Acronis

Acronis®
vmProtect™ 6

Benutzeranleitung

Inhaltsverzeichnis

1 Einführung in Acronis vmProtect 6.0

Acronis ist der festen Überzeugung, dass durch die Virtualisierung und den Übergang zum Cloud Computing nicht nur eine bessere Art der Computernutzung entsteht, sondern sich so auch Ausfallzeiten verringern und schnellere Recovery-Zeiten bei gleichzeitiger Kostenersparnis erreichen lassen. Leider wurden die meisten Backup- und Recovery-Lösungen für physikalische Systeme entwickelt und sind daher entweder nicht ausreichend leistungsfähig für eine virtuelle Umgebung oder bieten nicht dieselben (Kosten-)Vorteile, die durch eine Virtualisierung potenziell erreichbar wären.

Acronis arbeitet mit vollem Engagement an der Unterstützung seiner Kunden und Vertriebspartner, damit diese alle Vorteile der Virtualisierung genießen können; es ist unser Ziel, in den folgenden Punkten neue Maßstäbe für Backup und Recovery in einer virtualisierten Umgebung zu setzen:

- Verringern von Betriebs- und Wartungskosten im IT-Bereich, um durch den Einsatz einer benutzerfreundlichen und leicht zu implementierenden Technologie die Unternehmensleistung zu steigern;
- Minimieren von Betriebskosten und Ausschöpfen aller Vorteile einer VMware vSphere-Umgebung durch Bereitstellung einer speziell für virtualisierte Umgebungen entwickelten Backup- und Recovery-Lösung;
- Minimieren des Risikos eines Datenverlusts durch auf Acronis Online Storage gespeicherte Offsite-Backups.

2 Acronis vmProtect 6.0 – Überblick

Acronis vmProtect 6.0 ist eine umfassende Backup- und Recovery-Lösung für VMware vSphere™-Umgebungen. Sie ermöglicht das Erstellen von Backups ganzer ESX oder ESXi virtueller Maschinen ohne Einsatz des Agenten sowie die Wiederherstellung ganzer Maschinen oder einzelner Dateien und Ordner.

2.1 Funktionen von Acronis vmProtect

Mit der preisgekrönten Imaging-Technologie von Acronis, erstellt Acronis vmProtect 6.0 exakte Images (Backups) von virtuellen Maschinen einschließlich des Gast-Betriebssystems, der Konfigurationsdateien, Anwendungen, Ressourcenpool- bzw. vApp-Eigenschaften und Datenspeicher-Einstellungen. Sie können ein solches Backup dann entweder auf dem ursprünglichen oder einem neuen ESX- bzw. ESXi-Host wiederherstellen. Eine der wichtigsten neuen Funktionen ist die Möglichkeit, eine virtuelle Maschine ohne Wiederherstellung direkt aus dem Backup zu starten, und die VM nach einem Ausfall so in nur wenigen Sekunden wieder betriebsbereit zu machen.

Weitere neue Funktionen sind z.B.:

- Die Auswahlmöglichkeit zwischen virtueller Appliance und Windows-basierter Installation
- Web-basierte und einfach zu bedienende Bedienoberfläche
- LAN-freies Backup mit Direktzugriff auf gemeinsam genutzten Storage
- Schnelle Wiederherstellung durch sofortiges Ausführen einer VM von Backup auf einem vorhandenen ESX- oder ESXi-Host
- Neues, verbessertes und für den Modus 'Nur inkrementell' optimiertes Storage-Format für Backups
- Gleichzeitige Backups mehrerer virtueller Maschinen
- Unterstützung für die vApp- und Ressourcenpool-Einstellungen für Backup bzw. Recovery
- Unterstützung von Changed Block Tracking (CBT)

Die wichtigsten Vorteile von Acronis vmProtect 6.0 sind:

1. **Einfach zu bedienen:** Acronis vmProtect kann entweder als virtuelle Appliance bereitgestellt oder auf einer Windows-Maschine installiert und über die brandneue webbasierte Schnittstelle verwaltet werden. Die fundierte Erfahrung von Acronis mit dem Design intuitiver GUIs sowie die Fokussierung auf VMware ermöglichen über die Schnittstelle den sofortigen Start ohne eine Dokumentation lesen oder erkunden zu müssen und verhindert gefährliche Fehler bei der Bedienung oder Konfiguration.
2. **Mehr Funktionalität:** Zusätzlich zu den Standardfunktionen Backup und Wiederherstellung bietet vmProtect einzigartige Funktionalität wie zum Beispiel: Das Ausführen einer virtuellen Maschine direkt von Backup; eine unbegrenzte Anzahl von P2V-Konvertierungen; Backups auf den Cloud-basierten Acronis Online Storage; Industriestandard 256-Bit-Verschlüsselung für den Schutz der Backups.
3. **Geringes TCO (Total Cost of Ownership):** Die Anschaffungskosten für vmProtect werden anhand günstiger Listenpreise per CPU berechnet. Die virtuelle Appliance erfordert keine spezielle Maschinen- oder Windows-Lizenz; die verlässliche und intuitive Lösung spart Administratorzeit und Verwaltungskosten ein.
4. **Eine sichere Investition durch die Zusammenarbeit mit einem etablierten Hersteller**

3 So funktioniert Acronis vmProtect 6.0

3.1 Backup und Wiederherstellung von virtuellen Maschinen

Genau wie physikalische Maschinen sollte auch eine virtuelle Maschine (oder mehrere VMs als virtuelle Infrastruktur) geschützt werden. Nachdem Sie den Acronis vmProtect 6.0-Agenten installiert haben, können Sie:

- Backups von einer oder mehreren virtuellen, auf dem Server angesiedelten Maschinen erstellen, ohne dass zusätzliche Software auf jeder virtuellen Maschine installiert werden muss
- eine virtuelle Maschine zu derselben oder einer anderen virtuellen Maschine wiederherstellen, die sich entweder auf demselben Server oder auf einem anderen Virtualisierungsserver befindet Die im Backup einer virtuellen Maschine gespeicherte Konfiguration wird ebenso zu einer neuen virtuellen Maschine wiederhergestellt wie die Daten der virtuellen Laufwerke.

Eine virtuelle Maschine kann während der Backup-Erstellung online ('Ausführung'), offline ('gestoppt') oder 'angehalten' sein – oder zwischen diesen Stadien wechseln.

Während der Wiederherstellung zu einer virtuellen Maschine muss diese jedoch offline (gestoppt) sein. Die Maschine wird vor Ausführung der Wiederherstellung automatisch gestoppt. Sie können sich auch dafür entscheiden, die Maschinen manuell zu stoppen.

Weitere Informationen finden Sie in den Abschnitten 'Backups virtueller Maschinen erstellen' (S. 22) und 'Backups von virtuellen Maschinen wiederherstellen' (S. 34).

3.2 Backup-Archivstruktur

Acronis vmProtect ermöglicht Ihnen das Erstellen von Backups virtueller Maschinen unter Verwendung eines der beiden folgenden Backup-Archiv-Schemata: das Backup-Schema für mehrere Dateien (Legacy-Modus) oder das Backup-Schema für eine einzelne Datei (Modus 'Nur inkrementell').

In Acronis vmProtect ist das Backup-Schema 'Eine Datei' standardmäßig eingestellt.

3.2.1 Backup-Schema mit mehreren Dateien (Legacy-Modus)

Mit diesem Schema werden die Daten bei jedem Backup in einer separaten Archivdatei gespeichert (Dateiendung .tib). Bei erstmaliger Ausführung wird ein Voll-Backup erstellt. Die weiteren Backups werden gemäß der inkrementellen Methode ausgeführt.

Definieren Sie Aufbewahrungsregeln für die Backups und spezifizieren Sie die entsprechenden Einstellungen. Die veralteten Backups, d.h. Backups, die älter sind als die (in den Aufbewahrungsregeln) definierte Anzahl von Tagen, werden dynamisch entsprechend folgender Vorgehensweise gelöscht:

Beachten Sie, dass es nicht möglich ist, ein Backup zu löschen, wenn Abhängigkeiten bestehen. Wenn Sie zum Beispiel ein Voll-Backup und einen Satz inkrementelle Backups haben, können Sie das Voll-Backup nicht löschen. Denn dann wäre es unmöglich, die inkrementellen Backups wiederherzustellen. Backups, die (gemäß den Aufbewahrungsregeln) zu löschen sind, werden erst

dann gelöscht, wenn alle abhängigen Backups ebenfalls gelöscht werden sollen. Diese Einschränkung lässt sich durch Verwendung des Backup-Modus 'Nur inkrementell' umgehen.

3.2.2 Backup-Schema mit einer einzelnen Datei (Modus 'Nur inkrementell')

Gewöhnlich werden alle Backups eine bestimmte Zeit lang aufbewahrt (Aufbewahrungszeit) oder eine Richtlinie gibt vor, dass nur die letzten X Backups in der Backup-Kette aufbewahrt werden sollen. Backup-Archive werden täglich, wöchentlich usw. verwaltet. Die wesentliche Einschränkung bei der Verwendung des Legacy-Modus für Backup-Archive ist, dass es nicht möglich ist, beliebige Backups aus der Backup-Kette zu löschen, da möglicherweise Abhängigkeiten von nachfolgenden Backups bestehen. Ein Backup-Archiv im Format 'Nur inkrementell' ist hier vorteilhaft.

Der Modus 'Nur inkrementell' verwendet ein Archivformat der neuen Generation, das mehrere Backups von verschiedenen virtuellen Maschinen enthalten kann. Nach dem ersten Voll-Backup werden alle späteren Backups in diesem Archiv im inkrementellen Modus gespeichert. Physikalisch gesehen befinden sich alle Daten in einer Datei, im Gegensatz zum Legacy-Archivformat, bei dem jedes Backup in einer separaten .tib-Datei gespeichert wird. Deshalb ermöglicht, im Gegensatz zu einem Archiv im Legacy-Modus, ein Archiv des Formats 'Nur inkrementell' das Löschen eines beliebigen Backups, auch wenn Abhängigkeiten bestehen.

Wenn ein bestimmtes Backup aufgrund der vordefinierten Aufbewahrungsregeln abläuft (z.B. 'Lösche Backups, die älter sind als 2 Tage'), dann markiert der Backup-Algorithmus die veralteten Backup-Blöcke als 'freie' Blöcke.

Die Blöcke in dem abgelaufenen Backup, bei denen Abhängigkeiten bestehen (und die zum Wiederherstellen späterer Backups erforderlich sind), werden nicht als 'frei' markiert, um die Archiv-Konsistenz zu wahren. Das Archiv soll für die Wiederherstellung eines Backups nur Daten enthalten, die nicht älter als zwei Tage sind (Aufbewahrungszeit). Das ist die Grundregel eines Archivs im Modus 'Nur inkrementell'. Alle anderen Daten im Archiv werden als zum Löschen vorgesehen, d.h. als 'freier' Speicherplatz markiert. Das erste Archiv belegt weiterhin den gleichen Speicherplatz, aber alle neueren Backups werden zunächst in die 'freien' Blöcke geschrieben; erst, wenn alle 'freien' Blöcke belegt sind, wächst die Gesamtgröße des Archivs.

Mit diesem Ansatz wird die Archivgröße auf ein Minimum begrenzt und übermäßiges Wachstum vermieden. Außerdem bedeutet die Implementierung dieses Backup-Schemas eine erhebliche Zeit- und Kostenersparnis bei der Verwaltung der Backups im Archiv, da die Markierung der 'freien' Blöcke fast sofort geschieht. Die Einschränkungen des Legacy-Modus treffen somit nicht auf Archive mit dem Modus 'Nur inkrementell' zu.

Die Gesamtgröße eines Archivs im Modus 'Nur inkrementell' umfasst die Größe sowohl der 'genutzten' als auch der 'freien' Blöcke. Ein Archiv im Modus 'Nur inkrementell' wächst gewöhnlich nicht uneingeschränkt, sondern bleibt immer innerhalb der Gesamtgröße der aufzubewahrenden Backups.

4 Installation von Acronis vmProtect 6.0

4.1 Voraussetzungen

4.1.1 Unterstützte Betriebssysteme

Acronis vmProtect unterstützt folgende Dateisysteme:

- Windows XP Professional SP3 (x86, x64).
- Windows Server 2003/2003 R2 – Standard-, Enterprise-, Small Business Server-Editionen (x86, x64)
- Windows Vista – alle Editionen (x86, x64)
- Windows 7 – alle 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

4.1.2 Systemanforderungen

Unter Windows installierte Komponenten:

Editionsname	Arbeitsspeicher (zusätzlich zu dem für Betriebssystem und laufende Anwendungen)	Erforderlicher Speicherplatz bei Installation oder Update	Durch Komponenten belegter Speicherplatz
vmProtect	80 MB	1 GB	500 MB

Zum Ausführen der einzelnen Tasks (Backup, Recovery, VM ausführen, Validieren usw.) benötigt der Agent ca. 100 MB Arbeitsspeicher. Acronis vmProtect kann bis zu fünf parallele Tasks (z.B. parallele Backup-Tasks) gleichzeitig ausführen. Werden mehr als fünf Tasks gleichzeitig ausgeführt, dann verarbeitet der Agent nur die ersten fünf Tasks; alle weiteren Tasks verbleiben mit dem Status 'wartend' in der Warteschlange.

Beachten Sie weiterhin, dass Acronis vmProtect 6.0 folgende TCP-Ports reserviert und immer nutzt: 111 (sunrpc), 9000 (WCS), 764 (nfs_server), 9876 (Remote Agent Service).

Im Folgenden sind die Umgebungen aufgelistet, die Acronis vmProtect 6.0 unterstützen:

- VMware vSphere (Virtual Infrastructure)
- Server-Typen: ESX und ESXi
- Versionen: 4.0, 4.1, 5.0.
- Editionen/Lizenzen
  - VMware vSphere Standard (Hot-Add wird NICHT unterstützt)
  - VMware vSphere Advanced
  - VMware vSphere Enterprise
  - VMware vSphere Enterprise Plus
  - VMware vSphere Essentials

- VMware vSphere Essentials Plus
- VMware vSphere Hypervisor (Free ESXi wird NICHT unterstützt).

Um den problemlosen Betrieb der Acronis vmProtect Web Console zu gewährleisten, sollte eine der folgenden Webbrowser-Versionen auf Ihrem Rechner installiert sein:

- Mozilla Firefox 3.6 oder höher
- Internet Explorer 7.0 oder höher
- Opera 10.0 oder höher
- Safari 5.0 oder höher
- Google Chrome 10,0 oder höher

4.1.3 So installieren Sie die VMware-Tools

Acronis vmProtect erfordert die Installation von VMware-Tools. So installieren Sie die VMware Tools:

- Führen Sie den VMware Infrastructure/vSphere Client aus.
- Stellen Sie eine Verbindung zum ESX-Server her.
- Wählen Sie die virtuelle Maschine und starten Sie das Gastbetriebssystem.
- Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie Gast –> VMware Tools installieren/aktualisieren.
- Folgen Sie den Bildschirmanweisungen.

Für die Funktion **VM von Backup ausführen** muss ein VMkernel-Netzwerk auf dem ESX-Server konfiguriert werden. Dazu gehen Sie im vSphere Client über **Konfiguration**->**Netzwerk** und fügen den VMkernel-Verbindungstyp zu den vSwitch-Eigenschaften hinzu.

4.2 Installationsoptionen

Zuerst müssen Sie die Acronis vmProtect-Software installieren, die Verbindung mit dem ESX(i)-Host konfigurieren und die Anmeldedaten für die Acronis vmProtect-Webkonsole einrichten.

Beim Start des Acronis vmProtect Installationspaketes erscheint das Installationsmenü. Acronis vmProtect bietet drei grundsätzliche Installationsoptionen an:

- **Acronis vmProtect 6.0 als virtuelle Appliance auf einem ESX(i)-Host installieren**
- **Acronis vmProtect 6.0 als Windows Agenten installieren**
- **Installationsdateien extrahieren**

Die ersten beiden Optionen erlauben Ihnen das Installieren der Software auf einem Remote-ESX(i)-Host (siehe Acronis vmProtect 6.0 als virtuelle Appliance auf einem ESX(i)-Host installieren (S. 11)) oder auf Ihrem lokalen PC (siehe Acronis vmProtect 6.0 als Windows Agenten installieren (S. 12)). Mit der dritten Option können Sie die Installationsdateien extrahieren (siehe Installationsdateien extrahieren (S. 14)) und Acronis vmProtect entweder remote bereitstellen oder manuell mit Hilfe von Standard-Installationswerkzeugen lokal installieren.

Bei einer vollständig virtualisierten Infrastruktur ist das Deployment der Acronis vmProtect Virtual Appliance auf einem ESX-Host vorzuziehen.

Wenn ein physikalischer Rechner als Konsole für die Verwaltung aller Funktionen von vmProtect zur Verfügung steht, ist die Installation des Acronis vmProtect Windows Agenten auf einem lokalen Rechner die beste Wahl.

Wenn Sie die Installation des Windows Agenten bzw. der virtuellen Appliance nicht mit dem Standard-Installationsprogramm vornehmen, Fehler beheben müssen oder nur eine bestimmte Komponente installieren wollen, ohne die gesamte Installationsprozedur auszuführen, können Sie sich auch für die Extraktion der Installationsdateien entscheiden.

4.2.1 Acronis vmProtect 6.0 als virtuelle Appliance auf einem ESX(i)-Host installieren

Sie können die Acronis vmProtect-Software auch direkt auf einem ESX(i)-Host installieren. Dieser Prozess einer Remote-Installation der Acronis vmProtect Virtual Appliance auf einem ESX(i)-Host wird als Deployment bezeichnet. Die Software zum Ausführen aller erforderlichen Acronis-Dienste wird auf einer separaten kleinen virtuellen Maschine unter einem speziell angepassten Betriebssystem (kleine Linux-Distribution) installiert.

1. Lesen Sie zunächst die Lizenzvereinbarung für Acronis vmProtect, markieren Sie das Kontrollkästchen um sie anzunehmen und klicken Sie dann auf **Weiter**.
2. Spezifizieren Sie die Anmeldedaten für den gewünschten ESX(i)-Server oder das vCenter: IP-Adresse oder Host-Name, Benutzername und Kennwort. Wenn Sie auf **Weiter** klicken, überprüft das Installationsprogramm automatisch die Verbindung und testet die Anmeldung.
3. Dann überprüft das Installationsprogramm, ob frühere Versionen von Acronis vmProtect oder eine andere Acronis-Software auf dem angegebenen ESX(i)-Server installiert sind. Wenn dort bereits eine veraltete Version der Acronis Virtual Appliance installiert ist, fordert das Installationsprogramm zu einem Update auf die neueste Version oder zum Erstellen einer neuen Virtual Appliance auf.
4. Geben Sie einen Appliance-Namen (VM) an und wählen Sie ESX(i)-Host und Datenspeicher als Ziel für das Deployment der Acronis vmProtect-Software. Den Standardnamen der Appliance können Sie entweder beibehalten oder ändern. Der Appliance-Name muss innerhalb des ESX(i)-Hosts eindeutig sein. Wenn Sie in einem vorangehenden Installationsschritt das vCenter einschließlich der Anmeldedaten angegeben haben, müssen Sie nun in dem entsprechenden Listenfeld einen ESX(i)-Host in diesem vCenter auswählen. Anderenfalls ist keine Auswahl möglich und es wird Ihr ESX(i)-Host direkt angezeigt.

   Wählen Sie nun einen Datenspeicher auf dem gewählten ESX(i)-Host. Ist nicht genügend Speicherplatz für die Installation auf dem Datenspeicher vorhanden, erfolgt eine Warnmeldung sowie die Empfehlung, Speicherplatz auf dem gewählten Datenspeicher freizugeben oder einen anderen Datenspeicher zu wählen. Es darf auf dem spezifizierten Datenspeicher nur eine einzige virtuelle Appliance mit dem spezifizierten Namen geben. Wenn der Appliance-Name dort bereits vorhanden ist, müssen Sie entweder den Appliance-Namen ändern oder einen anderen Datenspeicher wählen.
5. Geben Sie die Netzwerkeinstellungen für die virtuelle Appliance an. In diesem Schritt werden die Standardnetzwerkeinstellungen wie IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Servereinstellungen usw. angegeben. Standardmäßig ermittelt die Appliance die Netzwerkeinstellungen automatisch.
6. Im nächsten Schritt entscheiden Sie, ob Sie am Acronis Programm zur Kundenzufriedenheit (CEP) teilnehmen wollen oder nicht.
7. Nach dem Ausführen aller erforderlichen Schritte des Installationsassistenten wird eine Zusammenfassung der auszuführenden Deployment-Aktionen angezeigt – zu installierende Komponenten, erforderlicher Speicherplatz, Kontoinformationen und ausgewähltes Ziel (Host und Datenspeicher).

   Dann beginnt das Acronis vmProtect-Installationsprogramm mit dem Deployment der virtuellen Appliance. Im Fortschrittsbalken wird der jeweilige Installationsschritt angezeigt. Nach

erfolgreichem Abschluss des Deployments startet die Appliance automatisch. Warten Sie, bis der gesamte Prozess abgeschlossen und alles überprüft worden ist. Dies kann mehrere Minuten dauern.

Wenn die Installationsprozedur erfolgreich abgeschlossen ist und alle Acronis vmProtect-Komponenten erfolgreich bereitgestellt wurden, wird die Seite 'Deployment wurde erfolgreich abgeschlossen' angezeigt. Markieren Sie hier das Kontrollkästchen, um die Acronis vmProtect-Webkonsole (im Standardbrowser) auszuführen und eine Verbindung zur neu bereitgestellten Acronis vmProtect Virtual Appliance herzustellen. Klicken Sie auf **Schließen**. Standardmäßig sind Login:Kennwort für die Acronis vmProtect-Webkonsole **root:root**.

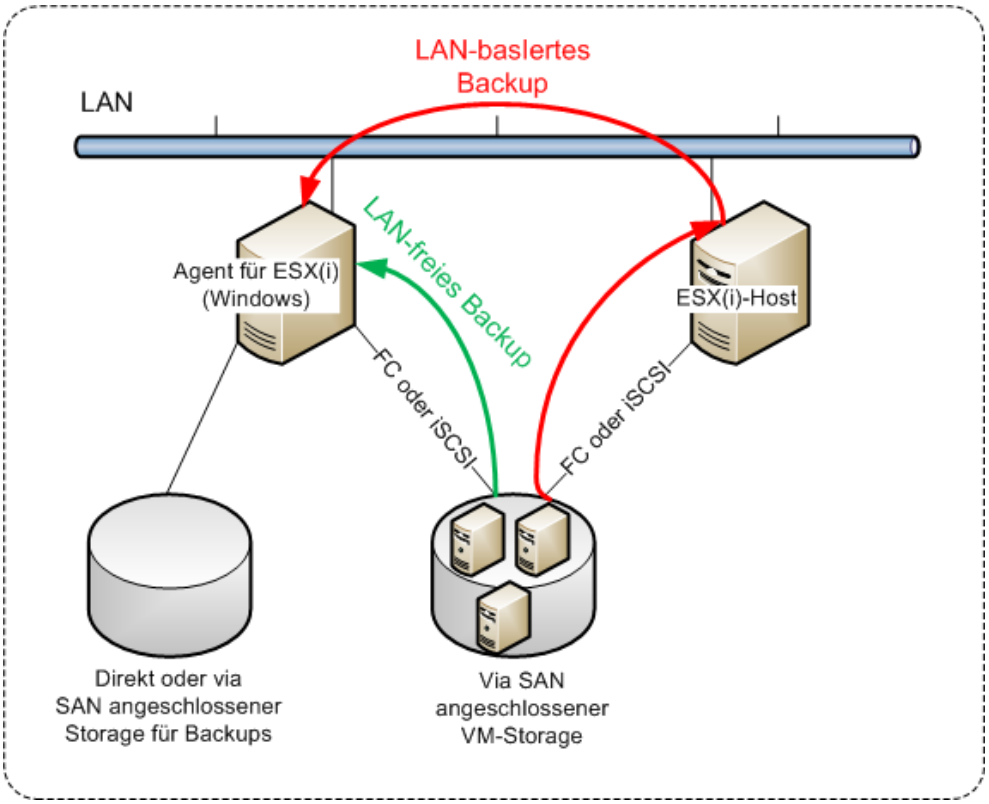
Bei Auftreten eines Problems wird die virtuelle Appliance (bzw. die Teile, die bereits während der Installation bereitgestellt wurden) automatisch vom ESX(i) entfernt. Die Seite **Installation der vmProtect-Komponenten fehlgeschlagen** wird angezeigt. Hier wird eine Zusammenfassung der installierten und nicht installierten Komponenten angezeigt. Der Link **Log anzeigen** öffnet ein Fenster mit detaillierten Informationen, der Link **Fehlersuche** öffnet die Webseite mit der Beschreibung des aufgetretenen Fehlers in der Acronis Knowledge Base auf http://kb.acronis.com. Falls Sie hier keine Lösung für das Problem finden, kontaktieren Sie den Acronis Support (S. 85).

4.2.2 Acronis vmProtect 6.0 als Windows Agenten installieren

Falls Ihre produktiven ESX(i)-Hosts so stark ausgelastet sind, dass eine Ausführung der virtuellen Appliances nicht wünschenswert ist, dann sollten Sie die Installation des Acronis vmProtect Windows Agenten auf einer physikalischen Maschine außerhalb der ESX(i)-Infrastruktur erwägen.

Falls Ihr ESX(i) einen per SAN angeschlossenen Storage verwendet, dann installieren Sie den Agenten auf einer Maschine, die an dasselbe SAN angeschlossen ist. Der Agent führt das Backup der virtuellen Maschinen dann direkt vom Storage aus, statt über den ESX(i)-Host und das LAN. Diese Fähigkeit wird auch als 'LAN-freies Backup' bezeichnet.

Das nachfolgende Diagramm illustriert LAN-basierte und LAN-freie Backups. Ein LAN-freier Zugriff auf virtuelle Maschinen ist verfügbar, falls Sie ein per Fibre Channel (FC) oder iSCSI angebundenes Storage Area Network haben. Um die Übertragung von Backup-Daten via LAN komplett ausschließen zu können, müssen Sie die Backups auf einem lokalen Laufwerk der Agenten-Maschine oder auf einem per SAN angebundenen Storage speichern.



Der Acronis vmProtect Windows Agent kann auf jeder Maschine installiert werden, die unter Windows läuft und die Systemanforderungen erfüllt. Es folgt eine Kurzbeschreibung der Schritte, die für die vollständige Installation des Windows Agent erforderlich sind.

1. Lesen Sie zunächst die Lizenzvereinbarung für Acronis vmProtect, markieren Sie das Kontrollkästchen um sie anzunehmen und klicken Sie dann auf **Weiter**.
2. Spezifizieren Sie Anmeldedaten für die Acronis-Dienste. Die Komponente Acronis Managed Machine Service (die für die Kernfunktionalität von Acronis vmProtect verantwortlich ist) wird als Dienst ausgeführt. Spezifizieren Sie das Konto, unter dem der Dienst der Komponente nach der Installation ausgeführt wird (dieses Konto erhält automatisch auf der Maschine die Berechtigungen 'Anmelden als Dienst'). Hier können Sie die Anmeldedaten eines beliebigen Windows-Benutzers mit den Zugriffsrechten **'Lokal anmelden'** auf der Maschine, auf der der Agent installiert ist, eingeben. Dies kann ein beliebiges Benutzerkonto sein, z.B. aus der Gruppe **Administratoren**, **Hauptbenutzer** oder **Benutzer**. Tragen Sie den HTTPS-Port ein, z.B. den Standard-Port 9877. Um nach Installation des Acronis vmProtect Agenten mit der Acronis-Webkonsole zu arbeiten, öffnen Sie Ihren Webbrowser und geben Sie die Adresse 'https://Server:Port' in die Adresszeile ein.

   Beachten Sie, dass der Name Ihres lokalen Rechners, auf dem Acronis vmProtect installiert ist, keinen Unterstrich (_) enthalten darf, damit die Verbindung zum installierten Agenten über den Browser (Webkonsole) funktioniert. Geben Sie die Anmeldedaten eines Benutzers mit administrativen Berechtigungen auf der Maschine an.
3. Wählen Sie einen Installationspfad für die Komponenten, d.h., geben Sie einen Zielort für die Installation der Software an. Standardmäßig wird Acronis vmProtect im Zielordner

C:\Programme\Acronis installiert. Sie können auch einen anderen Zielordner angeben, indem Sie einen neuen Ordnernamen eingeben oder einen vorhandenen Ordner auswählen. Wenn der Ordner nicht existiert, wird er automatisch bei der Installation erstellt. Die Schaltfläche **Speicherplatznutzung** gibt an, wie viel Speicherplatz auf den verschiedenen Volumes des Rechners verfügbar ist und unterstützt Sie bei der Auswahl eines Ziellaufwerks für die Installation. Wenn auf dem ausgewählten Volume nicht ausreichend Speicherplatz verfügbar ist, werden Sie dazu aufgefordert, den erforderlichen Speicherplatz freizugeben oder ein anderes Volume zu wählen. Wählen Sie das gewünschte Ziel aus und klicken Sie auf **Weiter.**

4. Lesen Sie die Informationen über das Acronis Programm zur Kundenzufriedenheit (ACEP) und entscheiden Sie, ob Sie daran teilnehmen wollen; klicken Sie dann auf **Weiter**. Der Hauptzweck des ACEP besteht darin, Benutzerstatistiken zu sammeln, um so die Funktionalität unserer Software sowie den Support und die Kundenzufriedenheit zu verbessern.
5. Nach Abschluss aller erforderlichen Schritte des Installationsassistenten wird eine Zusammenfassung der auszuführenden Installationsaktionen angezeigt – zu installierende Komponenten, erforderlicher Speicherplatz, Kontoinformationen und ausgewähltes Ziel.
6. Klicken Sie auf **Installation**, um mit der Einrichtung zu beginnen. Der Fortschrittsbalken für die Installation von Acronis vmProtect wird angezeigt. Die Windows-Firewall kann Sie während der Installation auffordern, entsprechende TCP/IP-Ports freizugeben. Die Appliance benötigt dies, um korrekt zu arbeiten. Um die Verbindung zuzulassen, klicken Sie in der Dialogbox der Windows-Firewall auf die Schaltfläche **Nicht mehr blocken**. Warten Sie, bis die Installation beendet ist. Dies kann mehrere Minuten dauern.

Wenn die Installationsprozedur erfolgreich abgeschlossen ist und alle Acronis vmProtect-Komponenten erfolgreich installiert wurden, wird die Seite 'Installation wurde abgeschlossen' angezeigt. Aktivieren Sie, falls gewünscht, das Kontrollkästchen, um die Acronis vmProtect-Webkonsole auszuführen und klicken Sie auf **Schließen**.

Wenn die Installationsprozedur fehlschlägt und alle oder einige Acronis vmProtect-Komponenten aus irgendeinem Grund nicht installiert werden konnten, wird die Seite 'Installation der vmProtect-Komponenten fehlgeschlagen' angezeigt. Es wird eine Zusammenfassung der installierten und nicht installierten Komponenten angezeigt. Der Link **Log anzeigen** öffnet ein Fenster mit detaillierten Informationen, der Link **Fehlersuche** öffnet eine Webseite mit der Beschreibung des aufgetretenen Fehlers in der Acronis Knowledge Base auf http://kb.acronis.com. Wenn Sie trotzdem keine Lösung für das Problem finden, nehmen Sie Kontakt mit dem Acronis Support (S. 85) auf.

4.2.3 Installationsdateien extrahieren

Das Acronis vmProtect-Installationspaket bietet Ihnen die Möglichkeit, die Installationsdateien auf Ihren Rechner zu extrahieren, um sie dann manuell auszuführen und mit Hilfe von Standardwerkzeugen zu installieren.

Klicken Sie im Hauptmenü für die Acronis vmProtect-Installation auf den Eintrag **Installationsdateien extrahieren**. Wählen Sie die Komponenten aus, die als separate Installationsdateien auf dem PC gespeichert werden sollen:

- Acronis vmProtect.msi – die Hauptinstallationsdatei für den Acronis vmProtect Windows Agenten
- AcronisESXAppliance.ovf und zwei .vmdk-Dateien – Installationsdateien für die Acronis vmProtect Virtual Appliance

Spezifizieren Sie das Ziel, an dem die Dateien extrahiert werden sollen und klicken Sie dann auf **Extrahieren**. Die Schaltfläche **Speicherplatznutzung** gibt an, wie viel Speicherplatz auf den

verschiedenen Volumes des Rechners verfügbar ist und unterstützt Sie bei der Auswahl eines Ziellaufwerks für die Extraktion der Dateien.

Schließen Sie das Dialogfenster, wenn das Extrahieren vollständig abgeschlossen wurde.

4.2.4 Konfiguration der Einstellungen für die Verbindung mit dem ESX(i)-Host

Detaillierte Informationen über das Einrichten und die Konfiguration der Anmeldedaten für eine Verbindung mit dem ESX(i)-Host finden Sie im Abschnitt ESX-Hosts verwalten (S. 75).

4.2.5 Einen lokal angeschlossenen Storage verwenden

Sie können an einen Agenten für ESX(i) (Virtuelle Appliance) ein zusätzliches Laufwerk anschließen, so dass der Agent seine Backups zu diesem lokal angeschlossenen Storage durchführen kann. Solche Backups sind normalerweise schneller als Backups über das LAN und verbrauchen auch keine Netzwerkbandbreite. Wir empfehlen die Verwendung dieser Methode, wenn eine einzelne virtuelle Appliance die komplette virtuelle Umgebung verwaltet, die auf einem per SAN angeschlossenen Storage liegt.

Sie können den Storage zu einem bereits arbeitenden Agenten hinzufügen oder wenn Sie einen Import des Agenten von einer OVF-Vorlage durchführen.

So schließen Sie einen Storage an einen bereits arbeitenden Agenten an

1. Klicken Sie in der VMware vSphere-Bestandsliste (Inventory) mit der rechten Maustaste auf den Agenten für ESX(i) (Virtuelle Appliance).
2. Fügen Sie das Laufwerk hinzu, indem Sie die Einstellungen der virtuellen Maschine bearbeiten. Die Laufwerksgröße muss mindestens 10 GB betragen.

   Seien Sie vorsichtig, wenn Sie ein bereits existierendes Laufwerk hinzufügen. Sobald der Storage erstellt wird, gehen alle zuvor auf dem Laufwerk enthaltenen Daten verloren.
3. Gehen Sie zur Konsole der virtuellen Appliance. Der Link **Storage erstellen** ist im unteren Bereich der Anzeige verfügbar. Wenn nicht, klicken Sie auf **Aktualisieren**.
4. Klicken Sie auf den Link **Storage erstellen**, wählen Sie das Laufwerk und spezifizieren Sie eine Bezeichnung für dieses.

Details: Die Länge der Bezeichnung ist aufgrund von Dateisystembeschränkungen auf 16 Zeichen limitiert.

So wählen Sie einen lokal angeschlossen Storage als Backup-Ziel

Erweitern Sie bei Erstellung eines Backup-Tasks im Dialog **Backup-Ziel–>Durchsuchen** das Element **Lokale Ordner** und wählen Sie das lokal angeschlossene Laufwerk aus, z.B. D:\.

Dieselbe Vorgehensweise gilt für 'Datei-Recovery' und andere Backup-Aktionen.

4.3 Deinstallation von Acronis vmProtect 6.0

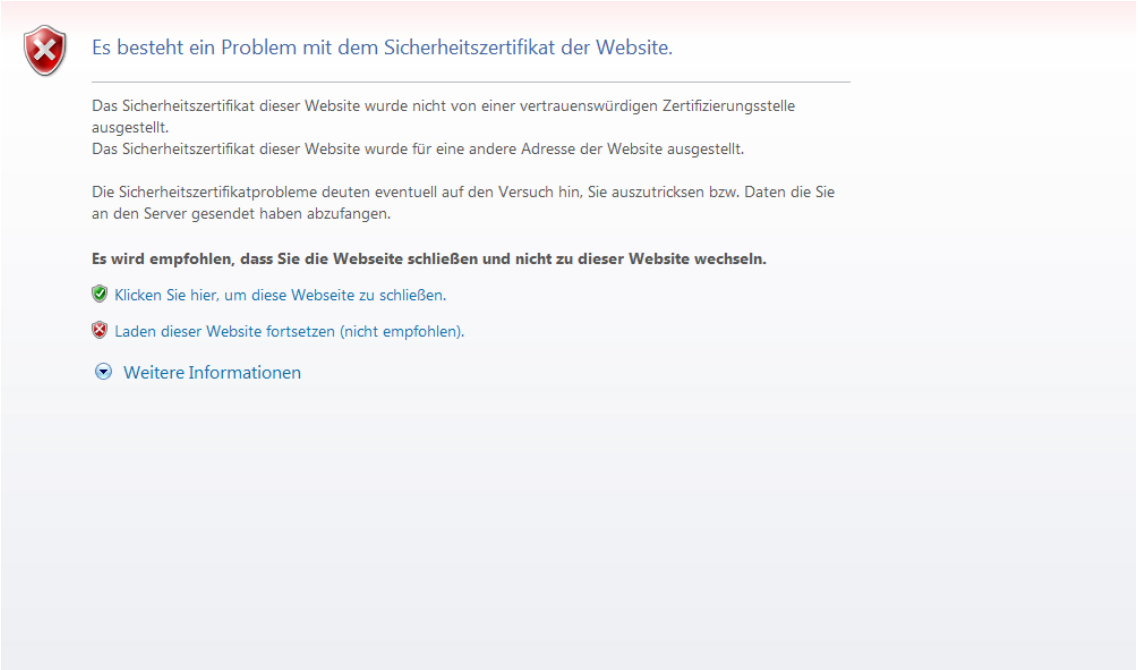
Um den Acronis vmProtect Windows Agenten zu deinstallieren, verwenden Sie das Standardtool von Windows **Programme hinzufügen oder entfernen**.

Um die Acronis vmProtect Virtual Appliance zu deinstallieren, müssen Sie mit Hilfe des VMware vSphere Client die VM mit der virtuellen Appliance manuell vom ESX-Host entfernen.

5 Erste Schritte

Sobald Sie Acronis vmProtect installiert haben bzw. die Acronis vmProtect Virtual Appliance bereitgestellt ist, können Sie die Acronis vmProtect-Webkonsole ausführen. Die Webkonsole öffnet sich im Standard-Webbrowser.

Beachten Sie, dass der (agentenseitig installierte) Acronis vmProtect-Webserver, der die Benutzeroberfläche darstellt, selbst-signierte Zertifikate verwendet. Wenn Sie über den Webbrowser eine Verbindung zum Acronis-Agenten herstellen, erscheint daher möglicherweise die Fehlermeldung 'Es besteht ein Problem mit dem Sicherheitszertifikat der Website'. Um diese Meldung zu unterdrücken, sollten Sie das selbst-signierte Zertifikat zur Liste der vertrauenswürdigen Zertifikate hinzufügen. Die genaue Vorgehensweise ist dabei abhängig von der Art des verwendeten Webbrowsers. Weitere Informationen finden Sie in der Hilfe für Ihren Browser.



Fehlermeldung zum Zertifikat

Wenn sich die Webkonsole im Webbrowser öffnet, wird zunächst ein Anmeldefenster angezeigt, in dem Sie die Anmeldedaten für Acronis vmProtect eintragen müssen. Bei einer Virtual Appliance-basierten Installation sind Login:Kennwort standardmäßig root:root. Bei einer Windows Agent-basierten Installation können Sie die Anmeldedaten eines beliebigen Windows-Benutzers eingeben, der **Administratorrechte** für die Maschine hat, auf der der Agent installiert ist. Der Benutzer sollte auch die Rechte **Lokal anmelden**, **Auf diesen Computer vom Netzwerk aus zugreifen** und **Anmelden als Stapelverarbeitungsauftrag** erhalten. Diese Rechte können über **Start** –> **Ausführen** –> secpol.msc –> **Sicherheitseinstellungen** –> **Lokale Richtlinien** –> **Benutzerrechte-Zuweisungen** überprüft werden.

Anmeldeseite

Nach der Anmeldung an Acronis vmProtect öffnet sich die Willkommensseite mit dem Bereich 'Schnellstart' im Dashboard. Die drei Schaltflächen in diesem Bereich geben einen Hinweis, womit Sie beginnen sollten:

- Damit Sie den ersten Backup-Task zur Sicherung virtueller Maschinen ausführen können, müssen Sie zunächst im ESX-Host-Bereich (S. 75) die IP-Adresse bzw. den Hostnamen und die Anmeldedaten für das vCenter oder einen eigenständigen ESX-Host spezifizieren, auf dem diese Maschinen laufen.
- Durch Einrichten eines ESX-Hosts werden Lizenzen noch nicht automatisch an diesen gebunden. Daher müssen Sie als nächstes die Lizenzen auf der Lizenzen-Seite (S. 71) einrichten.
- Nach dem Einrichten der ESX-Hosts und Lizenzen können Sie den Neuer Backup-Task-Assistenten (S. 22) ausführen, der Sie durch alle Schritte des Backup-Prozesses führen wird.

5.1 Dashboard-Verwaltung

Wenn Sie Acronis vmProtect installiert haben und starten (d.h. eine Verbindung zur Acronis vmProtect-Komponente über die Webkonsole herstellen), erscheint das Dashboard-Standardfenster. Zunächst ist das Dashboard in zwei Bereiche unterteilt: den Bereich **Schnellstart** und den Bereich **Virtuelle Maschinen**, der allgemeine Informationen über die vCenter, ESX(i)-Hosts, die Anzahl der auf den ESX(i)-Hosts verwalteten Maschinen und die Anzahl der gemounteten virtuellen Maschinen enthält. Die Ansicht **Dashboard** enthält zunächst den Bereich **Schnellstart**, ändert sich aber, wenn ein Backup-Task erstellt worden ist: Der Bereich **Schnellstart** verschwindet und die (unten beschriebenen) zusätzlichen Bereiche werden angezeigt.

Der Hauptarbeitsbereich des Acronis vmProtect-Dashboards gibt einen Überblick über alle aktuell laufenden Tasks bzw. Einzelheiten zu den zuletzt abgeschlossenen Tasks, wenn aktuell keine Tasks laufen. Das Dashboard bietet eine extrem benutzerfreundliche Umgebung für einen Überblick über den aktuellen Status der Backup- bzw. Recovery- Tasks sowie anderer Tasks. Für erfolgreiche und fehlgeschlagene Tasks werden verschiedene Farben verwendet. Da das Dashboard alle Aktionen anzeigt, die Ihnen mit Acronis vmProtect zur Verfügung stehen, ist es ein sehr nützliches Tool für schnelle operative Entscheidungen.

Zum Dashboard wechseln Sie, indem Sie auf das Acronis vmProtect Logo links oben klicken – oder auf die Schaltfläche **Startseite** im Hauptmenü. Außer den **Alarmmeldungen** lässt sich jede Gruppe im Dashboard über ihr eigenes Minimieren-Symbol in der Taskleiste verbergen.

Tasks

Der Bereich **Tasks** enthält eine Zusammenfassung der aktuell laufenden Tasks bzw. des zuletzt durchgeführten Tasks, wenn aktuell keine Tasks laufen. Der Fortschrittsbalken zeigt an, wie viel Prozent der Backup-/Recovery-Tasks abgeschlossen sind, den Task-Namen, die Anfangszeit, die verbleibende Zeit und die aktuelle Geschwindigkeit. Vom Block 'Tasks' im Dashboard aus können Sie direkt das Task-Log öffnen, einen Task anhalten, oder zur Seite **Tasks anzeigen** wechseln.

Virtuelle Maschinen

Der Bereich **Virtuelle Maschinen** zeigt die Namen der Hosts und Cluster (vCenter), die Gesamtanzahl der auf dem bzw. den verwalteten ESX(i)-Host(s) laufenden VMs sowie die Anzahl der gemounteten virtuellen Maschinen an (*siehe Abschnitt 'Gemountete VMs' (S. 66)).*

Statistiken

Der Bereich **Statistiken** enthält eine Zusammenfassung der Ausführung von Backup- bzw. Recovery-Tasks. Die Informationen werden in Form eines Diagramms angezeigt und lassen sich so visuell schnell erfassen und analysieren. Erfolgreich abgeschlossene Tasks sind grün markiert. Fehlgeschlagene Tasks sind rot markiert. Tasks, die mit Warnungen abgeschlossen wurden, sind gelb markiert. Wenn Sie mit der Maus auf ein Diagramm zeigen, können Sie sich die Prozentangaben für die Tasks und detaillierte Statistiken für ein bestimmtes Datum anzeigen lassen. Außerdem können Sie die Ansicht 'Statistiken' ändern, indem Sie auf **Stündlich**, **Täglich** oder **Wöchentlich** klicken.

Speicherorte

Der Bereich **Speicherorte** enthält die Gesamtstatistiken zum Status der Backup-Speicherorte. Er nennt die Gesamtzahl der Backups sowie Informationen zur Größe des belegten, anderweitig belegten und freien Speicherplatzes (in Megabytes/Gigabytes und in Prozent). Belegter Speicherplatz ist der durch Acronis Backups belegte Speicherplatz. Anderweitig belegter Speicherplatz ist der durch Daten, die keine Backup-Archive sind, belegte Speicherplatz. Die Statistik für freien Speicherplatz ist nur für Speicherorte verfügbar, die eine Abfrage dieses Wertes unterstützen (für FTP-Speicherorte ist dieses Feld beispielsweise nicht verfügbar). Vom Bereich **Speicherorte** aus können Sie über den unten platzierten Link direkt zur Ansicht **Recovery-Punkte** wechseln.

5.2 Die Webkonsole verwenden

5.2.1 Registerlaschen im Menüband

Über das Menüband oben im Bildschirm können Sie die Software verwalten und alle Bedienfunktionen ausführen. Die grundlegenden Acronis vmProtect-Funktionen, auf die über das obere Menü Zugriff besteht, sind in den folgenden Abschnitten beschrieben.

Das Acronis vmProtect-Menüband hat drei Hauptregisterlaschen: Die Registerlaschen **Aktionen**, **Ansicht** und **Konfigurieren**. Eine vierte Acronis-Registerlasche erscheint dynamisch, je nach der aktuell ausgewählten **Ansicht** oder Aktion zum **Konfigurieren**.

Ansicht 'Dashboard'

Die in der Menübandleiste immer verfügbare Schaltfläche **Startseite** führt zur Ansicht **Dashboard**. Die Konfiguration des Dashboards wird im Abschnitt Dashboard-Verwaltung (S. 17) beschrieben.

1) Registerlasche 'Aktionen'

Die erste Registerlasche, **Aktionen**, enthält die Basisfunktionen von Acronis vmProtect; von hier aus können Sie folgende Basis-Tasks starten:

a. Backup-Task

Über die Schaltfläche **Backup** starten Sie den Backup-Assistenten. Die Einstellungen für den Backup-Assistenten werden im Abschnitt 'Backups virtueller Maschinen erstellen' (S. 22) beschrieben.

b. Recovery-Task

Über die Schaltfläche **Recovery** starten Sie den Recovery-Assistenten. Die Einstellungen für den Recovery-Assistenten werden im Abschnitt 'Backup virtueller Maschinen wiederherstellen' (S. 34) beschrieben.

c. 'VM von Backup ausführen'-Task

Über die Schaltfläche **VM von Backup ausführen** starten Sie den Assistenten 'VM von Backup ausführen'. Die Einstellungen des Assistenten 'VM von Backup ausführen' sind im Abschnitt 'VM von Backup ausführen' (S. 46) beschrieben.

d. Datei-Recovery-Task

Über die Schaltfläche **Datei-Recovery** starten Sie den 'Datei-Recovery'-Assistenten. Die Einstellungen für den 'Datei-Recovery'-Assistenten werden im Abschnitt 'Datei-Recovery' (S. 42) beschrieben.

e. Validierungstask

Über die Schaltfläche **Validieren** starten Sie einen neuen Validierungstask. Der Backup-Validierungstask ist im Abschnitt 'Backup validieren' (S. 64) beschrieben.

2) Registerlasche 'Ansicht'

Die zweite Registerlasche, **Ansicht**, enthält die wichtigsten Datenansichten für Acronis vmProtect und ermöglicht eine schnelle Navigation sowie den Wechsel zwischen folgenden einfachen Basisansichten:

a. Ansicht 'Tasks'

Dieser Link öffnet die Ansicht **Tasks**. Die Task-Verwaltung wird im Abschnitt 'Tasks verwalten' (S. 52) beschrieben.

b. Ansicht 'Recovery-Punkte'

Dieser Link öffnet die Ansicht **Recovery-Punkte**. Die Verwaltung der Recovery-Punkte wird im Abschnitt 'Recovery-Punkte verwalten' (S. 57) beschrieben.

c. Ansicht 'Gemountete VMs'

Dieser Link öffnet die Ansicht **Gemountete VMs**. Die Verwaltung von gemounteten virtuellen Maschinen wird im Abschnitt 'Gemountete VMs verwalten' (S. 66) beschrieben.

d. Ansicht 'Logs anzeigen'

Dieser Link öffnet die Ansicht **Logs anzeigen**. Die Log-Verwaltung wird im Abschnitt 'Logs verwalten' (S. 68) beschrieben.

3) Registerlasche 'Konfigurieren'

Die dritte Registerlasche, 'Konfigurieren', enthält die wichtigsten Werkzeuge für die Konfiguration von Acronis vmProtect; hier können Sie die Standardeinstellungen für einfache Backup- bzw. Recovery-Aktionen und andere Einstellungen vornehmen.

a. ESX-Hosts

Dieser Link öffnet die Seite **ESX-Hosts**-Verwaltung. Die Verwaltung von ESX(i)-Hosts wird im Abschnitt 'ESX-Hosts verwalten' (S. 75) beschrieben.

b. Lizenzen

Dieser Link öffnet die Seite **Lizenzen** verwalten. Die Lizenzverwaltung wird im Abschnitt 'Lizenzen verwalten' (S. 71) beschrieben.

c. Einstellungen

Die Einstellungen für **Abonnement für Online Backup aktivieren** und **Online Backup-Proxy** sind über das Menüband verfügbar. Hier können Sie z.B. alle erforderlichen Einstellungen für die Internetverbindung über einen Proxy-Server vornehmen.

Die Registerlasche **Konfigurieren** enthält außerdem zwei Links zu den **Backup-Einstellungen** und den **Recovery-Einstellungen**. Eine detaillierte Beschreibung der Backup- bzw. Recovery-Einstellungen sowie weiterer Einstellungen finden Sie im Abschnitt 'Einstellungen verwalten' (S. 79).

Klicken Sie auf die Schaltfläche **Backup-Einstellungen** bzw. **Recovery-Einstellungen** um die Seite mit den Backup- bzw. Recovery-Einstellungen zu öffnen; hier können Sie die Standardeinstellungen für alle Backup- bzw. Recovery-Tasks vornehmen.

4) Dynamische Registerlasche von vmProtect

Diese dynamische Registerlasche erscheint im Menüband und ändert ihr Aussehen je nach der aktuell ausgewählten Aktion in der Registerlasche **Ansicht** bzw. **Konfigurieren**. Die dynamische Registerlasche enthält Schaltflächen, die speziell zu den aktuellen Aktionen der Registerlasche **Ansicht** oder **Konfigurieren** gehören.

a. Ansicht -> Tasks

Wenn die Ansicht **Tasks** ausgewählt ist, erscheint die Registerlasche **Tasks** im Menüband. Die Seite zur Verwaltung der **Tasks** wird im Abschnitt 'Tasks verwalten' (S. 52) beschrieben.

b. Ansicht -> Recovery-Punkte

Wenn die Ansicht **Recovery-Punkte** ausgewählt ist, erscheint die Registerlasche **Recovery-Punkte** im Menüband. Die Seite zur Verwaltung der **Recovery-Punkte** wird im Abschnitt 'Recovery-Punkte verwalten' (S. 57) beschrieben.

c. Ansicht -> Gemountete VMs

Wenn die Ansicht **Gemountete VMs** ausgewählt ist, erscheint die Registerlasche **Gemountete VMs** im Menüband. Die Seite **Gemountete VMs** wird im Abschnitt 'Gemountete VMs verwalten' (S. 66) beschrieben.

d. Ansicht -> Logs anzeigen

Wenn die Ansicht **Logs anzeigen** ausgewählt ist, erscheint die Registerlasche **Logs** im Menüband. Die Seite zur Verwaltung der **Logs** wird im Abschnitt 'Logs verwalten' (S. 68) beschrieben.

e. Konfigurieren -> Lizenzen

Haben Sie **Konfigurieren**->**Lizenzen** ausgewählt, erscheint die Registerlasche **Lizenzen** im Menüband. Die Seite zur Verwaltung der **Lizenzen** wird im Abschnitt 'Lizenzen verwalten' (S. 71) beschrieben.

f. Konfigurieren -> ESX(i)-Hosts

Haben Sie **Konfigurieren**->**ESX(i)-Hosts** ausgewählt, erscheint die Registerlasche **Hosts** im Menüband. Die Seite zur Verwaltung der **ESX(i)-Hosts** wird im Abschnitt 'ESX-Hosts verwalten' (S. 75) beschrieben.

5.2.2 Link 'Abmeldung'

In der rechten oberen Ecke von Acronis vmProtect werden der aktuelle Benutzername und die Schaltfläche **Abmeldung** angezeigt, mit der Sie das Programm verlassen oder sich unter einem anderen Benutzernamen anmelden können.

6 Backups von virtuellen Maschinen erstellen

Klicken Sie im **Schnellstart** des Dashboards auf **Backup-Task erstellen** oder klicken Sie in der Registerlasche **Aktionen** im Hauptmenü auf **Backup**, um einen neuen Backup-Task zu erstellen. Der Assistent **Neuer Backup-Task** öffnet sich im Hauptarbeitsbereich und fordert Sie auf, die erforderlichen Informationen anzugeben sowie alle für die Erstellung des neuen Backup-Tasks erforderlichen Einstellungen vorzunehmen. Der Assistent enthält vier aufeinander folgende Schritte, die im gleichen Bereich erscheinen:

- Backup-Quelle
- Backup-Ort
- Zeitpunkt des Backups
- Art des Backups

Nachfolgend werden diese vier Schritte des Assistenten und die möglichen Optionen beschrieben.

6.1 Backup-Quelle

Im ersten Schritt wählen Sie die zu sichernden virtuellen Maschinen (oder vApps) aus. Auf der linken Seite werden alle vom Acronis vmProtect-Agenten verwalteten ESX-Hosts/vCenters sowie eine Liste der virtuellen Maschinen angezeigt. Ist die zu sichernde virtuelle Maschine nicht in der Liste, stellen Sie sicher, dass Sie den entsprechenden ESX-Host auf der Seite **Konfigurieren**->**ESX-Hosts** hinzugefügt haben.

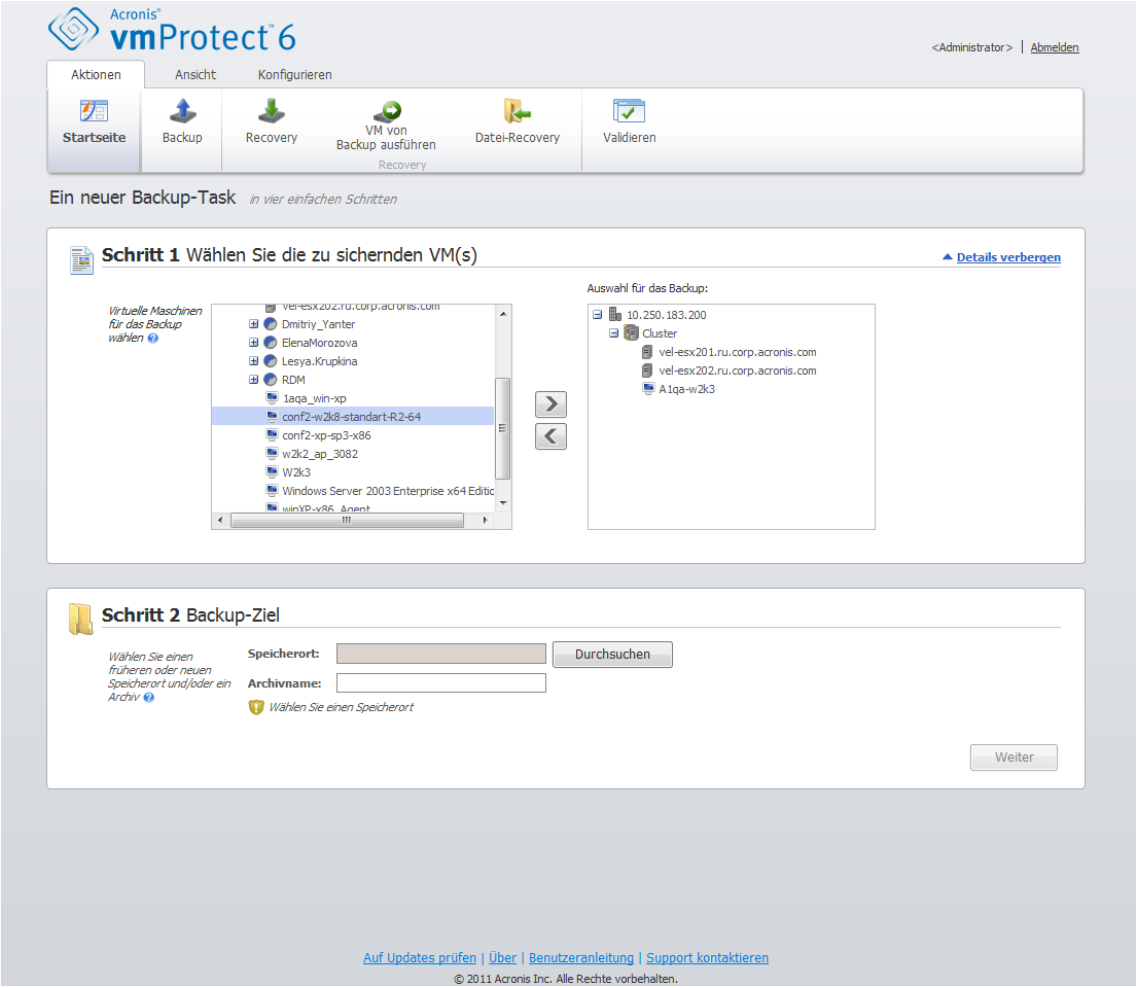
Die Auswahl der virtuellen Maschinen (oder vApps) erfolgt mit Hilfe der Schaltflächen **>** und **<** durch Verschieben von der linken Seite in die rechte. Die Liste auf der rechten Seite zeigt alle zum Backup ausgewählten virtuellen Maschinen. Mit der Schaltfläche **'>'** fügen Sie VMs zur Liste hinzu, mit der Schaltfläche **'<'** entfernen Sie die VMs aus der Liste.

Für das Backup dynamischer Maschinen-Gruppen wählen Sie im Baum die übergeordnete Einheit (z.B. den ESX-Host oder VMs-Ordner) und verschieben ihn mit derselben Schaltfläche **'>'** in die rechte Liste. So werden alle zu dieser Gruppe gehörenden Maschinen automatisch in die Backup-Liste aufgenommen. Maschinen, die in dieser Gruppe neu erstellt werden, werden automatisch durch den aktuellen Backup-Task mitgesichert.

Klicken Sie auf **Weiter**, wenn Sie die 'Backup-Quelle' ausgewählt haben, um **den ersten Schritt abzuschließen und fortzufahren.**

6.2 Backup-Ziel

Im zweiten Schritt bestimmen Sie einen Speicherort für das Backup-Archiv. Klicken Sie auf **Durchsuchen**, um einen Speicherort auszuwählen. Es öffnet sich ein Fenster mit den Optionen zum Durchsuchen, wo Sie den Pfad bestimmen oder ändern und einen Archivnamen festlegen können. Sie können entweder einen der zuvor verwendeten Speicherorte aus der Liste der letzten Speicherorte auswählen oder einen neuen Speicherort erstellen.



Assistent 'Backup erstellen', Schritt 2, 'Backup-Ziel'

Das Feld **Archivname** nennt den Namen des im Fenster **Durchsuchen** ausgewählten Archivs.

Die linke Seite des Fensters **Durchsuchen** zeigt folgende Listen:

- Online Backup-Storages
- Lokale Ordner
- Netzwerkordner
- FTP- und SFTP-Server
- Letzte Speicherorte

Wählen Sie einen Speicherort-Typ aus dem links liegenden Verzeichnisbaum. Falls der gewählte Speicherort (Online Backup-Storage, Netzwerkordner oder FTP- bzw. SFTP-Server) eine Authentifizierung erfordert, erscheint zunächst im rechten Bereich ein Dialogfenster zur Eingabe der Anmeldedaten. Nach dem Anmelden zeigt dieser Bereich den Inhalt des ausgewählten Speicherorts an, d.h. die hier vorhandenen Archive.

Beachten Sie, dass für ein erfolgreiches Backup auf einem FTP- bzw. SFTP-Server Löschrechte für die entsprechende Datei und den entsprechenden Ordner auf diesem Server erforderlich sind.

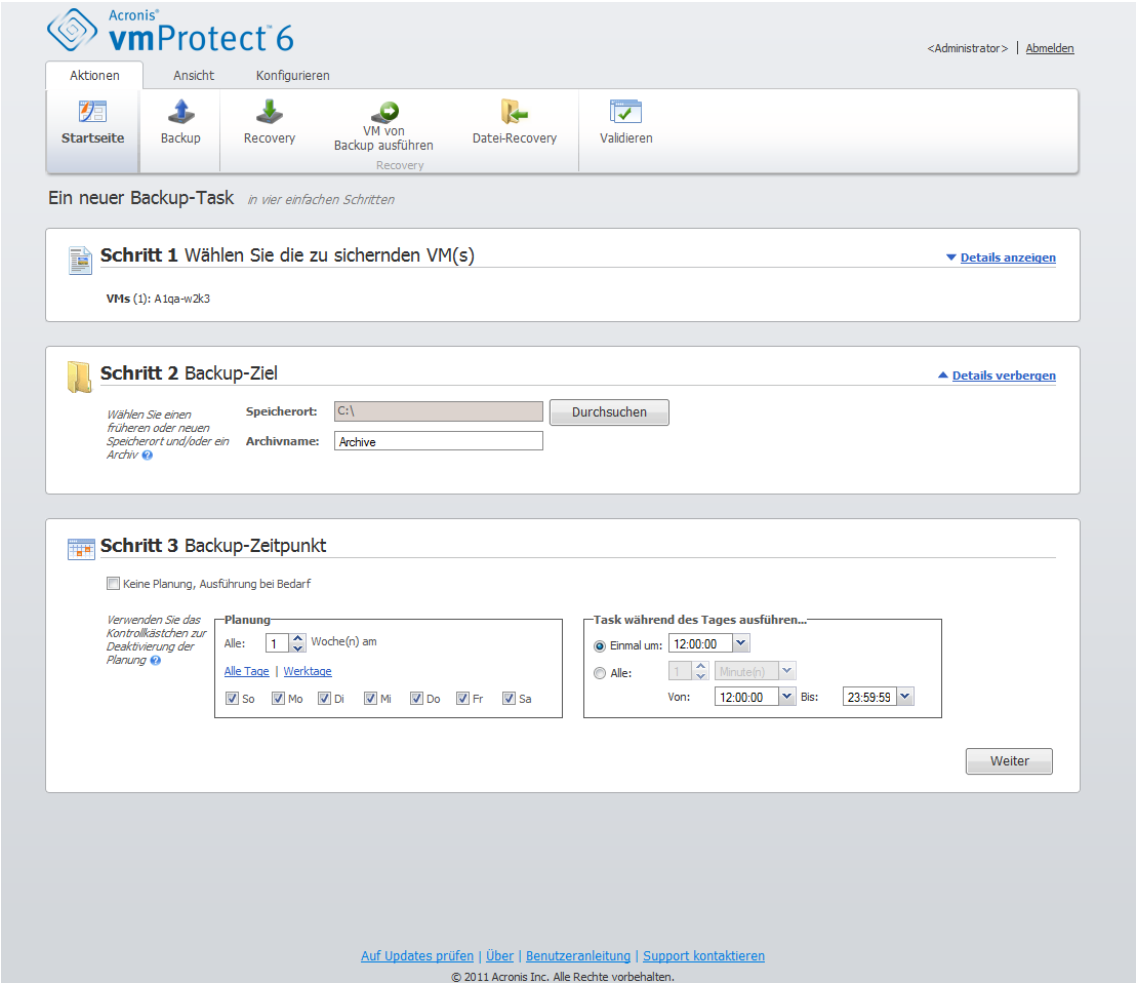
Alternativ zum Suchen des Speicherorts im Baum können Sie einen Pfad im entsprechenden Feld **Speicherort** unten eingeben und diesen Speicherort dann mit einem Klick auf **Go** durchsuchen. Auch hier erscheint im rechten Bereich dasselbe Dialogfenster, das zur Authentifizierung nach Login und Kennwort fragt.

Geben Sie im Feld **Archivname** den Archivnamen ein. Beachten Sie, dass es nicht empfehlenswert ist, mehrere Backup-Tasks Daten in dasselbe Archiv schreiben zu lassen. Die von verschiedenen Backup-Tasks auf das Archiv angewendeten Aufbewahrungsregeln können unvorhergesehene Folgen haben.

Klicken Sie auf **Weiter**, wenn Sie das 'Backup-Ziel' bestimmt haben, um den zweiten Schritt abzuschließen und mit dem dritten fortzufahren.

6.3 Backup-Zeitpunkt

Im dritten Schritt des Assistenten 'Backup-Task erstellen' legen Sie die Planung für die Datensicherung der virtuellen Maschinen fest. Es stehen Ihnen zwei Optionen zur Verfügung – die Planung regelmäßiger Backups oder das Erstellen eines einzelnen Backup-Tasks ('Keine Planung, Ausführung bei Bedarf'). Standardmäßig ist die Einstellung 'Keine Planung, Ausführung bei Bedarf' gewählt, womit der Backup-Task entweder direkt nach Fertigstellen aller Schritte des Assistenten startet oder später aus der Ansicht **Tasks** heraus ausgeführt werden kann.



Assistent 'Backup erstellen', Schritt 3, 'Backup-Zeitpunkt'

Deaktivieren Sie das Kontrollkästchen **Keine Planung, Ausführung bei Bedarf**, um eine Zeitplanung für die Datensicherung zu bestimmen. Acronis vmProtect ermöglicht für Windows- und Linux-Betriebssysteme eine wöchentliche Planung.

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt: Alle: <...> Woche (Wochen) am: <...>.
Spezifizieren Sie eine bestimmte Anzahl von Wochen und die Wochentage, an denen der Task

ausgeführt werden soll. 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: <...> oder Alle: <...> Von: <...> Bis: <...>.

Für den Befehl **Einmal: <...>** geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.

Für den Befehl **Alle: <...> Von: <...> Bis: <...>** geben Sie an, wie oft der Task während des angegebenen Zeitintervalls gestartet wird. Stellen Sie z.B. die Task-Planung auf 'Alle 1 Stunde' 'Von 10:00 Uhr bis 22:00 Uhr' ein, so läuft der Task an einem Tag zwischen 10:00 Uhr und 22:00 Uhr zwölf Mal.

Betrachten wir einige Planungsbeispiele.

'Ein Tag in der Woche'-Planung

Diese Backup-Planung wird häufig verwendet. Wenn der Backup-Task jeden Freitag um 22:00 Uhr laufen soll, müssen folgende Parameter gesetzt werden:

1. Alle: **1** Woche(n) am: **Fr**.
2. Einmal um: **22 Uhr**.

'Werktags'-Planung

Den Task jede Woche an Werktagen ausführen: von Montag bis Freitag. Während 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>**. Durch Auswahl von **Werktags** werden automatisch die korrespondierenden Kontrollkästchen (**Mo, Di, Mi, Do** und **Fr**) aktiviert, die anderen zwei bleiben jedoch unverändert.
2. Einmal um: **21:00 Uhr**.

Klicken Sie auf **Weiter**, wenn Sie die Backup-Planung abgeschlossen haben, um zum letzten Schritt im Assistenten zu gelangen.

6.4 Art des Backups

Im vierten Schritt legen Sie die Einstellungen des neuen Backup-Tasks fest.

6.4.1 Backup-Typ

Definieren Sie zunächst einen Archiv-Typ für das neue Backup. Acronis vmProtect kann Daten in zwei unterschiedlichen Archivtypen sichern – in einem Standard-Archiv (Legacy-Modus) oder einem Archiv im Modus 'Nur inkrementell'.

Den Archivtyp bestimmen Sie über die Option **Eine Datei für alle Backups**. Ist das Kontrollkästchen deaktiviert, dann wird jedes Backup in einer separaten Datei gespeichert. Das ist ein Archiv im Legacy-Modus (*Weitere Informationen finden Sie im Abschnitt 'Backup-Schema mit mehreren Dateien (Legacy-Modus)'* (S. 7)). Ist das Kontrollkästchen aktiviert (empfohlen), werden alle Backups physikalisch in eine Datei gespeichert. Das Archiv hat dann das neue, verbesserte Format 'Nur inkrementell' (*Weitere Informationen finden Sie im Abschnitt 'Backup-Schema mit einer Datei (Modus 'Nur inkrementell)'* (S. 8)).

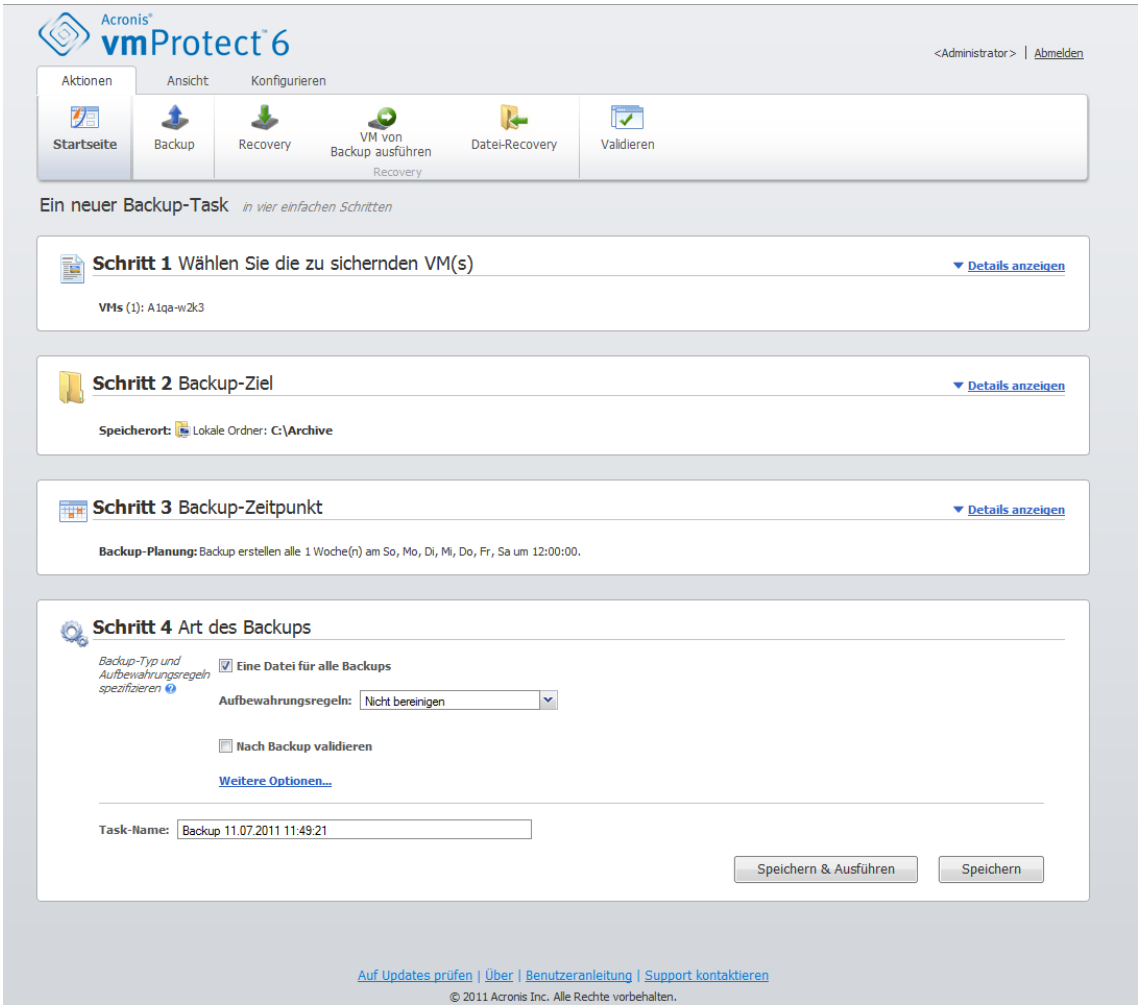
Wenn Sie einen vorhandenen Backup-Task bearbeiten oder ein vorhandenes Archiv als Backup-Speicherort auswählen, wird diese Option nicht angezeigt.

6.4.2 Aufbewahrungsregeln

Als nächstes müssen Sie die Aufbewahrungsregeln zur Verwaltung der Backups im Archiv festlegen. Welche Optionen verfügbar sind, hängt ab vom Setup der Planung im vorangehenden Schritt (*Abschnitt 'Backup-Zeitpunkt'* (S. 24)) und dem gewählten Archiv-Format (*Abschnitt 'Backup-Typ'* (S. 25)). So steht beispielsweise das Bereinigungsschema 'Großvater-Vater-Sohn' (GVS) für ungeplante Backup-Tasks nicht zur Verfügung. Die Auswahl 'Erstelle Voll-Backups alle: <...> ist für die Option 'Eine Datei für alle Backups' nicht verfügbar (da ein vollständiges Backup für das Archiv-Format 'Nur inkrementell' keinen Sinn macht). Nachfolgend finden Sie eine Beschreibung der einzelnen Aufbewahrungsregeln.

1. Nicht angegeben

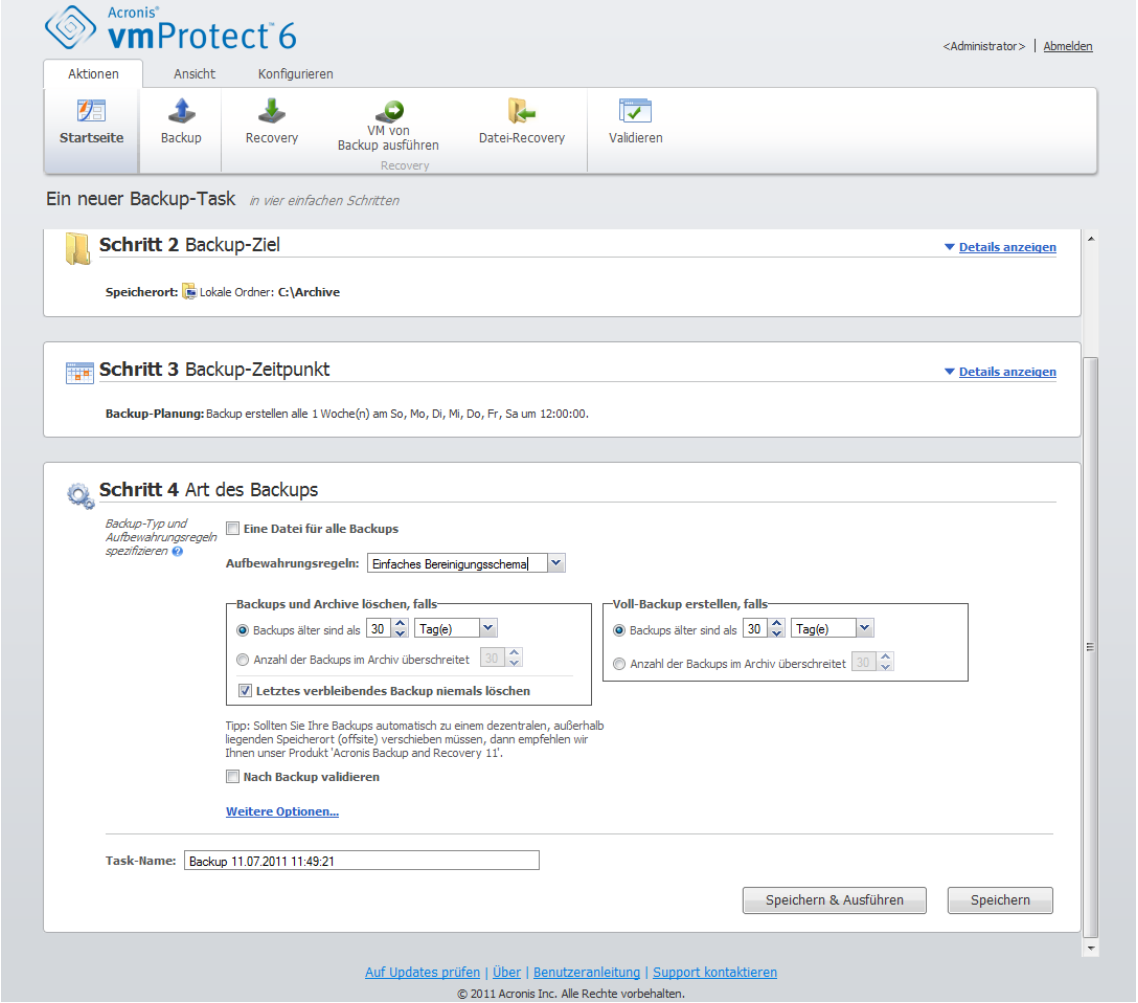
Wenn keine Aufbewahrungsregeln angegeben sind, erfolgt keine besondere Backup-Verwaltung, d.h. alle Backups werden unbegrenzt im Archiv gespeichert.



Assistent 'Backup erstellen', Schritt 4, Art des Backups, Aufbewahrungsregeln sind 'Nicht angegeben'

2. Einfaches Bereinigungsschema

Durch Auswahl des einfachen Bereinigungsschemas können Sie entweder eine bestimmte Anzahl von Backups im Archiv aufbewahren oder die Backups für einen bestimmten Zeitraum aufbewahren.

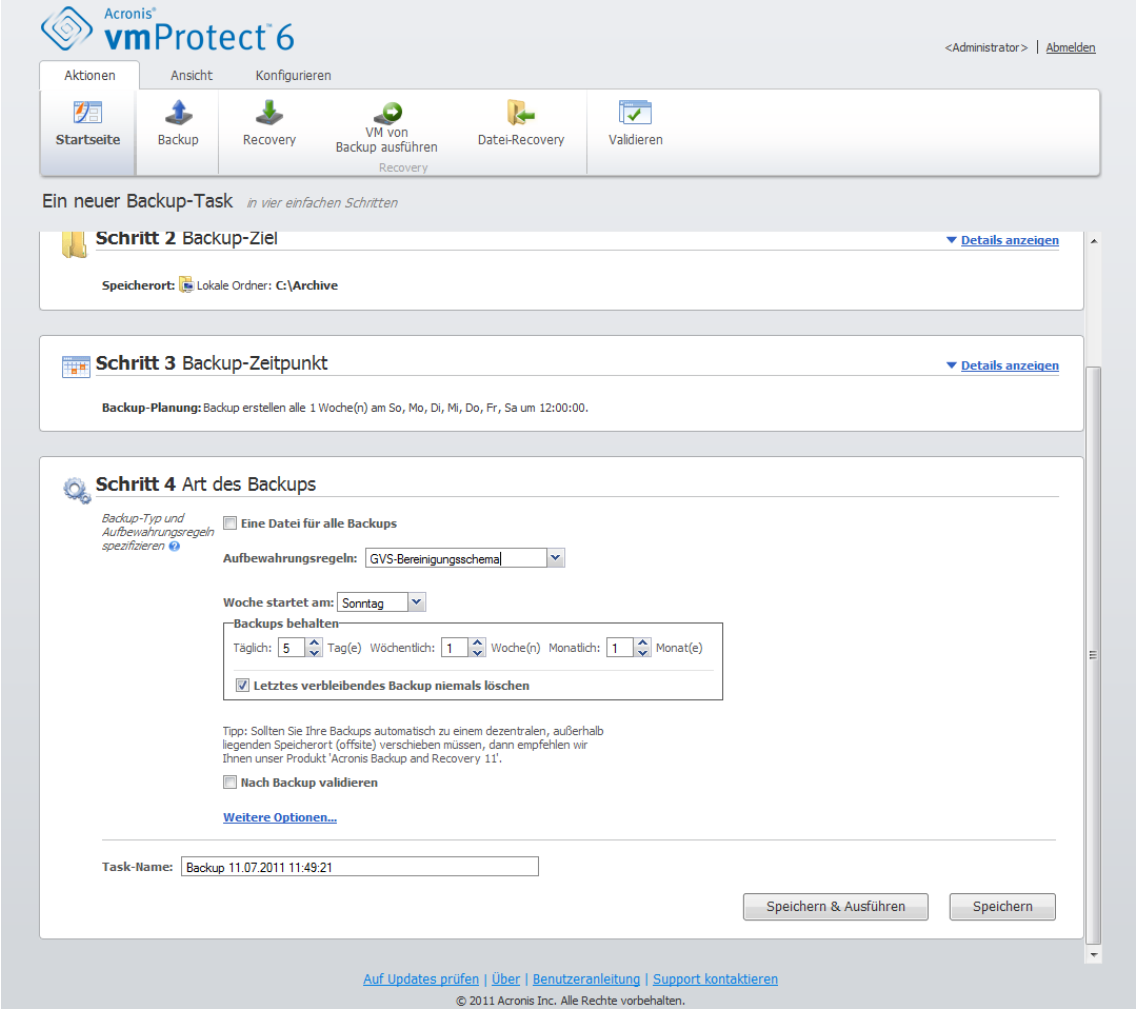


Assistent 'Backup erstellen', Schritt 4, Art des Backups, Einfaches Bereinigungsschema, 'Veraltete Backups löschen'

Mit der zweiten Option können Sie das Archiv bereinigen, wenn die Anzahl der Backups <...> überschreitet. Wenn Sie diesen Wert auf 1 setzen, wird im Archivmodus 'Nur inkrementell' ein synthetisches Voll-Backup erstellt, d.h. ein inkrementelles Backup, das nach seiner Fertigstellung unnötige alte Inhalte des Recovery-Punktes entfernt. Überschreitet die Anzahl der aufbewahrten Backups im Archiv 1, dann wird die Bereinigung entsprechend dem Archiv-Modus 'Nur inkrementell' ausgeführt (*Weitere Informationen finden Sie im Abschnitt 'Backup-Schema mit einer einzelnen Datei (Nur inkrementell)' (S. 8) in dieser Benutzeranleitung*).

3. GVS-Bereinigungsschema

Mit dem häufig verwendeten Bereinigungsschema 'Großvater-Vater-Sohn' können Sie eine bestimmte Anzahl von täglichen, wöchentlichen und monatlichen Backups aufbewahren. Geben Sie an, wie viele tägliche, wöchentliche und monatliche Backups aufbewahrt werden sollen. Alle über die Dauer eines Tages erstellten Backups gelten als 'tägliche' Backups und werden gelöscht, wenn dieses Datum abläuft. Die gleiche Regel gilt für 'wöchentliche' Backups.



Assistent 'Backup erstellen', Schritt 4, Art des Backups, 'GVS-Bereinigungsschema'

Beachten Sie, dass Aufbewahrungsregeln **nur vor** der Ausführung des Backup-Tasks angewendet werden. Der Grund hierfür ist, dass bei einem Archiv im Modus 'Nur inkrementell' nach dem Backup keine Recovery-Punkte entfernt werden müssen, da dadurch kein Speicherplatz frei wird. Überzählige Recovery-Punkte, die nach Ausführen eines Backups vorhanden und entsprechend den Aufbewahrungsregeln zu löschen sind, werden erst vor dem nächsten Backup gelöscht. Die Auswahl für die Aufbewahrungsregel **Backups und Archive löschen wenn** von **Backups sind älter als** 3 Tage oder **Anzahl der Backups im Archiv überschreitet** 3 speichert bis zu 4 Backups im Archiv und nicht 3.

Beachten Sie, dass im Archiv immer wenigstens **ein Backup** intakt bleibt, auch wenn dieses Backup aufgrund der spezifizierten Aufbewahrungsregeln gelöscht werden soll. So ist sichergestellt, dass Sie im Archiv jederzeit mindestens ein Backup zur Wiederherstellung verfügbar haben. Das hat solange Bestand, bis Sie das Kontrollkästchen **Nie das letzte verbliebene Backup löschen** (standardmäßig voreingestellt) deaktivieren; damit wird die Vorgehensweise des Programms festgelegt, wenn der letzte gültige Recovery-Punkt gelöscht werden soll. Das kann zum Beispiel passieren, wenn Sie auf eine Gruppe virtueller Maschinen einen Backup-Task anwenden und eine dieser Maschinen vom ESX-Host gelöscht wurde, also nicht mehr gesichert werden kann. An einem bestimmten Zeitpunkt sollen (gemäß den spezifizierten Aufbewahrungsregeln) auch alle Backups dieser gelöschten VM gelöscht werden. Dem aktivierten oder deaktivierten Kontrollkästchen der Option **Nie das letzte verbliebene Backup löschen** entsprechend wird das Löschen des letzten verbliebenen Backups also verhindert oder erzwungen.

6.4.3 Backup-Validierung

Aktivieren Sie das Kontrollkästchen **Backup nach Erstellung validieren**, um Backups nach der Erstellung auf Konsistenz zu überprüfen (Backup-Validierung – *weitere Informationen zur Backup-Validierung finden Sie im Abschnitt 'Backups validieren'* (S. 64)).

6.4.4 Andere Einstellungen

Klicken Sie auf **Weitere Optionen**, um das Fenster mit den zusätzlichen Einstellungen zu öffnen. Diese Optionen sind im Abschnitt 'Optionen' (S. 29) beschrieben.

6.4.5 Fertigstellen des Assistenten 'Backup-Task erstellen'

Um den Assistenten 'Neuer Backup-Task' abzuschließen, müssen Sie einen Namen für den Task vergeben. Beachten Sie, dass die Zeichen [ ] { } ; , . im Task-Namen nicht erlaubt sind.

Wenn Sie auf die Schaltfläche **Speichern** klicken, wird der Task mit den von Ihnen festgelegten Parametern gespeichert und erscheint in der Ansicht 'Tasks'. Das Klicken auf die Schaltfläche **Speichern und Ausführen** speichert den Task und führt ihn umgehend aus.

6.5 Optionen

Klicken Sie auf **Weitere Optionen** im letzten Schritt des Assistenten **Neuer Backup-Task**, um ein Fenster mit den Einstellungen zu öffnen. Wenn Sie keine Änderungen an den Einstellungen vornehmen, bleiben die Standardeinstellungen für den aktuellen Task bestehen. Wenn Einstellungen zu einem späteren Zeitpunkt geändert und als Standardeinstellungen gespeichert werden, wirkt sich dies nicht auf die mit den ursprünglichen Standardeinstellungen erstellten Tasks aus (diese behalten die zum Zeitpunkt der Erstellung gültigen Einstellungen bei).

Nachfolgend werden die einzelnen Einstellungen beschrieben.

6.5.1 Schutz des Archivs

Der Standardwert für den Parameter **Schutz des Archivs** ist 'Deaktiviert'. Diese Option ist nicht verfügbar, wenn bei Bearbeitung eines vorhandenen Tasks oder Erstellung eines neuen Tasks ein bereits vorhandenes Archiv angegeben wird.

Aktivieren Sie das Kontrollkästchen **Kennwort für das Archiv einrichten**, um das Archiv vor unbefugtem Zugriff zu schützen; tragen Sie dann ein Kennwort in das Feld **Kennwort eingeben** ein und noch einmal in das Feld **Kennwort bestätigen**. Das Kennwort unterscheidet Groß-/Kleinschreibung.

Das neu erstellte Archiv kann entweder nur mit einem Kennwort geschützt oder mit Hilfe des Advanced Encryption Standard-Verfahrens (AES) mit einer Tiefe von 128/192/256 Bit verschlüsselt werden. Wenn Sie **Nicht verschlüsseln** auswählen, wird das Archiv nur mit dem Kennwort geschützt. Wenn Sie die Verschlüsselung einsetzen möchten, wählen Sie eine der folgenden Stufen: AES 128, AES 192 oder AES 256.

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.

6.5.2 Ausschluss von Quelldateien

Mit den Regeln zum Ausschluss von Quelldateien bestimmen Sie, welche Quelldaten während des Backup-Prozesses übersprungen und so von der Liste der gesicherten Elemente ausgeschlossen werden. Dies können über den Pfad definierte Dateien oder Ordner sein, alle Systemdateien und alle versteckten Dateien, für die Ausschlusskriterien festgelegt werden können. Diese Einstellung ist nur bei Disk-Backups von virtuellen Maschinen mit NTFS- und FAT-Dateisystemen wirksam.

Bestimmen Sie mit Hilfe der folgenden Parameter, welche Dateien und Ordner ausgeschlossen werden sollen:

Dateien ausschließen, die folgende Kriterien erfüllen

Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner zu überspringen, die mit einem der Kriterien in der Liste übereinstimmen (sogenannte Dateimasken). Benutzen Sie die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Alle entfernen**, um die Liste der Dateimasken zu erstellen und verwalten.

Sie können in Dateimasken die Wildcards '*' und '?' benutzen.

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

Zum Beispiel können Sie den **Ausschluss von Quelldateien** definieren über den **Ausschluss von Dateien, die die folgenden Kriterien erfüllen**: *.tmp, *.~, *.bak

6.5.3 Komprimierungsgrad

Die Option **Komprimierungsgrad** definiert den Grad der Komprimierung für die zu sichernden Daten. Der Standardwert für diese Option 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 diese bereits stark komprimierte Dateien im Format .jpg, .pdf oder .mp3 enthält. Andere Formate, wie .doc- oder .xls, werden jedoch deutlich stärker komprimiert.

Wählen Sie einen der nachfolgenden Komprimierungsgrade:

- **Keine**. Die Daten werden so gesichert wie sie sind, ohne dabei komprimiert zu werden. Die resultierende Backup-Größe wird maximal sein.
- **Normal**. Dieser Komprimierungsgrad wird in den meisten Fällen empfohlen.
- **Hoch**. Die resultierende Backup-Größe wird üblicherweise kleiner sein als bei der Einstellung **Normal**.
- **Maximum**. Dies ist der höchste Grad der Datenkomprimierung. Allerdings wird für die Ausführung des Backup-Tasks auch die längste Zeit benötigt. Die maximale Komprimierung ist z.B. beim Backup auf Wechselmedien sinnvoll, um die Zahl der erforderlichen Datenträger zu verringern.

6.5.4 Fehlerbehandlung

Diese Optionen ermöglichen Ihnen vorzugeben, wie eventuell auftretende Fehler während einer Backup-Aktion behandelt werden.

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Der Task endet, sobald die Aktion erfolgreich war ODER die festgelegte Anzahl von Versuchen erreicht ist.

Wenn Sie das Kontrollkästchen **Bei Fehler neu versuchen** aktivieren, bestimmen Sie dazu die **Anzahl der Versuche** und das **Zeitintervall zwischen den Versuchen**. Standardmäßig ist diese Option mit folgenden Einstellungen aktiviert: **Anzahl der Versuche** – 5 und **Zeitintervall zwischen den Versuchen** – 30 Sekunden.

Wenn zum Beispiel mit den Standardeinstellungen das Backup-Ziel im Netzwerk nicht verfügbar oder erreichbar ist, versucht die Anwendung alle 30 Sekunden erneut, es zu erreichen, aber nur bis zu fünf Mal. Die Versuche werden aufgegeben, sobald die Verbindung gelingt oder die angegebene Zahl der Versuche erreicht ist.

6.5.5 Benachrichtigungen

1) E-Mail-Benachrichtigungen

Mit dieser Option richten Sie die E-Mail-Benachrichtigungen über wesentliche Ereignisse während eines Backups ein, z.B. über den erfolgreichen Abschluss, ein fehlgeschlagenes Backup oder einen erforderlichen Benutzereingriff. Standardmäßig ist diese Option deaktiviert.

Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung schicken**, um die entsprechende Funktion zu aktivieren.

Aktivieren Sie unter dem Kontrollkästchen **E-Mail-Benachrichtigungen schicken** die gewünschten Einstellungen folgendermaßen:

- **Wenn das Backup erfolgreich abgeschlossen wurde** – Eine Benachrichtigung wird versandt, wenn das Backup erfolgreich abgeschlossen wurde.
- **Wenn ein Backup fehlschlägt** – Die Benachrichtigung erfolgt, wenn das Erstellen des Backups nicht erfolgreich war.
- **Vollständiges Log zur Benachrichtigung hinzufügen** – Das vollständige Log wird mit der Benachrichtigung verschickt.

Geben Sie eine oder mehrere E-Mail-Adressen ein, an die die Benachrichtigungen geschickt werden. Die Adressen werden im Feld **E-Mail-Adressen** eingegeben, durch Semikolons getrennt.

Nennen Sie den für die Benachrichtigungen gewünschten **Betreff**.

SMTP-Server – Geben Sie den Namen des Postausgangsservers ein (SMTP-Server).

Port – Bestimmen Sie den Port des SMTP-Servers (der Standard-Port ist 25).

Benutzername – Geben Sie den Benutzernamen ein.

Kennwort – Geben Sie das Kennwort ein.

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 so erstellt, als stammten sie von der Zieladresse.

Verschlüsselung verwenden – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden und zwischen SSL- oder TLS-Verschlüsselung wählen.

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

2) SNMP-Benachrichtigungen

Diese Option definiert, ob der oder die Agenten auf der verwalteten Maschine das Ereignis-Log von Backup-Aktionen zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden. Standardeinstellung für diese Option ist: Deaktiviert**.**

Um auszuwählen, ob das Ereignis-Log der Backup-Aktion an Maschinen geschickt werden, auf denen SNMP-Verwaltungsanwendungen laufen, wählen Sie eine der folgenden Optionen:

- **Keine SNMP-Benachrichtigungen senden** – Der Versand des Ereignis-Logs von Backup-Aktionen an SNMP-Manager wird deaktiviert.
- **SNMP-Benachrichtigungen über Ereignisse bei Backup-Aktionen einzeln senden** – Das Ereignis-Log von Backup-Aktionen wird an spezifizierte SNMP-Manager geschickt.
  Ereignistypen, die geschickt werden – Wählen Sie die Ereignistypen, die übermittelt werden sollen. Informationen, Warnungen oder Fehler.
  Name oder IP des Servers – Geben Sie den Namen oder die IP-Adresse des Hosts ein, auf dem die SNMP-Verwaltungsanwendung läuft, die die Benachrichtigung bekommen soll.
  Community – Tragen Sie den Namen der SNMP-Community ein, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist **public**.
  Klicken Sie auf **Test-Mail senden**, um sicherzugehen, dass alle Einstellungen korrekt sind.

6.5.6 Erweiterte Einstellungen

1) Deduplizierung

Diese Option legt fest, ob Deduplizierung für das vom Backup-Task erstellte Archiv stattfindet oder nicht. Die Standardeinstellung für Deduplizierung ist: Aktiviert.

Deduplizierung erfolgt auf Archivebene. Es werden also nur die in diesem Archiv gespeicherten Daten dedupliziert. Mit anderen Worten, wenn es an einem Speicherort zwei Archive mit aktivierter Deduplizierung gibt, werden Daten, die möglicherweise in beiden Archiven vorhanden sind, nicht dedupliziert.

2) CBT-Backup

Diese Option legt fest, ob die Funktion Changed Block Tracking von VMware bei den virtuellen Maschinen, die sie unterstützen, verwendet werden soll. Die Standardeinstellung für CBT-Backup ist: Deaktiviert.

CBT überwacht alle Änderungen an Blöcken in der virtuellen Maschine. So wird die benötigte Zeit für das Erstellen von Backups erheblich reduziert. Die Zeit wird eingespart, weil Acronis vmProtect nicht überprüfen muss, welche Blöcke seit dem letzten Backup verändert wurden. Diese Information kommt von der VMware API.

3) FTP im Modus 'Aktiv' verwenden

Es ist möglich, FTP im Modus 'Aktiv' für FTP-Authentifizierung und Datentransfer zu verwenden. Die Standardeinstellung für 'FTP im Modus 'Aktiv' verwenden' ist: Deaktiviert.

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

Klicken Sie nach Festlegen der Einstellungen auf **OK**, um das Fenster zu schließen und sie nur auf den aktuellen Backup-Task anzuwenden.

6.6 Erstellten Backup-Task verwalten

Beim Bearbeiten eines existierenden Backup-Tasks sehen Sie alle Schritte des Backup-Assistenten, die Sie bei der Erstellung des Tasks abgeschlossen haben. Alle vier Schritte des Assistenten erscheinen gleichzeitig auf dem Bildschirm. Beachten Sie, dass Sie beim Bearbeiten eines existierenden Backup-Tasks nicht den Archivtyp (**Nur inkrementell** oder **Legacy-Modus**) modifizieren können. (*Weitere Informationen finden Sie in der Benutzeranleitung im Abschnitt 'Tasks verwalten'* (S. 52)).

7 Ein Backup virtueller Maschinen wiederherstellen

Klicken Sie in der Registerlasche **Aktionen** im Hauptmenü auf **Recovery**, um eine oder mehrere gesicherte virtuelle Maschinen wiederherzustellen. Der 'Backup-wiederherstellen'-Assistent öffnet sich im Hauptarbeitsbereich und fordert Sie auf, die für den Recovery-Task erforderlichen Informationen bereitzustellen und die notwendigen Einstellungen zu konfigurieren. Der Assistent besteht aus drei aufeinanderfolgenden Schritten, die im gleichen Bereich erscheinen:

- Recovery-Quelle
- Ort der Wiederherstellung
- Art der Wiederherstellung.

Nachfolgend werden diese drei Schritte des Recovery-Assistenten und deren Optionen beschrieben.

7.1 Recovery-Quelle

Im ersten Schritt des Assistenten 'Backup-wiederherstellen-Task' definieren Sie den Backup-Speicherort und wählen die wiederherzustellenden virtuellen Maschinen. Die ausgewählten Speicherorte werden nach Archiven und deren Inhalt durchsucht; das ist erforderlich, um den bzw. die Recovery-Punkte für die Wiederherstellung des Backups zu definieren.

Klicken Sie auf **Durchsuchen**, um einen Speicherort bzw. das Archiv zu wählen. Im erscheinenden Fenster mit den Optionen zum Durchsuchen definieren Sie den Pfad bzw. den Archivnamen. Hier finden Sie auch die zuvor verwendeten Speicherorte.

Es gibt zwei Wege, um Speicherorte im Browserfenster auszuwählen. Sie wählen zuerst einen Speicherort. In diesem Fall sehen Sie (unterhalb des gewählten Speicherorts) den gesamten Baum aller virtuellen Maschinen und deren dort vorhandenen Recovery-Punkte. Falls Sie anderenfalls einen Speicherort und ein Archiv wählen, sehen Sie nur den Inhalt des Archivs.

Beachten Sie: Wenn Sie ein Archiv mit dem Image einer physikalischen Maschine wählen (für die Migration von 'physikalischen zu virtuellen' Maschinen, P2V), stehen bei diesem Schritt keine weiteren Optionen zur Verfügung, weil solche Archive nur einen einzelnen Recovery-Punkt enthalten.

Falls sich am gewählten Speicherort irgendein durch Kennwort geschütztes Archiv oder Archive physikalischer Maschinen befinden, können die in diesen Archiven enthaltenen VMs nicht angezeigt werden und Sie erhalten eine Warnung. Um in diesem Fall Daten aus diesen Archiven wiederherzustellen, müssen Sie deren Namen direkt eingeben.

Sie können in der Liste auf der linken Seite eine beliebige virtuelle Maschine auswählen und auf die rechte Seite in den Bereich **Ausgewählte virtuelle Maschinen** verschieben. Die Auswahl der virtuellen Maschinen erfolgt mit Hilfe der Schaltflächen **>** und **<** durch Verschieben von der linken Seite in die rechte. Die Liste auf der rechten Seite zeigt dann alle für die Wiederherstellung ausgewählten virtuellen Maschinen. Mit der Schaltfläche **>** fügen Sie der Liste wiederherzustellende VMs hinzu, mit **<** entfernen Sie VMs aus ihr. Diese Liste enthält die ausgewählten virtuellen Maschinen und ihre neuesten verfügbaren Recovery-Punkte, d.h. die Zeitpunkte, auf die Sie zurücksetzen können.

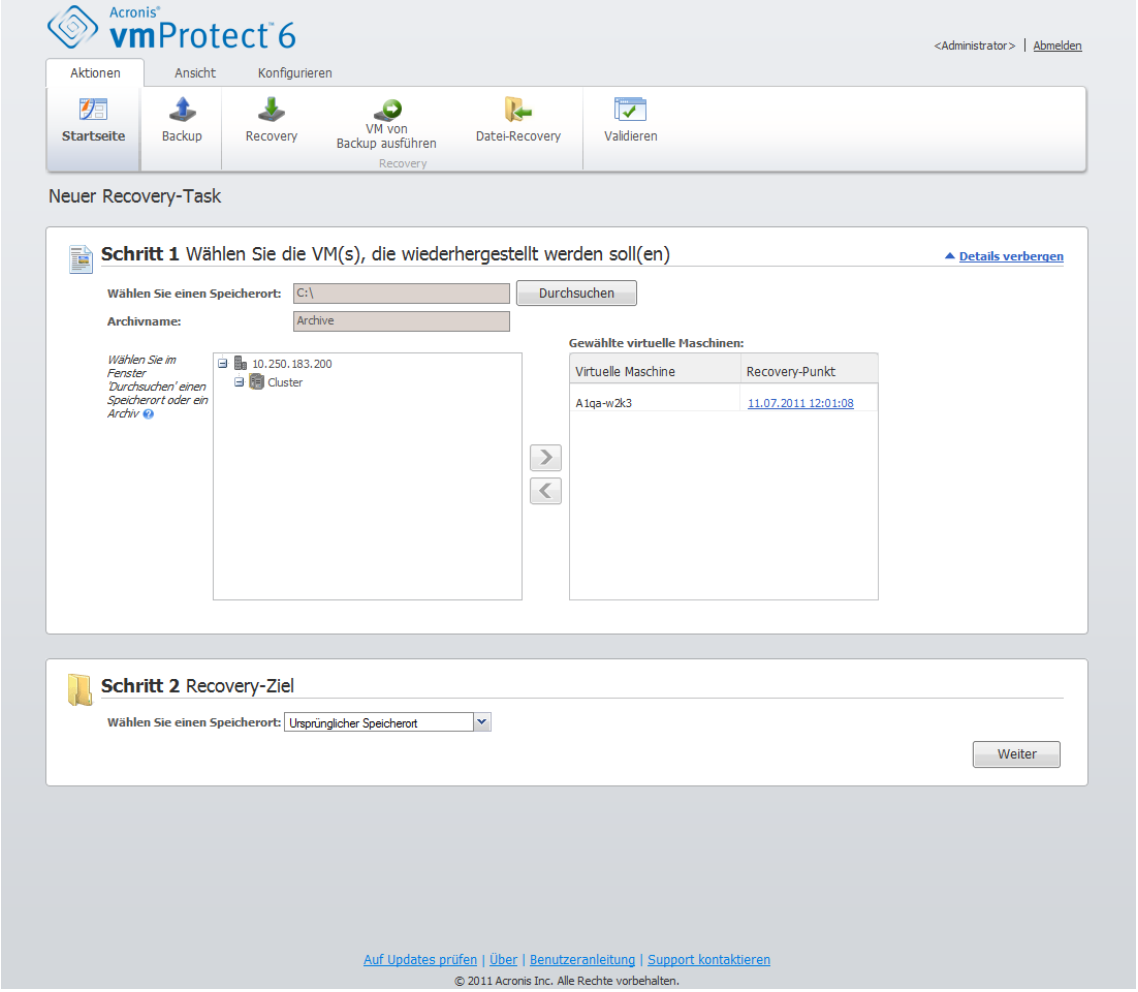
Standardmäßig wird der neueste Recovery-Punkt einer virtuellen Maschine voreingestellt. Klicken Sie auf den Recovery-Punkt, um ihn zu ändern. Im sich öffnenden Fenster können Sie dann einen anderen Recovery-Punkt wählen.

Im Fenster 'Recovery-Punkt auswählen' sehen Sie eine Liste mit allen für diese virtuelle Maschine verfügbaren Recovery-Punkten und wählen aus, welcher wiederhergestellt werden soll. Die Liste enthält den Namen des Archivs, in dem sich dieser Recovery-Punkt befindet sowie seinen Erstellungszeitpunkt.

Nachdem Sie die Recovery-Quelle bestimmt haben, klicken Sie auf **Weiter**, um **den ersten Schritt des Assistenten abzuschließen und fortzufahren.**

7.2 Ort der Wiederherstellung

Im zweiten Schritt des Assistenten 'Backup-wiederherstellen-Task' entscheiden Sie, wohin Sie die ausgewählte(n) virtuelle(n) Maschine(n) wiederherstellen.



Assistent 'Recovery-Task-erstellen', Schritt 2, 'Recovery-Ziel'

Zunächst bestimmen Sie mit dem Listenfeld **Speicherort auswählen** den gewünschten Zielort für den Recovery-Task. Wählen Sie aus, ob die ausgewählte(n) virtuelle(n) Maschine(n) an ihrem ursprünglichen Speicherort wiederhergestellt werden soll(en) oder auf einem anderen ESX-Host bzw. Datenspeicher. Die Liste zeigt nur die vom Acronis vmProtect Agenten verwalteten ESX-Hosts. Ist der gewünschte ESX-Host nicht in der Liste, stellen Sie sicher, dass er in der Ansicht **Konfigurieren** –> **ESX-Hosts** hinzugefügt wird.

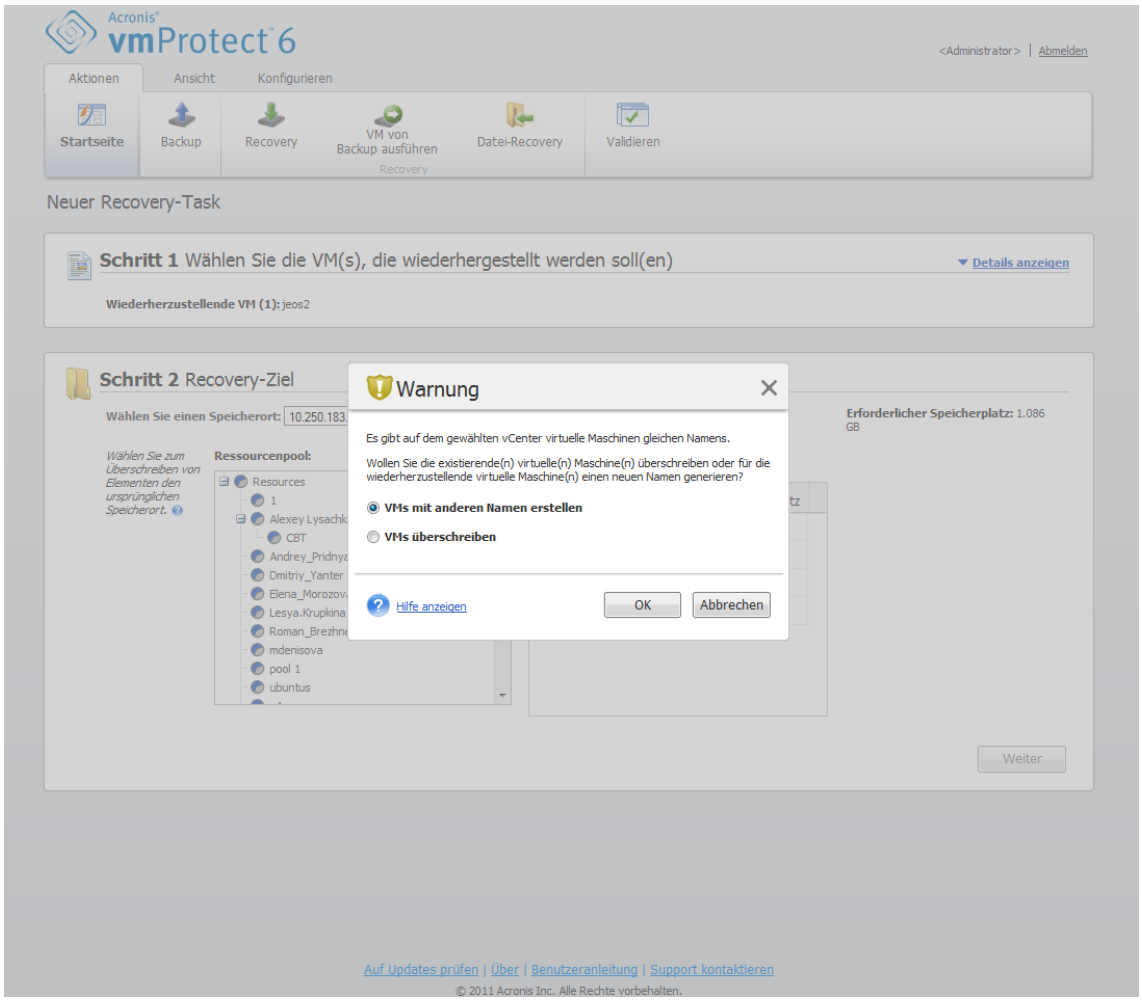
Beachten Sie beim Wiederherstellen am 'Ursprünglichen Speicherort', dass die wiederhergestellte VM eventuell nicht an demselben Speicherort erscheint, wo sie sich zum Zeitpunkt der Erstellung des Recovery-Punktes befand. Das ist der Fall, wenn die ausgewählte VM (definiert durch den Recovery-Punkt) zu einem anderen Host bzw. Datenspeicher, ESX-Host, Ressourcenpool oder vApp migriert wurde. Da die VMs ihre UUIDs während der Migration behalten, erfolgt die Wiederherstellung am aktuellen Speicherort der virtuellen Maschine. Ein Beispiel: Eine VM befand sich zum Zeitpunkt der Erstellung des Recovery-Punktes in der vApp1, wurde aber zwischenzeitlich zur vApp2 migriert. Dann wird diese VM in der vApp2 wiederhergestellt und überschreibt die existierende VM.

Sobald der ESX-Host definiert ist, wird automatisch eine Liste mit verfügbaren Ressourcenpools und Datenspeichern aufgebaut, in der Sie den genauen Speicherort für die wiederhergestellte(n) virtuelle(n) Maschine(n) festlegen können.

Definieren Sie außerdem das Format der wiederhergestellten virtuellen Laufwerke: 'Wie bei ursprünglicher VM' (empfohlen), 'Thin Provisioning' oder 'Thick Provisioning'. Thin Provisioning optimiert die Speicherplatzausnutzung der VM durch dynamische Zuordnung und intelligente Bereitstellung der verfügbaren physikalischen Speicherkapazität.

Auf Basis dieser Auswahl erscheint ein Hinweis, wie viel Speicherplatz auf dem Datenspeicher für eine erfolgreiche Wiederherstellung benötigt wird. Zum nächsten Schritt des 'Backup-wiederherstellen-Task'-Assistenten kommen Sie erst, nachdem Sie einen gültigen Datenspeicher mit ausreichend freiem Speicherplatz ausgewählt haben.

Beachten Sie, dass beim Wiederherstellen mehrerer virtueller Maschinen alle an jenem Ziel platziert werden, das bei diesem Schritt des Recovery-Assistenten festgelegt wird, zu einer jeweils neuen VM auf dem ausgewählten Datenspeicher.



Assistent 'Recovery-Task-erstellen', Schritt 2, Recovery-Ziel, Bestätigungs-Dialog 'Existierende VM überschreiben'

Falls sich auf dem ausgewählten ESX-Host oder Datenspeicher virtuelle Maschinen mit denselben Namen befinden, werden Sie um Bestätigung zum 'Überschreiben der existierenden VMs' gebeten. Diese Option bestimmt den Namen, der für eine wiederhergestellte virtuelle Maschine vergeben wird. Wenn Sie 'VMs überschreiben' wählen, werden die existierenden virtuellen Maschinen durch die wiederhergestellten ersetzt.

Beachten Sie, dass es in diesem Fall nicht möglich ist, einen Datenspeicher auszuwählen (weil der durch das Überschreiben der Zielmaschinen schon festgelegt ist); allerdings können Sie den Speicherort des Ressourcenpools für diese VM ändern, indem Sie ihn unter **Ressourcenpool** entsprechend auswählen.

Beachten Sie, dass Sie für eine erfolgreiche Wiederherstellung laufende existierende Maschinen entweder manuell stoppen oder bei den Recovery-Optionen **Ziel-VMs mit Start der Wiederherstellung ausschalten** aktiviert haben müssen (*siehe Abschnitt 'VM-Powermanagement* (S. 40)).

Wenn Sie **VMs mit anderen Namen erstellen** wählen, werden die wiederhergestellten VMs nach folgender Konvention benannt:

'[Ursprünglicher_Name_der_VM]_DATUM'

wobei 'Ursprünglicher_Name_der_VM' der ursprüngliche Name der wiederhergestellten virtuellen Maschine ist und DATUM das aktuelle Datum. War der Name der wiederhergestellten VM zum

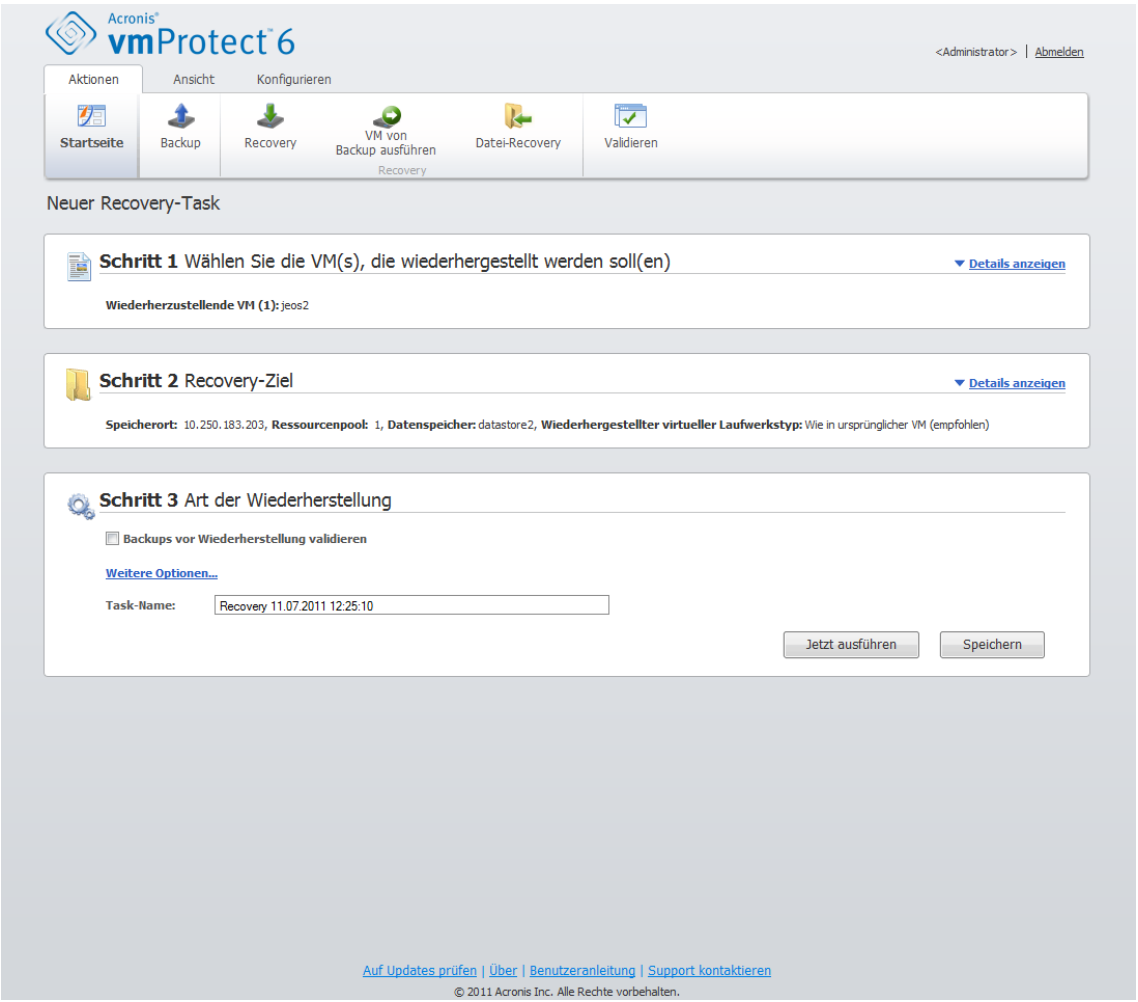
Beispiel 'VM_ursprünglich', wird sie nach der Wiederherstellung 'VM_ursprünglich_25.05.2011' benannt.

Nachdem Sie das Recovery-Ziel bestimmt haben, klicken Sie auf **Weiter**, um **den zweiten Schritt abzuschließen und zum letzten Schritt zu gelangen.**

7.3 Art der Wiederherstellung

Im dritten Schritt des Assistenten 'Backup-wiederherstellen-Task' bestimmen Sie die Einstellungen für den Recovery-Task.

Hier können Sie spezifizieren, ob die Archive vor der Wiederherstellung validiert werden (*weitere Informationen über die Backup-Validierung finden Sie im Abschnitt 'Backups validieren'* (S. 64)). Über **Weitere Optionen...** können Sie die Einstellungen des Recovery-Tasks anpassen.



Assistent 'Recovery-Task-erstellen', Schritt 3 'Art der Wiederherstellung'

Um den Assistenten abzuschließen und den 'Backup-wiederherstellen-Task' zu erstellen, müssen Sie dem Task einen Namen geben und seine Ausführung definieren. Beachten Sie, dass die Zeichen [ ] { } ; , . im Task-Namen nicht erlaubt sind.

Wenn Sie auf **Jetzt Ausführen** klicken, wird der Task sofort mit den spezifizierten Parametern ausgeführt. Den Fortschrittsbalken des Tasks finden Sie in den Ansichten **Tasks** und **Dashboard**. Diese Vorgehensweise bietet sich an, wenn Sie den Task nur einmal ausführen wollen. Das Task-Ergebnis erscheint im **Dashboard** und kann zudem in der Ansicht **Logs** überprüft werden.

Mit **Speichern** speichern Sie den Task in der Task-Liste (**Ansicht–>Tasks**). Das ist der komfortable Weg, wenn Sie diesen Task später von der Seite **Ansicht Tasks** aus manuell starten wollen oder planen, ihn mehrmals auszuführen.

7.4 Optionen

Über **Weitere Optionen…** im letzten Schritt des 'Backup-wiederherstellen-Task'-Assistenten gelangen Sie zum Fenster mit den erweiterten Einstellungen.

Wenn Sie keine Änderungen vornehmen, bleiben die Standardwerte für den aktuellen Recovery-Task erhalten. Beachten Sie, dass ein späteres Ändern bestimmter Einstellungen und deren Speichern als Standard nicht für jene Tasks gilt, die bereits mit den zuvor gewählten Standardeinstellungen erstellt wurden (die Task-Einstellungen entsprechen immer den bei der Erstellung gültigen Standardwerten).

7.4.1 Benachrichtigungen

1) E-Mail-Benachrichtigungen

Mit dieser Option richten Sie die E-Mail-Benachrichtigungen über wesentliche Ereignisse während eines Recovery-Tasks ein, wie den erfolgreichen Abschluss, ein fehlgeschlagenes Backup oder einen erforderlichen Benutzereingriff. Standardmäßig ist diese Option deaktiviert.

Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung schicken**, um die entsprechende Funktion zu aktivieren.

Aktivieren Sie unter dem Kontrollkästchen **E-Mail-Benachrichtigungen schicken** die gewünschten Einstellungen folgendermaßen:

- **Wenn die Wiederherstellung erfolgreich abgeschlossen wurde** – zum Versenden einer Benachrichtigung, wenn der Recovery-Task erfolgreich ausgeführt wurde.
- **Wenn eine Wiederherstellung fehlschlägt** – die Benachrichtigung erfolgt, wenn Wiederherstellung nicht erfolgreich war.
- **Vollständiges Log zur Benachrichtigung hinzufügen** – Das vollständige Log wird mit der Benachrichtigung verschickt.

Geben Sie eine oder mehrere E-Mail-Adressen ein, an die die Benachrichtigungen geschickt werden. Die Adressen werden im Feld **E-Mail-Adressen** eingegeben, durch Semikolons getrennt.

Nennen Sie den für die Benachrichtigungen gewünschten **Betreff**.

- **SMTP-Server** – Geben Sie den Namen des Postausgangsservers ein (SMTP-Server).
- **Port** – Bestimmen Sie den Port des SMTP-Servers (der Standard-Port ist 25).
- **Benutzername** – Geben Sie den Benutzernamen ein.
- **Kennwort** – Geben Sie das Kennwort ein.

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 so erstellt, als stammten sie von der Zieladresse.

Verschlüsselung verwenden – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden und zwischen SSL- oder TLS-Verschlüsselung wählen.

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

2) SNMP-Benachrichtigungen

Diese Option definiert, ob der oder die Agenten auf der verwalteten Maschine das Ereignis-Log von Recovery-Aktionen zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden. Standardmäßig ist diese Option deaktiviert**.**

Wählen Sie, ob Sie Log-Nachrichten über Ereignisse während der Recovery-Aktion an Maschinen mit laufenden SNMP-Anwendungen übermitteln wollen. Wählen Sie eine der folgenden Optionen:

- **SNMP-Benachrichtigungen über Ereignisse während der Recovery-Aktion einzeln senden** – Um das Ereignis-Log der Wiederherstellung an spezifizierte SNMP-Manager zu schicken.
  Ereignisse, die übermittelt werden – Wählen Sie die Ereignistypen, die übermittelt werden sollen: Informationen, Warnungen oder Fehler.
  Name oder IP des Servers – Geben Sie den Namen oder die IP-Adresse des Hosts ein, auf dem die SNMP-Verwaltungsanwendung läuft, die die Benachrichtigung bekommen soll.
  Community – Tragen Sie den Namen der SNMP-Community ein, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist 'public'.
  Klicken Sie auf **Test-Mail senden**, um sicherzugehen, dass alle Einstellungen korrekt sind.
- **Keine SNMP-Benachrichtigungen senden** – Es wird kein Ereignis-Log der Wiederherstellung an SNMP-Manager gesendet.

7.4.2 Fehlerbehandlung

Mit diesen Optionen geben Sie vor, wie während der Recovery-Aktion eventuell auftretende Fehler behandelt werden. Wählen Sie **Bei Fehler neu versuchen**, um den stillen Modus zu aktivieren.

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das **Zeitintervall zwischen den Versuchen** und die **Anzahl der Versuche** einstellen. Der Task endet, sobald die Wiederherstellung erfolgreich war ODER die festgelegte Anzahl von Versuchen erreicht ist.

Wenn Sie das Kontrollkästchen **Bei Fehler neu versuchen** aktivieren, bestimmen Sie dazu die **Anzahl der Versuche** und das **Zeitintervall zwischen den Versuchen**. Standardmäßig ist diese Option mit folgenden Einstellungen aktiviert: **Anzahl der Versuche** – 5 und **Zeitintervall zwischen den Versuchen** – 30 Sekunden. Wenn zum Beispiel das Recovery-Ziel im Netzwerk nicht verfügbar oder erreichbar ist, versucht die Anwendung alle 30 Sekunden erneut, es zu erreichen, aber nur bis zu fünf Mal. Die Versuche werden aufgegeben, sobald die Verbindung gelingt oder die angegebene Zahl der Versuche erreicht ist.

7.4.3 Zustand der VM steuern

Mit dieser Option konfigurieren Sie das Powermanagement der virtuellen Maschinen vor und nach Ausführung des Recovery-Tasks.

1) Ziel-VMs mit Start der Wiederherstellung ausschalten

Die Wiederherstellung zu einer existierenden Maschine ist unmöglich, während sie online ist, so dass sie automatisch ausgeschaltet wird, wenn ein Recovery-Task startet. Alle Benutzer werden von der Maschine getrennt, nicht gespeicherte Daten gehen verloren.

Diese Option ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen **Ziel-VMs mit Start der Wiederherstellung ausschalten**, um virtuelle Maschinen manuell vor der Wiederherstellung auszuschalten.

2) Ziel-VMs nach Abschluss der Wiederherstellung einschalten

Wurde eine Maschine aus einem Backup zu einer anderen Maschine wiederhergestellt, könnte das Replikat der existierenden Maschine im Netzwerk erscheinen. Sie sorgen für einen sicheren Betrieb, wenn Sie die wiederhergestellte virtuelle Maschine erst dann manuell einschalten, nachdem Sie die notwendigen Vorsichtsmaßnahmen getroffen haben.

Diese Option ist standardmäßig deaktiviert. Aktivieren Sie das Kontrollkästchen **Ziel-VMs nach Abschluss der Wiederherstellung einschalten**, um die virtuelle Maschine automatisch einzuschalten.

7.4.4 Erweiterte Einstellungen

FTP im Modus 'Aktiv' verwenden

Es ist möglich, FTP im Modus 'Aktiv' für FTP-Authentifizierung und Datentransfer zu verwenden. Die Standardeinstellung für **FTP im Modus 'Aktiv' verwenden** ist deaktiviert.

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

Klicken Sie nach Festlegen der Einstellungen auf **OK**, um das Fenster zu schließen und sie nur auf den aktuellen Recovery-Task anzuwenden.

7.5 Erstellten Recovery-Task verwalten

Beim Bearbeiten eines existierenden Recovery-Tasks sehen Sie alle Schritte des Assistenten, die sie bei der Erstellung des Tasks abgeschlossen haben. Alle drei Schritte des Assistenten erscheinen gleichzeitig auf dem Bildschirm. (*Weitere Informationen finden Sie im Abschnitt 'Tasks verwalten'* (S. 52)).

8 Datei-Recovery

Es ist gelegentlich nötig, nur eine oder bestimmte Dateien aus einem Backup-Archiv wiederherzustellen, ohne die gesamte virtuelle Maschine zu rekonstruieren. Die Funktion **Datei-Recovery** ermöglicht das Durchsuchen der Archive und die Wiederherstellung ausgewählter Dateien in einer durch das Archiv bestimmten Version (Recovery-Punkt). Das Wiederherstellungsziel wird durch die verfügbaren Optionen des Internetbrowsers definiert, in dem die vmProtect Management Console ausgeführt wird. (Der Dialog ist derselbe, der beim Speichern einer Internetseite mit dem Befehl **Datei**->**Speichern unter** angezeigt wird).

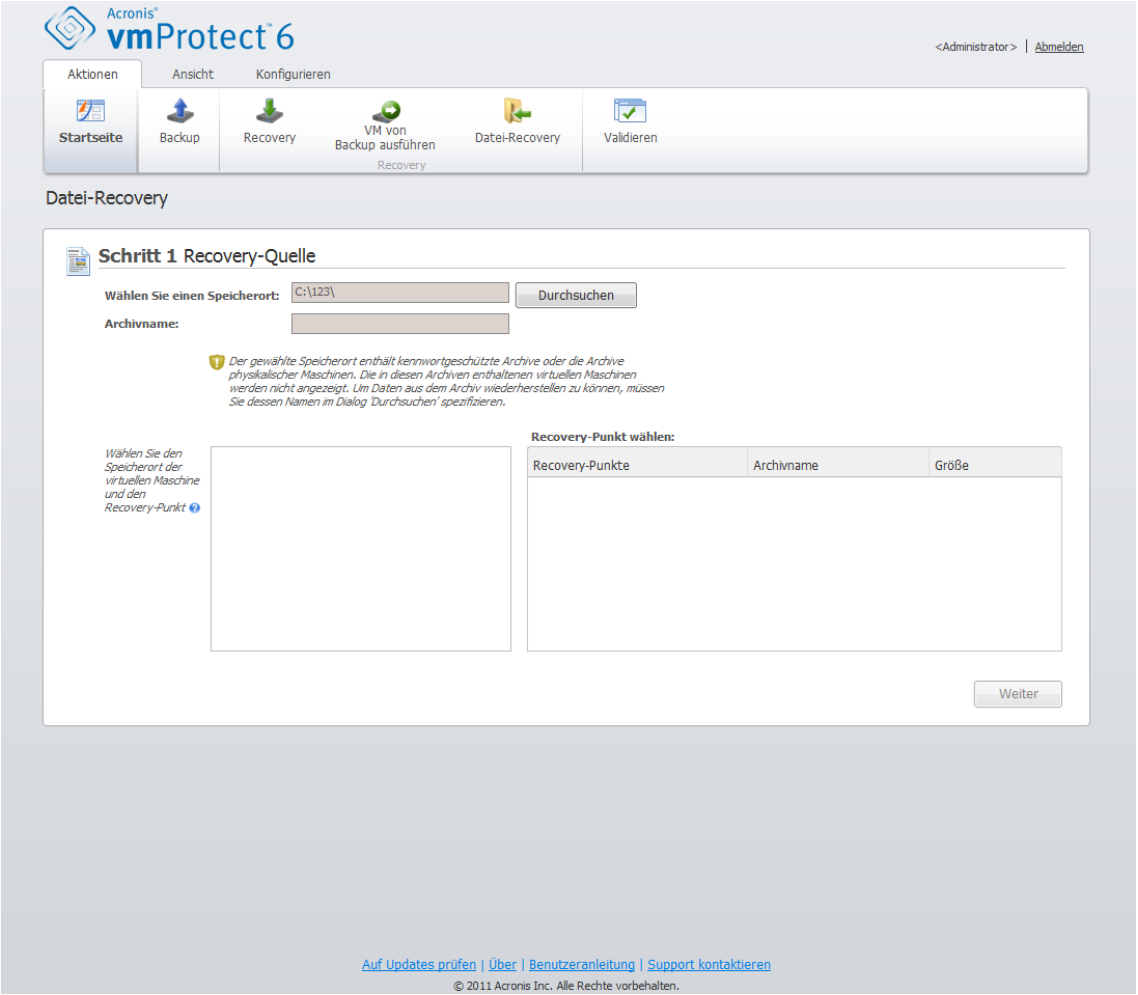
Klicken Sie auf **Datei-Recovery** auf der **Startseite** im Hauptmenü, um eine oder mehrere gesicherte Dateien wiederherzustellen. Der **Datei-Recovery**-Assistent öffnet sich im Hauptarbeitsbereich und fordert Sie auf, für die Wiederherstellung der Dateien die erforderlichen Informationen bereitzustellen und die notwendigen Einstellungen zu konfigurieren. Der Assistent enthält zwei Schritte:

- Recovery-Quelle
- Recovery-Punkt wählen

8.1 Recovery-Quelle

Zuerst bestimmen Sie den Backup-Speicherort, der nach Archiven und deren Inhalt durchsucht wird.

Klicken Sie auf **Durchsuchen**, um einen Speicherort bzw. das Archiv zu wählen. Im erscheinenden Fenster mit den Optionen zum Durchsuchen definieren Sie den Pfad bzw. den Archivnamen. Hier finden Sie auch die zuvor verwendeten Speicherorte unter **Letzte Speicherorte**.



Assistent für Datei-Recovery, Schritt 1, 'Recovery-Quelle'

Es gibt zwei Wege, Speicherorte im Browserfenster auszuwählen. Sie wählen zuerst einen Speicherort. In diesem Fall sehen Sie den gesamten Baum aller virtuellen Maschinen unterhalb des gewählten Speicherorts und alle deren Archive, die am gewählten Speicherort abgelegt sind. Falls Sie anderenfalls einen Speicherort und ein Archiv wählen, sehen Sie nur den Inhalt des Archivs.

Falls der ausgewählte Speicherort kennwortgeschützte Archive oder Archive von physikalischen Maschinen enthält, können die dort enthaltenen VMs nicht angezeigt werden und es erscheint folgende Warnung: Um in diesem Fall Daten aus diesen Archiven wiederherzustellen, müssen Sie deren Namen direkt eingeben.

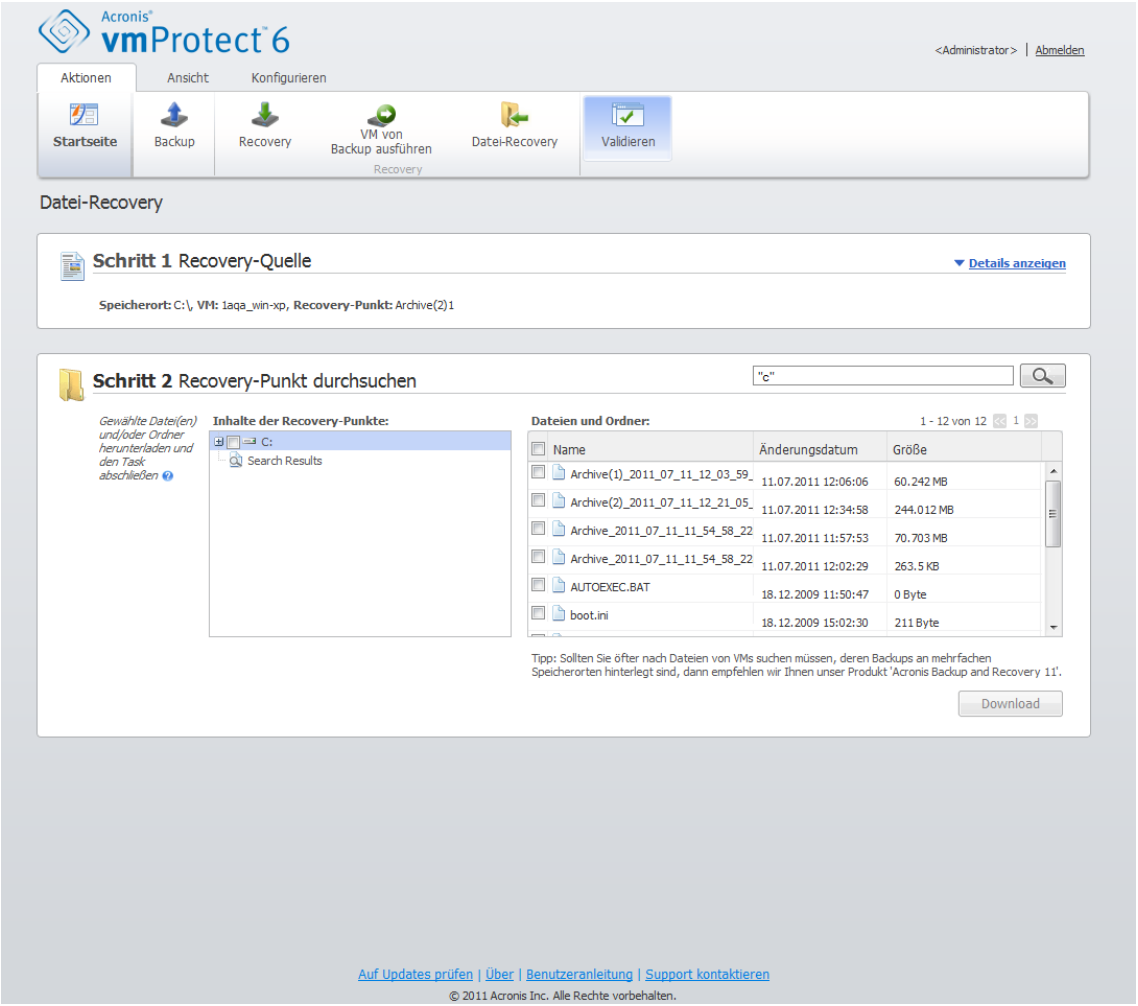
Der gewählte Speicherort wird nach Archiven und deren Inhalten durchsucht. Das Ergebnis der Suche sehen Sie als Baum die virtuellen Maschinen, die in den am gewählten Speicherort abgelegten Archiven oder im gewählten Archiv enthalten sind. Wenn Sie auf eine beliebige virtuelle Maschine klicken, erscheint auf der rechten Seite eine Liste aller dafür vorhandenen Recovery-Punkte.

Standardmäßig wird der neueste Recovery-Punkt einer Maschine vorausgewählt. Durch Klicken kann der Recovery-Punkt geändert werden. Beachten Sie, dass 'Datei-Recovery' gleichzeitig nur die Auswahl einer virtuellen Maschine und eines Recovery-Punkts erlaubt, während die Wiederherstellung eines Backups die Wiederherstellung mehrerer VMs bietet.

Nach Auswahl des Recovery-Punkts für die virtuelle Maschine führen Sie den nächsten Schritt aus. Dieser Recovery-Punkt definiert den Zustand der virtuellen Maschine, dem Sie die Dateien oder Verzeichnisse entnehmen wollen.

8.2 Recovery-Punkt untersuchen

Im zweiten Schritt des Assistenten für **Datei-Recovery** müssen Sie wählen, welche Dateien oder Ordner wiederhergestellt werden. Mit einem dem Windows-Explorer ähnlichen Datei-Browser sehen Sie den Inhalt des gewählten VM-Recovery-Punkts. Im Baum auf der linken Seite können Sie die Volumes und Ordner erweitern, um die Inhalte der Volumes und Ordner auf der rechten Seite zu durchsuchen und wiederherzustellende Inhalte auszuwählen.



Assistent für Datei-Recovery, Schritt 2 'Recovery-Punkt wählen'

Acronis vmProtect **Datei-Recovery** enthält eine Suchfunktion. Das Suchfeld ist oben rechts über der Liste der Dateien und Verzeichnisse. Sie können die Suche benutzen, wenn Sie den exakten Dateinamen der wiederherzustellenden Datei nicht wissen. Sie können die Dateien und Verzeichnisse in der Liste mit Hilfe von Dateimasken filtern.

Sie können dazu die Wildcards '*' und '?' als Dateimaske benutzen.

Fügen Sie dem Ordnernamen in der Maske einen Backslash (\) hinzu, um einen Ordner auszuschließen, dessen Pfad einen Laufwerksbuchstaben enthält, z.B. C:\Finanzen\

Sie können die Suchergebenisse anhand jeder Spalte sortieren: Name, Erstell- oder Aktualisierungsdatum, Größe und Verzeichnis. Wenn Sie zuerst nach einem beliebigen Feld sortieren, beispielsweise nach der Zeit, können Sie das Ergebnis anschließend noch nach einem weiteren Feld ordnen, zum Beispiel nach dem Namen. In diesem Fall wird eine Sortierung in zwei Ebenen erfolgen,

Name und Zeit. Auf diese Weise können Sie die notwendigen Dateien für die Wiederherstellung schnell finden.

Wenn Sie alle Dateien für die Wiederherstellung gewählt haben, klicken Sie auf **Download**. Sie sehen das Standardfenster (wie beispielsweise nach einem Klick mit der rechten Maustaste –> **Ziel speichern unter …**) in dem Sie den Ort zum Speichern der gewählten Dateien wählen. Alle gewählten Dateien und Verzeichnisse werden als einzelnes .zip-Archiv heruntergeladen.

9 VM von Backup ausführen

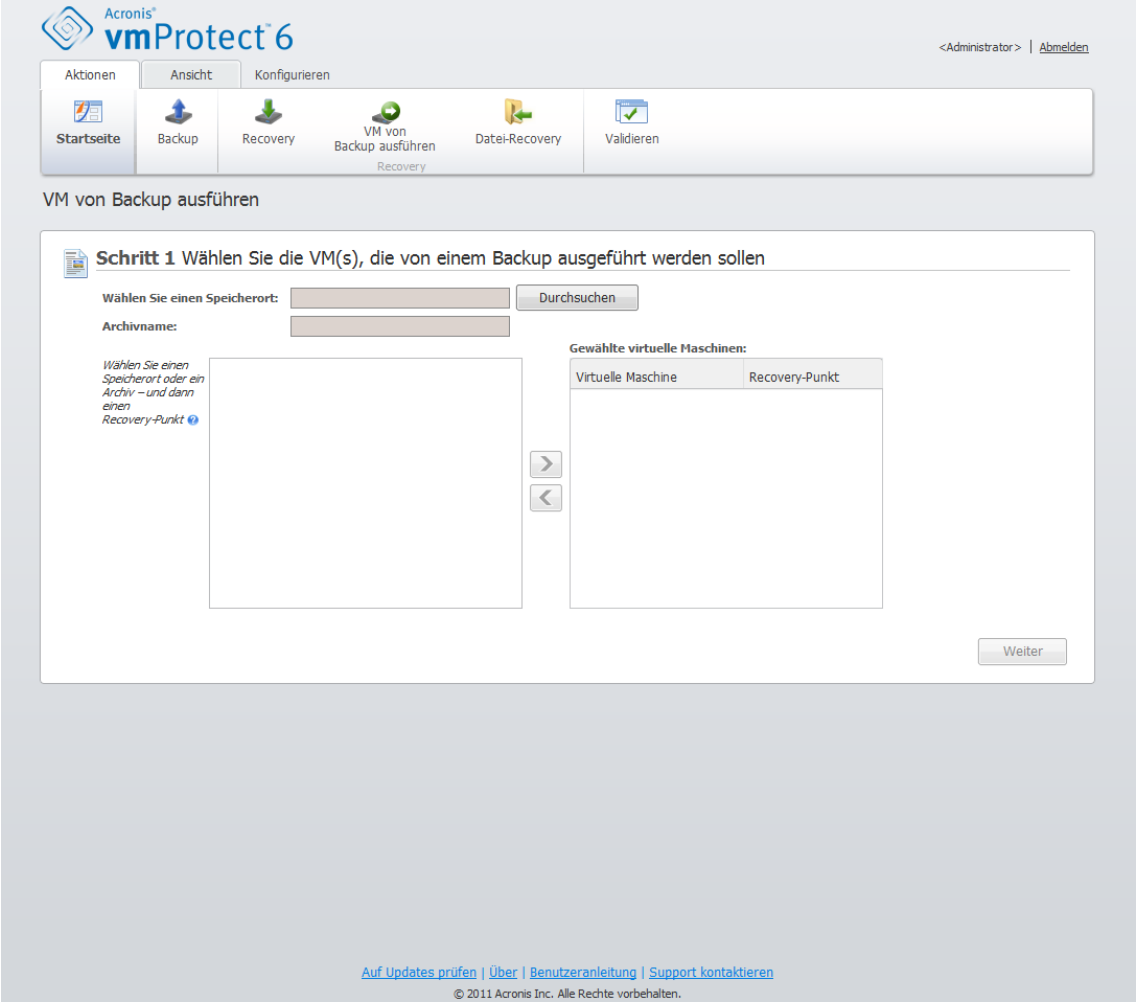
Klicken Sie auf **VM von Backup ausführen** auf der **Startseite** im Hauptmenü, um eine gesicherte virtuelle Maschine zu mounten, ohne sie wiederherzustellen. Der **VM von Backup ausführen**-Assistent öffnet sich im Hauptarbeitsbereich und fordert Sie auf, für die Wiederherstellung der Dateien die erforderlichen Informationen bereitzustellen und die notwendigen Einstellungen für den Task **VM von Backup ausführen** zu konfigurieren. Der Assistent enthält folgende drei Schritte:

- Auszuführende VM
- Ort der VM-Ausführung
- Erweiterte Einstellungen

Nachfolgend werden die Schritte des Assistenten **VM von Backup ausführen** und deren Optionen beschrieben.

9.1 Auszuführende VM

Im ersten Schritt des Assistenten **VM von Backup ausführen** definieren Sie zuerst den Backup-Speicherort und wählen die auszuführende virtuelle Maschine aus. Die gewählten Speicherorte werden nach Archiven und deren Inhalten durchsucht. Das ist notwendig, um den oder die Recovery-Punkte zu wählen, die den Zustand der virtuellen Maschine definieren, die Sie aus dem Backup heraus ausführen möchten. Der Prozess zum Ausführen einer VM von einem Backup wird auch als 'Mounten einer virtuellen Maschine' bezeichnet.



Assistent 'VM von Backup ausführen', Schritt 1, 'Auszuführende VM'

Klicken Sie auf **Durchsuchen**, um einen Speicherort bzw. das Archiv zu wählen. Im erscheinenden Fenster mit den Optionen zum Durchsuchen definieren Sie den Pfad bzw. den Archivnamen. Hier finden Sie auch die zuvor verwendeten Speicherorte unter **Letzte Speicherorte**. Beachten Sie, dass Sie für das 'Ausführen einer VM von Backup' als Speicherort nur **Netzwerkordner** oder **lokale Ordner** auswählen können. Andere Speicherorte wie **Online Backup Storage** oder **FTP/sFTP-Server** sind an dieser Stelle nicht verfügbar.

Es gibt zwei Wege, Speicherorte im Browserfenster auszuwählen. Sie wählen zuerst einen Speicherort. In diesem Fall sehen Sie den gesamten Verzeichnisbaum aller virtuellen Maschinen unterhalb des gewählten Speicherorts und alle deren Archive, die am gewählten Speicherort abgelegt sind. Falls Sie anderenfalls einen Speicherort und ein Archiv wählen, sehen Sie nur den Inhalt des Archivs.

Falls sich am gewählten Speicherort irgendein durch Kennwort geschütztes Archiv oder Archive physikalischer Maschinen befinden, können die in diesen Archiven enthaltenen VMs nicht angezeigt werden und Sie erhalten eine Warnung. Um in diesem Fall Daten aus diesen Archiven wiederherzustellen, müssen Sie deren Namen direkt eingeben.

Sie können in der Liste auf der linken Seite eine beliebige virtuelle Maschine auswählen und auf die rechte Seite in den Bereich **Ausgewählte virtuelle Maschinen** verschieben. Die Auswahl der virtuellen Maschinen erfolgt mit Hilfe der Schaltflächen **>** und **<** und durch Verschieben von der linken Seite in die rechte. Die Liste auf der rechten Seite zeigt dann alle zum Mounten ausgewählten virtuellen Maschinen. Mit der Schaltfläche **>** fügen Sie der Liste VMs hinzu, mit **<** entfernen Sie VMs

aus ihr. Die so aufgebaute Liste enthält die ausgewählten virtuellen Maschinen und ihre neuesten verfügbaren Recovery-Punkte, d.h., die Zeitpunkte, auf die Sie zurücksetzen können.

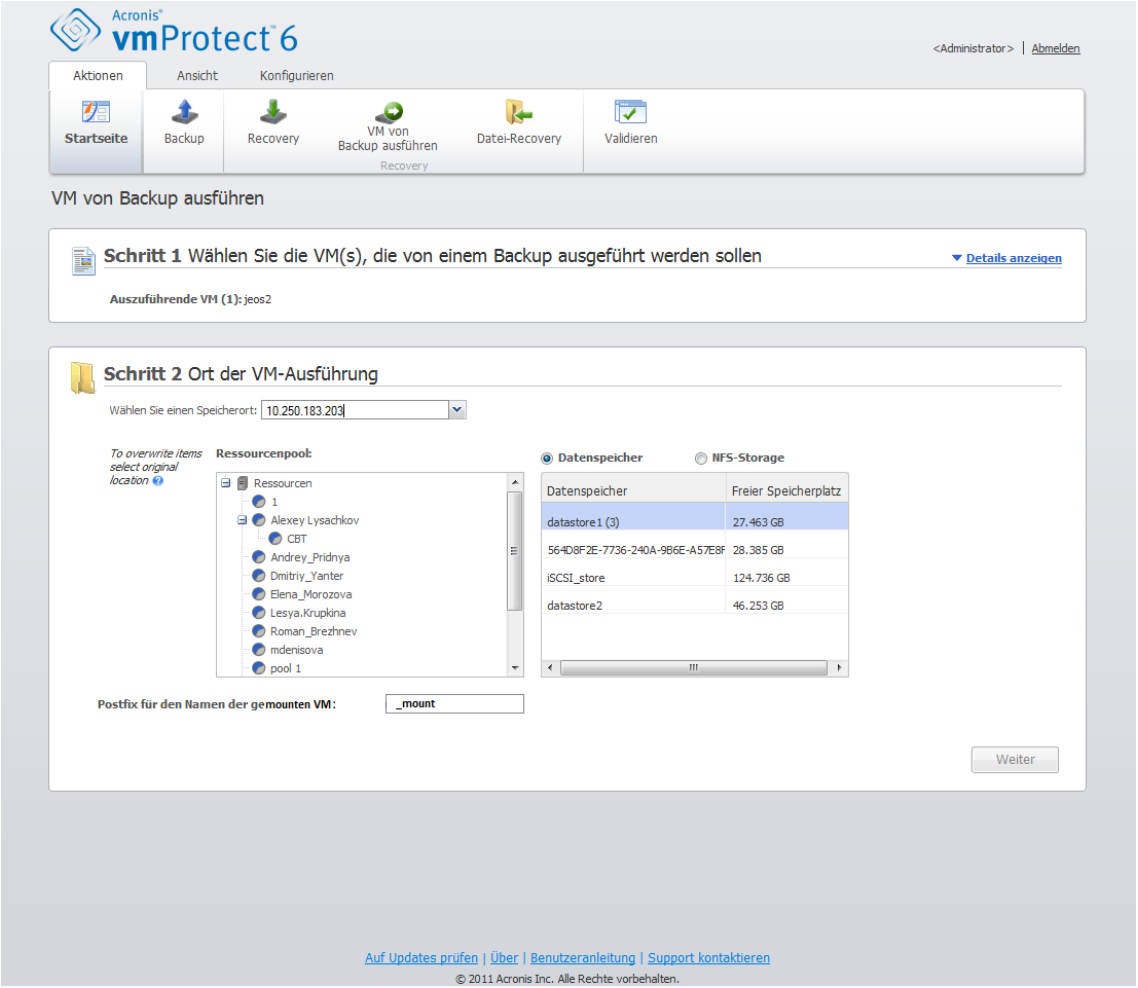
Standardmäßig wird der neueste Recovery-Punkt einer virtuellen Maschine voreingestellt. Klicken Sie auf den Recovery-Punkt, um ihn zu ändern. Im sich öffnenden Fenster können Sie dann einen anderen Recovery-Punkt wählen.

Im Fenster **Recovery-Punkt auswählen** sehen Sie eine Liste mit allen für diese virtuelle Maschine verfügbaren Recovery-Punkten und wählen aus, welcher gemountet werden soll. Die Liste enthält die Zeitstempel der Recovery-Punkte, den Dateinamen des den Recovery-Punkt enthaltenden Archivs und die Größe.

Nachdem Sie die 'Auszuführende VM' bestimmt haben, klicken Sie auf **Weiter**, um **den ersten Schritt des Assistenten zu beenden und fortzufahren.**

9.2 Ort der VM-Ausführung

Im zweiten Schritt entscheiden Sie, wo die ausgewählte(n) virtuelle(n) Maschinen(n) ausgeführt werden soll(en).



Assistent 'VM von Backup ausführen', Schritt 2, 'Ort der VM-Ausführung'

Zunächst bestimmen Sie mit dem Listenfeld **Speicherort auswählen** den ESX-Host, auf den Sie die ausgewählten VMs mounten wollen. Die Liste zeigt nur die vom Acronis vmProtect Agenten

verwalteten ESX-Hosts. Ist der gewünschte ESX-Host nicht in der Liste, stellen Sie sicher, dass er in der Ansicht **Konfigurieren** –> **ESX-Hosts** hinzugefügt wird.

Sobald der ESX-Host bestimmt ist, wird automatisch eine Liste mit verfügbaren Ressourcenpools aufgebaut, in der Sie den genauen Speicherort für die gemountete(n) virtuelle(n) Maschine(n) festlegen können. Die Wahl des Datenspeichers ist erforderlich, um zu definieren, wo die an den gemounteten virtuellen Maschinen vorgenommenen Änderungen gespeichert werden. Alternativ (aber nicht empfohlen) können Sie die Änderungen auf den NFS-Storage, den der Acronis vmProtect-Agent zur Verfügung stellt, speichern.

Beachten Sie, dass beim Mounten mehrerer virtueller Maschinen alle an jenem Ziel platziert werden, das bei diesem Schritt des Assistenten **VM von Backup ausführen** festgelegt wird; jede von ihnen in einem bestimmten Ressourcenpool. Die an diesen VMs vorgenommenen Änderungen werden in ein eindeutiges Verzeichnis auf dem ausgewählten Datenspeicher oder NFS-Storage gespeichert.

Ist kein Datenspeicher für die Sicherung der Änderungen verfügbar oder Sie können keinen durch Auswahl in der Liste bestimmen, so ist es möglich (aber nicht empfohlen), die VM auf den lokalen NFS-Storage des Acronis vmProtect Agent zu mounten.

Beachten Sie außerdem, dass der Acronis vmProtect Agent mit vMotion kompatibel ist (insbesondere mit Storage vMotion). Wird die gemountete VM mit Hilfe von Storage vMotion auf einen anderen Datenspeicher verschoben, verbleibt sie nach dem Trennen an ihrem neuen Speicherort. In diesem Fall ähnelt das Mounten dem Wiederherstellen eines Backups, weil bei vMotion alle Daten physikalisch zum neuen Speicherort verschoben werden.

Im Feld **Postfix für den Namen der gemounteten VM** geben Sie das Postfix für den Namen der gemounteten virtuellen Maschine ein. Dies ist erforderlich, weil es nicht möglich ist, zwei virtuelle Maschinen mit demselben Namen auf einem ESX-Host auszuführen, insbesondere wenn die ursprüngliche VM dort bereits läuft. Die gemountete VM wird auf Basis folgender Konvention benannt:

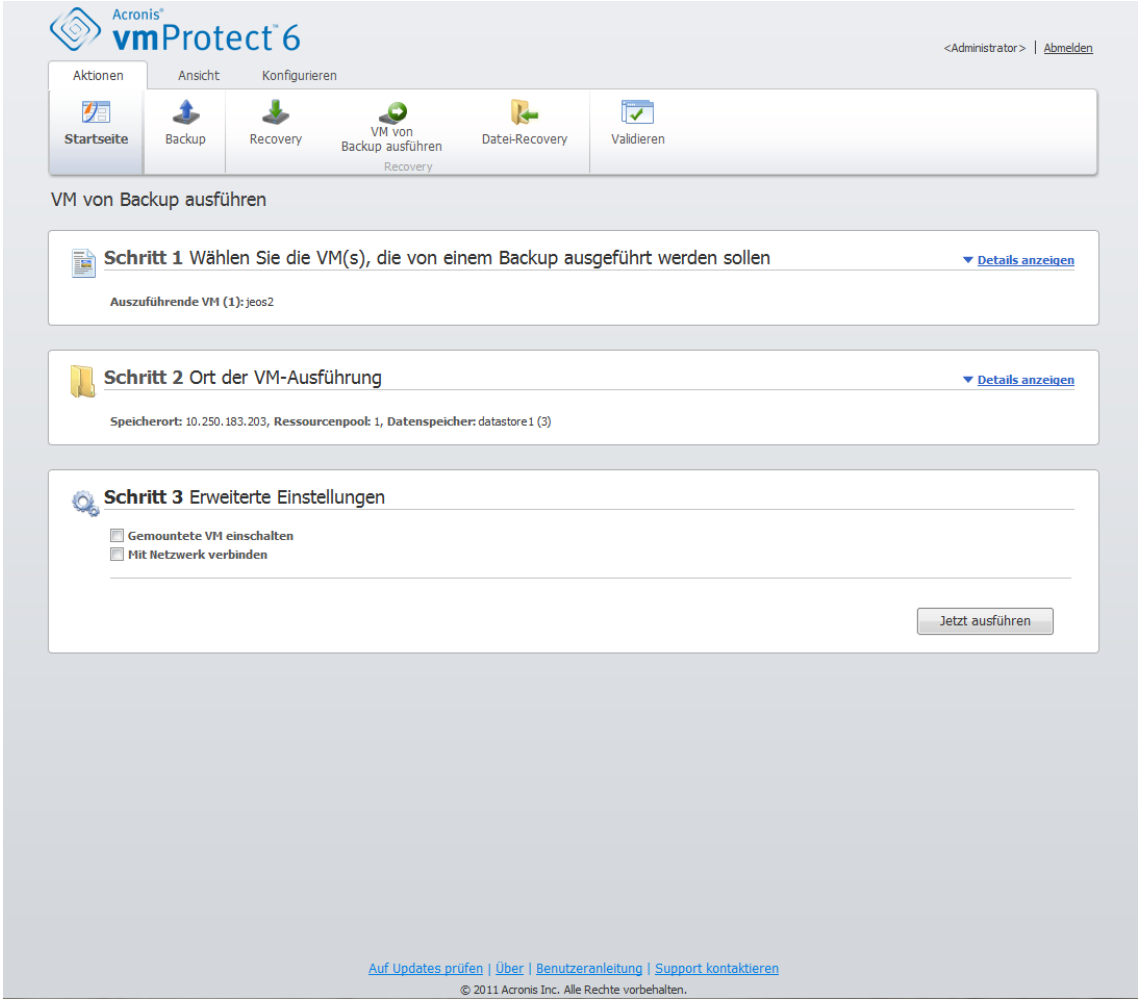
'[Ursprünglicher_Name_der_VM]_mount'

wobei 'Ursprünglicher_Name_der_VM' der ursprüngliche Name der gemounteten virtuellen Maschine ist und '_mount' der Postfix, den Sie ändern können. War der Name der gemounteten VM zum Beispiel 'VM_ursprünglich', wird sie nach dem Mounten 'VM_ursprünglich_mount' benannt.

Nachdem Sie den 'Ort der VM-Ausführung' bestimmt haben, klicken Sie auf **Weiter**, um **den zweiten Schritt abzuschließen und fortzufahren.**

9.3 Erweiterte Einstellungen

Im dritten Schritt des Assistenten aktivieren Sie die Kontrollkästchen **für die Optionen Gemountete VM einschalten und Mit dem Netzwerk verbinden.**



Assistent 'VM von Backup ausführen', Schritt 3 'Erweiterte Einstellungen'

Wählen Sie die Option **Gemountete VM einschalten**, um die Maschine nach Abschluss des Assistenten automatisch auszuführen. Beachten Sie, dass möglicherweise das Replikat der gemounteten Maschine (z.B. die ursprüngliche Maschine) im Netzwerk erscheint. Sie sind auf der sicheren Seite, wenn Sie die gemountete virtuelle Maschine manuell einschalten, nachdem Sie die notwendigen Vorsichtsmaßnahmen getroffen haben.

Aktivieren Sie das Kontrollkästchen **Mit dem Netzwerk verbinden**, wenn Sie eine ausgefallene VM mounten, die nicht mehr im Netzwerk vorhanden ist. Wenn Sie eine VM zu Testzwecken mounten (um eine gewisse Datenkonsistenz zu gewährleisten), während die ursprüngliche VM gerade ausgeführt wird, dann lassen Sie dieses Kontrollkästchen deaktiviert. Um Konflikte zu vermeiden, sollten Sie vor dem Einschalten einer VM ihre Netzwerk-Konfiguration manuell so ändern, dass sie nicht mehr mit dem Produktionsnetzwerk verbunden ist und sie anschließend mit einem isolierten, nicht-produktiven Netzwerk verbinden.

Nach einem Klick auf **Jetzt ausführen** erscheint die ausgewählte VM im VMware Infrastructure Client und Sie können sie wie jede andere virtuelle Maschine in der Umgebung verwalten. Um die VM zu trennen (zu stoppen), gehen Sie zur Seite **Ansicht–>Gemountete VMs**.

9.4 Verwalten der erstellten Aktion 'VM von Backup ausführen'

Es ist nicht möglich, die existierende Aktion **VM von Backup ausführen** zu bearbeiten. Sie können die gemounteten VMs nur über die Seite **Ansicht**->**Gemountete VMs** trennen.

10 Tasks verwalten

Klicken Sie im Hauptmenü in der Registerlasche **Ansicht** auf **Tasks** (**Ansicht**->**Tasks**), um die Seite **Tasks** zu öffnen; hier können Sie die Details einsehen und Task-Aktionen ausführen. Beachten Sie, dass auf der Seite **Tasks** nur das Ausführen von Basis-Aktionen mit existierenden Tasks möglich ist, Sie können hier keine neuen Tasks erstellen (um einen neuen Task für Backup, Recovery oder Validierung zu erstellen, gehen Sie zur Registerlasche **Startseite** in der Hauptsymbolleiste).

Die Seite **Tasks** enthält zwei Hauptbereiche: die **Tasks**-Liste und die **Task**-Details.

Die **Tasks**-Liste ist die allgemeine Liste aller im Acronis vmProtect-Agenten erstellten Tasks. Die Liste der Tasks enthält die Backup-, Recovery- und Validierungs-Aktionen, die über die entsprechenden Bereiche in der Registerlasche **Startseite** der Hauptsymbolleiste erstellt worden sind.

Die Tasks-Liste enthält folgende Spalten:

- **Name** – der Unique Task Identifier
- **Typ** – *Backup*, *Recovery* oder *Validierung*
- **Stadium und Fortschritt** – *Untätig* oder *In Arbeit*
- **Letzte Abschlusszeit** – Zeit, die seit der letzten Task-Fertigstellung verstrichen ist.

Derzeit gestoppte Tasks werden als 'Untätig' dargestellt. Für aktuell laufende Tasks nennt das Feld **Stadium und Fortschritt** den Fortschritt der laufenden Aktivität als Prozentangabe (z.B. 35%).

Außerdem werden für alle bereits ausgeführten Tasks die letzten Ergebnisse genannt – Erfolgreich, Warnung oder Fehler. Der Status der letztmaligen Task-Ausführung wird mit einem farbigen Symbol dargestellt – grün für einen erfolgreichen Abschluss, gelb – falls es eine Warnung gab oder rot – wenn ein Fehler auftrat. Für noch nicht ausgeführte Tasks werden weder ein Status angegeben, noch Angaben im Feld **Letzte Abschlusszeit** gemacht.

Durch Klicken auf die Spaltenköpfe können Sie die Tasks-Liste sortieren. Wiederholtes Klicken auf die Spaltenköpfe wechselt zwischen auf- und absteigender Sortierung.

Auf der Seite **Tasks**-Verwaltung können Sie über die entsprechenden Schaltflächen in der Menübandleiste beliebige Tasks aus der Liste **Ausführen**, **Abbrechen**, **Bearbeiten**, **Löschen** oder sich das **Log anzeigen** lassen (*siehe folgende Unterabschnitte*). Die Schaltflächen sind nur aktiv, wenn ein Task in der Liste markiert ist.

Durch Klicken auf einen der Tasks können Sie die **Task**-Details überprüfen. Die Details des gewählten Tasks erscheinen auf der rechten Seite, wo Sie zwischen den Registerlaschen wechseln können, um Informationen über ihn zu erhalten (*siehe Abschnitt 'Task-Details ansehen')* (S. 53)

10.1 Einen Task ausführen

Durch einen Klick auf **Ausführen** im oberen Menüband starten Sie den ausgewählten untätigen Task. Mit Aufnahme der Ausführung ändert sich der 'Untätig'-Status des Tasks und es erscheint ein Fortschrittsbalken.

Beachten Sie, dass Sie dann nur die Task-Logs ansehen (*sieheAbschnitt 'Task-Logs ansehen'* (S. 53)) oder den aktiven Task abbrechen können (*sieheAbschnitt 'Einen Task stoppen'* (S. 53)). Die anderen Schaltflächen – **Ausführen**, **Bearbeiten** und **Löschen** – sind deaktiviert. Um den aktiven Task bearbeiten oder löschen zu können, müssen Sie ihn erst stoppen.

10.2 Einen Task abbrechen

Durch einen Klick auf die Schaltfläche **Abbrechen** im oberen Menüband brechen Sie den ausgewählten aktiven Task ab. Diese Aktion müssen Sie bestätigen. Ist die Bestätigung erfolgt, wird der aktive Task sofort gestoppt und wechselt in den 'untätigen' Zustand.

Die Schaltfläche **Abbrechen** wird für den untätigen Task deaktiviert, weil nur aktuell laufende Tasks abgebrochen werden können.

10.3 Einen Task bearbeiten

Durch einen Klick auf **Bearbeiten** im oberen Menüband können Sie den ausgewählten Task ändern. Je nach Typ des Tasks gelangen Sie in den entsprechenden Teil der Registerlasche **Aktionen** – Backup erstellen, Backup wiederherstellen oder Backup validieren. Hier finden Sie alle Schritte der Assistenten für 'Backup', 'Recovery' oder 'Validierung', die Sie bei der Erstellung des Tasks abgeschlossen haben. Alle über den Assistenten gesetzten Einstellungen sind an dieser Stelle auf einen Blick einzusehen und veränderbar. (*Weitere Informationen finden Sie in den Abschnitten 'Backups von virtuellen Maschinen erstellen' (S. 22), 'Backup virtueller Maschinen wiederherstellen' (S. 34) und 'Backups validieren'* (S. 64)).

10.4 Einen Task löschen

Durch einen Klick auf **Löschen** im oberen Menüband können Sie den ausgewählten Task entfernen. Diese Aktion müssen Sie bestätigen. Ist die Bestätigung erfolgt, wird der Task sofort gelöscht.

10.5 Task-Logs ansehen

Durch einen Klick auf **Log anzeigen** im oberen Menüband können Sie die Logs des ausgewählten Tasks ansehen. Sie gelangen zur Ansicht **Logs** (**Ansicht**->**Logs anzeigen**), wo Sie alle Logs für den aktuellen Task finden (*siehe Abschnitt 'Logs verwalten'* (S. 68)).

10.6 Task-Details ansehen

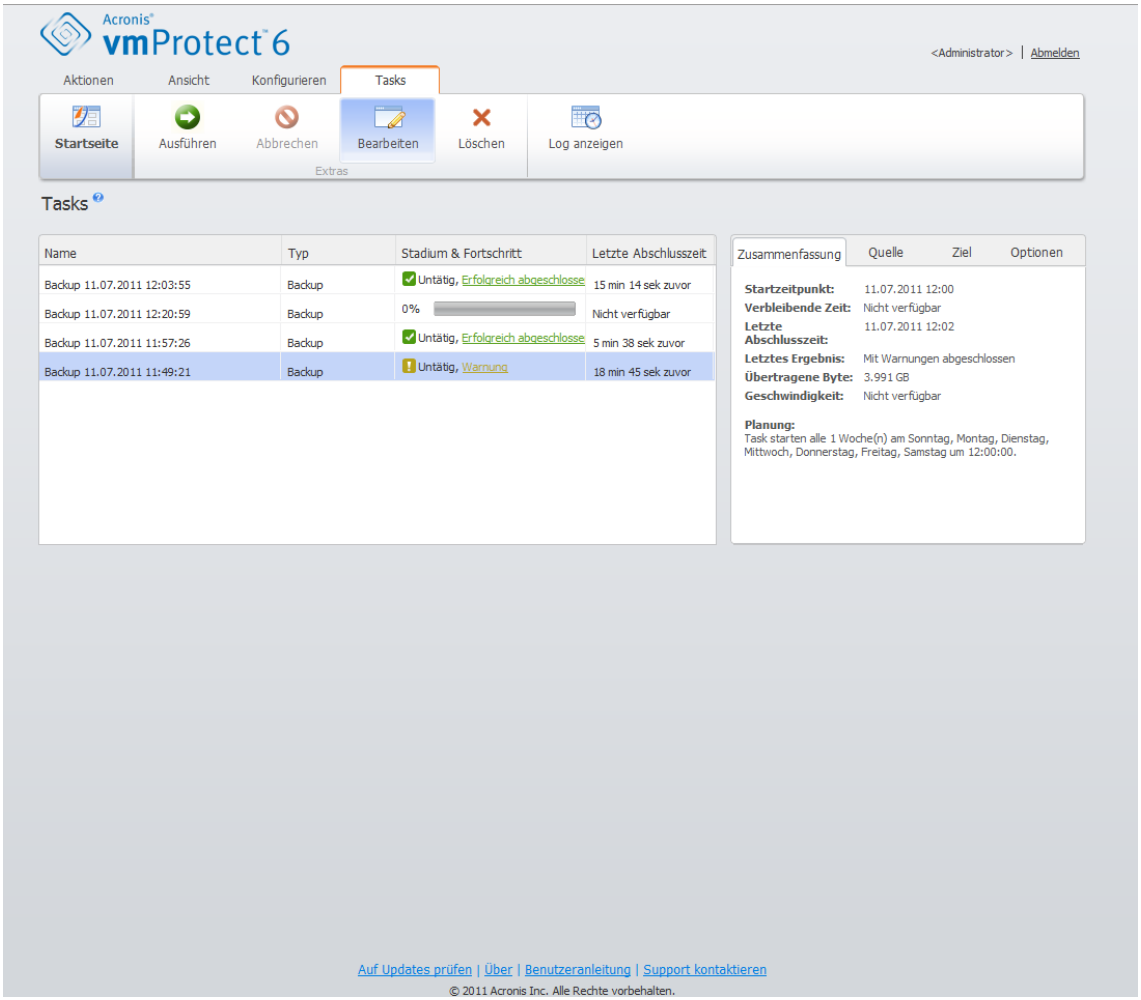
Durch das Auswählen eines Tasks in der Liste können Sie auf der rechten Seite seine Details einsehen. Die Informationen über den aktuell gewählten Task erscheinen in einer Registerlaschenansicht. Es gibt vier Registerlaschen – **Zusammenfassung**, **Quelle**, **Ziel** und **Optionen** (**Zusammenfassung** ist die Standardregisterlasche). Beachten Sie, dass die Registerlaschen je nach Typ des Tasks – Backup, Recovery oder Validierung – variierende Informationen enthalten. Untenstehende Abschnitte beschreiben den Inhalt der Registerlaschen für einen Backup-Task.

10.6.1 Registerkarte 'Zusammenfassung'

Die Registerkarte **Zusammenfassung** gibt eine Übersicht für den aktuell gewählten Task. Hier ist ein Beispiel für den möglichen Inhalt der Registerkarte **Zusammenfassung** bei einem Backup-Task:

Startzeitpunkt: 12:00 03/04/2011
Verbleibende Zeit: 30 Minuten
Letzte Abschlusszeit: N/A
Letztes Ergebnis: N/A
Übermittelte Byte: 150 MB

Geschwindigkeit: 20 MB/Sek.
Planung: Starte den Task jede Stunde Montags und Dienstags



Tasks verwalten, Task-Details ansehen, Registerkarte 'Zusammenfassung'

10.6.2 Registerlasche 'Quelle'

Die Registerlasche **Quelle** enthält den Baum mit den im Backup-Task enthaltenen ESX-Hosts und vApps bzw. VMs. Dieser Baum ist dynamisch. Ist ein gesamter ESX-Host für das Backup vorgesehen, wird der Baum für den aktuellen Status der Maschinen angezeigt (in derselben Liste), so wie bei VMware IC. Rechts vom ESX-Host ist gekennzeichnet, dass die gesamte Gruppe gesichert wird (Markierung 'Alle virtuellen Maschinen'). Hier ist ein Beispiel für den möglichen Inhalt der Registerlasche **Quelle**:

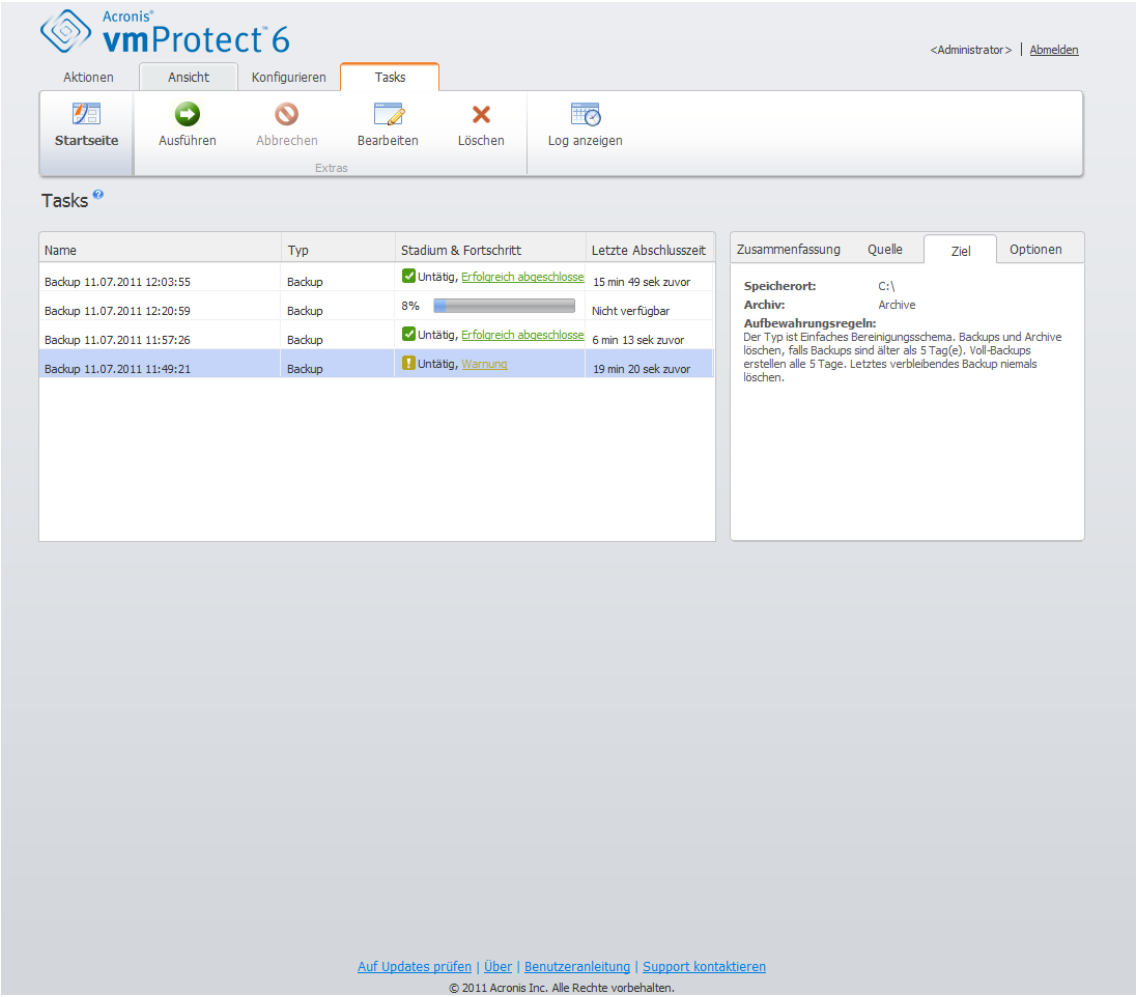
ESX Host 1 'Alle virtuellen Maschinen':
Small_vm

ESX-Host 2:
AcronisESXAppliance (10.250.40.30)

10.6.3 Registerkarte 'Ziel'

Die **Registerkarte Ziel gibt Informationen über den Speicherort des gesicherten Archivs. Hier ist ein Beispiel für den möglichen Inhalt der Registerkarte Ziel:**

Speicherort: \\NAS1\Backups\AcronisESX_Appliance_1557\azz11006765454cv\
Archiv: Archivname
Aufbewahrungsregeln: Lösche Backups, die älter als 30 Tage sind / Behalte nur die letzten 30 Backups

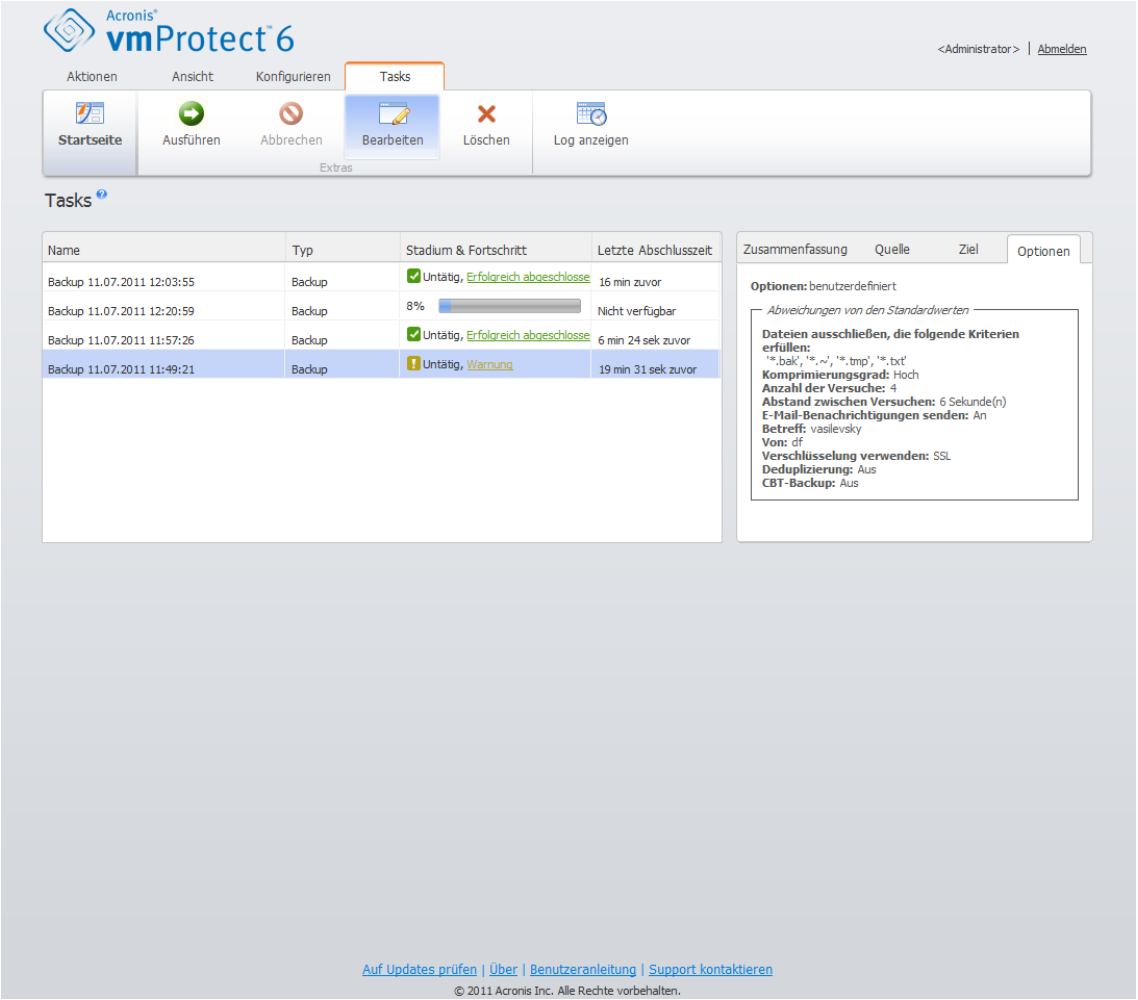


Tasks verwalten, Task-Details ansehen, Registerkarte 'Ziel'

10.6.4 Die Registerkarte 'Optionen'

Die Registerkarte **Optionen** nennt die Einstellungen für den aktuell gewählten Task. Diese Registerkarte zeigt nur die Optionen, die sich von den standardmäßig voreingestellten unterscheiden. Entsprechen alle Task-Optionen dem Standard, meldet diese Registerkarte lediglich 'Standardoptionen', ohne spezifische Werte anzugeben. Hier ist ein Beispiel für den möglichen Inhalt der Registerkarte **Optionen**:

Komprimierungsgrad: Maximum
Erneut versuchen, wenn ein Fehler auftritt: Aus
Nach Backup validieren: An
E-Mail-Benachrichtigungen: An
Typ der zu übermittelnden Ereignisse: Fehler



Tasks verwalten, Task-Details ansehen, Registerkarte 'Optionen'

11 Recovery-Punkte verwalten

Klicken Sie im Hauptmenü in der Registerkarte **Ansicht** auf **Recovery-Punkte**, um zur Seite **Recovery-Punkte** zu gelangen.

Die Ansicht **Recovery-Punkte** von Acronis vmProtect bietet eine Schnittstelle für die Verwaltung der für die virtuellen Maschinen verfügbaren Recovery-Punkte, d.h. die Zeitpunkte, auf die Sie die einzelnen Maschinen zurücksetzen können. Nach jedem erfolgreich abgeschlossenen Backup-Task wird ein neuer Recovery-Punkt erstellt und die Liste der Recovery-Punkte automatisch aktualisiert.

Nach Auswahl eines Recovery-Punktes können Sie mit ihm Basis-Aktionen durchführen. Durch Klicken auf die entsprechenden Schaltflächen in der Hauptsymbolleiste werden Aktionen für den ausgewählten Recovery-Punkt ausgeführt. Alle nachfolgend beschriebenen Aktionen werden durch einen Assistenten gesteuert und ermöglichen eine einfache Ausführung der gewünschten Tasks.

Die Ansicht **Recovery-Punkte** enthält drei Hauptbereiche:

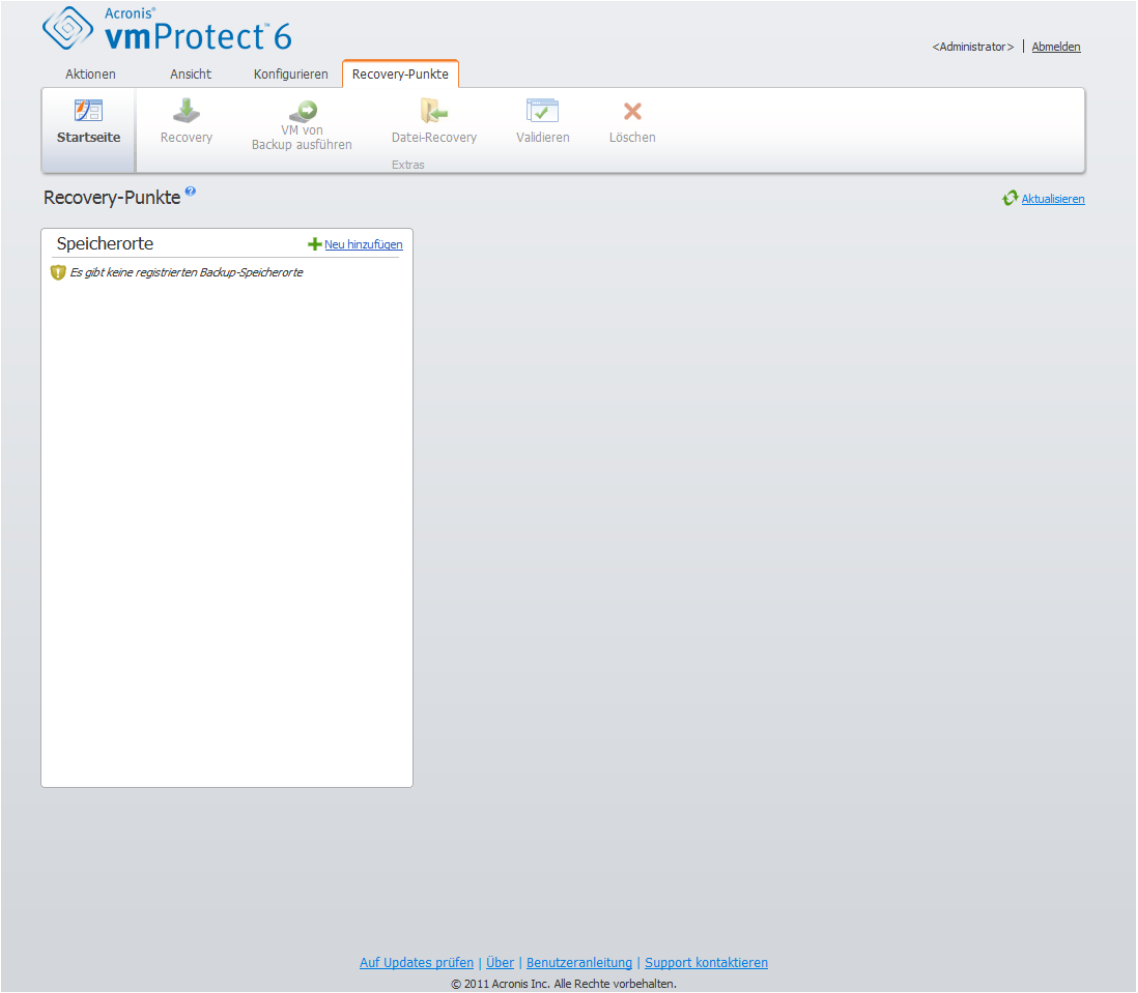
- die Backup-Speicherorte
- den Katalog virtueller Maschinen und
- die Liste der Recovery-Punkte.

An dieser Stelle geht es vor allem darum, (auf der linken Seite) den Backup-Speicherort festzulegen, der anschließend nach vorhandenen Archiven und deren Inhalt durchsucht wird. Die Suche ergibt (in der Mitte der Seite) einen Verzeichnisbaum der virtuellen Maschinen aller in dem gewählten Speicherort vorhandenen Archive. Wenn Sie in diesem Bereich auf eine beliebige virtuelle Maschine klicken, können Sie sich die verfügbaren Recovery-Punkte und Kurzinformationen für diese Maschine anzeigen lassen. Die entsprechende Liste erscheint auf der rechten Seite.

Die Liste der **Speicherorte** auf der linken Seite zeigt die registrierten Backup-Speicherorte (alle Speicherorte, die zuvor bereits als Backup-Ziel oder Recovery-Quelle verwendet wurden). Die Liste der **Speicherorte** enthält, für jeden Speicherort in einem separaten Block, die folgenden Elemente:

- **Speicherort**-Pfad, z.B. \\NAS1\Backups\Acronis\Recent\
- **Speicherort**-Statistiken:
  - **Größe der Backups**: z.B. 3,242 GB (22%)
  - **Belegter Speicherplatz**: z.B. 5,242 GB (36%)
  - **Freier Speicherplatz**: z.B. 9,412 GB (64%)
  - **Gesamter Speicherplatz** (**Belegter Speicherplatz** + **Freier Speicherplatz**): z.B. 14,654 GB.
- **Backups gesamt** (d.h. die Gesamtzahl der Recovery-Punkte am Speicherort)
- Die Schaltfläche **Anmeldedaten bearbeiten** ermöglicht das Ändern der Zugangsdaten zum Speicherort (bei Bedarf)
- Die Schaltfläche **Speicherort entfernen**, die den Speicherort aus der Liste der registrierten Speicherorte entfernt

Solange keine Speicherorte vorhanden sind, zeigt das Widget ein leeres Feld mit folgendem Text: 'Keine registrierten Backup-Speicherorte vorhanden'. Die beiden anderen Bereiche werden gar nicht angezeigt.



Recovery-Punkte verwalten, 'Keine Speicherorte verfügbar'

11.1 Einen Backup-Speicherort hinzufügen

Sie können Backup-Speicherorte direkt aus der Liste **Speicherorte** entfernen oder ihr hinzufügen. Klicken Sie auf die obige Schaltfläche **Neu hinzufügen**, um das Fenster 'Speicherort hinzufügen' zu öffnen.

Beachten Sie, dass die Aktion 'Entfernen' Archive nicht physikalisch vom Speicherort entfernt, sondern nur den Speicherort aus der Acronis vmProtect-Konfiguration löscht. Alle Backups im Speicherort bleiben intakt und sind sichtbar, wenn Sie diesen mit der entsprechenden Schaltfläche wieder **Hinzufügen**. Das Entfernen oder Hinzufügen von Speicherorten ist von Vorteil, wenn Sie überflüssige Backup-Speicherorte haben, die nicht länger aktuell sind und die Sie deshalb nicht sehen möchten.

Die linke Seite des Fensters 'Speicherort hinzufügen' zeigt folgende Listen:

- Online Backup-Storages
- Lokale Ordner
- Netzwerkordner
- FTP-Server
- SFTP-Server

Den gewünschten Speicherort können Sie nach Aufklappen der entsprechenden Ordnergruppe im Baum oder durch Eingabe seines vollständigen Pfads im Feld **Speicherort** auswählen.

Wählen Sie einen Typ der Backup-Speicherorte aus dem Baum auf der linken Seite. Falls der gewählte Speicherort (Online Backup-Storage, Netzwerkordner oder FTP- bzw. SFTP-Server) eine Authentifizierung erfordert, erscheint zunächst im rechten Bereich das Dialogfenster zur Eingabe der Anmeldedaten. Nach dem Anmelden zeigt dieser Bereich den Inhalt des ausgewählten Speicherorts an, d.h. die hier vorhandenen Archive.

Alternativ zum Suchen des Speicherorts im Baum können Sie seinen Pfad im entsprechenden Feld **Speicherort** eingeben und diesen Speicherort mit einem Klick auf **Go** durchsuchen. Auch hier erscheint im rechten Bereich dasselbe Dialogfenster, das zur Authentifizierung nach Login und Kennwort fragt.

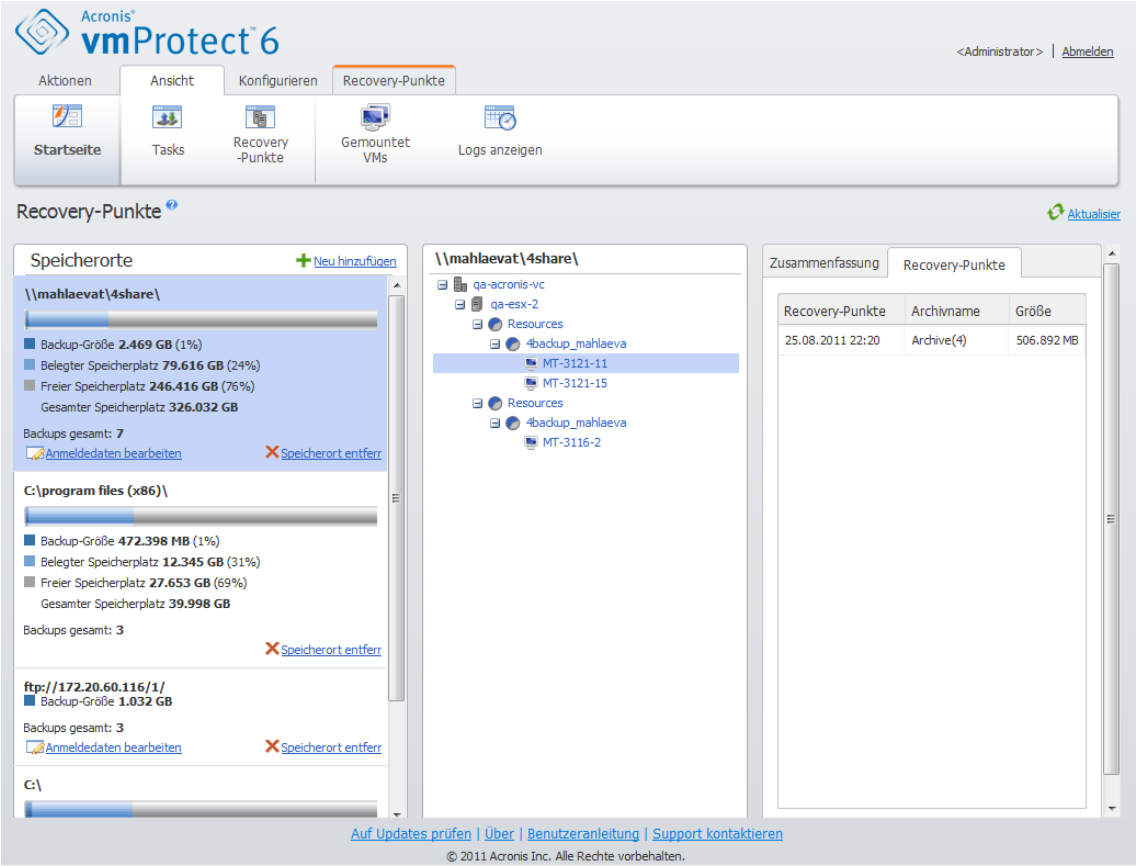
Um den Assistenten abzuschließen, wählen Sie im Feld **Speicherort** den Speicherort aus oder geben seinen Pfad ein und klicken dann auf **OK**. Die Schaltfläche **OK** bleibt ausgegraut, bis ein gültiger Speicherort ausgewählt ist.

11.2 Der Katalog 'Virtuelle Maschinen'

Der mittlere Bereich in der Ansicht **Recovery-Punkte** zeigt den Katalog 'Virtuelle Maschinen'. Der Verzeichnisbaum der virtuellen Maschinen und vApps baut darauf auf, was beim Parsing der Archive des auf der linken Seite gewählten Speicherorts gefunden wurde.

Falls dieser Speicherort kennwortgeschützte Archive oder Archive von physikalischen Maschinen enthält, erscheint im mittleren Bereich der Liste virtueller Maschinen folgende Warnung:

Warnung: Der ausgewählte Speicherort enthält kennwortgeschützte Archive oder Archive von physikalischen Maschinen. Der Inhalt solcher Archive ist in der Liste virtueller Maschinen nicht enthalten.



Recovery-Punkte verwalten, 'Kennwortgeschützter Speicherort'

In dieser Liste kann zu einem Zeitpunkt nur eine virtuelle Maschine ausgewählt sein. Das Fenster 'Details' (auf der rechten Seite) für die ausgewählte virtuelle Maschine enthält die nachfolgend erläuterten zwei Registerkarten – **Recovery-Punkte**-Liste und **Recovery-Punkte**-Details.

11.3 Liste der Recovery-Punkte

Die Liste der **Recovery-Punkte** im Bereich 'Details' listet alle verfügbaren Recovery-Punkte in folgenden Spalten auf:

- **Recovery-Punkte**: Die Spalte zeigt Datum und Zeit der Erstellung jedes Recovery-Punktes in der Liste.
- **Archivname**: zeigt den Archivnamen (im ausgewählten Speicherort), zu dem dieser Recovery-Punkt gehört.
- **Größe**: zeigt die physikalische Größe des Archivs (in MB oder GB), zu dem dieser Recovery-Punkt gehört.

Von der Liste der **Recovery-Punkte** können Sie zur Ansicht **Zusammenfassung** wechseln (siehe Abschnitt Registerlasche 'Zusammenfassung' (S. 61)).

Nach Auswahl eines bestimmten Recovery-Punktes in der Liste, können Sie alle im Abschnitt 'Aktionen mit ausgewählten Elementen' (S. 61) beschriebenen Aktionen durchführen.

11.4 Registerlasche 'Zusammenfassung'

Wenn Sie in die Registerlasche **Zusammenfassung** wechseln, sehen Sie die Informationen über den ausgewählten Recovery-Punkt im Überblick. Die Registerlasche zeigt folgenden Informationen:

- **VM-Kommentare** (vom VMware vSphere Client übernommen, aus der Registerlasche **Zusammenfassung** für die ausgewählte VM)
- **Gast-Betriebssystem** (vom VMware vSphere Client übernommen, aus der Registerlasche **Zusammenfassung** für die ausgewählte VM)
- **VM-Version** (vom VMware vSphere Client übernommen, aus der Registerlasche **Zusammenfassung** für die ausgewählte VM)
- **Bereitgestellter Storage** (vom VMware vSphere Client übernommen, aus der Registerlasche **Zusammenfassung** für die ausgewählte VM)
- **Verwendeter Storage** (vom VMware vSphere Client übernommen, aus der Registerlasche **Zusammenfassung** für die ausgewählte VM)
- **Gesamtanzahl bzw. -größe aller Recovery-Punkte**, zum Beispiel 23 Punkte bzw. 120 GB

11.5 Aktionen mit ausgewählten Elementen

Die Ansicht **Recovery-Punkte** bietet im Menüband folgende Schaltflächen, die Basis-Aktionen mit dem ausgewählten Recovery-Punkt ermöglichen:

- **Recovery**
- **VM von Backup ausführen**
- **Datei-Recovery** (Download von Gast-Dateien)
- **Validieren**
- **Löschen**.

Diese Aktionen sind verfügbar, wenn ein bestimmter Recovery-Punkt in der Liste ausgewählt ist (im Bereich 'Details' für die ausgewählte virtuelle Maschine, wie im Abschnitt 'Liste der Recovery-Punkte' (S. 60) beschrieben).

11.5.1 Recovery

Durch einen Klick auf **Recovery** im Menüband stellen Sie den ausgewählten Recovery-Punkt unter Verwendung des 'Recovery-Task'-Assistenten wieder her. Im Assistenten sind die im Abschnitt 'Backup virtueller Maschinen wiederherstellen' (S. 34) beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

11.5.2 VM von Backup ausführen

Durch einen Klick auf **VM von Backup ausführen** im Menüband aktivieren Sie den Assistenten 'VM von Backup ausführen' für das Mounten der virtuellen Maschine. Im Assistenten sind die im Abschnitt 'VM von Backup ausführen' (S. 46) beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

11.5.3 Datei-Recovery

Durch einen Klick auf **Datei-Recovery** im Menüband aktivieren Sie den 'Datei-Recovery'-Assistenten, um den Download der Gast-Dateien durchzuführen. Im Assistenten sind die im Abschnitt 'Datei-

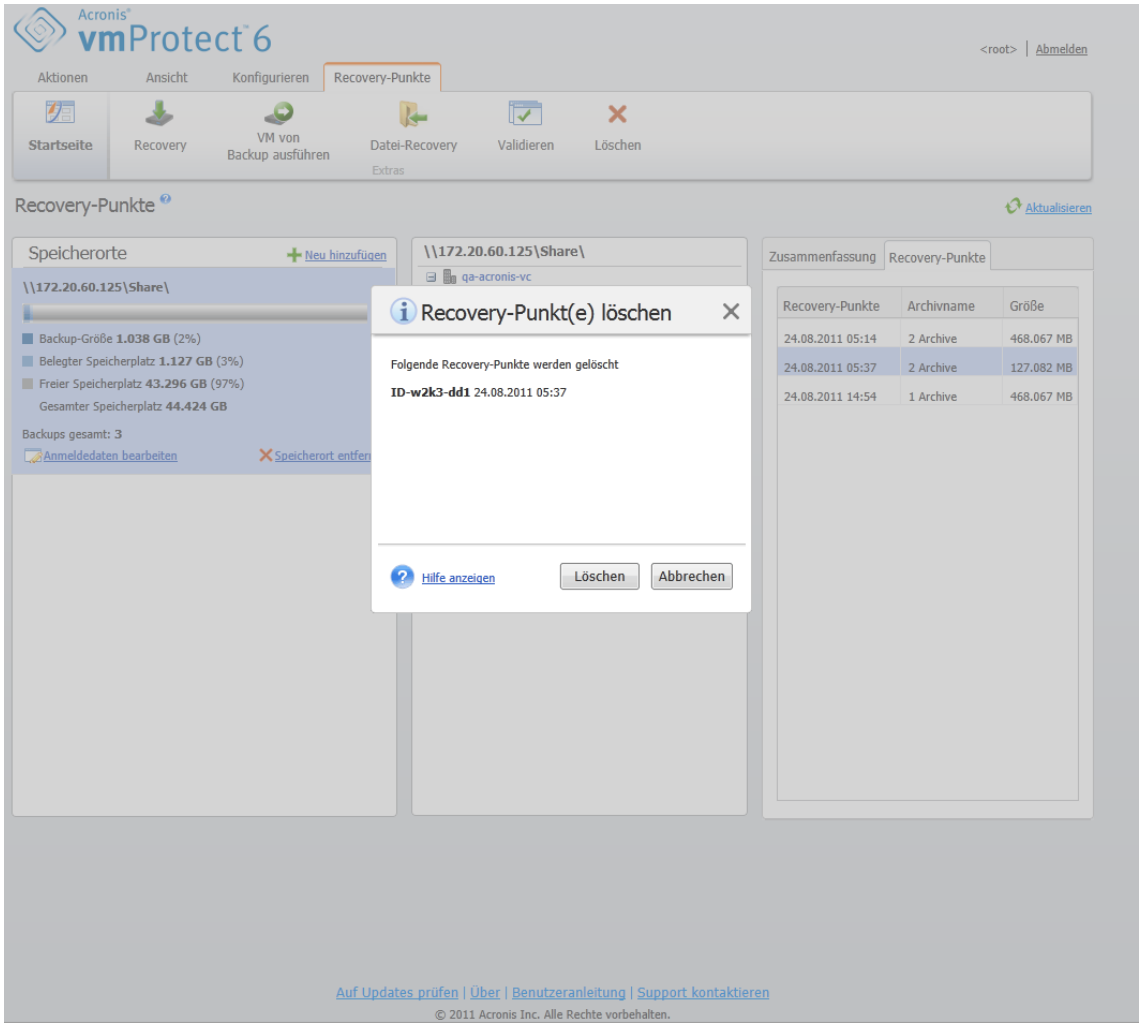
Recovery' (S. 42) beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

11.5.4 Validieren

Durch einen Klick auf **Validieren** im Menüband führen Sie die Backup-Validierung mit dem neuen Validierungstask durch. Im 'Validierungs'-Assistenten sind die im Abschnitt 'Backups validieren' (S. 64) beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

11.5.5 Löschen

Klicken Sie auf **Löschen** im Menüband, um den ausgewählten Recovery-Punkt zu entfernen. Das Fenster **Recovery-Punkt(e) löschen** erscheint und zeigt die Liste mit den zum Löschen markierten Recovery-Punkten.



Recovery-Punkte verwalten, Fenster 'Recovery-Punkte löschen'

Beachten Sie, dass in einem Archiv mit Legacy-Modus (S. 7) einige Recovery-Punkte Abhängigkeiten haben können. Damit ist das Löschen eines einzelnen Recovery-Punktes nicht möglich. In diesem Fall wird die Löschung der gesamten Kette von Recovery-Punkten vorgesehen, die von dem ausgewählten abhängen. Die Recovery-Punkte, die zu einem 'nur inkrementellen' Archiv (S. 8) gehören, können ohne Einschränkung gelöscht werden; die Liste der zu löschenden Elemente enthält den einzelnen Recovery-Punkt.

Nach Bestätigung der Aktion durch das Klicken auf **Löschen**, erscheint der Lösch-Task in der Ansicht **Tasks**. Nach seiner Beendigung verschwindet der Task. Das Ergebnis ist in der Ansicht **Dashboard** und in der Log-Datei zu sehen.

12 Andere Aktionen

12.1 Backups validieren (Aktionen -> Validieren)

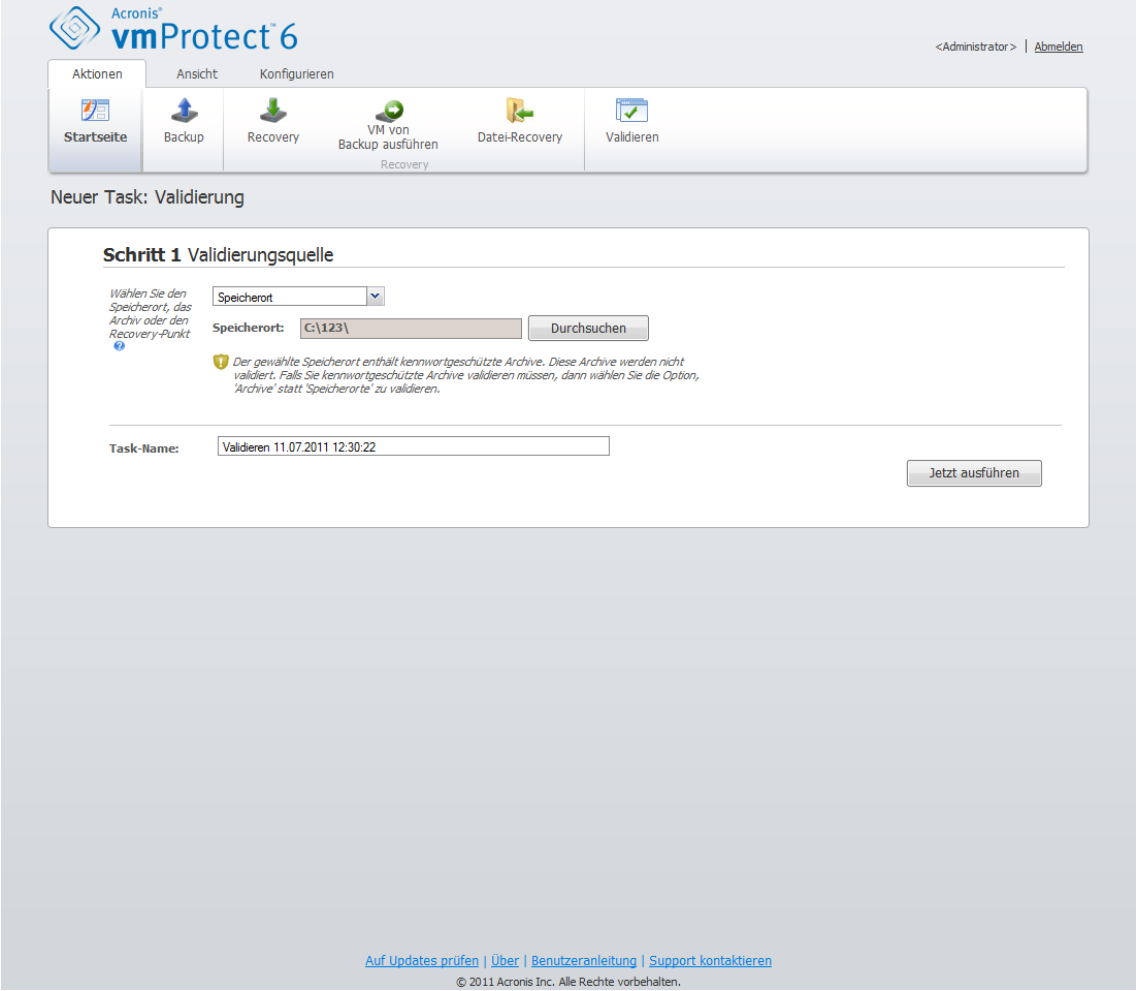
Die Validierung überprüft die Möglichkeit der Datenwiederherstellung aus einem Backup. Beachten Sie, dass eine erfolgreiche Validierung zwar eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, aber nicht alle Faktoren geprüft werden, die eine Wiederherstellung beeinflussen. Wenn Sie ein Betriebssystem sichern, kann nur eine probeweise durchgeführte Wiederherstellung zu einer neuen virtuellen Maschine den Erfolg der Wiederherstellung garantieren.

Mit Acronis vmProtect können Sie einen **Speicherort**, ein **Archiv** oder einen **Recovery-Punkt** validieren. Die Validierung eines Recovery-Punktes imitiert die Wiederherstellung aller Dateien eines Backups an einem Blindziel. Die Validierung eines Archivs überprüft alle Recovery-Punkte in diesem Archiv. Die Validierung eines Speicherorts überprüft die Wiederherstellung aller in diesem Speicherort gesicherten Archive.

12.1.1 Validierungsquelle

Zunächst bestimmen Sie aus drei verfügbaren Optionen den zu validierenden Elementtyp: **Speicherort**, **Archiv** oder **Recovery-Punkt**.

Speicherort – Die Validierung eines Speicherorts überprüft die Integrität aller dort befindlichen Archive. Beachten Sie, dass dies normalerweise mehr Zeit in Anspruch nimmt als die granulare Validierung spezifischer Archive oder Recovery-Punkte (vor allem, wenn sich mehrere Archive an diesem Speicherort befinden). Die Dauer der Validierung ist zudem von der Anzahl der Backups (Recovery-Punkte) in den einzelnen Archiven des gewählten Speicherorts abhängig. Beachten Sie, dass kennwortgeschützte Archive in diesem Fall nicht validiert werden. Dazu wählen Sie die Option 'Archive validieren'.



Task 'Backup-validieren'. Validierungsquelle. Speicherort

Archiv – Die Validierung eines Archivs überprüft die Integrität aller Backups (Recovery-Punkte) in dem spezifizierten Archiv. Im Allgemeinen ist diese Prozedur schneller als das Validieren des gesamten Speicherorts. Trotzdem ist es langsamer als das Validieren eines spezifischen Recovery-Punktes im Archiv.

Recovery-Punkt – Um sicherzustellen, dass Sie auf spezifische Recovery-Punkte zurücksetzen können, führen Sie eine granulare Validierung für genau diese Recovery-Punkte durch (sie müssen sich nicht im selben Archiv befinden).

Nach Auswahl des zu validierenden Elementtyps, bestimmen Sie den Backup-Speicherort. Sie können entweder einen Speicherort spezifizieren oder einen Speicherort und ein Archiv, um die Liste der Recovery-Punkte abzurufen. Wenn Sie einen Recovery-Punkt validieren, werden das ausgewählte Archiv oder der Speicherort nach dort vorhandenen Recovery-Punkten durchsucht. Das ist erforderlich, um den oder die Recovery-Punkte zu erfassen, die validiert werden sollen. Je nach dem für die Validierung gewählten Elementtyp bleiben einige Schaltflächen deaktiviert (zum Beispiel ist die Liste der Recovery-Punkte nicht zu sehen, wenn Sie einen Speicherort oder ein Archiv validieren).

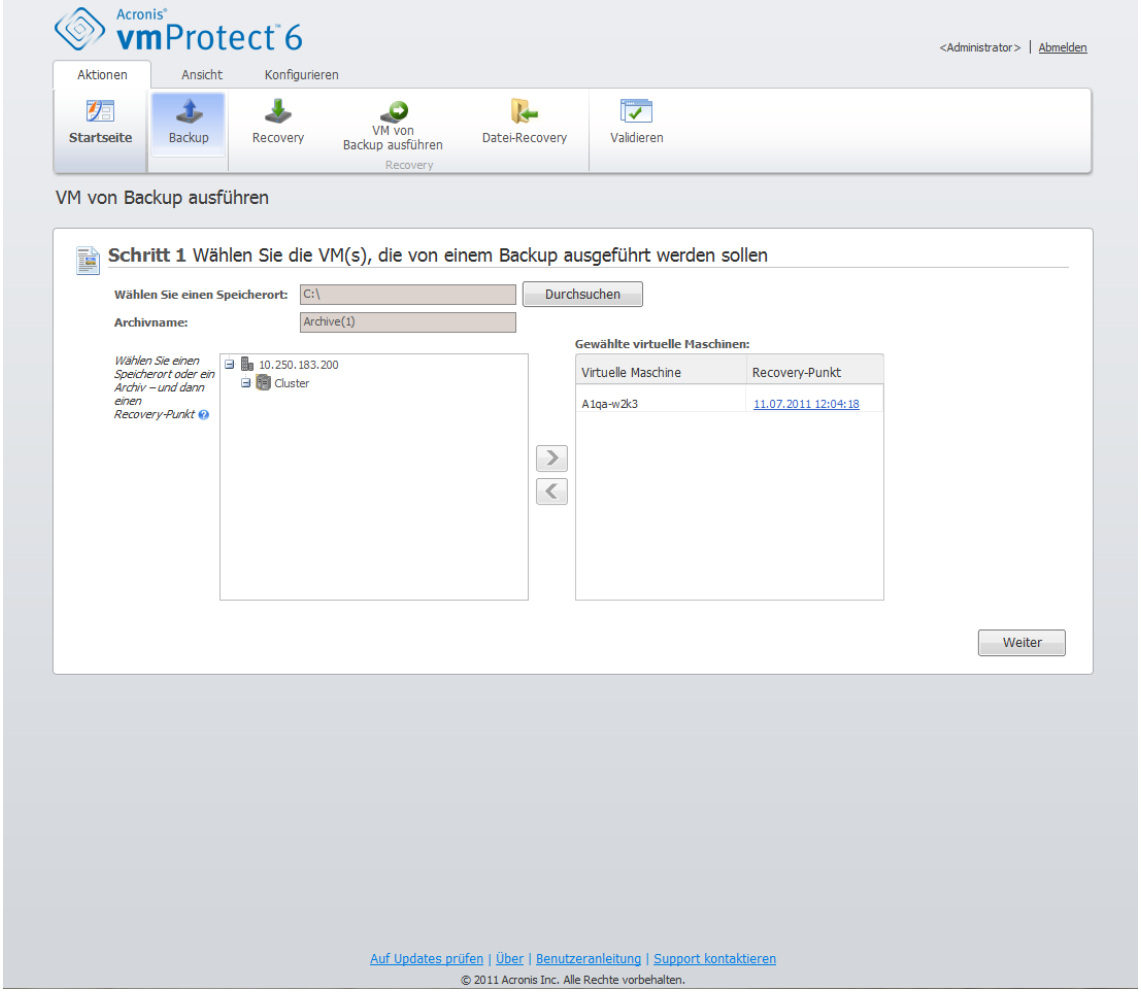
Den Speicherort bzw. das Archiv wählen Sie über die Schaltfläche **Durchsuchen**. Es öffnet sich ein Fenster mit den Optionen zum Durchsuchen, in dem Sie den Pfad bzw. den Archivnamen festlegen können.

Die Suche ergibt (unter dem Listenfeld für die Auswahl des Speicherorts) einen Baum der virtuellen Maschinen aller in dem gewählten Speicherort vorhandenen Archive (oder im Archiv selbst, wenn Sie

dieses direkt spezifiziert haben). Sie können jede dieser virtuellen Maschinen auswählen und in den Bereich 'Ausgewählte Virtuelle Maschinen' verschieben.

Im Bereich 'Ausgewählte virtuelle Maschinen' finden Sie eine Liste mit den ausgewählten virtuellen Maschinen sowie deren verfügbaren Recovery-Punkten (d.h. die Zeitpunkte, die einen bestimmten Zustand der Maschine enthalten). Durch Anklicken wählen Sie einen Recovery-Punkt aus.

Um den 'Validierungstask-erstellen'-Assistenten abzuschließen, müssen Sie einen Namen für den Task vergeben. Beachten Sie, dass die Zeichen [ ] { } ; . im Task-Namen nicht erlaubt sind.



Task 'Backup-validieren'. Validierungsquelle. Recovery-Punkt.

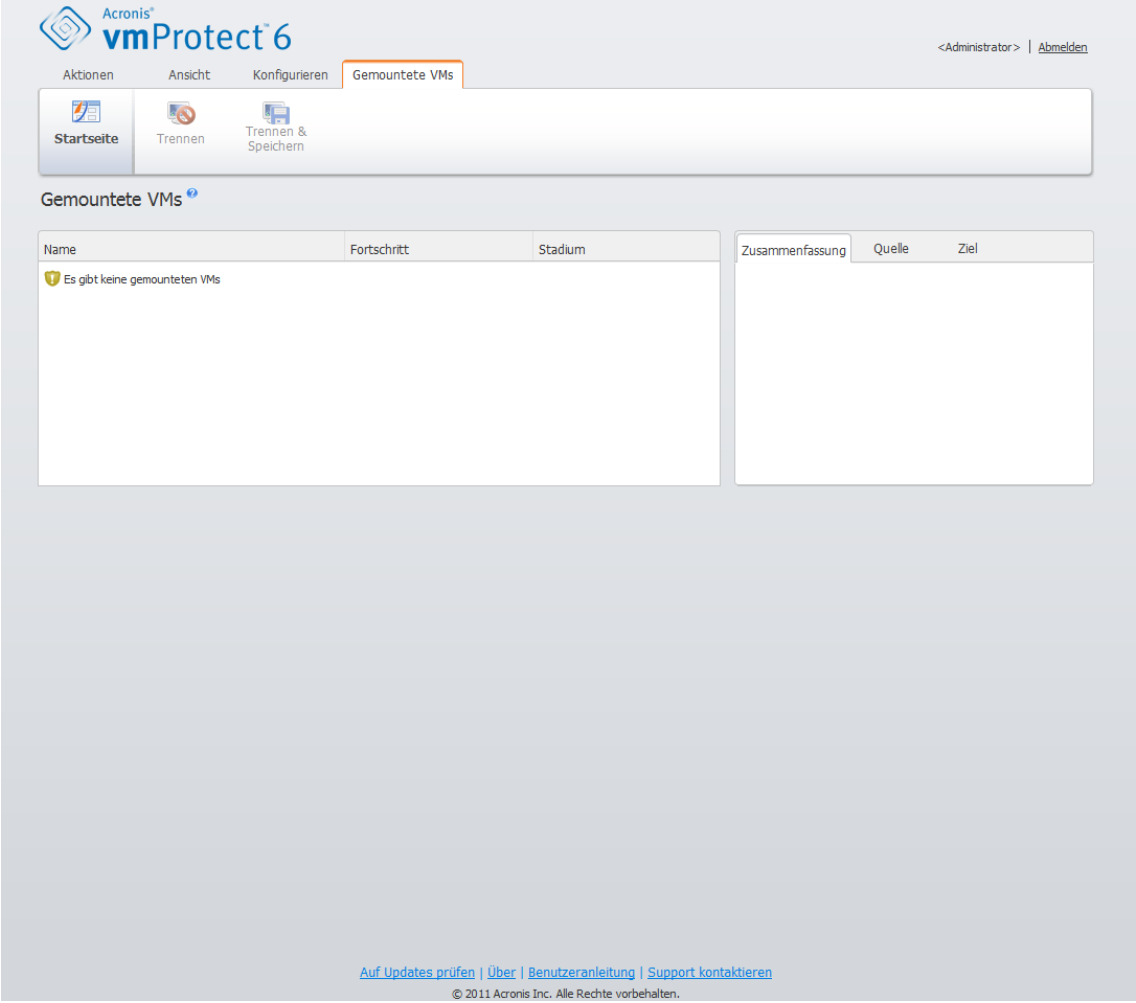
Wenn Sie auf **Jetzt ausführen** klicken, werden die ausgewählten Elemente validiert und der Fortschritt des neu erstellten Validierungstasks in der Ansicht **Tasks** angezeigt. Sein Ergebnis erscheint in den Ansichten **Dashboard** und **Logs anzeigen**.

12.2 Gemountete VMs verwalten (Ansicht->Gemountete VMs)

Klicken Sie in der Registerlasche **Ansicht** im Hauptmenüband von Acronis vmProtect auf **Gemountete VMs**, um die Seite **Gemountete VMs** zu öffnen.

12.2.1 Liste 'Gemountete VMs'

Die Ansicht **Gemountete VMs** gibt einen Überblick über die virtuellen Maschinen die gegenwärtig gemountet sind oder von Backup auf einem ESX-Host ausgeführt werden.



Ansicht 'Gemountete VMs'

Solange keine virtuelle Maschine ausgeführt wird, bleibt die Liste der gemounteten VMs leer. Nach Abschluss der Aktion **VM von Backup ausführen** (siehe Abschnitt 'VM von Backup ausführen' (S. 46)), öffnet sich die Ansicht 'Gemountete VMs' automatisch und zeigt die gerade gelaufenen Maschinen an.

In der Tabelle können Sie die Liste dieser Maschinen und ihren Zustand einsehen: 'Ausführung' (wenn die Maschine läuft) oder 'Gestoppt' (wenn nicht).

12.2.2 Details der gemounteten VMs

Sie können die Details von jeder der gemounteten virtuellen Maschinen prüfen, indem Sie sie in der Liste markieren. Die Details der gewählten virtuellen Maschine erscheinen auf der rechten Seite, wo Sie zwischen den Registerlaschen wechseln können, um zusätzliche Details zu prüfen.

Nach dem Auswählen einer der virtuellen Maschinen in der Liste können Sie auf der rechten Seite ihre Details einsehen. Die Informationen über den aktuell gewählten Task erscheinen in einer

Registerlaschenansicht. Es gibt drei Registerlaschen – 'Zusammenfassung', 'Quelle' und 'Ziel' ('Zusammenfassung' ist die Standardregisterlasche).

Die erste Registerlasche **Zusammenfassung** gibt einen Überblick über alle Details der aktuell gewählten virtuellen Maschine. Hier ein Beispiel für den möglichen Inhalt der Registerlasche **Zusammenfassung**:

Startzeit/ -datum: 20:11 11/05/2011

Die Registerlasche **Quelle** zeigt den Baum der gemounteten ESX-Hosts sowie vApps und VMs. Hier ein Beispiel für den Inhalt der Registerlasche **Quelle**:

Speicherort: \\Backups\
Archiv: Archivname

ESX Host 1 (10.250.40.30) 'Alle virtuellen Maschinen':
Small_vm

Die Registerlasche **Ziel** gibt Informationen über den Speicherort, auf dem die gewählte VM ausgeführt wird. Hier ein Beispiel für den Inhalt der Registerlasche **Ziel**:

ESX Host 1 (10.250.40.30) 'Alle virtuellen Maschinen':
Small_vm

12.2.3 VMs trennen

Die kontextabhängige Symbolleiste in der Ansicht Gemountete VMs hat zwei Schaltflächen, Trennen und **Trennen und Speichern**.

Nachdem Sie eine virtuelle Maschine in der Liste 'Gemountete VMs' ausgewählt haben, können Sie sie trennen (d.h., sie nicht mehr vom Backup ausführen); klicken Sie dazu auf die Schaltfläche **Trennen**.

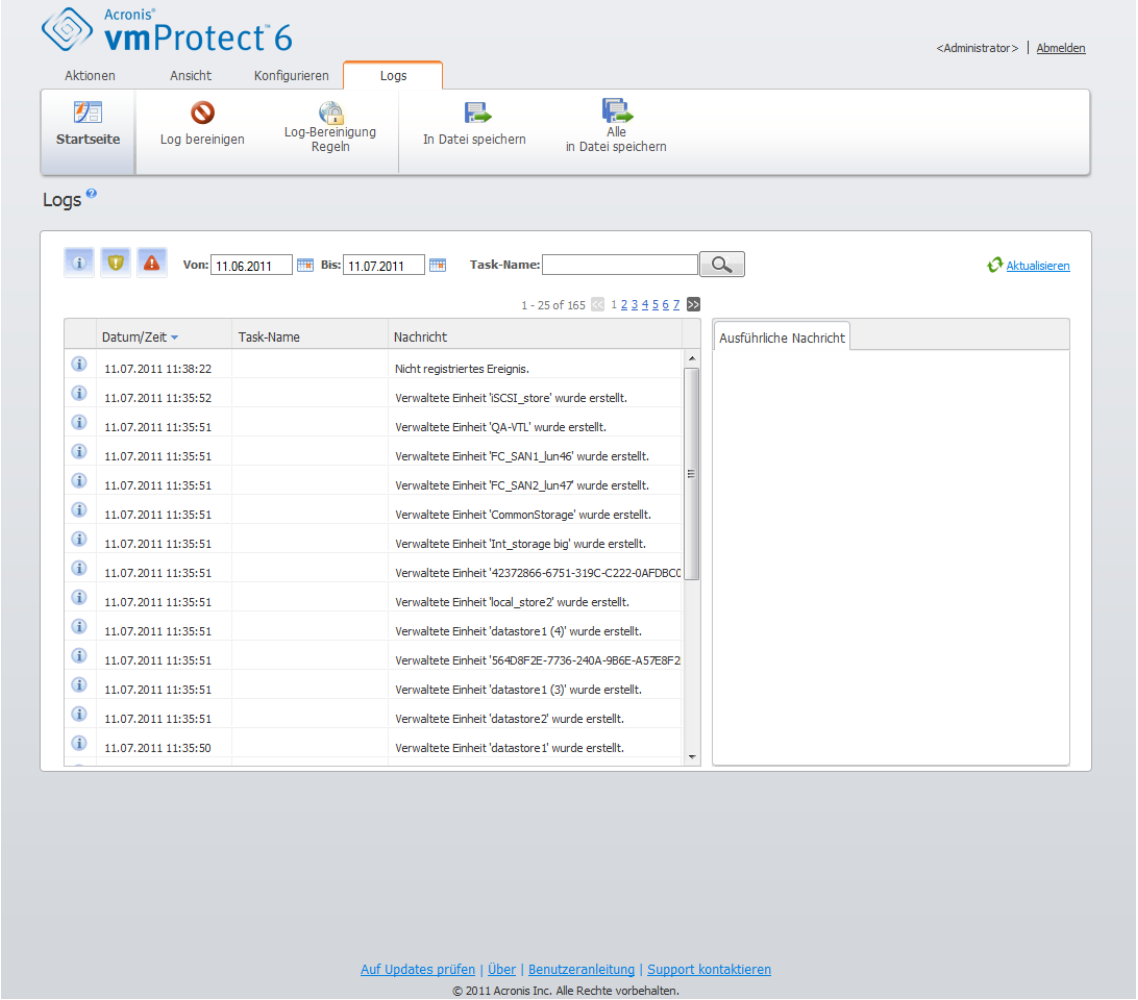
Durch die Aktion **Trennen und Speichern** wird die Maschine nicht mehr vom Backup ausgeführt und alle an der Maschine vorgenommenen Änderungen werden ins Archiv aufgenommen, wodurch ein neuer Recovery-Punkt hinzugefügt wird.

12.3 Logs verwalten (Ansicht -> Logs anzeigen)

Klicken Sie in der Registerlasche **Ansicht** im Hauptmenüband von Acronis vmProtect auf **Logs anzeigen**, um die Seite **Logs** zu öffnen.

12.3.1 Liste der Logs

Die Ansicht **Logs anzeigen** enthält eine Liste aller Ereignisse auf dem Acronis vmProtect-Agenten. Dazu gehören Backups, Recovery, Ausführen der VM von einem Backup usw. sowie Task- und Systemmeldungen, beispielsweise das Herstellen einer Verbindung zu verwalteten ESX-Hosts bzw. vCenters.



Liste der Logs

Die Log-Liste enthält die Spalten **Datum bzw.Zeit**, **Task-Name** und **Meldung**. Durch Klicken auf die Spaltenköpfe können Sie die Log-Liste sortieren. Wiederholtes Klicken auf die Spaltenköpfe wechselt zwischen auf- und absteigender Sortierung.

Außerdem können Sie die Log-Ereignisse anhand verschiedener Filter, die sich oberhalb der Liste befinden, sortieren.

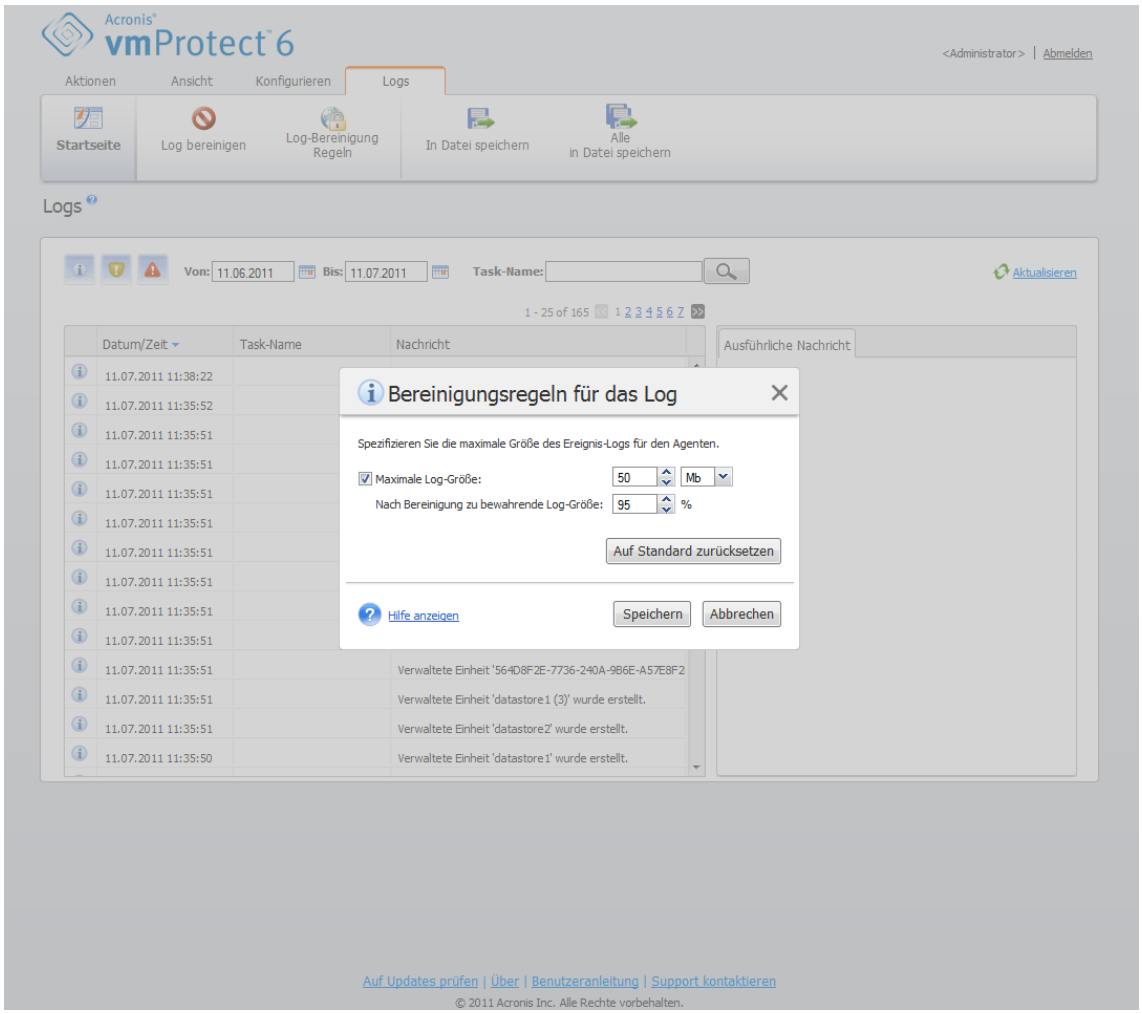
- Ereignis-Flags (Erfolg, Warnung oder Fehler)
- Datum/Zeit
- Task-Name

Das Anklicken eines Log-Ereignisses in der Liste öffnet eine detaillierte Meldung für dieses Log im rechten Fenster.

Über die kontextabhängige Symbolleiste können Sie die Log-Ereignisse bereinigen oder automatisierte Bereinigungsregeln festlegen, um die Größe der Logs in bestimmten Grenzen zu halten. Diese Aktionen sind in den folgenden Unterabschnitten beschrieben.

12.3.2 Log-Bereinigungsregeln

Klicken Sie auf **Log-Bereinigungsregeln** in der Hauptsymbolleiste, um die Regeln für die Aufbewahrung der Log-Einträge festzulegen. Diese Option spezifiziert also, wie das Log des Acronis vmProtect-Agenten bereinigt wird.



Log-Bereinigungsregeln

Um die Option **Log-Bereinigungsregeln** zu nutzen, aktivieren Sie das Kontrollkästchen. Definieren Sie dann die maximale Größe des Log-Ordners für den Agenten (unter Windows XP/2003 Server z.B. %ALLUSERSPROFILE%\Anwendungsdaten\Acronis\ABR10\MMS\LogEvents).

Sie können die **Maximale Log-Größe** und die Anzahl der Log-Einträge, die Sie behalten wollen, definieren.

Die Standardwerte für **Log-Bereinigungsregeln** sind:

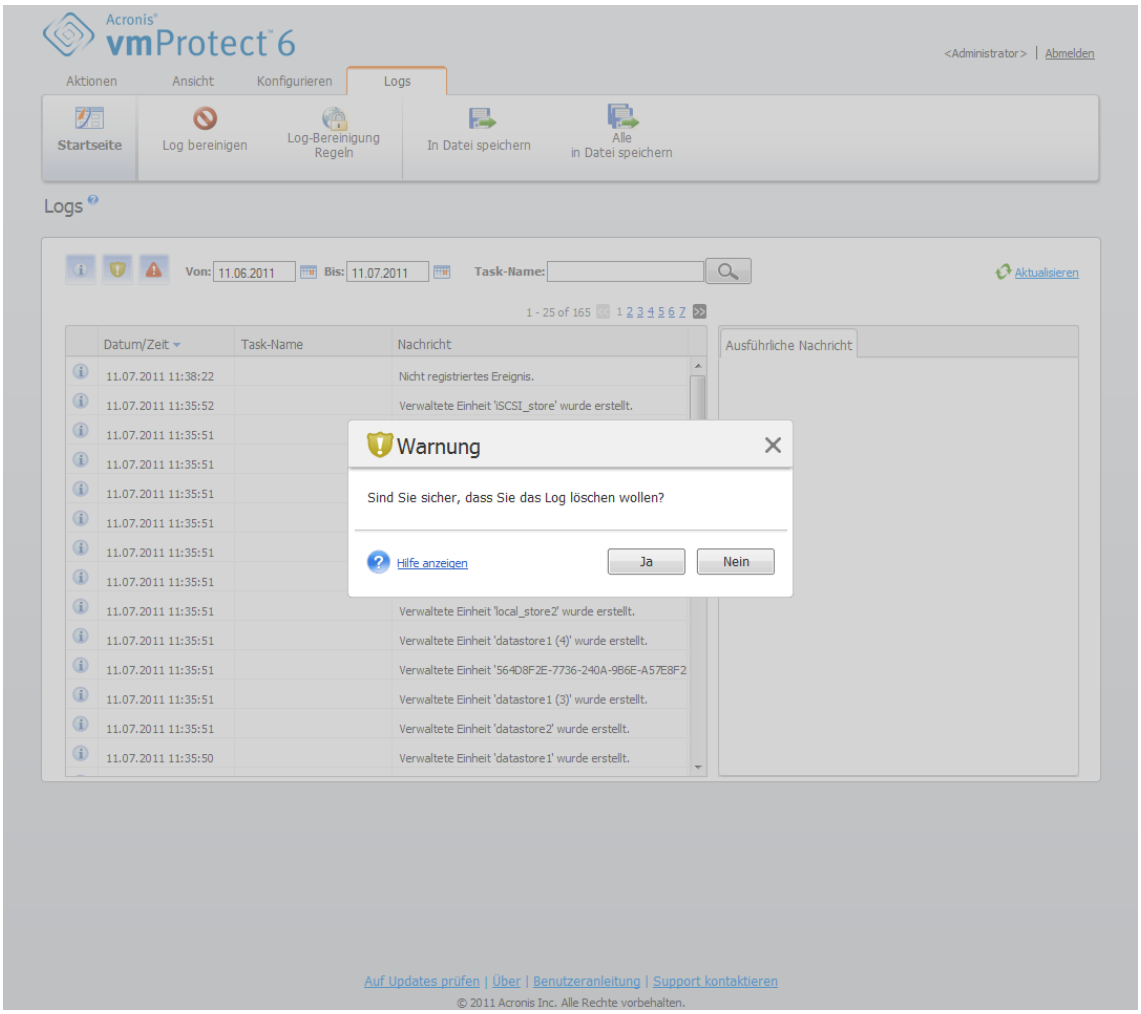
- **Maximale Log-Größe**: 50 MB.
- **Nach Bereinigung zu bewahrende Log-Größe**: 95%.

Mit **Auf Standardwerte zurücksetzen** gehen Sie auf die Voreinstellungen zurück.

Wenn die Option **Log-Bereinigungsregeln** aktiviert ist, vergleicht das Programm nach jeweils 100 Log-Einträgen die tatsächliche Log-Größe mit der voreingestellten **Maximalen Log-Größe**. Sobald die maximale Log-Größe überschritten ist, löscht das Programm die ältesten Log-Einträge. Mit der Standardeinstellung 95% wird ein Großteil des Logs beibehalten. Mit der Minimaleinstellung 1% wird das Log fast vollständig geleert.

12.3.3 Logs bereinigen

Klicken Sie auf **Logs bereinigen** in der Hauptsymbolleiste, um alle Log-Einträge zu löschen. Diese Aktion löscht alle Einträge im Acronis vmProtect-Log. Es erscheint die Warnmeldung 'Sind Sie sicher, dass Sie das Log löschen möchten?', um die Löschaktion zu bestätigen. Nach erfolgter Bestätigung werden alle Log-Einträge gelöscht.



Dialogfenster 'Log bereinigen'

12.3.4 Logs in Datei speichern

Klicken Sie in der Menübandleiste auf **In Datei speichern**, um die aus der Log-Liste gefilterten Einträge zu speichern. Die so erstellte .zip-Datei mit den ausgewählten Logs können Sie auf dem lokalen PC speichern. Die Aktion 'Logs in Datei speichern' kann Ihnen bei der Fehlerbehebung nach aufgetretenen Problemen helfen.

Außerdem können Sie über die Schaltfläche **Alle in Datei speichern** sämtliche Log-Einträge von Acronis vmProtect speichern.

12.4 Lizenzen verwalten (Konfigurieren –> Lizenzen)

Klicken Sie auf der Registerkarte **Konfigurieren** im Hauptmenüband von Acronis vmProtect auf **Lizenzen**, um die Seite **Lizenzen** zu öffnen.

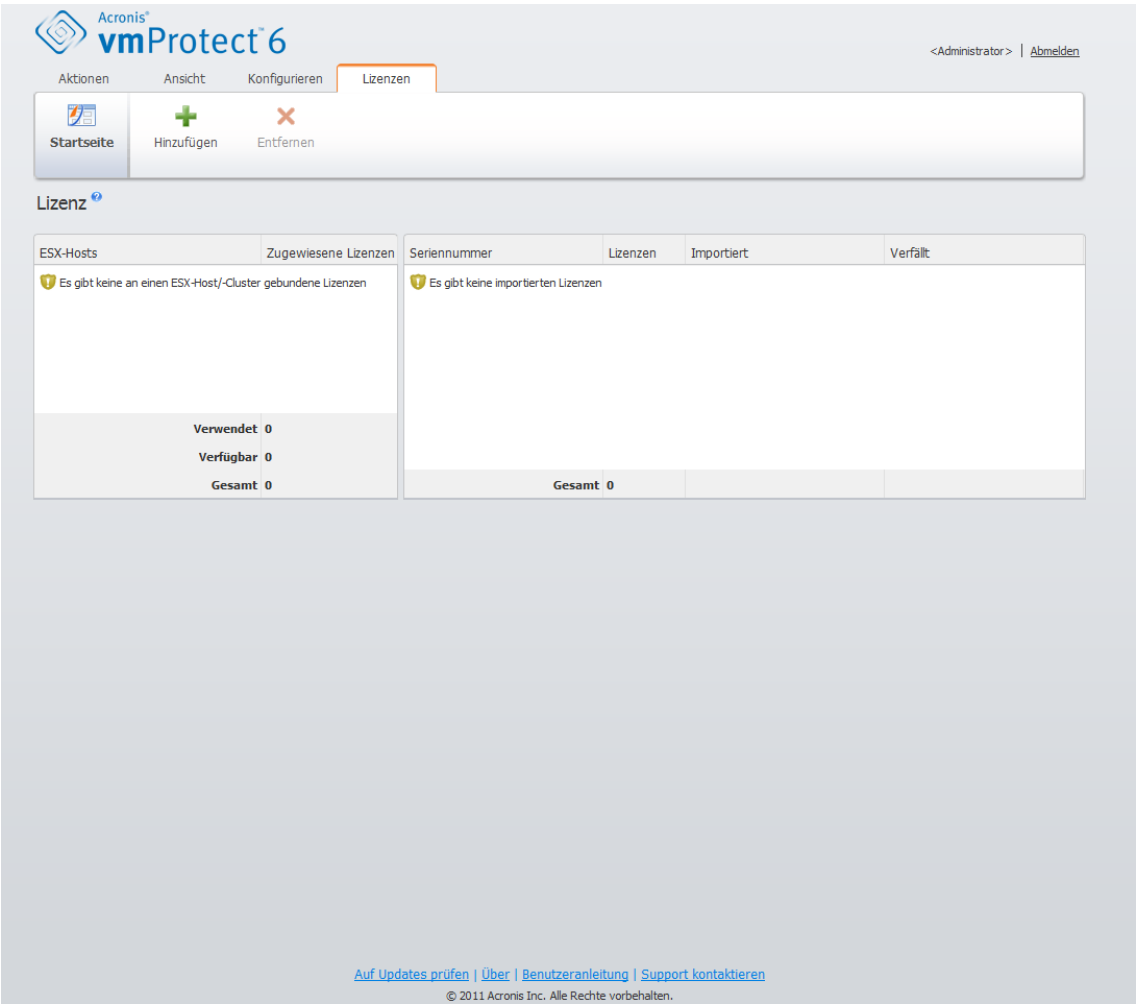
Die Ansicht **Lizenzen** gibt einen Überblick über die in den vmProtect-Agenten importierten Lizenzen. Hier können Sie über die entsprechenden Schaltflächen in der Symbolleiste die Lizenz-Seriennummern **Hinzufügen** oder die Anbindung der Lizenzen an ESX-Hosts **Entfernen**. Das Entfernen der Lizenzbindung gibt diese wieder frei.

Das Lizenzschema bei vmProtect besagt, dass jede CPU auf dem verwalteten ESX-Host bzw. Cluster eine eigene Lizenz braucht.

Beim ersten Ausführen von Acronis vmProtect sind an keinen ESX-Host oder Cluster Lizenzen gebunden. Hier können Sie, wie nachfolgend beschrieben, eine neue Lizenz hinzufügen.

Die importierten (hinzugefügten) Seriennummern können mehrere Lizenzen enthalten. Rechts auf der Seite **Lizenzen** sehen Sie die Liste der Seriennummern, die Anzahl der Lizenzen sowie deren Import- und Ablaufdatum.

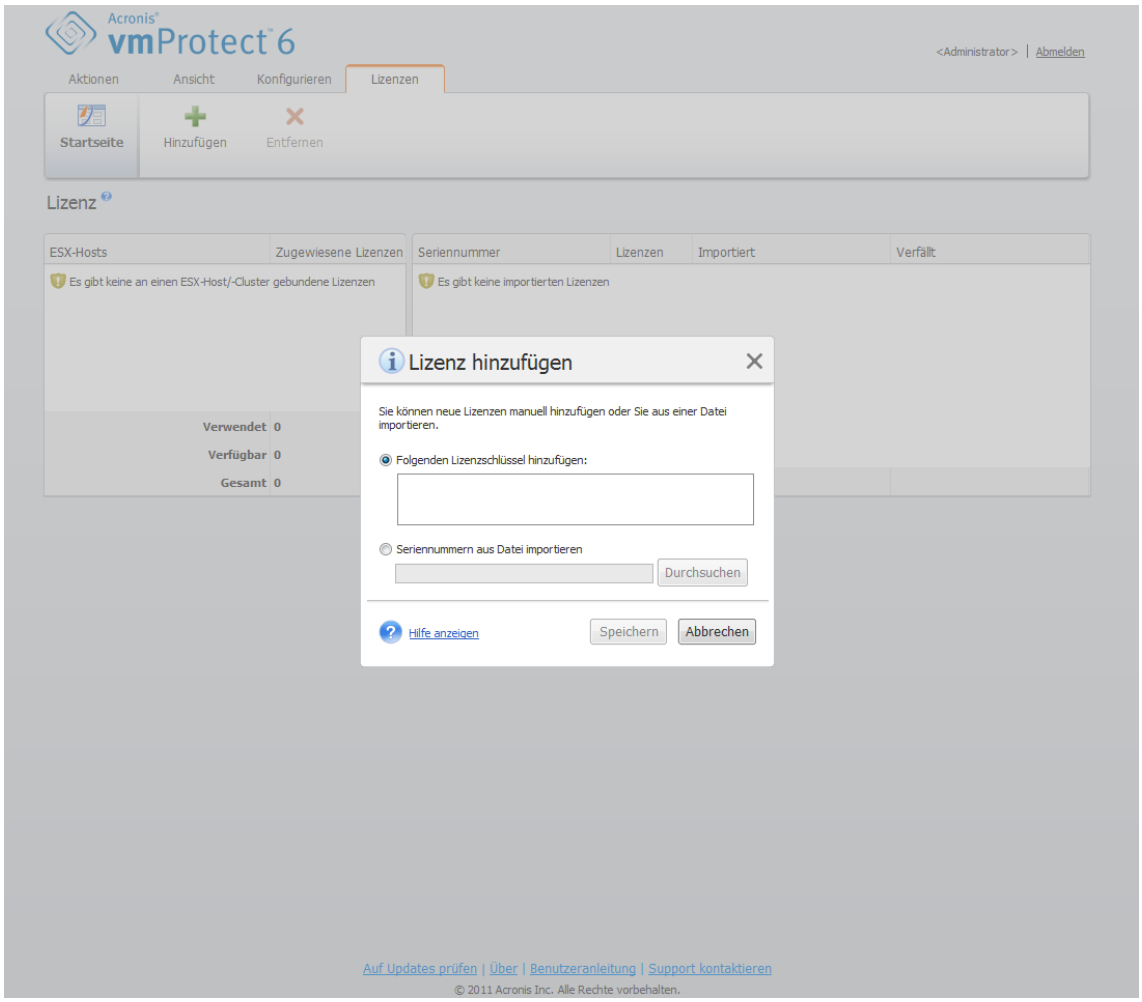
Die linke Seite enthält die Liste der ESX-Hosts bzw. Cluster, an die Lizenzen gebunden sind. Die Anbindung der Lizenzen an ESX-Hosts oder Cluster erfolgt bei der ersten Ausführung eines Backups oder einer Wiederherstellung mit virtuellen Maschinen, die auf diesem Host laufen. Bei einem Cluster sind die Lizenzen an alle in den Cluster integrierte Hosts gebunden. Das Entfernen eines Hosts vom Cluster gibt jedoch nicht automatisch die Lizenz frei. Sie können die Lizenzbindung aufheben, indem Sie den ESX-Host oder Cluster hier auswählen und auf die Schaltfläche **Entfernen** in der Symbolleiste klicken. Die zuvor an diesen Host gebundenen Lizenzen sind dann wieder frei und können auf einem anderen ESX-Host oder Cluster eingesetzt werden.



Seite 'Lizenzen verwalten', Lizenz-Liste

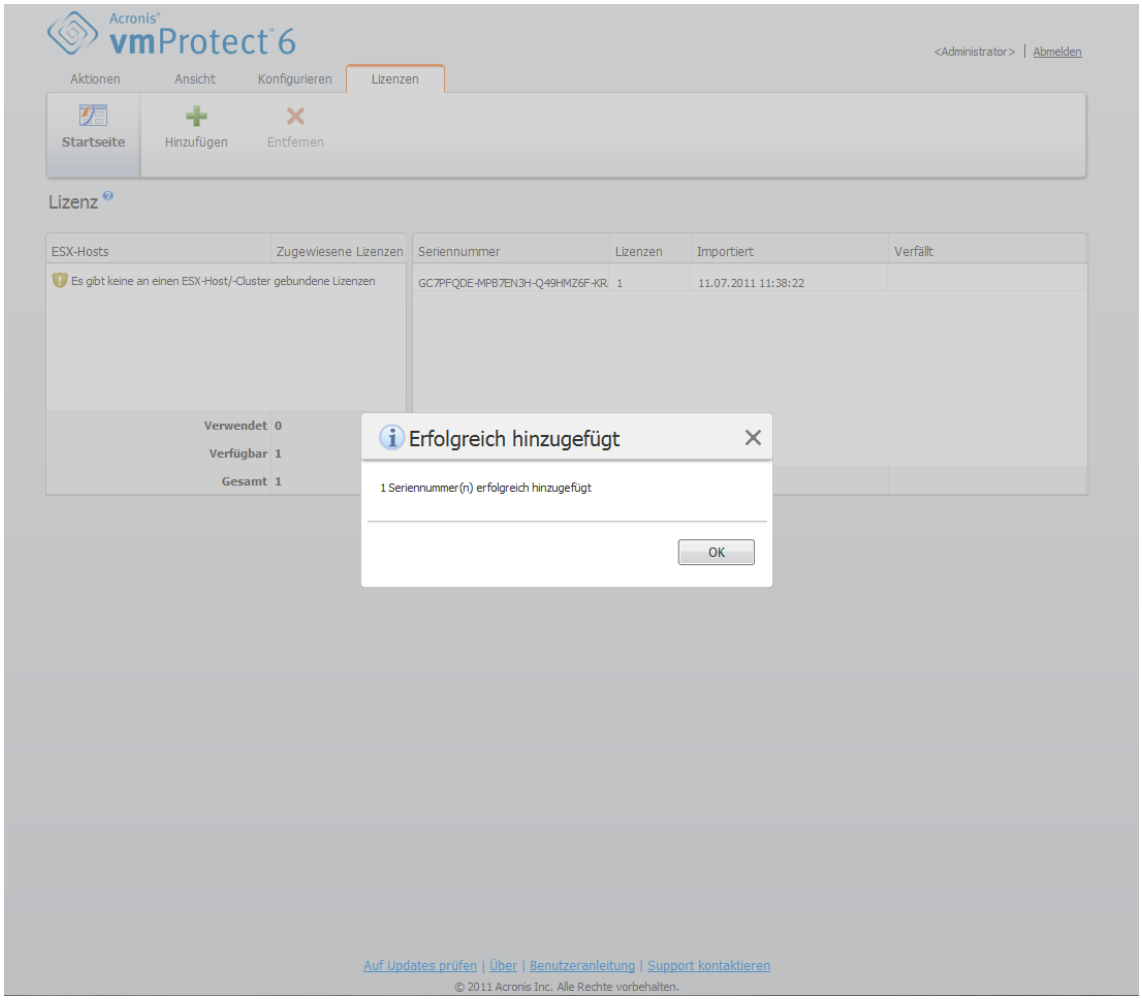
12.4.1 Lizenz hinzufügen

Sie können Lizenzen entweder durch Kopieren in das entsprechende Feld hinzufügen oder indem Sie die Datei mit den Lizenzen durchsuchen, die Sie importieren möchten. Acronis vmProtect unterstützt .txt und .cvs Dateiformate.



Seite Lizenzen verwalten, Dialog 'Lizenzen hinzufügen'

Beim Hinzufügen neuer Lizenzen erscheint folgende Meldung, die die Anzahl hinzugefügter Lizenzen angibt.



Seite Lizenzen verwalten, Meldung 'Erfolgreich hinzugefügt'

12.4.2 Fehler beim Hinzufügen von Lizenzen

Das Hinzufügen einer Lizenz kann aus folgenden Gründen fehlschlagen:

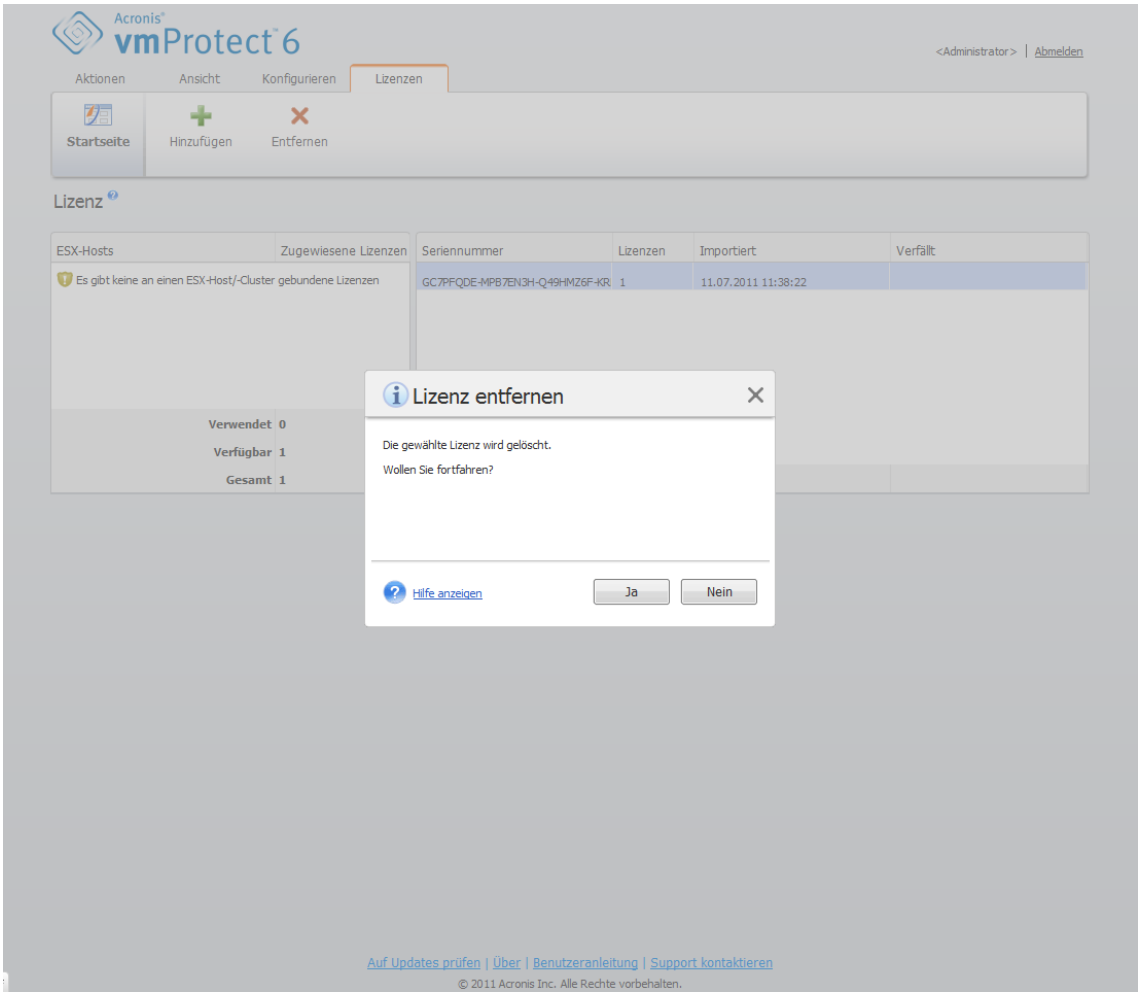
- Die Lizenz wurde bereits importiert
- Die Lizenz ist nicht korrekt.

Zudem können weitere Probleme auftreten. Wenn Sie sich sicher sind, dass Ihre Lizenz korrekt ist, diese sich aber trotzdem nicht hinzufügen lässt, wenden Sie sich an den Acronis Support (S. 85).

12.4.3 ESX-Host bzw. Lizenz entfernen

Wählen Sie einen ESX-Host oder Cluster in der Liste aus und klicken Sie auf **Entfernen**. Die Lizenzzuweisung wird für den gewählten ESX-Host zurückgesetzt und die Lizenzen werden freigegeben. Wenn Sie mit einer der auf diesem Host laufenden Maschinen eine Backup- oder Recovery-Aktion durchführen, werden die Lizenzen automatisch diesem Host wieder zugewiesen.

Das Entfernen der Lizenzbindung müssen Sie im Dialogfenster mit **Ja** bestätigen.



Seite Lizenzen verwalten, Bestätigungs-Dialog 'Lizenz entfernen'

12.5 ESX-Hosts verwalten (Konfigurieren -> ESX-Hosts)

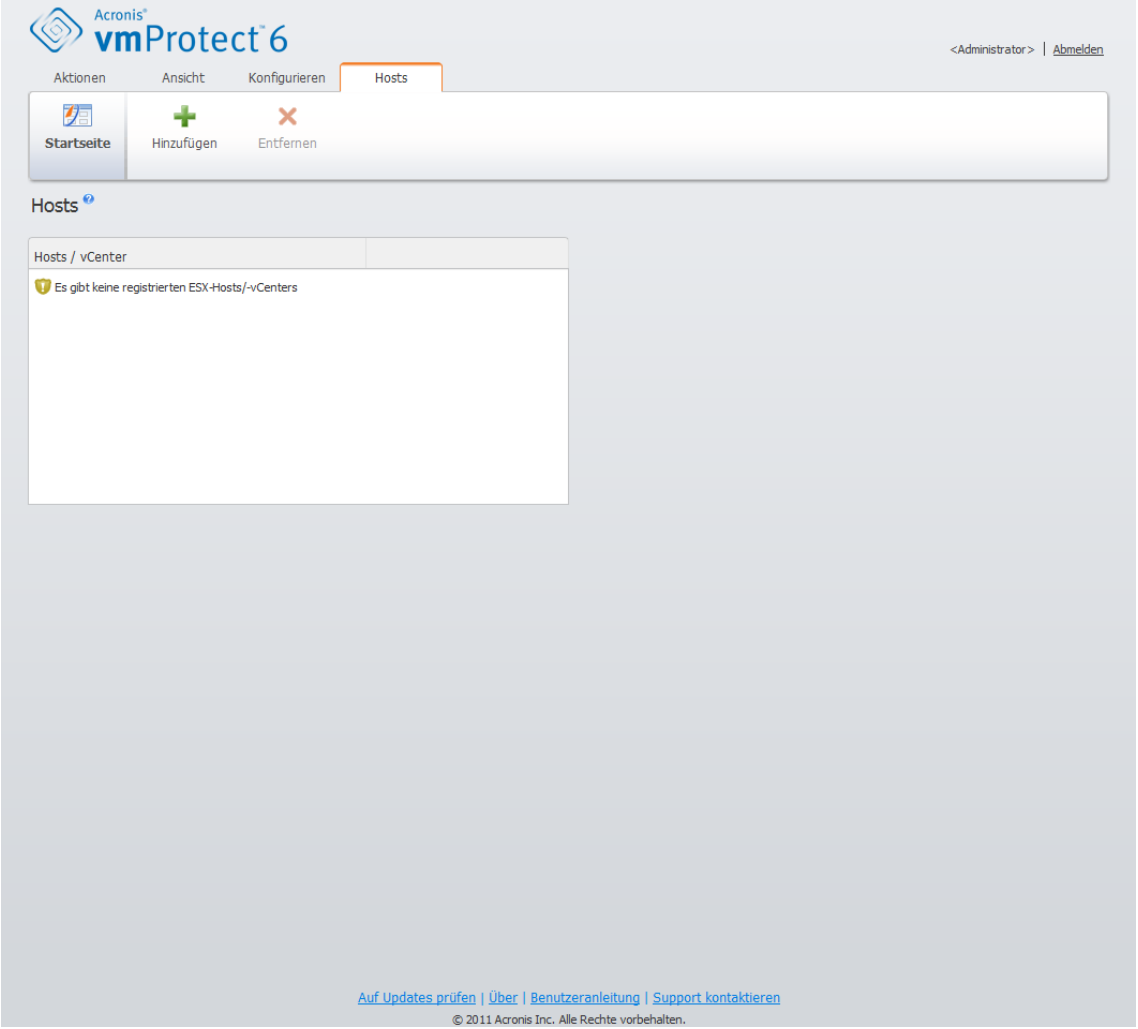
Klicken Sie in der Registerlasche **Konfigurieren** im Hauptmenüband von Acronis vmProtect auf **ESX-Hosts**, um die Seite **ESX-Hosts** zu öffnen.

12.5.1 Liste der ESX-Hosts

Die Ansicht **Hosts** bietet einen Überblick und eine Schnittstelle für die Verwaltung der ESX-Hosts bzw. vCenters, die in den Einstellungen des vmProtect-Agenten registriert sind. Über die Schaltflächen im Menüband können Sie der Liste andere ESX-Hosts hinzufügen oder sie aus dieser entfernen.

Beim ersten Ausführen von Acronis vmProtect gibt es keine registrierten ESX-Hosts oder Cluster. Auf dieser Seite können Sie, wie unten beschrieben, neue ESX-Hosts hinzufügen.

Nach dem Hinzufügen eines ESX-Hosts bzw. eines vCenters erscheint dieser/s in der Liste der Hosts.



Seite ESX-Hosts konfigurieren, 'Liste der Hosts'

Das Hinzufügen eines ESX-Hosts oder vCenters beinhaltet nicht automatisch die Anbindung der Lizenzen. Diese erfolgt erst, wenn Sie mit einer der auf diesem Host laufenden virtuellen Maschinen einen Backup- oder Recovery-Task ausführen. Nach Hinzufügen eines ESX-Hosts oder vCenters können Sie mit den virtuellen Maschinen, die auf diesem ESX-Host oder vCenters laufen, Backup- bzw. Recovery-Tasks ausführen.

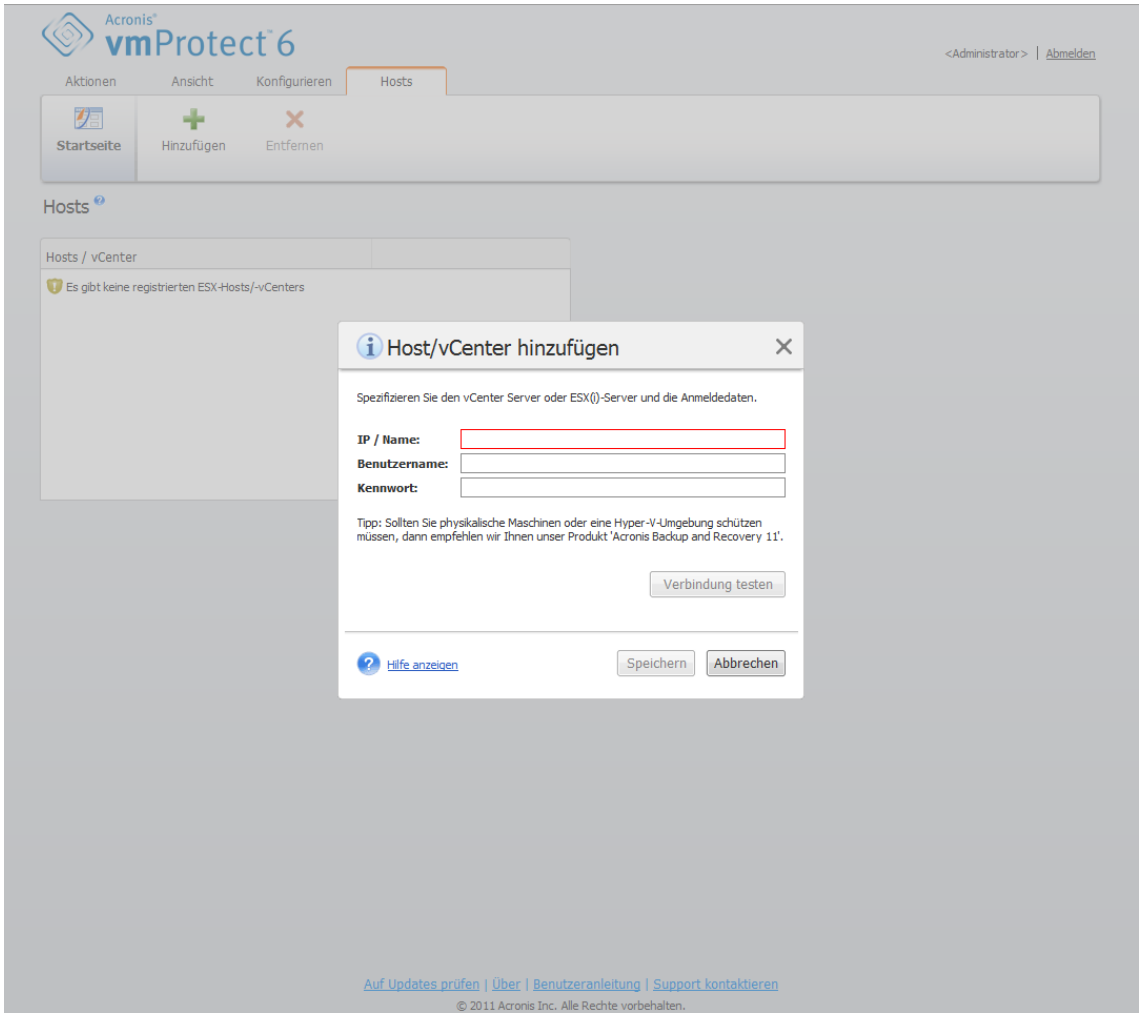
Durch Entfernen eines ESX-Hosts oder vCenters verschwinden alle Tasks, die den auf diesem ESX-Host oder vCenter laufenden virtuellen Maschinen zugewiesen worden waren. Falls der Task auch virtuelle Maschinen von anderen ESX-Hosts mit einschließt, bleibt er bestehen, auch wenn einer dieser ESX-Hosts in der Konfiguration entfernt wird.

Für eine erfolgreiche Verwaltung eines ESX-Hosts oder vCenters ist die Eingabe von Anmeldedaten erforderlich. Die Anmeldedaten können Sie hier eingeben; sie bleiben solange erhalten, bis Sie den ESX-Host bzw. das vCenter entfernen oder die Anmeldedaten manuell ändern. Falls zum Beispiel Ihr Unternehmen aus Sicherheitsgründen einen Kennwortwechsel verlangt, macht dies das Ändern der Anmeldedaten erforderlich. Wählen Sie dazu den ESX-Host bzw. das vCenter in der Liste aus und klicken Sie auf der rechten Seite auf **Anmeldedaten bearbeiten**.

12.5.2 Einen ESX-Host hinzufügen

Um einen ESX-Host bzw. ein vCenter hinzuzufügen, müssen Sie die IP-Adresse oder den Hostnamen sowie die Anmeldedaten angeben, um auf den gewünschten ESX-Host oder das vCenter zuzugreifen.

Um sicherzustellen, dass die verwendeten Anmeldedaten korrekt sind, können Sie die Verbindung mit einem Klick auf **Verbindung testen** überprüfen. Klicken Sie auf **Speichern**, um den ESX-Host oder das vCenter hinzuzufügen.



Seite ESX-Hosts verwalten, Dialog 'Host bzw. vCenter hinzufügen'

12.5.3 Einen ESX-Host hinzufügen, der Teil des vCenters ist

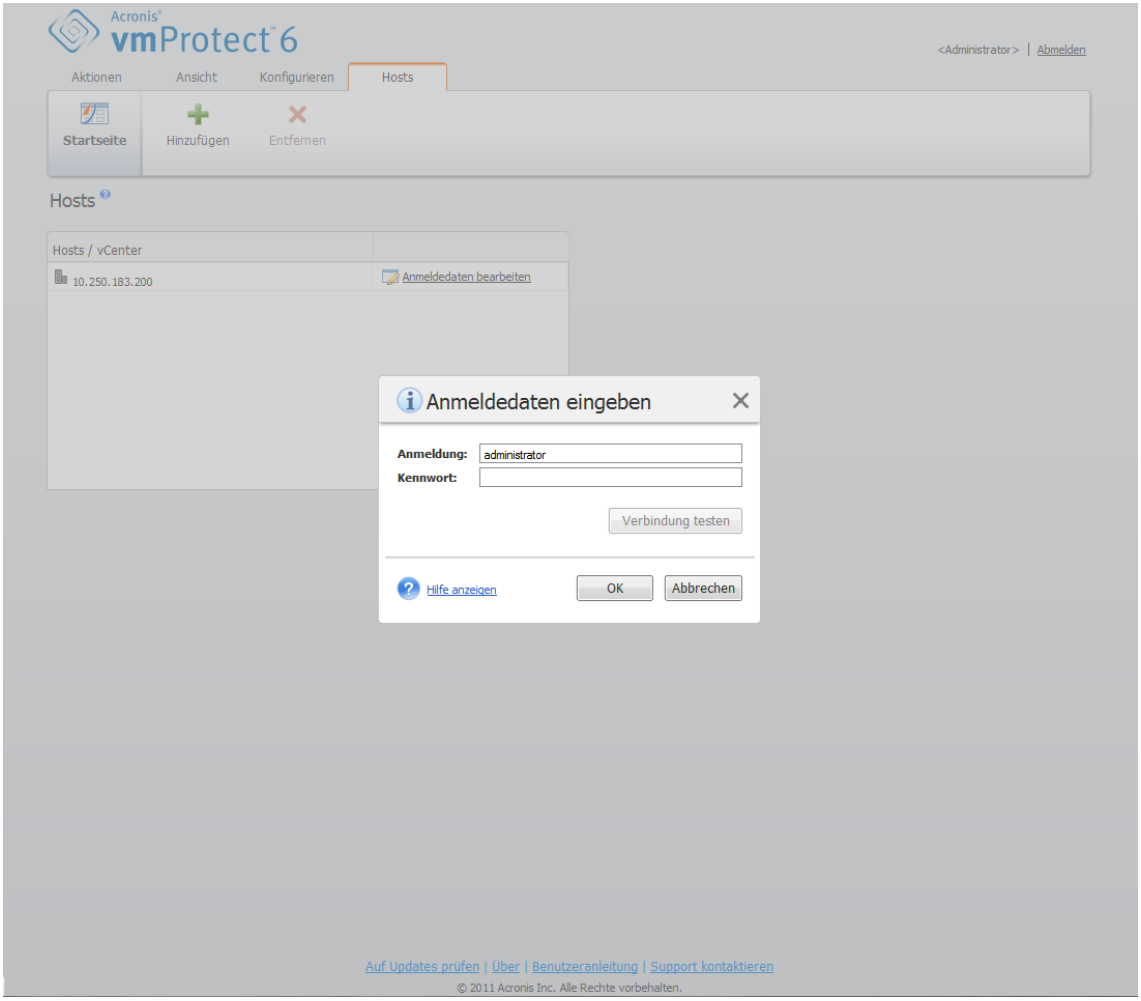
Wenn Sie anstelle eines vCenters einen ESX-Host, der Teil eines vCenters ist, direkt hinzufügen, ist das Hauptproblem, dass der Acronis vmProtect-Agent nicht in der Lage ist, die im Auftrag des vCenters am ESX-Host vorgenommenen Änderungen zu verfolgen. Das kann unvorhersehbare Auswirkungen haben. Wenn Sie zum Beispiel eine VM von Backup ausführen, werden beim Trennen die temporären Dateien nicht vom ESX-Host gelöscht, weil das vCenter sie sperrt. Darum wird dringend empfohlen, statt einzelner ESX-Hosts das vCenter hinzuzufügen.

Wenn Sie versuchen, einen ESX-Host hinzuzufügen, der Teil des vCenters ist, erscheint die folgende Warnmeldung. Klicken Sie auf **Nein**, um das vCenter hinzuzufügen.

12.5.4 Anmeldedaten

Falls zum Beispiel Ihr Unternehmen aus Sicherheitsgründen wechselnde Kennwörter verlangt, macht dies das Ändern der Anmeldedaten erforderlich. Wählen Sie den ESX-Host bzw. das vCenter in der Liste aus, klicken Sie auf **Anmeldedaten bearbeiten** und geben Sie Login und Kennwort für die

Verbindung zum ESX-Host bzw. vCenter ein. Wenn Sie Acronis vmProtect in einer Domänenumgebung ausführen, muss der Benutzername im Format Domäne\Benutzername eingegeben werden. Um sicherzustellen, dass die verwendeten Anmeldedaten korrekt sind, können Sie die Verbindung mit **Verbindung testen** überprüfen. Klicken Sie auf **OK**, um den ESX-Host bzw. das vCenter hinzuzufügen.



Seite ESX-Hosts verwalten, Dialog 'Anmeldedaten eingeben'

12.5.5 ESX-Host entfernen

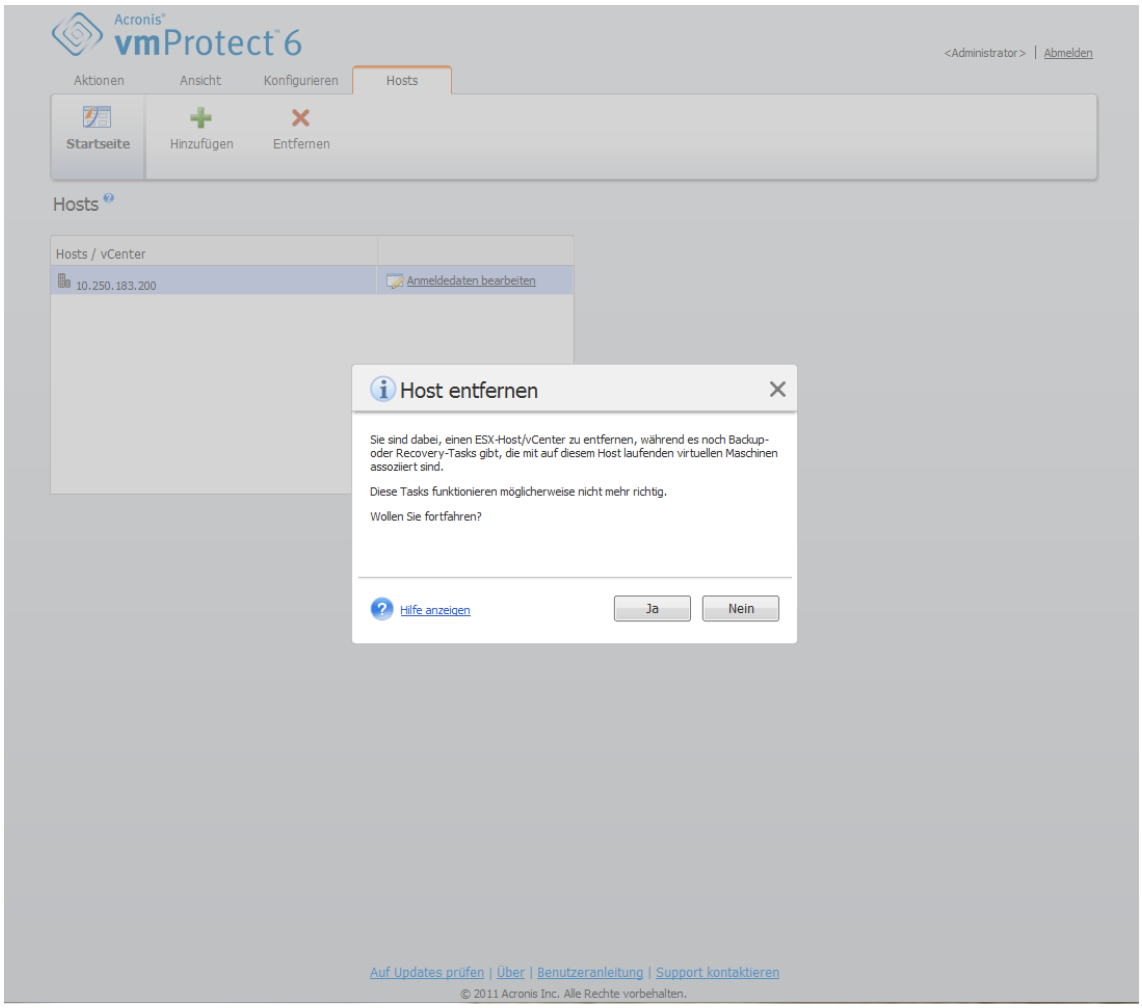
Das Entfernen eines ESX-Hosts von der Acronis vmProtect-Konfiguration kann erforderlich werden, wenn Sie keine weiteren Backups bzw. Wiederherstellungen über die auf diesem ESX-Host laufenden virtuellen Maschinen durchführen wollen. Die diesem Host zugewiesenen Lizenzen werden nicht automatisch entfernt. Um die Lizenzbindung aufzuheben, gehen Sie zur Seite Konfigurieren –> Lizenzen (S. 71).

Das Entfernen eines ESX-Hosts oder vCenters verursacht Fehlfunktionen bei den bestehenden Tasks, daher erscheint bei dieser Aktion folgende Warnmeldung:

„Sie sind dabei, einen ESX-Host bzw. ein vCenter zu entfernen, obwohl mit den auf diesem Host laufenden virtuellen Maschinen Backup- oder Recovery-Tasks verbunden sind. Möchten Sie eine automatische Anpassung dieser Tasks vornehmen, um die Änderungen in der Konfiguration widerzuspiegeln (die verbundenen Tasks werden entweder entfernt oder modifiziert)? Wenn Sie

'Nein' wählen, bleibt der Task intakt, funktioniert aber möglicherweise aufgrund des fehlenden ESX-Hosts bzw. vCenters nicht richtig.“

Mit der Auswahl **Ja** verschwinden alle Acronis vmProtect-Tasks, die von den auf diesem ESX-Host bzw. vCenter laufenden virtuellen Maschinen angewendet werden. Hatte ein Task virtuelle Maschinen von anderen ESX-Hosts mit eingeschlossen, wird er automatisch modifiziert, um die unnötigen virtuellen Maschinen von der Task-Konfiguration zu entfernen. Es bleiben also nur die virtuellen Maschinen übrig, die von den weiterhin registrierten ESX-Hosts verwaltet werden.



Seite ESX-Hosts verwalten, Dialog 'Host entfernen'

12.6 Einstellungen verwalten

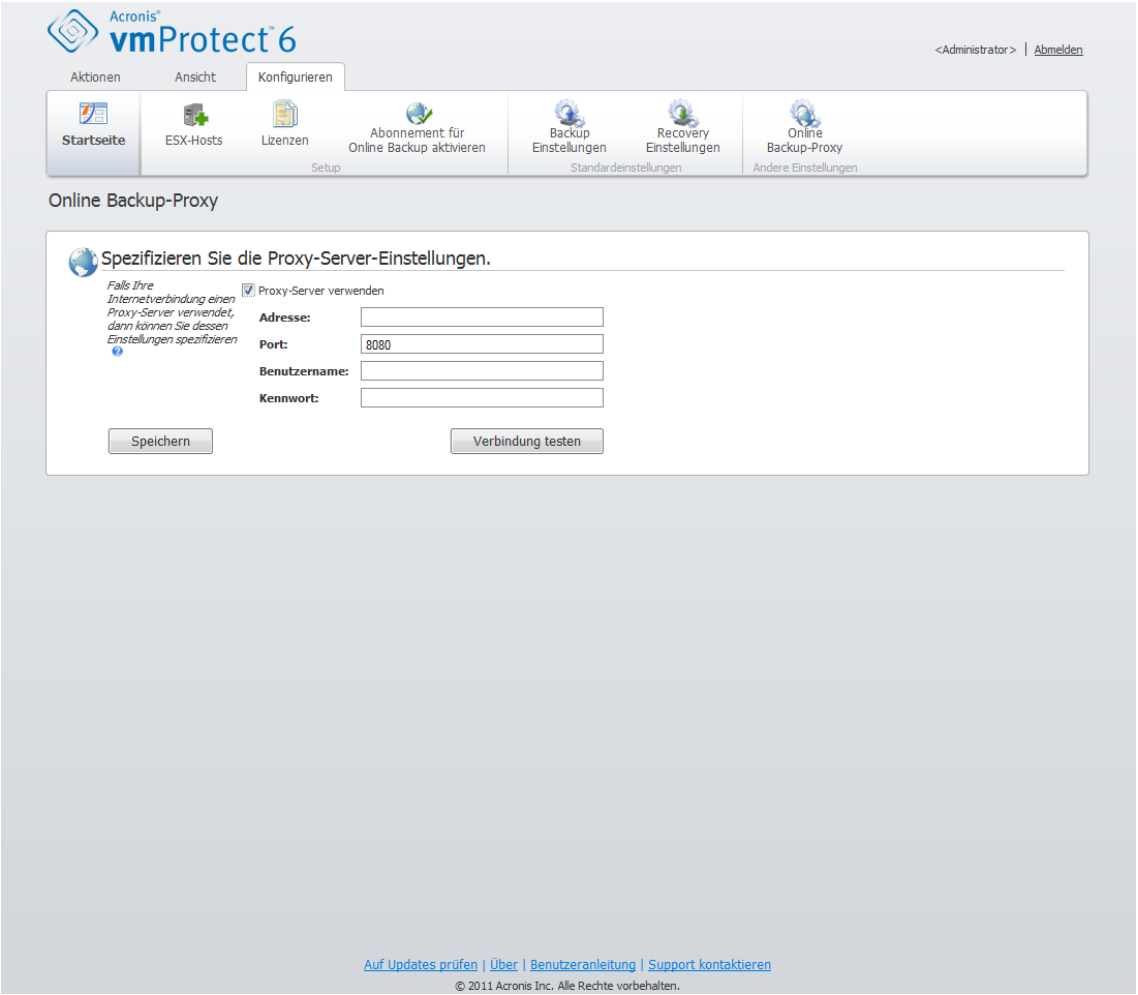
12.6.1 Online Backup-Proxy verwalten

Klicken Sie in der Registerkarte **Konfigurieren** im Hauptmenüband von Acronis vmProtect auf **Online Backup-Proxy**, um die Seite mit den Einstellungen für **Online Backup-Proxy** zu öffnen.

Die Einstellungen für Online Backup-Proxy sind nur wirksam für Backup- und Recovery-Aktionen, die mit Acronis Online Backup Storage über das Internet durchgeführt werden.

Diese Option bestimmt, ob der Acronis Agent die Internetverbindung über einen Proxy-Server herstellen soll.

Beachten Sie, dass Acronis vmProtect Online Backup Storage nur HTTP- und HTTPS-Proxy-Server unterstützt.



Einstellungen verwalten, Online Backup-Proxy

So konfigurieren Sie die Proxy-Server-Einstellungen:

Aktivieren Sie das Kontrollkästchen **Proxy-Server verwenden**.

- Geben Sie unter **Adresse** den Netzwerknamen oder die IP-Adresse des Proxy-Servers an, z.B.: proxy.beispielname.com oder 192.168.0.1
- Spezifizieren Sie unter **Port** die Port-Nummer des Proxy-Servers, z.B.: 80
- Wenn der Proxy-Server eine Authentifizierung benötigt, dann geben Sie die entsprechenden Anmeldedaten unter **Benutzername** und **Kennwort** an.

Klicken Sie auf die Schaltfläche **Verbindung testen**, wenn Sie die Proxy-Server-Einstellungen überprüfen wollen.

Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.

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

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

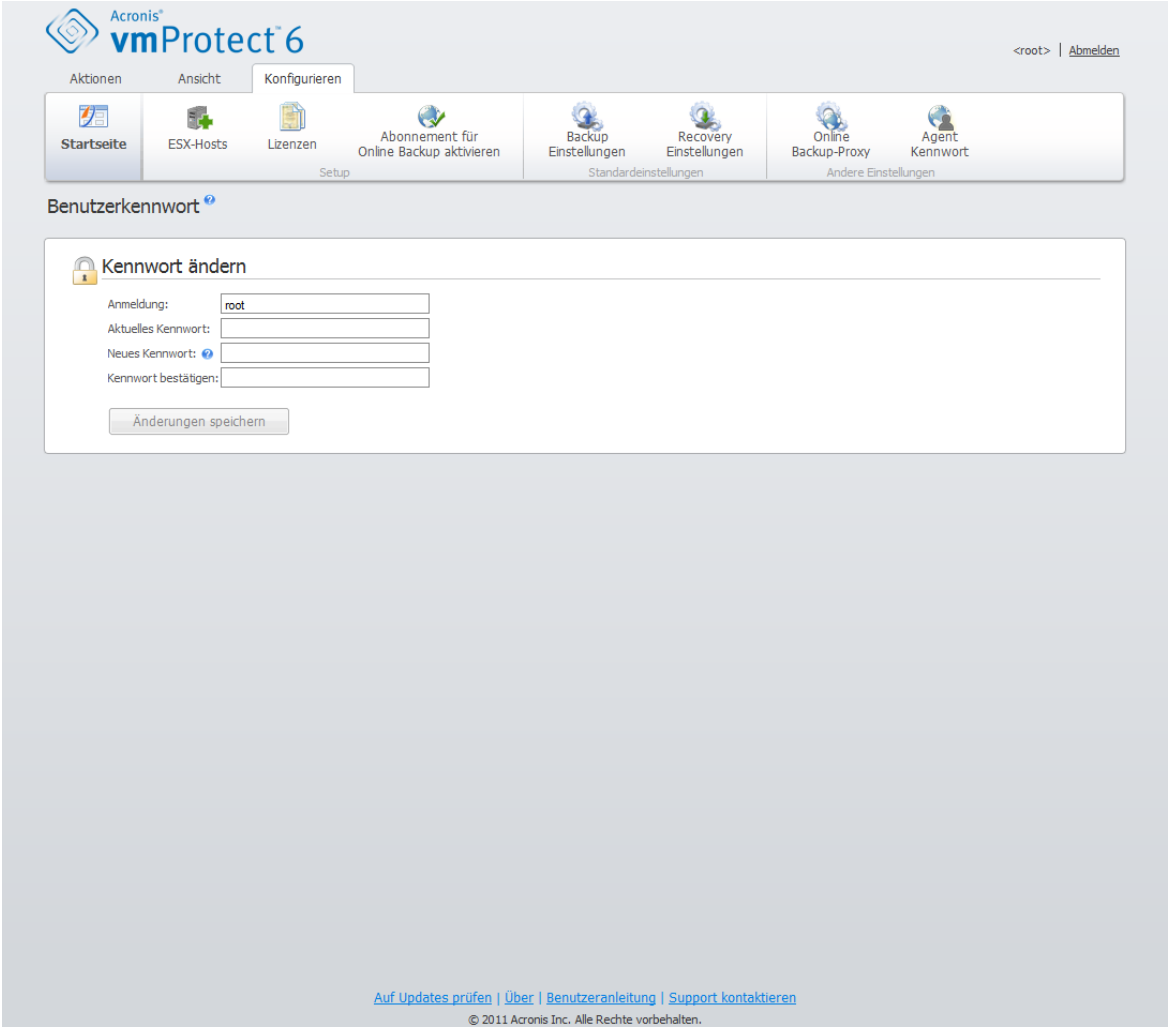
- Microsoft Internet Explorer: Klicken Sie im Menü **Extras** auf den Befehl **Internetoptionen**. Klicken Sie in der Registerkarte **Verbindungen** auf den Befehl **LAN-Einstellungen**.
- Mozilla Firefox: Klicken Sie im Menü **Extras** (zu erreichen über die **Firefox**-Schaltfläche oder über die Alt-Taste auf der Tastatur), erst auf **Einstellungen** und dann auf **Erweitert**. Klicken Sie in der Registerkarte **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**.

12.6.2 Kennwort für Agenten verwalten

Klicken Sie in der Registerkarte **Konfigurieren** im Hauptmenüband von Acronis vmProtect auf **Kennwort für Agenten**, um das **Benutzerkennwort** zu ändern.

Hier können Sie das Kennwort für den Benutzer des Acronis vmProtect Agenten ändern. Der Benutzername (Login) kann nicht geändert werden. Um das Kennwort zu ändern, müssen Sie zunächst das alte Kennwort und dann das neue Kennwort in die entsprechenden Felder eingeben und bestätigen.

Beachten Sie, dass die Option **Kennwort für Agenten** verwalten nur verfügbar ist, wenn der Agent als virtuelle Appliance (S. 11) installiert ist. Für die Verbindung mit dem Windows Agent (S. 12) verwendet Acronis vmProtect Windows Benutzerkonten (alle Konten mit lokaler Anmeldeberechtigung): Benutzer müssen zur Sicherheitsrichtlinie **Lokal anmelden erlauben** über **Start–>Secpol.msc–>Lokale Richtlinien–>Benutzerrechte-Zuweisungen**) hinzugefügt werden.



Einstellungen konfigurieren, Benutzerkennwort

Link 'Kennwort vergessen'

Auch wenn Sie Ihr Kennwort vergessen haben, können Sie es von der direkten Verwaltung des Acronis vmProtect-Agenten aus über den VMWare Infrastructure Client ändern. Dort können Sie die Konsole der Acronis vmProtect Virtual Appliance (der entsprechenden virtuellen Maschine) öffnen.

13 Optimale Vorgehensweisen

In diesem Abschnitt werden einige Beispiele für verschiedene Aktionen mit Acronis vmProtect gegeben.

Nach Installation des Acronis vmProtect-Agenten müssen Sie die Verbindung mit den Anmeldedaten herstellen.

1. Einen ESX-Host hinzufügen

Um Backups zu erstellen und andere Aktionen auszuführen, müssen Sie zuerst die IP-Adresse bzw. den Host-Namen sowie die Anmeldedaten für das vCenter oder den einzelnen ESX-Host angeben, auf dem die virtuellen Maschinen laufen. Klicken Sie im Bereich **Schnellstart** des **Dashboards** auf **ESX-Hosts konfigurieren** oder gehen Sie zur Ansicht **ESX-Hosts** im Menü **Konfigurieren** und klicken Sie auf **Hinzufügen**. Spezifizieren Sie den vCenter Server oder ESX(i)-Server und die Anmeldedaten. Detaillierte Informationen finden Sie im Abschnitt 'ESX-Hosts verwalten' (S. 75).

2. Lizenzen hinzufügen

Durch Einrichtung eines ESX-Hosts werden noch keine Lizenzen automatisch an diesen gebunden. Sie müssen die Lizenzen auf der Seite **Lizenzen** einrichten. Klicken Sie im **Dashboard** im Abschnitt **Schnellstart** auf **Lizenzen konfigurieren**, oder klicken Sie im Menü **Konfigurieren** auf die Ansicht **Lizenzen**. Klicken Sie dann auf **Hinzufügen** und geben Sie Ihren Lizenzschlüssel ein. Detaillierte Informationen finden Sie im Abschnitt 'Lizenzen verwalten' (S. 71).

Sie können anschließend mit dem Backup der virtuellen Infrastruktur beginnen.

13.1 Backups von virtuellen Maschinen auf einer Netzwerkfreigabe erstellen

Betrachten wir zunächst, wie Sie ein Backup mehrerer virtueller Maschinen (z.B. 5) erstellen und sie auf einer Netzwerkfreigabe sichern.

Nachdem Sie die **ESX-Hosts** und **Lizenzen** eingerichtet haben, müssen Sie den Assistenten **Backup-Task erstellen** ausführen, der Sie durch alle Schritte des Backup-Prozesses führt. Klicken Sie im **Dashboard** im Abschnitt **Schnellstart** auf **Backup-Task erstellen** oder klicken Sie in der Registerlasche **Startseite** im Hauptmenü auf **Backup**. Führen Sie dann alle Schritte des Assistenten **Neuer Backup-Task** aus. Detaillierte Informationen finden Sie im Abschnitt 'Backups von virtuellen Maschinen erstellen' (S. 22).

Wählen Sie im ersten Schritt des Assistenten **Neuer Backup-Task** die fünf virtuellen Maschinen aus. Durchsuchen Sie dann im zweiten Schritt die Netzwerkfreigabe, auf der die Backup-Archive gespeichert werden sollen. Wählen Sie im dritten und vierten Schritt die gewünschte Planung und Backup-Methode. Beenden Sie dann den Assistenten. Der erstellte Backup-Task führt dann die Aktion aus. Sie können den Fortschritt des Tasks in den Ansichten **Dashboard** (**Ansicht**->**Dashboard**) oder **Tasks** (**Ansicht**->**Tasks**) der Benutzeroberfläche von Acronis vmProtect verfolgen.

13.2 Das Backup einer virtuellen Maschine an einem neuen Speicherort wiederherstellen

Sie haben das Backup erstellt. Betrachten wir nun, wie Sie die gesicherte virtuelle Maschine wiederherstellen können, z.B. an einem neuen Speicherort.

Dazu müssen Sie den Assistenten 'Backup-wiederherstellen-Task' ausführen, der Sie durch alle Schritte der Wiederherstellung führt. Klicken Sie in der Registerlasche 'Startseite' im Hauptmenü auf 'Recovery'. Führen Sie dann alle Schritte des Assistenten aus. Weitere Informationen finden Sie im Abschnitt 'Backup virtueller Maschinen wiederherstellen' (S. 34).

Wählen Sie im ersten Schritt des Assistenten eine gesicherte virtuelle Maschine aus. Wählen Sie im zweiten Schritt den neuen Speicherort aus, an dem die Maschine wiederhergestellt werden soll. Wählen Sie im dritten Schritt die Einstellungen für den Recovery-Task und beenden Sie dann den Assistenten. Klicken Sie auf 'Jetzt ausführen', um die Maschine sofort wiederherzustellen oder auf 'Speichern', um die Wiederherstellung später auszuführen.

13.3 Recovery von Dateien und Ordnern

Die ersten zwei Fälle zeigen, wie Sie mit Acronis vmProtect Backup- und Recovery-Aktionen durchführen. Hier ein Beispiel, wie Sie ausgewählte Dateien aus einem bestimmten Archiv wiederherstellen können. Das ist der Fall, wenn Sie nur eine oder wenige Dateien aus einem Backup-Archiv wiederherstellen müssen, ohne die gesamte virtuelle Maschine zu rekonstruieren.

Führen Sie den **Datei-Recovery**-Assistenten aus, indem Sie in der Registerlasche **Startseite** im Hauptmenü auf **Datei-Recovery** klicken. Im ersten Schritt des 'Datei-Recovery'-Assistenten müssen Sie den Recovery-Punkt auswählen, der den Zustand der virtuellen Maschine definiert, dem Sie die Dateien oder Verzeichnisse entnehmen wollen. Wählen Sie im zweiten Schritt die wiederherzustellenden Dateien und klicken Sie auf **Download**. Detaillierte Informationen zu **Datei-Recovery** finden Sie im Abschnitt 'Datei-Recovery' (S. 42).

Betrachten wir nun eine andere Möglichkeit, denselben Assistenten auszuführen – nämlich durch direkten Zugriff auf den Recovery-Punkt aus der Ansicht **Recovery-Punkte**. Öffnen Sie die Registerlasche **Ansicht** und klicken Sie auf **Recovery-Punkte**. Wählen Sie den Zustand der virtuellen Maschine, in dem die Dateien wiederhergestellt werden sollen. Wählen Sie auf der rechten Seite den genauen Recovery-Punkt und klicken Sie dann auf die Schaltfläche **Datei-Recovery** im Kontextmenü. Sie kommen zum **Datei-Recovery**-Assistenten, in dessen ersten Schritt die Daten des ausgewählten Recovery-Punktes bereits eingetragen sind; deshalb müssen Sie nur auf **Weiter** klicken, um zum zweiten Schritt zu gelangen. Hier wählen Sie die wiederherzustellenden Dateien bzw. Ordner aus und klicken auf **Download**.

14 Support

14.1 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).

14.2 Fehlerbehebung (Troubleshooting)

Wenn Sie bei der Verwendung von Acronis vmProtect Probleme haben oder Sie sich an den Technischen Support von Acronis wenden, schicken Sie uns die gespeicherten Logs der durchgeführten Aktionen. Gehen Sie zur **Logs**-Seite (S. 68) und klicken Sie **Alle in Datei speichern** (S. 71).

Weitere Informationen zur Kontaktaufname mit dem Technischen Support von Acronis finden Sie hier http://www.acronis.com/support/.

15 Glossar

A

Agent (Acronis vmProtect-Agent)

Eine Anwendung, die das Backup und die Wiederherstellung von virtuellen Maschinen sowie andere Verwaltungs-Aktionen auf VMware ESX/ESXi Infrastructure ermöglicht, wie zum Beispiel die Task-Verwaltung und Aktionen mit verfügbaren Backups, Maschinen usw.

Acronis vmProtect enthält den Agenten für das Backup virtueller Maschinen, die sich auf einem VMware ESX/ESXi Virtualisierungs-Server befinden, mit dem der Agent verbunden ist. Jeder Agent kann mehrere ESX/ESXi-Hosts oder ein vCenter verwalten. Die optimale Vorgehensweise ist, statt spezifischer ESX/ESXi-Hosts, die vom vCenter verwaltet werden, das vCenter selbst auf dem Agenten zu registrieren. Sonst wird vMotion (S. 94) nicht unterstützt.

Der Agent ist entweder Windows-basiert, d.h. auf einer Windows-Plattform installiert, oder basiert auf einer Appliance, d.h., er läuft auf einer speziellen virtuellen Maschine auf einem ESX-Host.

Archiv

Siehe Backup-Archiv (S. 87).

Archiv-Format 'Nur inkrementell'

Ein Archiv (S. 86)-Format der neuen Generation, das mehrere Backups (S. 86) von verschiedenen virtuellen Maschinen enthalten kann. Alle Backups in diesem Archiv werden im inkrementellen Modus (S. 91) gespeichert. Physikalisch gesehen befinden sich alle Daten in einer einzigen Datei, im Gegensatz zum Legacy-Modus-Archivformat, bei dem jedes Backup in einer separaten .tib-Datei gespeichert wird. So funktioniert das Rotationsschema für Backups im 'Nur-inkrementellen'-Archiv:

Läuft ein bestimmtes Backup aufgrund der vordefinierten Aufbewahrungsregeln ab (z.B. 'Lösche alle Backups, die älter sind als 5 Tage'), so markiert das Programm diese veralteten Backup-Blöcke als 'freie' Blöcke. Die Blöcke im abgelaufenen Backup, bei denen Abhängigkeiten bestehen (möglicherweise werden sie aufgrund der inkrementellen Backup-Technologie in neueren Backups verwendet) werden nicht als 'frei' markiert, um die Archiv-Konsistenz zu wahren. Das Archiv benötigt weiterhin denselben Speicherplatz wie zuvor. Aber neuere Backups, die in dieses Archiv gespeichert werden, schreiben ihre Daten zunächst auf die 'freien' Blöcke und die Gesamtgröße des Archivs wächst erst, wenn alle 'freien' Blöcke belegt sind.

Mit diesem Ansatz wird die Archivgröße auf ein Minimum begrenzt und übermäßiges Wachstum vermieden.

B

Backup

Das Ergebnis einer einzelnen Backup-Aktion (S. 87) in Form eines einzelnen Recovery-Punktes (S. 92) in einem Archiv. (S. 87) Physikalisch gesehen handelt es sich um eine Datei, die eine Kopie der gesicherten Daten (Volumes einer virtuellen Maschine) einer spezifischen virtuellen Maschine zu einem spezifischen Zeitpunkt enthält. Backup-Dateien, die von Acronis vmProtect erstellt wurden,

haben die Dateierweiterung '.tib'. Eine Backup-Datei kann nützliche Daten von mehreren Maschinen sowie die erforderlichen Metadaten enthalten.

Backup (Aktion)

Eine Aktion, die eine Kopie der Daten erstellt, die auf dem Laufwerk einer Maschine existieren, um diese wiederherzustellen oder in den Zustand eines festgelegten Tags bzw. Zeitpunkts zurückzusetzen.

Backup-Archiv (Archiv)

Ein Satz von Backups (S. 86), die von einem Backup-Task (S. 87) erstellt und verwaltet werden. Ein Legacy-Modus-Archiv kann mehrere Voll-Backups (S. 95) enthalten, aber auch inkrementelle (S. 91) und differentielle Backups (S. 89). Ein Archiv im Nur inkrementell (S. 86)-Format enthält nur inkrementelle Backups (das erste Backup ist allerdings immer ein vollständiges). Backups, die zum gleichen Archiv gehören, werden immer am gleichen Ort gespeichert. Es können zwar mehrere Backup-Tasks dieselben Quelldaten in das selbe Archiv sichern, aber das übliche Szenario ist 'ein Task – ein Archiv'.

Backups in einem Archiv werden vom Backup-Task verwaltet. Manuelle Aktionen mit Archiven (Validierung (S. 93), Sichten des Inhalts, Mounten und Löschen von Backups) sollten nur mit Acronis vmProtect ausgeführt werden. Modifizieren Sie Ihre Archive bzw. Backups nur mit Werkzeugen von Acronis, aber nicht mit z.B. dem Windows Explorer oder dem Dateimanager eines Drittanbieters.

Backup-Optionen

Konfigurationsparameter einer Backup Aktion (S. 87) wie zum Beispiel der Schutz des Archivs, der Ausschluss von Quelldateien oder der Komprimierungsgrad. Backup-Optionen sind Bestandteil eines Backup-Tasks (S. 87).

Backup-Schema

Teil eines Backup-Tasks (S. 87), der die Backup-Planung sowie [optional] Aufbewahrungsregeln und eine Planung zur Bereinigung (S. 88) enthält. Beispielsweise: Führe ein Voll-Backup (S. 95) monatlich am letzten Tag des Monats um 10 Uhr und ein inkrementelles Backup (S. 91) an Sonntagen um 22 Uhr aus (für Archive (S. 86) im klassischen Format). Lösche Backups, die älter sind als 3 Monate. Prüfe auf solche Backups jedes Mal, wenn ein Backup abgeschlossen wurde. Wird das Backup im Nur inkrementell (S. 86)-Modus durchgeführt, ist es nicht erforderlich, den Typ (vollständig oder inkrementell) zu definieren.

Acronis vmProtect ermöglicht den Einsatz bekannter optimierter Backup-Schemata wie zum Beispiel GVS (S. 90), das Erstellen von benutzerdefinierten Backup-Schemata oder das Sichern aller Daten auf einmal.

Backup-Task (Task)

Ein Satz von Regeln, der spezifiziert, wie einzelne virtuelle Maschinen oder eine Gruppe virtueller Maschinen gesichert werden. Ein Backup-Task spezifiziert:

- Welche Daten gesichert werden (d.h. welche Maschinen)
- Wo die Backup-Archive gespeichert werden (Name des Backup-Archivs und der Speicherort)
- Das Backup-Schema, das den Zeitplan für die Sicherungen und [optional] die Aufbewahrungsregeln enthält

- [optional] Die Richtlinien für die Validierung der Archive
- Die Backup-Optionen

Ein Backup-Task kann beispielsweise folgende Informationen enthalten:

- Erstelle Backups für die virtuellen Maschinen 'VM1' und 'VM2' (diese Daten sichert der Task)
- Benenne das Backup-Archiv mit MySystemVolume und bestimme als seinen Speicherplatz \\server\backups\
- Führe ein Voll-Backup monatlich am letzten Tag des Monats um 10 Uhr und ein inkrementelles Backup an Sonntagen um 22 Uhr aus (für Archive (S. 86) im klassischen Format). Lösche Backups, die älter sind als 3 Monate (das ist das Backup-Schema)
- Validiere das letzte Backup unmittelbar nach seiner Erstellung (das ist die Validierungsregel)
- Schütze das Archiv mit einem Kennwort (das ist eine Option)

Physikalisch ist ein Backup-Task ein Satz vordefinierter Aktionen, die für die Ausführung durch den Agenten (S. 86) anhand spezifizierter Parameter konfiguriert ist (Backup-Optionen (S. 87)).

Bereinigung

Löschen von Backups (S. 86) aus einem Backup-Archiv (S. 87), um veraltete Backups zu entfernen oder um das Archiv daran zu hindern, die gewünschte Größe zu überschreiten.

Die Bereinigung wendet die vom Backup-Task (S. 87) bei der Erstellung des Archivs bestimmten Aufbewahrungsregeln an. 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 wurden oder nicht.

Weitere Informationen finden Sie in der Benutzeranleitung (S. 26).

Bootable Agent

Ein bootfähiges Notfallwerkzeug, das die Backup-Funktionalität des Acronis vmProtect-Agenten (S. 86) enthält. Es ist typisch für die P2V (S. 92)-Migration. Der bootfähige Agent basiert auf einem Linux-Kernel. Eine Maschine kann mit Hilfe eines bootfähigen Mediums (S. 88) in den bootfähigen Agenten gestartet werden.. Aktionen können nur lokal über die grafische Benutzeroberfläche konfiguriert und gesteuert werden.

Bootfähiges Medium

Ein physikalisches Medium (CD, DVD, USB-Stick oder ein anderes Medium, das vom BIOS der Maschine als Boot-Medium unterstützt wird), das den bootfähigen Agenten (S. 88) enthält.

Acronis vmProtect verwendet bootfähige Medien für das Sichern einer physikalischen Maschine, um dann eine P2V (S. 92)-Migration durchzuführen.

C

CBT (Changed Block Tracking)

Diese Funktion von VMware ESX erkennt, welche Blöcke der virtuellen Laufwerke sich geändert haben und übernimmt nur diese in den Backup- bzw. Replikations-Prozess. Wenn Sie die CBT-Technologie verwenden, steigern Sie die Geschwindigkeit des inkrementellen Backups bis zum 20-fachen.

D

Datenspeicher

Ein logischer Container, der die Dateien virtueller Maschinen und andere für Aktionen mit virtuellen Maschinen notwendige Dateien enthält. Datenspeicher können sich auf verschiedenen Typen physikalischer Speicher befinden, z.B. auf lokalem Storage, iSCSI, Fibre Channel SAN oder NFS. Datenspeicher können auf VMFS oder NFS basieren.

Deduplizierung

Methode, um identische Informationen in verschiedenen Kopien nur einmalig zu speichern.

Acronis vmProtect kann Deduplizierung auf alle Backup-Archive (S. 87) im Format Legacy-Modus (S. 92) oder 'Nur-inkrementell' (S. 86) anwenden. Das reduziert den für Archive benötigten Speicherplatz, den Backup-Datentransfer sowie die Netzwerkauslastung während der Backup-Erstellung.

Deduplizierung von Acronis vmProtect verwaltet nur jeweils die Daten, die sich innerhalb eines bestimmten Backup-Archivs befinden. Werden Backups also in zwei verschiedene Archive gespeichert (auch wenn diese sich am selben Speicherort befinden), so haben diese keine Beziehung zueinander und können duplizierte Daten enthalten.

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum letzten vorangegangenen Voll-Backup (S. 95). Sie müssen auf das entsprechende Voll-Backup zugreifen können, um Daten aus einem differentiellen Backup wiederherstellen zu können.

Direkte Verwaltung

Jede Verwaltungsaktion, die mit Hilfe der Verbindung zwischen Konsole (S. 86) und Agent (S. 91) auf dem Agenten (S. 86) ausgeführt wird.

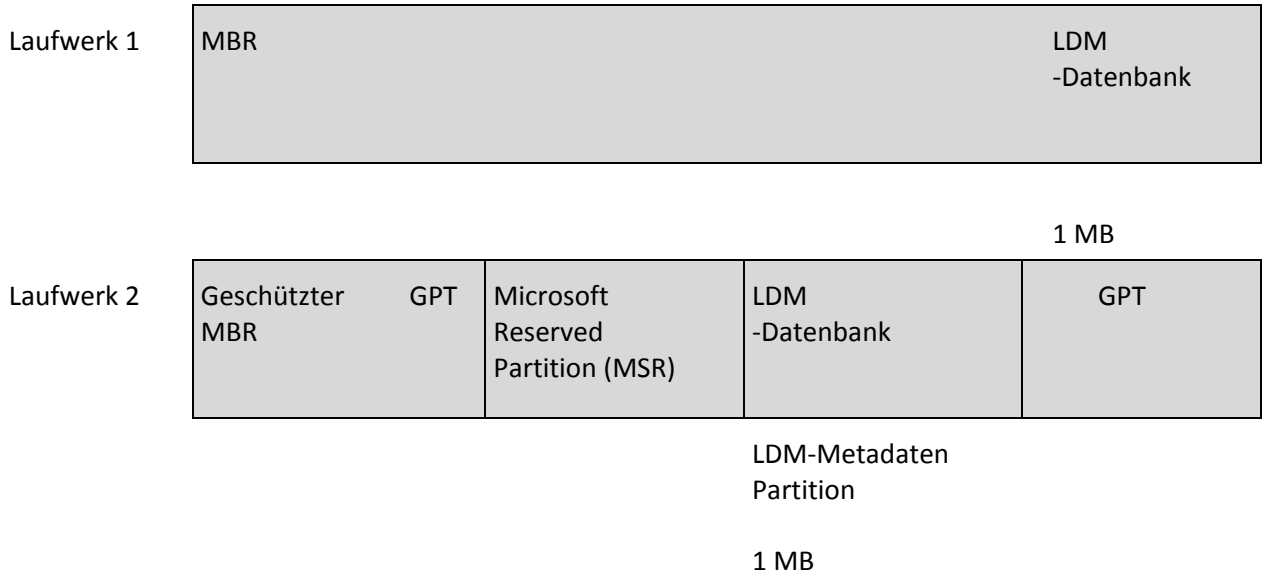
Distributed Resource Scheduler (DRS)

Eine spezifische Funktion des VMware vCenter, die mit Hilfe von vMotion (S. 94) eine automatische Lastverteilung bei einem ESX-Cluster vornimmt.

Dynamisches Laufwerk

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 einem GPT-Laufwerk 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 Laufwerke finden Sie in den folgenden Artikeln der Microsoft Knowledge Base:

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

Dynamisches Volume

Volume, das sich auf einem dynamischen Laufwerk (S. 89) oder genauer auf einer Laufwerksgruppe (S. 91) befindet. Dynamische Volumes können sich über mehrere Laufwerke erstrecken. Dynamische Volumes sind gewöhnlich abhängig vom gewünschten Ziel gestaltet:

- um die Größe zu erweitern (übergreifendes Volume)
- um die Zugriffszeit zu verringern (Stripeset-Volume)
- um die Fehlertoleranz durch redundante Informationen zu erreichen (gespiegelte und RAID-5-Volumes)

Beim Backup virtueller Maschinen, die dynamische Laufwerke enthalten, sichert Acronis vmProtect die logischen dynamischen Volumes anstelle der gesamten dynamischen Laufwerks-Struktur.

G

GVS (Großvater-Vater-Sohn)

Ein gängiges Backup-Schema (S. 87), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 87) und der Anzahl an Recovery-Punkten (S. 92) 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 unter 'Backup-Schema GVS'.

H

Hochverfügbarkeit (HA)

Spezielle Funktion des VMware vCenters, die bei einem Hardware-Fehler im Cluster die virtuellen Server automatisch auf einem anderen Host im Cluster neu startet.

I

Inkrementelles Backup

Backup (S. 86), welches Datenänderungen in Bezug zum letzten Backup speichert. Sie müssen auf andere Backups des gleichen Archivs (S. 86) zugreifen können, um Daten aus einem inkrementellen Backup wiederherstellen zu können.

K

Konsole (Acronis vmProtect Management Console)

Die Konsole ist eine vom Acronis vmProtect-Agenten im Internet bereitgestellte Benutzerschnittstelle, um die Funktionen des Produkts zugänglich zu machen. Auf diese Schnittstelle greifen Sie von jedem unterstützten Internetbrowser aus über eine spezielle URL zu; z.B. https://192.168.0.23:9876/, wobei 192.168.0.23 die IP-Adresse des AcronisPRODUCT_NAME>-Agenten (S. 86) ist und 9876 der Port. Wenn der Administrator eine direkte Internetverbindung zwischen Konsole und Agent herstellt, arbeitet er mit direkter Verwaltung (S. 89).

L

Laufwerksgruppe

Anzahl dynamischer Laufwerke (S. 89), die gemeinsame Konfigurationsdaten in ihren Logical Disk Manager (LDM)-Datenbanken speichern und deshalb als ein Ganzes verwaltet werden können. Normalerweise sind alle dynamischen Laufwerke, die innerhalb der gleichen Maschine erstellt wurden, Mitglieder der gleichen Laufwerksgruppe.

Sobald das erste dynamische Laufwerk vom LDM oder einem anderen Werkzeug zur Laufwerksverwaltung erstellt wird, kann der Name der Laufwerksgruppe im Registry-Key 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name' gefunden werden.

Die als nächstes erstellten oder importierten Laufwerke werden der gleichen Laufwerksgruppe hinzugefügt. Die Gruppe existiert solange, wie wenigstens eines ihrer Mitglieder existiert. Sobald das letzte dynamische Laufwerk von der Maschine getrennt oder in ein Basis-Laufwerk konvertiert wurde, wird die Gruppe stillgelegt, ihr Name bleibt jedoch im oben genannten Registry-Key erhalten. Falls ein dynamisches Laufwerk erneut erstellt oder angeschlossen wird, wird eine Laufwerksgruppe mit einem inkrementellen Namen erstellt.

Wenn eine Laufwerksgruppe zu einer anderen Maschine verschoben wird, wird sie als „fremd“ betrachtet und kann nicht benutzt werden, bis sie in eine existierende Laufwerksgruppe importiert wird. Der Import aktualisiert die Konfigurationsdaten auf den lokalen und 'fremden' Laufwerken, damit sie eine Einheit bilden. Wenn auf der Maschine keine Laufwerksgruppe existiert, wird die 'fremde' Gruppe so, wie sie ist, importiert (behält ihren ursprünglichen Namen).

Weitere Informationen über Laufwerksgruppen finden Sie auf in folgendem Knowledge Base-Artikel von Microsoft:

222189 Beschreibung der Datenträgergruppen in der Windows Datenträgerverwaltung http://support.microsoft.com/kb/222189/DE-DE/.

Legacy-Modus-Archiv

Siehe Backup-Archiv (S. 87).

M

Maschine (virtuelle Maschine)

Ein virtueller Computer, der anhand seiner Betriebssysteminstallation eindeutig identifiziert wird.

Media Builder

Spezielles Werkzeug zur Erstellung bootfähiger Medien (S. 88).

P

P2V

Migration einer physikalischen Maschine in eine virtuelle Umgebung. Ein typischer P2V-Prozess umfasst folgende Schritte:

- Das Backup einer physikalischen Maschine mit Hilfe spezieller bootfähiger Medien (S. 88) erstellen;
- Wiederherstellen dieses Backups in einer virtuellen Umgebung (ESX/ESXi-Server).

R

Recovery-Punkt

Tag und Zeitpunkt, zu dem die gesicherten Daten wiederhergestellt werden können.

Registrierte Maschine

Eine vom Acronis vmProtect-Agenten verwaltete virtuelle Maschine. Alle virtuellen Maschinen, die sich auf einem registrierten ESX/ESXi-Host oder vCenter befinden, werden automatisch registriert und können vom Acronis vmProtect-Agenten verwaltet werden.

Replikation

Ein Prozess, um virtuelle Maschinen zu einem neuen Speicherort zu replizieren (neuer Datenspeicher bzw. Ressourcenpool). Das Ergebnis dieses Prozesses ist eine duplizierte virtuelle Maschine, die unabhängig von der ursprünglichen ausgeführt wird.

Ressourcenpool

Ein VMware-Begriff, der das Konzept der Ressourcenverwaltung in einer virtualisierten ESX-Umgebung beschreibt. Ein Ressourcenpool ermöglicht die Aufteilung der Ressourcen eines autonomen ESX-Hosts oder eines ESX-Clusters in kleinere Pools. Konfiguriert wird der

Ressourcenpool mit der CPU- und Arbeitsspeicherleistung, die sich die in dem Ressourcenpool laufenden virtuellen Maschinen teilen. Ressourcenpools sind unabhängig und isoliert von anderen Ressourcenpools.

Mehrere physikalische Server können zu einem einzigen Ressourcenpool kombiniert werden und so die CPU- und Arbeitsspeicherkapazitäten verbinden.

Virtuelle Maschinen werden in Ressourcenpools ausgeführt und ziehen gleichzeitig ihre Ressourcen aus ihnen. So ermöglicht der Ressourcenpool den virtuellen Maschinen ein ständiges Gleichgewicht in ihrer Auslastung. Wenn die Auslastung ansteigt, weist der vCenter-Server automatisch zusätzliche Ressourcen zu und migriert virtuelle Maschinen transparent zwischen den Hosts im Ressourcenpool.

S

Storage vMotion

Spezielle Funktion des VMware vCenters, die das Verschieben einer laufenden virtuellen Maschine von einem Speichergerät zu einem anderen erlaubt.

T

Task

Bei Acronis vmProtect ist ein Task eine Abfolge von Aktionen auf einer registrierten Maschine zu einer festgelegten Zeit oder beim Eintreten eines bestimmten Ereignisses. Die Handlungen sind in einer XML-Skriptdatei beschrieben. Die Startbedingungen (Planung) stehen in geschützten Registry-Schlüsseln (beim Windows-basierten Agenten) oder in geschützten Dateien (bei Appliance-basierten Agenten).

U

Universal Restore (Acronis 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.

Acronis vmProtect verwendet die Universal Restore Technology vor allem für Szenarien bei P2V (S. 92)-Migration.

Universal Restore ist nicht verfügbar bei der Wiederherstellung eines Linux-Systems.

V

Validierung

Aktion, mit der die Möglichkeit einer Datenwiederherstellung aus einem Backup (S. 86) geprüft wird.

Die Validierung des Backups einer virtuellen Maschine berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Dieses Verfahren erfordert eine intensive Ressourcennutzung.

Obwohl eine erfolgreiche Validierung eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, werden nicht alle Faktoren geprüft, die eine Wiederherstellung beeinflussen. Wenn Sie ein Betriebssystem sichern, kann nur eine probeweise durchgeführte

Wiederherstellung zu einer neuen bzw. existierenden virtuellen Maschine oder das Ausführen der virtuellen Maschine aus dem Backup eine später erfolgreiche Wiederherstellung garantieren.

Validierungsregeln

Teil eines Backup-Tasks (S. 87). Richtlinien definieren, wann und wie oft eine Validierung durchzuführen ist und ob das gesamte Archiv (S. 86) zu validieren ist oder nur das dort enthaltene letzte Backup.

vApp

Eine Gruppe virtueller Maschinen, die als ein einziges Objekt verwaltet werden können. vApps vereinfachen die Verwaltung komplexer vielstufiger Anwendungen, die auf mehreren unabhängigen virtuellen Maschinen laufen. vApps verfügen über dieselben Basis-Aktionen wie virtuelle Maschinen und Ressourcenpools. Mit vApps bestimmen Sie die Reihenfolge, in der die virtuellen Maschinen im vApp eingeschaltet werden, weisen ihnen automatisch IP-Adressen zu und ermöglichen Anpassungen auf Anwendungsebene.

Bei Acronis vmProtect werden vApps als Container für VMs betrachtet. Dieser Container hat eigene Eigenschaften, die beim Backup mitgesichert werden und zusammen mit vApp wiederhergestellt werden, sobald Teile davon (oder das gesamte vApp) wiederhergestellt werden.

vCenter

Ein VMware vCenter-Server, vormals VMware VirtualCenter, verwaltet zentral VMware vSphere-Umgebungen und bieten IT-Administratoren, verglichen mit anderen Verwaltungsplattformen, erheblich verbesserte Funktionen zur Steuerung der virtuellen Umgebung.

Weitere Details finden Sie hier: http://www.vmware.com/products/vcenter-server/

Bei Acronis vmProtect wird das vCenter als Container für die virtuelle ESX-Infrastruktur angesehen, inklusive Datacenter, ESX-Hosts usw.

Verschlüsseltes Archiv

Ein Backup-Archiv (S. 87), das nach dem Advanced Encryption Standard (AES) verschlüsselt ist. Ist die Verschlüsselungsoption und ein Kennwort für das Archiv in den Backup-Optionen (S. 87) definiert, dann wird jedes zum Archiv gehörende Backup vom Agenten (S. 86) noch vor dem Ablegen des Backups am Zielort 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 verschlüsselt, wobei ein SHA-256-Hash-Wert des Kennworts als Schlüssel dient. Das Kennwort selbst wird nirgendwo auf dem Laufwerk oder in der Backup-Datei gespeichert, der Kennwort-Hash dient nur der Verifikation. Mit dieser zweistufigen Methode sind die gesicherten Daten vor unberechtigtem Zugriff geschützt – ein verlorenes Kennwort kann daher jedoch auch nicht wiederhergestellt werden.

vMotion

Eine spezielle Funktion des VMware vCenters, die die Migration operationaler virtueller Gast-Maschinen zwischen ähnlicher aber separater Hardware-Hosts, die den selben Storage teilen, ermöglicht. Jede dieser Überleitungen ist während der Migration für alle Benutzer der virtuellen Maschine völlig transparent.

Voll-Backup

Ein selbstständiges Backup (S. 86), das alle für ein Backup ausgewählten Daten enthält. Um die Daten aus einem Voll-Backup wiederherzustellen, benötigen Sie kein weiteres Backup.