeiten können.

Depot-Symbolleiste

Die Symbolleiste enthält einsatzbereite Schaltflächen, um mit dem gewählten persönlichen Depot Aktionen auszuführen. Zu Details siehe den Abschnitt Aktionen für persönliche Depots (S. 80).

Tortendiagramm mit Beschriftung

Das **Tortendiagramm** ermöglicht Ihnen, die Auslastung des Depots einzuschätzen. Es zeigt das Verhältnis von freiem und belegtem Platz im Depot an.

– Freier Platz: Platz auf dem Speichergerät, auf dem das Depot hinterlegt ist. Wenn das Depot z.B. auf einer Festplatte liegt, dann entspricht der freie Platz des Depots dem freien Platz der entsprechenden Partition.

– Belegter Platz: Gesamtgröße der Backup-Archive und ihrer Metadaten, sofern im Depot lokalisiert. Andere, von einem Benutzer möglicherweise in diesem Ordner hinterlegte Dateien werden nicht mitgezählt.

Die **Legende** zeigt die folgenden Informationen über das Depot an:

- vollständiger Pfad zum Depot
- Gesamtzahl der im Depot gespeicherten Archive und Backups
- das Verhältnis des belegten Speicherplatzes zur ursprünglichen Datengröße.

Inhalt des Depots

Der Abschnitt **Depot-Inhalt** enthält die Archiv-Tabelle und -Symbolleiste. Die Archiv-Tabelle zeigt die im Depot gespeicherten Archive und Backups an. Verwenden Sie die Archiv-Symbolleiste, um Aktionen mit den gewählten Archiven und Backups durchzuführen. Die Liste der Backups lässt sich durch Klicken auf das Plus-Zeichen erweitern, das links neben dem Archiv-Namen liegt. Alle Archive sind auf den folgenden Registerlaschen nach Typ gruppiert:

- Die Registerlasche **Disk-Archive** listet alle Archive auf, die Disk- bzw. Partitions-Backups (Images) enthalten.
- Die Registerlasche **Dateiarchive** listet alle Archive auf, die Datei-Backups enthalten.

Verwandte Abschnitte:

Aktionen mit im Depot gespeicherten Archiven (S. 81)

Aktionen mit Backups (S. 82)

Archive filtern und sortieren (S. 84)

Leisten des Fensterbereichs „Aktionen und Werkzeuge“

- **[Depot-Name]** Die Leiste **Aktionen** ist verfügbar, wenn Sie ein Depot im Depot-Verzeichnisbaum anklicken. Sie finden hier die gleichen Aktionen wie in der Depot-Werkzeugleiste.
- **[Archiv-Name]** Die Leiste **Aktionen** ist verfügbar, wenn Sie ein Archiv in der Archiv-Tabelle auswählen. Sie finden hier die gleichen Aktionen wie in der Archiv-Werkzeugleiste.
- **[Backup-Name]** Die Leiste **Aktionen** ist verfügbar, wenn Sie ein Archiv erweitern und auf eines seiner Backups klicken. Sie finden hier die gleichen Aktionen wie in der Archiv-Werkzeugleiste.

4.1.2 Auf persönliche Depots anwendbare Aktionen

Zugriff auf Aktionen

1. Verbinden Sie die Konsole mit dem Management Server.
2. Klicken Sie im Fensterbereich **Navigation** auf **Depots** –> **Persönlich**.

Alle hier beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Schaltflächen in der Depot-Symbolleiste ausgeführt. Sie können auf diese Aktionen auch über das Hauptmenüelement **[Depot-Name] Aktionen** zugreifen.

Anleitung zur Durchführung von Aktionen mit persönlichen Depots.

Aktion	Lösung
Persönliche Depots erstellen	Klicken Sie auf **Erstellen**. Die Prozedur zum Erstellen persönlicher Depots wird ausführlich im Abschnitt Ein persönliches Depot erstellen (S. 80) beschrieben.
Ein Depot bearbeiten	1. Wählen Sie das Depot. 2. Klicken Sie auf **Bearbeiten**. Auf der Seite **Persönliches Depot bearbeiten** können Sie den Depotnamen sowie die Informationen im Feld **Kommentare** bearbeiten.
Benutzerkonto für den Zugriff auf ein Depot ändern	Klicken Sie auf **Benutzer ändern**. Geben Sie im erscheinenden Dialogfenster die für den Zugriff auf das Depot benötigten Anmeldedaten ein.
Acronis Secure Zone erstellen	Klicken Sie auf **Acronis Secure Zone erstellen**. Die Prozedur zur Erstellung der Acronis Secure Zone ist ausführlich im Abschnitt Acronis Secure Zone erstellen (S. 166) erläutert.
Den Inhalt eines Depots durchsuchen	Klicken Sie auf **Durchsuchen**. Untersuchen Sie den gewählten Depot-Inhalt im erscheinenden Explorer-Fenster.
Ein Depot validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite Validierung (S. 151) mit dem bereits als Quelle vorausgewählten Depot. Die Validierung des Depots überprüft alle in diesem Ordner gespeicherten Archive.
Ein Depot löschen	Klicken Sie auf **Löschen**. Tatsächlich entfernt die Löschaktion aus der Ansicht **Depots** nur die Verknüpfung zum entsprechenden Ordner. Der Ordner selbst bleibt unberührt. Sie haben die Möglichkeit, die im Ordner enthaltenen Archive zu behalten oder zu löschen.
Die Informationen der Depot-Tabelle aktualisieren	Klicken Sie auf **Aktualisieren**. Während Sie den Inhalt eines Depots einsehen, können Archive dem Depot hinzugefügt, aus diesem gelöscht oder modifiziert werden. Klicken Sie auf **Aktualisieren**, damit die neuesten Veränderungen für die Depot-Informationen berücksichtigt werden.

Ein persönliches Depot erstellen

So erstellen Sie ein persönliches Depot

1. Geben Sie im Feld **Name** die Bezeichnung für das zu erstellende Depot ein.

2. [Optional] Geben Sie im Feld **Kommentare** eine Beschreibung für das Depot ein.
3. Klicken Sie im Feld **Pfad** auf **Ändern...**
   Spezifizieren Sie im Fenster **Pfad zum persönlichen Depot** das Verzeichnis, das als Depot verwendet wird. Ein persönliches Depot kann auf abnehmbaren oder entfernbaren Medien, auf einem Netzanteil, oder auf FTP organisiert werden.
4. Klicken Sie auf **OK**. Als Ergebnis erscheint das erstellte Depot in der Gruppe **Persönlich** des Depot-Verzeichnisbaums.

Persönliche Depots zusammenführen und verschieben

Was ist, wenn ich ein existierendes Depot von einem Ort zu einem anderen verschieben muss?

Verfahren Sie wie folgt:

1. Stellen Sie sicher, dass kein Backup-Plan das betreffende Depot beim Verschieben der Dateien verwendet oder deaktivieren Sie temporär (S. 107) die Automatik entsprechender Pläne.
2. Verschieben Sie das Depot-Verzeichnis mit all seinen Archiven manuell, unter Verwendung des Datei-Managers eines anderen Herstellers.
3. Ein neues Depot erstellen.
4. Bearbeiten Sie die Backup-Pläne und Tasks: Stellen Sie ihre Zielortangaben auf das neue Depot um.
5. Löschen Sie das alte Depot.

Wie kann ich zwei Depots zusammenführen?

Angenommen, Sie benutzen zwei Depots, *A* und *B*. Beide Depots werden von Backup-Plänen verwendet. Sie entscheiden, nur Depot *B* zu behalten, indem Sie alle Archive aus Depot *A* dorthin verschieben.

Zur Umsetzung verfahren Sie wie folgt:

1. Stellen Sie sicher, dass kein Backup-Plan das Depot *A* während der Zusammenführung verwendet oder deaktivieren Sie temporär (S. 107) die Automatik betreffender Pläne.
2. Verschieben Sie die Archive zum Depot *B* manuell unter Verwendung des Datei-Managers eines anderen Herstellers.
3. Bearbeiten Sie die Backup-Pläne, die das Depot *A* benutzen: Stellen Sie die Zielortangaben auf Depot *B* um.
4. Wählen Sie im Depot-Verzeichnisbaum das Depot *B* aus, um zu überprüfen, dass die Archive angezeigt werden. Wenn nicht, klicken Sie auf **Aktualisieren**.
5. Löschen Sie das Depot *A*.

4.2 Übliche Aktionen

4.2.1 Aktionen mit im Depot gespeicherten Archiven

Um mit einem Archiv eine beliebige Aktion durchzuführen, müssen Sie es zuerst auswählen. Wenn das Archiv mit einem Kennwort geschützt ist, werden Sie aufgefordert, dieses Kennwort einzugeben.

Alle nachfolgend beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Schaltflächen in der Symbolleiste ausgeführt. Sie können außerdem auf diese Aktionen zugreifen,

indem Sie die **[Archiv-Name] Aktionen**-Leiste (im Bereich **Aktionen und Werkzeuge**) bzw. das entsprechende Element **[Archiv-Name] Aktionen** im Hauptmenü verwenden.

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Archiven, die in einem Depot gespeichert sind.

Aktion	Lösung
Ein Archiv validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite **Validierung (S. 151) mit bereits als Quelle vorausgewählten Archiv.** Die Validierung eines Archivs überprüft die Gültigkeit aller Backups im Archiv.
Ein Archiv exportieren	Klicken Sie auf **Export**. Darauf öffnet sich die Seite **Export** (S. 159) mit dem vorausgewählten Archiv als Quelle. Beim Export wird ein Duplikat des Archivs einschließlich aller enthaltenen Backups am von Ihnen angegebenen Speicherort erstellt.
Ein einzelnes oder mehrere Archive löschen	1. Wählen Sie ein oder mehrere Archive, die Sie löschen wollen. 2. Klicken Sie auf **Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backup-Löschung** (S. 83), welches Kontrollkästchen für jedes Archiv bzw. Backup hat. Überprüfen Sie die Auswahl und korrigieren Sie diese, sofern nötig (aktivieren Sie das Kontrollkästchen für ein gewünschtes Archiv), danach bestätigen Sie die Löschaktion.
Alle Archive in einem Depot löschen	Beachten Sie, dass Sie nicht den gesamten Depot-Inhalt sehen, wenn auf die Depot-Liste ein Filter angewendet wurde. Stellen Sie sicher, dass das Depot keine zu bewahrenden Archive enthält, bevor Sie die Aktion starten. Klicken Sie auf **Alle Löschen**. Das Programm dupliziert Ihre Wahl in einem neuen Fenster, welches für jedes Archiv bzw. Backup Kontrollkästchen hat. Überprüfen Sie Ihre Wahl und korrigieren Sie diese falls nötig, bestätigen Sie dann die Löschaktion.

4.2.2 Aktionen mit Backups

Um mit einem Backup eine beliebige Aktion durchzuführen, müssen Sie es zuerst auswählen. Zur Wahl eines Backups erweitern Sie das Archiv und klicken dann auf das gewünschte Backup. Wenn das Archiv mit einem Kennwort geschützt ist, werden Sie aufgefordert, dieses Kennwort einzugeben.

Alle nachfolgend beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Schaltflächen in der Symbolleiste ausgeführt. Sie können auf diese Aktionen zugreifen, indem Sie die Leiste **[Backup-Name] Aktionen** (im Bereich **Aktionen und Werkzeuge**) bzw. das entsprechende Element **[Backup-Name] Aktionen** im Hauptmenü verwenden.

Nachfolgend finden Sie eine Anleitung, wie Sie Aktionen mit Backups durchführen.

Aktion	Lösung
Inhalt eines Backups in einem separaten Fenster einsehen	Klicken Sie auf **Inhalt anzeigen**. Überprüfen Sie im Fenster **Backup-Inhalt** die entsprechend angezeigte Information.
Recovery	Klicken Sie auf **Recovery**. Sie gelangen zur Seite **Daten wiederherstellen** mit dem bereits als Quelle

	vorausgewählten Backup.
Ein Backup validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite **Validierung (S. 151) mit dem bereits als Quelle vorausgewählten Backup. Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien eines Backups an einen virtuellen Zielort. Die Validierung eines Disk-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist.**
Ein Backup exportieren	Klicken Sie auf **Export**. Darauf öffnet sich die Seite **Export** (S. 159) mit dem vorausgewählten Backup als Quelle. Beim Export wird ein neues Archiv mit einer unabhängigen Kopie des Backups am von Ihnen angegebenen Speicherort erstellt.
Ein einzelnes oder mehrere Backups löschen	Wählen das gewünschte Backup und klicken Sie dann auf **Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backup-Löschung** (S. 83), welches Kontrollkästchen für jedes Archiv bzw. Backup hat. Überprüfen Sie die Auswahl und korrigieren Sie diese, sofern nötig (aktivieren Sie das Kontrollkästchen für ein gewünschtes Backup), danach bestätigen Sie die Löschaktion.
Alle Archive und Backups in einem Depot löschen	Beachten Sie, dass Sie nicht den gesamten Depot-Inhalt sehen, wenn auf die Depot-Liste ein Filter angewendet wurde. Stellen Sie sicher, dass das Depot keine zu bewahrenden Archive enthält, bevor Sie die Aktion starten. Klicken Sie auf **Alle Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backup-Löschung** (S. 83), welches Kontrollkästchen für jedes Archiv bzw. Backup hat. Überprüfen Sie Ihre Wahl und korrigieren Sie diese falls nötig, bestätigen Sie dann die Löschaktion.

4.2.3 Archive und Backups löschen

Das Fenster **Backups löschen** zeigt dieselbe Registerlasche wie die Ansicht „Depots“, jedoch mit Kontrollkästchen für jedes Archiv und Backup. Das von Ihnen zum Löschen gewählte Archiv bzw. Backup ist entsprechend markiert. Überprüfen Sie das von Ihnen zum Löschen gewählte Archiv bzw. Backup. Wenn Sie noch weitere Archive und Backups löschen müssen, aktivieren Sie die entsprechenden Kontrollkästchen, klicken dann auf **Ausgewählte löschen** und bestätigen die Löschaktion.

In diesem Fenster vorhandene Filter stammen von der Archiv-Liste der Ansicht „Depots“. Wenn also Filter auf die Archiv-Liste angewendet wurden, werden hier nur die zu diesen Filtern korrespondierenden Archive und Backups angezeigt. Löschen Sie alle Filter-Felder, um den gesamten Inhalt zu sehen.

Was passiert, wenn ich ein Backup lösche, das als Basis für ein inkrementelles oder differentielles Backup dient?

Das Programm konsolidiert die beiden Backups, um die Archiv-Konsistenz zu wahren. Ein Beispiel: Sie löschen ein Voll-Backup, behalten aber das nächste inkrementelle. Die Backups werden zu einem einzelnen Voll-Backup kombiniert, welches das Datum des inkrementellen Backups erhält. Wenn Sie ein inkrementelles oder differentielles Backup aus der Mitte einer Kette löschen, wird der resultierende Backup-Typ inkrementell.

Machen Sie sich bewusst, dass Konsolidierung nur eine Methode und keine Alternative zur Löschung ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup enthalten, im bewahrten inkrementellen oder differentiellen Backup jedoch abwesend waren.

Das Depot sollte genügend Speicherplatz für während einer Konsolidierung erstellte temporäre Dateien haben. Aus einer Konsolidierung resultierende Backups sind immer maximal komprimiert.

4.2.4 Archive filtern und sortieren

Nachfolgend finden sie eine Anleitung zum Filtern und Sortieren von Archiven in der Archiv-Tabelle.

Aktion	Lösung
Backup-Archive nach beliebigen Spalten sortieren	Klicken Sie auf die Spaltenköpfe, um die Archive aufsteigend zu sortieren. Kicken Sie erneut auf den Spaltenkopf, um die Archive absteigend zu sortieren.
Archive nach Name, Besitzer oder Maschine filtern	Geben Sie den Namen des Archivs (oder den des Besitzers bzw. der Maschine) in das Feld unterhalb des entsprechenden Spaltenkopfes ein. Sie erhalten als Ergebnis eine Liste der Archive, deren Namen (oder Namen der Besitzer bzw. Maschinen) vollständig oder partiell mit dem eingegebenen Wert übereinstimmen.

Archiv-Tabelle konfigurieren

Standardmäßig werden in der Tabelle sieben Spalten angezeigt, weitere sind versteckt. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete anzeigen lassen.

Spalten anzeigen oder verbergen

1. Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, um das Kontextmenü zu öffnen. Die angehakten Menü-Elemente korrespondieren zu den in der Tabelle präsenten Spaltenköpfen.
2. Klicken Sie auf die Elemente, die Sie anzeigen bzw. verbergen wollen.

5 Planung

Der Acronis-Scheduler hilft dem Administrator, Backup-Pläne an die tägliche Firmenroutine und den Arbeitsstil eines jeden Angestellten anzupassen. Die Tasks der Pläne werden systematisch so gestartet, dass kritische Daten als sicher geschützt bewahrt werden.

Der Scheduler verwendet die lokale Zeit der Maschine, auf der der Backup-Plan existiert. Bevor Sie eine Planung erstellen, überprüfen Sie, ob die Datums- bzw. Zeit-Einstellungen der Maschine korrekt sind.

Planung

Sie müssen ein oder mehrere Ereignisse spezifizieren, um zu bestimmen, wann ein Task ausgeführt werden soll. Der Task wird gestartet, sobald eines der Ereignisse eintritt. Die Tabelle führt die unter einem Linux-Betriebssystem verfügbaren Ereignisse auf.

Ereignisse
Zeit: Täglich, Wöchentlich, Monatlich
Verstrichene Zeit, seit das letzte erfolgreiche Backup abgeschlossen wurde. (geben Sie die Zeitdauer an)
Systemstart

Bedingung

Nur bei Backup-Aktionen können Sie zusätzlich zu den Ereignissen eine oder mehrere Bedingungen angeben. Sobald eines der Ereignisse eintritt, überprüft der Scheduler die Bedingungen und führt den Task aus, falls die Bedingung erfüllt ist. Bei multiplen Bedingungen müssen diese alle gleichzeitig zusammentreffen, um die Task-Ausführung zu ermöglichen. Die Tabelle führt die unter einem Linux-Betriebssystem verfügbaren Bedingungen auf.

Bedingung: Task nur starten, wenn
Host des Speicherorts verfügbar ist
Laufzeit des Tasks sich innerhalb des spezifizierten Zeitintervalls befindet
Zeitperiode verstrichen ist, seit das letzte erfolgreiche Backup abgeschlossen wurde

Für den Fall, dass ein Ereignis eintritt, aber die Bedingung (oder eine von mehreren Bedingungen) nicht erfüllt ist, wird das Verhalten des Schedulers durch die Backup-Option Task-Startbedingungen (S. 64) definiert.

Was ist, wenn

- **Was ist, wenn ein Ereignis eintritt (und eine Bedingung, sofern vorhanden, erfüllt ist), während die Ausführung des vorherigen Tasks noch nicht abgeschlossen ist?**

  Das Ereignis wird ignoriert.
- **Was ist, wenn ein Ereignis eintritt, während der Scheduler auf die Bedingung wartet, die für das vorherige Ereignis benötigt wurde?**

  Das Ereignis wird ignoriert.
- **Was ist, wenn die Bedingung für eine sehr lange Zeit nicht erfüllt wird?**

Wird die Verzögerung eines Backups zu riskant, so können Sie die Bedingung erzwingen (den Benutzer anweisen, sich abzumelden) oder den Task manuell ausführen. Sie können, damit diese Situation automatisiert gehandhabt wird, ein Zeitintervall definieren, nachdem der Task unabhängig von der Bedingung ausgeführt wird.

5.1 Tägliche Planung

Tägliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine tägliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Alle: <...> Tag(e)	Stellen Sie eine bestimmte Anzahl von Tagen ein, an denen Sie den Task ausgeführt haben wollen. Stellen Sie z.B. „Alle 2 Tage“ ein, so wird der Task an jedem zweiten Tag gestartet.

Wählen Sie im Bereich **Task während des Tages ausführen...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.
Alle: <...> **Von: <...>** **Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls erneut gestartet wird. Stellen Sie z.B. die Task-Frequenz auf „Jede 1 Stunde“ von 10:00 Uhr bis 22:00 Uhr ein, so erlaubt dies dem Task, zwölfmal zu laufen: von 10:00 vormittags bis 22:00 abends innerhalb eines Tages.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Tagen.

Erweiterte Planungseinstellungen sind nur für Maschinen verfügbar, die auf einem Acronis Backup & Recovery 10 Management Server registriert sind. Um diese Einstellungen zu spezifizieren, klicken Sie auf **Ändern** im Bereich **Erweiterte Einstellungen**.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

„Einfache“ tägliche Planung

Führe den Task jeden Tag um 18:00 Uhr aus.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Tage.
2. Einmal: **18:00 Uhr**.
3. Wirksam:

   Von: **nicht eingestellt**. Der Task wird noch am selben Tag gestartet, sofern er vor 18:00 Uhr erstellt wurde. Wurde der Task nach 18:00 Uhr erstellt, dann wird er das erste Mal am nächsten Tag um 18:00 Uhr gestartet.

   Bis: **nicht eingestellt**. Der Task wird für eine unbegrenzte Zahl an Tagen ausgeführt.

„Drei-Stunden-Zeitintervall über drei Monate“-Planung

Den Task alle drei Stunden ausführen. Der Task startet an einem bestimmten Datum (z.B. 15. September 2009) und endet nach drei Monaten.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Tage.
2. Alle: **3** Stunden

   Von: **24:00 Uhr** (Mitternacht) bis: **21:00 Uhr** – der Task wird daher achtmal pro Tag mit einem Intervall von 3 Stunden ausgeführt. Nach der letzten täglichen Wiederholung um 21:00 Uhr kommt der nächste Tag und der Task startet erneut von Mitternacht.
3. Wirksam:

   Von: **15.09.2009**. Wenn der 15.09.2009 das aktuelle Datum der Task-Erstellung ist und z.B. 13:15 Uhr die Erstellungszeit des Tasks, dann wird der Task gestartet, sobald das nächste Zeitintervall kommt: um 15:00 Uhr in unserem Beispiel.

   Bis: **15.12.2009**. An diesem Datum wird der Task das letzte Mal ausgeführt, der Task selbst ist jedoch immer noch in der Ansicht **Tasks** verfügbar.

Mehrere tägliche Planungen für einen Task

Es gibt F_lle, in denen es f_r Sie notwendig sein kann, den Task mehrmals am Tag laufen zu lassen oder sogar mehrmals am Tag mit unterschiedlichen Zeitintervallen. Erw_gen Sie in diesen F_llen, einem Task mehrere Zeitplanungen hinzuzuf_gen.

Angenommen, der Task soll z.B. jeden dritten Tag ausgef_hrt werden, beginnend vom 20.09.2009, f_nfmal am Tag:

- Zuerst um 8:00 Uhr.
- das zweite Mal um 12:00 Uhr (mittags)
- das dritte Mal um 15:00 Uhr
- das vierte Mal um 17:00 Uhr
- das f_nfte Mal um 19:00 Uhr

Der offensichtliche Weg ist es, f_nf einfache Zeitplanungen hinzuzuf_gen. Wenn Sie eine Minute _berlegen, k_nnen Sie sich einen optimaleren Weg ausdenken. Wie Sie sehen, betr_gt das Zeitintervall zwischen der ersten und zweiten Task-Wiederholung 4 Stunden und zwischen der dritten, vierten und f_nften sind es 2 Stunden. F_r diesen Fall besteht die optimale L_sung darin, dem Task zwei Planungen hinzuzuf_gen.

Erste t_gliche Planung

1. Alle: **3** Tage.
2. Alle: **4** Stunden.

   Von: **08:00 Uhr** bis: **12:00 Uhr**.
3. Wirksam:

   Von: **20.09.2009**.

   Bis: **nicht eingestellt**.

Zweite t_gliche Planung

1. Alle: **3** Tage.
2. Alle: **2** Stunden.

   Von: **15:00 Uhr** bis: **19:00 Uhr**.
3. Wirksam:

Von: **20.09.2009**.

Bis: **nicht eingestellt**.

5.2 Wöchentliche Planung

Eine wöchentliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine wöchentliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Alle: <...> Woche (Wochen) am: <...>	Spezifizieren Sie eine gewisse Zahl von Wochen und die Wochentage, an denen Sie den Task ausführen wollen. Mit einer Einstellung z.B. alle **2** Wochen am **Montag** wird der Task am Montag jeder zweiten Woche ausgeführt.

Wählen Sie im Bereich **Task während des Tages ausführen...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.
Alle: <...> **Von: <...>** **Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls gestartet wird. Eine Task-Frequenz von z.B. jede **1** Stunde von **10:00 Uhr** bis **22:00 Uhr** erlaubt es dem Task, während eines Tages 12-mal von 10:00 bis 22:00 Uhr zu laufen.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Wochen.

Erweiterte Planungseinstellungen sind nur für Maschinen verfügbar, die auf einem Acronis Backup & Recovery 10 Management Server registriert sind. Um diese Einstellungen zu spezifizieren, klicken Sie auf **Ändern** im Bereich **Erweiterte Einstellungen**.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

„Ein Tag in der Woche“-Planung

Den Task jeden Freitag um 22:00 Uhr ausf_hren, beginnend mit einem bestimmten Datum (z.B. 14.05.2009) und nach sechs Monaten endend.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Woche(n) am: **Fr**.
2. Einmal: **22:00 Uhr**.
3. Wirksam:

   Von: **13.05.2009**. Der Task wird am n_chsten Freitag um 22:00 Uhr gestartet.

   Bis: **13.11.2009**. An diesem Datum wird der Task das letzte Mal ausgef_hrt, der Task selbst ist jedoch nach diesem Datum immer noch in der Task-Ansicht verf_gbar. (Wenn dieser Tag kein Freitag w_re, dann w_rde der Task zuletzt an dem Freitag ausgef_hrt werden, der vor diesem Datum liegt.)

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die „Ein Tag in der Woche“-Planung wird dem Voll-Backup hinzugef_gt, w_hrend die inkrementellen Backups zur werkt_glichen Ausf_hrung geplant werden. Zu weiteren Details siehe die Beispiele _ber vollst_ndige und inkrementelle Backups sowie Bereinigungen im Abschnitt Benutzerdefiniertes Backup-Schema (S. 133).

„Werktags“-Planung

Den Task jede Woche an Werktagen ausf_hren: von Montag bis Freitag. W_hrend eines Werktags startet der Task nur einmal um 21:00 Uhr.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Woche(n) am: **<Werktags>** – die Wahl des Kontrollk_stchens <Werktags> aktiviert automatisch die korrespondierenden Kontrollk_stchen (**Mo**, **Di**, **Mi**, **Do** und **Fr**) und l_sst die verbliebenen unver_ndert.
2. Einmal: **21:00 Uhr**.
3. Wirksam:

   Von: **leer**. Wenn Sie den Task z.B. am Montag um 11:30 Uhr erstellt haben, dann wird er am selben Tag um 21:00 Uhr gestartet. Wurde der Task z.B. am Freitag nach 21:00 Uhr erstellt, dann wird er das erste Mal am n_chsten Wochentag (in unserem Beispiel Montag) um 21:00 Uhr gestartet.

   Enddatum: **leer**. Der Task wird f_r eine unbegrenzte Anzahl an Wochen erneut gestartet.

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die „Wochentags“-Planung wird den inkrementellen Backups hinzugef_gt, w_hrend das Voll-Backup mit einer Ausf_hrung an einem Tag in der Woche geplant wird. Zu weiteren Details siehe die Beispiele _ber vollst_ndige und inkrementelle Backups sowie Bereinigungen im Abschnitt Benutzerdefiniertes Backup-Schema (S. 133).

Mehrere wöchentliche Planungen für einen Task

In F_llen, in denen der Task an verschiedenen Tagen der Woche mit verschiedenen Zeitintervallen ausgef_hrt werden muss, sollten Sie erw_gen, jedem gew_nschten Tag oder mehreren Tagen der Woche eine geeignete Planung zuzuweisen.

Angenommen, Sie m_ssen den Task mit der folgenden Planung ausf_hren:

- Montag zweimal, um 12:00 Uhr (mittags) und 21:00 Uhr
- Dienstag: alle 3 Stunden, von 9:00 bis 21:00 Uhr
- Mittwoch: alle 3 Stunden, von 9:00 bis 21:00 Uhr
- Donnerstag: alle 3 Stunden, von 9:00 bis 21:00 Uhr
- Freitag: zweimal, um 12:00 Uhr und 21:00 Uhr (d.h. wie am Montag)
- Samstag: einmal um 21:00 Uhr
- Sonntag: einmal um 21:00 Uhr

Durch Kombinieren der identischen Zeiten k_nnen die folgenden drei Planungen dem Task hinzugef_gt werden:

Erste Planung

1. Alle: **1** Woche(n) am: **Mo**, **Fr**.
2. Alle: **9** Stunden

   Von: **12:00 Uhr** bis: **21:00 Uhr**.

3. Wirksam:
   Von: **nicht eingestellt**.
   Bis: **nicht eingestellt**.

Zweite Planung

1. Alle **1** Woche(n) am: **Di**, **Mi**, **Do**.
2. Alle **3** Stunden
   Von **09:00 Uhr** bis **21:00 Uhr**.
3. Wirksam:
   Von: **nicht eingestellt**.
   Bis: **nicht eingestellt**.

Dritte Planung

1. Alle: **1** Woche(n) am: **Sa, So**.
2. Einmal: **21:00 Uhr**.
3. Wirksam:
   Von: **nicht eingestellt**.
   Bis: **nicht eingestellt**.

5.3 Monatliche Planung

Eine monatliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine monatliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Monate: <...>	Wählen Sie den/die Monat(e), in der/denen Sie den Task ausführen wollen.
Tage: <...>	Bestimmen Sie die spezifischen Tage des Monats, um an diesen den Task auszuführen. Sie können außerdem den letzten Tag eines Monats auswählen, unabhängig von seinem tatsächlichem Datum.
Am(Um): <...> <...>	Bestimmen Sie die spezifischen Tage der Wochen, um an diesen den Task auszuführen.

Wählen Sie im Bereich **Task während des Tages ausführen...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.
Alle: <...> **Von: <...>** **Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls gestartet wird. Eine Task-Frequenz von z.B. jede **1** Stunde von **10:00 Uhr** bis **22:00 Uhr** erlaubt es dem Task, während eines Tages 12-mal von 10:00 bis 22:00 Uhr zu laufen.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Monaten.

Erweiterte Planungseinstellungen sind nur für Maschinen verfügbar, die auf einem Acronis Backup & Recovery 10 Management Server registriert sind. Um diese Einstellungen zu spezifizieren, klicken Sie auf **Ändern** im Bereich **Erweiterte Einstellungen**.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

„Letzter Tag eines jeden Monats"-Planung

Den Task einmal um 22:00 Uhr am letzten Tag eines jeden Monats ausf_hren.

Die Parameter der Planung werden wie folgt eingestellt:

1. Monate: **<Alle Monate>**.
2. Tage: **Letzter**. Der Task wird am letzten Tag eines jeden Monats ausgef_hrt, ungeachtet seines tats_chlichen Datums.
3. Einmal: **22:00 Uhr**.
4. Wirksam:

   Von: **leer**.

   Bis: **leer**.

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die „Letzter Tag eines jeden Monats"-Planung wird den Voll-Backups hinzugef_gt, w_hrend die differentiellen Backups zur einmaligen Ausf_hrung pro Woche und inkrementelle an Wochentagen geplant werden. Zu weiteren Details siehe die Beispiele _ber monatliche vollst_ndige, w_chentliche differentielle und t_gliche inkrementelle Backups sowie zu Bereinigung im Abschnitt Benutzerdefiniertes Backup-Schema (S. 133).

„Jahreszeiten"-Planung

Den Task an allen Werktagen w_hrend der n_rdlichen Herbst-Jahreszeit von 2009 und 2010 ausf_hren. W_hrend eines Werktages wird der Task alle 6 Stunden von 0:00 (Mitternacht) bis 18:00 Uhr gestartet.

Die Parameter der Planung werden wie folgt eingestellt:

1. Monate: **September, Oktober, November**.
2. Am(Um): **<alle> <Werktage>**.
3. Alle: **6** Stunden.

   Von: **00:00 Uhr** bis: **18:00 Uhr**.
4. Wirksam:

   Von: **30.08.2009**. Tats_chlich wird der Task am ersten Werktag des Septembers gestartet. Durch Einstellung dieses Datums bestimmen Sie lediglich, dass der Task in 2009 gestartet werden muss.

   Bis: **01.12.2010**. Tats_chlich wird der Task am letzten Werktag des Novembers enden. Durch Einstellung dieses Datums bestimmen Sie lediglich, dass der Task in 2010 nicht fortgesetzt werden darf, nachdem der Herbst in der n_rdlichen Hemisph_re endet.

Mehrere monatliche Planungen für einen Task

In F_llen, in denen der Task an verschiedenen Tagen oder Wochen mit verschiedenen, vom Monat abh_ngigen Zeitintervallen ausgef_hrt werden muss, sollten Sie erw_gen, jedem gew_nschten Monat oder mehreren Monaten eine geeignete Planung zuzuweisen.

Angenommen, der Task tritt am 01.11.2009 in Kraft.

- W_hrend des n_rdlichen Winters l_uft der Task einmal um 22:00 Uhr an jedem Werktag.
- W_hrend des n_rdlichen Fr_hlings und Herbstes l_uft der Task alle 12 Stunden an allen Werktagen.
- W_hrend des n_rdlichen Sommers l_uft der Task an jedem 1. und 15. eines Monats um 22:00 Uhr.

Somit werden die folgenden drei Planungen dem Task hinzugef_gt:

Erste Planung

1. Monate: **Dezember**, **Januar**, **Februar**.
2. Am(Um): **<Alle> <An allen Werktagen>.**
3. Einmal: **22:00 Uhr**.
4. Wirksam:

   Von: **01.11.2009**.

   Bis: **nicht eingestellt**.

Zweite Planung

1. Monate: **M_rz**, **April**, **Mai**, **September**, **Oktober**, **November**.
2. Am(Um): **<Alle> <An allen Werktagen>**.
3. Alle: **12 Stunden**

   Von: **00:00 Uhr** bis: **12:00 Uhr**.
4. Wirksam:

   Von: **01.11.2009**.

   Bis: **nicht eingestellt**.

Dritte Planung

1. Monate: **Juni**, **Juli**, **August**.
2. Tage: **1**, **15**.
3. Einmal: **22:00 Uhr**.
4. Wirksam:

   Von: **01.11.2009**.

   Bis: **nicht eingestellt**.

5.4 Bedingungen

Bedingungen erweitern den Scheduler mit mehr Flexibilität und ermöglichen es, Backup-Tasks abhängig von gewissen Bedingungen auszuführen. Sobald ein spezifiziertes Ereignis eintritt (siehe den Abschnitt „Planung (S. 85)“ zur Liste verfügbarer Ereignisse), überprüft der Scheduler die angegebene Bedingung und führt den Task aus, sofern die Bedingung zutrifft.

Für den Fall, dass ein Ereignis eintritt, aber die Bedingung (oder eine von mehreren Bedingungen) nicht erfüllt ist, wird das Verhalten des Schedulers durch die Backup-Option **Task-Startbedingungen** (S. 64) definiert. Dort können Sie angeben, wie wichtig die Bedingungen für die Backup-Strategie sind:

- Bedingungen sind zwingend – setzt die Ausführung des Backup-Tasks auf Wartestellung, bis alle Bedingungen zutreffen.

- Bedingungen sind wünschenswert, aber die Ausführung eines Backup-Tasks hat höhere Priorität – setzt den Task für das angegebene Zeitintervall auf Wartestellung. Wenn das Zeitintervall vergeht und die Bedingungen immer noch nicht zutreffen, führe den Task auf jeden Fall aus. Mit dieser Einstellung handhabt das Programm automatisch Situationen, wenn Bedingungen eine zu lange Zeit nicht zutreffen und eine weitere Verzögerung des Backups unerwünscht ist.
- Startzeit des Backup-Tasks ist relevant – überspringe den Backup-Tasks, wenn die Bedingungen zu dem Zeitpunkt, wenn der Task gestartet werden soll, nicht zutreffen. Ein Überspringen der Task-Ausführung macht Sinn, wenn Sie Daten ganz genau zur angegebenen Zeit sichern müssen, insbesondere, wenn die Ereignisse relativ häufig sind.

Bedingungen sind nur bei Verwendung des benutzerdefinierten Backup-Schemas (S. 133) verfügbar. Bedingungen können für vollständige, inkrementelle und differentielle Backups separat konfigurieren werden.

Multiple Bedingungen hinzufügen

Multiple Bedingungen müssen gleichzeitig zutreffen, um eine Task-Ausführung zu ermöglichen.

5.4.1 Host des Speicherorts verfügbar ist

Gilt für: Windows, Linux

„Host des Speicherorts ist verfügbar“ bedeutet, dass die Maschine, die das Ziel zum Speichern von Archiven auf einem Netzlaufwerk bereithält, verfügbar ist.

Beispiel:

Eine Datensicherung zu einem Netzwerk-Speicherort wird werktags um 21:00 Uhr durchgeführt. Wenn der Speicherort des Hosts zu dem Zeitpunkt nicht verfügbar ist (z.B. wegen Wartungsarbeiten), überspringe das Backup und warte bis zum nächsten Werktag, um den Task zu starten. Es wird angenommen, dass der Backup-Task besser überhaupt nicht gestartet werden soll, statt fehlzuschlagen.

- Ereignis: **Wöchentlich**, alle **1** Woche(n) an **<Werktagen>**; einmal um **21:00 Uhr**.
- Bedingung: **Host des Speicherorts verfügbar ist**
- Task-Startbedingungen: **Ausführung des Tasks übergehen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und der Host des Speicherorts verfügbar ist, startet der Backup-Task zur rechten Zeit.

(2) Wenn es 21:00 Uhr wird, der Host im Augenblick aber nicht verfügbar ist, dann startet der Backup-Task am nächsten Werktag, sofern der Host des Speicherorts dann verfügbar ist.

(3) Wenn der Host des Speicherorts an Werktagen um 21:00 Uhr niemals verfügbar ist, startet auch der Task niemals.

5.4.2 Entspricht Zeitintervall

Gilt für: Windows, Linux

Beschränkt die Startzeit eines Backup-Tasks auf ein angegebenes Zeitintervall.

Beispiel

Eine Firma verwendet unterschiedliche Speicherorte auf demselben netzwerkangebundenen Speicher zur Sicherung von Benutzerdaten und Servern. Der Arbeitstag startet um 8:00 und endet um 17:00 Uhr. Die Benutzerdaten sollen gesichert werden, sobald der User sich abmeldet, aber nicht vor 16:30 Uhr und nicht später als 22:00 Uhr. Die Firmen-Server werden jeden Tag um 23:00 Uhr per Backup gesichert. Daher sollten alle Daten der Benutzer vorzugsweise vor dieser Zeit gesichert werden, um Netzwerk-Bandbreite frei zu machen. Indem Sie das obere Limit auf 22:00 Uhr setzen, wird angenommen, dass die Sicherung der Benutzerdaten nicht länger als eine Stunde benötigt. Wenn ein Benutzer innerhalb des angegebenen Zeitintervalls noch angemeldet ist oder sich zu irgendeiner anderen Zeit abmeldet – sichere keine Benutzerdaten, d.h. überspringe die Task-Ausführung.

- Ereignis: **Beim Abmelden**, Der folgende Benutzer: **Jeder Benutzer**.
- Bedingung: **Entspricht dem Zeitintervall** von **16:30 Uhr** bis **22:00 Uhr**.
- Task-Startbedingungen: **Ausführung des Tasks übergehen**.

Ergebnis:

(1) Wenn sich der Benutzer zwischen 16:30 Uhr und 22:00 Uhr abmeldet, wird der Backup-Task unmittelbar nach der Abmeldung gestartet.

(2) Wenn sich der Benutzer zu einer anderen Zeit abmeldet, wird der Task übersprungen.

Was ist, wenn...

Was ist, wenn ein Task-Ausführung für einen bestimmten Zeitpunkt geplant ist und dieser außerhalb des spezifizierten Zeitintervalls liegt?

Ein Beispiel:

- Ereignis: **Täglich**, alle **1** Tage; einmal um **15:00 Uhr**.
- Bedingung: **Entspricht dem Zeitintervall** von **18:00 Uhr** bis **23:59:59 Uhr**.

In diesem Fall hängt die Antwort auf die Frage, ob und wann der Task ausgeführt wird, von den Task-Startbedingungen ab:

- Wenn die Task-Startbedingungen **Ausführung des Tasks übergehen** lauten, dann wird der Task niemals laufen.
- Wenn die Task-Startbedingungen **Warten, bis die Bedingungen erfüllt sind** lauten und das Kontrollkästchen **Task trotzdem ausführen nach** *deaktiviert* ist, wird der Task (für 15:00 Uhr geplant) um 18:00 Uhr gestartet — dem Zeitpunkt, wenn die Bedingung erfüllt ist.
- Wenn die Task-Startbedingungen **Warten, bis die Bedingungen erfüllt sind** lauten und das Kontrollkästchen **Task trotzdem ausführen nach** mit z.B. einer Wartezeit von **1 Stunde** *aktiviert* ist, wird der Task (für 15:00 Uhr geplant) um 16:00 Uhr gestartet — dem Zeitpunkt, zu dem die Warteperiode endet.

5.4.3 Zeit seit letztem Backup

Gilt für: Windows, Linux

Ermöglicht Ihnen, einen Backup-Task auf Warteposition zu setzen, bis das angegebene Zeitintervall verstreicht, seit das letzte Backup erfolgreich fertiggestellt wurde.

Beispiel:

Den Backup-Task bei Systemstart ausführen, aber nur, wenn mehr als 12 Stunden seit dem letzten erfolgreichen Backup verstrichen sind.

- Ereignis: **Beim Start**, führt den Task beim Starten der Maschine aus.
- Bedingung: **Zeit seit dem letzten Backup**, Zeit seit dem letzten Backup: **12** Stunden.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Ergebnis:

(1) Wenn die Maschine neu gestartet wird, bevor seit Abschluss des letzten erfolgreichen Backup 12 Stunden verstrichen sind, dann wird der Scheduler warten, bis die 12 Stunden abgelaufen sind und dann den Task starten.

(2) Wenn die Maschine mindestens 12 Stunden nach Abschluss des letzten erfolgreichen Backups neu gestartet wird, dann wird der Backup-Task direkt ausgeführt.

(3) Wenn die Maschine niemals neu gestartet wird, wird auch der Task niemals ausgeführt. Sie können das Backup in der Ansicht **Backup-Pläne und Tasks** manuell starten, falls das nötig ist.

6 Direkte Verwaltung

In diesem Abschnitt werden die Aktionen behandelt, die unter Verwendung der direkten Verbindung zwischen Konsole und Agent mit einer verwalteten Maschine ausgeführt werden können. Der Inhalt dieses Abschnitts gilt für autonome und erweiterte Editionen (Advanced Editions) von Acronis Backup & Recovery 10.

6.1 Eine verwaltete Maschine administrieren

In diesem Abschnitt werden die Ansichten beschrieben, die über den Navigationsbaum einer mit der Konsole verbundenen verwalteten Maschine verfügbar werden und erklärt, wie Sie mit diesen Ansichten arbeiten.

6.1.1 Dashboard

Verwenden Sie das Dashboard, um auf einen Blick einschätzen zu können, ob die Daten einer Maschine sicher geschützt sind. Das Dashboard zeigt eine Zusammenfassung der Tätigkeiten des Acronis Backup & Recovery 10 Agenten und ermöglicht Ihnen, Probleme schnell zu identifizieren und zu lösen.

Warnungen

Der Bereich „Warnung“ informiert Sie über auf der Maschine vorgekommene Probleme und bietet Ihnen Wege zu ihrer Lösung oder Untersuchung an. Die kritischsten Ereignisse werden zuerst angezeigt. Sollte es zum gegebenen Zeitpunkt keinen Alarm oder Warnungen geben, so zeigt das Display „Kein Alarm oder keine Warnungen“.

Typen von Alarmmeldungen

Die untere Tabelle illustriert Alarmmeldungen, die Sie möglicherweise beobachten:

	Beschreibung	Vorschlag	Kommentar
	Fehlgeschlagene Tasks: X	Auflösen	**Auflösen** öffnet die Ansicht **Backup-Pläne und Tasks** mit fehlgeschlagenen Tasks, wo Sie die Ursache des Fehlers untersuchen können.
	Tasks, die Interaktion erfordern: X	Auflösen	Jedes Mal, wenn ein Task eine Benutzerinteraktion benötigt, zeigt das Dashboard eine Mitteilung darüber, welche Aktion ausgeführt werden muss (z.B. eine neue CD einlegen oder Stopp/Wiederholen/Ignorieren auf einen Fehler hin).
	Überprüfung der Lizenz für die aktuelle Edition fehlgeschlagen. X Tag(e) verbleiben, bis Software aufhört zu arbeiten. Stellen Sie sicher, dass Sie eine gültige Lizenz auf dem Acronis License Server haben.	Verbinden	Der Acronis Backup & Recovery 10 Agent stellt beim Start und dann alle 1-5 Tage (Standard ist 1 Tag) eine Verbindung mit dem Acronis License Server her, entsprechend der Konfigurationsparameter des Agenten. Wenn die Lizenzprüfung 1-60 Tage, entsprechend der Konfigurationsparameter des Agenten, nicht zum Erfolg führt (Standard ist 30

			Tage), hört der Agent auf zu arbeiten, bis eine Lizenzprüfung erfolgreich durchgeführt wurde.
	Kann Lizenzschlüssel für die aktuelle Edition seit x Tagen nicht überprüfen. Entweder ist der Acronis License Server nicht verfügbar oder die Daten des Lizenz-Schlüssels sind beschädigt. Überprüfen Sie die Verbindungsmöglichkeit zum Server und starten Sie den Acronis License Server, um die Lizenzen zu verwalten. Stellen Sie sicher, dass Sie eine gültige Lizenz auf dem Acronis License Server haben.	Verbinden	Acronis Backup & Recovery 10 ist gestoppt. In den letzten *X* Tagen war der Agent nicht in der Lage zu prüfen, ob seine Lizenz auf dem Acronis License Server verfügbar ist. Wahrscheinliche Ursache ist, dass der License Server nicht verfügbar ist. Sie sollten außerdem sicherstellen, dass die Lizenzen auf dem License Server auch vorhanden sind oder dass die Lizenz-Daten nicht beschädigt waren. Der Agent wird nach einer erfolgreichen Lizenz-Überprüfung wieder arbeiten.
	Testversion des Produkts läuft in *X* Tagen ab Stellen Sie sicher, dass Sie eine gültige Lizenz auf dem Acronis License Server haben.	Verbinden	Sobald die Testversion des Produktes installiert ist, beginnt das Programm mit dem Countdown der bis zum Verfall des Testzeitraums verbleibenden Tage.
	Testperiode ist vorüber. Starten Sie den Installer und geben Sie eine Lizenz für die Vollversion ein. Stellen Sie sicher, dass Sie eine gültige Lizenz auf dem Acronis License Server haben.	Verbinden	15-Tage-Testzeitraum ist abgelaufen. Geben Sie einen vollständigen Lizenz-Schlüssel ein.
	Depots mit wenig freiem Speicherplatz: X	Depots ansehen	**Depots anzeigen** bringt Sie zur Ansicht **Depots**, wo Sie Größe, freien Platz sowie Inhalt des Depots untersuchen können und notwendige Schritte zur Vergrößerung des freien Platzes vornehmen können.
	Bootfähiges Medium wurde nicht erstellt	Jetzt erstellen	Damit Sie ein Betriebssystem auch dann wiederherstellen können, wenn die Maschine nicht mehr bootfähig ist, müssen Sie: 1. die Systempartition (und sofern davon verschieden auch die Boot-Partition) per Backup sichern 2. wenigstens ein bootfähiges Medium (S. 188) erstellen. **Jetzt erstellen** startet den Bootable Media Builder (S. 193).
	Keine Backups erstellt seit *X* Tagen	Backup jetzt	Das Dashboard warnt Sie, dass seit einer relativ langen Zeitperiode keine Daten der Maschine gesichert wurden. **Backup jetzt** bringt Sie zur Seite **Einen Backup-Plan erstellen**, wo Sie die Backup-Aktion sofort konfigurieren und ausführen können. Zur Konfiguration des als kritisch angesehenen Zeitintervalls wählen Sie **Optionen –> Konsolen-Optionen –> Zeitbasierter Alarm**.

⚠	Keine Verbindung zum Management Server seit x Tagen	Maschinen anzeigen	Diese Art von Meldung kann auf einer Maschine erscheinen, die auf einem Management Server registriert ist. Das Dashboard warnt Sie, dass die Verbindung abgebrochen sein könnte oder der Server nicht verfügbar sein kann, mit der Folge, dass die Maschine nicht zentral verwaltet wird.

Aktivitäten

Mit Hilfe des Kalenders können Sie den Aktivitätsverlauf des Acronis Backup & Recovery 10 Agenten auf der Maschine durchsuchen. Klicken Sie mit der rechten Maustaste auf ein beliebiges hervorgehobenes Datum und wählen Sie **Log anzeigen**, um die Ereignisliste nach Datum gefiltert einzusehen.

Im Abschnitt **Anzeige** (zur Rechten des Kalenders) können Sie bestimmen, welche Aktivitäten hervorgehoben werden, in Abhängigkeit von Anwesenheit und Schwere der Fehler.

	Grund
Fehler	Hebe das Datum in Rot hervor, sofern mindestens ein Fehler-Eintrag in der Ereignisanzeige zu diesem Datum erscheint.
Warnungen	Hebe das Datum in Gelb hervor, sofern kein Fehler-, aber mindestens ein Warnungs-Eintrag an diesem Tag in der Ereignisanzeige erschienen ist.
Informationen	Hebe das Datum in Grün hervor, wenn an diesem Tag nur Informationen-Einträge erschienen sind (normale Aktivität).

Der Link **Aktuelles Datum wählen** führt eine Auswahl direkt zum aktuellen Datum.

Systemansicht

Zeigt zusammengefasste Statistiken von Backup-Plänen und -Tasks sowie kurze Informationen über das letzte Backup. Klicken Sie auf die Einträge dieses Bereiches, um die relevanten Informationen zu erhalten. Das führt Sie zur Ansicht **Backup-Pläne und Tasks** (S. 99) mit bereits vorgefilterten Plänen und Tasks. Ein Beispiel: Falls Sie unter **Backup-Pläne** auf **Lokal** klicken, so wird die Ansicht **Backup-Pläne und Tasks** mit einer Backup-Plan-Liste geöffnet, die nach der Herkunft **Lokal** gefiltert ist.

Tasks erfordern Interaktion

Dieses Fenster fasst alle Tasks zusammen, die einen Benutzereingriff benötigen. Es ermöglicht Ihnen, für jeden Task eine Entscheidung zu treffen, wie z.B. einen Neustart zu bestätigen oder einen Neuversuch nach Freigabe von Festplattenplatz durchzuführen. So lange wenigstens ein Task eine Interaktion erfordert, können Sie dieses Fenster jederzeit vom **Dashboard** (S. 96) der verwalteten Maschine öffnen.

Durch Aktivierung des Kontrollkästchens für den Parameter **Fenster nicht zeigen, wenn Tasks Benutzereingriff benötigen (Diese Information wird bei den Task-Details und im Dashboard sichtbar)** werden die Tasks auf dem **Dashboard** zusammen mit anderen Alarmmeldungen und Warnungen angezeigt.

Alternativ können Sie die Stadien der Task-Ausführung in der Ansicht **Backup-Pläne und Tasks** (S. 99) überprüfen und Ihre Entscheidung für jeden Task im Bereich **Informationen** treffen (oder im Fenster **Task-Details** (S. 107)).

6.1.2 Backup-Pläne und Tasks

Die Ansicht **Backup-Pläne und Tasks** informiert Sie über die Datensicherung auf einer gegebenen Maschine. Sie ermöglicht Ihnen, Backup-Pläne und Tasks zu überwachen und zu verwalten.

Ein Backup-Plan ist ein Satz mit Richtlinien für den Schutz der gegebenen Daten auf einer gegebenen Maschine. Physikalisch ist ein Backup-Plan ein Paket von Tasks, die für Ausführung auf einer verwalteten Maschine gestaltet werden. Sehen Sie unter Backup-Plan_Ausführungsstadium (S. 99) nach, um herauszufinden, was ein Backup-Plan auf einer Maschine gerade tut. Der Status eines Backup-Plans ist ein kumulativer Status der Tasks dieses Plans. Der Status eines Backup-Plans (S. 100) hilft Ihnen abzuschätzen, ob die Daten erfolgreich geschützt sind.

Ein Task ist ein Satz sequenzieller Handlungen, der auf einer verwalteten Maschine zu einer festgelegten Zeit oder beim Eintreten eines bestimmten Ereignisses ausgeführt wird. Um den aktuellen Fortschritt eines Tasks im Überblick zu halten, verfolgen Sie sein Stadium (S. 101). Prüfen Sie den Status (S. 102) eines Tasks, um sein Ergebnis in Erfahrung zu bringen.

Arbeitsweise

- Nutzen Sie Filter, um in der Backup-Plan-Tabelle die gewünschten Backup-Pläne (Tasks) zu sehen. Standardmäßig zeigt die Tabelle die Pläne der verwalteten Maschine nach Namen sortiert. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu Details siehe den Abschnitt Backup-Pläne und Tasks filtern und sortieren (S. 106).
- Wählen Sie in der Backup-Tabelle den Backup-Plan (Task).
- Verwenden Sie die Schaltflächen der Symbolleiste, um eine Aktion auf den gewählten Plan (Task) anzuwenden. Zu Details siehe den Abschnitt Aktionen für Backup-Pläne und Tasks (S. 103). Sie können erstellte Pläne und Tasks starten, bearbeiten, stoppen und löschen.
- Verwenden Sie die Leiste **Information**, um zu einem gewählten Plan (Task) detaillierte Informationen zu sehen. Die Leiste ist standardmäßig eingeklappt. Sie können die Leiste aufklappen, indem Sie auf das Chevron-Symbol klicken. Der Inhalt der Leiste ist außerdem in den Fenstern **Plan-Details** (S. 109) bzw. **Task-Details** (S. 107) dupliziert.

Stadien (Zustände) und Statusmeldungen verstehen

Ausführungszustände von Backup-Plänen

Ein Backup-Plan kann sich in einem der folgenden Ausführungsstadien befinden: **Untätig; Wartend; Läuft; Stoppt; Interaktion erforderlich**.

Die Bezeichnungen für Plan-Zustände sind dieselben wie für Task-Zustände, weil ein Plan-Zustand ein kumulativer Status aller Tasks eines Plans ist.

	Stadium	Grund	Handhabung
1	**Interaktion erforderlich**	Wenigstens ein Task benötigt einen Benutzereingriff. Andernfalls siehe Punkt 2.	Identifizieren Sie die Tasks, die eine Interaktion erfordern (das Programm zeigt an, was zu tun ist) -> Stoppen Sie die betreffenden Tasks oder ermöglichen Sie ihre Ausführung (wechseln Sie das Medium, sorgen Sie für zusätzlichen Platz im Depot, ignorieren Sie einen Lesefehler, erstellen Sie eine fehlende Acronis Secure Zone).
2	**Läuft**	Wenigstens ein Task wird ausgeführt. Andernfalls siehe Punkt 3.	Es ist keine Handlung nötig.

3	**Wartend**	Wenigstens ein Task befindet sich in Wartestellung. Andernfalls siehe Punkt 4.	Warten auf Bedingung. Diese Situation ist recht gängig, jedoch kann die zu lange Verzögerung eines Tasks riskant sein. Die Lösung kann in Definition einer maximalen Verzögerung oder Erzwingen der Bedingung liegen (den Benutzer zur Abmeldung auffordern, eine benötigte Netzwerk-Verbindung einschalten). In Wartestellung während ein anderer Task benötigte Ressourcen blockiert. Eine einmalige Warte-Situation kann entstehen, wenn ein Task-Start verzögert wird oder eine Task-Ausführung aus bestimmten Gründen wesentlich länger als gewöhnlich dauert und daher einen anderen Task in der Ausführung hindert. Diese Situation wird automatisch gelöst, wenn der blockierende Task seinen Abschluss findet. Erwägen Sie, einen zu lange festhängenden Task zu stoppen, um dem nachfolgenden den Start zu ermöglichen. Eine andauernde Überlappung von Tasks kann das Ergebnis inkorrekt angelegter Zeit- bzw. Backup-Pläne sein. In solchen Fällen macht es dann natürlich Sinn, den entsprechenden Plan zu editieren.
4	**Stoppend**	Wenigstens ein Task stoppt seine Ausführung. Andernfalls siehe Punkt 5.	Es ist keine Handlung nötig.
5	**Untätig**	Alle Tasks befinden sich in Ruhestellung.	Es ist keine Handlung nötig.

Backup-Plan-Zustände

Ein Backup-Plan kann sich in einem der folgenden Ausführungszustände befinden: **Fehler, Warnung, OK**.

Der Status eines Backup-Plans wird aus den Ergebnissen zusammengestellt, die die Tasks dieses Plans bei ihren letzten Ausführungen meldeten.

	Status	Grund	Handhabung
1	**Fehler**	Wenigstens ein Task ist fehlgeschlagen. Andernfalls siehe Punkt 2.	Identifizieren Sie die fehlgeschlagenen Tasks -> Überprüfen Sie die Task-Ereignismeldungen, um den Grund des Fehlers zu ermitteln und setzen Sie dann eine oder mehrere der nachfolgenden Lösungen um: ▪ Entfernen Sie den Grund des Fehlers. -> [optional] Starten Sie den gescheiterten Task manuell. ▪ Bearbeiten Sie den lokalen Plan, falls der Fehler bei ihm lag, um sein zukünftiges Versagen zu verhindern. ▪ Bearbeiten Sie die Backup-Richtlinie des Management Servers, falls ein zentraler Plan fehlgeschlagen ist. Bei Erstellung eines Backup-Plans oder einer Richtlinie kann der Administrator eine Option aktivieren, dass die Ausführung des Plan gestoppt werden soll, sobald er den Status „Fehler“ annimmt. Die Ausführung des Backup-Plans kann durch Verwendung der Schaltfläche „Neustart“ wieder aufgenommen werden.
2	**Warnung**	Wenigstens ein Task wurde mit Warnungen abgeschlossen.	Prüfen Sie den Log-Eintrag, um die Warnmeldung zu lesen. -> [optional] Führen Sie Aktionen aus, um zukünftige Warnungen bzw. Fehler zu verhindern.

		Andernfalls siehe Punkt 3.	
3	**OK**	Alle Tasks wurden erfolgreich abgeschlossen.	Es ist keine Handlung nötig. Beachten Sie, dass ein Backup-Plan auch in Fällen den Status „OK“ zeigen kann, wenn keiner der Tasks bisher gestartet wurde oder einige Tasks gestoppt sind bzw. gestoppt wurden. Diese Situationen werden als normal betrachtet.

Task-Stadien

Ein Backup-Task kann sich in einem der folgenden Ausführungszustände befinden: **Untätig**; **Wartend**; **Läuft**; **Stoppt**; **Interaktion erforderlich**. Das anfängliche Task-Stadium ist **Untätig**.

Sobald der Task manuell gestartet wurde oder das als Auslöser spezifizierte Ereignis eingetreten ist, wechselt der Task entweder in das Stadium **Läuft** oder **Wartend**.

Läuft

Ein Task wechselt in das Stadium **Läuft**, wenn das im Scheduler definierte Ereignis eintritt UND alle im Backup-Plan definierten Bedingungen zutreffen UND kein anderer Task läuft, der benötigte Ressourcen blockiert. In diesem Fall verhindert also nichts die Ausführung des Tasks.

Wartend

Ein Task wechselt in das Stadium **Wartend**, wenn er im Begriff ist zu starten und dabei jedoch bereits ein anderer, die gleichen Ressourcen benutzender Task ausgeführt wird. Das bedeutet im Einzelnen, dass auf einer Maschine nicht mehr als ein Backup- oder Recovery-Task simultan laufen kann. Genauso wenig ist es möglich, dass ein Backup- und ein Recovery-Task simultan laufen. Sobald der andere Task die Ressource freigibt, wechselt der wartende Task in das Stadium **Läuft**.

Ein Task kann außerdem in das Stadium **Wartend** wechseln, wenn das im Scheduler spezifizierte Ereignis zwar erfolgt, jedoch die im Backup-Plan definierten Bedingungen nicht erfüllt sind. Zu Details siehe Task-Startbedingungen (S. 64).

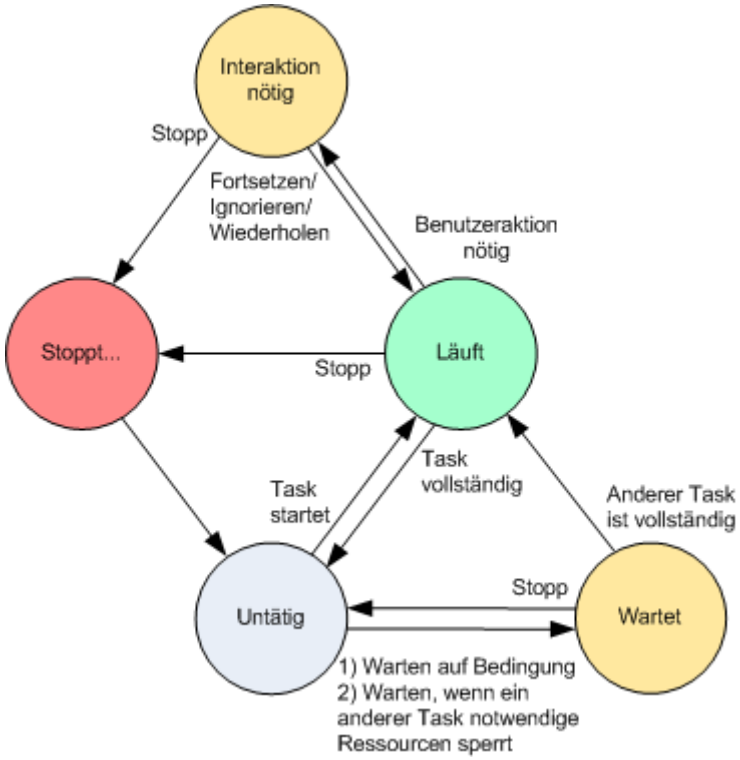
Interaktion erforderlich

Jeder laufende Task kann sich selbst in das Stadium **Interaktion erforderlich** versetzen, falls eine Benutzerinteraktion nötig ist, wie etwa ein Mediumwechsel oder das Ignorieren eines Lesefehlers. Das nächste Stadium kann **Stoppt** (falls der Benutzer den Stopp des Tasks wählt) sein oder **Läuft** (bei Wahl von Ignorieren/Wiederholen oder einer anderen Handlung, etwa Neustart, die den Task in das Stadium **Läuft** versetzen kann).

Stoppend

Der Benutzer kann einen gerade ablaufenden oder Interaktion anfordernden Task stoppen. Der Task wechselt darauf zuerst in das Stadium **Stoppt** und dann zu **Untätig**. Auch ein wartender Task kann gestoppt werden. Da der Task in diesem Fall nicht ausgeführt wird, bedeutet „Stoppt“, dass er aus der Warteschlange entfernt wird.

Diagramm der Task-Stadien



Zustände von Tasks

Ein Task kann sich in einem der folgenden Ausführungszustände befinden: **Fehler**; **Warnung**; **OK**.

Der Status eines Tasks wird aus dem Ergebnis der letzten Ausführung des Tasks ermittelt.

	Status	Grund	Handhabung
1	**Fehler**	Das letzte Ergebnis ist „Gescheitert“	Identifizieren Sie den fehlgeschlagenen Task. -> Überprüfen Sie die Task-Ereignismeldungen, um den Grund des Fehlers zu ermitteln und setzen Sie dann eine oder mehrere der nachfolgenden Lösungen um: ▪ Entfernen Sie den Grund des Fehlers. -> [optional] Starten Sie den gescheiterten Task manuell. ▪ Bearbeiten Sie den fehlgeschlagenen Task, um sein zukünftiges Misslingen zu verhindern. ▪ Bearbeiten Sie den lokalen Plan, falls der Fehler bei ihm lag, um sein zukünftiges Versagen zu verhindern. ▪ Bearbeiten Sie die Backup-Richtlinie des Management Servers, falls ein zentraler Plan fehlgeschlagen ist.
2	**Achtung**	Das letzte Ergebnis ist „Mit Warnungen abgeschlossen“	Prüfen Sie den Log-Eintrag, um die Warnmeldung zu lesen. -> [optional] Führen Sie Aktionen aus, um zukünftige Warnungen bzw. Fehler zu verhindern.
3	**OK**	Das letzte Ergebnis ist „Erfolgreich abgeschlossen“, „-“, oder „Gestoppt“	Es ist keine Handlung nötig. Das Stadium „-“ bedeutet, dass der Tasks nie gestartet wurde oder aber gestartet wurde, jedoch bisher nicht beendet wurde oder sein Ergebnis nicht verfügbar ist.

Mit Backup-Plänen und -Tasks arbeiten

Aktionen für Backup-Pläne und Tasks

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen für Backup-Pläne und Tasks.

Aktion	Lösung
Einen neuen Backup-Plan oder einen Task erstellen	Klicken Sie auf **Neu** und wählen Sie eine der folgenden Optionen: ▪ Backup-Plan (S. 113) ▪ Recovery-Task ▪ Validierungstask (S. 151)
Details eines Plans/Tasks einsehen	**Backup-Plan** Klicken Sie auf **Details anzeigen**. Überprüfen Sie dann im Fenster **Plan-Details** (S. 109) die entsprechenden Informationen. **Task** Klicken Sie auf **Details anzeigen**. Überprüfen Sie dann im Fenster **Task-Details** (S. 107) die entsprechenden Informationen.
Ereignisanzeige für Pläne/Tasks einsehen	**Backup-Plan** Klicken Sie auf **Log anzeigen**. Sie gelangen dadurch in die Ansicht **Log** (S. 110), die eine Liste der planbezogenen Log-Einträge enthält. **Task** Klicken Sie auf **Log anzeigen**. Sie gelangen dadurch in die **Log** (S. 110)-Ansicht, die eine Liste der Task-bezogenen Log-Einträge enthält.
Einen Plan/Task ausführen	**Backup-Plan** Klicken Sie auf **Ausführen**. Wählen Sie im Fenster **Backup-Plan ausführen** (S. 107) den zu startenden Task. Die Ausführung des Backup-Plans startet unmittelbar auch den dazugehörigen, ausgewählten Task, ungeachtet seiner Zeit-/Ereignis-Einstellungen und anderer Konditionen. *Warum kann ich einen Backup-Plan nicht ausführen?* ▪ Ihnen fehlen die dazugehörigen Berechtigungen. Ohne Administrator-Rechte kann ein Benutzer auf einer Maschine keine anderen Benutzern gehörenden Pläne ausführen. **Task** Klicken Sie auf **Ausführen**. Die Ausführung des Tasks startet unmittelbar, ungeachtet seiner Zeit-/Ereignis-Einstellungen und Bedingungen.

Einen Plan/Task stoppen	**Backup-Plan** Klicken Sie auf **Stopp**. Einen laufenden Backup-Plan zu stoppen bedeutet auch, alle seine Tasks zu stoppen. Daher werden alle Aktionen des Tasks abgebrochen. **Task** Klicken Sie auf **Stopp**. *Was passiert, wenn Sie einen Task stoppen?* Üblicherweise führt ein Stoppen des Tasks auch zum Abbruch seiner Aktionen (Backup, Wiederherstellung, Validierung, Export, Konvertierung, Migration). Der Task wechselt zuerst in das Stadium Stoppt und wird dann Untätig. Die Zeit-/Ereignis-Planung eines Tasks bleibt aber, sofern erstellt, weiter gültig. Um die Aktion abzuschließen, müssen Sie den Task erneut ausführen. ▪ Recovery-Task (von einem Festplatten-Backup): Die Ziel-Partition wird gelöscht und zu nicht zugeordnetem Speicher – Sie erhalten dasselbe Ergebnis, falls die Wiederherstellung fehlschlägt. Um die „verlorene“ Partition wiederherzustellen, müssen Sie den Task erneut ausführen. ▪ Recovery-Task (von einem Datei-Backup): Die abgebrochene Aktion kann zu Veränderungen im Zielordner führen. Manche Dateien werden möglicherweise wiederhergestellt, andere nicht, abhängig vom Zeitpunkt, wann Sie den Task gestoppt haben. Um alle Dateien wiederherzustellen, müssen Sie den Task erneut ausführen.

Einen Plan/Task editieren	**Backup-Plan** Klicken Sie auf **Bearbeiten**. Die Bearbeitung eines Backup-Plans wird auf dieselbe Art durchgeführt wie das Erstellen (S. 113), mit Ausnahme folgender **Einschränkungen**: Beim Bearbeiten eines Backup-Plans ist es nicht immer möglich, alle Optionen für Backup-Schemata zu verwenden, falls das erstellte Archiv nicht leer ist (d.h. Backups enthält). 1. Es ist nicht möglich, das Schema zu Großvater-Vater-Sohn oder zu Türme von Hanoi zu wechseln. 2. Sie können die Zahl der Level nicht ändern, falls das Schema Türme von Hanoi verwendet wird. In allen anderen Fällen kann das Schema verändert werden und sollte weiterhin so arbeiten, als wenn bereits existierende Archive durch ein neues Schema erstellt wurden. Bei leeren Archiven sind alle Veränderungen möglich. *Warum kann ich einen Backup-Plan nicht bearbeiten?* ▪ Der Backup-Plan wird zur Zeit ausgeführt. Die Bearbeitung eines gegenwärtig laufenden Backup-Plans ist unmöglich. ▪ Ihnen fehlen die dazugehörigen Berechtigungen. Ohne Administrator-Rechte kann ein Benutzer auf einer Maschine keine anderen Benutzern gehörenden Pläne bearbeiten. ▪ Der Backup-Plan hat einen zentralen Ursprung. Eine direkte Bearbeitung von zentralen Backup-Plänen ist nicht möglich. Sie müssen die ursprünglichen Backup-Richtlinien bearbeiten. **Task** Klicken Sie auf **Bearbeiten**. *Warum kann ich den Task nicht bearbeiten?* ▪ Der Task gehört zu einem Backup-Plan Nur Tasks, die nicht zu einem Backup-Plan gehören, wie etwa ein Wiederherstellungs-Plan, können durch direkte Bearbeitung modifiziert werden. Bearbeiten Sie den Backup-Plan, wenn Sie einen Task verändern müssen, der zu einem lokalen Backup-Plan gehört. Ein zu einem zentralen Backup-Plan gehörender Task kann durch Bearbeitung derjenigen zentralen Richtlinie modifiziert werden, die den Plan hervorgebracht hat. Dies kann jedoch nur vom Management Server Administrator getan werden. ▪ Ihnen fehlen die dazugehörigen Berechtigungen. Ohne Administrator-Rechte kann ein Benutzer auf einer Maschine keine anderen Benutzern gehörenden Tasks modifizieren.

Einen Plan/Task löschen	**Backup-Plan** Klicken Sie auf **Löschen**. *Was passiert, wenn ich einen Backup-Plan lösche?* Durch Löschung eines Backup-Plans werden auch alle seine Tasks gelöscht. *Warum kann ich einen Backup-Plan nicht löschen?* ▪ Der Backup-Plan befindet sich im Stadium „Läuft“ Ein Backup-Plan kann nicht gelöscht werden, falls mindestens einer seiner Tasks gerade ausgeführt wird. ▪ Ihnen fehlen die dazugehörigen Berechtigungen. Ohne Administrator-Rechte kann ein Benutzer auf einer Maschine keine anderen Benutzern gehörenden Pläne löschen. ▪ Der Backup-Plan hat einen zentralen Ursprung. Ein zentraler Plan kann vom Management Server Administrator gelöscht werden, indem dieser die Backup-Richtlinie, die den Plan produziert hat, widerruft. **Task** Klicken Sie auf **Löschen**. *Warum kann ich den Task nicht löschen?* ▪ Der Task gehört zu einem Backup-Plan Ein zu einem Backup-Plan gehörender Task kann nicht aus dem Plan separat gelöscht werden. Bearbeiten Sie den Plan, um den Task zu entfernen – oder löschen Sie den gesamten Plan. ▪ Ihnen fehlen die dazugehörigen Berechtigungen. Ohne Administrator-Rechte kann ein Benutzer auf einer Maschine keine anderen Benutzern gehörenden Tasks löschen.
Tabelle aktualisieren	Klicken Sie auf **Aktualisieren**. Die Management Konsole wird die Liste der auf der Maschine existierenden Backup-Pläne und Tasks mit den neusten Informationen aktualisieren. Obwohl die Liste auf der Basis von Ereignissen automatisch aktualisiert wird, kann es sein, dass die Daten infolge einer gewissen Latenz nicht augenblicklich von der verwalteten Maschine abgerufen werden. Eine manuelle Aktualisierung garantiert daher, dass auch die allerneusten Daten angezeigt werden.

Backup-Pläne und Tasks filtern und sortieren

Aktion	Lösung
Backup-Pläne und Tasks sortieren nach: Name, Stadium, Status, Typ, Ursprung usw.	Klicken Sie auf die Spaltenköpfe, um die Backup-Pläne und Tasks aufsteigend zu sortieren. Kicken Sie erneut auf den Spaltenkopf, um die Pläne und Tasks absteigend zu sortieren.
Pläne/Tasks nach Namen und Besitzer filtern	Geben Sie den Namen eines Plans/Tasks oder den eines Besitzers in das Feld unterhalb der entsprechenden Spaltenkopf-Bezeichnung ein. Sie erhalten als Ergebnis eine Liste der Tasks, deren

	Bezeichnungen/Besitzer vollständig oder partiell mit dem eingegebenen Wert übereinstimmen.
Pläne und Tasks nach Stadium, Status, Typ, Ursprung, letztes Ergebnis, Zeit-/Ereignisplan filtern.	Wählen Sie im Feld unterhalb des entsprechenden Spaltenkopfes den benötigten Wert aus einer Liste.

Tabelle der Backup-Pläne und Tasks konfigurieren

Standardmäßig werden in der Tabelle sechs Spalten angezeigt, weitere sind versteckt. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete anzeigen lassen.

Spalten anzeigen oder verbergen

1. Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, um das Kontextmenü zu öffnen. Die angehakten Menü-Elemente korrespondieren zu den in der Tabelle präsenten Spaltenköpfen.
2. Klicken Sie auf die Elemente, die Sie anzeigen bzw. verbergen wollen.

Backup-Plan ausführen

Ein Backup-Plan wird als „In Ausführung“ betrachtet, wenn wenigstens einer seiner Tasks gerade ausgeführt wird. Das Fenster **Backup-Plan ausführen** lässt Sie den Task eines gewählten Backup-Plans auch manuell starten, ungeachtet seiner Zeit-/Ereignisplanung.

So führen Sie einen Task eines gewählten Backup-Plans aus

1. Wählen Sie den Task des Backup-Plans, den Sie starten müssen. Überprüfen Sie die in Registerlaschen zusammengefassten Task-Informationen im unteren Bereich des Fensters, um sich über Ihre Auswahl zu vergewissern. Diese Informationen sind außerdem auch noch einmal im Fenster **Task details** (S. 107) dupliziert.
2. Klicken Sie auf **OK**.

Backup-Plan temporär deaktivieren

Die zeitweilige Deaktivierung eines Backup-Plans wird benötigt, wenn Archive mit Hilfe eines Datei-Managers eines Drittherstellers von einem Depot zu einem anderen verschoben werden.

Dies trifft jedoch nur auf Backup-Pläne zu, die lediglich benutzerdefinierte Backup-Schemata verwenden.

So deaktivieren Sie einen Backup-Plan

1. Klicken Sie auf **Bearbeiten**.
2. Wechseln Sie zu den Optionen für die Task-Planung und deaktivieren Sie die Zeitplanung für die gewünschte Periode, indem Sie die Parameter für **Startdatum** bzw. **Enddatum** verändern.

Task-Details

Das Fenster **Task-Details** (wird auch in der Liste **Informationen** dupliziert) sammelt alle Informationen über den gewählten Task.

Wenn ein Task das Eingreifen eines Benutzers erfordert, dann erscheinen eine Meldung und Aktionen-Schaltflächen über den Registerlaschen. Die Meldung enthält eine kurze Beschreibung des Problems. Die Schaltflächen ermöglichen, den Task oder Backup-Plan zu wiederholen oder zu stoppen.

Task-Typen

Die nachfolgende Tabelle fasst alle Task-Typen zusammen, die in Acronis Backup & Recovery 10 vorkommen. Die aktuell von Ihnen beobachteten Task-Typen hängen von der Edition und Komponente des Produkts ab, mit der die Konsole verbunden ist.

Task-Name	Beschreibung
Backup (Laufwerk)	Laufwerke und Volumes per Backup sichern
Backup (Datei)	Dateien und Verzeichnisse per Backup sichern
Backup (virtuelle Maschine)	Eine komplette virtuelle Maschine oder ihre Laufwerke per Backup sichern
Recovery (Laufwerk)	Wiederherstellung eines Disk-Backups
Recovery (Datei)	Wiederherstellung von Dateien und Ordnern
Recovery (Volume)	Recovery von Partitionen eines Disk-Backups
Recovery (MBR)	Wiederherstellung des Master Boot Records
Recovery (Festplatte zu existierender VM)	Recovery eines Disk-/Volume-Backups zu einer existierenden virtuellen Maschine
Recovery (Laufwerk zu neuer VM)	Recovery eines Disk-/Partitions-Backups zu einer neuen virtuellen Maschine
Recovery (existierende VM)	Recovery eines Virtuelle-Maschinen-Backups zu einer existierenden virtuellen Maschine
Recovery (neue VM)	Recovery eines Virtuelle-Maschinen-Backups zu einer neuen virtuellen Maschine
Validierung (Archiv)	Validierung eines einzelnen Archivs
Validierung (Backup)	Validierung von Backups
Validierung (Depot)	Validierung aller in einem Depot vorhandenen Archive
Bereinigung	Backups auf Basis von Aufbewahrungsregeln von einem Backup-Archiv löschen
ASZ-Erstellung	Acronis Secure Zone erstellen
ASZ-Verwaltung	Acronis Secure Zone in der Größe ändern, Kennwort ändern, löschen
Laufwerksverwaltung	Aktionen zum Laufwerksverwaltung
Verdichten	Auf einem Storage Node durchgeführter Service-Task
Indizieren	Deduplizierungs-Task, ausgeführt durch den Storage Node im Depot, nachdem ein Backup fertiggestellt wurde

Eine Kombination der folgenden Registerlaschen erscheint, abhängig von den Task-Typen und ob der Task gerade ausgeführt wird:

Task

Die Registerlasche **Task** steht für alle Task-Varianten zur Verfügung. Sie stellt allgemeine Informationen über einen ausgewählten Task zur Verfügung.

Archiv

Die Registerlasche **Archiv** ist für Backup-, Archiv-Validierungs- und Bereinigungs-Tasks verfügbar.

Sie stellt Informationen über das Archiv zur Verfügung: über seinen Namen, Typ, Größe, wo gespeichert usw.

Backup

Die Registerlasche **Backup** ist für Wiederherstellungs-, Backup-Validierungs- und Export-Tasks verfügbar.

Sie stellt Details über das ausgewählte Backup zur Verfügung: wann es erstellt wurde, sein Typ (vollständig, inkrementell, differentiell), Informationen über das Archiv und das Depot, in dem das Backup gespeichert ist.

Einstellungen

Die Registerlasche **Einstellungen** zeigt Informationen zur Planung und gegenüber Standardwerten veränderten Optionen an.

Fortschritt

Die Registerlasche **Fortschritt** ist verfügbar, während ein Task ausgeführt wird. Sie steht für alle Task-Varianten zur Verfügung. Die Registerlasche bietet Informationen über den Fortschritt des Tasks, die verstrichene Zeit und andere Parameter.

Backup-Plan-Details

Das Fenster **Backup-Plan-Details** (in der Leiste **Informationen** auch noch mal dupliziert) fasst in vier Registerlaschen alle Informationen zu einem ausgewählten Backup-Plan zusammen.

Falls einer der Tasks des Plans einen Benutzereingriff benötigt, erscheint im oberen Bereich der Registerlaschen eine entsprechende Meldung. Sie enthält eine kurze Beschreibung des Problems und Aktionsschaltflächen, über die Sie die passende Aktion wählen oder den Plan stoppen können.

Backup-Plan

Die Registerlasche **Backup-Plan** stellt die folgenden allgemeinen Informationen über einen ausgewählten Plan zur Verfügung:

- **Name** – Bezeichnung des Backup-Plans
- **Ursprung** – ob der Plan auf der verwalteten Maschine durch direkte Verwaltung (lokaler Ursprung) erstellt wurde – oder auf der Maschine als Ergebnis einer vom Management Server verteilten Backup-Richtlinie erschien (zentraler Ursprung)
- **Richtlinie** (für Backup-Pläne mit zentralem Ursprung) – Name der Backup-Richtlinie, deren Deployment den Backup-Plan erstellte
- **Konto** – Name des Kontos, unter dem der Plan läuft
- **Besitzer** – Name des Benutzers, der den Plan erstellt oder zuletzt modifiziert hat
- **Stadium** – Ausführungsstadium (S. 99) des Backup-Plans
- **Status** – Status (S. 100) des Backup-Plans
- **Planung** – ob der Task über eine Zeit-/Ereignisplanung verfügt oder auf manuellen Start gesetzt ist
- **Letztes Backup** – wie viel Zeit seit dem letzten Backup verstrichen ist.
- **Erstellung** – Datum, an dem der Backup-Plan erstellt wurde
- **Kommentar** – Beschreibung des Plans (sofern verfügbar)

Source

Die Registerlasche **Quelle** stellt die folgenden Informationen über die zum Backup ausgewählten Daten zur Verfügung:

- **Quelltyp** – die Art der Daten (S. 116), die zum Backup ausgewählt wurden
- **Elemente für das Backup** – die für die Sicherung ausgewählten Elemente und ihre Größe

Ziel

Die Registerlasche **Ziel** stellt die folgenden Informationen zur Verfügung:

- **Speicherort** – Bezeichnung des Depots oder Pfad zu dem Verzeichnis, wo das Archiv gespeichert wird
- **Archivname** – Bezeichnung des Archivs
- **Archiv-Kommentare** – Beschreibung zu einem Archiv (sofern vorhanden)

Einstellungen

Die Registerlasche **Einstellungen** zeigt die folgenden Informationen:

- **Backup-Schema** – das gewählte Backup-Schema und all seine Einstellungen inkl. Planung
- **Validierung** (falls ausgewählt) – Ereignisse, vor oder nach denen eine Überprüfung ausgeführt wird – und Validierungs-Planung
- **Backup-Optionen** – gegenüber den Standardwerten veränderte Backup-Optionen

6.1.3 Log

Die Ereignisanzeige speichert den Ablauf aller von Acronis Backup & Recovery 10 auf der Maschine durchgeführten Aktionen bzw. aller Aktionen, die der Benutzer auf der Maschine unter Verwendung des Programms vorgenommen hat. Wenn ein Benutzer z.B. einen Task editiert hat, wird der entsprechende Eintrag der Ereignisanzeige hinzugefügt. Bei Ausführung eines Tasks durch das Programm werden der Ereignisanzeige mehrere Einträge hinzugefügt. Mit der Ereignisanzeige können Sie Aktionen und die Ergebnisse von Task-Ausführungen einschließlich möglicher Fehler untersuchen.

Mit Log-Einträgen arbeiten

- Verwenden Sie Filter, um die gewünschten Log-Einträge zu sehen. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu Details siehe den Abschnitt Log-Einträge filtern und sortieren (S. 111).
- Wählen Sie in der Log-Tabelle einen (oder mehrere) Log-Einträge, um eine Aktion darauf auszuführen. Zu Details siehe den Abschnitt Aktionen für Log-Einträge (S. 111).
- Verwenden Sie die Leiste **Information**, um zu einem gewählten Log-Eintrag detaillierte Informationen einzusehen. Die Leiste ist standardmäßig eingeklappt. Sie können die Leiste aufklappen, indem Sie auf das Chevron-Symbol klicken. Der Inhalt der Leiste ist außerdem im Fenster **Details zu Log-Einträgen** (S. 112) dupliziert.

Die Ereignisliste mit vorgefilterten Log-Einträgen öffnen

Sie können die **Ereignisanzeige** mit für ein bestimmtes Element vorgefilterten Log-Einträgen öffnen, wenn Sie die betreffenden Elemente in anderen Administrator-Ansichten (**Dashboard**, **Backup-Pläne und Tasks**) ausgewählt haben. Auf diese Weise müssen Sie nicht selber Filter für die Log-Tabelle konfigurieren.

Ansicht	Aktion
Dashboard	Klicken Sie im Kalender mit der rechten Maustaste auf ein hervorgehobenes Datum und wählen Sie dann **Log anzeigen**. Die **Log-Ansicht** erscheint mit einer Liste der für das betreffende Datum bereits gefilterten Log-Einträge.

Backup-Pläne und Tasks	Wählen Sie einen Backup-Plan oder Task und klicken Sie dann auf **Log anzeigen**. Die Log-Ansicht wird eine Liste von Log-Einträgen anzeigen, die sich auf den gewählten Plan oder Task beziehen.

Aktionen für Log-Einträge

Alle nachfolgend beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Elemente in der Log-**Symbolleiste** ausgeführt. All diese Aktionen können außerdem über das Kontextmenü (durch Klicken mit der rechten Maustaste auf den Log-Eintrag) ausgeführt werden – oder über den Balken **Log-Aktionen** (in der Leiste **Aktionen und Werkzeuge**).

Nachfolgend finden Sie eine Anleitung zur Ausführung von Aktionen auf Log-Einträge.

Aktion	Lösung
Einen einzelnen Log-Eintrag wählen	Klicken Sie auf ihn.
Mehrere Log-Einträge wählen	▪ *Nicht zusammenhängend*: Halten Sie **Strg** gedrückt und klicken Sie nacheinander auf die gewünschten Log-Einträge ▪ *Zusammenhängend*: Wählen Sie einen einzelnen Log-Eintrag, halten Sie dann die **Umschalt**-Taste gedrückt und klicken Sie auf einen weiteren Eintrag. Darauf werden auch alle Einträge zwischen der ersten und letzten Auswahl gewählt.
Details zu einem Log-Eintrag einsehen	1. Wählen Sie einen Log-Eintrag. 2. Wählen Sie eine der nachfolgenden Varianten: ▪ Klicken Sie auf **Details anzeigen**. Die Details des Log-Eintrags werden in einem separaten Fenster angezeigt. ▪ Erweitern Sie die Informationsleiste, indem Sie auf das Chevron-Symbol klicken.
Gewählte Log-Einträge in eine Datei speichern	1. Wählen Sie einen einzelnen oder mehrere Log-Einträge. 2. Klicken Sie auf **Auswahl in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und einen Namen für die Datei.
Alle Log-Einträge in eine Datei speichern	1. Stellen Sie sicher, dass keine Filter gesetzt sind. 2. Klicken Sie auf **Alle in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und einen Namen für die Datei.
Alle gefilterten Log-Einträge in eine Datei speichern	1. Setzen Sie Filter, um eine Liste von Log-Einträgen zu erhalten, die den Filterkriterien entsprechen. 2. Klicken Sie auf **Alle in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und einen Namen für die Datei. Anschließend werden die Log-Einträge der Liste gespeichert.
Alle Log-Einträge löschen	Klicken Sie auf **Log löschen**. Alle Einträge werden aus dem Log gelöscht und es wird ein neuer Log-Eintrag erstellt. Er enthält Informationen darüber, wer die Einträge gelöscht hat und wann.

Log-Einträge filtern und sortieren

Nachfolgend finden Sie eine Anleitung zum Filtern und Sortieren von Log-Einträgen.

Aktion	Lösung
Log-Einträge für eine gegebene Zeitperiode anzeigen	1. Wählen Sie im Feld **Von** das Datum, von dem ausgehend die Liste der Log-Einträge angezeigt werden soll. 2. Wählen Sie im Feld **Bis** das Datum, bis zu dem die Liste der Log-Einträge angezeigt werden soll.
Log-Einträge nach Typ filtern	Drücken oder Lösen Sie die folgenden Symbolleisten-Schaltflächen:  Fehlermeldungen filtern  Warnmeldungen filtern  Informationsmeldungen filtern
Log-Einträge nach dem ursprünglichen Backup-Plan oder der verwalteten Einheit filtern	Wählen Sie unter dem Säulenkopf **Backup-Plan** (oder **Typ der verwalteten Einheit**) den Backup-Plan oder den verwalteten Typ von der Liste.
Log-Einträge nach Task, verwalteter Einheit, Maschine, Code, Besitzer filtern	Geben Sie den benötigten Wert (Task-Name, Maschinen-Name, Besitzer-Name usw.) in das Feld unterhalb des betreffenden Spaltenkopfes ein. Sie erhalten als Ergebnis eine Liste von Log-Einträgen, die vollständig oder partiell mit den eingegebenen Werten übereinstimmt.
Log-Einträge nach Datum und Zeit sortieren	Klicken Sie auf die Spaltenköpfe, um die Log-Einträge aufsteigend zu sortieren. Klicken Sie erneut auf den Spaltenkopf, um die Log-Einträge absteigend zu sortieren.

Die Log-Tabelle konfigurieren

Standardmäßig werden in der Tabelle sieben Spalten angezeigt, weitere sind versteckt. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete anzeigen lassen.

Spalten anzeigen oder verbergen

1. Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, um das Kontextmenü zu öffnen. Die angehakten Menü-Elemente korrespondieren zu den in der Tabelle präsenten Spaltenköpfen.
2. Klicken Sie auf die Elemente, die Sie anzeigen bzw. verbergen wollen.

Details zu Log-Einträgen

Zeigt für den gewählten Log-Eintrag detaillierte Informationen an und erlaubt Ihnen, die Details in die Zwischenablage zu kopieren.

Klicken Sie auf die Schaltfläche **In Zwischenablage kopieren**, um die Details zu kopieren.

Datenfelder der Log-Einträge

Ein lokaler Log-Eintrag enthält die folgenden Daten-Felder:

- **Typ** – Typ des Ereignisses (Fehler, Warnung, Information)
- **Datum** – Datum und Zeit, beim dem das Ereignis auftrat
- **Backup-Plan** – der Backup-Plan (sofern vorhanden), auf den sich das Ereignis bezieht
- **Task** – der Task (sofern vorhanden), auf den sich das Ereignis bezieht

- **Code** – der Programm-Code des Ereignisses. Jeder Ereignis-Typ im Programm hat seinen eigenen Code. Ein Code ist eine Integer-Zahl, die vom Acronis Support Service verwendet werden kann, um das Problem zu lösen.
- **Modul** – die Nummer des Programm-Moduls, wo das Ereignis aufgetreten ist. Es handelt sich um eine Integer-Zahl, die vom Acronis Support Service verwendet werden kann, um das Problem zu lösen.
- **Besitzer** – Benutzername des Backup-Plan-Besitzers (nur unter einem Betriebssystem)
- **Meldung** – eine Textbeschreibung des Ereignisses.

Die von Ihnen kopierten Log-Einträge sehen wie folgt aus:

```
-------------------------Details Log-Einträge--------------------------
Typ:                        Information
Datum und Zeit:             TT.MM.JJJJ HH:MM:SS
Backup-Plan:                Names des Backup-Plans
Task:                       Task-Name
Nachricht:                  Beschreibung der Aktion
Code:                       12(3x45678A)
Modul:                      Name des Moduls
Besitzer:                   Besitzer des Plans
-----------------------------------------------------------------------
```

Die Anzeige von Datum und Zeit variiert in Abhängigkeit von Ihren lokalen Einstellungen.

6.2 Einen Backup-Plan erstellen

Bevor Sie Ihren ersten Backup-Plan (S. 186) erstellen, sollten Sie sich mit den grundlegenden Konzepten (S. 17) vertraut machen, die in Acronis Backup & Recovery 10 verwendet werden.

Zur Erstellung eines Backup-Plans führen Sie folgende Schritte aus.

Allgemein

Name des Plans

[Optional] Geben Sie einen eindeutigen Namen für den Backup-Plan ein. Ein bewusst gewählter Name macht es leichter, diesen Plan zu identifizieren.

Anmeldedaten des Plans: (S. 115)

[Optional] Der Backup-Plan wird im Namen des Benutzers laufen, der den Plan erstellt hat. Sie können, sofern notwendig, die Konto-Anmeldedaten für den Plan ändern. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Kommentare

[Optional] Geben Sie eine Beschreibung bzw. einen Kommentar für den Backup-Plan ein. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Bezeichnung

[Optional] Geben Sie für die zu sichernde Maschine eine Textbezeichnung ein. Diese Bezeichnung kann verwendet werden, um die Maschine in verschiedenen Szenarien zu identifizieren. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Backup-Quelle

Typ der Quelle (S. 116)

Wählen Sie die Art der Daten, die Sie per Backup sichern wollen. Der Typ der Daten hängt von den auf der Maschine installierten Agenten ab.

Elemente für das Backup (S. 116)

Spezifizieren Sie die für das Backup gedachten Daten-Elemente. Die Liste der zu sichernden Elemente hängt vom zuvor spezifizierten Daten-Typ ab.

Anmeldeinformationen: (S. 117)

[Optional] Stellen Sie Anmeldedaten für die Quelldaten zur Verfügung, falls das Konto des Plans keine Zugriffserlaubnis für die Daten hat. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Ausschließungen (S. 118)

[Optional] Definieren Sie Ausschließungen für spezifische Datei-Typen, die Sie nicht mit ins Backup aufnehmen wollen. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Backup-Ziel

Archiv (S. 119)

Spezifizieren Sie den Pfad zu dem Ort, wo das Backup-Archiv gespeichert wird und den Namen des Archivs. Es ist ratsam, das Archiv innerhalb des Speicherortes eindeutig zu benennen. Der vorgegebene Archivname ist Archive(N), wobei N die Sequenznummer des Archivs im gewählten Speicherort ist.

Backup-Dateien unter Verwendung des Archivnamens benennen, wie in Acronis True Image Echo, anstelle automatisch generierter Namen

Nicht verfügbar, wenn Sie ein Backup auf Band oder in eine Acronis Secure Zone durchführen.

[Optional] Aktivieren Sie dieses Kontrollkästchen, wenn Sie für die Backups des Archivs eine vereinfachte Dateibenennung verwenden wollen.

Anmeldeinformationen: (S. 125)

[Optional] Stellen Sie Anmeldedaten für den Speicherort zur Verfügung, falls das Konto des Plans keine Zugriffserlaubnis für den Ort hat. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Kommentare für das Archiv

[Optional] Tragen Sie Kommentare für das Archiv ein. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Art des Backups

Backup-Schema (S. 126)

Spezifizieren Sie, wann und wie oft Ihre Daten gesichert werden sollen, definieren Sie, wie lange die erzeugten Backup-Archive im gewählten Speicherort aufbewahrt werden sollen; erstellen Sie einen Zeitplan zur Bereinigung der Archive. Verwenden Sie bekannte, optimierte Backup-Schemata wie Großvater-Vater-Sohn oder Türme von Hanoi; erstellen Sie ein maßgeschneidertes Backup-Schema oder führen Sie das Backup sofort aus.

Archiv validieren

Validierungszeitpunkt (S. 136)

[Optional] Definieren Sie, wann und wie eine Validierung durchzuführen ist und ob das gesamte Archiv zu validieren ist oder nur das letzte Archiv im Backup.

Backup-Optionen

Einstellungen

[Optional] Konfigurieren Sie Parameter für eine Backup-Aktion, wie zum Beispiel die Befehle vor bzw. nach dem Backup, die maximale Bandbreite im Netzwerk, die dem Backup zugeteilt

wird, oder den Komprimierungsgrad für das Backup-Archiv. Sofern Sie in diesem Abschnitt nichts tun, werden die Standardwerte (S. 48) verwendet.

Wird irgendeine Einstellung gegenüber dem Standardwert geändert, so wird der neue Wert über eine Zeile angezeigt. Die Statusanzeige über die Einstellungen ändert sich von **Standard** zu **Benutzerdefiniert**. Sollten Sie die Einstellung erneut ändern, so wird die Zeile ebenfalls den neuen Wert anzeigen, sofern er nicht dem Standardwert entspricht. Die Zeile verschwindet, wenn der Standardwert gesetzt wird, daher sehen Sie in diesem Abschnitt der **Backup-Plan erstellen**-Seite immer nur Werte, die von den Standardeinstellungen abweichen.

Um alle Einstellungen auf Standardwerte zurückzusetzen, klicken Sie auf **Auf Standard zurücksetzen**.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um den Backup-Plan zu erstellen.

Danach kann es sein, dass Sie zur Eingabe eines Kennworts (S. 115) aufgefordert werden.

Sie können auf den von Ihnen erstellten Plan in der Ansicht **Backup-Pläne und Tasks** (S. 99) zur Untersuchung und Verwaltung zugreifen.

6.2.1 Warum fragt das Programm nach einem Kennwort?

Ein geplanter oder aufgeschobener Task muss unabhängig davon, ob ein Benutzer angemeldet ist, ausgeführt werden. In Fällen, in denen Sie die Anmeldedaten, unter denen ein Task ausgeführt wird, nicht explizit angegeben haben, schlägt das Programm die Verwendung Ihres Benutzerkontos vor. Geben Sie Ihr Kennwort ein, spezifizieren Sie ein anderes Konto oder ändern Sie die geplante Ausführung auf manuell.

6.2.2 Anmeldedaten für Backup-Pläne

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, unter dem die Tasks des Plans ausgeführt werden.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Unter dem aktuellen Benutzer ausführen**

     Die Tasks werden mit den Anmeldedaten ausgeführt, mit denen der Benutzer angemeldet ist, der die Tasks startet. Sollte einer der Tasks nach Zeit-/Ereignis-Planung laufen, so werden Sie bei Abschluss der Plan-Erstellung nach dem Passwort des aktuellen Benutzers gefragt.
   - **Folgende Anmeldedaten benutzen**

     Die Tasks werden immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 23), um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

6.2.3 Typ der Quelle

Wählen Sie den Daten-Typ, den Sie auf der verwalteten Maschine per Backup erfasst haben wollen. Die Liste der verfügbaren Daten-Typen hängt von den Agenten ab, die auf der Maschine laufen:

Dateien

Ist verfügbar, sofern der Acronis Backup & Recovery 10 Agent für Windows (oder für Linux) installiert ist.

Aktivieren Sie diese Option, um spezifische Dateien und Ordner zu sichern.

Sollten Sie nicht um die Wiederherstellung des Betriebssystems mit seinen Einstellungen und Anwendungen besorgt sein, sondern nur gewisse Daten sicher bewahren wollen (z.B. ein aktuelles Projekt), so wählen Sie „File-Backup“. Das reduziert die Größe des Archivs und spart Speicherplatz.

Laufwerke/Volumes

Ist verfügbar, sofern der Acronis Backup & Recovery 10 Agent für Windows (oder für Linux) installiert ist.

Aktivieren Sie diese Option, um Festplatten bzw. Partitionen zu sichern. Sie müssen Benutzerrechte als Administrator oder Backup-Operator haben, um Festplatten oder Partitionen per Backup sichern zu können.

Das Backup von Laufwerken und Volumes ermöglicht, im Fall eines schweren Daten-Schadens oder Hardware-Ausfalls das komplette System wiederherzustellen. Die Backup-Prozedur ist schneller als das Kopieren von Dateien und kann den Backup-Prozess signifikant beschleunigen, wenn es darum geht, große Daten-Mengen zu sichern.

Hinweis für Linux-Benutzer: *Es wird empfohlen, dass Sie vor dem Backup alle Volumes trennen, die wie z.B. ext2 kein Journaling-Dateisystem enthalten. Anderenfalls könnten diese Volumes bei der Wiederherstellung beschädigte Dateien enthalten oder die Wiederherstellung dieser Volumes mit Größenänderung schlägt fehl.*

6.2.4 Elemente für das Backup

Die Elemente für das Backup hängen vom zuvor gewählten Quell-Typ (S. 116) ab.

Laufwerke und Volumes wählen

So legen Sie Laufwerke/Volumes für ein Backup fest

1. Aktivieren Sie die Kontrollkästchen der zu sichernden Laufwerke bzw. Volumes. Sie können eine beliebige Zusammenstellung von Laufwerken und Volumes bestimmen.

   Falls Betriebssystem und Boot-Loader auf unterschiedlichen Volumes liegen, nehmen Sie immer beide mit in das Backup auf. Diese Laufwerke müssen auch zusammen wiederhergestellt werden, da anderenfalls ein hohes Risiko besteht, dass das Betriebssystem nicht startet.

   In Linux werden logische Volumes und MD-Geräte unter **Dynamisch und GPT** angezeigt. Zu weiteren Informationen über das Backup solcher Volumes und Geräte siehe „Backup von LVM-Volumes und MD-Geräten (Linux) (S. 34)“.
2. [Optional] Um ein Laufwerk bzw. Volume auf physikalischer Ebene als exakte Kopie zu sichern, aktivieren Sie das Kontrollkästchen **Sektor-für-Sektor sichern**. Das resultierende Backup wird die gleiche Größe wie das gesicherte Laufwerk haben (sofern die Option **Komprimierungsrate** auf **Ohne** eingestellt ist). Verwenden Sie das Sektor-für-Sektor-Backup, um Laufwerke mit nicht

erkanntem oder nicht unterstütztem Dateisystem und anderen proprietären Datenformaten zu sichern.

3. Klicken Sie auf **OK**.

Was genau speichert das Backup eines Laufwerks oder Volumes?

Bei unterstützten Dateisystemen und ausgeschalteter Option 'Sektor-für-Sektor sichern' speichert ein Laufwerk-/Volume-Backup nur solche Sektoren, die Daten enthalten. Das reduziert die Größe des resultierenden Backups und beschleunigt die Ausführung von Backup und Wiederherstellung.

Windows

Die Auslagerungsdatei (pagefile.sys) und die Ruhezustandsdatei (hiberfil.sys) werden nicht gesichert. Nach einer Wiederherstellung werden die Dateien an passender Position mit einer Größe von Null erneut erzeugt.

Ein Volume-Backup speichert alle Dateien und Ordner des gewählten Volumes, unabhängig von ihren Attributen (inkl. versteckter oder System-Dateien), den Boot-Record, die File Allocation Table (FAT) und – sofern vorhanden – auch Root und Track 0 (inkl. Master Boot Record, MBR) des Laufwerks. Der Boot-Code eines GPT-Volumes wird nicht vom Backup erfasst.

Ein Laufwerk-Backup speichert alle Volumes des betreffenden Laufwerks (inkl. versteckter Volumes wie Wartungs-Volumes von Herstellern) und den Track Zero mit dem Master Boot Record (MBR).

Linux

Ein Volume-Backup speichert alle Dateien und Ordner des gewählten Laufwerkes (unabhängig von ihren Attributen), einen Boot-Record und den Dateisystem-Super-Block.

Ein Laufwerk-Backup speichert alle Volumes des Laufwerks, inkl. 'Track Zero' mit dem 'Master Boot Record'.

Dateien und Ordner wählen

So bestimmen Sie die zu sichernden Dateien bzw. Ordner:

1. Erweitern Sie die Elemente des lokalen Verzeichnisbaums, um seine verschachtelten Ordner und Dateien einzusehen.
2. Wählen Sie ein Element, indem Sie das entsprechende Kontrollkästchen im Verzeichnisbaum aktivieren. Die Aktivierung eines Ordner-Kontrollkästchens bedeutet, dass sein gesamter Inhalt (Dateien und Ordner) im Backup erfasst wird. Das gilt auch für neue Dateien, die zukünftig hier erscheinen.

   Ein dateibasiertes Backup ist für die Wiederherstellung eines Betriebssystems nicht ausreichend. Sie müssen ein Disk-Backup durchführen, um Ihr Betriebssystem wiederherstellen zu können.

   Verwenden Sie die Tabelle im rechten Teil des Fensters, um die verschachtelten Elemente zu durchsuchen und auszuwählen. Die Aktivierung des Kontrollkästchens neben dem Spaltenkopf **Name** wählt automatisch alle Elemente der Tabelle aus. Durch Deaktivierung des Kontrollkästchens werden alle Elemente automatisch abgewählt.
3. Klicken Sie auf **OK**.

6.2.5 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf die zu sichernden Daten benötigt werden.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:

- **Anmeldedaten des Plans benutzen**

  Das Programm greift auf die Quelldaten unter Verwendung derjenigen Anmeldedaten des Backup-Plans zu, wie sie im Abschnitt „Allgemein“ spezifiziert wurden.

- **Folgende Anmeldedaten benutzen**

  Das Programm greift auf die Quelldaten unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das Konto des Plans keine Zugriffserlaubnis für die Daten hat.

  Spezifizieren Sie:

  - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
  - **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

6.2.6 Ausschließungen

Definieren Sie Ausschließungen für spezifische Datei-Typen, die Sie nicht mit ins Backup aufnehmen wollen. Sie könnten z.B. Datenbank-Dateien, versteckte oder System-Dateien bzw. Ordner wie auch Dateien mit speziellen Erweiterungen vom Archiv ausschließen wollen.

Dateien und Verzeichnisse zum Ausschließen spezifizieren:

Verwenden Sie einen der nachfolgenden Parameter:

- **Ausschluss aller Systemdateien und Systemordner**

  Diese Option ist nur für Dateisysteme wirksam, die von Windows unterstützt werden. Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner mit dem Attribut **Versteckt** zu überspringen. Bei Ordnern mit dem Attribut **Versteckt** wird der gesamte Inhalt ausgeschlossen – einschließlich solcher Dateien, die nicht **versteckt** sind.

- **Ausschluss aller Systemdateien und Systemordner**

  Diese Option ist nur für Dateisysteme wirksam, die von Windows unterstützt werden. Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner mit dem Attribut **System** zu überspringen. Bei Ordnern mit dem Attribut **System** wird der gesamte Inhalt ausgeschlossen – einschließlich solcher Dateien, die nicht mit **System** gekennzeichnet sind.

*Sie können die Attribute von Dateien oder Ordnern über ihre Datei-/Ordner-Eigenschaften einsehen oder durch Verwendung des Kommandozeilenbefehls **attrib**. Weitere Informationen finden Sie im Hilfe und Support-Center von Windows.*

- **Dateien ausschließen, die folgenden Kriterien entsprechen**

  Aktivieren Sie dieses Kontrollkästchen, um Dateien und Ordner zu überspringen, deren Bezeichnungen mit einem der Kriterien in der Liste übereinstimmen (Dateimaske genannt) – verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Alle entfernen**, um die Liste der Dateimasken zu erstellen.

  Sie können ein oder mehrere Wildcard-Zeichen (* und ?) in einer Datei-Maske verwenden:

  Das Asterisk (*) steht für Null oder mehrere Zeichen im Dateinamen; so ergibt z.B. die Datei-Maske Doc*.txt Dateien wie Doc.txt und Document.txt.

  Das Fragezeichen (?) steht für exakt ein Zeichen in einem Dateinamen, so ergibt z.B. die Datei-Maske Doc?.txt Dateien wie Doc1.txt und Docs.txt – aber nicht Doc.txt oder Doc11.txt.

Fügen Sie einem als Kriterium angegebenen Ordnernamen ein Backslash (\) hinzu, um einen Ordner zu spezifizieren, dessen Pfad einen Laufwerksbuchstaben enthält, beispielsweise: C:\Finanzen\

Beispiele für Ausschließungen

Kriterium	Beispiel	Beschreibung
Windows und Linux		
Per Name	F.log F	Schließt alle Dateien namens „F.log“ aus Schließt alle Ordner namens „F“ aus
Per Maske (*)	*.log F*	Schließt alle Dateien mit der Erweiterung „.log“ aus Schließt alle Dateien und Ordner aus, deren Namen mit „F“ beginnen (etwa die Ordner F, F1 und die Dateien F.log, F1.log)
Per Maske (?)	F???.log	Schließt alle .log-Dateien aus, deren Namen am Ende vier Zeichen enthalten und mit „F“ beginnen
Windows		
Per Dateipfad	C:\Finanzen\F.log	Schließt die Datei aus, die „F.log“ heißt und im Ordner „C:\Finanzen“ vorliegt
Per Ordnerpfad	C:\Finanzen\F\	Schließt den Ordner „C:\Finanzen\F“ aus (stellen Sie sicher, dass Sie den vollständigen Pfade angeben, beginnend mit einem Laufwerksbuchstaben)
Linux		
Per Dateipfad	/home/user/Finanzen/F.log	Schließt die Datei aus, die „F.log“ heißt und im Ordner „/home/user/Finanzen“ vorliegt
Per Ordnerpfad	/home/user/Finanzen/	Schließt den Ordner „/home/user/Finanzen“ aus

6.2.7 Archiv

Definieren Sie den Speicherort und den Namen für das Archiv.

1. Ziel wählen

Tragen Sie den vollständigen Pfad zum Zielort in das Feld **Pfad** ein oder wählen Sie das gewünschte Ziel im Verzeichnisbaum.

- Klicken Sie zur Speicherung von Backups auf dem Acronis Online Backup Storage auf **Anmelden**, geben Sie anschließend die Anmeldedaten zum Zugriff auf den Online Storage ein. Erweitern Sie dann die Gruppe **Online Backup Storage** und wählen Sie das Konto.

  Bevor Sie Ihre Backups auf dem Online Storage sichern können, müssen Sie für den Online Backup-Dienst ein Abonnement kaufen und das Abonnement auf der zu sichernden Maschine aktivieren. Die Online Backup-Funktion steht unter Linux und bootfähigen Medien nicht zur Verfügung.

  Acronis Backup & Recovery Online ist möglicherweise in Ihrer Region nicht verfügbar. Zu weiteren Informationen klicken Sie hier: http://www.acronis.de/my/backup-recovery-online/.

- Um das Backup zu einem zentralen Depot durchzuführen, erweitern Sie die Gruppe **Zentral** und wählen dort das Depot.
- Um das Backup zu einem persönlichen Depot durchzuführen, erweitern Sie die Gruppe **Persönlich** und wählen dort das Depot.

- Um Daten zu einem lokalen Ordner auf der Maschine zu sichern, erweitern Sie die Gruppe **Lokale Ordner** und wählen das gewünschte Verzeichnis.
- Um Daten zu einer Netzwerkfreigabe zu sichern, erweitern Sie die Gruppe **Netzwerkordner**, wählen die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

  Hinweis für Linux-Benutzer: *Um eine CIFS-Netzfreigabe (Common Internet File System) anzugeben, die zu einem Mount-Point wie z.B.* ***/mnt/freigabe****, wählen Sie diesen Mount-Point statt der Netzfreigabe aus.*

- Für das Backup der Daten auf einen **FTP-** oder **SFTP-**Server, tragen Sie Servername oder Adresse im Feld **Pfad** folgendermaßen ein:

  ftp://ftp_server:port _nummer oder **sftp://sftp_server:port_nummer**

  Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP.

  Nach Eintragen der Anmeldinformationen sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server.

  Sie können auf den Server auch als Benutzer 'anonymous' zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten.

  Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

- Um Daten zu einem lokal angeschlossenen Bandgerät zu sichern, erweitern Sie die Gruppe **Bandlaufwerke** und klicken auf das benötigte Gerät.

2. Archiv-Tabelle verwenden

Die Tabelle zeigt für jeden gewählten Speicherort die Namen dort enthaltener Archive an, um Ihnen die Wahl des richtigen Ziels zu erleichtern. Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Das neue Archiv benennen

Sobald Sie den Zielort für das Archiv gewählt haben, erstellt das Programm einen Namen für das neue Archiv und zeigt diesen im Feld **Name** an. Der Name sieht normalerweise wie Archiv(1) aus. Der generierte Name ist innerhalb des gewählten Speicherortes eindeutig. Wenn Sie mit dem automatisch generierten Namen einverstanden sind, dann klicken Sie auf **OK**. Anderenfalls geben Sie einen anderen, eindeutigen Namen ein und klicken dann auf **OK**.

Backup zu einem existierenden Archiv

Sie können einen Backup-Plan so konfigurieren, dass das Backup zu einem existierenden Archiv erfolgt. Zur Umsetzung wählen Sie das Archiv in der Tabelle oder geben die entsprechende Bezeichnung in das Feld **Name** ein. Sollte das Archiv mit einem Kennwort geschützt sein, wird das Programm in einem Pop-up-Fenster danach fragen.

Durch Wahl des existierenden Archivs erzeugen Sie eine Interaktion mit einem anderen Backup-Plan, der das Archiv ebenfalls verwendet. Das ist kein Problem, falls der andere Plan eingestellt ist, aber im Allgemeinen sollten Sie folgender Regel folgen: „Ein Backup-Plan – ein Archiv“. Das Gegenteil zu tun, behindert das Programm nicht in seiner Funktion, aber ist unpraktisch bzw. uneffizient, mit Ausnahme einiger Spezialfälle.

Warum zwei oder mehr Backup-Pläne nicht in dasselbe Archive sichern sollten

1. Ein Backup von unterschiedlichen Quellen in dasselbe Archiv durchzuführen, bewirkt vom Standpunkt der Bedienbarkeit aus schwierig zu handhabende Archive. Wenn es darauf ankommt, eine Wiederherstellung durchzuführen, zählt jede Sekunde, während Sie sich jedoch vielleicht im Inhalt des Archivs verlieren.

   Mit demselben Archiv operierende Backup-Pläne sollten auch dieselben Daten-Elemente sichern (z.B. zwei Pläne, die Laufwerk C: sichern).

2. Werden auf ein Archiv multiple Aufbewahrungsregeln angewendet, so macht dies den Inhalt des Archivs auf gewisse Weise unkalkulierbar. Da jede Regel auf das gesamte Archiv angewendet wird, kann es leicht passieren, dass Backups, die zu einem Backup-Plan gehören, zusammen mit Backups gelöscht werden, die zum anderen Plan gehören. Sie sollten insbesondere kein klassisches Verhalten der Backup-Schemata GVS und Türme von Hanoi erwarten.

   Normalerweise sollte jeder komplexe Backup-Plan in seine eigenen Archive sichern.

6.2.8 Vereinfachte Benennung von Backup-Dateien

Wenn Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** aktivieren:

- Der Dateiname des ersten (vollständigen) Backups im Archiv wird aus dem Archivnamen zusammengesetzt, beispielsweise: **MeineDateien.tib.** Die Dateinamen der nachfolgenden (inkrementellen oder differentiellen) Backups erhalten eine zusätzliche Kennziffer, beispielsweise: **MeineDateien2.tib**, **MeineDateien3.tib** und so weiter.

  Diese einfache Namensschema ermöglicht Ihnen, von einer Maschine ein 'transportierbares' Image auf ein entfernbares Medium zu erstellen – oder die Backups durch Verwendung eines Skripts an einen anderen Speicherort zu verschieben.

- Die Software löscht vor Erstellung eines neuen Voll-Backups das komplette Archiv und startet danach ein neues.

  Dieses Verhalten ist nützlich, wenn Sie mehrere USB-Festplatten abwechselnd verwenden und jedes Laufwerk ein einzelnes Voll-Backup (S. 123) oder alle während einer Woche erstellten Backups (S. 123) behalten soll. Sie könnten am Ende aber ganz ohne Backups dastehen, falls ein Voll-Backup zu Ihrem einzigen Laufwerk fehlschlägt.

  Dieses Verhalten lässt sich aber unterdrücken, wenn Sie dem Archivnamen die [Datum]-Variable (S. 125) hinzufügen.

Wenn Sie *nicht* das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** aktivieren:

- Jedes Backup erhält einen eindeutigen Dateinamen mit exaktem Datumsstempel sowie dem Backup-Typ, beispielsweise: **MeineDateien_2010_03_26_17_01_38_960D.tib**. Diese Standard-Dateibenennung ermöglicht eine weitreichendere Nutzung von Backup-Zielorten und Backup-Schemata.

Einschränkungen

Bei Verwendung der vereinfachten Dateibenennung ist folgende Funktionalität nicht verfügbar:

- Konfiguration vollständiger, inkrementeller und differentieller Backups innerhalb eines einzigen Backup-Plans. Sie müssen separate Backup-Pläne für jeden Backup-Typ erstellen.
- Backups zu einem verwalteten Depot, auf Band, zu einer Acronis Secure Zone oder dem Acronis Online Backup Storage.
- Aufbewahrungsregeln konfigurieren

- Regelmäßige Konvertierung von Backups zu einer virtuellen Maschine einrichten
- Die Verwendung von Zahlen am Ende eines Archivnamens

Tipp: *Folgende Zeichen sind bei FAT16-, FAT32- und NTFS-Dateisystemen für Dateinamen nicht erlaubt: Backslash (\), Schrägstrich (/), Doppelpunkt (:), Sternchen (Asterisk) (*), Fragezeichen (?), Anführungszeichen ("), Kleiner-als-Zeichen (<), Größer-als-Zeichen (>) und Hochstrich (|).*

Verwendungsbeispiele

Dieser Abschnitt zeigt Ihnen Beispiele für die Verwendung der vereinfachten Dateibenennung.

Beispiel 1. Tägliches Backup ersetzt das alte

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Voll-Backup sichern.
- Sie wollen das Backup lokal in der Datei **MeineMaschine.tib** speichern.
- Sie wollen, dass jedes neue Backup das jeweilige alte ersetzt.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans **MeineMaschine** als Archivnamen, aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen** und legen Sie danach **Voll** als Backup-Typ fest.

Ergebnis. Das Archiv besteht aus einer einzigen Datei: MeineMaschine.tib. Diese Datei wird vor Erstellung eines neuen Backups wieder gelöscht.

Beispiel 2. Tägliche Voll-Backups mit Datumsstempel

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Voll-Backup sichern.
- Sie möchten ältere Backups per Skript zu einem Remote-Speicherort verschieben.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans **MeineMaschine** als Archivnamen, aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** und legen Sie danach **Voll** als Backup-Typ fest.

Ergebnis:

- Die Backups vom 1. Januar 2011, 2. January 2011 (usw.) werden entsprechend als 'MeineMaschine-1.1.2011.tib', 'MeineMaschine-2.1.2011.tib' (usw.) gespeichert.
- Ihr Skript kann ältere Backups auf Basis des Datumsstempels verschieben.

Siehe auch „Die Variable [Date]“ (S. 125).

Beispiel 3. Stündliche Backups innerhalb eines Tages

Betrachten Sie folgendes Szenario:

- Sie möchten von den wichtigsten Dateien Ihres Servers an jedem Tag stündliche Backups erstellen.
- Das erste Backup eines jeden Tages soll 'vollständig' sein und um Mitternacht ausgeführt werden – die nachfolgenden Backups des Tages sollen differentiell sein und um 01:00 Uhr, 02:00 Uhr (usw.) ausgeführt werden.

- Ältere Backups sollen im Archiv aufbewahrt werden.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans **ServerDateien([Date])** als Archivnamen, aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**, legen Sie **Differentiell** als Backup-Typ fest – und planen Sie dann für die Backups eine stündliche Ausführung (ab Mitternacht).

Ergebnis:

- Die 24 Backups vom 1. Januar 2011 werden als 'ServerDateien(1.1.2011).tib', 'ServerDateien(1.1.2011)2.tib' (usw.) bis zu 'ServerDateien(1.1.2011)24.tib' gespeichert.
- Die Backups des folgenden Tags starten mit einem Voll-Backup namens 'ServerDateien(2.1.2011).tib'.

Siehe auch „Die Variable [Date]“ (S. 125).

Beispiel 4. Tägliche Voll-Backups mit täglichem Laufwerkswechsel

Betrachten Sie folgendes Szenario:

- Sie möchten von Ihrer Maschine tägliche Voll-Backups in die Datei **MeineMaschine.tib** erstellen – auf einer externen Festplatte (oder ähnlichem Laufwerk).
- Sie haben zwei dieser Laufwerke. Jedes verwendet beim Anschluss an die Maschine den Laufwerksbuchstaben **D**.
- Sie möchten die Laufwerke vor jedem Backup wechseln, so dass eines der Laufwerke die Backups von heute enthält, das andere die von gestern.
- Jedes neue Backup soll das Backup auf dem aktuell angeschlossenen Laufwerk ersetzen.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans **MeineMaschine** als Archivnamen und **D:** als Archiv-Speicherort, aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** und legen Sie danach **Voll** als Backup-Typ fest.

Ergebnis: Jedes Laufwerk wird nur je ein Voll-Backup enthalten. Während ein Laufwerk an die Maschine angeschlossen ist, können Sie das andere zur Erreichung einer zusätzlichen Datensicherheit außer Haus lagern.

Beispiel 5. Tägliche Voll-Backups mit wöchentlichen Laufwerkswechsel

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit täglichen Backups sichern. ein Voll-Backup an jedem Montag und inkrementelle Backups von Dienstag bis Sonntag.
- Backups sollen zum Archiv **MeineMaschine** auf einer externen Festplatte (oder ähnlichem Laufwerk) erstellt werden.
- Sie haben zwei dieser Laufwerke. Jedes verwendet beim Anschluss an die Maschine im Betriebssystem den Laufwerksbuchstaben **D**.
- Die Laufwerke sollen an jedem Montag gewechselt werden, so dass ein Laufwerk die Backups der aktuellen Woche (Montag bis Sonntag) enhält – und das andere Laufwerk die Backups der letzten Woche.

Sie müssen in diesem Szenario zwei Backup-Pläne folgendermaßen erstellen:

a) Spezifizieren Sie bei Erstellung des ersten Backup-Plans **MeineMaschine** als Archivnamen, **D:** als Archiv-Speicherort, aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** und legen Sie **Voll** als Backup-Typ fest – planen Sie anschließend für die Backups eine wöchentliche Ausführung an jedem Montag.

b) Spezifizieren Sie bei Erstellung des zweiten Backup-Plans dieselben Einstellungen wie im ersten Backup-Plan, nur dass Sie **Inkrementell** als Backup-Typ wählen und für die Backups eine wöchentliche Ausführung von Dienstag bis Sonntag planen.

Ergebnis:

- Bevor das 'Montags-Backup' erstellt wird (durch den ersten Backup-Plan), werden alle auf dem aktuell angeschlossenen Laufwerk liegenden Backups gelöscht.
- Während ein Laufwerk an die Maschine angeschlossen ist, können Sie das andere zur Erreichung einer zusätzlichen Datensicherheit außer Haus lagern.

Beispiel 6. Backups während der Arbeitszeit

Betrachten Sie folgendes Szenario:

- Sie möchten von den wichtigsten Dateien Ihres Servers an jedem Tag Backups erstellen.
- Das erste Backup eines Tages soll vollständig sein und um 01:00 Uhr ausgeführt werden.
- Die Backups während der Arbeitszeit sollen differentiell sein und stündlich von 8:00 Uhr bis 17:00 Uhr ausgeführt werden.
- Dem Namen einer jeden Backup-Datei soll das Erstelldatum hinzugefügt werden.

Sie müssen in diesem Szenario zwei Backup-Pläne folgendermaßen erstellen:

a) Spezifizieren Sie bei Erstellung des ersten Backup-Plans **ServerDateien([Date])** als Archivnamen, aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**, legen Sie **Voll** als Backup-Typ fest – und planen Sie dann für die Backups eine tägliche Ausführung um 01:00 Uhr.

b) Spezifizieren Sie bei Erstellung des zweiten Backup-Plans dieselben Einstellungen wie im ersten Backup-Plan, nur dass Sie **Differentiell** als Backup-Typ wählen und die Backups folgendermaßen planen:
   - **Task starten**: **Täglich**
   - **Alle**: **1 Stunde(n)**
   - **Von**: **08:00:00 Uhr**
   - **Bis**: **17:01:00 Uhr**

Ergebnis:

- Das Voll-Backup vom 31. Januar 2011 wird als 'ServerDateien(31.1.2011).tib' gespeichert.
- Die 10 differentiellen Backups vom 31. Januar 2011 werden als 'ServerDateien(31.1.2011)2.tib', 'ServerDateien(31.1.2011)3.tib' (usw.) bis zu 'ServerDateien(31.1.2011)11.tib' gespeichert.
- Die Backups des folgenden Tags (1. Februar) starten mit einem Voll-Backup namens 'ServerDateien(1.2.2011).tib'. Die differentiellen Backups starten mit 'ServerDateien(1.2.2011)2.tib'.

Siehe auch „Die Variable [Date]“ (S. 125).

Die Variable '[DATE]'

Wenn Sie die Variable **[DATE]** zur Verwendung im Archivnamen spezifizieren, enthält der Dateiname eines jeden Backups sein entsprechendes Erstelldatum.

Bei Verwendung dieser Variable wird das erste Backup eines neuen Tages ein Voll-Backup. Die Software löscht vor Erstellung des nächsten Voll-Backups alle schon früher an diesem Tag erstellten Backups. Backups, die vor diesem Tag erstellt wurden, bleiben erhalten. Das bedeutet, dass Sie multiple Voll-Backups (mit oder ohne inkrementelle Erweiterungen) speichern können, jedoch nicht mehr als ein Voll-Backup pro Tag. Sie können Backups nach Datum sortieren, kopieren, verschieben sowie manuell oder per Skript löschen.

Das Datumsformat ist *d.m.yyyy*. Beispielsweise 31.1.2011 für den 31. Januar 2011. (Beachten Sie die fehlende Null bei Monatsziffer.)

Sie können die Variable an jeder Stelle im Archivnamen positionieren. Sie können zudem Groß- und Kleinbuchstaben in dieser Variable verwenden.

Beispiele

Beispiel 1. Angenommen Sie führen für zwei Tage, startend am 31. Januar 2011, zweimal täglich inkrementelle Backups aus (um Mitternacht und zur Mittagszeit). Falls der Archivname **MeinArchiv-[DATE]-** lautet, sieht die Liste der Backup-Dateien nach zwei Tagen folgendermaßen aus:

MeinArchiv-31.1.2011-.tib (vollständig, erstellt am 31. Januar um Mitternacht)
MeinArchiv-31.1.2011-2.tib (inkrementell, erstellt am 31. Januar, zur Mittagszeit)
MeinArchiv-1.2.2011-.tib (vollständig, erstellt am 1. Februar um Mitternacht)
MeinArchiv-1.2.2011-2.tib (inkrementell, erstellt am 1. Februar, zur Mittagszeit)

Beispiel 2. Angenommen, Sie erstellen Voll-Backups mit gleicher Planung und gleichem Archivnamen wie im vorherigen Beispiel. In diesem Fall sieht die Liste der Backup-Dateien nach dem zweiten Tag wie folgt aus:

MeinArchiv-31.1.2011-.tib (vollständig, erstellt am 31. Januar, zur Mittagszeit)
MeinArchiv-1.2.2011-.tib (vollständig, erstellt am 1. Februar, zur Mittagszeit)

Hintergrund des Ergebnisses ist, dass die um Mitternacht erstellten Voll-Backups durch am selben Tag neu erstellte Voll-Backups ersetzt werden.

Backup-Aufteilung und vereinfachte Dateibenennung

Wenn ein Backup entsprechend der Einstellungen unter Backup-Aufteilung (S. 61) aufgesplittet wird, dann wird die gleiche Indizierung auch für die Namensteile des Backups verwendet. Der Dateiname für das nächste Backup erhält den nächsten verfügbaren Index.

Angenommen, das erste Backup des Archives **MeineDateien** wurde in zwei Teile aufgeteilt. Die Dateinamen dieses Backups sind folglich **MeineDateien1.tib** und **MeineDateien2.tib**. Das zweite Backup (als nicht aufgeteilt angenommen) wird **MeineDateien3.tib** genannt.

6.2.9 Zugriff auf die Anmeldedaten für den Speicherort des Archivs

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das Backup-Archiv gespeichert wird. Der Benutzer, dessen Name angegeben wird, wird als Besitzer des Archivs betrachtet.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Plans benutzen**

     Das Programm greift auf die Quelldaten unter Verwendung derjenigen Anmeldedaten des Backup-Plans zu, wie sie im Abschnitt „Allgemein“ spezifiziert wurden.
   - **Folgende Anmeldedaten benutzen**

     Das Programm greift auf die Quelldaten unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das Konto des Plans keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Warnung: *Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.*

6.2.10 Backup-Schemata

Wählen Sie eins der verfügbaren Backup-Schemata:

- **Backup jetzt** – um einen Backup-Task zum manuellen Starten zu erstellen und den Task unmittelbar nach seiner Erstellung auszuführen.
- **Backup später** – um einen Backup-Task zum manuellen Starten zu erstellen – oder eine einmalige, in der Zukunft liegende Task-Ausführung zu planen.
- **Einfach** – um zu planen, wann und wie oft die Daten gesichert werden und Aufbewahrungsregeln zu spezifizieren.
- **Großvater-Vater-Sohn** – um das Großvater-Vater-Sohn-Backup-Schema zu verwenden. Das Schema erlaubt es nicht, dass Daten mehr als einmal am Tag gesichert werden. Sie bestimmen den Wochentag, an dem das tägliche Backup ausgeführt wird und wählen von diesen Tagen noch einen Tag zum wöchentlichen und monatlichen Backup. Dann definieren Sie die Aufbewahrungsregeln für die täglichen (entspricht dem „Sohn“), wöchentlichen („Vater“) und monatlichen („Großvater“) Backups. Abgelaufene Backups werden automatisch gelöscht.
- **Türme von Hanoi** – um das Backup-Schema Türme von Hanoi zu verwenden, wo Sie planen, wann und wie oft gesichert wird (Sitzungen), und die Zahl der Backup-Level (bis zu 16) bestimmen. In diesem Schema können die Daten mehrmals pro Tag gesichert werden. Indem Sie die Backup-Planung aufstellen und die Backup-Level wählen, erhalten Sie automatisch die Roll-back-Periode – die garantierte Zahl von Sitzungen, zu der Sie jederzeit zurückgehen können. Der automatische Bereinigungsmechanismus hält die benötigte Roll-back-Periode aufrecht, indem er die abgelaufenen Backups löscht und von jedem Level die neusten Backups behält.
- **Benutzerdefiniert** – um ein benutzerdefiniertes Schema zu erstellen, wo Sie frei sind, eine Backup-Strategie in der für Ihr Unternehmen benötigten Art aufzustellen: Spezifizieren Sie multiple Zeit-/Ereignis-Pläne für verschiedene Backup-Typen, fügen Sie Bedingungen hinzu und definieren Sie die Aufbewahrungsregeln.

- **Initial Seeding** – zum lokalen Speichern eines Voll-Backups, das später auf dem Acronis Online Backup Storage hinterlegt wird.

Schema „Backup jetzt“

Mit dem Schema „**Backup jetzt**“ wird die Sicherung augenblicklich ausgeführt, sobald Sie im unteren Bereich der Seite auf **OK** klicken.

Wählen Sie im Feld **Backup-Typ**, ob Sie ein vollständiges, inkrementelles oder differentielles Backup (S. 21) erstellen wollen.

Schema „Backup später“

Mit dem Schema „Backup später“ wird die Sicherung nur einmal ausgeführt, am von Ihnen angegebenen Zeitpunkt (Datum, Uhrzeit).

Spezifizieren Sie die passenden Einstellungen wie folgt

Backup-Typ	Wählen Sie den Typ des Backups: vollständig, inkrementell oder differentiell. Ein Voll-Backup wird unabhängig von Ihrer Auswahl immer dann erstellt, wenn es noch kein vollständiges Backup im Archiv gibt.
Datum und Zeit	Spezifizieren Sie, wann das Backup starten soll.
Task wird manuell gestartet	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Task auf keinen Zeitplan setzen müssen und ihn anschließend manuell ausführen wollen.

Schema „Einfach“

Mit dem Backup-Schema „Einfach“ planen Sie lediglich, wann und wie oft Ihre Daten gesichert werden sollen und definieren die Aufbewahrungsregeln. Beim ersten Mal wird immer ein Voll-Backup erstellt. Die nachfolgenden Backups werden inkrementell.

Zum Erstellen des Backup-Schemas „Einfach“ spezifizieren Sie die passenden Einstellungen wie folgt:

Backup	Bestimmen Sie die Backup-Planung – wann und wie oft die Daten gesichert werden sollen. Siehe den Abschnitt Planung (S. 85), um mehr über das Aufstellen von Zeit/-Ereignis-Planungen zu lernen.
Aufbewahrungsregel	Für das Schema „Einfach“ ist nur eine Aufbewahrungsregel (S. 32) verfügbar. Definieren Sie die Aufbewahrungsperiode für die Backups.

Schema Großvater-Vater-Sohn

Auf einen Blick

- Täglich inkrementelle, wöchentlich differentielle und monatliche Voll-Backups.
- Benutzerdefinierbarer Tag für wöchentliche und monatliche Backups
- Benutzerdefinierbare Aufbewahrungsperiode für Backups jeden Typs

Beschreibung

Angenommen, Sie wollen einen Backup-Plan aufstellen, der regelmäßig eine Serie täglicher (T), wöchentlicher (W) und monatlicher (M) Backups produziert. Beispiel: Die nachfolgende Tabelle zeigt eine exemplarische zweimonatige Periode für einen solchen Plan.

	Mo	Di	Mi	Do	Fr	Sa	So
Jan 1—Jan 7	T	T	T	T	W	-	-
Jan 8—Jan 14	T	T	T	T	W	-	-
Jan 15—Jan 21	T	T	T	T	W	-	-
Jan 22—Jan 28	T	T	T	T	M	-	-
Jan 29—Feb 4	T	T	T	T	W	-	-
Feb 5—Feb 11	T	T	T	T	W	-	-
Feb 12—Feb 18	T	T	T	T	W	-	-
Feb 19—Feb 25	T	T	T	T	M	-	-
Feb 26—Mrz 4	T	T	T	T	W	-	-

Die täglichen Backups laufen an jedem Wochentag außer freitags, welcher für wöchentliche und monatliche Backups gelassen wird. Monatliche Backups laufen an jedem vierten Freitag, während die wöchentlichen Backups an allen übrigen Freitagen laufen.

- Monatliche Backups („Großvater“) sind vollständig;
- Wöchentliche Backups ("Vater) sind differentiell;
- Tägliche Backups („Sohn“) sind inkrementell.

Parameter

Sie können für ein Schema Großvater-Vater-Sohn (GVS) folgende Parameter einstellen.

Backup starten:	Spezifiziert, wann das Backup starten soll. Der Standardwert ist 12:00 Uhr.
Sichern:	Spezifiziert die Tage, an denen das Backup ausgeführt werden soll. Der Standardwert ist Werktags.
Wöchentlich/monatlich:	Spezifiziert, welchen der im Feld **Sichern an** gewählten Tage Sie für wöchentliche und monatliche Backups reservieren wollen. Ein monatliches Backup wird an jedem vierten dieser Tage durchgeführt. Der Standardwert ist Freitag.
Backups aufbewahren:	Spezifizieren Sie, wie lange die Backups im Archiv gespeichert werden sollen. Die Zeitdauer kann in Stunden, Tagen, Wochen, Monaten oder Jahren gesetzt werden. Für monatliche Backups können Sie auch **Unbegrenzt behalten** wählen, falls Sie diese für immer speichern wollen. Die Standardwerte für jeden Backup-Typ sind wie folgt: Täglich: 7 Tage (empfohlenes Minimum) Wöchentlich: 4 Wochen Monatlich: unbegrenzt Die Aufbewahrungsperiode für wöchentliche Backups muss die für tägliche überschreiten; die Periode für monatliche Backups muss größer sein als die für wöchentliche. Es wird für tägliche Backups eine Aufbewahrungsperiode von wenigstens einer Woche empfohlen.

Stets gilt, dass ein Backup solange nicht gelöscht wird, bis alle auf ihm beruhenden Backups ebenfalls von einer Löschung betroffen sind. Aus diesem Grund kann es sein, dass ein wöchentliches oder monatliches Backup noch einige Tage über sein Ablaufdatum im Archiv verbleibt.

Startet ein Zeitplan mit einem täglichen oder wöchentlichen Backup, so wird an dieser Stelle ein Voll-Backup erstellt.

Beispiele

Jeder Tag der vergangenen Woche, jede Woche des vergangenen Monats

Betrachten wir ein allgemein als nützlich angesehenes GVS-Backup-Schema.

- Dateien jeden Tag sichern, einschließlich am Wochenende
- Ermöglicht die Wiederherstellung von Dateien von jedem der vergangenen sieben Tage
- Zugriff auf die wöchentlichen Backups des vergangenen Monats haben.
- Monatliche Backups unbegrenzt behalten.

Die Parameter des Backup-Schemas können dann wie folgt gesetzt werden.

- Backup starten: **23:00:00 Uhr**
- Sichern: **Alle Tage**
- Wöchentlich/monatlich: **Samstag** (als Beispiel)
- Backups aufbewahren:
  - Täglich: **1 Woche**
  - Wöchentlich: **1 Monat**
  - Monatlich: **unbegrenzt**

Als Ergebnis wird ein Archiv aus täglichen, wöchentlichen und monatlichen Backups erstellt. Tägliche Backups sind für die sieben Tage seit Erstellung verfügbar. Ein Beispiel: Ein tägliches Backup vom Sonntag (1. Januar) wird bis zum nächsten Sonntag (8. Januar) verfügbar sein, das erste wöchentliche Backup vom Samstag (7. Januar) wird auf dem System bis zum 7. Februar gespeichert. Monatliche Backups werden nie gelöscht.

Begrenzte Speicherung

Sofern Sie nicht eine Unmenge von Platz zur Speicherung eines riesigen Archivs einrichten wollen, sollten Sie ein GVS-Schema aufsetzen, welches Ihre Backups kurzlebiger macht, gleichzeitig aber auch sicherstellt, dass Ihre Informationen im Fall eines unbeabsichtigten Datenverlustes wiederhergestellt werden können.

Angenommen, Sie müssen:

- Backups am Ende eines jeden Arbeitstages durchführen
- fähig sein, eine versehentlich gelöschte oder ungewollt modifizierte Datei wiederherzustellen, falls dies relativ schnell entdeckt wurde
- zehn Tage nach seiner Erstellung noch Zugriff auf ein wöchentliches Backup haben
- monatliche Backups für ein halbes Jahr aufbewahren.

Die Parameter des Backup-Schemas können dann wie folgt gesetzt werden.

- Backup starten: **18:00:00 Uhr**
- Sichern: **Werktags**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **1 Woche**
  - Wöchentlich: **10 Tage**

- Monatlich: **6 Monate**

Mit Hilfe dieses Schemas steht Ihnen eine Woche zur Verfügung, um die frühere Version einer beschädigten Datei aus einem täglichen Backup wiederherzustellen, außerdem haben Sie einen 10-Tage-Zugriff auf wöchentliche Backups. Jedes monatliche Voll-Backup wird über sechs Monate nach seinem Erstelldatum verfügbar sein.

Arbeitsplan

Angenommen, Sie sind Finanzberater in Teilzeit und arbeiten dienstags und donnerstags in einer Firma. An diesen Tagen führen Sie häufig Änderungen an Ihren Finanzdokumenten, Mitteilungen durch und aktualisieren Ihre Tabellenkalkulationen etc. auf Ihrem Notebook. Um diese Daten per Backup zu sichern, wollen Sie vermutlich:

- die Veränderungen an den finanziellen Mitteilungen, Tabellenkalkulationen etc. verfolgen, die Sie dienstags und donnerstags durchgeführt haben (tägliches inkrementelles Backup).
- eine wöchtenliche Zusammenfassung aller Dateiveränderungen seit dem letzten Monat haben (wöchentliche differentielle Backups am Freitag)
- ein monatliches Voll-Backup Ihrer Dateien haben.

Weiterhin sei angenommen, dass Sie sich einen Zugriff auf alle Backups, inkl. der täglichen, für wenigstens sechs Monate bewahren wollen.

Das nachfolgende GVS-Schema passt für diesen Zweck:

- Backup starten: **23:30 Uhr**
- Sichern: **Dienstag, Donnerstag, Freitag**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **6 Monate**
  - Wöchentlich: **6 Monate**
  - Monatlich: **5 Jahre**

Tägliche inkrementelle Backups werden hier dienstags und donnerstags erstellt, zusammen mit an Freitagen durchgeführten wöchentlichen und monatlichen Backups. Beachten Sie, dass um **Freitag** im Feld **Wöchentlich/monatlich** auswählen zu können, Sie ihn zuerst im Feld **Backup an** auswählen müssen.

Ein solches Archiv würde es Ihnen erlauben, Ihre Finanzdokumente vom ersten und letzten Tag der Arbeit zu vergleichen und eine fünfjährige Geschichte aller Dokumente zu haben.

Keine täglichen Backups

Betrachten Sie ein exotischeres GVS-Schema:

- Backup starten: **12:00 Uhr**
- Sichern: **Freitag**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **1 Woche**
  - Wöchentlich: **1 Monat**
  - Monatlich: **unbegrenzt**

Ein Backup wird daher nur freitags durchgeführt. Dies macht Freitag zur einzigen Wahl für wöchentliche und monatliche Backups, ohne dass ein Tag für tägliche Backups bleibt. Das resultierende „Großvater-Vater“-Archiv wird daher nur aus wöchentlichen differentiellen und monatlichen vollständigen Backups bestehen.

Obwohl es möglich ist, GVS für die Erstellung eines solchen Archivs zu verwenden, ist das eigene Schema in dieser Situation flexibler.

Schema Türme von Hanoi

Auf einen Blick

- Bis zu 16 Level mit vollständigen, differentiellen und inkrementellen Backups
- Backups des nächsten Levels sind doppelt so selten wie die des vorherigen Levels
- Es wird jeweils ein Backup eines Levels gespeichert.
- Eine höhere Dichte hin zu jüngeren Backups

Parameter

Sie können beim Schema Türme von Hanoi die folgenden Parameter einstellen.

Planung	Einen täglichen (S. 86), wöchentlichen (S. 88) oder monatlichen (S. 90) Zeitplan einstellen. Beim Konfigurieren der Plan-Einstellungen können Sie sowohl einfache Zeitpläne erstellen (Beispiel für einen einfachen täglichen Zeitplan: ein Backup-Task wird täglich um 10 Uhr ausgeführt) – genauso wie auch komplexere Zeitpläne (Beispiel für einen komplexen täglichen Plan: ein Task wird jeden dritten Tag ausgeführt, beginnend vom 15. Januar. An den betreffenden Tagen wird der Task alle 2 Stunden von 10:00 bis 22:00 Uhr wiederholt). Auf diese Weise spezifizieren komplexe Zeitpläne die Sitzungen, an denen das Schema ausgeführt werden soll. In der nachfolgenden Betrachtung können „Tage“ durch „geplante Sitzungen“ ersetzt werden.
Zahl der Level	Bestimmen Sie zwischen 2 bis 16 Backup-Level. Zu Details siehe die nachfolgend dargestellten Beispiele.
Roll-Back Periode	Garantierte Zahl von Sitzungen, die Sie jederzeit im Archiv zurückgehen können. Automatisch kalkuliert, abhängig von den Zeitplan-Parametern und der gewählten Level-Zahl. Zu Details siehe das nachfolgend dargestellte Beispiel.

Beispiel

Die **Zeitplan**-Parameter sind wie folgt eingestellt

- Wiederholen: Jeden Tag
- Frequenz: Einmalig um 18:00 Uhr

Zahl der Level: 4

So sieht der Zeitplan der ersten 14 Tage (oder 14 Sitzungen) für dieses Schema aus. Schattierte Zahlen kennzeichnen die Backup-Level.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Die Backups unterschiedlicher Level haben unterschiedliche Typen:

- *Letzte-Ebene*-Backups (hier Ebene 4) sind Voll-Backups;
- Die Backups von *Zwischen-Leveln* (2, 3) sind differentiell;
- *Erste-Ebene* -Backups (1) sind inkrementell.

Ein Bereinigungsmechanismus stellt sicher, dass nur die jeweils neusten Backups jeder Ebene behalten werden. So sieht das Archiv am 8. Tag aus, ein Tag vor Erstellung eines neuen Voll-Backups.

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

Das Schema erlaubt eine effiziente Datenspeicherung: mehr Backups sammeln sich zur gegenwärtigen Zeit hin an. Mit vier Backups können Sie die Daten von heute, gestern, vor einer halben oder einer ganzen Woche wiederherstellen.

Roll-Back Periode

Die Zahl der Tage, die Sie im Archiv zurückgehen können, variiert in Abhängigkeit von den Tagen: Die garantiert verfügbare, minimale Zahl an Tagen wird Roll-Back Periode genannt.

Die nachfolgende Tabelle zeigt Voll-Backups und Roll-Back Perioden für Schemata mit unterschiedlichen Leveln.

Zahl der Level	Voll-Backup alle	Zurück an unterschiedlichen Tagen	Roll-Back Periode
2	2 Tage	1 bis 2 Tage	1 Tag
3	4 Tage	2 bis 5 Tage	2 Tage
4	8 Tage	4 bis 11 Tage	4 Tage
5	16 Tage	8 bis 23 Tage	8 Tage
6	32 Tage	16 bis 47 Tage	16 Tage

Durch Hinzufügen eines Levels werden Voll-Backup und Roll-back-Perioden jeweils verdoppelt.

Warum die Zahl von Wiederherstellungstagen variiert, ergibt sich aus dem vorherigen Beispiel.

Das sind die verfügbaren Backups am 12. Tag (Zahlen in Grau kennzeichnen gelöschte Backups).

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

Das Backup vom 5. Tag liegt immer noch vor, weil bisher kein neues differentielles Backup für Level 3 erstellt wurde. Da es auf dem Voll-Backup von Tag 1 basiert, ist dieses Backup ebenfalls verfügbar. Dies ermöglicht es, bis zu 11 Tage zurückzugehen, was dem Best-Case-Szenario entspricht.

Am folgenden Tag wird jedoch ein neues differentielles Backup der dritten Ebene erstellt und das alte Voll-Backup gelöscht.

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

Dies ermöglicht nur ein Wiederherstellungs-Intervall von 4 Tagen, was dem Worst-Case-Szenario entspricht.

Am Tag 14 beträgt das Intervall 5 Tage. Es steigt an den nachfolgenden Tagen, bevor es wieder abnimmt – und so weiter.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Die Roll-Back-Periode verdeutlicht, wie viele Tage auch im schlimmsten Fall garantiert verfügbar sind. Bei einem Vier-Level-Schema beträgt sie vier Tage.

Benutzerdefiniertes Backup-Schema

Auf einen Blick

- benutzerdefinierte Zeitplanung und Bedingungen für Backups jeden Typs
- benutzerdefinierte Zeitplanung und Aufbewahrungsregeln

Parameter

Parameter	Bedeutung
Voll-Backup	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein Voll-Backup durchgeführt werden soll. Ein Beispiel: Das Voll-Backup kann zur Ausführung an jedem Sonntag um 1:00 Uhr angesetzt werden, sobald alle Benutzer abgemeldet wurden.
Inkrementell	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein inkrementelles Backup durchgeführt werden soll. Anstelle des inkrementellen wird ein Voll-Backup erstellt, sofern das Archiv zum Zeitpunkt der Task-Ausführung kein Voll-Backup enthält.
Differentiell	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein differentielles Backup durchgeführt werden soll. Anstelle des differentiellen wird ein Voll-Backup erstellt, sofern das Archiv zum Zeitpunkt der Task-Ausführung kein Voll-Backup enthält.
Archiv bereinigen	Gibt an, wie alte Backups entfernt werden können: entweder durch das regelmäßige Anwenden von Aufbewahrungsregeln (S. 32) oder durch das Bereinigen des Archivs während eines Backups, wenn am Zielspeicherort kein Platz mehr verfügbar ist. Standardmäßig werden keine Aufbewahrungsregeln angegeben und alte Backups daher nicht automatisch gelöscht. **Aufbewahrungsregeln verwenden** Geben Sie Aufbewahrungsregeln und Kriterien für ihre Anwendung an. Diese Einstellung empfiehlt sich für Backup-Ziele wie z.B. freigegebene Ordner oder zentrale Depots. **Speicherplatzprobleme beim Backup** Das Archiv wird nur während eines Backups bereinigt, sofern nicht ausreichend Speicherplatz für ein neues Backup vorhanden ist. In diesem Fall verhält sich das Programm folgendermaßen: ▪ Das älteste Voll-Backup einschließlich aller abhängigen inkrementellen bzw. differentiellen Backups wird gelöscht ▪ Wenn nur ein vollständiges Backup vorhanden ist und ein neues Voll-Backup gerade erstellt wird, dann wird das letzte vollständige Backup mit allen abhängigen inkrementellen bzw. differentiellen Backups gelöscht. ▪ Wenn nur ein vollständiges Backup vorhanden ist und ein inkrementelles bzw. differentielles Backup gerade erstellt wird, erscheint eine Fehlermeldung, dass nicht genügend freier Speicher vorhanden ist. Diese Einstellung empfiehlt sich bei der Sicherung auf einem USB-Laufwerk oder der Acronis Secure Zone. Die Einstellung ist nicht auf verwaltete Depots anwendbar. Mit dieser Einstellung kann das letzte Backup im Archiv gelöscht werden, falls auf

	dem Speichermedium nicht ausreichend Platz für mehr als ein Backup vorhanden ist. Bedenken Sie jedoch, dass Ihnen damit möglicherweise kein Backup bleibt, falls das Programm aus irgendeinem Grund das neue Backup nicht erstellen kann.
Aufbewahrungsregeln anwenden: (nur wenn Aufbewahrungsregeln erstellt wurden)	Spezifiziert, wann die Aufbewahrungsregeln (S. 32) angewendet werden. Die Bereinigungsprozedur kann z.B. so aufgesetzt werden, dass sie nach jedem Backup und zudem nach Zeitplanung abläuft. Diese Option ist nur dann verfügbar, wenn Sie wenigstens eine Regel in den **Aufbewahrungsregeln** definiert haben.
Zeitplan für Bereinigung (nur wenn **Nach Zeitplan** ausgewählt ist)	Spezifiziert einen Zeitplan zur Bereinigung des Archivs. Die Bereinigung kann z.B. so definiert werden, dass sie planmäßig am letzten Tag eines jeden Monats startet. Diese Option ist nur verfügbar, wenn Sie **Nach Zeitplan** unter **Regeln anwenden** gewählt haben.

Beispiele

Wöchentliches Voll-Backup

Das folgende Schema bringt ein Voll-Backup hervor, das jede Freitagnacht erstellt wird.

Voll-Backup: **Planung: Wöchentlich** jeden **Freitag** um **22:00 Uhr**

Hier werden alle Parameter außer **Planung** bei **Voll-Backup** leer gelassen. Alle Backups in diesem Archiv werden unbegrenzt behalten (es wird keine Bereinigung des Archivs vorgenommen).

Voll- und inkrementelles Backup plus Bereinigung

Mit dem nachfolgenden Schema wird das Archiv aus wöchentlichen Voll-Backups und täglichen inkrementellen Backups bestehen. Eine zusätzliche Bedingung ist, dass ein Voll-Backup nur startet, wenn sich alle Benutzer abgemeldet haben.

Voll-Backup: Planung: Wöchentlich jeden **Freitag** um **22:00 Uhr**

Voll-Backup: Bedingungen: Benutzer ist abgemeldet

Inkrementell: Planung: Wöchentlich, an jedem Werktag um **21:00 Uhr**

Weiterhin sollen alle Backups, die älter als ein Jahr sind, aus dem Archiv gelöscht und die Bereinigung nach Erstellung eines neuen Backups durchgeführt werden.

Aufbewahrung: Lösche Backups älter als **12 Monate**

Aufbewahrungsregeln anwenden: Nach Backup

Vorgegeben ist, dass einjährige Backups solange nicht gelöscht werden, bis alle davon abhängenden inkrementellen Backups ebenfalls Objekt einer Löschaktion werden. Weitere Informationen finden Sie bei Aufbewahrungsregeln (S. 32).

Monatliche Voll-, wöchentliche differentielle und tägliche inkrementelle Backups plus Bereinigung

Dieses Beispiel demonstriert die Verwendung aller im benutzerdefinierten Schema verfügbaren Optionen.

Angenommen, Sie benötigen ein Schema, das monatliche Voll-Backups, wöchentliche differentielle und tägliche inkrementelle Backups produziert. Die Backup-Planung sieht dann wie folgt aus.

Voll-Backup: Planung: Monatlich jeden **letzten Sonntag** des Monats um **21:00 Uhr**

Inkrementell: Planung: Wöchentlich jeden **Werktag** um **19:00 Uhr**

Differentiell: Planung: Wöchentlich jeden **Samstag** um **20:00 Uhr**

Weiterhin wollen Sie Bedingungen hinzufügen, die erfüllt sein müssen, damit ein Backup-Task startet. Diese werden im Feld **Bedingungen** für jeden Backup-Typ eingestellt.

Voll-Backup: **Bedingungen**: **Speicherort verfügbar**

Inkrementell: **Bedingungen**: **Benutzer ist abgemeldet**

Differentiell: **Bedingungen**: **Benutzer ist untätig**

Als Folge startet ein Voll-Backup – ursprünglich für 21:00 geplant – möglicherweise später: sobald der Backup-Speicherort verfügbar wird. Vergleichbar warten die Backup-Tasks für inkrementelle bzw. differentielle Backups solange, bis alle Benutzer abgemeldet bzw. untätig sind.

Abschließend erstellen Sie Aufbewahrungsregeln für das Archiv: Behalten Sie nur Backups, die nicht älter als sechs Monate sind, und lassen Sie die Bereinigung nach jedem Backup-Task sowie an jedem letzten Tag eines Monats ausführen.

Aufbewahrungsregeln: Lösche Backups älter als **6 Monate**

Aufbewahrungsregeln anwenden: **Nachdem Backup**, **nach Planung**

Planung für die Bereinigung: **Monatlich** am **letzten Tag** von **allen Monaten** um **22:00 Uhr**

Standardmäßig wird ein Backup solange nicht gelöscht, wie es abhängige Backups hat, die behalten werden müssen. Wird z.B. ein Voll-Backup einer Löschaktion unterworfen, während es noch inkrementelle oder differentielle, von ihm abhängende Backups gibt, so wird die Löschung solange verschoben, bis alle abhängenden Backups ebenfalls gelöscht werden können.

Weitere Informationen finden Sie bei Aufbewahrungsregeln (S. 32).

Resultierende Tasks

Jedes benutzerdefinierte Schema produziert immer drei Backup-Tasks und – für den Fall, dass Aufbewahrungsregeln definiert wurden – einen Bereinigungs-Task. In der Task-Liste wird jeder Task entweder als **Geplant** (wenn eine Zeitplanung eingestellt wurde) oder als **Manuell** (wenn keine Zeitplanung eingestellt wurde) aufgeführt.

Sie können jeden Backup- oder Bereinigungs-Task jederzeit starten, unabhängig davon, ob er eine Zeitplanung hat.

Im ersten der zurückliegenden Beispiele wurde eine Zeitplanung nur für Voll-Backups aufgesetzt. Das Schema resultiert dennoch in drei Backup-Tasks, die Ihnen den manuellen Start eines jeden Backup-Typs ermöglichen:

- Voll-Backup, läuft jeden Freitag um 22:00 Uhr.
- Inkrementelles Backup, läuft manuell
- Differentielles Backup, läuft manuell

Sie können jeden dieser Backup-Tasks ausführen, indem Sie ihn aus der Task-Liste im Abschnitt **Backup-Pläne und Tasks** des linken Fensterbereichs wählen.

Das Schema resultiert in vier Tasks, wenn Sie außerdem Aufbewahrungsregeln in ihrem Backup-Schema spezifiziert haben: drei Backup-Tasks und ein Bereinigungs-Task.

6.2.11 Archiv validieren

Setzen Sie einen Validierungs-Task auf, um zu überprüfen, ob gesicherte Daten wiederherstellbar sind. Der Validierungs-Task scheitert und der Backup-Plan erhält den Status „Fehler“, wenn das Backup die Überprüfung nicht erfolgreich bestehen konnte.

Spezifizieren Sie die folgenden Parameter, um eine Validierung anzulegen

1. **Validierungs-Zeitpunkt** – bestimmen Sie, wann die Validierung durchgeführt wird. Da eine Validierung eine Ressourcen-intensive Aktion ist, empfiehlt es sich, sie so zu **planen**, dass sie nicht zu Hauptbelastungszeiten der verwalteten Maschine erfolgt. Wenn die Validierung dagegen ein wichtiger Teil Ihrer Strategie zur Datensicherung ist und Sie es bevorzugen, sofort informiert zu werden, ob die gesicherten Daten intakt und daher erfolgreich wiederherstellbar sind, dann sollten Sie die Validierung direkt nach Backup-Erstellung durchführen.
2. **Was validieren** – bestimmen Sie, ob das komplette Archiv oder das letzte Backup im Archiv überprüft wird. Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Die Validierung eines Image-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Die Validierung eines Archivs überprüft alle Backups des Archivs und kann viel Zeit sowie System-Ressourcen benötigen.
3. **Validierungs-Zeitplan** (erscheint nur, falls Sie in Schritt 1 „Nach Zeitplan“ ausgewählt haben) – definiert den Zeitplan für die Validierung. Zu weiteren Informationen siehe den Abschnitt Zeitplanung (S. 85).

6.3 Daten wiederherstellen

Wenn eine Daten-Wiederherstellung ansteht, sollten Sie als Erstes berücksichtigen, welches die funktionellste Methode ist: Verbinden Sie die Konsole mit der verwalteten, **das Betriebssystem ausführenden Maschine** und erstellen Sie den Recovery-Task.

Sollte auf der verwalteten Maschine **das Betriebssystem nicht mehr starten** oder sollten Sie eine **Wiederherstellung auf fabrikneue Hardware** durchführen müssen, so booten Sie die Maschine von einem bootfähigen Medium (S. 188) oder durch Verwendung des Acronis Startup Recovery Managers (S. 42). Erstellen Sie dann einen Recovery-Task.

Um Linux-Software-RAID-Geräte (auch bekannt als **MD-Geräte**) bzw. Geräte wiederherzustellen, die durch den Logical Volume Manager (LVM) (auch bekannt als **logische Volumes** erzeugt wurden, müssen Sie vor der Wiederherstellung erst manuell die korrespondierende Volume-Struktur erzeugen. Weitere Informationen dazu finden Sie unter „MD-Geräte und logische Volumes wiederherstellen (S. 179)“.

Zur Erstellung eines Recovery-Tasks führen Sie folgende Schritte aus

Allgemein

Task-Name

[Optional] Geben Sie einen eindeutigen Namen für den Recovery-Task ein. Ein bewusst gewählter Name macht es leichter, diesen Task zu identifizieren.

Anmeldedaten für den Task (S. 138)

[Optional] Der Task wird im Namen des Benutzers laufen, der den Task erstellt. Sie können, sofern notwendig, die Konto-Anmeldedaten für den Task ändern. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Recovery-Quelle

Archiv (S. 138)

Wählen Sie das Archiv, aus dem die Daten wiederhergestellt werden sollen.

Datentyp (S. 139)

Angewendet auf: Laufwerk-Recovery

Bestimmen Sie den Datentyp, den Sie von dem gewählten Laufwerk-Backup wiederherstellen müssen.

Inhalt (S. 140)

Bestimmen Sie das Backup und den wiederherzustellenden Inhalt.

Anmeldedaten (S. 141)

[Optional] Stellen Sie Anmeldedaten für den Speicherort des Archivs zur Verfügung, falls das Benutzerkonto des Tasks für diesen keine Zugriffserlaubnis hat. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Recovery-Ziel

Dieser Abschnitt erscheint, nachdem das benötigte Backup gewählt und der wiederherzustellende Datentyp definiert wurde. Die von Ihnen hier anzugebenden Parameter hängen vom wiederherzustellenden Datentyp ab.

Laufwerke

Volumes

Dateien (S. 145)

Sie müssen möglicherweise Anmeldedaten für den Zielort angeben. Überspringen Sie diesen Schritt, wenn Sie auf einer Maschine arbeiten, die Sie mit einem bootfähigen Medium gestartet haben.

Anmeldedaten (S. 146)

[Optional] Stellen Sie die Anmeldedaten für den Zielort zur Verfügung, falls mit den Anmeldedaten des Tasks keine Wiederherstellung der Daten möglich ist. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Recovery-Zeitpunkt

Recovery (S. 147)

Bestimmen Sie, wann die Wiederherstellung beginnen soll. Der Task kann unmittelbar nach Erstellung starten, für einen bestimmten Tag bzw. Zeitpunkt geplant werden oder auch einfach nur zur manuellen Ausführung gespeichert werden.

Recovery-Optionen

Einstellungen

[Optional] Passen Sie die Aktion durch Konfiguration der Recovery-Optionen an, z.B. Vor-/Nach-Befehle, Recovery-Priorität, Fehlerhandhabung oder Benachrichtigungsoptionen. Sofern Sie in diesem Abschnitt nichts tun, werden die Standardwerte (S. 68) verwendet.

Wird irgendeine Einstellung gegenüber dem Standardwert geändert, so wird der neue Wert über eine Zeile angezeigt. Die Statusanzeige über die Einstellungen ändert sich von **Standard** zu **Benutzerdefiniert**. Sollten Sie die Einstellung erneut ändern, so wird die Zeile ebenfalls

den neuen Wert anzeigen, sofern er nicht dem Standardwert entspricht. Die Zeile verschwindet beim Setzen des Standardwerts, daher sehen Sie immer nur Werte, die von den vorgegebenen im Abschnitt **Einstellungen** abweichen.

Ein Klick auf **Auf Standard zurücksetzen** setzt alle Einstellungen auf die Standardwerte zurück.

Nachdem Sie alle benötigten Schritte abgeschlossen haben, klicken Sie auf **OK**, um den Recovery-Task erstellen zu lassen.

6.3.1 Anmeldedaten für den Task

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, mit dem der Task ausgeführt wird.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Unter dem aktuellen Benutzer ausführen**

     Der Task wird mit den Anmeldedaten des Benutzers ausgeführt, der die Tasks startet. Wenn der Task nach Zeit-/Ereignis-Planung laufen soll, werden Sie bei Abschluss der Task-Erstellung nach dem Passwort des aktuellen Benutzers gefragt.
   - **Folgende Anmeldedaten benutzen**

     Der Task wird immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Zu weiteren Informationen über die Verwendung von Anmeldedaten in Acronis Backup & Recovery 10 siehe den Abschnitt Besitzer und Anmeldedaten (S. 23).

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 23), um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

6.3.2 Auswahl des Archivs

Auswahl des Archivs

1. Tragen Sie den vollständigen Pfad zum Speicherort in das Feld **Pfad** ein oder wählen Sie den gewünschten Ort im Verzeichnisbaum.
   - Falls das Archiv auf dem Acronis Online Backup Storage gespeichert wurde, klicken Sie auf **Anmelden** und geben anschließend die Anmeldedaten zum Zugriff auf den Online Storage ein. Erweitern Sie dann die Gruppe **Online Backup Storage** und wählen Sie das Konto.

   Auf dem Acronis Online Backup Storage gespeicherte Backups können nicht exportiert oder gemountet werden.
   - Um die Archive in einem zentralen Depot abzulegen, erweitern Sie die Gruppe **Zentral** und wählen dort dieses Depot.
   - Um die Archive in einem persönlichen Depot abzulegen, erweitern Sie die Gruppe **Persönlich** und wählen dort dieses Depot.

- Wenn das Archiv in einem lokalen Ordner auf der Maschine gespeichert ist, erweitern Sie die Gruppe **Lokale Ordner** und wählen das gewünschte Verzeichnis.

Wenn sich das Archiv auf Wechselmedien befindet, z.B. auf DVDs, legen Sie zuerst die letzte DVD ein und dann, nach Aufforderung durch das Programm, die Datenträger von Beginn an in der richtigen Reihenfolge.

- Wenn das Archiv auf einer Netzwerkfreigabe gespeichert ist, erweitern Sie die Gruppe **Netzwerk-Ordner**, wählen dann die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

Hinweis für Linux-Benutzer: *Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Point (etwa /mnt/share) angeschlossen ist, wählen Sie diesen Mount-Point statt der Netzwerkfreigabe aus.*

- Wenn das Archiv auf einem **FTP-** oder **SFTP-**Server gespeichert ist, tragen Sie Servername oder Adresse im Feld **Pfad** folgendermaßen ein:

  ftp://ftp_server:port _number oder sftp://sftp_server:port number

  Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP.

  Nach Eintragen der Anmeldinformationen sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server.

  Sie können auf den Server auch als Benutzer 'anonymous' zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

- Wenn die Daten auf einem lokal angeschlossenen Bandgerät gespeichert sind, erweitern Sie die Gruppe **Bandlaufwerke** und klicken auf das benötigte Gerät.

Bei Ausführung auf einer Maschine, die mit einem bootfähigen Medium gestartet wurde:

- Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein:

  bsp://knoten_adresse/depot_name/

- Um auf ein nicht verwaltetes zentrales Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.

2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die im gewählten Depot bzw. Ordner enthalten sind.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.
3. Klicken Sie auf **OK**.

6.3.3 Datentyp

Bestimmen Sie den Datentyp, den Sie von dem gewählten Disk-Backup wiederherstellen wollen:

- **Festplatten** – um Festplatten wiederherzustellen
- **Partitionen** – um Partitionen wiederherzustellen
- **Dateien** – um bestimmte Dateien und Ordner wiederherzustellen

6.3.4 Auswahl des Inhalts

Die Darstellung in diesem Fenster hängt vom Typ der Daten ab, die im Archiv gespeichert sind.

Wahl der Festplatten/Partitionen

So wählen Sie ein Backup sowie die Festplatten/Partitionen zur Wiederherstellung:

1. Bestimmen Sie eines der aufeinander folgenden Backups anhand des Zeitstempels. Auf diese Weise können Sie die Daten der Festplatte auf einen bestimmten Zeitpunkt zurücksetzen.

   Spezifizieren Sie die wiederherzustellenden Elemente. Standardmäßig sind alle Elemente des angegebenen Backups ausgewählt. Wollen Sie bestimmte Elemente nicht wiederherstellen, so deaktivieren Sie die Auswahl.
   Um Informationen über eine Festplatte/Partition zu erhalten, klicken Sie auf diese mit der rechten Maustaste und wählen dann **Informationen**.
2. Klicken Sie auf **OK**.

Einen MBR wählen

Sie wählen normalerweise den MBR der Festplatte aus, wenn:

- das Betriebssystem nicht booten kann
- die Festplatte neu ist und keinen MBR hat
- Sie maßgeschneiderte bzw. Nicht-Windows-Boot-Loader (wie LILO und GRUB) wiederherstellen
- die Festplatten-Geometrie von der im Backup gespeicherten abweicht.

Es gibt vermutlich noch andere Situationen, bei denen Sie den MBR wiederherstellen müssen, aber die oberen sind die häufigsten.

Bei Wiederherstellung eines MBR von einem auf ein anderes Laufwerk stellt Acronis Backup & Recovery 10 auch Track 0 (Spur Null) wieder her, was keinen Einfluss auf die Partitionstabelle und das Partitionslayout des Ziellaufwerks hat. Acronis Backup & Recovery 10 aktualisiert nach einer Wiederherstellung automatisch die Windows Boot-Loader, daher ist es bei Windows-Systemen nicht notwendig, den MBR und Track 0 wiederherzustellen, außer der MBR ist beschädigt.

Auswahl von Dateien

So wählen Sie ein Backup und Dateien zur Wiederherstellung:

1. Bestimmen Sie eines der aufeinander folgenden Backups anhand seines Zeitstempels. Auf diese Weise können Sie die Dateien/Ordner auf einen bestimmten Zeitpunkt zurücksetzen.
2. Spezifizieren Sie die wiederherzustellenden Dateien und Ordner durch Auswahl der korrespondierenden Kontrollkästchen im Verzeichnisbaum des Archivs.

   Bei Wahl eines Ordners werden automatisch auch alle darin enthaltenen Ordner und Dateien ausgewählt.

   Verwenden Sie die rechts im Verzeichnisbaum des Archivs liegende Tabelle, um die Unterelemente auszuwählen. Die Aktivierung des Kontrollkästchens für den Spaltenkopf **Name** wählt automatisch alle Elemente der Tabelle aus. Durch Deaktivierung des Kontrollkästchens werden alle Elemente automatisch abgewählt.
3. Klicken Sie auf **OK**.

6.3.5 Anmeldedaten für den Speicherort

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das Backup-Archiv gespeichert ist.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Das Programm greift auf den Speicherort unter Verwendung derjenigen Task-Konto-Anmeldedaten zu, wie sie im Abschnitt „Allgemein“ spezifiziert wurden.
   - **Folgende Anmeldedaten benutzen**

     Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

6.3.6 Auswahl des Ziels

Spezifizieren Sie das Ziel, zu dem die gewählten Daten wiederhergestellt werden.

Laufwerke

Die verfügbaren Laufwerksziele hängen davon ab, welcher Agent auf der Maschine arbeitet.

Recovery nach:

Physikalische Maschine

Die gewählten Laufwerke werden zu den physikalischen Laufwerken der Maschine wiederhergestellt, mit der die Konsole verbunden ist. Auf diese Auswahl hin fahren Sie dann mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Laufwerk Nr.:

Laufwerk Nr. (MODELL) (S. 143)

Bestimmten Sie für jedes Quelllaufwerk das entsprechende Ziellaufwerk.

NT-Signatur (S. 142)

Bestimmten Sie, auf welche Art die wiederhergestellte Disk-Signatur gehandhabt wird. Eine Disk-Signatur wird von Windows sowie Linux-Kernel Version 2.6 und später verwendet.

Zielfestplatte

So spezifizieren Sie ein Ziellaufwerk:

1. Bestimmen Sie eine Festplatte, wohin Sie die gewählte Festplatte wiederhergestellt haben wollen. Der Platz der Zielfestplatte sollte mindestens die Größe der unkomprimierten Daten des Images haben.
2. Klicken Sie auf **OK**.

Alle auf der Zielfestplatte gespeicherten Daten werden durch die im Backup befindlichen Daten ersetzt, seien Sie also vorsichtig und achten Sie auf noch nicht gesicherte Daten, die noch benötigt werden.

NT-Signatur

Wird zusammen mit einem Disk-Backup auch der MBR gesichert, so müssen Sie die Bootfähigkeit des Betriebssystems auch für die Partition der Zielfestplatte bewahren. Das Betriebssystem muss eine zu den Informationen der Systempartition (z.B. Laufwerksbuchstabe) passende NT-Festplatten-Signatur haben (welche im Master Boot Record hinterlegt ist). Zwei Festplatten mit derselben NT-Signatur können jedoch nicht richtig unter einem Betriebssystem arbeiten.

Wenn aber auf einer Maschine zwei Festplatten, die ein System-Laufwerk enthalten, dieselbe NT-Signatur haben, so startet das Betriebssystem von der ersten Festplatte, erkennt dabei die gleiche Signatur auf der zweiten Festplatte, erzeugt automatisch eine neue, eindeutige NT-Signatur und weist diese dann der zweiten Platte zu. Als Konsequenz verlieren darauf dann alle Volumes des zweiten Laufwerks ihre Laufwerksbuchstaben, werden Verzeichnispfade ungültig und können Programme ihre Dateien nicht mehr finden. Das Betriebssystem auf dieser Festplatte kann daher auch nicht mehr booten.

Um die Bootfähigkeit des Systems auf der Partition der Zielfestplatte zu bewahren, wählen Sie eine der folgenden Möglichkeiten:

- **Automatische Auswahl**

  Eine neue NT-Signatur wird nur erstellt, wenn die bestehende Signatur nicht identisch mit der im Backup ist. Andernfalls wird die bestehende NT-Signatur beibehalten.
- **Neu erstellen**

  Das Programm wird eine neue NT-Signatur für die Zielfestplatte erstellen.
- **Aus dem Backup wiederherstellen**

  Das Programm wird die NT-Signatur auf der Zielfestplatte mit einer aus dem Disk-Backup ersetzen.

  Eine Wiederherstellung der Laufwerkssignatur kann aus folgenden Gründen wünschenswert sein:
  - Acronis Backup & Recovery 10 erstellt geplante Tasks unter Verwendung der Signatur der Quellfestplatte. Sie müssen kürzlich erzeugte Tasks nicht neu erstellen oder bearbeiten, wenn Sie dieselbe Disk-Signatur wiederherstellen.
  - Einige installierte Anwendungen verwenden eine Disk-Signatur zur Lizenzierung oder für andere Einsatzzwecke.
- **Existierende erhalten**

  Das Programm belässt die existierende NT-Signatur der Zielfestplatte wie sie ist.

Volumes

Die verfügbaren Ziele für Volumes hängen davon ab, welcher Agent auf der Maschine arbeitet.

Recovery nach:

Physikalische Maschine

Die gewählten Volumes (Partitionen) werden zu den physikalischen Laufwerken der Maschine wiederhergestellt, mit der die Konsole verbunden ist. Auf diese Auswahl hin fahren Sie dann mit der nachfolgend beschriebenen, regulären Laufwerks-Mapping-Prozedur fort.

[Disk Nr.] MBR wiederherstellen auf: [wenn der Master Boot Record für die Wiederherstellung ausgewählt ist]

Laufwerk Nr. (S. 143)

Wählen Sie das Laufwerk, auf der der Master Boot Record wiederhergestellt wird.

NT-Signatur: (S. 142)

Bestimmen Sie, wie die Laufwerk-Signatur im MBR gehandhabt wird. Eine Disk-Signatur wird von Windows sowie Linux-Kernel Version 2.6 und später verwendet.

[Volume] wiederherstellen auf:

Laufwerk Nr. /Volume (S. 143)

Ordnen Sie nacheinander jedem Quell-Volume einem Volume des Ziellaufwerkes oder 'nicht zugeordnetem' Speicherplatz zu.

Größe:

[Optional] Ändern Sie Größe, Position oder andere Eigenschaften des wiederhergestellten Volumes.

MBR-Ziel

So spezifizieren Sie ein Ziellaufwerk:

1. Wählen Sie das Ziellaufwerk aus, auf dem Sie den MBR wiederherstellen möchten.
2. Klicken Sie auf **OK**.

Ziel für ein Volume

So spezifizieren Sie ein Ziel für ein Volume:

1. Bestimmen Sie ein Volume oder nicht zugeordneten Festplattenplatz, wohin Sie das gewählte Volume wiederherstellen wollen. Das Ziel-Volume bzw. der nicht zugeordnete Speicherplatz sollten mindestens die Größe der unkomprimierten Daten des Images haben.
2. Klicken Sie auf **OK**.

Alle auf dem Ziel-Volume gespeicherten Daten werden durch die im Backup befindlichen Daten ersetzt, seien Sie also vorsichtig und achten Sie auf noch nicht gesicherte Daten, die noch benötigt werden.

Bei Verwendung bootfähiger Medien

Laufwerksbuchstaben, die unter Windows-basierten Boot-Medien zu sehen sind, können von der Art abweichen, wie Windows normalerweise Laufwerke identifiziert. So könnte z.B. die Zuordnung des Laufwerks D: unter dem Rettungs-Utility dem Laufwerk E: entsprechen, das unter Windows erscheint.

Achtung! Um sicherzugehen ist es ratsam, den Laufwerken eindeutige Namen zuzuweisen.

Ein Linux-basiertes bootfähiges Medium zeigt lokale Festplatten und Volumes als ungeladen an (sda1, sda2...).

Eigenschaften von Partitionen

Größenveränderung und Verlagerung

Sie können bei Wiederherstellung eines Volumes auf ein Basis-Laufwerk vom Typ MBR das Volume in seiner Größe oder Lage verändern, indem Sie dessen Darstellung bzw. Ränder mit der Maus verschieben oder indem Sie korrespondierende Werte in die entsprechenden Felder eingeben. Durch Verwendung dieser Funktion können Sie den Speicherplatz zwischen den wiederherzustellenden Volumes aufteilen. In diesem Fall müssen Sie zuerst das Volume wiederherstellen, welches in seiner Größe reduziert werden soll.

Tipp: *Die Größe eines Volumes kann nicht angepasst werden, wenn es aus einem Backup wiederhergestellt wird, das auf mehrere DVDs oder Bänder aufgeteilt wurde. Um die Größe des Volumes zu ändern, kopieren Sie alle Teile des Backups an einen einzigen Speicherort auf einer Festplatte (oder ähnlichem Laufwerk).*

Eigenschaften

Typ

Ein Basis-Laufwerk vom Typ MBR kann bis zu vier primäre Volumes enthalten – oder bis zu drei primäre Volumes sowie ein bis mehrere logische Laufwerke. Das Programm wählt standardmäßig den ursprünglichen Typ des Volumes. Sie können diese Einstellung ändern (falls erforderlich).

- **Primär**. Die Informationen über primäre Volumes sind in der MBR-Partitionstabelle enthalten. Die meisten Betriebssysteme können nur von einem primären Volume auf dem ersten Laufwerk booten, zudem ist die Zahl primärer Volumes limitiert.

  Wählen Sie bei Wiederherstellung eines System-Volumes auf ein Basis-Laufwerk vom Typ MBR das Kontrollkästchen 'Aktiv'. Ein aktives Volume wird zum Starten eines Betriebssystems verwendet. Wenn Sie jedoch 'Aktiv' für ein Volume ohne installiertes Betriebssystem wählen, kann das die Maschine daran hindern, zu booten. Ein logisches Laufwerk oder ein dynamisches Volume kann nicht auf 'Aktiv' gesetzt werden.
- **Logisch**. Die Informationen über logische Volumes sind nicht im MBR, sondern in der erweiterten Partitionstabelle hinterlegt. Die Anzahl logischer Volumes auf einer Festplatte (oder ähnlichem Laufwerk) ist nicht limitiert. Ein logisches Volume kann nicht als 'Aktiv' gesetzt werden. Wenn Sie ein System-Volume auf ein anderes Laufwerk mit eigenen Volumes (Partitionen) und Betriebssystem wiederherstellen, benötigen Sie wahrscheinlich nur die entsprechenden Daten. In diesem Fall können Sie das Volume auch als logisches Laufwerk wiederherstellen, um lediglich auf seine Daten zuzugreifen.

Dateisystem

Ändern Sie, falls benötigt, das Dateisystem der Partition. Das Programm wählt standardmäßig das ursprüngliche Dateisystem der Partition. Acronis Backup & Recovery 10 kann folgende Dateisysteme zueinander konvertieren: FAT16 –> FAT32 und Ext2 –> Ext3. Für Volumes mit anderen nativen Dateisystemen ist diese Option nicht verfügbar.

Angenommen, Sie wollen ein Volume von einem alten FAT16-Laufwerk mit niedriger Kapazität auf einer neueren Festplatte wiederherstellen. FAT16 wäre nicht effektiv und es könnte unter Umständen auch unmöglich sein, dieses Dateisystem auf das neue Laufwerk zu übertragen. Hintergrund ist, dass FAT16 nur Volumes bis 4GB unterstützt, daher können Sie ein 4GB FAT16-Volume nicht ohne Änderung des Dateisystems auf ein Laufwerk wiederherstellen, welches über dieser Begrenzung liegt. In diesem Fall wäre es sinnvoll, das Dateisystem von FAT16 zu FAT32 zu wechseln.

Ältere Betriebssysteme (MS-DOS, Windows 95 und Windows NT 3.x, 4.x) unterstützen jedoch kein FAT32 und sind daher nicht betriebsbereit, nachdem Sie das Volume wiederhergestellt und das Dateisystem geändert haben. Diese können normalerweise nur auf ein FAT16-Volume wiederhergestellt werden.

Logische Laufwerksbuchstaben (nur für Windows)

Weisen Sie der wiederhergestellten Partition einen Laufwerksbuchstaben zu. Wählen Sie den gewünschten Buchstaben aus einen Listenfeld.

- Mit der Standardauswahl „AUTO“ wird der Partition der erste freie Buchstabe zugewiesen.
- Wählen Sie dagegen „Nein“, so erhält das wiederhergestellte Laufwerk keinen Buchstaben, womit es vom Betriebssystem verborgen wird. Sie sollten solchen Partitionen keinen Laufwerksbuchstaben zuweisen, auf die Windows nicht zugreifen kann, z.B. mit Dateisystemen anders als FAT oder NTFS.

Ziel für Dateien

So spezifizieren Sie ein Ziel:

1. Wählen Sie einen Speicherort, in den die gesicherten Dateien wiederhergestellt werden:
   - **Ursprünglicher Speicherort** – Dateien und Ordner werden zu dem Pfad wiederhergestellt, mit dem sie auch gesichert wurden. Falls Sie z.B. alle Dateien und Ordner aus C:\Dokumente\Finanzen\Berichte\ gesichert hatten, so werden die Daten zu genau diesem Pfad wiederhergestellt. Sollte der Ordner nicht existieren, so wird er automatisch erstellt.
   - **Neuer Speicherort** – die Dateien werden zu dem Speicherort wiederhergestellt, den Sie im Verzeichnisbaum angeben. Dabei werden die Dateien und Ordner ohne Anlegen eines vollständigen Pfades zurückgesichert, es sei denn, Sie deaktivieren das Kontrollkästchen **Ohne absolute Pfade wiederherstellen**.
2. Klicken Sie auf **OK**.

Ausschließungen vom Recovery

Richten Sie Ausschlusskriterien für spezielle Dateien ein, die sie nicht wiederherstellen wollen.

Benutzen Sie die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Alle entfernen**, um die Liste der Dateimasken zu verwalten. Dateien, deren Namen die Kriterien eine dieser Masken erfüllen, werden während der Wiederherstellung übersprungen.

Sie können ein oder mehrere Wildcard-Zeichen (* und ?) in einer Datei-Maske verwenden:

- Das Asterisk (*) steht für Null oder mehrere Zeichen im Dateinamen; so ergibt z.B. die Datei-Maske Doc*.txt Dateien wie Doc.txt und Document.txt.
- Das Fragezeichen (?) steht für exakt ein Zeichen in einem Dateinamen, so ergibt z.B. die Datei-Maske Doc?.txt Dateien wie Doc1.txt und Docs.txt – aber nicht Doc.txt oder Doc11.txt.

Beispiele für Ausschließungen

Kriterium	Beispiel	Beschreibung
Windows und Linux		
Nach Name	F.log F	Schließt alle Dateien namens „F.log“ aus Schließt alle Ordner namens „F“ aus

Per Maske (*)	*.log F*	Schließt alle Dateien mit der Erweiterung „.log“ aus Schließt alle Dateien und Ordner aus, deren Namen mit „F“ beginnen (etwa die Ordner F, F1 und die Dateien F.log, F1.log)
Per Maske (?)	F???.log	Schließt alle .log-Dateien aus, deren Namen am Ende vier Zeichen enthalten und mit „F“ beginnen
Windows		
Per Dateipfad	Finanzen\F.log	Schließt Dateien namens „F.log“ aus allen Ordnern aus, die den Namen „Finanzen“ haben
Per Ordnerpfad	Finanzen\F\ oder Finanzen\F	Schließt Unterordner namens „F“ aus allen Ordnern aus, die den Namen „Finanzen“ haben
Linux		
Per Dateipfad	/home/user/Finanzen/F.log	Schließt die Datei aus, die „F.log“ heißt und im Ordner „/home/user/Finanzen“ vorliegt

Die oberen Einstellungen sind nicht für Dateien oder Ordner wirksam, die ausdrücklich zur Wiederherstellung ausgewählt wurden. Ein Beispiel: Angenommen, Sie haben das Verzeichnis „MeinOrdner“ sowie die (außerhalb dieses Ordners liegende) Datei „MeineDatei.tmp“ gewählt – und festgelegt, dass alle .tmp-Dateien übersprungen werden sollen. In diesem Fall werden alle .tmp-Dateien in „MeinOrdner“ während der Wiederherstellungs-Prozedur übersprungen, jedoch nicht die Datei „MeineDatei.tmp“.

Überschreiben

Bestimmen Sie, was passieren soll, wenn das Programm im Zielordner eine Datei gleichen Namens wie im Archiv findet:

- **Existierende Datei überschreiben** – dies gibt der Datei im Backup eine höhere Priorität als der Datei auf der Festplatte.
- **Existierende Datei überschreiben wenn älter** – Dateien mit den jüngsten Veränderungen erhalten Priorität, egal ob sie im Backup oder auf der Festplatte sind.
- **Existierende Datei nicht überschreiben** – dies gibt der Datei auf der Festplatte eine höhere Priorität als der Datei im Backup.

Falls Sie das Überschreiben von Dateien erlauben, haben Sie dennoch die Option, spezielle Dateien vor dem Überschreiben zu schützen durch Ausschluss (S. 145) aus der Wiederherstellung.

6.3.7 Anmeldedaten für das Ziel

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Das Programm greift auf den Zielort unter Verwendung derjenigen Task-Konto-Anmeldedaten zu, wie sie im Abschnitt 'Allgemein' spezifiziert wurden.
   - **Folgende Anmeldedaten benutzen**

     Das Programm greift auf den Zielort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das Konto des Tasks keine Zugriffserlaubnis für den Zielort hat.

Spezifizieren Sie:

- **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
- **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

6.3.8 Zeitpunkt

Bestimmen Sie, wann der Recovery-Task beginnen soll:

- **Jetzt wiederherstellen** – der Recovery-Task wird gestartet, sobald Sie auf das abschließende **OK** geklickt haben.
- **Später wiederherstellen** – der Recovery-Tasks wird zu dem Tag bzw. Zeitpunkt gestartet, den Sie angeben.

Wenn Sie keine Planung für den Task benötigen und ihn anschließend manuell starten wollen, dann aktivieren Sie das Kontrollkästchen **Task wird manuell gestartet (keine Planung)**.

6.3.9 MD-Geräte für eine Wiederherstellung zusammenstellen (Linux)

Wenn Sie in Linux eine Wiederherstellung von einem Laufwerk-Backup auf ein existierendes MD-Gerät (auch Linux Software-RAID genannt) durchführen, dann stellen Sie sicher, dass dieses **Gerät zusammengestellt** ist (zum Zeitpunkt der Wiederherstellung).

Ist das Gerät nicht verfügbar, so holen Sie dies durch Verwendung des Utilities **mdadm** nach. Hier sind zwei Beispiele:

Beispiel 1. Der folgende Befehl erstellt das Gerät /dev/md0, kombiniert aus den Volumes /dev/sdb1 und /dev/sdc1:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb1 /sdc1
```

Beispiel 2. Der folgende Befehl erstellt das Gerät /dev/md0, kombiniert aus den Disks /dev/sdb und /dev/sdc:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb /dev/sdc
```

Orientieren Sie sich an den nachfolgenden Anleitungen, wenn für die Wiederherstellung ein Neustart der Maschine erforderlich ist (üblich, falls die wiederherzustellenden Volumes ein Boot-Volume enthält):

- Wenn alle Teile des MD-Gerätes Volumes sind (typischer Fall, so wie im ersten Beispiel), dann stellen Sie sicher, dass der Typ eines jeden Volumes (Partitionstyp oder System-ID genannt) vom Typ '**Linux raid automount**' ist — der Hexadezimal-Code dieses Volume- bzw. Partitionstypes ist 0xFD. Dies garantiert, dass das Gerät nach dem Neustart automatisch zusammengestellt wird. Verwenden Sie ein Partitionierungswerkzeug wie **fdisk**, um den Volume-Typ einzusehen oder zu verändern.
- Führen Sie anderenfalls (wie im zweiten Beispiel) die Recovery-Aktion von einem bootfähigen Medium aus. In diesem Fall ist auch kein Neustart erforderlich. Bei Verwendung bootfähiger Medien müssen Sie das MD-Gerät vermutlich manuell oder automatisch erstellen, wie unter MD-Geräte und logische Volumes wiederherstellen (S. 179) beschrieben.

6.3.10 Troubleshooting zur Bootfähigkeit

Wenn ein System zum Zeitpunkt seines Backups bootfähig war, erwarten Sie auch, dass es nach einer Wiederherstellung booten kann. Informationen, die das Betriebssystem zum Booten speichert und verwendet, können jedoch bei einer Wiederherstellung ungültig werden, insbesondere, wenn Sie die Partitionsgröße, Speicherorte oder Ziellaufwerke ändern. Acronis Backup & Recovery 10 aktualisiert Windows Boot-Loader automatisch nach einer Wiederherstellung. Auch andere Boot-Loader werden möglicherweise gefixt, es gibt jedoch Fälle, bei denen Sie selbst die Loader reaktivieren müssen. Speziell, wenn Sie Linux-Partitionen wiederherstellen, ist es manchmal notwendig, Fehlerkorrekturen anzuwenden oder Boot-Veränderungen durchzuführen, damit Linux korrekt startet und geladen werden kann.

Nachfolgend eine Zusammenfassung typischer Situationen, die zusätzliche Benutzereingriffe benötigen.

Warum ein wiederhergestelltes Betriebssystem nicht mehr bootfähig sein kann

- **Das BIOS der Maschine ist so konfiguriert, dass es von einer anderen Festplatte bootet.**

  Lösung: Konfigurieren Sie das BIOS so, dass es von der Festplatte bootet, auf der das Betriebssystem liegt.

- **Das System wurde auf abweichender Hardware wiederhergestellt und die neue Hardware ist inkompatibel mit den wichtigsten, im Backup enthaltenen Treibern,**

  Lösung für Windows: Stellen Sie die Partition erneut wieder her. Entscheiden Sie sich bei Konfiguration der Wiederherstellung für die Verwendung von Acronis Universal Restore und spezifizieren Sie die passenden HAL- und Massenspeicher-Treiber.

- **Windows wurde zu einem dynamischen Laufwerk wiederhergestellt, das nicht bootfähig sein kann.**

  Lösung: Führen Sie eine Wiederherstellung von Windows auf eine Basis-, Simple- oder Mirrored-Partition durch.

- **Eine Systempartition wurde zu einer Festplatte wiederhergestellt, die keinen MBR hat.**

  Wenn Sie die Wiederherstellung einer Systempartition auf einem Laufwerk ohne MBR konfigurieren, fragt Sie das Programm, ob Sie zusammen mit der Systempartition auch den MBR wiederherstellen wollen. Entscheiden Sie sich nur dann gegen eine Wiederherstellung, wenn Sie nicht wollen, dass das System bootfähig wird.

  Lösung: Stellen Sie die Partition zusammen mit dem MBR der korrespondierenden Festplatte wieder her.

- **Das System verwendet den Acronis OS Selector**

  Weil der Master Boot Record (MBR) während der System-Wiederherstellung ausgetauscht werden kann, ist es möglich, dass der Acronis OS Selector, der den MBR verwendet, funktionsunfähig wird. Reaktivieren Sie den Acronis OS Selector folgendermaßen, wenn dies passieren sollte:

  Lösung: Starten Sie die Maschine mit dem bootfähigen Medium des Acronis Disk Director und wählen Sie im Menü **Extras -> OS Selector aktivieren**.

- **Das System verwendet GRand Unified Bootloader (GRUB) und wurde von einem normalen Backup (nicht „Raw“ bzw. Sektor-für-Sektor) wiederhergestellt.**

  Ein Teil des GRUB-Loaders liegt entweder in den ersten Sektoren der Festplatte oder in den ersten Sektoren der Partition. Der Rest befindet sich im Dateisystem einer der Partitionen. Die Bootfähigkeit des Systems kann nur dann automatisch wiederhergestellt werden, wenn GRUB innerhalb der ersten Sektoren der Festplatte sowie im Dateisystem liegt, zu dem ein

direkter Zugriff möglich ist. In allen anderen Fällen muss der Benutzer den Boot-Loader manuell reaktivieren.

Lösung: Reaktivieren Sie den Boot-Loader. Sie müssen möglicherweise auch noch die Konfigurationsdatei reparieren.

- **Das System verwendet Linux Loader (LILO) und wurde von einem normalen Backup (nicht „Raw“ bzw. Sektor-für-Sektor) wiederhergestellt.**

  LILO enthält zahlreiche Verweise zu absoluten Sektor-Nummern und kann daher nicht automatisch repariert werden, außer wenn alle Daten genau zu denjenigen Sektoren wiederhergestellt werden, die dieselben absoluten Nummern wie auf der Quellfestplatte haben.

  Lösung: Reaktivieren Sie den Boot-Loader. Sie müssen außerdem möglicherweise aus dem im vorherigen Punkt genannten Grund die Konfigurationsdatei des Loaders reparieren.

- **Der System-Loader zeigt zur falschen Partition.**

  Dies kann passieren, wenn System- bzw. Boot-Partitionen nicht zu ihrer ursprünglichen Position wiederhergestellt werden.

  Lösung:

  Für Windows-Loader wird dies durch eine Anpassung der Dateien „boot.ini“ bzw. „boot/bcd“ behoben. Acronis Backup & Recovery 10 führt dies automatisch durch und daher ist es unwahrscheinlich, dass Sie dieses Problem erleben.

  Für die Loader von GRUB und LILO müssen Sie die Konfigurationsdateien korrigieren. Hat sich die Nummer der Linux Root-Partition verändert, so ist es außerdem empfehlenswert, dass Sie „„/etc/fstab““ anpassen, damit korrekt auf das SWAP-Laufwerk zugegriffen werden kann.

- **Linux wurde von einem LVM-Partitions-Backup auf eine Basis-MBR-Festplatte wiederhergestellt.**

  Ein solches System kann nicht booten, weil sein Kernel versucht, das Root-Dateisystem von der LVM-Partition zu mounten.

  Lösung: Ändern Sie die Konfiguration des Loaders und „/etc/fstab“, so dass die LVM-Partition nicht mehr verwendet wird, und reaktivieren Sie den Boot-Loader.

So reaktivieren Sie GRUB und ändern die Konfiguration

Für gewöhnlich sollten Sie die passende Prozedur in den Unterlagen zum Boot-Loader nachschlagen. Es gibt auch den entsprechenden Artikel in der Knowledge Base auf der Acronis-Website.

Nachfolgend ein Beispiel, wie Sie GRUB reaktivieren, wenn das Systemlaufwerk (Volume) auf identische Hardware wiederhergestellt wird.

1. Starten Sie Linux oder starten Sie von einem bootfähigen Medium und drücken Sie dann Strg+Alt+F2.
2. Mounten Sie das System, das Sie wiederherstellen:

```
mkdir /mnt/system/
mount -t ext3 /dev/sda2 /mnt/system/ # root partition
mount -t ext3 /dev/sda1 /mnt/system/boot/ # boot partition
```

3. Mounten Sie die Dateisysteme **proc** und **dev** an das wiederherzustellende System:

```
mount -t proc none /mnt/system/proc/
mount -o bind /dev/ /mnt/system/dev/
```

4. Sichern Sie eine Kopie der „menu“-Datei von GRUB, indem Sie einen der folgenden Befehle ausführen:

```
cp /mnt/system/boot/grub/menu.lst /mnt/system/boot/grub/menu.lst.backup
```

oder

```
cp /mnt/system/boot/grub/grub.conf /mnt/system/boot/grub/grub.conf.backup
```

5. Bearbeiten Sie die Datei **/mnt/system/boot/grub/menu.lst** (für Debian-, Ubuntu- und SUSE Linux-Distributionen) oder die Datei **/mnt/system/boot/grub/grub.conf** (für Fedora- und Red Hat Enterprise Linux-Distributionen) — z.B. wie folgt:

   ```
   vi /mnt/system/boot/grub/menu.lst
   ```

6. Suchen Sie in der Datei **menu.lst** (alternativ **grub.conf**) den Menü-Eintrag, der zu dem von Ihnen wiederhergestellten System korrespondiert. Dieser Menü-Eintrag sieht folgendermaßen aus:

   ```
   title Red Hat Enterprise Linux Server (2.6.24.4)
         root (hd0,0)
         kernel /vmlinuz-2.6.24.4 ro root=/dev/sda2 rhgb quiet
         initrd /initrd-2.6.24.4.img
   ```

   Die Zeilen, die mit **title**, **root**, **kernel** bzw. **initrd** beginnen, legen Folgendes fest:

   - Den Titel des Menü-Eintrages.
   - Das Gerät, auf dem sich der Linux-Kernel befindet – üblicherweise die Boot- oder root-Partition, im vorliegenden Beispiel **root (hd0,0)**.
   - Der Pfad zum Kernel auf diesem Gerät und der root-Partition – im vorliegenden Beispiel ist der Pfad **/vmlinuz-2.6.24.4** und die root-Partition ist **/dev/sda2**. Sie können die root-Partition über ihre Bezeichnung (in der Form von **root=LABEL=/**), den Identifier (in der Form von **root=UUID=***some_uuid*) oder den Gerätenamen (**root=/dev/sda2**) spezifizieren.
   - Der Pfad zum Dienst **initrd** auf diesem Gerät.

7. Bearbeiten Sie die Datei **/mnt/system/etc/fstab**, um die Namen all der Geräte zu korrigieren, die sich als Ergebnis der Wiederherstellung verändert haben.
8. Starten Sie die Shell von GRUB, indem Sie einen der folgenden Befehle ausführen:

   ```
   chroot /mnt/system/ /sbin/grub
   ```

   oder

   ```
   chroot /mnt/system/ /usr/sbin/grub
   ```

9. Spezifizieren Sie das Laufwerk, auf dem sich GRUB befindet – üblicherweise die Boot- oder root-Partition.

   ```
   root (hd0,0)
   ```

10. Installieren Sie GRUB. Um GRUB z.B. in den Master Boot Record (MBR) der ersten Festplatte zu installieren, führen Sie den folgenden Befehl aus:

    ```
    setup (hd0)
    ```

11. Benden Sie die Shell von GRUB:

    ```
    quit
    ```

12. Trennen Sie die gemounteten Datei-Systeme und starten Sie dann neu:

    ```
    umount /mnt/system/dev/
    umount /mnt/system/proc/
    umount /mnt/system/boot/
    umount /mnt/system/
    reboot
    ```

13. Rekonfigurieren Sie den Boot-Loader durch die Verwendung von Tools und der Dokumentation, die zur von Ihnen verwendeten Linux-Distribution gehört. In Debian und Ubuntu z.B. müssen Sie vermutlich einige kommentierte Zeilen in der Datei **/boot/grub/menu.lst** bearbeiten und dann das Script **update-grub** ausführen; ansonsten treten die Änderungen nicht in Kraft.

6.4 Depots, Archive und Backups validieren

Validierung ist eine Aktion, mit der die Möglichkeit der Datenwiederherstellung aus einem Backup geprüft wird.

Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Die Validierung eines Festplatten- oder Partitions-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Beide Prozeduren sind Ressourcen-intensiv.

Die Validierung eines Archivs bestätigt die Gültigkeit aller Backups im Archiv. Die Validierung eines Depots (bzw. Speicherorts) bewirkt eine Überprüfung aller in diesem Depot (Speicherort) hinterlegten Archive.

Obwohl eine erfolgreiche Validierung eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, werden nicht alle Faktoren geprüft, die eine Wiederherstellung beeinflussen. Wenn Sie das Betriebssystem gesichert haben, kann nur eine testweise Wiederherstellung in einer bootfähigen Umgebung auf eine Ersatzfestplatte eine erfolgreiche Wiederherstellung garantieren. Sie sollten zumindest sicherstellen, dass das Backup unter Verwendung eines bootfähigen Mediums erfolgreich validiert werden kann.

Verschiedene Varianten, einen Validierungs-Task zu erstellen

Die Verwendung der Seite „Validierung“ ist der übliche Weg, um einen Validierungs-Task zu erstellen. Sie können hier Validierungen sofort ausführen oder eine Validierungsplanung für jedes Backup, jedes Archiv oder für jeden Speicherort, zu dem Sie Zugriff haben.

Die Validierung eines Archivs oder des letzten Backups in dem Archiv kann auch als Teil eines Backup-Plans durchgeführt werden. Zu weiteren Informationen siehe den Abschnitt Einen Backup-Plan erstellen (S. 113).

Sie können auf die Seite **Validierung** aus der Ansicht **Depots** (S. 77) zugreifen. Klicken Sie mit der rechten Maustaste auf das zu überprüfende Objekt (Archiv, Backup oder Depot) und wählen Sie im Kontextmenü **Validieren**. Darauf öffnet sich die Seite „Validierung“ mit dem vorausgewählten Objekt als Quelle. Sie müssen dann nur noch wählen, wann validiert werden soll, und (optional) einen Namen für den Tasks angeben.

Zur Erstellung eines Validierungs-Tasks führen Sie die folgenden Schritte aus.

Allgemein

Task-Name

[Optional] Geben Sie einen eindeutigen Namen für den Validierungs-Task ein. Ein bewusst gewählter Name macht es leichter, diesen Task zu identifizieren.

Anmeldedaten (S. 152)

[Optional] Der Validierungs-Task wird im Namen des Benutzers laufen, der den Task erstellt. Sie können, sofern notwendig, die Anmeldedaten für den Task ändern. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht** , um auf diese Option zuzugreifen.

Validierungsquelle

Validieren

Wählen Sie ein zu validierendes Objekt:

Archiv (S. 152) – in diesem Fall müssen Sie das benötigte Archiv angeben.

Backup (S. 154) – spezifizieren Sie zuerst das Archiv und wählen Sie in diesem dann das gewünschte Backup.

Depot (S. 154) – wählen Sie ein Depot (oder anderen Speicherort), dessen Archive validiert werden sollen.

Anmeldedaten für den Zugriff (S. 154)

[Optional] Stellen Sie Anmeldedaten für die Quelle zur Verfügung, falls das Benutzerkonto des Tasks dafür nicht genügend Zugriffsrechte hat. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Validierungszeitpunkt

Validieren (S. 155)

Geben Sie an, wann und wie oft die Validierung durchgeführt werden soll.

Nachdem Sie alle notwendigen Einstellungen konfiguriert haben, klicken Sie auf **OK**, um den Validierungs-Task zu erstellen.

6.4.1 Anmeldedaten für den Task

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, mit dem der Task ausgeführt wird.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Unter dem aktuellen Benutzer ausführen**

     Der Task wird mit den Anmeldedaten des Benutzers ausgeführt, der die Tasks startet. Wenn der Task nach Zeit-/Ereignis-Planung laufen soll, werden Sie bei Abschluss der Task-Erstellung nach dem Passwort des aktuellen Benutzers gefragt.
   - **Folgende Anmeldedaten benutzen**

     Der Task wird immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Zu weiteren Informationen über die Verwendung von Anmeldedaten in Acronis Backup & Recovery 10 siehe den Abschnitt Besitzer und Anmeldedaten (S. 23).

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 23), um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

6.4.2 Auswahl des Archivs

Auswahl des Archivs

1. Tragen Sie den vollständigen Pfad zum Speicherort in das Feld **Pfad** ein oder wählen Sie den gewünschten Ort im Verzeichnisbaum.

- Falls das Archiv auf dem Acronis Online Backup Storage gespeichert wurde, klicken Sie auf **Anmelden** und geben anschließend die Anmeldedaten zum Zugriff auf den Online Storage ein. Erweitern Sie dann die Gruppe **Online Backup Storage** und wählen Sie das Konto.

Auf dem Acronis Online Backup Storage gespeicherte Backups können nicht exportiert oder gemountet werden.

- Um die Archive in einem zentralen Depot abzulegen, erweitern Sie die Gruppe **Zentral** und wählen dort dieses Depot.
- Um die Archive in einem persönlichen Depot abzulegen, erweitern Sie die Gruppe **Persönlich** und wählen dort dieses Depot.
- Wenn das Archiv in einem lokalen Ordner auf der Maschine gespeichert ist, erweitern Sie die Gruppe **Lokale Ordner** und wählen das gewünschte Verzeichnis.

Wenn sich das Archiv auf Wechselmedien befindet, z.B. auf DVDs, legen Sie zuerst die letzte DVD ein und dann, nach Aufforderung durch das Programm, die Datenträger von Beginn an in der richtigen Reihenfolge.

- Wenn das Archiv auf einer Netzwerkfreigabe gespeichert ist, erweitern Sie die Gruppe **Netzwerk-Ordner**, wählen dann die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

Hinweis für Linux-Benutzer: *Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Point (etwa /mnt/share) angeschlossen ist, wählen Sie diesen Mount-Point statt der Netzwerkfreigabe aus.*

- Wenn das Archiv auf einem **FTP-** oder **SFTP-**Server gespeichert ist, tragen Sie Servername oder Adresse im Feld **Pfad** folgendermaßen ein:

  ftp://ftp_server:port _number oder sftp://sftp_server:port number

  Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP.

  Nach Eintragen der Anmeldinformationen sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server.

  Sie können auf den Server auch als Benutzer 'anonymous' zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

- Wenn die Daten auf einem lokal angeschlossenen Bandgerät gespeichert sind, erweitern Sie die Gruppe **Bandlaufwerke** und klicken auf das benötigte Gerät.

Bei Ausführung auf einer Maschine, die mit einem bootfähigen Medium gestartet wurde:

- Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein:

  bsp://knoten_adresse/depot_name/
- Um auf ein nicht verwaltetes zentrales Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.

2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die im gewählten Depot bzw. Ordner enthalten sind.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder

modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Klicken Sie auf **OK**.

6.4.3 Auswahl der Backups

So spezifizieren Sie ein zu validierendes Backup.

1. Wählen Sie im oberen Fensterbereich ein Backup anhand des Zeitstempels.

   Der untere Teil des Fensters zeigt den Inhalt des gewählten Backups, um Sie darin zu unterstützen, das richtige Backup herauszufinden.

2. Klicken Sie auf **OK**.

6.4.4 Wahl des Speicherorts

So wählen Sie einen Speicherort

Tragen Sie den vollständigen Pfad zum Speicherort in das Feld **Pfad** ein oder wählen Sie den gewünschten Speicherort im **Verzeichnisbaum**.

- Um ein zentrales Depot auszuwählen, erweitern Sie die Gruppe **Zentral** und wählen dort dieses Depot.
- Um ein persönliches Depot auszuwählen, erweitern Sie die Gruppe **Persönlich** und wählen dort dieses Depot.
- Um einen lokalen Ordner auszuwählen (CD-/DVD-Laufwerk oder ein lokal angeschlossenes Bandgerät), erweitern Sie die Gruppe **Lokale Ordner** und klicken auf den gewünschten Ordner.
- Um eine Netzwerkfreigabe zu wählen, erweitern Sie die Gruppe **Netzwerkordner**, wählen die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.
- Um einen **FTP-** oder **SFTP-**Server zu wählen, erweitern Sie die korrespondierende Gruppe und wählen die entsprechenden Ordner auf dem Server.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

Archiv-Tabelle verwenden

Die Tabelle zeigt für jeden gewählten Ort die Namen dort enthaltener Archive an, um Ihnen die Wahl des richtigen Speicherorts zu erleichtern. Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

6.4.5 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das Backup-Archiv gespeichert ist.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

Das Programm greift auf den Speicherort unter Verwendung derjenigen Task-Konto-Anmeldedaten zu, wie sie im Abschnitt „Allgemein“ spezifiziert wurden.

- **Folgende Anmeldedaten benutzen**

  Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

  Spezifizieren Sie:

  - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
  - **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

6.4.6 Validierungszeitpunkt

Da eine Validierung eine Ressourcen-intensive Aktion ist, empfiehlt es sich, sie so zu planen, dass sie nicht zu Hauptbelastungszeiten der verwalteten Maschine erfolgt. Bevorzugen Sie es dagegen, sofort informiert zu werden, ob die gesicherten Daten intakt und daher erfolgreich wiederherstellbar sind, so sollten Sie erwägen, die Validierung direkt nach der Task-Erstellung zu starten.

Wählen Sie eine der folgenden Optionen:

- **Jetzt** – um den Validierungs-Tasks direkt nach seiner Erstellung zu starten, sobald Sie also auf der Validierungs-Seite auf OK geklickt haben.
- **Später** – um einen einmaligen Validierungs-Task zu starten, zu dem von Ihnen angegeben Datum/Zeitpunkt.

  Spezifizieren Sie die passenden Parameter wie folgt:

  - **Datum und Zeit** – das Datum und die Uhrzeit, wann der Task gestartet werden soll.
  - **Task wird manuell gestartet (keine Planung)** – aktivieren Sie dieses Kontrollkästchen, falls Sie den Task später manuell starten wollen.
- **Nach Planung** – um den Task zu planen. Um mehr über die Konfiguration der Planungs-Parameter zu lernen, schauen Sie in den Abschnitt Planung (S. 85).

6.5 Image anschließen (mounten)

Durch das Mounten der Partitionen eines Disk-Backups (Images) können Sie die entsprechenden Laufwerke so ansprechen, als ob es sich um physikalische Festplatten handeln würde. Wenn mehrere Partitionen im selben Backup enthalten sind, dann können Sie diese in einer einzigen Mount-Aktion gleichzeitig anschließen. Die Mount-Aktion ist verfügbar, wenn die Konsole mit einer verwalteten, unter Windows oder Linux laufenden Maschine verbunden ist.

Ein Anschließen der Partitionen im Lese-Schreib-Modus erlaubt Ihnen, den Backup-Inhalt zu modifizieren, d.h. Dateien und Ordner zu speichern, zu verschieben, zu erstellen oder zu löschen und aus einer Datei bestehende, ausführbare Programme zu starten.

Einschränkungen: *Das Anschließen von Partitions-Backups, die in einem Acronis Backup & Recovery 10 Storage Node hinterlegt sind, ist nicht möglich.*

Einsatzszenarien:

- **Freigeben**: gemountete Images können für Benutzer des Netzwerkes einfach freigegeben werden.
- **Notlösung zur Datenbank-Wiederherstellung**: mounten Sie ein Image, das eine SQL-Datenbank von einer kürzlich ausgefallenen Maschine enthält. Auf diese Weise erhalten Sie Zugriff auf die Datenbank, bis die ausgefallene Maschine wiederhergestellt ist.
- **Offline Virus-Bereinigung**: wenn eine Maschine befallen ist, fährt der Administrator diese herunter, startet mit einem bootfähigen Medium und erstellt ein Image. Danach mountet der Administrator dieses Image im Schreib-/Lese-Modus, scannt und bereinigt es mit einem Antivirus-Programm und stellt schließlich die Maschine wieder her.
- **Fehlerüberprüfung**: Wenn eine Wiederherstellung durch einen Laufwerksfehler fehlschlägt, mounten Sie das Image im Lese-/Schreib-Modus. Überprüfen Sie dann das gemountete Laufwerk mit dem Befehl **chkdsk /r**.

Führen Sie die folgenden Schritte aus, um ein Abbild anzuschließen.

Source

Archiv (S. 156)

Spezifizieren Sie den Pfad zum Speicherort des Archivs und wählen Sie die in diesem enthaltenen Disk-Backups.

Backup (S. 158)

Wählen Sie das Backup.

Anmeldeinformationen: (S. 158)

[Optional] Geben Sie die Anmeldeinformationen für den Speicherort des Archivs an. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht** , um auf diese Option zuzugreifen.

Einstellungen für das Mounten

Partitionen (S. 158)

Bestimmen Sie die anzuschließenden Partitionen und konfigurieren Sie die Mount-Einstellungen für jedes Laufwerk: Weisen Sie einen Laufwerksbuchstaben zu oder geben Sie den Mount-Punkt an, entscheiden Sie sich dann für den Lese-/Schreib- oder Nur-Lese-Zugriffsmodus.

Nachdem Sie alle benötigten Schritte abgeschlossen haben, klicken Sie auf **OK**, um die Partitionen zu mounten.

6.5.1 Auswahl des Archivs

Auswahl des Archivs

1. Tragen Sie den vollständigen Pfad zum Speicherort in das Feld **Pfad** ein oder wählen Sie den gewünschten Ort im Verzeichnisbaum.
   - Falls das Archiv auf dem Acronis Online Backup Storage gespeichert wurde, klicken Sie auf **Anmelden** und geben anschließend die Anmeldedaten zum Zugriff auf den Online Storage ein. Erweitern Sie dann die Gruppe **Online Backup Storage** und wählen Sie das Konto.

   Auf dem Acronis Online Backup Storage gespeicherte Backups können nicht exportiert oder gemountet werden.

- Um die Archive in einem zentralen Depot abzulegen, erweitern Sie die Gruppe **Zentral** und wählen dort dieses Depot.
- Um die Archive in einem persönlichen Depot abzulegen, erweitern Sie die Gruppe **Persönlich** und wählen dort dieses Depot.
- Wenn das Archiv in einem lokalen Ordner auf der Maschine gespeichert ist, erweitern Sie die Gruppe **Lokale Ordner** und wählen das gewünschte Verzeichnis.

Wenn sich das Archiv auf Wechselmedien befindet, z.B. auf DVDs, legen Sie zuerst die letzte DVD ein und dann, nach Aufforderung durch das Programm, die Datenträger von Beginn an in der richtigen Reihenfolge.

- Wenn das Archiv auf einer Netzwerkfreigabe gespeichert ist, erweitern Sie die Gruppe **Netzwerk-Ordner**, wählen dann die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

Hinweis für Linux-Benutzer: *Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Point (etwa /mnt/share) angeschlossen ist, wählen Sie diesen Mount-Point statt der Netzwerkfreigabe aus.*

- Wenn das Archiv auf einem **FTP-** oder **SFTP-**Server gespeichert ist, tragen Sie Servername oder Adresse im Feld **Pfad** folgendermaßen ein:

  ftp://ftp_server:port _number oder sftp://sftp_server:port number

  Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP.

  Nach Eintragen der Anmeldinformationen sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server.

  Sie können auf den Server auch als Benutzer 'anonymous' zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

- Wenn die Daten auf einem lokal angeschlossenen Bandgerät gespeichert sind, erweitern Sie die Gruppe **Bandlaufwerke** und klicken auf das benötigte Gerät.

Bei Ausführung auf einer Maschine, die mit einem bootfähigen Medium gestartet wurde:

- Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein:

  bsp://knoten_adresse/depot_name/

- Um auf ein nicht verwaltetes zentrales Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.

2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die im gewählten Depot bzw. Ordner enthalten sind.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.
3. Klicken Sie auf **OK**.

6.5.2 Auswahl der Backups

So wählen Sie ein Backup aus:

1. Bestimmen Sie eines der Backups anhand seines Zeitstempels.
2. Die untere Tabelle zeigt zur Unterstützung bei der Wahl des richtigen Backups die in diesem Backup enthaltenen Partitionen an.

   Um mehr Informationen über ein Laufwerk zu erhalten, klicken Sie mit der rechten Maustaste darauf und wählen im Kontextmenü **Informationen**.
3. Klicken Sie auf **OK**.

6.5.3 Anmeldeinformationen:

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Aktuelle Anmeldedaten benutzen**

     Das Programm greift auf den Speicherort unter Verwendung der Anmeldedaten des aktuellen Benutzers zu.
   - **Folgende Anmeldedaten benutzen**

     Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das aktuelle Benutzerkonto keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:

     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

6.5.4 Auswahl der Partition

Bestimmen Sie die anzuschließenden Partitionen und konfigurieren Sie die Parameter zum Mounten für jedes der gewählten Laufwerke wie folgt:

1. Aktivieren Sie das Kontrollkästchen für jede Partition, die Sie mounten müssen.
2. Klicken Sie auf das gewählte Laufwerk, um die Parameter zum Mounten einzustellen.
   - **Zugriffsmodus** – bestimmen Sie den Modus, mit dem Sie das Laufwerk anschließen wollen:
     - **Nur Lesen** – ermöglicht Ihnen das Durchsuchen und Öffnen von Dateien innerhalb des Backups, ohne dass es zu irgendwelchen Änderungen kommen kann.
     - **Lesen/Schreiben** – in diesem Modus geht das Programm davon aus, dass der Backup-Inhalt verändert wird, und erstellt ein inkrementelles Backup, um diese Veränderungen aufzunehmen.

- **Laufwerksbuchstabe zuweisen** (in Windows) – Acronis Backup & Recovery 10 wird dem angeschlossenen Laufwerk einen freien Laufwerksbuchstaben zuweisen. Wählen Sie sofern benötigt aus dem Listenfeld einen anderen Laufwerksbuchstaben.
- **Mount-Punkt** (in Linux) – spezifiziert das Verzeichnis, wo Sie die Partition gemountet haben wollen.

3. Sollten mehrere Partitionen zum Anschließen ausgewählt sein, so klicken Sie auf jedes Laufwerk, um wie im vorherigen Schritt beschrieben die Parameter zum Mounten einzustellen.
4. Klicken Sie auf **OK**.

6.6 Gemountete Images verwalten

Sobald eine Partition angeschlossen wurde, können Sie im Backup enthaltene Dateien und Ordner mit einem Datei-Manager durchsuchen und gewünschte Dateien zu einem beliebigen Ziel kopieren. Sie müssen daher keine vollständige Wiederherstellungsprozedur durchführen, wenn Sie nur einige Dateien und Ordner aus einem Partitions-Backup entnehmen müssen.

Images durchsuchen

Über das Durchsuchen von angeschlossenen Partitionen können Sie den Laufwerksinhalt einsehen und auch modifizieren (sofern im Lese-/Schreib-Modus gemountet).

Um eine angeschlossene Partition zu durchsuchen, wählen Sie das Laufwerk in der Tabelle aus und klicken auf **Durchsuchen**. Darauf öffnet sich das Fenster des Standard-Datei-Managers und erlaubt Ihnen so, den Inhalt des gemounteten Laufwerkes zu untersuchen.

Abbild abschalten

Ein gemountetes Laufwerk im System zu belassen, benötigt einiges an System-Ressourcen. Es ist daher empfehlenswert, dass Sie die Laufwerke, nachdem alle notwendigen Aktionen abgeschlossen wurden, wieder abschalten. Ein Laufwerk bleibt bis zum nächsten Neustart des Betriebssystems gemountet, wenn Sie es nicht manuell abschalten.

Um ein Image abzuschalten, wählen Sie es in der Tabelle aus und klicken dann auf **Abschalten**.

Um alle gemounteten Laufwerke abzuschalten, klicken Sie auf **Alle abschalten**.

6.7 Archive und Backups exportieren

Beim Export wird eine Kopie des Archivs bzw. eine unabhängige Teilkopie des Archivs am von Ihnen angegebenen Speicherort erstellt. Das ursprüngliche Archiv bleibt unverändert.

Ein Export ist möglich für:

- **ein einzelnes Archiv** – es wird eine exakte Kopie erstellt
- **ein einzelnes Backup** – es wird ein Archiv erstellt, das aus einem einzelnen vollständigen Backup besteht. Beim Export eines inkrementellen oder differentiellen Backup werden die vorhergehenden Backups bis hin zum letzten vollständigen Backup konsolidiert
- **eine eigene Auswahl von Backups** in einem Archiv – das resultierende Archiv enthält nur die angegebenen Backups. Eine Konsolidierung erfolgt nach Bedarf; das resultierende Archiv kann daher Voll-Backups enthalten, aber auch inkrementelle und differentielle Backups.

Einsatzszenarien

Mit einem Export können Sie ausgewählte Backups von einer Reihe inkrementeller Backups trennen, um so die Wiederherstellung zu beschleunigen, auf Wechselmedien und externe Medien zu schreiben, oder für andere Zwecke.

Beispiel. Wenn Sie Daten zu einem Remote-Speicherort über eine instabile Netzwerkverbindung oder bei niedriger Netzwerkbandbreite übertragen (etwa ein Backup durch ein WAN unter Verwendung eines VPN-Zugriffs), können Sie das anfängliche Voll-Backup auch auf ein abtrennbares Medium speichern. Schicken Sie das Medium danach zu dem Remote-Speicherort. Dort wird das Backup dann von diesem Medium zu dem als eigentliches Ziel fungierenden Storage exportiert. Nachfolgende inkrementelle Backups, die üblicherweise deutlich kleiner sind, werden dann per Netzwerk/Internet übertragen.

Beim Export eines verwalteten Depots auf ein Wechselmedium erhalten Sie ein tragbares, nicht verwaltetes Depot für den Einsatz in folgenden Szenarien:

- Sie können eine Kopie Ihres Depots oder der wichtigsten Archive räumlich getrennt aufbewahren
- Sie können eine reelle Kopie Ihres Depots zu einer entfernten Niederlassung mitnehmen
- Im Fall von Netzwerkproblemen oder einem Ausfall des Storage Node ist die Wiederherstellung ohne Zugriff auf den Storage Node möglich
- Wiederherstellung des Storage Node selbst.

Beim Export eines Festplatten-basierten Depots auf ein Bandgerät handelt es sich um eine einfache Form des Archiv-Staging nach Bedarf.

Der Name des resultierenden Archivs

Standardmäßig erbt das exportierte Archiv den Namen des ursprünglichen Archivs. Da es nicht empfehlenswert ist, mehrere Archive mit gleichem Namen an einem Ort zu speichern, sind folgende Aktionen bei Verwendung des vorgegebenen Archivnamens deaktiviert:

- Export von Teilen eines Archivs zum selben Speicherort
- Export eines Archivs oder von Teilen eines Archivs zu einem Speicherort, an dem es ein Archiv mit demselben Namen gibt
- Zweimaliger Export eines Archivs oder von Teilen eines Archivs zum selben Speicherort

Wählen Sie in allen genannten Fällen einen Archivnamen, der im Zielordner oder dem Zieldepot nicht vergeben ist. Wenn Sie den Export unter Verwendung desselben Namens erneut ausführen müssen, löschen Sie zunächst das aus dem vorhergehenden Export resultierende Archiv.

Die Optionen des resultierenden Archivs

Das exportierte Archiv erbt die Optionen des ursprünglichen Archivs einschließlich Verschlüsselung und Kennworts. Beim Export eines kennwortgeschützten Archivs werden Sie zur Eingabe des Kennworts aufgefordert. Wenn das ursprüngliche Archiv verschlüsselt ist, wird mit dem Kennwort auch das resultierende Archiv verschlüsselt.

Speicherort für Quelle und Ziel

Wenn die Konsole mit einer **verwalteten Maschine** verbunden ist, können Sie Exports von Archiven oder Teilen eines Archivs von und zu jedem beliebigen Speicherort durchführen, auf den der auf der Maschine befindliche Agent Zugriff hat. Dazu gehören persönliche Depots, lokal angeschlossene Bandgeräte, Wechselmedien und, in den Advanced Editionen, verwaltete und nicht verwaltete zentrale Depots.

Wenn die Konsole mit einem **Management Server** verbunden ist, stehen zwei Exportmethoden zur Verfügung:

- Export aus einem **verwalteten Depot**. Der Export wird vom Storage Node übernommen, der das Depot verwaltet. Das Ziel kann eine Netzwerkfreigabe oder ein lokaler Ordner auf dem Storage Node sein.
- Export aus einem **nicht verwalteten zentralen Depot**. Der Export wird vom Agenten übernommen, der auf der angegebenen verwalteten Maschine installiert ist. Das Ziel kann jeder Speicherort sein, auf den der Agent Zugriff hat, einschließlich eines verwalteten Depots.

Tipp: *Wählen Sie bei der Konfiguration eines Exports in ein deduplizierendes, verwaltetes Depot eine Maschine, auf der der Deduplizierungs-Add-on für den Agenten installiert ist. Andernfalls wird der Export-Task fehlschlagen.*

Aktionen mit einem Export-Task

Ein Export-Task startet sofort, nachdem die Konfiguration abgeschlossen ist. Sie können einen Export-Task wie jeden anderen Task stoppen oder löschen.

Sobald ein Export-Task abgeschlossen wurde, können Sie ihn jederzeit erneut ausführen. Löschen Sie zunächst das aus der letzten Ausführung des Task resultierende Archiv, falls es sich noch im Zieldepot befindet. Andernfalls wird der Task fehlschlagen. Sie können bei einem Export-Task das Zielarchiv nicht umbenennen (das ist eine Einschränkung).

Tipp: *Dieses Staging-Szenario kann manuell umgesetzt werden, indem Sie immer erst den Task zum Löschen des Archivs und dann den Export-Task ausführen.*

Verschiedene Varianten, einen Export-Task zu erstellen

Gewöhnlich werden Export-Tasks über die Seite **Exportieren** erstellt. Dort können Sie jedes Backup oder Archiv exportieren, auf das Sie Zugriffsrechte besitzen.

Auf die Seite **Exportieren** können Sie aus der Ansicht **Depots** zugreifen. Klicken Sie mit der rechten Maustaste auf das zu exportierende Objekt (Archiv oder Backup) und wählen Sie im Kontextmenü **Exportieren**. Darauf öffnet sich die Seite **Exportieren** mit dem vorausgewählten Objekt als Quelle. Sie müssen dann nur noch einen Ziel-Speicherort wählen und (optional) einen Namen für den Task angeben.

Führen Sie die folgenden Schritte aus, um ein Archiv oder ein Backup zu exportieren.

Allgemein

Task-Name

[Optional] Geben Sie einen eindeutigen Namen für den Task ein. Ein bewusst gewählter Name macht es leichter, diesen Task zu identifizieren.

Anmeldedaten für den Task (S. 162)

[Optional] Der Export-Task wird im Namen des Benutzers laufen, der den Task erstellt. Sie können, sofern notwendig, die Anmeldedaten für den Task ändern. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht** , um auf diese Option zuzugreifen.

Export-Quelle

Exportieren

Wählen Sie ein zu exportierendes Objekt:

Archiv (S. 138) – in diesem Fall müssen Sie nur das benötigte Archiv angeben.

Backups (S. 164) – spezifizieren Sie zuerst das Archiv und wählen Sie in diesem dann das bzw. die gewünschte(n) Backup(s).

Anmeldeinformationen: (S. 164)

[Optional] Stellen Sie Anmeldedaten für die Quelle zur Verfügung, falls das Benutzerkonto des Tasks dafür nicht genügend Zugriffsrechte hat. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht** , um auf diese Option zuzugreifen.

Export-Ziel

Archiv (S. 164)

Geben Sie den Pfad zu dem Speicherort an, wo das neue Archiv erstellt wird.

Vergeben Sie einen eindeutigen Namen und Kommentar für das neue Archiv.

Anmeldeinformationen: (S. 166)

[Optional] Stellen Sie Anmeldedaten für den Ziel-Speicherort zur Verfügung, falls das Benutzerkonto des Tasks nicht ausreichende Zugriffsrechte darauf hat. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht** , um auf diese Option zuzugreifen.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um den Export zu starten.

6.7.1 Anmeldedaten für den Task

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, mit dem der Task ausgeführt wird.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Unter dem aktuellen Benutzer ausführen**

     Der Task wird mit den Anmeldedaten des Benutzers ausgeführt, der die Tasks startet. Wenn der Task nach Zeit-/Ereignis-Planung laufen soll, werden Sie bei Abschluss der Task-Erstellung nach dem Passwort des aktuellen Benutzers gefragt.
   - **Folgende Anmeldedaten benutzen**

     Der Task wird immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Zu weiteren Informationen über die Verwendung von Anmeldedaten in Acronis Backup & Recovery 10 siehe den Abschnitt Besitzer und Anmeldedaten (S. 23).

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 23), um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

6.7.2 Auswahl des Archivs

Auswahl des Archivs

1. Tragen Sie den vollständigen Pfad zum Speicherort in das Feld **Pfad** ein oder wählen Sie den gewünschten Ort im Verzeichnisbaum.
   - Falls das Archiv auf dem Acronis Online Backup Storage gespeichert wurde, klicken Sie auf **Anmelden** und geben anschließend die Anmeldedaten zum Zugriff auf den Online Storage ein. Erweitern Sie dann die Gruppe **Online Backup Storage** und wählen Sie das Konto.

   Auf dem Acronis Online Backup Storage gespeicherte Backups können nicht exportiert oder gemountet werden.

   - Um die Archive in einem zentralen Depot abzulegen, erweitern Sie die Gruppe **Zentral** und wählen dort dieses Depot.
   - Um die Archive in einem persönlichen Depot abzulegen, erweitern Sie die Gruppe **Persönlich** und wählen dort dieses Depot.
   - Wenn das Archiv in einem lokalen Ordner auf der Maschine gespeichert ist, erweitern Sie die Gruppe **Lokale Ordner** und wählen das gewünschte Verzeichnis.

   Wenn sich das Archiv auf Wechselmedien befindet, z.B. auf DVDs, legen Sie zuerst die letzte DVD ein und dann, nach Aufforderung durch das Programm, die Datenträger von Beginn an in der richtigen Reihenfolge.

   - Wenn das Archiv auf einer Netzwerkfreigabe gespeichert ist, erweitern Sie die Gruppe **Netzwerk-Ordner**, wählen dann die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

   ***Hinweis für Linux-Benutzer:** Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Point (etwa /mnt/share) angeschlossen ist, wählen Sie diesen Mount-Point statt der Netzwerkfreigabe aus.*

   - Wenn das Archiv auf einem **FTP-** oder **SFTP-**Server gespeichert ist, tragen Sie Servername oder Adresse im Feld **Pfad** folgendermaßen ein:

     ftp://ftp_server:port _number oder sftp://sftp_server:port number

     Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP.

     Nach Eintragen der Anmeldinformationen sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server.

     Sie können auf den Server auch als Benutzer 'anonymous' zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten.

   Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

   - Wenn die Daten auf einem lokal angeschlossenen Bandgerät gespeichert sind, erweitern Sie die Gruppe **Bandlaufwerke** und klicken auf das benötigte Gerät.

   Bei Ausführung auf einer Maschine, die mit einem bootfähigen Medium gestartet wurde:

   - Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein:

     bsp://knoten_adresse/depot_name/
   - Um auf ein nicht verwaltetes zentrales Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.

2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die im gewählten Depot bzw. Ordner enthalten sind.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.
3. Klicken Sie auf **OK**.

6.7.3 Auswahl der Backups

So wählen Sie ein zu exportierendes Backup aus

1. Aktivieren Sie oben im Fenster das bzw. die entsprechende(n) Kontrollkästchen.

   Um sicherzugehen, dass Sie das richtige Backup ausgewählt haben, klicken Sie auf das Backup; die untere Tabelle zeigt die in diesem Backup enthaltenen Volumes an.

   Um mehr Informationen über ein Volume zu erhalten, klicken Sie mit der rechten Maustaste darauf und wählen Sie im Kontextmenü **Informationen**.
2. Klicken Sie auf **OK**.

6.7.4 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, die für einen Zugriff auf den Ort notwendig sind, an dem das Quell-Archiv (oder das Backup) gespeichert ist.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Das Programm greift auf den Speicherort unter Verwendung derjenigen Task-Konto-Anmeldedaten zu, wie sie im Abschnitt „Allgemein“ spezifiziert wurden.
   - **Folgende Anmeldedaten benutzen**

     Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:

     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

6.7.5 Wahl des Speicherorts

Spezifizieren Sie das Ziel, wohin das exportierte Objekt gespeichert werden soll. Backups dürfen nicht in dasselbe Archiv exportiert werden.

1. Exportziel wählen

Tragen Sie den vollständigen Pfad zum Zielort in das Feld **Pfad** ein oder wählen Sie das gewünschte Ziel im Verzeichnisbaum.

- Um Daten in ein zentrales, nicht verwaltetes Depot zu exportieren, erweitern Sie die Gruppe **Zentrale Depots** und wählen dort ein Depot.
- Um Daten in ein persönliches Depot zu exportieren, erweitern Sie die Gruppe **Persönliche Depots** und wählen dort ein Depot.
- Um Daten in einen lokalen Ordner auf der Maschine zu exportieren, erweitern Sie die Gruppe **Lokale Ordner** und wählen das gewünschte Verzeichnis.
- Um Daten zu einer Netzwerkfreigabe zu exportieren, erweitern Sie die Gruppe **Netzwerkordner**, wählen die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

  ***Hinweis für Linux-Benutzer**: Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Point wie z.B. /mnt/share angeschlossen ist, wählen Sie diesen Mount-Point statt der Netzwerkfreigabe aus.*

- Zum Datenexport auf einen **FTP-** oder **SFTP-**Server tragen Sie Server-Namen oder -Adresse folgendermaßen in das Feld **Pfad** ein:

  ftp://ftp_server:port _number oder **sftp://sftp_server:port number**

  Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP.

  Nach Eintragen der Anmeldinformationen sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server.

  Sie können auf den Server auch als Benutzer 'anonymous' zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten.

  Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

- Um Daten auf ein lokal angeschlossenes Bandgerät zu exportieren, erweitern Sie die Gruppe **Bandlaufwerke** und klicken auf das benötigte Gerät.

2. Archiv-Tabelle verwenden

Die rechte Tabelle zeigt für jeden im Baum gewählten Speicherort die Namen der dort enthaltenen Archive an, um Ihnen die Wahl des richtigen Ziels zu erleichtern.

Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Das neue Archiv benennen

Standardmäßig erbt das exportierte Archiv den Namen des ursprünglichen Archivs. Da es nicht empfehlenswert ist, mehrere Archive mit gleichem Namen an einem Ort zu speichern, sind folgende Aktionen bei Verwendung des vorgegebenen Archivnamens deaktiviert:

- Export von Teilen eines Archivs zum selben Speicherort
- Export eines Archivs oder von Teilen eines Archivs zu einem Speicherort, an dem es ein Archiv mit demselben Namen gibt

- Zweimaliger Export eines Archivs oder von Teilen eines Archivs zum selben Speicherort

Wählen Sie in allen genannten Fällen einen Archivnamen, der im Zielordner oder dem Zieldepot nicht vergeben ist. Wenn Sie den Export unter Verwendung desselben Namens erneut ausführen müssen, löschen Sie zunächst das aus dem vorhergehenden Export resultierende Archiv.

6.7.6 Anmeldedaten für das Ziel

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das resultierende Archiv gespeichert wird. Der Benutzer, dessen Name angegeben wird, wird als Besitzer des Archivs betrachtet.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Das Programm greift auf den Speicherort unter Verwendung derjenigen Task-Konto-Anmeldedaten zu, wie sie im Abschnitt „Allgemein“ spezifiziert wurden.
   - **Folgende Anmeldedaten benutzen**

     Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

6.8 Acronis Secure Zone

Die Acronis Secure Zone ist eine sichere Partition auf dem Festplattenplatz einer verwalteten Maschine, in der Backup-Archive gespeichert werden können, so dass die Wiederherstellung einer Festplatte auf der gleichen Festplatte erfolgen kann, auf der sich auch die Backups selbst befinden.

Verschiedene Windows-Anwendungen, wie z.B. die Acronis Disk Management-Tools, können auf die Zone zugreifen.

Weitere Informationen über die Vorteile und Beschränkungen der Acronis Secure Zone finden Sie unter dem Thema Acronis Secure Zone (S. 41) im Abschnitt „Proprietäre Acronis-Technologien“.

6.8.1 Acronis Secure Zone erstellen

Sie können die Acronis Secure Zone erstellen, während das Betriebssystem läuft oder Sie ein bootfähiges Medium benutzen.

Zur Erstellung der Acronis Secure Zone führen Sie die folgenden Schritte aus.

Platz

Festplatte (S. 167)

Wählen Sie (sofern mehrere vorhanden) eine Festplatte, auf der die Zone erstellt werden soll. Die Acronis Secure Zone wird unter Verwendung von nicht zugeordnetem Speicherplatz oder auf Kosten freien Speicherplatzes der Partition erstellt.

Größe (S. 167)

Spezifizieren Sie die exakte Größe der Zone. Verschieben oder Größenveränderung einer gesperrten Partition, wie der aktuellen Betriebssystempartition, benötigen einen Neustart.

Einstellungen

Kennwort (S. 168)

[Optional] Schützen Sie die Acronis Secure Zone vor unerlaubtem Zugriff mit einem Kennwort. Das Kennwort wird bei jeder die Zone betreffende Aktion erfragt.

Klicken Sie auf OK, nachdem Sie die benötigten Einstellungen konfiguriert haben. Überprüfen Sie im Fenster Ergebnisbestätigung (S. 168) das erwartete Layout und klicken Sie auf OK, um die Erstellung der Zone zu starten.

Acronis Secure Zone Laufwerk

Die Acronis Secure Zone kann auf jeder fest installierten Festplatte liegen. Die Acronis Secure Zone wird immer am Ende der Festplatte eingerichtet. Eine Maschine kann auch nur eine Acronis Secure Zone haben. Die Acronis Secure Zone wird unter Verwendung von nicht zugeordnetem Speicherplatz oder auf Kosten freien Speicherplatzes der Partitionen erstellt.

Die Acronis Secure Zone kann nicht auf einem dynamischen Datenträger oder einer Festplatte eingerichtet werden, die nach dem GPT-Schema partitioniert ist.

So weisen Sie der Acronis Secure Zone Speicherplatz zu

1. Wählen Sie (sofern mehrere vorhanden) eine Festplatte, auf der die Zone erstellt werden soll. Nicht zugeordneter Festplattenplatz wird standardmäßig ausgewählt. Das Programm zeigt den insgesamt für die Acronis Secure Zone verfügbaren Speicherplatz an.
2. Wenn Sie der Zone mehr Speicherplatz zuweisen müssen, können Sie die Partitionen wählen, von denen freier Platz genommen werden soll. Das Programm zeigt erneut den insgesamt für die Acronis Secure Zone verfügbaren Speicherplatz an, basierend auf Ihrer Auswahl. Sie können die exakte Größe der Zone im Fenster **Acronis Secure Zone Größe** (S. 167) einstellen.
3. Klicken Sie auf **OK**.

Acronis Secure Zone Größe

Geben Sie die Größe der Acronis Secure Zone ein oder ziehen Sie am Schieber, um eine Größe zwischen der minimalen und maximalen zu wählen. Die minimale Größe beträgt ca. 50 MB, abhängig von der Geometrie der Festplatte. Die maximale Größe entspricht dem nicht zugeordneten Festplattenplatz plus dem gesamten freien Platz aller im vorherigen Schritt gewählten Partitionen.

Beachten Sie Folgendes, wenn Sie Speicherplatz von der Boot- bzw. System-Partition verwenden müssen:

- Ein Verschieben oder eine Größenänderung der Partition, von der das System gegenwärtig bootet, verlangen einen Neustart.

- Die Verwendung des gesamten freien Speichers einer Systempartition kann dazu führen, dass das Betriebssystem instabil wird oder sogar nicht mehr startet. Stellen Sie also nicht die maximale Größe für die Zone ein, falls Sie die Boot- bzw. System-Partition gewählt haben.

Kennwort für die Acronis Secure Zone

Die Vergabe eines Kennwortes schützt die Acronis Secure Zone vor unerlaubtem Zugriff. Das Programm wird bei allen Aktionen, die die Zone und dort gespeicherte Archive betreffen, nach dem Kennwort fragen – wie etwa Backup und Wiederherstellung, Archiv-Validierung, Größenveränderung und Löschen der Zone.

So vergeben Sie ein Kennwort

1. Wählen Sie **Kennwort verwenden**.
2. Tippen Sie das neue Kennwort in das Feld **Kennwort eingeben** ein.
3. Tragen Sie das Kennwort im Eingabefeld **Kennwortbestätigung** erneut ein.
4. Klicken Sie auf **OK**.

So deaktivieren Sie ein Kennwort

1. Wählen Sie **Nicht verwenden**.
2. Klicken Sie auf **OK**.

Ergebnisbestätigung

Das Fenster **Ergebnisbestätigung** zeigt das erwartete Partitionslayout entsprechend der von Ihnen gewählten Einstellungen. Klicken Sie auf **OK**, falls Sie mit dem Layout einverstanden sind, worauf die Erstellung der Acronis Secure Zone startet.

So werden die Einstellungen umgesetzt

Die nachfolgende Erläuterung hilft Ihnen zu verstehen, welche Auswirkung die Erstellung der Acronis Secure Zone auf eine Festplatte hat, die mehrere Partitionen enthält.

- Die Acronis Secure Zone wird immer am Ende der Festplatte eingerichtet. Bei Kalkulation des endgültigen Partitionslayouts wird das Programm zuerst nicht zugeordneten, am Ende liegenden Festplattenplatz verwenden.
- Sollte der nicht zugeordnete Speicherplatz am Ende der Festplatte nicht ausreichen, jedoch zwischen den Partitionen noch nicht zugeordneter Speicherplatz vorhanden sein, so werden die Partitionen verschoben, um dem Endbereich mehr nicht zugeordneten Speicherplatz hinzuzufügen.
- Wenn dann der zusammengetragene nicht zugeordnete Speicherplatz immer noch nicht ausreicht, wird das Programm freien Speicherplatz von Partitionen beziehen, die Sie auswählen und deren Größe proportional verkleinern. Die Größenveränderung einer gesperrten Partition benötigt einen Neustart.
- Auf einem Laufwerk sollte jedoch genügend freier Platz vorhanden sein, so dass Betriebssystem und Anwendungen arbeitsfähig sind, z.B. zum Erstellen temporärer Dateien. Das Programm wird keine Partition verkleinern, deren freier Speicherplatz dadurch kleiner als 25% der Gesamtgröße wird. Nur wenn alle Partitionen der Festplatte mindestens 25% freien Speicherplatz haben, wird das Programm mit der proportionalen Verkleinerung der Partitionen fortfahren.

Daraus wird ersichtlich, dass es nicht ratsam ist, für die Zone die maximal mögliche Größe einzustellen. Sie haben am Ende dann auf keinem Laufwerk mehr freien Speicherplatz, was dazu führen kann, dass Betriebssystem und Anwendungen instabil arbeiten oder nicht mehr starten.

6.8.2 Acronis Secure Zone verwalten

Die Acronis Secure Zone wird als persönliches Depot (S. 189) betrachtet. Einmal auf einer verwalteten Maschine erstellt, ist die Zone stets in der Liste **Persönliche Depots** präsent. Die Acronis Secure Zone kann sowohl von zentralen Backup-Plänen als auch von lokalen Plänen verwendet werden.

Sollten Sie die Acronis Secure Zone schon früher verwendet haben, so werden Sie einen radikalen Wechsel in ihrer Funktionalität feststellen. Die Zone führt von allein keine automatischen Bereinigungen, also das Löschen alter Archive, mehr aus. Nutzen Sie zum Sichern in die Zone Backup-Schemata mit automatischer Bereinigung oder löschen Sie veraltete Backups manuell unter Verwendung der Verwaltungsfunktionalität des Depots.

Durch das neue Verhalten der Acronis Secure Zone erhalten Sie die Fähigkeit:

- in der Zone lokalisierte Archive und in ihnen enthaltene Backups aufzulisten
- den Inhalt eines Backups zu untersuchen
- ein Partitions-Backup zu mounten, um Dateien aus dem Backup auf eine physikalische Platte zu kopieren
- Archive und Backups aus Archiven sicher zu löschen.

Um mehr über das Arbeiten mit Depots zu erfahren, siehe den Abschnitt Depots (S. 77).

Acronis Secure Zone vergrößern

So vergrößern Sie die Acronis Secure Zone

1. Klicken Sie auf der Seite **Acronis Secure Zone verwalten** auf **Vergrößern**.
2. Bestimmen Sie die Volumes, deren freier Speicher zur Vergrößerung der Acronis Secure Zone verwendet werden soll.
3. Spezifizieren Sie die neue Größe der Zone, indem Sie:
   - am Schieber ziehen und so eine Größe zwischen dem gegenwärtigen und dem maximalen Wert wählen. Die maximale Größe entspricht dem nicht zugeordneten Festplattenspeicherplatz plus dem gesamten freien Speicher aller gewählten Partitionen;
   - einen exakten Wert für die Größe der Acronis Secure Zone eingeben.

   Bei Vergrößerung der Zone verfährt das Programm wie folgt:
   - Zuerst wird es den nicht zugeordneten Festplattenspeicherplatz benutzen. Falls notwendig, werden Partitionen verschoben, jedoch nicht in ihrer Größe verändert. Das Verschieben einer gesperrten Partition benötigt einen Neustart.
   - Sollte nicht genügend nicht zugeordneter Speicher vorhanden sein, so wird das Programm freien Speicherplatz von den ausgewählten Partitionen beziehen, deren Größe dabei proportional verkleinert wird. Die Größenveränderung einer gesperrten Partition benötigt einen Neustart.

   Die Verkleinerung einer Systempartition auf ihre minimale Größe kann das Betriebssystem der Maschine am Booten hindern.
4. Klicken Sie auf **OK**.

Die Acronis Secure Zone verkleinern

So verkleinern Sie die Acronis Secure Zone

1. Klicken Sie auf der Seite **Acronis Secure Zone verwalten** auf **Verkleinern**.

2. Bestimmen Sie Partitionen, die den freigewordenen Speicherplatz nach Verkleinerung der Zone zugesprochen bekommen.
3. Spezifizieren Sie die neue Größe der Zone, indem Sie:
   - am Schieber ziehen und so eine Größe zwischen dem gegenwärtigen und minimalen Wert wählen. Die minimale Größe beträgt ca. 50 MB, abhängig von der Geometrie der Festplatte.
   - einen exakten Wert im Feld **Acronis Secure Zone Größe** eingeben.
4. Klicken Sie auf **OK**.

Acronis Secure Zone löschen

So löschen Sie eine Acronis Secure Zone:

1. Wählen Sie im Bereich **Acronis Secure Zone Aktionen** (in der Seitenleiste **Aktionen und Werkzeuge**) **Löschen**.
2. Wählen Sie im Fenster **Acronis Secure Zone löschen** die Volumes, welchen Sie den durch die Zone freigegebenen Platz zuweisen wollen – klicken Sie dannn auf **OK**.

   Der Platz wird proportional auf jedes Volume verteilt, sofern Sie mehrere ausgewählt haben. Der freigegebene Bereich wird zu 'nicht zugeordneten' Speicherplatz, wenn Sie kein Volume auswählen.

Nachdem Sie auf **OK** geklickt haben, beginnt Acronis Backup & Recovery 10 mit der Löschung der Zone.

6.9 Acronis Startup Recovery Manager

Der Acronis Startup Recovery Manager ist eine Modifikation des bootfähigen Agenten (S. 188), befindet sich unter Windows auf der Systemfestplatte, bzw. unter Linux auf der /boot-Partition, und ist so konfiguriert, dass er durch Drücken von F11 während des Boot-Vorgangs gestartet wird. Dies bietet eine Alternative zum Einsatz separater Medien oder zu einer Netzwerkverbindung für den Start der bootfähigen Rettungsumgebung.

Aktivieren von

Aktiviert die Boot-Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Manager…“ (sofern Sie keinen GRUB Boot-Loader haben) oder fügt den Menü-Eintrag „Acronis Startup Recovery Manager“ zum Menü von GRUB hinzu (sofern Sie GRUB haben). Wenn das System nicht bootet, können Sie das bootfähige Rettungswerkzeug starten, indem Sie die F11-Taste drücken oder es aus dem Menü auswählen.

Auf der Systemfestplatte (bzw. der /boot-Partition unter Linux) sollten mindestens 70 MB freier Speicherplatz verfügbar sein, um den Acronis Startup Recovery Manager zu aktivieren.

Die Aktivierung des Acronis Startup Recovery Manager überschreibt den Master Boot Record (MBR) mit seinem eigenen Boot-Code, außer Sie verwenden den GRUB Boot-Loader und dieser ist im MBR installiert. Daher müssen Sie möglicherweise auch die Boot-Loader von Drittherstellern reaktivieren, wenn diese installiert sind.

Wenn Sie unter Linux einen anderen Boot-Loader als GRUB verwenden (wie etwa LILO), sollten Sie erwägen, diesen statt in den MBR in den Boot-Record einer Linux-root- oder Boot-Partition zu installieren, bevor Sie den ASRM aktivieren. Andernfalls konfigurieren Sie den Boot-Loader manuell nach der Aktivierung.

Nicht aktivieren

Deaktiviert die Boot-Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers…“ (oder den Menü-Eintrag in GRUB). Falls der Acronis Startup Recovery Manager nicht aktiviert ist, müssen Sie zur Wiederherstellung eines nicht mehr bootfähigen Systems Folgendes tun:

- Booten Sie die Maschine mit Hilfe eines separaten bootfähigen Rettungsmediums.
- Verwenden Sie einen Netzwerk-Boot von einem Acronis PXE Server oder Microsoft Remote Installation Services (RIS).

Zu Details siehe den Abschnitt Bootfähige Medien (S. 171).

6.10 Bootfähiges Medium

Bootfähiges Medium

Ein bootfähiges Medium ist ein physikalisches Medium (CD, DVD, USB-Laufwerk oder andere Medien, die vom BIOS einer Maschine als Boot-Gerät unterstützt werden), das auf jeder PC-kompatiblen Maschine startet und es Ihnen ermöglicht, den Acronis Backup & Recovery 10 Agenten in einem Linux-Umfeld oder unter Windows Preinstallation Environment (WinPE) auszuführen (also ohne die Hilfe eines bereits vorhandenen Betriebssystems). Bootfähige Medien werden am häufigsten benutzt, um:

- ein Betriebssystem wiederherzustellen, das nicht mehr bootet
- auf Daten zuzugreifen und diese zu sichern, die in einem beschädigten System überlebt haben
- ein Betriebssystem auf einen fabrikneuen Computer auszubringen
- Volumes vom Typ Basis oder Dynamisch auf fabrikneuen Festplatten einzurichten
- Sektor-für-Sektor-Backups von Laufwerken mit nicht unterstütztem Dateisystem auszuführen,
- offline beliebige Daten zu sichern, die online wegen eingeschränkten Zugangs, permanenter Sperrung durch laufende Anwendungen oder aus anderem Grund nicht gesichert werden können.

Eine Maschine kann in die genannten Umgebungen entweder mit physikalischen Medien oder durch Netzwerk-Booten von einem Acronis PXE Server, von einem Windows Deployment Service (WDS) oder Remote Installation Service (RIS) gestartet werden. Diese Server mit ihren hochgeladenen, bootfähigen Komponenten können auch als eine Art bootfähiger Medien betrachtet werden. Sie können mit demselben Assistenten bootfähige Medien erstellen und den PXE Server oder WDS/RIS-Dienste konfigurieren.

Linux-basierte bootfähige Medien

Linux-basierte Medien, die den bootfähigen Acronis Backup & Recovery 10 Agenten enthalten, verwenden einen Linux-Kernel. Der Agent kann auf jeder PC-kompatiblen Hardware booten und dort Aktionen ausführen, einschließlich auf fabrikneuer Hardware und Maschinen mit beschädigten oder nicht unterstützten Dateisystemen. Diese Aktionen können per Management Konsole konfiguriert und gesteuert werden – lokal oder per Remotesteuerung.

PE-basierte bootfähige Medien

PE-basierte bootfähige Medien enthalten ein funktionsreduziertes Windows, Windows Preinstallation Environment (WinPE) genannt, sowie ein Acronis Plug-in für WinPE. Das ist eine Modifikation des Acronis Backup & Recovery 10 Agenten, damit dieser unter WinPE laufen kann.

WinPE hat sich gerade im weiträumigen Umfeld mit unterschiedlicher Hardware als praktischste bootfähige Lösung erwiesen.

Vorteile:

- Die Verwendung von Acronis Backup & Recovery 10 in WinPE bietet mehr Funktionalität als die Verwendung Linux-basierter bootfähiger Medien. Indem Sie auf der PC-kompatiblen Hardware WinPE booten, können Sie nicht nur den Acronis Backup & Recovery 10 Agenten verwenden, sondern auch PE-Befehle, Skripte und andere Plug-ins, die Sie in WinPE eingebunden haben.
- Auf PE basierende bootfähige Medien helfen, Linux-bezogene Probleme zu umgehen; z.B. fehlende Unterstützung für RAID-Controller oder gewisse RAID-Level. Medien, die auf PE 2.x basieren (also auf dem Kernel von Windows Vista oder Windows Server 2008), ermöglichen das dynamische Laden notwendiger Gerätetreiber.

6.10.1 Linux-basierte bootfähige Medien

Wenn Sie den Media Builder verwenden, müssen Sie Folgendes spezifizieren:

1. [Optional] Parameter für den Linux-Kernel. Trennen Sie multiple Parameter mit Leerzeichen.

   Um z.B. einen Anzeigemodus für den bootfähigen Agenten jedes Mal auszuwählen, wenn das Medium startet, geben Sie an: **vga=ask**

   Eine Liste der Parameter finden Sie unter Kernel Parameter (S. 173).
2. Die bootfähigen Acronis-Komponenten, die für das Medium bestimmt sind.
   - Universal Restore kann dann aktiviert werden, wenn Acronis Backup & Recovery 10 Universal Restore auf der Maschine installiert ist, auf der das Medium erstellt wird.
3. [Optional] Das Timeout-Intervall für das Boot-Menü sowie die Komponente, die automatisch nach dem Timeout gestartet wird.
   - Sofern nicht anders konfiguriert, wartet der Acronis Loader auf eine Auswahl, ob das Betriebssystem (sofern vorhanden) oder die Acronis-Komponente gestartet werden soll.
   - Wenn Sie z.B. **10 Sek.** für den bootfähigen Agenten einstellen, wird dieser 10 Sekunden nach Anzeige des Menüs starten. Dies ermöglicht den unbeaufsichtigten Betrieb vor Ort, wenn von einem PXE Server oder WDS/RIS gebootet wird.
4. [Optional] Remote-Anmeldeeinstellungen:
   - Einzugebender Benutzername und Kennwort auf Konsolenseite bei Verbindung zum Agenten. Wenn Sie diese Felder frei lassen, wird die Verbindung in dem Augenblick aktiviert, wenn Sie irgendein Symbol in das Eingabefenster eintippen.
5. [Optional] Netzwerk-Einstellungen (S. 174):
   - TCP/IP-Einstellungen, die dem Netzwerkadapter der Maschine zugewiesen werden.
6. [Optional] Netzwerk-Port (S. 175):
   - Der TCP-Port, den der bootfähige Agent auf einkommende Verbindungen kontrolliert.
7. Der zu erstellende Medien-Typ. Sie können:
   - CD, DVD oder andere bootfähige Medien erstellen (z.B. USB-Sticks), sofern das BIOS der Hardware das Booten von diesen Medien erlaubt
   - ein ISO-Image der bootfähigen Disc erstellen, um es später auf einen leeren Rohling zu brennen
   - die gewählten Komponenten auf den Acronis PXE Server hochladen
   - die gewählten Komponenten auf einen WDS/RIS hochladen.

8. [Optional] Windows System-Treiber zur Verwendung durch Acronis Universal Restore. Dieses Fenster erscheint nur, wenn das Acronis Universal Restore Add-on installiert ist und ein anderes Medium als PXE oder WDS/RIS gewählt wurde.
9. Pfad zur ISO-Datei des Mediums oder Name oder IP-Adresse inklusive Anmeldedaten für PXE oder WDS/RIS.

Kernel-Parameter

In diesem Fenster können Sie einen oder mehrere Parameter des Linux-Kernel angeben. Diese werden automatisch wirksam, wenn das bootfähige Medium startet.

Typischerweise kommen diese Parameter zur Anwendung, wenn während der Arbeit mit bootfähigen Medien Probleme auftauchen. Normalerweise brauchen Sie in dieses Feld nichts einzutragen.

Sie können jeden dieser Parameter auch durch Drücken der Taste F11 im Boot-Menü angeben.

Parameter

Trennen Sie mehrere Parameter mit Leerzeichen.

acpi=off

Deaktiviert ACPI (Advanced Configuration and Power Interface). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.

noapic

Deaktiviert APIC (Advanced Programmable Interrupt Controller). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.

vga=ask

Erfragt den Grafikkartenmodus, der in der grafischen Benutzeroberfläche eines bootfähigen Mediums verwendet werden soll. Ist kein **vga**-Parameter angegeben, wird der Videomodus automatisch erkannt.

vga=*mode_number*

Spezifiziert den Grafikkartenmodus, der in der grafischen Benutzeroberfläche des bootfähigen Mediums verwendet werden soll. Die Modus-Nummer wird unter *mode_number* im Hexadezimalformat angegeben, z.B.: **vga=0x318**

Die Bildschirmauflösung und die Anzahl der Farben für eine Modus-Nummer können sich von Maschine zu Maschine unterscheiden. Es wird empfohlen, zunächst den Parameter **vga=ask** zu verwenden, um einen Wert für *mode_number* auszuwählen.

quiet

Deaktiviert die Anzeige von Pop-up-Meldungen während der Linux-Kernel geladen wird und startet danach die Management Konsole.

Dieser Parameter wird implizit bei der Erstellung von bootfähigen Medien spezifiziert; Sie können ihn jedoch im Boot-Menü entfernen.

Wenn der Parameter nicht angegeben ist, werden alle Meldungen beim Start angezeigt, gefolgt von einer Eingabeaufforderung. Geben Sie bei der Eingabeaufforderung folgenden Befehl ein, um die Management Konsole zu starten: **/bin/product**

nousb

Deaktiviert, dass das USB-Subsystem geladen wird.

nousb2

Deaktiviert die USB 2.0-Unterstützung. USB 1.1-Geräte arbeiten, auch wenn dieser Parameter gesetzt ist. Mit dem Parameter können Sie manche USB-Laufwerke im USB 1.1-Modus verwenden, wenn sie im USB 2.0-Modus nicht arbeiten.

nodma

Deaktiviert den Speicherdirektzugriff (DMA) für alle IDE-Festplatten. Verhindert auf mancher Hardware ein Einfrieren des Kernels.

nofw

Deaktiviert die Unterstützung für die FireWire (IEEE1394)-Schnittstelle.

nopcmcia

Deaktiviert die Erkennung von PCMCIA-Hardware.

nomouse

Deaktiviert die Maus-Unterstützung.

module_name=**off**

Deaktiviert das Modul, dessen Name in *module_name* angeben ist. Um beispielsweise die Nutzung des SATA-Moduls zu deaktivieren, geben Sie folgenden Wert an: **sata_sis=off**

pci=bios

Erzwingt die Verwendung des PCI-BIOS statt direkt auf die Hardware-Geräte zuzugreifen. Dieser Parameter kann hilfreich sein, z.B. wenn die Maschine eine nicht standardgemäße PCI Host-Bridge hat.

pci=nobios

Deaktiviert die Verwendung des PCI BIOS und erlaubt nur direkte Hardware-Zugriffsmethoden. Dieser Parameter kann z.B. hilfreich sein, wenn das bootfähige Medium nicht startet und dies wahrscheinlich durch das BIOS verursacht wird.

pci=biosirq

Verwendet PCI BIOS-Aufrufe, um die Interrupt Routing-Tabelle zu erhalten. Dieser Parameter kann hilfreich sein, wenn es dem Kernel nicht gelingt, Unterbrechungsanforderungen (IRQs) zuzuordnen oder den sekundären PCI-Bus auf dem Mainboard zu finden.

Auf einigen Maschinen funktionieren diese Aufrufe möglicherweise nicht richtig. Es kann unter Umständen aber der einzige Weg sein, die Interrupt Routing-Tabelle anzuzeigen.

Netzwerk-Einstellungen

Sie erhalten während der Erstellung bootfähiger Acronis-Medien die Möglichkeit, die Netzwerkverbindungen vorzukonfigurieren, die vom bootfähigen Agenten verwendet werden. Die folgenden Parameter können vorkonfiguriert werden:

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server
- WINS-Server

Sobald der bootfähige Agent auf einer Maschine gestartet ist, wird die Konfiguration auf die Netzwerkkarte (NIC) der Maschine angewendet. Wenn die Einstellungen nicht vorkonfiguriert

wurden, benutzt der Agent eine DHCP-Autokonfiguration. Sie haben außerdem die Möglichkeit, die Netzwerkeinstellungen manuell vorzunehmen, sobald der bootfähige Agent auf der Maschine läuft.

Mehrfache Netzwerkverbindungen vorkonfigurieren

Sie können die TCP/IP-Einstellungen für bis zu zehn Netzwerkkarten vorkonfigurieren. Um sicherzustellen, dass jede Netzwerkkarte die passenden Einstellungen bekommt, sollten Sie das Medium auf dem Server erstellen, für den das Medium konfiguriert wird. Wenn Sie eine existierende NIC im Assistentenfenster anwählen, werden ihre Einstellungen zur Speicherung auf das Medium übernommen. Die MAC-Adresse jeder existierenden NIC wird ebenso auf dem Medium gespeichert.

Sie können die Einstellungen ändern, mit Ausnahme der MAC-Adresse; oder Einstellungen für nicht existierende NICs konfigurieren, falls das nötig ist.

Sobald der bootfähige Agent auf dem Server gestartet ist, fragt er die Liste der verfügbaren NICs ab. Diese Liste ist nach den Steckplätzen sortiert, die von den NICs belegt werden. An der Spitze stehen die, die dem Prozessor am nächsten liegen.

Der bootfähige Agent teilt jeder bekannten NIC die passenden Einstellungen zu, wobei die NICs anhand ihrer MAC-Adressen identifiziert werden. Nachdem die NICs mit bekannten MAC-Adressen konfiguriert wurden, bekommen die verbliebenen NICs (beginnend mit der untersten in der Liste) die Einstellungen zugewiesen, die Sie für unbekannte NICs vorkonfiguriert haben.

Sie können bootfähige Medien für jede beliebige Maschine konfigurieren – und nicht nur für die Maschine, auf der das Medium erstellt wurde. Um dies durchzuführen, konfigurieren Sie die NICs entsprechend ihrer Steckplatzreihenfolge in der betreffenden Maschine. NIC1 besetzt den zum Prozessor am nächsten liegenden Steckplatz, NIC2 wiederum den folgenden und so weiter. Wenn der bootfähige Agent auf der Maschine startet, wird er keine NICs mit bekannter MAC-Adresse finden und daher die NICs in der von Ihnen bestimmten Reihenfolge konfigurieren.

Beispiel

Der bootfähige Agent könnte einen der Netzwerkadapter zur Kommunikation mit der Management Konsole innerhalb des Fertigungsnetzwerkes nutzen. Für diese Verbindung könnte eine automatische Konfiguration durchgeführt werden. Größere Datenmengen für eine Wiederherstellung könnten über die zweite NIC übertragen werden, die in das dafür bestimmte Backup-Netzwerk mit Hilfe statischer TCP/IP-Einstellungen eingebunden ist.

Netzwerk-Port

Bei der Erstellung bootfähiger Medien finden Sie eine Option zur Vorkonfiguration des Netzwerk-Ports, auf dem der bootfähige Agent nach einkommenden Verbindungen horcht. Es besteht die Wahl zwischen:

- dem Standard-Port
- dem aktuell verwendeten Port
- dem neuen Port (geben Sie die Port-Nummer ein)

Sofern der Port nicht vorkonfiguriert wurde, verwendet der Agent die Standard-Port-Nummer (9876). Dieser Port wird außerdem auch als Standard von der Acronis Backup & Recovery 10 Management Console verwendet.

6.10.2 Verbindung zu einer Maschine, die von einem Medium gebootet wurde

Sobald eine Maschine von einem bootfähigen Medium gestartet ist, erscheint ein Konsolenfenster mit den IP-Adressen, die per DHCP oder als manuell vorkonfigurierte Werte zugewiesen wurden.

Remote-Verbindung

Um remote zu einer Maschine zu verbinden, wählen Sie **Verbinden –> Remote-Maschine verwalten** im Menü der Konsole und spezifizieren Sie eine der IP-Adressen der Maschine. Halten Sie Benutzername und Passwort bereit, sofern diese bei Erstellung des Bootmediums konfiguriert wurden.

Lokale Verbindung

Die Acronis Backup & Recovery 10 Management Console ist auf dem bootfähigen Medium immer vorhanden. Jeder, der zum Terminal der Maschine physikalischen Zugang hat, kann die Konsole ausführen und sich verbinden. Klicken Sie einfach **Management Konsole starten** im Startfenster des bootfähigen Agenten.

6.10.3 Mit bootfähigen Medien arbeiten

Die Arbeitsweise mit einer Maschine, die per bootfähigem Medium gestartet wurde, ist sehr ähnlich zu den Backup- und Recovery-Aktionen unter dem sonst üblichen Betriebssystem. Der Unterschied ist folgender:

1. Laufwerksbuchstaben, die unter Windows-basierten Boot-Medien zu sehen sind, können von der Art abweichen, wie Windows seine Laufwerke normalerweise identifiziert. So könnte beispielsweise die Zuordnung des Laufwerks D: unter dem Notfallwerkzeug dem Laufwerk E: entsprechen, welches Windows verwendet.

   Achtung! Um auf der sicheren Seite zu sein, ist es ratsam, den jeweils verwendeten Volumes eindeutige Namen zuzuweisen.

2. Ein Linux-typisches bootfähiges Medium zeigt lokale Laufwerke und Volumes als 'unmounted' an (sda1, sda2...).
3. Ein bootfähiges Medium im Stil 'Linux-basiert' kann keine Backups auf ein NTFS-formatiertes Volume schreiben. Wechseln Sie zum Stil 'Windows-basiert', wenn Sie diese Funktion benötigen.
4. Sie können den Arbeitsstil des bootfähigen Mediums zwischen Windows- und Linux-basiert umschalten, indem Sie **Extras** –> **Volume-Darstellung ändern** wählen.
5. Der Verzeichnisbaum **Navigation** ist in der Benutzeroberfläche des Mediums nicht vorhanden. Verwenden Sie den Menübefehl **Navigation**, um zwischen verschiedenen Ansichten umzuschalten.
6. Es können keine geplanten Tasks benutzt werden, da grundsätzlich keine Tasks erstellt werden können. Um eine Aktion zu wiederholen, konfigurieren Sie sie von Anfang an neu.
7. Der Speicherzeitraum für Ereignisse (Logs) ist auf die aktuelle Sitzung beschränkt. Sie können die gesamte Ereignisliste oder gefilterte Logs in eine Datei speichern.
8. Zentrale Depots werden im Verzeichnisbaum des Fensters **Archiv** nicht angezeigt.

   Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein:

   bsp://knoten_adresse/depot_name/

   Um auf ein nicht verwaltetes zentrales Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.

   Nach Eingabe der Anmeldedaten sehen Sie eine Liste der Archive, die sich im Depot befinden.

Einen Anzeigemodus einstellen

Bei einer von einem bootfähigen Medium gestarten Maschine wird der Anzeigemodus basierend auf der Hardware-Konfiguration automatisch erkannt (Monitor- und Grafikkarten-Spezifikationen). Sollte aus irgendeinem Grund der Darstellungsmodus nicht korrekt erkannt werden, gehen Sie folgendermaßen vor:

1. Drücken Sie im Boot-Menü auf F11.
2. Geben Sie in die Eingabeaufforderung folgenden Befehl ein: **vga=ask**, fahren Sie dann mit dem Boot-Vorgang fort.
3. Wählen Sie aus der Liste der verfügbaren Darstellungsmodi den passenden durch Eingabe seiner Nummer (z.B. **318**), drücken Sie dann auf Enter.

Falls Sie diese Schritte nicht jedes Mal ausführen möchten, wenn Sie auf einer bestimmten Hardwarekonfiguration von einem Boot-Medium starten, erstellen Sie das Medium mit der entsprechenden Modus-Nummer (in unserem Beispiel: **vga=0x318**) im Fenster **Kernel-Parameter** (weitere Informationen finden Sie im Abschnitt Bootable Media Builder (S. 172)).

iSCSI- und NDAS-Geräte konfigurieren

Dieser Abschnitt beschreibt, wie iSCSI (Internet Small Computer System Interface)- und NDAS (Network Direct Attached Storage)-Geräte bei der Arbeit mit bootfähigen Medien konfiguriert werden.

Diese Geräte sind über eine Netzwerkschnittstelle mit der Maschine verbunden und werden angezeigt, als wären sie lokal angeschlossene Geräte. Im Netzwerk werden iSCSI-Geräte über ihre IP-Adresse und NDAS-Geräte über ihre Geräte-ID identifiziert.

iSCSI-Geräte werden manchmal auch als iSCSI-Target bezeichnet. Eine Hard- oder Software-Komponente, die das Zusammenspiel von Maschine und iSCSI-Target ermöglicht, wird als iSCSI-Initiator bezeichnet. Der Name des iSCSI-Initiators wird üblicherweise durch den Administrator des Servers bestimmt, der das Gerät hostet.

So fügen Sie ein iSCSI-Gerät hinzu

1. Führen sie in einem (Linux- oder PE-basierten) Boot-Medium die Management Konsole aus.
2. Klicken Sie auf **iSCSI/NDAS-Geräte konfigurieren** (in einem Linux-basierten Medium) bzw. auf **iSCSI-Setup ausführen** (in einem PE-basierten Medium).
3. Geben Sie vom Host des iSCSI-Gerät die IP-Adresse und den Port an und zudem den Namen des iSCSI-Initiators.
4. Benötigt der Host eine Authentifizierung, dann geben Sie Benutzernamen und Kennwort ein.
5. Klicken Sie auf **OK**.
6. Wählen Sie das iSCSI-Gerät aus der Liste und klicken Sie dann auf **Verbinden**.
7. Spezifizieren Sie bei Erscheinen einer Eingabeaufforderung Benutzernamen und Kennwort, um auf das iSCSI-Gerät zugreifen zu können.

So fügen Sie ein NDAS-Gerät hinzu

1. Führen sie in einem Linux-basierten Boot-Medium die Management Konsole aus.
2. Klicken Sie auf **iSCSI/NDAS-Geräte konfigurieren**.
3. Klicken Sie in **NDAS-Geräte** auf **Gerät hinzufügen**.
4. Geben Sie die 20-stellige Geräte-ID an.

5. Geben Sie den fünfstelligen Schreibschlüssel an, wenn Sie erlauben wollen, dass Daten auf das Gerät geschrieben werden. Ohne diesen Schlüssel wird das Gerät nur im 'Read-only'-Modus verfügbar sein.
6. Klicken Sie auf **OK**.

6.10.4 Liste verfügbarer Befehle und Werkzeuge auf Linux-basierten Boot-Medien

Linux-basierte Boot-Medien enthalten folgende Kommandos und Befehlszeilen-Werkzeuge, die Sie bei Ausführung einer Eingabeaufforderung nutzen können. Zum Starten der Eingabeaufforderung drücken Sie Strg+Alt+F2, während Sie in der Management Konsole des bootfähigen Mediums sind.

Acronis-Befehlszeilen-Werkzeuge

- `acronis`
- `asamba`
- `lash`
- `restoreraids`
- `trueimagecmd`
- `trueimagemnt`

Linux-Befehle und Werkzeuge

`busybox`	`ifconfig`	`rm`
`cat`	`init`	`rmmod`
`cdrecord`	`insmod`	`route`
`chmod`	`iscsiadm`	`scp`
`chown`	`kill`	`scsi_id`
`chroot`	`kpartx`	`sed`
`cp`	`ln`	`sg_map26`
`dd`	`ls`	`sh`
`df`	`lspci`	`sleep`
`dmesg`	`lvm`	`ssh`
`dmraid`	`mdadm`	`sshd`
`e2fsck`	`mkdir`	`strace`
`e2label`	`mke2fs`	`swapoff`
`echo`	`mknod`	`swapon`
`egrep`	`mkswap`	`sysinfo`
`fdisk`	`more`	`tar`
`fsck`	`mount`	`tune2fs`
`fxload`	`mtx`	`udev`

```
gawk       mv           udevinfo
gpm        pccardctl    udevstart
grep       ping         umount
growisofs  pktsetup     uuidgen
grub       poweroff     vconfig
gunzip     ps           vi
halt       raidautorun  zcat
hexdump    readcd
hotplug    reboot
```

6.10.5 MD-Geräte und logische Volumes wiederherstellen

Um MD-Geräte (auch Linux-Software-RAID genannt) bzw. durch den Logical Volume Manager (LVM) erzeugte Geräte (auch logische Volumes genannt) wiederherzustellen, müssen Sie vor der Wiederherstellung erst die korrespondierende Volume-Struktur erzeugen.

Sie können die Volume-Struktur auf eine der folgenden Arten erstellen:

- Automatisch auf Linux-basierten Boot-Medien mit der Management Konsole oder einem Skript – siehe Volume-Struktur automatisch erstellen (S. 179).
- Manuell unter Verwendung der Utilities **mdadm** und **lvm** – siehe Volume-Struktur manuell erstellen (S. 180).

Volume-Struktur automatisch erstellen

Angenommen, Sie haben Ihre Volume-Struktur im Verzeichnis /etc/Acronis gespeichert (S. 36) und dass das Volume mit diesem Verzeichnis im Archiv enthalten ist.

Um die Volume-Struktur auf einem Linux-basierten Boot-Medium neu zu erstellen, verwenden Sie eine der nachfolgend beschriebenen Methoden.

Vorsicht: *Wenn Sie die folgenden Schritte ausführen, wird die aktuelle Volume-Struktur auf der Maschine durch die im Archiv gespeicherte Struktur ersetzt. Damit werden die aktuell auf einigen bzw. allen Ziellaufwerken der Maschine gespeicherten Daten gelöscht.*

Bei veränderter Laufwerkskonfiguration. Ein MD-Gerät oder ein logisches Volume befindet sich auf einem bzw. mehreren Laufwerk(en), wovon jedes eine bestimmte Größe hat. Wenn Sie eines dieser Laufwerke zwischen Backup und Wiederherstellung austauschen – oder die Volumes auf einer anderen Maschine wiederherstellen – müssen Sie sicherstellen, dass die neue Laufwerkskonfiguration genug Laufwerke umfasst, die mindestens genau so groß wie die ursprünglichen Laufwerke sind.

So erstellen Sie die Volume-Struktur mit der Management Konsole

1. Booten Sie die Maschine von einem Linux-basierten Boot-Medium.
2. Klicken Sie auf **Acronis Bootable Agent**. Wählen Sie dann **Management Konsole starten**.
3. Wählen Sie in der Management Konsole **Recovery**.

   Unter dem Inhalt des Archivs zeigt Acronis Backup & Recovery 10 eine Meldung an, dass Informationen über die Volume-Struktur gefunden wurden.

4. Klicken Sie in dem Bereich, in dem die Meldung erscheint, auf **Details**.
5. Überprüfen Sie die Volume-Struktur und klicken Sie dann auf **RAID/LVM übernehmen** um sie zu erstellen.

So erstellen Sie die Volume-Struktur durch Verwendung eines Skripts

1. Booten Sie die Maschine von einem Linux-basierten Boot-Medium.
2. Klicken Sie auf **Acronis Bootable Agent**. Wählen Sie dann **Management Konsole starten**.
3. Klicken Sie in der Symbolleiste auf **Aktionen** und dann **Shell starten**. Alternativ können Sie auch Strg+Alt+F2 drücken.
4. Führen Sie das Skript **restoreraids.sh** aus, unter Angabe des vollen Dateinamens für das Archiv – beispielsweise:

   ```
   /bin/restoreraids.sh
   smb://server/backups/linux_machine_2010_01_02_12_00_00_123D.tib
   ```

5. Wechseln Sie zurück zur Management Konsole durch Drücken von Strg+Alt+F1 – oder durch Eingabe des folgenden Befehls: **/bin/product**
6. Klicken Sie auf **Recovery**, spezifizieren Sie dann den Pfad zum Archiv sowie andere benötigte Parameter und klicken Sie dann **OK**.

Sollte Acronis Backup & Recovery 10 die Volume-Struktur nicht erstellen (oder nicht im Archiv vorliegen), dann erstellen Sie die Struktur manuell.

Volume-Struktur manuell erstellen

Das Nachfolgende beschreibt eine allgemeine Prozedur und ein Beispiel für eine Wiederherstellung von MD-Geräten sowie logischen Volumes durch Verwendung eines Linux-basierten Boot-Mediums. Sie können ein ähnliches Verfahren unter Linux benutzen.

So stellen Sie MD-Geräte und logische Volumes wieder her:

1. Booten Sie die Maschine von einem Linux-basierten Boot-Medium.
2. Klicken Sie auf **Acronis Bootable Agent**. Wählen Sie dann **Management Konsole starten**.
3. Klicken Sie in der Symbolleiste auf **Aktionen** und dann **Shell starten**. Alternativ können Sie auch Strg+Alt+F2 drücken.
4. Sofern notwendig, können Sie die Struktur der im Archiv gespeicherten Laufwerke durch Verwendung des Werkzeugs **trueimagecmd** untersuchen. Sie können außerdem das Werkzeug **trueimagemnt** benutzen, um eines oder mehrere dieser Volumes so anzuschließen, als würde es sich um reguläre Volumes handeln (siehe „Backup-Volumes mounten“ im Verlauf dieses Themas).
5. Erstellen Sie eine dem Archiv entsprechende Volume-Struktur durch Verwendung des Werkzeugs **mdadm** (für MD-Geräte), des Werkzeugs **lvm** (für logische Volumes) oder durch beide.

   Anmerkung: *Logical Volume Manager-Werkzeuge wie* ***pvcreate*** *und* ***vgcreate****, die unter Linux normalerweise verfügbar sind, sind auf dem Boot-Medium nicht enthalten. Sie müssen daher das* ***lvm****-Werkzeug als korrespondierenden Befehl verwenden:* ***lvm pvcreate****,* ***lvm vgcreate****, etc.*

6. Sollten Sie das Backup zuvor durch Verwendung des **trueimagemnt**-Werkzeugs gemountet haben, so nutzen Sie das Utility erneut, um das Backup abzuschalten (siehe „Backup-Volumes mounten“ im Verlauf dieses Themas).
7. Wechseln Sie zurück zur Management Konsole durch Drücken von Strg+Alt+F1 – oder durch Eingabe des folgenden Befehls: **/bin/product**

   (Starten Sie an dieser Stelle die Maschine nicht neu. Ansonsten müssen Sie die Volume-Struktur wieder neu erstellen.)

8. Klicken Sie auf **Recovery**, spezifizieren Sie dann den Pfad zum Archiv sowie andere benötigte Parameter und klicken Sie dann **OK**.

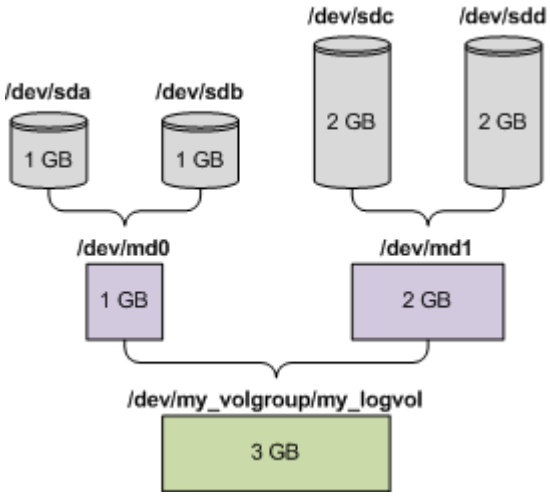
Anmerkung: *Diese Prozedur funktioniert nicht, wenn Sie zum Acronis Backup & Recovery 10 Bootable Agent remote verbunden sind, weil hier für diesen Fall die Eingabeaufforderung nicht verfügbar ist.*

Beispiel

Angenommen, Sie haben zuvor ein Laufwerk-Backup auf einer Maschine mit folgender Laufwerkskonfiguration durchgeführt:

- Die Maschine hat zwei 1-Gigabyte und zwei 2-Gigabyte-SCSI-Laufwerke, die als **/dev/sda**, **/dev/sdb**, **/dev/sdc** beziehungsweise **/dev/sdd** angeschlossen sind.
- Die ersten und zweiten Laufwerkspaare sind als zwei MD-Geräte konfiguriert, beide in RAID-1-Konfiguration – und angeschlossen als **/dev/md0** beziehungsweise **/dev/md1**.
- Ein logisches Volume basiert auf den beiden MD-Geräten und ist als **/dev/my_volgroup/my_logvol** gemountet.

Das folgende Bild illustriert diese Konfiguration.



Stellen Sie Daten von dieser Maschine wie folgt wieder her.

Schritt 1: Volume-Struktur erstellen

1. Booten Sie die Maschine von einem Linux-basierten Boot-Medium.
2. Drücken Sie Strg+Alt+F2 in der Management Konsole.
3. Führen Sie folgenden Befehle aus, um die MD-Geräte zu erstellen:

```
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[ab]
mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sd[cd]
```

4. Führen Sie folgende Befehle aus, um die logische Volume-Gruppe zu erstellen:

   Vorsicht: *Der Befehl* ***pvcreate*** *zerstört alle Daten auf den Geräten* ***/dev/md0*** *und* ***/dev/md1****.*

   ```
   lvm pvcreate /dev/md0 /dev/md1
   lvm vgcreate my_volgroup /dev/md0 /dev/md1
   lvm vgdisplay
   ```

   Die Ausgabe des **lvm vgdisplay**-Befehls wird Zeilen ähnlich wie diese enthalten:

```
--- Volume group ---
VG Name     my_volgroup
...
VG Access   read/write
VG Status   resizable
...
VG Size     1.99 GB
...
VG UUID     0qoQ4l-Vk7W-yDG3-uF1l-Q2AL-C0z0-vMeACu
```

5. Führen Sie folgenden Befehl aus, um das logische Volume zu erstellen; wobei Sie im **-L**-Parameter die gegebene Größe durch **VG Size** spezifizieren:

   ```
   lvm lvcreate -L1.99G --name my_logvol my_volgroup
   ```

6. Aktivieren Sie die Volume-Gruppe durch Ausführung folgenden Befehls:

   ```
   lvm vgchange -a y my_volgroup
   ```

7. Drücken Sie Strg+Alt+F1, um zur Management Konsole zurückzukehren.

Schritt 2: Wiederherstellung starten

1. Wählen Sie in der Management Konsole **Wiederherstellen**.
2. Wählen Sie bei **Archiv** den Befehl **Ändern** und spezifizieren dann den Archivnamen.
3. Wählen Sie bei **Backup** den Befehl **Ändern** und dann das Backup, aus dem Sie die Daten wiederherstellen möchten.
4. Wählen Sie bei **Datentyp** den Befehl **Volumes**.
5. Aktivieren Sie bei **Wiederherstellen von** das Kontrollkästchen neben **my_volgroup-my_logvol**.
6. Wählen Sie unter **Recovery-Ziel** den Befehl **Ändern** und aktivieren Sie jenes logische Volume, das Sie in Schritt 1 erzeugt haben. Nutzen Sie die Chevron-Symbole zum Aufklappen der Laufwerksliste.
7. Wählen Sie **OK**, um die Wiederherstellung zu starten.

Für eine vollständige Liste aller Befehle und Utilities, die Sie in der Betriebssystem-Umgebung des Boot-Mediums verwenden können, siehe 'Liste der verfügbaren Befehle und Werkzeuge in Linux-basierten Boot-Medien (S. 178)'. Für eine detaillierte Beschreibung der **trueimagecmd** und **trueimagemnt**-Werkzeuge siehe die Acronis Backup & Recovery 10-Befehlszeilen-Referenz.

Backup-Volumes mounten (anschließen)

Möglicherweise wollen Sie ein in einem Laufwerk-Backup gespeichertes Volume mounten, um einige Dateien vor dem Start der Wiederherstellung einzusehen.

So mounten Sie ein Backup-Volume

1. Verwenden Sie das **--list**-Kommando, um die im Backup gespeicherten Volumes aufzulisten. Beispielsweise:

   ```
   trueimagecmd --list --filename:smb://server/backups/linux_machine.tib
   ```

   Die Ausgabe wird Zeilen ähnlich wie diese enthalten:

   ```
   Num  Idx Partition Flags Start Size      Type
   ---- --- --------- ----- ----- --------- ------
   Disk 1:
            Table           0               Table
   Disk 2:
            Table           0               Table
   ...
   Dynamic & GPT Volumes:
   DYN1 4   my_volgroup-my_logvol 12533760  Ext2
   ```


Für den nächsten Schritt benötigen Sie den Volume-Index, der in der **Idx**-Spalte enthalten ist.

2. Verwenden Sie das **--mount**-Kommando, wobei der Volume-Index über den **-i**-Parameter spezifiziert wird. Beispielsweise:

```
trueimagemnt --mount /mnt --filename smb://server/backups/linux_machine.tib -i
4
```

Dieses Kommando schließt das logische Volume DYN1, dessen Index im Backup die 4 ist, an den Mount-Punkt /mnt an.

So trennen Sie ein Backup-Volume wieder (unmount)

- Verwenden Sie das **--unmount**-Kommando, wobei Sie den Mount-Punkt des Volumes als Parameter spezifizieren. Beispielsweise:

```
trueimagemnt --unmount /mnt
```

6.11 Sammeln von Systeminformationen

Das Werkzeug zum Sammeln von Systeminformationen sammelt Daten über die Maschine, mit der die Management Konsole verbunden ist, und speichert sie in einer Datei. Sie können diese Datei dem Acronis Technical Support zur Verfügung stellen, wenn Sie diesen kontaktieren.

Diese Option ist bei bootfähigen Medien verfügbar und für Maschinen, auf denen der Agent für Windows, Agent für Linux, oder der Acronis Backup & Recovery 10 Management Server installiert ist.

So sammeln Sie Systeminformationen

1. Wählen Sie in der Management Konsole aus dem Hauptmenü **Hilfe** –> **Systeminformation von 'Maschinenname' sammeln**.
2. Spezifizieren Sie einen Speicherort für die Datei mit den Systeminformationen.

7 Glossar

A

Acronis Active Restore

Geschützte Technologie von Acronis, die ein System sofort verfügbar macht, nachdem die Wiederherstellung des Systems angefangen hat. Das System bootet aus dem Backup (S. 190) und die Maschine wird betriebsbereit, um notwendige Dienste zur Verfügung zu stellen. Die für eingehende Anforderungen notwendigen Daten werden mit der höchsten Priorität, alle anderen im Hintergrund wiederhergestellt. Einschränkungen:

- das Backup muss sich auf einem lokalen Laufwerk befinden (irgendeinem Gerät, das durch das BIOS verfügbar gemacht wird mit Ausnahmen des Bootens über das Netzwerk)
- Linux-Images werden nicht unterstützt.

Acronis Plugin für WinPE

Modifikation von Acronis Backup & Recovery 10 Agent für Windows, die in einer Preinstallation Environment ausgeführt werden kann. Das Plugin kann mit Hilfe von Bootable Media Builder zu einem Image für WinPE (S. 198) hinzugefügt werden. Die resultierenden bootfähigen Medien (S. 188) können benutzt werden, jede PC-kompatible Maschine zu starten, und, mit gewissen Einschränkungen, die meisten direkten Verwaltungsaufgaben (S. 190) ohne Hilfe des Betriebssystems auszuführen. Aktionen können entweder lokal über die Benutzerschnittstelle oder remote mit Hilfe der Konsole (S. 192) konfiguriert und gesteuert werden.

Acronis Secure Zone

Sichere Partition zur Ablage von Backup-Archiven (S. 185) auf einer verwalteten Maschine (S. 197). Vorteile:

- Ermöglicht die Wiederherstellung eines Laufwerks auf dasselbe Laufwerk, auf der auch die Laufwerk-Backups hinterlegt sind
- bietet eine kosteneffektive und handliche Methode zum Schutz vor Softwarefehlern, Virusangriffen, Bedienerfehlern
- Beseitigt die Notwendigkeit, in jedem Fall für Backup oder Wiederherstellung ein separates Medium oder eine Netzwerkverbindung bereitstellen zu müssen. Diese Funktion ist besonders nützlich für mobile Benutzer.
- kann als primärer Speicherort für die Funktion „Dual Destination Backup“ dienen.

Einschränkungen: Acronis Secure Zone kann nicht auf dynamischen Laufwerken (S. 190) oder Laufwerken mit GPT-Partitionsschema eingerichtet werden.

Die Acronis Secure Zone wird als persönliches Depot (S. 193) betrachtet.

Acronis Startup Recovery Manager (ASRM)

Eine Modifikation des bootfähigen Agenten (S. 188), auf dem Systemlaufwerk liegend und konfiguriert, um beim Booten zu starten, wenn die Taste F11 gedrückt wird. Acronis Startup Recovery Manager bietet eine Alternative zu Rettungsmedien oder einer Netzwerkverbindung, um ein bootfähiges Rettungswerkzeug zu starten.

Der Acronis Startup Recovery Manager ist besonders für mobile Anwender nützlich. Wenn ein Fehler auftritt, bootet der Benutzer die Maschine neu, drückt die F11-Taste, sobald die Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers…“ erscheint, und stellt dann die Daten auf die gleiche Weise wie mit den gewöhnlichen bootfähigen Medien wieder her.

Einschränkungen: Erfordert die Reaktivierung von Boot-Loadern außer Windows-Loadern und GRUB.

Agent (Acronis Backup & Recovery 10 Agent)

Anwendung, die das Backup und die Wiederherstellung von Daten und andere Verwaltungsaufgaben auf der Maschine (S. 193) ermöglicht, wie z.B. die Task-Verwaltung und Aktionen mit Festplatten.

Die Art Daten, die gesichert werden können, hängt vom Typ des Agenten ab. Acronis Backup & Recovery 10 enthält die Agenten für das Backup von Festplatten und Dateien und die Agenten für das Backup virtueller Maschinen, die auf Virtualisierungs-Servern bereitgestellt werden.

Agentenseitige Bereinigung

Bereinigung (S. 187), ausgeführt vom Agent (S. 185) in Übereinstimmung mit dem Backup-Plan (S. 186), der das Archiv (S. 185) erstellt hat. Agentenseitige Bereinigung erfolgt in nicht verwalteten Depots (S. 193).

Agentenseitige Validierung

Validierung (S. 196), ausgeführt vom Agent (S. 185) in Übereinstimmung mit dem Backup-Plan (S. 186), der das Archiv (S. 185) erstellt hat. Agentenseitige Validierung erfolgt in nicht verwalteten Depots (S. 193).

Archiv

Siehe Backup-Archiv (S. 185).

Auswahlregel

Teil einer Backup-Richtlinie (S. 186). Ermöglicht dem Administrator des Management Servers (S. 193), die Daten der Maschine für das Backup auszuwählen.

B

Backup

Ein Backup ist das Ergebnis einer einzelnen Backup-Aktion (S. 185). Physikalisch gesehen handelt es sich um eine Datei oder Bandaufzeichnung, die eine Kopie der gesicherten Daten zu einem spezifischen Zeitpunkt enthält. Backup-Dateien, die von Acronis Backup & Recovery 10 erstellt wurden, haben die Dateierweiterung tib. TIB-Dateien, die das Ergebnis eines Backup-Exports (S. 191) oder Konsolidierung (S. 192) sind, werden ebenfalls als Backups bezeichnet.

Backup (Aktion)

Aktion, die eine Kopie der Daten erstellt, die auf der Festplatte einer Maschine (S. 193) existieren, um diese wiederherzustellen oder in den Zustand zu einem festgelegten Tag bzw. Zeitpunkt zurückzusetzen.

Backup-Archiv (Archiv)

Satz von Backups (S. 185), die mit einem Backup-Plan (S. 186) erstellt und verwaltet werden. Ein Archiv kann mehrere Voll-Backups (S. 197) enthalten, aber auch inkrementelle (S. 192) und differentielle Backups (S. 189). Backups, die dem gleichen Archiv zugehören, werden immer am gleichen Ort gespeichert. Es können zwar mehrere Backup-Pläne die gleiche Quelle in das gleiche Archiv sichern, aber das vorherrschende Szenario ist „ein Plan – ein Archiv".

Backups in einem Archiv werden vom Backup-Plan verwaltet. Manuelle Aktionen mit Archiven – Validierung (S. 196), Einsicht in den Inhalt, Mounten und Löschen von Backups – sollten nur mit Acronis Backup & Recovery 10 ausgeführt werden. Modifizieren Sie Ihre Archive nur mit Werkzeugen von Acronis, nicht aber z.B. mit dem Windows Explorer oder dem Dateimanager eines Drittanbieters.

Backup-Optionen

Konfiguration der Parameter für eine Backup-Aktion (S. 185), wie zum Beispiel die Befehle vor bzw. nach dem Backup, die maximale Bandbreite im Netzwerk, die dem Backup zugeteilt wird, oder die Datenkomprimierungsrate. Backup-Optionen sind Bestandteil eines Backup-Plans (S. 186).

Backup-Plan (Plan)

Satz mit Richtlinien für den Schutz der gegebenen Daten auf einer gegebenen Maschine. Ein Backup-Plan spezifiziert:

- welche Daten gesichert werden sollen
- wo die Backup-Archive (S. 185) gespeichert werden (Namen der Backup-Archive und Speicherort)
- das Backup-Schema (S. 187), das den Zeitplan für die Sicherungen und [optional] die Aufbewahrungsregeln enthält
- [optional] die Richtlinien für die Validierung (S. 196) der Archive
- die Backup-Optionen (S. 186).

Zum Beispiel kann ein Sicherstellungsplan die folgenden Informationen enthalten:

- Backup von Volume C: **(Daten, die der Plan schützen wird)**
- Benenne das Archiv mit MySystemVolume und stelle es nach \server\backups **(Name des Backup-Archivs und der Speicherort)**.
- Führe ein Voll-Backup monatlich am letzten Tag des Monats um 10:00 AM und ein inkrementelles Backup an Sonntagen um 10:00 PM aus. Lösche Backups, die älter sind als 3 Monate **(Backup-Schema).**
- Validiere das letzte Backup unmittelbar nach seiner Erstellung **(Richtlinie zur Validierung)**.
- Schütze das Archiv mit einem Kennwort **(Option)**.

Physikalisch ist ein Backup-Plan ein Paket von Tasks (S. 195), die zur Ausführung auf einer verwalteten Maschine (S. 197) gestaltet werden.

Ein Backup-Plan kann direkt auf der Maschine erstellt werden (lokaler Plan) oder erscheint auf der Maschine als Ergebnis der Verteilung einer Backup-Richtlinie (S. 186) – zentraler Plan (S. 198).

Backup-Richtlinie (Richtlinie)

Template für einen Backup-Plan, das vom Administrator des Management Servers (S. 193) erstellt und auf dem Management Server gespeichert wurde. Eine Backup-Richtlinie enthält die gleichen Regeln wie ein Backup-Plan, aber nicht explizit die Information, welche Daten zu sichern sind.

Anstelle dessen können Auswahlregeln (S. 185) benutzt werden, wie z.B. Umgebungsvariablen. Wegen dieser flexiblen Auswahl kann eine Backup-Richtlinie zentral für mehrere Maschinen angewendet werden. Wenn ein Datenelement explizit angegeben ist (z.B. /dev/sda oder C:\Windows), wird die Richtlinie dieses Element auf jeder Maschine sichern, auf der dieser genaue Pfad gefunden wird.

Durch die Anwendung einer Richtlinie auf eine Maschinengruppe verteilt der Administrator mehrere Backup-Pläne mit einer einzigen Aktion.

Der Arbeitsablauf bei der Benutzung von Richtlinien ist wie folgt beschrieben.

1. Der Administrator erstellt eine Backup-Richtlinie.
2. Der Administrator wendet die Richtlinie auf eine Maschinengruppe oder eine einzelne Maschine (S. 193) an.
3. Der Management Server verteilt die Richtlinie auf die Maschinen.
4. Auf jeder Maschine findet der dort installierte Agent (S. 185) die Datenelemente mit Hilfe der Auswahlregeln. Wenn die Auswahlregel z.B. [Alle Volumes] umfasst, wird die ganze Maschine gesichert.
5. Auf jeder Maschine erstellt der Agent, der auf der Maschine installiert ist, einen Backup-Plan (S. 186) unter Benutzung der Regeln, die durch die Richtlinie spezifiziert wurden. Ein solcher Plan heißt zentraler Plan (S. 198).
6. Auf jeder Maschine erstellt der Agent, der auf der Maschine installiert ist, einen Satz zentraler Aufgaben (S. 198), die den Plan ausführen.

Backup-Schema

Teil eines Backup-Plans (S. 186), der den Zeitplan für das Backup und [optional] die Aufbewahrungsregeln und den Zeitplan für die Bereinigung (S. 187) mit einschließt. Beispielsweise führe monatlich ein Voll-Backup (S. 197) am letzten Tag des Monats um 10:00 Uhr aus – und ein inkrementelles Backup (S. 192) an Sonntagen um 22:00 Uhr. Lösche Backups, die älter sind als 3 Monate. Prüfe auf solche Backups jedes Mal, wenn ein Backup abgeschlossen wurde.

Acronis Backup & Recovery 10 bietet die Möglichkeit, bekannte optimierte Backup-Schemata wie zum Beispiel GVS und Türme von Hanoi zu verwenden, benutzerdefinierte Backup-Schemata zu erstellen oder alle Daten auf einmal zu sichern.

Bereinigung

Löschen von Backups (S. 185) aus einem Backup-Archiv (S. 185), um veraltete Backups zu entfernen oder um das Archiv daran zu hindern, die gewünschte Größe zu überschreiten.

Die Bereinigung basiert auf den einem Archiv hinzugefügten Aufbewahrungsregeln, die durch den Backup-Plan (S. 186) bestimmt werden, der das Archiv erstellt hat. Diese Aktion prüft, ob das Archiv seine maximale Größe überschritten hat und ob Backups abgelaufen sind. Als Ergebnis dieser Prüfung werden möglicherweise Backups gelöscht, je nachdem, ob Aufbewahrungsregeln verletzt werden oder nicht.

Weitere Informationen finden Sie bei Aufbewahrungsegeln (S. 32).

Bereinigung aufseiten des Storage Node

Bereinigung (S. 187), ausgeführt durch einen Storage Node (S. 195) gemäß des Backup-Plans (S. 186), auf dessen Grundlage die in einem verwalteten Depot (S. 197) abgelegten Archive (S. 185) erstellt

wurden. Als Alternative zur agentenseitigen Bereinigung (S. 185) befreit die Bereinigung auf dem Storage Node die produktiven Server von unnötiger CPU-Last.

Da der Zeitplan auf der Maschine (S. 193) existiert, auf der sich der Agent (S. 185) befindet, und die Zeit bzw. die Ereignisse der Maschine benutzt werden, muss der Agent jedes Mal die Storage Node-seitige Bereinigung auslösen, wenn die geplante Zeit erreicht wird oder das Ereignis eintritt. Dafür muss der Agent online sein.

Die nachfolgende Tabelle fasst die von Acronis Backup & Recovery 10 für die Bereinigung verwendeten Typen zusammen.

	Bereinigung	
	Agentenseitig	**Auf Seiten des Storage Node**
Angewandt auf:	Archiv	Archiv
Eingeleitet durch:	Agent	Agent
Ausgeführt von:	Agent	Storage Node
Geplant durch:	Backup-Plan	Backup-Plan
Aufbewahrungsregel von:	Backup-Plan	Backup-Plan

Bootable Agent

Bootfähiges Wiederherstellungswerkzeug, das die meisten Funktionen von Acronis Backup & Recovery 10 Agent (S. 185) enthält. Der bootfähige Agent basiert auf einem Linux-Kernel. Eine Maschine (S. 193) kann entweder mit Hilfe bootfähiger Medien (S. 188) oder über den Acronis PXE Server in den bootfähigen Agenten gestartet werden. Aktionen können entweder lokal über die Benutzerschnittstelle oder remote mit Hilfe der Konsole (S. 192) konfiguriert und gesteuert werden.

Bootfähiges Medium

Physikalische Medien (CD, DVD, USB-Sticks oder andere Medien, die vom BIOS einer Maschine (S. 193) als Boot-Gerät unterstützt werden), die den bootfähigen Agenten (S. 188) oder die Windows Preinstallation Environment (WinPE) (S. 198) mit dem Acronis Plug-in für WinPE (S. 184) enthalten. Eine Maschine kann außerdem in die genannten Umgebungen gestartet werden, wenn die Möglichkeit genutzt wird, per Acronis PXE Server oder Microsoft Remote Installation Service (RIS) über das Netzwerk zu booten. Diese Server mit ihren hochgeladenen, bootfähigen Komponenten können auch als eine Art bootfähiges Medium angesehen werden.

Bootfähige Medien werden am häufigsten benutzt, um:

- ein Betriebssystem wiederherzustellen, das nicht mehr bootet
- auf Daten zuzugreifen und diese zu sichern, die in einem beschädigten System „überlebt“ haben
- ein Betriebssystem auf fabrikneue Computer zu verteilen
- Basis-Volumes oder dynamische Volumes (S. 191) auf fabrikneuen Festplatten (bzw. ähnlichen Laufwerken) einzurichten
- Laufwerke mit nicht unterstütztem Dateisystem per Sektor-für-Sektor-Backup zu sichern
- Daten 'offline' zu sichern, die wegen einer Zugangsbeschränkung, einer Sperrung durch laufende Anwendungen oder wegen anderer Gründe nicht 'online' gesichert werden können.

D

Datenträgergruppe

Anzahl dynamischer Laufwerke (S. 190), die ihre Konfigurationendaten in ihren LDM-Datenbanken speichern und deshalb als ein Ganzes verwaltet werden können. Normalerweise sind alle dynamischen Datenträger, die innerhalb der gleichen Maschine (S. 193) erstellt wurden, Mitglieder der gleichen Datenträgergruppe.

Sobald das erste dynamische Datenträger vom LDM oder einem anderen Festplattenverwaltungswerkzeug erstellt wird, kann der Name der Datenträgergruppe im Registry-Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name gefunden werden.

Das nächste erstellte oder importierte Datenträger wird zur gleichen Datenträgergruppe hinzugefügt. Die Gruppe existiert, so lange wenigstens eine ihrer Mitglieder existiert. Nachdem der letzte dynamische Datenträger abgeschaltet oder in einen Basisdatenträger konvertiert wurde, ist die Gruppe stillgelegt, obwohl der Name im oben genannten Registry-Key erhalten bleibt. Falls erneut ein dynamischer Datenträger erstellt oder wieder angeschlossen wird, wird eine Datenträgergruppe mit einem inkrementellen Namen erstellt.

Wenn eine Datenträgergruppe zu einer anderen Maschine verschoben wird, wird sie als „fremd“ betrachtet und kann nicht benutzt werden, bis sie in eine existierende Datenträgergruppe importiert wird. Der Import aktualisiert die Konfigurationsdaten auf den lokalen und den 'fremden' Datenträgern, damit sie eine Einheit bilden. Eine 'fremde' Gruppe wird importiert, wie sie ist (wird den ursprünglichen Namen haben), wenn keine Datenträgergruppe auf der Maschine existiert.

Weitere Informationen über Datenträgergruppen finden Sie auf den Microsoft-Webseiten:

222189 Beschreibung der Datenträgergruppen in der Windows Datenträgerverwaltung http://support.microsoft.com/kb/222189/de.

Deduplizierendes Depot

Verwaltetes Depot (S. 197) mit aktivierter Deduplizierung (S. 189).

Deduplizierung

Methode, um identische Informationen in verschiedenen Kopien nur einmalig zu speichern.

Acronis Backup & Recovery 10 kann die Deduplizierungstechnologie auf Backup-Archive (S. 185) anwenden, die auf Storage Nodes (S. 195) gespeichert sind. Das reduziert den für Archive benötigten Speicherplatz, den Backup-Datentransfer sowie die Netzwerkauslastung während der Backup-Erstellung.

Depot

Ort für die Ablage von Backup-Archiven (S. 185). Ein Depot kann auf einem lokalen Laufwerk, auf einem Netzlaufwerk oder auf einem entfernbaren Medium wie einem USB-Laufwerk organisiert werden. Es gibt keine Limits für die Größe eines Depots oder die Zahl der Backups in einem Depot. Sie können die Größe jedes Archivs durch Bereinigung (S. 187) begrenzen, aber die Gesamtgröße der Archive in einem Depot wird nur durch die Größe des Speichers selbst begrenzt.

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum letzten vorangegangenen Voll-Backup (S. 197). Sie benötigen den Zugriff auf das entsprechende Voll-Backup, um die Daten aus einem differentiellen Backup wiederherzustellen.

Direkte Verwaltung

Jede Verwaltungsaktion, die auf einer verwalteten Maschine (S. 197) unter Benutzung der direkten Verbindung zwischen Konsole (S. 192)und Agent (S. 185) ausgeführt wird (im Gegensatz zu zentraler Verwaltung (S. 198), wenn die Aktionen auf dem Management Server (S. 193) vorbereitet und dann durch den Server an die verwalteten Maschinen verteilt werden).

Die zentralen Verwaltungsaktionen umfassen:

- Erstellen und Verwalten lokaler Backup-Pläne (S. 193)
- Erstellen und Verwalten lokaler Tasks (S. 193), wie z.b. Recovery-Tasks
- Erstellen und Verwalten persönlicher Depots (S. 193) und der dort gespeicherten Archive
- Statusverfolgung, Fortschrittskontrolle und Konfiguration der Eigenschaften zentraler Tasks (S. 198), die auf der Maschine existieren
- Ansehen und Verwalten von Logs der Aktionen des Agenten
- Festplattenverwaltungsaktionen wie das Klonen einer Festplatte sowie das Erstellen und Konvertieren von Volumes.

Eine Art direkter Verwaltung erfolgt beim Benutzen bootfähiger Medien (S. 188). Einige der direkten Verwaltungsaktionen kann auch über die Benutzerschnittstelle des Managementservers durchgeführt werden. Dafür muss aber entweder ein explizite oder eine implizite direkte Verbindung zur ausgewählten Maschine bestehen.

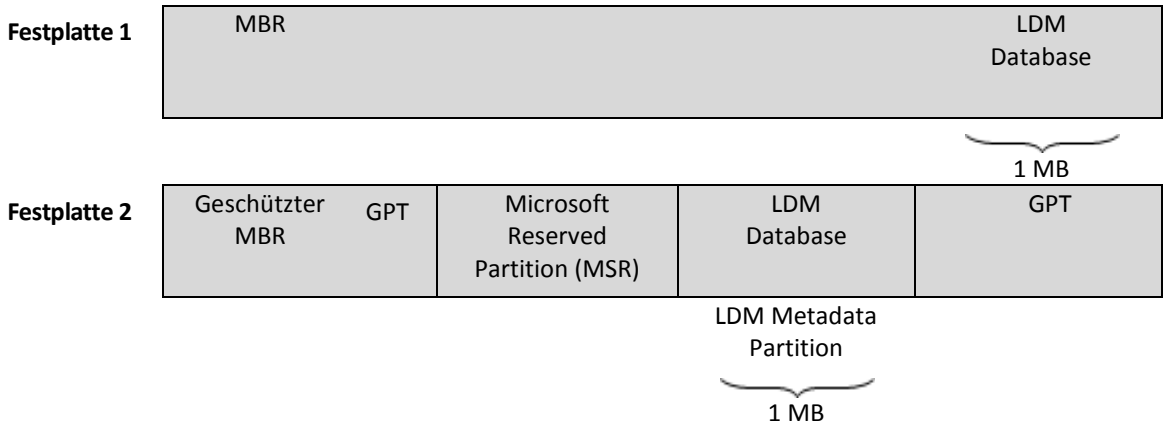
Disk-Backup (Image)

Backup (S. 185), das eine auf den Sektoren basierende Kopie einer Festplatte oder Partition in gepackter Form enthält. Normalerweise werden nur Sektoren kopiert, die Daten enthalten. Acronis Backup & Recovery 10 bietet aber eine Option, um Raw-Images zu erstellen, d.h. alle Sektoren zu kopieren, um z.B. das Imaging nicht unterstützter Dateisysteme zu ermöglichen.

Dynamische Festplatten

Laufwerk, das vom Logical Disk Manager (LDM) verwaltet wird, der in Windows seit Windows 2000 verfügbar ist. LDM unterstützt die flexible Zuweisung von Volumes auf einem Speichergerät für bessere Fehlertoleranz, bessere Leistung oder eine höhere Volume-Größe.

Ein dynamisches Laufwerk kann entweder das Partitionierungsschema 'Master Boot Record' (MBR) oder 'GUID-Partitionstabelle' (GPT) verwenden. Zusätzlich zu MBR oder GPT hat jedes dynamische Laufwerk eine versteckte Datenbank, wo der LDM die Konfiguration der dynamischen Volumes speichert. Jedes dynamische Laufwerk hält für eine bessere Speicherzuverlässigkeit die vollständigen Informationen über alle dynamischen Laufwerke bereit, die in der Datenträgergruppe existieren. Die Datenbank besetzt das letzte Megabyte einer MBR-Festplatte. Auf einer GPT-Festplatte erstellt Windows eine dedizierte LDM-Metadaten-Partition, die Platz von der Microsoft Reserved Partition (MSR) entnimmt.



Organisation dynamischer Festplatten auf Basis MBR (Festplatte 1) und GPT (Festplatte 2).

Weitere Informationen über dynamische Datenträger finden Sie im Artikel der Microsoft Knowledgebase:

Disk Management (Windows XP Professional Resource Kit) http://technet.microsoft.com/en-us/library/bb457110.aspx.

816307 Empfohlene Verfahrensweisen für die Verwendung dynamischer Datenträger auf Windows Server 2003-Computern http://support.microsoft.com/kb/816307/de.

Dynamische Gruppe

Gruppe von Maschinen (S. 193), die automatisch vom Management Server (S. 193) gemäß der Kriterien für die Mitgliedschaft aufgefüllt wird, die vom Administrator angegeben werden. Acronis Backup & Recovery 10 bietet folgende Mitgliedskriterien:

- Betriebssystem
- Organisationseinheit des Active Directory
- IP-Adressbereich.

Eine Maschine verbleibt in einer dynamischen Gruppe, solange die Maschine die Kriterien der Gruppe erfüllt. Die Maschine wird automatisch aus der Gruppe entfernt, sobald

- sich die Eigenschaften der Maschine so ändern, dass die Maschine die Kriterien nicht mehr erfüllt ODER
- der Verwalter die Kriterien so ändert, dass die Maschine sie nicht mehr erfüllt.

Es gibt keinen anderen Weg, eine physikalische Maschine aus einer dynamischen Gruppe zu entfernen, als diese aus dem Management Server herauszunehmen.

Dynamisches Volume

Volume, das sich auf auf einem dynamischen Datenträger (S. 190) oder genauer auf einer Datenträgergruppe (S. 188) befindet. Dynamische Volumes können sich über mehrere Laufwerke erstrecken. Dynamische Datenträger sind gewöhnlich abhängig vom gewünschten Ziel gestaltet:

- um die Größe zu erweitern (übergreifendes Volume)
- um die Zugriffszeit zu verringern (Stripesetvolume)
- um die Fehlertoleranz durch redundante Informationen zu erreichen (gespiegelte und RAID-5-Volumes).

E

Exportieren

Eine Aktion, bei der eine Kopie bzw. unabhängige Teilkopie eines Archivs (S. 185) am von Ihnen angegebenen Speicherort erstellt wird. Ein Export kann ein einziges Archiv, ein einziges Backup (S. 185) oder eine Auswahl von Backups aus dem gleichen Archiv umfassen. Ein vollständiges Depot (S. 189) kann über die Befehlszeilenschnittstelle exportiert werden.

G

GVS (Großvater-Vater-Sohn)

Populäres Backup-Schema (S. 187), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 185) und der Anzahl von Wiederherstellungspunkten (S. 198) sorgen soll, die im Archiv enthalten sind. GVS ermöglicht ein Recovery mit täglicher Rasterung für die letzten Tage, wöchentlicher Rasterung für die letzten Wochen und monatlicher Rasterung für jede Zeit in der Vergangenheit.

Weitere Informationen finden Sie bei Backup-Schema GVS (S. 25).

I

Image

Gleichbedeutend mit Disk-Backup (S. 190).

Inkrementelles Backup

Backup (S. 185), das die Änderungen an den Daten im Vergleich zum letzten vorangegangenen Backup speichert. Sie benötigen den Zugriff auf die anderen Backups des gleichen Archivs (S. 185), um Daten aus einem inkrementellen Backup wiederherzustellen.

K

Konsole (Acronis Backup & Recovery 10 Management Console)

Werkzeug für den Remote- oder lokalen Zugriff auf Acronis Agents (S. 185) und Acronis Backup & Recovery 10 Management Server (S. 193).

Wenn die Konsole zum Management Server verbunden ist, kann der Administrator Backup-Richtlinien (S. 186) einrichten und verwalten sowie auf andere Funktionen des Management-Servers zugreifen, d.h. er arbeitet mit zentraler Verwaltung (S. 198). Wenn der Administrator eine direkte Verbindung zwischen Konsole und Agent herstellt, arbeitet er mit direkter Verwaltung (S. 190).

Konsolidierung

Kombinieren zweier oder weiterer subsequenter Backups (S. 185), die zum gleichen Archiv (S. 185) gehören, in ein Backup.

Konsolidierung könnte beim Löschen von Backups gebraucht werden, entweder manuell oder während der Bereinigung (S. 187). Zum Beispiel könnten die Aufbewahrungsregeln erfordern, ein abgelaufenes Voll-Backup (S. 197) zu löschen, aber die nächste inkrementelle Sicherung (S. 192) zu

erhalten. Die Backups werden in ein einzelnes Voll-Backup kombiniert und mit dem Datum des inkrementellen Backups versehen. Da die Konsolidierung viel Zeit und Systemressourcen beansprucht, bieten die Aufbewahrungsregeln eine Option, Backups mit Abhängigkeiten nicht zu löschen. Im Beispiel wird das Voll-Backup erhalten, bis auch das inkrementelle Backup veraltet ist. Dann werden beide Backups gelöscht.

L

Lokaler Backup-Plan

Backup-Plan (S. 186), erstellt auf einer verwalteten Maschine (S. 197) durch direkte Verwaltung (S. 190).

Lokaler Task

Task (S. 195), der zu einem lokalen Backup-Plan (S. 193) gehört, oder ein Task, der zu gar keinem Plan gehört, wie z.B. ein Recovery-Task. Ein lokaler Task, der zu einem Backup-Plan gehört, kann nur durch Bearbeiten des Plans verändert werden, andere lokale Tasks können direkt verändert werden.

M

Management Server (Acronis Backup & Recovery 10 Management Server)

Zentraler Server für die Datensicherung innerhalb des Unternehmensnetzes. Acronis Backup & Recovery 10 Management Server versorgt den Administrator mit:

- einen zentralen Zugriffspunkt auf die Acronis Backup & Recovery 10-Infrastruktur
- einem einfachen Weg zum Schutz der Daten auf zahlreichen Maschinen (S. 193) unter Benutzung von Backup-Richtlinien (S. 186) und Gruppierung
- unternehmensweiter Monitoring-Funktionalität
- der Fähigkeit, zentrale Depots (S. 199) für die Ablage der Backup-Archive (S. 185) des Unternehmens zu erstellen
- der Fähigkeit, Storage Node (S. 195) zu verwalten.

Wenn es mehrere Management Server im Netzwerk gibt, dann arbeiten diese unabhängig voneinander, verwalten verschiedene Maschinen und benutzen verschiedene zentrale Depots für die Ablage der Archive.

Maschine

Ein physikalischer oder virtueller Computer, der eindeutig anhand seiner Betriebssysteminstallation identifiziert wird. Maschinen mit mehreren Betriebssystemen (Multi-Boot-Systeme) werden auch als mehrfache Maschinen betrachtet.

Media Builder

Spezielles Werkzeug zum Erstellen bootfähiger Medien (S. 188).

N

Nicht verwaltetes Depot

Jedes Depot (S. 189), das kein verwaltetes Depot (S. 197) ist.

P

Persönliches Depot

Lokales oder im Netzwerk befindliches Depot (S. 189), das durch direkte Verwaltung (S. 190) erstellt wurde. Nachdem ein persönliches Depot erstellt wurde, erscheint ein Shortcut bei **Persönliche Depots** im Fensterbereich **Navigation**. Mehrere Maschinen können den gleichen physikalischen Speicherort benutzen, z.B. ein freigegebenes Netzlaufwerk oder ein persönliches Depot.

Physikalische Maschine

Auf dem Acronis Backup & Recovery 10 Management Server entspricht eine physikalische Maschine einer registrierten Maschine (S. 194). Eine virtuelle Maschine wird als physikalisch betrachtet, wenn ein Acronis Backup & Recovery 10 Agent auf der Maschine installiert und die Maschine auf dem Management Server registriert ist.

Plan

Siehe Backup-Plan (S. 186).

R

Registrierte Maschine

Maschine (S. 193), die durch einen Management Server (S. 193) verwaltet wird. Eine Maschine kann zur gleichen Zeit nur auf einem Management Server registriert sein. Eine registrierte Maschine entsteht durch ein Verfahren zur Registrierung (S. 194).

Registrierung

Verfahren, das eine verwaltete Maschine (S. 197) zu einem Management Server (S. 193) hinzufügt.

Die Registrierung stellt eine Vertrauensstellung zwischen dem Agenten (S. 185) auf der Maschine und dem Server her. Während der Registrierung ruft die Konsole das Client-Zertifikat des Management Servers ab und leitet es an den Agent weiter, der es später beim Herstellen der Verbindung zur Authentifizierung benutzt. Dies hilft, Versuche von Angreifern des Netzwerks zu verhindern, eine Verbindung unter Vortäuschung eines vertrauten Auftraggebers (des Management Servers) herzustellen.

Richtlinien

Siehe Backup-Richtlinien (S. 186).

S

Standardgruppe

Gruppe von Maschinen, die immer auf einem Management Server (S. 193) existiert, also eingebaut ist.

Ein Management Server hat zwei eingebaute Gruppen, die alle Maschinen von jedem Typ enthalten: alle physikalischen Maschinen (S. 194), alle virtuellen Maschinen (S. 197).

Eingebaute Gruppen können nicht gelöscht, zu anderen Gruppen verschoben oder manuell modifiziert werden. Innerhalb eingebauter Gruppen können keine benutzerdefinierten Gruppen erstellt werden. Es gibt keinen anderen Weg, eine physikalische Maschine aus der Standardgruppe zu entfernen, als diese aus dem Management Server herauszunehmen. Virtuelle Maschinen werden gelöscht, wenn deren Host-Server entfernt wird.

Auf eine Standardgruppe kann eine Backup-Richtlinie (S. 186) angewendet werden.

Statische Gruppe

Maschinengruppe, die der Administrator eines Management Servers (S. 193) durch manuelles Hinzufügen von Maschinen zur betreffenden Gruppe auffüllt. Eine Maschine verbleibt in einer statischen Gruppe, bis der Administrator diese von der Gruppe oder vom Management Server entfernt.

Storage Node (Acronis Backup & Recovery 10 Storage Node)

Server, der für die Benutzung verschiedener Ressourcen optimiert ist, die für den Schutz von Unternehmendaten erforderlich sind. Dieses Ziel wird durch die Organisation von verwalteten Speichergruppen (S. 197) erreicht. Storage Nodes ermöglichen dem Verwalter:

- verwaltete Maschinen (S. 197) durch Benutzung der Storage Node-seitigen Bereinigung (S. 187) und der Storage Node-seitigen Validierung (S. 195) von unnötiger CPU-Last zu befreien,
- den für die Archive (S. 185) verwendeten Backup-Traffic und den Speicherplatz durch Deduplizierung (S. 189) drastisch zu senken,
- mit Hilfe verschlüsselter Depots (S. 197) den Zugriff auf Backup-Archive zu verhindern, auch wenn das Speichermedium gestohlen wurde oder durch einen Unbefugten auf die Archive zugegriffen wird.

Storage Node-seitige Validierung

Validierung (S. 196), ausgeführt durch einen Storage Node (S. 195) gemäß des Backup-Plans (S. 186), auf dessen Grundlage die auf einem verwalteten Backup-Speicher (S. 197) gespeicherten Archive (S. 185) erstellt wurden. Als Alternative zur agentenseitigen Validierung (S. 185) befreit die Validierung auf dem Storage Node die produktiven Server von unnötiger CPU-Last.

T

Task

In Acronis Backup & Recovery 10 ist ein Task ein Satz sequenzieller Handlungen, der auf einer verwalteten Maschine (S. 197) zu einer festgelegten Zeit oder beim Eintreten eines bestimmten Ereignisses ausgeführt wird. Die Handlungen sind in einer XML-Skript-Datei beschrieben. Die Startbedingungen (Planung) stehen in geschützten Registry-Schlüsseln.

Türme von Hanoi

Populäres Backup-Schema (S. 187), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 185) und der Anzahl von Wiederherstellungspunkten (S. 198) sorgen soll, die im Archiv enthalten sind. Im Gegensatz zum GVS (S. 192)-Schema, das lediglich drei Level für die Wiederherstellungsauflösung hat (täglich, wöchentlich und monatlich), ist es mit dem Schema „Türme von Hanoi“ möglich, den zeitlichen Abstand zwischen Wiederherstellungspunkten bei

steigendem Alter des Backups kontinuierlich zu reduzieren. Das ermöglicht eine sehr effiziente Verwendung des Backup-Speichers.

Weitere Informationen finden Sie unter Backup-Schema „Türme von Hanoi“ (S. 29).

U

Universal Restore (Acronis Backup & Recovery 10 Universal Restore)

Geschützte Acronis-Technologie, um Windows auf abweichender Hardware oder einer virtuellen Maschine bootfähig zu machen. Universal Restore behandelt abweichende Geräte, die kritisch für den Betriebssystemstart sind, wie z.B. Speicher-Controller, Hauptplatine oder Chipsatz.

Universal Restore ist nicht verfügbar:

- wenn die Maschine über den Acronis Startup Recovery Manager (S. 184) (unter Benutzung von F11) gebootet wurde,
- das wiederherzustellende Image in der Acronis Secure Zone (S. 184) abgelegt ist oder
- wenn Acronis Active Restore (S. 184) benutzt wird,

weil alle diese Funktionen hauptsächlich für sofortige Datenwiederherstellung auf der gleichen Maschine gedacht sind.

Universal Restore ist nicht verfügbar bei der Wiederherstellung eines Linux-Systems.

V

Validierung

Aktion, mit der die Möglichkeit einer Datenwiederherstellung aus einem Backup (S. 185) geprüft wird.

Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Vorhergehende Produktversionen gingen davon aus, dass ein Datei-Backup gültig ist, wenn die Metadaten aus dem File-Header konsistent sind. Die jetzige Methode ist zeitaufwendiger, aber viel zuverlässiger. Die Validierung eines Image-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Dieses Verfahren nutzt die Ressourcen intensiv.

Obwohl die erfolgreiche Validierung eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, werden nicht alle Faktoren geprüft, die eine Wiederherstellung beeinflussen. Wenn Sie das Betriebssystem gesichert haben, kann nur ein Test der Wiederherstellung unter Verwendung eines bootfähigen Mediums auf eine Ersatzfestplatte eine erfolgreiche Wiederherstellung in der Zukunft garantieren.

Validierungsrichtlinien

Teil eines Backup-Plans (S. 186). Richtlinien definieren, wann und wie eine Validierung (S. 196) durchzuführen ist und ob das gesamte Archiv (S. 185) zu validieren ist oder nur das letzte Archiv im Backup.

Verschlüsseltes Archiv

Backup-Archiv (S. 185), das nach dem Advanced Encryption Standard (AES) verschlüsselt ist. Wenn die Verschlüsselungsoption und ein Kennwort für das Archiv in den Backup-Optionen (S. 186)

definiert werden, wird jedes Backup, das zum Archiv gehört, vom Agent (S. 185) vor dem Speichern am Speicherort verschlüsselt.

Der kryptografische Algorithmus AES arbeitet im Cipher Block Chaining Mode (CBC) und benutzt einen zufällig erstellten Schlüssel mit der benutzerdefinierten Größe von 128, 192 oder 256 Bit. Der Kodierungsschlüssel ist dann mit AES-256 unter Benutzung eines SHA-256-Hash-Werts des angegebenen Kennworts verschlüsselt. Das Kennwort selbst wird nirgendwo auf der Festplatte oder in der Backup-Datei gespeichert, es wird nur der Kennwort-Hash-Wert für Bestätigungszwecke benutzt. Mit dieser zweistufigen Methode sind die gesicherten Daten vor jedem unberechtigten Zugriff geschützt, aber ein verlorenes Kennwort kann unmöglich wiederhergestellt werden.

Verschlüsseltes Depot

Verwaltetes Depot (S. 197), bei dem ein Storage Node (S. 195) alles dorthin Geschriebene verschlüsselt bzw. alles von dort Gelesene transparent entschlüsselt, wobei ein für das Depot spezifischer Encryption Key benutzt wird, der auf dem Knoten gespeichert ist. Falls das Speichermedium gestohlen wird oder eine unbefugte Person darauf zugreift, wird der Übeltäter den Inhalt des Depots ohne Zugriff auf den Storage Node nicht entschlüsseln können. Verschlüsselte Archive (S. 196) werden über die Verschlüsselung des Agenten (S. 185) erstellt.

Verwaltete Maschine

Physikalische oder virtuelle Maschine (S. 193), auf der wenigstens ein Acronis Backup & Recovery 10 (S. 185) Agent installiert ist.

Verwaltetes Depot

Zentrales Depot (S. 199), das durch einen Storage Node (S. 195) verwaltet wird. Auf Archive (S. 185) in einem verwalteten Depot kann folgendermaßen zugegriffen werden:

bsp://node_address/vault_name/archive_name/

Physikalisch können sich verwaltete Depots auf einem freigegebenen Netzlaufwerk, einem SAN, NAS oder auf einer lokalen Festplatte des Storage Nodes oder einer Bandbibliothek befinden, die lokal an den Storage Node angeschlossen ist. Der Storage Node stellt die Storage Node-seitige Bereinigung (S. 187) und die Storage Node-seitige Validierung (S. 195) für jedes Archiv bereit, das im verwalteten Depot gespeichert ist. Ein Administrator kann zusätzliche Aktionen spezifizieren, die der Storage Node durchführen soll, z.B. Deduplizierung (S. 189) oder Verschlüsselung.

Ein verwaltetes Depot ist in sich abgeschlossen, d.h., es enthält alle Metadaten, die ein Storage Node für die Verwaltung des Depots benötigt. Falls der Storage Node ausfällt oder seine Datenbank beschädigt wurde, ermittelt der neue Storage Node die Metadaten und erstellt die Datenbank neu. Wenn das Depot mit einem anderen Storage Node verbunden wird, findet das gleiche Verfahren statt.

Virtuelle Maschine

Auf dem Acronis Backup & Recovery 10 Management Server wird eine Maschine (S. 193) als virtuell angesehen, wenn das Backup vom Virtualisierungs-Host erstellt werden kann, ohne dass ein Agent (S. 185) auf der Maschine installiert werden muss. Eine virtuelle Maschine erscheint im Management Server nach der Registrierung des Virtualisierungs-Servers, der die Maschine hostet, wenn Acronis Backup & Recovery 10 Agent für virtuelle Maschinen auf diesem Server installiert ist.

Voll-Backup

Selbstständiges Backup (S. 185), das alle Daten enthält, die für die Sicherung gewählt wurden. Sie benötigen kein weiteres Backup, um die Daten aus einem Voll-Backup wiederherzustellen.

W

Wiederherstellungspunkt

Tag und Zeitpunkt, zu dem die gesicherten Daten wiederhergestellt werden können.

WinPE (Windows Preinstallation Environment)

Minimales Windows-System, das auf einem der folgenden Kernel basiert:

- Windows XP Professional mit Service Pack 2 (PE 1.5)
- Windows Server 2003 mit Service Pack 1 (PE 1.6)
- Windows Vista (PE 2.0)
- Windows Vista SP1 und Windows Server 2008 (PE 2.1).

WinPE wird üblicherweise von OEMs und Unternehmen für Deployment, Test, Diagnose und Systemreparaturen benutzt. Eine Maschine kann in die WinPE über PXE, CD-ROM, USB-Flash-Laufwerke oder Festplatten gebootet werden. Das Acronis Plugin für WinPE (S. 184) ermöglicht die Ausführung von Acronis Backup & Recovery 10 Agent (S. 185) in der Preinstallation Environment.

Z

Zentrale Verwaltung

Verwaltung der Acronis Backup & Recovery 10 Infrastruktur durch eine zentrale Verwaltungseinheit, die Acronis Backup & Recovery 10 Management Server (S. 193) genannt wird. Die zentralen Verwaltungsaktionen umfassen:

- Erstellen, Verwenden und Verwalten von Backup-Richtlinien (S. 186)
- Erstellen und Verwalten statischer (S. 195) und dynamischer Gruppen (S. 191) von Maschinen (S. 193)
- Verwalten von existierenden Tasks (S. 195) auf den Maschinen
- Erstellen und Verwalten von zentralen Depots (S. 199) für die Speicherung von Archiven
- Verwalten von Storage Node (S. 195)
- Überwachen der Tätigkeiten der Komponenten von Acronis Backup & Recovery 10, Einsicht in die zentralen Logs u.a.

Zentraler Backup-Plan

Backup-Plan (S. 186), der auf der verwalteten Maschine (S. 197) als Ergebnis der Verteilung einer Backup-Richtlinie (S. 186) durch den Management Server (S. 193) erscheint. Ein solcher Plan kann nur durch Bearbeitung der Backup-Richtlinie modifiziert werden.

Zentraler Task

Task (S. 195), der zu einem zentralen Backup-Plan (S. 198) gehört. Solch ein Task erscheint auf der verwalteten Maschine (S. 197) infolge der Verteilung einer Backup-Richtlinie (S. 186) durch den

Management Server (S. 193) und kann nur durch Bearbeiten des Sicherstellungsgrundsatzes modifiziert werden.

Zentrales Depot

Ein Speicherort im Netzwerk, der vom Administrator des Management Servers (S. 193) zugeteilt wird, um als Speicherplatz für die Backup-Archive (S. 185) zu dienen. Ein zentrales Depot kann von einem Storage Node (S. 195) verwaltet werden oder es ist nicht verwaltet. Die Gesamtzahl und Größe der Archive, die in einem zentralen Depot gespeichert werden können, werden nur von der Speichergröße begrenzt.

Sobald der Administrator ein zentrales Depot erstellt, werden dessen Name und der Pfad zum Depot an alle auf dem Server registrierten Maschinen (S. 194) verteilt. Der Shortcut zum Depot erscheint auf den Maschinen in der Liste der zentralen Depots. Jeder Backup-Plan (S. 186), der auf den Maschinen existiert, einschließlich der lokalen Pläne, kann das zentrale Depot benutzen.

Auf einer Maschine, die nicht auf dem Management Server registriert ist, kann ein Benutzer mit den entsprechenden Rechten Backups zum zentralen Depot ausführen, wenn er den vollen Pfad zum Depot verwendet. Wenn das Depot verwaltet wird, werden die Archive des Benutzers vom Storage Node ebenso wie andere Archive behandelt, die im Depot gespeichert worden sind.