Acronis
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.DE

Acronis® Backup & Recovery ™ 10 Advanced Workstation

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 Advanced Workstation erbt 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
- Skalierbarkeit – von einzelnen Maschinen bis zu tausenden Firmen-Computern
- Zentrale Verwaltung für verteilte Workstations
- Dedizierte Server zur Optimierung der Speicher-Ressourcen

Acronis Backup & Recovery 10 Advanced Workstation 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**

  Daten-Deduplizierung, um Speicherbedarf und Auslastung von Netzwerkbandbreiten zu reduzieren

  Flexible Deduplizierungsmechanismen zur Deduplizierung von Daten an der Quelle und am Speicherort

  Verbesserte Unterstützung von Roboter-Bandbibliotheken

  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.

- **Richtlinien-basierte, zentrale Verwaltung**

  Backup-Richtlinien für ganze Gruppen von Maschinen

  Statisches und dynamisches Gruppieren von Maschinen

- **Einfaches Arbeiten mit virtuellen Umgebungen**

  Konvertierung von Backups zu komplett konfigurierten virtuellen Maschinen von Typ VMware, Microsoft, Parallels, Citrix oder Red Hat KVM

- **Neu gestaltete Benutzeroberfläche (GUI)**

  Dashboard (Anzeigetafel) für schnelle operative Entscheidungen

  Überblick aller konfigurierten und laufenden Aktionen mit Farbkodierung für erfolgreiche und fehlgeschlagene Aktionen
- **Sicherheit auf Unternehmensebene**

  Kontrolle der Benutzerrechte über ausführbare Aktionen und Zugriff auf Backups

  Dienste mit minimalen Benutzerrechten ausführen

  Eingeschränkter Fernzugriff auf einen Backup-Agenten

  Sichere Kommunikation zwischen den Komponenten des Produkts

  Verwendung unabhängiger Zertifikate zur Authentifizierung der Komponenten

  Optionen zur Datenverschlüsselung bei Übertragung und Speicherung

  Backup ferngesteuerter Maschinen hinter einer Firewall zu einem zentralen Storage Node

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.

   Windows

   Starten Sie die Konsole, indem Sie sie aus dem Startmenü auswählen.
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. 28)“.

Informationen zu den Elementen der grafischen Benutzeroberfläche finden Sie unter „Management Konsole verwenden (S. 11)“.

Zentrale Verwaltung

Es wird empfohlen, zunächst zu versuchen, einzelne Maschinen direkt zu verwalten, wie oben beschrieben.

So beginnen Sie mit der zentralen Verwaltung:

1. Installieren Sie den Acronis Backup & Recovery 10 Management Server (S. 20).
2. Installieren Sie die Acronis Backup & Recovery 10-Agenten auf den Maschinen, auf denen Daten geschützt werden müssen. Registrieren Sie jede Maschine auf dem Management Server, wenn Sie die Agenten installieren. Tragen Sie dazu die IP-Adresse oder den Namen des Servers und die Anmeldedaten des zentralen Administrators ins Installationsprogramm ein.
3. Installieren Sie Acronis Backup & Recovery 10 Management Console (S. 22) auf der Maschine, von der aus Sie arbeiten möchten. Sollten Sie sich zwischen der Konsolen-Distribution für Windows und Linux entscheiden können, wird empfohlen, die Konsole zu verwenden, die unter Windows installiert wird. Installieren Sie den Acronis Bootable Media Builder.
4. Starten Sie die Konsole. Erstellen Sie das bootfähige Medium.
5. Verbinden Sie die Konsole mit dem Management Server.

Vereinfachte Arbeitsweise mit zentraler Verwaltung

- **Backup**

Wählen Sie über das Steuerelement **Backup** die Maschine aus, für die Sie ein Backup ausführen möchten und erstellen Sie dann einen Backup-Plan (S. 420) auf der Maschine. Sie können Backup-Pläne auf mehreren Maschinen nacheinander erstellen.

- **Recovery**

Wählen Sie über das Steuerelement **Wiederherstellen** die Maschine aus, auf der Daten wiederhergestellt werden müssen und erstellen Sie einen Recovery-Task auf der Maschine. Sie können Recovery-Tasks auf mehreren Maschinen nacheinander erstellen.

Wenn Sie die gesamte Maschine oder ein Betriebssystem, das nicht gestartet werden kann, wiederherstellen möchten, verwenden Sie ein bootfähiges Medium (S. 422). Sie können die Aktionen für das bootfähige Medium mit dem Management Server nicht steuern. Sie können aber die Konsole vom Server trennen und an die Maschine anschließen, die vom Medium aus gebootet wird.

- **Pläne und Tasks verwalten**

Wenn Sie die auf den registrierten Maschinen vorhandenen Pläne und Tasks verwalten möchten, wählen Sie zuerst **Maschinen –> Alle Maschinen** im Verzeichnisbaum **Navigation** aus und dann die einzelnen Maschinen. Im darunter befindlichen Bereich **Informationen** werden der Zustand und die Details zu Plänen und Tasks angezeigt, die auf den einzelnen Maschinen vorhanden sind. Außerdem können Sie in diesem Bereich Pläne und Tasks starten, stoppen, bearbeiten und löschen.

Sie können auch die Ansicht **Tasks** verwenden, um alle auf den registrierten Maschinen vorhandenen Tasks anzuzeigen. Die Tasks können nach Maschinen, Backup-Plänen und anderen Parametern gefiltert werden. Weitere Informationen finden Sie in der kontextsensitiven Hilfe.

- **Anzeigen des Logs**

Um das zentrale Log anzuzeigen, das von den registrierten Maschinen zusammengestellt wurde, wählen Sie **Log** im Verzeichnisbaum **Navigation**. Die Log-Einträge können nach Maschinen, Backup-Plänen und anderen Parametern gefiltert werden. Weitere Informationen finden Sie in der kontextsensitiven Hilfe.

- **Zentrale Depots erstellen**

Wenn Sie sich dafür entscheiden, alle Backup-Archive an einem oder wenigen Netzwerkorten zu speichern, dann erstellen Sie zentrale Depots an diesen Speicherorten. Nachdem Sie ein Depot erstellt haben, können Sie seinen Inhalt anzeigen und verwalten. Wählen Sie dazu **Depot –> Zentral –> 'Name des Depots'** im Verzeichnisbaum **Navigation** aus. Der Shortcut zum Depot wird an alle registrierten Maschinen verteilt. Das Depot kann in jedem von Ihnen oder anderen Benutzern der registrierten Maschinen erstellten Backup-Plan als Zielspeicherort für das Backup angegeben werden.

Fortgeschrittene Arbeitsweise mit zentraler Verwaltung

Um die Fähigkeiten der zentralen Verwaltung in Acronis Backup & Recovery 10 bestmöglich zu nutzen, gehen Sie wie folgt vor:

- **Deduplizierung verwenden**
  1. Installieren Sie den Acronis Backup & Recovery 10 Storage Node (S. 21) und fügen Sie diesen dem Management Server hinzu.
  2. Erstellen Sie das deduplizierende verwaltete Depot auf dem Storage Node.
  3. Installieren Sie das Acronis-Add-on zur Deduplizierung für den Agenten auf allen Maschinen, für die ein Backup auf dem deduplizierenden Depot erstellt wird.

4. Stellen Sie sicher, dass die von Ihnen erstellten Backup-Pläne das verwaltete Depot als Zielspeicherort für die Backup-Archive verwenden.

- **Erstellen Sie eine Backup-Richtlinie anstelle von Backup-Plänen**

Richten Sie eine Backup-Richtlinie ein und wenden Sie diese auf die Gruppe **Alle Maschinen** an. Auf diese Weise können Backup-Pläne mit einer einzigen Aktion auf alle Maschinen verteilt werden. Wählen Sie **Aktionen –> Backup-Richtlinie erstellen** aus dem oberen Menü aus und schauen Sie dann in der kontextsensitiven Hilfe nach.

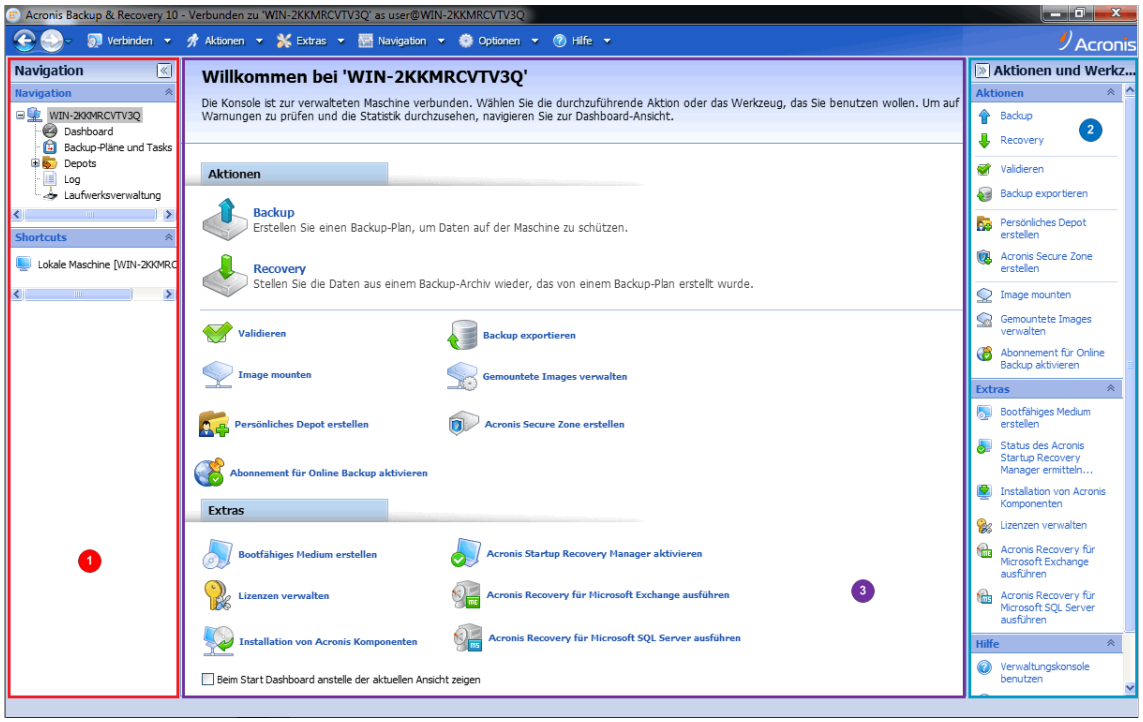
- **Gruppieren Sie die Maschinen, die auf dem Management Server registriert sind**

Gruppieren Sie die registrierten Maschinen anhand geeigneter Parameter, erstellen Sie verschiedene Richtlinien und wenden Sie die einzelnen Richtlinien auf die entsprechende Gruppe von Maschinen an. Weitere Informationen finden Sie unter „Gruppieren der registrierten Maschinen (S. 62)“.

Ein aussagekräftiges Beispiel für die zentrale Verwaltung wird im Abschnitt „Einrichten einer zentralen Datensicherung in einem heterogenen Netzwerk (S. 58)“ gegeben.

1.2.1 Verwaltungskonsole benutzen

Sobald die Konsole mit einer verwalteten Maschine (S. 431) oder einem Management Server (S. 427) 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. 12)).

2	Seitenleiste **Aktionen und Werkzeuge**	Enthält Zusammenstellungen von ausführbaren Aktionen und Werkzeugen (siehe Abschnitt Seitenleiste „Aktionen und Werkzeuge“ (S. 13)).
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. 15) 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.
  - **Datenträgerverwaltung**. Verwenden Sie diese Ansicht, um Aktionen für die Festplatten einer Maschine auszuführen.

Ansichten für einen Management Server

Wenn die Konsole mit einem Management Server verbunden ist, sind die folgenden Ansichten im Navigationsbaum verfügbar.

- **[Name des Management Servers]**. Die oberste Ebene des Baums (root) wird auch **Willkommens-Ansicht** genannt. Hier wird der Name des Management Servers angezeigt, mit dem die Konsole momentan verbunden ist. Verwenden Sie diese Ansicht, um schnell auf wichtige Aktionen zuzugreifen, die auf dem Management Server verfügbar sind.
  - **Dashboard**. Verwenden Sie diese Ansicht, um auf einen Blick einschätzen zu können, ob die Daten auf den beim Management Server registrierten Maschinen erfolgreich gesichert sind.
  - **Backup-Richtlinien**. Verwenden Sie diese Ansicht, um auf dem Management Server bestehende Backup-Richtlinien zu verwalten.
  - **Physikalische Maschinen**. Verwenden Sie diese Ansicht, um auf dem Management Server registrierte Maschinen zu verwalten.
  - **Depots**. Verwenden Sie diese Ansicht, um zentrale Depots und darin gespeicherte Archive zu verwalten: Sie können hier neue verwaltete und nicht verwaltete Depots erstellen oder bestehende Depots umbenennen oder löschen.
  - **Storage Nodes**. Verwenden Sie diese Ansicht, um Storage Nodes zu verwalten. Sie können hier einen Storage Node hinzufügen, damit Sie zentrale Depots erstellen können, die vom Knoten verwaltet werden.
  - **Tasks**. Verwenden Sie diese Ansicht, um Tasks zu verwalten, auszuführen, zu bearbeiten, zu stoppen und zu löschen, ihre Zustände zu überwachen und den Verlauf eines Tasks zu überprüfen.
  - **Log**. Verwenden Sie diese Ansicht, um den Verlauf von zentralen Verwaltungsaktionen zu untersuchen, z.B. das Erstellen einer Gruppe aus verwalteten Einheiten, das Anwenden einer Richtlinie oder das Verwalten eines zentralen Depots. Außerdem können Sie den Verlauf von Aktionen untersuchen, die in den lokalen Logs der registrierten Maschinen und Storage Nodes protokolliert sind.

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.

   Wenn die Konsole zu einem beliebigen Zeitpunkt mit Acronis Management Server verbunden war, wird der Shortcut automatisch als **AMS [Name der Maschine]** hinzugefügt.

Bereich „Aktionen und Werkzeuge“

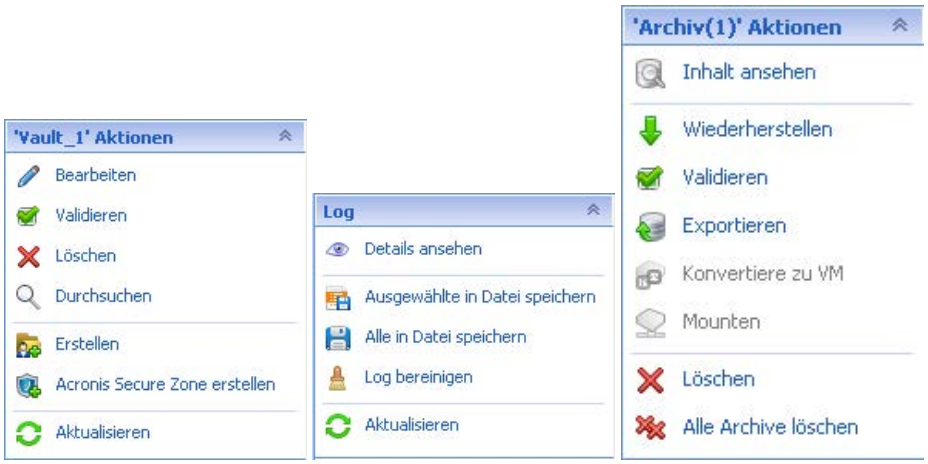
Im Bereich **Aktionen und Werkzeuge** können Sie in einfacher und effizienter Weise mit Acronis Backup & Recovery 10 arbeiten. Die Bereiche der Seitenleisten bieten einen schnellen Zugriff auf die Aktionen und Werkzeuge des Programms. Alle Elemente des Bereichs **Aktionen und Werkzeuge** sind außerdem 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. 16) 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. 16)).

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.

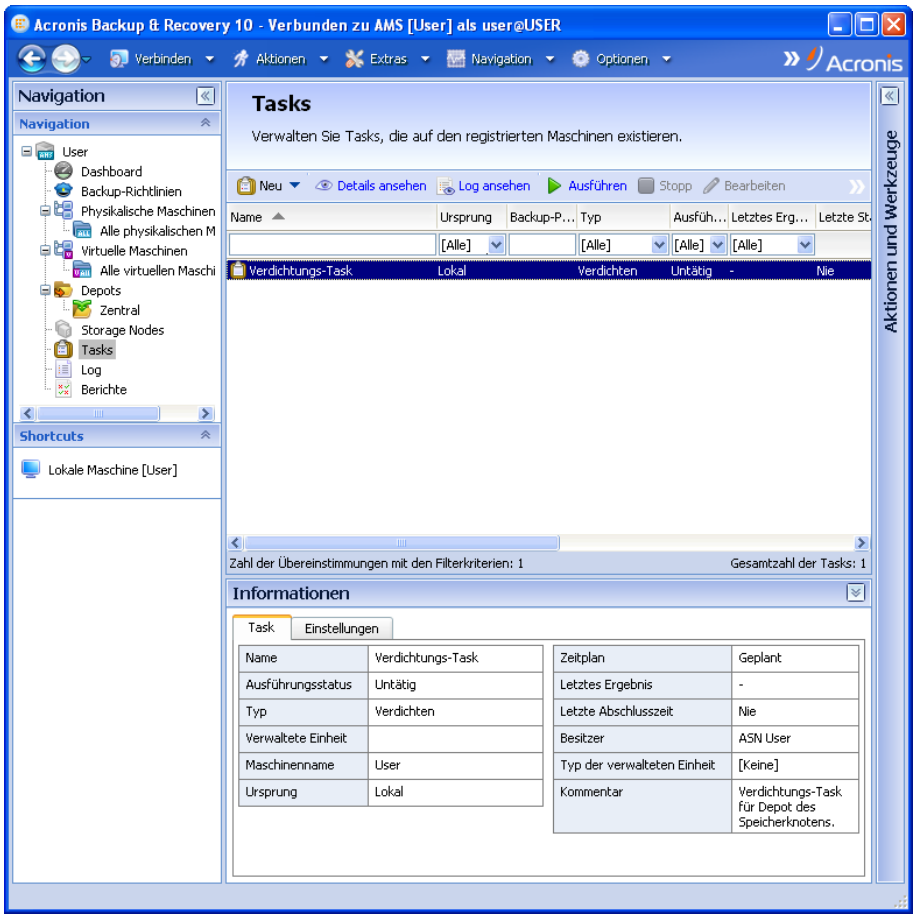
Die Verwaltungskonsole „merkt sich“, wie die Begrenzungslinien der Seitenleisten eingestellt sind. Wenn Sie die Verwaltungskonsole das nächste Mal starten, befinden sich alle Begrenzungslinien der Seitenleiste an der zuvor eingestellten Position.

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. 12) klicken, wird eine entsprechende Ansicht angezeigt.



Ansicht „Tasks“

Übliche Arbeitsweise mit Ansichten

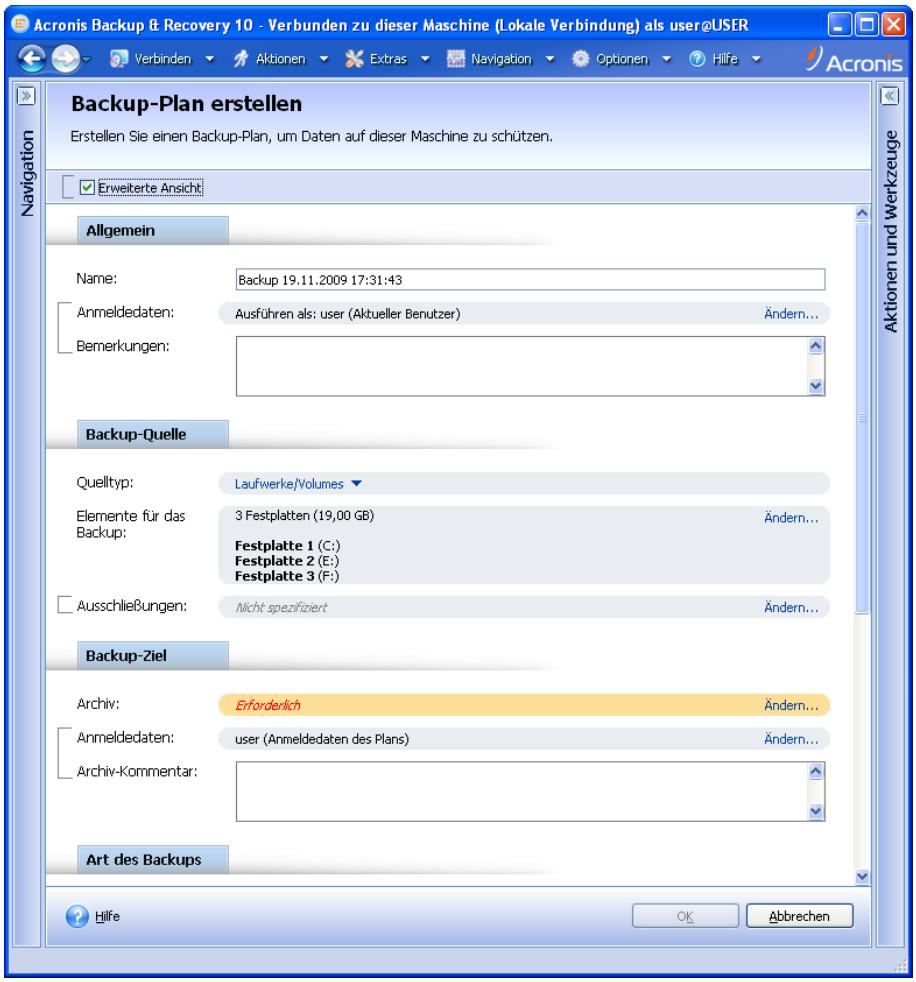
In der Regel enthält jede Ansicht eine Tabelle mit Elementen, eine Symbolleiste mit Schaltflächen für die Tabelle sowie den unteren Fensterbereich **Informationen**.

- 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.

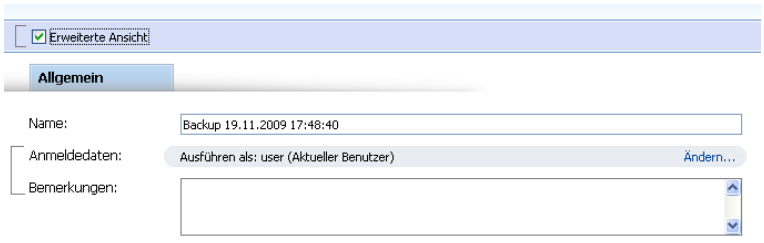


Aktionsseite – Backup-Plan erstellen

Steuerelemente verwenden und Einstellungen festlegen

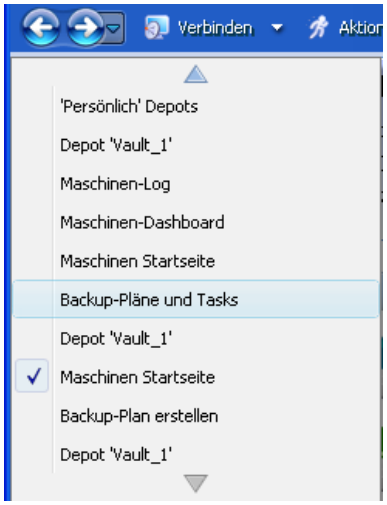
Aktionsseiten können auf zwei verschiedene Weisen dargestellt werden: Einfach und erweitert. Bei der einfachen Darstellung werden bestimmte Felder ausgeblendet, wie z.B. Anmeldeinformationen, Kommentare usw. Wenn die erweiterte Darstellung aktiviert ist, dann werden alle verfügbaren Felder angezeigt.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

In Acronis Backup & Recovery 10 gibt es drei Komponenten-Typen.

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.

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.

Komponenten für zentrale Verwaltung

Diese mit den Advanced Editions ausgelieferten Komponenten bieten die Fähigkeit zur zentralen Verwaltung. Zur Verwendung dieser Komponenten wird keine Lizenz benötigt.

Konsole

Die Konsole bietet eine grafische Benutzeroberfläche sowie eine Remote-Verbindung mit den Agenten und anderen Acronis Backup & Recovery 10-Komponenten.

1.3.1 Agent für Windows

Dieser Agent ermöglicht unter Windows, Ihre Daten auf Laufwerk- und Datei-Ebene zu schützen.

Laufwerk-Backup

Der Schutz auf Laufwerksebene basiert auf Sicherung des gesamten Dateisystems eines Laufwerks bzw. Volumes, einschließlich aller zum Booten des Betriebssystems notwendigen Informationen; oder – beim Sektor-für-Sektor-Ansatz – auf Sicherung aller Laufwerkssektoren (raw-Modus). Ein Backup, welches die Kopie eines Laufwerks oder Volumes in gepackter Form enthält, wird auch Laufwerk-Backup (Disk-Backup, Partition-Backup, Volume-Backup) oder Laufwerk-Image (Partition-Image, Volume-Image) genannt. Aus solchen Backups können Laufwerke oder Volumes in ihrer Gesamtheit wiederhergestellt werden, es können aber auch einzelne Dateien oder Ordner wiederhergestellt werden.

Datei-Backup

Der Schutz der Daten auf Datei-Ebene basiert auf der Sicherung von Dateien und Ordnern, die sich auf der Maschine, auf der der Agent installiert ist oder auf einem freigegebenen Netzlaufwerk befinden. 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.

Andere Aktionen

Konvertierung zu einer virtuellen Maschine

Alternativ zur Konvertierung eines Laufwerk-Backups in eine virtuelle Laufwerksdatei, wobei zusätzliche Aktionen für die Verfügbarkeit des virtuellen Laufwerks nötig wären, erfolgt die Konvertierung durch den Agent für Windows durch Wiederherstellung eines Laufwerk-Backups in eine neue virtuelle Maschine eines der folgenden Typen: VMware Workstation, Microsoft Virtual PC, Parallels Workstation oder Citrix XenServer Open Virtual Appliance (OVA). Die Dateien der vollständig konfigurierten und operationalen Maschine werden in dem von Ihnen ausgewählten Ordner abgelegt. Sie können die Maschine unter Verwendung der entsprechenden Virtualisierungssoftware starten oder die Dateien der Maschine für eine künftige Verwendung vorbereiten.

Laufwerksverwaltung

Agent für Windows enthält Acronis Disk Director Lite - ein nützliches Werkzeug zur Laufwerksverwaltung. Aktionen zur Laufwerksverwaltung, wie das Klonen und Konvertieren von Laufwerken, das Erstellen, Formatieren und Löschen von Volumes; das Ändern des Partitionsschemas eines Laufwerks zwischen MBR und GPT oder das Ändern einer Laufwerksbezeichnung können sowohl im Betriebssystem als auch durch Nutzung eines bootfähigen Mediums durchgeführt werden.

Universal Restore

Mit dem Add-on Universal Restore können Sie die Funktion zur Wiederherstellung abweichender Hardware auf der Maschine verwenden, auf der der Agent installiert ist und Sie können bootfähige Medien mit dieser Funktion erstellen. Universal Restore kümmert sich um Unterschiede bei Geräten, die kritisch für den Windows-Start sind, wie z.B. Speicher-Controller, Hauptplatine oder Chipsatz.

Deduplizierung

Dank dieses Add-ons kann der Agent Daten in einem deduplizierenden Depot sichern, das vom Acronis Backup & Recovery 10 Storage Node verwaltet wird.

1.3.2 Komponenten für zentrale Verwaltung

In diesem Abschnitt werden die Komponenten aufgeführt, die in den Acronis Backup & Recovery 10-Editionen enthalten sind und die Fähigkeit zur zentralen Verwaltung bieten. Zusätzlich zu diesen Komponenten müssen die Acronis Backup & Recovery 10-Agenten auf allen Maschinen installiert werden, auf denen Daten geschützt werden müssen.

Management Server

Acronis Backup & Recovery 10 Management Server ist der zentrale Server, der für die Sicherung von Daten im Unternehmensnetzwerk sorgt. Der Management Server bietet dem Administrator:

- einen zentralen Zugriffspunkt auf die Acronis Backup & Recovery 10-Infrastruktur
- einem einfachen Weg zum Schutz der Daten auf zahlreichen Maschinen (S. 427) unter Benutzung von Backup-Richtlinien (S. 420) und Gruppierung
- unternehmensweite Monitoring- und Berichts-Funktionalität
- der Fähigkeit, zentrale Depots (S. 433) zur Ablage von Backup-Archiven (S. 419) des Unternehmens zu erstellen
- der Fähigkeit, Storage Nodes (S. 429) zu verwalten.

Gibt es mehrere Management Server im Netzwerk, dann arbeiten diese unabhängig voneinander, verwalten verschiedene Maschinen und benutzen verschiedene zentrale Depots zur Ablage der Archive.

Die Datenbanken des Management Servers

Der Management Server verwendet drei Microsoft-SQL-Datenbanken:

- Die Konfigurationsdatenbank, in der eine Liste registrierter Maschinen zusammen mit anderen Konfigurationsinformationen gespeichert ist. Dazu gehören z.B. vom Administrator erstellte Backup-Richtlinien.
- Die Synchronisierungsdatenbank, die zur Synchronisierung des Management Servers mit den registrierten Maschinen und Storage Nodes verwendet wird. Dies ist eine Datenbank, die schnell veränderliche operationale Daten enthält.
- Die Berichtsdatenbank, in der das zentrale Log gespeichert wird. Diese Datenbank kann sehr groß werden. Ihre Größe hängt von dem von Ihnen festgelegten Log-Level ab.

Die Konfigurations- und die Synchronisierungsdatenbank sollten sich auf demselben Microsoft-SQL-Server (auch operationaler Server genannt) befinden, der vorzugsweise auf derselben Maschine installiert wird wie der Management Server. Die Berichtsdatenbank kann auf demselben oder auf einem anderen SQL-Server konfiguriert werden.

Wenn Sie einen Management Server installieren, können Sie für die operationalen und Berichts-Server festlegen, welcher Server verwendet werden sollen. Die folgenden Optionen sind verfügbar:

1. Microsoft SQL Server 2005 Express, das mit dem Installationspaket geliefert wird und auf derselben Maschine installiert wird. In diesem Fall wird eine SQL-Server-Instanz mit drei Datenbanken auf der Maschine erstellt.
2. Microsoft SQL Server 2008 (beliebige Edition), bereits auf einer beliebigen Maschine installiert.
3. Microsoft SQL Server 2005 (beliebige Edition), bereits auf einer beliebigen Maschine installiert.

VMware vCenter-Integration

Diese Funktion bietet die Möglichkeit, virtuelle Maschinen in der Benutzeroberfläche des Management Servers zu sehen, die von einem VMware vCenter-Server verwaltet werden, den

Backup-Status dieser Maschinen im vCenter zu sehen und die von Acronis Backup & Recovery 10 erstellten Maschinen automatisch im vCenter zu registrieren.

Integration ist für alle Acronis Backup & Recovery 10 Advanced Editions verfügbar, eine Virtual Edition-Lizenz ist nicht erforderlich. Auf dem vCenter-Server wird keine Software-Installation benötigt.

Diese Funktion ermöglicht das automatische Deployment und die Konfiguration des Agenten für ESX/ESXi auf irgendeinem ESX/ESXi-Server, der nicht notwendigerweise durch das vCenter verwaltet wird.

Storage Node

Der Acronis Backup & Recovery 10 Storage Node ist ein Server zur Optimierung der Auslastung verschiedener Ressourcen (z.B. der Speicherkapazität in einem Unternehmen, der Netzwerkbandbreite oder der CPU-Last auf den verwalteten Maschinen), die zur Sicherung der Daten eines Unternehmens erforderlich sind. Dieses Ziel wird durch Organisation und Verwaltung der Speicherorte erreicht, die als dedizierte Speicher für die Backup-Archive des Unternehmens (verwaltete Depots) dienen.

Die Storage Nodes ermöglichen die Schaffung einer hochgradig skalierbaren und – im Hinblick auf die unterstützte Hardware – flexiblen Speicherinfrastruktur. Es können bis zu 20 Storage Nodes eingerichtet werden, von denen jeder in der Lage ist, bis zu 20 Depots zu verwalten. Der Administrator steuert die Storage Nodes zentral vom Acronis Backup & Recovery 10 Management Server (S. 427) aus. Die direkte Verbindung einer Konsole mit einem Storage Node ist nicht möglich.

Einrichten der Speicher-Infrastruktur

Installieren Sie die Storage Nodes, fügen Sie diese dem Management Server hinzu (dieser Vorgang ist mit der Registrierung (S. 428) einer verwalteten Maschine vergleichbar) und erstellen Sie zentrale Depots (S. 433). Wenn Sie ein zentrales Depot erstellen, geben Sie den Pfad zum Depot, dem Storage Node, der das Depot verwalten wird, sowie die Verwaltungsaktionen an, die auf dem Depot ausgeführt werden sollen.

Ein verwaltetes Depot kann organisiert werden:

- auf für den Storage Node lokal verfügbaren Festplatten
- auf einer Netzwerkfreigabe
- auf einem Storage Area Network (SAN)
- auf einem Network Attached Storage-Gerät (NAS)
- auf einer Bandbibliothek, die lokal mit dem Storage Node verbunden ist.

Folgende Verwaltungsaktionen können ausgeführt werden.

Storage Node-seitige Bereinigung und Validierung

Archive, die in nicht verwalteten Depots gespeichert werden, werden durch die Agenten (S. 419) verwaltet, die die Archive erstellen. Das bedeutet, dass die einzelnen Agenten nicht nur Backups der Daten auf ein Archiv ausführen, sondern auch Dienst-Tasks ausführen, die für das Archiv, die Aufbewahrungsregeln und die Validierungsregeln zutreffend sind, die im Backup-Plan (S. 420) angegeben sind. Um die verwalteten Maschinen von unnötiger CPU-Last zu befreien, kann die Ausführung der Dienst-Tasks an den Storage Node delegiert werden. Da die Planung der Tasks auf der Maschine liegt, auf der sich der Agent befindet und da daher die Zeit bzw. die Ereignisse der Maschine benutzt werden, muss der Agent die Storage Node-seitige Bereinigung (S. 421) und die Storage Node-seitige Validierung (S. 429) entsprechend der Planung auslösen. Dafür muss der Agent

online sein. Die weitere Verarbeitung wird vom Storage Node übernommen.

Diese Funktionalität kann in einem verwalteten Depot nicht deaktiviert werden. Die nächsten beiden Aktionen sind optional.

Deduplizierung

Ein verwaltetes Depot kann als deduplizierendes Depot konfiguriert werden: Das bedeutet, dass identische Daten nur einmal in das Backup auf dieses Depot aufgenommen werden, um die Netzwerkauslastung während des Backups und den durch die Archive benötigten Speicherplatz zu minimieren. Zu weiteren Informationen siehe den Abschnitt „Deduplizierung (S. 69)“ in der Benutzeranleitung.

Verschlüsselung

Ein verwaltetes Depot kann so konfiguriert werden, dass alle darauf geschriebenen Daten verschlüsselt und alle davon gelesenen Daten vom Storage Node transparent entschlüsselt werden, wobei ein für das Depot spezifischer Kodierungsschlüssel benutzt wird, der auf dem Server des Knotens gespeichert wird. Falls das Speichermedium gestohlen wird oder eine unbefugte Person darauf zugreift, wird der Übeltäter den Inhalt des Depots ohne Zugriff auf diesen speziellen Storage Node nicht entschlüsseln können.

Sollte ein Archiv bereits durch den Agenten verschlüsselt sein, dann wird die Verschlüsselung auf Storage Node-Seite noch einmal über die durch den Agenten ausgeführte gelegt.

PXE Server

Der Acronis PXE Server ermöglicht es, Maschinen mit bootfähigen Acronis-Komponenten über das Netzwerk zu starten.

Booten über das Netzwerk:

- Eliminiert die Notwendigkeit eines Technikers vor Ort, um das bootfähige Medium (S. 422) in das zu bootende System einzulegen
- Reduziert bei Gruppen-Operationen die zum Booten mehrerer Maschinen benötigte Zeit (im Vergleich zu physikalischen Bootmedien)

License Server

Der Server ermöglicht Ihnen, Lizenzen von Acronis-Produkten zu verwalten und die Komponenten zu installieren, für die Lizenzen erforderlich sind.

Weitere Informationen über Acronis License Server finden Sie unter „Verwenden von Acronis License Server“.

1.3.3 Management Console

Acronis Backup & Recovery 10 Management Console ist ein administratives Werkzeug zum Remote- und lokalen Zugriff auf die Acronis Backup & Recovery 10-Agenten sowie auf den Acronis Backup & Recovery 10 Management Server, falls die Produkt-Editionen über eine Funktion zur zentralen Verwaltung verfügen.

Die Konsole hat zwei Distributionen: zur Installation unter Windows und zur Installation unter Linux. Obwohl beide Distributionen eine Verbindung zu jedem Acronis Backup & Recovery 10-Agenten und Acronis Backup & Recovery 10 Management Server ermöglichen, wird empfohlen, die Konsole für Windows zu verwenden, wenn diese Möglichkeit besteht. Die unter Linux installierte Konsole ist in

ihrer Funktionalität eingeschränkt:

- Eine Remote-Installation von Acronis Backup & Recovery 10-Komponenten ist nicht verfügbar
- Active Directory-bezogene Features, z.B. das Durchsuchen von AD, sind nicht verfügbar.

1.3.4 Bootable Media Builder

Acronis Bootable Media Builder ist ein spezielles Werkzeug zur Erstellung von bootfähigen Medien (S. 422). Der auf Windows installierte Media Builder kann bootfähige Medien schaffen, die entweder auf Windows Preinstallation Environment (WinPE) oder einem Linux-Kernel basieren.

Das Add-on für Universal Restore (S. 19) ermöglicht die Erstellung eines bootfähigen Mediums, das die Fähigkeit zur Wiederherstellung auf abweichende Hardware bietet. Universal Restore kümmert sich um Unterschiede bei Geräten, die kritisch für den Windows-Start sind, wie z.B. Speicher-Controller, Hauptplatine oder Chipsatz.

Das Add-on für Deduplizierung (S. 19) ermöglicht Ihnen die Erstellung bootfähiger Medien, die Backups auf deduplizierende Depots erstellen können.

1.3.5 Acronis WOL Proxy

Diese Option funktioniert in Kombination mit den erweiterten Planungseinstellungen für **Wake-On-LAN verwenden** (S. 180). Verwenden Sie diese Option, wenn der Management Server Backup-Maschinen in einem anderen Subnetz einschalten soll.

Kurz bevor die geplante Aktion startet, verschickt der Management Server so genannte 'Magic Packets', um die entsprechenden Maschinen einzuschalten. (Ein Magic Packet ist ein Paket, das 16 Mal in Folge die MAC-Adresse der Empfänger-Netzwerkkarte enthält). Der in dem anderen Subnetz installierte Acronis WOL Proxy sendet die Pakete an die Maschinen in diesem Subnetz.

Voreinstellung ist: **Ausgeschaltet**.

So aktivieren Sie diese Option:

1. Installieren Sie Acronis WOL Proxy auf einem Server im Subnetz, auf dem die Maschinen sich befinden, die Sie einschalten möchten. Bei diesem Server muss eine ständige Verfügbarkeit der Dienste gewährleistet sein. Wenn mehrere Subnetze vorhanden sind, installieren Sie Acronis WOL Proxy in jedem Subnetz, in dem Sie die Funktion Wake-On-LAN benötigen.
2. So aktivieren Sie **Acronis WOL Proxy** in den **Optionen des Management Servers**:
   a. Aktivieren Sie das Kontrollkästchen **Folgende Proxies verwenden**.
   b. Klicken Sie auf **Hinzufügen** und geben Sie den Namen oder die IP-Adresse der Maschine ein, auf der der Acronis WOL Proxy installiert ist. Geben Sie die Anmeldedaten für die Maschine ein.
   c. Wiederholen Sie diesen Schritt, wenn es mehrere Acronis WOL Proxies gibt.
3. Aktivieren Sie beim Planen einer Backup-Richtlinie die Einstellung **Wake-On-LAN verwenden**.

Sie können außerdem Proxies aus der Liste löschen. Denken Sie daran, dass jede Änderung dieser Option Auswirkungen auf den gesamten Management Server hat. Wenn Sie einen Proxy aus der Liste löschen, wird die Funktion Wake-On-LAN im entsprechenden Subnetz für alle Richtlinien, einschließlich der bereits angewandten Richtlinien, deaktiviert.

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 License Server

- Windows XP Professional SP2+ (x86, x64)
- Windows 2000 SP4 – alle Editionen, mit Ausnahme der Datacenter Edition
- Windows Server 2003/2003 R2 – Standard und Enterprise Editionen (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista – alle Editionen mit Ausnahme von Vista Home Basic und Vista Home Premium (x86, x64)
- Windows 7 SP1 – alle Editionen mit Ausnahme der Starter- und Home-Editionen (x86, x64)
- Windows Server 2008 – Standard und Enterprise Editionen (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1 – Standard, Enterprise, Datacenter und Foundation Editionen
- Windows MultiPoint Server 2010

Acronis Backup & Recovery 10 Management Console

- Windows XP Professional SP2+ (x86, x64)
- Windows 2000 SP4 – alle Editionen, mit Ausnahme der Datacenter Edition
- Windows Server 2003/2003 R2 – Standard und Enterprise Editionen (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista – alle Editionen (x86, x64)
- Windows 7 SP1 – alle Editionen (x86, x64)

- Windows Server 2008 – Standard und Enterprise Editionen (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1 – Standard, Enterprise, Datacenter und Foundation Editionen
- Windows MultiPoint Server 2010

Acronis Backup & Recovery 10 Management Server und Acronis Backup & Recovery 10 Storage Node

- Windows XP Professional SP2+ (x86, x64)
- Windows 2000 SP4 – alle Editionen, mit Ausnahme der Datacenter Edition
- Windows Server 2003/2003 R2 – Standard und Enterprise Editionen (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista – alle Editionen mit Ausnahme von Vista Home Basic und Vista Home Premium (x86, x64)
- Windows 7 SP1* – alle Editionen mit Ausnahme der Starter- und Home-Editionen (x86, x64)
- Windows Server 2008 – Standard und Enterprise Editionen (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1* – Standard, Enterprise, Datacenter und Foundation Editionen
- Windows MultiPoint Server 2010*

* Acronis Backup & Recovery 10 Storage Node verarbeitet Bandbibliotheken und Autoloader mit Hilfe von Removable Storage Management (RSM). Weil Windows 7, Windows Server 2008 R2 und Windows MultiPoint Server 2010 kein RSM unterstützen, kann ein auf diesen Betriebssystemen installierter Storage Node auch keine Bandbibliotheken und Autoloader unterstützen.

Acronis Backup & Recovery 10 Agent für Windows

- Windows 2000 Professional SP4
- Windows XP Professional SP2+ (x86, x64)
- Windows Vista – alle Editionen mit Ausnahme von Vista Home Basic und Vista Home Premium (x86, x64)
- Windows 7 SP1 – alle Editionen mit Ausnahme der Starter- und Home-Editionen (x86, x64)

Acronis-Produkte bieten keine Unterstützung für Systeme mit EFI (Extensible Firmware Interface). Obwohl es möglich ist, ein GPT-Volume mit Acronis wiederherzustellen, falls Windows auf diesem installiert ist, wird das wiederhergestellte System nicht bootfähig sein. Acronis Backup & Recovery 10 kann Betriebssysteme dann sichern und wiederherstellen, wenn Sie im BIOS/MBR-Modus installiert sind – und das auch, wenn Sie auf EFI-fähigen Servern laufen. Die meisten Server haben BIOS-Einstellungen, die es erlauben, eine Installations-CD im BIOS/MBR- statt EFI-Modus zu booten. Der MBR-Modus gewährleistet, dass das Boot-Laufwerk nach der Installation im MBR- statt im GPT-Standard partitioniert ist.

1.6 Systemanforderungen

Unter Windows installierte Komponenten

Komponente	Speicher (zusätz. zu dem für OS und akt. Programme)	Erforderlicher Festplattenplatz während Installation oder Update	Durch Komponenten belegter Platz	Erweitert
Vollständige Installation	300 MB	2.7 GB	1.7 GB einschließlich SQL Express Server	
Agent für Windows	120 MB	700 MB	260 MB	
Bootable Media Builder	80 MB	700 MB	300 MB	CD-RW- oder DVD-RW-Laufwerk
Management Console	30 MB	950 MB	450 MB	Bildschirmauflösung 1024*768 Pixel oder höher
Management Server	40 MB	250 MB 400 MB für SQL Express Server	250 MB 400 MB für SQL Express Server	
Wake-on-LAN Proxy	Unerheblich	30 MB	5 MB	
Storage Node	100 MB	150 MB	150 MB Erforderlicher Platz für die Band-Datenbank, falls eine Bandbibliothek benutzt wird: ca. 1 MB pro 10 Archive	Empfohlene Hardware: 4 GB RAM Hochgeschwindigkeits-Storage wie Hardware RAID
License Server	Unerheblich	25 MB	25 MB	
PXE Server	5 MB	80 MB	15 MB	

Netzwerkkarten oder virtuelle Netzwerkadapter sind üblicherweise für alle Komponenten erforderlich.

Bootfähiges Medium

Medientyp	Arbeitsspeicher	ISO-Image-Größe	Erweitert
Basierend auf Windows PE	512 MB	300 MB	
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

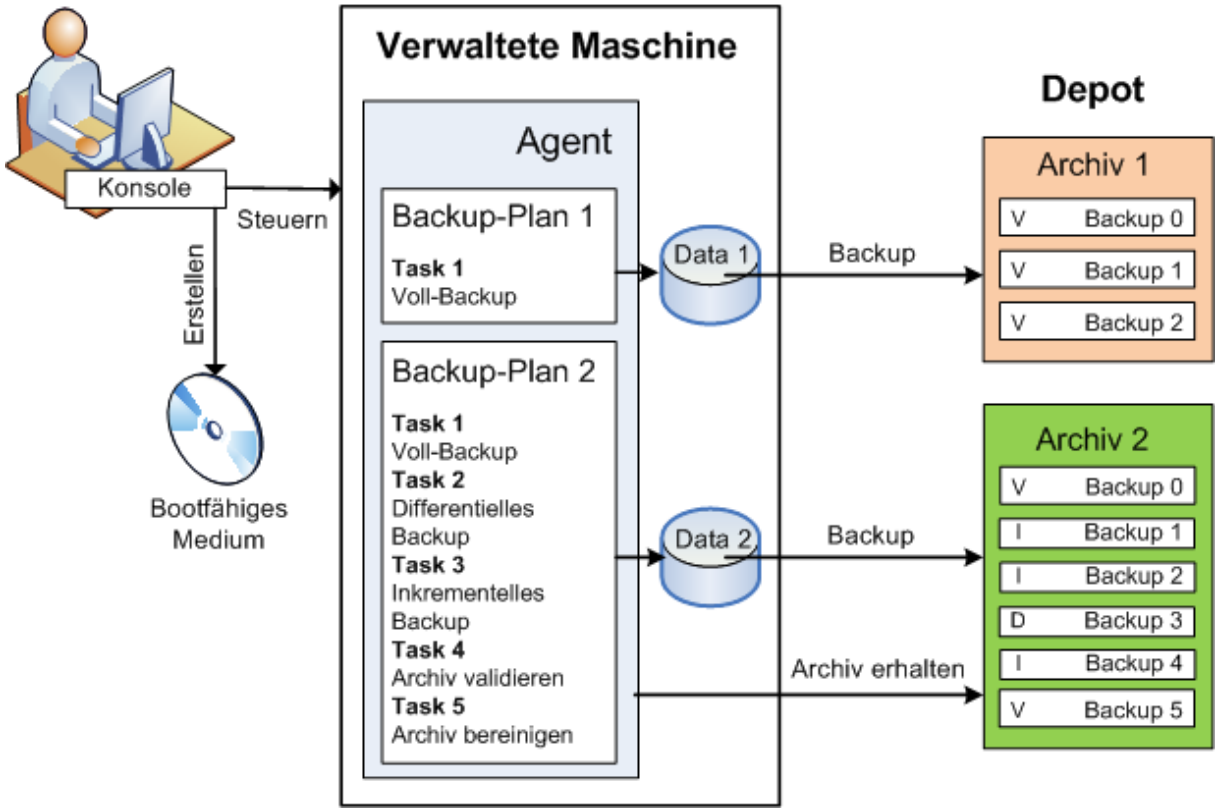
Machen Sie sich mit den grundlegenden Begriffen in der Benutzeroberfläche und Dokumentation von Acronis Backup & Recovery 10 vertraut. Fortgeschrittene Anwender können diesen Abschnitt auch als eine Schnellanleitung verwenden. Entsprechende Details können zudem in der kontextsensitiven Hilfe gefunden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

Backup unter einem Betriebssystem

1. Um die Daten einer Maschine zu schützen, installieren Sie auf dieser den Acronis Backup & Recovery 10 Agent (S. 419), wodurch die Maschine von diesem Zeitpunkt an zu einer verwalteten Maschine (S. 431) wird.
2. Um die Maschine mit einer grafischen Benutzeroberfläche zu managen, installieren Sie die Acronis Backup & Recovery 10 Management Console (S. 426) 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. 422).
4. Verbinden Sie die Konsole mit der verwalteten Maschine.
5. Einen Backup-Plan (S. 420) erstellen.

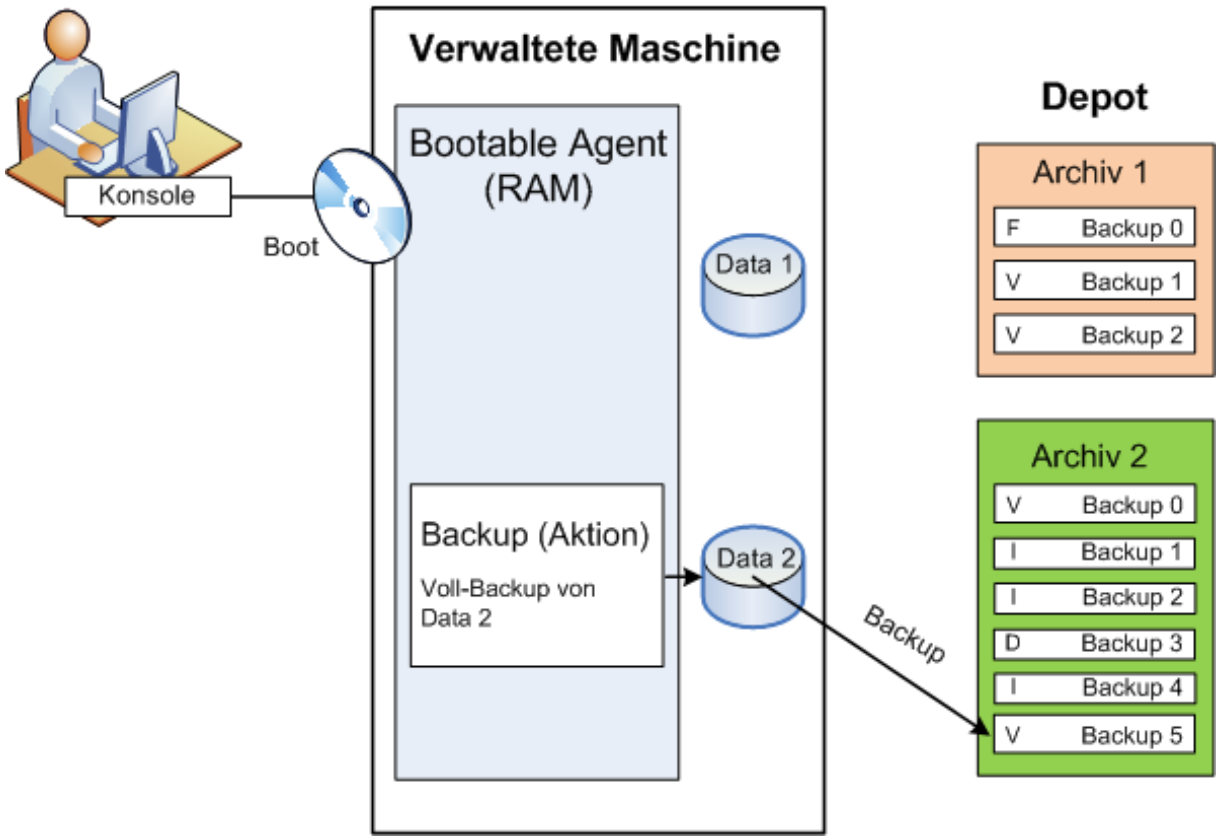
   Zur Umsetzung müssen Sie im Minimum die zu sichernden Daten sowie den Zielort spezifizieren, wo das erstellte Backup (S. 419) gespeichert wird. Das erstellt eine minimale, aus einem Task (S. 429) bestehende Backup-Aufgabe, die ein vollständiges Backup (S. 419) Ihrer Daten immer dann erstellt, wenn der 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. 32) erstellen, Wartungsaktionen wie Backup-Validierung (S. 430) durchführen oder veraltete Backups löschen (Säuberung (S. 421)). 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. 423) 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.



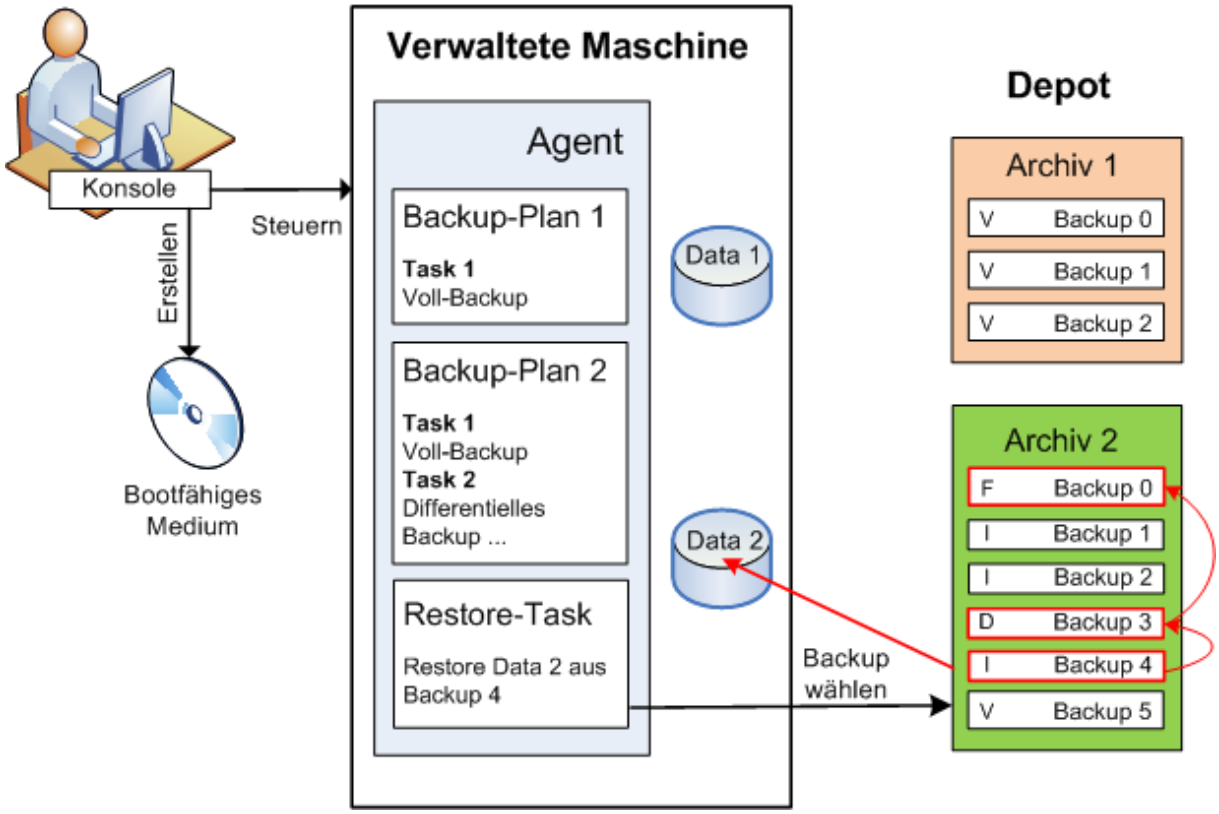
Recovery unter einem Betriebssystem

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.

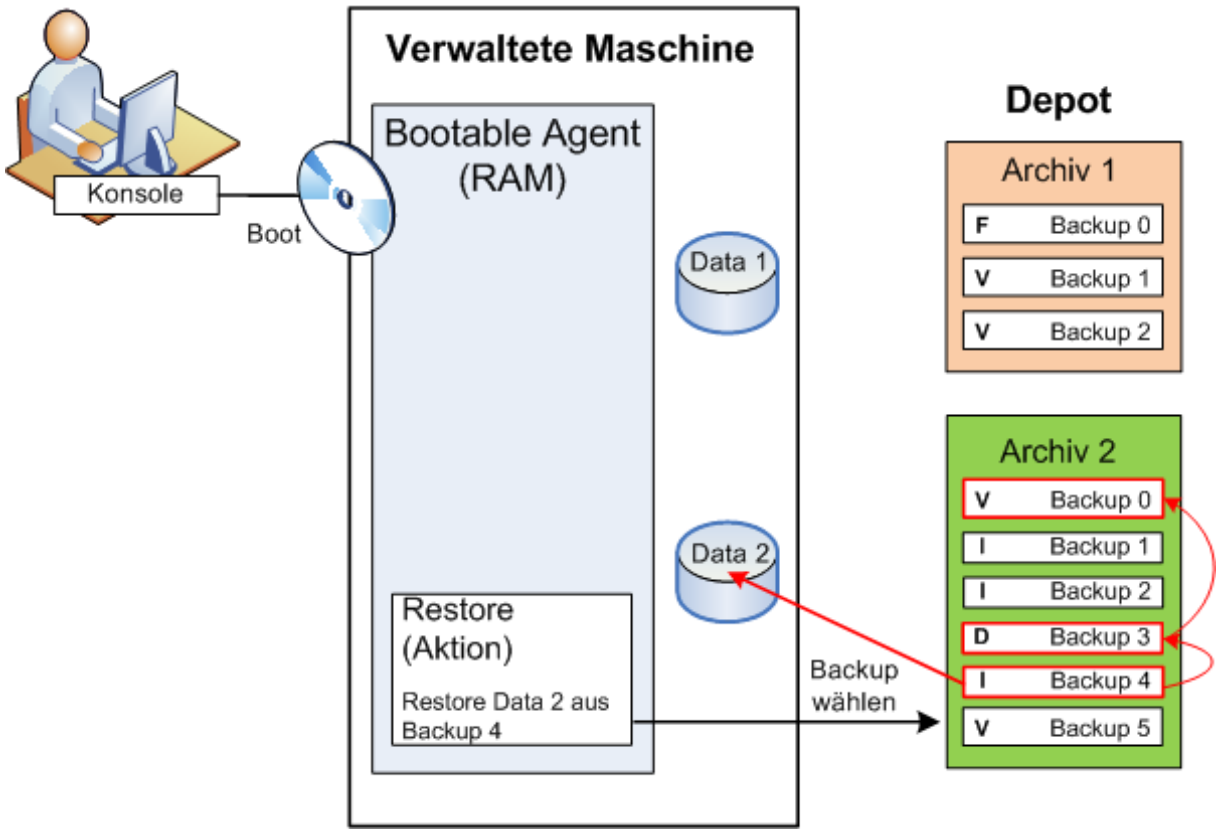
Das nachfolgende Diagramm illustriert die Datenwiederherstellung unter einem Betriebssystem (online). Während die Wiederherstellung auf der Maschine abläuft, kann keine Backup-Aktion stattfinden. Falls benötigt, können Sie die Konsole mit einer anderen Maschine verbinden und auf dieser dann eine Wiederherstellungsaktion 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. 419) 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

Der Umfang von Verwaltungsrechten, die ein Benutzer bei Verwaltung einer unter Windows laufenden Maschine hat, hängt von seinen allgemeinen Benutzerrechten auf der betreffenden Maschine ab.

Reguläre Benutzer

Ein regulärer Benutzer, wie es etwa ein Mitglied der Gruppe „Benutzer“ ist, verfügt über die folgenden Verwaltungsrechte:

- Durchführung von Backup und Wiederherstellung auf Datei-Ebene, mit Dateien, auf die der Benutzer Zugriffsrechte hat – jedoch ohne Nutzung von Backup-Snapshots auf Datei-Ebene
- Backup-Pläne und Tasks erstellen und diese verwalten
- Die Backup-Pläne und Tasks anderer Nutzer können eingesehen, jedoch nicht verwaltet werden.
- Einsicht in die lokale Ereignisanzeige

Administrative Benutzer

Benutzer mit administrativen Privilegien auf der Maschine (wie Mitglieder der Gruppe „Administratoren“ oder „Backup Operatoren“) haben zusätzlich folgende Verwaltungsrechte:

- Backup und Wiederherstellung der kompletten Maschine oder von beliebigen Daten auf der Maschine, mit oder ohne Festplatten-Snapshot

Mitglieder der Gruppe 'Adminstratoren' können außerdem:

- Backup-Pläne und Tasks, die anderen Benutzern auf der Maschine gehören, einsehen und verwalten.

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 (S. 151) zusätzlich berücksichtigen.)

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

GVS-bezogene Einstellungen eines Backup-Plans

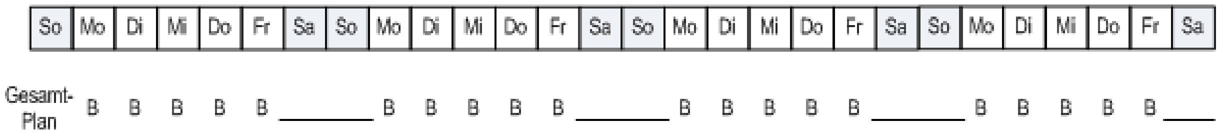
Backup starten:

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.

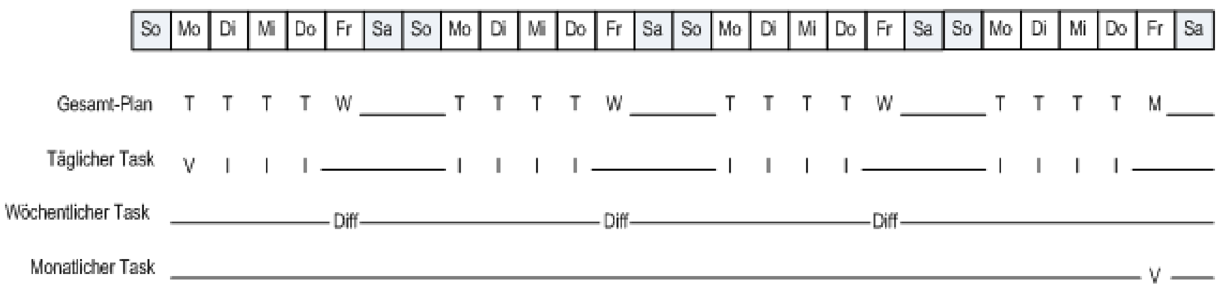
„T“ steht für das als täglich betrachtete Backup. „W“ steht für das als wöchentlich betrachtete Backup. „M“ steht für das als monatlich betrachtete Backup.

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

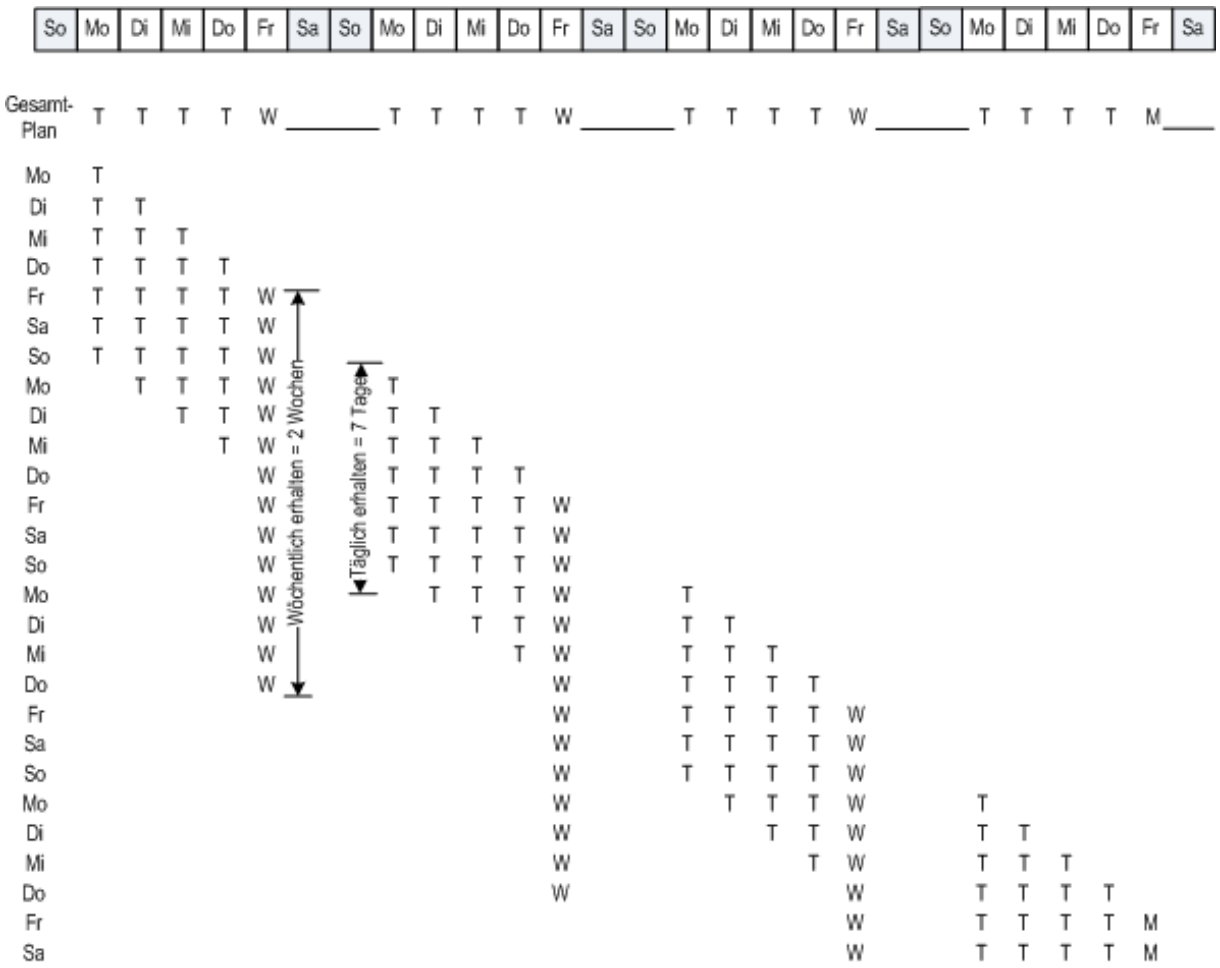
Dieser Schritt definiert die Aufbewahrungsregel für monatliche Backups. Der Bereinigungs-Task wird nach jedem monatlichen Backup ausgeführt und löscht alle monatlichen Backups. die älter als von Ihnen spezifiziert sind. Die monatliche Backup-Aufbewahrungsperiode kann nicht kleiner als die wöchentliche 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

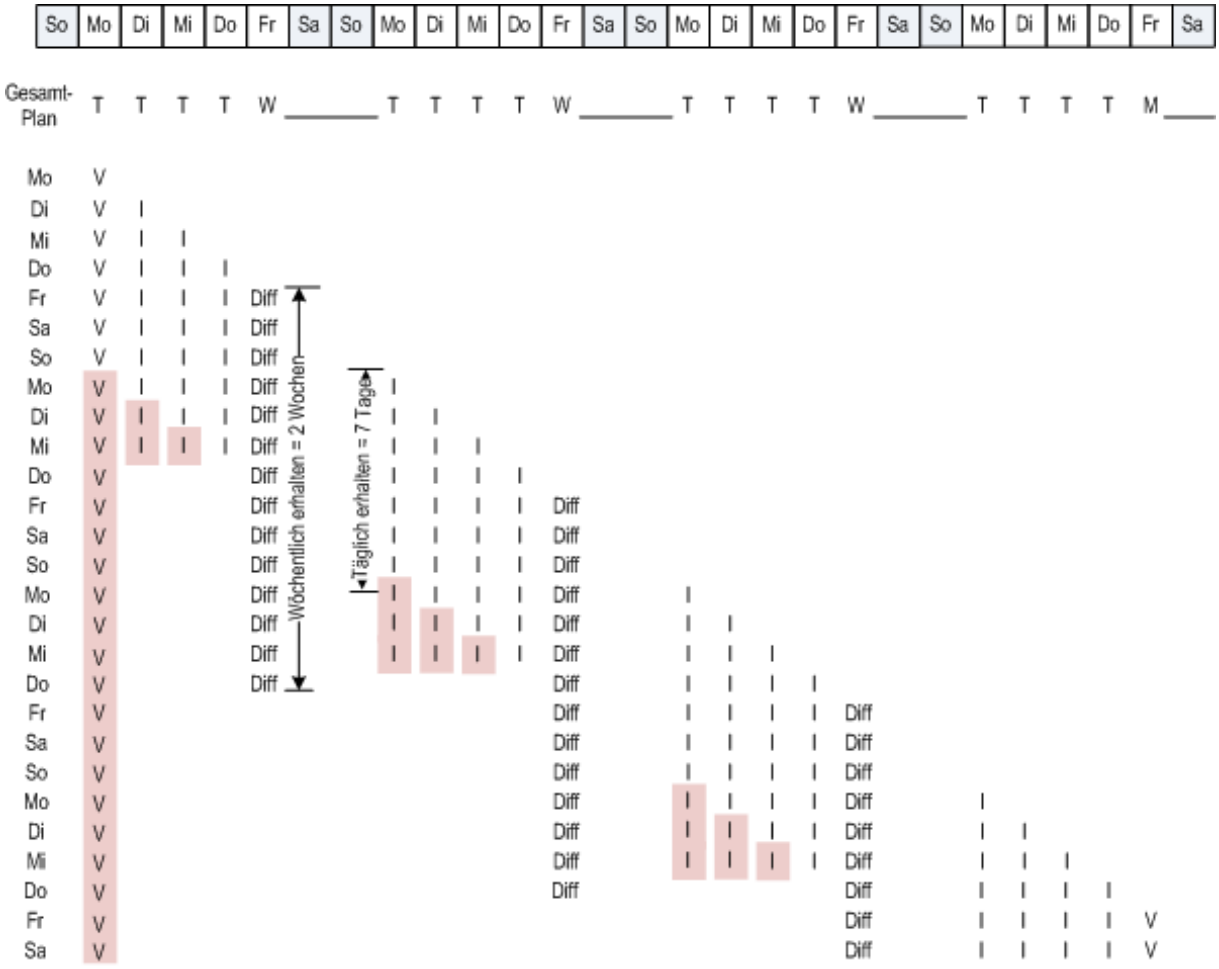
Unter realistischen Umständen wird der Archivinhalt etwas vom idealen Schema abweichen.

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 (S. 157).

2.7 Aufbewahrungsregeln

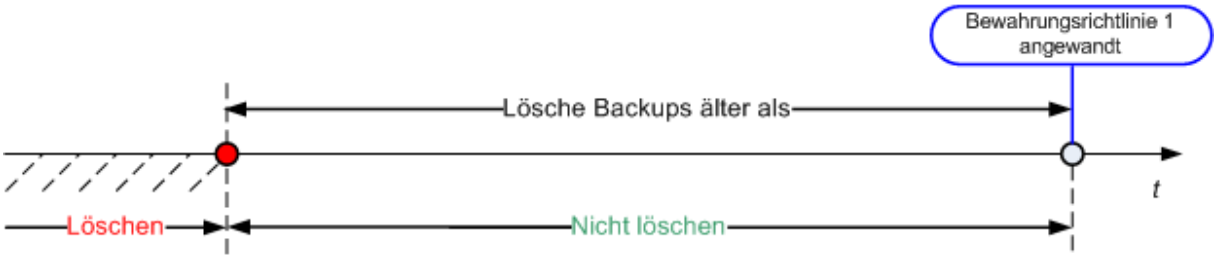
Durch einen Backup-Plan erstellte Backups bilden ein Archiv. Die zwei in diesem Abschnitt beschriebenen Aufbewahrungsregeln ermöglichen Ihnen, Archivgröße und Lebenszeit

(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. 225); beachten Sie dabei aber das Risiko, möglicherweise das letzte Backup verlieren zu können.

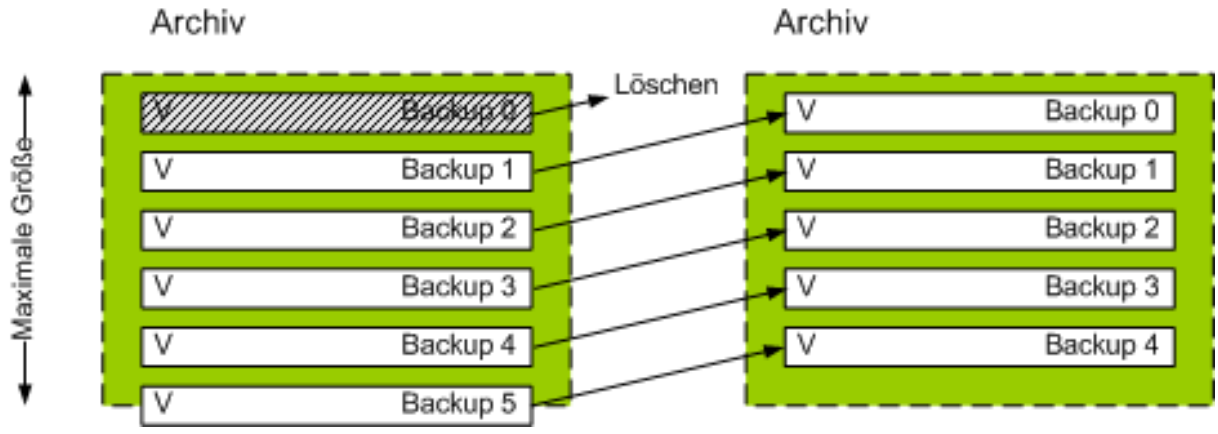
1. Lösche Backups älter als

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

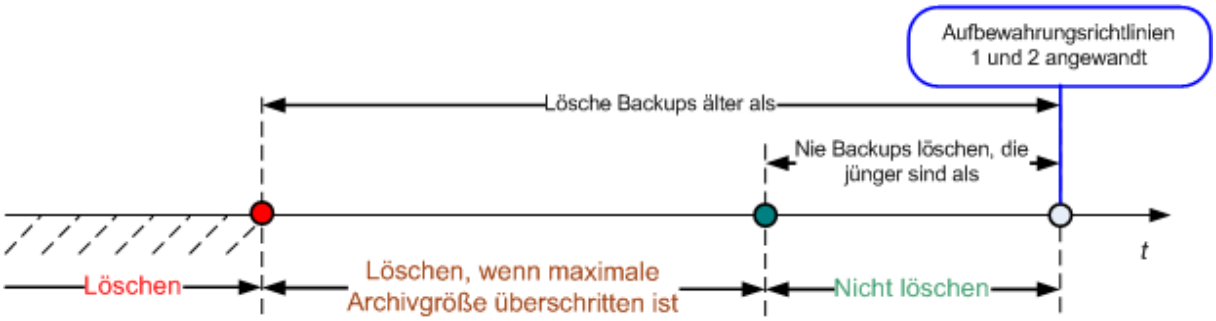
Dies ist die maximale Größe für das Archiv. Jedes Mal, wenn eine Aufbewahrungsregel angewendet wird, vergleicht das Programm die aktuelle Archivgröße mit dem von Ihnen gesetzten Grenzwert und löscht die ältesten Backups, um die Archivgröße innerhalb dieses Wertes zu halten. Das untere Diagramm zeigt 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. 130)“ 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 Dynamische Volumes (Windows) werden gesichert

Dieser Abschnitt erläutert in Kürze Backup und Wiederherstellung dynamischer Volumes (S. 425) durch Acronis Backup & Recovery 10. Basis-Laufwerke, die eine GUID-Partitionstabelle (GPT) verwenden, werden ebenso besprochen.

Ein dynamisches Volume ist ein Volume, das sich auf einem dynamischen Laufwerk (S. 424) oder

genauer auf einer Laufwerksgruppe (S. 422) befindet. Acronis Backup & Recovery 10 unterstützt die folgenden dynamischen Laufwerkstypen/RAID-Level:

- Einfach/Übergreifend
- Stripeset (RAID 0)
- Gespiegelt (RAID 1)
- eine Stripeset-Spiegelung (RAID 0+1)
- RAID 5.

Acronis Backup & Recovery 10 kann dynamische Volumes und (mit kleinen Einschränkungen) GPT-Volumes vom Typ 'Basis' sichern und wiederherstellen.

Dynamische Volumes werden gesichert

Das Backup dynamischer Volumes sowie der Laufwerke von GPT-Volumes erfolgt auf dieselbe Art wie bei MBR-Basisdatenträgern. Beim Erstellen eines Backup-Plans über die Benutzeroberfläche stehen all diese Laufwerkstypen als **Backup-Objekte** zur Auswahl. Wenn Sie die Befehlszeileneingabe verwenden, so spezifizieren Sie dynamische oder GPT-Volumes mit dem DYN-Präfix.

Befehlszeilen-Beispiele

```
trueimagecmd /create /partition:DYN1,DYN2 /asz
```

Dies wird Backups der Laufwerke DYN1 und DYN2 in der Acronis Secure Zone erstellen.

```
trueimagecmd /create /harddisk:DYN /asz
```

Dies wird Backups aller dynamischen Volumes des Systems in der Acronis Secure Zone erstellen.

Der Boot-Code von GPT-Volumes wird nicht gesichert oder wiederhergestellt.

Dynamische Volumes werden wiederhergestellt

Ein dynamisches Volume kann wiederhergestellt werden

- über jeden existierenden Laufwerkstyp
- zu 'nicht zugeordneten' Speicherplatz einer Laufwerksgruppe
- zu 'nicht zugeordneten' Speicherplatz eines Basis-Laufwerks.

Recovery über ein existierendes Laufwerk

Wenn ein dynamisches Laufwerk über ein existierendes Laufwerk ('Basis' oder 'dynamisch) wiederhergestellt wird, so werden die Daten des Ziellaufwerks mit dem Inhalt des Backups überschrieben. Der Typ des Ziellaufwerkes (Basis, einfach/übergreifend, Stripeset, gespiegelt, RAID 0+1, RAID 5) wird nicht verändert. Die Größe des Ziellaufwerkes muss ausreichend sein, um den Inhalt des Backups aufnehmen zu können.

Recovery zu nicht zugeordneten Speicherplatz einer Laufwerksgruppe

Wenn ein dynamisches Laufwerk auf den nicht zugeordneten Speicherplatz einer Datenträgergruppe wiederhergestellt wird, so werden der Typ und der Inhalt des resultierenden Laufwerkes wiederhergestellt. Die Größe nicht zugeordneten Speicherplatzes muss ausreichend sein, um den Inhalt des Backups aufnehmen zu können. Die Art, wie der nicht zugeordnete Speicherplatz über die Datenträger verteilt ist, ist ebenfalls wichtig.

Beispiel

Stripeset-Volumes verbrauchen gleich große Mengen an Speicherplatz auf jedem Laufwerk.

Angenommen, Sie wollen ein 30 GB-Stripeset-Volume auf eine Laufwerksgruppe wiederherstellen, die aus zwei Laufwerken besteht. Jedes Laufwerk hat Volumes und eine

gewisse Menge nicht zugeordneten Speicherplatzes. Die Gesamtgröße des nicht zugeordneten Speicherplatzes beträgt 40 GB. Die Wiederherstellung führt immer zu einem Stripeset-Volume, wenn der nicht zugeordnete Speicherplatz gleichmäßig zwischen den Laufwerken verteilt ist (20 GB und 20 GB).

Wenn eines der Laufwerke über 10 GB und das andere über 30 GB an nicht zugeordnetem Speicher verfügt, so hängt das Wiederherstellungsergebnis von der Größe der wiederherzustellenden Daten ab.

- Beträgt die Datengröße weniger als 20 GB, dann kann ein Laufwerk 10 GB und das andere die verbliebenen 10 GB halten. Auf diese Art wird ein Stripeset-Volume auf beiden Laufwerken erzeugt, wobei auf dem zweiten Laufwerk 20 GB an verfügbarem, nicht zugeordnetem Speicher verbleiben.
- Wenn die Datengröße über 20 GB liegt, so können die Daten nicht gleichmäßig zwischen beiden Laufwerken verteilt werden, aber in ein einzelnes Simple-Laufwerk eingepasst werden. Ein Volume vom Typ 'Einfach', das alle Daten aufnehmen kann, wird auf dem zweiten Laufwerk erstellt. Die erste Festplatte verbleibt dagegen unangetastet.

	Gesichert (Quelle):		
Wiederhergestellt zu:	**Dynamisches Volume**	**MBR-Basisdatenträger-Laufwerk**	**GPT-Basisdatenträger-Laufwerk**
Dynamisches Volume	Dynamisches Volume Typ wie der des Ziels	Dynamisches Volume Typ wie der des Ziels	Dynamisches Volume Typ wie der des Ziels
Nicht zugeordneter Speicherplatz (Laufwerksgruppe)	Dynamisches Volume Typ wie der des Ziels	Dynamisches Volume Einfach	Nicht verfügbar
MBR-Basisdatenträger-Laufwerk	MBR-Basisdatenträger-Laufwerk	MBR-Basisdatenträger-Laufwerk	MBR-Basisdatenträger-Laufwerk
GPT-Basisdatenträger-Laufwerk	GPT-Basisdatenträger-Laufwerk	GPT-Basisdatenträger-Laufwerk	GPT-Basisdatenträger-Laufwerk
Nicht zugeordneter Speicherplatz (MBR-Basis-Laufwerk)	MBR-Basisdatenträger-Laufwerk	MBR-Basisdatenträger-Laufwerk	MBR-Basisdatenträger-Laufwerk
Nicht zugeordneter Speicherplatz (GPT-Basis-Laufwerk)	GPT-Basisdatenträger-Laufwerk	GPT-Basisdatenträger-Laufwerk	GPT-Basisdatenträger-Laufwerk

Laufwerke während einer Wiederherstellung verschieben und in der Größe anpassen

Sie können das resultierende Basisdatenträger-Laufwerk (MBR und GPT) während einer Wiederherstellung in der Größe verändern oder seine Position auf dem Laufwerk ändern. Ein resultierendes dynamisches Laufwerk kann jedoch weder verschoben noch in seiner Größe angepasst werden.

Datenträgergruppen und Laufwerke vorbereiten

Vor Wiederherstellung eines dynamischen Volumes auf ein fabrikneues System sollten Sie auf der Ziel-Hardware eine Laufwerksgruppe erstellen.

Möglicherweise müssen Sie auch verfügbaren, nicht zugeordneten Speicherplatz auf einer existierenden Laufwerksgruppe erstellen oder vergrößern. Dies kann durch Löschen von Laufwerken oder Konvertieren von Basis- zu dynamischen Datenträgern umgesetzt werden.

Möglicherweise wollen Sie den Typ des Ziel-Volumes ändern (Basis, einfach/übergreifend, Stripeset, gespiegelt, RAID 0+1, RAID 5). Dies kann durch Löschen des Ziellaufwerks und Erstellung eines neuen Laufwerks auf dem resultierenden 'nicht zugeordneten' Speicherplatz durchgeführt werden.

Acronis Backup & Recovery 10 enthält ein nützliches Disk Management Utility, welches Ihnen die Durchführung der oberen Aktionen ermöglicht (unter einem Betriebssystem oder direkt auf einem fabrikneuen System). Zu weiteren Informationen über Acronis Disk Director Lite siehe den Abschnitt Laufwerksverwaltung (S. 291).

2.9 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 (S. 21). Storage Node gewährleisten einen vollautomatischen Betrieb von Bandbibliotheken und Autoloadern (S. 139).

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.

2.9.1 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	-	-	-	+

2.9.2 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. 119).

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. 430) 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. 418) 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.

2.10 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"

2.11 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.

2.11.1 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. 115)-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. 423) betrachtet. Einmal auf einer verwalteten Maschine erstellt, ist die Zone stets in der Liste **Persönliche Depots** präsent. Zentrale Backup-Pläne (S. 432) können die Acronis Secure Zone ebenso benutzen wie lokale Pläne (S. 427).

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. 165)'.

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.

2.11.2 Acronis Startup Recovery Manager

Eine Modifikation des bootfähigen Agenten (S. 422) 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.

2.11.3 Universal Restore (Acronis Backup & Recovery 10 Universal Restore)

Acronis Backup & Recovery 10 Universal Restore ist eine proprietäre Acronis-Technologie, die Ihnen hilft, Windows auf abweichender Hardware oder einer virtuellen Maschine wiederherzustellen und zu booten. Universal Restore behandelt abweichende Geräte, die kritisch für den Betriebssystemstart sind, wie z.B. Speicher-Controller, Hauptplatine oder Chipsatz.

Verwendungszweck von Acronis Backup & Recovery 10 Universal Restore

Es ist einfach, ein System von einem Festplatten-Backup (Image) auf genau dasselbe System oder auf identische Hardware wiederherzustellen. Wenn Sie jedoch das Motherboard austauschen oder eine andere Prozessor-Version verwenden, was bei einem Hardware-Fehler sehr leicht möglich ist, kann es passieren, dass das wiederhergestellte System nicht mehr bootfähig ist. Ein Versuch, das System auf einen neuen, deutlich leistungsfähigeren Computer zu übertragen, wird normalerweise zum selben, bootunfähigen Ergebnis führen, weil die neue Hardware inkompatibel zu den wichtigsten, im Image enthaltenen Treibern ist.

Auch die Verwendung des Microsoft System Preparation Tool (Sysprep) löst das Problem nicht, weil Sysprep nur die Installation von Treibern für Plug-and-Play-Geräte erlaubt (Soundkarten, Netzwerkadapter, Grafikkarten etc.). Was aber die Treiber für Hardware Abstraction Layer (HAL) und Massenspeichergeräte betrifft, so müssen diese auf dem Quell- und Zielcomputer identisch sein (siehe Microsoft Knowledge Base, Artikel 302577 und 216915).

Die Universal Restore-Technologie bietet eine effiziente Lösung zur hardwareunabhängigen Systemwiederherstellung durch Austausch essentieller Treiber für Hardware Abstraction Layer (HAL) und Massenspeichergeräte.

Universal Restore ist geeignet für:

1. sofortige Wiederherstellung eines ausgefallenen Systems auf abweichender Hardware.
2. Hardware-unabhängiges Klonen und Verteilung von Betriebssystemen
3. Maschinen-Migration physikalisch zu physikalisch, physikalisch zu virtuell und virtuell zu physikalisch.

Die Universal Restore-Prinzipien

1. Automatische Wahl der Treiber für HAL und Massenspeichergeräte

   Universal Restore sucht nach Treibern in von Ihnen spezifizierten Netzwerkordnern, auf Wechselmedien und in den Standardordnern für Treiber auf dem wiederherzustellenden System.

Universal Restore analysiert den Kompatibilitätslevel aller gefundenen Treiber und installiert die Treiber für HAL und Massenspeichergeräte, die am besten für die Ziel-Hardware passen. Auch Treiber für Netzwerkadapter werden gesucht und an das Betriebssystem weitergereicht, welches sie beim ersten Start automatisch installiert.

*Der Standardordner von Windows zum Speichern von Treibern ist im Registry-Wert **DevicePath** hinterlegt, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** gefunden werden kann. Normalerweise lautet dieser Speicherordner „WINDOWS/inf".*

2. Manuelle Wahl des Treibers für Massenspeichergeräte

   Falls die Hardware des Zielcomputers für Festplatten einen speziellen Massenspeichergeräte-Kontroller verwendet (wie SCSI, RAID oder Fibre Channel), so können Sie den passenden Treiber unter Umgehung der automatischen Treiber-Suche-und-Installations-Prozedur manuell installieren.

3. Treiber für Plug-and-Play-Geräte installieren.

   Universal Restore ist auf den eingebauten Plug-and-Play-Erkennungs- und Konfigurationsprozess angewiesen, um Hardware-Unterschiede bei Geräten zu handhaben, die unkritisch für den Systemstart sind, wie etwa Grafik, Audio und USB. Windows übernimmt während der Anmeldephase die Kontrolle über diesen Prozess; sollten dabei einige der neuen Geräte nicht erkannt werden, so bekommen Sie die Chance, die entsprechenden Treiber später manuell zu installieren.

Universal Restore und Microsoft Sysprep

Universal Restore ist kein Tool zur Systemvorbereitung. Sie können es auf jedes Windows-Image anwenden, das durch ein Acronis-Produkt erstellt wurde, inklusive auf Images von Systemen, die mit Microsoft System Preparation Tool (Sysprep) vorbereitet wurden. Nachfolgend ein Beispiel für die Verwendung beider Tools auf demselben System.

Universal Restore entfernt nicht den Security Identifier (SID) und die Benutzerprofil-Einstellungen, um das System ohne Neuverbindung zur Domain oder Neuzuordnung der Netzwerk-Benutzerprofile unmittelbar nach Wiederherstellung ausführen zu können. Wenn Sie vorhaben, die oberen Einstellungen auf einem wiederhergestellten System zu verändern, dann können Sie das System auch mit Sysprep vorbereiten, dann ein Image erstellen und es (sofern benötigt unter Verwendung von Universal Restore) wiederherstellen.

Einschränkungen

Universal Restore ist nicht verfügbar:

- wenn ein Computer über den Acronis Startup Recovery Manager (unter Benutzung von F11) gebootet wurde – oder
- das Backup-Image in der Acronis Secure Zone liegt – oder
- wenn Acronis Active Restore 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.

Universal Restore erwerben

Universal Restore ist kostenlos enthalten in Acronis Backup & Recovery 10 SBS Edition und Acronis Backup & Recovery 10 Advanced Server Virtual Edition.

Universal Restore wird für die anderen Produktausgaben getrennt erworben, hat seine eigene Lizenz

und wird als separate Funktion über eine eigene Setup-Datei installiert. Sie müssen neue bootfähige Medien erstellen, um das neu installierte Add-on auch in der bootfähigen Umgebung einsetzbar zu machen.

2.11.4 Acronis Active Restore

Active Restore ist eine geschützte Acronis-Technologie, die ein System sofort verfügbar macht, nachdem die Wiederherstellung des Systems angefangen hat.

Kunden, die mit Acronis Recovery für Microsoft Exchange vertraut sind, können festhalten, dass hier Active Restore verwendet wird, um eine unmittelbare Verfügbarkeit eines Exchange Informationsspeichers nach Start der Wiederherstellung zu erreichen. Die Wiederherstellung des Informationsspeichers basiert zwar auf der gleichen Technologie, wird aber in einer anderen Art vollzogen als die in diesem Abschnitt beschriebene Wiederherstellung des Betriebssystems.

Unterstützte Betriebssysteme

Acronis Active Restore ist für die Wiederherstellung von Windows (beginnend mit Windows 2000) verfügbar.

Einschränkungen

Der einzig unterstützte Ablageort für Archive ist ein lokales Laufwerk oder um präziser zu sein: jedes über das BIOS der Maschine ansprechbare Gerät. Das kann die Acronis Secure Zone, eine USB-Festplatte, ein USB-Stick oder jede interne Festplatte sein.

So wird dabei vorgegangen

Beim Konfigurieren einer Wiederherstellungsaktion wählen Sie die Laufwerke bzw. Volumes, um diese aus einem Backup wiederherzustellen. Acronis Backup & Recovery 10 scannt die gewählten, im Backup befindlichen Festplatten oder Laufwerke. Findet der Scan dabei ein unterstütztes Betriebssystem, so wird Acronis Active Restore als Option verfügbar.

Sofern Sie die Option nicht aktivieren, erfolgt die System-Wiederherstellung auf die übliche Art und wird die Maschine erst nach vollständiger Wiederherstellung wieder einsatzbereit.

Falls Sie die Option jedoch aktivieren, so wird die nachfolgende Sequenz von Aktionen festgelegt:

Sobald die System-Wiederherstellung gestartet ist, bootet das Betriebssystem aus dem Backup heraus. Die Maschine wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Die für eingehende Anforderungen notwendigen Daten werden mit der höchsten Priorität, alle anderen im Hintergrund wiederhergestellt.

Da die Bedienung solcher Anforderungen simultan zur Wiederherstellung erfolgt, kann das Betriebssystem verlangsamt werden – auch dann, wenn in den Recovery-Optionen die Prozesspriorität auf **Niedrig** eingestellt wurde. Auf diese Art wird die Systemausfallzeit auf Kosten einer temporären Performance-Verschlechterung auf ein Minimum reduziert.

Einsatzszenarien

1. Die Verfügbarkeit eines Systems gehört zu den Effizienzkriterien.

   Beispiele: Client-bezogene Online-Dienste, Web-Einzelhändler, Wahllokale
2. Das Verhältnis von System zu Speicherplatz ist stark in Richtung Speicher verzerrt.

   Einige Maschinen werden als Speicheranlagen genutzt, wobei das Betriebssystem nur ein kleines Speichersegment beansprucht, während der restliche Festplattenplatz der Archivierung dient,

etwa für Videos, Audio- oder andere Multimedia-Dateien. Einige dieser Speicher-Laufwerke können verglichen zum System extrem groß sein, so dass praktisch die komplette Wiederherstellungszeit der Rückgewinnung der Dateien gewidmet wird, obwohl sie erst später gebraucht werden könnten (wenn in naher Zukunft überhaupt).

Entscheiden Sie sich dagegen für Acronis Active Restore, so wird das System in kurzer Zeit wieder einsatzfähig sein. Benutzer werden in die Lage versetzt, benötigte Dateien aus dem Datenspeicher zu öffnen und zu verwenden, während alle restlichen, nicht sofort benötigten Dateien im Hintergrund weiter wiederhergestellt werden.

Beispiele: Datenspeicher für Film- oder Musiksammlungen bzw. Multimedia-Dateien

Anwendung

1. Speichern Sie das Backup des Systemlaufwerks bzw. -volumes an einer Position, auf die über das System-BIOS zugegriffen werden kann. Das kann die Acronis Secure Zone, eine USB-Festplatte, ein USB-Stick oder jede interne Festplatte sein.

   Falls Betriebssystem und Boot-Loader auf unterschiedlichen Partitionen 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.

2. Bootfähiges Medium erstellen.
3. Booten Sie die Maschine mit einem bootfähigen Medium, wenn es zu einem Systemausfall kommt. Starten Sie die Konsole und verbinden Sie sich mit dem bootfähigen Agenten.
4. Konfigurieren Sie die System-Wiederherstellung: Bestimmen Sie die Systemfestplatte bzw. -partition und aktivieren Sie dann das Kontrollkästchen **Acronis Active Restore verwenden**.

   Acronis Active Restore wählt für das Hochfahren und die nachfolgende Wiederherstellung das erste beim Backup-Scan gefundene Betriebssystem. Versuchen Sie nicht, mehr als ein Betriebssystem unter Verwendung von Active Restore wiederherzustellen, damit die Ergebnisse berechenbar bleiben. Wählen Sie auch bei Wiederherstellung eines Multi-Boot-Systems nur jeweils eine System-Partition und Boot-Partition.

5. Sobald die System-Wiederherstellung gestartet ist, bootet das Betriebssystem aus dem Backup heraus. Das Acronis Active Restore-Symbol erscheint im Infobereich der Taskleiste. Die Maschine wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Ein das System sofort benutzender Anwender sieht den Verzeichnisbaum mit seinen Symbolen, kann Dateien öffnen oder Anwendungen starten, selbst wenn diese noch nicht wiederhergestellt wurden.

   Die Acronis Active Restore-Treiber fangen Systemanfragen ab und setzen Dateien, die zur Erfüllung der einkommenden Anfrage notwendig sind, auf höchste Wiederherstellungspriorität. Und während diese „on-the-fly“-Wiederherstellung fortschreitet, wird der anhaltende Wiederherstellungsprozess in den Hintergrund transferiert.

   Solange die Recovery-Aktion nicht abgeschlossen ist, sollten Sie nicht versuchen, die Maschine herunterzufahren oder einen Neustart durchzuführen. Falls Sie Ihr Maschine ausschalten, gehen alle seit dem letzten Systemstart durchgeführten Änderungen verloren. Das System wird dann nicht wiederhergestellt, auch nicht partiell. Die einzig verbliebene Lösung in diesem Fall ist es dann, den Wiederherstellungsprozess von einem bootfähigen Medium aus neu zu starten.

6. Die Hintergrund-Wiederherstellung geht solange weiter, bis alle gewählten Laufwerke wiederhergestellt wurden, alle Ereignismeldungen gemacht wurden und das Acronis Active Restore-Symbol aus dem Infobereich der Taskleiste verschwindet.

2.12 Zentrale Verwaltung verstehen

Dieser Abschnitt enthält einen Überblick über die zentrale Datensicherung mit Acronis Backup & Recovery 10. Bevor Sie diesen Abschnitt lesen, sollten Sie wissen, wie Daten auf einer einzelnen

Maschine geschützt werden (S. 28).

2.12.1 Grundlegende Konzepte

Backup-Richtlinien anwenden und ihre Ausführung verfolgen

Zum Schutz der Daten einer einzelnen Maschine installieren Sie auf dieser einen Agenten (S. 419) oder multiple Agenten für verschiedene, zu schützende Daten-Typen. Sie verbinden die Konsole mit der Maschine und erstellen einen Backup-Plan (S. 420) oder multiple Backup-Pläne.

Was, wenn Sie mehrere hundert Maschinen zu verwalten haben? Die Erstellung eines Backup-Plans auf jeder Maschine benötigt Zeit, wobei die Pläne an sich ziemlich gleich sein können – etwa, wenn Sie das System-Laufwerk und die Benutzerdokumente sichern müssen. Genauso zeitaufwendig ist die separate Verfolgung der Plan-Ausführung auf jeder Maschine.

Um die Verwaltungsaktionen auf multiple Maschinen zu übertragen, installieren Sie den Acronis Backup & Recovery 10 Management Server (S. 427) und registrieren (S. 428) dann die Maschinen auf diesem Server. Danach können Sie Maschinen-Gruppen erstellen und so multiple Maschinen als Ganzes verwalten. Sie können alle oder eine Auswahl von Maschinen schützen, indem Sie einen gemeinsamen Backup-Plan aufsetzen, der Backup-Richtlinie (S. 420) genannt wird.

Sobald Sie die Richtlinie auf eine Gruppe von Maschinen anwenden, verteilt der Management Server diese Richtlinie zu jeder einzelnen dieser Maschinen. Die Agenten finden auf jeder Maschine die zu sichernden Elemente und erstellen korrespondierende zentrale Backup-Pläne (S. 432). Sie können die jeweiligen Zustände der Richtlinien auf einem Bildschirm überwachen und, sofern benötigt, zu jeder Maschine, jedem Plan oder Task navigieren, um den entsprechenden Status und die Log-Einträge einzusehen. Der Management Server ermöglicht außerdem, lokal hervorgebrachte Aktivitäten des Agenten zu überwachen und zu verwalten.

Da Sie die Konsole eher mit dem Management Server als mit jeder Maschine verbinden und Sie alle Verwaltungsaktionen durch die zentrale Verwaltungseinheit ausführen, wird diese Art von Verwaltung zentrale Verwaltung (S. 432) genannt.

Eine zentrale Verwaltung schließt nicht die direkte Verwaltung (S. 424) jeder einzelnen Maschine aus. Sie können die Konsole mit jeder Maschine verbinden und jede direkte Verwaltungsaktion durchführen. Zentrale Backup-Pläne können jedoch nur durch den Management Server verwaltet werden, da eine gut durchdachte Richtlinie automatisch funktioniert und nur selten einen menschlichen Eingriff benötigt.

Mit Hilfe des Management Servers können Sie einen oder mehrere zentrale Archiv-Speicher erstellen (zentrale Depots (S. 433)), die von den registrierten Maschinen gemeinsam benutzt werden. Ein zentrales Depot kann von jeder Backup-Richtlinie wie auch von jedem Backup-Plan (der auf der registrierten Maschine durch direkte Verwaltung erstellt wurde) verwendet werden.

Einen verwalteten Archiv-Speicher organisieren

Wie groß sollte die Kapazität des zentralen Depots sein? Was, wenn die Übertragung beträchtlicher Backups zum Depot einen Stau im Netzwerk verursacht? Beeinträchtigt das Backup eines in Betrieb befindlichen Produktionsservers seine Performance? Um sicherzustellen, dass das zentrale Backup keine Geschäftsprozesse der Firma ausbremst und um die zum Schutz der Daten benötigten Ressourcen zu minimieren, installieren Sie einen Acronis Backup & Recovery 10 Storage Node (S. 429) und konfigurieren ihn zur Verwaltung eines oder multipler zentraler Depots. Solche Depots werden verwaltete Depots (S. 431) genannt.

Der Storage Node hilft dem Agenten, Backups vor Übertragung zu verwalteten Depots zu

deduplizieren (S. 423) und dedupliziert selbst bereits in den Depots liegende Backups. Deduplizierung führt zu verringertem Backup-Traffic und spart Speicherplatz. Der Storage Node unternimmt außerdem mit Archiven eigene Aktionen (wie Validierung oder Bereinigung), welche ansonsten durch den Agenten ausgeführt werden und befreit so die verwalteten Maschinen von unnötiger Rechenlast. Und nicht zuletzt ermöglicht der Acronis Backup & Recovery 10 Storage Node die Verwendung einer Bandbibliothek als verwaltetes Depot für die Speicherung von Backup-Archiven.

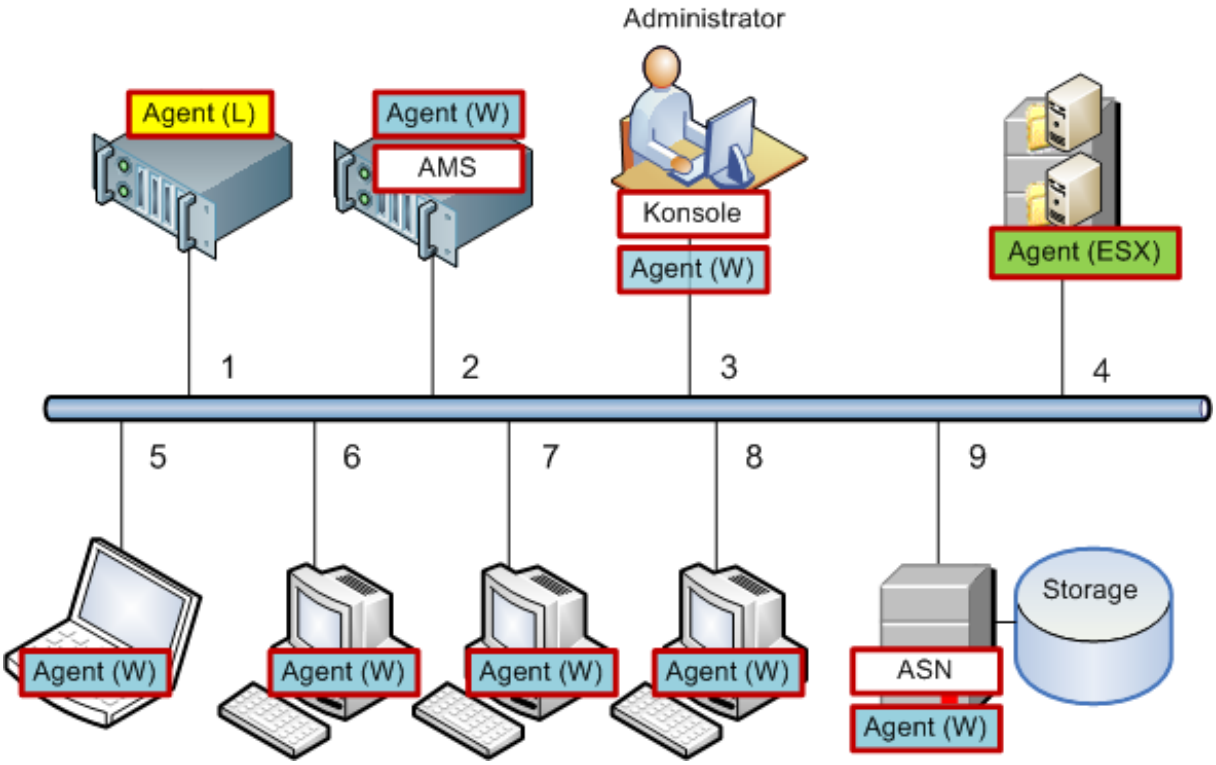
Sie können mehr als einen Storage Node, von denen jeder etliche Depots verwaltet, aufsetzen und zentral vom Acronis Backup & Recovery 10 Management Server aus steuern.

Zu detaillierten Informationen über Storage Nodes siehe Acronis Backup & Recovery 10 Storage Node (S. 21).

2.12.2 Zentrale Datensicherung in einem heterogenen Netzwerk einrichten

Angenommen, Ihre Netzwerk-Infrastruktur beinhaltet Server (1, 2, 9) und Workstations (3, 5-8), die mit Windows und Linux laufen. Sie verfügen außerdem über einen VMware ESX-Server (4), der zwei Gast-Systeme hostet.

Sie müssen nun jeden Server als Ganzes schützen, die Benutzerdaten auf den Workstations und den virtuellen Maschinen. Sie wollen den Zustand der Datensicherung verfolgen können, sicherstellen, dass die Backup-Archive keine doppelten Informationen speichern und dass veraltete Backups auf Zeitbasis aus dem Speicher gelöscht werden. Diese Ziele lassen sich durch regelmäßiges Backup der gewünschten Daten-Elemente in ein zentrales Depot mit Deduplizierung erreichen.



Die Acronis-Infrastruktur einrichten

1. Installieren Sie die Acronis Backup & Recovery 10 Management Console **[Konsole]** auf der Maschine, von der aus Sie bevorzugt arbeiten **(3)**. Die Konsole ermöglicht Ihnen, über eine

grafische Benutzeroberfläche (GUI) auf andere Acronis-Komponenten zuzugreifen und diese zu verwalten.

2. Installieren Sie den Acronis Backup & Recovery 10 Management Server **[AMS]** auf einem der Windows Server **(2)**. Der Management Server ist Ihre Einstiegsstelle zur Acronis-Infrastruktur.
3. Installieren Sie den Acronis Backup & Recovery 10 Agenten auf jeder Maschine, auf der Sie Festplatten, Partitionen oder Dateien per Backup sichern wollen.
   - **Agent (W)** – Agent für Windows
   - **Agent (L)** – Agent für Linux.

   Registrieren Sie jede Maschine auf dem Management Server, wenn Sie die Agenten installieren. Um dies zu tun, geben Sie Namen oder IP-Adresse des Servers sowie die Anmeldedaten des Server-Administrators in das entsprechende Fenster des Installationsassistenten ein. Alternativ können Sie die Maschinen auch später unter Verwendung ihrer Namen oder IP-Adressen dem Management Server hinzufügen
4. Installieren Sie Acronis Backup & Recovery 10 Agent für ESX/ESXi **[Agent (ESX)]** auf dem ESX-Server **(4)**, um die virtuellen Maschinen vom Host aus per Backup zu sichern. Der Agent wird als eine „Virtual Appliance“ ausgeliefert.
5. Installieren Sie den Acronis Backup & Recovery 10 Storage Node **[ASN]** auf einem der Windows Server **(9)**. Der Storage Node ermöglicht Ihnen, die Infrastruktur zum Speichern von Backup-Archiven zu organisieren und die Funktion Deduplizierung zu verwenden. Der Storage Node kann gemeinsam mit dem Management Server installiert werden, sofern der Host leistungsfähig genug ist.

   Registrieren Sie den Storage Node auf dem Management Server auf dieselbe Art wie die Agenten, wenn Sie ihn installieren.

Installationstipps

- AMS (Management Server) und ASN (Storage Node) können beide auch auf einem Workstation-Betriebssystem installiert werden.
- In einem Netzwerk können multiple Storage Nodes vorhanden sein. Jeder dieser Storage Nodes kann bis zu 20 lokale oder Remote-Depots verwalten.
- Auf einer Maschine können mehrere Acronis Backup & Recovery 10-Komponenten mit einer einzigen Installationsprozedur aufgespielt werden.
- Sie können die Komponenten in einer Active Directory-Domain durch Verwendung der Gruppenrichtlinie verteilen.

Den Storage Node einrichten

Stellen Sie vor Verwendung des Storage Nodes sicher, dass alle Benutzer, die zu den Depots des Knotens ein Backup durchführen werden, auf dem Storage Node auch ein Windows-Benutzerkonto haben.

- Falls der Storage Node in eine Active Directory-Domain eingebunden ist, können alle Benutzer der Domain zum Storage Node Backups durchführen – und alle Domain-Administratoren werden zu Storage Node-Administratoren.
- Erstellen Sie in einer Arbeitsgruppe ein lokales Benutzerkonto für jeden Benutzer, der sein Backup zum Storage Node durchführen wird. Mitglieder der Gruppe Administratoren werden auch Administratoren des Storage Nodes. Sie können auch später noch weitere, benötigte Benutzerkonten hinzufügen.

1. Führen Sie die Konsole aus und verbinden Sie sich zum Management Server.
2. Erstellen Sie, wie unter Aktionen mit zentralen Depots (S. 133) beschrieben, ein verwaltetes Depot. Aktivieren Sie die Deduplizierung, wenn Sie das verwaltete Depot erstellen.

Gruppen und Richtlinien einrichten

Eine ausführliche Erläuterung, wann und warum Sie Maschinen in Gruppen organisieren müssen, können Sie im Abschnitt Registrierte Maschinen gruppieren (S. 62) finden. Hier finden Sie nun einige Szenarien erläutert, die durch die zuvor genannte Acronis Backup & Recovery 10-Implementation unterstützt werden.

Server schützen

Sie werden höchstwahrscheinlich auf jedem der Server (abhängig von ihren Rollen) individuelle Backup-Pläne erstellen. Es ist jedoch notwendig, zumindest einmal ein Voll-Backup des gesamten Servers durchzuführen. Wahrscheinlich wollen Sie ein Backup des Servers vor Wartungsarbeiten durchführen, nach Installation oder Aktualisierung von Software, vor einem Standortumzug oder Ähnlichem. In unserem Beispiel gibt es jedoch keine Notwendigkeit, regelmäßig den gesamten Server zu sichern. Sie können veraltete Backups manuell löschen, da diese nicht sehr zahlreich sind.

1. Erstellen Sie eine Richtlinie, um **[Alle Laufwerke]** per Backup in das verwaltete Depot des Storage Nodes zu sichern. Sie wählen **Backup später ausführen**, den manuellen Start und dann als Backup-Typ **Voll**.
2. Erstellen Sie einen statischen Gruppennamen, z.B. S_1. Fügen Sie dieser Gruppe alle Server hinzu. (Ein Storage Node kann für den Fall hinzugefügt werden, dass sich das verwaltete Depot nicht auf den lokalen Festplatten des Storage Nodes befindet. Anderenfalls wird der Archiv-Speicher per Backup zu sich selbst gesichert.)
3. Wenden Sie die Richtlinie auf die Gruppe S_1 an. Stellen Sie sicher, dass die Richtlinie erfolgreich an jeden der Server verteilt wurde. Das Stadium Richtlinien-Deployments muss sich von **Wird Verteilt** zu **Verteilt** ändern und der Status muss **OK** sein. So können Sie die resultierenden Backup-Pläne auf jedem der Server einsehen:
   a. Navigieren Sie zur Gruppe **Alle Maschinen** oder zur Gruppe S_1.
   b. Wählen Sie den Server.
   c. Wählen Sie die Registerlasche **Backup-Pläne und Tasks** in der Leiste **Informationen**.

Wenn Sie die Gelegenheit brauchen und haben, einen der Server zu sichern, so navigieren Sie wie eben beschrieben zum Backup-Plan, wählen diesen und führen ihn aus.

Workstations schützen

So setzen Sie die am häufigsten verwendete Planung auf: wöchentliches vollständiges und tägliches inkrementelles Backup der Standardordner für Dokumente der Benutzer. Zusätzlich werden Sie nur die Backups der letzten 7 Tage behalten.

1. Erstellen Sie eine Richtlinie, um **[Alle Benutzerprofil-Ordner]** per Backup in das verwaltete Depot des Storage Nodes zu sichern. Das bewirkt ein Backup des Ordners, in dem die Benutzerprofile liegen (z.B. „C:\Dokumente und Einstellungen“ in Windows XP). Wählen Sie das Backup-Schema **Benutzerdefiniert**.
   a. Planen Sie die vollständigen Backups wie folgt: **Wöchentlich**, jede Woche an: Sonntag, Task-Ausführung einmal um 00:00 Uhr (Mitternacht). Erweiterte Einstellungen: Wake-on-LAN: An. Möglicherweise möchten Sie auch die Startzeit des Backups innerhalb eines Zeitfensters verteilen, um die Netzwerknutzung und CPU-Belastung des Storage Nodes zu optimieren.
   b. Planen Sie die inkrementellen Backups wie folgt: **Wöchentlich**, jede Woche an: Wochentags, Task-Ausführung einmal um 20:00 Uhr. Konfigurieren Sie außerdem wie benötigt die erweiterten Einstellungen.
   c. Konfigurieren Sie die Aufbewahrungsregeln wie folgt: **Lösche Backups älter als**: 7 Tage. **Beim Löschen eines Backups, das Abhängigkeiten hat:** Backups konsolidieren. Belassen Sie die

verbliebenen Aufbewahrungsregeln in den Standardeinstellungen. In **Aufbewahrungsregeln verwenden**, aktivieren Sie **Nach dem Backup**.

2. Erstellen Sie eine dynamische Gruppe, z.B. mit der Bezeichnung W_1. Spezifizieren Sie **%Windows%XP%** und **%Windows%Vista%** als Kriterium. Auf diese Weise wird jede später auf dem Management Server registrierte Workstation der Gruppe hinzugefügt und durch dieselbe Richtlinie geschützt.
3. Wenden Sie die Richtlinie auf die Gruppe W_1 an. Stellen Sie sicher, dass die Richtlinie erfolgreich an jede der Workstations verteilt wurde. Das Stadium Richtlinien-Deployments muss sich von **Wird Verteilt** zu **Verteilt** ändern und der Status muss **OK** sein. So können Sie die resultierenden Backup-Pläne auf jeder Workstation einsehen:
   a. Navigieren Sie zur Gruppe **Alle Maschinen** oder zur Gruppe W_1.
   b. Wählen Sie die Workstation.
   c. Wählen Sie die Registerlasche **Backup-Pläne und Tasks** in der Leiste **Informationen**.

   Sie können die resultierenden, auf den Workstations erstellten Tasks außerdem in der Ansicht **Tasks** einsehen.
4. Verwenden Sie das **Dashboard** oder die Ansicht **Tasks**, um die täglichen, auf die Richtlinie bezogenen Aktivitäten zu verfolgen. Sobald Sie sich vergewissert haben, dass alle Tasks wie spezifiziert laufen, können Sie sich auf die Überprüfung des Richtlinienstatus in der Ansicht **Backup-Richtlinien** beschränken.

Sie können außerdem die Backup-Schemata „GVS“ oder „Türme von Hanoi“ verwenden, um Daten auf täglicher Basis zu schützen.

Virtuelle Maschinen schützen

Der Acronis Backup & Recovery 10 Agent für ESX/ESXi bietet eine hohe Flexibilität, um virtuelle Maschinen auf verschiedene Arten zu schützen:

- Verbinden Sie die Konsole mit der „Virtual Appliance“ (Agent für ESX/ESXi) und erstellen Sie einen Backup-Plan, der alle oder einige der virtuellen Maschinen sichert.
- Verbinden Sie die Konsole mit der „Virtual Appliance“ (Agent für ESX/ESXi) und erstellen Sie einen individuellen Backup-Plan für jede Maschine. Der Plan wird dann die von Ihnen spezifizierten Laufwerke per Backup sichern.
- Registrieren Sie die „Virtual Appliance“ (Agent für ESX/ESXi) auf dem Management Server. Alle virtuellen Maschinen, mit Ausnahme der „Virtual Appliance“, erscheinen in der Gruppe **Alle virtuellen Maschinen**. Sie können diese Maschinen gruppieren und jede Richtlinie auf diese anwenden, die Festplatten oder Partitionen sichert.
- Installieren Sie den Agenten für Windows oder den Agenten für Linux auf jeder virtuellen Maschine. Registrieren Sie die Maschinen auf dem Management Server. Die Maschinen werden als physikalische Maschinen betrachtet. Sie können eine Backup-Richtlinie auf diese Maschinen anwenden oder auf jeder Maschine einen Backup-Plan separat erstellen. Wenn auf eine der Maschinen ein Mitgliedschafts-Kriterium zutrifft, welches für eine dynamische Gruppe aus physikalischen Maschinen definiert wurde, dann wird die Maschine durch die Richtlinie, die auf diese Gruppe angewendet wird, ebenfalls geschützt.

Andere erweiterte Produkt-Editionen als die „Virtual Edition“ (nämlich Acronis Backup & Recovery 10 Advanced Server, Advanced Server SBS Edition und Advanced Workstation) ermöglichen es nur, die letzte der oberen Methoden zu verwenden.

2.12.3 Registrierte Maschinen gruppieren

Sobald eine Maschine am Management Server registriert (S. 428) wurde, erscheint sie in der integrierten Gruppe (S. 428) **Alle Maschinen**. Indem Sie eine Backup-Richtlinie auf diese Gruppe anwenden, schützen Sie alle registrierten Maschinen. Die Sachlage ist jedoch so, dass eine einzelne Richtlinie aufgrund der unterschiedlichen Aufgaben der Maschinen nicht ausreichend sein kann. Die zu sichernden Daten sind spezifisch für jede Abteilung, manche Daten müssen häufig erfasst werden, andere vielleicht nur zweimal im Jahr; von daher werden Sie wohl verschiedene Richtlinien für diverse Arten von Maschinen erstellen. In diesem Fall sollten Sie die Erstellung benutzerdefinierter Gruppen erwägen.

2.12.4 Richtlinien für Maschinen und Gruppen

Dieser Abschnitt hilft Ihnen, vom Management Server durchgeführte Aktionen (wie automatisches Deployment und widerrufene Richtlinien) besser zu verstehen, wenn also einzelne oder eine Vielzahl von Richtlinien auf Maschinen und verschachtelte Maschinengruppen angewendet werden; wenn eine Richtlinie von Maschinen und Gruppen widerrufen wird oder wenn eine Maschine oder Gruppe von einer Gruppe zu einer anderen verschoben wird.

Werden Backup-Richtlinien auf Gruppen angewendet, so führt das zur Anpassung der Richtlinien auf jedem Mitglied (jeder Maschine) dieser Gruppe. Bei jeder Hierarchie-Änderung (z.B. Verschieben, Entfernen, Erstellen von Gruppen, Hinzufügen von Maschinen zu statischen Gruppen oder wenn Maschinen einer Gruppe basierend auf dynamischen Kriterien beitreten) kann es zu einer großen Zahl von „Vererbungsänderungen“ kommen. Machen Sie sich mit diesem Abschnitt vertraut, um sicherzustellen, dass Ihre Aktionen zu den von Ihnen gewünschten Ergebnissen führen und um das Ergebnis automatisierter Aktionen durch den Acronis Backup & Recovery 10 Management Server besser zu verstehen.

Anwenden, Verteilen und Widerrufen

Anwenden – eine Richtlinie erstellt eine Korrespondenz zwischen der Richtlinie und einer oder mehreren Maschinen. Dieser Prozess findet innerhalb der Datenbank des Management Servers statt und benötigt nur wenig Zeit.

Verteilen – eine Richtlinie überträgt die eingerichtete Korrespondenz zu den Maschinen. Physikalisch gesehen wird auf jeder Maschine ein Bündel von Tasks erstellt, entsprechend der durch die Richtlinie vermittelten Konfiguration.

Widerrufen einer Richtlinie ist die umgekehrte Aktion zur Summe aus Anwenden und Verteilen. Widerrufen entfernt die Korrespondenz zwischen der Richtlinie und einer bzw. mehreren Maschinen und entfernt die Tasks von den Maschinen.

Sollte eine Maschine momentan nicht benutzbar bzw. nicht erreichbar sein, so werden die Veränderungen auf der Maschine verbreitet, sobald sie wieder verfügbar wird. Das Verteilen einer Richtlinie an multiple Maschinen wird also einige Zeit dauern. Dasselbe gilt auch für das Widerrufen. Diese beiden Prozesse können langlebig sein, so dass der Management Server den Status jeder Maschine verfolgt und anzeigt, mit der er arbeitet, wie auch den kumulativen Status der Richtlinie.

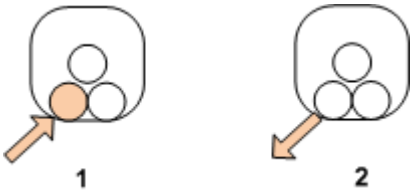
Eine Richtlinie für eine Maschine oder eine Gruppe

Im Diagramm verdeutlicht jedes nummerierte Schema das Ergebnis der entsprechend nummerierten Aktion.

Der Container steht für eine Gruppe; der farbige Kreis steht für eine Maschine mit angewendeter

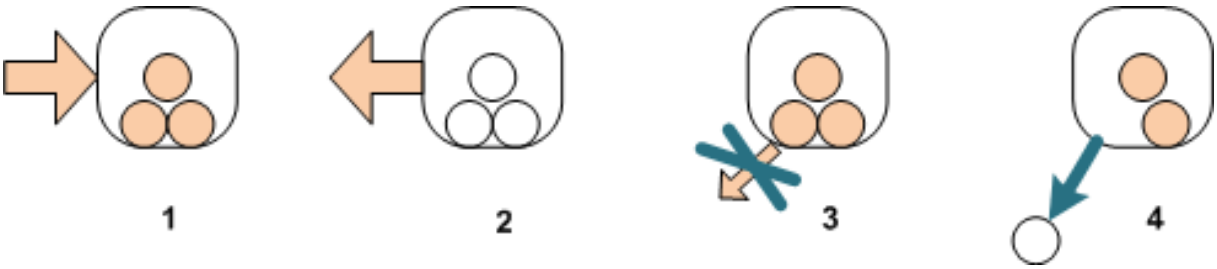
Richtlinie; der dunkel gefärbte Kreis steht für eine Maschine mit zwei Anwendungen derselben Richtlinie; der weiße Kreis steht für eine Maschine, auf die keine Richtlinie angewendet wird.

Richtlinie für eine Maschine



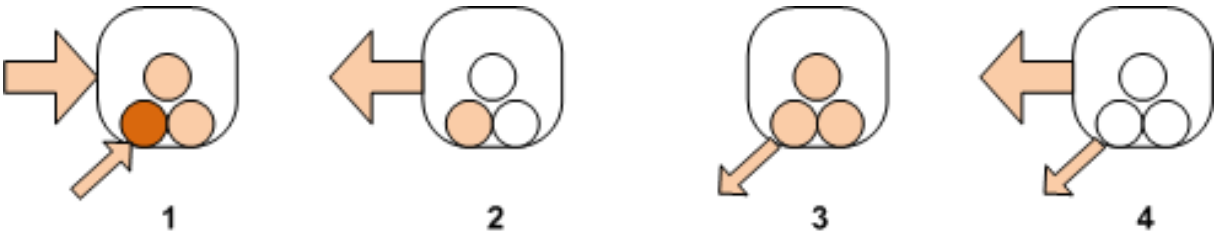
1. Eine Richtlinie kann auf eine Maschine angewendet werden.
2. Eine Richtlinie kann von einer Maschine widerrufen werden.

Richtlinie für eine Gruppe



1. Eine Richtlinie kann auf eine Gruppe angewendet werden.
2. Eine Richtlinie kann von einer Gruppe widerrufen werden.
3. Eine auf eine Gruppe angewendete Richtlinie kann nicht von einer Maschine widerrufen werden.
4. Entfernen Sie die Maschine von der Gruppe, um die Richtlinie von der Maschine zu widerrufen.

Die gleiche Richtlinie für eine Gruppe und eine Maschine



1. Die gleiche Richtlinie kann auf eine Gruppe und auf eine Maschine angewendet werden. Auf der Maschine ändert sich bei zweiter Anwendung derselben Richtlinie nichts, aber der Server merkt sich, dass die Richtlinie zweimal angewendet wurde.
2. Eine von einer Gruppe widerrufene Richtlinie verbleibt jedoch auf der Maschine.
3. Eine von der Maschine widerrufene Richtlinie verbleibt auf der Gruppe und daher auch auf der Maschine.
4. Um die Richtlinie vollständig von der Maschine zu widerrufen, widerrufen Sie sie von beiden, der Gruppe und der Maschine.

Aktionen mit einer Maschine

Dieser Abschnitt beschreibt vereinfacht, was mit den Richtlinien für eine Maschine passiert, wenn die Maschine von einer Gruppe verschoben, kopiert oder gelöscht wird.

Im Diagramm steht der Container für eine Gruppe; der einfarbige Kreis steht für eine Maschine mit einer angewendeten Richtlinie; der zweifarbige Kreis steht für eine Maschine mit zwei angewendeten

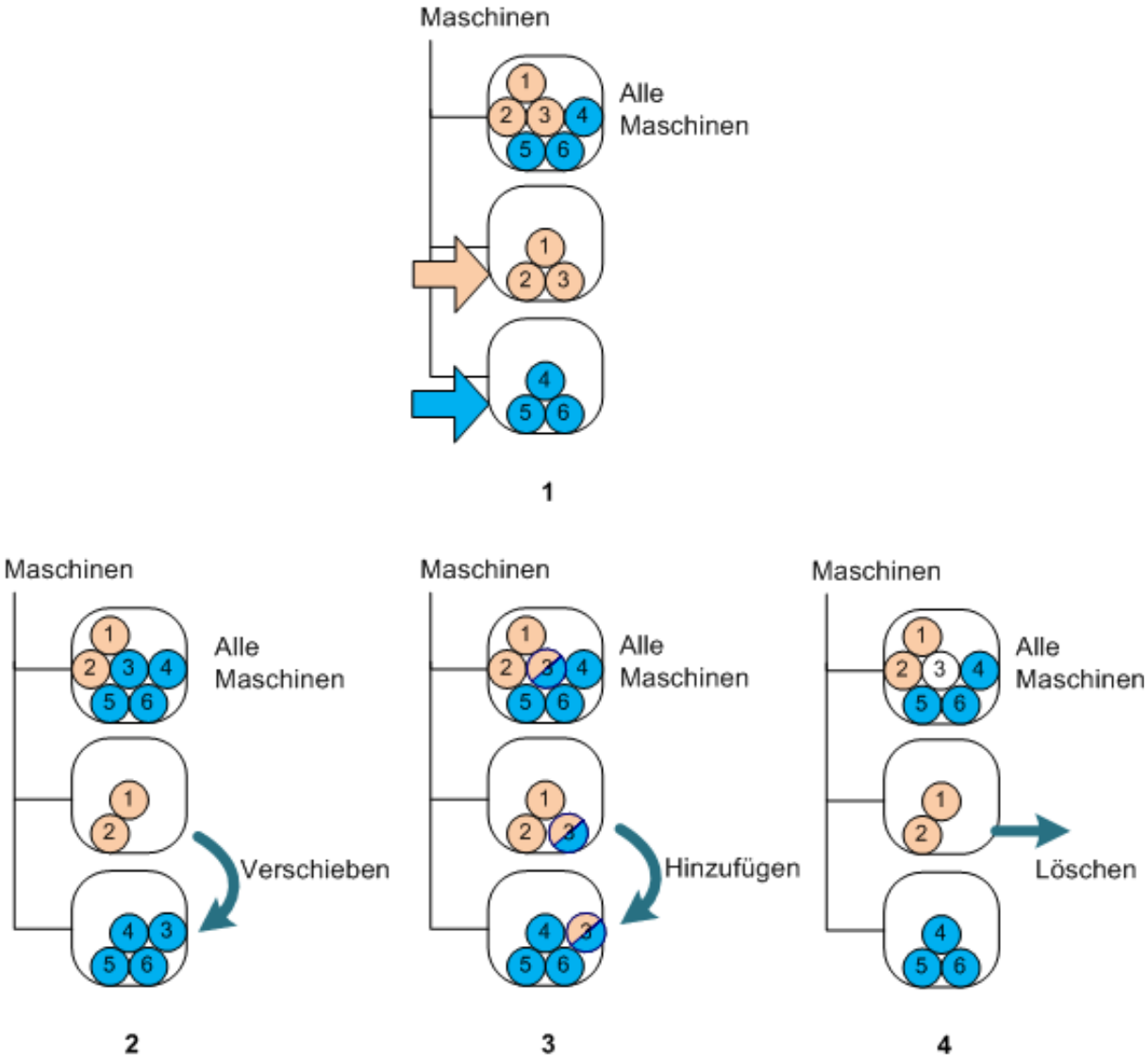
Richtlinien; der weiße Kreis steht für eine Maschine ohne angewendete Richtlinie.

1. Der anfängliche Zustand: Zwei benutzerdefinierte Gruppen enthalten unterschiedliche Maschinen. Eine Richtlinie wird auf die eine Gruppe angewendet, eine andere Richtlinie auf eine weitere Gruppe. Das nächste Schema verdeutlicht die Ergebnisse der angegebenen Aktionen.

2. **Verschieben zu Gruppe:** Maschine Nr. 3 wird von einer Gruppe zu einer anderen verschoben. Die „orangefarbene“ Richtlinie wird widerrufen, die „blaue“ Richtlinie wird auf die Maschine angewendet.

3. **Zu anderer Gruppe hinzufügen**: Maschine Nr. 3 wird einer anderen Gruppe hinzugefügt. Sie wird Mitglied beider Gruppen. Die „blaue“ Richtlinie wird angewendet, aber die „orangefarbene“ Richtlinie verbleibt auf der Maschine.

4. **Entfernen aus der Gruppe**: Maschine Nr. 3 wird aus der Gruppe entfernt. Die „orangefarbene“ Richtlinie wird von der Maschine widerrufen. Die Maschine verbleibt in der Gruppe **Alle Maschinen**.

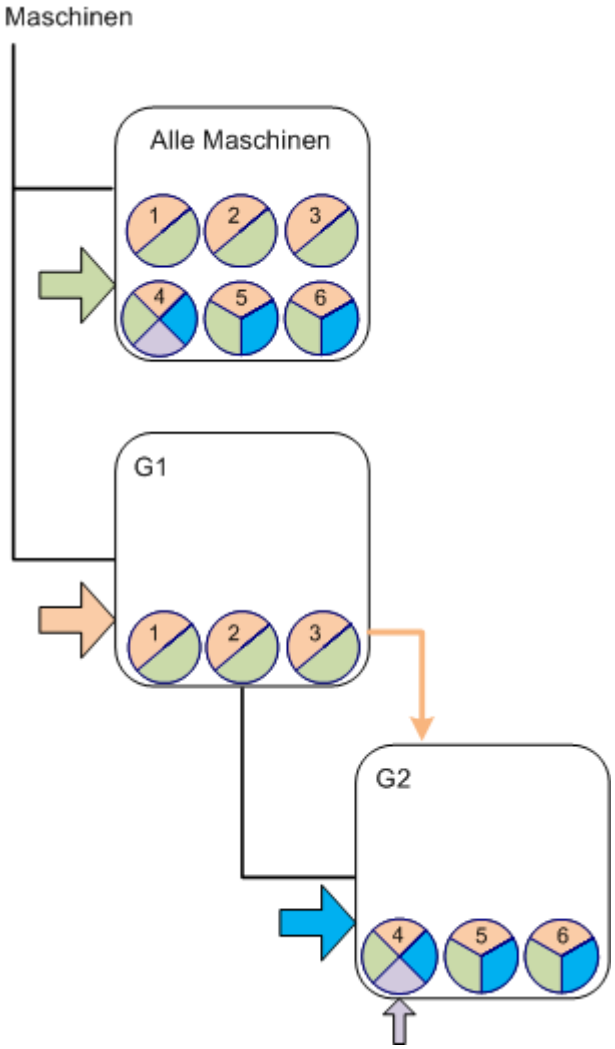


Vererbung von Richtlinien

Richtlinien-Vererbung ist einfach zu verstehen, wenn wir annehmen, dass eine Maschine nur Mitglied einer Gruppe sein kann – mit Ausnahme der Gruppe **Alle Maschinen**. Beginnen wir mit diesem

vereinfachten Denkansatz.

Im unteren Diagramm steht der Container für eine Gruppe; der zweifarbige Kreis steht für eine Maschine mit zwei angewendeten Richtlinien; der dreifarbige Kreis steht für eine Maschine mit drei angewendeten Richtlinien und so weiter.



Abgesehen von der Gruppe **Alle Maschinen** haben wir die benutzerdefinierte Gruppe G1 an der Wurzel und die benutzerdefinierte Gruppe G2, welche das „Kind“ von G1 ist.

Die „grüne“ Richtlinie, angewendet auf die Gruppe **Alle Maschinen**, wird auf alle Maschinen vererbt.

Die „orangefarbene“ Richtlinie, angewendet auf G1, wird von allen G1-Mitgliedern und auch all ihren Untergruppen geerbt, gleichermaßen unmittelbar wie indirekt.

Die „blaue“ Richtlinie, angewendet auf G2, wird nur von den G2-Mitgliedern geerbt, da G2 keine Untergruppen hat.

Die „violette“ Richtlinie wird direkt auf Maschine Nr. 4 angewendet. Sie wird auf Maschine Nr. 4 ungeachtet einer Mitgliedschaft der Maschine in einer Gruppe existieren.

Angenommen, wir erstellen die Gruppe G3 auf der Wurzelebene. Falls auf die Gruppe keine Richtlinie angewendet wird, sollen all ihre Mitglieder als „grün“ eingestuft werden. Wird nun z.B. Maschine Nr. 1 zu Gruppe G3 hinzugefügt, so wird diese Maschine die „orangefarbene“ und die „grüne“ Richtlinie tragen, ungeachtet der Tatsache, dass G3 nichts mit der „orangefarbenen“ Richtlinie zu tun hat.

Das erklärt, warum es schwierig ist, die Vererbung von Richtlinien von der Spitze der Hierarchie aus zu verfolgen, wenn dieselbe Maschine in mehreren Gruppen enthalten ist.

In der Praxis ist es wesentlich einfacher, die Vererbung von der Maschinen-Seite aus zu betrachten. Zur Umsetzung navigieren Sie zu einer die Maschine enthaltenen Gruppe, wählen dort diese Maschine und wechseln anschließend zur Registerlasche **Backup-Richtlinien** in der **Informations**-Leiste. Die Spalte **Vererbung** zeigt, ob eine Richtlinie geerbt wurde oder direkt auf die Maschine angewendet wird. Klicken Sie auf **Vererbung durchsuchen**, um die Vererbungsabfolge der Richtlinie einzusehen. In unserem Beispiel sind die Richtlinien-Namen, die **Vererbungs**-Spalte und die Vererbungsabfolge folgendermaßen:

Für Maschine	**Richtlinie**	**Vererbung**	**Vererbungsabfolge**

Nr. 1 oder Nr. 2 oder Nr. 3	„grün“	Geerbt	Alle Maschinen -> Nr. 1 oder Nr. 2 oder Nr. 3
	„orangefarben“	Geerbt	G1 -> Nr. 1 oder Nr. 2 oder Nr. 3
#4	„grün“	Geerbt	Alle Maschinen -> Nr. 4
	„orangefarben“	Geerbt	G1 -> G2 -> Nr. 4
	„blau“	Geerbt	G2 -> Nr. 4
	„violett“	Direkt angewendet	
Nr. 5 oder Nr. 6	„grün“	Geerbt	Alle Maschinen -> Nr. 5 oder Nr. 6
	„orangefarben“	Geerbt	G1 -> G2 -> Nr. 5 oder Nr. 6
	„blau“	Geerbt	G2 -> Nr. 5 oder Nr. 6

2.12.5 Stadien und Status von Backup-Richtlinien

Mit zentraler Verwaltung kann der Administrator über einfache Parameter den Zustand der gesamten IT-Infrastruktur überwachen. Stadium und Status einer Backup-Richtlinie sind ebenfalls in solchen Parametern enthalten. Probleme erscheinen, wenn überhaupt, auf der untersten Basis der Infrastruktur (Tasks auf verwalteten Maschinen) im kumulativen Richtlinien-Status. Der Administrator kann den Status auf einen Blick überprüfen. Sollte der Status nicht OK sein, so kann der Administrator mit einigen Klicks in die Problemdetails navigieren.

Dieser Abschnitt hilft Ihnen, die vom Management Server angezeigten Stadien und Statusmeldungen der Richtlinien zu verstehen.

Stadien des Richtlinien-Deployments auf einer Maschine

Um diesen Parameter einzusehen, wählen Sie im Verzeichnisbaum eine die Maschine enthaltene Gruppe, dann die Maschine selbst und darauf die Registerlasche **Backup-Richtlinien** in der Leiste **Informationen**.

Sobald Sie eine Richtlinie auf eine Maschine oder Gruppe von Maschinen anwenden, verteilt der Server die Richtlinie an diese Maschinen. Auf jeder dieser Maschinen erstellt der Agent dann einen Backup-Plan. Während die Richtlinie zur Maschine übertragen und der Backup-Plan erstellt wird, ist das Stadium des Richtlinien-Deployments auf der Maschine **Wird verteilt**.

Sobald der Backup-Plan erfolgreich erstellt wurde, wird das Richtlinien-Stadium der Maschine **Verteilt**.

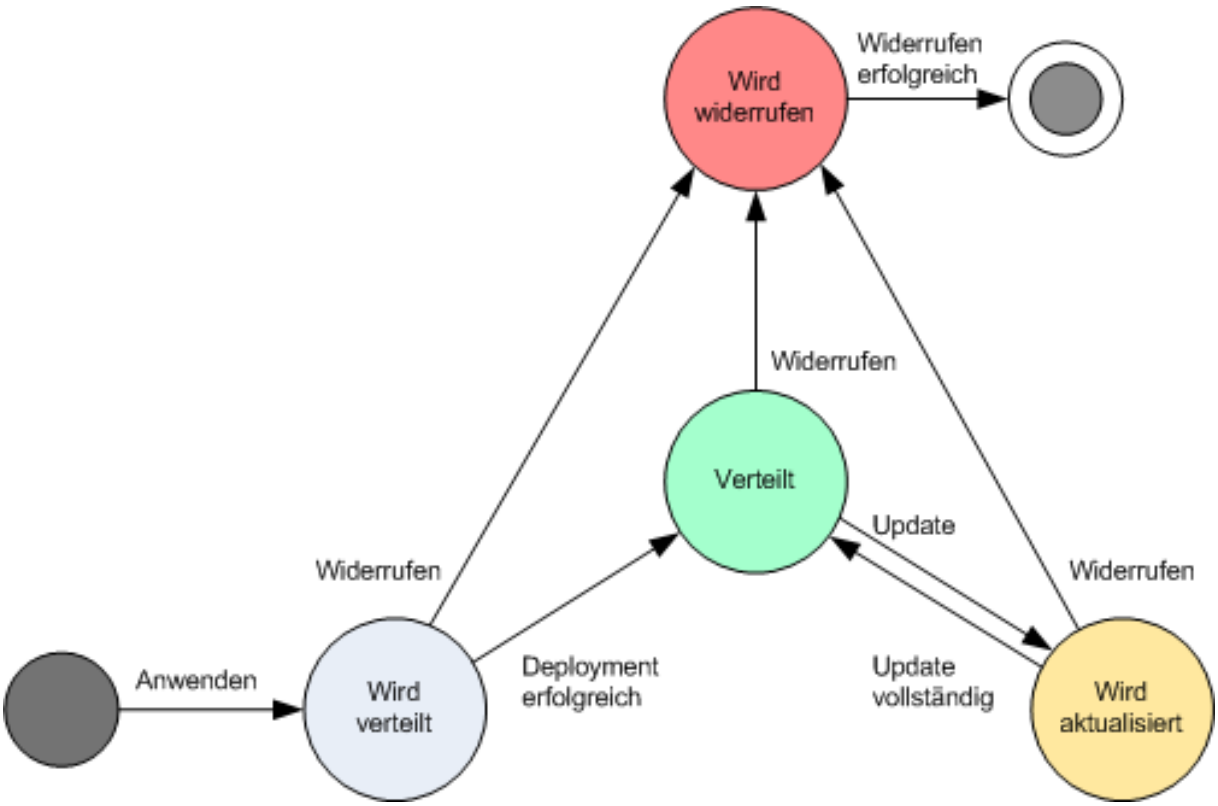
Unter bestimmten Umständen kann es notwendig sein, die Richtlinie anzupassen. Durch Bestätigung der Änderungen aktualisiert der Management Server die Richtlinie auf allen Maschinen, auf die sie verteilt wurde. Während die Änderungen zu den Maschinen übertragen werden und der Agent den Backup-Plan aktualisiert, ist das Stadium der Richtlinie auf der Maschine **Wird aktualisiert**. Das Stadium wechselt wieder zu **Verteilt**, sobald die Richtlinie aktualisiert wurde. Dieses Stadium bedeutet, dass die Richtlinie funktioniert und gegenwärtig keine Veränderungen an ihr vorgenommen werden.

Eine Richtlinie, die während ihrer Verteilung modifiziert wird, verbleibt im Stadium **Wird verteilt**. Der Management Server beginnt einfach damit, die modifizierte Richtlinie von Anfang an zu verteilen.

Möglicherweise müssen Sie die Richtlinie von der Maschine oder der die Maschine enthaltenen Gruppe widerrufen. Sobald Sie die Änderungen bestätigen, widerruft der Management Server die Richtlinie von der Maschine. Während die Änderungen zu den Maschinen übertragen werden und der Agent den Backup-Plan löscht, ist das Stadium der Richtlinie auf der Maschine **Wird widerrufen**.

Sie verändern eventuell die Gruppierungsbedingungen oder die Maschine ändert ihre Eigenschaften, so dass die Maschine eine Gruppe verlässt und in eine andere aufgenommen wird. Dies kann dazu führen, dass eine Richtlinie widerrufen und eine andere verteilt wird. In diesem Fall wird das erste Stadium der Richtlinie auf der Maschine zu **Wird widerrufen** und das zweite Stadium wird **Wird verteilt**. Die Richtlinien können in der Benutzeroberfläche (GUI) gleichzeitig oder eine nach der anderen erscheinen.

Diagramm der Backup-Richtlinien-Zustände



Richtlinien-Status auf einer Maschine

Um diesen Parameter einzusehen, wählen Sie im Verzeichnisbaum eine Maschinen-Gruppe, dann die Maschine und darauf die Registerlasche **Backup-Richtlinien** in der Leiste **Informationen**.

In jedem der Stadien kann die Backup-Richtlinie einen Status wie folgt haben: **Fehler**; **Warnung**; **OK**. Während sich die Richtlinie im Stadium **Verteilt** befindet, reflektiert ihr Status, wie erfolgreich die Richtlinie ausgeführt wurde. Befindet sich die Richtlinie in irgendeinem anderen Stadium, so reflektiert ihr Status, wie erfolgreich sie modifiziert wurde.

Richtlinienstatus, wenn die zu sichernden Daten auf einer Maschine nicht gefunden werden

Eine Backup-Richtlinie kann auf eine Maschine angewendet werden, die über keine mit den Auswahlregeln (S. 419) übereinstimmenden Daten verfügt. Während der Verteilung der Richtlinie werden keine Fehler oder Warnmeldungen aufgezeichnet, da angenommen wird, dass die Daten noch zukünftig auftauchen können. Wie üblich wird ein Backup-Plan erstellt und das Stadium der Richtlinie auf **Verteilt** geändert.

Falls bei Start des Backup-Tasks keine zu sichernden Daten gefunden werden, schlägt er fehl und der Richtlinienstatus wechselt auf **Fehler**. Wenn wenigstens eines der Daten-Elemente gefunden wird, wird der Backup-Task mit einer Warnmeldung erfolgreich abgeschlossen. Der Richtlinienstatus wird sich auf entsprechende Weise ebenfalls verändern.

Die Backup-Tasks werden wie durch die Richtlinie geplant starten und solange ein vergleichbares Ergebnis produzieren, bis alle Daten-Elemente auf der Maschine auftauchen oder die Richtlinie so bearbeitet wird, dass die nicht existierenden Daten-Elemente ausgeschlossen werden.

Beispiele

Angenommen, die Auswahlregel legt fest, dass die Richtlinie die Laufwerke D: und F: sichern soll. Die Richtlinie wird auf Linux- und Windows-Maschinen gleichermaßen angewendet. Sobald das erste Backup gestartet ist, erhält die Richtlinie auf Linux-Maschinen den Status **Fehler** – wie auch auf Windows-Maschinen, die keine entsprechenden Laufwerke haben. Die Richtlinie erhält den Status **Warnung** auf solchen Windows-Maschinen, die entweder ein D:- oder F:- Laufwerk haben, es sei denn, ein Fehler-produzierendes Ereignis tritt auf.

Eine Richtlinie, die die Laufwerke [System] und „/dev/sda1“ sichern muss, wird auf den Windows-Maschinen den Status **Warnung** erhalten (da „/dev/sda“ nicht gefunden wird) und auch auf den Linux-Maschinen, die das Laufwerk „/dev/sda1“ haben (während das Laufwerk [System] nicht gefunden wird). Auf Linux-Maschinen, die kein SCSI-Gerät haben, erhält die Richtlinie den Status **Fehler**.

Die nachfolgende Tabelle vermittelt Ihnen die Details.

Stadium	Status	Beschreibung
Verteile	**Fehler**	Das Deployment-Log enthält Fehler, z.B. dass der Platz auf der Festplatte nicht ausreicht.
	Achtung	Die Deployment-Ereignisanzeige enthält Warnungen: Die Maschine ging während des Deployments offline oder konnte seit n Tagen nicht verbinden
	OK	Die Deployment-Ereignisanzeige hat keine Fehler und Warnungen.
Verteilt	**Fehler**	Der Status des korrespondierenden Backup-Plans ist **Fehler**.
	Achtung	Der Status des korrespondierenden Backup-Plans ist **Warnung**.
	OK	Der Status des korrespondierenden Backup-Plans ist **OK**.
Aktualisiere	**Fehler**	Die Aktualisierungs-Ereignisanzeige enthält Fehler: kann gesperrten Task nicht löschen, der Acronis-Dienst ist gestoppt…
	Achtung	Die Aktualisierungs-Ereignisanzeige enthält Warnungen.
	OK	Die Aktualisierungs-Ereignisanzeige hat keine Fehler und Warnungen.
Widerrufe	**Fehler**	Log zum Widerrufen enthält Fehler.
	Achtung	Die Widerrufs-Ereignisanzeige enthält Warnungen.
	OK	Die Widerrufs-Ereignisanzeige hat keine Fehler und Warnungen.

Ergänzend zu Deployment-Stadium und -Zuständen, die sich auf eine spezielle Maschine beziehen, enthält die Backup-Richtlinie auch Deployment-Stadien und -Zustände von Maschinen-Gruppen sowie das kumulative Deployment-Stadium bzw. den Status der Richtlinie selbst.

Stadien des Richtlinien-Deployments auf einer Gruppe

Um diesen Parameter einzusehen, wählen Sie **Maschinen** im Verzeichnisbaum, dann die Gruppe und

darauf die Registerlasche **Backup-Richtlinien** in der Leiste **Informationen**.

Dieses Stadium wird definiert als Kombination aus den Deployment-Stadien der Richtlinien auf den Maschinen dieser Gruppe und ihrer Untergruppen.

Beispiel: Sie haben die Richtlinie auf eine Gruppe bestehend aus den Maschinen A und B angewendet. Während das Deployment auf beiden Maschinen stattfindet, ist das Richtlinien-Stadium auf der Gruppe „Wird verteilt“. Wird das Deployment auf einer der Maschinen fertiggestellt, während es auf der anderen noch weiterläuft, so ist das Stadium „Wird verteilt, Verteilt“. Wurde das Deployment auf beiden Maschinen fertiggestellt, so ist das Stadium „Verteilt“.

Richtlinien-Status auf einer Gruppe

Um diesen Parameter einzusehen, wählen Sie **Maschinen** im Verzeichnisbaum, dann die Gruppe und darauf die Registerlasche **Backup-Richtlinien** in der Leiste **Informationen**.

Dieser Status ist als der schwerwiegendste Status der Richtlinen auf den Maschinen dieser Gruppe und ihrer Untergruppen definiert. Der Status ist „OK“, wenn die Richtlinie gegenwärtig auf keine Maschine angewendet wird.

Kumulatives Stadium und kumulativer Status einer Richtlinie

Ergänzend zu Deployment-Stadium und Status, die sich auf eine spezielle Maschine beziehen, hat die Backup-Richtlinie auch ein kumulatives Deployment-Stadium bzw. einen kumulativen Status.

Das kumulative Stadium einer Backup-Richtlinie

Wählen Sie **Backup-Richtlinie** im Verzeichnisbaum, um diesen Parameter einzusehen. Die Spalte **Deployment-Stadium** zeigt das kumulative Deployment-Stadium jeder Richtlinie an.

Dieses Stadium wird definiert als eine Kombination der Deployment-Stadien all der Maschinen, auf die die Richtlinie angewendet wurde (direkt oder durch Vererbung). Wird die Richtlinie gegenwärtig auf keine Maschine angewendet, so hat sie kein Deployment-Stadium und die Spalte zeigt „Nicht angewendet“.

Beispiel: Sie haben die Richtlinie auf Maschine A angewendet. Die Richtlinie wurde erfolgreich verteilt. Dann modifizieren Sie die Richtlinie und wenden Sie unmittelbar auf die Gruppe an, die aus den Maschinen B und C besteht. Die Richtlinie muss daraufhin auf A aktualisiert sowie auf B und C verteilt werden. Während die Prozesse stattfinden, sieht das kumulative Stadium der Richtlinie evtl. aus wie „Wird aktualisiert, Wird verteilt“, wechselt dann zu „Wird aktualisiert, Verteilt“ oder „Verteilt, Wird verteilt“ und endet normalerweise mit „Verteilt“.

Der kumulative Status einer Backup-Richtlinie

Wählen Sie **Backup-Richtlinie** im Verzeichnisbaum, um diesen Parameter einzusehen. Die Spalte **Status** zeigt den kumulative Deployment-Status jeder Richtlinie an.

Dieser Status ist als der schwerwiegendste Status der Richtlinie auf allen Maschinen definiert, auf die die Richtlinie angewendet wird. Der Status ist „OK“, wenn die Richtlinie auf keine Maschine angewendet wird.

2.12.6 Deduplizierung

Dieser Abschnitt beschreibt den Deduplizierungsmechanismus, der entwickelt wurde, um Datenwiederholungen dadurch zu eliminieren, dass identische Daten in Archiven nur noch einmal gespeichert werden.

Überblick

Deduplizierung ist ein Prozess zur Minimierung von durch Daten belegten Speicherplatz, indem Daten-Wiederholungen erkannt werden und identische Daten nur noch einmal gespeichert werden.

Ein Beispiel: Ein Depot enthält zwei Kopien derselben Datei – egal ob im selben oder einem anderen Archiv; wenn Deduplizierung aktiviert ist, wird die Datei nur noch einmal gespeichert und ein Link auf die zweite, entfernte Datei gesetzt.

Deduplizierung kann außerdem die Netzwerklast reduzieren: Sollte während eines Backups eine Datei oder ein Datenblock als bereits gespeichertes Duplikat erkannt werden, so wird sein Inhalt nicht noch einmal über das Netzwerk übertragen.

Deduplizierung wird auf Festplattendatenblöcke (Block-Ebene-Deduplizierung) und auf Dateien (Datei-Ebene-Deduplizierung) angewendet, entsprechend den Backups auf Festplatten-Ebene und Datei-Ebene.

Deduplizierung besteht in Acronis Backup & Recovery 10 aus zwei Schritten:

Deduplizierung an der Quelle

Die Durchführung erfolgt während eines Backups auf einer verwalteten Maschine. Der Acronis Backup & Recovery 10 Agent nutzt den Storage Node, um zu bestimmen, welche Daten dedupliziert werden können und überträgt dann keine Daten mehr, deren Duplikate bereits im Depot vorliegen.

Deduplizierung auf dem Ziel

Durchführung im Depot nach Fertigstellung eines Backups. Der Storage Node analysiert die Archive des Depots und dedupliziert dann die dort befindlichen Daten.

Sie erhalten beim Erstellen eines Backup-Plans die Option, die Deduplizierung an der Quelle auszuschalten. Das kann zu schnelleren Backups führen, aber auch zu größerer Last für das Netzwerk und den Storage Node.

Deduplizierendes Depot

Ein verwaltetes, zentrales Depot mit aktivierter Deduplizierung wird *Deduplizierendes Depot* genannt. Beim Erstellen eines verwalteten, zentralen Deopts können Sie festlegen, ob die Deduplizierung eingeschaltet wird oder nicht. Ein deduplizierendes Depot kann nicht auf einem Bandgerät erstellt werden.

Deduplizierungsdatenbank

Ein Acronis Backup & Recovery 10 Storage Node, der ein deduplizierendes Depot verwaltet, hält eine Deduplizierungs-Datenbank aufrecht, die die Hash-Werte aller im Depot liegenden Elemente enthält (mit Ausnahme solcher, die nicht deduplizierbar sind, etwa verschlüsselte Dateien).

Die Deduplizierungs-Datenbank wird in dem Ordner gespeichert, der bei Erstellung des Depots in der Ansicht **Erstelle zentrales Depot** durch den **Datenbank-Pfad** spezifiziert wird. Eine Deduplizierungs-Datenbank kann nur in einen lokalen Ordner erstellt werden.

Die Größe einer Deduplizierungs-Datenbank beträgt ungefähr ein Prozent der Gesamtgröße aller Archive in einem Depot. Mit anderen Worten, jedes Terabyte an neuen (nicht doppelten) Daten fügt der Datenbank ca. 10 GB hinzu.

Sollte eine Datenbank beschädigt sein oder der Storage Node verloren gehen, während das Depot Archive und der Service-Ordner Metadaten enthält, so rescannt der neue Storage Node das Depot

und erstellt die Datenbank wieder neu.

So funktioniert Deduplizierung

Deduplizierung an der Quelle

Bei Durchführung eines Backups zu einem deduplizierenden Depot liest der Acronis Backup & Recovery 10 Agent die gesicherten Elemente (Disk-Datenblöcke bei Disk-Backup oder Dateien bei File-Backup) und kalkuliert dann für jeden Block einen Fingerabdruck. Ein solcher Fingerabdruck, auch *Hash-Wert* genannt, repräsentiert den Inhalt des jeweiligen Elements innerhalb des Depots.

Bevor ein Element zum Depot übertragen wird, fragt der Agent die Deduplizierungs-Datenbank ab, um zu bestimmen, ob der Hash-Wert dieses Elements identisch zu einem bereits gespeicherten Element ist.

Wenn dem so ist, so überträgt der Agent nur den Hash-Wert des Elementes, wenn nicht, so wird das Element selbst übertragen.

Einige Elemente (z.B. verschlüsselte Dateien oder Disk-Datenblöcke mit einer vom Standard abweichenden Größe) können nicht dedupliziert werden, weswegen der Agent solche Elemente auch ohne Hash-Wert-Kalkulation zum Depot überträgt. Mehr Informationen über die Beschränkung von Deduplizierung auf Datei- und Disk-Ebene finden Sie unter Deduplizierungs-Beschränkungen (S. 73).

Deduplizierung auf dem Ziel

Nachdem die Sicherung auf einem deduplizierenden Depot abgeschlossen ist, führt der Storage Node den **Indizierungs-Task** zur Deduplizierung von Daten in dem Depot wie folgt aus:

1. Er verschiebt die Elemente (Laufwerksblöcke oder Dateien) aus den Archiven in eine spezielle Datei innerhalb des Depots, wo doppelt vorhandene Elemente dann nur noch einmal gespeichert werden. Diese Datei wird **Deduplizierungs-Datenspeicher** genannt. Sind im Depot sowohl Laufwerk- wie auch Datei-basierte Backups vorhanden, dann gibt es für diese zwei separate Datenspeicher. Nicht-deduplizierbare Elemente verbleiben in den Archiven.
2. In den Archiven ersetzt der Storage Node die verschobenen Elemente durch einen mit ihnen korrespondierenden Verweis.

Als Ergebnis enthält das Depot eine gewisse Zahl einmaliger, deduplizierter Elemente, wobei jedes Element einen oder mehrere zu ihm gehörende Verweise in den Archiven des Depots hat.

Die Indizierung kann einige Zeit dauern. Sie können den Fortschritt des Tasks in der Ansicht **Tasks** auf dem Management Server einsehen.

Verdichten

Wurden ein oder mehrere Backups bzw. Archive vom Depot gelöscht (entweder manuell oder durch Bereinigung), so kann das Depot Elemente enthalten, die sich nicht mehr auf irgendwelche Archive beziehen. Solche Elemente werden dann durch einen **Verdichtungs-Task** gelöscht, bei dem es sich um einen geplanten, vom Storage Node ausgeführten Task handelt.

Als Standardvorgabe läuft der Verdichtungs-Task jeweils sonntags in der Nacht um 03:00 Uhr. Sie können die Planung des Tasks ändern, wie unter Aktionen für Storage Nodes (S. 342) (Abschnitt „Die Planung des Verdichtungs-Task ändern“) beschrieben. Sie können den Task außerdem manuell starten oder stoppen – und zwar in der Ansicht **Tasks**.

Da das Löschen unbenutzter Elemente ein Ressourcen verbrauchender Prozess ist, wird der Verdichtungs-Task nur ausgeführt, wenn sich eine ausreichende Datenmenge angesammelt hat. Der Grenzwert wird über den Konfigurationsparameter **Compacting Trigger Threshold** (S. 358) bestimmt.

Wann Deduplizierung am effektivsten ist

Nachfolgend einige Beispiele, wann Deduplizierung die besten Ergebnisse erzielt:

- Beim Sichern ähnlicher Daten aus verschiedenen Quellen im **Voll-Backup-Modus**. Das ist z.B. beim Backup von Betriebssystem und Anwendungen der Fall, wenn diese von einer Quelle aus per Netzwerk verteilt wurden.
- Bei Durchführung **inkrementeller Backups** von ähnlichen Daten aus verschiedenen Quellen unter der Annahme, dass **die Daten-Veränderungen ebenfalls ähnlich sind**. Das ist z.B. der Fall, wenn Sie Updates zu diesen Systemen verteilen und auf diese dann das inkrementelle Backup anwenden.
- Bei Durchführung von **inkrementellen Backups** von Daten, die sich nicht selbst, aber **ihren Speicherplatz geändert** haben. Das ist z.B. der Fall, wenn multiple Teile von Daten durch das Netzwerk oder innerhalb eines Systems zirkulieren. Jedes Mal, wenn ein Teil dieser Daten verschoben wird, wird dieser in das inkrementelle Backup aufgenommen, welches an Größe zunimmt, während es aber keine neuen Daten enthält. Deduplizierung hilft, dieses Problem zu lösen: Jedes Mal, wenn ein Element an einem neuen Ort erscheint, wird statt des Elements selbst eine Referenz auf dieses gespeichert.

Deduplizierung und inkrementelle Backups

Bei zufälliger Veränderung von Daten führt die Deduplizierung daraus resultierender inkrementeller Backups zu keinem großen Effekt, denn:

- Die deduplizierten Elemente, die sich nicht verändert haben, sind in den inkrementellen Backups nicht enthalten.
- Die deduplizierten Elemente, die sich nicht verändert haben, sind nicht mehr identisch und werden daher auch nicht dedupliziert.

Optimale Vorgehensweisen bei der Deduplizierung

Diese Empfehlungen sollten Sie bei der Deduplizierung beachten:

- Achten Sie beim Erstellen eines deduplizierenden Depots darauf, dass sich das **Depot und die Deduplizierungsdatenbank auf unterschiedlichen Laufwerken befinden.** Das beschleunigt die Deduplizierung, da bei diesem Prozess gleichzeitig auf das Depot und die Datenbank zugegriffen wird.
- Für die Indizierung eines Backups muss im Depot **freier Speicherplatz vorhanden sein, der 1,1x der Größe des Archivs, zu dem das Backup gehört**, entspricht. Wenn nicht ausreichend freier Speicherplatz im Depot vorhanden ist, wird die Indizierung fehlschlagen; nach 5–10 Minuten beginnt sie erneut, da nun infolge einer Bereinigung oder eines anderen Indizierungs-Tasks Speicherplatz freigegeben worden sein sollte. Je mehr freier Speicherplatz in einem Depot verfügbar ist, desto schneller wird die Größe Ihrer Archive auf ein Minimum reduziert.
- Beim Backup von mehreren Systemen mit ähnlichen Inhalten sollten Sie **zunächst eines dieser Systeme sichern**, damit der Acronis Backup & Recovery 10 Storage Node alle Systemdateien als mögliche Deduplizierungselemente indizieren kann. Das führt zu schnelleren Backup-Prozessen und verringertem Netzwerkverkehr (aufgrund effektiver Deduplizierung an der Quelle), unabhängig davon, ob die Backups simultan durchgeführt werden oder nicht.

  Stellen Sie sicher, dass vor dem Start weiterer Backups der **Indizierungs-Task die Deduplizierung des ersten Backup abgeschlossen hat** und sich im Leerlauf befindet. Der Status eines Indizierungs-Task wird in der Liste der Tasks auf dem Acronis Backup & Recovery 10 Management Server angezeigt.

Deduplizierungsverhältnis

Das Deduplizierungs-Verhältnis gibt die Größe der Archive in einem deduplizierenden Depot im Verhältnis zu der Größe an, die sie in einem nicht-deduplizierenden Depot belegen würden.

Beispiel: Angenommen, Sie sichern zwei Dateien mit identischem Inhalt von zwei Maschinen. Beträgt die Größe jeder Datei ein Gigabyte, so ist die Größe der Backups in einem nicht-deduplizierenden Depot ungefähr 2 GB, in einem deduplizierenden jedoch nur noch ca. 1 GB. Das ergibt ein Deduplizierungsverhältnis von 2:1 bzw. 50%.

Im umgekehrten Fall, wenn beide Dateien unterschiedliche Inhalte haben, würde die Backup-Größe in den deduplizierenden bzw. nicht-deduplizierenden Depots ungefähr gleich sein (2 GB) – mit einem Deduplizierungsverhältnis von 1:1 oder 100%.

Zu erwartende Verhältniswerte

Obwohl das Deduplizierungs-Verhältnis unter manchen Umständen sehr hoch sein kann (wie im oberen Beispiel, bei Zunahme der Maschinen ergäben sich sogar Verhältnisse von 3:1, 4:1 etc.), liegt unter typischen Umständen eine vernünftige Erwartung bei einem Verhältnis von 1,2:1 und 1,6:1.

Als realistischeres Beispiel sei angenommen, dass Sie ein Backup auf Datei- oder Disk-Ebene von zwei Maschinen mit gleichartigen Festplatten durchführen. Auf beiden Maschinen belegen gemeinsame Dateien 50% des Festplattenplatzes (z.B. 1 GB), während die für jede Maschine spezifischen Dateien die übrigen 50% (zusätzlich 1 GB) einnehmen.

In einem deduplizierenden Depot wird daher die Größe des Backups der ersten Maschine 2 GB betragen, während die Backup-Größe der zweiten Maschine 1 GB sein wird. In einem nicht-deduplizierenden Depot würden die Backups dagegen insgesamt 4 GB belegen. Daraus resultiert ein Deduplizierungsverhältnis von 4:3 bzw. ca. 1,33:1.

In ähnlicher Weise erhalten Sie bei drei Maschinen ein Verhältnis von 1,5:1 und bei vier Maschinen eins von 1,6:1. Es nähert sich 2:1, je mehr solcher Maschinen zum selben Depot gesichert werden. Das bedeutet, dass Sie z.B. ein 10 TB-Speichergerät statt eines mit 20 TB kaufen können.

Die tatsächliche Menge an reduzierter Kapazität wird durch zahlreiche Faktoren beeinflusst, wie etwa der Art der gesicherten Daten, der Backup-Häufigkeit und der Backup-Aufbewahrungsperiode.

Deduplizierungs-Beschränkungen

Beschränkungen für Deduplizierung auf Block-Ebene

Während eines Festplatten-Backups in ein Archiv, das in einem deduplizierenden Depot gespeichert wird, erfolgt unter folgenden Umständen keine Deduplizierung der Laufwerks-Datenblöcke:

- falls das Laufwerk komprimiert ist
- falls die Größe der Zuordnungseinheit des Laufwerkes – auch bekannt als Cluster-Größe oder Block-Größe – nicht durch 4 KB teilbar ist.

  Tipp: *Auf den meisten NTFS- und ext3-Laufwerken beträgt die Größe der Zuordnungseinheit 4 KB, so dass eine Deduplizierung auf Block-Ebene also möglich ist. Andere Größen von Zuordnungseinheiten, die eine Deduplizierung auf Block-Ebene ermöglichen, sind z.B. 8 KB, 16 KB und 64 KB.*

- falls Sie das Archiv mit einem Passwort schützen

  Tipp: *Verzichten Sie auf einen Passwortschutz des Archivs und verschlüsseln Sie stattdessen das deduplizierende Depot mit einem Passwort (was bei Erstellung des Depots möglich ist), um die Daten im Archiv bei gleichzeitiger Bewahrung der Deduplizierungsmöglichkeit zu schützen.*

Festplatten-Datenblöcke, die nicht dedupliziert wurden, werden im Archiv so gespeichert, als wären sie in einem nicht-deduplizierenden Depot.

Beschränkungen für Deduplizierung auf Datei-Ebene

Während eines Datei-Backups in ein Archiv, das in einem deduplizierenden Depot gespeichert wird, erfolgt unter folgenden Umständen keine Deduplizierung der Dateien:

- falls die Datei verschlüsselt ist und das Kontrollkästchen **Verschlüsselte Dateien im Archiv unverschlüsselt speichern** deaktiviert ist (Standardeinstellung)
- falls die Datei kleiner als 4 KB ist
- falls Sie das Archiv mit einem Passwort schützen

Dateien, die nicht dedupliziert wurden, werden im Archiv so gespeichert, als wären sie in einem nicht-deduplizierenden Depot.

Deduplizierung und NTFS-Datenströme

Im NTFS-Dateisystem kann eine Datei mit einem oder mehreren zusätzlichen Datensätzen assoziiert sein – häufig *Alternative Datenströme* genannt.

Beim Backup einer solchen Datei werden auch all ihre alternativen Datenströme mit gesichert. Diese Datenströme werden jedoch auch dann nie dedupliziert, wenn die Datei selbst es wird.

2.12.7 Rechte für zentrale Verwaltung

Dieser Abschnitt beschreibt die benötigten Benutzerrechte, um eine Maschine lokal oder remote zu verwalten, eine auf dem Acronis Backup & Recovery 10 Management Server registrierte Maschine zu verwalten oder um auf einen Acronis Backup & Recovery 10 Storage Node zuzugreifen bzw. diesen zu verwalten.

Verbindungsarten zu einer verwalteten Maschine

Es gibt zwei Arten von Verbindungen zu einer verwalteten Maschine: lokale Verbindungen und Remote-Verbindungen.

Lokale Verbindung

Eine lokale Verbindung wird auf einer Maschine zwischen der Acronis Backup & Recovery 10 Management Console und dem Acronis Backup & Recovery 10 Agent auf derselben Maschine aufgestellt.

So stellen Sie eine lokale Verbindung her

- Klicken Sie in der Symbolleiste auf **Verbinden**, anschließend auf **Neue Verbindung** und danach auf **Diese Maschine**.

Remote-Verbindung

Eine Remote-Verbindung wird zwischen der Acronis Backup & Recovery 10 Management Console auf einer Maschine und dem Acronis Backup & Recovery 10 Agenten auf einer anderen Maschine etabliert.

Sie müssen möglicherweise zum Aufbau der Remote-Verbindung Anmeldedaten zur Verfügung stellen.

So stellen Sie eine Remote-Verbindung her

1. Klicken Sie in der Symbolleiste auf **Verbinden**, anschließend auf **Neue Verbindung** und danach auf **Eine Remote-Maschine verwalten**.
2. Geben Sie im Feld **Maschine** den Namen oder die IP-Adresse der Remote-Maschine an, zu der Sie sich verbinden wollen oder klicken Sie auf **Durchsuchen**, um die gewünschte Maschine aus einer Liste auszuwählen.
3. Zur Angabe von für die Verbindung benötigten Anmeldedaten klicken Sie auf **Optionen** und geben dann in die Felder **Benutzername** und **Kennwort** die entsprechenden Werte ein. In Windows werden die aktuellen Anmeldedaten verwendet (unter denen die Konsole läuft), falls Sie das Feld **Benutzername** leer lassen.
4. Um das Passwort des angegebenen Benutzernamens zu speichern, aktivieren Sie das Kontrollkästchen **Kennwort speichern**, worauf dieses an einem sicheren Ort auf der Maschine, die die Konsole ausführt, gesichert wird.

Rechte für lokale Verbindungen

Eine lokale Verbindung auf einer unter Windows laufenden Maschine kann von jedem Benutzer etabliert werden, der auf dieser Maschine das Benutzerrecht „lokal anmelden“ hat.

Rechte für Remote-Verbindungen in Windows

Um zu einer unter Windows laufenden Maschine eine Remote-Verbindung aufzubauen, muss der Benutzer auf dieser Maschine Mitglied der Sicherheitsgruppe Acronis Remote Users sein.

Nach Aufbau der Remote-Verbindung hat der Benutzer, wie unter Benutzerrechte auf einer verwalteten Maschine (S. 34) beschrieben, Verwaltungsrechte auf der Remote-Maschine.

Anmerkung: *Auf einer Remote-Maschine, die unter Windows Vista mit eingeschalteter Benutzerkontensteuerung (UAC) läuft und die nicht Teil einer Domain ist, kann nur der standardmäßige Administrator-Benutzer Daten per Backup sichern und Festplattenverwaltungsaktionen ausführen. Sie können diese Beschränkung überwinden, indem Sie die Maschine in eine Domain aufnehmen oder auf der Maschine die Benutzerkontensteuerung (UAC) ausschalten (standardmäßig ist UAC eingeschaltet). Dasselbe gilt für Maschinen, auf denen Windows Server 2008 und Windows 7 läuft.*

Zu Informationen über Acronis-Sicherheitsgruppen und ihre Standardmitglieder siehe Acronis Sicherheitsgruppen (S. 75).

Acronis Sicherheitsgruppen

Auf einer mit Windows laufenden Maschine bestimmen Acronis Sicherheitsgruppen, wer die Maschine aus der Ferne verwalten und als Acronis Backup & Recovery 10 Management Server-Administrator agieren kann.

Diese Gruppen werden erstellt, wenn die Acronis Backup & Recovery 10 Agenten oder der Acronis Backup & Recovery 10 Management Server installiert werden. Sie können dann während der Installation spezifizieren, welche Benutzer in jede Gruppe aufgenommen werden.

Acronis Backup & Recovery 10 Agenten

Bei Installation des Acronis Backup & Recovery 10 Agent für Windows auf einer Maschine wird auch die Gruppe **Acronis Remote Users** erstellt (oder aktualisiert).

Ein Benutzer, der Mitglied dieser Gruppe ist, kann die Maschine durch Verwendung der Acronis Backup & Recovery 10 Management Console aus der Ferne verwalten, gemäß den unter Benutzerrechte auf einer verwalteten Maschine (S. 34) beschriebenen Verwaltungsrechten.

Standardmäßig enthält diese Gruppe alle Mitglieder der Gruppe Administratoren.

Acronis Backup & Recovery 10 Management Server

Wird der Acronis Backup & Recovery 10 Management Server auf einer Maschine installiert, so werden dabei zwei Gruppen erstellt (oder aktualisiert):

Acronis Centralized Admins

Ein Benutzer, der Mitglied dieser Gruppe ist, ist ein Management Server Administrator. Management Server Administratoren können sich unter Verwendung der Acronis Backup & Recovery 10 Management Console zum Management Server verbinden; sie haben dieselben Verwaltungsrechte auf der registrierten Maschine wie Benutzer mit Administratorrechten auf dieser Maschine – ungeachtet der Inhalte der dortigen Acronis Sicherheitsgruppen.

Damit ein Management Server-Administrator sich auch *remote* mit dem Management Server verbinden kann, muss er außerdem Mitglied der Gruppe Acronis Remote-Benutzer sein.

Kein Benutzer – auch kein Mitglied der Gruppe Administratoren – kann ein Administrator des Management Servers sein, ohne Mitglied der Gruppe Acronis Centralized Admins zu sein.

Standardmäßig enthält diese Gruppe alle Mitglieder der Gruppe Administratoren.

Acronis Remote Users

Ein Benutzer, der Mitglied dieser Gruppe ist, kann sich unter Verwendung der Acronis Backup & Recovery 10 Management Console remote zum Management Server verbinden – sofern dieser Benutzer auch Mitglied der Gruppe Acronis Centralized Admins ist.

Standardmäßig enthält diese Gruppe alle Mitglieder der Gruppe Administratoren.

Auf einem Domain-Controller

Ist eine Maschine ein Domain-Controller in einer Active Directory-Domain, so sind die Namen und Standardinhalte der Acronis Sicherheitsgruppen unterschiedlich:

- Anstatt **Acronis Remote Users** und **Acronis Centralized Admins** lauten die Bezeichnungen der Gruppen *DCNAME* **$ Acronis Remote Users** bzw. *DCNAME* **$ Acronis Centralized Admins**; wobei *DCNAME* für den NetBIOS-Namen des Domain-Controllers steht. Jedes Dollar-Zeichen ist auf beiden Seiten von einem Leerzeichen umgeben.
- Statt explizit die Namen aller Mitglieder der Gruppe Administratoren aufzunehmen, wird die Administratoren-Gruppe selbst aufgenommen.

Tipp: *Um ordnungsgemäße Gruppen-Namen zu gewährleisten, sollten Sie eine Acronis-Komponente auf dem Domain-Controller installieren, nachdem Sie diesen aufgesetzt haben. Wurden die Komponenten installiert, bevor Sie den Domain-Controller aufgesetzt haben, so erstellen Sie die Gruppen* DCNAME ***$ Acronis Remote Users*** *und* DCNAME ***$ Acronis Centralized Admins*** *manuell und nehmen dann die Mitglieder von Acronis Remote Users sowie Acronis Centralized Admins in die neu erstellten Gruppen auf.*

Benutzerrechte auf einem Storage Node

Der Umfang an Berechtigungen, die ein Benutzer auf einem Acronis Backup & Recovery 10 Storage Node hat, hängt von den Berechtigungen ab, die dieser Benutzer auf der Maschine mit dem installierten Storage Node hat.

Ein regulärer Benutzer, wie es etwa ein Mitglied der Gruppe „Benutzer“ auf dem Storage Node ist, kann:

- Archive in jedem zentralen, durch den Storage Node verwalteten Depot erstellen.
- dem Benutzer gehörende Archive einsehen und verwalten.

Ein Benutzer, der auf dem Storage Node Mitglied der Gruppe „Administratoren“ ist, kann zusätzlich:

- jedes Archiv in jedem zentralen, durch den Storage Node verwalteten Depot einsehen und verwalten.
- zentrale, durch den Storage Node zu verwaltende Depots erstellen – vorausgesetzt der Benutzer ist außerdem auch Acronis Backup & Recovery 10 Management Server-Administrator.
- den Zeit-/Ereignisplan eines Verdichtungs-Tasks neu aufsetzen, wie unter Aktionen mit Storage Nodes (S. 342) im Abschnitt „Zeit-/Ereignisplan des Verdichtungs-Task ändern“ beschrieben.

Benutzer mit diesen zusätzlichen Berechtigungen werden außerdem Storage Node-Administratoren genannt.

Empfehlungen zu Benutzerkonten

Damit Benutzer auf ein zentrales, durch den Storage Node verwaltetes Depot zugreifen können, müssen Sie sicherstellen, dass diese Benutzer auch die Berechtigung zum Zugriff auf den Storage Node über das Netzwerk haben.

Sind die Maschine des Benutzers und die des Storage Nodes gemeinsam in einer Active Directory-Domain, müssen Sie wahrscheinlich keine weiteren Schritte durchführen: alle Benutzer sind üblicherweise Mitglieder der Gruppe „Domain-Benutzer“ und können so auch auf den Storage Node zugreifen.

Anderenfalls müssen Sie auf der Maschine, auf der der Storage Node installiert ist, zusätzliche Benutzerkonten einrichten. Wir empfehlen, für jeden auf den Storage Node zugreifenden Benutzer ein separates Benutzerkonto zu erstellen, so dass die Benutzer nur auf die je ihnen gehörenden Archive zugreifen können.

Folgen Sie bei Erstellung der Konten diesen Leitlinien:

- Fügen Sie die Konten der Benutzer, die auch als Storage Node-Administratoren agieren sollen, zur Gruppe **Administratoren** hinzu.
- Die Konten der anderen Benutzer fügen Sie der Gruppe **Benutzer** hinzu.

Erweiterte Berechtigung für Maschinen-Administratoren

Ein Benutzer, der auf einer Maschine auch Mitglied der Gruppe Administratoren ist, kann jedes Archiv, welches *von dieser Maschine* in einem verwalteten Depot erstellt wurde, einsehen und verwalten – ungeachtet welcher Art das Konto dieses Benutzers auf dem Storage Node ist.

Beispiel

Angenommen, zwei Benutzer auf einer Maschine, BenutzerA und BenutzerB, erstellen Backups von dieser Maschine – mit Hilfe eines Storage Nodes zu einem zentralen Depot. Diese Benutzer sollen auf dem Storage Node reguläre (nicht-administrative) Benutzerkonten haben, nämlich BenutzerA_SK bzw. BenutzerB_SK.

Normalerweise kann BenutzerA nur auf Archive zugreifen, die von BenutzerA erstellt wurden (und BenutzerA_SK gehören), was für BenutzerB entsprechend gilt (Zugriff nur auf von BenutzerB erstellte Archive, die BenutzerB_SK gehören).

Ist BenutzerA jedoch Mitglied der Gruppe Administratoren auf dieser Maschine, so kann er zusätzlich auf die Archive zugreifen, die von BenutzerB dieser Maschine erstellt wurden – und das obwohl das Konto von BenutzerA auf dem Storage Node ein reguläres ist.

Rechte des Management Server-Administrators

Normalerweise arbeitet der Acronis Backup & Recovery 10 Management Server-Administrator auf einer registrierten Maschine – im Sinne des Acronis Managed Machine Service (auch als Acronis-Dienst) dieser Maschine und mit denselben Rechten, die dieser Dienst hat.

Bei Erstellung einer Backup-Richtlinie hat der Management Server-Administrator aber auch alternativ die Möglichkeit, explizit ein bestimmtes Benutzerkonto anzugeben, unter dem der zentrale Backup-Plan auf den registrierten Maschinen ausgeführt wird. Für diesen Fall muss das Benutzerkonto jedoch auf allen Maschinen vorhanden sein, zu der die zentrale Richtlinie verteilt wird. Dies ist nicht immer effizient.

Ein Anwender muss, um Management Server-Administrator zu sein, auch Mitglied der Gruppe Acronis Centralized Admins sein – und zwar auf der Maschine, auf der auch der Management Server installiert ist.

Rechte für Acronis-Dienste

Der Acronis Backup & Recovery 10 Agent für Windows, der Acronis Backup & Recovery 10 Management Server sowie der Acronis Backup & Recovery 10 Storage Node werden als Dienste ausgeführt. Wenn Sie eine dieser Komponenten installieren, müssen Sie das Konto angeben, unter dem der Dienst der Komponente ausgeführt wird.

Sie können für jeden Dienst entweder ein spezielles Benutzerkonto erstellen (zumeist empfohlen) oder das vorhandene Konto eines lokalen oder eines Domain-Benutzers angeben – beispielsweise: .**\LokalerBenutzer** oder **DomainName\DomainBenutzer**.

Wenn Sie sich entscheiden, spezielle Benutzerkonten für diese Dienste zu erstellen, dann generiert das Setup-Programm folgende Benutzerkonten:

- Für den Dienst des Acronis Backup & Recovery 10 Agenten für Windows das Konto **Acronis Agent User**
- Für den Dienst des Acronis Backup & Recovery 10 Management Server das Konto **AMS User**
- Für den Dienst des Acronis Backup & Recovery 10 Storage Nodes das Konto **ASN User**

Den neu erstellten Konten werden folgende Rechte zugewiesen:

- Allen drei Konten wird das Benutzerrecht **Anmelden als Dienst** erteilt.
- Dem Benutzerkonto Acronis Agent User werden die Benutzerrechte **Speicherquoten für einen Prozess anpassen** und **Token auf Prozessebene ersetzen** zugewiesen.
- Die Benutzerkonten Acronis Agent User und ASN User werden der Gruppe **Backup Operatoren** zugeordnet.
- Das Konto 'AMS User' ist in der Gruppe **Acronis Centralized Admins** enthalten.

Das Setup-Programm ordnet die aufgelisteten Benutzerrechte jedem bestehenden Konto zu, das Sie zur Ausführung des entsprechenden Diensts angeben.

Wenn Sie sich dafür entscheiden, ein bestehendes Benutzerkonto für den Agenten-Dienst oder den Dienst für den Storage Node zu spezifizieren, dann stellen Sie sicher, dass das Konto zur Gruppe **Backup Operatoren** gehört, bevor Sie mit der Installation fortfahren.

Wenn Sie sich dazu entschließen, für den Dienst des Management Servers ein existierendes Benutzerkonto anzugeben, wird dieses Konto der Gruppe **Acronis Centralized Admins** automatisch hinzugefügt.

Wenn die Maschine Teil einer Active Directory-Domain ist, stellen Sie sicher, dass die

Sicherheitsrichtlinien der Domain nicht eine Vergabe der aufgelisteten Benutzerrechte an die in diesem Abschnitt beschriebenen Konten (egal ob bereits existierend oder neu erstellt) verhindern.

Wichtig: *Geben Sie nach der Installation kein anderes Benutzerkonto zur Ausführung eines Komponentendienstes an. Anderenfalls kann die Komponente aufhören zu arbeiten.*

Den neu erstellten Benutzerkonten wird außerdem Zugriff auf den Registry-Schlüssel „HKEY_LOCAL_MACHINE\SOFTWARE\Acronis“ (Acronis-Registry-Key genannt) mit den folgenden Rechten gewährt: **Wert abfragen**, **Wert festlegen**, **Unterschlüssel erstellen**, **Unterschlüssel auflisten**, **Benachrichtigen**, **Löschen** und **Lesekontrolle**.

Es gibt zusätzlich zwei Acronis-Dienste, die unter einem System-Konto laufen.

- Der Dienst **Acronis Scheduler2** ermöglicht eine Zeit-/Ereignisplanung für die Tasks der Acronis-Komponenten. Er läuft unter dem Konto „Lokales System“ und kann unter keinem anderen Konto ausgeführt werden.
- Der Dienst **Acronis Remote Agent** ermöglicht die Verbindungsfähigkeit zwischen den Acronis-Komponenten. Er läuft unter dem Konto „Netzwerkdienst“ und kann unter keinem anderen Konto ausgeführt werden.

2.12.8 Kommunikation zwischen den Komponenten von Acronis Backup & Recovery 10

Dieser Abschnitt beschreibt, wie die verschiedenen Komponenten von Acronis Backup & Recovery 10 miteinander unter Verwendung sicherer Authentifizierung und Verschlüsselung kommunizieren.

Dieser Abschnitt bietet Ihnen außerdem Informationen über die Konfiguration von Kommunikationseinstellungen, die Wahl eines Netzwerk-Ports zur Kommunikation und die Verwaltung von Sicherheitszertifikaten.

Sichere Kommunikation

Acronis Backup & Recovery 10 verfügt über die Fähigkeit, die Datenübertragung zwischen seinen Komponenten innerhalb eines Lokalen Netzwerkes (LAN) und durch ein Perimeternetz (auch bekannt als demilitarisierte Zone, DMZ) abzusichern.

Es existieren zwei Mechanismen, um die sichere Kommunikation zwischen den Acronis Backup & Recovery 10-Komponenten zu gewährleisten:

- **Sichere Authentifizierung** ermöglicht die sichere Übertragung von zur Etablierung einer Verbindung benötigten Zertifikaten, nämlich durch Verwendung des Secure Sockets Layer-Protokolls (SSL).
- **Verschlüsselte Kommunikation** ermöglicht eine sichere Informationsübertragung zwischen zwei beliebigen Komponenten, z.B. zwischen dem Acronis Backup & Recovery 10 Agenten und dem Acronis Backup & Recovery 10 Storage Node, indem die übertragenen Daten verschlüsselt werden.

Zu Anleitungen über das Aufsetzen sicherer Authentifizierung und Daten-Verschlüsselung siehe Kommunikationsoptionen konfigurieren (S. 80).

Zu Anleitungen über die Verwaltung von zur sicheren Authentifizierung eingesetzten SSL-Zertifikaten siehe SSL-Zertifikate (S. 84).

Beachten Sie: *Die Komponenten früherer Acronis-Produkte, einschließlich solcher aus der Acronis True Image Echo-Familie, können sich nicht mit den Acronis Backup & Recovery 10-Komponenten verbinden, ungeachtet der*

Client- und Server-Anwendungen

Es gibt zwei relevante Gruppen beim sicheren Kommunikationsprozess:

- **Client-Anwendung** oder einfach nur Client, womit eine Applikation gemeint ist, die Verbindungen aufzubauen versucht.
- **Server-Anwendung** oder einfach nur Server, womit eine Anwendung gemeint ist, zu der der Client eine Verbindung aufzubauen versucht.

Wenn sich z.B. die Acronis Backup & Recovery 10 Management Console zum Acronis Backup & Recovery 10 Agenten auf einer Remote-Maschine verbindet, so ist erstere der Client und letztere der Server.

Eine Acronis-Komponente kann als Client- oder Server-Anwendung oder beides agieren, wie der nachfolgenden Tabelle zu entnehmen.

Name der Komponente	Kann Client sein	Kann Server sein
Acronis Backup & Recovery 10 Management Console	Ja	Nein
Acronis Backup & Recovery 10 Agent	Ja	Ja
Acronis Backup & Recovery 10 Management Server	Ja	Ja
Acronis Backup & Recovery 10 Storage Node	Ja	Ja
Acronis PXE Server	Nein	Ja
Acronis Backup & Recovery 10 Bootable Agent	Ja	Ja

Kommunikationseinstellungen konfigurieren

Sie können die Kommunikationseinstellungen (etwa verschlüsselte Datenübertragung) für Acronis Backup & Recovery 10-Komponenten (die auf einer oder mehreren Maschinen installiert sind) durch Nutzung von Acronis Administrative Template (administrative Vorlage) konfigurieren. Zu Informationen, wie die administrative Vorlage geladen wird, siehe So laden Sie Acronis Administrative Template (S. 357).

Wird das administrative Template auf eine Maschine angewendet, so definiert sie nur die Kommunikationseinstellungen aller Komponenten dieser Maschine; wird sie aber auf eine Domain oder Organisationseinheit angewendet, so definiert sie die Kommunikationseinstellungen aller Komponenten von allen Maschinen dieser Domain bzw. Organisationseinheit.

Kommunikationseinstellungen konfigurieren

1. Klicken Sie auf **Start** und dann auf **Ausführen** und geben Sie **gpedit.msc** ein.
2. Erweitern Sie in der **Gruppenrichtlinien**-Konsole den Ast **Computerkonfiguration** und danach den Ast **Administrative Vorlagen**, wo Sie auf Acronis klicken.
3. Klicken Sie im rechtsliegenden Acronis-Fensterbereich doppelt auf eine Kommunikationseinstellung, die Sie konfigurieren wollen. Das administrative Template enthält die folgenden Optionen (jede Option wird später in diesem Abschnitt erläutert):
   - **Ports für Remote Agent**
   - **Optionen für Client-Verschlüsselung**

- **Optionen für Server-Verschlüsselung**

4. Starten Sie alle laufenden Acronis-Komponenten neu, bevorzugt durch einen Windows-Neustart, damit die neuen Kommunikationseinstellungen wirksam werden. So gehen Sie vor, wenn kein Neustart möglich ist:
   - Sollte die Acronis Backup & Recovery 10 Management Console laufen, so schließen Sie diese und starten sie neu.
   - Sollte eine andere Acronis-Komponente laufen, wie etwa der Acronis Backup & Recovery 10 Agent für Windows oder der Acronis Backup & Recovery 10 Management Server, so starten Sie deren korrespondierende Dienste mit Hilfe des **Dienste**-Snap-ins von Windows neu.

Ports für Remote Agent

Spezifiziert den Port, den die Komponente für eingehende und ausgehende Kommunikation mit anderen Acronis-Komponenten verwendet.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird den Standard-TCP-Port mit der Nummer 9876 verwenden.

Aktiviert

Die Komponente wird den angegebenen Port verwenden; geben Sie die entsprechende Port-Nummer in das Feld **Server TCP-Port** ein.

Ausgeschaltet

Gleichbedeutend mit **Nicht konfiguriert**.

Zu Details über den Netzwerk-Port und Anleitungen, wie dieser unter Linux sowie einer bootfähigen Umgebung spezifiziert wird, siehe Konfiguration des Netzwerk-Ports (S. 83).

Optionen für Client-Verschlüsselung

Spezifiziert, ob eine verschlüsselte Datenübertragung erfolgt, sofern die Komponente als Client-Applikation agiert, und ob selbst-signierten SSL-Zertifikaten vertraut wird.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird die Standardeinstellungen verwenden, welche darin bestehen, Verschlüsselung wenn möglich zu nutzen und selbst-signierten SSL-Zertifikaten zu vertrauen (siehe die nachfolgende Option).

Aktiviert

Verschlüsselung ist eingeschaltet. Wählen Sie in **Verschlüsselung** Folgendes:

Aktiviert

Die Datenübertragung erfolgt verschlüsselt, falls auch bei der Server-Applikation die Verschlüsselung eingeschaltet ist, anderenfalls bleibt die Übertragung unverschlüsselt.

Ausgeschaltet

Verschlüsselung ist ausgeschaltet und jede Verbindung zu einer Server-Applikation, die eine Verschlüsselung erfordert, wird nicht hergestellt.

Erforderlich

Die Datenübertragung erfolgt verschlüsselt, wird aber nur aufgebaut, falls bei der Server-

Applikation die Verschlüsselung aktiviert ist (siehe „Optionen für Server-Verschlüsselung“).

Parameter zur Authentifizierung

Eine Aktivierung des Kontrollkästchens **Selbst-signierten Zertifikaten vertrauen** erlaubt dem Client, sich mit einer Server-Applikation zu verbinden, die selbst-signierte SSL-Zertifikate benutzt (wie solche Zertifikate, die während der Installation von Acronis Backup & Recovery 10-Komponenten erstellt wurden) — siehe SSL-Zertifikate (S. 84).

Sie sollten dieses Kontrollkästchen aktiviert lassen, außer Sie verwenden in Ihrem Umfeld eine Public Key-Infrastruktur (PKI).

Wählen Sie Folgendes in **Verwende Agent-Zertifikatsauthentifizierung**:

Nicht benutzen

Die Verwendung von SSL-Zertifikaten ist deaktiviert. Zu Server-Applikationen, die die Verwendung von SSL-Zertifikaten benötigen, werden keine Verbindungen aufgebaut.

Verwende wenn möglich

Die Verwendung von SSL-Zertifikaten ist aktiviert. Der Client wird SSL-Zertifikate nutzen, sofern ihre Verwendung auch bei der Server-Applikation eingeschaltet ist – anderenfalls werden sie nicht verwendet.

Immer verwenden

Die Verwendung von SSL-Zertifikaten ist aktiviert. Die Verbindung wird nur dann aufgebaut, wenn die Verwendung von SSL-Zertifikaten auch auf der Server-Applikation eingeschaltet ist.

Ausgeschaltet

Gleichbedeutend mit **Nicht konfiguriert**.

Optionen für Server-Verschlüsselung

Spezifiziert, ob die Datenübertragung verschlüsselt erfolgen soll, wenn die Komponente als Server-Applikation agiert.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird die Standardeinstellung verwenden, welche „verwende Verschlüsselung wenn möglich“ ist (siehe nachfolgende Option).

Aktiviert

Verschlüsselung ist eingeschaltet. Wählen Sie in **Verschlüsselung** Folgendes:

Aktiviert

Die Datenübertragung erfolgt verschlüsselt, falls auch bei der Client-Applikation die Verschlüsselung eingeschaltet ist, anderenfalls bleibt die Übertragung unverschlüsselt.

Ausgeschaltet

Verschlüsselung ist ausgeschaltet; zu Client-Applikationen, die Verschlüsselung erfordern, werden keine Verbindungen aufgebaut.

Erforderlich

Die Datenübertragung erfolgt verschlüsselt, wird aber nur aufgebaut, falls bei der Client-Applikation die Verschlüsselung aktiviert ist (siehe „Optionen für Client-Verschlüsselung“).

Parameter zur Authentifizierung

Wählen Sie Folgendes in **Verwende Agent-Zertifikatsauthentifizierung**:

Nicht benutzen

Die Verwendung von SSL-Zertifikaten ist deaktiviert. Zu Client-Applikation, die die Verwendung von SSL-Zertifikaten benötigen, werden keine Verbindungen aufgebaut.

Verwende wenn möglich

Die Verwendung von SSL-Zertifikaten ist aktiviert. Der Server wird SSL-Zertifikate nutzen, sofern ihre Verwendung auch bei der Client-Applikation eingeschaltet ist – anderenfalls werden sie nicht verwendet.

Immer verwenden

Die Verwendung von SSL-Zertifikaten ist aktiviert. Die Verbindung wird nur dann aufgebaut, wenn die Verwendung von SSL-Zertifikaten auch auf der Client-Applikation eingeschaltet ist.

Ausgeschaltet

Gleichbedeutend mit **Nicht konfiguriert**.

Konfiguration des Netzwerk-Ports

Die Komponenten von Acronis Backup & Recovery 10 benutzen als Standard den TCP-Port 9876. Der Server lauscht auf diesem Port nach einkommenden Verbindungen. Dieser Port wird außerdem auch als Standard vom Acronis-Client verwendet. Es kann sein, dass Sie während der Installation von Komponenten aufgefordert werden, die Öffnung des Ports zu bestätigen oder den Port manuell zu öffnen, sofern Sie eine andere als die Windows-Firewall verwenden.

Sie können den Port nach der Installation jederzeit wieder auf einen bevorzugten Wert oder zur Erfüllung von Sicherheitszwecken ändern. Diese Aktion benötigt den Neustart des Acronis Remote Agenten (unter Windows) oder von Acronis_agent (unter Linux).

Nachdem der Port auf der Server-Seite geändert wurde, verbinden Sie sich zum Server durch folgende Adress- bzw. URL-Schreibweise: <Server-IP>:<Port> oder <Server-Hostname>:<Port>.

Anmerkung: *Falls Sie Network Address Translation (NAT) verwenden, können Sie den Port auch unter Verwendung von Port-Mapping konfigurieren.*

Port-Konfiguration im Betriebssystem

Windows

Um die Port-Nummern ändern zu können, laden und konfigurieren Sie die von Acronis zur Verfügung gestellten aministrativen Vorlagen, wie es im Abschnitt Kommunikationseinstellungen konfigurieren (S. 80) beschrieben ist.

Linux

Spezifizieren Sie den Port in der Datei /etc/Acronis/Policies/Agent.config. Starten Sie den Acronis_agent Daemon neu.

Konfiguration des Ports in einer bootfähigen Umgebung

Sie erhalten während der Erstellung bootfähiger Acronis-Medien die Möglichkeit, die Netzwerkverbindungen vorzukonfigurieren, die vom bootfähigen Acronis Backup & Recovery 10 Agent verwendet werden. Es besteht die Wahl zwischen:

- dem Standard-Port (9876)

- 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.

SSL-Zertifikate

Die Acronis Backup & Recovery 10-Komponten verwenden Secure Sockets Layer (SSL)-Zertifikate für eine sichere Authentifizierung.

Die SSL-Zertifikate für die Komponenten können einer von zwei Typen sein:

- **Selbst-signierte Zertifikate** sind solche Zertifikate, wie sie automatisch während der Installation einer Acronis-Komponente generiert werden.
- **Nicht-selbst-signierte Zertifikate** sind Zertifikate, die durch Dritte, nämlich vertrauenswürdige Zertifizierungsstellen (Certificate Authority, CA) – z.B. VeriSign® or Thawte™ — oder durch die Zertifizierungsstelle Ihrer Organisation ausgestellt werden.

Zertifikats-Pfad

Alle auf einer Maschine installierten Acronis-Komponenten verwenden, wenn sie als Server-Applikation agieren, ein SSL-Zertifikat, welches als Server-Zertifikat bezeichnet wird.

In Windows werden der Zertifikatspfad und der Dateiname des Server-Zertifikates über den Registry-Key `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Encryption\Server` spezifiziert. Der Standard-Pfad ist %SystemDrive%\Programme\Common Files\Acronis\Agent.

Bei selbst-signierten Zertifikaten wird der „Fingerabdruck“ des Zertifikats (auch Fingerprint oder Hash genannt) für zukünftige Host-Identifizierung verwendet: Hat sich ein Client schon einmal unter Verwendung eines selbst-signierten Zertifikates mit einem Server verbunden und versucht erneut eine Verbindung aufzubauen, so überprüft der Server, ob der Fingerabdruck des Zertifikates derselbe ist wie beim vorherigen Verbindungsversuch.

Selbst-signierte Zertifikate

Auf unter Windows laufenden Maschinen wird, falls der Zertifikatsspeicher noch kein Server-Zertifikat enthält, ein selbst-signiertes Server-Zertifikat automatisch generiert und eingebunden, sobald irgendeine Acronis-Komponente installiert wird (mit Ausnahme der Acronis Backup & Recovery 10 Management Console).

Sollte die Maschine nach Erstellung des selbst-signierten Zertifikates umbenannt werden, so können Sie dieses Zertifikat nicht länger verwenden, sondern müssen ein neues erstellen.

So erstellen Sie ein neues selbst-signiertes Zertifikat

1. Melden Sie sich als Mitglied der Administrator-Gruppe an.
2. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie ein: **cmd**
3. Führen Sie folgenden Befehl aus (beachten Sie die Anführungszeichen):
   ```
   "%CommonProgramFiles%\Acronis\Utils\acroniscert" --reinstall
   ```
4. Starten Sie Windows oder die laufenden Acronis-Dienste neu.

Nicht-selbst-signierte Zertifikate

Als Alternative zu selbst-signierten Zertifikaten können Sie auch Zertifikate von unabhängigen, vertrauenswürdigen Zertifizierungsstellen (Certificate Authorities, CA) verwenden oder solche, die von der Zertifizierungsstelle Ihrer Firma mit Hilfe von Acronis Certificate Command-line Utility erstellt wurden.

So installieren Sie das Zertifikat einer unabhängigen Zertifizierungsstelle

1. Klicken Sie auf **Start**, dann auf **Ausführen** und geben Sie dort ein: **certmgr.msc**
2. Klicken Sie in der **Zertifikate**-Konsole doppelt auf den Namen des Zertifikates, das Sie installieren wollen.
3. Klicken Sie in der Registerlasche **Details** innerhalb der Liste der angezeigten Felder auf **Fingerabdruck**.
4. Wählen und kopieren Sie den Wert des Feldes (den Zertifikats-Fingerabdruck), eine Zeichenfolge etwa wie **20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85**.
5. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie Folgendes in das Feld **Öffnen** ein:

   ```
   "%CommonProgramFiles%\Acronis\Utils\acroniscert.exe"     --install
   "20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85"
   ```

   (Beachten Sie die Anführungszeichen, ersetzen Sie den hier gezeigten Beispiels-Fingerabdruck mit dem Ihres tatsächlichen Zertifikates.)

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. 431) oder zum Management Server (S. 427) 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. 428) 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 Optionen des Management Servers

Die Optionen für den Management Server ermöglichen Ihnen, das Verhalten von Acronis Backup & Recovery 10 Management Server zu steuern.

Um auf die Optionen des Management Servers zuzugreifen, verbinden Sie die Konsole zum Management Server und wählen dann **Optionen > Management Server Optionen** im Menü.

3.2.1 Aufzeichnungslevel

Diese Option legt fest, ob der Management Server das Log der Ereignisse auf den registrierten Maschinen im zentralen Log sammeln muss, das in einer zugeordneten Datenbank gespeichert wird und in der Ansicht **Log** zur Verfügung steht. Sie können die Option für alle Ereignisse auf einmal setzen oder die Ereignistypen auswählen, die gesammelt werden. Wenn Sie das Sammeln von Ereigniseinträgen vollständig deaktivieren, wird das zentrale Log nur das Log des Management Servers enthalten.

Voreinstellung ist: **Logs sammeln** für **Alle Ereignisse**.

Benutzen Sie das Listenfeld **Ereignisse, die protokolliert werden**, um die Art der Ereignisse anzugeben, die gesammelt werden:

- **Alle Ereignisse** – alle Ereignisse (Informationen, Warnungen und Fehler) der auf dem Management Server registrierten Maschinen werden in das zentrale Log eingetragen.
- **Fehler und Warnungen** – Warnungen und Fehler werden im zentralen Log aufgezeichnet.
- **Nur Fehler** – nur Fehler werden im zentralen Log aufgezeichnet.

Um das Sammeln der Ereignis-Logs auszuschalten, deaktivieren Sie das Kontrollkästchen **Logs sammeln**.

3.2.2 Log-Bereinigungsregeln

Diese Option spezifiziert, wie das zentrale Ereignis-Log bereinigt wird, das in der Berichtsdatenbank des Management Server gespeichert ist.

Diese Option definiert die maximale Größe der Berichtsdatenbank.

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.

Auch wenn Sie die Größenbeschränkung für das Log entfernen, werden ab einer Log-Größe von 4 GB keine weiteren Ereignisse in einer SQL Server Express Datenbank protokolliert, da die Datenbankgröße für die SQL Express Edition auf 4 GB beschränkt ist. Setzen Sie die maximale Log-Größe auf ca. 3,8 GB, um die maximale Größe der SQL Express Datenbank zu nutzen.

Diesen Parameter können Sie auch im Acronis Administrative Template (S. 361) setzen.

3.2.3 Ereignisverfolgung

Sie können den Management Server so konfigurieren, dass er die Ereignisse außer in seinem eigenen Log auch in der Ereignisanzeige von Windows protokolliert.

Sie können den Management Server so konfigurieren, dass er Simple Network Management Protocol (SNMP)-Objekte an einen spezifizierten SNMP-Manager sendet.

Ereignisanzeige von Windows

Diese Option definiert, ob der Management Server seine eigenen Ereignis-Logs in der Ereignisanzeige von Windows aufzeichnen muss. (Um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**.) Sie können die Ereignisse filtern, die aufgezeichnet werden.

Voreinstellung ist: **Ausgeschaltet**.

Wählen Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option einzuschalten.

Verwenden Sie das Kontrollkästchen **Ereignisse, die protokolliert werden**, um die Ereignisse zu filtern, die in der Ereignisanzeige von Windows aufgeführt werden:

- **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
- **Fehler und Warnungen**
- **Nur Fehler**.

Deaktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option auszuschalten.

SNMP-Benachrichtigungen

Diese Option definiert, ob der Management Server seine eigenen Ereignis-Logs an spezifizierte Simple Network Management Protocol (SNMP)-Manager schicken muss. 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. 50)“.

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.

3.2.4 Domain-Zugriffsberechtigungen

Die Option bestimmt den vom Management Server verwendeten Benutzernamen und das Kennwort, um auf die Domain zuzugreifen.

Voreinstellung ist: Keine Anmeldedaten

Der Management Server benötigt Domain-Anmeldedaten, wenn er mit einer dynamischen Gruppe arbeitet, die auf dem **Organisationseinheit**-Kriterium (S. 333) basiert. Wenn Sie eine solche Gruppe erstellen und über diese Option keine Anmeldedaten angegeben werden, wird das Programm von Ihnen die Anmeldedaten erfragen und in dieser Option speichern.

Es ist ausreichend, die Anmeldedaten eines Benutzers zu spezifizieren, der Mitglied der Gruppe **Domain-Benutzer** auf der Domaine ist.

3.2.5 Acronis WOL Proxy

Diese Option funktioniert in Kombination mit den erweiterten Planungseinstellungen für **Wake-On-LAN verwenden** (S. 180). Verwenden Sie diese Option, wenn der Management Server Backup-Maschinen in einem anderen Subnetz einschalten soll.

Kurz bevor die geplante Aktion startet, verschickt der Management Server so genannte 'Magic Packets', um die entsprechenden Maschinen einzuschalten. (Ein Magic Packet ist ein Paket, das 16 Mal in Folge die MAC-Adresse der Empfänger-Netzwerkkarte enthält). Der in dem anderen Subnetz installierte Acronis WOL Proxy sendet die Pakete an die Maschinen in diesem Subnetz.

Voreinstellung ist: **Ausgeschaltet**.

So aktivieren Sie diese Option:

1. Installieren Sie Acronis WOL Proxy auf einem Server im Subnetz, auf dem die Maschinen sich befinden, die Sie einschalten möchten. Bei diesem Server muss eine ständige Verfügbarkeit der Dienste gewährleistet sein. Wenn mehrere Subnetze vorhanden sind, installieren Sie Acronis WOL Proxy in jedem Subnetz, in dem Sie die Funktion Wake-On-LAN benötigen.
2. So aktivieren Sie **Acronis WOL Proxy** in den **Optionen des Management Servers**:
   a. Aktivieren Sie das Kontrollkästchen **Folgende Proxies verwenden**.

b. Klicken Sie auf **Hinzufügen** und geben Sie den Namen oder die IP-Adresse der Maschine ein, auf der der Acronis WOL Proxy installiert ist. Geben Sie die Anmeldedaten für die Maschine ein.

c. Wiederholen Sie diesen Schritt, wenn es mehrere Acronis WOL Proxies gibt.

3. Aktivieren Sie beim Planen einer Backup-Richtlinie die Einstellung **Wake-On-LAN verwenden**.

Sie können außerdem Proxies aus der Liste löschen. Denken Sie daran, dass jede Änderung dieser Option Auswirkungen auf den gesamten Management Server hat. Wenn Sie einen Proxy aus der Liste löschen, wird die Funktion Wake-On-LAN im entsprechenden Subnetz für alle Richtlinien, einschließlich der bereits angewandten Richtlinien, deaktiviert.

3.2.6 Optionen für VM-Schutz

Diese Optionen definieren das Verhalten eines Management Servers, bezogen auf Backup und Recovery von virtuellen Maschinen, die auf einem Virtualisierungsserver gehostet werden.

VMware vCenter-Integration

Diese Option definiert die Anzeige von virtuellen Maschinen, die durch einen VMware vCenter Server im Management Server verwaltet werden und die Anzeige des Backup-Status dieser Maschinen im vCenter.

Integration ist für alle Acronis Backup & Recovery 10 Advanced Editions verfügbar, eine Virtual Edition-Lizenz ist nicht erforderlich. Auf dem vCenter Server wird keine Software-Installation benötigt.

Auf Seite des Management Servers

Bei aktivierter Integration erscheint die Inventaranzeige **VMs and Templates** des vCenters in der Benutzeroberfläche des Management Servers, unter **Navigation** –> **Virtuelle Maschinen**.

Aus Sicht des Management Servers handelt es sich um eine dynamische Gruppe von virtuellen Maschinen. Der Gruppenname entspricht dem Namen oder der IP-Adresse des vCenter Servers, je nachdem, was bei Konfiguration der Integration angegeben wurde. Der Inhalt der Gruppe wird mit dem vCenter Server synchronisiert und kann auf Seite des Management Servers nicht geändert werden. Sollte es zu einer zeitweiligen Inkonsistenz kommen, dann klicken Sie mit der rechten Maustaste auf die Gruppe und wählen **Aktualisieren**.

Die vom vCenter Server verwalteten virutellen Maschinen erscheinen außerdem in der Gruppe **Alle virtuellen Maschinen**. Die können sich die Eigenschaften und den Betriebszustand der virtuellen Maschinen anzeigen lassen, Gruppen virtueller Maschinen erstellen und virtuelle Maschinen zu existierenden Gruppen hinzufügen.

Für eine virtuelle Maschine ist kein Backup und Recovery möglich, außer der Acronis Backup & Recovery 10 Agent für ESX/ESXi wurde zum Host der virtuellen Maschine verteilt (S. 338). Solche Maschinen erscheinen als nicht verwaltbar (ausgegraut).

Sobald der Agent zu einem ESX/ESXi-Host verteilt wurde (erfordert eine Lizenz für Acronis Backup & Recovery 10 Advanced Server Virtual Edition), sind die virtuellen Maschinen dieses Host bereit für die Verteilung einer Backup-Richtlinie oder für ein individuelles Backup. Solche Maschinen erscheinen als verwaltbar.

*Wenn ein Agent für Windows oder ein Agent für Linux in einem Gast-System installiert ist, auf seinem Host aber kein Agent für ESX/ESXi vorhanden ist, erscheint die virtuelle Maschine unter **Virtuelle Maschinen** als nicht verwaltbar. Eine solche Maschine muss wie eine physikalische verwaltet werden.*

Auf Seite des vCenter Servers

Bei aktivierter Integration speichert und zeigt der vCenter Server Informationen darüber an, wann und wie jede virtuelle Maschine per Backup gesichert wurde. Dieselben Informationen werden in den Spalten **Status** und **Letztes Backup** auf dem Management Server angezeigt.

Backup-Status – der schwerwiegendste Status aller Backup-Pläne und Backup-Richtlinien auf der Maschine. Zu weiteren Informationen siehe „Backup-Plan-Zustände (S. 192)“ und „Richtlinien-Status auf einer Maschine (S. 67)“.

Letztes Backup – wie viel Zeit seit dem letzten erfolgreichen Backup verstrichen ist.

Sie können diese Informationen in der Zusammenfassung der virtuellen Maschine einsehen (**Summary** –> **Annotations**) oder auf der Registerlasche **Virtual Machines** für jeden Host, Datacenter, Ordner oder gesamten vCenter Server (beispielsweise **View** –> **Inventory** –> **Hosts and Clusters** –> Host wählen –> **Virtual Machines**).

3.2.7 Online Backup-Proxy

Diese Option ist nur für Verbindungen zum Acronis Online Backup Storage über das Internet wirksam.

Diese Option bestimmt, ob sich der Management Server mit dem Internet über einen Proxy-Server verbinden soll.

Beachten Sie: *Acronis Backup & Recovery 10 unterstützt nur HTTP- und HTTPS-Proxy-Server.*

Die Proxy-Einstellungen für Agent und Management Server müssen separat konfiguriert werden, auch wenn sie auf derselben Maschine installiert sind.

So ändern Sie die Proxy-Server-Einstellungen

1. Aktivieren Sie das Kontrollkästchen **Einen Proxy-Server verwenden**.
2. Geben Sie unter **Adresse** den Netzwerknamen oder die IP-Adresse des Proxy-Servers an – beispielsweise: **proxy.beispielname.com** oder **192.168.0.1**
3. Spezifizieren Sie unter **Port** die Port-Nummer des Proxy-Servers – beispielsweise: **80**
4. Sollte der Proxy-Server eine Authentifizierung benötigen, dann geben Sie die entsprechenden Anmeldedaten unter **Benutzername** und **Kennwort** an.
5. Klicken Sie auf die Schaltfläche **Verbindung testen**, wenn Sie die Proxy-Server-Einstellungen überprüfen wollen.

3.3 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.

3.3.1 Verwaltung der Maschine

Diese Option legt fest, ob die Maschine zentral durch Acronis Backup & Recovery 10 Management Server verwaltet werden muss.

Um diese Option nutzen zu können, müssen Sie als Mitglied der Gruppe der **Administratoren** auf der Maschine angemeldet sein.

Sie können die Maschine auf dem Management Server registrieren, wenn Sie den Acronis Backup & Recovery 10 Agent installieren. Wenn die Maschine nicht registriert ist, wählen Sie **Zentrale Verwaltung**, das wird die Registrierung (S. 428) einleiten. Alternativ können Sie die Maschine auch serverseitig im Management Server hinzufügen. Jede der drei beschriebenen Registrierungsmethoden erfordert die Privilegien eines Administrators.

Die Auswahl von **Autonome Verwaltung** auf einer registrierten Maschine wird die Kommunikation der Maschine mit dem Server stoppen. Die Maschine erscheint als **Zurückgezogen** auf dem Management Server. Der Management Server Administrator kann die Maschine vom Server löschen oder die Maschine erneut registrieren.

Voreinstellung ist: **Autonome Verwaltung**.

So richten Sie die zentrale Verwaltung auf der Maschine ein:

1. Wählen Sie **Zentrale Verwaltung**.
2. Spezifizieren Sie die Angaben für **Management Server IP/Name**.
3. Spezifizieren Sie auf Anforderung den Benutzernamen und das Kennwort des Administrators des Management Servers.
4. Unter **Registrierungsadresse der Maschine** wählen Sie aus, wie die Maschine auf dem Management Server registriert wird: anhand des Namens (empfohlen) oder anhand der IP-Adresse.
5. Klicken Sie auf **OK** und die Maschine wird auf dem Management Server registriert.

Um die zentrale Verwaltung auszuschalten, wählen Sie **Autonome Verwaltung**.

3.3.2 Ereignisverfolgung

Es ist möglich, die von auf der verwalteten Maschine agierenden Agenten erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder 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. 97) 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.

Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

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

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse in der Ereignisanzeige von Windows aufzeichnen müssen. (Um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**.) Sie können die Ereignisse filtern, die geloggt werden.

Sie können die Einstellungen in den Standardoptionen für Backup und Recovery (S. 97) 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.

Voreinstellung ist: **Ausgeschaltet**.

Wählen Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option einzuschalten.

Verwenden Sie das Kontrollkästchen **Ereignisse, die protokolliert werden**, um die Ereignisse zu filtern, die in der Ereignisanzeige von Windows aufgeführt werden:

- **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
- **Fehler und Warnungen**
- **Nur Fehler**.

Deaktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option auszuschalten.

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. 97) 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. 50)“.

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. 95).

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.

3.3.3 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 (S. 366) setzen.

3.3.4 Online Backup-Proxy

Diese Option ist nur wirksam, wenn Backup- und Recovery-Aktionen mit dem Acronis Online Backup Storage über das Internet durchgeführt werden.

Diese Option bestimmt, ob sich der Acronis Agent mit dem Internet über einen Proxy-Server verbinden soll.

Beachten Sie: *Acronis Backup & Recovery 10 unterstützt nur HTTP- und HTTPS-Proxy-Server.*

So ändern Sie die Proxy-Server-Einstellungen

1. Aktivieren Sie das Kontrollkästchen **Einen Proxy-Server verwenden**.
2. Geben Sie unter **Adresse** den Netzwerknamen oder die IP-Adresse des Proxy-Servers an – beispielsweise: **proxy.beispielname.com** oder **192.168.0.1**
3. Spezifizieren Sie unter **Port** die Port-Nummer des Proxy-Servers – beispielsweise: **80**
4. Sollte der Proxy-Server eine Authentifizierung benötigen, dann geben Sie die entsprechenden Anmeldedaten unter **Benutzername** und **Kennwort** an.
5. Klicken Sie auf die Schaltfläche **Verbindung testen**, wenn Sie die Proxy-Server-Einstellungen überprüfen wollen.

Wenn Sie die Proxy-Server-Einstellungen nicht kennen, bitten Sie Ihren Netzwerk-Administrator oder Internetzugangsprovider um Unterstützung.

Alternativ können Sie auch versuchen, diese Einstellungen aus der Konfiguration Ihres Webbrowsers zu entnehmen. Die nachfolgenden Befehle zeigen, wo Sie diese in drei populären Webbrowsern finden können.

- **Microsoft Internet Explorer.** Klicken Sie im Menü **Extras** auf den Befehl **Internetoptionen**. Klicken Sie in der Registerlasche **Verbindungen** auf den Befehl **LAN-Einstellungen**.
- **Mozilla Firefox.** Klicken Sie im Menü **Extras** auf den Befehl **Einstellungen** und dann auf **Erweitert**. Klicken Sie in der Registerlasche **Netzwerk**, im Bereich **Verbindung**, auf den Befehl **Einstellungen**.
- **Google Chrome.** Klicken Sie unter **Optionen** auf **Details**. Und im Bereich **Netzwerk** dann auf **Proxy-Einstellungen ändern**.

3.3.5 Programm zur Kundenzufriedenheit (CEP)

Diese Option legt fest, ob die Maschine am Acronis Programm zur Kundenzufriedenheit (ACEP) teilnimmt.

Falls Sie **Ja, ich möchte am ACEP teilnehmen** aktivieren, werden auf der Maschine Hardware-Konfigurationsinformationen, am häufigsten und am wenigsten verwendete Funktionen sowie Probleme gesammelt und regelmäßig an Acronis geschickt. Die Ergebnisse sind dazu gedacht, Verbesserungen bei der Software und Funktionalität zu ermöglichen, um die Bedürfnisse von Acronis-Kunden noch besser zu erfüllen.

Acronis sammelt keine persönliche Daten. Lesen Sie die Teilnahmebedingungen auf der Acronis-Website oder in der Benutzeroberfläche des Produkts, um mehr über das ACEP zu erfahren.

Die Option wird anfangs während der Installation des Acronis Backup & Recovery 10-Agenten konfiguriert. Sie können diese Einstellung jederzeit in der Benutzeroberfläche des Programms ändern (**Optionen** –> **Optionen der Maschine** –> **Programm zur Kundenzufriedenheit (CEP)**). Diese Option kann außerdem durch Verwendung der Gruppenrichtlinien-Infrastruktur (S. 369) konfiguriert werden. Eine per Gruppenrichtlinie definierte Einstellung kann nicht durch Verwendung der

Programmoberfläche geändert werden, außer die Gruppenrichtlinie wird auf der Maschine deaktiviert.

3.4 Standardoptionen für Backup und Recovery

3.4.1 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 Windows		**Bootfähiges Medium (Linux-basiert oder PE-basiert)**	
	Laufwerk-Backup	**Datei-Backup**	**Laufwerk-Backup**	**Datei-Backup**
Schutz des Archivs (S. 99) (Kennwort und Verschlüsselung)	+	+	+	+
Ausschluss von Quelldateien (S. 100)	+	+	+	+
Vor-/Nach-Befehle für das Backup (S. 101)	+	+	nur PE	nur PE
Befehle vor/nach der Datenerfassung (S. 103)	+	+	-	-
Multi-Volume-Snapshot (S. 105)	+	+	-	-
Snapshot für Backup auf Dateiebene (S. 105)	-	+	-	-
VSS verwenden (S. 106)	+	+	-	-

Komprimierungsrate (S. 107)	+	+	+	+
Backup-Performance:				
Backup-Priorität (S. 107)	+	+	-	-
Schreibgeschwindigkeit auf Laufwerk (S. 108)	Ziel: HDD	Ziel: HDD	Ziel: HDD	Ziel: HDD
Datendurchsatz im Netzwerk (S. 108)	Ziel: Netzlaufwerk	Ziel: Netzlaufwerk	Ziel: Netzlaufwerk	Ziel: Netzlaufwerk
Beschleunigtes inkrementelles und differentielles Backup (S. 111)	+	-	+	-
Backup-Aufteilung (S. 112)	+	+	+	+
Sicherheit auf Dateiebene (S. 112):				
Dateisicherheitseinstellungen in den Backups erhalten	-	+	-	-
Verschlüsselte Dateien in Archiven unverschlüsselt speichern	-	+	-	-
Medienkomponenten	Ziel: Wechselmedien	Ziel: Wechselmedien	-	-
Fehlerbehandlung (S. 114):				
Während der Durchführung keine Meldungen bzw. Dialoge zeigen (stiller Modus)	+	+	+	+
Bei Fehler neu versuchen	+	+	+	+
Fehlerhafte Sektoren ignorieren	+	+	+	+
Dual-Destination (S. 115)	Ziel: lokal	Ziel: lokal	-	-
Task-Startbedingungen (S. 115)	+	+	-	-
Task-Fehlerbehandlung (S. 116)	+	+	-	-
Band-Unterstützung (S. 117)	Ziel: Verwaltetes Depot in einer Bandbibliothek	Ziel: Verwaltetes Depot in einer Bandbibliothek	Ziel: Verwaltetes Depot in einer Bandbibliothek	Ziel: Verwaltetes Depot in einer Bandbibliothek
Erweiterte Einstellungen (S. 119):				
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

Archivattribut zurücksetzen	-	+	-	+
Nach Abschluss des Backups die Maschine automatisch neu starten	-	-	+	+
Backup nur nach dem Übertragen zum Depot deduplizieren	Ziel: dedupl. Depot	Ziel: dedupl. Depot	Ziel: dedupl. Depot	Ziel: dedupl. Depot
FTP im Modus 'Aktiv' verwenden	Ziel: FTP-Server	Ziel: FTP-Server	Ziel: FTP-Server	Ziel: FTP-Server
Benachrichtigungen:				
E-Mail (S. 109)	+	+	-	-
Win Pop-up (S. 110)	+	+	-	-
Ereignisverfolgung:				
Ereignisanzeige von Windows (S. 110)	+	+	-	-
SNMP (S. 111)	+	+	-	-

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.

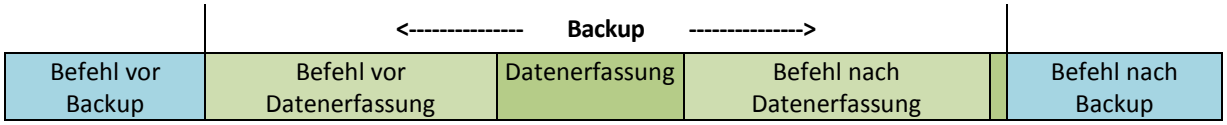
   Wenn das Kontrollkästchen nicht ausgewählt ist, dann hat das Ergebnis der Befehlsausführung keinen Einfluss auf Erfolg oder Misserfolg des Tasks. Sie können das Ergebnis der Befehlsausführung durch Ansicht des Logs oder der Fehler und Warnungen verfolgen, die auf dem **Dashboard** dargestellt werden.
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 (S. 106) 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. 101) 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.

Multi-Volume Snapshot

Diese Option ist nur wirksam für Windows-Betriebssysteme.

Diese Option gilt immer für Backups auf Festplattenebene (Images). Diese Option gilt auch für Backups auf Dateiebene, wenn diese unter Verwendung eines Snapshots erstellt werden. (Die Option Snapshot für Backup auf Dateiebene (S. 105) bestimmt, ob bei einem solchen Backup ein Snapshot

benutzt wird oder nicht.)

Die Option bestimmt, ob Snapshots mehrerer Volumes gleichzeitig erfolgen oder einer nach dem anderen.

Voreinstellung ist: **Aktiviert.**

Wenn diese Option auf **Aktivieren** gesetzt wird, werden die Snapshots aller zu sichernden Volumes zum gleichen Zeitpunkt erstellt. Benutzen Sie diese Option, um ein zeitkonsistentes Backup von Daten zu erstellen, die über mehrere Datenträger verteilt sind, z.B. für eine Oracle Datenbank.

Wenn diese Option auf **Deaktivieren** gesetzt wird, erfolgen die Snapshots der Volumes nacheinander. Falls sich also Daten über mehrere Volumes erstrecken, werden diese zu unterschiedlichen Zeiten gesichert und das resultierende Backup könnte nicht konsistent sein.

Volume Shadow Copy Service

Diese Option ist nur wirksam für Windows-Betriebssysteme.

Diese Option definiert, ob ein Provider für einen Volume Shadow Copy Service (VSS, Schattenkopie-Dienst für Volumes) – entweder Acronis VSS oder Microsoft VSS – Anwendungen, die VSS-kompatibel sind, über den Start eines Backups benachrichtigen muss. Dies sichert einen konsistenten Zustand der Daten, die von den Anwendungen benutzt werden, vor allem aber die Vollendung aller Datenbank-Transaktionen für den Moment, in dem Acronis Backup & Recovery 10 den Snapshot nimmt. Datenkonsistenz sichert vor allem, dass die Anwendung in einem korrekten Zustand wiederhergestellt wird und unmittelbar nach der Wiederherstellung operational ist.

Voreinstellung ist: **Snapshots unter Verwendung von VSS erstellen**

Acronis Backup & Recovery 10 wählt den VSS-Provider automatisch, abhängig vom auf der Maschine laufenden Betriebssystem und ob die Maschine Mitglied einer Active Directory-Domain ist.

Snapshots ohne Verwendung von VSS erstellen

Verwenden Sie diese Option, wenn Ihre Datenbank mit VSS nicht kompatibel ist. Der Snapshot der Daten wird von Acronis Backup & Recovery 10 übernommen. Der Backup-Prozess ist am schnellsten, aber die Datenkonsistenz von Anwendungen, deren Transaktionen zum Zeitpunkt des Snapshots nicht vollendet sind, kann nicht garantiert werden. Sie können auch Befehle vor/nach der Datenerfassung (S. 103) verwenden, um anzugeben, welche Befehle vor und nach dem Snapshot ausgeführt werden sollen, um sicherzustellen, dass die Daten in einem konsistenten Zustand gesichert werden. Spezifizieren Sie z.B. einen Befehl vor der Datenerfassung, der diese Datenbank suspendiert und alle Cache-Speicher leert, um zu sichern, dass alle Transaktionen vollendet sind, und ergänzen Sie Befehle nach der Datenerfassung, damit die Datenbank nach dem Erstellen des Snapshots den Betrieb wieder aufnimmt.

Volume Shadow Copy Writer

Bevor Sie die Daten einer VSS-kompatiblen Anwendung sichern, müssen Sie sicherstellen, das die Volume Shadow Copy Writer für diese Anwendung eingeschaltet sind – und zwar, indem Sie die Liste der Writer untersuchen, die im Betriebssystem präsent sind. Um diese Liste anzusehen, benutzen Sie den Befehl:

```
vssadmin list writers
```

Beachten Sie: *In Microsoft Windows Small Business Server 2003 ist der Writer für Microsoft Exchange Server 2003 als Standard ausgeschaltet. Anweisungen, wie Sie den Writer aktivieren, finden Sie im entsprechenden Artikel von Microsoft Hilfe und Support http://support.microsoft.com/kb/838183/de.*

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, die von den Backup-Aktionen auf verwalteten Maschinen erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder an spezifizierte SNMP-Manager zu senden.

Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

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

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse der Backup-Aktionen in der Ereignisanzeige von Windows aufzeichnen müssen. (Um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**.) Sie können die Ereignisse filtern, die geloggt werden.

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

Wählen Sie, ob Ereigniseinträge der Backup-Aktionen an die Ereignisanzeige von Windows übergeben 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. 92).
- **Folgende Ereignisse protokollieren** – für das Loggen der Ereignisse der Backup-Aktionen in der Ereignisanzeige. Arten der Ereignisse, die geloggt werden:
  - **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
  - **Fehler und Warnungen**
  - **Nur Fehler**
- **Nicht protokollieren** – für das Ausschalten der Protokollierung der Ereignisse der Backup-Aktionen in der Ereignisanzeige.

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. 50)“.

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. 92).
- **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.

Sicherheit auf Dateiebene

Diese Optionen sind nur für Backups auf Dateiebene unter Windows-Betriebssystemen wirksam.

Verschlüsselte Dateien in Archiven unverschlüsselt speichern

Diese Option definiert, ob die Dateien vor der Speicherung im Archiv entschlüsselt werden.

Voreinstellung ist: **Ausgeschaltet**.

Ignorieren Sie diese Option, wenn Sie keine Verschlüsselung benutzen. Aktivieren Sie diese Option, wenn verschlüsselte Dateien in das Backup einbezogen werden und Sie wollen, dass ein beliebiger Benutzer nach der Wiederherstellung auf die Dateien zugreifen kann. Andernfalls wird nur der Benutzer, der die Dateien bzw. Verzeichnisse ursprünglich verschlüsselt hat, darauf zugreifen können. Die Entschlüsselung ist auch nützlich, wenn Sie verschlüsselte Dateien auf verschiedenen Maschinen wiederherstellen wollen.

*Die Dateiverschlüsselung steht in Windows zur Verfügung unter Verwendung des NTFS-Dateisystems mit Encrypting File System (EFS). Um auf die Verschlüsselungseinstellungen einer Datei oder eines Verzeichnisses zuzugreifen, wählen Sie **Eigenschaften > Allgemein > Erweitert> Inhalt verschlüsseln**.*

Dateisicherheitseinstellungen in Archiven erhalten

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

Voreinstellung ist: **Aktiviert.**

Wenn die Option eingeschaltet ist, werden Dateien und Ordner mit der ursprünglichen Erlaubnis zum Lesen, Schreiben oder Ausführen für jeden Benutzer oder jede Benutzergruppe im Archiv gespeichert. Wenn Sie auf einer Maschine geschützte Dateien bzw. Ordner ohne den in den Berechtigungen angegebenen Benutzer wiederherstellen, werden Sie wahrscheinlich nicht in der Lage sein, diese Dateien bzw. Ordner zu lesen oder zu verändern.

Um dieses Problem zu beseitigen, sollten Sie die Aufbewahrung von Dateisicherheitseinstellungen in Archiven unwirksam machen. Die wiederhergestellten Dateien und Ordner erben dann immer die Rechte des Ordners, in den sie wiederhergestellt werden, oder die der Festplatte, wenn sie an der Wurzel wiederhergestellt werden.

Alternativ können Sie die Wiederherstellung (S. 124) der Sicherheitseinstellungen unwirksam machen, selbst wenn diese im Archiv gespeichert sind. Das Ergebnis wird das gleiche sein – die Dateien erben die Zugriffsrechte vom übergeordneten Ordner.

*Um auf die NTFS-Zugriffsrechte von Datei oder Ordnern zuzugreifen, wählen Sie **Eigenschaften** > **Sicherheit**>.*

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. 422) 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. 172) und Bedingungen (S. 184).

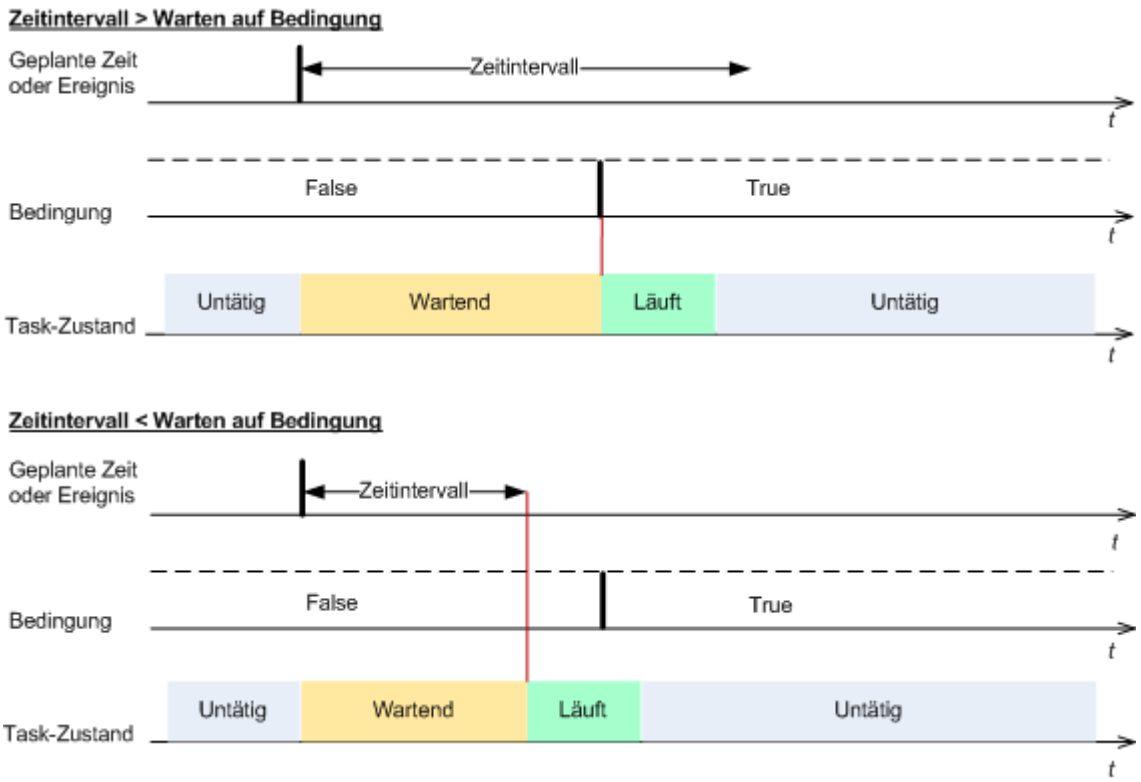
Voreinstellung ist: **Warten, bis die Bedingungen erfüllt sind.**

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

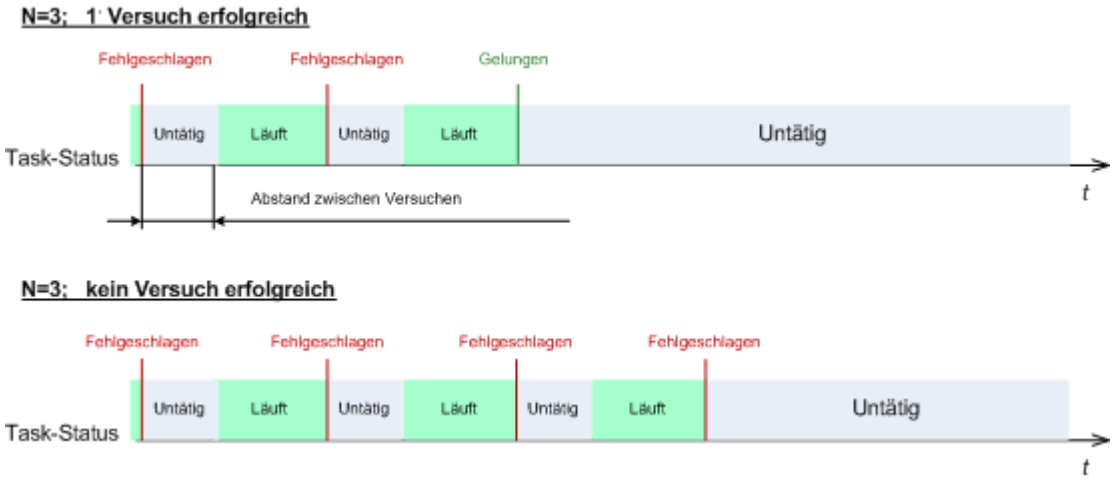
Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

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.

Band-Unterstützung

Diese Optionen sind wirksam, wenn das Backup-Ziel ein verwaltetes Depot auf einer Bandbibliothek ist.

Mit Hilfe der Optionen für die **Band-Unterstützung** können Sie angeben, wie Backups durch die Backup-Tasks auf die Bänder verteilt werden.

Bei einigen Kombinationen der Bandoptionen kann die Verwendungseffizienz der gesamten Bandbibliothek sowie der einzelnen Bänder beeinträchtigt werden. Wenn Sie diese Optionen nicht aufgrund einiger spezieller Anforderungen ändern müssen, lassen Sie sie unverändert.

Ein Archiv kann mehrere Bänder beanspruchen. In solchen Fällen wird ein sogenannter **Bandsatz** zur Aufbewahrung der Backups verwendet.

Ein **Bandsatz** ist eine logische Gruppe aus einem oder mehreren Bändern, die Backups von bestimmten geschützten Daten enthalten. Ein Bandsatz kann auch Backups anderer Daten enthalten.

Ein **separater Bandsatz** ist ein Bandsatz, der nur Backups von speziellen geschützten Daten enthält. Andere Backups können nicht auf einen separaten Bandsatz geschrieben werden.

(Für die zu erstellende Backup-Richtlinie/den zu erstellenden Backup-Plan) Einen separaten Bandsatz verwenden

Voreinstellung ist: **Ausgeschaltet**.

Wenn Sie diese Option unverändert lassen, werden die Backups, die zur erstellten Richtlinie oder zum erstellten Plan gehören, möglicherweise auf Bänder geschrieben, die Backups enthalten, die mit anderen Backup-Richtlinien geschrieben wurden und Daten anderer Maschinen enthalten. In

ähnlicher Weise können Backups von anderen Richtlinien auf Bänder geschrieben werden, die Backups dieser Richtlinie enthalten. Solche Bänder verursachen allerdings keine Probleme, da das Programm die Bänder automatisch verwaltet.

Wenn diese Option aktiviert ist, werden die Backups, die zur erstellten Richtlinie bzw. zum erstellten Plan gehören, in einen separaten Bandsatz eingeordnet. Andere Backups werden nicht auf diesen Bandsatz geschrieben.

Wenn die Konsole mit dem Management Server verbunden ist

Die Option **Einen separaten Bandsatz verwenden** lässt sich noch genauer definieren. Sie können also für die zu erstellende Backup-Richtlinie einen separaten Bandsatz für alle Maschinen oder für jede einzelne Maschine verwenden.

Standardmäßig ist die Option **Einen einzelnen Bandsatz für alle Maschinen** ausgewählt. Im Allgemeinen werden die Bänder mit dieser Option effizienter genutzt als mit der Option **Einen separaten Bandsatz für jede einzelne Maschine verwenden**. Die zweite Option kann jedoch z.B. hilfreich sein, wenn es spezielle Anforderungen gibt, die Bänder mit Backups von einer bestimmten Maschine außerhalb des Standorts zu lagern.

Wenn die Option **Einen separaten Bandsatz verwenden** aktiviert ist, kann es zu einer Situation kommen, in der das Backup auf ein Band geschrieben werden muss, das sich momentan nicht im Bandbibliothek-Gerät befindet. Bestimmen Sie, was in einem solchen Fall geschehen soll.

- **Auf Benutzerantwort warten** – Der Backup-Task gelangt in das Stadium **Interaktion erforderlich** und wartet darauf, dass das Band mit dem erforderlichen Label in das Bandbibliothek-Gerät geladen wird.
- **Freies Band benutzen** – Das Backup wird auf ein freies Band geschrieben, so dass die Aktion nur dann unterbrochen wird, wenn in der Bibliothek kein freies Band vorhanden ist.

Immer ein freies Band benutzen

Wenn Sie die folgenden Optionen unverändert lassen, wird jedes Backup auf das Band geschrieben, das durch die Option **Einen separaten Bandsatz verwenden** angegeben wird. Wenn einige der folgenden Optionen aktiviert sind, fügt das Programm einem Bandsatz immer dann neue Bänder hinzu, wenn ein Voll-Backup, ein inkrementelles oder ein differentielles Backup erstellt wird.

- **Für jedes Voll-Backup**

Voreinstellung ist: **Ausgeschaltet**.

Wenn diese Option aktiviert ist, wird jedes Voll-Backup auf ein freies Band geschrieben. Das Band wird speziell für diese Aktion in ein Laufwerk geladen. Wenn die Option **Einen separaten Bandsatz verwenden** aktiviert ist, werden nur inkrementelle und differentielle Backups auf dem Band angefügt.

- **Für jedes differentielle Backup**

Voreinstellung ist: **Ausgeschaltet**.

Wenn diese Option aktiviert ist, wird jedes differentielle Backup auf ein freies Band geschrieben. Diese Option ist nur verfügbar, wenn die Option zur Verwendung eines freien Bandes für jedes Voll-Backup ausgewählt ist.

- **Für jedes inkrementelle Backup**

Voreinstellung ist: **Ausgeschaltet**.

Wenn diese Option aktiviert ist, wird jedes inkrementelle Backup auf ein freies Band geschrieben. Diese Option ist nur verfügbar, wenn die Option zur Verwendung eines freien Bandes für jedes Voll-

Backup und jedes differentielle Backup ausgewählt ist.

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 (S. 70).

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. 285).

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.

3.4.2 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:

- Die 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 Windows		**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. 122)	+	+	nur PE	nur PE
Recovery-Priorität (S. 124)	+	+	-	-
Sicherheit auf Dateiebene (S. 124):				
Dateien mit ihren Sicherheitseinstellungen wiederherstellen	-	+	-	+
Fehlerbehandlung (S. 127):				
Meldungen und Dialogboxen während der Aktion nicht zeigen (stiller Modus)	+	+	+	+

Neu versuchen, wenn ein Fehler auftritt	+	+	+	+
Erweiterte Einstellungen (S. 128):				
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. 125)	+	+	-	-
Win Pop-up (S. 126)	+	+	-	-
Ereignisverfolgung:				
Ereignisanzeige von Windows (S. 126)	+	+	-	-
SNMP (S. 127)	+	+	-	-

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 (S. 112) 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, die von den Recovery-Aktionen auf verwalteten Maschinen erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder an spezifizierte SNMP-Manager zu senden.

Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

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

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse der Recovery-Aktionen in der Windows Ereignisanzeige (Unterpunkt Anwendungen) aufzeichnen müssen (um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**). Sie können die Ereignisse filtern, die geloggt werden.

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

Wählen Sie, ob Ereigniseinträge der Recovery-Aktionen an die Ereignisanzeige von Windows übergeben werden.

Wählen Sie eine der nachfolgenden Varianten:

- **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. 92).

- **Folgende Ereignisse protokollieren** – für das Loggen der Ereignisse der Recovery-Aktionen in der Ereignisanzeige. Arten der Ereignisse, die geloggt werden:
  - **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
  - **Fehler und Warnungen**
  - **Nur Fehler**
- **Nicht protokollieren** – für das Ausschalten der Protokollierung der Ereignisse der Recovery-Aktionen in der Ereignisanzeige.

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. 50)“.

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. 92).
- **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.

Zentrale und persönliche Depots

Ein zentrales Depot ist ein im Netzwerk liegender Speicherort, der vom Administrator des Management Servers zugeteilt wird, um als Speicherplatz für die Backup-Archive zu dienen. Ein zentrales Depot kann von einem Storage Node verwaltet werden (verwaltetes Depot) oder es wird

nicht verwaltet.

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.

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.

 **Zentral**. Diese Gruppe ist verfügbar, wenn die Konsole mit einer verwalteten Maschine oder einem Management Server verbunden ist. Erweitern Sie die Gruppe, damit eine Liste zentraler, vom Management Server Administrator hinzugefügter Depots angezeigt wird.

Klicken Sie auf ein zentrales Depot im Depot-Verzeichnisbaum, um eine Detailansicht dieses Depots (S. 132) zu öffnen und führen Sie dann Aktionen mit dem Depot (S. 133) bzw. den dort gespeicherten Archiven (S. 168) und Backups (S. 169) aus.

 **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. 165) zu öffnen und führen Sie dann Aktionen mit dem Depot (S. 167) bzw. den dort gespeicherten Archiven (S. 168) und Backups (S. 169) aus.

4.1 Zentrale Depots

Ein zentrales Depot ist ein im Netzwerk liegender Speicherort, der vom Administrator des Management Servers zugeteilt wird, um als Speicherplatz für die Backup-Archive zu dienen. Ein zentrales Depot kann von einem Storage Node verwaltet werden oder er ist nicht verwaltet. Die Zahl und die 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 verteilt. Der Shortcut zum Depot erscheint auf den Maschinen in der Gruppe **Depots –> Zentral**. Jeder Backup-Plan, der auf den Maschinen existiert, einschließlich lokaler 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 ist, werden die Archive des Benutzers, genauso wie andere im Depot gespeicherte Archive, durch den Storage Node verwaltet.

Verwaltete Depots

Ein verwaltetes Depot ist ein zentrales Depot, das durch einen Storage Node verwaltet wird.

Der Storage Node führt Bereinigungen (S. 421) und Validierungen (S. 429) für jedes im verwalteten Depot gespeicherte Archiv so durch, wie durch die Backup-Pläne (S. 420) beschrieben. Bei Erstellung eines verwalteten Depots kann ein Administrator zusätzliche, vom Storage Node durchzuführende Aktionen spezifizieren: Deduplizierung und Verschlüsselung. Zu weiteren Informationen siehe 'Durch Storage Nodes durchgeführte Aktionen'.

Ein verwaltetes Depot ist 'in sich geschlossen', es enthält alle Metadaten, die ein Storage Node zur Verwaltung des Depots benötigt. Ein Depot kann an einen anderen Storage Node angeschlossen

werden. Der neue Storage Node fragt die Metadaten von dem Depot ab und erstellt die Datenbank neu, die zur Verwaltung des Depots erforderlich ist. Zu weiteren Informationen siehe den Abschnitt 'Ein verwaltetes Depot anschließen (S. 138)'.

Auf verwaltete Depots zugreifen

Benutzer müssen Administrator- oder Benutzerberechtigungen haben, um auf das Depot zugreifen zu können. Administratoren des Management Servers erhalten diese Administratorberechtigungen standardmäßig. Berechtigungen für andere Benutzer können Sie bei Erstellung oder Bearbeitung des Depots definieren. Zu weiteren Informationen siehe den Abschnitt 'Benutzerberechtigungen auf einem Storage Node (S. 76)'.

Nicht verwaltete Depots

Ein nicht verwaltetes Depot ist ein zentrales Depot, das von keinem Storage Node verwaltet wird. Ein Benutzer muss Zugriffsrechte aus dem Netzwerk auf den betreffenden Speicherort haben, um auf ein nicht verwaltetes Depot zugreifen zu können.

Jeder Benutzer, der Berechtigungen zum Lesen/Schreiben von Dateien in ein nicht verwaltetes Depot hat, kann:

- Daten zu dem nicht verwalteten Depot per Backup sichern
- Daten von jedem im nicht verwalteten Depot liegenden Backup wiederherstellen
- alle im nicht verwalteten Depot hinterlegten Archive einsehen und verwalten.

4.1.1 Mit der Ansicht „Zentrales Depot“ arbeiten

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

Depot-Symbolleiste

Die Symbolleiste enthält einsatzbereite Schaltflächen, um mit dem gewählten zentralen Depot Aktionen auszuführen. Zu Details siehe den Abschnitt Aktionen für zentrale Depots (S. 133).

Tortendiagramm mit Beschriftung

Das **Tortendiagramm** ermöglicht Ihnen, die Auslastung des Depots einzuschätzen. Es zeigt das Verhältnis von freiem und belegtem Platz im Depot an. Das Tortendiagramm ist nicht verfügbar, wenn das Depot auf einer Bandbibliothek lokalisiert ist.

– 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.

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

- [nur für verwaltete Depots] der Name des Storage Nodes, der das Depot verwaltet
- vollständiger Pfad zum Depot
- Gesamtzahl der im Depot gespeicherten Archive und Backups
- das Verhältnis des belegten Speicherplatzes zur ursprünglichen Datengröße
- [nur für verwaltete Depots] Status der Deduplizierung (S. 69) (An, Aus)

- [nur für verwaltete Depots] Status der Verschlüsselung (Ja, Nein)

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. 168)

Aktionen mit Backups (S. 169)

Archive filtern und sortieren (S. 171)

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 Aktionen für zentrale Depots

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

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit zentralen Depots.

Aktion	Lösung
Ein verwaltetes oder nicht verwaltetes Depot erstellen	1. Klicken Sie auf **Erstellen**. 2. Bestimmen Sie im Feld **Typ** die gewünschte Variante des Depots: **Verwaltet** oder **Nicht verwaltet**. Die Prozedur zur Erstellung zentraler Depots wird ausführlich in den nachfolgenden Abschnitten beschrieben: ▪ ein verwaltetes, zentrales Depot erstellen (S. 135) ▪ ein nicht verwaltetes zentrales Depot erstellen (S. 137)
Ein verwaltetes oder nicht verwaltetes Depot bearbeiten	1. Wählen Sie das Depot. 2. Klicken Sie auf **Bearbeiten**. Abhängig vom gewählten Depot (verwaltet oder nicht verwaltet) öffnet sich eine entsprechende Seite zur Bearbeitung:

	▪ Auf der Seite **Verwaltetes Depot bearbeiten** können Sie den Depotnamen, das Verschlüsselungs-Kennwort (sofern das Depot verschlüsselt ist) sowie die Informationen im Feld **Kommentare** bearbeiten. ▪ Auf der Seite **Nicht verwaltetes Depot bearbeiten** können Sie den Depotnamen sowie die Informationen im Feld **Kommentare** bearbeiten.
Ein Depot validieren	1. Wählen Sie das Depot. 2. Klicken Sie auf **Validieren**. Sie gelangen zur Seite Validierung (S. 252) mit dem bereits als Quelle vorausgewählten Depot. Die Validierung des Depots überprüft alle in diesem Depot enthaltenen Archive.
Ein Depot löschen	1. Wählen Sie das Depot. 2. Klicken Sie auf **Löschen**. Sie werden gefragt, ob Sie die im Depot gespeicherten Archive behalten wollen oder ob das Depot mitsamt all seiner Archive gelöscht werden soll. Pläne und Tasks, die dieses Depot verwenden, werden als Resultat der Aktion fehlschlagen. Wenn Sie sich dazu entschließen, die Archive eines verwalteten Depots zu behalten, dann wird das Depot vom Storage Node abgetrennt. Sie können dieses Depot aber später immer noch wieder an denselben oder einen anderen Storage Node anbinden.
Ein nicht verwaltetes Depot durchsuchen	1. Wählen Sie das nicht verwaltete Depot. 2. Klicken Sie auf **Durchsuchen**. Das Depot ist danach zur Untersuchung mit dem Standard-Datei-Manager verfügbar.
Ein verwaltetes Depot anschließen, das ohne Entfernung seines Inhaltes gelöscht wurde.	Klicken Sie auf **Anschließen**. Die Prozedur zum Anschließen eines verwalteten Depots an einen Storage Node wird ausführlich im Abschnitt Ein verwaltetes Depot anschließen (S. 138) beschrieben.
Benutzer-Anmeldedaten für den Zugriff auf ein Depot ändern.	Klicken Sie auf **Benutzer ändern**. Eine Änderung der Anmeldedaten ist nur für solche Depots verfügbar, die auf einem gemeinsam benutzten Speicherort liegen.
Informationen eines Depots aktualisieren	Klicken Sie auf **Aktualisieren**. Während Sie den Inhalt eines Depots einsehen, können Archive dem Depot hinzugefügt, von diesem gelöscht oder modifiziert werden. Klicken Sie auf **Aktualisieren**, damit die neusten Veränderungen für die Depot-Informationen berücksichtigt werden.
Aktionen für eine Bandbibliothek auf einem verwalteten Depot	
Band-Kennzeichnungen vergeben und eine Inventarisierung der Bandbibliothek auf einem verwalteten Depot ausführen	Klicken Sie auf **Bänder verwalten**. Definieren Sie im Fenster **Band-Verwaltung** Kennzeichnungen für die Bänder und aktualisieren Sie die Inventarisierung. Zu weiteren Details siehe den Abschnitt Bandbibliotheken verwalten (S. 145).

Bänder in einem verwalteten Depot erneut scannen	Klicken Sie auf **Bänder erneut scannen**. Das erneute Scannen liest Informationen über den Inhalt der vom Benutzer gewählten Bänder ein und aktualisiert die Datenbank des Storage Nodes. Diese Aktion wird ausführlich im Abschnitt Erneut scannen (S. 146) beschrieben.

Ein verwaltetes, zentrales Depot erstellen

So erstellen Sie ein verwaltetes, zentrales Depot

Depot

Name

Geben Sie dem Depot einen eindeutigen Namen. Eine Erstellung von zwei zentralen Depots mit gleichem Namen ist nicht gestattet.

Kommentare

[Optional] Vergeben Sie für das zu erstellende Depot eine charakteristische Beschreibung.

Typ

Wählen Sie den Typ **Verwaltet**.

Storage Node

Bestimmen Sie den Acronis Backup & Recovery 10 Storage Node, der das Depot verwalten wird. Sie müssen möglicherweise Anmeldedaten zum Zugriff auf den Storage Node eingeben.

Pfad (S. 136)

Spezifizieren Sie, wo das Depot erstellt wird. Verwaltete, zentrale Depots können auf einer Netzwerkfreigabe, einem SAN, NAS oder auf einer für den Storage Node lokalen Festplatte liegen.

Datenbankpfad (S. 136)

Spezifizieren Sie auf dem Speicher-Server einen lokalen Ordner, um dort eine Depot-spezifische Datenbank zu erstellen. Diese Datenbank wird die Metadaten speichern, die zur Katalogisierung von Archiven und zur Durchführung einer Deduplizierung benötigt werden.

Deduplizierung

[Optional] Bestimmen Sie, ob eine Archiv-Deduplizierung für das Depot aktiviert werden soll. Eine Deduplizierung reduziert den von Archiven belegten Speicherplatz und die Datenübertragungsmenge für Backups. Sie reduziert die Größe der im Depot liegenden Archive, indem redundante Daten (wie doppelte Dateien und Festplatten-Datenblöcke) eliminiert werden.

Auf Bandgeräten ist keine Deduplizierung möglich.

Um mehr darüber zu erfahren, wie Deduplizierung funktioniert, siehe den Abschnitt Deduplizierung (S. 70).

Komprimierung

[Optional] Bestimmen Sie, ob die Deduplizierungsdatenspeicher komprimiert werden sollen. Diese Einstellung ist nur verfügbar, sofern eine Deduplizierung aktiviert wurde.

Verschlüsselung (S. 136)

[Optional] Bestimmen Sie, ob das Depot per Verschlüsselung geschützt werden soll. Alle zum Depot geschriebenen Daten werden verschlüsselt und alle von ihm gelesenen werden durch den Storage Node wieder transparent entschlüsselt (unter Verwendung eines Depot-spezifischen, auf dem Storage Node hinterlegten Kodierungsschlüssels).

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um die Erstellung des verwalteten Depots auszuführen.

Pfad zum Depot

So spezifizieren Sie den Pfad, wo das verwaltete Depot erstellt wird

1. Tragen Sie den vollständigen Pfad zum Verzeichnis in das Feld **Pfad** ein oder wählen Sie den gewünschten Ordner im Verzeichnisbaum. Verwaltete Depots können organisiert werden:
   - auf für den Storage Node lokal verfügbaren Festplatten
   - auf einem Netzlaufwerk
   - auf einem Storage Area Network (SAN)
   - auf einem Network Attached Storage-Gerät (NAS)
   - auf einer Bandbibliothek, die lokal mit dem Storage Node verbunden ist.

   Um am gewählten Speicherort für das Depot einen neuen Ordner zu erstellen, klicken Sie auf **Ordner erstellen**.
2. Klicken Sie auf **OK**.

Ein Depot kann nur in einem leeren Ordner angelegt werden.

Es wird nicht empfohlen, ein selbst deduplizierendes *verwaltetes Depot auf einem FAT32-Volume zu erstellen. Ein solches Depot könnte alle deduplizierten Elemente möglicherweise in zu große Dateien speichern. Weil die maximale Dateigröße in den FAT-Dateisystemen auf 4 GB begrenzt ist, könnte der Storage Node aufhören zu arbeiten, wenn diese Grenze erreicht ist.*

*Die Zugriffsrecht des Ordner müssen dem Benutzerkonto, unter dem der Dienst des Storage Nodes läuft, (standardmäßig der **ASN User**) Schreibzugriffe erlauben. Spezifizieren Sie bei Vergabe der Zugriffsrechte das Benutzerkonto explizit (verwenden sie nicht einfach **Jeder**).*

Pfad zur Datenbank des Depots

So spezifizieren Sie den Pfad, wo die Depot-Datenbank erstellt wird

1. Wählen Sie aus den **Lokalen Ordnern** des Storage Nodes das gewünschte Verzeichnis aus oder geben Sie seinen vollständigen Pfad in das Feld **Pfad** ein.

   Um für die Datenbank einen neuen Ordner zu erstellen, klicken Sie auf **Ordner erstellen**.
2. Klicken Sie auf **OK**.

Bei Wahl des Ordners für die Datenbank des Depots sollten Sie folgende Aspekte berücksichtigen:

- Dieser Ordner muss auf einem fest eingebauten Laufwerk liegen. Versuchen Sie nicht, die Datenbank auf ein externes, entfernbares Laufwerk zu legen.
- Die Größe des Ordners kann beträchtlich werden – als Richtwert kann 200 GB pro 8 TB benutzten Speicherplatzes (also ca. 2,5 Prozent) dienen.
- Die Zugriffsrecht des Ordner müssen dem Benutzerkonto, unter dem der Dienst des Storage Nodes läuft, (standardmäßig der **ASN User**) Schreibzugriffe erlauben. Spezifizieren Sie bei Vergabe der Zugriffsrechte das Benutzerkonto explizit (verwenden sie nicht einfach **Jeder**).

Verschlüsselung des Depots

Wenn Sie ein Depot durch Verschlüsselung schützen, werden alle zu diesem Depot geschriebenen Daten verschlüsselt und alle von ihm gelesenen durch den Storage Node wieder transparent entschlüsselt (unter Verwendung eines Depot-spezifischen, auf dem Storage Node hinterlegten Kodierungsschlüssels). 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.

Diese Verschlüsselung hat nichts mit der Verschlüsselung von Archiven zu tun, wie sie über einen Backup-Plan spezifiziert und durch einen Agenten ausgeführt wird. Sollte ein Archiv bereits verschlüsselt sein, dann wird die Verschlüsselung aufseiten des Storage Nodes noch einmal über die durch den Agenten ausgeführte gelegt.

So schützen Sie ein Depot per Verschlüsselung

1. Aktivieren Sie das Kontrollkästchen **Verschlüsselung**.
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:
   - **AES 128** – die Depot-Inhalte werden mit Hilfe des Advanced Encryption Standard-Verfahrens (AES) und 128-Bit verschlüsselt.
   - **AES 192** – der Depot-Inhalt wird mit Hilfe von Advanced Standard Encryption (AES) und einem 192-Bit-Schlüssel verschlüsselt.
   - **AES 256** – der Depot-Inhalt 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 der im Depot gespeicherten Archive benötigen, 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 gespeichert, es wird nur der Kennwort-Hash-Wert für Bestätigungszwecke benutzt. Mit dieser zweistufigen Methode sind die Archive vor jedem unberechtigten Zugriff geschützt, aber ein verlorenes Kennwort kann unmöglich wiederhergestellt werden.

Ein nicht verwaltetes zentrales Depot erstellen

So erstellen Sie ein nicht verwaltetes, zentrales Depot

Depot

Name

Geben Sie dem Depot einen eindeutigen Namen. Eine Erstellung von zwei zentralen Depots mit gleichem Namen wird nicht gestattet.

Kommentare

Vergeben Sie für das zu erstellende Depot eine charakteristische Beschreibung.

Typ

Wählen Sie den Typ **Nicht verwaltet**.

Pfad (S. 138)

Spezifizieren Sie, wo das Depot erstellt wird.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um die Erstellung des nicht verwalteten, zentralen Depots auszuführen.

Pfad zum Depot

So spezifizieren Sie den Pfad, wo das nicht verwaltete Depot erstellt wird

1. Geben Sie den vollständigen Pfad zum Verzeichnis in das Feld 'Pfad' ein, oder wählen Sie den gewünschten Ordner aus dem Verzeichnisbaum. Nicht verwaltete Depots können organisiert werden:
   - Acronis Online Backup Storage
   - auf einer Netzwerkfreigabe
   - auf einem Storage Area Network (SAN)
   - auf einem Network Attached Storage-Gerät (NAS)
   - auf FTP- und SFTP-Servern.

   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 für das Depot einen neuen Ordner zu erstellen, klicken Sie auf 'Ordner erstellen'.

   Ein Depot kann nur in einem leeren Ordner angelegt werden.
2. Klicken Sie auf OK.

Ein verwaltetes Depot anschließen

Ein durch einen Storage Node verwaltetes Depot kann an einen anderen Storage Node angeschlossen werden. Das kann notwendig werden, wenn Sie Storage Node-Hardware ausrangieren, wenn der Storage Node verloren geht oder um Lastspitzen zwischen Storage Nodes auszugleichen. Als Folge stoppt der erste Storage Node die Verwaltung des Depots. Der zweite Knoten scannt die Archive des Depots, erstellt die zum Depot korrespondierende Datenbank, füllt sie mit Daten auf und beginnt dann mit der Verwaltung des Depots.

Beim Löschen eines verwalteten Depots erhalten Sie die Option, die im Depot enthaltenen Archive zu bewahren. Der sich so aus einer Löschaktion ergebende Speicherort kann ebenso an denselben oder einen anderen Storage Node angeschlossen werden.

Persönliche oder zentrale, nicht verwaltete Depots können nicht angeschlossen werden.

So schließen Sie ein verwaltetes Depot an einen Storage Node an

Depot

Storage Node

Bestimmen Sie den Acronis Backup & Recovery 10 Storage Node, der das Depot verwalten wird.

Pfad

Geben Sie den Pfad zu dem Speicherort an, wo die Archive gespeichert sind.

Datenbankpfad

Spezifizieren Sie auf dem Speicher-Server einen lokalen Ordner, um dort eine Depot-spezifische Datenbank zu erstellen. Diese Datenbank wird die Metadaten speichern, die zur Katalogisierung von Archiven und zur Durchführung einer Deduplizierung benötigt werden.

Kennwort

Stellen Sie das Kennwort für ein verschlüsseltes Depot zur Verfügung.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um das Anschließen des Depots auszuführen. Diese Prozedur kann eine gewisse Zeit benötigen, da der Storage Node die

Archive scannen muss, die Metadaten in die Datenbank schreibt und die Archive dedupliziert, sofern es ursprünglich ein deduplizierendes Depot war.

4.1.3 Bandbibliotheken

In diesem Abschnitt wird detailliert beschrieben, wie robotergestützte Bandgeräte als Depot zur Speicherung von Backup-Archiven verwendet werden.

Eine Bandbibliothek (Roboterbibliothek) ist eine Speichereinrichtung mit hoher Kapazität, die aus den folgenden Komponenten besteht:

- einem oder mehreren Bandlaufwerken
- mehreren (bis zu mehreren Tausend) Kassettenschächten zur Aufnahme der Bandkassetten
- einem oder mehreren Loadern (Robotermechanismen), deren Aufgabe im Wechseln der Bandkassetten zwischen den Kassettenschächten und den Bandlaufwerken besteht
- Barcode-Lesegeräten (optional).

Überblick

Acronis Backup & Recovery 10 bietet über den Acronis Backup & Recovery 10 Storage Node eine vollständige Unterstützung für Bandbibliotheken. Der Storage Node sollte auf der Maschine installiert sein, an die eine Bandbibliothek angeschlossen ist. Der Storage Node kann gleichzeitig mehr als eine Bandbibliothek zur Aufbewahrung von Archiven verwenden.

Zur Verwaltung der Medien in einer Bandbibliothek verwendet der Storage Node den Windows-Wechselmediendienst (RSM). Weitere Informationen finden Sie im Abschnitt RSM-Medienpools (S. 141).

In einer speziellen Datenbank des Storage Nodes werden die Informationen zum Backup-Inhalt gespeichert, der auf die Bänder geschrieben wurde. Auf diese Weise können einige Aktionen (z.B. eine Bereinigung (S. 421)) ziemlich schnell ausgeführt werden, ohne dass auf die Medien zugegriffen werden muss. Da die Inhaltsinformationen in der Datenbank gespeichert sind, ist es selbst dann möglich, den Inhalt eines auf einem Band befindlichen Backup-Archivs über die Konsole anzuzeigen, wenn die Bandbibliothek ausgeschaltet ist. Zum Erstellen eines inkrementellen oder differentiellen Backups verwendet das Programm die Datenbank, anstatt ein Band mit dem Voll-Backup zu laden, zu mounten, zurückzuspulen und zu lesen. Ein Band muss jedoch z.B. gelesen werden, um ein Backup zu validieren (S. 430) oder um Daten aus einem Backup wiederherzustellen.

Eine Bandbibliothek kann lokal an einer Maschine angeschlossen sein, auf der der Agent installiert ist. Das ist aber nur möglich, wenn die Bibliothek als einzelnes Bandlaufwerk angesehen wird. Der Agent kann ein solches Gerät verwenden, um Backups zu schreiben und zu lesen; jedoch unterscheidet sich das Format des Backups vom Format der Backups auf den Bändern, die durch den Storage Node geschrieben wurden. Informationen zur Lesbarkeit von Archiven auf Bändern, die von unterschiedlichen Komponenten anderer Produktversionen von Acronis Backup & Recovery 10 geschrieben wurden, finden Sie im Abschnitt Bandkompatibilitätstabelle (S. 48).

Acronis Backup & Recovery 10 ermöglicht Ihnen, eine Verteilung der Backups nach Medien festzulegen. Z.B. kann ein separater Bandsatz für das Backup spezieller Daten verwendet werden und die Backups aller anderen Daten werden auf ein beliebiges, im Moment gemountetes Band geschrieben, das selbst nicht zu dem Bandsatz gehört. Weitere Informationen finden Sie im Abschnitt Band-Unterstützung (S. 117).

Die Backup-Schemata (Großvater-Vater-Sohn (S. 36), Türme von Hanoi (S. 40)) unterstützen Sie spürbar durch die Erstellung einer effektiven Planung und von Aufbewahrungsrichtlinien für die

Backups in einer Bandbibliothek. In Kombination mit den Bandoptionen ermöglichen Ihnen die Backup-Schemata (im automatischen Modus), die Bänder wiederzuverwenden, die nach dem Löschen von Backups als frei angesehen werden. Weitere Informationen finden Sie im Abschnitt Bandrotation (S. 149).

Hardware

Eine Bandbibliothek (Roboterbibliothek) ist eine Speichereinrichtung mit hoher Kapazität, die aus den folgenden Komponenten besteht:

- einem oder mehreren Bandlaufwerken
- mehreren (bis zu mehreren Tausend) Kassettenschächten zur Aufnahme der Bandkassetten
- einem oder mehreren Loadern (Robotermechanismen), deren Aufgabe im Wechseln der Bandkassetten zwischen den Kassettenschächten und den Bandlaufwerken besteht
- Barcode-Lesegeräten (optional).

An der Seite der Kassette jedes Bandes kann ein spezielles Label angebracht sein, das folgende Elemente enthält:

- einen Barcode, der durch ein spezielles Lesegerät eingescannt werden kann; dieses Lesegerät ist in der Regel an einem Loader befestigt
- einen lesbaren Ziffernwert für den Barcode.

Solche Labels werden zur Identifizierung der Bänder in der Bandbibliothek bzw. speziell für die Lagerung außerhalb des Standorts verwendet.

Wenn alle Kassetten in einer Bandbibliothek über Barcodes verfügen, kann die Bibliothek automatisch durch eine Software verwaltet werden.

Bandbibliotheken sind eine kostengünstige Lösung für Datenspeicher mit einer hohen Kapazität. Zudem eignen sich Bänder perfekt für eine Archivierung, da die Kassetten außerhalb des Standorts gelagert werden können, wodurch die Sicherheit der Daten noch erhöht wird. Allerdings ist zum Lesen selbst kleiner Datenmengen aus einer Bandbibliothek erheblich mehr Zeit erforderlich (von einigen Sekunden bis hin zu einigen Minuten) als bei anderen Typen von Datenspeichern. Die optimale Verfahrensweise bei der Verwendung von Bändern ist durch „WENIGER Lese-/Schreibanforderungen bei GRÖSSEREN Datenmengen“ gegeben. Daher ist ein systematischer Zugriff auf sehr große Datenmengen eher für eine Bandbibliothek geeignet als der zufällige Zugriff auf kleinere Datenmengen.

Einschränkungen

Bei Verwendung von Bandbibliotheken gelten folgende Einschränkungen:

1. Die Aktion Konsolidierung (S. 426) ist für Archive, die sich auf Bändern befinden, nicht möglich. Es ist nicht möglich, ein einzelnes, separates Backup von einem Band zu löschen. Es ist nicht möglich, alle auf einem Band gespeicherten Backups zu löschen. Nach dieser Aktion können jedoch alle inkrementellen und differentiellen Backups, die auf anderen Bändern gespeichert sind und auf den gelöschten Backups basieren, nicht zur Datenwiederherstellung verwendet werden. In den Aufbewahrungsrichtlinien eines **benutzerdefinierten** Backup-Plans ist die Option **Wenn sich das Löschen eines Backups auf andere Backups auswirkt –> Das Backup konsolidieren** deaktiviert. Hier ist nur die Option **Löschung aufschieben** verfügbar.
2. Deduplizierung (S. 423) ist für Archive, die sich auf Bandspeichergeräten befinden, nicht verfügbar.
3. Eine Dateiwiederherstellung aus einem auf einem Band gespeicherten Disk-Backup ist zwar möglich, kann aber sehr lange dauern.

4. Ein Band mit Backups, die durch den Storage Node geschrieben wurden, kann aufgrund von Unterschieden im Bandformat nicht auf einem Bandgerät gelesen werden, das lokal an eine Maschine angeschlossen ist, auf der der Agent installiert ist. Informationen zur Lesbarkeit von Archiven auf Bändern, die von unterschiedlichen Komponenten anderer Produktversionen von Acronis Backup & Recovery 10 geschrieben wurden, finden Sie im Abschnitt Bandkompatibilitätstabelle (S. 48).
5. Barcode-Drucker werden nicht verwendet.

RSM-Medienpools

Acronis Backup & Recovery 10 verwendet den Windows-Wechselmediendienst (RSM) zur Verwaltung von Bandkassetten, die Bestandteil von Bandbibliotheken sind.

Zur Trennung des Zugriffs auf Medien durch unterschiedliche Programme verwendet RSM logische Mediengruppen, sogenannte „Medienpools“. Im Manager gibt es zwei Kategorien von Medienpools: **System** und **Anwendung**.

Zu den Medienpools vom Typ **System** gehören der Pool **Freie Medien**, der Pool **Import** und der Pool **Unbekannte Medien**. In den **Systempools** werden Medien gehalten, die momentan nicht von Anwendungen verwendet werden. Im Pool **Freie Medien** befinden sich Medien, die als frei angesehen werden und von Anwendungen verwendet werden können. Der Pool **Import** und der Pool **Unbekannte Medien** sind temporäre Pools für Medien, die neu in einer bestimmten Bibliothek sind.

Über den Wechselmediendienst kann eine Anwendung ihre eigenen Pools mit eigenem Namen erhalten, Medien aus dem Pool **Freie Medien** in ihre eigenen Pools verschieben, die Medien in ihren eigenen Pools für bestimmte Zwecke verwenden, Medien an den Pool **Freie Medien** zurückgeben usw.

Der Storage Node in Acronis Backup & Recovery 10 verwaltet die Bänder, die zum **Acronis**-Pool gehören.

Wenn Sie die Kassettenschächte einer Bandbibliothek mit nicht verwendeten Bändern füllen, werden alle Bänder automatisch in den Pool **Freie Medien** gestellt.

Wenn ein Band bereits verwendet wurde, versucht der Wechselmediendienst, die registrierte Anwendung zu erkennen, auf die sich das Band bezieht. Wenn die Anwendung nicht gefunden wird, verschiebt der Wechselmediendienst das Band in den Pool **Unbekannte Medien**. Wenn die Anwendung nicht gefunden wird, aber die RSM-Datenbank keine Informationen zu dem Band hat, wird es in den Pool **Import** verschoben. Wenn die RSM-Datenbank über die Informationen verfügt, wird das Band in seinen eigenen Pool für die Anwendung verschoben.

Der Acronis Backup & Recovery 10 Storage Node ermöglicht dem Wechselmediendienst, Bänder zu erkennen, die mit Produkten der Familien Acronis True Image Echo, Acronis True Image 9.1 oder mit Acronis Backup & Recovery 10-Komponenten geschrieben wurden. Der Storage Node findet alle Bänder, die während der Aktion Inventarisierung (S. 145) im „Acronis“-Format in den **Acronis**-Pool geschrieben wurden.

Die Acronis Backup & Recovery 10-Komponenten verwenden den Pool **Unbekannte Medien** nicht. Wenn Sie die Verwendung eines Bandes aus diesem Pool erzwingen möchten, verschieben Sie das Band unter Verwendung des Wechselmedien-Snap-Ins in den Pool **Freie Medien** (**Systemsteuerung –> Verwaltung –> Computerverwaltung –> Wechselmedien –> Medienpools**).

*Wenn ein Band in den Pool **Freie Medien** verschoben wurde, wird es als frei angesehen und Anwendungen können darauf zugreifen und schreiben. Dadurch gehen die Daten auf dem Band verloren.*

Wenn alle Backups von einem Band gelöscht wurden, wird dieses nicht an den Pool **Freie Medien** zurückgegeben. Es verbleibt im **Acronis**-Pool als freies Band, das wiederverwendet werden kann. Wenn also ein Storage Node ein neues Band benötigt, dann sucht er zunächst im **Acronis**-Pool und erst danach im Pool **Freie Medien** nach einem freien Band.

Danach arbeitet der Acronis Backup & Recovery 10 Storage Node nur mit den Bändern, die zum **Acronis**-Pool gehören.

Erste Schritte bei der Verwendung einer Bandbibliothek

Wenn Sie ein Bandbibliothek-Gerät an eine Maschine angeschlossen haben, auf der der Acronis Backup & Recovery 10 Storage Node installiert ist und Sie ein Backup zur Bandbibliothek durchführen möchten, dann müssen Sie lediglich einen Archivspeicher auf dem Gerät erstellen, das unter Storage Node-Verwaltung steht.

Voraussetzungen

Ein Bandbibliothek-Gerät muss entsprechend der Installationsanweisungen des Geräteherstellers auf einer Maschine installiert werden, auf der Windows ausgeführt wird.

Wenn der Wechselmediendienst (RSM) in Ihrer Windows-Version enthalten ist, dann muss er aktiviert werden.

In Microsoft Windows XP und Microsoft Windows Server 2003:

- Der Wechselmediendienst ist Teil des Betriebssystems und wird zu Beginn aktiviert.

So aktivieren Sie den Wechselmediendienst in Microsoft Windows Server 2008:

1. Klicken Sie auf **Verwaltung > Serververwaltung > Funktionen > Funktion hinzufügen**.
2. Aktivieren Sie das Kontrollkästchen **Wechselmediendienst**.

So aktivieren Sie den Wechselmediendienst in Microsoft Windows Vista:

1. Klicken Sie auf **Systemsteuerung –> Programme –> Programme und Funktionen –> Windows-Funktionen ein- oder ausschalten**.
2. Aktivieren Sie das Kontrollkästchen **Wechselmedienverwaltung**.

Füllen Sie die Kassettenschächte der Bibliothek mit Bandkassetten. Wenn ein Band keinen Barcode erhält oder sein Barcode beschädigt ist, dann können Sie zur späteren Identifikation ein Label für das Band definieren.

Auf den lokalen und Remote-Maschinen sollten der Acronis Backup & Recovery 10 Management Server sowie die Acronis Backup & Recovery 10 Management Console installiert sein und der Acronis Backup & Recovery 10 Storage Node sollte auf der Maschine mit dem Bandbibliothek-Gerät installiert sowie auf dem Management Server registriert sein.

Bandbibliothek als verwaltetes Depot

Um Datensicherungsaktionen unter Verwendung einer Bandbibliothek zu ermöglichen, müssen Sie ein verwaltetes Depot für die Bandbibliothek erstellen. Sie können ein Depot über die Konsolenansicht **Zentrale Depots** erstellen. Weitere Informationen finden Sie im Abschnitt Erstellen eines verwalteten, zentralen Depots (S. 135).

Am einfachsten ist es jedoch, ein Depot über die Ansicht **Storage Nodes** zu erstellen. Wählen Sie dazu den Storage Node aus, mit dem die Bandbibliothek verbunden ist und klicken Sie dann auf **Depot erstellen**. Die Seite **Zentrales Depot erstellen** wird mit den vorausgewählten Parametern

angezeigt. Sie müssen lediglich den **Namen** des Depots angeben, bevor Sie auf **OK** klicken.

Nachdem Sie das Depot erstellt haben, können Sie darauf über die Konsolenansicht **Zentrale Depots** zugreifen. Daraufhin kann die Bandbibliothek für Backups verwendet werden.

Mit Acronis Backup & Recovery 10 kann nur ein Depot pro Bandgerät erstellt werden.

Wenn alle Kassetten einer Bandbibliothek über Barcodes verfügen und der Pool **Freie Medien** im Wechselmediendienst genügend Bänder für das ausgewählte Backup-Schema enthält, kann die Bibliothek vollautomatisch eingesetzt werden.

Sie können mit dem Depot selbst dann arbeiten, wenn alle Kassettenschächte der Bandbibliothek leer sind. Wenn während der Backup-Aktion keine Bänder in den Kassettenschächten der Bandbibliothek verfügbar sind, werden Sie im Fenster **Tasks erfordern Interaktion** aufgefordert, ein Band zu laden.

Wenn der Barcode des Bandes nicht gelesen werden kann, werden Sie in einem weiteren Fenster **Tasks erfordern Interaktion** aufgefordert, das Band mit einem Label zu versehen.

Aktionen mit einem Banddepot

Wenn in der Seitenleiste **Navigation** der Konsole ein Banddepot ausgewählt wird, enthält die Symbolleiste auf der Seite **Zentrale Depots** die beiden folgenden Aktionen, die nur für Bandbibliotheken verwendet werden können:

- Durch die Aktion **Bänder verwalten** wird das Fenster **Bandverwaltung** geöffnet, in dem Sie die Informationen zu den Kassettenschächten der Bibliothek aktualisieren, die Bänder in den Kassettenschächten inventarisieren und Labels für die Bänder definieren können. Wenn Sie einem Band ein neues Label zugewiesen haben, können Sie mit Hilfe dieser Aktion das Band kurz auswerfen, um das gleiche Label an der Außenseite der Kassette anzubringen.
- Durch die Aktion **Bänder erneut durchsuchen** wird das Fenster **Bänder werden neu durchsucht** angezeigt. In diesem können Sie Kassettenschächte auswählen und die Aktion Erneut durchsuchen (S. 146) starten, um einige spezielle Informationen zum Inhalt der angegebenen Bänder zu lesen.

Auf einem Banddepot können die Funktionen **Bearbeiten**, **Löschen**, **Validieren** und **Aktualisieren** ausgeführt werden.

Es ist zu beachten, dass diese Funktionen über einige spezielle Features für eine Bandbibliothek verfügen. So können Sie mit der Aktion **Bearbeiten** ein Bandbibliothek-Gerät ersetzen, ohne die Aktion **Erneut durchsuchen** ausführen zu müssen. Durch die Aktion **Löschen** werden alle Informationen auf dem ausgewählten Banddepot aus der Datenbank des Storage Nodes entfernt, d.h. dass die Aktion die Inhaltsdaten aller Bänder löscht, sobald diese Daten vom Storage Node auf dem Bandbibliothek-Gerät verwendet werden.

*Bei der Aktion **Löschen** wird der Inhalt des Depots aus der Datenbank im Storage Node gelöscht, ohne dass auf die Bänder zugegriffen wird. Pläne und Tasks, die dieses Depot verwenden, werden als Resultat der Aktion fehlschlagen.*

*Die Backup-Archive, die zu einem gelöschten zentralen Depot auf einer Bandbibliothek gehören, werden ebenfalls gelöscht. Diese Archive können jedoch über einen beliebigen Storage Node mit Hilfe der Aktion **Erneut durchsuchen** wiederhergestellt werden.*

Aktionen mit Archiven auf Bändern in einer Bibliothek

Die folgenden Funktionen werden häufig bei der Archivdatenverwaltung für ein in der Konsolenansicht **Zentrale Depots** ausgewähltes Backup-Archiv eingesetzt, wenn das aktuelle Depot

eine Bandbibliothek ist: **Validieren**, **Löschen**, **Alle Archive löschen**. Eine Löschung der Datenbank im Storage Node erfolgt, ohne dass auf die Bänder zugegriffen wird. Ein Backup-Archiv, das aus einem Banddepot gelöscht wird, kann nach dem Löschen durch die Aktion Erneut durchsuchen (S. 146) wiederhergestellt werden. Dieser Vorgang wird dann bei allen Bändern durchgeführt, auf denen die Daten des Archivs gespeichert sind.

Wenn von einem Band ein Backup gelöscht wurde, dann kann dieses Backup durch die Aktion **Erneut durchsuchen** wiederhergestellt werden, da hierbei die Informationen zum Inhalt des Backups in der Datenbank im Storage Node neu erstellt werden.

Wenn alle Backups von einem Band gelöscht wurden, wird dieses als frei angesehen. Das hat zur Folge, dass gelöschte Backups unwiederbringlich verloren sind, sobald wieder neu auf das Band geschrieben wird.

Backup in einer Bandbibliothek

Beim Erstellen einer Backup-Richtlinie/eines Backup-Plans mit einem Bandbibliothek-Ziel richten Sie das Backup genau so ein wie bei anderen Speichergeräten. Der einzige Unterschied besteht in den zusätzlichen Optionen für die Band-Unterstützung (S. 117), die während der Erstellung der Backup-Richtlinie/des Backup-Plans eingerichtet werden können. Diese Optionen ermöglichen Ihnen anzugeben, wie die erstellte Backup-Richtlinie bzw. der erstellte Backup-Plan Bänder aus der Bandbibliothek verwenden soll; die Optionen sind jedoch bereits so eingestellt, dass die Nutzungseffizienz der gesamten Bandbibliothek und jedes einzelnen Bandes gesteigert wird.

Wenn Sie die Bandoptionen sehen und ändern möchten, wählen Sie **Optionen –> Standardoptionen für Backup und Wiederherstellung –> Backup-Standardoptionen –> Band-Unterstützung** aus dem oberen Menü.

Wenn Sie die Einstellungen der zu erstellenden Backup-Richtlinie bzw. des zu erstellenden Backup-Plans ändern möchten, klicken Sie im Abschnitt **Backup-Optionen** auf der Seite **Backup-Richtlinie/Backup-Plan erstellen** auf **Ändern…**. Dadurch wird das Fenster **Backup-Optionen** geöffnet, wo die Seite **Band-Unterstützung** mit den vordefinierten Werten angezeigt wird.

Wenn Sie das Backup zu einem Band durchführen und das Ende des Bandes erreicht ist, dann wird automatisch ein freies Band gemountet und die Aktion wird mit dem neuen Band fortgesetzt.

Während ein Backup-Task ausgeführt wird, können Sie über die Konsole auf die folgenden bandspezifischen Informationen zugreifen:

- Anzahl der Bänder, die vom aktuellen Backup-Vorgang verwendet werden
- Labels der Bänder, die bis zum aktuellen Zeitpunkt vom Task verwendet wurden (für den Fall, dass das Backup aufgeteilt wird)
- Label des Bandes, auf das im Moment geschrieben wird.

Wiederherstellung aus einer Bandbibliothek

Die Wiederherstellung von Daten aus Archiven, die sich auf Bandgeräten befinden, erfolgt in derselben Art und Weise wie bei anderen Speichergeräten.

Bei der Wiederherstellung beginnen Sie mit der Erstellung eines Recovery-Tasks. Danach wählen Sie das Depot sowie das Archiv und das Backup aus, aus dem Daten wiederhergestellt werden sollen. Bei Erstellung des Tasks verwendet das Programm die Datenbank im Storage Node, anstatt auf die Bänder zuzugreifen. Allerdings erfordert die Auswahl der wiederherzustellenden Daten (d.h. einige Dateien oder bestimmte Volumes) das Lesen von einem oder mehreren Bändern und kann daher zeitaufwendig sein.

Das Programm findet die Bänder und legt sie automatisch in der richtigen Reihenfolge ein. Das Fenster **Task erfordert Interaktion** wird angezeigt, wenn ein benötigtes Band nicht gefunden wird.

Denken Sie daran, dass bei der Ausführung einer Datenwiederherstellung möglicherweise auf mehrere Bänder zugegriffen werden muss. Bei Recovery aus einem inkrementellen Backup kann es z.B. erforderlich sein, die folgenden, Backups enthaltenden Bänder zu laden, zu mounten, zurückzuspulen und zu lesen:

- Bänder, auf denen das inkrementelle Backup gespeichert ist, das zur Wiederherstellung der Daten ausgewählt wurde
- Bänder, auf denen das Voll-Backup gespeichert wurde, das als letztes vor dem inkrementellen Backup erstellt wurde
- Bänder, auf denen das differentielle Backup gespeichert wurde, das als letztes nach dem letzten Voll-Backup, aber vor dem ausgewählten inkrementellen Backup erstellt wurde, falls notwendig
- Bänder, die alle inkrementellen Backups enthalten, die nach dem letzten Voll-Backup oder dem letzten differentiellen Backup vor dem ausgewählten inkrementellen Backup erstellt wurden, falls notwendig.

Während ein Recovery-Task ausgeführt wird, können Sie über die Verwaltungskonsole auf die folgenden bandspezifischen Informationen zugreifen:

- Labels von allen Bändern, die möglicherweise für die Aktion benötigt werden
- Label des Bandes, das im Moment gelesen wird
- Labels der Bänder, die bereits gelesen wurden
- Labels der Bänder, die darauf warten, noch gelesen zu werden, mit Informationen zu ihrer momentanen Verfügbarkeit (geladen oder nicht).

Verwalten einer Bandbibliothek

Zur Verwaltung einer Bandbibliothek sind im Produkt die folgenden Tasks/Vorgänge verfügbar:

- Inventarisierung (S. 145)
- Erneut scannen (S. 146)
- Labeling (Kennzeichnen) (S. 146)

Jeder Benutzer mit Zugriff auf ein verwaltetes Depot auf einer Bandbibliothek kann diese Aktionen ausführen. Es ist jedoch nicht möglich, dass zwei oder mehr Benutzer eine Bandbibliothek gleichzeitig verwalten, da einige Aktionen mehrere Minuten, Stunden und sogar Tage dauern können. Wenn z.B. ein Benutzer den Task **Erneut durchsuchen** auf einer Bandbibliothek startet, werden die Anforderungen anderer Benutzer zur Ausführung desselben Tasks automatisch storniert, da er bereits auf dem Depot ausgeführt wird.

Inventarisierung

Ein Storage Node benötigt Informationen zu einem Band in seiner eigenen Datenbank, um mit dem Band arbeiten zu können. Nach Erstellung des Depots besteht daher der nächste Schritt im Allgemeinen darin, die Bänder zu inventarisieren.

Inventarisierung ist ein Vorgang, der es dem Storage Node ermöglicht, die Bänder zu erkennen, die momentan in den Kassettenschächten der Bandbibliothek geladen sind. Dieser Vorgang ist relativ schnell durchzuführen. Dabei werden normalerweise nur die Barcodes der Kassetten gelesen, ohne dass die Daten auf den Bändern gelesen werden müssen. Wenn ein Barcode nicht gelesen werden kann, dann wird das Band gemountet, damit nur sein GUID-Bezeichner gelesen werden kann.

Die **Inventarisierung** kann manuell durch einen Benutzer oder automatisch durchgeführt werden, wenn ein Zugriff auf kürzlich hinzugefügte Bänder erforderlich ist.

Zum Starten des Vorgangs wählen Sie das Banddepot in der Seitenleiste **Navigation** der Konsole aus. Klicken Sie auf **Bänder verwalten** und klicken Sie dann im Fenster **Bandverwaltung** auf **Inventarisierung starten**.

Wenn die Inventarisierung abgeschlossen ist, erhält der Benutzer eine Liste der Bänder, die momentan in der Bibliothek geladen sind.

Führen Sie diesen Vorgang jedes Mal aus, wenn Sie neue Bänder in die Kassettenschächte der Bandbibliothek laden.

Erneut scannen

Wie bereits erwähnt, speichert der Storage Node Informationen zu Bändern und ihren Inhalten in einer speziellen Datenbank. Beim Task **Erneut durchsuchen** werden Informationen zum Inhalt von Bändern, die vom Benutzer ausgewählt werden, gelesen und die Datenbank aktualisiert.

Der Task kann sehr lange dauern und kann daher nur manuell gestartet werden. Sie sollten alle Kassettenschächte auswählen, die ein Band enthalten, das Sie neu durchsuchen möchten, bevor Sie den Task starten.

Führen Sie den Task **Erneut durchsuchen** aus:

- für Bänder, die für den Storage Node unbekannt sind
- wenn die Datenbank im Storage Node verloren gegangen oder beschädigt ist
- für Bänder, deren Inhalt veraltet ist (wenn z.B. der Inhalt eines Bandes durch einen anderen Storage Node oder manuell verändert wurde).

Denken Sie daran, dass möglicherweise einige Backups auf dem Band erhalten bleiben, die vor dem erneuten Durchsuchen des Bandes gelöscht wurden. Daher werden nach Abschluss des Tasks alle derartigen Backups in der Datenbank im Storage Node wiederhergestellt und für die Datenwiederherstellung verfügbar gemacht.

Beim erneuten Durchsuchen sollte das Label eines Bandes in der Datenbank im Storage Node gespeichert werden. Wenn ein für den Vorgang ausgewählter Kassettenschacht ein Band enthält, das noch immer kein Label hat, dann wird der Task **Erneut durchsuchen** für das Band unterbrochen, damit der Vorgang Labeling (S. 146) ausgeführt werden kann.

Labeling (Kennzeichnen)

Wenn ein für die Datenwiederherstellung erforderliches Band nicht gefunden werden kann, wird das Fenster **Task erfordern Interaktion** angezeigt, in dem der Benutzer aufgefordert wird, das Band zu besorgen und in einen Kassettenschacht der Bandbibliothek einzuführen. Alle Bandkassetten benötigen also einen Barcode oder ein anderweitig lesbares Label.

Sollte ein Band kein Label haben, müssen Sie ein solches definieren, bevor das Band verwendet wird.

Wenn Sie für ein Band ein bestimmtes Label (z.B. „MeineArbeit“ für ein Band, auf dem speziell Backups von Daten im Verzeichnis „C:\Arbeit“ erstellt werden) anstelle eines Barcode-Labels einsetzen müssen, dann verwenden Sie ebenfalls den Vorgang **Labeling**.

Wählen Sie zum Starten des Vorgangs das Banddepot in der Seitenleiste **Navigation** der Konsole aus und klicken Sie in der Symbolleiste auf **Bänder verwalten**. Daraufhin wird im Fenster

Bandverwaltung eine Liste der Kassettenschächte der Bibliothek angezeigt, die Bänder enthalten. Für jedes Band, das zum Pool **Freie Medien** oder **Acronis** gehört, wird im Datenfeld für den Kassettenschacht das Label angezeigt. Für Bänder im Pool **Importmedien**, die von Acronis erstellte Backups enthalten, wird ebenfalls das Label angezeigt (dabei kann es sich z.B. um Bänder aus anderen Bandbibliotheken handeln).

Ein nicht verwendetes Band mit einem Barcode erhält standardmäßig ein Label, das diesem Barcode entspricht. Wenn ein Barcode fehlt oder beschädigt ist, dann wird die Bezeichnung des Labels automatisch erstellt. Sie können vorgeschlagene Labels übernehmen oder ein eigenes Label als einfachen Text angeben.

Bänder aus dem Pool **Freie Medien** oder **Importmedien** können umbenannt werden, sofern das Benutzerkonto, mit dem der Dienst für den Storage Node ausgeführt wird (**ASN User**), Schreibzugriff auf diese Pools hat. Diese Rechte werden dem **ASN User** nicht während der Installation zugewiesen und müssen daher möglicherweise manuell hinzugefügt werden.

Wenn Sie ein eigenes Label für ein Band definieren möchten, wählen Sie ein damit zusammenhängendes Datenfeld aus, geben Sie ein neues Label ein, klicken Sie auf **Band auswerfen**, bringen Sie dieselbe Beschriftung auf der Kassette an (um eine Verbindung mit dem Label herzustellen) und setzen Sie das Band wieder in denselben Kassettenschacht ein.

Nachdem alle erforderlichen Bandlabels angegeben wurden, drücken Sie auf **Label festlegen**, um die Labels in der Datenbank im Storage Node zu speichern.

Band-Unterstützung

Diese Optionen sind wirksam, wenn das Backup-Ziel ein verwaltetes Depot auf einer Bandbibliothek ist.

Mit Hilfe der Optionen für die **Band-Unterstützung** können Sie angeben, wie Backups durch die Backup-Tasks auf die Bänder verteilt werden.

Bei einigen Kombinationen der Bandoptionen kann die Verwendungseffizienz der gesamten Bandbibliothek sowie der einzelnen Bänder beeinträchtigt werden. Wenn Sie diese Optionen nicht aufgrund einiger spezieller Anforderungen ändern müssen, lassen Sie sie unverändert.

Ein Archiv kann mehrere Bänder beanspruchen. In solchen Fällen wird ein sogenannter **Bandsatz** zur Aufbewahrung der Backups verwendet.

Ein **Bandsatz** ist eine logische Gruppe aus einem oder mehreren Bändern, die Backups von bestimmten geschützten Daten enthalten. Ein Bandsatz kann auch Backups anderer Daten enthalten.

Ein **separater Bandsatz** ist ein Bandsatz, der nur Backups von speziellen geschützten Daten enthält. Andere Backups können nicht auf einen separaten Bandsatz geschrieben werden.

(Für die zu erstellende Backup-Richtlinie/den zu erstellenden Backup-Plan) Einen separaten Bandsatz verwenden

Voreinstellung ist: **Ausgeschaltet**.

Wenn Sie diese Option unverändert lassen, werden die Backups, die zur erstellten Richtlinie oder zum erstellten Plan gehören, möglicherweise auf Bänder geschrieben, die Backups enthalten, die mit anderen Backup-Richtlinien geschrieben wurden und Daten anderer Maschinen enthalten. In ähnlicher Weise können Backups von anderen Richtlinien auf Bänder geschrieben werden, die Backups dieser Richtlinie enthalten. Solche Bänder verursachen allerdings keine Probleme, da das Programm die Bänder automatisch verwaltet.

Wenn diese Option aktiviert ist, werden die Backups, die zur erstellten Richtlinie bzw. zum erstellten Plan gehören, in einen separaten Bandsatz eingeordnet. Andere Backups werden nicht auf diesen Bandsatz geschrieben.

Wenn die Konsole mit dem Management Server verbunden ist

Die Option **Einen separaten Bandsatz verwenden** lässt sich noch genauer definieren. Sie können also für die zu erstellende Backup-Richtlinie einen separaten Bandsatz für alle Maschinen oder für jede einzelne Maschine verwenden.

Standardmäßig ist die Option **Einen einzelnen Bandsatz für alle Maschinen** ausgewählt. Im Allgemeinen werden die Bänder mit dieser Option effizienter genutzt als mit der Option **Einen separaten Bandsatz für jede einzelne Maschine verwenden**. Die zweite Option kann jedoch z.B. hilfreich sein, wenn es spezielle Anforderungen gibt, die Bänder mit Backups von einer bestimmten Maschine außerhalb des Standorts zu lagern.

Wenn die Option **Einen separaten Bandsatz verwenden** aktiviert ist, kann es zu einer Situation kommen, in der das Backup auf ein Band geschrieben werden muss, das sich momentan nicht im Bandbibliothek-Gerät befindet. Bestimmen Sie, was in einem solchen Fall geschehen soll.

- **Auf Benutzerantwort warten** – Der Backup-Task gelangt in das Stadium **Interaktion erforderlich** und wartet darauf, dass das Band mit dem erforderlichen Label in das Bandbibliothek-Gerät geladen wird.
- **Freies Band benutzen** – Das Backup wird auf ein freies Band geschrieben, so dass die Aktion nur dann unterbrochen wird, wenn in der Bibliothek kein freies Band vorhanden ist.

Immer ein freies Band benutzen

Wenn Sie die folgenden Optionen unverändert lassen, wird jedes Backup auf das Band geschrieben, das durch die Option **Einen separaten Bandsatz verwenden** angegeben wird. Wenn einige der folgenden Optionen aktiviert sind, fügt das Programm einem Bandsatz immer dann neue Bänder hinzu, wenn ein Voll-Backup, ein inkrementelles oder ein differentielles Backup erstellt wird.

- **Für jedes Voll-Backup**

Voreinstellung ist: **Ausgeschaltet**.

Wenn diese Option aktiviert ist, wird jedes Voll-Backup auf ein freies Band geschrieben. Das Band wird speziell für diese Aktion in ein Laufwerk geladen. Wenn die Option **Einen separaten Bandsatz verwenden** aktiviert ist, werden nur inkrementelle und differentielle Backups auf dem Band angefügt.

- **Für jedes differentielle Backup**

Voreinstellung ist: **Ausgeschaltet**.

Wenn diese Option aktiviert ist, wird jedes differentielle Backup auf ein freies Band geschrieben. Diese Option ist nur verfügbar, wenn die Option zur Verwendung eines freien Bandes für jedes Voll-Backup ausgewählt ist.

- **Für jedes inkrementelle Backup**

Voreinstellung ist: **Ausgeschaltet**.

Wenn diese Option aktiviert ist, wird jedes inkrementelle Backup auf ein freies Band geschrieben. Diese Option ist nur verfügbar, wenn die Option zur Verwendung eines freien Bandes für jedes Voll-Backup und jedes differentielle Backup ausgewählt ist.

Bandrotation

Wenn alle Backups von einem Band gelöscht werden, d.h. wenn die Informationen zum letzten Backup auf dem Band aus der Datenbank im Storage Node gelöscht werden, dann wird das Band als leer angesehen und kann während des Backup-Zyklus wiederverwendet werden. Dieselbe Bandrotation ermöglicht Ihnen mit einer minimalen Zahl von Bandkassetten auszukommen, ohne unter benutzten Bändern begraben zu werden.

Acronis Backup & Recovery 10 ermöglicht Ihnen, beim Ausführen von Backups auf Bandbibliotheken die Bandrotation vollständig zu automatisieren.

Dieser Abschnitt enthält hilfreiche Informationen zur Auswahl des Backup-Schemas und der Bandoptionen für die Bandrotation.

Zur Berechnung der Anzahl der Bänder, die für das Bandrotationsschema erforderlich sind, können Sie die Vorgehensweise verwenden, die im Abschnitt Bandplanung (S. 162) beschrieben wurde.

Auswählen eines Backup-Schemas

Wenn Sie eine Backup-Richtlinie/einen Backup-Plan mit einem Bandbibliothek-Ziel erstellen, dann stehen Ihnen die folgenden Backup-Schemata zur Verfügung: **Backup jetzt**, **Backup später**, **Großvater-Vater-Sohn**, **Türme von Hanoi** oder **Benutzerdefiniert**. Das Backup-Schema **Einfach** ist deaktiviert, da eine Konsolidierung der Backups für Archive, die sich auf Bändern befinden, nicht möglich ist.

Acronis Backup & Recovery 10 ermöglicht eine Automatisierung der Bandrotation für die Backup-Schemata **Großvater-Vater-Sohn**, **Türme von Hanoi** und **Benutzerdefiniert**.

Großvater-Vater-Sohn (S. 36) (GVS) und Türme von Hanoi (S. 40) (TvH) sind die am häufigsten eingesetzten Backup-Schemata bei Bandbibliothek-Geräten. Diese Schemata werden so optimiert, dass die beste Balance zwischen der Größe eines Backup-Archivs, der Anzahl der vom Archiv aus verfügbaren Wiederherstellungspunkte und der Menge der für die Archivierung erforderlichen Bänder erhalten bleibt.

Wenn Ihr Backup-Archiv eine Wiederherstellung mit täglicher Auflösung für die letzten Tage, wöchentlicher Auflösung für die letzten Wochen und monatlicher Auflösung für jede Zeit in der Vergangenheit bieten muss, dann ist das zu bevorzugende Schema das GVS-Schema (**Großvater-Vater-Sohn**).

Wenn das Hauptziel darin besteht, Daten für einen längstmöglichen Zeitraum zu sichern, wobei die Anzahl der eingesetzten Bänder, die permanent in eine kleine Bandbibliothek (z.B. Autoloader) geladen sind, minimal ist, dann ist die beste Lösung wahrscheinlich das TvH-Schema (**Türme von Hanoi**).

Das Backup-Schema **Benutzerdefiniert** ermöglicht Ihnen, einen Zeitplan für das Backup sowie Aufbewahrungsrichtlinien anzugeben, anhand derer die gewünschte Bandrotation definiert wird. Verwenden Sie dieses Schema, wenn die Schemata **Großvater-Vater-Sohn** und **Türme von Hanoi** für Ihre Zwecke nicht ausreichend sind. Wenn z.B. die Gesamtgröße der geschützten Daten deutlich kleiner als die Größe des Bandes ist, dann besteht die beste Lösung darin, das Backup-Schema **Benutzerdefiniert** mit regelmäßigen Voll-Backups auf täglicher/wöchentlicher/monatlicher Basis auszuwählen, dazu einige einfache Aufbewahrungsrichtlinien festzulegen und die Bandoptionen bei ihren Standardwerten zu belassen.

Auswahlkriterien

Jedes Mal, wenn Sie ein Bandrotationsschema für eine zu erstellende Backup-Richtlinie/einen zu erstellenden Backup-Plan konzipieren, müssen Sie folgende Aspekte berücksichtigen:

- Gesamtgröße der zu schützenden Daten
- ungefähre Größe der täglichen Änderungen an den Daten
- ungefähre Größe der wöchentlichen Änderungen an den Daten
- Anforderungen an das Backup-Schema (Häufigkeit, Leistung und Dauer des Backup-Vorgangs)
- Anforderungen an die Aufbewahrung von Backups (minimale/maximale Aufbewahrungsdauer für Backups; Notwendigkeit der Lagerung von Bandkassetten außerhalb des Standorts)
- Leistungsfähigkeit der Bandbibliothek (Anzahl der Laufwerke, Loader, Kassettenschächte und verfügbare Bänder; Kapazität der Bänder)
- Anforderungen für die Durchführung von Datenwiederherstellungen (maximale Dauer)

Sie müssen jeden Aspekt, der für Ihren Fall relevant ist, analysieren und so die wichtigsten Kriterien für Ihre Auswahl bestimmen. Wählen Sie danach ein Backup-Schema aus und geben Sie die Bandoptionen an.

Beachten Sie, dass die Kombination eines beliebigen Backup-Schemas mit verschiedenen Bandoptionen zu recht unterschiedlichen Ergebnissen im Hinblick auf die effektive Verwendung von Bändern und Geräten führt.

Fallanalyse

Angenommen, Sie müssen eine automatische Bandrotation für folgende Fälle einrichten:

- die Gesamtgröße der zu schützenden Daten beträgt etwa 320 GB
- die ungefähre Größe der täglichen Änderungen an den Daten beläuft sich auf etwa 16 GB
- die ungefähre Größe der wöchentlichen Änderungen an den Daten ist nicht größer als 40 GB
- die Bandkapazität beträgt 400 GB.

Lassen Sie uns jetzt die Ergebnisse einer Kombination der beiden Backup-Schemata GVS und TvH mit unterschiedlichen Bandoptionen für den Fall analysieren.

Alle nachfolgend analysierten Beispiele sind eine vereinfachende Annäherung an den echten Fall, geben Ihnen aber einen Eindruck von der allgemeinen Konzeption der Verteilung von Backups auf Bändern.

Legende zu den Abbildungen für die Fallbeispiele

Die täglichen/inkrementellen Backups (16 GB) werden in den Abbildungen als grüne Rechtecke angezeigt:  .

Die wöchentlichen/differentiellen Backups (40 GB) werden als blaue Rechtecke angezeigt:  .

Monatliche Voll-Backups (320 GB) werden orangefarben gezeichnet:

 .

Das gesamte Band (400 GB) wird als graues Rechteck gezeichnet:

 .

Verwenden des Rotationsschemas „Großvater-Vater-Sohn“

Die Bandrotation für das GVS-Backup-Schema wird in erster Linie durch die Bandoptionen definiert, die für die zu erstellende Backup-Richtlinie/den zu erstellenden Backup-Plan angegeben wurden.

Angenommen, die GVS-Einstellungen sind wie folgt:

- **Backup starten: 23:00:00 Uhr**
- **Backup an: Werktags**
- **Wöchentlich/monatlich: Freitag**
- **Backups aufbewahren: Täglich: 2 Wochen; Wöchentlich 2 Monate; Monatlich: 1 Jahr**.

Das Hauptziel besteht in einer vollständigen Automatisierung der Bandrotation mit diesen Einstellungen.

Denken Sie daran, dass in dieser Implementierung des GVS-Schemas ein monatliches Backup ein Voll-Backup, ein wöchentliches Backup ein differentielles Backup und ein tägliches Backup ein inkrementelles Backup ist. Das erste Backup ist immer vollständig. Wenn also die Backup-Richtlinie bzw. der Backup-Plan am Mittwoch startet und Voll-Backups an jedem vierten Freitag erstellt werden sollen, dann ist das erste Backup am Mittwoch kein inkrementelles, sondern ein Voll-Backup.

In den folgenden Abschnitten werden Beispiele analysiert, die zeigen, wie das GVS-Schema mit verschiedenen Bandoptionen kombiniert werden kann:

- GVS-Beispiel 1 (S. 151). Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt. Alle Optionen unter **Immer ein freies Band benutzen** sind nicht ausgewählt. Diese Kombination erfordert 25 Bänder für die Rotation.
- GVS-Beispiel 2 (S. 154). Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt. Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ausgewählt ist. Die anderen Optionen unter **Immer ein freies Band benutzen** sind nicht ausgewählt. Diese Kombination erfordert 16 Bänder für die Rotation.
- GVS-Beispiel 3 (S. 156). Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt. Alle Optionen unter **Immer ein freies Band benutzen** sind ausgewählt. Diese Kombination erfordert 28 Bänder für die Rotation.

Diese Beispiele veranschaulichen, wie die Anzahl der Bänder, die für eine automatische Rotation erforderlich sind, von den Bandoptionen abhängt. Wenn in einer Bandbibliothek nicht genügend Bänder für die automatische Rotation vorhanden sind, wird von Zeit zu Zeit das Fenster **Tasks brauchen Interaktion** angezeigt, in dem Sie aufgefordert werden, ein freies Band in die Bibliothek zu laden.

GVS-Beispiel 1

Angenommen, für den Backup-Plan gelten die folgenden Bandoptionen:

- Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ist nicht ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** ist nicht ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist nicht ausgewählt.

Angenommen, der erste Backup-Vorgang ist für Freitag, den 1. Januar geplant. An diesem Tag wird um 23:00 Uhr das erste Voll-Backup (320 GB auf dem Band mit einer Größe von 400 GB) erstellt. Da die Option **Einen separaten Bandsatz verwenden** ausgewählt ist, wird das aktuell gemountete Band ausgeworfen (wenn es kein freies Band ist). Danach wird speziell für das Backup der Daten ein freies

Band geladen. Dieses Band ist in der folgenden Abbildung mit der Nummer „01“ markiert. Entsprechend der Legende, die im Abschnitt Fallanalyse (S. 150) beschrieben ist, wird das Voll-Backup in der Abbildung als orangefarbenes Rechteck dargestellt.

Die angegebenen Einstellungen für das GVS-Backup-Schema haben zur Folge, dass nur an **Werktagen** ein Backup der Daten durchgeführt wird. Daher wird das nächste Backup am Montag, dem 4. Januar zur selben Zeit (**23:00 Uhr**) erstellt. Dieses Backup ist ein inkrementelles Backup (16 GB), das auf dasselbe Band 01 geschrieben wird, da die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** nicht ausgewählt ist. Das Backup wird in der Abbildung als grünes Rechteck gezeichnet.

Die nächsten drei inkrementellen Backups werden am 5., 6. und 7. Januar auf Band 01 geschrieben. Das führt dazu, dass momentan nur 16 GB freier Speicherplatz auf dem Band verfügbar sind.

Am 8. Januar wird das differentielle Backup der Daten (40 GB) auf demselben Band 01 aufgezeichnet, da die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist nicht ausgewählt. Das Band erreicht jedoch sein Ende, nachdem die ersten 16 GB des Backups geschrieben wurden. Danach wird das Band abgeschaltet und durch einen Loader aus dem Laufwerk in einen Kassettenschacht ausgeworfen. Daraufhin wird ein freies Band in dasselbe Laufwerk geladen und gemountet und danach wird das Backup (die letzten 24 GB) mit dem Beginn des neuen Bandes fortgesetzt.

In der nächsten Abbildung wird der gegenwärtige Zustand des Backup-Archivs veranschaulicht. Das differentielle Backup wird in der Abbildung als blaues Rechteck gezeichnet. Nummer 1 im grünen Rechteck markiert das inkrementelle Backup, das am Montag der ersten Woche des Jahres erstellt wurde.

Danach werden die folgenden Backups auf Band 02 geschrieben:

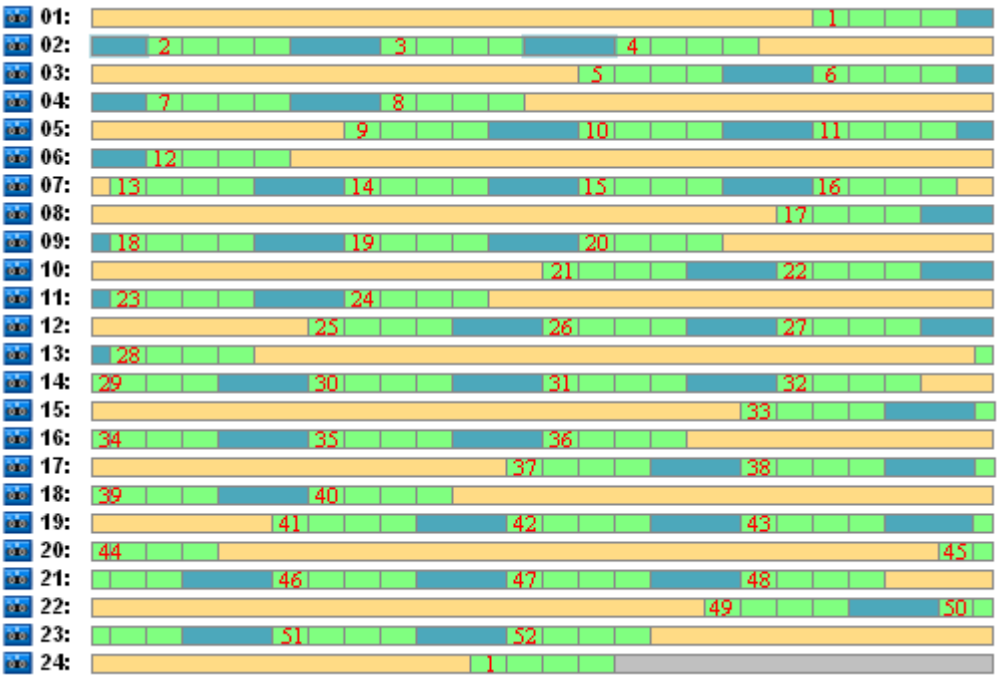
- vier inkrementelle Backups und ein differentielles Backup für die zweite Woche
- vier inkrementelle Backups und ein differentielles Backup für die dritte Woche
- vier inkrementelle Backups für die vierte Woche.

Das nächste Voll-Backup (320 GB) sollte am Freitag der vierten Woche geschrieben werden. Auf Band 02 sind im Moment jedoch nur 104 GB freier Speicherplatz verfügbar. Wenn also das Band sein Ende erreicht, dann wird die Aufzeichnung am Beginn von Band 03 fortgesetzt.

Denken Sie daran, dass beim GVS-Schema nach jeder Backup-Aktion der **Bereinigungs**-Task gestartet wird. Dieser Task löscht alle veralteten Backups. In der nächsten Abbildung werden dunkelgraue Rechtecke anstelle der Backups angezeigt, die bis zum gegenwärtigen Zeitpunkt gelöscht wurden.

Physikalisch befinden sich die gelöschten Backups noch auf den Bändern. Es werden jedoch die Informationen zu den Backups aus der Datenbank im Storage Node gelöscht.

In der folgenden Abbildung werden die gelöschten Backups als vorhanden angezeigt, es wird aber die Bandauslastung während des ganzen Jahres für das GVS-Backup-Schema in Kombination mit den angegebenen Bandoptionen veranschaulicht. Eine Zahl im grünen Rechteck markiert ein inkrementelles Backup, das am Montag der entsprechenden Woche des Jahres erstellt wurde.



Bandauslastung während des ersten Jahres

In der nächsten Abbildung wird die tatsächliche Auslastung der Bänder mit freiem Speicherplatz anstelle der gelöschten Backups am ersten Freitag des folgenden Jahres angezeigt. Zu der Zeit wird das differentielle Backup (blaues Rechteck) auf Band 24 geschrieben.

Das auf Band 01 gespeicherte Voll-Backup wird gelöscht, nachdem am Freitag der 52. Woche das nächste Voll-Backup auf den Bändern 23 und 24 erstellt wurde. Da alle Backups auf Band 01 gelöscht wurden, wird das Band als frei erachtet und kann erneut verwendet werden.

Die weitere Analyse des Beispiels zeigt, dass die maximale Anzahl der Bänder, die zum Speichern der Backups erforderlich ist, bei 25 liegt. Dieses Maximum wird in der 16. Woche des folgenden Jahres erreicht.

Die oben erwähnten Abbildungen zeigen, dass eine Datenwiederherstellung ein oder zwei Bänder für ein Voll-Backup, zwei oder drei Bänder für ein differentielles Backup und eins, zwei oder drei Bänder für ein inkrementelles Backup erfordert.

Wenn wir z.B. Daten aus einem Backup wiederherstellen müssen, das am Montag der 52. Woche erstellt wurde, dann sind zum Ausführen des Tasks die folgenden Bänder erforderlich:

- Band 23 mit einem inkrementellen Backup (markiert mit „52“) und einem differentiellen Backup, das am Freitag der 51. Woche erstellt wurde
- Band 21 und Band 22, die ein Voll-Backup enthalten, das am Freitag der 48. Woche erstellt wurde.

Das Beispiel enthüllt die folgenden Defizite, die bei dieser Schema-Kombination mit den angegebenen Bandoptionen zu beobachten sind:

- in der Regel ist jede Datenwiederherstellung ein langer Prozess, der das Laden, Mounten, Zurückspulen und Lesen von einem (3 % – für Backups, die in der Abbildung „Bandauslastung während des ersten Jahres“ angezeigt werden), zwei (65 %) oder drei (32 %) Bändern erfordert
- 22 Bänder werden verwendet, um 13 monatliche Voll-Backups zu speichern, wenn die Größe des monatlichen Backups kleiner als die Kapazität des Bandes ist, so dass die Aufbewahrung von Daten teurer wird
- 25 Bänder sind für eine volle jährliche Rotation der Backups erforderlich.

GVS-Beispiel 2

Angenommen, für den Backup-Plan gelten die folgenden Bandoptionen:

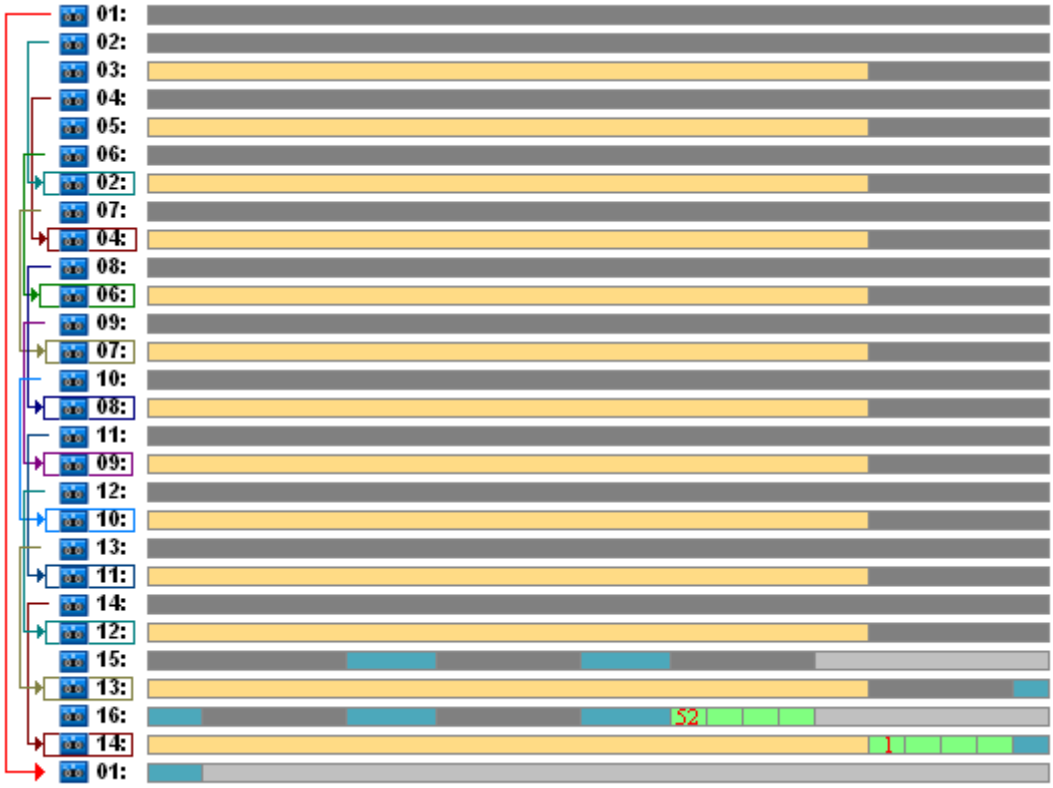
- Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** ist nicht ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist nicht ausgewählt.

Das Beispiel unterscheidet sich in nur einem Punkt vom vorhergehenden Beispiel. Dieser betrifft die Auswahl der Option **Immer ein freies Band benutzen: für jedes Voll-Backup**.

In der folgenden Abbildung werden die gelöschten Backups als vorhanden angezeigt, es wird aber die Bandauslastung während des ganzen Jahres für das GVS-Backup-Schema in Kombination mit den angegebenen Bandoptionen veranschaulicht. Eine Zahl im grünen Rechteck markiert ein inkrementelles Backup, das am Montag der entsprechenden Woche des Jahres erstellt wurde.

Wenn alle Backups während des Jahres aufbewahrt werden müssen, dann erfordert das Archiv 28 Bänder.

Da bei dem GVS-Backup-Schema eine automatische Löschung der veralteten Backups erzwungen wird, behalten die Bänder am ersten Freitag des zweiten Jahres nur die Backups, die in der nächsten Abbildung angezeigt werden.



Diese Abbildung veranschaulicht, dass das Bandrotationsschema **GVS-Beispiel 2** besser für den Fall geeignet ist als **GVS-Beispiel 1**. Das Bandrotationsschema **GVS-Beispiel 2** hat für den analysierten Fall die folgenden Vorteile:

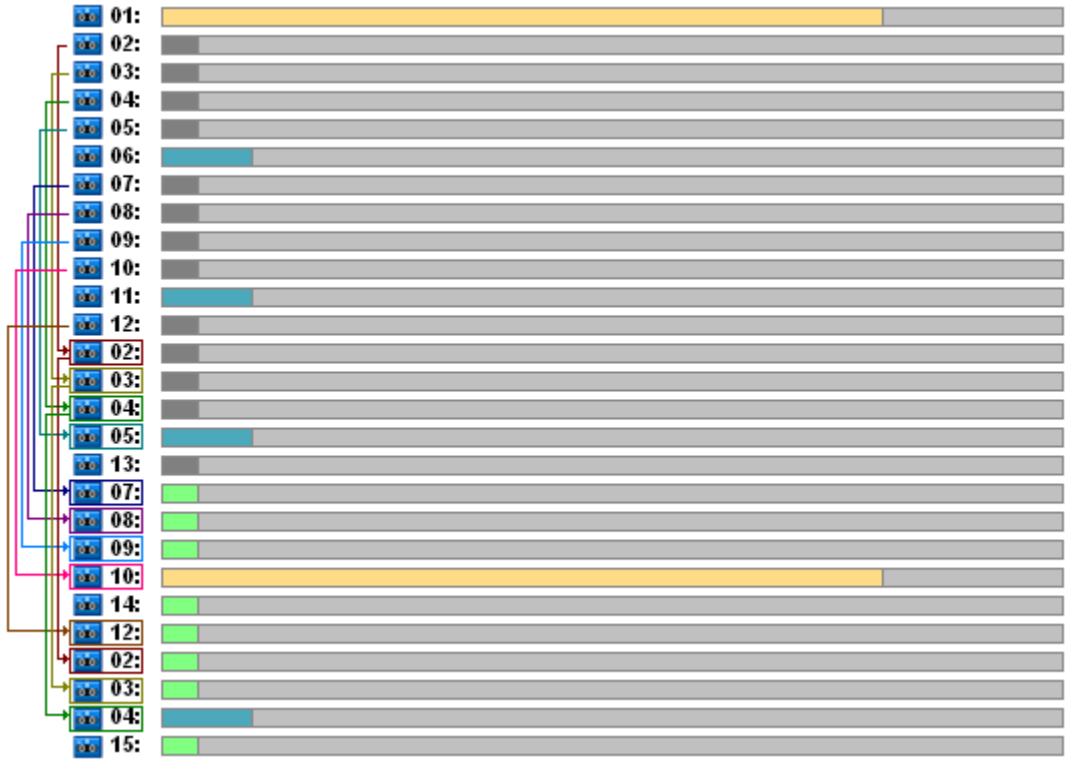
- anstelle von 25 werden nur 16 Bänder verwendet
- ein Recovery-Task erfordert ein (25 %) oder zwei (75 %) Bänder
- die Datenwiederherstellung aus einem Voll-Backup erfordert nur ein Band, wodurch die Datenwiederherstellung aus einem inkrementellen oder differentiellen Backup beschleunigt werden kann.

GVS-Beispiel 3

Angenommen, für den Backup-Plan gelten die folgenden Bandoptionen:

- Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist ausgewählt.

Diese Optionen definieren das klassische Bandrotationsschema für GVS. In der Abbildung wird der Beginn des Rotationsschemas gezeigt, das 8 Bänder für tägliche Backups, 6 Bänder für wöchentliche Backups und 13 Bänder für monatliche Backups (da es 13 Vier-Wochen-Zyklen in einem Jahr gibt) für den analysierten Fall verwendet. Und ein Band wird für das nächste Backup benötigt. Insgesamt sind für das Rotationsschema zusammen mit den Optionen 28 Bänder erforderlich.



Zur Wiederherstellung der Daten sind für ein Voll-Backup nur ein Band, für ein differentielles Backup zwei Bänder und für ein inkrementelles Backup zwei oder drei Bänder erforderlich.

Dieses Schema hat die folgenden Vorteile:

- Der Zugriff auf ein beliebiges Voll-Backup erfordert lediglich ein Band.
- Durch das Löschen von Backups werden Bänder geleert und können daraufhin wiederverwendet werden.

Der auffälligste Nachteil ist die große Zahl erforderlicher Bändern, die zu 5-10 % verwendet werden.

Wenn ein tägliches Backup für eine Woche (4 Backups) und ein wöchentliches Backup für einen Monat (4 Backups) aufbewahrt werden soll, dann ergibt sich die Gesamtzahl erforderlicher Bänder zu 4+4+13+1 = 22.

Verwenden des Rotationsschemas „Türme von Hanoi“

Das TvH-Schema erfordert im Vergleich zum GVS-Schema weniger Bänder für die Rotation. Daher ist das TvH-Schema das am besten geeignete Schema für kleine Bandbibliotheken, insbesondere bei der Verwendung von Autoloadern.

Nachdem das TvH-Backup-Schema ausgewählt wurde, ist es möglich, einen Zeitplan für das Schema sowie die Anzahl der Level anzugeben.

Entsprechend der optimalen Verfahrensweise sollten fünf Level verwendet werden, wenn Sie das Schema „Türme von Hanoi“ auf wöchentliche Backups anwenden und es sollten acht Level verwendet werden, wenn Sie das Schema auf tägliche Backups anwenden. Im ersten Fall besteht die Rotation aus 16 wöchentlichen Sitzungen, wodurch eine Roll-Back-Periode (die minimale Zahl der Tage, die Sie im Archiv zurückgehen können) von 8 Wochen gesichert ist. Die Bandrotation für den zweiten Fall umfasst 128 tägliche Sitzungen und erlaubt also eine Roll-Back-Periode von 64 Tagen. Die Roll-Back-Periode ist immer die Hälfte der Sitzungsanzahl.

Jedes zusätzliche Level verdoppelt nicht nur die Anzahl der Sitzungen, sondern auch das Alter des ältesten Backups.

Lassen Sie uns zu dem Fall zurückkehren, der im Abschnitt Fallanalyse (S. 150) beschrieben wurde; dabei wird von folgenden TvH-Einstellungen ausgegangen:

- **Planung:** **Führe den Task jeden Tag um 23:00 Uhr aus. Einmalig.**
- **Zahl der Level:** **5**

Das Schema Türme von Hanoi mit fünf Leveln sichert eine Roll-Back-Periode von 8 days. Die Backups auf den Levels mit den Nummern 1 bis 5 werden im Folgenden durch die Buchstaben A, B, C, D bzw. E bezeichnet. Danach ergibt sich folgende Rotationsvorlage für die Backup-Sequenz im Archiv: E-A-B-A-C-A-B-A-D-A-B-A-C-A-B-A. Im TvH-Schema mit fünf Levels sind alle Backups auf dem ersten Level (A) inkrementell, die Backups auf dem fünften Level (E) sind Voll-Backups und die anderen Backups auf den Levels 2, 3 und 4 (B, C und D) sind differentiell.

Die Bandrotation für das TvH-Schema hängt wesentlich von den Bandoptionen ab, deren Standardeinstellungen nicht immer für eine optimale Verwendung der Bänder und der gesamten Bandbibliothek sorgen.

Das Ziel besteht darin, die Bandoptionen auszuwählen, die eine minimale Anzahl von Bändern für die Rotation erfordern.

In den folgenden Abschnitten werden Beispiele analysiert, die zeigen, wie das TvH-Schema mit verschiedenen Bandoptionen kombiniert werden kann:

- TvH-Beispiel 1 (S. 158). Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt. Alle Optionen unter **Immer ein freies Band benutzen** sind nicht ausgewählt. Diese Kombination erfordert 5 Bänder für die Rotation.
- TvH-Beispiel 2 (S. 159). Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt. Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ausgewählt ist. Die anderen Optionen unter **Immer ein freies Band benutzen** sind nicht ausgewählt. Diese Kombination erfordert 4 Bänder für die Rotation.
- TvH-Beispiel 3 (S. 161). Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt. Alle Optionen unter **Immer ein freies Band benutzen** sind ausgewählt. Diese Kombination erfordert 7 Bänder für die Rotation.

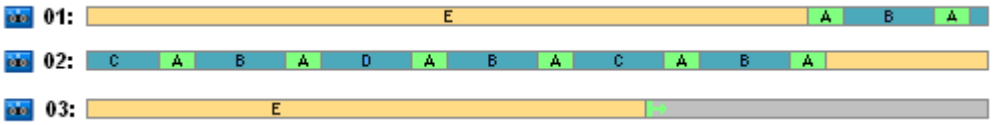
TvH-Beispiel 2 erfordert 4 Bänder. Dies ist die Mindestzahl für diesen Fall. Also sind hier die Einstellungen für die Bandoptionen die besten im Vergleich zu den Optionen für die anderen Beispiele.

TvH-Beispiel 1

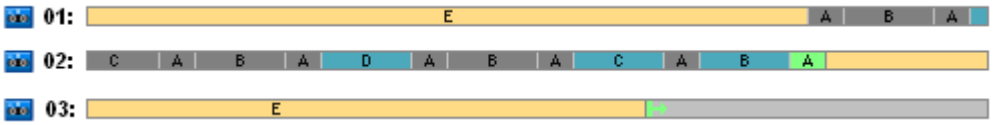
Angenommen, für den Backup-Plan gelten die folgenden Bandoptionen:

- Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ist nicht ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** ist nicht ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist nicht ausgewählt.

In der folgenden Abbildung wird die Verwendung der Bänder für eine Kombination aus TvH-Schema und den oben erwähnten Bandoptionen angezeigt. Der sich wiederholende Teil des Schemas enthält sechzehn Backup-Sitzungen. In der Abbildung wird das Stadium des Backup-Archivs zu dem Zeitpunkt gezeigt, zu dem die siebzehnte Sitzung beendet wird.

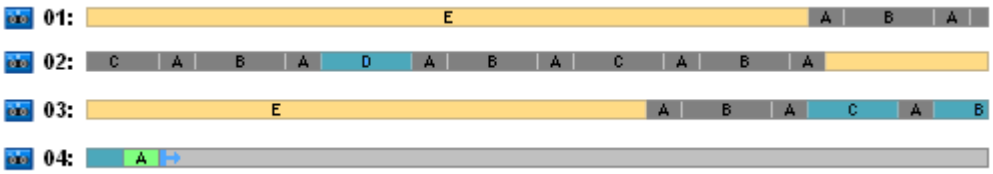


Da beim Backup-Schema „Türme von Hanoi“ die Anwesenheit eines einzigen Backups auf jedem Level zwingend ist, werden alle veralteten Backups automatisch gelöscht. In der nächsten Abbildung werden die gelöschten Backups als dunkelgraue Rechtecke gezeichnet. Das gelöschte Backup bleibt zwar immer noch auf den Bändern gespeichert, aber die Informationen dazu werden aus der Datenbank im Storage Node gelöscht.



In der Abbildung wird das Voll-Backup gezeigt, das momentan auf Band 01 gespeichert ist und nicht gelöscht werden kann, da es als Basis für die aktuellen differentiellen (D, C, B) und inkrementellen (A) Backups dient, die auf Band 02 gespeichert sind. Die Löschung des Voll-Backups wird aufgeschoben, bis alle vier oben erwähnten Backups gelöscht wurden.

In der nächsten Abbildung wird der Inhalt der Bänder zum Zeitpunkt unmittelbar vor Erstellung des neuen Backups auf Level D dargestellt:



In diesem Moment nimmt das Datenarchiv vier Bänder ein und die Gesamtgröße der Backups, die bis zum gegenwärtigen Zeitpunkt geschrieben wurden, ist für das Beispiel maximal. Wenn jedoch in Zukunft ein Voll-Backup am Ende des Bandes geschrieben wird, nimmt das Archiv fünf Bänder ein.

Nachdem das nächste Backup auf Level D erstellt wird, wird Band 01 geleert und kann wiederverwendet werden.

Es gilt festzuhalten, dass das TvH-Schema in Kombination mit den angegebenen Optionen für den analysierten Fall die folgenden Eigenschaften aufweist:

- die letzte Abbildung zeigt, dass die Datenwiederherstellung das Laden und Mounten von bis zu drei Bändern (ein Band – 16 %, zwei Bänder – 72 %, drei Bänder – 12 %) sowie das Zurückspulen und Lesen von einem (6 %), zwei (50 %) oder drei (44 %) Backups erfordert
- bei einem Schema mit fünf Levels sind für diesen Fall bis zu fünf Bänder erforderlich.

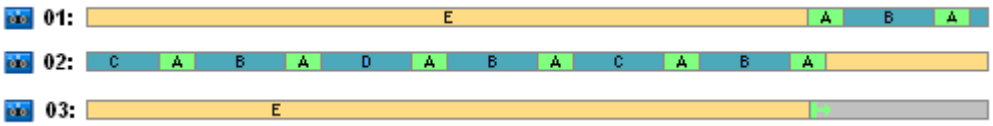
TvH-Beispiel 2

Angenommen, für den Backup-Plan gelten die folgenden Bandoptionen:

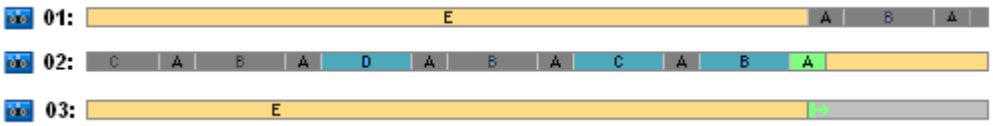
- Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** ist nicht ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist nicht ausgewählt.

Der einzige Unterschied zwischen **TvH-Beispiel 2** und **TvH-Beispiel 1** besteht darin, dass die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ausgewählt ist.

Die erste Abbildung zeigt die Verwendung der Bänder für eine Kombination aus TvH-Schema und den oben erwähnten Bandoptionen. Der sich wiederholende Teil des Schemas enthält sechzehn Backup-Sitzungen. In der Abbildung wird das Stadium des Backup-Archivs zu dem Zeitpunkt gezeigt, zu dem die siebzehnte Sitzung beendet wird.



In der folgenden Abbildung werden die momentan gelöschten Backups als dunkelgraue Rechtecke gezeichnet.



Die Abbildung zeigt, dass es zwei Voll-Backups auf Level E gibt, da das erste Voll-Backup momentan eine Basis für die differentiellen Backups D, C und B ist und diese wiederum eine Basis für das inkrementelle Backup A sind. Daher wird die Löschung des Voll-Backups aufgeschoben, bis alle Backups D, C, B und A gelöscht wurden.

Die nächste Abbildung zeigt die Verwendung des Bandes zum Zeitpunkt unmittelbar vor Erstellung eines neuen Backups auf Level D:

Im Moment nimmt das Backup-Archiv vier Bänder ein. Dies ist die maximal Anzahl an Bändern, die für dieses Beispiel erforderlich ist.

Nachdem das nächste Backup auf Level D erstellt wird, werden beide Bänder 01 und 02 geleert und können wiederverwendet werden.

Es gilt festzuhalten, dass das TvH-Schema in Kombination mit den angegebenen Optionen für den analysierten Fall die folgenden Eigenschaften aufweist:

- Die Datenwiederherstellung erfordert Zugriff auf die Backups, die auf einem (25 %) oder zwei

Bändern (75 %) gespeichert sind

- Bei einem Schema mit fünf Levels können bis zu vier Bänder erforderlich sein.

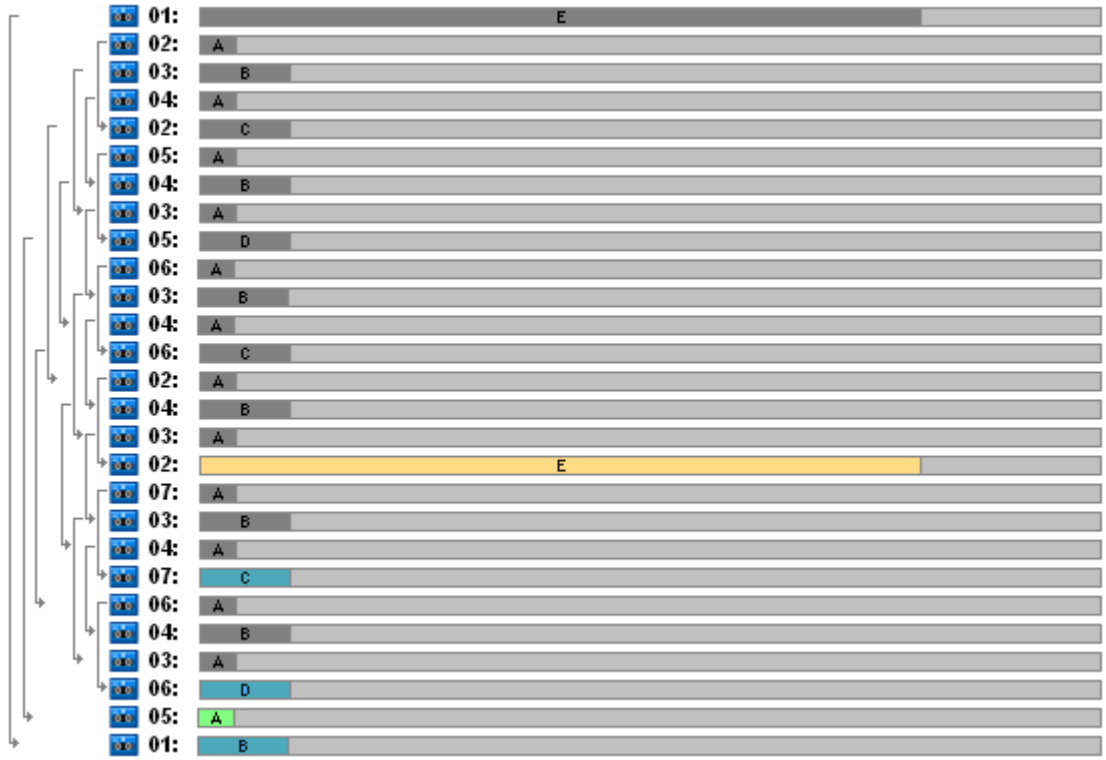
So wird in diesem speziellen Fall durch Auswahl der Option **Immer ein freies Band benutzen: für jedes Voll-Backup** die Verwendungseffizienz der Bänder in der Bibliothek deutlich gesteigert.

TvH-Beispiel 3

Angenommen, für den Backup-Plan gelten die folgenden Bandoptionen:

- Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** ist ausgewählt.
- Die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist ausgewählt.

Die Abbildung zeigt die Bandrotation für das TvH-Schema mit diesen Optionen.



Die maximale Anzahl der Bänder, die in der Rotation verwendet werden, beträgt sieben. Dies ist mehr als im klassischen TvH-Schema mit fünf Levels.

Zwei zusätzliche Bänder werden benötigt für:

1. die Aufbewahrung eines alten Voll-Backups (aufgeschobene Löschung), da dies die Basis für Backups auf anderen Levels ist
2. die Aufbewahrung eines alten Backups eines Levels, bis ein neues Backup auf diesem Level erfolgreich erstellt wurde.

Das Beispiel veranschaulicht, dass hier die Verwendungseffizienz des Bandes reduziert ist. Außerdem erfordert die Datenwiederherstellung einen Zugriff auf Backups, die auf einem (Voll-Backups, 6 %), zwei (differentielle Backups, 44 %) oder drei (inkrementelle Backups, 50 %) Bändern gespeichert sind. Daher wird bei dieser Aktion durchschnittlich mehr Zeit benötigt als in den vorherigen Beispielen.

Bandplanung

Nachdem Sie das Backup-Schema und die Bandoptionen angegeben haben, sollten Sie die Anzahl der Bänder bestimmen, die mindestens erforderlich ist, um die Bandrotation vollautomatisch durchführen zu können.

Zur Vereinfachung der Bandplanung lassen Sie uns die Möglichkeit außer Acht lassen, dass die errechneten Bänder Backups von anderen Daten enthalten. Das impliziert, dass die Option **Einen separaten Bandsatz verwenden** aktiviert ist.

Bei Berechnung der Bandanzahl sollten Sie folgende Aspekte berücksichtigen:

- Größe des Voll-Backups
- Durchschnittliche Größe der inkrementellen Backups
- Durchschnittliche Größe der differentiellen Backups
- Angegebener Komprimierungsgrad für Backups von Daten
- Bandrotationsschema (Häufigkeit von Backups, Aufbewahrungsrichtlinien)
- Bandanhangoptionen
- Anforderungen für die Unterstützung von Bandkassettenarchiven außerhalb des Standorts.

Es gibt keine allgemeingültige Formel zur Berechnung der Anzahl der Bänder, die für alle möglichen Kombinationen der oben aufgeführten Parameter erforderlich ist. Allgemein müssen bei der Ermittlung der Band-Anzahl für einen Fall jedoch die folgenden Schritte berücksichtigt werden:

1. Zeichnen (oder schreiben) Sie eine Kette von Backups bis zu dem Zeitpunkt, an dem das erste Backup gelöscht werden kann
2. Berücksichtigen Sie die Bandanhangoptionen; die Kette ist möglicherweise auf verschiedene Bandsätze aufgeteilt
3. Berechnen Sie die Anzahl der Bänder in den einzelnen Bandsätzen
4. Die Summe der berechneten Werte ergibt die Gesamtzahl der Bänder, die für den Fall benötigt wird.

Bandplanung: Beispiel 1

Angenommen, Sie haben einen Fall mit den folgenden Merkmalen:

- Die Größe des Voll-Backups beträgt **V_GB**
- Die durchschnittliche Größe der inkrementellen Backups beträgt **I_GB**
- Die durchschnittliche Größe der differentiellen Backups beträgt **D_GB**
- Der Komprimierungsgrad entspricht einem durchschnittlichen Reduzierungskoeffizienten **KG**
- Das ausgewählte Bandrotationsschema ist **Türme von Hanoi** mit **vier** Levels
- Folgende Bandoptionen sind festgelegt:
  - Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt.
  - Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ist nicht ausgewählt.
  - Die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** ist nicht ausgewählt.
  - Die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist nicht ausgewählt
- Die Größe des Bandes ist **B_GB**.

Durch das TvH-Schema (Türme von Hanoi) mit vier Levels (A, B, C und D) wird die folgende Serie von

Backups angegeben, die durchgeführt werden, bevor das erste Backup gelöscht wird: D (Voll), A, B, A, C, A, B, A, D, A, B, A, C. Die angegebenen Bandoptionen erfordern für keines der Backups die Verwendung eines freien Bandes. Daher wird die Backupserie automatisch geteilt und auf einem neuen Band fortgesetzt, wenn das Ende des aktuellen Bandes erreicht ist. Es muss ein Bandsatz berechnet werden.

Gesamtanzahl der erforderlichen Bänder = Aufrunden ((2*V_GB + 6*I_GB + 5*D_GB) * KG / B_GB) + 1.

Das oben beschriebene TvH-Beispiel 1 (S. 158) basiert auf dem Backup-Schema „Türme von Hanoi“ mit fünf Levels und denselben Bandoptionen. Die Backup-Serie war die folgende: E (Voll), A, B, A, C, A, B, A, D, A, B, A, C, A, B, A, E, A, B, A, C, A, B, A, D.

Gesamtzahl erforderlichen Bänder = Aufrunden ((2*V_GB + 12*I_GB + 11*D_GB) * KG / B_GB) + 1 = Aufrunden ((2*320 + 12*16 + 11*40) * 1 / 400) + 1 = Aufrunden (3,18) + 1 = 5 (Bänder).

Bandplanung: Beispiel 2

Angenommen, Sie haben einen Fall mit den folgenden Merkmalen:

- Die Größe des Voll-Backups beträgt **V_GB**
- Die durchschnittliche Größe der inkrementellen Backups beträgt **I_GB**
- Die durchschnittliche Größe der differentiellen Backups beträgt **D_GB**
- Der Komprimierungsgrad entspricht einem durchschnittlichen Reduzierungskoeffizienten **KG**
- Das ausgewählte Bandrotationsschema ist **Benutzerdefiniert** mit den folgenden Einstellungen:
  - **Voll-Backup – alle 10 Tage**
  - **Differentielles Backup – alle 2 Tage**
  - **Inkrementelles Backup – jeden Tag, alle 6 Stunden**
  - **Aufbewahrungsregeln: Lösche Backups älter als 5 Tage**
- Folgende Bandoptionen sind festgelegt:
  - Die Option **Einen separaten Bandsatz verwenden** ist ausgewählt.
  - Die Option **Immer ein freies Band benutzen: für jedes Voll-Backup** ist ausgewählt.
  - Die Option **Immer ein freies Band benutzen: für jedes inkrementelle Backup** ist nicht ausgewählt.
  - Die Option **Immer ein freies Band benutzen: für jedes differentielle Backup** ist nicht ausgewählt
- Die Größe des Bandes ist **B_GB**.

Der Fall definiert eine Backup-Serie, die aus zwei Abschnitten besteht. Die nachfolgende Abbildung zeigt die Abschnitte zu dem Zeitpunkt, bevor das erste Backup gelöscht wird. In der Abbildung werden die Voll-Backups, die differentiellen und die inkrementellen Backups als orangefarbene, blaue bzw. grüne Rechtecke dargestellt.

Zu dem Zeitpunkt werden einige Backups durch den Bereinigungs-Task gelöscht. Die Löschung der veralteten Backups, die in dunklen Farben dargestellt werden, wird aufgeschoben, da diese Backups grundlegend für die gegenwärtigen Backups sind.

Da die exakte Beziehung zwischen der Bandgröße und der Größe des Backups nicht bekannt ist, ist es nicht möglich, die Anzahl der Bänder zu bestimmen, die nach dem Löschvorgang frei sein werden. Bei der Berechnung wird also diese Möglichkeit außer Acht gelassen.

Bandsatz 01 sollte (Aufrunden ((V_GB + 4*D_GB + 5*7*I_GB) * KG / B_GB)) Bänder zum Speichern der Backups enthalten. Bandsatz 02 muss (Aufrunden ((V_GB + 1*D_GB + 7*I_GB) * KG / B_GB)) Bänder enthalten. Die Summe der berechneten Werte ergibt die Gesamtzahl der Bänder, die für den Fall benötigt wird.

Was ist, wenn

- **Was ist, wenn ich Bänder mit Backups von einer Bandbibliothek zu einer anderen verschieben muss?**

  1. Wenn beide Bandbibliotheken an derselben Maschine angeschlossen sind, auf der der Acronis Backup & Recovery 10 Storage Node installiert ist (d.h. dass die Bibliotheken vom selben Storage Node verwaltet werden), dann enthält die Datenbank im Storage Node alle erforderlichen Informationen über den Inhalt der verschobenen Bänder. Sie müssen also lediglich eine Inventarisierung (S. 145) des verwalteten Depots auf der Bibliothek vornehmen, in der die Bänder platziert werden.
  2. Wenn Sie Bänder in eine Bandbibliothek verschieben, die von einem anderen Storage Node verwaltet wird, dann sollten Sie jedes neu positionierte Band erneut durchsuchen (S. 146), um dem Storage Node die auf dem Band enthaltenen Informationen zu den Backups bereitzustellen.

- **Was ist, wenn ich ein Band aus der Bandbibliothek im lokalen Bandgerät verwenden muss (oder umgekehrt)?**

  Die Acronis-Agenten erstellen Backups auf Bändern in einem Format, das sich vom Format des Storage Nodes unterscheidet. Aus diesem Grund ist es nicht möglich, Bänder zwischen Bandgeräten, die mit einem Storage Node verbunden sind und solchen, die mit einer verwalteten Maschine verbunden sind, auszutauschen: Ein per Storage Node beschriebenes Band kann nicht von einem Agenten in einem lokal angeschlossenen Bandgerät gelesen werden. Der Storage Node kann allerdings Bänder lesen, die von einem Agenten geschrieben wurden. In der Bandkompatibilitätstabelle (S. 48) erhalten Sie umfassende Informationen zur Kompatibilität von Bandformaten in Acronis Backup & Recovery 10.

- **Was ist, wenn ich den Storage Node neu installieren oder die Bandbibliothek an einer anderen Maschine anschließen muss?**

  Installieren Sie einen Storage Node auf der Maschine, an der die Bandbibliothek angeschlossen ist, erstellen Sie ein zentrales Depot für die Bandbibliothek und suchen Sie dann erneut nach allen Bändern, die Backups enthalten.

- **Was ist, wenn ich meinen Storage Node verloren habe und Daten von einem Band wiederherstellen muss?**

  Wenn Sie wissen, auf welchem Band sich die Daten befinden, die Sie wiederherstellen möchten und wenn Sie darüber hinaus ein Bandgerät mit einem Depot haben, das von einem Storage Node verwaltet wird, dann legen Sie die Bandkassette in das Gerät ein, gehen Sie zur Konsolenansicht **Zentrale Depots**, wählen Sie das Depot aus, durchsuchen Sie das Band erneut, wählen Sie das Archiv und das Backup aus, aus dem Daten wiederhergestellt werden sollen und erstellen Sie den Recovery-Task.

  Wenn Sie nicht wissen, auf welchem Band sich die Daten befinden, die Sie wiederherstellen

möchten, müssen Sie jedes Band erneut durchsuchen, bis Sie die Daten gefunden haben. Normalerweise müssen Sie hier lediglich die Schritte ausführen, die bereits beschrieben wurden, mit der Ausnahme, dass die erneute Suche jetzt auf mehreren Bändern anstelle von einem Band ausgeführt werden muss.

- **Was ist, wenn ich Daten von einem Echo-Band wiederherstellen muss?**

  Verwenden Sie die Tabelle im Abschnitt Bandkompatibilitätstabelle (S. 48), um herauszufinden, welche Acronis Backup & Recovery 10-Komponenten Daten von Ihrem Band lesen können.

4.2 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. 34).

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.

4.2.1 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. 167).

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. 168)

Aktionen mit Backups (S. 169)

Archive filtern und sortieren (S. 171)

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.

4.2.2 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. 167) 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. 268) 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. 252) 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. 199) 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. 199) 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*.

4.3 Übliche Aktionen

4.3.1 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. 252) 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. 261) 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. 170), 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.

4.3.2 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 zur Durchführung von Aktionen mit Backups.

Aktion	Lösung
Den 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 bereits als Quelle

	vorausgewählten Backup.
Eine Festplatte/Partition als virtuelle Maschine wiederherstellen	Klicken Sie mit der rechten Maustaste auf das Disk-Backup und wählen im Kontextmenü **Als virtuelle Maschine wiederherstellen**. Sie gelangen zur Seite **Daten wiederherstellen** mit bereits als Quelle vorausgewählten Backup. Wählen Sie Zielort sowie Typ der neuen virtuellen Maschine und fahren Sie dann so wie bei einer regulären Festplatten- bzw. Volume-Wiederherstellung fort.
Ein Backup validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite **Validierung (S. 252) mit bereits als Quelle vorausgewählten Backup. Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten 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. 261) 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. 170), welches für jedes Archiv bzw. Backup Kontrollkästchen 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. 170), welches für jedes Archiv bzw. Backup Kontrollkästchen hat. Überprüfen Sie Ihre Wahl und korrigieren Sie diese falls nötig, bestätigen Sie dann die Löschaktion.

4.3.3 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.

4.3.4 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 Ereignisse auf, die unter Windows-Betriebssystemen verfügbar sind.

Ereignis
Zeit: Täglich, Wöchentlich, Monatlich
Verstrichene Zeit, seit das letzte erfolgreiche Backup abgeschlossen wurde. (geben Sie die Zeitdauer an)
Benutzeranmeldung (jeder Benutzer, aktueller Benutzer, geben Sie das Benutzerkonto an)
Benutzerabmeldung* (jeder Benutzer, aktueller Benutzer, geben Sie das Benutzerkonto an) *'Herunterfahren' ist nicht dieselbe Aktion wie 'Abmeldung'. Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt.
Systemstart
Änderung beim freien Platz (spezifizieren Sie die Größenänderung des freien Speicherplatzes für jedes Laufwerk, das für ein Backup gewählt wurde oder zu sichernde Daten enthält).
Ein Ereignis in der Windows-Ereignisanzeige (spezifizieren Sie die Parameter des Ereignisses)
Bei Alarm durch Acronis Drive Monitor

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 Bedingungen auf, die unter Windows-Betriebssystemen verfügbar sind.

Bedingung: Task nur starten, wenn
Benutzer untätig ist (ein Bildschirmschoner ausgeführt wird oder die Maschine gesperrt ist)
Host des Speicherorts verfügbar ist
Laufzeit des Tasks sich innerhalb des spezifizierten Zeitintervalls befindet

Benutzer alle abgemeldet sind
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. 115) 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 (S. 180) 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 (S. 180) 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. 225).

„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. 225).

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 (S. 180) 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. 225).

„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 Erweiterte Planungseinstellungen

Die folgenden erweiterten Einstellungen sind verfügbar, wenn Sie in einer Backup-Richtlinie einen täglichen, wöchentlichen oder monatlichen Zeitplan konfigurieren.

Wake-On-LAN benutzen

Wenn diese Einstellung aktiviert ist, verwendet der Acronis Backup & Recovery 10 Management Server die WOL-Funktion (Wake-On-LAN), um ausgeschaltete, registrierte Maschinen „aufzuwecken“, wenn die geplante Startzeit für ein Backup, eine Bereinigung oder eine Validierung erreicht ist. Wenn der Backup-Task auf den einzelnen Maschinen mit Verzögerung gestartet wird (siehe die nächste Einstellung), dann weckt der Management Server die Maschinen entsprechend dieser Verzögerungen auf.

Bevor Sie diese Einstellung verwenden, vergewissern Sie sich, dass Sie Wake-on-LAN auf den registrierten Maschinen aktiviert haben. Die BIOS-Konfiguration der Maschine, die Konfiguration des Netzwerkadapters und die Konfiguration des Betriebssystems müssen so sein, dass die Maschine aus dem „Soft-Off“-Zustand – auch als Energiezustand S5 oder G2 bekannt – aufgeweckt werden kann.

Startzeit innerhalb des Zeitfensters verteilen

Wenn diese Einstellung aktiviert ist, startet der Backup-Task auf den einzelnen registrierten Maschinen mit einer bestimmten Verzögerung zu der Startzeit, die in der Richtlinie festgelegt ist. Dadurch werden die tatsächlichen Startzeiten des Tasks im Zeitintervall verteilt.

Möglicherweise möchten Sie diese Einstellung verwenden, wenn Sie eine Backup-Richtlinie zur Ausführung von Backups für mehrere Maschinen auf einem Netzwerkspeicherort erstellen, um eine übermäßige Netzwerklast zu vermeiden.

Die Verzögerungswerte reichen von Null bis zur angegebenen maximalen Verzögerung und sie werden entsprechend der ausgewählten Verteilungsmethode bestimmt.

Der Verzögerungswert für die einzelnen Maschinen wird bestimmt, wenn die Richtlinie auf der Maschine verteilt wird und er bleibt so lange gleich, bis Sie die Richtlinie bearbeiten und den maximalen Verzögerungswert ändern.

Die Bedingungen werden, falls vorhanden, zur tatsächlichen Startzeit eines Tasks auf den einzelnen Maschinen überprüft.

Das folgende Beispiel veranschaulicht diese Einstellung.

Beispiel 1

Angenommen, Sie verteilen eine Backup-Richtlinie für drei Maschinen mit dem folgenden Zeitplan:

Task starten: **Täglich**
Einmal um: **09:00:00 Uhr**

Startzeit innerhalb des Zeitfensters verteilen
Maximale Verzögerung: **1 Stunde**
Verteilungsmethode: **Zufällig**

Die Startzeit des Tasks kann auf den einzelnen Maschinen ein beliebiger Zeitpunkt zwischen 09:00:00 Uhr und 09:59:59 Uhr sein, also z.B.:

Erste Maschine: Jeden Tag um 09:30:03 Uhr

Zweite Maschine: Jeden Tag um 09:00:00 Uhr

Dritte Maschine: Jeden Tag um 09:59:59 Uhr

Beispiel 2

Angenommen, Sie verteilen eine Backup-Richtlinie für drei Maschinen mit dem folgenden Zeitplan:

Task starten: **Täglich**
Alle: **2 Stunden** Von: **09:00:00 Uhr** Bis: **11:00:00 Uhr**

Startzeit innerhalb des Zeitfensters verteilen
Maximale Verzögerung: **1 Stunde**
Verteilungsmethode: **Zufällig**

Dann kann der Zeitpunkt, an dem der Task erstmalig auf jeder der Maschinen ausgeführt wird, ein beliebiger Zeitpunkt zwischen 09:00:00 Uhr und 09:59:59 Uhr sein. Die Zeit zwischen der ersten und der zweiten Ausführung beträgt exakt zwei Stunden, z.B.:

Erste Maschine: Jeden Tag um 09:30:03 Uhr und 11:30:03 Uhr

Zweite Maschine: Jeden Tag um 09:00:00 Uhr und 11:00:00 Uhr

Dritte Maschine: Jeden Tag um 09:59:59 Uhr und 11:59:59 Uhr

Erweiterte Einstellungen spezifizieren

1. Stellen Sie eine Verbindung mit dem Management Server oder mit einer darauf registrierten Maschine her und beginnen Sie dann mit der Erstellung einer Backup-Richtlinie oder eines Backup-Plans.
2. Wählen Sie unter **Art des Backups** das Schema („Einfach“, „Türme von Hanoi“ oder „Benutzerdefiniert“) aus und klicken Sie dann auf **Ändern**, um eine Planung für das Schema anzugeben.
3. Wählen Sie unter **Task starten** die Option **Täglich**, **Wöchentlich** oder **Monatlich** aus.
4. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Ändern**.
5. Wenn Sie die Verwendung der Wake-On-LAN-Funktion ermöglichen möchten, aktivieren Sie das Kontrollkästchen **Wake-on-LAN benutzen**.
6. Wenn Sie die Startzeiten der zentralen Backup-Tasks verteilen möchten, aktivieren Sie das Kontrollkästchen **Startzeit innerhalb des Zeitfensters verteilen** und geben Sie dann den maximalen Verzögerungswert und die Verteilungsmethode an.

5.5 Bei einem Ereignis in der Windows Ereignisanzeige

Diese Art der Planung ist nur in Windows-Betriebssystemen wirksam.

Sie können einen Backup-Task so planen, dass er gestartet wird, wenn ein bestimmtes Windows-Ereignis in eine der Protokolllisten (Anwendungen, Sicherheit oder System) aufgenommen wird.

Angenommen, Sie wollen einen Backup-Plan aufstellen, der automatisch ein vollständiges Notfall-Backup Ihrer Daten durchführt, sobald Windows entdeckt, dass die Festplatte vor einem Ausfall steht.

Parameter

Protokollname

Spezifizieren Sie den Namen eines Protokolls. Wählen Sie den Namen einer Standard-Protokollliste (**Anwendung**, **Sicherheit** oder **System**) oder geben Sie den Namen einer Protokollliste ein – beispielsweise: **Microsoft Office Sitzungen**

Ereignisquelle

Spezifizieren Sie die Quelle des Ereignisses, welche typischerweise das Programm oder die Systemkomponente angibt, die das Ereignis verursachte – beispielsweise: **disk**

Ereignistyp

Geben Sie den Typ des Ereignisses an: **Fehler**, **Warnung**, **Informationen**, **Überprüfung erfolgreich** oder **Überprüfung fehlgeschlagen**.

Ereignis-Kennung:

Bezeichnet die Ereignis-Nummer, die üblicherweise die spezielle Art der Ereignisse unter Ereignissen derselben Quelle identifiziert.

So tritt z.B. ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **7** auf, wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, während ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **15** stattfindet, wenn eine Festplatte noch nicht zugriffsbereit ist.

Beispiele

„Fehlerhafte Blöcke"-Notfall-Backup

Treten ein oder mehrere fehlerhafte Blöcke plötzlich auf einer Festplatte auf, so deutet das üblicherweise auf einen baldigen Ausfall der Festplatte hin. Angenommen, Sie wollen einen Backup-Plan erstellen, der die Daten einer Festplatte sichert, sobald eine solche Situation eintritt:

Wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, nimmt es ein Ereignis mit der Ereignis-Quelle **disk** und der Ereignis-Kennung **7** in die Protokollliste **System** auf; der Typ des Ereignisses ist **Fehler**.

Wenn Sie den Plan erstellen, geben Sie Folgendes im Bereich **Planung** ein bzw. wählen es aus:

- **Protokollname**: **System**
- **Ereignis-Quelle**: **disk**
- **Ereignis-Typ**: **Fehler**
- **Ereignis-Kennung**: **7**

Wichtig: *Um sicherzustellen, dass ein solcher Task trotz Vorhandenseins der fehlerhaften Blöcke fertiggestellt wird, müssen Sie angeben, dass der Task diese ignoriert. Zur Umsetzung gehen Sie in den* ***Backup-Optionen*** *zum Unterpunkt* ***Fehlerbehandlung*** *und aktivieren das Kontrollkästchen* ***Fehlerhafte Sektoren ignorieren****.*

Vor-Update-Backup in Windows Vista

Angenommen Sie wollen einen Backup-Plan erstellen, der automatisch ein Backup des Systems durchführt – z.B. durch Sicherung der Partition, auf der Windows installiert ist – jedes Mal, wenn Windows davor steht, Updates zu installieren.

Nach dem Download eines oder mehrerer Updates und Planung der Installation nimmt Windows Vista ein Ereignis mit der Quelle **Microsoft-Windows-WindowsUpdateClient** und der Ereignis-Nummer **18** in die Protokollliste **System** auf; der Typ dieses Ereignisses ist **Informationen**.

Wenn Sie den Plan erstellen, geben Sie Folgendes im Bereich **Planung** ein bzw. wählen es aus:

- **Protokollname**: **System**
- **Ereignis-Quelle**: **Microsoft-Windows-WindowsUpdateClient**
- **Ereignis-Typ**: **Informationen**
- **Ereignis-Kennung**: **18**

Tipp: *Um einen vergleichbaren Backup-Plan für unter Windows XP laufende Maschinen aufzusetzen, ersetzen Sie den Text in* ***Ereignis-Quelle*** *mit* ***Windows Update Agent*** *und lassen Sie die übrigen Felder gleich.*

So können Sie Ereignisse in der Ereignisanzeige einsehen

So öffnen Sie eine Meldung in der Ereignisanzeige

1. Klicken Sie auf dem Desktop oder im **Start-**Menü mit der rechten Maustaste auf **Computer** und dann im Kontextmenü auf **Verwalten**.
2. Erweitern Sie in der Konsole **Computerverwaltung** den Zweig **System** und dann **Ereignisanzeige**.
3. Klicken Sie in der **Ereignisanzeige** auf den Namen einer Protokollliste, die Sie einsehen wollen – z.B. **Anwendung**.

   Beachten Sie: *Um die Sicherheitsprotokollliste öffnen zu können (****Sicherheit****), müssen Sie Mitglied der Gruppe „Administratoren“ sein.*

So können Sie die Eigenschaften eines Ereignisses einsehen, inklusive seiner Quelle und Nummer (Ereigniskennung).

1. Klicken Sie in der **Ereignisanzeige** auf den Namen einer Protokollliste, die Sie einsehen wollen – z.B. **Anwendung**.

   Beachten Sie: *Um die Sicherheitsprotokollliste öffnen zu können (****Sicherheit****), müssen Sie Mitglied der Gruppe „Administratoren“ sein.*

2. Klicken Sie im rechten Fensterbereich der Protokollliste auf den Namen des Ereignisses, dessen Eigenschaften Sie sehen wollen.
3. Im Dialogfenster **Eigenschaften** sehen Sie alle Informationen des Ereignisses, wie etwas seinen Ursprung im Feld **Quelle** und seine Nummer, die im Feld **Ereignis-Kennung** angezeigt wird.

Sind Sie fertig, so klicken Sie auf **OK**, um das Dialogfenster **Eigenschaften** wieder zu schließen.

5.6 Bei Alarm durch Acronis Drive Monitor

Diese Planung gilt für Windows-Betriebssysteme mit installiertem Acronis® Drive Monitor™.

Acronis Drive Monitor gibt Meldungen über Laufwerkszustände aus, die auf dem internen Laufwerksüberwachungssystem 'S.M.A.R.T.' beruhen. Sie können – basierend auf den Alarmmeldungen des Acronis Drive Monitors – Notfall-Backups Ihrer Daten als Ergänzung zu Ihren regulären Backups konfigurieren. Ein entsprechendes Notfall-Backup wird gestartet, wenn eines Ihrer Datenlaufwerke auszufallen droht.

Das Backup wird ausgeführt, sobald der Laufwerkszustand eine Warngrenze oder kritische Grenze erreicht hat. Sie können für jedes Laufwerk eine Anzeige zum Laufwerkszustand (in Prozent) einsehen, wenn Sie den Acronis Drive Monitor öffnen.

Alarmmeldungen zur Laufwerkstemperatur verursachen jedoch keinen Backup-Start.

Tipp: *Falls Ihr Backup-Plan das benutzerdefinierte Backup-Schema (S. 225) verwendet, dann können Sie das Notfall-Backup ganz einfach dadurch aufsetzen, dass Sie demselben Backup-Plan eine Extra-Planung*

hinzufügen. Bei Verwendung eines anderen Backup-Schemas müssen Sie einen separaten Backup-Plan erstellen.

5.7 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. 172)“ 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. 115) 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. 225) 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.

Beispiel:

Es ist notwendig, den Backup-Task auszuführen, nachdem sich der freie Platz der verwalteten Maschine um wenigstens 1 GB geändert hat, aber nur, wenn alle Benutzer abgemeldet sind und seit dem letzten Backup mehr als 12 Stunden verstrichen sind.

Stellen Sie Planung, Bedingungen und die **Task-Startbedingungen** in den Backup-Optionen folgendermaßen ein:

- Planung: **Wenn sich der freie Platz geändert hat**; Wert: Task ausführen, wenn der freie Speicherplatz mindestens geändert wurde um: **1 GB**.
- Bedingung: **Benutzer sind abgemeldet**; Wert: Task nur dann pünktlich starten, wenn alle Benutzer abgemeldet sind.
- Bedingung: **Zeit seit letztem Backup**; Wert: Zeit seit letztem Backup: **12 Stunden**.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Wenn sich der freie Platz um mehr als 1 GB ändert, wird der Scheduler warten, bis beide Bedingungen gleichzeitig zutreffen und dann den Backup-Task ausführen.

5.7.1 Benutzer ist untätig

Gilt für: Windows

„Benutzer ist untätig“ bedeutet, dass auf der verwalteten Maschine ein Bildschirmschoner läuft oder die Maschine gesperrt ist.

Beispiel:

Starte den Backup-Task auf der verwalteten Maschine täglich um 21:00 Uhr, möglichst, wenn der Benutzer untätig ist. Ist der Benutzer um 23 Uhr immer noch aktiv, starte den Task dennoch.

- Ereignis: **Täglich**, alle **1** Tage; einmal um: **09:00:00 PM**.
- Bedingung: **Benutzer ist untätig**.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, den Task dennoch starten nach **2** Stunde(n).

Ergebnis:

(1) Wenn der Benutzer vor 21 Uhr untätig wird, startet der Backup-Task um 21 Uhr.

(2) Wenn der Benutzer zwischen 21 und 23 Uhr untätig wird, startet der Backup-Task sofort, nachdem der Benutzer untätig wurde.

(3) Wenn der Benutzer um 23 Uhr immer aktiv ist, startet der Backup-Task dennoch.

5.7.2 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.

5.7.3 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.

5.7.4 Benutzer ist abgemeldet

Gilt für: Windows

Ermöglicht Ihnen, einen Backup-Task auf Warteposition zu setzen, bis sich alle Benutzer auf der verwalteten Maschine von Windows abgemeldet haben.

Beispiel

Führe den Backup-Task um 20:00 Uhr am ersten und dritten Freitag eines jeden Monats aus, möglichst, wenn alle Benutzer abgemeldet sind. Sollte einer der Benutzer um 23:00 Uhr immer noch angemeldet sein, führe den Task dennoch aus.

- Ereignis: **Monatlich**, Monate: **<Alle>**; An: **<Erster>**, **<Dritter>** **<Freitag>**; einmalig um **20:00 Uhr**.
- Bedingung: **Benutzer sind abgemeldet**.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, den Task dennoch starten nach **3** Stunde(n).

Ergebnis:

(1) Wenn alle Benutzer um 20:00 Uhr abgemeldet sind, startet der Backup-Task um 20:00 Uhr.

(2) Wenn sich der letzte Benutzer zwischen 20:00 und 23:00 Uhr abmeldet, wird der Backup-Task sofort ausgeführt, nachdem sich der Benutzer abgemeldet hat.

(3) Wenn ein Benutzer um 23:00 Uhr immer noch angemeldet ist, startet der Backup-Task dennoch.

5.7.5 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. 422) erstellen. **Jetzt erstellen** startet den Bootable Media Builder (S. 427).
	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. 191) 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. 188) 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. 191) überprüfen und Ihre Entscheidung für jeden Task im Bereich **Informationen** treffen (oder im Fenster **Task-Details** (S. 199)).

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. 191) 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. 192) 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. 193). Prüfen Sie den Status (S. 194) 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. 198).
- 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. 195). 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. 201) bzw. **Task-Details** (S. 199) 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	Prüfen Sie den Log-Eintrag, um die Warnmeldung zu lesen. -> [optional] Führen Sie Aktionen aus, um zukünftige Warnungen bzw. Fehler zu

		abgeschlossen. Andernfalls siehe Punkt 3.	verhindern.
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. 115).

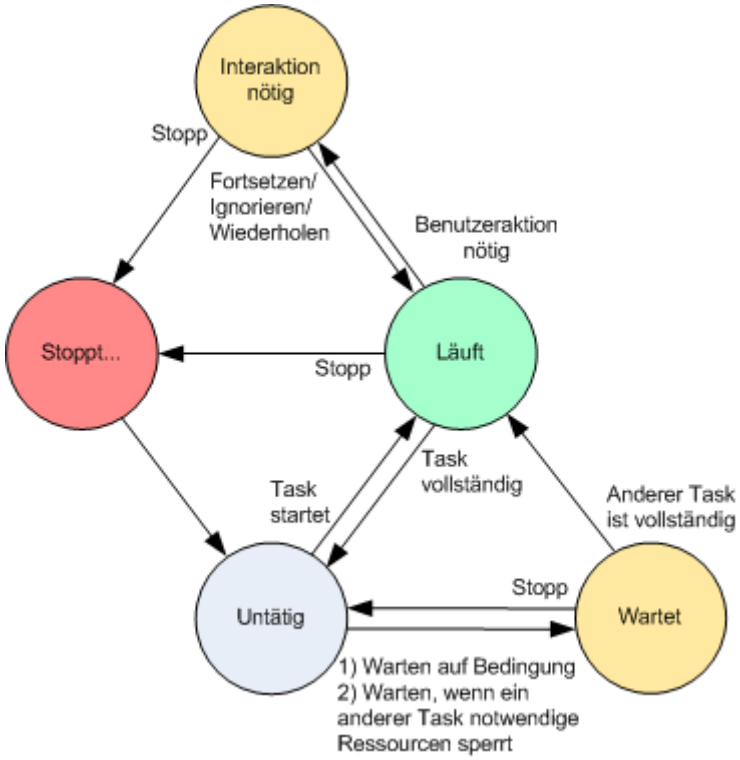
Interaktion erforderlich

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. 205) ▪ Recovery-Task ▪ Validierungstask (S. 252)
Details eines Plans/Tasks einsehen	**Backup-Plan** Klicken Sie auf **Details anzeigen**. Überprüfen Sie dann im Fenster **Plan-Details** (S. 201) die entsprechenden Informationen. **Task** Klicken Sie auf **Details anzeigen**. Überprüfen Sie dann im Fenster **Task-Details** (S. 199) die entsprechenden Informationen.
Ereignisanzeige für Pläne/Tasks einsehen	**Backup-Plan** Klicken Sie auf **Log anzeigen**. Sie gelangen dadurch in die Ansicht **Log** (S. 202), die eine Liste der planbezogenen Log-Einträge enthält. **Task** Klicken Sie auf **Log anzeigen**. Sie gelangen dadurch in die **Log** (S. 202)-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. 199) 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. 205), 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. 199) 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. 191) des Backup-Plans
- **Status** – Status (S. 192) 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. 208), 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. 203).
- 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. 203).
- 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. 204) 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. 420) erstellen, sollten Sie sich mit den grundlegenden Konzepten (S. 28) 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. 208)

[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. 208)

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. 209)

Spezifizieren Sie die für das Backup gedachten Daten-Elemente. Die Liste der zu sichernden Elemente hängt vom zuvor spezifizierten Daten-Typ ab.

Anmeldeinformationen: (S. 210)

[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. 210)

[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. 212)

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 Backups zu einem verwalteten Depot, auf Band, zu einer Acronis Secure Zone oder dem Acronis Online Backup Storage durchführen.

[Optional] Aktivieren Sie dieses Kontrollkästchen, wenn Sie für die Backups des Archivs eine vereinfachte Dateibenennung verwenden wollen.

Anmeldeinformationen: (S. 218)

[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. 219)

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. 229)

[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. 97) 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**.

In VM konvertieren

Gilt für: **Laufwerk/Volume**-Backups, Backups von **kompletten virtuellen Maschinen** oder den **Laufwerken einer virtuellen Maschine**

Nicht verfügbar für Maschinen, die unter Linux laufen

Durch das Einrichten einer regelmäßigen Konvertierung erhalten Sie eine Kopie Ihres Servers oder Ihrer Workstation auf einer virtuellen Maschine, die sofort einsatzbereit ist, falls die ursprüngliche Maschine ausfällt. Die Konvertierung kann von demselben Agenten ausgeführt werden, der die Backups ausführt, oder von einem Agenten, der auf einer anderen Maschine installiert ist. Im letzteren Fall muss das Archiv an einem Ort mit Netzwerkfreigabe gespeichert werden, z.B. einem Netzwerkordner oder einem verwalteten Depot, damit die andere Maschine auf das Archiv zugreifen kann.

Konvertierungszeitpunkt (S. 229)

[Optional] Geben Sie an, ob jedes vollständige, inkrementelle oder differentielle Backup konvertiert werden soll oder stellen Sie einen Zeitplan für die Konvertierung des jeweils letzten Backups auf. Geben Sie bei Bedarf einen Konvertierungsplan an.

Host (S. 230)

Geben Sie an, welche Maschine die Konvertierung ausführen soll. Auf der Maschine muss der Acronis Backup & Recovery 10 Agent für Windows, der Agent für ESX/ESXi oder der Agent für Hyper-V installiert sein.

Virtualisierungs-Server (S. 230)

Hier bestimmen Sie Typ und Speicherort der virtuellen Maschine. Welche Optionen verfügbar sind, hängt davon ab, welchen Host Sie im vorangehenden Schritt ausgewählt haben.

Storage (S. 230)

Wählen Sie auf dem Virtualisierungs-Server oder in dem Ordner einen Speicherort, an dem die Dateien für die Virtuelle Maschine gespeichert werden sollen.

Resultierende VMs

Spezifizieren Sie einen Namen für die virtuelle Maschine.

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. 208) aufgefordert werden.

Sie können auf den von Ihnen erstellten Plan in der Ansicht **Backup-Pläne und Tasks** (S. 191) 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. 34), 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. 208) 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)“.
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 (S. 411) und das Abonnement auf der zu sichernden Maschine aktivieren (S. 412). Die Online Backup-Funktion steht unter Linux und bootfähigen Medien nicht zur Verfügung.

  Acronis Backup & Recovery 10 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. 216) oder alle während einer Woche erstellten Backups (S. 216) 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. 217) 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. 217).

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. 217).

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. 217).

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. 112) 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. 32) 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. 172), um mehr über das Aufstellen von Zeit/-Ereignis-Planungen zu lernen.
Aufbewahrungsregel	Für das Schema „Einfach“ ist nur eine Aufbewahrungsregel (S. 42) 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. 173), wöchentlichen (S. 175) oder monatlichen (S. 177) 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. 42) 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. 42) 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. 42).

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. 42).

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.

Initial Seeding

Dieses Backup-Schema ist nur verfügbar, wenn Sie eine Lizenz für Initial Seeding besitzen und den Online Backup Storage als Backup-Ziel ausgewählt haben.

Initial Seeding ermöglicht Ihnen, das erste Backup (üblicherweise ein Voll-Backup und sehr groß) durch Verwendung einer Festplatte (oder ähnlichen Laufwerks) statt per Internetübertragung zum Online Storage hochzuladen. Nachfolgende Backups (üblicherweise inkrementell und daher deutlich kleiner) können dann per Internet übertragen werden, sobald das Voll-Backup im Online Storage angekommen ist.

Wenn Sie eine große Datenmenge sichern, ermöglicht Initial Seeding eine schnellere Auslieferung der Daten und geringere Übertragungskosten.

Konsultieren Sie zu weiteren Details den Abschnitt „Initial Seeding FAQ (S. 402)“.

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. 172).

6.2.12 Reguläre 'Konvertierung zu virtueller Maschine' aufsetzen.

Sie können bei Erstellung eines Backup-Plans (S. 205) einstellen, dass Laufwerke oder Volume-Backups regulär zu einer virtuellen Maschine konvertiert werden. Dieser Abschnitt gibt Ihnen die Informationen, um die entsprechenden Einstellungen vornehmen können.

Eine Planung zur Konvertierung aufsetzen

Ein bei Ausführung eines Backup-Plans erstelltes Disk-Backup (S. 424) kann sofort oder per Planung zu einer virtuellen Maschine konvertiert werden – oder durch eine Kombination beider Methoden.

Der Konvertierungstask wird auf der zu sichernden Maschine erstellt und verwendet die Zeiteinstellungen der Maschine.

Als Folge der ersten Konvertierung wird eine neue virtuelle Maschine erstellt. Jede nachfolgende Konvertierung wird diese Maschine je wieder ganz neu erstellen. Zuerst wird eine neue (temporäre) virtuelle Maschine erstellt. Sobald diese Aktion erfolgreich abgeschlossen wurde, wird die alte Maschine ersetzt. Kommt es bei Erstellung der temporären Maschine zu einem Fehler, dann wird diese temporäre Maschine gelöscht. Dadurch endet der Task immer mit einer einzelnen Maschine, jedoch wird während der Konvertierung zusätzlicher Speicherplatz benötigt, um die temporäre Maschine aufzunehmen.

Die alte virtuelle Maschine muss zum Zeitpunkt der Konvertierung ausgeschaltet sein, ansonsten ist es nicht möglich, sie zu löschen und wird der Konvertierungstask fehlschlagen. Sollte das passieren, dann können Sie den Konvertierungstask manuell neu starten, nachdem die betreffende Maschine ausgeschaltet wurde. Änderungen, die an der Maschine durchgeführt wurden, während sie eingeschaltet war, werden überschrieben.

Einen Host zur Ausführung der Konvertierung wählen

Geben Sie an, welche Maschine die Konvertierung ausführen soll. Auf der Maschine muss der Acronis Backup & Recovery 10 Agent für Windows, der Agent für ESX/ESXi oder der Agent für Hyper-V installiert sein.

Berücksichtigen Sie die nachfolgenden Überlegungen.

Welcher Agent ist auf dem Host installiert?

Typ und Speicherort der resultierenden virtuellen Maschine hängen von dem Agenten ab, der auf dem gewählten Host vorliegt.

- Der **Agent für Windows** ist auf dem Host installiert

  Es stehen verschiedene Typen virtueller Maschinen zur Auswahl: VMware Workstation, Microsoft Virtual PC, oder Parallels Workstation. Die Dateien der neuen virtuellen Maschine werden in dem von Ihnen ausgewählten Ordner abgelegt.
- Der **Agent für ESX/ESXi** ist auf dem Host installiert

  Auf dem ESX/ESXi-Server wird eine virtuelle VMware-Maschine erstellt.

  Aus einem Backup resultierende virtuelle Maschinen sind nicht dazu gedacht, per Backup gesichert zu werden und erscheinen daher nicht auf dem Management Server, außer dessen Integration mit dem VMware vCenter-Server ist aktiviert. Bei aktivierter Integration erscheinen solche Maschinen als nicht verwaltbar. Auf Sie kann auch keine Backup-Richtlinie angewendet werden.
- Der **Agent für Hyper-V** ist auf dem Host installiert

  Sie können entweder auf dem Hyper-V-Server eine virtuelle Maschine erstellen oder in dem von Ihnen gewählten Ordner eine VMware Workstation, Microsoft Virtual PC oder Parallels Workstation Maschine erstellen lassen.

  Infolge eines Backups auf dem Hyper-V-Server erstellte virtuelle Maschinen erscheinen nicht auf dem Management Server, weil solche Maschinen nicht dazu gedacht sind, per Backup gesichert zu werden.

Was versteht man unter der Rechenleistung des Hosts?

Der Konvertierungstask wird auf der zu sichernden Maschine erstellt und verwendet die Zeiteinstellungen der Maschine. Tatsächlich wird der Task von dem von Ihnen bestimmten Host ausgeführt und daher auch dessen CPU-Ressourcen beanspruchen. Verwenden mehrere Backup-Pläne denselben Host, dann werden auf diesem mehrere Konvertierungstasks in einer Warteschlange abgearbeitet; deren vollständige Abarbeitung kann eine beträchtliche Zeit benötigen.

Welcher Storage wird für die virtuellen Maschinen verwendet?

Netzwerk-Verwendung

Im Gegensatz zu gewöhnlichen Backups (tib-Dateien), werden die 'Virtuellen Maschinen'-Dateien unkomprimiert durch das Netzwerk übertragen. Aus Sicht der Netzwerkverwendung ist es daher am besten, ein SAN oder einen lokalen Storage für den Host zu verwenden, der die Konvertierung ausführt. Sie können jedoch kein lokales Laufwerk wählen, wenn die Konvertierung von derselben Maschine durchgeführt wird, die auch gesichert wird. Die Verwendung eines NAS macht ebenfalls Sinn.

Speicherplatz für Laufwerke

Auf VMware ESX/ESXi werden neue Maschinen mit vorab zugewiesenen (pre-allocated) Laufwerken

erstellt. Das bedeutet, dass die virtuelle Laufwerksgröße immer gleich zur ursprünglichen Laufwerkskapazität ist. Angenommen, die ursprüngliche Laufwerksgröße beträgt 100 GB, dann wird das korrespondierende virtuelle Laufwerk 100 GB belegen, selbst wenn das Laufwerk nur Daten von 10 GB speichert.

Auf einem Hyper-V-Server erstellte virtuelle Maschinen oder Maschinen vom 'Workstation-Typ' (VMware Workstation, Microsoft Virtual PC oder Parallels Workstation) verwenden so viel Laufwerksspeicherplatz wie von den ursprünglichen Daten belegt wird. Da der Speicherplatz nicht 'pre-allocated' ist, ist für das physikalische Laufwerk, auf dem die virtuelle Maschine laufen wird, zu erwarten, dass zur Vergrößerung der virtuellen Laufwerke ausreichend Speicherplatz vorhanden ist.

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. 422) oder durch Verwendung des Acronis Startup Recovery Managers (S. 52). Erstellen Sie dann einen Recovery-Task.

Acronis Universal Restore (S. 53) ermöglicht Ihnen eine Wiederherstellung und das Booten von **Windows auch auf abweichender Hardware** oder auf einer virtuellen Maschine.

Ein **Windows-System kann in Sekunden wieder online gebracht werden**, noch während die Wiederherstellung im Hintergrund abläuft. Dank der proprietären Technologie Acronis Active Restore (S. 55) kann Acronis Backup & Recovery 10 die Maschine in das im Backup vorliegende Betriebssystem „hinein“ booten, ganz so, als ob das System auf einer physikalischen Festplatte vorliegen würde. Das System wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Auf diese Weise bleibt die Ausfallszeit des Systems minimal.

Ein **dynamisches Volume** kann über ein bereits existierendes Volume, den 'nicht zugeordneten' Speicherplatz einer Laufwerksgruppe oder den 'nicht zugeordneten' Speicherplatz eines einzelnen Basis-Laufwerks wiederhergestellt werden. Um mehr über die Wiederherstellung dynamischer Volumes zu erfahren, wechseln Sie zum Abschnitt Microsoft LDM (dynamische Volumes) (S. 45).

Der Acronis Backup & Recovery 10 Agent für Windows hat die Fähigkeit, ein Laufwerk- bzw. Volume-Backup zu einer neuen virtuellen Maschine folgenden Typs wiederherzustellen: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) oder Red Hat KVM. Die virtuelle Appliance kann dann zu einem XenServer importiert werden. Die Maschine mit VMware Workstation kann mit dem Tool VMware OVF in ein offenes Virtualisierungsformat (OVF) konvertiert werden. Sie können mit dem Acronis Backup & Recovery 10 Agenten für Hyper-V oder dem Agenten für ESX/ESXi eine neue virtuelle Maschine auf dem entsprechenden Virtualisierungs-Server erstellen.

Sie müssen möglicherweise vor einer Wiederherstellung die Zielfestplatten vorbereiten. Acronis Backup & Recovery 10 enthält ein nützliches Disk Management Utility, welches Ihnen erlaubt, Volumes zu erstellen oder zu löschen, das Partitionsschema eines Laufwerks zu ändern, eine Laufwerksgruppe zu erstellen und andere Laufwerksverwaltung-Aktionen auf der Ziel-Hardware durchzuführen (unter einem Betriebssystem oder direkt auf einem fabrikneuen System). Zu weiteren Informationen über Acronis Disk Director LV lesen Sie den Abschnitt Laufwerksverwaltung (S. 291).

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. 234)

[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. 234)

Wählen Sie das Archiv, aus dem die Daten wiederhergestellt werden sollen.

Datentyp (S. 235)

Angewendet auf: Laufwerk-Recovery

Bestimmen Sie den Datentyp, den Sie von dem gewählten Laufwerk-Backup wiederherstellen müssen.

Inhalt (S. 235)

Bestimmen Sie das Backup und den wiederherzustellenden Inhalt.

Anmeldedaten (S. 236)

[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

Acronis Active Restore

[OPTIONAL] Das Kontrollkästchen für **Acronis Active Restore** ist verfügbar, wenn Sie Windows wiederherstellen (unterstützt ab Windows 2000). Acronis Active Restore bringt ein System unmittelbar wieder online, sobald die Wiederherstellung gestartet ist. Das Betriebssystem bootet aus dem Backup-Image 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.

Siehe Acronis Active Restore (S. 55) zu weiteren Details.

Dateien (S. 243)

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. 244)

[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. 245)

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.

[Optional] Acronis Universal Restore

Angewendet auf: Wiederherstellung des Windows-Betriebssystem und der Systempartition

Universal Restore (S. 245)

Verwenden Sie Acronis Universal Restore, wenn Sie Windows auf abweichender Hardware wiederherstellen und booten müssen.

Automatische Suche nach Treibern

Spezifizieren Sie, wo das Programm nach HAL-, Massenspeichergeräte- und Netzwerkadapter-Treibern suchen soll. Acronis Universal Restore wird die Treiber installieren, die besser für die Ziel-Hardware geeignet sind.

Treiber für Massenspeicher, die unbedingt installiert werden sollen

[Optional] Geben Sie die Massenspeichergeräte-Treiber manuell an, wenn die automatische Treiber-Suche die passenden Treiber nicht findet. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

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. 121) 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. 34).

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 34), 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

Verfügbar, wenn der Acronis Backup & Recovery 10 Agent für Windows oder Agent für Linux installiert ist.

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.

Neue virtuelle Maschine (S. 242)

Wenn der Acronis Backup & Recovery 10 Agent für Windows installiert ist.

Die gewählten Laufwerke werden zu einer neuen virtuellen Maschine mit einem der folgenden Typen wiederhergestellt: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) oder Red Hat KVM. Die Dateien der virtuellen Maschinen werden zu dem von Ihnen angegebenen Ziel gespeichert.

Wenn der Acronis Backup & Recovery 10 Agent für Hyper-V oder der Agent für ESX/ESXi installiert ist.

Diese Agenten ermöglichen es, eine neue virtuelle Maschine auf einem von Ihnen angegebenen Virtualisierungs-Server zu erstellen.

Die neue virtuelle Maschine wird automatisch konfiguriert, wo möglich, wird die Konfiguration der Quellmaschine kopiert. Die Konfiguration wird im Abschnitt **Einstellungen der virtuellen Maschine** (S. 242) angezeigt. Überprüfen Sie die Einstellungen und führen Sie, sofern benötigt, Änderungen aus.

Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Existierende virtuelle Maschine

Verfügbar, wenn der Acronis Backup & Recovery 10 Agent für Hyper-V oder der Agent für ESX/ESXi installiert ist.

Mit dieser Auswahl spezifizieren Sie den Virtualisierungs-Server und die virtuelle Zielmaschine. Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Beachten Sie, dass die Zielmaschine vor der Wiederherstellung automatisch ausgeschaltet wird. Modifizieren Sie die Power-Einstellungen der virtuellen Maschine, falls Sie es bevorzugen, diese manuell auszuschalten.

Laufwerk Nr.:

Laufwerk Nr. (MODELL) (S. 240)

Bestimmten Sie für jedes Quelllaufwerk das entsprechende Ziellaufwerk.

NT-Signatur (S. 238)

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. Wenn Sie dieselbe Disk-Signatur wiederherstellen, müssen Sie bereits erzeugte Tasks nicht neu erstellen oder bearbeiten.
  - Einige installierte Anwendungen verwenden eine Disk-Signatur zur Lizenzierung oder für andere Einsatzzwecke.
  - Das ermöglicht es, alle Windows Systemwiederherstellungspunkte auf der wiederhergestellten Festplatte zu behalten.
  - So stellen Sie VSS-Snapshots (VSS = virtueller Schattenkopie-Dienst) wieder her, die von der Windows Vista-Funktion „Vorherige Versionen“ verwendet werden

- **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

Verfügbar, wenn der Acronis Backup & Recovery 10 Agent für Windows oder Agent für Linux installiert ist.

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.

Neue virtuelle Maschine (S. 242)

Wenn der Acronis Backup & Recovery 10 Agent für Windows installiert ist.

Die gewählten Volumes (Partitionen) werden zu einer neuen virtuellen Maschine mit einer der folgenden Typen wiederhergestellt: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) oder Red Hat KVM. Die Dateien der virtuellen Maschinen werden zu dem von Ihnen angegebenen Ziel gespeichert.

Wenn der Acronis Backup & Recovery 10 Agent für Hyper-V oder der Agent für ESX/ESXi installiert ist.

Diese Agenten ermöglichen es, eine neue virtuelle Maschine auf einem von Ihnen angegebenen Virtualisierungs-Server zu erstellen.

Die neue virtuelle Maschine wird automatisch konfiguriert, wo möglich, wird die Konfiguration der Quellmaschine kopiert. Die Konfiguration wird im Abschnitt **Einstellungen der virtuellen Maschine** (S. 242) angezeigt. Überprüfen Sie die Einstellungen und führen Sie, sofern benötigt, Änderungen aus.

Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerks-Mapping-Prozedur fort.

Existierende virtuelle Maschine

Verfügbar, wenn der Acronis Backup & Recovery 10 Agent für Hyper-V oder der Agent für ESX/ESXi installiert ist.

Mit dieser Auswahl spezifizieren Sie den Virtualisierungs-Server und die virtuelle Zielmaschine. Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerks-Mapping-Prozedur fort.

Beachten Sie, dass die Zielmaschine vor der Wiederherstellung automatisch ausgeschaltet wird. Modifizieren Sie die Power-Einstellungen der virtuellen Maschine, falls Sie es bevorzugen, diese manuell auszuschalten.

[Disk Nr.] MBR wiederherstellen auf: [wenn der Master Boot Record für die Wiederherstellung ausgewählt ist]

Laufwerk Nr. (S. 240)

Wählen Sie das Laufwerk, auf der der Master Boot Record wiederhergestellt wird.

NT-Signatur: (S. 238)

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.

[Laufwerk] [Buchstabe] wiederherstellen auf:

Laufwerk Nr. /Volume (S. 240)

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.

Typ der virtuellen Maschine / Wahl des Virtualisierungs-Servers

Die neue virtuelle Maschine kann entweder auf einem Virtualisierungs-Server erstellt werden (benötigt einen installierten Acronis Backup & Recovery 10 Agenten für Hyper-V oder für ESX/ESXi) oder in jedem zugreifbaren lokalen Ordner bzw. Netzwerk-Ordner.

So bestimmen Sie den Virtualisierungs-Server, auf dem die virtuelle Maschine erstellt wird:

1. Wählen Sie die Option **Auf dem Virtualisierungs-Server ablegen, den ich auswähle**.
2. Wählen Sie im linken Teil des Fensters den Virtualisierungs-Server. Verwenden Sie den rechten Fensterbereich, um Details über den gewählten Server einzusehen.
3. Klicken Sie auf **OK**, um zur Seite **Recovery** zurückzukehren.

So wählen Sie den Typ der virtuellen Maschine

1. Wählen Sie die Option **Als Dateien des von mir gewählten VM-Typs in dem Ordner speichern, den ich angebe**.
2. Wählen Sie im linken Teil des Fensters den Typ der virtuellen Maschine. Verwenden Sie den rechten Fensterbereich, um Details über den gewählten Typ der virtuellen Maschine einzusehen.
3. Klicken Sie auf **OK**, um zur Seite **Recovery** zurückzukehren.

Einstellungen der virtuellen Maschine

Sie können die nachfolgenden Einstellungen der virtuellen Maschinen konfigurieren.

Storage

Anfangseinstellung: Der Standardspeicher des Virtualisierungs-Servers, sofern die neue Maschine auf dem Virtualisierungs-Server erstellt wird. Anderenfalls der persönliche Ordner für Dokumente des aktuellen Benutzers.

Das ist der Speicherort, an dem die neue virtuelle Maschine erstellt wird. Ob Sie den Speicherort auf dem Virtualisierungs-Server verändern können oder nicht, hängt vom Fabrikat und den Einstellungen des Virtualisierungs-Produkts ab. VMware ESX darf mehrere Speicherorte haben. Ein Microsoft Hyper-V-Server ermöglicht das Erstellen einer neuen virtuellen Maschine in jedem lokalen Ordner.

Arbeitsspeicher

Anfangseinstellung: Die Standardeinstellungen des Virtualisierungs-Servers, sofern nicht im Backup enthalten.

Dies ist die Menge des Hauptspeichers, der der neuen virtuellen Maschine zugeteilt ist. Der einstellbare Bereich für die Speicherzuteilung hängt von der Hardware des Hosts ab, dessen Betriebssystem und den Einstellungen des Virtualisierungs-Produkts. Als Beispiel könnte es den virtuellen Maschinen nicht erlaubt sein, mehr als 30% des Arbeitsspeichers zu verwenden.

Laufwerke

Anfangseinstellung: Die Zahl und Größe der Laufwerke der Quellmaschine.

Für gewöhnlich ist die Zahl der Laufwerke gleich denen der Quellmaschine, sie kann jedoch abweichen, wenn das Programm weitere Laufwerke hinzufügen muss, um die Laufwerke der Quellmaschine aufzunehmen, weil durch das Virtualisierungs-Produkt entsprechende Limitierungen gesetzt sind. Sie können der Konfiguration der Maschine weitere virtuelle Laufwerke hinzufügen oder in manchen Fällen das vorgeschlagene Laufwerk löschen.

Die Implementierung von Xen-Maschinen basiert auf Microsoft Virtual PC und hat daher dieselben

Einschränkungen: bis zu 3 IDE-Laufwerke und 1 Prozessor. SCSI-Laufwerke werden nicht unterstützt.

Prozessoren

Anfangseinstellung: Die Standardeinstellungen des Servers, sofern nicht im Backup enthalten oder wenn die gesicherten Einstellungen vom Virtualisierungs-Server nicht unterstützt werden.

Es handelt sich um die Zahl der Prozessoren für die neue virtuelle Maschine. In den meisten Fällen ist sie auf einen Prozessor eingestellt. Wird der Maschine mehr als ein Prozessor zugewiesen, so kann das Ergebnis nicht garantiert werden. Die Zahl virtueller Prozessoren kann durch die CPU-Konfiguration des Hosts, das Virtualisierungs-Produkt und das Betriebssystems des Gastes limitiert werden. Üblicherweise stehen mehrere virtuelle Prozessoren auf Hosts zur Verfügung, die selbst mehrere Prozessoren haben. Eine Multi-Core Host-CPU oder Hyper-Threading kann mehrfache virtuelle Prozessoren auch auf einem Single-Prozessor-Host ermöglichen.

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. 243) 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 Universal Restore

Verwenden Sie Acronis Backup & Recovery 10 Universal Restore, wenn Sie Windows auf abweichender Hardware wiederherstellen und booten müssen. Universal Restore behandelt abweichende Geräte, die kritisch für den Betriebssystemstart sind, wie z.B. Speicher-Controller, Hauptplatine oder Chipsatz.

Um mehr über die Universal Restore-Technologie zu erfahren, siehe den Abschnitt Universal Restore (S. 53).

Acronis Backup & Recovery 10 Universal Restore ist nicht verfügbar, wenn:

- eine Maschine über den Acronis Startup Recovery Manager (unter Benutzung von F11) gebootet wurde
- das Backup-Image in der Acronis Secure Zone liegt
- Sie die Verwendung von Acronis Active Restore (S. 418) gewählt haben,

weil alle diese Funktionen hauptsächlich für sofortige Datenwiederherstellung auf der gleichen Maschine gedacht sind.

Vorbereitung

Bevor Sie Windows auf abweichende Hardware wiederherstellen, sollten Sie sicherstellen, dass Sie für den neuen Festplatten-Controller und Chipsatz die passenden Treiber haben. Diese Treiber sind für den Start des Betriebssystems entscheidend. Verwenden Sie die vom Hardware-Hersteller mitgelieferte CD bzw. DVD oder laden Sie die Treiber von der Website des Herstellers herunter. Die Treiber sollten die Erweiterungen *.inf, *.sys oder *.oem haben. Wenn Sie die Treiber im Format *.exe, *.cab oder *.zip herunterladen, dann extrahieren Sie diese unter Verwendung einer Dritthersteller-Anwendung wie WinRAR (http://www.rarlab.com) oder Universal Extractor (http://legroom.net/software/uniextract).

Der praktischste Ansatz ist es, die Treiber für all die in Ihrer Organisation verwendete Hardware an einem Aufbewahrungsort zu speichern, sortiert nach Gerätetyp oder Hardware-Konfiguration. Sie können eine Kopie des Aufbewahrungsortes auf einer DVD oder einem USB-Stick vorhalten; verwenden Sie einige Treiber und fügen Sie diese dem bootfähigen Medien hinzu; erstellen Sie für

jeden Ihrer Server ein benutzerdefiniertes bootfähiges Medium mit den notwendigen Treibern (und der notwendigen Netzwerk-Konfiguration). Alternativ können Sie auch einfach jedes Mal, wenn Universal Restore verwendet wird, den Pfad zum Aufbewahrungsort angeben.

Stellen Sie sicher, dass Sie bei Verwendung eines bootfähigen Mediums auf das Gerät mit den Treibern zugreifen können. Auch wenn Sie eine Wiederherstellung des Systemlaufwerks unter Windows konfigurieren, wird die Maschine neu gestartet und die Recovery-Aktion dann in einer Linux-basierten Umgebung durchgeführt. Verwenden Sie ein WinPE-basiertes Medium, falls das Gerät unter Windows verfügbar ist, aber von einem Linux-basierten Notfallmedium nicht erkannt wird.

Universal Restore-Einstellungen

Automatische Suche nach Treibern

Spezifizieren Sie, wo das Programm nach Hardware Abstraction Layer- (HAL), Festplatten-Controller- und Netzwerkadapter-Treibern suchen soll:

- Befinden sich die Treiber auf einer Disc des Herstellers oder anderen Wechselmedien, so aktivieren Sie **Wechselmedien durchsuchen**.

- Liegen die Treiber in einem Netzwerk-Ordner oder auf einem bootfähigen Medium, so spezifizieren Sie den Pfad zu diesem Ordner im Feld **Ordner durchsuchen**.

Während der Wiederherstellung führt Universal Restore eine rekursive Suche in allen Unterordnern des angegebenen Verzeichnisses durch, findet aus allen verfügbaren die am besten passenden HAL- und Festplatten-Controller-Treiber heraus und installiert diese in das wiederhergestellte System. Universal Restore sucht außerdem nach Treibern für Netzwerk-Adapter, der Pfad des gefundenen Treibers wird dann dem Betriebssystem durch Universal Restore übermittelt. Wenn die Hardware über mehrere Netzwerkkarten verfügt, so versucht Universal Restore, die Treiber aller Karten zu konfigurieren. Für den Fall, dass Universal Restore am angegebenen Speicherort keinen kompatiblen Treiber finden kann, wird das problematische Gerät angegeben und nach einer Disc oder einem Netzwerk-Pfad zu dem Treiber gefragt.

Sobald Windows bootet, wird es die Standardprozedur zur Installation neuer Hardware initialisieren. Der Treiber für den Netzwerk-Adapter wird stillschweigend installiert, sofern er eine Microsoft Windows-Signatur hat. Anderenfalls erfragt Windows Ihre Bestätigung zur Installation des unsignierten Treibers.

Danach können Sie die Netzwerk-Verbindung konfigurieren und Treiber für Grafikkarte, USB- und andere Geräte spezifizieren.

Treiber für Massenspeicher, die unbedingt installiert werden

Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Wenn die Ziel-Hardware einen spezifischen Massenspeicher-Controller wie RAID (insbesondere NVIDIA RAID) oder einen Fibre Channel-Adapter verwendet, dann spezifizieren Sie die passenden Treiber im Feld **Treiber**.

Die hier angegebenen Treiber haben Priorität. Sie werden auch installiert, mit entsprechenden Warnungen, wenn das Programm einen besseren Treiber findet.

Benutzen Sie diese Option nur, wenn die automatische Suche nach Treibern nicht hilft, das System zu starten.

Treiber für eine virtuelle Maschine

Bei Wiederherstellung eines Systems zu einer virtuellen Maschine wird die Universal Restore-Technologie im Hintergrund angewendet, weil das Programm weiß, welche Treiber für die unterstützten virtuellen Maschinen benötigt werden.

Wenn Sie ein System zu einer existierenden virtuellen Maschine wiederherstellen, die einen SCSI-Festplatten-Controller verwendet, dann stellen Sie sicher, dass Sie die SCSI-Treiber für die virtuelle Umgebung im Schritt **Massenspeicher-Treiber, die auf jeden Fall installiert werden** angeben. Verwenden Sie die Treiber, die mit der Software für Ihre virtuellen Maschinen gebundelt sind, oder laden Sie die neuste Treiberversion von der Website des Software-Herstellers.

6.3.10 Konvertieren eines Laufwerk-Backups in eine virtuelle Maschine

Alternativ zur Konvertierung einer tib-Datei in eine virtuellen Laufwerksdatei, wobei zusätzliche Aktionen für die Verfügbarkeit des virtuellen Laufwerks erforderlich wären, erfolgt die Konvertierung in Acronis Backup & Recovery 10 so, dass ein Laufwerk-Backup in einer neuen, vollständig konfigurierten und betriebsbereiten virtuellen Maschine wiederhergestellt wird. Sie können bei der Vorbereitung der Wiederherstellungsaktion die Konfiguration der virtuellen Maschine an Ihre speziellen Anforderungen anpassen.

Mit **Acronis Backup & Recovery 10 Agent für Windows** können Sie ein Disk-Backup (bzw. Volume-Backup) in einer neuen virtuellen Maschine eines der folgenden Typen wiederherstellen: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) oder Red Hat KVM.

Die Dateien der neuen virtuellen Maschine werden in dem von Ihnen ausgewählten Ordner abgelegt. Sie können die Maschine unter Verwendung der entsprechenden Virtualisierungssoftware starten oder die Dateien der Maschine für eine künftige Verwendung vorbereiten. Die Citrix XenServer Open Virtual Appliance (OVA) kann unter Verwendung eines Citrix XenCenter zu einem XenServer importiert werden. Die Maschine mit VMware Workstation kann mit dem Tool VMware OVF in ein offenes Virtualisierungsformat (OVF) konvertiert werden.

Mit **Acronis Backup & Recovery 10 Agent für Hyper-V** oder **Agent für ESX/ESXi** können Sie ein Disk-Backup (bzw. Volume-Backup) in einer neuen virtuellen Maschine auf dem entsprechenden Virtualisierungs-Server wiederherstellen.

Tipp. *Microsoft Virtual PC unterstützt keine Laufwerke die größer sind als 127 GB. Acronis ermöglicht Ihnen, eine Virtual PC-Maschine mit größeren Laufwerken zu erstellen, so dass Sie die Laufwerke an eine virtuelle Microsoft Hyper-V-Maschine anbinden können.*

So konvertieren Sie ein Disk-Backup zu einer virtuellen Maschine

1. Verbinden Sie die Konsole mit einer Maschine, auf der der Agent für Windows, der Agent für Hyper-V oder der Agent für ESX/ESXi installiert ist.
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Recovery**, um die Seite **Daten wiederherstellen** zu öffnen. Beginnen Sie mit der Erstellung eines Recovery-Tasks, wie in Daten wiederherstellen beschrieben. Wählen Sie das Archiv und wählen Sie dann das Disk-Backup bzw. das Volume-Backup aus, das Sie konvertieren möchten.
   - Verwenden Sie die Seitenleiste **Navigation**, um zu dem Depot zu navigieren, in dem das Archiv gespeichert ist. Wählen Sie das Archiv und wählen Sie dann das Disk-Backup bzw. das Volume-Backup aus, das Sie konvertieren möchten. Klicken Sie auf **Als virtuelle Maschine wiederherstellen**. Die Seite **Daten wiederherstellen** wird mit dem ausgewählten Backup geöffnet.
3. Unter **Datentyp** wählen Sie entsprechend des Objekts, das Sie konvertieren möchten, entweder **Laufwerke** oder **Volumes**.

4. Unter **Inhalt** wählen Sie die zu konvertierenden Datenträger (Disks) oder Volumes mit den MBRs (Master Boot Records) der entsprechenden Datenträger.
5. Unter **Wiederherstellen nach** wählen Sie **Neue virtuelle Maschine**.
6. Unter **VM-Server** wählen Sie den Typ der neuen, zu erstellenden virtuellen Maschine *oder* Sie wählen aus, auf welchem Virtualisierungs-Server die Maschine erstellt werden soll.
7. Unter **VM-Name** tragen Sie den Namen für die neue virtuelle Maschine ein.
8. [Optional] Überprüfen Sie die **Einstellungen für die virtuelle Maschine (S. 242) und** nehmen Sie gegebenenfalls Änderungen vor. Hier können Sie den Pfad auf die neue virtuelle Maschine ändern.

   In ein und demselben Ordner kann nicht derselbe Maschinentyp mit demselben Namen noch einmal erstellt werden. Wenn Sie eine Fehlermeldung erhalten, die durch identische Namen hervorgerufen wurde, dann ändern Sie entweder den VM-Namen oder den Pfad.

9. Wählen Sie für jeden Quelldatenträger oder jedes Quell-Volume und die MBRs den Zieldatenträger aus.

   Unter Microsoft Virtual PC, wo sich der Loader des Betriebssystems auf Laufwerk 1 befindet, müssen Sie unbedingt dieses Laufwerk oder Volume wiederherstellen. Anderenfalls wird das Betriebssystem nicht starten. Das kann durch Ändern der Reihenfolge der Boot-Geräte im BIOS nicht repariert werden, weil Virtual PC diese Einstellungen ignoriert.

10. Unter **Recovery-Zeitpunkt** geben Sie an, wann der Recovery-Task beginnen soll.
11. [Optional] Überprüfen Sie die **Recovery-Optionen** und ändern Sie die Standardeinstellungen gegebenenfalls ab. Sie können bei **Recovery-Optionen –> Zustand der VM steuern**, ob Sie die neue virtuelle Maschine automatisch starten möchten, nachdem die Wiederherstellung vollständig ist. Diese Option ist nur verfügbar, wenn die neue Maschine auf einem Virtualisierungs-Server erstellt wird.
12. Klicken Sie auf **OK**. Wenn der Recovery-Task für einen späteren Zeitpunkt geplant ist, geben Sie die Anmeldedaten an, unter denen der Task ausgeführt wird.

Daraufhin gelangen Sie zur Ansicht **Backup-Pläne und Tasks**, in der Sie das Stadium und den Fortschritt des Recovery-Tasks überprüfen können.

Aktionen nach Konvertierung

Die resultierende Maschine hat immer eine SCSI-Laufwerksschnittstelle und Basis-MBR-Volumes. Falls die Maschine einen benutzerdefinierten Boot-Loader verwendet, müssen Sie diesen möglicherweise mit einem Zeiger auf die neuen Geräte konfigurieren und den Loader reaktivieren. Die Konfiguration von GRUB ist unter „So reaktivieren Sie GRUB und ändern die Konfiguration (S. 250)“ beschrieben.

Tipp. *Wenn Sie auf einer Linux-Maschine logische (LVM-)Volumes erhalten wollen, sollten Sie eine alternative Konvertierungsmethode erwägen. Erstellen Sie eine neue virtuelle Maschine, die Sie per bootfähigem Medium booten und führen Sie dann die Wiederherstellung genau so durch, wie Sie es mit einer physikalischen Maschine tun. Die LVM-Struktur kann dann, sofern diese im Backup gespeichert wurde, während der Wiederherstellung automatisch neu erstellt werden (S. 285).*

6.3.11 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.

Über Windows-Loader

Windows NT/2000/XP/2003

Ein Teil der Loader ist im Boot-Sektor hinterlegt, der Rest befindet sich in den Dateien ntldr, boot.ini, ntdetect.com, ntbootdd.sys. Boot.ini ist eine Textdatei, die die Konfiguration des Loaders enthält. Beispiel:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/noexecute=optin /fastdetect
```

Windows Vista/2008 Server

Ein Teil des Loaders ist im Boot-Sektor hinterlegt, der Rest in den Dateien bootmgr und boot\bcd. Während des Windows-Starts wird boot\bcd in den Registry-Schlüssel HKLM \BCD00000000 gemountet.

6.3.12 Den Storage Node wiederherstellen

In Ergänzung zur Datensicherung auf ein zentrales, durch einen Acronis Backup & Recovery 10 Storage Node verwaltetes Depot möchten Sie möglicherweise auch ein Disk-Backup derjenigen Maschine durchführen, auf der der Storage Node selbst installiert ist.

Dieser Abschnitt beschreibt, wie Sie den Storage Node, der auf dem Management Server registriert ist, für den Fall wiederherstellen, dass Storage Node und Management Server auf verschiedenen Maschinen installiert sind (wenn Sie auf derselben Maschine installiert sind, stellen Sie einfach diese wieder her).

Betrachten Sie folgendes Szenario:

- Sie haben eine Maschine mit dem Management Server und eine Maschine mit dem Storage Node.
- Der Storage Node ist auf dem Management Server registriert.
- Sie haben die Maschine mit dem Storage Node bereits früher gesichert und sie eben erst wiederhergestellt – entweder auf derselben Maschine oder einer anderen.

Bevor Sie den wiederhergestellten Storage Node verwenden, folgen Sie diesen Schritten:

- Wenn Sie den Storage Node auf derselben Maschine wiederhergestellt haben und zwischen Backup und Wiederherstellung keine zentralen, durch den Storage Node verwalteten Depots hinzugefügt oder entfernt wurden, dann tun sie nichts.
- Anderenfalls tun Sie Folgendes:
  1. Erstellen Sie eine Verbindung mit dem Management Server und entfernen Sie den Storage Node von diesem.

  Anmerkung: *Alle durch den Storage Node verwalteten Depots werden ebenfalls vom Management Server entfernt. Es gehen keine Archive verloren.*

  2. Fügen Sie den Storage Node dem Management Server wieder hinzu, indem Sie die Maschine spezifizieren, auf dem der wiederhergestellte Storage Node installiert ist.
  3. Erstellen Sie die benötigten verwalteten Depots neu.

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. 205).

Sie können auf die Seite **Validierung** aus der Ansicht **Depots** (S. 130) 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. 254)

[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. 254) – in diesem Fall müssen Sie das benötigte Archiv angeben.

Backup (S. 255) – spezifizieren Sie zuerst das Archiv und wählen Sie in diesem dann das gewünschte Backup.

Depot (S. 256) – wählen Sie ein Depot (oder anderen Speicherort), dessen Archive validiert werden sollen.

Anmeldedaten für den Zugriff (S. 256)

[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. 257)

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. 34).

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 34), 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. 172).

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. 258)

Spezifizieren Sie den Pfad zum Speicherort des Archivs und wählen Sie die in diesem enthaltenen Disk-Backups.

Backup (S. 259)

Wählen Sie das Backup.

Anmeldeinformationen: (S. 260)

[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. 260)

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.
- **ein komplettes Depot**, das über die Befehlszeilenschnittstelle exportiert werden kann. Weitere Informationen finden Sie in der Acronis Backup & Recovery 10 Befehlszeilen-Referenz.

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. 264)

[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. 234) – in diesem Fall müssen Sie nur das benötigte Archiv angeben.

Backups (S. 265) – spezifizieren Sie zuerst das Archiv und wählen Sie in diesem dann das bzw. die gewünschte(n) Backup(s).

Anmeldeinformationen: (S. 265)

[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. 266)

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. 267)

[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. 34).

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 34), um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

6.7.2 Auswahl des Archivs

So wählen Sie ein Archiv aus

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.

Für den Management Server: Wählen Sie im Verzeichnisbaum das verwaltete Depot aus.

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. Falls das Archiv kennwortgeschützt ist, müssen Sie das entsprechende Kennwort eingeben.

   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.

Für den Management Server enthält der Verzeichnisbaum:

- Die Gruppe 'Lokale Ordner', zum Datenexport auf für den Storage Node lokal verfügbare Laufwerke.
- Die Gruppe 'Netzwerkordner', zum Datenexport auf eine Netzwerkfreigabe. 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.

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. 51) 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. 269)

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. 269)

Spezifizieren Sie die exakte Größe der Zone. Verschieben oder Größenveränderung einer gesperrten Partition, wie der aktuellen Betriebssystempartition, benötigen einen Neustart.

Einstellungen

Kennwort (S. 269)

[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. 270) 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. 269) 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. 423) 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. 130).

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. 422), 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. 272).

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 So erstellen Sie bootfähige Medien

Um ein physikalisches Medium erzeugen zu können, muss die Maschine über einen CD-/DVD-Brenner verfügen oder ein Flash-Laufwerk (z.B. USB-Stick) anschließbar sein. Um PXE oder WDS/RIS

konfigurieren zu können, muss die Maschine eine Netzverbindung haben. Der Bootable Media Builder kann außerdem das ISO-Image einer bootfähigen Disc erstellen, um dieses später auf ein leeres Medium zu brennen.

Linux-basierte bootfähige Medien

Starten Sie den Bootable Media Builder entweder über die Management Konsole durch **Werkzeuge –> Bootfähiges Medium erstellen** oder als eigene Komponente.

Bestimmen Sie, wie Volumes und Netzwerk-Ressourcen gehandhabt werden – den so genannten 'Stil' des Mediums:

- Ein Medium im Linux-Stil stellt Volumes zum Beispiel als hda1 und sdb2 dar. Es versucht, MD-Geräte und logische Volumes (vom LVM verwaltet) vor Start einer Wiederherstellung zu rekonstruieren.
- Ein Medium, das Volumes im Windows-Stil behandelt, verwendet Laufwerksbuchstaben zur Darstellung von Volumes, beispielsweise C: und D:. Es bietet Zugriff auf dynamische Volumes (LDM verwaltet).

Der Assistent wird Sie durch alle notwendigen Aktionen führen. Details finden Sie unter 'Linux-basierte bootfähige Medien (S. 275)'.

PE-basierte bootfähige Medien

Das Acronis Plug-in kann WinPE-Distributionen hinzugefügt werden, die auf folgenden Windows-Kerneln basieren:

- 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).
- Windows 7 (PE 3.0)

Wenn Sie bereits ein Medium mit einer PE1.x-Distribution haben, dann entpacken Sie die ISO-Datei des Mediums in einen lokalen Ordner und starten den Bootable Media Builder über die Management Konsole mit **Extras –> Bootfähiges Medium erstellen** oder als separate Komponente. Der Assistent wird Sie durch alle notwendigen Aktionen führen. Weitere Details finden Sie unter Acronis Plug-in zu WinPE 1.x hinzufügen (S. 279).

Um PE 2.x oder 3.0-Images erstellen oder modifizieren zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Automated Installation Kit (WAIK) installiert ist. Alle weiteren Aktionen sind im Abschnitt Acronis Plug-in zu WinPE 2.x oder 3.0 hinzufügen (S. 280) beschrieben.

Wenn Sie keine Maschine mit WAIK haben, gehen Sie wie folgt vor:

1. Downloaden und installieren Sie das Windows Automated Installation Kit (WAIK).

   Automated Installation Kit (AIK) für Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?displaylang=de&FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2

   Automated Installation Kit (AIK) für Windows Vista SP1 und Windows Server 2008 (PE 2.1):

   http://www.microsoft.com/Downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=de

   Automated Installation Kit (AIK) für Windows 7 (PE 3.0):

http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=696dd665-9f76-4177-a811-39c26d3b3b34

Sie können die Systemanforderungen zur Installation finden, indem Sie den unteren Links folgen.

2. [optional] Brennen Sie das WAIK auf DVD oder kopieren Sie es auf ein Flash-Laufwerk (USB-Stick).
3. Installieren Sie Microsoft .NET Framework v.2.0 von diesem Kit (NETFXx86 oder NETFXx64, von Ihrer Hardware abhängig).
4. Installieren Sie Microsoft Core XML (MSXML) 5.0 oder 6.0 Parser von diesem Kit.
5. Installieren Sie Windows AIK von diesem Kit.
6. Installieren Sie Bootable Media Builder auf der gleichen Maschine.

Es ist empfehlenswert, dass Sie sich mit der dem Windows AIK beiliegenden Hilfe-Dokumentation vertraut machen. Um auf die Dokumentation zuzugreifen, wählen Sie **Microsoft Windows AIK –> Documentation** im Startmenü.

BartPE verwenden

Sie können ein BartPE-Image mit integriertem Acronis Plug-in erzeugen, indem Sie den BartPE Builder verwenden. Details finden Sie unter BartPE mit Acronis Plug-in für Windows-Distribution erzeugen (S. 281)

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. 276).
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. 277):
   - TCP/IP-Einstellungen, die dem Netzwerkadapter der Maschine zugewiesen werden.
6. [Optional] Netzwerk-Port (S. 278):
   - 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 (S. 279). 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.

Treiber für Universal Restore

Während der Erstellung der bootfähigen Medien erhalten Sie eine Option, um Windows-Treiber dem Medium hinzuzufügen. Diese Treiber werden von Universal Restore verwendet, sofern Windows auf einer Maschine wiederhergestellt wird, die im Bezug zum ursprünglichen Backup-System beim Prozessor, Mainboard oder Massenspeichergeräten abweicht.

Sie können Universal Restore auch konfigurieren:

- um das Medium nach Treibern zu durchsuchen, die auf die Ziel-Hardware am besten passen
- um die Massenspeicher-Treiber einzubinden, die Sie ausdrücklich vom Medium aus spezifiziert haben. Dies ist notwendig, wenn die Ziel-Hardware einen spezifischen Massenspeicher-Kontroller für Festplatten verwendet (wie SCSI, RAID oder Fiber Channel-Adapter).

Weitere Informationen finden Sie bei Universal Restore (S. 245).

Die Treiber werden im sichtbaren Treiber-Ordner auf dem bootfähigen Medium hinterlegt. Die Treiber werden nicht in den RAM der Ziel-Maschine geladen, daher muss das Medium während der Universal Restore-Aktion eingelegt bzw. verbunden bleiben.

Das Hinzufügen von Treibern zu bootfähigen Medien ist unter folgenden Bedingungen möglich:

1. Das Acronis Backup & Recovery 10 Universal Restore Add-on ist auf der für die Erstellung der bootfähigen Medien verwendeten Maschine installiert UND
2. Sie erzeugen ein Wechselmedium (oder sein ISO-Abbild) oder anschließbares Medium wie einen USB-Stick. Treiber können nicht auf einen PXE Server oder WDS/RIS hochgeladen werden.

Die Treiber können zur Liste nur in Gruppen hinzugefügt werden, indem die INF-Dateien oder Ordner hinzugefügt werden, die solche Dateien enthalten. Die Wahl einzelner Treiber aus den INF-Dateien ist nicht möglich, der Media Builder informiert Sie jedoch über den Inhalt der Dateien.

So fügen Sie Treiber hinzu:

1. Klicken Sie auf **Hinzufügen** und wählen Sie dann die INF-Datei oder den die INF-Dateien enthaltenden Ordner.
2. Wählen Sie die INF-Datei oder den Ordner aus.
3. Klicken Sie auf **OK**.

Die Treiber können aus der Liste nur in Gruppen, durch Löschen der INF-Dateien, entfernt werden.

So entfernen Sie Treiber:

1. Wählen Sie die INF-Datei aus.
2. Klicken Sie auf **Entfernen**.

Das Acronis-Plug-in zu WinPE 1.x hinzufügen

Das Acronis-Plug-in für WinPE kann hinzugefügt werden zu:

- Windows PE 2004 (1.5) (Windows XP Professional mit Service Pack 2)
- Windows PE 2005 (1.6) (Windows Server 2003 mit Service Pack 1).

Um das Acronis-Plug-in WinPE 1.x hinzuzufügen:

1. Entpacken Sie alle Dateien Ihrer WinPE 1.x ISO in einen separaten Ordner auf Ihrer Festplatte (oder einem ähnlichen Laufwerk).

2. Starten Sie den Bootable Media Builder entweder über die Management Konsole durch **Werkzeuge –> Bootfähiges Medium erstellen** oder als eigene Komponente.
3. Wählen Sie den **Typ des bootfähigen Mediums: Windows PE**.
   - Wählen Sie **Verwende WinPE-Dateien im spezifizierten Ordner**
4. Geben Sie den Pfad zum Ordner mit den WinPE-Dateien an.
5. Spezifizieren Sie die Netzwerkeinstellungen (S. 277) für den Netzwerkadapter der Maschine oder wählen Sie eine Auto-Konfiguration per DHCP.
6. Geben Sie den vollen Pfad für die zu entstehende ISO-Datei an (einschließlich des Dateinamens).
7. Überprüfen Sie Ihre Einstellungen im Abschlussfenster und klicken Sie auf **Fertig stellen**.
8. Brennen Sie die ISO-Datei auf CD oder DVD (durch das Brennprogramm eines Drittherstellers) oder kopieren Sie die Daten auf ein Flash-Laufwerk wie einen USB-Stick (Daten und Flash-Laufwerk müssen zum Booten separat angepasst werden).

Sobald eine Maschine mit WinPE gebootet ist, startet Acronis Backup & Recovery 10 automatisch.

Das Acronis-Plug-in zu WinPE 2.x oder 3.0 hinzufügen

Der Bootable Media Builder bietet drei Methoden, um Acronis Backup & Recovery 10 in WinPE 2.x oder 3.0 einzubinden:

- Das Acronis-Plug-in einem existierenden PE-ISO-Abbild hinzufügen. Das ist praktisch, wenn Sie das Plug-in einem früher konfiguriertem, in Verwendung befindlichem PE-ISO-Abbild hinzufügen müssen.
- Ein PE-ISO-Abbild mit dem Plug-in neu erstellen.
- Das Acronis-Plug-in einer WIM-Datei zur zukünftigen Verwendung hinzufügen (manuelle ISO-Erstellung, andere Tools dem Abbild hinzufügen, usw.).

Um die beschriebenen Aktionen durchführen zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Automated Installation Kit (WAIK) installiert ist. Sofern Sie keine solche Maschine haben, bereiten Sie diese wie unter So erstellen Sie bootfähige Medien (S. 273) beschrieben vor.

Bootable Media Builder unterstützt nur x86 WinPE 2.x oder 3.0 (32-Bit-Version). Diese WinPE-Distributionen können aber auch auf x64-Hardware verwendet werden.

Ein PE-Abbild, das auf WinPE 2.0 basiert, benötigt mindestens 256MB RAM zum Arbeiten. Die empfohlene Speichergröße für PE 2.0 ist 512MB. Ein PE-Abbild, das auf WinPE 3.0 basiert, benötigt mindestens 512MB RAM zum Arbeiten.

Das Acronis-Plug-in einem ISO-Image von WinPE 2.x oder 3.0 hinzufügen

So fügen Sie das Acronis-Plug-in einem WinPE 2.x oder 3.0 ISO-Abbild hinzu:

1. Wenn Sie das Plug-in der existierenden WinPE-ISO-Datei hinzufügen, entpacken Sie alle Dateien Ihrer WinPE-ISO in einen separaten Laufwerksordner.
2. Starten Sie den Bootable Media Builder entweder über die Management Konsole durch **Werkzeuge –> Bootfähiges Medium erstellen** oder als eigene Komponente.
3. Wählen Sie den **Typ des bootfähigen Mediums: Windows PE**.

   Wenn Sie eine neue PE-ISO-Datei erstellen:
   - Wählen Sie **Erstelle Windows PE 2.x oder 3.0 automatisch**
   - Die Software führt das passende Skript aus und wechselt zum nächsten Fenster.

   So fügen Sie das Plug-in einem existierenden PE-ISO-Abbild hinzu:
   - Wählen Sie **Verwende WinPE-Dateien im spezifizierten Ordner**

- Geben Sie den Pfad zum Ordner mit den WinPE-Dateien an.

4. Spezifizieren Sie die Netzwerkeinstellungen (S. 277) für den Netzwerkadapter der Maschine oder wählen Sie eine Auto-Konfiguration per DHCP.
5. [Optional] Spezifizieren Sie die Windows-Treiber, die Windows PE hinzugefügt werden sollen. Wenn Sie eine Maschine mit Windows PE booten, ermöglichen Ihnen diese Treiber, auf Geräte zuzugreifen, auf denen sich Ihre Backup-Archive befinden. Klicken Sie auf **Hinzufügen** und geben Sie den Pfad zur notwendigen *. inf-Datei für einen entsprechenden SCSI-, RAID- oder SATA-Controller, einen Netzwerkadapter, ein Bandlaufwerk oder andere Geräte an. Sie müssen dieses Verfahren für jedem Treiber wiederholen, den Sie in das resultierende WinPE-Boot-Medium aufnehmen wollen.
6. Wählen Sie, ob Sie ein ISO- oder WIM-Image erstellen oder das Medium auf einen Acronis PXE-Server laden möchten.
7. Geben Sie den vollen Pfad einschließlich Dateiname zur resultierenden Image-Datei an – oder spezifizieren Sie einen PXE-Server, inklusive Benutzername und Kennwort für den Zugriff.
8. Überprüfen Sie Ihre Einstellungen im Abschlussfenster und klicken Sie auf **Fertig stellen**.
9. Brennen Sie die ISO-Datei auf CD oder DVD (durch das Brennprogramm eines Drittherstellers) oder kopieren Sie die Daten auf ein Flash-Laufwerk wie einen USB-Stick (Daten und Flash-Laufwerk müssen zum Booten separat angepasst werden).

Sobald eine Maschine mit WinPE gebootet wird, startet Acronis Backup & Recovery 10 automatisch.

So erstellen Sie ein PE-Abbild (ISO-Datei) von einer resultierenden WIM-Datei:

- Ersetzen Sie die vorgegebene boot.wim-Datei im Windows PE-Ordner mit der neu erstellten WIM-Datei. Für das genannte Beispiel geben Sie ein:

  ```
  copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- verwenden Sie das Tool **Oscdimg**. Für das genannte Beispiel geben Sie ein:

  ```
  oscdimg -n –bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
  c:\winpe_x86\winpe_x86.iso
  ```

Weitere Informationen zur Anpassung von Windows PE finden Sie im Windows PE-Benutzerhandbuch (Winpe.chm).

BartPE mit Acronis Plug-in für Windows-Distributionen erstellen

1. Bart's PE Builder verwenden.
2. Installieren Sie Bootable Media Builder mit der Acronis Backup & Recovery 10 Installationsdatei.
3. Ändern Sie den aktuellen Ordner in den Ordner, in dem das Acronis Plug-in für WinPE installiert ist – standardmäßig ist dies: C:\Programme\Acronis\Bootable Components\WinPE.

   Wenn das Plug-in in einem anderen als dem Standardordner installiert ist, dann änden Sie den Pfad entsprechend (Sie finden den Speicherort des Plug-Ins im Registry-Key HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Bootable Components\Settings\WinPE).
4. Entpacken Sie die WinPE.zip-Datei in den aktuellen Ordner.
5. Führen Sie folgenden Befehl aus:

   ```
   export_license.bat
   ```

6. Kopiert den Inhalt des aktuellen Verzeichnisses — standardmäßig: C:\Programme\Acronis\Bootable Components\WinPE— nach %BartPE folder%\plugins\Acronis.
7. Legen Sie die CD Ihrer Windows-Distribution ein, sofern Sie nicht bereits eine Kopie der Windows-Installationsdateien auf dem Laufwerk haben.
8. Starten Sie Bart's PE Builder.

9. Spezifizieren Sie den Pfad zu den Windows-Installationsdateien oder Ihrer Windows-Distributions-CDs.
10. Klicken Sie auf **Plugins** und überprüfen Sie, ob das Acronis-Plug-in als 'Aktiv' angezeigt wird. Sofern nicht, aktivieren Sie es.
11. Spezifizieren Sie den Ausgabeordner sowie den vollen Pfad für die zu erstellende ISO-Datei (einschließlich des Dateinamens) oder das zu erstellende Medium.
12. BartPE-Medium erstellen.
13. Brennen Sie die ISO-Datei auf CD oder DVD (sofern nicht schon geschehen) oder kopieren Sie die Daten auf ein Flash-Laufwerk wie einen USB-Stick (Flash-Laufwerk müssen zum Booten vom Anwender zuvor separat angepasst werden).

Nachdem die Maschine mit BartPE gebootet wurde und Sie die Netzwerkverbindung konfiguriert haben, wählen Sie zum Starten **Go –> System –> Storage –> Acronis Backup & Recovery 10**.

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. 275)).

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. 285).
- Manuell unter Verwendung der Utilities **mdadm** und **lvm** – siehe Volume-Struktur manuell erstellen (S. 286).

Volume-Struktur automatisch erstellen

Angenommen, Sie haben Ihre Volume-Struktur im Verzeichnis /etc/Acronis gespeichert 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**.

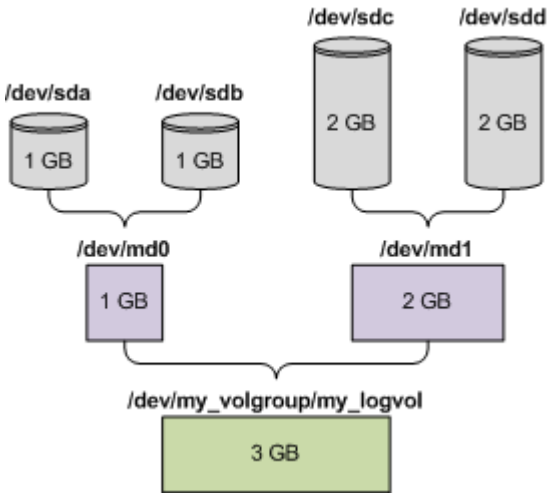
Anmerkung: *Diese Prozedur funktioniert nicht, wenn Sie zum Acronis Backup & Recovery 10 Bootable Agent remote verbunden sind, weil hier für diesen Fall die Eingabeaufforderung nicht verfügbar ist.*

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. 284)'. 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
```

6.10.6 Acronis PXE Server

Der Acronis PXE Server ermöglicht es, Maschinen mit bootfähigen Acronis-Komponenten über das Netzwerk zu starten.

Booten über das Netzwerk:

- Eliminiert die Notwendigkeit eines Technikers vor Ort, um das bootfähige Medium in das zu bootende System einzulegen
- Reduziert bei Gruppen-Operationen die zum Booten mehrerer Maschinen benötigte Zeit (im Vergleich zu physikalischen Bootmedien).

Bootfähige Komponenten werden vom Acronis Bootable Media Builder zum Acronis PXE Server hochgeladen. Um eine bootfähige Komponente hochzuladen, starten Sie den Bootable Media Builder (entweder über die Management Konsole durch **Extras –> Bootfähiges Medium erstellen** oder als eigene Komponente) und folgen Sie dann den Schritt-für-Schritt-Anweisungen, die detailliert im Abschnitt „Bootable Media Builder (S. 275)“ beschrieben sind.

Das Booten mehrerer Maschinen über den Acronis PXE Server macht insbesondere Sinn, wenn im Netzwerk ein Dynamic Host Control Protocol (DHCP)-Server vorhanden ist. Dann erhalten die Netzwerkadapter der gebooteten Maschinen automatisch eine IP-Adresse.

Acronis PXE Server-Installation

Den Acronis PXE Server installieren

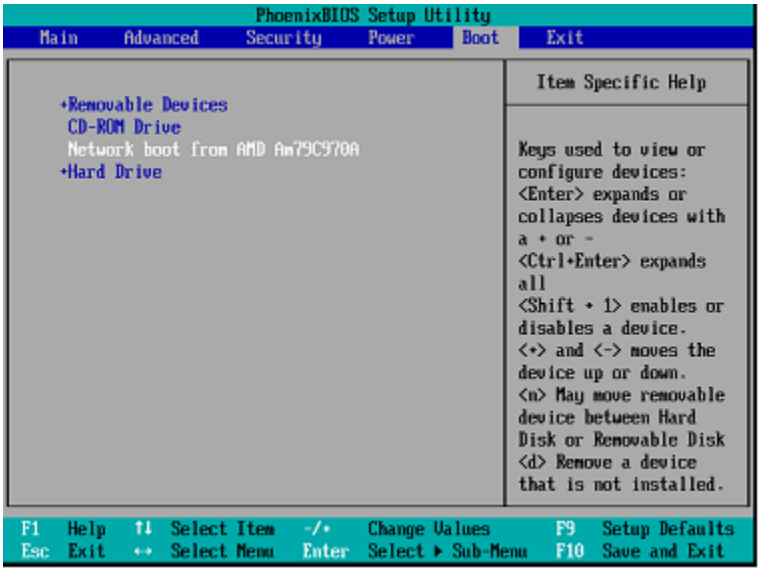
1. Führen Sie die Setup-Datei von Acronis Backup & Recovery 10 aus.
2. Wählen Sie den Acronis PXE Server von der Liste der **Komponenten für zentrale Verwaltung**.
3. Folgen Sie den Bildschirmanweisungen.

Acronis PXE Server läuft unmittelbar nach der Installation als Dienst. Später wird er automatisch nach jedem System-Neustart ausgeführt. Sie können den Acronis PXE Server so wie jeden anderen Windows-Dienst starten oder stoppen.

Eine Maschine für das Booten von PXE konfigurieren

Für fabrikneue Maschinen reicht es aus, dass ihr BIOS das Booten von Netzwerk unterstützt.

Auf einer Maschine, die ein Betriebssystem auf ihrer Festplatte hat, muss das BIOS so konfiguriert werden, dass der Netzwerkadapter entweder das erste Boot-Gerät ist – oder zumindest vor der Festplatte aufgelistet ist. Das Beispiel zeigt eine typische BIOS-Konfiguration. Wenn Sie kein bootfähiges Medium einlegen, wird die Maschine vom Netz booten.



In einigen BIOS-Versionen müssen Sie die geänderten BIOS-Einstellungen, nach Aktivierung des Netzwerkadapters, erst abspeichern, damit die Netzwerkkarte in der Liste der Boot-Geräte erscheint.

Sollte Ihre Hardware mehrere Netzwerkadapter haben, so stellen Sie sicher, dass das Netzwerkkabel auch in der vom BIOS unterstützten Karte steckt.

PXE und DHCP auf dem gleichen Server

Sollten ein Acronis PXE und DHCP-Server auf derselben Maschine laufen, so fügen Sie dem DHCP-Server die Option 60 hinzu: „Client Identifier“ entspricht dem String-Wert „PXE Client“. Das kann folgendermaßen erfolgen:

```
C:\WINDOWS\system32>netsh
netsh>dhcp
netsh>dhcp>server \\<server_machine_name> or <IP address>
netsh dhcp>add optiondef 60 PXEClient STRING 0 comment=”Option added for PXE support”
netsh dhcp>set optionvalue 60 STRING PXEClient
```

Über Subnetze hinweg arbeiten

Damit der Acronis PXE Server auch in anderen Subnetzen arbeiten kann (über einen Switch hinweg), muss der Switch PXE-Netzwerkverkehr weiterreichen können. Die IP-Adressen des PXE Servers sind auf Pro-Netzwerkadapter-Basis konfiguriert, unter Verwendung von IP-Helfer-Funktionalität wie bei DHCP-Server-Adressen. Für mehr Informationen schlagen Sie hier nach: http://support.microsoft.com/kb/257579/de.

6.11 Laufwerksverwaltung

Acronis Disk Director Lite ist ein Tool zur Vorbereitung der Festplatten-/Partitionskonfiguration einer Maschine für die Wiederherstellung von Laufwerksabbildern, die mit Acronis Backup & Recovery 10-Software gespeichert wurden.

Nachdem ein Laufwerk gesichert und sein Image an einem sicheren Speicherplatz hinterlegt wurde, kann es vorkommen, dass sich die Festplattenkonfiguration der Maschine durch Austausch einer Platte oder durch Hardware-Verlust ändert. In diesem Fall hat der Benutzer durch die Hilfe des Acronis Disk Director Lite die Möglichkeit, die notwendige Festplattenkonfiguration wieder so zu erstellen, dass das Laufwerksabbild exakt „wie es war“ wiederhergestellt werden kann (oder mit jeder Abweichung der Platten-/Laufwerksstruktur, die der Benutzer notwendig hält).

Alle Aktionen auf Laufwerke und Volumes bergen ein gewisses Risiko für Datenverlust. Aktionen auf System- oder Daten-Laufwerken müssen sehr sorgfältig ausgeführt werden, um mögliche Probleme mit dem Boot-Ablauf oder Festplattendatenspeicher zu vermeiden.

Aktionen mit Festplatten und Laufwerken benötigen eine gewisse Zeit und Stromverlust, unbeabsichtigtes Ausschalten der Maschine oder versehentliches Drücken des Reset-Schalters während der Prozedur kann zur Beschädigung des Laufwerkes und Datenverlust führen.

Alle Aktionen mit den Volumes dynamischer Laufwerke in Windows XP und Windows 2000 setzen voraus, dass der Acronis Managed Machine Service unter einem Benutzerkonto mit Administratorrechten ausgeführt wird.

Treffen Sie alle notwendigen Vorsichtsmaßnahmen (S. 291), um einen möglichen Datenverlust zu vermeiden.

6.11.1 Grundlegende Vorsichtsmaßnahmen

Treffen Sie alle notwendigen Vorsichtsmaßnahmen, um mögliche Schäden an der Laufwerks- bzw. Volume-Struktur oder Datenverlust abzuwenden und beachten Sie folgende grundsätzliche Regeln:

1. Erstellen Sie von Laufwerken, auf denen Volumes erstellt oder verwaltet werden, ein Backup. Indem Sie wichtige Daten auf ein anderes Laufwerk, eine Netzwerkfreigabe oder Wechselmedien sichern, können Sie – wohl wissend, dass Ihre Daten gut geschützt sind – beruhigt mit Ihren Laufwerken bzw. Volumes arbeiten.
2. Überprüfen Sie Ihre Festplatte, um sicherzustellen, dass sie voll funktionstüchtig ist und keine defekten Sektoren oder Dateisystemfehler enthält.
3. Führen Sie keine Laufwerks- bzw. Volume-Aktionen aus, während andere Programme mit Low-Level-Zugriff auf Laufwerke ausgeführt werden. Beenden Sie diese Programme bevor Sie Acronis Disk Director Lite ausführen.

Durch diese einfachen Vorsichtsmaßnahmen schützen Sie sich vor versehentlichem Datenverlust.

6.11.2 Acronis Disk Director Lite ausführen

Sie können Acronis Disk Director Lite unter Windows ausführen oder von einem bootfähigen Medium starten.

Acronis Disk Director Lite unter Windows ausführen

Wenn Sie die Acronis Backup & Recovery 10 Management Console starten und mit einer verwalteten Maschine verbinden, steht die Ansicht **Laufwerksverwaltung** im Zweig **Navigation** der Konsole zur Verfügung, von wo aus Sie den Acronis Disk Director Lite starten können.

Acronis Disk Director Lite von einem bootfähigen Medium ausführen

Sie können Acronis Disk Director Lite auf einer fabrikneuen, einer Nicht-Windows-Maschine oder einer, die nicht booten kann, ausführen. Um dies zu tun, booten Sie die Maschine von einem bootfähigen Medium (S. 422), das mit dem Acronis Bootable Media Builder erstellt wurde; starten die Management Konsole und klicken dann auf **Laufwerksverwaltung**.

6.11.3 Auswählen des Betriebssystems für die Datenträgerverwaltung

Auf einer Maschine mit zwei oder mehr Betriebssystemen hängt die Darstellung der Datenträger und Volumes davon ab, welches Betriebssystem gerade ausgeführt wird.

Ein Volume kann in verschiedenen Windows-Betriebssystemen auch unterschiedliche Buchstaben haben. Es kann z.B. sein, dass Volume „E:“ als „D:“ oder „L:“ angezeigt wird, wenn Sie ein anderes Windows-Betriebssystem booten, das auf derselben Maschine installiert ist. (Es ist aber auch möglich, dass dieses Volume unter allen auf der Maschine installierten Windows-Betriebssystemen als „E:“ angezeigt wird.)

Ein unter einem Windows-Betriebssystem erstellter dynamischer Datenträger wird in einem anderen Betriebssystem als **Fremder Datenträger** angesehen oder möglicherweise von diesem Betriebssystem gar nicht unterstützt.

Wenn Sie eine Aktion zur Datenträgerverwaltung mit einer solchen Maschine ausführen müssen, dann müssen Sie angeben, für welches Betriebssystem das Laufwerkslayout angezeigt und die Datenträgerverwaltungsaktion ausgeführt wird.

Der Name des aktuell ausgewählten Betriebssystems wird in der Symbolleiste der Konsole hinter **Das aktuelle Laufwerkslayout ist für:** angezeigt. Um ein anderes Betriebssystem auszuwählen, klicken Sie im Fenster **Auswahl des Betriebssystems** auf den Namen des Betriebssystems. Dieses Fenster wird unter den bootfähigen Medien angezeigt, nachdem Sie auf **Laufwerksverwaltung** geklickt haben. Das Laufwerkslayout wird so angezeigt, wie es dem ausgewählten Betriebssystem entspricht.

6.11.4 Ansicht „Laufwerksverwaltung“

Acronis Disk Director Lite wird über die **Laufwerksverwaltung**-Ansicht der Konsole kontrolliert.

Der oberste Bereich der Ansicht enthält eine Laufwerks- und Volume-Tabelle mit der Möglichkeit zur Sortierung, zur Anpassung der Spalten und verfügt über eine Symbolleiste. Die Tabelle präsentiert alle verfügbaren Laufwerke, zugewiesene Laufwerksbuchstaben und -bezeichnungen, Laufwerkstyp sowie -kapazität, freien und benutzten Speicherplatz, Dateisystem und Status eines jeden Laufwerks. Die Symbolleiste beinhaltet Icons zum Starten der Aktionen **Rückgängig**, **Wiederherstellen**und **Ausführen**, die sich auf ausstehende Aktionen (S. 307) beziehen.

Über den grafischen Bereich im unteren Teil der Ansicht werden alle Laufwerke und ihre Volumes noch einmal als Rechtecke visualisiert, inklusive ihrer Basisdaten (Bezeichnung, Laufwerksbuchstabe, Größe, Status, Typ und Dateisystem).

Beide Teile der Ansicht bilden zudem den verfügbaren nicht zugeordneten Speicherplatz ab, der zur Erstellung von Laufwerken verwendet werden kann.

Aktionen starten

Jede Aktion kann folgendermaßen gestartet werden:

- vom Kontextmenü der Laufwerke oder Festplatten (in der Tabelle und in der grafischen Ansicht)
- aus dem Menü **Laufwerksverwaltung** der Konsole
- aus dem Bereich **Aktionen** auf der Seitenleiste **Aktionen und Werkzeuge**

*Beachten Sie, dass die Liste verfügbarer Aktionen im Kontextmenü, im Menü **Auswahl** und im Seitenleistenbereich **Aktionen** vom ausgewählten Volume- oder Laufwerkstyp abhängt. Dasselbe trifft auch für nicht zugeordneten Speicher zu.*

Ergebnisanzeige von Aktionen

Die Ergebnisse aller geplanten Festplatten- oder Laufwerksaktionen werden sofort in der Ansicht **Laufwerksverwaltung** der Konsole angezeigt. Wenn Sie z.B. ein Laufwerk erstellen, wird dies sofort angezeigt – und zwar sowohl in der Tabelle als auch in der unteren, grafischen Ansicht. Auch alle anderen Laufwerksänderungen, inklusive geänderter Laufwerksbuchstaben oder -bezeichnungen, werden sofort in der Ansicht dargestellt.

6.11.5 Festplattenaktionen

Acronis Disk Director Lite ermöglicht folgende auf Festplatten anwendbare Aktionen:

- Disk Initialisierung (S. 293) – richtet neue, dem System hinzuzufügende Hardware ein
- Einfaches Festplatten-Klonen (S. 294) – überträgt die kompletten Daten einer Quell- auf eine Zielplatte (Basisdatenträger vom MBR-Typ)
- Festplatten konvertieren: MBR zu GPT (S. 296) – konvertiert eine MBR-Partitionstabelle zu GPT
- Festplatten konvertieren: GPT zu MBR (S. 297) – konvertiert eine GPT-Partitionstabelle zu MBR
- Festplatten konvertieren: Basis zu Dynamisch (S. 297) – konvertiert einen Basis- zu einem dynamischen Datenträger
- Festplatten konvertieren: Dynamisch zu Basis (S. 298) – konvertiert einen dynamischen zu einem Basisdatenträger

Die Vollversion des Acronis Disk Director verfügt über weitere Werkzeuge zum Arbeiten mit Festplatten.

Acronis Disk Director Lite benötigt einen exklusiven Zugriff auf das Ziellaufwerk. Das bedeutet, dass dann auch kein anderes Disk ManagementLaufwerksverwaltung-Werkzeug (etwa die Windows Datenträgerverwaltung) auf sie zugreifen kann. Sollten Sie eine Meldung erhalten, dass das Laufwerk nicht blockiert werden kann, so schließen Sie das die Platte gerade benutzende Laufwerksverwaltung-Werkzeug und starten erneut. Schließen Sie alle aktiven Festplatten-Werkzeuge, sofern Sie nicht bestimmen können, welche Anwendung das Laufwerk gerade blockiert.

Festplatten-Initialisierung

Wenn Sie dem System eine neue Festplatte hinzufügen, so erkennt Acronis Disk Director Lite die veränderte Konfiguration und integriert die neue Platte in die Liste aktueller Laufwerke und Volumes. Sollte die Festplatte noch nicht initialisiert sein oder ein unbekanntes Dateisystem verwenden, so können Sie noch keine Programme auf ihr installieren und keine Daten auf ihr speichern.

In diesem Fall wird Acronis Disk Director Lite erkennen, dass die Festplatte verwendet werden kann, und die Notwendigkeit, diese zu initialisieren. Das Fenster **Laufwerksverwaltung** stellt die neu erkannte Hardware als grauen Balken mit grauem Symbol dar, um so die Nichtverwendbarkeit zu

visualisieren.

So initialisieren Sie ein Laufwerk:

1. Wählen das zu initialisierende Laufwerk.
2. Klicken Sie mit der rechten Maustaste auf das gewählte Volume und wählen Sie im Kontextmenü **Initialisieren**. Das nachfolgende Fenster **Disk-Initialisierung** versorgt Sie mit grundlegenden Hardware-Details wie Laufwerksnummer oder Kapazität und bietet an, Sie bei der Wahl Ihrer nun möglichen Aktionen zu unterstützen.
3. Sie können in diesem Fenster das Partitionsschema der Disk (MBR oder GPT) und den Disk-Typ (Basis oder Dynamisch) einstellen. Die neue Laufwerksstatus wird sofort grafisch in der **Laufwerksverwaltung**-Ansicht der Konsole angezeigt.
4. Indem Sie auf **OK** klicken, fügen Sie die Disk-Initialisierung der Liste ausstehender Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 307). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Nach der Initialisierung bleibt der ganze Festplattenplatz unzugeorndet und kann daher für die Programminstallation oder zur Dateiaufbewahrung nicht benutzt zu werden. Um den Speicherplatz verfügbar zu machen, fahren Sie nun normalerweise mit der Aktion **Volume erstellen** fort.

Wenn Sie weitere Einstellungen des Laufwerks ändern wollen, so können Sie dafür auch später noch die Werkzeuge von Acronis Disk Director Lite verwenden.

Einfaches Festplatten-Klonen

Manchmal ist es notwendig, alle Daten einer Festplatte auf eine andere zu übertragen. Typische Gründe sind eine Vergrößerung des Systemlaufwerks, die Einrichtung eines neuen Systems oder die Räumung des Laufwerks aufgrund eines Hardware-Fehlers. Wie auch immer: die Gründe für die Aktion **Basisdatenträger klonen** können als Notwendigkeit zum exakten Transfer aller Daten einer Quell- auf eine Zielplatte zusammengefasst werden.

Acronis Disk Director Lite ermöglicht Ihnen die Durchführung der Aktion nur mit Basisdatenträgern mit MBR-Partitionsschema.

So planen Sie die Aktion **Basisdatenträger klonen**:

1. Wählen Sie die zu klonende Festplatte.
2. Bestimmen Sie die Zielfestplatte für die Klonaktion.
3. Wählen Sie die Methoden zum Klonen und spezifizieren Sie zusätzliche Optionen.

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

*Es wird empfohlen, einen aktivierten Acronis Startup Recovery Manager (S. 418) (ASRM) zu deaktivieren, bevor Sie ein Systemlaufwerk klonen. Andernfalls könnte das geklonte Betriebssystem möglicherweise nicht starten. Nach dem Klonen können Sie den ASRM aktivieren. Wenn die Deaktivierung nicht möglich ist, dann wählen Sie die Methode **Wie vorliegend**, um die Festplatte zu klonen.*

Quell- und Zielfestplatten bestimmen

Das Programm zeigt eine Liste aller partitionierten Laufwerke und fordert den Anwender dann auf, die Quelle zu wählen, von der die Daten zu einer anderen Platte übertragen werden.

Als Nächstes folgt die Wahl der Zielfestplatte für die Klonaktion. Das Programm ermöglicht die Wahl nur solcher Laufwerke, deren Größe ausreichend ist, um alle Daten des Quelllaufwerks verlustfrei aufzunehmen.

Sollten sich auf der gewählten Zielfestplatte Daten befinden, wird eine Warnung angezeigt: "**Das gewählte Ziellaufwerk ist nicht leer. Die Daten auf dem Laufwerk werden überschrieben.**", was bedeutet, dass alle derzeit auf dem gewählten Laufwerk verfügbaren Daten unwiederbringlich verloren gehen.

Klon-Methoden und erweiterte Optionen

Die Aktion **Basis-Laufwerk klonen** bedeutet normalerweise, dass alle Informationen des Quelllaufwerks "**Wie vorliegend**" auf das Ziellaufwerk übertragen werden. Sollte also das Zielllaufwerk gleich groß oder größer sein, so können alle Informationen exakt wie auf der Quelle gespeichert übertragen werden.

Durch die große Bandbreite verfügbarer Hardware ist es jedoch durchaus normal, dass das Ziellaufwerk eine andere Größe als die Quelle hat. Sollte das Ziellaufwerk größer sein, so kann es ratsam sein, unter Verwendung der Option **Volumes proportional anpassen** die Quelllaufwerke so anzupassen, dass auf dem Ziel nicht zugeordneter Speicherplatz vermieden wird. Die Option **Basisdatenträger klonen** „wie vorliegend" bleibt bestehen, nur wird die Standardmethode zum Klonen inkl. proportionaler Vergrößerung aller **Quell**--Laufwerke so durchgeführt, dass auf der **Ziel**-Festplatte kein nicht zugeordneter Speicherplatz verbleibt.

Ist das Ziel kleiner, so steht die Option **Wie vorliegend** nicht mehr zur Verfügung wird die proportionale Größenanpassung **Quell**-Laufwerke zwingend notwendig. Das Programm analysiert das **Ziellaufwerk** daraufhin, ob seine Größe ausreicht, alle Daten des **Quelllaufwerks** verlustfrei aufnehmen zu können. Nur wenn ein Transfer mit proportionaler Größenanpassung der **Quell**-Laufwerke ohne Datenverlust möglich ist, kann der Anwender mit der Aktion fortfahren. Sollte wegen einer Größenbeschränkung eine sichere Übertragung der **Quell**-Daten auf das **Ziel**-Laufwerk auch mit proportionaler Größenanpassung nicht möglich sein, dann die Aktion **Basis-Laufwerk klonen** nicht mehr fortgesetzt werden.

Wenn Sie vorhaben, ein Laufwerk zu klonen, das ein **System-Volume** enthält, sollten Sie die **Erweiterten Optionen** beachten.

Indem Sie auf **Abschluss** klicken, fügen Sie das Laufwerk-Klonen der Liste ausstehender Aktionen hinzu.

(Damit die hinzugefügte Aktion durchgeführt werden, müssen Sie diese ausführen (S. 307) lassen. Wenn Sie das Programm ohne Ausführung der offenen Aktionen beenden, werden diese alle verworfen.)

Erweiterte Optionen verwenden

Wenn Sie ein Laufwerk klonen, das ein **System-Volume** enthält, müssen Sie auch die Bootfähigkeit des Betriebssystems für das Ziellaufwerk bewahren. Das bedeutet, dass das Betriebssystem System-Laufwerks-Informationen (z.B. Laufwerksbuchstabe) erhalten muss, die zur NT-Festplatten-Signatur passen (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 diesem Laufwerk kann daher auch nicht mehr booten.

Ihnen stehen zwei Alternativen zur Verfügung, um die Bootfähigkeit auf dem Ziellaufwerk zu

erhalten:

1. Kopieren der NT-Signatur – um die Zielfestplatte mit der NT-Signatur zu versehen, die zu den ebenfalls auf die Platte kopierten Registry-Schlüsseln passt
2. NT-Signatur belassen – um die alte Disk-Signatur des Ziellaufwerks zu bewahren und das Betriebssystem an diese anzupassen

Falls Sie die NT-Signatur kopieren müssen:

1. Aktivieren Sie das Kontrollkästchen **NT-Signatur kopieren**. Sie erhalten eine Warnung: "Wenn sich auf der Festplatte ein Betriebssystem befindet, so entfernen Sie entweder die Quell- oder Zielfestplatte aus dem Computer, bevor Sie diesen erneut starten. Anderenfalls wird das Betriebssystem von der ersten der beiden Festplatten starten und das Betriebssystem der zweiten Platte seine Bootfähigkeit verlieren." Das Kontrollkästchen **Computer nach dem Klonen ausschalten** hat den Fokus und ist automatisch deaktiviert.
2. Klicken Sie auf **Abschluss**, um die Aktion zur Liste der ausstehenden Aktionen hinzuzufügen.
3. Klicken Sie auf **Ausführen** in der Symbolleiste und dann **Fertig stellen** im Fenster **Ausstehende Aktionen**.
4. Warten Sie dann, bis die Aktion beendet ist.
5. Und danach, bis der Computer ausgeschaltet wird.
6. Entfernen Sie entweder die Quell- oder Zielfestplatte aus dem Computer.
7. Schalten Sie den Computer wieder ein.

Falls Sie die NT-Signatur bewahren müssen:

1. Entfernen Sie sofern nötig das Häkchen im Kontrollkästchen **NT-Signatur kopieren**.
2. Entfernen Sie sofern nötig das Häkchen im Kontrollkästchen **Computer nach dem Klonen ausschalten**.
3. Klicken Sie auf **Abschluss**, um die Aktion zur Liste der ausstehenden Aktionen hinzuzufügen.
4. Klicken Sie auf **Ausführen** in der Symbolleiste und dann **Fertig stellen** im Fenster **Ausstehende Aktionen**.
5. Warten Sie dann, bis die Aktion beendet ist.

Festplatten konvertieren: MBR zu GPT

In folgenden Fällen kann es angebracht sein, einen MBR- in einen GPT-Basisdatenträger zu konvertieren:

- Wenn Sie mehr als 4 primäre Laufwerke auf einem Laufwerk benötigen.
- Wenn Sie die Zuverlässigkeit der Festplatte gegen möglichen Datenverlust erhöhen müssen.

Wenn Sie einen MBR- in einen GPT-Basisdatenträger konvertieren müssen:

1. Bestimmen Sie den MBR-Basisdatenträger, der zu GPT konvertiert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie dann **Zu GPT konvertieren** im Kontextmenü.

   Sie erhalten eine Warnmeldung, dass Sie im Begriff sind, von MBR nach GPT zu konvertieren.
3. Indem Sie auf **OK** klicken, fügen Sie MBR-zu-GPT-Konvertierung der Liste der ausstehenden Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 307). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Beachten Sie: Ein GPT-partitioniertes Laufwerk reserviert am Ende des partitionierten Bereiches Speicherplatz für einen benötigten Backupbereich, in dem Kopien des GPT-Headers und der Partitionstabelle gespeichert werden. Sollte die Festplatte so voll sein, dass keine automatische Verringerung der Laufwerksgröße möglich ist,

so wird die MBR-zu-GPT-Konvertierung fehlschlagen.

Die Aktion kann außerdem nicht rückgängig gemacht werden. Wenn Sie eine MBR-Festplatte mit einer primären Partition haben, diese erst zu GPT und dann wieder zurück zu MBR konvertieren, so wird die Partition zu einem logischen Laufwerk, welches dann nicht mehr als Systempartition verwendet werden kann.

Wenn Sie ein Betriebssystem installieren wollen, das GPT-Festplatten nicht unterstützt, so ist eine Rückkonvertierung der Festplatte zu MBR über dasselbe Menü möglich (der Befehl für diese Aktion lautet **Zu MBR konvertieren**).

Konvertierung dynamischer Datenträger: MBR zu GPT

Eine direkte MBR-zu-GPT-Konvertierung von dynamischen Datenträgern wird von Acronis Disk Director Lite nicht unterstützt. Sie können jedoch zum selben Ziel kommen, wenn Sie die folgenden Konvertierungen durchführen:

1. MBR Festplatten-Konvertierung: Dynamisch zu Basis (S. 298) unter Verwendung der Aktion **Zu Basis konvertieren**.
2. Konvertierung von Basisdatenträgern: MBR zu GPT durch Verwendung der Aktion **Zu GPT konvertieren**.
3. GPT Festplatten-Konvertierung: Basis zu Dynamisch (S. 297) durch Verwendung der Aktion **Zu Dynamisch konvertieren**.

Festplatten konvertieren: GPT zu MBR

Wenn Sie ein Betriebssystem installieren wollen, das GPT-Festplatten nicht unterstützt, so ist eine Konvertierung der GPT-Platte zu MBR möglich (der Befehl für diese Aktion lautet **Zu MBR konvertieren**).

Wenn Sie eine GPT-Festplatte zu MBR konvertieren müssen:

1. Bestimmen Sie die GPT-Festplatte, die zu MBR konvertiert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie dann **Zu MBR konvertieren** im Kontextmenü.

   Sie erhalten eine Warnmeldung, dass Sie im Begriff sind, von GPT nach MBR zu konvertieren.

   Ihnen werden die Auswirkungen auf das System erläutert, wenn das gewählte Lafuwerk von GPT zu MBR konvertiert wird. Z.B., dass die Konvertierung bewirken kann, dass das System nicht mehr auf das Laufwerk zugreifen und somit auch das Betriebssystem nicht mehr starten kann – oder dass auf manche Volumes des gewählten GPT-Laufwerks im MBR-Modus nicht mehr zugegriffen werden kann (weil diese jenseits der 2 TByte-Grenze liegen).

   Beachten Sie, dass ein zu einer GPT-Festplatte gehörendes Laufwerk nach der irreversiblen Konvertierung zu einer logischen Partition wird.
3. Indem Sie auf **OK** klicken, fügen Sie die GPT-zu-MBR-Konvertierung der Liste der ausstehenden Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 307). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Festplatten konvertieren: Basis zu Dynamisch

In folgenden Fällen ist eine Konvertierung von Basis- zu dynamischen Datenträgern angebracht:

- Wenn Sie die Festplatte als Teil einer dynamischen Laufwerksgruppe verwenden wollen.
- Wenn Sie eine erhöhte Zuverlässigkeit der Datenspeicherung auf der Festplatte erreichen wollen.

Wenn Sie einen Basis- zu einem dynamischen Datenträger konvertieren müssen:

1. Wählen Sie den zu konvertierenden Basisdatenträger.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Zu Dynamisch konvertieren**. Ihnen wird eine abschließende Warnung angezeigt, dass die Konvertierung von Basis zu Dynamisch ansteht.
3. Sobald Sie in dieser Warnmeldung auf **OK** klicken, wird die Konvertierung sofort durchgeführt und falls notwendig der Computer neu gestartet.

Beachten Sie: Ein dynamischer Datenträger belegt das letzte Megabyte des physikalischen Laufwerks mit einer Datenbank, die eine so genannte Four-Level-Beschreibung (Volume-Component-Partition-Disk) für jedes dynamische Laufwerk enthält. Sollte sich während der Konvertierung zu Dynamisch herausstellen, dass der Basisdatenträger voll ist und daher die Laufwerksgröße nicht automatisch reduziert werden kann, so schlägt die Konvertierungsaktion fehl.

Sollten Sie irgendwann den dynamischen wieder zu einem Basisdatenträger zurückwandeln wollen, etwa um ein Betriebssystem zu verwenden, welches dynamische Datenträger nicht unterstützt, so können Sie dafür dasselbe Menü verwenden (wobei der Aktionsbefehl **Zu Basis konvertieren** lautet).

Konvertierung eines System-Laufwerkes

Acronis Disk Director Lite benötigt nach einer Basis-zu-Dynamisch-Konvertierung keinen Neustart des Betriebssystems, sofern:

1. Auf der Festplatte nur ein Betriebssystem vom Typ Windows Server 2008/Vista vorhanden ist.
2. Auf dem Computer dieses Betriebssystem läuft.

Die Konvertierung von 'Basis' zu 'Dynamisch' eines Laufwerks, das eine Systempartition enthält, benötigt einiges an Zeit – wobei jeder Stromausfall, jedes unbeabsichtigte Ausschalten oder versehentliche Drücken des Reset-Schalters während der Aktion den Verlust der Bootfähigkeit bewirken kann.

Anders als der Windows Disk Manager bewahrt das Programm die Bootfähigkeit eines **Offline-Betriebssystems** nach der Aktion.

Laufwerk konvertieren: Dynamisch zu Basis

Eine Rückkonvertierung von dynamischen zu Basis-Laufwerken ist z.B. dann angebracht, wenn Sie ein Betriebssystem verwenden wollen, dass dynamische Laufwerke nicht unterstützt.

Wenn Sie ein Laufwerk von 'Dynamisch' zu 'Basis' konvertieren müssen:

1. Wählen Sie das zu konvertierende dynamische Laufwerk.
2. Klicken Sie mit der rechten Maustaste auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Zu 'Basis' konvertieren**. Ihnen wird eine abschließende Warnung angezeigt, dass die Konvertierung von Dynamisch zu Basis ansteht.

   Ihnen werden die Auswirkungen auf das System erläutert, wenn das gewählte Laufwerk vom Typ 'Dynamisch' zu 'Basis' konvertiert wird. Z. B. dass die Umwandlung bewirken kann, dass das System nicht mehr auf das Laufwerk zugreifen und somit auch ein Betriebssystem nicht mehr starten kann – oder dass Sie für den Fall, dass das zu konvertierende Laufwerke Volumes von einem Typ enthält, die nur von dynamischen Laufwerken unterstützt werden (alle Laufwerkstypen außer Volumes vom Typ 'Einfach') über den möglichen Verlust von Daten infolge der Konvertierung gewarnt werden.

   Beachten Sie, dass die Aktion nicht auf dynamische Laufwerke angewendet werden kann, die übergreifende, Stripeset- oder RAID-5-Volumes enthalten.

3. Sobald Sie in dieser Warnmeldung auf **OK** klicken, wird die Konvertierung sofort durchgeführt.

Nach der Umwandlung werden 8 MB des Laufwerksspeichers für zukünftige Konvertierungen von Basis zu Dynamisch reserviert.

Der resultierende nicht zugeordnete Speicherplatz und die anvisierte maximale Volume-Größe können von Fall zu Fall variieren (z.B. weil die Größe einer Spiegelung die Größe einer anderen Spiegelung bedingt oder weil die letzten 8 MB Speicherplatz für zukünftige Konvertierungen von 'Basis' zu 'Dynamisch' reserviert werden).

Systemlaufwerk konvertieren

Acronis Disk Director Lite benötigt nach einer Dynamisch-zu-Basis-Konvertierung keinen Neustart des Betriebssystems, sofern:

1. Auf dem Laufwerk ist nur ein Betriebssystem vom Typ Windows Server 2008/Vista installiert.
2. Die Maschine dieses Betriebssystem ausführt.

Die Dynamisch-zu-Basis-Konvertierung Festplatte, die eine Systempartition enthält, benötigt einiges an Zeit – wobei jeder Stromausfall, jedes unbeabsichtigte Ausschalten oder versehentliche Drücken des Reset-Schalters während der Aktion den Verlust der Bootfähigkeit bewirken kann.

Anders als der Windows Disk Manager gewährleistet das Programm:

- sichere Konvertierung eines dynamischen zu einem Basis-Laufwerk, sofern dieses Laufwerk Volumes **mit Daten** für einfache und gespiegelte Volumes enthält.
- in Multiboot-Systemen die Bootfähigkeit eines Systems, das während der Aktion **offline** war.

Laufwerkstatus ändern

Die Funktion 'Laufwerkstatus ändern' gilt für die Betriebssysteme Windows Vista SP1+, Windows Server 2008 und Windows 7 und bezieht sich auf die aktuelle Laufwerksstruktur (S. 292).

Der Laufwerksstatus erscheint immer in der grafischen Anzeige des Laufwerks neben dem Laufwerksnamen; es gibt folgende Möglichkeiten:

- **Online**

  Der Status 'online' bedeutet, dass auf das Laufwerk im Modus Lesen-Schreiben zugegriffen werden kann. Dies ist der normale Laufwerkstatus. Wenn das Laufwerk nur im Lesemodus verfügbar sein soll, wählen Sie das Laufwerk aus und ändern Sie den Status zu 'offline'; wählen Sie dazu **Disk-Status zu offline ändern** im Menü **Aktionen**.

- **Offline**

  Der Status 'offline' bedeutet, dass auf das Laufwerk nur im Lesemodus zugegriffen werden kann. Um den Modus des gewählten Laufwerks von offline zurück zu online zu ändern, wählen Sie **Disk-Status auf online ändern** im Menü **Aktionen**.
  Wenn ein Laufwerk den Status offline hat und der Laufwerkname als **Fehlend** angegeben ist, kann das Betriebssystem dieses Laufwerk nicht finden bzw. nicht identifizieren. Es ist möglicherweise defekt, getrennt oder abgeschaltet. Informationen darüber, wie Sie ein als fehlend und offline gekennzeichnetes Laufwerk wieder in den Status online bringen, finden Sie in diesem Artikel in der Microsoft Knowledge Base: http://technet.microsoft.com/de-de/library/cc732026%28WS.10%29.aspx.

Fremdlaufwerke importieren

Auf einer Maschine mit zwei oder mehr Betriebssystemen hängt die Laufwerks- bzw. Volume-Darstellung davon ab, welches Betriebssystem gerade läuft.

Normalerweise sind alle dynamischen Laufwerke, die innerhalb der gleichen Maschine und desselben

Betriebssystems erstellt wurden, Mitglieder derselben Laufwerksgruppe. Wenn eine Laufwerksgruppe zu einer anderen Maschine verschoben – oder einem anderem Betriebssystem auf derselben Maschine hinzugefügt wird – wird sie als **fremd** betrachtet. Fremde Laufwerksgruppen können solange nicht verwendet werden, bis sie in die existierende Laufwerksgruppe hinzugefügt werden. Wenn auf der Maschine keine Laufwerksgruppe existiert, wird die 'fremde' Gruppe so, wie sie ist, importiert (behält ihren ursprünglichen Namen).

Um auf Fremdlaufwerke zugreifen zu können, müssen Sie diese Laufwerke zur Konfiguration Ihrer Maschine unter Verwendung der Aktion **Fremdlaufwerke importieren** hinzufügen.

Alle dynamischen Laufwerke der fremden Laufwerksgruppe werden zur gleichen Zeit importiert, Sie können also kein einzelnes dynamisches Laufwerk importieren.

So importieren Sie Fremdlaufwerke

1. Klicken Sie mit der rechten Maustaste auf eines der Fremdlaufwerke und wählen Sie dann **Fremdlaufwerke importieren**.

   Es erscheint ein Fenster, in dem alle zur Maschine hinzugefügten, dynamischen Fremdlaufwerke aufgelistet sind und Informationen über die zu importierenden Volumes angezeigt werden. Über die Statusinformationen der Volumes können Sie feststellen, ob Sie alle benötigten Laufwerke der Laufwerksgruppe importieren. Wenn Sie alle benötigten Laufwerke importieren, werden deren Volumes alle mit dem Status **Fehlerfrei** angezeigt. Ein von **Fehlerfrei** abweichender Status ist ein Zeichen dafür, dass nicht alle Laufwerke importiert wurden.

   Weitere Informationen über die Statusinformationen von Volumes finden Sie in folgendem (englischen) Microsoft-Artikel: http://technet.microsoft.com/en-us/library/cc771775.aspx
2. Klicken Sie auf **OK**, um die Importaktion der Fremdlaufwerke zur Liste der ausstehenden Aktionen hinzuzufügen.

Die Ergebnisse ausstehender Aktionen werden unmittelbar so angezeigt, als wenn die Aktionen bereits ausgeführt wurden.

Damit die ausstehenden Aktion durchgeführt werden, müssen Sie diese ausführen lassen. Wenn Sie das Programm ohne Ausführung der offenen Aktionen beenden, werden diese alle verworfen.

6.11.6 Aktionen für Volumes

Acronis Disk Director Lite ermöglicht folgende auf Partitionen anwendbare Aktionen:

- Partition erstellen (S. 301) – erstellt neue Partitionen mit Hilfe des Assistenten zur Partitionserstellung
- Partition löschen (S. 305) – löscht eine gewählte Partition
- Aktiv setzen (S. 305) – kennzeichnet eine gewählte Partition als „Aktiv“, so dass ein hier installiertes Betriebssystem gebootet werden kann.
- Laufwerksbuchstaben ändern (S. 306) – wechselt den Laufwerksbuchstaben der gewählten Partition
- Bezeichnung ändern (S. 306) – ändert die Datenträgerbezeichnung der gewählten Partition
- Volume formatieren (S. 307) – formatiert ein Volume mit einem benötigten Dateisystem

Die Vollversion des Acronis Disk Director verfügt über weitere Werkzeuge zum Arbeiten mit Partitionen.

Acronis Disk Director Lite benötigt einen exklusiven Zugriff auf die Zielpartition. Das bedeutet, dass dann auch kein anderes Laufwerksverwaltung-Werkzeug (etwa die Windows Datenträgerverwaltung) auf sie zugreifen kann. Sollten Sie eine Meldung erhalten, dass die Partition nicht blockiert werden kann, so schließen Sie das die

Partition gerade benutzende Laufwerksverwaltung-Werkzeug und starten erneut. Schließen Sie alle aktiven Festplatten-Werkzeuge, sofern Sie nicht bestimmen können, welche Anwendung die Partition gerade blockiert.

Eine Partition erstellen

Beispiele, wann eine neue Partition benötigt wird:

- Wiederherstellung eines früher gesicherten Backups mit exakt derselben Konfiguration;
- separate Speicherung von Sammlungen ähnlicher Dateien – z.B. Sammlungen von MP3- oder Videodateien auf einer separaten Partition;
- Sicherung der Backups (Images) anderer Partitionen/Festplatten auf einem besonderen Laufwerk;
- Installation eines neuen Betriebssystems (oder einer Auslagerungsdatei) auf einer neuen Partition;
- Hinzufügen neuer Hardware zu einem Computer.

Das Werkzeug zum Erstellen neuer Partitionen in Acronis Disk Director Lite ist der **Assistent zur Partitionserstellung**.

Verschiedene Arten dynamischer Volumes

Einfaches Volume (Simple)

Ein Laufwerk, das vom freien Speicherplatz eines einzelnen physikalischen Laufwerks erstellt wurde. Es kann aus einer oder auch mehreren Regionen auf der Festplatte bestehen, die durch den „Logical Disk Manager“ (LDM) von Windows virtuell vereint werden. Es stellt keine zusätzlichen Vorteile bereit, weder bei der Geschwindigkeit noch bei der Größe.

Übergreifendes Volume (Spanned)

Ein Laufwerk, basierend auf dem freien Speicher mehrerer physikalischer Festplatten, die durch den LDM miteinander verbunden sind. Bis zu 32 Laufwerke können zu einen Volume integriert werden, was zwar einerseits Hardware-Größenbeschränkungen sprengt, aber andererseits auch bedingt, dass bei Ausfall nur eines Laufwerks die Gesamtheit aller Daten verloren geht und kein Teil dieses übergreifenden Laufwerkes entfernt werden kann, ohne dass das ganze Laufwerk zerstört wird. Daher bringt ein übergreifendes Volume weder eine bessere Zuverlässigkeit, noch eine bessere E/A-Rate.

Stripeset-Volume

Ein manchmal auch RAID-0 genanntes Laufwerk, das aus gleich großen „Daten-Stripesets“ besteht, die quer über alle verwendeten Laufwerke geschrieben werden; was bedeutet, dass Sie zur Erstellung eines Stripeset-Volumes zwei oder mehr dynamische Laufwerke benötigen. Die Laufwerke in einem Volume vom Typ 'Stripeset' müssen nicht identisch sein, aber auf jeder Laufwerk, das Sie in das Volume aufnehmen wollen, muss ungenutzter Speicher vorhanden sein und die Größe des Volumes wird bestimmt durch die Größe des kleinsten Speicherplatzes. Der Datenzugriff bei einem Volume vom Typ 'Stripeset' ist üblicherweise schneller als der vergleichbare Zugriff auf ein einziges physikalisches Laufwerk, weil die Eingabe/Ausgabe-Operationen über mehr als ein Laufwerk verteilt werden.

Laufwerke vom Typ 'Stripeset' werden zur Performance-Steigerung und nicht wegen besserer Zuverlässigkeit erstellt, da sie keine redundanten Informationen enthalten.

Gespiegeltes Volume (Mirrored)

Ein manchmal auch RAID-1 genannter, fehlertoleranter Laufwerkstyp, dessen Daten auf zwei identischen physikalischen Festplatten dupliziert werden. Alle Daten des einen Laufwerks werden

zur Schaffung der Datenredundanz auf das andere Laufwerk kopiert. Nahezu jedes Laufwerk kann gespiegelt werden, einschließlich System- und Boot-Laufwerke – falls der Laufwerke ausfällt, kann immer noch auf die Daten des verbliebenen Laufwerks zugegriffen werden. Leider gibt es starke Hardware-Begrenzungen bezüglich Größe und Geschwindigkeit bei der Verwendung von gespiegelten Volumes.

Gespiegeltes Stripeset-Volume

Ein auch RAID-1+0 genanntes, fehlertolerantes Volume, welches die Vorteile erhöhter E/A-Geschwindigkeit des Typs 'Stripeset' mit der Redundanz beim Typ 'Gespiegelt' kombiniert. Was jedoch bleibt, ist ein offensichtlicher, von der 'Spiegelung'-Architektur stammender Nachteil: ein schlechtes Laufwerk-zu-Volume-Größenverhältnis.

RAID-5

Ein fehlertolerantes Stripeset-Volume, dessen Daten über eine Zusammenstellung (Array) von drei oder noch mehr Laufwerken quer verteilt sind. Die Festplatten müssen nicht identisch sein, aber jede Festplatte des „Volumes“ muss über gleich große Blöcke an nicht zugeordnetem Speicherplatz verfügen. Außerdem werden über das Laufwerk-Array auch Paritätsdaten (speziell berechnete Werte, die im Fehlerfall zur Datenrekonstruktion verwendet werden können) verteilt gespeichert. Und diese Paritätsdaten werden immer auf einem anderen Laufwerk als die eigentlichen Daten gespeichert. Sollte eine physikalische Platte ausfallen, so kann der Anteil des RAID-5-Laufwerks, der auf dieser Festplatte lag, aus den verbliebenen Daten und den Paritätsdaten wiederhergestellt werden. Ein RAID-5-Volume bietet erhöhte Zuverlässigkeit und ermöglicht die Speicherbegrenzungen physikalischer Laufwerke zu überwinden, wobei das Disk-zu-Volume-Größenverhältnis besser ist als bei Laufwerken vom Typ 'Gespiegelt' (Mirrored).

Der Assistent zur Partitionserstellung

Der Assistent zur **Partitionserstellung** ermöglicht Ihnen, jeden Partitionstyp (inkl. System und Aktiv) anzulegen, ein Dateisystem zu wählen, einen Laufwerksbuchstaben zuzuweisen und noch weitere Laufwerksverwaltung-Funktionen zu verwenden.

Sie können Schritt für Schritt Aktionsparameter eingeben und jederzeit für Korrekturen auch wieder zu vorherigen Schritten zurückwechseln. Um Sie bei Ihrer Wahl zu unterstützen, ist jeder Parameter mit detaillierten Anweisungen ergänzt.

So erstellen Sie eine neue Partition:

Starten Sie den **Assistenten zur Partitionserstellung** durch Wahl des Befehls **Partition erstellen** im Seitenleistenbereich **Assistenten** – oder rechtsklicken Sie auf einen nicht zugeordneten Speicherplatz und wählen im erscheinenden Kontextmenü **Partition erstellen**.

Bestimmen Sie den zu erstellenden Partitionstyp

In diesem ersten Schritt müssen Sie die Art der Partition spezifizieren, die Sie erstellen wollen. Die folgenden Partitionstypen stehen zur Verfügung:

- Basis
- Einfach/Übergreifend
- Stripset
- Gespiegelt
- RAID-5

Ihnen wird eine kurze Beschreibung für jeden Partitionstyp angezeigt (zum besseren Verständnis der Vorteile und Beschränkungen jeder möglichen Partitionsarchitektur).

*Sollte das aktuelle, auf dem Computer installierte Betriebssystem den gewählten Partitionstyp nicht unterstützen, so erhalten Sie eine entsprechende Warnung. In diesem Fall wird die **Weiter**-Schaltfläche deaktiviert, so dass Sie zum Fortsetzen der Partitionserstellung einen anderen Partitionstyp wählen müssen.*

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: Ziellaufwerk wählen (S. 303).

Ziellaufwerk wählen

Der nächste Assistentenschritt fordert Sie auf, die Festplatte zu wählen, deren unzugeordneter Speicher für die Partitionserstellung genutzt wird.

So erstellen Sie ein Basis-Volume:

- Wählen Sie die Zielfestplatte und den nicht zugeordneten Speicherplatz, von dem die Basis-Volume erstellt werden soll.

So erstellen Sie eine einfaches/übergreifendes Volume:

- Wählen Sie eine oder mehrere Zielfestplatten, auf der/denen die Partition erstellt wird.

So erstellen Sie ein gespiegeltes Volume:

- Wählen Sie zwei Ziellaufwerke, auf denen das Volume erstellt wird.

So erstellen Sie eine Stripeset-Volume:

- Wählen Sie zwei oder mehr Ziellaufwerke, auf denen das Volume erstellt wird.

So erstellen Sie eine RAID-5-Partition:

- Wählen Sie drei Ziellaufwerke, auf denen das Volume erstellt wird.

Nach der Wahl der Laufwerke ermittelt der Assistent die maximale Größe des resultierenden Volumes, das sich aus der Menge des auf dem Laufwerk verfügbaren, nicht zugeordneten Speicherplatzes sowie gegebenen Anforderungen des zuvor bestimmten Volume-Typs ableitet.

Wenn Sie versuchen, ein **dynamisches** Laufwerk auf einem oder mehreren **Basisdatenträgern** anzulegen, so erhalten Sie eine Warnmeldung, dass die gewählten Festplatten automatisch zu dynamischen Datenträgern konvertiert werden.

Sofern erforderlich (abhängig vom gewählten Partitionstyp), werden Sie aufgefordert, Ihrer Auswahl eine notwendige Anzahl von Laufwerken hinzuzufügen.

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: Partitionstyp festlegen (S. 302).

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: Partitionsgröße festlegen (S. 303).

Partitionsgröße festlegen

Auf der dritten Assistentenseite können Sie die Größe der zukünftigen Partition definieren, abhängig von den zuvor gemachten Einstellungen. Um die benötigte Größe innerhalb der minimalen und maximalen Grenzen einzustellen, können Sie den Schieberegler verwenden oder die gewünschten Werte im Eingabefenster eintippen oder die Begrenzungslinien der grafischen Laufwerksdarstellung mit der Maus verschieben.

Bei Verwendung des maximalen Wertes wird normalerweise der gesamte nicht zugeordnete Speicherplatz in die Laufwerkserstellung eingeschlossen. Der resultierende nicht zugeordnete

Speicher und die anvisierte maximale Laufwerksgröße können von Fall zu Fall variieren (z.B. weil die Größe einer Mirror-Platte die Größe einer anderen Mirror-Platte bedingt oder weil auf der Festplatte die letzten 8 MB für zukünftige Konvertierungen von Basis zu Dynamisch reserviert werden).

Wenn bei Basis-Partitionen einiger nicht zugeordneter Speicherplatz auf der Festplatte verbleibt, so können Sie außerdem die Position der neuen Partition wählen.

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: Ziellaufwerk wählen (S. 303).

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: Volume-Optionen einstellen (S. 304).

Volume-Optionen einstellen

Im nächsten Assistentenschritt können Sie einen **Laufwerksbuchstaben** zuweisen (Standard ist der erste freie Buchstabe im Alphabet) und optional die **Datenträgerbezeichnung** (Standard ist keine Bezeichnung). Hier spezifizieren Sie außerdem das **Dateisystem** und die **Clustergröße**.

Der Assistent fordert Sie auf, eines der Windows-Dateisysteme zu wählen: FAT16 (bei Partitionsgrößen über 2 GB deaktiviert), FAT32 (bei Partitionsgrößen über 2 TB deaktiviert), NTFS oder Sie lassen die Partition **Unformatiert**.

Bei Wahl der Clustergröße können Sie jede Zahl aus den für ein bestimmtes Dateisystem vorgegebenen Größen wählen. Beachten Sie, dass das Programm Ihnen schon die Clustergröße vorschlägt, die zum Volume und dem gewählten Dateisystem am besten passt.

Beim Erstellen einer Basis-Volume, die auch als System-Volume verwendet werden kann, offeriert der Assistent eine geänderte Anzeige mit der Möglichkeit, den **Partitionstyp** auf **Primär**, **Aktiv** oder **Logisch** einzustellen.

Primär ist die gängige Wahl, wenn ein Betriebssystem auf dem Volume installiert werden soll. Wählen Sie **Aktiv**, wenn Sie auf dem Volume ein Betriebssystem installieren wollen, von dem der Computer beim Start direkt bootet. Wenn die Einstellung **Primär** nicht ausgewählt ist, so ist auch die Option **Aktiv** ausgeschaltet. Soll das Volume nur zum Speichern von Daten verwendet werden, so wählen Sie **Logisch**.

---

*Ein Basisdatenträger kann bis zu vier primäre Volumes enthalten. Sollten diese schon existieren, so muss das Laufwerk zur Erstellung weiterer primärer Volumes in ein dynamisches Volume konvertiert werden – anderenfalls sind die Einstellungen **Aktiv** und **Primär** deaktiviert und Sie können nur den Volume-Typ **Logisch** wählen. Durch eine Warnmeldung werden Sie gegebenenfalls darauf hingewiesen, dass von diesem Volume nicht gebootet werden kann.*

*Wenn Sie für eine neue Datenträgerbezeichnung Ziffern verwenden, die vom aktuell installierten Betriebssystem nicht unterstützt werden, erhalten Sie auch eine Warnung und die **Weiter**-Schaltfläche wird deaktiviert. Sie müssen die Bezeichnung ändern, um mit der Erstellung des neuen Volumes fortzufahren.*

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: Partitionsgröße festlegen (S. 303).

Durch Klicken auf **Abschluss** wird die geplante Aktion abgeschlossen.

Zur Abarbeitung der geplanten Aktion klicken Sie zuerst auf **Ausführen** in der Symbolleiste und dann auf **Fertig stellen** im erscheinenden Fenster **Ausstehende Aktionen.**

Sollten Sie bei FAT16/FAT32 eine Clustergröße von 64K oder bei NTFS eine Größe von 8-64KB eingestellt haben, so kann Windows das Volume zwar mounten, aber bei manchen anderen Programmen (z.B. Setup-

Programmen) kann es zu Fehlkalkulationen bei der Laufwerksgrößenberechnung kommen.

Volume löschen

Diese Version von Acronis Disk Director Lite hat eine reduzierte Funktionalität, weil sie hauptsächlich zur Vorbereitung fabrikneuer Systeme für die Wiederherstellung zuvor gesicherter Partitionsabbilder gedacht ist. Funktionen zur Größenänderung bestehender Partitionen und zur Erstellung neuer Partitionen unter Verwendung des Speicherplatzes bereits vorhandener Partitionen finden sich nur in der Vollversion, so dass mit der vorliegenden Lite-Version das Löschen von Partitionen manchmal der einzige Weg sein kann, um benötigten Festplattenplatz ohne Veränderung der Festplattenkonfiguration freizugeben.

Nachdem eine Partition gelöscht wurde, wird sie dem nicht zugeordneten Speicherplatz der Platte hinzugefügt. Das lässt sich nutzen, um eine neue Partition zu erstellen oder den Partitionstyp einer anderen zu verändern.

So löschen Sie eine Partition:

1. Wählen Sie eine Festplatte und auf dieser die zu löschende Partition.
2. Wählen Sie den Befehl **Partition löschen** oder einen entsprechenden Eintrag in der **Aktionen**-Liste der Seitenleiste – oder klicken Sie auf das Symbol **Partition löschen** in der Symbolleiste.

   Sollten sich auf der Partition Daten befinden, so werden Sie mit einer Meldung gewarnt, dass alle Informationen unwiederbringlich verloren gehen.
3. Indem Sie im Fenster **Partition löschen** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 307). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die aktive Partition setzen

Wenn Sie über mehrere primäre Partitionen verfügen, so müssen Sie eine davon als Boot-Partition spezifizieren. Dafür können Sie die Partition so einstellen, dass sie „aktiv“ wird. Auf einer Festplatte kann jedoch nur ein Laufwerk aktiv sein: wird eine Partition neu als aktiv gesetzt, dann wird bei einer zuvor aktiven Partition die entsprechende Einstellung aufgehoben.

So setzen Sie eine Partition aktiv:

1. Bestimmen Sie eine primäre Partition auf einem MBR-Basisdatenträger, die aktiv gesetzt werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Aktiv setzen**.

   Sofern keine andere aktive Partition im System vorliegt, wird die Operation zur Liste der ausstehenden Aktionen hinzugefügt.

   Beachten Sie, dass sich durch das Aktivsetzen der neuen Partition wiederum der Laufwerksbuchstabe einer zuvor aktiven Partition ändern kann und daher installierte Anwendungsprogramme evtl. nicht mehr lauffähig sein können.
3. Sollte im System eine andere Partition aktiv sein, so erhalten Sie eine Warnmeldung, dass diese bisherige aktive Partition zuerst auf passiv gesetzt werden muss. Indem Sie im **Warndialog** auf **OK** klicken, wird das Setzen der aktiven Partition zur Liste ausstehender Aktionen hinzugefügt.

   Beachten Sie: Selbst wenn ein Betriebssystem auf der neuen aktiven Partition liegt, kann es unter Umständen sein, dass der Computer dennoch nicht von ihr booten kann. Sie müssen Ihre Entscheidung bestätigen, damit die neue Partition als aktiv gesetzt wird.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 307). Wenn Sie das

Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

Laufwerksbuchstaben ändern

Das Windows-Betriebssystem weist Festplatten-Laufwerken ihre Laufwerksbuchstaben während des Startvorgangs zu. Diese Laufwerksbuchstaben werden vom Betriebssystem und Anwendungsprogrammen verwendet, um Dateien und Ordner auf den Partitionen zu finden.

Das Hinzufügen neuer Festplatten sowie das Erstellen oder Löschen von Partitionen auf existierenden Platten kann Ihre Systemkonfiguration ändern. Das kann zur Folge haben, dass manche Anwendungsprogramme nicht mehr normal funktionieren oder Benutzerdateien nicht mehr automatisch gefunden bzw. geöffnet werden können. Um dem entgegenzuwirken, können Sie vom Betriebssystem auf die Partitionen zugewiesene Laufwerksbuchstaben manuell ändern.

So ändern Sie den Laufwerksbuchstaben einer Partition, der vom Betriebssystem zugewiesen wurde:

1. Wählen Sie die Partition, deren Laufwerksbuchstabe geändert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Laufwerksbuchstabe ändern**.
3. Wählen Sie im Dialog **Laufwerksbuchstabe ändern** den neuen Laufwerksbuchstaben.
4. Indem Sie im Fenster **Laufwerksbuchstabe ändern** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

   (Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 307). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

Volume-Bezeichnung ändern

Die Bezeichnung eines Volumes ist ein optionales Attribut. Es handelt sich um einen Namen, der dem Volume zur leichteren Erkennung zugeordnet wird. So kann z.B. ein Volume SYSTEM genannt werden (Volume für das Betriebssystem) oder PROGRAMME (Volume für Anwendungen) oder DATEN (Volume für Dokumente), was jedoch nicht bedeutet, dass auf diesem Volume nur noch Daten gespeichert werden können, die dieser Bezeichnung entsprechen.

Unter Windows werden die Volume-Bezeichnungen im Verzeichnisbaum des Explorers angezeigt: Laufwerk1(C:), Laufwerk2(D:), Laufwerk3(E:), etc. Laufwerk1, Laufwerk2 und Laufwerk3 sind Volume-Bezeichnungen. Eine Volume-Bezeichnung ist außerdem auch in den Öffnen-/Speichern-Dialogen aller Anwendungsprogramme sichtbar.

So ändern Sie die Bezeichnung eines Volumes:

1. Rechtsklicken Sie auf das gewünschte Volume und wählen Sie **Bezeichnung ändern**.
2. Geben Sie in das Textfeld des Dialoges **Bezeichnung ändern den neuen Laufwerksnamen ein.**
3. Indem Sie im Fenster **Bezeichnung ändern** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

   *Wenn Sie für die neue Bezeichnung des Volumes Zeichen verwenden, die vom aktuell installierten Betriebssystem nicht unterstützt werden, erhalten Sie eine Warnung und die **Weiter**-Schaltfläche wird deaktiviert. Um mit der Änderung der Volume-Bezeichnung fortfahren zu können, dürfen Sie für die Aktion nur noch unterstützte Zeichen verwenden.*

   (Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 307). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Bezeichnung wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

Volume formatieren

Fälle, in denen es angebracht sein kann, ein Volume mit einem neuen Dateisystem zu formatieren:

- Um zusätzlichen Speicherplatz zu gewinnen, der zuvor durch eine ungünstige Clustergröße auf FAT16- oder FAT32-Dateisystemen verloren ging.
- Um auf dem Volume befindliche Daten auf schnelle und relativ verlässliche Art zu zerstören

So formatieren Sie ein Volume:

1. Wählen Sie das zu formatierende Volume.
2. Klicken Sie mit der rechten Maustaste auf das betreffende Volume und wählen Sie im Kontextmenü **Formatieren**.

   Darauf erscheint das Fenster **Volume formatieren**, in dem Sie die Einstellungen für das neue Dateisystem vornehmen können. Sie können eines der Windows-Dateisysteme wählen: FAT16 (bei Volume-Größen über 2 GB deaktiviert), FAT32 (bei Volume-Größen über 2 TB deaktiviert) oder NTFS.

   Falls notwendig, können Sie im Textfeld für das Volume eine Bezeichnung eingeben: standardmäßig ist dieses Fenster leer.

   Bei Wahl der Clustergröße können Sie jede Zahl aus den für ein bestimmtes Dateisystem vorgegebenen Größen wählen. Beachten Sie, dass das Programm Ihnen schon die Clustergröße vorschlägt, die zum Volume und dem gewählten Dateisystem am besten passt.
3. Wenn Sie auf **OK** klicken, um mit dem Befehl **Volume formatieren** fortzufahren, wird dieser der Liste ausstehender Aktionen hinzugefügt.

   (Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausführen (S. 307). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Volume-Struktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

Sollten Sie bei FAT16/FAT32 eine Clustergröße von 64K oder bei NTFS eine Größe von 8-64KB eingestellt haben, so kann Windows das Volume zwar mounten, aber bei manchen anderen Programmen (z.B. Setup-Programmen) kann es zu Fehlkalkulationen bei der Laufwerksgrößenberechnung kommen.

6.11.7 Ausstehende Aktionen

Alle vom Anwender manuell oder mit Hilfe eines Assistenten zusammengestellten Aktionen werden solange als ausstehend angesehen, bis der Anwender durch Anstoß eines entsprechenden Befehls bewirkt, dass alle Änderungen dauerhaft gemacht werden. Bis dahin visualisiert Acronis Disk Director Lite lediglich die neue Laufwerksstruktur so, wie es sich aus den geplanten, auf Laufwerken und Volumes anzuwendenden Aktionen ergibt. Dieser Ansatz ermöglicht geplante Aktionen zu kontrollieren, beabsichtigte Änderungen doppelt überprüfen zu können und sofern nötig Aktionen vor der Ausführung jederzeit abbrechen zu können.

Das Programm zeigt Ihnen also zuerst eine Liste aller ausstehenden Aktionen an, um Sie vor unbeabsichtigten Änderungen Ihrer Laufwerke zu bewahren.

Sie finden in der Anzeige **Laufwerksverwaltung** eine Symbolleiste, die Icons zum Starten der Befehle **Rückgängig**, **Wiederherstellen** und **Ausführen** enthält, welche speziell für die ausstehenden Aktionen gedacht sind. Sie können diese Befehle außerdem über das Menü **Disk ManagementLaufwerksverwaltung** der Konsole starten.

Alle geplanten Operationen werden zur Liste der ausstehenden Aktionen hinzugefügt.

Über den Befehl **Rückgängig** können Sie je den letzten Befehl in dieser Liste zurücksetzen. Solange die Liste nicht leer ist, steht dieser Befehl zur Verfügung.

Über den Befehl **Wiederherstellen** können Sie die letzte ausstehende und zuvor rückgängig gemachte Aktion wieder zurückholen.

Der Befehl **Ausführen** bringt Sie zum Fenster **Ausstehende Aktionen**, in dem Sie die Liste dieser ausstehenden Aktionen noch einmal einsehen können. Durch Klick auf **Fertig stellen** wird dann die Ausführung gestartet. Sobald Sie den Befehl **Fertig stellen** gewählt haben, sind Sie jedoch nicht mehr in der Lage, irgendeinen Befehl oder eine Aktion rückgängig zu machen. Sie können die Umsetzung aber vorher durch Klicken auf **Abbrechen** aufheben. In dem Fall werden an der Liste der ausstehenden Aktionen keine Veränderungen durchgeführt.

Da Acronis Disk Director Lite, wenn Sie das Programm ohne die ausstehenden Aktionen auszuführen beenden, alle Aktionen verwirft, erhalten Sie eine entsprechende Warnmeldung, wenn Sie das **Laufwerksverwaltung** einfach verlassen.

6.12 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 Zentrale Verwaltung

In diesem Abschnitt werden die Aktionen behandelt, die unter Verwendung der Komponenten für die zentrale Verwaltung ausgeführt werden können. Der Inhalt dieses Abschnitts gilt nur für die erweiterten Editionen (Advanced Editions) von Acronis Backup & Recovery 10.

7.1 Acronis Backup & Recovery 10 Management Server administrieren

In diesem Abschnitt werden die Ansichten beschrieben, die über den Naivigationsbaum eines mit der Konsole verbundenen Management Servers verfügbar werden und erklärt, wie Sie mit diesen Ansichten arbeiten.

7.1.1 Dashboard

Verwenden Sie das Dashboard, um auf einen Blick die Integrität der geschützten Daten auf den registrierten Maschinen einschätzen zu können. Auf dem Dashboard wird eine Zusammenfassung der Aktivitäten des Acronis Backup & Recovery 10-Agenten angezeigt. Außerdem können Sie nach freiem Speicherplatz in den verwalteten Depots suchen sowie Probleme schnell erkennen und beheben.

Warnungen

Im Bereich „Alarmmeldungen“ werden Sie über Ereignisse informiert, die in zentralen Depots auf dem Management Server und auf registrierten Maschinen aufgetreten sind und Sie haben die Möglichkeit, diese zu lösen oder zu untersuchen. 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*	Tasks ansehen	**Tasks ansehen** öffnet die Ansicht **Backup-Pläne und Tasks** mit den fehlgeschlagenen Tasks, wo Sie die Ursache der Fehlfunktion ermitteln können.
	Tasks, die Interaktion erfordern: *X*	Auflösen	Wenn für mindestens einen Task in der Datenbank des Management Servers menschliches Eingreifen erforderlich ist, wird auf dem Dashboard ein Alarm angezeigt. Klicken Sie auf **Auflösen...**, um das Fenster **Tasks erfordern Interaktion** zu öffnen. In diesem Fenster können Sie die einzelnen Fälle untersuchen und eine Entscheidung fällen.
	Prüfen der Lizenzen auf *X* Maschine(n) fehlgeschlagen	Log anzeigen	Der Acronis Backup & Recovery 10-Agent stellt beim Start und dann alle 1-5 Tage (entsprechend der Konfigurationsparameter des Agenten) eine Verbindung mit dem Acronis License Server her. Der Alarm wird angezeigt, wenn die Lizenz-Prüfung auf mindestens einem Agenten nicht erfolgreich war. Dies kann passieren, wenn der License Server nicht

			verfügbar war oder wenn die Lizenz-Daten beschädigt sind. Klicken Sie auf **Log anzeigen**, um die Ursache einer nicht erfolgreichen Prüfung zu ermitteln. Wenn die Lizenz-Prüfung 1-60 Tage (entsprechend der Konfigurationsparameter des Agenten) nicht zum Erfolg führt, hört der Agent auf zu arbeiten, bis eine Lizenz-Prüfung erfolgreich durchgeführt wurde.
	Depots mit wenig freiem Speicherplatz: *X*	Depots ansehen	Der Alarm wird angezeigt, wenn auf mindestens einem zentralen Depot weniger als 10% freier Speicherplatz verfügbar ist. Wenn Sie auf **Depots ansehen** klicken, gelangen Sie zur Ansicht **Zentrale Depots (S. 132),** in der Sie die Größe des Depots, den freien Speicherplatz und Inhalt überprüfen sowie die Schritte einleiten können, die zur Erhöhung des freien Speicherplatzes notwendig sind.
	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. 422) erstellen. **Jetzt erstellen** startet den Bootable Media Builder (S. 427).
	Keine Backups erstellt seit *X* Tag(en) auf *Y* Maschine(n)	Liste anzeigen	Sie werden vom Dashboard gewarnt, dass seit einer gewissen Zeit keine Daten-Backups auf einigen registrierten Maschinen erstellt wurden. Zum Konfigurieren der Zeitdauer, die als kritisch angesehen werden soll, wählen Sie **Optionen –> Konsolenoptionen –> Zeitbasierte Alarmmeldungen** aus.
	Keine Verbindung zum Management Server seit *X* Tag(en): *Y* Maschine(n)	Maschinen anzeigen	Das Dashboard warnt Sie, dass seit einer gewissen Zeit keine Verbindung zwischen einigen registrierten Maschinen und dem Management Server aufgebaut werden konnte, was darauf hindeutet, dass die Maschinen möglicherweise nicht zentral verwaltet werden. Klicken Sie auf **Maschinen anzeigen**, um die Ansicht **Maschinen** zu öffnen, die eine Liste der Maschinen, gefiltert nach dem Feld „Letzte Verbindung“, enthält. Zum Konfigurieren der Zeitdauer, die als kritisch angesehen werden soll, wählen Sie **Optionen –> Konsolenoptionen –> Zeitbasierte Alarmmeldungen** aus.
	Es wird empfohlen, den Management Server zu sichern, um dessen Konfiguration zu schützen. Installieren Sie den Agent auf der Maschine mit dem Management Server und	Acronis-Komponenten installieren	Installieren Sie den Acronis Backup & Recovery 10 Agenten für Windows, um die Maschine zu sichern, auf der sich der Acronis Backup & Recovery 10 Management Server befindet. Klicken Sie auf **Jetzt installieren**, um das

	fügen die Maschine zum AMS hinzu.		Installationsprogramm zu starten.
⚠	Acronis Backup & Recovery 10 Management Server wurde seit *X* Tag(en) nicht gesichert	Backup jetzt	Der Alarm wird nur angezeigt, wenn der Acronis Backup & Recovery 10 Agent für Windows auf dem Management Server installiert ist. Der Alarm warnt Sie, dass seit einer gewissen Zeit kein Daten auf dem Management Server gesichert wurden. Wenn Sie auf **Backup jetzt** klicken, gelangen Sie zur Seite **Backup-Plan erstellen**, wo Sie die Backup-Aktion sofort konfigurieren und starten können. Zum Konfigurieren der Zeitdauer, die als kritisch angesehen werden soll, wählen Sie **Optionen –> Konsolenoptionen –> Zeitbasierte Alarmmeldungen** aus.

Aktivitäten

Im Säulendiagramm können Sie den täglichen Verlauf der Aktivitäten des Acronis Backup & Recovery 10-Agenten untersuchen. Der Verlauf basiert auf den Log-Einträgen, die auf den registrierten Maschinen und auf dem Management Server erfasst wurden. Das Diagramm zeigt die Anzahl der Log-Einträge jedes einzelnen Typs (Fehler, Warnung, Information) für einen bestimmten Tag an.

Die Statistik für das ausgewählte Datum wird rechts vom Diagramm angezeigt. Alle Felder in der Statistik sind interaktiv, d.h. wenn Sie also auf ein Feld klicken, wird die Ansicht **Log** geöffnet und in dieser sind die Log-Einträge nach dem betreffenden Feld vorgefiltert.

Im oberen Bereich des Diagramms können Sie die Aktivitäten auswählen, die in Abhängigkeit von der Anwesenheit und dem Schweregrad der Fehler ausgeführt werden sollen.

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

Systemansicht

Im Abschnitt **Systemansicht** wird eine zusammengefasste Statistik der registrierten Maschinen, Tasks, Backup-Richtlinien und zentralen Backup-Pläne gezeigt. Klicken Sie auf die Elemente dieses Bereiches (mit Ausnahme der zentralen Backup-Pläne), um relevante Informationen zu erhalten. Auf diese Weise gelangen Sie zur entsprechenden Ansicht mit vorgefilterten Maschinen, Tasks oder Backup-Richtlinien. Wenn Sie z.B. unter **Tasks** auf **Untätig** klicken, wird die Ansicht **Tasks** geöffnet und die Tasks nach dem Zustand **Untätig** gefiltert angezeigt.

Die Informationen, die im Abschnitt **Systemansicht** dargestellt werden, werden jedes Mal aktualisiert, wenn sich der Management Server mit den Maschinen synchronisiert. Die Informationen in den anderen Abschnitten werden alle 10 Minuten sowie jedes Mal, wenn Sie auf das Dashboard zugreifen, aktualisiert.

Depots

Im Abschnitt **Depots** werden die Informationen zu den zentral verwalteten Depots angezeigt. Sie können Depots nach Namen oder nach belegtem Speicherplatz sortieren. In einigen Fällen ist die Information zum freien Speicherplatz in einem Depot möglicherweise nicht verfügbar, z.B. dann, wenn sich das Depot in einer Bandbibliothek befindet (Banddepot). Wenn das Depot selbst nicht verfügbar (offline) ist, dann wird die Meldung „Depot ist nicht verfügbar“ angezeigt.

7.1.2 Backup-Richtlinien

Wenn Sie mehrere Maschinen als Gesamtheit verwalten und schützen möchten, können Sie ein Template für einen Backup-Plan erstellen, eine sogenannte „Backup-Richtlinie“. Durch Anwendung dieses Templates auf eine Gruppe von Maschinen können Sie mehrere Backup-Pläne mit einer einzigen Aktion verteilen. Backup-Richtlinien gibt es nur auf dem Acronis Backup & Recovery 10 Management Server.

Sie müssen sich nicht mit jeder Maschine einzeln verbinden, um zu prüfen, ob die Daten erfolgreich gesichert wurden. Überprüfen Sie stattdessen den kumulativen Status der Richtlinie (S. 312) auf allen verwalteten Maschinen, auf die diese Richtlinie angewendet wird.

Um herauszufinden, ob eine Backup-Richtlinie momentan verteilt, widerrufen oder aktualisiert wird, überprüfen Sie das Verteilungsstadium (S. 312) der Richtlinie.

Arbeitsmöglichkeiten mit der Ansicht „Backup-Richtlinien“

- Verwenden Sie die Aktionsschaltflächen der **Symbolleiste**, um neue Richtlinien zu erstellen, vorhandene Richtlinien auf Maschinen anzuwenden oder andere Aktionen mit Backup-Richtlinien (S. 314) auszuführen.
- Verwenden Sie die Registerkarten des Bereichs **Informationen**, um detaillierte Informationen zur ausgewählten Richtlinie anzuzeigen und weitere Aktionen auszuführen, z.B. die Richtlinie aufzuheben, Details zur Maschine (Gruppe) anzuzeigen, auf die die Richtlinie angewendet wird usw. Der Bereich ist standardmäßig eingeklappt. Sie können die Leiste aufklappen, indem Sie auf das  Chevron-Symbol klicken. Der Inhalt des Bereichs ist außerdem im Fenster Richtlinien-Details (S. 316) dupliziert.
- Verwenden Sie die Funktion zum Filtern und Sortieren (S. 316) der Richtlinientabelle, um diese einfacher durchsuchen und überprüfen zu können.

Verteilungsstadien von Backup-Richtlinien

Das Verteilungsstadium einer Backup-Richtlinie ist eine Kombination der Richtlinien-Verteilungsstadien auf allen Maschinen, auf die die Richtlinie angewendet wird. Wenn z.B. die Richtlinie auf drei Maschinen angewendet wird und auf der ersten Maschine das Stadium „Wird verteilt“, auf der zweiten Maschine das Stadium „Wird aktualisiert“ und auf der dritten Maschine das Stadium „Verteilt“ aufweist, dann hat die Richtlinie das Stadium „Wird verteilt, Wird aktualisiert, Verteilt“.

Das Verteilungsstadium einer Backup-Richtlinie auf einer Gruppe von Maschinen ist eine Kombination der Richtlinien-Verteilungsstadien auf den Maschinen, die zu der Gruppe gehören.

Weitere Informationen zu den Verteilungsstadien von Backup-Richtlinien finden Sie im Abschnitt Stadien und Status von Backup-Richtlinien (S. 66).

Zustände von Backup-Richtlinien

Der Status einer Backup-Richtlinie ist der kumulative Status der Richtlinienzustände auf allen Maschinen, auf die die Richtlinie angewendet wird. Wenn z.B. die Richtlinie auf drei Maschinen angewendet wird und auf der ersten Maschine den Status „OK“, auf der zweiten Maschine den Status „Warnung“ und auf der dritten Maschine den Status „Fehler“ aufweist, dann hat die Richtlinie den Status „Fehler“.

Der Status einer Backup-Richtlinie auf einer Gruppe von Maschinen ist der kumulative Status der Richtlinienzustände auf den Maschinen, die zu der Gruppe gehören.

In der folgenden Tabelle wird eine Zusammenfassung der möglichen Zustände einer Backup-Richtlinie gezeigt.

	Status	Grund	Handhabung
1	**Fehler**	Der Richtlinienstatus auf mindestens einer Maschine ist „Fehler“. Andernfalls siehe Punkt 2.	Überprüfen Sie das Log oder identifizieren Sie die fehlgeschlagenen Tasks, um die Ursache der Fehlfunktion zu ermitteln und führen Sie dann eine oder mehrere der folgenden Aktionen aus: ▪ Entfernen Sie den Grund des Fehlers. -> [optional] Starten Sie den gescheiterten Task manuell. ▪ Bearbeiten Sie die Backup-Richtlinie, um ein zukünftiges Auftreten der Fehlfunktion zu verhindern.
2	**Achtung**	Der Richtlinienstatus auf mindestens einer Maschine ist „Warnung“. Andernfalls siehe Punkt 3.	Überprüfen Sie die auf dem Log angezeigten Warnungen -> [optional] Führen Sie bestimmte Aktionen aus, um um zukünftige Warnungen bzw. Fehler zu verhindern.
3	**OK**	Der Richtlinienstatus ist auf allen Maschinen „OK“.	Es ist keine Handlung nötig. Beachten Sie, dass der Status einer Backup-Richtlinie, die nicht auf eine Maschine angewendet wird, ebenfalls „OK“ ist.

Was zu tun ist, wenn eine Richtlinie einen Fehlerstatus aufweist

1. Um die Ursache für das Auftreten einer Fehlfunktion zu ermitteln, führen Sie eine oder mehrere der folgenden Aktionen aus:
   - Klicken Sie auf den Hyperlink **Fehler**, um den Log-Eintrag des letzten aufgetretenen Fehlers anzuschauen.
   - Wählen Sie die Richtlinie aus und klicken Sie auf **Tasks anzeigen**. Überprüfen Sie die Tasks, deren letztes Ergebnis **Fehlgeschlagen** ist: Wählen Sie einen Task aus und klicken Sie dann auf **Log anzeigen**. Wählen Sie einen Log-Eintrag aus und klicken Sie dann auf **Details anzeigen**. Dieser Ansatz ist geeignet, wenn die Richtlinie das Stadium „Verteilt“ aufweist. Das bedeutet, dass die Tasks der Richtlinie bereits auf den verwalteten Maschinen vorhanden sind.
   - Wählen Sie die Richtlinie aus und klicken Sie auf **Log anzeigen**. Klicken Sie auf die mit „Fehler“ gekennzeichneten Log-Einträge, um die Ursache des Fehlers zu ermitteln: Wählen Sie einen Log-Eintrag aus und klicken Sie dann auf **Details anzeigen**. Dieser Ansatz ist geeignet, wenn die Fehler auftreten, während die Richtlinie verteilt, widerrufen oder aktualisiert wird.

   *Wenden Sie in der Ansicht **Tasks** den Filter **Letztes Ergebnis –> Fehlgeschlagen** an, falls es zu viele Tasks gibt. Sie können auch die fehlgeschlagenen Tasks nach Backup-Plänen oder Maschinen sortieren.*

   *Wenden Sie in der Ansicht **Logs** den Filter „Fehler“ an, falls es zu viele Log-Einträge gibt. Sie können auch die „Fehler“-Einträge nach Backup-Plänen, verwalteten Einheiten oder Maschinen sortieren.*

2. Wenn die Ursache für das Auftreten einer Fehlfunktion klar ist, dann führen Sie eine oder mehrere der folgenden Aktionen aus:
   - Entfernen Sie die Ursache der Fehlfunktion. Danach können Sie den fehlgeschlagenen Task manuell starten, um die Konsistenz des Backup-Schemas aufrechtzuerhalten, wenn die Richtlinie z.B. das Backup-Schema GVS oder „Türme von Hanoi“ verwendet.
   - Bearbeiten Sie die Backup-Richtlinie, um ein zukünftiges Auftreten der Fehlfunktion zu verhindern.

*Verwenden Sie den Abschnitt **Aktivitäten** im Dashboard, um schnell auf die „Fehler“-Einträge im Log zuzugreifen.*

Was zu tun ist, wenn eine Richtlinie einen Warnungsstatus aufweist

1. Um die Ursache für das Auftreten einer Warnung zu ermitteln, führen Sie eine oder mehrere der folgenden Aktionen aus:
   - Klicken Sie auf den Hyperlink **Warnung**, um den Log-Eintrag der letzten aufgetretenen Warnung anzuschauen.
   - Wählen Sie die Richtlinie aus und klicken Sie auf **Tasks anzeigen**. Überprüfen Sie die Tasks, deren letztes Ergebnis **Mit Warnungen abgeschlossen** ist: Wählen Sie einen Task aus und klicken Sie dann auf **Log anzeigen**. Dieser Ansatz ist geeignet, wenn die Richtlinie das Stadium „Verteilt“ aufweist. Das bedeutet, dass die Tasks der Richtlinie bereits auf den verwalteten Maschinen vorhanden sind.
   - Wählen Sie die Richtlinie aus und klicken Sie auf **Log anzeigen**. Klicken Sie auf die mit „Warnung“ gekennzeichneten Log-Einträge, um die Ursache der Warnung zu ermitteln: Wählen Sie einen Log-Eintrag aus und klicken Sie dann auf **Details anzeigen**. Dieser Ansatz ist geeignet, wenn die Warnungen aufgetreten sind, während die Richtlinie verteilt, widerrufen oder aktualisiert wurde.

   *Wenden Sie in der Ansicht **Tasks** den Filter **Letztes Ergebnis –> Mit Warnungen abgeschlossen** an, falls es zu viele Tasks gibt. Sie können auch mit Warnung abgeschlossene Tasks nach Backup-Plänen oder Maschinen sortieren.*

   *Wenden Sie in der Ansicht **Logs** den Filter „Warnung ⚠“ an, falls es zu viele Log-Einträge gibt. Sie können auch die „Warnungs“-Einträge nach Backup-Plänen, verwalteten Einheiten oder Maschinen sortieren.*
2. Wenn die Ursache für eine Warnung klar ist, wollen Sie möglicherweise Aktionen ausführen, mit denen ein zukünftiges Auftreten von Warnungen oder Fehlern verhindert werden kann.

*Verwenden Sie den Abschnitt **Aktivitäten** im Dashboard, um schnell auf die „Warnungs“-Einträge im Log zuzugreifen.*

Was zu tun ist, wenn eine Richtlinie den Status „OK“ aufweist

Es ist keine Handlung nötig.

Aktionen für Backup-Richtlinien

Alle nachfolgend beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Elemente in der Tasks-**Symbolleiste** ausgeführt. Die Aktionen können außerdem über das Kontextmenü (indem Sie mit der rechten Maustaste auf die ausgewählte Backup-Richtlinie klicken) ausgeführt weden – oder über den Balken **'Name der Backup-Richtlinie'-Aktionen** in der Leiste **Aktionen und Werkzeuge**.

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Backup-Richtlinien.

Aktion	Lösung
Backup-Richtlinie erstellen	Klicken Sie auf **Backup-Richtlinie erstellen**. Die Vorgehensweise zum Erstellen einer Backup-Richtlinie wird ausführlich im Abschnitt Erstellen einer Backup-Richtlinie (S. 374) beschrieben.
Richtlinie auf Maschinen oder Gruppen anwenden	Klicken Sie auf **Anwenden auf**. Geben Sie im Fenster Auswahl der Maschine (S. 315) die Maschinen (Gruppen) an, auf die die ausgewählte Backup-Richtlinie angewendet werden soll. Wenn die Maschine

	momentan offline ist, wird die Richtlinie verteilt, sobald die Maschine wieder online ist.
Eine Richtlinie bearbeiten	Klicken Sie auf **Bearbeiten**. Die Bearbeitung von Richtlinien wird auf die gleiche Weise ausgeführt wie die Erstellung (S. 374). Sobald die Richtlinie bearbeitet wurde, aktualisiert der Management Server die Richtlinie auf allen Maschinen, auf die die Richtlinie verteilt wurde.
Eine Richtlinie löschen	Klicken Sie auf **Löschen**. Daraufhin wird die Richtlinie auf den Maschinen, auf die sie verteilt wurde, widerrufen und vom Management Server gelöscht. Wenn die Maschine momentan offline ist, wird die Richtlinie widerrufen, sobald die Maschine wieder online ist.
Details einer Richtlinie anzeigen oder eine Richtlinie widerrufen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie im Fenster Richtliniendetails (S. 316) die Informationen zur ausgewählten Richtlinie. Sie können dort außerdem die Richtlinie auf den Maschinen oder Gruppen widerrufen, auf denen die Richtlinie angewendet wurde.
Tasks einer Richtlinie anzeigen	Klicken Sie auf **Tasks ansehen**. Die Ansicht Tasks (S. 345) zeigt eine Liste der Tasks an, die sich auf die ausgewählte Richtlinie beziehen.
Log einer Richtlinie anzeigen	Klicken Sie auf **Log anzeigen**. Die Ansicht Log (S. 347) wird eine Liste der Log-Einträge anzeigen, die sich auf die ausgewählte Richtlinie beziehen.
Eine Liste von Richtlinien aktualisieren	Klicken Sie auf **Aktualisieren**. Die Management Konsole aktualisiert die Liste der Backup-Richtlinien vom Management Server mit den neuesten Informationen. Obwohl die Richtlinien-Liste auf der Basis von Ereignissen automatisch aktualisiert wird, kann es sein, dass die Daten infolge einer gewissen Verzögerung nicht augenblicklich vom Management Server abgerufen werden. Eine manuelle Aktualisierung garantiert daher, dass auch die allerneusten Daten angezeigt werden.

Auswahl der Maschine

So wenden Sie die Backup-Richtlinie auf Maschinen oder auf Gruppen von Maschinen an

1. Bestimmen Sie, auf welche der folgenden Elemente die ausgewählte Backup-Richtlinie angewendet werden soll
   - **Gruppen**

     Wählen Sie in der Gruppenstruktur die Gruppe(n) aus, auf die die Richtlinie angewendet werden soll. Im rechten Teil des Fensters werden die Maschinen der ausgewählten Gruppe aufgelistet.
   - **Individuelle Maschinen**

     Wählen Sie in der Gruppenstruktur die entsprechende Gruppe aus. Wählen Sie dann im rechten Teil des Fensters die Maschinen aus, auf die die Richtlinie angewendet werden soll.
2. Klicken Sie auf **OK**.

Der Acronis Backup & Recovery 10 Management Server verteilt die Richtlinie auf die ausgewählten Maschinen und die Maschinen, die zu den ausgewählten Gruppen gehören.

Backup-Richtlinien filtern und sortieren

Nachfolgend finden Sie eine Anleitung zum Filtern und Sortieren von Backup-Richtlinien.

Aktion	Lösung
Backup-Richtlinien nach einer beliebigen Spalte sortieren	Klicken Sie auf die Spaltenköpfe, um die Backup-Richtlinien aufsteigend zu sortieren. Kicken Sie erneut auf den Spaltenkopf, um die Backup-Archive absteigend zu sortieren.
Backup-Richtlinien nach Name/Besitzer filtern	Geben Sie den Namen einer Richtlinie/den Namen eines Besitzers in die Felder unter dem entsprechenden Spaltenkopf ein. Sie erhalten als Ergebnis eine Liste von Backup-Richtlinien, deren Bezeichnungen/Besitzer vollständig oder partiell mit dem eingegebenen Wert übereinstimmen.
Backup-Richtlinien nach Verteilungsstadium, Status, Quelltyp, letztem Ergebnis und Planung filtern	Wählen Sie im Feld unterhalb des entsprechenden Spaltenkopfes den benötigten Wert aus einer Liste.

Die Backup-Richtlinien-Tabelle konfigurieren

Standardmäßig werden in der Tabelle sieben Spalten angezeigt, weitere sind versteckt. Sie können die Darstellung der Spalten nach Ihren Bedürfnissen und Vorlieben anpassen.

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.

Richtliniendetails

Im Fenster **Richtliniendetails** werden alle Informationen zur ausgewählten Backup-Richtlinie in fünf Registerkarten zusammengefasst. Außerdem können Sie hier Aktionen für Maschinen und Maschinengruppen ausführen, auf denen die Richtlinie angewendet wird.

Diese Informationen sind auch im Bereich **Informationen** verfügbar.

Backup-Richtlinie

Auf der Registerkarte werden Informationen zur ausgewählten Richtlinie angezeigt.

Source

Die Registerkarte zeigt Informationen zum Typ der zu sichernden Quelle sowie Regeln zur Auswahl der Quelle an.

Ziel

Auf der Registerkarte werden Informationen zum Backup-Ziel angezeigt.

Einstellungen

Auf der Registerkarte werden Informationen zum von der Richtlinie verwendeten Backup-Schema sowie zu Backup-Optionen angezeigt, die gegenüber den Standardeinstellungen verändert wurden.

Angewandt auf

Die Registerkarte zeigt eine Liste von Maschinen und Gruppen an, auf die die ausgewählte Richtlinie angewendet wird.

Aktionen

Aktion	Lösung
Details zur Maschine (Gruppe) anzeigen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie im Fenster Maschinendetails (S. 325)/Gruppendetails (S. 334) alle Informationen zur ausgewählten Maschine (oder zur ausgewählten Gruppe).
Tasks der Maschine (Gruppe) anzeigen	Klicken Sie auf **Tasks ansehen**. In der Ansicht Tasks (S. 345) wird eine Liste der Tasks angezeigt. Diese sind bereits nach der ausgewählten Maschine (Gruppe) gefiltert.
Log der Maschine (Gruppe) anzeigen	Klicken Sie auf **Log anzeigen**. In der Ansicht Log (S. 347) wird eine Liste der Log-Einträge angezeigt. Diese sind bereits nach der ausgewählten Maschine (Gruppe) gefiltert.
Richtlinie auf der Maschine (Gruppe) widerrufen.	Klicken Sie auf **Widerrufen**. Der Management Server entfernt die Richtlinie von der ausgewählten Maschine bzw. der ausgewählten Maschinengruppe. Die Richtlinie selbst verbleibt auf dem Management Server.

7.1.3 Physikalische Maschinen

Mit Acronis Backup & Recovery 10 kann der Administrator Daten sichern und Verwaltungsaktionen für mehrere Maschinen gleichzeitig ausführen. Der Administrator kann dem Management Server eine Maschine durch Angabe des Namens oder der IP-Adresse der Maschine hinzufügen und Maschinen aus dem Active Directory oder aus einer Textdatei importieren. Sobald eine Maschine auf dem Management Server registriert (S. 428) ist, ist sie für Gruppierungen, für die Anwendung von Backup-Richtlinien sowie für die Überwachung der Aktivitäten im Zusammenhang mit der Sicherung der Daten verfügbar.

Um abzuschätzen, ob die Daten auf einer verwalteten Maschine erfolgreich gesichert werden, kann der Administrator des Management Servers deren Status überprüfen. Der Status einer Maschine wird definiert durch den schwerwiegendsten Status aller Backup-Pläne (S. 191) (lokal und zentral), die auf der Maschine vorhanden sind, sowie aller Backup-Richtlinien (S. 312), die auf die Maschine angewendet werden. Er kann die Werte „OK“, „Warnung“ oder „Fehler“ annehmen.

Gruppen

Der Administrator des Management Servers kann Maschinen gruppieren. Eine Maschine kann in mehreren Gruppen Mitglied sein. Innerhalb einer beliebigen durch den Administrator erstellten Gruppe können eine oder mehrere verschachtelte Gruppen erstellt werden.

Durch eine Gruppierung ist es möglich, die Sicherung der Daten z.B. nach den Abteilungen eines Unternehmens, nach Active Directory-Domains oder Organisationseinheiten innerhalb einer Domain, nach verschiedenen Benutzergruppen oder nach Standorten zu organisieren.

Das Hauptziel einer Gruppierung besteht darin, mehrere Maschinen mit einer einzigen Richtlinie zu sichern. Sobald eine Maschine in einer Gruppe auftaucht, wird die Richtlinie, die auf die Gruppe angewendet wird, auch auf die Maschine angewendet und durch die Richtlinie werden die neuen

Tasks auf der Maschine erstellt. Sobald eine Maschine aus einer Gruppe entfernt wird, wird die Richtlinie, die auf die Gruppe angewendet wird, auf der Maschine widerrufen und die von der Richtlinie erstellten Tasks werden entfernt.

Standardgruppe – eingebaute Gruppe, die auf einem Management Server immer vorhanden ist. Diese Gruppe kann weder gelöscht noch umbenannt werden. Eine Standardgruppe kann keine verschachtelten Gruppen enthalten. Auf eine Standardgruppe kann eine Backup-Richtlinie angewendet werden. Ein Beispiel für eine Standardgruppe ist die Gruppe **Alle physikalischen Maschinen**, die aus allen Maschinen besteht, die auf dem Management Server registriert sind.

Benutzerdefinierte Gruppen – Gruppen, die manuell vom Administrator des Management Servers erstellt wurden.

- *Statische Gruppen*

  Statische Gruppen enthalten Maschinen, die der Gruppe durch den Administrator manuell hinzugefügt wurden. Ein statisches Mitglied verbleibt in der Gruppe, bis der Administrator das Mitglied aus der Gruppe entfernt oder die korrespondierende verwaltete Maschine vom Management Server löscht.

- *Dynamische Gruppen*

  Dynamische Gruppen enthalten Maschinen, die entsprechend der durch den Administrator vorgegebenen Kriterien automatisch hinzugefügt werden. Sobald die Kriterien angegeben sind, analysiert der Management Server die Eigenschaften der vorhandenen Maschinen und jeder neu registrierten Maschine. Die Maschine, die ein bestimmtes dynamisches Kriterium erfüllt, erscheint in allen Gruppen, die dieses dynamische Kriterium verwenden.

Weitere Informationen zum Gruppieren von Maschinen finden Sie im Abschnitt „Gruppieren der registrierten Maschinen (S. 62)“.

Weitere Informationen zur Anwendung von Richtlinien auf Maschinen und Gruppen finden Sie im Abschnitt „Richtlinien auf Maschinen und Gruppen (S. 62)“.

Arbeitsmöglichkeiten mit Maschinen

- Fügen Sie dem Management Server zuerst virtuelle Maschinen hinzu. Sie können Maschinen hinzufügen, indem Sie die Ansicht **Physikalische Maschinen** oder die Gruppe **Alle physikalischen Maschinen** im **Navigationsbaum** auswählen.
- Wählen Sie die Gruppe, in der sich die gewünschte Maschine befindet, und wählen Sie dann die Maschine.
- Verwenden Sie die Aktionsschaltflächen in der **Symbolleiste**, um Aktionen mit der Maschine (S. 321) auszuführen.
- Verwenden Sie die Registerkarten im Bereich **Informationen**, um detaillierte Informationen zur ausgewählten Maschine anzuzeigen und weitere Aktionen auszuführen, beispielsweise Tasks zu starten/stoppen, Richtlinien zu widerrufen, die Vererbung einer Richtlinie zu überprüfen usw. Der Bereich ist standardmäßig eingeklappt. Sie können die Leiste aufklappen, indem Sie auf das Chevron-Symbol klicken. Der Inhalt des Bereichs ist außerdem im Fenster **Maschinendetails** (S. 325) verfügbar.
- Verwenden Sie die Funktion zum Filtern und Sortieren (S. 330), um die betreffenden Maschinen einfacher suchen und überprüfen zu können.

Arbeitsmöglichkeiten mit Gruppen

- Wählen Sie in der Ansicht **Physikalische Maschinen** die Gruppe aus.
- Verwenden Sie die Aktionsschaltflächen in der Symbolleiste, um Aktionen mit der ausgewählten

Gruppe (S. 331) auszuführen.

- Verwenden Sie die Registerkarten im Bereich **Informationen**, um detaillierte Informationen zur ausgewählten Gruppe anzuzeigen und weitere Aktionen auszuführen, z.B. Richtlinien zu widerrufen oder die Vererbung einer Richtlinie zu überprüfen. Die Leiste ist standardmäßig eingeklappt. Sie können die Leiste aufklappen, indem Sie auf das Chevron-Symbol klicken. Der Inhalt des Bereichs ist außerdem im Fenster **Gruppendetails** (S. 334) verfügbar.

Aktionen mit Maschinen

Maschinen auf dem Management Server registrieren

Sobald die Maschine der Gruppe **Alle physikalischen Maschinen** hinzugefügt oder in diese importiert wird, wird sie auf dem Management Server registriert. Auf registrierten Maschinen können Backup-Richtlinien verteilt und andere zentrale Verwaltungsaktionen ausgeführt werden. Die Registrierung stellt eine Vertrauensstellung (Trusted Relationship) zwischen dem Agenten auf der Maschine und dem Management Server her.

Aktionen zum Hinzufügen und Importieren sind verfügbar, wenn Sie die Ansicht **Physikalische Maschinen** oder die Gruppe **Alle physikalischen Maschinen** im Navigationsbaum auswählen.

Aktion	Lösung
Eine neue Maschine zum Management Server hinzufügen	Klicken Sie auf **Maschine zum AMS hinzufügen**. Wählen Sie im Fenster **Maschine hinzufügen** (S. 321) die Maschine aus, die dem Management Server hinzugefügt werden soll.
Maschinen aus dem Active Directory importieren	Klicken Sie auf **Maschinen aus dem Active Directory importieren**. Geben Sie im Fenster **Maschinen aus dem Active Directory importieren** (S. 322) die Maschinen oder Organisationseinheiten an, deren Maschinen in den Management Server importiert werden sollen.
Maschinen aus einer Textdatei importieren	Klicken Sie auf **Maschinen aus Datei importieren**. Suchen Sie im Fenster **Maschinen aus Datei importieren** (S. 324) nach einer TXT- oder CSV-Datei, die die Namen (oder IP-Adressen) der Maschinen enthält, die in den Management Server importiert werden sollen.

Die Verwaltungskonsole spricht den Agenten an und löst die Registrierung aus. Da für die Registrierung die Teilnahme des Agenten erforderlich ist, kann diese Aktion nicht ausgeführt werden, wenn die Maschine offline ist.

Ein weiterer Agent, der auf einer registrierten Maschine registriert wird, wird automatisch auch auf demselben Management Server registriert. Mehrere Agenten werden gemeinsam registriert und deregistriert.

Anwenden von Richtlinien

Aktion	Lösung
Eine Backup-Richtlinie auf eine Maschine anwenden	Klicken Sie auf **Backup-Richtlinie anwenden**. Geben Sie im Fenster **Auswahl der Richtlinie** die Backup-Richtlinie an, die Sie auf die ausgewählte Maschine anwenden möchten.

Gruppierungsaktionen

Aktion	Lösung
Eine benutzerdefinierte statische oder dynamische Gruppe erstellen	Klicken Sie auf **Gruppe erstellen**. Geben Sie im Fenster **Gruppe erstellen** (S. 332) die erforderlichen Parameter für die Gruppe an. Die neue Gruppe wird in der Gruppe erstellt, in der die Maschine Mitglied ist (mit Ausnahme der Standardgruppe **Alle physikalischen Maschinen**).
Eine Maschine einer anderen statischen Gruppe hinzufügen	Klicken Sie auf **Zu anderer Gruppe hinzufügen**. Geben Sie im Fenster **Zu Gruppe hinzufügen** (S. 324) die Gruppe an, in die die ausgewählte Maschine kopiert werden soll. Die Backup-Richtlinien, die auf die Gruppen angewendet werden, in denen die Maschine Mitglied ist, werden auf die Maschine angewendet.
Für Maschinen in benutzerdefinierten Gruppen	
Maschinen zu einer statischen Gruppe hinzufügen	Klicken Sie auf **Maschinen zu Gruppe hinzufügen**. Wählen Sie im Fenster **Maschinen zu Gruppe hinzufügen** (S. 325) die Maschinen aus, die hinzugefügt werden sollen.
Eine Maschine in eine andere statische Gruppe verschieben	Klicken Sie auf **Verschieben zu Gruppe**. Wählen Sie im Fenster **Verschieben zu Gruppe** (S. 324) die Gruppe aus, in die die Maschine verschoben werden soll. Alle Backup-Richtlinien, die auf die Gruppe angewendet wurden, in der die Maschine Mitglied war, werden widerrufen. Die Backup-Richtlinien, die auf die Gruppe angewendet werden, in der die Maschine jetzt Mitglied ist, werden auf die Maschine verteilt.
Eine Maschine aus der aktuellen statischen Gruppe entfernen	Klicken Sie auf **Entfernen von Gruppe**. Die Backup-Richtlinien, die für die Gruppe gelten, werden auf der Maschine automatisch widerrufen.

Löschen der ausgewählten Maschine vom Management Server

Aktion	Lösung
Eine Maschine vom Management Server löschen	Klicken Sie auf **Maschine von AMS löschen**. Daraufhin werden die Backup-Richtlinien widerrufen und die Shortcuts zu zentralen Depots von der Maschine gelöscht. Wenn die Maschine aktuell nicht verfügbar ist, werden die Aktionen mit der Maschine ausgeführt, sobald die Maschine wieder für den Management Server verfügbar ist.

Andere Aktionen

Direkte Verwaltungsaktionen	
Einen Backup-Plan auf einer Maschine erstellen	Klicken Sie auf **Backup**. Diese Aktion wird ausführlich im Abschnitt „Einen Backup-Plan erstellen (S. 205)“ beschrieben.
Daten wiederherstellen	Klicken Sie auf **Recovery**. Diese Aktion wird ausführlich im Abschnitt „Daten wiederherstellen“ beschrieben.

Eine Maschine direkt verbinden	Klicken Sie auf **Direkt verbinden.** Stellt eine direkte Verbindung mit der verwalteten Maschine her. Ermöglicht die Administrierung einer verwalteten Maschine und die Ausführung aller direkten Verwaltungsaktionen.
Andere Aktionen	
Detaillierte Informationen zu einer Maschine anzeigen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie im Fenster **Maschinendetails** (S. 325) die Informationen zur Maschine.
Auf einer Maschine vorhandene Tasks anzeigen	Klicken Sie auf **Tasks ansehen**. Die Ansicht **Tasks** (S. 345) wird mit einer Liste der Tasks angezeigt, die auf der Maschine vorhanden sind.
Log-Einträge einer Maschine anzeigen	Klicken Sie auf **Log anzeigen**. Die Ansicht **Log** (S. 347) wird mit einer Liste der Log-Einträge für die Maschine angezeigt.
Aktualisieren aller Maschinen-bezogenen Informationen	Klicken Sie auf **Synchronisieren**. Der Management Server schickt eine Abfrage an die Maschine und aktualisiert die Datenbank mit den neuesten Informationen. Die Liste der virtuellen Maschinen wird bei der Synchronisierung automatisch aktualisiert.
Eine Liste von Maschinen aktualisieren	Klicken Sie auf **Aktualisieren**. Die Verwaltungskonsole aktualisiert die Liste der Maschinen vom Management Server mit den neuesten Informationen. Obwohl die Liste der Maschinen auf der Basis von Ereignissen automatisch aktualisiert wird, kann es sein, dass die Daten aufgrund einer gewissen Verzögerung nicht augenblicklich vom Management Server abgerufen werden. Eine manuelle Aktualisierung garantiert daher, dass auch die allerneusten Daten angezeigt werden.

Eine Maschine dem Management Server hinzufügen

Um Backup-Richtlinien vom Acronis Backup & Recovery 10 Management Server auf eine verwaltete Maschine verteilen und andere zentrale Verwaltungsaktionen ausführen zu können, müssen Sie die Maschine auf dem Management Server registrieren.

So fügen Sie eine Maschine hinzu

1. Im Verzeichnisbaum **Navigation** wählen Sie **Physikalische Maschinen**.
2. Klicken Sie in der Symbolleiste auf **Maschine zum AMS hinzufügen**.
3. Geben Sie im Feld **IP/Name** den Namen oder die IP-Adresse der Maschine ein oder klicken Sie auf **Durchsuchen...** und suchen Sie im Netzwerk nach der Maschine.

   HInweis für Benutzer der Virtual Edition: *Wenn Sie einen VMware ESX/ESXi Host hinzufügen, geben Sie die IP der Virtual Appliance mit laufenden Acronis Backup & Recovery 10 Agent für ESX/ESXi an.*

4. Geben Sie Benutzernamen und Kennwort eines Benutzers ein, der Mitglied der Gruppe **Administrator** auf der Maschine ist.

   HInweis für Benutzer der Virtual Edition: *Wenn Sie einen VMware ESX/ESXi Host hinzufügen, spezifizieren Sie Benutzernamen und Kennwort für den vCenter oder ESX/ESXi Host.*

   Klicken Sie auf **Optionen** und spezifizieren Sie:

- **Benutzername**. Achten Sie bei Eingabe des Namens eines Benutzerkontos für Active Directory darauf, auch den Domain-Namen anzugeben (Domain\Benutzername).
- **Kennwort**. Das Kennwort für das Konto.

Aktivieren Sie das Kontrollkästchen **Kennwort speichern**, um das Kennwort für künftige Verbindungen zu speichern.

5. Klicken Sie auf **OK**.

Maschinenseitige Registrierung auslösen

Die Registration kann auch maschinenseitig ausgelöst werden.

1. Verbinden Sie die Konsole mit der Maschine, auf der Acronis Backup & Recovery 10 Agent installiert ist. Wenn Sie zur Eingabe von Anmeldedaten aufgefordert werden, dann spezifizieren Sie die Anmeldedaten eines Mitglieds der Gruppe der **Administratoren** auf dieser Maschine.
2. Wählen Sie aus dem Menü **Optionen** –> **Optionen der Maschine** –> **Verwaltung der Maschine**.
3. Wählen Sie **Zentrale Verwaltung** und spezifizieren Sie den Management Server, auf dem die Maschine registriert werden soll. Siehe "Verwaltung der Machine (S. 92)" für Details.

Maschinen aus dem Active Directory importieren

So importieren Sie Maschinen aus dem Active Directory

1. Wählen Sie im **Navigationsbaum** den Eintrag  **Physikalische Maschinen** oder  **Alle physikalischen Maschinen**.
2. Klicken Sie in der Symbolleiste auf  **Maschinen aus dem Active Directory importieren**.
3. Geben Sie im Feld **Suchen nach** den Namen der Maschine (oder der Organisationseinheit) ein und klicken Sie dann auf  **Suchen**. Sie können das Sternchen (*) verwenden, um eine beliebige Anzahl von Zeichen im Namen einer Maschine (oder einer Organisationseinheit) zu ersetzen.

   Im linken Teil des Fensters werden die Namen der Maschinen (oder Organisationseinheiten) angezeigt, die vollständig oder teilweise mit dem eingegebenen Wert übereinstimmen. Klicken Sie auf das Element, das Sie für den Import hinzufügen möchten und klicken Sie auf **Hinzufügen>>**. Das Element wird in den rechten Teil des Fensters verschoben. Um alle gefunden Elemente hinzuzufügen, klicken Sie auf **Alle hinzufügen>>**.

   Wenn mehr als 1000 Übereinstimmungen gefunden wurden, werden nur die ersten 1000 Elemente angezeigt. In diesem Fall wird empfohlen, die Suche zu verfeinern und erneut auszuführen.

   Im rechten Teil des Fensters werden die für den Import ausgewählten Elemente angezeigt. Falls erforderlich, entfernen Sie die fälschlicherweise ausgewählten Elemente unter Verwendung der entsprechenden Schaltflächen  **Entfernen** bzw.  **Alle entfernen**.
4. Klicken Sie auf **OK**, um den Importvorgang zu starten.

Synchronisieren von Maschinen mit einer Textdatei

Während der Synchronisierung passt der Management Server die Gruppe **Alle physikalischen Maschinen** entsprechend der als .txt- oder .csv-Datei zur Verfügung gestellten Liste von Maschinen an. Der Management Server:

- Fügt Maschinen aus der Liste hinzu, die nicht registriert sind
- Löscht registrierte Maschinen, die nicht in der Liste enthalten sind
- Löscht registrierte Maschinen aus der Liste, deren derzeitige Verfügbarkeit (S. 325) als **Zurückgezogen** angegeben ist, und versucht, sie erneut hinzuzufügen.

Nun sind nur physikalische Maschinen, die in der Datei aufgelistet sind, in der Gruppe **Alle**

physikalischen Maschinen enthalten.

Anforderungen für die Textdatei

In der Datei sollte eine Maschine pro Zeile jeweils mit ihrem Namen oder ihrer IP-Adresse aufgeführt sein.

Beispiel:

```
Maschinenname_1
Maschinenname_2
192.168.1.14
192.168.1.15
```

Hat die angegebene Datei keinen Inhalt, werden alle physikalischen Maschinen vom Management Server gelöscht.

Eine registrierte Maschine muss über ihre Registrierungsadresse spezifiziert werden, was bedeutet, dass Sie exakt denselben Host-Namen, den 'Fully Qualified Domain Name' (FQDN) oder die IP-Adresse angeben müssen, die verwendet wurden, als die Maschine ursprünglich dem Management Server hinzugefügt wurde. Anderenfalls wird die Maschine gelöscht und erneut so hinzugefügt, als wäre sie eine andere Maschine. Das bedeutet, dass alle Richtlinien, egal ob geerbt oder direkt angewendet, von der Maschine widerrufen werden und dass ihre Mitgliedschaft in der statischen Gruppe verloren geht.

Die Registrierungsadresse einer Maschine kann in der Spalte **Registrierungsadresse** in jeder Management Server-Ansicht gefunden werden, in der die Maschine enthalten ist (standardmäßig ist die Spalte versteckt).

Um Diskrepanzen zu vermeiden, können Sie die Maschinen zu Anfang von einer Textdatei importieren. Modifizieren Sie nach Bedarf diese Datei später durch Hinzufügen oder Entfernen von Maschinen – aber ändern Sie nicht die Namen bzw. Adressen der Maschinen, die registriert bleiben müssen.

So synchronisieren Sie Maschinen mit einer Textdatei

1. Wählen Sie im Verzeichnisbaum **Navigation** den Eintrag **Physikalische Maschinen** oder **Alle physikalischen Maschinen**.
2. Klicken Sie in der Symbolleiste auf **Maschinen mit Textdatei synchronisieren**.
3. Geben Sie im Feld **Pfad** den Pfad zu einer .txt- oder .csv-Datei ein oder klicken Sie auf **Durchsuchen** und wählen Sie dann im Fenster **Durchsuchen** die Datei aus.
4. Geben Sie unter **Anmeldeeinstellungen** Namen und Kennwort eines Benutzers ein, der Mitglied der Gruppe Administratoren für alle in der Datei aufgelisteten Maschinen ist.
5. Wählen Sie **OK**, um die Synchronisation der Maschinen zu starten.

Befehlszeilenwerkzeug zur Synchronisation

Der Acronis Backup & Recovery 10 Management Server verfügt über ein Befehlszeilenwerkzeug, mit dem Sie eine Batch-Datei erstellen können, um den Synchronisations-Task unter Verwendung des Windows Scheduler zu planen.

So synchronisieren Sie Maschinen mit einer Textdatei unter Verwendung der Befehlzeile

1. Melden Sie sich als ein Mitglied der Sicherheitsgruppe **Acronis Centralized Admins** an.
2. Wechseln Sie in der Eingabeaufforderung zu dem Ordner, wo der Acronis Backup & Recovery 10 Management Server installiert wurde – standardmäßig ist das: **C:\Programme\Acronis\AMS**.
3. Führen Sie den folgenden Befehl aus:

```
syncmachines [Pfad_zur_Datei] {Benutzername Kennwort}
```

wobei:

- [Pfad_zur_Datei] der Pfad zu einer .txt- oder .csv-Datei ist, die die Liste der Maschinen enthält. Das Befehlszeilenwerkzeug akzeptiert keine Leerzeichen in der Pfadbezeichnung.
- {Benutzername Kennwort} gehören zu einem Benutzer, der auf allen in der Datei gelisteten Maschinen ein Mitglied der Gruppe 'Administratoren' ist. Wenn nichts angegeben, wird der „Single Sign-on“-Mechanismus verwendet, um auf allen Maschinen Aktionen auszuführen.

Maschinen aus einer Textdatei importieren

So importieren Sie Maschinen aus einer Textdatei

1. Wählen Sie im **Navigationsbaum** den Eintrag **Physikalische Maschinen** oder **Alle physikalischen Maschinen**.
2. Klicken Sie in der Symbolleiste auf **Maschinen aus Datei importieren**.
3. Geben Sie im Feld **Pfad** einen Pfad zu der .txt- oder .csv-Datei ein oder klicken Sie auf **Durchsuchen** und wählen Sie dann im Fenster **Durchsuchen** die Datei aus.

   Eine TXT- oder CSV-Datei sollte die Namen von Maschinen oder ihre IP-Adressen enthalten, wobei die Angaben für jede der Maschinen auf einer neuen Zeile beginnen.

   Beispiel:

   ```
   Maschinenname_1
   Maschinenname_2
   192.168.1.14
   192.168.1.15
   ```
4. Geben Sie unter **Anmeldeeinstellungen** Namen und Kennwort eines Benutzers ein, der Mitglied der Gruppe Administratoren für alle in der Datei aufgelisteten Maschinen ist.
5. Klicken Sie auf **OK**, um den Importvorgang zu starten.

Eine Maschine einer anderen Gruppe hinzufügen

So fügen Sie die ausgewählte Maschine einer anderen Gruppe hinzu

1. Wählen Sie die Gruppe aus, der die Maschine hinzugefügt werden soll.
2. Klicken Sie auf **OK**.

Die hinzugefügte Maschine wird Mitglied von mehr als einer Gruppe. Im Ergebnis verbleiben die Backup-Richtlinien, die auf die erste Gruppe angewendet wurden, auf der Maschine und die Backup-Richtlinien, die auf die zweite, dritte usw. Gruppe angewendet werden, werden auf die Maschine verteilt.

Eine Maschine in eine andere Gruppe verschieben

So verschieben Sie die ausgewählte Maschine in eine andere Gruppe

1. Wählen Sie in der Gruppenstruktur die Gruppe aus, in die die Maschine verschoben werden soll.
2. Klicken Sie auf **OK**.

Die zu verschiebende Maschine verlässt eine Gruppe und wird Mitglied einer anderen Gruppe. Im Ergebnis werden die Backup-Richtlinien, die auf die erste Gruppe angewendet wurden, auf der Maschine widerrufen und die Backup-Richtlinien, die auf die zweite, dritte usw. Gruppe angewendet werden, werden auf die Maschine verteilt.

Maschinen zu einer Gruppe hinzufügen

So fügen Sie der ausgewählten Gruppe Maschinen hinzu

1. Wählen Sie in der Gruppenstruktur die Gruppe, deren Maschinen hinzugefügt werden sollen.
2. Wählen Sie im rechten Teil des Fensters die Maschinen aus.
3. Um weitere Maschinen aus anderen Gruppen hinzuzufügen, wiederholen Sie für jede dieser Gruppen die Schritte 1 und 2.
4. Klicken Sie auf **OK**, um die Maschinen hinzuzufügen.

Sobald die Maschinen in der Gruppe auftauchen, wird die Richtlinie, die auf die Gruppe angewendet wird (falls vorhanden), auf die Maschinen verteilt. Wenn eine der ausgewählten Maschinen nicht verfügbar oder aktuell nicht erreichbar ist, wird die Aktion im Management Server als „Ausstehend“ abgelegt und sie wird ausgeführt, sobald die Maschine für den Server wieder verfügbar ist.

Maschinendetails

Fasst alle Informationen zur ausgewählten Maschine auf vier Registerkarten zusammen. Hier kann der Administrator des Management Servers Aktionen für die Backup-Pläne und Tasks, die auf der Maschine vorhanden sind, sowie für die auf die Maschine angewendeten Richtlinien ausführen.

Diese Informationen sind auch im Bereich **Informationen** verfügbar.

Maschine

Auf dieser Registerkarte werden die folgenden Informationen über registrierte Maschinen angezeigt:

- **Name** – Name der ausgewählten Maschine (wird vom **Computernamen** in Windows bezogen)
- **IP-Adresse** – IP-Adresse der ausgewählten Maschine
- **Status** – Status der Maschine. Wird bestimmt durch den schwerwiegendsten Status (S. 192) aller Backup-Pläne (lokal und zentral), die auf der Maschine vorhanden sind und der Backup-Richtlinien (S. 312), die auf die Maschine angewendet werden.
- **Letzte Verbindung** – Zeit, die vergangen ist, seit der Management Server das letzte Mal mit der Maschine verbunden war.
- **Letztes erfolgreiches Backup** – Zeit, die seit dem letzten erfolgreichen Backup vergangen ist.
- **Verfügbarkeit:**
  - **Online** – Maschine ist für den Management Server verfügbar. Das bedeutet, dass die letzte Verbindung des Management Servers mit der Maschine erfolgreich war. Die Verbindung wird alle 2 Minuten aufgebaut.
  - **Offline** – Maschine ist für den Management Server nicht verfügbar. Sie ist ausgeschaltet oder das Netzwerkkabel ist nicht angeschlossen.
  - **Unbekannt** – Dieser Status besteht nach dem Hinzufügen der Maschine so lange, bis zum ersten Mal eine Verbindung zwischen dem Management Server und der Maschine hergestellt wird oder bis der Dienst des Management Servers gestartet wird.
  - **Zurückgezogen** – Die Maschine wurde auf einem anderen Management Server registriert oder in **Optionen –> Maschinen-Optionen –> Verwaltung der Maschine** (S. 92) wurde der Parameter **Autonome Verwaltung** ausgewählt. In diesem Fall ist es nicht möglich, die Maschine über den aktuellen Management Server zu steuern. Sie können jedoch die Kontrolle über die Maschine zurückerlangen, wenn Sie die Adresse des Management Servers in den Einstellungen für die **Verwaltung der Maschine** angeben.
  - **Abgelaufen** – für den Agenten der Maschine ist der Testzeitraum abgelaufen. Verwenden Sie zur Angabe eines vollständigen Lizenzschlüssels die Funktion **Lizenz ändern** oder führen Sie

das Setup-Programm aus und folgen Sie seinen Anweisungen.

- **Installierte Agenten** – Namen der Acronis-Agenten, die auf der Maschine installiert sind.
- **Betriebssystem** – Betriebssystem, unter dem der Agent der Maschine ausgeführt wird.
- **Prozessor** – CPU-Typ, der in der verwalteten Maschine arbeitet
- **CPU-Clock** – Taktrate der CPU
- **RAM** – Hauptspeichergröße
- **Kommentar** – Beschreibung der Maschine (wird von der **Computerbeschreibung** in Windows bezogen)

Backup-Richtlinien

Zeigt eine Liste von Backup-Richtlinien, die auf die ausgewählte Maschine angewendet wurden und ermöglicht dem Administrator des Management Servers, die folgenden Aktionen auszuführen:

Aktion	Lösung
Details einer Richtlinie anzeigen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie im Fenster **Richtliniendetails** (S. 316) alle Informationen, die sich auf die ausgewählte Backup-Richtlinie beziehen.
Tasks einer Richtlinie anzeigen	Klicken Sie auf **Tasks ansehen**. Die Ansicht **Tasks** (S. 345) wird mit einer Liste der Tasks angezeigt, die sich auf die ausgewählte Backup-Richtlinie beziehen.
Log einer Richtlinie anzeigen	Klicken Sie auf **Log anzeigen**. Die Ansicht **Log** (S. 347) wird mit einer Liste der Log-Einträge angezeigt, die sich auf die ausgewählte Backup-Richtlinie beziehen.
Richtlinie auf der Maschine widerrufen	Klicken Sie auf **Widerrufen**. Der Management Server wird die Richtlinie auf der Maschine widerrufen. Die Richtlinie selbst verbleibt auf dem Management Server. Für den Fall, dass die Maschine Mitglied einer Gruppe ist und dass die Richtlinie auf die Gruppe angewendet wird, können Sie die Richtlinie auf einer einzelnen Maschine nur widerrufen, wenn Sie vorher die Maschine aus der Gruppe entfernen.
Überprüfen, woher die angewendete Richtlinie kam	Klicken Sie auf **Vererbung durchsuchen**. Im Fenster **Vererbungsabfolge** (S. 330) wird die Vererbungsabfolge der Richtlinie angezeigt, die auf die Maschine angewendet wurde.

Filtern und Sortieren

Das Filtern und Sortieren der Backup-Richtlinien erfolgt auf die gleiche Weise wie für die Ansicht **Backup-Richtlinien**. Weitere Informationen finden Sie im Abschnitt „Backup-Richtlinien filtern und sortieren (S. 316)“.

Pläne und Tasks

Zeigt eine Liste der (lokalen und zentralen) Pläne sowie der Tasks an, die auf der ausgewählten Maschine vorhanden sind.

Aktionen

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

Aktion	Lösung
Details eines Plans/Tasks einsehen	**Backup-Plan** Klicken Sie auf **Details anzeigen**. Überprüfen Sie dann im Fenster **Plan-Details** (S. 201) die entsprechenden Informationen. **Task** Klicken Sie auf **Details anzeigen**. Überprüfen Sie dann im Fenster **Task-Details** (S. 199) die entsprechenden Informationen.
Ereignisanzeige für Pläne/Tasks einsehen	**Backup-Plan** Klicken Sie auf **Log anzeigen**. Sie gelangen dadurch in die Ansicht **Log** (S. 202), die eine Liste der planbezogenen Log-Einträge enthält. **Task** Klicken Sie auf **Log anzeigen**. Sie gelangen dadurch in die **Log** (S. 202)-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. 199) den Task, den Sie ausführen müssen. Die Ausführung des Backup-Plans startet unmittelbar auch den dazugehörigen, ausgewählten Task, ungeachtet seiner Zeit-/Ereignis-Einstellungen und anderer Konditionen. **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. Abhängig davon, wann Sie den Task gestoppt haben, werden manche Dateien wiederhergestellt, andere hingegen nicht. 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. 205), mit Ausnahme folgender **Einschränkungen**: Es ist nicht immer möglich, die Eigenschaften eines Backup-Schemas zu ändern, 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 die bereits existierenden 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. ▪ 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.

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. ▪ 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.
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.

Filtern und Sortieren

Das Filtern und Sortieren der Backup-Richtlinien erfolgt auf die gleiche Weise wie in der Ansicht **Backup-Pläne und Tasks** für die direkte Verwaltung. Weitere Informationen finden Sie im Abschnitt „Backup-Pläne und Tasks filtern und sortieren (S. 198)“.

Mitglied von

Diese Registerkarte wird nur angezeigt, wenn die ausgewählte Maschine Mitglied einer oder mehrerer benutzerdefinierter Gruppen ist. Auf der Registerkarte wird eine Liste der Gruppen angezeigt, in denen die Maschine Mitglied ist.

Aktionen

Aktion	Lösung
Details einer Gruppe anzeigen	Klicken Sie auf **Details anzeigen**. Sie gelangen zum Fenster „Gruppendetails“. Dort können Sie alle Informationen in Bezug auf diese Gruppe überprüfen.
Tasks in Bezug auf eine Gruppe anzeigen	Klicken Sie auf **Tasks ansehen**. Sie gelangen zur Ansicht „Tasks“. In dieser werden die vorgefilterten Tasks

	angezeigt, die sich auf die ausgewählte Backup-Gruppe beziehen.
Log in Bezug auf eine Gruppe anzeigen	Klicken Sie auf **Log anzeigen**. Dies öffnet die Ansicht „Log“ mit vorgefilterten Log-Einträgen für die ausgewählte Gruppe.
Eine Maschine aus einer Gruppe entfernen	Klicken Sie auf **Entfernen**. Die zentralen Pläne, die an die übergeordnete Gruppe verteilt wurden, wirken sich nicht länger auf diese Maschine aus.

Gehostete virtuelle Maschinen

Auf diesem Reiter wird eine Liste der Maschinen angezeigt, die auf dem ausgewählten Virtualisierungsserver gehostet oder von der angegebenen Virtual Appliance verwaltet werden.

Auf Basis dieser Liste von gehosteten, virtuellen Maschinen können Sie eine dynamische Gruppe erstellen. Dazu klicken Sie auf **Dynamische Gruppe erstellen**. Auf die erstellte Gruppe können Sie in der Virtuelle Maschinen-Ansicht (S. 337) zugreifen.

Vererbungsabfolge

Im Fenster **Vererbungsabfolge** können Sie überprüfen, woher die Richtlinie kam, die auf die Maschine angewendet wurde.

Die Richtlinie, die direkt auf die Maschine angewendet wurde, wird wie folgt angezeigt:
Maschinenname

Die Richtlinie, die infolge von Vererbung auf die Maschine angewendet wird, wird wie im folgenden Beispiel angezeigt:
Gruppe1 –> **Gruppe2** –> Gruppe3 –> Maschine1

Gruppe1 in der Wurzel enthält *Gruppe2*, auf die die Richtlinie direkt angewendet wird. *Gruppe2* enthält ihrerseits die untergeordnete *Gruppe3*, die die Richtlinie von der übergeordneten Gruppe erbt, und wendet die Richtlinie auf *Maschine1* an.

Die Maschine (oder Gruppe), auf die die Richtlinie direkt angewendet wurde, wird fettgedruckt angezeigt und mit einem Symbol gekennzeichnet.

Alle Elemente sind interaktiv. Wenn Sie also auf eine Maschine oder eine Gruppe klicken, wird die Ansicht mit deren übergeordneter Gruppe geöffnet.

Maschinen filtern und sortieren

Aktion	Lösung
Maschinen nach einer beliebigen Spalte sortieren	Klicken Sie auf die Spaltenüberschriften, um die Maschinen in aufsteigender Reihenfolge zu sortieren. Kicken Sie erneut auf die Spaltenüberschrift, um die Maschinen in absteigender Reihenfolge zu sortieren.
Maschinen nach Name filtern	Geben Sie den Namen einer Maschine in das Feld unter der entsprechenden Spaltenüberschrift ein. Sie erhalten als Ergebnis eine Liste von Maschinen, deren Name vollständig oder teilweise mit dem eingegebenen Wert übereinstimmt.

Maschine nach Status, letzter Verbindung, letztem Backup oder Verfügbarkeit filtern.	Wählen Sie in einem Feld unter der entsprechenden Spaltenüberschrift den benötigten Wert aus der Liste.

Maschinentabelle konfigurieren

Standardmäßig werden in der Tabelle fünf 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.

Aktionen für Gruppen

Aktionen sind verfügbar, wenn Sie die Ansicht **Physikalische Maschinen** im **Navigationsbaum** auswählen und dann auf eine Gruppe klicken.

Nachfolgend finden Sie eine Anleitung zur Ausführung von Aktionen auf gewählte Gruppen.

Aktion	Lösung
Eine benutzerdefinierte statische oder dynamische Gruppe erstellen	Klicken Sie auf **Gruppe erstellen**. Geben Sie im Fenster **Gruppe erstellen** (S. 332) die erforderlichen Parameter für die Gruppe an. Benutzerdefinierte Gruppen können im Stammordner (**Physikalische Maschinen**) oder in anderen benutzerdefinierten Gruppen erstellt werden.
Eine Backup-Richtlinie auf eine Gruppe anwenden	Klicken Sie auf **Backup-Richtlinie anwenden**. Geben Sie im Fenster **Auswahl der Richtlinie** die Backup-Richtlinie an, die Sie auf die ausgewählte Gruppe anwenden möchten. Wenn es in der ausgewählten Gruppe Untergruppen gibt, wird die Backup-Richtlinie auch auf diese angewendet.
Detaillierte Informationen zu einer Gruppe anzeigen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie im Fenster **Gruppendetails** (S. 334) die Informationen zur ausgewählten Gruppe.
Eine benutzerdefinierte Gruppe/Untergruppe umbenennen	Klicken Sie auf **Umbenennen**. Geben Sie in der Spalte **Name** einen neuen Namen für die ausgewählte Gruppe ein. Standardgruppen können nicht umbenannt werden.
Eine benutzerdefinierte Gruppe bearbeiten	Klicken Sie auf **Bearbeiten**. Ändern Sie im Fenster **Gruppe bearbeiten** (S. 334) die erforderlichen Parameter für die Gruppe.
Eine benutzerdefinierte Gruppe in eine andere verschieben	Klicken Sie auf **Verschieben nach**. Geben Sie im Fenster **Verschieben zu Gruppe** (S. 334) eine Gruppe an, die die neue übergeordnete Gruppe für die ausgewählte Gruppe wird.

Eine benutzerdefinierte Gruppe löschen	Klicken Sie auf **Löschen**. Beim Löschen einer übergeordneten Gruppe werden auch deren Untergruppen gelöscht. Backup-Richtlinien, die auf die übergeordnete Gruppe angewendet und von deren Untergruppen geerbt wurden, werden für alle Mitglieder der gelöschten Gruppen widerrufen. Die Richtlinien, die direkt auf die Mitglieder angewendet werden, bleiben bestehen.
Eine Liste von Gruppen aktualisieren	Klicken Sie auf **Aktualisieren**. Die Verwaltungskonsole aktualisiert die Liste der Gruppen vom Management Server mit den neuesten Informationen. Obwohl die Liste der Gruppen auf der Basis von Ereignissen automatisch aktualisiert wird, kann es sein, dass die Daten aufgrund einer gewissen Verzögerung nicht augenblicklich vom Management Server abgerufen werden. Eine manuelle Aktualisierung garantiert daher, dass auch die allerneuesten Daten angezeigt werden.

Eine benutzerdefinierte statische oder dynamische Gruppe erstellen

So erstellen Sie eine Gruppe

1. Geben Sie im Feld **Gruppenname** einen Namen für die zu erstellende Gruppe ein.
2. Wählen Sie den Typ der Gruppe:
   a. **Statisch** – zum Erstellen einer Gruppe, die Maschinen enthält, die manuell hinzugefügt werden.
   b. **Dynamisch** – zum Erstellen einer Gruppe, die Maschinen enthält, die entsprechend der angegebenen Kriterien automatisch hinzugefügt werden.

      Klicken Sie auf **Kriterien hinzufügen** und wählen Sie das Kriterienmuster aus.

      - **Betriebssystem**

        Alle Maschinen, auf denen das ausgewählte Betriebssystem ausgeführt wird, werden zu Mitgliedern der dynamischen Gruppe.
      - **Organisationseinheit** (S. 333)

        Alle Maschinen, die zur angegebenen Organisationseinheit gehören, werden zu Mitgliedern der dynamischen Gruppe.
      - **IP-Adressbereich**

        Alle Maschinen, deren IP-Adressen in dem angegeben IP-Bereich liegen, werden zu Mitgliedern der dynamischen Gruppe.
      - **In txt/csv-Datei aufgelistet** (S. 333)

        Alle Maschinen, die in der angegebenen .txt- oder .csv-Datei aufgelistet sind, werden zu Mitgliedern der dynamischen Gruppe.
3. Geben Sie im Feld **Kommentar** eine Beschreibung der erstellten Gruppe ein.
4. Klicken Sie auf **OK**.

Multiple Kriterien hinzufügen

Durch das Hinzufügen von multiplen Kriterien wird ein Zustand entsprechend der folgenden Regeln geschaffen:

a) Alle Einträge des gleichen Kriteriums werden durch logische Addition (ODER) miteinander verknüpft.

Z.B. werden durch die Kriterienmenge

Betriebssystem: Windows Server 2008

Betriebssystem: Windows Server 2003

alle Maschinen derselben Gruppe hinzugefügt, auf denen das Betriebssystem Windows 2000 ODER Windows 2003 ausgeführt wird.

b) Einträge für unterschiedliche Kriterien werden durch logische Multiplikation (UND) miteinander verknüpft

Z.B. werden durch die Kriterienmenge

Betriebssystem:	Windows Server 2008
Betriebssystem:	Windows Server 2003
Organisationseinheit:	SERVER
IP-Bereich:	192.168.17.0 - 192.168.17.55

alle Maschinen derselben Gruppe hinzugefügt, auf denen das Betriebssystem Windows 2000 oder Windows 2003 ausgeführt wird, die aber außerdem zur Organisationseinheit SERVER gehören und deren IP-Adressen im Bereich 192.168.17.0 – 192.168.17.55 liegen.

Wie lange verbleibt das Mitglied einer dynamischen Gruppe in der Gruppe?

Das Mitglied einer dynamischen Gruppe verbleibt in der Gruppe, solange es die entsprechenden Kriterien erfüllt. Das Mitglied wird automatisch aus der Gruppe entfernt, sobald

- sich das Mitglied so ändert, dass es nicht länger die Kriterien erfüllt
- der Administrator die Kriterien so ändert, dass das Mitglied 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.

Kriterium „Organisationseinheit“

Das Kriterium „Organisationseinheit“ wird für die Domain, zu der der Management Server aktuell gehört, wie folgt spezifiziert: *OU=OU1*

Wählen Sie eine organisatorische Einheit im Active Directory durch einen Klick auf **Durchsuchen** oder durch manuelle Eingabe. Wenn die Anmeldedaten für die Domänen in den Optionen des Management Servers nicht angegeben wurden, wird das Programm danach fragen. Die Anmeldedaten werden unter Domänen-Zugriffsberechtigungen (S. 90) gespeichert.

Ein Beispiel: Angenommen, die Domain *us.corp.example.com* hat OU1 (befindet sich im Stammverzeichnis), OU1 hat OU2 und OU2 hat OU3. Und Sie müssen die Maschinen von OU3 hinzufügen. Das Kriterium wird daher sein: *OU=OU3, OU=OU2, OU=OU1*

Falls OU3 „Child Container“ hat und Sie die Maschinen dieser Container ebenfalls der Gruppe hinzufügen müssen, dann aktivieren Sie das Kontrollkästchen **Child Container einschließen**.

Kriterium 'In txt/csv-Datei aufgelistet'

Wenn Sie dieses Kriterium verwenden, beinhaltet die dynamische Gruppe die in der .txt- oder .csv-Datei aufgelisteten Maschinen.

Wenn Sie die Datei später verändern, ändert sich der Inhalt der Gruppe entsprechend. Die Datei wird alle 15 Minuten geprüft.

Wenn Sie die Datei später löschen, oder sie nicht mehr verfügbar ist, entspricht der Inhalt der Gruppe der letzten Version der Liste, die in der Datei gespeichert war.

Anforderungen für die Textdatei

In der Datei sollte eine Maschine pro Zeile jeweils mit ihrem Namen oder ihrer IP-Adresse aufgeführt sein.

Beispiel:

```
Maschinenname_1
Maschinenname_2
192.168.1.14
192.168.1.15
```

Eine registrierte Maschine muss über ihre Registrierungsadresse spezifiziert werden, was bedeutet, dass Sie exakt denselben Host-Namen, den 'Fully Qualified Domain Name' (FQDN) oder die IP-Adresse angeben müssen, die verwendet wurden, als die Maschine ursprünglich dem Management Server hinzugefügt wurde. Anderenfalls wird die Maschine der Gruppe nicht hinzugefügt. Die Registrierungsadresse einer Maschine kann in der Spalte **Registrierungsadresse** in jeder Management Server-Ansicht gefunden werden, in der die Maschine enthalten ist (standardmäßig ist die Spalte versteckt).

Eine Gruppe in eine andere verschieben

So verschieben Sie die ausgewählte Gruppe in eine andere Gruppe oder an die Wurzel

1. Klicken Sie in der Gruppenstruktur auf die Gruppe, in die die ausgewählte Gruppe verschoben werden soll. Sie können eine beliebige benutzerdefinierte Gruppe (statisch oder dynamisch) in eine andere benutzerdefinierte Gruppe eines beliebigen Typs oder an die Wurzel verschieben.

   Die Wurzel der Maschinenstruktur enthält *Gruppen der ersten Ebene*. Gruppen, die andere Gruppen enthalten, werden *übergeordnete Gruppen* genannt. Gruppen, die sich in übergeordneten Gruppen befinden, werden *Untergruppen* genannt. Alle Backup-Richtlinien, die auf die übergeordnete Gruppe angewendet werden, werden auch auf die Untergruppen angewendet.
2. Klicken Sie auf **OK**.

Benutzerdefinierte Gruppen bearbeiten

Die Bearbeitung einer benutzerdefinierten Gruppe wird auf die gleiche Weise ausgeführt wie die Erstellung (S. 332).

Die Änderung des Typs einer Gruppe führt dazu, dass diese konvertiert wird. Jede benutzerdefinierte Gruppe kann in eine dynamische Gruppe konvertiert werden, wenn sie vorher statisch war, und umgekehrt.

- Geben Sie bei der Konvertierung einer statischen Gruppe in eine dynamische Gruppe die Gruppierungskriterien an. Alle Mitglieder in der statischen Gruppe, die die angegebenen Kriterien nicht erfüllen, werden aus der dynamischen Gruppe entfernt.
- Für die Konvertierung einer dynamischen Gruppe in eine statische Gruppe sind zwei Optionen verfügbar – Sie können entweder den aktuellen Inhalt der Gruppe beibehalten oder die Gruppe leeren.

Gruppendetails

Fasst alle Informationen zur ausgewählten Gruppe auf zwei Registerkarten zusammen. Ermöglicht die Ausführung von Aktionen für die Richtlinien, die auf die Gruppe angewendet werden.

Diese Informationen sind auch im Bereich **Informationen** verfügbar.

Gruppe

Zeigt die folgenden Informationen über die Gruppe:

- **Name** – Name der ausgewählten Gruppe
- **Übergeordnete Gruppe** (nur für Untergruppen) – Name der übergeordneten Gruppe
- **Maschinen** – Zahl der Maschinen in der Gruppe
- **Typ** – Typ der Gruppe (statisch oder dynamisch)
- **Kriterien** (nur für dynamische Gruppen) – Gruppierungskriterien
- **Kommentar** – Gruppenbeschreibung (wenn vorhanden)

Backup-Richtlinien

Zeigt eine Liste der Backup-Richtlinien, die sich auf die Gruppe beziehen und ermöglicht die Ausführung folgender Aktionen:

Aktion	Lösung
Details einer Richtlinie anzeigen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie im Fenster Richtliniendetails (S. 316) alle Informationen, die sich auf die ausgewählte Backup-Richtlinie beziehen.
Tasks einer Richtlinie anzeigen	Klicken Sie auf **Tasks ansehen**. Die Ansicht Tasks (S. 345) wird mit einer Liste der Tasks angezeigt, die sich auf die ausgewählte Backup-Richtlinie beziehen.
Log einer Richtlinie anzeigen	Klicken Sie auf **Log anzeigen**. Die Ansicht Log (S. 347) wird mit einer Liste der Log-Einträge angezeigt, die sich auf die ausgewählte Backup-Richtlinie beziehen.
Richtlinie auf der Gruppe widerrufen	Klicken Sie auf **Widerrufen**. Der Management Server widerruft die Richtlinie auf der Gruppe. Während die Änderungen an die Maschinen übertragen werden und die Agenten die Backup-Pläne löschen, ist das Richtlinienstadium für die Gruppe **Wird widerrufen**. Die Richtlinie selbst verbleibt auf dem Management Server.
Überprüfen, woher die auf die Gruppe angewendete Richtlinie kam	Klicken Sie auf **Vererbung durchsuchen**. Im Fenster **Vererbungsabfolge** (S. 335) wird die Vererbungsabfolge der Richtlinie angezeigt, die auf die Gruppe angewendet wurde.

Filtern und Sortieren

Das Filtern und Sortieren der Backup-Richtlinien erfolgt auf die gleiche Weise wie für die Ansicht „Backup-Richtlinien“. Weitere Informationen finden Sie im Abschnitt „Backup-Richtlinien filtern und sortieren (S. 316)“.

Vererbungsabfolge

Im Fenster **Vererbungsabfolge** können Sie überprüfen, woher die Richtlinie kam, die auf die Gruppe angewendet wurde.

Die Richtlinie, die direkt auf die Gruppe angewendet wird, wird wie folgt angezeigt:
Gruppenname

Das folgende Beispiel veranschaulicht, wie die Richtlinie angezeigt wird, die infolge von Vererbung

auf die Maschine angewendet wird.
Gruppe1 –> **Gruppe2** –> Gruppe3

Gruppe1 in der Wurzel enthält *Gruppe2*, auf die die Richtlinie direkt angewendet wird. *Gruppe2* enthält ihrerseits die untergeordnete *Gruppe3*, die die Richtlinie von der übergeordneten Gruppe erbt.

Die Gruppe, auf die die Richtlinie direkt angewendet wurde, wird fettgedruckt angezeigt und mit einem Symbol gekennzeichnet.

Alle Elemente sind interaktiv. Wenn Sie also auf eine Gruppe klicken, wird die Ansicht mit deren übergeordneter Gruppe geöffnet.

7.1.4 Virtuelle Maschinen

Sie können virtuelle Maschinen unter Verwendung einer oder beider der folgenden Methoden zentral verwalten:

Hinzufügen einer virtuellen Maschine als physikalische Maschine

Installieren Sie den Agenten für Windows oder den Agenten für Linux in Acronis Backup & Recovery 10 auf der virtuellen Maschine und registrieren (S. 321) Sie ihn auf dem Management Server. Die virtuelle Maschine wird wie eine physikalische Maschine behandelt. Sie wird unter **Maschinen mit Agenten** in der Gruppe **Alle Maschinen mit Agenten** erscheinen.

Dieser Ansatz ist für folgende Situationen geeignet:

- Die Maschine wird nicht auf einem Virtualisierungsserver gehostet.
- Sie haben keine Lizenz für die Acronis Backup & Recovery 10 Virtual Edition.
- Die Virtual Edition unterstützt keine Backups auf Hypervisor-Ebene für dieses spezielle Virtualisierungsprodukt.
- Sie müssen Beschränkungen bei Backups auf Hypervisor-Ebene überwinden.

Hinzufügen einer virtuellen Maschine als virtuelle Maschine

Auf dem Acronis Backup & Recovery 10 Management Server wird eine Maschine als virtuell angesehen, wenn das Backup vom Virtualisierungshost erstellt werden kann, ohne dass ein Agent auf der Maschine installiert werden muss. Dies ist möglich, wenn Sie die Acronis Backup & Recovery 10 Advanced Server Virtual Edition verwenden.

Es gibt verschiedene Arten, wie Sie eine virtuelle Maschine zum Management Server hinzufügen können:

- Aktivieren Sie die Integration (S. 91) des Management Servers mit dem vCenter-Server.

  Ergebnis: Die vom vCenter-Server verwalteten virtuellen Maschinen erscheinen unter **Virtuelle Maschinen** in der Gruppe **Alle virtuellen Maschinen**. Die Maschinen sehen wie unverwaltet aus (sind ausgegraut), können jedoch gesichert werden, falls während der Integration die Funktion zum automatischen Deployment des Agenten aktiviert wurde.
- Installieren und konfigurieren Sie den Agenten für ESX(i) VMware vSphere (Virtuelle Appliance) oder den Agenten für ESX(i) VMware vSphere (Windows). Registrieren Sie den Agenten auf dem Management Server.

  Ergebnis: Die Maschine mit dem Agenten (die virtuelle Appliance oder der Windows-Host) erscheint unter **Maschinen mit Agenten** in der Gruppe **Alle Maschinen mit Agenten**. Die vom Agenten verwalteten virtuellen Maschinen erscheinen unter **Virtuelle Maschinen** in der Gruppe

Alle virtuellen Maschinen.

- Installieren Sie den Agenten für Hyper-V auf einem Hyper-V-Host oder auf allen Knoten eines Hyper-V-Clusters. Registrieren Sie den/die Agenten auf dem Management Server.

  Ergebnis: Der Hyper-V-Host (Knoten) erscheint unter **Maschinen mit Agenten** in der Gruppe **Alle Maschinen mit Agenten**. Die von dem/den Agenten verwalteten virtuellen Maschinen erscheinen unter **Virtuelle Maschinen** in der Gruppe **Alle virtuellen Maschinen**.

Virtuelle Maschinen, die zum Management Server als virtuelle Maschinen hinzugefügt wurden, sind im Verzeichnisbaum **Navigation** unter **Virtuelle Maschinen** präsent. Dieser Abschnitt beschreibt die für diese Maschinen verfügbaren Aktionen.

Virtuelle Maschinen auf einem Management Server

Verfügbarkeit virtueller Maschinen

Virtuelle Maschinen werden als verfügbar angezeigt, wenn der Agent für den Management Server verfügbar ist und außerdem die Maschinen für den Agenten verfügbar sind. Die Liste der virtuellen Maschinen wird dynamisch jedes Mal aktualisiert, wenn sich der Management Server mit den Agenten synchronisiert.

Wenn der Virtualisierungs-Server oder die Virtual Appliance nicht mehr verfügbar sind oder zurückgezogen werden, dann werden die virtuellen Maschinen ausgegraut.

Wenn virtuelle Maschinen für einen Agenten nicht mehr verfügbar sind (dies geschieht, wenn Maschinen aus dem Bestand des Virtualisierungs-Servers entfernt oder vom Datenträger gelöscht werden oder wenn der Storage des Servers nicht eingeschaltet oder getrennt ist), dann verschwinden die Maschinen aus der Gruppe **Alle virtuellen Maschinen** sowie aus anderen Gruppen, in denen sie enthalten sind. Tasks, mit denen ein Backup dieser virtuellen Maschinen erstellt wird, schlagen fehl und es erfolgt ein entsprechender Eintrag im Log. Das hat zur Folge, dass die Erstellungsrichtlinie in den Status Fehler wechselt.

Ob sich eine virtuelle Maschine im Online- oder Offline-Stadium befindet, hat keinen Einfluss auf das Backup, da Backups für virtuelle Maschinen in beiden Fällen erstellt werden können.

Richtlinien für virtuelle Maschinen

Richtlinien, mit denen Backups von Festplatten und Volumes erstellt werden können, können auf virtuelle Maschinen ebenso wie auf physikalische Maschinen angewendet werden. Richtlinien, mit denen Backups auf Datei-Ebene ausgeführt werden, können nicht auf virtuelle Maschinen angewendet werden. Weitere Informationen zu Backups und zur Wiederherstellung virtueller Maschinen, zu unterstützten Gast-Betriebssystemen und zu Datenträgerkonfigurationen finden Sie unter „Backup von virtuellen Maschinen erstellen“.

Anwenden einer Richtlinie auf eine Gruppe virtueller Maschinen

Für jede Maschine wird durch einen separaten Task ein Backup in einem separaten Archiv erstellt. Der Standardname des Archivs enthält den Namen der virtuellen Maschine sowie den Namen der Richtlinie. Es wird empfohlen, den Standardnamen des Archivs beizubehalten, damit die Backups der einzelnen Maschinen im Speicherdepot leicht zu finden sind.

Gruppierung von virtuellen Maschinen

Der Abschnitt **Virtuelle Maschinen** des Navigationsbaums enthält eine Standardgruppe mit dem Namen **Alle virtuellen Maschinen**. Sie können diese Gruppe manuell nicht ändern, löschen oder verschieben. Sie können auf diese Gruppe Richtlinien anwenden, mit denen Backups von Festplatten oder Volumes erstellt werden.

Sie können statische und dynamische Gruppen von virtuellen Maschinen erstellen. Jede virtuelle Maschine, die aktuell verfügbar ist, kann einer statischen Gruppe hinzugefügt werden. Sie können keine Gruppen erstellen, die gleichzeitig physikalischen und virtuelle Maschinen enthalten.

Für die Mitgliedschaft von virtuellen Maschinen in dynamischen Gruppen gelten folgende Kriterien:

- **Typ des Virtualisierungs-Servers (Hyper-V, ESX/ESXi).**

Mit diesem Kriterium können Sie eine dynamische Gruppe von virtuellen Maschinen erstellen, die auf allen registrierten Servern vom Typ Hyper-V (bzw. ESX/ESXi) gehostet werden. Jede Maschine, die diesen Servern hinzugefügt wird, erscheint in dieser Gruppe. Jede Maschine, die aus diesen Servern gelöscht wird, verschwindet aus dieser Gruppe.

- **Host/VA**

Mit diesem Kriterium können Sie eine dynamische Gruppe von virtuellen Maschinen erstellen, die auf einem angegebenen Virtualisierungs-Server gehostet oder von der angegebenen Virtual Appliance verwaltet werden.

VMware vCenter-Integration

Wenn Sie VMware vSphere verwenden, sollten Sie den Management Server mit Ihrem vCenter Server integrieren.

So integrieren Sie den Management Server mit einem VMware vCenter Server:

1. Klicken Sie im Verzeichnisbaum **Navigation** mit der rechten Maustaste auf **Virtuelle Maschinen** und wählen Sie anschließend **VMware vCenter-Integration**.
2. Klicken Sie auf **Integration konfigurieren**
3. Aktivieren Sie das Kontrollkästchen **VMware vCenter-Integration aktivieren**
4. Spezifizieren Sie die IP-Adresse oder den Namen des vCenter Servers und stellen Sie die Anmeldedaten für den Zugriff auf den Server zur Verfügung
5. Klicken Sie auf **OK**

Infolgedessen erscheint auf dem Management Server unter **Virtuelle Maschinen** eine Gruppe mit gleichem Namen wie der vCenter Server. Zu weiteren Informationen siehe „VMware vCenter-Integration (S. 91)“.

So entfernen Sie die Integration mit einem VMware vCenter Server:

1. Klicken Sie im Verzeichnisbaum **Navigation** mit der rechten Maustaste auf **Virtuelle Maschinen** und wählen Sie anschließend **VMware vCenter-Integration**.
2. Klicken Sie auf **Integration konfigurieren**
3. Deaktivieren Sie das Kontrollkästchen **VMware vCenter-Integration aktivieren**
4. Klicken Sie auf **OK**

Die Gruppe, die den gleichen Namen wie der vCenter Server hat, wird entfernt und auf diese Gruppe (oder Untergruppen von dieser) angewendete Richtlinien werden widerrufen.

Virtuelle Maschinen, deren Host durch einen Agenten für ESX/ESXi verwaltet wird, verbleiben in der Gruppe **Alle virtuelle Maschinen** wie auch in anderen Gruppen. Richtlinien, die auf diese Gruppen oder direkt auf diese Maschinen angewendet wurden, bleiben weiterhin funktionell auf diesen Maschinen. Auf diese Art werden durch Entfernung der Integration nur Maschinen entfernt, die nicht verwaltbar sind.

Deployment und Aktualisierung des Agenten für ESX/ESXi

Der Acronis Backup & Recovery 10 Management Server stellt eine einfache Möglichkeit zur

Verfügung, um den Agenten für ESX/ESXi zu jedem VMware ESX- oder ESXi-Server zu verteilen, dessen virtuelle Maschinen Sie per Backup sichern wollen.

Auf jedem von Ihnen spezifizierten und auf dem Management Server registrierten ESX/ESXi-Server wird eine Virtual Appliance mit dem Agenten erstellt. Die virtuellen, auf ihrem Host dynamisch gruppierten Maschinen erscheinen auf dem Management Server, worauf Sie in der Lage sind, auf diese virtuellen Maschinen Backup-Richtlinien anzuwenden oder jede Maschine individuell per Backup zu sichern.

Ein Update bereits installierter Agenten wird auf dieselbe Art durchgeführt wie ein Deployment. Bei Auswahl eines Hosts oder Clusters, auf dem der Agent installiert ist, wird Ihnen eine Aktualisierung des Agenten auf diesem Host angeboten.

Wenn Sie VMware vSphere verwenden, sollten Sie den Management Server mit Ihrem vCenter-Server integrieren (S. 338), bevor Sie mit dem Deployment des Agenten beginnen. In diesem Fall müssen Sie nicht jeden Host manuell spezifizieren.

So verteilen Sie den Agenten für ESX/ESXi auf VMware ESX/ESXi-Server:

1. Klicken Sie im Verzeichnisbaum **Navigation** mit der rechten Maustaste auf **Virtuelle Maschinen** oder klicken Sie mit der rechten Maustaste auf diejenige Gruppe, die denselben Namen wie der vCenter-Server hat.
2. Klicken Sie auf **ESX-Agent verteilen**.
3. **ESX/ESXi-Hosts**

   Bei einem vCenter-Server wird eine Liste der ESX/ESXi-Hosts und -Cluster angezeigt, die vom vCenter-Server eingeholt wurde. Wählen Sie die Hosts und Cluster, auf die der Agent verteilt werden soll oder aktivieren Sie das Kontrollkästchen **Alle markieren**.

   In einem vCenter-Cluster sichert ein einzelner Agent für ESX/ESXi die virtuellen Maschinen, die auf allen Hosts des Clusters vorgehalten werden. Weitere Informationen finden Sie unter „Unterstützung für vCenter-Cluster (S. 341)“.

   Sie können einen einzelnen Host durch Angabe seiner IP-Adresse oder seines Namens der Liste hinzufügen. Geben Sie für jeden Host, den Sie zu der Liste hinzufügen, einen Benutzernamen und Kennwort an. In diesem Fenster kann kein vCenter-Server angegeben werden.

   Wenn Sie einen Host oder Cluster wählen, wo der Agent bereits installiert vorliegt, zeigt der rechte Bereich des Fensters **ESX-Agenten verteilen** Folgendes an: **ESX-Agent auf diesem Host aktualisieren**. Andere Einstellungen sind nicht verfügbar. Falls Sie nur das Update benötigen, fahren Sie direkt mit Schritt Nr. 6 fort.
4. [Optional] **Die Einstellungen des Agenten**

   Sie können beim Deployment der Agenten für ESX/ESXi Standardeinstellungen oder benutzerdefinierte Einstellungen für jeden Agenten verwenden. Die Einstellungen sind wie folgt:

   Datenspeicher: Der Datenspeicher auf dem ESX/ESXi-Host, auf dem die Virtual Appliance gespeichert wird. Beim Deployment des Agenten auf einen vCenter-Cluster ist dies der Datenspeicher, der von allen im Cluster enthaltenen Servern gemeinsam genutzt wird. Weitere Informationen finden Sie unter „Unterstützung für vCenter-Cluster (S. 341)“.

   Netzwerkschnittstelle: Internes Netzwerk des Hosts, in das die Virtual Appliance eingebunden wird. Wenn es mehrere Netzwerke auf dem Host gibt, wählt das Programm dasjenige, welches besser zur Agenten-Ausführung geeignet ist und spezifiziert dieses Netzwerk als **Standard**. Es stehen nur solche Netzwerke zur Auswahl zur Verfügung, die eine Verbindung zur 'Service Console' des Hosts (oder zum 'Management Network' in Bezug auf die VMware Infrastructure) haben. Das ist entscheidend für die Ausführung des Agenten.

   Die nächste Einstellung erscheint unterschiedlich, abhängig davon, wie Sie das Deployment des

Agenten durchführen werden.

Bei Deployment durch den vCenter-Server – **Das Konto, das zur Verbindung des Agenten mit dem vCenter-Server verwendet wird.**

Bei direktem Deployment zum ESX/ESXi-Server – **Das Konto, das zur Verbindung des Agenten mit dem ESX-Server verwendet wird.**

Der Management Server verwendet dieses Konto zum Aufbau einer Vertrauensstellung (Trusted Relationship) mit dem Agenten während der Registrierung. Zentrale Backup-Pläne und Recovery-Tasks, die vom Management Server stammen, werden standardmäßig unter diesem Konto ausgeführt. Was bedeutet, dass dieses Konto die notwendigen Berechtigungen auf dem vCenter-Server haben muss.

Standardmäßig verwendet die Software das Konto, welches Sie bereits spezifiziert haben – entweder bei Konfiguration der vCenter-Integration oder beim Zugriff auf den ESX/ESXi-Server. Sie haben aber auch, falls nötig, die Möglichkeit, Anmeldedaten für ein anderes Konto anzugeben.

Die **Zeitzone** der Virtual Appliance wird automatisch gemäß der Zeitzone des Management Servers eingestellt. Sie können die Zeitzone direkt in der Benutzeroberfläche der Virtual Appliance ändern, wie unter "ESX/ESXi Virtual Appliance installieren" beschrieben. Es ist auch möglich, jedoch nicht empfehlenswert (außer, wenn absolut notwendig), das Konto und die Netzwerkeinstellungen zu ändern.

5. **Lizenzen**

   Klicken Sie auf **Lizenz zur Verfügung stellen**.

   Wenn Sie die Testversion des Produktes installieren, wählen Sie **Folgende Testlizenz verwenden** und tragen Sie die Testlizenz ein. Deduplizierung ist in der Testversion immer aktiviert.

   Bei Installation eines gekauften Produkts wählen Sie **Verwende eine Lizenz von folgendem Acronis License Server** – und spezifizieren dann den License Server, der über eine ausreichende Zahl von Lizenzen für Acronis Backup & Recovery 10 Advanced Server Virtual Edition verfügt. Für jeden von Ihnen gewählten Host benötigen Sie eine Lizenz.

   Damit Sie deduplizierte Backups erstellen können, benötigt ein Agent eine separat verkaufte Lizenz zur Deduplizierung. Wenn Sie solche Lizenzen in den License Server importiert haben, können Sie das Kontrollkästchen **Deduplizierung aktivieren...** einschalten, damit die Agenten die Lizenz erhalten.

   Wenn Sie *nur* das Produkt für Online Backup installieren wollen, dann wählen Sie **Nur Online Backup (kein Lizenzschlüssel erforderlich)**. Bei dieser Option wird angenommen, dass Sie zur Durchführung des ersten Backups ein Abonnement für den Acronis Backup & Recovery 10 Online Service bereits haben oder eingehen.

6. Klicken Sie auf **ESX-Agent verteilen**.

Deployment-Fortschritt und -Ergebnis überwachen

Die Erstellung oder Aktualisierung der Virtual Appliances kann einige Zeit benötigen. Überwachen Sie den Fortschritt der Aktionen am unteren Ende der virtuellen Maschinen-Ansichten, unterhalb der Leiste **Informationen**. Nach Erstellung und Registrierung einer Virtual Appliance erscheint auf dem Management Server eine korrespondierende Gruppe virtueller Maschinen.

Falls das Deployment abgeschlossen wurde, aber die Gruppe virtueller Maschinen fehlt

Gehen Sie unter Verwendung des vSphere/VMware Infrastructure Client in die Virtual Appliance-Konsole und überprüfen Sie die Konfiguration des Agenten. Installieren Sie, falls erforderlich, den Agenten manuell – wie unter „Installieren der Virtual Appliance für ESX/ESXi“ beschrieben. Fügen Sie

die Virtual Appliance dem Management Server manuell hinzu, wie unter „Eine Maschine dem Management Server hinzufügen (S. 321)“ beschrieben.

Unterstützung für vCenter-Cluster

In einem vCenter-Cluster sichert ein einzelner Agent für ESX/ESXi die virtuellen Maschinen, die auf allen Hosts des Clusters vorgehalten werden.

Deployment des Agenten für ESX/ESXi zu einem Cluster

Wenn Sie das Deployment des Agenten vom Management Server aus konfigurieren, können Sie einen Cluster als regulären ESX-Host auswählen. Die Virtual Appliance (VA) des Agenten wird zu einem Storage verteilt, den alle Hosts des Clusters gemeinsam nutzen. Normalerweise ist das eine NFS-Freigabe oder eine SAN-LUN, die mit jedem der Hosts verbunden ist.

Angenommen, der Cluster enthält drei Server.

- Server 1 verwendet die Storages A, B, C, D
- Server 2 verwendet die Storages C, D, E
- Server 3 verwendet die Storages B, C, D

Die VA kann zu C oder D verteilt werden. Gibt es keinen von allen Servern gemeinsam genutzten Storage, können Sie die VA manuell in jeden der Hosts importieren. Das funktioniert, jedoch ist dann die Backup-Performance weit davon entfernt, optimal zu sein.

Die Virtual Appliance des Agenten kann nach dem Deployment auf jedem der im Cluster integrierten Hosts erscheinen, abhängig von der Konfiguration der Lastverteilung.

Die VA des Agenten im Cluster bewegen

Die Arbeit des Agenten wird nicht beeinflusst, wenn der Distributed Resource Scheduler (DRS) die Virtual Appliance zu einem anderen Host migriert.

Einen Cluster von Servern erstellen, die bereits Agenten haben

Es ist empfehlenswert, dass Sie den Agenten für ESX/ESXi von allen Servern bis auf einen entfernen. Bewahren Sie den Agenten, dessen VA auf dem gemeinsam genutzen Storage vorliegt. Führen Sie einen Neustart der VA aus, so dass diese über den Cluster informiert ist.

7.1.5 Storage Node

Der Acronis Backup & Recovery 10 Storage Node hilft Ihnen, die Verwendung verschiedener Ressourcen zu optimieren, die für Schutz der Daten eines Unternehmens erforderlich sind. Dieses Ziel wird durch Organisation der verwalteten Depots (S. 431) erreicht, die als dedizierte Speicher für die Backup-Archive des Unternehmens dienen.

Ein Storage Node ermöglicht Ihnen:

- verwaltete Maschinen durch Benutzung der Storage Node-seitigen Bereinigung (S. 421) und der Storage Node-seitigen Validierung (S. 429) von unnötiger CPU-Last zu befreien.
- den für die Archive verwendeten Backup-Traffic und Speicherplatz durch Deduplizierung (S. 70) drastisch zu senken.
- mit Hilfe verschlüsselter Depots (S. 431) den Zugriff auf Backup-Archive zu verhindern, auch wenn das Speichermedium gestohlen wurde oder durch einen Unbefugten auf die Archive zugegriffen wird.

Weitere Informationen zum Acronis Backup & Recovery 10 Storage Node finden Sie im Abschnitt Acronis Backup & Recovery 10 Storage Node (S. 21).

Die wichtigsten Elemente der Ansicht „Storage Node“

- **Liste der Storage Nodes mit Symbolleiste**

  Über die Symbolleiste können Sie Aktionen (S. 342) für den ausgewählten Storage Node ausführen (S. 342). In der Liste der Storage Nodes werden Online- und Offline-Storage Nodes angezeigt, die dem Management Server hinzugefügt wurden. Sie enthält außerdem Informationen zur Gesamtzahl aller Backups und Archive im Storage Node.

- **Bereich „Informationen“**

  Enthält detaillierte Informationen zum ausgewählten Storage Node und ermöglicht Ihnen die Verwaltung des Verdichtungs-Tasks. Die Leiste ist standardmäßig eingeklappt. Sie können die Leiste aufklappen, indem Sie auf das Chevron-Symbol klicken. Der Inhalt des Bereichs ist außerdem im Fenster **Details zum Storage Node** (S. 344) verfügbar.

Arbeitsmöglichkeiten mit Storage Nodes (typischer Ablauf)

1. Installieren Sie den Acronis Backup & Recovery 10 Storage Node.
2. Erstellen Sie ein Benutzerkonto für jeden Benutzer, dem Sie Zugriff auf den Storage Node gestatten möchten.

   Anmerkung: *Sie können diesen Schritt überspringen, wenn sich der Storage Node und die Maschinen des Benutzers in derselben Active Directory-Domain befinden.*

   Informationen über Benutzerrechte auf einem Storage Node und in seinen verwalteten Depots finden Sie unter Benutzerrechte auf einem Storage Node (S. 76).
3. Fügen Sie (S. 343) den Storage Node dem Acronis Backup & Recovery 10 Management Server hinzu (S. 343).
4. Ein verwaltetes Depot erstellen (S. 135): Geben Sie den Pfad zum Depot an, wählen Sie den Storage Node aus, der das Depot verwalten wird und wählen Sie die Verwaltungsaktionen aus, wie z.B. Deduplizierung oder Verschlüsselung.
5. Erstellen Sie eine Backup-Richtlinie (S. 374) oder einen Backup-Plan, bei der bzw. dem das verwaltete Depot verwendet wird.

Aktionen für Storage Nodes

Alle hier beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Schaltflächen in der Symbolleiste ausgeführt. Auf die Aktionen kann auch über die Leiste **Storage Nodes** (im Bereich **Aktionen und Werkzeuge**) sowie über das Element **Storage Nodes** des Hauptmenüs zugegriffen werden.

Um eine Aktion mit einem Storage Node auszuführen, der dem Management Server hinzugefügt wurde, wählen Sie zunächst den Storage Node aus.

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Storage Nodes.

Aktion	Lösung
Dem Management Server einen Storage Node hinzufügen	Klicken Sie auf **Hinzufügen**. Geben Sie im Fenster Storage Node hinzufügen (S. 343) die Maschine an, auf der der Storage Node installiert ist. Wenn ein Storage Node hinzugefügt wird, wird eine Vertrauensstellung (Trusted Relationship) zwischen dem Management Server und dem Storage Node in der gleichen Weise aufgebaut wie beim Hinzufügen von Maschinen zum Server.

	Nachdem der Storage Node dem Management Server hinzugefügt wurde, können Sie verwaltete Depots auf dem Knoten erstellen.
Einen Storage Node vom Management Server entfernen	Klicken Sie auf **Entfernen**. Nachdem der Storage Node vom Management Server entfernt wurde, verschwinden die vom Storage Node verwalteten Depots aus der Liste der Depots (S. 130) und sind danach nicht mehr für Aktionen verfügbar. Alle Pläne und Tasks, die diese Depots verwenden, werden fehlschlagen. Alle Datenbanken und Depots dieses Storage Nodes bleiben unberührt. Es ist möglich, einen bereits entfernten Storage Node dem Management Server wieder hinzuzufügen. Daraufhin werden alle vom Storage Node verwalteten Depots in der Depot-Liste angezeigt und sind wieder für alle Pläne und Tasks verfügbar, die diese Depots verwendet haben.
Ein zentral verwaltetes Depot auf dem ausgewählten Storage Node erstellen	Klicken Sie auf **Depot erstellen**. Die Seite Verwaltetes Depot erstellen (S. 135) wird mit dem vorausgewählten Storage Node geöffnet. Führen Sie die verbleibenden Schritte zum Erstellen des Depots aus.
Die Planung des Verdichtungs-Tasks ändern	Nach dem Löschen von Backups aus deduplizierenden Depots (entweder manuell oder während einer Bereinigung), erscheinen möglicherweise nicht referenzierte Daten in den deduplizierenden Depots und ihren Datenbanken. Durch den Verdichtungsvorgang werden solche Daten gelöscht, um mehr freien Speicherplatz zu schaffen. Pro Storage Node ist nur ein Verdichtungs-Task verfügbar. Klicken Sie auf **Verdichten neu planen**. Legen Sie im Fenster **Planung** die Zeit-/Ereignisplanung für den Verdichtungsvorgang fest. Nur die Zeitereignisse (tägliche (S. 173), wöchentliche (S. 175) und monatliche (S. 177) Planungen) können eingerichtet werden. Voreinstellung ist: Den Task jede **Woche** am **Sonntag** um **03:00:00 Uhr** starten. **Einmalig**.
Details zum Storage Node anzeigen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie im Fenster **Details zum Storage Node** (S. 344) (dessen Inhalt auch im Bereich **Informationen** verfügbar ist) die Informationen zum Storage Node und den Depots, die von diesem Knoten verwaltet werden. Sie können auch den Verdichtungs-Task verwalten: den Task manuell starten und stoppen.
Die Liste der Storage Nodes aktualisieren	Klicken Sie auf **Aktualisieren**. Die Verwaltungskonsole aktualisiert die Liste der Storage Nodes vom Management Server mit den neuesten Informationen. Obwohl die Liste der Storage Nodes auf der Basis von Ereignissen automatisch aktualisiert wird, kann es sein, dass die Daten infolge einer gewissen Latenz nicht augenblicklich vom Management Server abgerufen werden. Eine manuelle Aktualisierung garantiert daher, dass auch die allerneusten Daten angezeigt werden.

Einen Storage Node hinzufügen

So fügen Sie einen Storage Node hinzu

1. Geben Sie im Feld **IP/Name** den Namen oder die IP-Adresse der Maschine ein, auf der sich der Storage Node befindet oder klicken Sie auf **Durchsuchen...** und durchsuchen Sie das Netzwerk nach der Maschine.

   Benutzen Sie den vollständigen Domänennamen (fully-qualified domain name, FQDN) des Storage Nodes, d.h., einen Domänennamen der mit einer Top-Level Domain endet. Sie können

weder „127.0.0.1 noch „localhost“ als IP oder Namen des Storage Nodes verwenden. Diese Einstellungen sind auch dann nicht zu verwenden, wenn sich Management Server und Storage Node auf der gleichen Maschine befinden, weil alle Agenten nach dem Erhalt der verteilten Richtlinie, die den Speicherkonten benutzt, auf den Speicherkonten so zugreifen würden, als wenn dieser auf dem Host des Agenten selbst installiert wäre.

2. Wenn Sie ein gültiges Benutzerkonto für die Maschine angeben möchten, klicken Sie auf **Optionen>>** und geben Sie dann den folgenden Wert ein:
   - **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. Das Benutzerkonto muss Mitglied der Gruppe „Administratoren“ auf der Maschine sein.
   - **Kennwort**. Das Kennwort für das Konto.

   Aktivieren Sie das Kontrollkästchen **Kennwort speichern**, um das Kennwort für das Konto zu speichern.
3. Klicken Sie auf **OK**.

Da zur Registrierung eine Beteiligung des Storage Nodes erforderlich ist, kann diese Aktion nicht ausgeführt werden, wenn die Maschine offline ist.

Details zum Storage Node

Im Fenster **Details zum Storage Node** werden alle Informationen zum Acronis Backup & Recovery 10 Storage Node in vier Registerkarten zusammengefasst. Diese Informationen sind auch im Bereich **Informationen** verfügbar.

Eigenschaften des Storage Nodes

Auf dieser Registerkarte werden die folgenden Informationen zum ausgewählten Storage Node angezeigt:

- **Name** – Der Name der Maschine, auf der der Storage Node installiert ist
- **IP** – Die IP-Adresse der Maschine, auf der der Storage Node installiert ist
- **Verfügbarkeit**:
  - **Unbekannt** – Dieser Status wird so lange angezeigt, bis nach dem Hinzufügen des Storage Nodes zum ersten Mal eine Verbindung zwischen dem Management Server und dem Storage Node hergestellt wird oder bis der Dienst des Management Servers gestartet wird.
  - **Online** – Der Storage Node ist für den Management Server verfügbar. Dies bedeutet, dass die letzte Verbindung des Management Servers mit dem Knoten erfolgreich war. Die Verbindung wird alle 2 Minuten aufgebaut.
  - **Offline** – Der Storage Node ist nicht verfügbar.
  - **Zurückgezogen** – Der Storage Node wurde auf einem anderen Management Server registriert. In diesem Fall ist es nicht möglich, den Knoten vom aktuellen Management Server aus zu steuern.
- **Archive** – Die Gesamtzahl aller Archive, die in allen vom Storage Node verwalteten Depots gespeichert sind
- **Backups** – Die Gesamtzahl aller Backups, die in den Archiven aller vom Storage Node verwalteten Depots gespeichert sind.

Depots

Auf dieser Registerkarte wird eine Liste der Depots angezeigt, die vom Storage Node verwaltet werden.

Wenn Sie ein verwaltetes Depot öffnen möchten, um es genauer zu untersuchen oder Aktionen darauf auszuführen, dann wählen Sie das Depot aus und klicken Sie auf **Depot anzeigen** (in der Symbolleiste der Registerkarte). Führen Sie in der Ansicht **Zentrales Depot** (S. 131) die gewünschten Aktionen aus.

Dienste

Auf dieser Registerkarte werden die Parameter für die Planung des Verdichtungs-Tasks angezeigt.

Dienst-Tasks

Auf dieser Registerkarte kann der Administrator des Management Servers den Verdichtungs-Task verwalten und dessen Parameter überprüfen. Auf einem Storage Node kann nur ein Verdichtungs-Task vorhanden sein.

7.1.6 Aufgaben

In der Ansicht **Tasks** können Sie die Tasks, die auf den registrierten Maschinen vorhanden sind, überwachen und verwalten. Sie können die Details, Stadien und Ausführungsergebnisse von Tasks anzeigen sowie Tasks ausführen, stoppen und löschen.

Wenn Sie herausfinden möchten, welcher Task momentan auf einer Maschine ausgeführt wird, überprüfen Sie den Ausführungsstadium des Tasks. Der Status eines Tasks hilft Ihnen bei der Einschätzung, ob ein Task erfolgreich abgeschlossen wurde.

Weitere Informationen zu Stadien und Zuständen finden Sie in den Abschnitten Task-Stadien (S. 193) und Task-Zustände (S. 194).

Arbeitsmöglichkeiten mit Tasks

- Verwenden Sie die Filter- und Sortierfunktionen (S. 347), um gewünschte Tasks in der Tabelle anzuzeigen.
- Wählen Sie einen Task aus, um eine Aktion mit ihm auszuführen.

Aktionen für Tasks

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Tasks.

Aktion	Lösung
Einen neuen Backup-Plan oder einen Task auf einer registrierten Maschine erstellen	Klicken Sie auf **Neu** und wählen Sie eine der folgenden Optionen: ▪ Backup-Plan (S. 205) ▪ Recovery-Task ▪ Validierungstask (S. 252) Dann müssen Sie die registrierte Maschine angeben, auf der der ausgewählte Task bzw. Backup-Plan ausgeführt werden soll.
Details eines Tasks anzeigen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie dann im Fenster Task-Details (S. 199) alle Informationen, die sich auf den ausgewählten Task beziehen.
Log eines Tasks anzeigen	Klicken Sie auf **Log anzeigen**. Die Ansicht Log (S. 347) wird eine Liste der Log-Einträge anzeigen, die sich auf den ausgewählten Task beziehen.

Einen Task ausführen	Klicken Sie auf **Ausführen**. Die Ausführung des Tasks startet unmittelbar, ungeachtet seiner Zeit-/Ereignis-Planung.
Einen Task stoppen	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 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 Laufwerk-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, zu dem Sie den Task gestoppt haben. Um alle Dateien wiederherzustellen, müssen Sie den Task erneut ausführen.
Einen Task bearbeiten	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 Task löschen	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. ▪ **Dies ist ein integrierter Verdichtungs-Task** Jeder Storage Node verfügt über einen integrierten Dienst-Task, der auch Verdichtungs-Task genannt wird. Dieser Task kann nicht gelöscht werden.

Tasks-Tabelle aktualisieren	Klicken Sie auf **Aktualisieren**. Die Management Konsole wird die Liste der auf der Maschine existierenden Tasks mit den neusten Informationen aktualisieren. Obwohl die Liste der Tasks auf der Basis von Ereignissen automatisch aktualisiert wird, kann es sein, dass die Daten infolge einer gewissen Verzögerung nicht augenblicklich von der verwalteten Maschine abgerufen werden. Eine manuelle Aktualisierung garantiert daher, dass auch die allerneusten Daten angezeigt werden.

Tasks filtern und sortieren

Nachfolgend finden Sie eine Anleitung zum Filtern und Sortieren von Tasks.

Aktion	Lösung
Eine Anzahl anzuzeigender Tasks festlegen	Wählen Sie **Optionen –> Konsolenoptionen –> Zahl der Tasks** (S. 87) und legen Sie den gewünschten Wert fest. Es können maximal 500 Tasks angezeigt werden. Wenn die Anzahl den angegebenen Wert überschreitet, verwenden Sie Filter, um die Tasks anzuzeigen, die sich außerhalb des Anzeigebereichs befinden.
Tasks nach Spalten sortieren	Klicken Sie auf die Spaltenköpfe, um die Tasks aufsteigend zu sortieren. Kicken Sie erneut auf den Spaltenkopf, um die Tasks absteigend zu sortieren.
Tasks nach Name, Besitzer oder Backup-Plan filtern.	Geben Sie den Namen des Tasks (den Namen des Besitzers oder den Namen des Backup-Plans) in das Feld unter dem entsprechenden Spaltenkopf ein. Sie erhalten als Ergebnis eine Liste von Tasks, deren Namen (bzw. Namen der Besitzer oder Namen der Backup-Pläne) vollständig oder partiell mit dem eingegebenen Wert übereinstimmen.
Tasks nach Typ, Ausführungsstadium, Status, Typ, Ursprung, letztem Ergebnis und Planung filtern.	Wählen Sie im Feld unterhalb des entsprechenden Spaltenkopfes den benötigten Wert aus einer Liste.

Tasks-Tabelle konfigurieren

Standardmäßig werden in der Tabelle acht 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.

7.1.7 Log

Das Log in Acronis Backup & Recovery 10 speichert den Verlauf von Aktionen, die die Software auf einer Maschine ausführt bzw. die ein Benutzer unter Verwendung der Software auf der Maschine ausführt. Wenn Benutzer z.B. Tasks bearbeiten, dann wird dem Log ein Eintrag hinzugefügt. Bei Ausführung eines Tasks durch die Software werden dem Log mehrere Einträge mit Informationen darüber hinzugefügt, welche Aktionen aktuell ausgeführt werden.

Lokale und zentrale Protokollierung in Acronis Backup & Recovery 10

Acronis Backup & Recovery 10 hat lokale und zentrale Ereignis-Logs.

Lokales Ereignis-Log

Ein lokales Ereignis-Log enthält Informationen über die Aktionen von Acronis Backup & Recovery 10 auf einer verwalteten Maschine. So erzeugen z.B. das Erstellen eines Backup-Plans, das Ausführen eines Backup-Plans, das Verwalten von Archiven in persönlichen Depots oder das Ausführen eines Recovery-Tasks jeweils Ereignisse, die im lokalen Ereignis-Log protokolliert werden. Physikalisch ist ein Ereignis-Log eine Sammlung von auf der Maschine gespeicherten XML-Dateien. Auf das lokale Ereignis-Log einer verwalteten Maschine kann zugegriffen werden, wenn die Konsole mit der Maschine verbunden ist. Die Protokollierung lokaler Ereignis kann nicht deaktiviert werden.

Außerdem werden Aktionen protokolliert, die unter Verwendung bootfähiger Medien ausgeführt werden. Hierbei ist allerdings die Lebenszeit des Logs auf die Dauer der aktuellen Sitzung beschränkt. Beim Neustart wird das Log gelöscht, Sie können aber das Log in eine Datei speichern, während die Maschine mit dem Medium gebootet wird.

Der Acronis Backup & Recovery 10 Storage Node hat sein eigenes lokales Ereignis-Log. Auf die Ereignisse dieses Logs kann nur über das zentrale Log zugegriffen werden.

Zentrales Ereignis-Log

Mit Log-Einträgen arbeiten

- Die maximale Anzahl von Einträgen, die in dem zentralen Log gespeichert werden können, beträgt 50.000. Die maximale Anzahl von Einträgen, die angezeigt werden können, beträgt 10.000. Falls die Anzahl der Log-Einträge größer als 10.000 ist, verwenden Sie die Filter- und Sortierfunktionen, um gewünschte Log-Einträge in der Tabelle anzuzeigen. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu Details siehe den Abschnitt Log-Einträge filtern und sortieren (S. 350).
- Wählen Sie einen oder mehrere Log-Einträge in der Log-Tabelle aus, um darauf eine Aktion auszuführen. Zu Details siehe den Abschnitt Aktionen für Log-Einträge (S. 349).
- 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. 350) dupliziert.

Möglichkeiten zum Öffnen der Log-Ansicht mit vorgefilterten Log-Einträgen

Wenn Sie Elemente in anderen Verwaltungsansichten (Dashboard, Maschinen, Backup-Richtlinien, Tasks) ausgewählt haben, können Sie eine Ansicht bereits gefilterter Log-Einträge für das betreffende Element öffnen. 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.
Maschinen	Wählen Sie eine Maschine oder eine Gruppen von Maschinen aus und klicken Sie dann auf **Log anzeigen**. Die Log-Ansicht wird eine Liste von Log-Einträgen anzeigen, die sich auf die ausgewählte Maschine oder Gruppen von Maschinen beziehen.
Backup-Richtlinien	Wählen Sie eine Backup-Richtlinie und klicken Sie dann auf **Log anzeigen**. Die Log-Ansicht wird eine Liste der Log-Einträge anzeigen, die sich auf die ausgewählte Richtlinie beziehen.

Aufgaben	Wählen Sie einen Task aus und klicken Sie auf **Log anzeigen**. Die Log-Ansicht erscheint mit einer Liste der Log-Einträge, die zum ausgewählten Task gehören.

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-Level einrichten	Klicken Sie auf **Log-Level einstellen**. Geben Sie im Fenster **Log-Level** (S. 88) an, ob die Log-Ereignisse registrierter Maschinen im zentralen Log erfasst werden sollen.

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 zum zentralen Log-Eintrag

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 zentraler Log-Eintrag enthält die folgenden Datenfelder:

- **Typ** – Ereignistyp (Fehler, Warnung, Information)
- **Datum** – Datum und Uhrzeit des Ereignisses
- **Richtlinie** – Die Backup-Richtlinie, auf die sich das Ereignis bezieht (sofern vorhanden)
- **Task** – Der Task, auf den sich das Ereignis bezieht (sofern vorhanden)
- **Typ der verwalteten Einheit** – Typ der verwalteten Einheit, in der das Ereignis aufgetreten ist

(sofern vorhanden)

- **Verwaltete Einheit** – Name der verwalteten Einheit, in der das Ereignis aufgetreten ist (sofern vorhanden)
- **Maschine** – Name der Maschine, in der das Ereignis aufgetreten ist (sofern vorhanden)
- **Code** – Leer oder der Programmfehlercode, wenn das Ereignis vom Typ „Fehler“ ist. Der Fehlercode ist eine Integer-Zahl, die vom Acronis-Support zum Lösen des Problems verwendet werden kann.
- **Modul** – Leer oder die Nummer des Programmmoduls, in dem ein Fehler 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 Besitzers (S. 34) der Richtlinie bzw. des Backup-Plans
- **Nachricht** – 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
Verwalteter Einheitstyp:      Maschine
Verwaltete Einheit:           ENTITY_NAME
Maschine:                     MACHINE_NAME
Meldung:
Beschreibung der Aktion
Code:                         12(3x45678A)
Modul:                        Name des Moduls
Besitzer:                     Besitzer des Plans
------------------------------------------------------------------------
```

7.1.8 Berichte

Mit der Berichtsfunktion stehen dem Administrator des Management Server detaillierte und wohlstrukturierte Informationen über die Sicherung von Unternehmensdaten zur Verfügung. Die Berichte dienen als Werkzeug für eine gründliche Analyse der gesamten Backup-Infrastruktur innerhalb des Unternehmensnetzwerks.

Der Management Server erstellt Berichte anhand von Statistiken und Logs, die auf den registrierten Maschinen erfasst und in speziellen Datenbanken gespeichert werden.

Die Berichte werden basierend auf Berichtsvorlagen erstellt. In den Vorlagen ist definiert, welche Informationen ein Bericht enthalten soll und wie diese Informationen dargestellt werden sollen.

Acronis Backup & Recovery 10 Management Server bietet Berichtsvorlagen für:

- Registrierte Maschinen
- Auf dem Management Server vorliegende Backup-Richtlinien
- Auf den registrierten Maschinen vorliegende lokale und zentrale Backup-Pläne
- Auf den registrierten Maschinen vorliegende lokale und zentrale Tasks
- In den zentral verwalteten Depots gespeicherte Archive und Backups
- Statistiken über zentral verwaltete Depots
- Verlaufshistorie der Task-Aktivitäten

Berichte über Maschinen, Backup-Richtlinien, Backup-Pläne, Tasks und Archive sowie Backups enthalten Informationen ab dem gegenwärtigen Zeitpunkt.

Berichte über die Statistiken von Depots und Task-Aktivitäten sind intervallbasiert und bieten zurückliegende Informationen für ein angegebenes Zeitintervall, welches von Tagen bis Jahren reichen kann (abhängig von der in den Datenbanken enthaltenen Datenmenge).

Berichte generieren

Um einen Bericht zu erstellen, wählen Sie eine Berichtsvorlage in der Ansicht **Berichte** und klicken dann in der Symbolleiste auf **Generieren**.

Es gibt zwei Typen von Berichtsvorlagen: benutzerdefinierbar und vordefiniert. In einer benutzerdefinierbaren Berichtsvorlage können Sie mit Filtern festlegen, welche Einträge ein Bericht enthalten soll. Eine vordefinierte Berichtsvorlage ist vorgegeben, so dass Sie einen Report mit einem Klick generieren können.

Die Informationen des Berichts werden entsprechend der Vorlageneinstellungen selektiert, gruppiert und sortiert. Berichte öffnen sich in einem separaten interaktiven Fenster, in dem die Tabellen erweitert oder reduziert werden können. Sie können Berichte auch in eine XML-Datei exportieren und sie später in Microsoft Excel oder Microsoft Access öffnen.

Bericht über die Maschinen

In dieser Ansicht können Sie Berichte über die Maschinen erstellen, die auf dem Management Server registriert sind. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Maschinen in den Bericht aufgenommen werden sollen. Nur die Maschinen, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Maschinen**: Liste der Maschinen. Wählen Sie physikalische Maschinen oder virtuelle Maschinen aus.
- **Status**: Der Status der Maschinen – **OK**, **Warnung** bzw. **Fehler**.
- **Letzte Verbindung** (nur die physikalischen Maschinen): Der Zeitraum, innerhalb dessen die letzte Verbindung zwischen den Maschinen und dem Management Server erfolgte.
- **Letztes erfolgreiches Backup**: Der Zeitraum, innerhalb dessen das letzte erfolgreiche Backups auf jeder der Maschinen beendet wurde.
- **Nächstes Backup**: Der Zeitraum, innerhalb dessen das nächste geplante Backup auf jeder der Maschinen starten wird.
- **Betriebssystem**: Die Betriebssysteme, die auf den Maschinen laufen.
- **IP-Adresse** (nur die physikalischen Maschinen): Der Adressbereich der letzten bekannten IP-Adressen für die Maschinen.
- **Verfügbarkeit** (nur die physikalischen Maschinen): Die Verfügbarkeit der Maschinen – **Online** oder **Offline**.

In der Standardeinstellung werden alle physikalischen Maschinen in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.

- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

Bericht über Backup-Richtlinien

In dieser Ansicht können Sie Berichte über die Backup-Richtlinien auf dem Management Server erstellen. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Backup-Richtlinien in den Bericht aufgenommen werden sollen. Nur die Backup-Richtlinien, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Backup-Richtlinien**: Liste der Backup-Richtlinien.
- **Quelltyp**: Die Art der Daten, die mit diesen Backup-Richtlinien gesichert werden – **Laufwerke/Volumes** bzw. **Dateien**.
- **Deployment-Stadium**: Der Deployment-Stadium der Backup-Richtlinien – z.B. **Verteilt**.
- **Status**: Die Zustände der Backup-Richtlinien – **OK**, **Warnung** bzw. **Fehler**.
- **Planung**: Die Planungsart der Backup-Richtlinien – **Manuell** oder **Geplant**. Bei manuellen Planung muss die Ausführung des entsprechenden zentralen Backup-Plans manuell gestartet werden.
- **Besitzer**: Die Liste der Benutzer, die die Backup-Richtlinien erstellt haben.

In der Standardeinstellung werden alle Backup-Richtlinien in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.
- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

Bericht über Backup-Pläne

In dieser Ansicht können Sie Berichte über die Backup-Pläne auf den registrierten Maschinen erstellen. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Backup-Pläne in den Bericht aufgenommen werden sollen. Nur die Backup-Pläne, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Ursprung**: Die Planungsart der Backup-Pläne – **Lokal** oder **Zentral**.
- **Backup-Richtlinien** (nur für zentrale Backup-Pläne verfügbar): Die Backup-Richtlinien, auf denen die zentralen Backup-Pläne basieren.
- **Maschinen**: Die Liste der Maschinen, auf denen sich die Backup-Pläne befinden.
- **Ausführungsstadium**: Das Ausführungsstadium der Backup-Pläne – z.B. **Laufend**.
- **Status**: Die Zustände der Backup-Pläne – **OK**, **Warnung** bzw. **Fehler**.
- **Letzte Abschlusszeit**: Der Zeitraum, innerhalb dessen das letzte Backup unter jedem der Backup-Pläne beendet wurde.
- **Planung**: Die Planungsart der Backup-Pläne – **Manuell** oder **Geplant**. Bei der manuellen Planung muss die Ausführung eines Backup-Plans manuell gestartet werden.
- **Besitzer**: Die Liste der Benutzer, die die Backup-Pläne erstellt haben.

In der Standardeinstellung werden alle Backup-Pläne auf allen Maschinen in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.
- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

Bericht über Tasks

In dieser Ansicht können Sie Berichte über die Tasks erstellen, die auf den registrierten Maschinen ausgeführt werden. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Tasks in den Bericht aufgenommen werden sollen. Nur die Tasks, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Ursprung**: Der Ursprung der Tasks – **Zentral**, **Lokal** bzw. **Lokal ohne Backup-Plan**. Zentrale Tasks gehören zu einem zentralen Backup-Plan. Lokale Tasks (z.B. ein Recovery-Task) gehören nicht unbedingt zu einem Backup-Plan.
- **Backup-Richtlinien** (nur zentrale Tasks): Die Backup-Richtlinien, auf denen die Tasks basieren.
- **Maschinen**: Die Liste der Maschinen, auf denen sich die Tasks befinden.
- **Typ**: Die Task-Typen – z.B. Tasks für Disk-Backups.
- **Ausführungsstadium**: Das Ausführungsstadium der Tasks – z.B. **Läuft**.
- **Letztes Ergebnis**: Die letzten Ergebnisse der Tasks – **Erfolgreich abgeschlossen**, **Mit Warnungen abgeschlossen** bzw. **Fehlgeschlagen**.
- **Planung**: Die Planungsart der Tasks – **Manuell** oder **Geplant**. Bei der manuellen Planung muss die Ausführung eines Task manuell gestartet werden.
- **Besitzer**: Die Liste der Benutzer, die die Tasks erstellt haben.
- **Dauer**: Anfang und Ende des Zeitraums, in dem die einzelnen Tasks zuletzt ausgeführt wurden.

In der Standardeinstellung werden alle Tasks auf allen Maschinen in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.
- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

Bericht über Archive und Backups

In dieser Ansicht können Sie Berichte über die Archive erstellen, die in zentral verwalteten Depots gespeichert sind. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Archive in den Bericht aufgenommen werden sollen. Nur die

Archive, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Depots**: Die Liste der zentral verwalteten Depots, in denen die Archive gespeichert sind.
- **Maschinen**: Die Liste der registrierten Maschinen, auf denen die Archive erstellt worden sind.
- **Typ**: Die Archiv-Typen – laufwerksbasierte bzw. dateibasierte Archive.
- **Besitzer**: Die Liste der Benutzer, die die Archive erstellt haben.
- **Erstellungszeit**: Der Zeitraum seit Erstellen des letzten Backup in den einzelnen Archiven.
- **Belegter Speicherplatz**: Der Speicherplatz, den die einzelnen Archive belegen.
- **Gesicherte Daten**: Die Begrenzungen für die Gesamtgröße aller Daten, die gegenwärtig in den einzelnen Archiven gespeichert sind. Diese Größe kann sich durch Komprimierung oder Deduplizierung von der des belegten Speicherplatzes unterscheiden.
- **Zahl der Backups**: Die Beschränkungen für die Anzahl der Backups in den einzelnen Archive.

In der Standardeinstellung werden alle Archive, die in den zentral verwalteten Depots gespeichert sind, in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.
- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

Bericht über Statistiken für Depots

In dieser Ansicht können Sie einen Bericht über die Nutzung der zentral verwalteten Depots erstellen, die gegenwärtig zum Management Server hinzugefügt werden. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n) und einem oder mehreren Diagramm(en).

Berichtsumfang

Unter **Berichtsumfang** bestimmen Sie den Zeitraum, für den der Bericht erstellt werden soll. Der Bericht wird das Stadium der gewählten Depots für die angegebene Zeit an jedem Tag des Berichtszeitraums darstellen.

Filter

Unter **Filter** bestimmen Sie, welche zentral verwalteten Depots in den Bericht aufgenommen werden sollen, und ob er eine Gesamtübersicht über alle ausgewählten Depots enthalten soll.

Diese Gesamtübersicht zeigt den gesamten freien und belegten Speicherplatz, die Gesamtmenge der gesicherten Daten, die Gesamtzahl der Archive und Backups, sowie die Durchschnittswerte für die ausgewählten Depots.

Mit den standardmäßigen Filtereinstellungen werden Informationen über alle zentral verwalteten Depots sowie die Gesamtsumme in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, welche Diagramme in den Bericht aufgenommen werden sollen. Die Diagramme zeigen die Speicherplatzbelegung in den Depots an.

Bericht über Task-Aktivitäten

In dieser Ansicht können Sie Berichte über die Tasks erstellen, die sich in einem von Ihnen gewählten Zeitraum auf den registrierten Maschinen befanden. Solch ein Bericht besteht aus einem oder mehreren Diagramm(en) – ein Diagramm pro Maschine.

Die Diagramme zeigen an, wie oft an einem bestimmten Tag die einzelnen Tasks mit einem dieser Ergebnisse beendet wurden: „Erfolgreich abgeschlossen“, „Mit Warnungen abgeschlossen“ und „Fehlgeschlagen“.

Berichtsumfang

Unter **Berichtsumfang** bestimmen Sie den Zeitraum, für den der Bericht erstellt werden soll.

Filter

Unter **Filter** bestimmen Sie, welche Tasks in den Bericht aufgenommen werden sollen. Nur die Tasks, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Ursprung**: Der Ursprung der Tasks – **Zentral**, **Lokal** bzw. **Lokal ohne Backup-Plan**. Zentrale Tasks gehören zu einem zentralen Backup-Plan. Lokale Tasks (z.B. ein Recovery-Task) gehören nicht unbedingt zu einem Backup-Plan.
- **Backup-Richtlinien** (nur zentrale Tasks): Die Backup-Richtlinien, auf denen die Tasks basieren. In der Standardeinstellung werden alle Backup-Richtlinien aus dem angegebenen Berichtszeitraum in den Bericht aufgenommen.
- **Maschinen**: Die Liste der Maschinen, auf denen sich die Tasks befinden.
- **Typ**: Die Task-Typen – z.B. Tasks für Disk-Backups.
- **Besitzer**: Die Liste der Benutzer, die die Tasks erstellt haben.

In der Standardeinstellung werden alle Tasks, die sich zu irgendeiner Zeit während des Berichtszeitraum auf den registrierten Maschinen befanden, in den Bericht aufgenommen.

Spaltenauswahl

Im Fenster **Spaltenauswahl** bestimmen Sie, welche Tabellenspalten in welcher Reihenfolge in den Bericht aufgenommen werden sollen.

Die Tabellenspalten werden im Bericht entsprechend der Liste **Im Bericht anzeigen** dargestellt. Dabei entspricht der oberste Listeneintrag der Spalte ganz links im Bericht.

Verwenden Sie bei der Auswahl der anzuzeigenden Spalten die Pfeiltasten links und rechts um Spalten aus – oder abzuwählen, und die Pfeiltasten oben und unten um die Reihenfolge der Spalten zu ändern.

Einige Spalten – z.B. **Maschinenname** in einem Bericht über Maschinen – können nicht abgewählt oder nach oben bzw. unten verschoben werden.

Berichtsansicht

Ermögliche Sie die Ausführung 'Aktiver Inhalte' (JavaScript) in Ihrem Webbrowser, damit Datums- und andere Informationen in den erstellten Berichten korrekt angezeigt werden. Sie können die Ausführung 'Aktiver Inhalte' für die aktuelle Webseite temporär zulassen oder sie auch permanent aktivieren. Um die Ausführung 'Aktiver Inhalte' im Internet Explorer temporär einzuschalten, klicken Sie auf die standardmäßig am Kopf der Webseite erscheinende Informationsleiste und dann auf **Blockierte Inhalte zulassen**.

Um 'Aktive Inhalte' dauerhaft zuzulassen

klicken Sie im Internet Explorer

1. im Menü **Extras** auf **Internetoptionen** und dann auf die Registerlasche **Erweitert**.
2. Aktivieren Sie im Abschnitt **Sicherheit** das Kontrollkästchen **Ausführung aktiver Inhalte in Dateien auf dem lokalen Computer zulassen**.
3. Klicken Sie auf **OK**.

in Mozilla Firefox

1. Klicken Sie im Menü **Extras, Einstellungen** auf **Inhalt**.
2. Stellen Sie sicher, dass das Kontrollkästchen **JavaScript aktivieren** angewählt ist.
3. Klicken Sie auf **OK**.

7.2 Acronis Backup & Recovery 10-Komponenten konfigurieren

Es gibt drei Arten, die verschiedenen Parameter von Acronis Backup & Recovery 10-Komponenten in Windows zu konfigurieren:

- durch Verwendung des Acronis Administrative Template
- durch Verwendung der grafischen Benutzeroberfläche (GUI)
- durch Modifikation der Windows Registry

Unter Linux werden Parameter nicht durch Verwendung der administrativen Vorlage und Registry-Modifikation konfiguriert, sondern durch das Bearbeiten korrespondierender Konfigurationsdateien.

Falls die Werte eines per administrativer Vorlage gesetzten Parameters von denen abweichen, die per Benutzeroberfläche (GUI) gesetzt wurden, so erhalten die vorlagenbasierten Parameter Vorrang und werden sofort wirksam; die in der GUI angezeigten Werte werden dementsprechend abgeändert.

Die folgenden Abschnitte erläutern beide Arten der Konfiguration sowie die Parameter, die konfiguriert werden.

7.2.1 Durch die administrative Vorlage gesetzte Parameter

Der nachfolgende Abschnitt erläutert die Parameter der Acronis Backup & Recovery 10-Komponenten, die unter Verwendung des Acronis Administrative Template konfiguriert werden können. Zu Informationen, wie Sie die administrative Vorlage anwenden, siehe Acronis Administrative Template anwenden (S. 357).

Die administrative Vorlage enthält die Konfigurations-Parameter für Acronis Backup & Recovery 10 Agent, Acronis Backup & Recovery 10 Management Server und Acronis Backup & Recovery 10 Storage Node (wie in den entsprechenden Abschnitten zu diesem Thema beschrieben).

Acronis Administrative Template laden

Das von Acronis zur Verfügung gestellte administrative Template ermöglicht das Fein-Tuning einiger sicherheitsbezogener Funktionen, inklusive verschlüsselter Kommunikationseinstellungen. Durch den Microsoft Gruppenrichtlinien-Mechanismus können die Richtlinien-Einstellungen des Templates auf einen einzelnen Computer wie auch auf eine Domain angewendet werden.

So laden Sie das Acronis Administrative Template

1. Führen Sie den Editor für Windows Gruppenrichtlinien-Objekte aus (%windir%\system32\gpedit.msc).
2. Öffnen Sie das zur Bearbeitung gewünschte Gruppenrichtlinien-Objekt (Group Policy object, GPO).
3. Erweitern Sie den Ast **Computerkonfiguration**.
4. Klicken Sie mit der rechten Maustaste auf **Administratives Template**.
5. Klicken Sie auf **Template hinzufügen/entfernen**.
6. Klicken Sie auf **Hinzufügen**.
7. Wechseln Sie zum Acronis Administrative Template (\Programme\Common Files\Acronis\Agent\Acronis_agent.adm oder \Programme\Acronis\BackupAndRecoveryConsole\Acronis_agent.adm) und klicken Sie dann auf **Öffnen**.

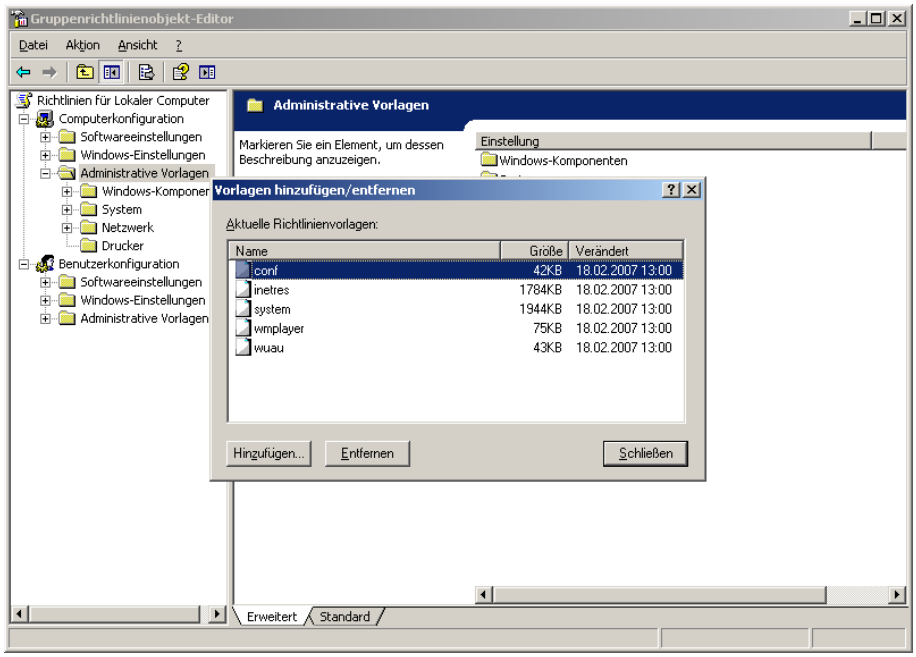
Sobald das Template geladen wurde, können Sie sie öffnen und gewünschte Einstellungen bearbeiten. Nachdem Sie das Template geladen oder dessen Einstellungen bearbeitet haben, sollten Sie die konfigurierten Komponente(n) oder einige ihrer Dienste neu starten.

Zu detaillierten Informationen über den Windows Gruppenrichtlinien-Editor siehe:

http://msdn2.microsoft.com/en-us/library/aa374163.aspx

Zu detaillierten Informationen über Gruppenrichtlinien siehe:

http://msdn2.microsoft.com/en-us/library/aa374177.aspx



Acronis Backup & Recovery 10 Storage Node

Der nachfolgende Abschnitt erläutert die Parameter des Acronis Backup & Recovery 10 Storage Nodes, die unter Verwendung des Acronis Administrative Template konfiguriert werden können.

Client Connection Limit

Beschreibung: Spezifiziert die maximale Zahl gleichzeitiger Verbindungen zum Storage Node

durch die Agenten, die Backup- oder Recovery-Aktionen ausführen.

*Mögliche Werte:*Jede ganze Zahl zwischen **1** und **2.147.483.647**

Standardwert: **10**

Acronis Backup & Recovery 10-Agenten verbinden sich mit dem Storage Node, um bei Backups oder Wiederherstellungen auf seine verwalteten Depots zuzugreifen. Der Parameter **Client Connection Limit** bestimmt die maximale Zahl solcher Verbindungen, die der Storage Node simultan handhaben kann.

Wenn diese Grenze erreicht ist, wird der Storage Node die Backup-Warteschlange (siehe Parameter) für die Agenten benutzen, die Verbindung erwarten.

Backup Queue Limit

Beschreibung: Spezifiziert die maximale Zahl von Acronis Backup & Recovery 10-Komponenten in der Storage Node-Backup-Warteschlange.

*Mögliche Werte:*Jede ganze Zahl zwischen **1** und **2.147.483.647**

Standardwert: **50**

Die Backup-Warteschlange ist eine Liste von Acronis Backup & Recovery 10-Komponenten, die auf eine Verbindung zum Storage Node warten – oder die gegenwärtig zu ihm verbunden sind (siehe vorherigen Parameter).

Sollte die Zahl der Komponenten in der Backup-Queue gleich dem Wert in **Backup Queue Limit** sein und eine weitere Komponente eine Verbindung aufzubauen versuchen, so stellt der Storage Node diese Komponente nicht in die Warteschlange.

In diesem Fall schlägt die Verbindung der Komponente zum Storage Node fehl. Sollte es sich bei der Komponente um einen Acronis Backup & Recovery 10 Agent handeln, so wird der korrespondierende Backup- bzw. Recovery-Task mit dem Status **Fehlgeschlagen** gestoppt.

Depot-Warnungen und -Beschränkungen

Spezifiziert die Menge freien Speicherplatzes in einem Depot (als absoluten Wert und prozentual) unterhalb derer ein Fehler im Log aufgezeichnet wird.

Dieser Parameter enthält die folgenden Einstellungen:

Vault Free Space Warning Limit

Beschreibung: Spezifiziert die Menge freien Speicherplatzes in einem verwalteten Depot, in Megabyte, unterhalb derer eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **200**

Der freie Speicherplatz eines Depots ist die Menge freien Speicherplatzes eines Mediums, etwa ein Laufwerk-Volume, welches das Depot enthält.

Falls die Menge freien Speicherplatzes in einem Depot einen Wert erreicht, der gleich oder geringer ist als unter **Vault Free Space Warning Limit** angegeben, wird eine Warnmeldung in die Ereignisanzeige des Depots aufgenommen und so auf das betreffende Depot hingewiesen. Sie können die Warnmeldungen des Storage Nodes im Dashboard einsehen.

Vault Free Space Warning Percentage

Beschreibung: Spezifiziert die Menge freien Speicherplatzes in einem verwalteten Depot, in Prozent seiner Gesamtgröße, unterhalb derer eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **10**

Die Gesamtgröße eines Depots entspricht seinem freien Speicherplatz plus der Größe aller in diesem Depot enthaltenen Archive.

Ein Beispiel: Angenommen, zwei Depots, Depot A und Depot B, sind beide auf einem Laufwerk gespeichert. Nehmen Sie weiter an, die Größe der Archive im Depot A ist 20 GB ist und die Größe der Archive im Depot B beträgt 45 GB.

Sollte das Laufwerk 5 GB freien Speicherplatz haben, so beträgt die Gesamtgröße des Depots A 20 GB + 5 GB = 25 GB und die des Depots B 45 GB + 5 GB = 50 GB – unabhängig von der Größe des Laufwerkes.

Der Prozentsatz an freiem Speicherplatz eines Depots entspricht seinem freien Platz geteilt durch seine Gesamtgröße. In Bezug auf das vorherige Beispiel entspricht das beim Depot A 5 GB / 25 GB = 20% an freien Speicherplatz – während Depot B 5 GB / 50 GB = 10% an freiem Speicherplatz hat.

Falls der Prozentsatz an freiem Platz in einem Depot einen Wert erreicht, der gleich oder geringer ist als unter **Vault Free Space Warning Percentage** angegeben, wird eine Warnmeldung in die Ereignisanzeige des Depots aufgenommen und so auf das betreffende Depot hingewiesen. Sie können die Warnmeldungen des Storage Nodes im Dashboard einsehen.

Anmerkung: *Die Parameter* ***Vault Free Space Warning Limit*** *und* ***Vault Free Space Warning Percentage*** *sind unabhängig voneinander. Jedes Mal, wenn einer der beiden Schwellenwerte erreicht wird, wird eine Warnmeldung aufgenommen.*

Vault Free Space Error Limit

Beschreibung: Spezifiziert die Menge freien Speicherplatzes in einem verwalteten Depot, in Megabyte, unterhalb derer eine Fehlermeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird und jedes Backup zum Depot unterbunden wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **50**

Falls die Menge freien Platzes in einem Depot einen Wert erreicht, der gleich oder geringer ist als unter **Vault Free Space Error Limit** angegeben, wird eine Fehlermeldung in die Ereignisanzeige des Depots aufgenommen. Backups, die in das Depot ausgeführt werden, werden solange scheitern, bis der freie Platz des Depots wieder über dem Limit liegt.

Vault Database Free Space Warning Limit

Beschreibung: Spezifiziert die Menge freien Speicherplatzes (in Megabyte) eines Laufwerks, welches die Datenbank eines verwalteten Depots enthält, unterhalb derer eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **20**

Falls die Menge freien Speicherplatzes auf dem Volume, welches die Datenbank eines verwalteten Depots enthält, einen Wert erreicht, der gleich oder geringer ist als unter **Vault Database Free Space Warning Limit** angegeben, wird eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen und so auf das betreffende Depot hingewiesen. Sie können die Warnmeldungen des Storage Nodes im Dashboard einsehen.

Die Datenbank wird im Depot in einem lokalen Ordner gespeichert, dessen Name bei Erstellung des Depots im **Datenbank-Pfad** spezifiziert wird.

Vault Database FreeSpace Error Limit

Beschreibung: Spezifiziert die Menge freien Speicherplatzes (in Megabyte) eines Laufwerks, welches die Datenbank eines verwalteten Depots enthält, unterhalb derer eine

Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird und jedes Backup zum Depot unterbunden wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **10**

Falls die Menge freien Platzes auf dem Laufwerk, das die Datenbank eines verwalteten Depots enthält, einen Wert erreicht, der gleich oder geringer ist als unter **Vault Database Free Space Error Limit** angegeben, wird eine Fehlermeldung in die Ereignisanzeige des Storage Nodes aufgenommen. Backups, die in das Depot ausgeführt werden, werden solange scheitern, bis der freie Platz wieder über dem Limit liegt.

Sie können die Fehlermeldungen des Storage Nodes im Dashboard einsehen.

Die Datenbank wird im Depot in einem lokalen Ordner gespeichert, dessen Name bei Erstellung des Depots unter '**Datenbank-Pfad**' spezifiziert wird.

Acronis Backup & Recovery 10 Management Server

Der nachfolgende Abschnitt erläutert die Parameter des Acronis Backup & Recovery 10 Management Server, die unter Verwendung des Acronis Administrative Template konfiguriert werden können.

Collecting Logs

Spezifiziert, wann Log-Einträge von Maschinen gesammelt werden, die durch den Acronis Backup & Recovery 10 Management Server verwaltet werden.

Dieser Parameter enthält zwei Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob Log-Einträge über die Ereignisse der Komponenten auf den registrierten Maschinen erfasst werden sollen.

Mögliche Werte: **True** oder **False**

Standardwert: True

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad der gesammelten Einträge. Nur Einträge mit Leveln größer oder gleich zu den unter **Trace Level** angegebenen Werten werden gesammelt.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: 0 (alle Einträge werden gesammelt)

Bereinigungsregeln für das Log

Spezifiziert, wie das zentrale Ereignis-Log bereinigt wird, das in der Berichtsdatenbank des Management Servers gespeichert ist.

Dieser Parameter hat die folgenden Einstellungen:

Maximale Größe

Beschreibung: Spezifiziert die maximale Größe des zentralen Ereignis-Logs in Kilobyte.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **1048576** (1 GB)

Zu erhaltender Anteil

Beschreibung: Spezifiziert die maximale Log-Größe in Prozent, die bei der Bereinigung zu erhalten ist

Mögliche Werte: Jede ganze Zahl zwischen **0** und **100**

Standardwert: **95**

Details zur Bereinigung des zentralen Ereignis-Logs finden Sie unter Bereinigungsregeln für das Log (S. 88).

Windows Event Log

Spezifiziert, wann Ereignisse von Acronis Backup & Recovery 10 Management Server in der Ereignisanzeige von Windows aufgezeichnet werden.

Dieser Parameter hat zwei Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob die Ereignisse des Acronis Backup & Recovery 10 Management Servers im Ereignis-Log aufgezeichnet werden sollen.

Mögliche Werte: **True** oder **False**

Standardwert: False

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad von Ereignissen, damit diese in das Ereignis-Log aufgenommen werden. Nur Ereignisse mit Leveln größer oder gleich zu den unter **Trace Level** angegebenen Werten werden gesammelt.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: **4** (nur Fehler und kritische Fehler werden aufgezeichnet — falls **Trace State** auf **True** gesetzt ist)

SNMP

Spezifiziert die Art der Ereignisse des Management Servers, über die Benachrichtigungen mit Hilfe des Simple Network Management Protocols (SNMP) verschickt werden sollen.

Dieser Parameter enthält folgende Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob SNMP-Benachrichtigungen verschickt werden sollen.

Mögliche Werte: **True** oder **False**

Standardwert: False

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad der Ereignisse, damit SNMP-Benachrichtigungen über diese verschickt werden. Nur Benachrichtigungen über Ereignisse, deren Schweregrad größer oder gleich zu **Trace Level** ist, werden versendet.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: 4 (nur Fehler und kritische Fehler werden gesendet – falls **Trace State** auf **True** gesetzt ist)

SNMP-Adresse

Beschreibung: Spezifiziert den Netzwerknamen oder die IP-Adresse des SNMP-Servers.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

SNMP-Community

Beschreibung: Spezifiziert den Community-Namen für die SNMP-Benachrichtigungen.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: öffentlich

Synchronisation

Spezifiziert, wie sich der Acronis Backup & Recovery 10 Management Server mit registrierten Maschinen verbindet, um zentrale Richtlinien zu verteilen, Logs und Backup-Plan-Zustände zu erfragen und ähnliche Aktionen – zusammenfassend Synchronisation genannt.

Dieser Parameter hat die folgenden Einstellungen:

Maximum Connections

Beschreibung: Spezifiziert die maximale Zahl gleichzeitiger Synchronisationsverbindungen, die aufrechterhalten werden sollen.

Mögliche Werte: Jede ganze Zahl zwischen 1 und 500

Standardwert: 200

Solange die Gesamtzahl online registrierter Maschinen den unter **Maximum Connections** angegebenen Wert nicht überschreitet, wird die Verbindung zu diesen Maschinen immer aufrechterhalten und führt der Management Server mit jeder Maschine periodische Synchronisationen aus.

Im anderen Fall verbindet er sich mit der Zahl von registrierten Maschinen, die der zugewiesenen Anzahl gleichzeitiger Verbindungen entspricht. Wurde die Synchronisation für eine Maschine abgeschlossen, so trennt sich der Management Server von dieser und nutzt die freigewordene Verbindung zur Synchronisation mit einer weiteren Maschine und so weiter.

(Anmerkung: Verbindungen zu Maschinen mit hoher Synchronisations-Priorität — siehe **Periode-High Priority** später in diesem Abschnitt — werden voraussichtlich immer aufrechterhalten.)

Synchronisations-Verbindungen haben nichts mit den Verbindungen zu tun, wie sie zwischen Acronis Backup & Recovery 10 Management Server und der Acronis Backup & Recovery 10 Management Console erfolgen.

Maximum Workers

Beschreibung: Spezifiziert die maximale Zahl von Threads, die zur Synchronisation verwendet werden sollen.

Mögliche Werte: Jede ganze Zahl zwischen 1 und 100

Standardwert: 30

Der Prozess des Management Servers nutzt spezielle Threads – auch Arbeits-Threads genannt – um die Synchronisation mit einer registrierten, verbundenen Maschine durchzuführen.

Jeder Arbeits-Thread führt die Synchronisation nur mit je einer Maschine gleichzeitig aus.

Eine zur Synchronisation verbundene Maschine wartet auf einen verfügbaren Arbeits-Thread. Daher wird die tatsächliche Zahl von Arbeits-Threads nie die maximale Zahl von Verbindungen überschreiten (siehe **Maximum Connections**, wie zuvor beschrieben).

Periode (in Sekunden)

Beschreibung: Spezifiziert, wie oft (in Sekunden) die Synchronisation für Maschinen, die eine normale Synchronisationspriorität haben, durchgeführt wird – typischerweise Maschinen ohne aktuell ausgeführte, zentrale Backup-Tasks.

Mögliche Werte: Jede ganze Zahl zwischen 120 und 2147483647

Standardwert: 120

Der Acronis Backup & Recovery 10 Management Server versucht die Synchronisation für jede Maschine mit normaler Priorität je einmal innerhalb des Zeitraums durchzuführen, der in

Sekunden über **Period** vorgegeben wurde – wobei er je einen verfügbaren Arbeits-Thread verwendet (siehe **Maximum Workers**, wie zuvor beschrieben).

Sollte es weniger Arbeits-Threads als Maschinen mit normaler Priorität geben, so kann das tatsächliche Intervall zwischen den Synchronisationen länger als der angegebene Wert des Parameters sein.

Period-High Priority (in Sekunden)

Beschreibung: Spezifiziert, wie oft (in Sekunden) die Synchronisation für Maschinen, die eine hohe Synchronisationspriorität haben, durchgeführt wird – typischerweise Maschinen mit aktuell ausgeführten, zentralen Backup-Tasks.

Mögliche Werte: Jede ganze Zahl zwischen 15 und 2147483647

Standardwert: 15

Dieser Parameter ist analog zu dem eben beschriebenen Parameter **Period**.

Real-Time Monitoring

Beschreibung: Spezifiziert, ob ein Echtzeit-Monitoring von registrierten Maschinen durchgeführt werden soll, statt einen Polling-Mechanimus zu verwenden.

Mögliche Werte: **True** oder **False**

Standardwert: False

Standardmäßig ist es der Acronis Backup & Recovery 10 Management Server, der sich mit den registrierten Maschinen verbindet, um eine Synchronisation durchzuführen – insbesondere, um Daten wie Backup-Logs abzurufen. Dieser Ansatz ist auch als Polling-Mechanismus bekannt.

Falls jedoch **Real Time Monitoring** auf **True** gesetzt ist, sendet der Management Server stattdessen Anfragen an die Maschinen, neue Daten anzubieten, wenn diese auftauchen bzw. entstehen – und geht dann in einen Lauschmodus. Dieser Ansatz wird Echtzeit-Monitoring genannt.

Echtzeit-Monitoring kann den Netzwerkverkehr reduzieren – z.B. wenn zentrale Backup-Tasks selten ablaufen. Es ist jedoch nur dann effektiv, wenn es relativ wenig registrierte Maschinen gibt.

Vermeiden Sie es, Echtzeit-Monitoring zu aktivieren, wenn die Zahl an registrierten Maschinen die maximale Zahl gleichzeitiger Verbindungen übersteigt (siehe **Maximum Connections**, weiter oben in diesem Abschnitt).

Zweiter Verbindungsversuch

Beschreibung: Spezifiziert, ob ein erneuter Verbindungsversuch zu einer registrierten Maschine unternommen werden soll, indem die letztbekannte IP-Adresse verwendet wird, nachdem ein Verbindungsversuch unter Verwendung des Host-Namens gescheitert ist.

Mögliche Werte: **True** oder **False**

Standardwert: False

Der Acronis Backup & Recovery 10 Management Server verwendet beim Verbindungsversuch mit einer registrierten Maschine zuerst ihren Netzwerknamen – vorausgesetzt die Maschine wurde dem Management Server über ihren Namen hinzugefügt.

Falls der Parameter **Second Connection Attempt** auf **True** gesetzt ist und eine Verbindung zur Maschine unter Verwendung ihres Netzwerknamens gescheitert ist, so macht der Management Server einen zweiten Verbindungsversuch, indem er diesmal die letzte IP-Adresse verwendet, die mit diesem Netzwerknamen assoziiert war.

Wir empfehlen, den Parameter **Second Connection Attempt** nur in solchen Netzwerken auf **True** zu setzen, die denen es häufiger zu Problemen mit DNS-Servern kommt und wo sich die IP-Adressen der Maschinen selten ändern (ist z.B. der Fall bei festen IP-Adressen oder langen

DHCP-Lease-Zeiten).

Diese Einstellung hat keinen Effekt auf Maschinen, die dem Management Server über eine IP-Adresse hinzugefügt wurden.

Offline Period Threshold (in Sekunden)

Beschreibung: Spezifiziert das maximale Intervall, in Sekunden, zwischen den erneuten Verbindungsversuchen zu einer registrierten Maschine, die offline zu sein scheint.

Mögliche Werte: Jede ganze Zahl zwischen 120 und 2147483647

Standardwert: 1800

Normalerweise verbindet sich der Management Server zu jeder registrierten Maschine nach einem bestimmten Zeitintervall (siehe **Period** und **Period-High Priority** zuvor in diesem Abschnitt). Wenn der Management Server entdeckt, dass die Maschine offline ist, verdoppelt er dieses Intervall; er behält die Verdopplung dieses Intervalls mit jedem Folgeversuch bei, bis der unter **Offline Period Threshold** spezifizierte Wert erreicht ist. Sobald die Maschine wieder online ist, wird das Zeitintervall erneut normal.

Dieser Ansatz hat das Ziel, die Ressourcen des Management Servers effizient zu nutzen und die Netzwerklast zu reduzieren.

Backup

Spezifiziert den Ort und die Anfangsgröße des Storages für Snapshots – eine temporäre Datei, die beim Backup der Daten durch einen Snapshot benutzt wird. Die Datei wird gelöscht, sobald das Backup vollständig ist.

Mit der Standardeinstellung wird der Storage für Snapshots im temporären Windows-Ordner eingerichtet und belegt 50 Prozent des verfügbaren Platzes, der auf dem Volume vorhanden ist, das diesen Ordner enthält. Es wird mehr Platz verwendet, wenn das für den Snapshot erforderlich ist.

Sie können die Anfangsgröße für den Snapshot-Storage erhöhen – oder diesen auf ein anderes Volume verlegen – wenn Probleme mit dem Backup von Daten auftreten, die sich während des Backups umfangreich ändern.

Dieser Parameter wird benutzt beim Erstellen einer Backup-Richtlinie und auf alle zentralen Backup-Pläne angewandt, die auf dieser Richtlinie basieren. Änderungen an diese Parameter beeinflussen bereits existierende Backup-Richtlinien (und deren zentralen Backup-Pläne) nicht.

Dieser Parameter hat die folgenden Einstellungen:

Snapshot Storage Path

Beschreibung: Spezifiziert das Verzeichnis, in dem der Snapshot-Storage platziert wird.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Wenn keine Eintragung vorgenommen wird, wird das temporäre Verzeichnis benutzt, das üblicherweise durch die Umgebungsvariablen TMP oder TEMP definiert ist.

Sie können einen lokalen Ordner auf einem beliebigen Volume angeben, einschließlich eines Volumes, das Sie sichern.

Snapshot Storage Absolute Size

Beschreibung: Spezifiziert die Anfangsgröße des Snapshot-Storages in Megabyte.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **0**

Bei Vorgabe von **0** benutzt der Management Server die Einstellung bei **Snapshot Storage Relative Size**.

Die Anfangsgröße wird den verfügbaren Platz abzüglich 50 MB nicht überschreiten.

Snapshot Storage Relative Size

Diese Einstellung ist nur wirksam, wenn die bei **Snapshot Storage Absolute Size** der Wert **0** eingestellt ist.

Beschreibung: Spezifiziert die Anfangsgröße des Snapshot-Storages als Prozentwert des Festplattenplatzes, der zum Zeitpunkt des Backup-Starts zur Verfügung steht.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **100**

Standardwert: **50**

Beträgt der Wert **0**, dann wird kein Snapshot-Storage erstellt.

Die Anfangsgröße wird den verfügbaren Platz abzüglich 50 MB nicht überschreiten.

Die Erstellung von Snapshots ist auch ohne Snapshot-Storage möglich.

Die Größe des Snapshot-Storages beeinflusst die Größe des Backups nicht.

Acronis Backup & Recovery 10 Agent für Windows

Der nachfolgende Abschnitt erläutert die Parameter des Acronis Backup & Recovery 10-Agenten, die unter Verwendung des Acronis Administrative Template konfiguriert werden können.

Lizenzierung

Spezifiziert, wie oft der Agent seine Lizenz auf dem License Server überprüft und wie lange er ohne einen License Server arbeiten kann.

License Check Interval (in Tagen)

Beschreibung: Spezifiziert, wie oft (in Tagen) nach Lizenz-Verfügbarkeit auf dem Acronis License Server geprüft werden soll.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **5**

Standardwert: 1

Der Acronis Backup & Recovery 10 Agent überprüft periodisch, ob sein Lizenzschlüssel auf dem License Server vorhanden ist. Die erste Überprüfung wird jedes Mal durchgeführt, wenn der Acronis Backup & Recovery 10 Agent startet, weitere Überprüfungen erfolgen dann je einmal in der Zahl von Tagen, die unter **License Check Interval** angegeben wurden.

Eine Warnung wird in die Ereignisanzeige des Agenten aufgenommen, wenn er sich nicht mit dem License Server verbinden kann. Sie können die Warnung im Dashboard einsehen.

Wenn der Wert **0** beträgt, wird keine Lizenzprüfung durchgeführt; ohne Lizenz wird die Funktionalität von Acronis Backup & Recovery 10 nach der Zahl von Tagen deaktiviert, die unter **Maximum Time Without License Server** vorgegeben wurde (siehe nächsten Parameter).

Siehe auch **License Server Connection Retry Interval** weiter unten in diesem Abschnitt.

Maximum Time Without License Server (in Tagen)

Beschreibung: Spezifizieren Sie, wie viele Tage Acronis Backup & Recovery 10 normal arbeiten wird, bis seine Funktionalität deaktiviert wird.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **60**

Standardwert: 30

Falls der Acronis License Server nicht verfügbar ist, wird Acronis Backup & Recovery 10 für die Zahl an Tagen mit voller Funktionalität weiterarbeiten, wie unter **Maximum Time Without License Server** spezifiziert – gezählt vom Beginn der Installation oder von der letzten erfolgreichen Überprüfung.

License Server Connection Retry Interval (in Stunden)

Beschreibung: Spezifiziert das Intervall, in Stunden, zwischen zwei Verbindungsversuchen,

falls der Acronis License Server nicht verfügbar ist.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **24**

Standardwert: 1

Falls während einer Lizenzschlüssel-Überprüfung (siehe **License Check Interval**, weiter oben in diesem Abschnitt) der Acronis Backup & Recovery 10 Agent sich nicht mit dem License Server verbinden konnte, so wird er dies je einmal innerhalb der Zahl an Stunden erneut versuchen, wie sie über **License Server Connection Retry Interval** vorgegeben wurden.

Sollte der Wert **0** betragen, so erfolgen keine erneuten Verbindungsversuche, der Agent überprüft stattdessen die Lizenz nur noch wie durch **License Check Interval** bestimmt.

License Server Address

Beschreibung: Spezifiziert den Netzwerknamen oder die IP-Adresse des Acronis License Servers.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Bereinigungsregeln für das Log

Spezifiziert, wie das Log das Agenten bereinigt wird.

Dieser Parameter hat die folgenden Einstellungen:

Maximale Größe

Beschreibung: Spezifiziert die maximale Größe des Log-Ordners des Agenten in Kilobyte.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **1048576** (1 GB)

Zu erhaltender Anteil

Beschreibung: Spezifiziert die maximale Log-Größe in Prozent, die bei der Bereinigung zu erhalten ist.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **100**

Standardwert: **95**

Details zur Bereinigung des Agent-Logs finden Sie unter Bereinigungsregeln für das Log (S. 95).

Windows Event Log

Spezifiziert, wann Ereignisse von Acronis Backup & Recovery 10 Agent in der Ereignisanzeige von Windows aufgezeichnet werden.

Dieser Parameter hat zwei Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob die Ereignisse des Agenten in das Ereignis-Log aufgenommen werden sollen.

Mögliche Werte: **True** oder **False**

Standardwert: False

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad von Ereignissen, damit diese in das Ereignis-Log aufgenommen werden. Nur Ereignisse mit Leveln größer oder gleich zu den unter **Trace Level** angegebenen Werten werden gesammelt.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: **4** (nur Fehler und kritische Fehler werden aufgezeichnet — falls **Trace State** auf **True** gesetzt ist)

SNMP

Spezifiziert die Art der Ereignisse des Agenten, über die Benachrichtigungen mit Hilfe des Simple Network Management Protocols (SNMP) verschickt werden sollen.

Dieser Parameter hat die folgenden Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob SNMP-Benachrichtigungen verschickt werden sollen.

Mögliche Werte: **True** oder **False**

Standardwert: False

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad der Ereignisse, damit SNMP-Benachrichtigungen über diese verschickt werden. Nur Benachrichtigungen über Ereignisse, deren Schweregrad größer oder gleich zu **Trace Level** ist, werden versendet.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: **4** (nur Fehler und kritische Fehler werden aufgezeichnet — falls **Trace State** auf **True** gesetzt ist)

SNMP-Adresse

Beschreibung: Spezifiziert den Netzwerknamen oder die IP-Adresse des SNMP-Servers.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

SNMP-Community

Beschreibung: Spezifiziert den Community-Namen für die SNMP-Benachrichtigungen.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: öffentlich

Backup

Spezifiziert den Ort und die Anfangsgröße des Storages für Snapshots – eine temporäre Datei, die beim Backup der Daten durch einen Snapshot benutzt wird. Die Datei wird gelöscht, sobald das Backup vollständig ist.

Mit der Standardeinstellung wird der Storage für Snapshots im temporären Windows-Ordner eingerichtet und mit 50 Prozent des verfügbaren Platzes initialisiert, der auf dem Volume vorhanden ist, das diesen Ordner enthält. Es wird mehr Platz verwendet, wenn das für den Snapshot erforderlich ist.

Sie können die Anfangsgröße für den Snapshot-Storage erhöhen – oder diesen auf ein anderes Volume verlegen – wenn Probleme mit dem Backup von Daten auftreten, die sich während des Backups umfangreich ändern.

Dieser Parameter wird bei Erstellung eines Backup-Plans verwendet. Eine Änderung dieses Parameters wirkt sich nicht auf existierende Backup-Pläne aus.

Dieser Parameter hat die folgenden Einstellungen:

Snapshot Storage Path

Beschreibung: Spezifiziert das Verzeichnis, in dem der Snapshot-Storage erstellt wird.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Wenn keine Eintragung vorgenommen wird, wird das temporäre Verzeichnis benutzt, das üblicherweise durch die Umgebungsvariablen TMP oder TEMP definiert ist.

Sie können einen lokalen Ordner auf einem beliebigen Volume angeben, einschließlich eines Volumes, das Sie sichern.

Snapshot Storage Absolute Size

Beschreibung: Spezifiziert die Anfangsgröße des Snapshot-Storages in Megabyte.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **0**

Bei Vorgabe von **0** benutzt der Management Server die Einstellung bei **Relative Größe des Snapshot-Storages**.

Die Anfangsgröße wird den verfügbaren Platz abzüglich 50 MB nicht überschreiten.

Snapshot Storage Relative Size

Diese Einstellung ist nur wirksam, wenn die bei **Snapshot Storage Absolute Size** der Wert **0** eingestellt ist.

Beschreibung: Spezifiziert die Anfangsgröße des Snapshot-Storages als Prozentwert des Festplattenplatzes, der zum Zeitpunkt des Backup-Starts zur Verfügung steht.

Mögliche Werte: Jede ganze Zahl zwischen **0** und **100**

Standardwert: **50**

Beträgt der Wert **0**, dann wird kein Snapshot-Storage erstellt.

Die Anfangsgröße wird den verfügbaren Platz abzüglich 50 MB nicht überschreiten.

Die Erstellung von Snapshots ist auch ohne Snapshot-Storage möglich.

Die Größe des Snapshot-Storages beeinflusst die Größe des Backups nicht.

Acronis Backup & Recovery 10

Dieser Abschnitt der administrativen Vorlage spezifiziert die Verbindungsparameter und Parameter zur Ereignisverfolgung für die nachfolgenden Acronis Backup & Recovery 10-Komponenten:

- Acronis Backup & Recovery 10 Management Server
- Acronis Backup & Recovery 10 Agent
- Acronis Backup & Recovery 10 Storage Node

Verbindungsparameter

Ports für Remote Agent

Spezifiziert den Port, den die Komponente für eingehende und ausgehende Kommunikation mit anderen Acronis-Komponenten verwendet.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird den Standard-TCP-Port mit der Nummer 9876 verwenden.

Aktiviert

Die Komponente wird den angegebenen Port verwenden; geben Sie die entsprechende Port-Nummer in das Feld **Server TCP-Port** ein.

Deaktiviert

Gleichbedeutend mit **Nicht konfiguriert**.

Optionen für Client-Verschlüsselung

Spezifiziert, ob eine verschlüsselte Datenübertragung erfolgt, sofern die Komponente als Client-Applikation agiert, und ob selbst-signierten SSL-Zertifikaten vertraut wird.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird die Standardeinstellungen verwenden, also möglichst mit Verschlüsselung zu arbeiten und selbst-signierten SSL-Zertifikaten zu vertrauen (siehe die nachfolgende Option).

Aktiviert

Verschlüsselung ist eingeschaltet. Wählen Sie in **Verschlüsselung** Folgendes:

Aktiviert

Die Datenübertragung erfolgt verschlüsselt, falls auch bei der Server-Applikation die Verschlüsselung eingeschaltet ist, anderenfalls bleibt die Übertragung unverschlüsselt.

Deaktiviert

Verschlüsselung ist ausgeschaltet – es werden keine Verbindungen zu Server-Applikationen aufgebaut, die eine Verschlüsselung erfordern.

Erforderlich

Die Datenübertragung erfolgt verschlüsselt, wird aber nur aufgebaut, falls bei der Server-Applikation die Verschlüsselung aktiviert ist (siehe „Optionen für Server-Verschlüsselung“).

Parameter zur Authentifizierung

Eine Aktivierung des Kontrollkästchens **Selbst-signierten Zertifikaten vertrauen** erlaubt dem Client, sich mit einer Server-Applikation zu verbinden, die selbst-signierte SSL-Zertifikate benutzt (wie solche Zertifikate, die während der Installation von Acronis Backup & Recovery 10-Komponenten erstellt wurden) — siehe SSL-Zertifikate (S. 84).

Sie sollten dieses Kontrollkästchen aktiviert lassen, außer Sie verwenden in Ihrem Umfeld eine Public Key-Infrastruktur (PKI).

Wählen Sie Folgendes in **Verwende Agent-Zertifikatsauthentifizierung**:

Nicht verwenden

Die Verwendung von SSL-Zertifikaten ist deaktiviert. Zu Server-Applikationen, die die Verwendung von SSL-Zertifikaten erfordern, werden keine Verbindungen aufgebaut.

Verwende wenn möglich

Die Verwendung von SSL-Zertifikaten ist aktiviert. Der Client wird SSL-Zertifikate nutzen, sofern ihre Verwendung auch bei der Server-Applikation eingeschaltet ist – anderenfalls werden sie nicht verwendet.

Immer verwenden

Die Verwendung von SSL-Zertifikaten ist aktiviert. Die Verbindung wird nur dann aufgebaut, wenn die Verwendung von SSL-Zertifikaten auch auf der Server-Applikation eingeschaltet ist.

Deaktiviert

Gleichbedeutend mit **Nicht konfiguriert**.

Optionen für Server-Verschlüsselung

Spezifiziert, ob die Datenübertragung verschlüsselt erfolgen soll, wenn die Komponente als Server-Applikation agiert.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird die Standardeinstellung verwenden, welche „verwende Verschlüsselung wenn möglich“ ist (siehe nachfolgende Option).

Aktiviert

Verschlüsselung ist eingeschaltet. Wählen Sie in **Verschlüsselung** Folgendes:

Aktiviert

Die Datenübertragung erfolgt verschlüsselt, falls auch bei der Client-Applikation die Verschlüsselung eingeschaltet ist, anderenfalls bleibt die Übertragung unverschlüsselt.

Deaktiviert

Verschlüsselung ist deaktiviert; es werden keine Verbindungen zu Client-Applikationen aufgebaut, die eine Verschlüsselung erfordern.

Erforderlich

Die Datenübertragung erfolgt verschlüsselt, wird aber nur aufgebaut, falls bei der Client-Applikation die Verschlüsselung aktiviert ist (siehe „Optionen für Client-Verschlüsselung“).

Parameter zur Authentifizierung

Wählen Sie Folgendes in **Verwende Agent-Zertifikatsauthentifizierung**:

Nicht verwenden

Die Verwendung von SSL-Zertifikaten ist deaktiviert. Zu Client-Applikation, die die Verwendung von SSL-Zertifikaten erfordern, werden keine Verbindungen aufgebaut.

Verwende wenn möglich

Die Verwendung von SSL-Zertifikaten ist aktiviert. Der Server wird SSL-Zertifikate nutzen, sofern ihre Verwendung auch bei der Client-Applikation eingeschaltet ist – anderenfalls werden sie nicht verwendet.

Immer verwenden

Die Verwendung von SSL-Zertifikaten ist aktiviert. Die Verbindung wird nur dann aufgebaut, wenn die Verwendung von SSL-Zertifikaten auch auf der Client-Applikation eingeschaltet ist.

Deaktiviert

Gleichbedeutend mit **Nicht konfiguriert**.

Parameter für die Ereignisverfolgung

In Windows können Ereignisse, die in Acronis Backup & Recovery 10 auftreten, in der Ereignisanzeige, in eine Datei oder beides aufgezeichnet werden.

Jedes Ereignis hat ein Level von Null bis Fünf, basierend auf dem Schweregrad des Ereignisses – wie in der nachfolgenden Tabelle aufgelistet:

Level	Name	Beschreibung
0	Unbekannt	Ereignis, dessen Schweregrad unbekannt oder nicht zutreffend ist
1	Debug	Für Debug-Zwecke verwendetes Ereignis
2	Informationen	Informierendes Ereignis, wie etwa über den erfolgreichen Aktionsabschluss oder Start eines Dienstes
3	Warnung	Ereignis, das ein möglicherweise bevorstehendes Problem ist, wie etwa zu wenig freier Platz in einem Depot
4	Fehler	Ereignis, das zum Verlust von Daten oder Funktionalität führte
5	Kritisch	Ereignis, das zum Abbruch eines Prozesses (z.B. Prozess des Agenten) führte

Ereignis-verfolgende Parameter werden über folgende Einstellungen im administrativen Template

spezifiziert:

File Trace Minimal Level

Beschreibung: Spezifiziert den niedrigsten Schweregrad, ab dem Ereignisse in die Datei aufgezeichnet werden. Nur Ereignisse mit Leveln größer oder gleich zu **File Trace Minimal Level** werden aufgezeichnet.

Mögliche Werte: Jeder Schweregrad von **Unbekannt** bis **Kritisch** oder **Blockiert**, um überhaupt keine Ereignisse aufzuzeichnen

Standardwert: 2 (Ereignisse mit Schweregrad 2 bis 5 werden aufgezeichnet)

Die Log-Dateien befinden sich innerhalb des Ordners **%ALLUSERSPROFILE%\Application Data\Acronis**, im Unterverzeichnis **Logs** für die betreffende Komponente.

Win32 Trace Minimal Level

Beschreibung: Spezifiziert den niedrigsten Schweregrad, ab dem Ereignisse in der Ereignisanzeige des Systems aufgezeichnet werden. Nur Ereignisse mit Leveln größer oder gleich zu **Win32 Trace Minimal Level** werden aufgezeichnet.

Mögliche Werte: Jeder Schweregrad von **Unbekannt** bis **Kritisch** oder **Blockiert**, um überhaupt keine Ereignisse aufzuzeichnen

Standardwert: 4 (Ereignisse über Fehler und kritische Fehler werden aufgezeichnet)

Programm zur Kundenzufriedenheit (CEP)

Spezifiziert, ob die Maschine, auf der die Acronis Backup & Recovery 10-Komponente installiert wird, am Programm zur Kundenzufriedenheit (CEP) teilnimmt.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Standardmäßig nimmt die Maschine nicht am Programm zur Kundenzufriedenheit (CEP) teil.

Aktiviert

Wählen Sie unter **Ermögliche, Berichte an Acronis zu senden** eine der folgenden Optionen:

Aktivieren

Auf der Maschine werden Informationen gesammelt (über die Hardware-Konfiguration, am häufigsten und am wenigsten verwendete Funktionen, sowie Probleme) und regelmäßig an Acronis geschickt. Die Ergebnisse sind dazu gedacht, Verbesserungen bei der Software und Funktionalität zu ermöglichen, um die Bedürfnisse von Acronis-Kunden noch besser zu erfüllen. Acronis sammelt keine persönliche Daten. Die Teilnahmebedingungen können auf der Acronis-Website gefunden werden.

Deaktivieren

Es wird keine Information verschickt.

Deaktiviert

Gleichbedeutend mit **Nicht konfiguriert**.

7.2.2 Per grafische Benutzeroberfläche (GUI) gesetzte Parameter

Die folgenden Parameter können mit Hilfe der grafischen Benutzeroberfläche (GUI) gesetzt werden:

- Für den Acronis Backup & Recovery 10 Management Server: **Collecting Logs**, **Windows Event Log**, **SNMP**, **SNMP Address** und **SNMP Community**
- Für Acronis Backup & Recovery 10 Agent: **Windows Event Log**, **SNMP**, **SNMP Address**, **SNMP Community** und **Customer Experience Program**

Sie finden die Beschreibung zu diesen Parametern im entsprechenden Abschnitt über die Konfiguration durch die administrative Vorlage.

7.2.3 Per Windows-Registry gesetzte Parameter

Der nachfolgende Abschnitt erläutert die Parameter des Acronis Backup & Recovery 10 Storage Nodes, die nur durch Bearbeitung der Registry konfiguriert werden können.

Auf Deduplizierung bezogene Parameter

CompactingTriggerThreshold

Beschreibung: Spezifiziert den Prozentsatz genutzter Elemente im Datenspeicher, unterhalb dessen Verdichtung stattfindet.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **80**

Registry-Schlüssel:
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ASN\Configuration\StorageNode\CompactingTriggerThreshold

Wenn Backups von einem deduplizierenden Depot gelöscht werden, können dessen deduplizierenden Datenspeicher (S. 71) ungenutzte Elemente enthalten: Dateien oder Laufwerkblöcke, auf die es von keinem Backup aus mehr einen Bezug gibt. Der Storage Node arbeitet beide Datenspeicher ab, damit die ungenutzten Elemente gelöscht werden. Diese Aktion wird 'Verdichten' bzw. 'Verdichtung' genannt.

Da Verdichtung eine Ressourcen verbrauchende Aktion ist, sollte sie nur stattfinden, wenn die Anzahl ungenutzer Elemente signifikant ist.

Der Parameter **CompactingTriggerThreshold** ermöglicht Ihnen, eine Balance zwischen dem für die ungenutzten Elemente benötigten, zusätzlichen Speicherplatz und der Verdichtungshäufigkeit einzustellen. Je größer der Wert dieses Parameters, desto weniger ungenutzte Elemente sind im Datenspeicher erlaubt – vermutlich ist jedoch eine häufigere Verdichtung notwendig.

Dieser Parameter gilt separat für Laufwerk- und Datei-basierte Backups. Verdichtung kann daher für einen Datenspeicher durchgeführt und für einen anderen übersprungen werden.

Auf Depot-Datenbanken bezogene Parameter

Die folgenden zwei Parameter bestimmten Pfade zu internen Datenbanken von Acronis Backup & Recovery 10 Storage Node, die Informationen über verwaltete Depots enthalten.

Die Datenbank, die in dem Ordner hinterlegt ist, der über den Parameter **DatabasePath** spezifiziert wird, ist üblicherweise klein. Die Datenbank, die jedoch in dem Ordner hinterlegt ist, der über den Parameter **TapeDatabasePath** spezifiziert wird (Band-Datenbank genannt), kann ziemlich groß werden, falls die Bandbibliothek Tausende von Archiven enthält. In diesem Fall könnten Sie erwägen, die Band-Datenbank auf einem anderen Volume zu speichern.

Wichtig: *Eine Modifikation dieser Parameter wird nicht empfohlen. Sollten Sie dennoch einen Parameter anpassen müssen, so tun Sie dies vor Erstellung eines korrespondierenden verwalteten Depots (Band oder Nicht-Band). Anderenfalls wird der Storage Node seinen Zugriff auf diese Depots solange verlieren, bis Sie diese wieder anbinden – das erneute Anbinden eines Storage Nodes, insbesondere eines selbst-deduplizierenden, kann jedoch eine beträchtliche Zeitspanne benötigen.*

DatabasePath

Beschreibung: Spezifiziert den Ordner, wo ein Acronis Backup & Recovery 10 Storage Node seine Datenbank der 'Nicht-Band'-Depots hinterlegt.

Diese Datenbank enthält eine Liste von Depots, die vom Storage Node verwaltet werden und keine Band-Depots sind (siehe nächsten Parameter). Ihre typische Größe liegt üblicherweise nicht über einigen Kilobyte.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: C:\Programme\Acronis\StorageNode

Registry-Schlüssel:
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ASN\Configuration\StorageNode\DatabasePath

TapesDatabasePath

Beschreibung: Spezifiziert den Ordner, wo ein Acronis Backup & Recovery 10 Storage Node seine Datenbank der Band-Depots hinterlegt.

Diese Datenbank enthält eine Liste von Band-Depots, die durch den Storage Node verwaltet werden. Ihre Größe hängt von der Zahl der Archive ab, die in der Bandbibliothek gespeichert sind – mit einer üblichen Entsprechung von 10 MB pro einhundert Archive.

Mögliche Werte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Acronis\BackupAndRecovery\TapeLocation\

Registry-Schlüssel:
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\TapesDatabasePath

7.3 Eine Backup-Richtlinie erstellen

Eine Backup-Richtlinie kann gleichermaßen auf Windows- und Linux-Maschinen angewendet werden.

Zur Erstellung einer Backup-Richtlinie führen Sie folgende Schritte aus.

Allgemein

Richtlinienname

[Optional] Geben Sie einen eindeutigen Namen für die Backup-Richtlinie ein. Ein bewusst gewählter Name macht es leichter, diese Richtlinie innerhalb anderer zu identifizieren.

Typ der Quelle

Wählen Sie die Art der Elemente, die Sie per Backup sichern wollen. **Laufwerk/Volume** oder **Dateien**.

Anmeldedaten der Richtlinie (S. 377)

[Optional] Sie können, sofern notwendig, die Konto-Anmeldedaten für die Richtlinie ändern. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Kommentare für die Richtlinie

[Optional] Geben Sie eine Beschreibung bzw. einen Kommentar für die Backup-Richtlinie ein. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Bezeichnung

[Optional] Geben Sie für die zu sichernde(n) Maschine(n) eine Textbezeichnung ein. Diese Bezeichnung kann verwendet werden, um die Maschine oder eine Gruppe von Maschinen in verschiedenen Szenarien zu identifizieren. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Backup-Quelle

Elemente für das Backup (S. 377)

Definieren Sie die zu sichernden Daten-Elemente auf jeder Maschine, zu der die Richtlinie verteilt wird. Auf jeder dieser Maschinen wird der Agent die Daten-Elemente durch Verwendung der von Ihnen spezifizierten Regeln finden. Wenn die Auswahlregel z.B. [Alle Volumes] umfasst, wird die ganze Maschine gesichert.

Anmeldeinformationen: (S. 382)

[Optional] Stellen Sie Anmeldedaten für die Quelldaten zur Verfügung, falls das Konto der Backup-Richtlinie keine Zugriffserlaubnis für diese Daten hat. Wählen Sie das Kontrollkästchen **Erweiterte Ansicht**, um auf diese Option zuzugreifen.

Ausschließungen (S. 383)

[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. 384)

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 Speicherort muss zu dem Zeitpunkt verfügbar sein, wenn der Management Server mit der Verteilung der Richtlinie beginnt.

Anmeldeinformationen: (S. 385)

[Optional] Stellen Sie Anmeldedaten für den Speicherort zur Verfügung, falls das Konto der Backup-Richtlinie keine Zugriffserlaubnis für diesen 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. 386)

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 wohlbekannte, 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

[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 im Management Server definierten Standardwerte (S. 97) 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-Richtlinie erstellen**-Seite immer nur Werte, die von den Standardeinstellungen abweichen.

Um alle Einstellungen auf Standardwerte zurückzusetzen, klicken Sie auf **Auf Standard zurücksetzen**.

Während der Backup-Aktion werden die Standardoptionen für Backups der registrierten Maschine ignoriert.

In VM konvertieren

Gilt für: **Laufwerk/Volume**-Backup

Nicht wirksam für Maschinen, die unter Linux laufen

Durch das Einrichten einer regelmäßigen Konvertierung erhalten Sie eine Kopie Ihres Servers oder Ihrer Workstation auf einer virtuellen Maschine, die sofort einsatzbereit ist, falls die ursprüngliche Maschine ausfällt. Die Konvertierung kann von jeder Maschine ausgeführt wird, die auf dem Management Server registriert ist und auf der sich der Acronis Backup & Recovery 10 Agent mit der entsprechenden Funktionalität befindet. Das Archiv muss an einem Speicherort mit Netzwerkfreigabe hinterlegt werden, wie einem Netzwerkordner oder einem verwalteten Depot, damit die gewählte Maschine auf das Archiv zugreifen kann.

Konvertierungszeitpunkt (S. 229)

[Optional] Geben Sie an, ob jedes vollständige, inkrementelle oder differentielle Backup konvertiert werden soll oder stellen Sie einen Zeitplan für die Konvertierung des jeweils letzten Backups auf. Geben Sie bei Bedarf einen Konvertierungsplan an.

Host (S. 230)

Geben Sie an, welche Maschine die Konvertierung ausführen soll. Auf der Maschine muss der Acronis Backup & Recovery 10 Agent für Windows, der Agent für ESX/ESXi oder der Agent für Hyper-V installiert sein.

Virtualisierungs-Server (S. 230)

Hier bestimmen Sie Typ und Speicherort der virtuellen Maschine. Welche Optionen verfügbar sind, hängt davon ab, welchen Host Sie im vorangehenden Schritt ausgewählt haben.

Storage (S. 230)

Wählen Sie auf dem Virtualisierungs-Server oder in dem Ordner einen Speicherort, an dem die Dateien für die Virtuelle Maschine gespeichert werden sollen.

Resultierende VMs

Spezifizieren Sie einen Namen für die zu erstellenden virtuellen Maschinen. Der Standardname besteht aus Variablen, die den Namen der Richtlinie und den Namen der zu sichernden Maschine reflektieren. Sie können dem Namen Suffixe anhängen, aber löschen Sie nie die Variablen, da jede virtuelle Maschine einen eindeutigen, noch nicht vergebenen Namen haben muss.

Ordner auf VMware vCenter

Wenn der Management Server mit dem vCenter Server integriert ist, erscheinen die resultierenden Maschinen im Ordner **Acronis Backups** auf dem vCenter. Sie können einen Unterordner für die Maschinen spezifizieren, die aus der Ausführung der Richtlinie

resultieren.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um die Backup-Richtlinie zu erstellen.

7.3.1 Anmeldedaten der Richtlinie

Geben Sie die Anmeldedaten ein, unter denen die zentralen Tasks auf den Maschinen laufen werden.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Acronis-Dienstes verwenden**

     Die Tasks werden unter dem Konto des Acronis-Dienstes ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.
   - **Folgende Anmeldedaten benutzen**

     Die Tasks werden 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**.

Um mehr über Anmeldedaten für Acronis-Dienste zu erfahren, siehe den Abschnitt Rechte für Acronis-Dienste (S. 78).

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 34), um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

7.3.2 Elemente für das Backup

Definieren Sie Auswahlregeln zum Sichern der Elemente, die im Feld **Quelltyp** des Abschnitts „Allgemein“ ausgewählt wurden.

Auswahlregeln zum Sichern von Laufwerken (S. 377)

Auswahlregeln für Backup-Quelle (S. 381)

Auswahlregeln zum Sichern von Laufwerken

Definieren Sie Regeln zur Laufwerksauswahl, nach denen die Laufwerke auf den Maschinen gesichert werden, auf die die Richtlinie angewendet wird.

So definieren Sie Regeln zur Laufwerksauswahl

Wählen Sie die Regel in der ersten Zeile von der Liste oder geben Sie sie manuell ein. Klicken Sie auf die nächste leere Zeile, um eine andere Regel hinzuzufügen, oder geben Sie diese manuell ein. Das Programm merkt sich manuell eingegebene Regeln und wenn Sie das nächste Mal das Fenster öffnen, stehen diese Regeln zur Auswahl in der Liste bereit.

Die folgende Tabelle erläutert die vordefinierten, von der Liste auswählbaren Regeln.

Mit einbeziehen	In der Spalte Partition:	Kommentare
Windows- und Linux-Partitionen		
Alle Partitionen	Geben Sie ein oder wählen Sie aus: **[Alle Partitionen]**	Bezieht sich auf alle Partitionen von Maschinen, die unter Windows laufen – und auf alle gemounteten Partitionen von Maschinen, die unter Linux laufen.
Windows-Partitionen		
Partition C:	Geben Sie **C:** ein oder wählen Sie die Partition von der Liste	
Systempartition	Geben Sie ein oder wählen Sie aus: **[SYSTEM]**	Die Systempartition enthält die Hardware-spezifischen Dateien, die zum Start von Windows benötigt werden, wie Ntldr, Boot.ini und Ntdetect.com. Es gibt nur eine Systempartition, selbst wenn mehrere Windows-Betriebssysteme auf dem Computer installiert sind. Zu mehr Details siehe „Bemerkungen zu Windows-Maschinen“.
Boot-Partition	Geben Sie ein oder wählen Sie aus: **[BOOT]**	Bezieht sich auf die Boot-Partition der registrierten Maschine. Die Boot-Partition enthält den Windows-Ordner und die dazugehörigen Dateien für das Windows-Betriebssystem (üblicherweise im Ordner Windows\System32 liegend). Es kann, muss sich aber nicht um dasselbe Laufwerk wie die Systempartition handeln. Sind mehrere Betriebssysteme auf dem Computer installiert, dann ist dies die Boot-Partition des Betriebssystems, in dem der Agent arbeitet. Zu mehr Details siehe „Bemerkungen zu Windows-Maschinen“.
Alle fest eingebauten Laufwerke	Geben Sie ein oder wählen Sie aus: **[Fest eingebaute Laufwerke]**	Bezieht sich auf alle Laufwerke außer Wechselmedien. Fest eingebaute Laufwerke beinhalteten Partitionen auf SCSI-, ATAPI-, ATA-, SSA-, SAS- und SATA-Geräten sowie auf RAID-Arrays.
Linux-Partitionen		
Erste Partition auf der ersten IDE-Festplatte einer Linux-Maschine	Geben Sie ein oder wählen Sie aus: **/dev/hda1**	hda1 ist der Standard-Gerätename für die erste Partition der ersten IDE-Festplatte. Zu mehr Details siehe „Bemerkungen zu Linux-Maschinen“.
Erste Partition auf der ersten SCSI-Festplatte einer Linux-Maschine	Geben Sie ein oder wählen Sie aus: **/dev/sda1**	sda1 ist der Standard-Gerätename für die erste Partition der ersten SCSI-Festplatte. Zu mehr Details siehe „Bemerkungen zu Linux-Maschinen“.
Erste Partition auf der ersten Software-RAID-Festplatte einer Linux-Maschine	Geben Sie ein oder wählen Sie aus: **/dev/md1**	md1 ist der Standard-Gerätename für die erste Partition des ersten Software-RAID-Laufwerkes. Zu mehr Details siehe „Bemerkungen zu Linux-Maschinen“.

Namen von Templates unterscheiden Groß/Kleinschreibung.

Was genau speichert das Backup einer Festplatte oder Partition?

Bei unterstützten Dateisystemen speichert ein Festplatten-/Partitions-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 Partitions-Backup speichert alle Dateien und Ordner des gewählten Laufwerks, unabhängig ihrer Attribute (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) der Festplatte. Der Boot-Code eines GPT-Volumes wird nicht vom Backup erfasst.

Ein Festplatten-Backup speichert alle Partitionen der betreffenden Platte (inkl. versteckter Partitionen wie Wartungs-Partitionen von Herstellern) und den Track Zero mit dem Master Boot Record (MBR).

Linux

Ein Partitions-Backup speichert alle Dateien und Ordner des gewählten Laufwerkes (unabhängig von ihren Attributen), einen Boot-Record und den Dateisystem-Super-Block.

Ein Festplatten-Backup speichert alle Partitionen der Platte, inkl. des Track Zero mit dem Master Boot Record.

Partitionen mit einem nicht unterstützten Dateisystem werden per Sektor-für-Sektor-Backup gesichert.

Bemerkungen zu Windows-Maschinen

Bei Windows-Versionen vor Windows 7 und Windows Server 2008 R2 liegen Systemdateien und Boot-Loader auf demselben Volume, es sei denn, während der Systeminstallation wurde explizit ein anderes Volume angegeben. Wenn sich die Windows-Dateien und der Loader auf demselben Volume befinden, ist die je einzelne Auswahl der Option **[SYSTEM]** oder **[BOOT]** ausreichend, um das Betriebssystem vollständig zu sichern. Anderenfalls wählen Sie sowohl **[SYSTEM]** als auch **[BOOT]**.

Beginnend mit Windows 7 und Windows Server 2008 R2 erstellen diese Betriebssystem-Versionen bei Ihrer Installation auf einem neuen Laufwerk ein dediziertes System-Volume mit der Kennzeichnung **System-reserviert**. Wenn Sie **[SYSTEM]** wählen, wird nur dieses dedizierte Volume gesichert. Wählen Sie immer sowohl **[SYSTEM]** als auch **[BOOT]**, wenn Sie Maschinen mit diesen Betriebssystemen sichern.

Weil Backup-Richtlinien üblicherweise auf viele Maschinen mit unterschiedlichen Betriebssystemen angewendet werden, empfiehlt Acronis, immer sowohl das System- wie auch Boot-Volume zum Backup auszuwählen, um die Integrität des Betriebssystem sicherzustellen.

Bemerkungen zu Linux-Maschinen

Sie können Windows- und Linux-Volumes gemeinsam in eine zentrale Backup-Richtlinie aufnehmen.

Es ist z.B. möglich, eine Richtlinie aufzusetzen, um Volume **C:** auf Windows-Maschinen zu sichern und Partition (Volumes) **/dev/hda1** auf Linux-Maschinen.

Anders als bei Windows gibt es in Linux keine klare Unterscheidung zwischen einem Laufwerk (Partition/Volume) und einem Ordner (Verzeichnis). Linux hat ein Root-Volume (als /

gekennzeichnet), an das Elemente verschiedenen Typs – inkl. Laufwerke, Verzeichnisse und System-Geräte – angeschlossen werden (gemountet), die so einen zur Datei- und Ordner-Struktur von Windows vergleichbaren Verzeichnisbaum bilden.

Lassen Sie z.B. eine Linux-Maschine ein Laufwerk enthalten, das in drei Volumes (bzw. Partitionen) aufgeteilt ist: die erste, zweite und dritte Partition. Diese Partitionen (Volumes) sind im Verzeichnisbaum als /dev/hda1, /dev/hda2 bzw. /dev/hda3 verfügbar. Um z.B. ein Laufwerk-Backup des dritten Volumes durchzuführen, können Sie in die Zeile der Dialogfenster **Auswahlregeln zum Sichern von Volumes** '/dev/hda3' eingeben.

Ein Linux-Volume kann außerdem irgendwo innerhalb des Verzeichnisbaums gemountet werden. '/dev/hda3' kann z.B. als Unterordner innerhalb des Verzeichnisbaums geladen werden, etwa als '/home/usr/docs'. In diesem Fall können Sie entweder '/dev/hda3' oder '/home/usr/docs' in das Feld 'Volume' eingeben, um ein Laufwerk-Backup des dritten Volume durchzuführen.

Im Allgemeinen sollten Sie beim Aufsetzen einer zentralen Richtlinie zur Durchführung von Laufwerk-Backups auf Linux-Maschinen sicherstellen, dass die im Feld 'Volume' eingegebenen Pfade zu richtigen Volumes (Partitionen) (wie '/dev/hda2' oder '/home/usr/docs' aus dem vorherigen Beispiel) und nicht mit Verzeichnissen korrespondieren.

Standardnamen für Linux-Volumes

Namen wie /dev/hda1 reflektieren die übliche Art, IDE-Laufwerks-Volumes in Linux zu bezeichnen. Das Präfix „hd“ kennzeichnet den Laufwerktyp (IDE), „a“ bedeutet, dass es das erste IDE-Laufwerk des Systems ist und „1“ bezeichnet das erste Volume auf dem Laufwerk.

Im Allgemeinen besteht der Standardname für ein Linux-Volume aus drei Komponenten:

- Laufwerkstyp; 'hd' für IDE-, 'sd' für SCSI- und 'md' für Software-RAID-Laufwerke (z.B. für dynamische Volumes);
- Laufwerksnummer; „a“ für das erste, „b“ für das zweite Laufwerk usw.;
- Partitionnummer auf dem Laufwerk; „1“ für das erste Volume, „2“ für das zweite usw.

Um das Backup gewählter Laufwerke unabhängig von ihrem Typ zu garantieren, sollten Sie erwägen, drei Einträge in das Dialogfenster **Auswahlregeln für die zu sichernden Volumes** aufzunehmen, einen für jeden möglichen Typ. Um z.B. das erste Laufwerk einer jeden Linux-Maschine unter einer zentralen Richtlinie zu sichern, können Sie die folgenden Zeilen in das Feld 'Volume' eingeben:

/dev/hda1

/dev/sda1

/dev/mda1

Namen für logische Volumes

Um logische Volumes (auch LVM-Volumes genannt) zu sichern, müssen Sie deren vollständige Namen in den Auswahlregeln spezifizieren: Der vollständige Name eines logischen Volumes beinhaltet die Volume-Gruppe, zu der das Volume gehört.

Spezifizieren Sie als Beispiel folgende Auswahlregeln, um zwei logische Volumes namens **lv_root** und **lv_bin** – beide zur Volume-Gruppe **vg_mymachine** gehörend – zu sichern:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

Verwenden Sie das Utilitiy **lvdisplay**, um auf einer Maschine eine Liste der logischen Volumes

einzusehen. In unserem Beispiel sieht die Ausgabe ungefähr wie folgt aus:

```
--- Logical volume ---
LV Name          /dev/vg_mymachine/lv_root
VG Name          vg_mymachine
…

--- Logical volume ---
LV Name          /dev/vg_mymachine/lv_bin
VG Name          vg_mymachine
…
```

Tipp: *Damit später bei Recovery-Aktionen die Volume-Strukturinformation automatisch erstellt werden kann, sollten Sie sicherstellen, dass auf jeder Maschine das Volume mit mit dem Verzeichnis* ***/etc/Acronis*** *zum Backup ausgewählt ist. Zu weiteren Details siehe „Die Volume-Strukturinformation sichern“.*

Auswahlregeln für Backup-Quelle

Definieren Sie Regeln zur Dateiauswahl, nach denen Dateien bzw. Ordner auf den Maschinen gesichert werden, auf die die Richtlinie angewendet wird.

So definieren Sie Regeln zur Dateiauswahl

Wählen Sie die Regel in der ersten Zeile von der Liste oder geben Sie sie manuell ein. Klicken Sie auf die nächste leere Zeile, um eine andere Regel hinzuzufügen, oder geben Sie diese manuell ein.

Das Programm merkt sich manuell eingegebene Regeln und wenn Sie das nächste Mal das Fenster öffnen, stehen diese zusammen mit den Standardregeln zur Auswahl in der Liste bereit.

Windows

Vollständiger Pfad

Wählen Sie die zu sichernden Dateien und Ordner. Wenn Sie explizit einen Pfad zu einer Datei bzw. Ordner angegeben haben, dann wird die Richtlinie dieses Element auf jeder Maschine sichern, auf der dieser Pfad gefunden wird.

Mit einbeziehen	In der Spalte „Dateien und Ordner“ geben Sie Folgendes ein oder wählen es aus:
Datei Text.doc im Ordner D:\Arbeit	**D:\Arbeit\Text.doc**
Ordner C:\Windows	**C:\Windows**

Umgebungsvariablen

Manche Umgebungsvariablen verweisen auf Windows-Ordner. Die Verwendung solcher Variablen statt vollständiger Datei- und Verzeichnis-Pfade, stellt die Sicherung der richtigen Windows-Ordner sicher, unabhängig davon, wo Windows auf einer bestimmten Maschine lokalisiert ist.

Mit einbeziehen	In der Spalte „Dateien und Ordner“ geben Sie Folgendes ein oder wählen es aus	Kommentare
Ordner „Programme“	**%PROGRAMFILES%**	Verweist auf den Ordner für Programme (z.B. **C:\Programme**)
Windows-Ordner	**%WINDIR%**	Verweist auf den Ordner, wo Windows gespeichert ist (z.B. **C:\Windows**)

Allgemeine Daten für alle Benutzerprofile	**%ALLUSERSPROFILE%**	Verweist auf den Ordner, wo die allgemeinen Daten für alle Benutzerprofile hinterlegt sind, (**C:\Dokumente und Einstellungen\All Users** in Windows XP und **C:\Users bzw. C:\Benutzer** in Windows Vista und Windows 7)

Sie können auch andere Umgebungsvariablen oder eine Kombination von Umgebungsvariablen und Text verwenden. Um z.B. auf den Ordner „Acronis“ im Ordner „Programme“ der Maschine zu verweisen, geben Sie ein: **%PROGRAMFILES%\Acronis**

Vorlagen

Vorlagen sind ähnlich zu Umgebungsvariablen, aber bereits vorangepasst.

Mit einbeziehen	In der Spalte „Dateien und Ordner“ geben Sie Folgendes ein oder wählen es aus:	Kommentare
Alle Dateien auf allen Partitionen einer Maschine	**[Alle Dateien]**	Verweist auf alle Dateien auf allen Partitionen der Maschine.
Alle auf einer Maschine existierenden Benutzerprofile	**[All Profiles-Ordner]**	Verweist zum Ordner, in dem alle Benutzerprofile gespeichert sind (z.B. **C:\Dokumente und Einstellungen** in Windows XP und **C:\Users bzw. C:\Benutzer** in Windows Vista und Windows 7).

Linux

Mit einbeziehen	In der Spalte „Dateien und Ordner“ geben Sie Folgendes ein oder wählen es aus:
Die Textdatei „Datei.txt“ auf der Partition „/dev/hda3“, gemountet an „/home/usr/docs“	**/dev/hda3/Datei.txt** oder **/home/usr/docs/Datei.txt**
Home-Verzeichnis der allgemeinen Benutzer	**/home**
Das Heim-Verzeichnis des Benutzers „root“.	**/root**
Verzeichnis für alle Benutzer-bezogenen Programme	**/usr**
Verzeichnis für System-Konfigurationsdateien	**/etc**

7.3.3 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:
   - **Verwende die Anmeldedaten der Richtlinie:**

     Das Programm greift auf die Quelldaten unter Verwendung derjenigen Anmeldedaten der Backup-Richtlinie 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 die Anmeldedaten der Richtlinie keinen Zugriff auf die Daten erlauben.

  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**.

7.3.4 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

7.3.5 Archiv

Geben Sie an, wo die Archive gespeichert werden sollen und definieren Sie Namen für die neuen Backup-Archive.

1. Das Ziel für die Archive wählen

Wählen Sie, wo die Archive der Maschinen gespeichert werden:

- Alle Archive der Maschinen an einem einzelnen Ort speichern
  - 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 (S. 411) und das Abonnement auf der zu sichernden Maschine aktivieren (S. 412). Die Online Backup-Funktion steht unter Linux nicht zur Verfügung.

  Acronis Backup & Recovery 10 Online ist möglicherweise in Ihrer Region nicht verfügbar. Zu weiteren Informationen klicken Sie hier: http://www.acronis.de/my/backup-recovery-online/.

  - Um die Archive in einem zentralen Depot abzulegen, erweitern Sie die Gruppe Zentral und wählen dort dieses Depot.
  - Um die Archive auf einer Netzwerkfreigabe zu sichern, erweitern Sie die Gruppe Netzwerk-

Ordner, 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 die Archive auf einem FTP- oder SFTP-Server zu speichern, erweitern Sie die korrespondierende Gruppe und greifen auf den entsprechenden Server zu, wo Sie dann den Ordner wählen, in dem die Archive gespeichert werden sollen.

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 jeder Maschine im angegebenen Ordner auf der Maschine speichern

  Geben Sie im Feld Pfad den vollständigen Pfad zu dem Ordner an. Dieser Pfad wird auf jeder Maschine erstellt, auf die die Richtlinie angewendet wird.
- Archiv aller Maschinen in der Acronis Secure Zone der Maschine speichern

  Die Acronis Secure Zone muss auf jeder Maschine erstellt werden, auf die die Richtlinie angewendet wird. Zu weiteren Informationen über die Erstellung der Acronis Secure Zone siehe den Abschnitt Acronis Secure Zone erstellen (S. 268).

2. Die Archive benennen

Die Daten jeder Maschine werden zu einem separaten Archiv gesichert. Definieren Sie Namen für diese Archive.

Das Programm generiert einen einheitlichen Namen für die neuen Archive und zeigt diesen im Feld Name an. Der Name entspricht dem Muster [Richtlinienname]_[Maschinenname]_Archive1. Sind Sie mit dem automatisch generierten Namen nicht einverstanden, so konstruieren Sie einen anderen.

Wenn Sie die Option Alle Archive der Maschinen an einem einzelnen Ort speichern wählen, dann müssen Sie Variablen verwenden, um eindeutige Bezeichnungen für die Archive innerhalb des Speicherortes zu ermöglichen.

1. Klicken Sie auf Variablen hinzufügen und wählen Sie dann
   - [Machine name] – Platzhalter für den Namen der Maschine
   - [Policy name] – Platzhalter für den Namen der Backup-Richtlinie

   Als Ergebnis erscheint folgende Regel im Feld Name: [Machine name]_[Policy name]_Archiv1

   Wird also z.B. die SYSTEM_BACKUP genannte Backup-Richtlinie auf drei Maschinen angewendet (z.B. FINABT1, FINABT2, FINABT3), dann werden die folgenden drei Archive am Speicherort erstellt:

   FINABT1_SYSTEM_BACKUP_Archiv1

   FINABT2_SYSTEM_BACKUP_Archiv1

   FINABT3_SYSTEM_BACKUP_Archiv1
2. Klicken Sie auf OK.

Der Name hat das Format ArchivN, wobei N eine fortlaufende Nummer ist. Wenn das Programm feststellt, dass ein Archiv1 bereits am Speicherort vorliegt, wird es automatisch den Namen Archiv2 vorschlagen.

7.3.6 Anmeldedaten für den Speicherort

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das Backup-Archiv gespeichert wird. Der Benutzername dieser Anmeldedaten wird als Besitzer des

Archivs betrachtet.

Anmeldedaten spezifizieren

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Verwende die Anmeldedaten der Richtlinie:**

     Das Programm greift auf den Speicherort unter Verwendung der Anmeldedaten der Backup-Richtlinie 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, sofern die Anmeldedaten der Richtlinie keinen Zugriff auf den Speicherort erlauben. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder einen Storage Node 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.*

7.3.7 Wahl des Backup-Schemas

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. 32) 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. 172), um mehr über das Aufstellen von Zeit/-Ereignis-Planungen zu lernen.
Aufbewahrungsregel	Für das Schema „Einfach“ ist nur eine Aufbewahrungsregel (S. 42) 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.
Erweiterte Einstellungen:	Um Erweiterte Planungseinstellungen (S. 180) zu spezifizieren, klicken Sie auf **Ändern** im Bereich **Erweiterte Einstellungen**.

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. 173), wöchentlichen (S. 175) oder monatlichen (S. 177) 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	Garantierte Zahl von Sitzungen, die Sie jederzeit im Archiv zurückgehen können. Automatisch

Periode	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. 42) 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. 42) 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. 42).

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. 42).

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.

Initial Seeding

Dieses Backup-Schema ist nur verfügbar, wenn Sie eine Lizenz für Initial Seeding besitzen und den Online Backup Storage als Backup-Ziel ausgewählt haben.

Initial Seeding ermöglicht Ihnen, das erste Backup (üblicherweise ein Voll-Backup und sehr groß) durch Verwendung einer Festplatte (oder ähnlichen Laufwerks) statt per Internetübertragung zum Online Storage hochzuladen. Nachfolgende Backups (üblicherweise inkrementell und daher deutlich kleiner) können dann per Internet übertragen werden, sobald das Voll-Backup im Online Storage angekommen ist.

Wenn Sie eine große Datenmenge sichern, ermöglicht Initial Seeding eine schnellere Auslieferung der Daten und geringere Übertragungskosten.

Konsultieren Sie zu weiteren Details den Abschnitt „Initial Seeding FAQ (S. 402)“.

7.3.8 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. 172).

8 Online Backup

Dieser Abschnitt vermittelt Details zur Verwendung von Acronis Backup & Recovery 10 Online. Dieser Service ermöglicht Online Backups zum Acronis Online Backup Storage.

Acronis Backup & Recovery 10 Online ist möglicherweise in Ihrer Region nicht verfügbar. Zu weiteren Informationen klicken Sie hier: http://www.acronis.de/my/backup-recovery-online/.

Um Backups zum Online Storage oder ein Recovery vom Online Storage einzurichten, folgen Sie den Schritten, die in den zugehörigen Abschnitten beschrieben sind:

Einen Backup-Plan erstellen (S. 205)

Eine Backup-Richtlinie erstellen (S. 374)

Daten wiederherstellen

Der Hauptunterscheid besteht darin, dass Sie den Online Storage als Backup-Ziel wählen.

Host-basierte Backups von virtuellen Maschinen sind mit der Virtual Edition von Acronis Backup & Recovery 10 möglich. Sie können alle vom Agent für ESX/ESXi oder Agent für Hyper-V verwaltete Maschinen mit einem einzigen Abonnement für virtuelle Maschinen sichern.

8.1 Einführung in Acronis Backup & Recovery 10 Online

Dieser Abschnitt enthält eine kurze Übersicht über Acronis Backup & Recovery 10 Online und beantwortet Fragen, die möglicherweise während der Evaluierung oder Benutzung des Programms auftreten können.

8.1.1 Was ist Acronis Backup & Recovery 10 Online?

Acronis Backup & Recovery 10 Online ist ein Dienst, der Ihnen das Backup von Daten zum Acronis Online Backup Storage ermöglicht. Um diese Dienstleistung zu nutzen, müssen Sie ein Abonnement erwerben, welches den für Backups reservierten Speicherplatz (die Storage Quota) festlegt sowie den Zeitraum für die Nutzung des Online-Services.

Es ist für jede physikalische Maschine, die Sie sichern wollen, ein separates Abonnement erforderlich. Das zu erwerbende Abonnement für Server oder Workstations hängt vom Windows-Betriebssystem ab, welches auf der Maschine läuft. Andere Betriebssysteme werden von Acronis Backup & Recovery 10 Online nicht unterstützt.

Virtuelle, auf einem VMware ESX(i)- oder Microsoft Hyper-V-Host laufende Maschinen können unter Verwendung eines einzelnen Abonnements für virtuelle Maschinen gesichert werden.

Beispiel: Ein Workstation-Abonnement für 250 GB/1 Jahr bedeutet, dass Sie die entsprechenden Daten von einer Maschine, deren Betriebssystem kein Windows-Server-Betriebssystem ist, für ein ganzes Jahr sichern können. Die Backups können nicht mehr als 250 GB belegen.

8.1.2 Was für Daten können gesichert und wiederhergestellt werden?

Sie können Dateien, Volumes, Laufwerke oder die komplette physikalische Maschine so häufig wie gewünscht sichern. Anders als die meisten anderen Backup-Lösungen ermöglicht Acronis Backup & Recovery 10 Online vom Online Storages aus auch eine Wiederherstellung auf fabrikneue Computer. Einzelne Dateien können sowohl aus Laufwerk- wie auch Datei-basierten Backups wiederhergestellt werden.

Zu weiteren Informationen über das Backup virtueller Maschinen siehe „So können Sie virtuelle Maschinen zum Online Storage sichern (S. 399)“.

8.1.3 Wie lange werden Backups auf dem Online Storage aufbewahrt?

Ihr Backup verbleibt auf dem Online Storage, bis es von Ihnen gelöscht wird oder das Abonnement abläuft. Eine Datenwiederherstellung vom Online Storage ist bis zu 30 Tage nach Ablauf des Abonnements möglich.

Zur effektiven Nutzung des Online Storage-Speicherplatzes haben Sie die Möglichkeit, die Aufbewahrungsregel „**Lösche Backups älter als**“ einzustellen.

Beispiel

Für einen Datei-Server können Sie beispielsweise folgende Backup-Strategie verwenden.

Sichern Sie kritische Dateien zweimal täglich per Planung. Stellen Sie die Aufbewahrungsregel „**Lösche Backups älter als**“ auf 7 Tage ein. Das bedeutet, dass die Software nach jeder Sicherung überprüft, ob es Backups gibt, die älter als 7 Tage sind und diese dann automatisch löscht.

Führen Sie bei einem Server die Backups des System-Volumes manuell aus (wenn erforderlich). Beispielsweise nachdem Sie Betriebssystem-Updates aufgespielt haben. Löschen Sie nicht mehr benötigte Backups manuell.

8.1.4 Wie sicher sind die Daten?

Backups können mit Hilfe des kryptographischen Algorithmus 'Advanced Encryption Standard' (AES) und eines frei gewählten Kennworts verschlüsselt werden. Das gewährleistet, dass keine andere Person auf Ihre Daten zugreifen kann.

8.1.5 So können Sie virtuelle Maschinen zum Online Storage sichern

Verwenden Sie eine oder beide der folgenden Methoden.

Installieren Sie die Acronis Software auf dem Virtualisierungs-Host

Dieser Ansatz ist praktisch, wenn das auf dem Host-Server installierte Virtualisierungsprodukt VMware ESX(i), Windows Server 2008 mit Hyper-V oder Microsoft Hyper-V-Server ist.

Sie können mit einem Abonnement für virtuelle Maschinen eine komplette virtuelle Maschine oder ihre Volumes sichern. Das Abonnement gilt für alle vom Host bereitgestellten Maschinen oder den kompletten vCenter-Cluster. Backup und Recovery auf Dateiebene ist für virtuelle Maschinen nicht

möglich – jedoch für einen Windows-Host.

Die Installation der Software sowie die Durchführung von Backup- und Recovery-Aktionen sind in der Schnellstartanleitung für die Acronis Backup & Recovery 10 Virtual Edition beschrieben. Wenn Sie nur Acronis Backup & Recovery 10 Online Backup installieren, müssen Sie während der Installation keinen Lizenzschlüssel eingeben.

Host-basierte Backups stehen nur für kommerzielle Lizenzen von VMware ESXi zur Verfügung. Verwenden Sie den unteren Ansatz, falls Ihr ESXi-Server mit einer freien Lizenz arbeitet.

Installieren Sie die Acronis Software auf dem Gastsystem

Die virtuelle Maschine wird wie eine physikalische Maschine behandelt. Sie benötigen für diese Maschine ein separates Server- oder Workstation-Abonnement. Dieser Ansatz ist für folgende Situationen geeignet:

- die Maschine wird nicht auf einem Virtualisierungs-Server gehostet
- das auf dem Host-Server installierte Virtualisierungsprodukt ist *nicht* VMware ESX(i), Windows Server 2008 mit Hyper-V oder Microsoft Hyper-V-Server
- Sie möchten Befehle vor/nach dem Backup bzw. vor/nach der Datenerfassung auf der Maschine verwenden
- Sie möchten Backup- und Recovery-Aktionen auf Dateiebene durchführen
- Sie möchten ein unabhängiges Laufwerk oder ein RDM-Laufwerk (über den physikalischen Kompatibilitätsmodus angebunden) auf einer laufenden ESX(i)-Maschine sichern.

Die Installation der Software sowie die Durchführung von Backup- und Recovery-Aktionen entsprechen denen auf einer physikalischen Maschine.

8.1.6 FAQ zu Backup und Recovery

Dieser Abschnitt beantwortet typische Fragen zu Backup- und Recovery-Aktionen

Welche Backup-Methoden sind verfügbar?

Vollständige und inkrementelle Backup-Methoden stehen über folgende Backup-Schemata zur Verfügung.

Backup jetzt (sofortiger Start) oder **Backup später** (verzögerter Start). Sie können entweder die vollständige oder inkrementelle Backup-Methode wählen. Bei erstmaliger Task-Ausführung wird ein Voll-Backup erstellt. Wenn Sie den Backup-Task erneut ausführen, wird die ausgewählte Backup-Methode angewendet. Auf diese Art erhalten Sie entweder ein neues Voll-Backup oder ein inkrementelles. Da Voll-Backups mehr Speicherplatz belegen, empfiehlt Acronis, dass Sie inkrementelle Backups wählen, wenn Sie Ihre Backups manuell ausführen wollen.

Einfach (Start nach Planung). Das erste Backup ist vollständig, spätere Backups inkrementell. Sie können mit diesem Backup-Schema eine Aufbewahrungsregel zur automatischen Lösung alter Backups einstellen.

Ein weiteres, nur für den Online Storage verfügbares Backup-Schema ist **Initial Seeding**. Es entspricht dem Schema **Backup jetzt** unter Verwendung eines lokalen Speicherorts und der Voll-Backup-Methode. Um dieses Schema zu verwenden, benötigen Sie eine 'Initial Seeding (S. 402)'-Lizenz.

Ist der Online Storage auch von Acronis Bootable Media aus verfügbar?

Wiederherstellungen vom Acronis Online Backup Storage sind möglich, Backups zum Online Storage

dagegen nicht.

Kann Acronis Universal Restore verwendet werden, wenn eine Systemwiederherstellung vom Online Storage aus erfolgt?

Ja. Acronis Universal Restore ist immer verfügbar, wenn Sie ein System aus dem Online Storage wiederherstellen. Der Einsatz von Acronis Universal Restore bei Wiederherstellungen aus anderen Storage-Typen erfordert jedoch eine separate Lizenz.

Was passiert, wenn während einer Online Backup- oder Recovery-Aktion die Netzwerkverbindung verloren geht?

Die Software wird alle 30 Sekunden versuchen, den Online Storage zu erreichen. Nach fünf Versuchen wird der Backup- oder Recovery-Task fehlschlagen.

Sie können die Zahl der Versuche und die Zeitspanne zwischen den Versuchen unter **Fehlerbehandlung** mit der Option **Bei Fehler neu versuchen** ändern. Jeder Backup-Plan oder Recovery-Task enthält diese Option.

Was passiert, wenn Ihnen der Speicherplatz ausgeht?

Wenn die Backups einer Maschine den per Abonnement erlaubten Speicherplatz zu überschreiten drohen, erhalten Sie eine Alarmmeldung per E-Mail. Sie können diese Alarmmeldung auch auf der Webseite zur Kontoverwaltung sehen (neben der Maschine). Das bedeutet, dass Sie für zukünftige Backups Speicherplatz freimachen müssen. Sie können auch eine Aufbewahrungsregel (S. 399) einstellen oder bearbeiten, damit es nicht mehr zu einem Überlauf kommt. Sobald der belegte Speicherplatz das Limit erreicht, verweigern die Backups ihre Ausführung.

Wofür ist der Bereinigungstask gedacht?

Jeder Backup-Plan mit gesetzter Bereinigungsregel enthält zusätzlich zum Backup-Task auch einen Bereinigungstask. Der Bereinigungstask überprüft das auf Basis des Backup-Plans erstellte Archiv nach Backups, die ihre 'Lebensdauer' überschritten haben. Wenn solche Backups gefunden werden, bewirkt der Task, dass der Online Storage diese löscht. Da die Löschung auf Seiten des Online Storage durchgeführt wird, werden keine CPU-Ressourcen von Ihrer Maschine beansprucht.

Der Bereinigungstask läuft nach jedem Online Backup, auch wenn das Backup selbst fehlgeschlagen ist. Zudem wird auch immer das letzte erfolgreiche Backup bewahrt. Weitere Informationen über die Aufbewahrungsregel finden Sie unter „Wie lange werden Backups auf dem Online Storage aufbewahrt? (S. 399)“.

Es ist normalerweise nicht notwendig, den Bereinigungstask manuell zu starten oder zu stoppen. Sie können dies jedoch in der Ansicht **Backup-Pläne und Tasks** tun.

Wie bewirken Sie, dass eine wiederhergestellte Maschine ihr Abonnement erkennt?

Wenn Sie eine physikalische Maschine aus einem Backup wiederherstellen, wird auch ein neuer 'Machine Identifier' erstellt. Daher kann die Maschine keine Backups zu dem Abonnement durchführen, das sie vor der Recovery-Aktion verwendet hat.

Um die Maschine zum selben Abonnement zu sichern, müssen Sie dieses der Maschine erneut zuweisen (S. 413). Wenn Sie dies tun, können die nächsten Backups der Maschine wieder inkrementell sein. Wenn Sie der Maschine ein neues Abonnement zuweisen, muss die Software ein neues Voll-Backup durchführen.

8.1.7 FAQ zu Initial Seeding

Dieser Abschnitt erklärt, was Initial Seeding ist, warum es für Sie vorteilhaft ist und zudem einige Details zu seiner Verwendung.

Was ist Initial Seeding?

Initial Seeding ist ein Extra-Service, bei dem Sie das initiale Voll-Backup lokal ausführen und dieses dann auf einer Festplatte (oder einem ähnlichen Laufwerk) an Acronis senden.

Acronis lädt das Backup dann zum Online Storage hoch. Danach können Sie dieses Voll-Backup – manuell oder nach Zeitplan – mit nachfolgenden inkrementellen Backups erweitern.

Das Laufwerk erhalten Sie zurück, aber es ist nicht möglich, davon ein Recovery durchzuführen. Ein Recovery ist von einem lokal angeschlossenen Gerät jedoch mit der Option 'Large Scale Recovery (S. 407)' möglich.

Wann ist Initial Seeding sinnvoll?

Dieser Dienst hilft Ihnen, beim initialen Voll-Backup Zeit und Netzwerkverkehr zu sparen. Das ist nützlich, wenn Sie sehr große Datenmengen oder komplette Maschinen zum Online Storage sichern.

Ist Initial Seeding ein kostenpflichtiger Dienst?

Ja, Sie benötigen eine 'Initial Seeding'-Lizenz für jede Maschine.

Welche Laufwerkstypen können für Initial Seeding verwendet werden?

Acronis akzeptiert Festplatten (und ähnliche Laufwerke) mit folgenden Schnittstellentypen: IDE, ATA, SATA sowie per USB angeschlossene Laufwerke. SCSI-Laufwerke werden nicht akzeptiert.

Sie können das Backup direkt auf das Gerät erstellen lassen – oder auf einen lokalen Ordner oder Netzwerkordner speichern und das Backup anschließend auf das Gerät kopieren. Sorgen Sie dafür, dass das Gerät nur ein Volume hat und das Dateisystem NTFS oder FAT32 verwendet.

Kann mehr als ein Backup pro einzelner 'Initial Seeding'-Lizenz übermittelt werden?

Ja, wenn die Backups von derselben Maschine stammen und auf dem gleichen Laufwerk übermittelt werden.

Sie könnten beispielsweise ein Volume-Backup und eine bestimmte Anzahl von Datei-Backups übermitteln. Erstellen Sie so viele 'Initial Seeding'-Backups wie Sie wollen und senden Sie diese auf demselben Laufwerk an Acronis. Die Lizenz für Initial Seeding gilt als benutzt, sobald der Upload zum Online Storage beginnt. Sie erhalten eine Benachrichtigung per E-Mail, die Sie entsprechend informiert. Danach erfordert die Erstellung eines neuen 'Initial Seeding'-Backups eine neue 'Initial Seeding'-Lizenz.

Können Backups mehrerer Maschinen auf einem Laufwerk übermittelt werden?

Ja. Sie benötigen aber dennoch je eine Lizenz pro Maschine.

Wie kann eine 'Initial Seeding'-Lizenz erworben werden?

Sie können eine 'Initial Seeding'-Lizenz von einem Acronis-Partner oder im Acronis Online Store

kaufen. Verwenden Sie den Link www.acronis.de/my/backup-recovery-online/#buy, um einen Partner zu finden oder einen Online-Kauf durchzuführen.

Nachdem Sie eine Lizenz von einem Acronis-Partner erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit einem Registrierungscode. Klicken Sie auf derselben Webseite auf **Neuen Registrierungscode eingeben** und registrieren Sie die Lizenz. Die Lizenz wird dann über die Registerlasche **Initial Seeding / Recovery** zur Verfügung gestellt.

Eine über den Acronis Online Store erworbene Lizenz wird unmittelbar nach Abschluss des Zahlvorgangs verfügbar.

Wie wird Initial Seeding ausgeführt?

1. Entscheiden Sie sich für das Medium (S. 402), das Sie für den Versand verwenden wollen.
2. Schließen Sie das Medium bzw. Laufwerk an die Maschine an, die Sie per Backup sichern wollen. Alternativ können Sie das Backup auch zu einem lokalen Ordner oder einer Netzwerkfreigabe sichern – und es anschließend dann auf das Medium kopieren/verschieben.
3. Starten Sie Acronis Backup & Recovery 10, klicken Sie auf **Backup** und erstellen Sie auf der Maschine einen Backup-Plan:
   - Spezifizieren Sie den **Online Backup Storage** als **Backup-Ziel**.
   - Wählen Sie bei **Backup-Quelle** die Laufwerke/Volumes oder Dateien/Ordner, die Sie sichern wollen.
   - Wählen Sie bei **Backup-Schema** die Einstellung **Initial Seeding**. Spezifizieren Sie das besprochene Medium als Backup-Ziel.
   - [Optional, aber dringend empfohlen] Aktivieren Sie unter **Backup-Optionen** –> **Schutz des Archivs** eine Verschlüsselung für das Backup.
   - [Optional, aber dringend empfohlen] Aktivieren Sie die Backup-Überprüfung unter **Archiv-Validierung**.

   Das Backup startet unmittelbar, sobald Sie abschließend auf **OK** klicken.
4. [Optional] Wenn Sie dem Medium weitere Backups hinzufügen wollen, wiederholen Sie Schritt 3 und wählen Sie unter **Backup-Quelle** jeweils die entsprechenden Daten aus. (Verändern Sie den Backup-Plan nicht, erstellen Sie jeweils einen neuen Plan!).
5. [Optional] Wenn Sie Backups von einer anderen Maschine hinzufügen wollen, dann schließen Sie das Medium an diese Maschine an und wiederholen Sie die entsprechenden Schritte.
6. Verpacken (S. 404) Sie das Medium zusammen mit einem frankierten Rücksendeetikett und senden Sie es über den herkömmlichen Postweg an Acronis. Sie finden die Adresse auf der Webseite zur Kontoverwaltung unter **Initial Seeding / Recovery** –> **Laufende Aufträge** –> **Initial Seeding-Aufträge** –> **Data Center-Adresse**.
7. Kennzeichnen Sie auf derselben Webseite den Auftrag als „Versendet“ und verfolgen (S. 406) Sie den Auftragsstatus.
8. Sobald Sie sehen, dass das Backup auf den Online Storage hochgeladen wurde, können Sie den Backup-Plan so bearbeiten, dass inkrementelle Backups erstellt werden.
   - Wählen Sie bei **Backup-Schema** den Befehl **Backup jetzt**, bei manuellen Backups **Backup später** oder bei geplanten Backups **Einfach**.
   - Spezifizieren Sie bei **Einfach** eine Planung und (optional) eine Aufbewahrungsregel.
   - Klicken Sie auf **Speichern**.

   Ihr Backup-Plan wird bei manuellem oder geplantem Start dem anfänglichen, auf dem Online Storage gespeicherten Backup weitere inkrementelle Backups hinzufügen.

Wie verpacken Sie ein Laufwerk zur Versendung richtig?

Es ist sehr wichtig, dass Sie Ihre Festplatte (oder ein ähnliches Laufwerk) zur Versendung sorgfältig verpacken. Durch eine sorgfältige Verpackung schützen Sie Ihr Laufwerk vor Transportschäden.

Laufwerkstypen

Acronis akzeptiert Festplatten (und ähnliche Laufwerke) mit folgenden Schnittstellentypen: IDE, ATA, SATA sowie per USB angeschlossene Laufwerke.

SCSI-Laufwerke werden nicht akzeptiert.

Verpackung

Verwenden Sie – sofern möglich/verfügbar – die Originalverpackung des Laufwerks. Anderenfalls können Sie geeignetes Verpackungsmaterial auch bei entsprechenden Poststationen oder ähnlichen Geschäften erhalten.

Nachfolgend finden Sie Hinweise zur geeigneten Verpackung Ihres Laufwerks.

Schritt 1

Entfernen Sie Ihr Laufwerk vorsichtig von der entsprechenden Maschine.

Schritt 2

Stecken Sie das Laufwerk in eine Antistatikhülle, um es vor elektrostatischen Entladungen zu schützen. Falls Sie keine Antistatikhülle zur Verfügung haben, können Sie es als Alternative auch mit Alufolie umwickeln.

Schritt 3

Verwenden Sie eine stabile Box, die mindestens doppelt so groß wie das Laufwerk ist. Wickeln Sie

das Laufwerk über alle 6 Seiten mit einer Luftpolsterfolie so ein, dass es genau in die Box passt und sich in dieser nicht bewegen kann.

*Verwenden Sie **keine** Styropor-**Chips** zur Verpackung, da diese nicht genügend Schutz bieten.*
*Versenden Sie das Laufwerk **nicht** einfach in einer herkömmlichen **gepolsterten Versandtasche**.*

Schritt 4

Wählen Sie das von Ihnen gewünschte Transportunternehmen für den Versand. Erstellen bzw. drucken Sie (z.B. über einen entsprechenden Online-Dienst des Transportunternehmens) zwei bereits frankierte Versandetiketten:

1. Das **Versandetikett zur Hinsendung** Ihres Laufwerks. Dieses Etikett gehört auf die Oberseite der Box. Sie müssen das Paket dann an ein Acronis Data Center versenden. Die Adresse des entsprechenden Data Centers finden Sie auf der Webseite zur Kontenverwaltung innerhalb der Registerlasche **Initial seeding/Recovery** (indem Sie auf den Befehl **Data Center-Adresse anzeigen** klicken).

   Falls Sie möglichst schnell mit der Erstellung inkrementeller Backups beginnen wollen, sollten Sie erwägen, einen Express- bzw. Nachtversanddienst zu verwenden. Sobald die Daten beim Data Center eingetroffen sind, stehen Sie üblicherweise am darauf folgenden Arbeitstag zur Verfügung.
2. Das **Versandetikett zur Rücksendung** Ihres Laufwerks. Legen Sie dieses Etikett in die Box zum Laufwerk. Zur Rücksendung wird dieselbe Verpackung verwendet (außer diese wurde beschädigt). Wenn Sie Ihrer Sendung kein frankiertes Etikett beilegen, wird Ihr Laufwerk **sicher entsorgt**.

   Sie können zur Rücksendung Ihres Laufwerks eine kostengünstige Methode bzw. ein Transportunternehmen Ihrer Wahl verwenden.

Schritt 5

Versiegeln Sie die Box sicher mit einem stabilen Klebeband. Kleben Sie dann das **Versandetikett zur**

Hinsendung Ihres Laufwerks auf die Oberseite der Box – achten Sie darauf, dass das Etikett nicht über eine der Kanten geklebt ist.

Wie kann der Auftragsstatus für Initial Seeding verfolgt werden?

Auf der Acronis-Website zeigt die Registerlasche **Initial Seeding / Recovery** den Status aller Aufträge. Sie erhalten zusätzlich eine E-Mail-Benachrichtigung über wichtige Ereignisse.

- **Verfügbar** – Die Lizenz kann für jede Maschine verwendet werden.
- **Ein Auftrag wurde erstellt** – Das erste Backup ist bereit für den Start und die Lizenz kann für keine andere Maschine mehr verwendet werden. Sie können von diesem Punkt an den Auftrag auch abbrechen, wenn etwas falsch läuft. Dadurch wird die Lizenz an den Pool verfügbarer Lizenzen zurückgegeben.
- **Ein Voll-Backup wurde gestartet** – Dieser Zustand wird eingestellt, wenn das erste Backup ausgeführt wird. Ab diesem Moment beginnt die Laufzeit des Vertrags.
- **Ein Voll-Backup wurde erfolgreich abgeschlossen** – Das Backup wurde fertig gestellt und der Auftrag ist bereit zur Versendung. Sie können das Medium jetzt verschicken:

  Schritt 1. Verpacken Sie das Medium gemäß der Anleitung zur Verpackung und Versand des Laufwerks (S. 404), um Beschädigungen beim Transport zu vermeiden. Falls Sie wollen, dass das Medium nach dem Upload der Daten an Sie zurückgeschickt wird, legen Sie der Verpackung neben dem Laufwerk auch ein vorbereitetes, ausreichend frankiertes Rücksendeetikett bei.

  Schritt 2. Verschicken Sie das Laufwerk mit dem von Ihnen gewünschten Transportunternehmen zum Acronis Data Center.

  Schritt 3. Teilen Sie uns den Versand des Pakets mit, indem Sie Ihren Auftrag als „Versendet“ kennzeichnen.

  Sie erhalten eine Benachrichtung, sobald Acronis den Auftrag erhalten hat und sobald der Auftrag abgeschlossen wurde. Sofern erforderlich, werden Sie von Acronis während der Auftragsbearbeitung kontaktiert.
- [Gelegentlich] **Fehler bei Backup-Erstellung** – Während der Sicherung ist ein Fehler aufgetreten. Überprüfen Sie die Parameter des Backup-Plans und versuchen Sie es dann erneut.
- **Das Medium wurde versendet** – Dieser Status wird eingestellt, nachdem Sie den Auftrag mit „Versendet“ gekennzeichnet haben.
- **Das Medium wurde von Acronis erhalten** – Acronis hat mit der Bearbeitung Ihres Auftrages begonnen. Von diesem Punkt an können Sie den Auftrag nicht mehr abbrechen. Die Erstellung eines neuen 'Initial Seeding'-Backups auf derselben Maschine erfordert eine neue 'Initial Seeding'-Lizenz.
- **Der Upload der Daten wurde gestartet** – Das Upload der Daten zum Acronis Online Backup Storage hat begonnen.

- **Der Upload der Daten wurde abgeschlossen** – Das anfängliche Voll-Backup wurde erfolgreich auf den Online Storage hochgeladen. Sie können nun inkrementelle Online Backups durchführen.
- **Der Auftrag wurde ausgeführt. Das Medium wurde zurückgeschickt** (oder: **Rücksendung des Mediums wurde nicht angefordert**) – Das Medium wurde zurückgeschickt (Transportunternehmen und Sendeverfolgungsnummer sind angegeben). Falls dem Medium kein frankiertes Versandetikett beigelegt wurde, wird das Medium entsorgt.
- [Gelegentlich] **Auftrag ist in Wartestellung** – Ihr Auftrag wurde wegen technischer Schwierigkeiten bei der Bearbeitung des Auftrages pausiert. Acronis arbeitet an einer Lösung der Probleme.
- [Gelegentlich] **Der Auftrag wurde abgebrochen** – Der Auftrag wurde noch vor Versendung des Mediums abgebrochen, dessen Rücksendung ist daher nicht erforderlich.
- [Gelegentlich] **Der Auftrag wurde abgebrochen. Das Medium wurde zurückgeschickt** (oder: **Rücksendung des Mediums wurde nicht angefordert**) – Der Auftrag wurde abgebrochen, während das Medium im Data Center war. Das Medium wurde zurückgeschickt (Transportunternehmen und Sendeverfolgungsnummer sind angegeben). Falls dem Medium kein frankiertes Versandetikett beigelegt wurde, wird das Medium entsorgt.

8.1.8 FAQ zu Large Scale Recovery

Dieser Abschnitt erklärt, was Large Scale Recovery ist, warum es für Sie vorteilhaft ist und zudem einige Details zu seiner Verwendung.

Was ist Large Scale Recovery?

Large Scale Recovery ist ein Extra-Service, mit dem Sie eine Kopie der Backups erhalten, welche sich im Online Storage befinden. Anschließend können Sie die Daten aus dieser Kopie wiederherstellen.

Sobald Sie ein Large Scale Recovery für eine bestimmte Maschine ordern, sendet Acronis Ihnen ein USB-Laufwerk mit allen Backups, die Sie von dieser Maschine erstellt haben. Sie können die Daten direkt vom Laufwerk wiederherstellen oder die Backups zu einem lokalen oder Netzwerkordner kopieren.

Wann ist Large Scale Recovery sinnvoll?

Der Dienst hilft Zeit und Netzwerkverkehr zu sparen, beispielsweise im Desasterfall, bei Wiederherstellung großer Datenmengen oder kompletter Maschinen. Eine Wiederherstellung von Daten im Bereich vieler Hundert Gigabytes über das Internet kann Tage dauern. Dieser Prozess ermöglicht Ihnen eine schnellere Wiederherstellung.

Muss Initial Seeding zur Nutzung von Large Scale Recovery ausgeführt werden?

Nein, diese Dienstleistungen sind voneinander unabhängig.

Ist Large Scale Recovery kostenpflichtig?

Ja, Sie benötigen je eine Lizenz für Large Scale Recovery pro Maschine. Durch diese Lizenz wird Ihnen bei Bedarf ein Laufwerk zugeschickt, das alle aktuell verfügbaren Backups dieser Maschine enthält. Um auch zukünftige Backups zu erhalten, benötigen Sie eine neue 'Large Scale Recovery'-Lizenz.

Kann ein Large Scale Recovery auf einer anderen Maschine erfolgen?

Ja. Sie können Ihre Daten beliebig oft auf jeder gewünschten Maschine wiederherstellen. Acronis

Universal Restore ist bereits integriert, so dass Sie ein Betriebssystem auch auf abweichender Hardware wiederherstellen können.

Können Backups mehrerer Maschinen gemeinsam auf einem Laufwerk zurückerhalten werden?

Nein. Es ist ein separates Laufwerk für jede Maschine erforderlich.

Wie kann eine Lizenz für Large Scale Recovery erworben werden?

Sie können eine 'Large Scale Recovery'-Lizenz von einem Acronis-Partner oder im Acronis Online Store kaufen. Verwenden Sie den Link www.acronis.de/my/backup-recovery-online/#buy, um einen Partner zu finden oder einen Online-Kauf durchzuführen.

Nachdem Sie eine Lizenz von einem Acronis-Partner erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit einem Registrierungscode. Klicken Sie auf derselben Webseite auf **Neuen Registrierungscode eingeben** und registrieren Sie die Lizenz. Die Lizenz wird dann über die Registerlasche **Initial Seeding / Recovery** zur Verfügung gestellt.

Eine über den Acronis Online Store erworbene Lizenz wird unmittelbar nach Abschluss des Zahlvorgangs verfügbar.

Wie kann der Auftragsstatus für Large Scale Recovery verfolgt werden?

Auf der Acronis-Website zeigt die Registerlasche **Initial Seeding / Recovery** den Status aller Aufträge. Sie erhalten zusätzlich eine E-Mail-Benachrichtigung über wichtige Ereignisse.

- **Verfügbar** – Die Lizenz kann für eine beliebige Maschine verwendet werden.
- **Ein Auftrag wurde erstellt** – Dieser Status ist nach Auftragsabschluss für Large Scale Recovery eingestellt. Diese Lizenz kann nicht mehr für eine andere Maschine verwendet werden. Sie können von diesem Punkt an den Auftrag auch abbrechen, wenn etwas falsch läuft. Dadurch wird die Lizenz an den Pool verfügbarer Lizenzen zurückgegeben.
- **Der Auftrag wird bearbeitet** – Das Data Center hat mit der Auftragsbearbeitung begonnen.
- **Schreibe Daten** – Ihre Backups werden gerade auf das Medium geschrieben. Von diesem Punkt an können Sie den Auftrag nicht mehr abbrechen.
- **Schreiben der Daten wurde abgeschlossen** – Ihre Backups wurden erfolgreich auf das Medium geschrieben.
- **Bereit, das Medium zu versenden** – Ihr Auftrag wurde bearbeitet und das Medium wird in Kürze verschickt.
- **Der Auftrag wurde ausgeführt. Das Medium wurde versendet** – Das Medium wurde an Sie verschickt (Transportunternehmen und Sendeverfolgungsnummer sind angegeben).
- [Gelegentlich] **Auftrag ist in Wartestellung** – Ihr Auftrag wurde wegen technischer Schwierigkeiten bei der Bearbeitung des Auftrages pausiert. Acronis arbeitet an einer Lösung der Probleme.
- [Gelegentlich] **Der Auftrag wurde abgebrochen** – Der Auftrag wurde abgebrochen.
- [Gelegentlich] **Adresse ist nicht zustellbar** – Acronis kann das Laufwerk nicht verschicken. Klicken Sie auf der gleichen Webseite auf **Meine Lieferadresse ändern** und spezifizieren Sie die richtige Adresse für den Auftrag.
- [Gelegentlich] **Adresse wurde aktualisiert** – Dieser Status wird eingestellt, nachdem Sie die Zustelladresse auf der Acronis-Website geändert haben.

Wie wird Large Scale Recovery ausgeführt?

Der Recovery-Vorgang ist identisch zu anderen Wiederherstellungen vom Online Storage. Sie spezifizieren lediglich den Pfad zum Speicherort Ihrer Backups. Weitere, detaillierte Informationen zu Recovery-Aktionen finden Sie in der kontextabhängigen Hilfe.

8.1.9 FAQ zum Abonnement-Lebenszyklus

Dieser Abschnitt erläutert den Lebenszyklus eines Abonnement und die Aktionen mit Abonnements, die Sie auf der Webseite zur Kontonverwaltung ausführen können.

Wie kann auf die Webseite zur Kontoverwaltung zugegriffen werden?

So gelangen Sie über die Acronis-Website auf die entsprechende Webseite:

1. Wählen Sie **Mein Konto**.
2. Melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie noch nicht registriert sind).
3. Navigieren Sie zu **Online Backup** –> **Für Unternehmen**.

So gelangen Sie über Acronis Backup & Recovery 10 auf die entsprechende Webseite:

1. Klicken Sie im Menü **Aktionen** auf **Abonnements für Online Backup aktivieren**.
2. Klicken Sie auf **Zur Webseite der Kontoverwaltung gehen**
3. Melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie noch nicht registriert sind).

Wo sind erworbene Abonnements zu finden?

Wenn Sie Abonnements von einem Acronis-Partner erworben haben, sollten Sie eine Bestätigungs-E-Mail mit den Registrierungscodes für jedes Abonnement erhalten haben. Erstellen Sie – falls noch nicht vorhanden – ein Konto auf der Acronis-Website und melden Sie sich an. Navigieren Sie zu **Online Backup** –> **Für Unternehmen**. Das ist die *Webseite zur Kontoverwaltung*. Klicken Sie auf **Neuen Registrierungscode eingeben** und registrieren Sie die Lizenz. Diese Abonnements erscheinen in der Liste verfügbarer Abonnements in der Registerlasche **Abonnements verwalten**.

Wenn Sie Abonnements online über die Acronis-Website erworben haben, können Sie diese unverzüglich auf der Webseite zur Kontoverwaltung finden. Neu erhaltene Abonnements sind in der Registerlasche **Abonnements verwalten** aufgelistet.

Wann beginnt ein Abonnement?

Ein Abonnement beginnt erst zu einem Zeitpunkt Ihrer Wahl, nicht beim Erwerb.

Die Zeit läuft erst ab, sobald das Abonnement aktiviert wird. Die erste Aktivierung erfolgt, sobald Sie ein Abonnement einer bestimmten Maschine zuweisen. Dazu muss eine entsprechende Acronis-Software installiert sein.

Was passiert bei Ablauf eines Abonnements?

Einen Monat vor Ablaufdatum des Abonnements erhalten Sie eine Alarmmeldung per E-Mail. Sie können diese Alarmmeldung auch auf der Webseite zur Kontoverwaltung sehen (neben der Maschine). Das bedeutet, dass Sie das Abonnement erneuern (S. 410) müssen, um mit den Backups der Maschine fortfahren zu können.

Falls Sie das Abonnement nicht erneuern, können Sie noch weitere fünf Tage nach Ablaufdatum zum

Online Storage sichern. Sie können Daten aus dem Online Storage noch bis zu 30 Tage nach Ablaufdatum wiederherstellen.

Wie wird ein Abonnement erneuert?

Erwerben Sie ein anderes Abonnement und spezifizieren Sie dieses als nächstes Abonnement für die Maschine. Das neue Abonnement wird aktiviert, sobald das aktuelle Abonnement endet.

Ein abgelaufenes Abonnement kann innerhalb von fünf Tagen nach Ablauf erneuert werden. In solchen Fällen wird das neue Abonnement unverzüglich aktiviert.

Ein einzelnes Abonnement erneuern

So erneuern Sie ein Abonnement

1. Gehen Sie zur Webseite der Kontoverwaltung.
2. Sorgen Sie dafür, dass ein Abonnement mit der *gleichen* Storage-Quota verfügbar ist.
3. Wählen Sie die Maschine, deren Abonnement Sie erneuern wollen und klicken Sie dann auf **Erneuern**.

Das Abonnement erscheint für die gewählte Maschine in der Spalte **Nächstes Abonnement**.

Mehrere aktivierte Abonnements auf einmal erneuern

Diese Aktion ist möglich, wenn die Anzahl der neuen Abonnements mit der Zahl der gegenwärtig genutzten Abonnements übereinstimmt.

Sorgen Sie dafür, dass die neuen Abonnements auf der Webseite zur Kontoverwaltung verfügbar sind. Klicken Sie dann auf **Alle erneuern**. Das Bestätigungsfenster fasst zusammen, welche Abonnements erneuert werden. Wenn für einige Maschinen keine identischen Abonnements gefunden werden, haben Sie die Option, den automatischen Vorgang abzubrechen und jedes Abonnement einzeln zu erneuern.

Was bedeutet „Automatisches Erneuern“?

Wenn ein Abonnement endet, wird das nächste Abonnement automatisch aus den verfügbaren Abonnements gewählt, also automatisch erneuert. Das nächste Abonnement muss zum aktuellen Abonnement identisch sein.

Wenn kein identisches Abonnement gefunden wird, erfolgt keine automatische Erneuerung und die Backups könnten fehlschlagen. Es werden keine Abonnements automatisch gekauft. Es können nur Abonnements verwendet werden, die zum Zeitpunkt der automatischen Erneuerung verfügbar sind. Sie können die automatische Erneuerung für jedes einzelne Abonnement wählen oder als Aktion für alle vorhandenen, aktivierten Abonnements.

Wofür gibt es die Spalte „Gruppe“?

Damit können Sie solche Aktionen wie **Alle erneuern** oder **Alle automatisch erneuern** auf ausgewählte Abonnements anwenden. Spezifizieren Sie den gewünschten Gruppennamen (beispielsweise Verkaufsabteilung), bei den Abonnements, die Sie gruppieren wollen. Klicken Sie auf den Spaltenkopf **Gruppe**, um die Abonnements zu sortieren und wenden Sie dann die gewünschten Aktionen auf die Gruppe an.

Kann ein Abonnement auf einer Maschine widerrufen werden?

Sie können ein einmal aktiviertes Abonnement nicht erneut in die Liste der verfügbaren

Abonnements stellen, aber sie können es einer beliebigen Maschine über die Benutzeroberfläche von Acronis Backup & Recovery 10 neu zuweisen (S. 413).

Können Abonnements gekündigt werden?

Warten Sie einfach, bis das Abonnement abgelaufen ist. Rückerstattungen sind bei Abonnements für Online Backup nicht möglich.

8.2 Was sind meine ersten Schritte?

Melden Sie sich bei Ihrem Konto auf der Acronis-Website an (oder erstellen Sie ein Konto, falls Sie noch nicht registriert sind) und navigieren Sie zu **Online Backup**, **Für Unternehmen**. Das ist die *Webseite zur Kontoverwaltung*. Sie können hier ein Test-Abonnement erhalten, einen Acronis-Partner finden oder ein Abonnement online kaufen. Neu erhaltene Abonnements sind als verfügbare Abonnements in der Registerlasche **Abonnements verwalten** aufgelistet.

Wenn Sie Ihre Abonnements von einem Acronis-Partner erworben haben, dann registrieren Sie diese manuell unter Verwendung des Links '**Neuen Registrierungscode eingeben**'. Der Registrierungscode kommt zusammen mit der Kaufbestätigung per E-Mail.

Danach installieren Sie die Acronis Software (falls noch nicht installiert) und müssen nun jedes Abonnement einer Maschine zuweisen (S. 412). Dadurch werden die Abonnements aktiviert. Sie können anschließend mit dem Backup zum Acronis Online Backup Storage beginnen.

8.3 Abonnement wählen

Normalerweise wählen Sie ein Abonnement auf Basis des auf der Maschine laufenden Betriebssystems.

Von Acronis Backup & Recovery 10 Online unterstützte Server-Betriebssysteme:

- Windows 2000 Server/Advanced Server
- Windows Server 2003/2003 R2 – Standard-, Enterprise-, Small Business Server-Editionen (x86, x64)
- Windows Server 2008 – Standard-, Enterprise-, Small Business Server-, Foundation-Editionen (x86, x64)
- Windows Server 2008 R2 – Standard-, Enterprise-, Small Business Server-, Datacenter-, Foundation-Editionen
- Windows MultiPoint Server 2010

Von Acronis Backup & Recovery 10 Online unterstützte Workstation-Betriebssysteme:

- Windows 2000 Professional SP4
- Windows XP Professional SP2+ (x86, x64)
- Windows Vista – alle Editionen mit Ausnahme von Vista Home Basic und Vista Home Premium (x86, x64)
- Windows 7 – alle Editionen mit Ausnahme der Starter- und Home-Editionen (x86, x64)

Von Acronis Backup & Recovery 10 Online unterstützte Virtualisierungsprodukte (Host-basiertes Backup von virtuellen Maschinen):

- VMware ESX Infrastructure 3.5 Update 2+
- VMware ESX(i) 4.0 und 4.1

(Host-basierte Backups stehen nur für kommerzielle Lizenzen von VMware ESXi zur Verfügung).

- Windows Server 2008/2008 R2 (x64) mit Hyper-V
- Microsoft Hyper-V Server 2008/2008 R2

Wenn es sich abzeichnet, dass Ihre Backups die Storage-Quota dieses Abonnementtyps überschreiten dürften, können Sie ein Abonnement mit größerer Storage-Quota verwenden. Sie können beispielsweise auf einer Workstation auch ein Abonnement für Server oder für virtuelle Maschinen verwenden. Oder Sie können auf einem Server, der kein Virtualisierungs-Server ist, auch ein Abonnement für virtuelle Maschinen verwenden.

Die umgekehrte Verwendung ist jedoch nicht möglich. Sie können einen Server nicht mit einem Workstation-Abonnement sichern. Wenn Sie versuchen, virtuelle ESX(i)- oder Hyper-V-Maschinen von einem Host zu sichern, der ein Server-Abonnement verwenden, dann schlägt das Backup fehl. Mit einem Server-Abonnement können Sie nur den Windows-Host sichern. Mit einem Abonnement für virtuelle Maschinen können Sie dagegen sowohl den Windows-Host wie auch dessen virtuelle Maschinen sichern.

Test-Abonnements

Sie können per Konto ein freies Abonnement für Workstations, Server oder virtuelle Maschinen erhalten. Die Storage-Quota des Test-Abonnements ist gleich zu der des Standard-Abonnements. Der Abonnementzeitraum ist auf 2 Monate beschränkt.

Ein Test-Abonnement zu erhalten ist solange möglich, bis Sie ein bezahltes Abonnement eingehen. Sie können ein Test-Abonnement zusammen mit bezahlten Abonnements verwenden. Für Test-Abonnements gelten die gleichen Ablaufregeln wie für bezahlte Abonnements.

Sie können den Dienst nach Ablauf des Test-Abonnements weiter verwenden, wenn Sie denselben Typ von Abonnement erwerben und das Test-Abonnement erneuern, indem Sie das gekaufte Abonnement spezifizieren. Die auf dem Online Storage gesicherten Daten bleiben erhalten. Regelmäßige Backups Ihrer Maschinen werden ohne Unterbrechung fortgesetzt. Ein erneutes Voll-Backup ist nicht nötig.

8.4 Abonnements für Online Backup aktivieren

Damit eine Maschine zum Online Storage gesichert werden kann, müssen Sie ein Abonnement für den Acronis Backup & Recovery 10 Online-Service erwerben und aktivieren. Sie können Abonnements über die Acronis-Website oder von einem Acronis-Reseller erwerben.

Beachten Sie vor Aktivierung eines Abonnements folgende Hinweise:

- Sobald Sie ein Abonnement aktivieren, startet der Abonnementzeitraum. Damit Sie den Abonnementszeitraum voll ausschöpfen können, aktivieren Sie das Abonnement erst, wenn alles für ein Backup der Maschine eingerichtet ist.
- Wenn einer Maschine bereits ein Abonnement zugewiesen wurde, wird das neue Abonnement das alte ersetzen. Sie können das alte Abonnement einer anderen Maschine neu zuweisen – siehe dazu den Abschnitt „Aktiviertes Abonnement neu zuweisen“.

8.4.1 Abonnements aktivieren

Stellen Sie zu Beginn sicher, dass die Maschinen, deren Abonnements Sie aktivieren möchten, auf dem Management Server registriert und verfügbar sind (eingeschaltet).

So aktivieren Sie Abonnements

1. Verbinden Sie die Konsole mit dem Management Server.
2. Klicken Sie im Fensterbereich **Aktionen** auf **Abonnement für Online Backup aktivieren**
3. Spezifizieren Sie Benutzername und Kennwort zur Anmeldung am Online Storage.
4. Wählen Sie die Maschine und klicken Sie auf **Abonnement wählen**.
5. Wählen Sie unter **Verfügbare Abonnements** dasjenige, welches Sie für die Maschine aktivieren möchten.
6. Klicken Sie auf **Jetzt aktivieren**.
7. Führen Sie die beschriebenen Schritte für jede Maschine aus, für die Sie ein Abonnement aktivieren möchten.

Alternativ können Sie ein Abonnement aktivieren, wenn anstelle des Management Servers die Konsole zur Maschine verbunden ist.

8.4.2 Aktiviertes Abonnement erneut zuweisen

Manchmal möchten Sie vielleicht ein bereits aktiviertes Abonnement anstelle eines verfügbaren Abonnements verwenden. Typische Beispiele wären folgende:

- Sie benötigen bei einer der Maschinen keine Backups mehr und möchten das Abonnement dieser Maschine für ein andere verwenden.
- Sie haben auf einer Maschine Acronis Backup & Recovery 10 erneut installiert und möchten deren Online Backups fortsetzen.
- Sie haben die Maschine auf fabrikneue Hardware wiederhergestellt (oder in einen Zustand, in dem noch kein Abonnement aktiviert war) und möchten deren Online Backups fortsetzen.

Wenn Sie ein Abonnement neu zuweisen, startet der Abonnementzeitraum nicht von Neuem.

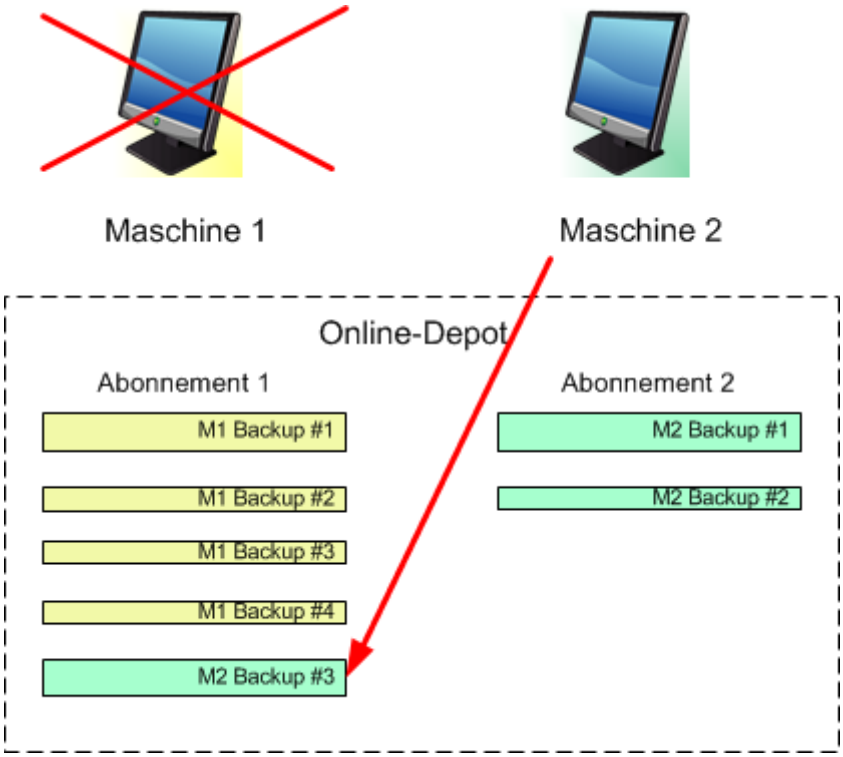
So weisen Sie einer Maschine ein aktiviertes Abonnement zu

1. Gehen Sie auf der Maschine, der Sie ein aktiviertes Abonnement zuweisen möchten, in das Fenster zum Aktivieren des Abonnements.
2. Wählen Sie bei **Aktivierte Abonnements** ein aktiviertes Abonnement, welches Sie der Maschine neu zuweisen wollen.
3. Klicken Sie auf **Jetzt aktivieren**.

Beispiel

Das untere Diagram verdeutlich, was passiert, wenn Sie ein Abonnement einer anderen Maschine neu zuweisen. Angenommen, Maschine 1 hat vier Backups in Abonnement 1. Maschine 2 hat zwei Backups in Abonnement 2. Zu diesem Zeitpunkt weisen Sie das Abonnement 1 auf Maschine 2 neu zu. Maschine 2 erstellt ihr drittes Backup zu Abonnement 1.

In Abhängigkeit von Ihren Einstellungen wird dieses Backup entweder vollständig oder inkrementell. Seine Größe ist aber vermutlich nicht geringer als die Größe eines Voll-Backups. Es ist daher nicht praktisch, ein Abonnement einer Maschine neu zuzuweisen, deren erstes Backup als 'Initial Seeding' durchgeführt wurde. Sie müssen dann entweder das 'Initial Seeding' erneut ausführen (was eine neue Lizenz benötigt) oder das beträchtlich große Backup über das Internet übertragen.



Alle früher erstellten Backups verbleiben intakt. Sie können diese manuell löschen, falls notwendig. Beachten Sie aber, dass Backups von einem Abonnement nur durch die Maschine gelöscht werden können, der das Abonnement zugewiesen wurde. Sie haben beispielsweise folgende Optionen.

Vor erneuter Zuweisung

Löschen Sie Backups vom Abonnement 1 unter Verwendung von Maschine 1 (sofern verfügbar und angeschaltet). Löschen Sie Backups von Abonnement 2 unter Verwendung von Maschine 2.

Nach erneuter Zuweisung

Löschen Sie Backups von Abonnement 1 unter Verwendung von Maschine 2. Sie können Backups von Abonnement 2 nicht löschen, solange Sie dieses Abonnement keiner anderen Maschine zuweisen.

8.5 Proxy-Einstellungen konfigurieren

Wenn eine oder mehrere Maschinen mit installiertem Agent per Proxy-Server auf das Internet zugreifen, dann müssen Sie jeden entsprechenden Agenten zur Verwendung des Proxy-Servers konfigurieren.

Der Management Server verbindet sich mit dem Internet, um Informationen über die Online-Backup-Abonnements abzurufen. Deshalb müssen die Proxy-Einstellungen auch für den Management Server konfiguriert werden.

Die Proxy-Einstellungen für Agent und Management Server müssen separat konfiguriert werden, auch wenn sie auf derselben Maschine installiert sind.

So konfigurieren Sie die Proxy-Einstellungen für den Agent

1. Verbinden Sie die Konsole mit der Maschine, deren Proxy-Einstellungen Sie konfigurieren wollen.
2. Klicken Sie im Menü **Optionen** auf **Optionen der Maschine**.
3. Klicken Sie auf **Online Backup-Proxy**.

4. Tragen Sie die Einstellungen für den Proxy-Server ein. Konsultieren Sie die kontextabhängige Hilfe, um detaillierte Informationen (S. 96) zu den Einstellungen zu erhalten.
5. Wiederholen Sie die Schritte 2-5 für alle Maschinen, die per Proxy-Server auf das Internet zugreifen.

So konfigurieren Sie die Proxy-Einstellungen für den Management Server

1. Verbinden Sie die Konsole mit dem Management Server.
2. Klicken Sie im Menü **Optionen** auf **Optionen des Management Servers**.
3. Klicken Sie auf **Online Backup-Proxy**.
4. Tragen Sie die Einstellungen für den Proxy-Server ein. Konsultieren Sie die kontextabhängige Hilfe, um detaillierte Informationen (S. 96) zu den Einstellungen zu erhalten.

8.6 Beschränkungen des Online Storages

Abweichend von anderen, ebenfalls in Acronis Backup & Recovery 10 verfügbare Storages hat der Online Storage nachfolgende Einschränkungen.

Aktionen

Folgende Aktionen sind nicht möglich.

Backup-Aktionen:

- Backup von einem bootfähigen Medium ausgehend
- Backup unter Linux
- Erstellen differentieller Backups
- Verwendung der Backup-Schemata **Großvater-Vater-Sohn (GVS)**, **Türme von Hanoi** und **Benutzerdefiniert**
- Vereinfachte Benennung der Backup-Dateien
- Konvertieren eines Backups in eine virtuelle Maschine.

Recovery-Aktion:

- Ein Backup als virtuelle Maschine wiederherstellen

Aktionen mit Backups:

- Backup exportieren
- Backup mounten

Aktionen mit Archiven (ein Archiv ist eine Zusammenstellung von Backups):

- Ein Archiv exportieren

Diese Einschränkungen gelten auch für Backups mit Initial Seeding bzw. Wiederherstellungen mit Large Scale Recovery.

Backup- und Recovery-Optionen

Einige Backup- und Recovery-Optionen werden bei Online Backups nicht unterstützt. Beispielsweise:

- **Backup-Aufteilung** (S. 112)
- **Dual-Destination** (S. 115)

Durch Verwendung der Option '**Backup-Performance –> Datendurchsatz im Netzwerk**' können Sie die Übertragungsrate in Kilobyte pro Sekunde (aber nicht in Prozent) variieren.

Befehlszeilen-Modus

Die Befehlszeilenprogramme von Acronis Backup & Recovery 10 unterstützen kein Online Backup.

8.7 Terminologiereferenz

Nachfolgend finden Sie einige Begriffe in Bezug auf Acronis Backup & Recovery 10 Online.

Ein Abonnement aktivieren

Ermöglicht der Maschine, den Online Storage in Übereinstimmung mit dem Abonnement zu verwenden. Der Abonnementszeitraum beginnt abzulaufen, sobald das Abonnement aktiviert ist.

Aktiviertes Abonnement

Ein Abonnement, das aktuell von einer Maschine verwendet wird.

Ein Abonnement einer Maschine zuweisen

Ein Abonnement für eine spezielle Maschine reservieren. Der Abonnementzeitraum beginnt solange nicht, bis das Abonnement aktiviert ist.

Zugeteiltes Abonnement

Ein Abonnement, welches einer Maschine zugewiesen wurde.

Verfügbares Abonnement

Ein Abonnement, welches noch keiner Maschine zugewiesen wurde.

Extra-Service

Ein Dienst, den Sie zusätzlich zu Abonnements für Online Backup verwenden können.

Initial Seeding

Initial Seeding ist ein Extra-Service, bei dem Sie das anfängliche Voll-Backup lokal ausführen und dieses dann per Festplatte (oder mit einem vergleichbaren Laufwerk) an Acronis senden. Acronis lädt das Backup dann zum Online Storage hoch. Danach können Sie dieses Voll-Backup – manuell oder nach Zeitplan – mit nachfolgenden inkrementellen Backups erweitern.

Large Scale Recovery

Large Scale Recovery ist ein spezieller Service, mit dem Sie eine Kopie der Backups erhalten, welche sich im Online Storage befinden. Anschließend können Sie die Daten aus dieser Kopie wiederherstellen.

Lizenz

Nicht zu verwechseln mit Produktlizenzen von Acronis Backup & Recovery 10.

Erlaubnis für eine Maschine, einen Extra-Service von Acronis Backup & Recovery 10 Online zu verwenden.

Sie können 'Initial Seeding'-Lizenzen bzw. 'Large Scale Recovery'-Lizenzen erwerben.

Ein Abonnement neu zuweisen

Ein bereits aktiviertes Abonnement einer anderen Maschine zuweisen.

Registrierungscode

Zeichenkette zur Registrierung eines Abonnements oder einer Lizenz, die bei einem Acronis-Partner erworben wurde.

Wenn Sie ein solches Abonnement oder eine solche Lizenz erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit den Registrierungscodes für jede von diesen. Danach tragen Sie diese Registrierungscodes auf der Webseite zur Kontoverwaltung ein – worauf diese Abonnements und Lizenzen zur Benutzung verfügbar werden.

Ein Abonnement erneuern

Zuweisen eines Abonnements, das die gleiche Storage-Quota wie das gegenwärtige, bereits aktivierte Abonnement hat.

Dieses Abonnement wird aktiviert, sobald das aktuelle Abonnement endet.

Storage-Quota

Menge an Speicherplatz auf dem Online Storage, die eine Maschine gemäß des Abonnements verwenden kann.

Abonnement

Erlaubnis für eine Maschine, eine bestimmte Menge an Speicherplatz für eine bestimmte Zeitdauer auf dem Online Storage zu verwenden.

Abonnementzeitraum

Zeitraum, in dem ein Abonnement aktiviert bleibt. Sie können die Maschine während dieses Zeitraums sichern und wiederherstellen. Eine Wiederherstellung ist auch noch für weitere 30 Tage nach Ablauf des Zeitraums möglich.

Eine Abonnement-Zuweisung aufheben

Macht ein bereits zugewiesenes Abonnement wieder verfügbar.

Sie können die Zuweisung eines Abonnements aufheben, so lange es nicht aktiviert wurde.

9 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. 424) 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. 432) hinzugefügt werden. Die resultierenden bootfähigen Medien (S. 422) können benutzt werden, jede PC-kompatible Maschine zu starten, und, mit gewissen Einschränkungen, die meisten direkten Verwaltungsaufgaben (S. 424) ohne Hilfe des Betriebssystems auszuführen. Aktionen können entweder lokal über die Benutzerschnittstelle oder remote mit Hilfe der Konsole (S. 426) konfiguriert und gesteuert werden.

Acronis Secure Zone

Sichere Partition zur Ablage von Backup-Archiven (S. 419) auf einer verwalteten Maschine (S. 431). 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. 424) oder Laufwerken mit GPT-Partitionsschema eingerichtet werden.

Die Acronis Secure Zone wird als persönliches Depot (S. 427) betrachtet.

Acronis Startup Recovery Manager (ASRM)

Eine Modifikation des bootfähigen Agenten (S. 422), 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. 427) 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. 421), ausgeführt vom Agent (S. 419) in Übereinstimmung mit dem Backup-Plan (S. 420), der das Archiv (S. 419) erstellt hat. Agentenseitige Bereinigung erfolgt in nicht verwalteten Depots (S. 427).

Agentenseitige Validierung

Validierung (S. 430), ausgeführt vom Agent (S. 419) in Übereinstimmung mit dem Backup-Plan (S. 420), der das Archiv (S. 419) erstellt hat. Agentenseitige Validierung erfolgt in nicht verwalteten Depots (S. 427).

Archiv

Siehe Backup-Archiv (S. 419).

Auswahlregel

Teil einer Backup-Richtlinie (S. 420). Ermöglicht dem Administrator des Management Servers (S. 427), die Daten der Maschine für das Backup auszuwählen.

B

Backup

Ein Backup ist das Ergebnis einer einzelnen Backup-Aktion (S. 419). 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. 425) oder Konsolidierung (S. 426) sind, werden ebenfalls als Backups bezeichnet.

Backup (Aktion)

Aktion, die eine Kopie der Daten erstellt, die auf der Festplatte einer Maschine (S. 427) existieren, um diese wiederherzustellen oder in den Zustand zu einem festgelegten Tag bzw. Zeitpunkt zurückzusetzen.

Backup-Archiv (Archiv)

Satz von Backups (S. 419), die mit einem Backup-Plan (S. 420) erstellt und verwaltet werden. Ein Archiv kann mehrere Voll-Backups (S. 431) enthalten, aber auch inkrementelle (S. 426) und differentielle Backups (S. 423). 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. 430), 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. 419), 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. 420).

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. 419) gespeichert werden (Namen der Backup-Archive und Speicherort)
- das Backup-Schema (S. 421), das den Zeitplan für die Sicherungen und [optional] die Aufbewahrungsregeln enthält
- [optional] die Richtlinien für die Validierung (S. 430) der Archive
- die Backup-Optionen (S. 420).

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. 429), die zur Ausführung auf einer verwalteten Maschine (S. 431) 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. 420) – zentraler Plan (S. 432).

Backup-Richtlinie (Richtlinie)

Template für einen Backup-Plan, das vom Administrator des Management Servers (S. 427) 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. 419) 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. 427) an.
3. Der Management Server verteilt die Richtlinie auf die Maschinen.
4. Auf jeder Maschine findet der dort installierte Agent (S. 419) 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. 420) unter Benutzung der Regeln, die durch die Richtlinie spezifiziert wurden. Ein solcher Plan heißt zentraler Plan (S. 432).
6. Auf jeder Maschine erstellt der Agent, der auf der Maschine installiert ist, einen Satz zentraler Aufgaben (S. 432), die den Plan ausführen.

Backup-Schema

Teil eines Backup-Plans (S. 420), der den Zeitplan für das Backup und [optional] die Aufbewahrungsregeln und den Zeitplan für die Bereinigung (S. 421) mit einschließt. Beispielsweise führe monatlich ein Voll-Backup (S. 431) am letzten Tag des Monats um 10:00 Uhr aus – und ein inkrementelles Backup (S. 426) 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. 419) aus einem Backup-Archiv (S. 419), 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. 420) 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. 42).

Bereinigung aufseiten des Storage Node

Bereinigung (S. 421), ausgeführt durch einen Storage Node (S. 429) gemäß des Backup-Plans (S. 420), auf dessen Grundlage die in einem verwalteten Depot (S. 431) abgelegten Archive (S. 419) erstellt

wurden. Als Alternative zur agentenseitigen Bereinigung (S. 419) befreit die Bereinigung auf dem Storage Node die produktiven Server von unnötiger CPU-Last.

Da der Zeitplan auf der Maschine (S. 427) existiert, auf der sich der Agent (S. 419) 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. 419) enthält. Der bootfähige Agent basiert auf einem Linux-Kernel. Eine Maschine (S. 427) kann entweder mit Hilfe bootfähiger Medien (S. 422) 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. 426) konfiguriert und gesteuert werden.

Bootfähiges Medium

Physikalische Medien (CD, DVD, USB-Sticks oder andere Medien, die vom BIOS einer Maschine (S. 427) als Boot-Gerät unterstützt werden), die den bootfähigen Agenten (S. 422) oder die Windows Preinstallation Environment (WinPE) (S. 432) mit dem Acronis Plug-in für WinPE (S. 418) 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. 425) 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. 424), 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. 427) 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. 431) mit aktivierter Deduplizierung (S. 423).

Deduplizierung

Methode, um identische Informationen in verschiedenen Kopien nur einmalig zu speichern.

Acronis Backup & Recovery 10 kann die Deduplizierungstechnologie auf Backup-Archive (S. 419) anwenden, die auf Storage Nodes (S. 429) 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. 419). 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. 421) 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. 431). 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. 431) unter Benutzung der direkten Verbindung zwischen Konsole (S. 426)und Agent (S. 419) ausgeführt wird (im Gegensatz zu zentraler Verwaltung (S. 432), wenn die Aktionen auf dem Management Server (S. 427) vorbereitet und dann durch den Server an die verwalteten Maschinen verteilt werden).

Die zentralen Verwaltungsaktionen umfassen:

- Erstellen und Verwalten lokaler Backup-Pläne (S. 427)
- Erstellen und Verwalten lokaler Tasks (S. 427), wie z.b. Recovery-Tasks
- Erstellen und Verwalten persönlicher Depots (S. 427) und der dort gespeicherten Archive
- Statusverfolgung, Fortschrittskontrolle und Konfiguration der Eigenschaften zentraler Tasks (S. 432), 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. 422). 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.

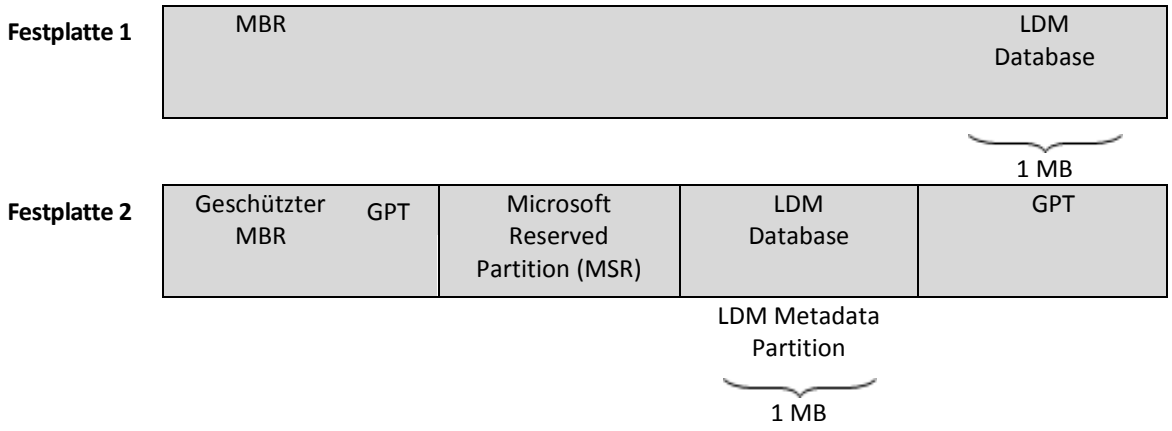
Disk-Backup (Image)

Backup (S. 419), 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. 427), die automatisch vom Management Server (S. 427) 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. 424) oder genauer auf einer Datenträgergruppe (S. 422) 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. 419) am von Ihnen angegebenen Speicherort erstellt wird. Ein Export kann ein einziges Archiv, ein einziges Backup (S. 419) oder eine Auswahl von Backups aus dem gleichen Archiv umfassen. Ein vollständiges Depot (S. 423) kann über die Befehlszeilenschnittstelle exportiert werden.

G

GVS (Großvater-Vater-Sohn)

Populäres Backup-Schema (S. 421), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 419) und der Anzahl von Wiederherstellungspunkten (S. 432) 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. 36).

I

Image

Gleichbedeutend mit Disk-Backup (S. 424).

Inkrementelles Backup

Backup (S. 419), 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. 419), 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. 419) und Acronis Backup & Recovery 10 Management Server (S. 427).

Wenn die Konsole zum Management Server verbunden ist, kann der Administrator Backup-Richtlinien (S. 420) einrichten und verwalten sowie auf andere Funktionen des Management-Servers zugreifen, d.h. er arbeitet mit zentraler Verwaltung (S. 432). Wenn der Administrator eine direkte Verbindung zwischen Konsole und Agent herstellt, arbeitet er mit direkter Verwaltung (S. 424).

Konsolidierung

Kombinieren zweier oder weiterer subsequenter Backups (S. 419), die zum gleichen Archiv (S. 419) gehören, in ein Backup.

Konsolidierung könnte beim Löschen von Backups gebraucht werden, entweder manuell oder während der Bereinigung (S. 421). Zum Beispiel könnten die Aufbewahrungsregeln erfordern, ein abgelaufenes Voll-Backup (S. 431) zu löschen, aber die nächste inkrementelle Sicherung (S. 426) 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. 420), erstellt auf einer verwalteten Maschine (S. 431) durch direkte Verwaltung (S. 424).

Lokaler Task

Task (S. 429), der zu einem lokalen Backup-Plan (S. 427) 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. 427) unter Benutzung von Backup-Richtlinien (S. 420) und Gruppierung
- unternehmensweiter Monitoring-Funktionalität
- der Fähigkeit, zentrale Depots (S. 433) für die Ablage der Backup-Archive (S. 419) des Unternehmens zu erstellen
- der Fähigkeit, Storage Node (S. 429) 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. 422).

N

Nicht verwaltetes Depot

Jedes Depot (S. 423), das kein verwaltetes Depot (S. 431) ist.

P

Persönliches Depot

Lokales oder im Netzwerk befindliches Depot (S. 423), das durch direkte Verwaltung (S. 424) 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. 428). 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. 420).

R

Registrierte Maschine

Maschine (S. 427), die durch einen Management Server (S. 427) 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. 428).

Registrierung

Verfahren, das eine verwaltete Maschine (S. 431) zu einem Management Server (S. 427) hinzufügt.

Die Registrierung stellt eine Vertrauensstellung zwischen dem Agenten (S. 419) 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. 420).

S

Standardgruppe

Gruppe von Maschinen, die immer auf einem Management Server (S. 427) existiert, also eingebaut ist.

Ein Management Server hat zwei eingebaute Gruppen, die alle Maschinen von jedem Typ enthalten: alle physikalischen Maschinen (S. 428), alle virtuellen Maschinen (S. 431).

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. 420) angewendet werden.

Statische Gruppe

Maschinengruppe, die der Administrator eines Management Servers (S. 427) 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. 431) erreicht. Storage Nodes ermöglichen dem Verwalter:

- verwaltete Maschinen (S. 431) durch Benutzung der Storage Node-seitigen Bereinigung (S. 421) und der Storage Node-seitigen Validierung (S. 429) von unnötiger CPU-Last zu befreien,
- den für die Archive (S. 419) verwendeten Backup-Traffic und den Speicherplatz durch Deduplizierung (S. 423) drastisch zu senken,
- mit Hilfe verschlüsselter Depots (S. 431) 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. 430), ausgeführt durch einen Storage Node (S. 429) gemäß des Backup-Plans (S. 420), auf dessen Grundlage die auf einem verwalteten Backup-Speicher (S. 431) gespeicherten Archive (S. 419) erstellt wurden. Als Alternative zur agentenseitigen Validierung (S. 419) 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. 431) 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. 421), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 419) und der Anzahl von Wiederherstellungspunkten (S. 432) sorgen soll, die im Archiv enthalten sind. Im Gegensatz zum GVS (S. 426)-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. 40).

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. 418) (unter Benutzung von F11) gebootet wurde,
- das wiederherzustellende Image in der Acronis Secure Zone (S. 418) abgelegt ist oder
- wenn Acronis Active Restore (S. 418) 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. 419) 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. 420). Richtlinien definieren, wann und wie eine Validierung (S. 430) durchzuführen ist und ob das gesamte Archiv (S. 419) zu validieren ist oder nur das letzte Archiv im Backup.

Verschlüsseltes Archiv

Backup-Archiv (S. 419), das nach dem Advanced Encryption Standard (AES) verschlüsselt ist. Wenn die Verschlüsselungsoption und ein Kennwort für das Archiv in den Backup-Optionen (S. 420) definiert werden, wird jedes Backup, das zum Archiv gehört, vom Agent (S. 419) 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. 431), bei dem ein Storage Node (S. 429) 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. 430) werden über die Verschlüsselung des Agenten (S. 419) erstellt.

Verwaltete Maschine

Physikalische oder virtuelle Maschine (S. 427), auf der wenigstens ein Acronis Backup & Recovery 10 (S. 419) Agent installiert ist.

Verwaltetes Depot

Zentrales Depot (S. 433), das durch einen Storage Node (S. 429) verwaltet wird. Auf Archive (S. 419) 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. 421) und die Storage Node-seitige Validierung (S. 429) 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. 423) 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. 427) als virtuell angesehen, wenn das Backup vom Virtualisierungs-Host erstellt werden kann, ohne dass ein Agent (S. 419) 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. 419), 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. 418) ermöglicht die Ausführung von Acronis Backup & Recovery 10 Agent (S. 419) 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. 427) genannt wird. Die zentralen Verwaltungsaktionen umfassen:

- Erstellen, Verwenden und Verwalten von Backup-Richtlinien (S. 420)
- Erstellen und Verwalten statischer (S. 429) und dynamischer Gruppen (S. 425) von Maschinen (S. 427)
- Verwalten von existierenden Tasks (S. 429) auf den Maschinen
- Erstellen und Verwalten von zentralen Depots (S. 433) für die Speicherung von Archiven
- Verwalten von Storage Node (S. 429)
- Überwachen der Tätigkeiten der Komponenten von Acronis Backup & Recovery 10, Einsicht in die zentralen Logs u.a.

Zentraler Backup-Plan

Backup-Plan (S. 420), der auf der verwalteten Maschine (S. 431) als Ergebnis der Verteilung einer Backup-Richtlinie (S. 420) durch den Management Server (S. 427) erscheint. Ein solcher Plan kann nur durch Bearbeitung der Backup-Richtlinie modifiziert werden.

Zentraler Task

Task (S. 429), der zu einem zentralen Backup-Plan (S. 432) gehört. Solch ein Task erscheint auf der verwalteten Maschine (S. 431) infolge der Verteilung einer Backup-Richtlinie (S. 420) durch den Management Server (S. 427) und kann nur durch Bearbeiten des Sicherstellungsgrundsatzes

modifiziert werden.

Zentrales Depot

Ein Speicherort im Netzwerk, der vom Administrator des Management Servers (S. 427) zugeteilt wird, um als Speicherplatz für die Backup-Archive (S. 419) zu dienen. Ein zentrales Depot kann von einem Storage Node (S. 429) 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. 428) verteilt. Der Shortcut zum Depot erscheint auf den Maschinen in der Liste der zentralen Depots. Jeder Backup-Plan (S. 420), 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.