Acronis

Acronis® vmProtect™ 8

Benutzeranleitung

Urheberrechtserklärung

Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch folgende Patente abgedeckt: U.S. Patent # 7,047,380; U.S. Patent # 7,246,211; U.S. Patent # 7,318,135; U.S. Patent # 7,366,859; U.S. Patent # 7,636,824; U.S. Patent # 7,831,789; U.S. Patent # 7,886,120; U.S. Patent # 7,934,064; U.S. Patent # 7,949,635; U.S. Patent # 7,979,690; U.S. Patent # 8,069,320; U.S. Patent # 8,073,815; U.S. Patent # 8,074,035.

Inhaltsverzeichnis

1 Einführung in Acronis vmProtect 8 7

2 Acronis vmProtect 8 – Überblick 8

2.1 Funktionen von Acronis vmProtect 8 8

3 So funktioniert Acronis vmProtect 9

3.1 Backup und Wiederherstellung von virtuellen Maschinen 9

3.2 Backup-Archivstruktur 9

3.2.1 Backup-Schema mit mehreren Dateien (Legacy-Modus) 9

3.2.2 Backup-Schema mit einer einzelnen Datei (Modus 'Nur inkrementell') 10

4 Installation von Acronis vmProtect 11

4.1 Voraussetzungen 11

4.1.1 Unterstützte Betriebssysteme 11

4.1.2 Systemanforderungen 11

4.1.3 So installieren Sie die VMWare Tools 13

4.1.4 Berechtigungen für Backup und Recovery von VMs 13

4.2 Installationsoptionen 16

4.2.1 Acronis vmProtect 8 als virtuelle Appliance auf einem ESX(i)-Host installieren 17

4.2.2 Acronis vmProtect 8 als Windows Agenten installieren 18

4.2.3 Installationsdateien extrahieren 20

4.2.4 Konfiguration der Verbindungseinstellungen des ESX(i)-Hosts 21

4.2.5 Einen lokal angeschlossenen Storage verwenden 21

4.3 Deinstallation von Acronis vmProtect 22

5 Erste Schritte 23

5.1 Dashboard-Verwaltung 24

5.2 Die Webkonsole verwenden 25

5.2.1 Registerkarten im Menüband 25

5.2.2 Link 'Abmeldung' 28

6 vCenter-Integration 29

7 Backups von virtuellen Maschinen erstellen 33

7.1 Wählen Sie die zu sichernden VMs 33

7.2 Backup-Zeitpunkt 34

7.3 Backup-Ziel 35

7.4 Art des Backups 40

7.4.1 Exchange-aware Backup-Einstellungen 40

7.4.2 Backup-Validierung 41

7.4.3 Andere Einstellungen 42

7.4.4 Fertigstellen des Assistenten 'Backup-Task erstellen' 42

7.5 Optionen 42

7.5.1 Schutz des Archivs 42

7.5.2 Ausschluss von Quelldateien 43

7.5.3 Komprimierungsgrad 43

7.5.4 Fehlerbehandlung 44

7.5.5 Desaster-Recovery-Plan 44

7.5.6 Benachrichtigungen 45

7.5.7 Erweiterte Einstellungen 47
7.6 Erstellten Backup-Task verwalten 47
8 Replikation 48
8.1 Neuer Replikations-Task 48
8.1.1 Wählen Sie die zu replizierenden VMs 48
8.1.2 Replikationszeitpunkt 49
8.1.3 Speicherort und Datenspeicher für das Replikat wählen 50
8.1.4 Optionen für Replikations-Task 50
8.2 Replizierte VMs verwalten 51
8.2.1 Manager für replizierte VMs 51
8.2.2 Failover 52
8.2.3 Failback-VM vom Replikat 53
8.2.4 VM-Replikat löschen 55
9 Backups von virtuellen Maschinen wiederherstellen 56
9.1 Wählen Sie die wiederherzustellenden VMs 56
9.2 Recovery-Ziel 57
9.3 Art der Wiederherstellung 60
9.4 Optionen 61
9.4.1 Benachrichtigungen 61
9.4.2 Fehlerbehandlung 62
9.4.3 VM-Energieverwaltung 62
9.4.4 Erweiterte Einstellungen 63
9.4.5 Recovery-Einstellungen für den Exchange Server 63
9.5 Erstellten Recovery-Task verwalten 63
10 Exchange-Server-Backup-Extraktion 64
10.1 Datenbanken extrahieren 64
10.2 Postfächer extrahieren 66
10.3 Postfachinhalte extrahieren 68
11 VM von Backup ausführen 70
11.1 Wählen Sie die VMs, die von einem Backup ausgeführt werden sollen 70
11.2 Ort der VM-Ausführung 71
11.3 Erweiterte Einstellungen 73
11.4 Verwalten der Aktion 'VM von Backup ausführen' 74
12 Datei-Recovery 75
12.1 Wählen Sie die VMs, aus denen Dateien extrahiert werden sollen 75
12.2 Recovery-Punkt durchsuchen 76
13 P2V-Migration 78
13.1 So führen Sie eine P2V-Migration aus 78
14 ESXi-Hosts auf fabrikneuer Hardware wiederherstellen (Bare Metal Recovery) 79
14.1 Backup einer ESXi-Host-Konfiguration 79
14.2 Recovery einer ESXi-Host-Konfiguration 82

15 Tasks verwalten 85
15.1 Einen Task ausführen 85
15.2 Einen Task abbrechen 86
15.3 Einen Task bearbeiten 86
15.4 Einen Task löschen 86
15.5 Task-Logs ansehen 86
15.6 Task-Details ansehen 86
16 Recovery-Punkte verwalten 89
16.1 Einen Backup-Speicherort hinzufügen 90
16.2 Der Katalog 'Virtuelle Maschinen' 91
16.3 Liste der Recovery-Punkte 92
16.4 Registerkarte 'Zusammenfassung' 92
16.5 Aktionen mit ausgewählten Elementen 92
16.5.1 Recovery 93
16.5.2 Exchange-Recovery 93
16.5.3 VM von Backup ausführen 93
16.5.4 Datei-Recovery 93
16.5.5 Validieren 93
16.5.6 Löschen 93
17 Andere Aktionen 94
17.1 Backups validieren 94
17.1.1 Validierungsquelle 94
17.2 Gemountete VMs verwalten 96
17.2.1 Liste 'Gemountete VMs' 96
17.2.2 Details der gemounteten VMs 97
17.2.3 VMs trennen 98
17.3 Logs verwalten 98
17.3.1 Liste der Logs 98
17.3.2 Logs bereinigen 99
17.3.3 Log-Bereinigungsregeln 100
17.3.4 Logs in Datei speichern 101
17.4 Lizenzen verwalten 101
17.4.1 Lizenz hinzufügen 102
17.4.2 Fehler beim Hinzufügen von Lizenzen 103
17.4.3 Lizenz bzw. ESX(i)-Host entfernen 103
17.4.4 Verfügbare Lizenzen 103
17.5 ESX(i)-Hosts verwalten 104
17.5.1 Liste der ESX(i)-Hosts 104
17.5.2 ESX(i)-Host hinzufügen 105
17.5.3 ESX(i)-Host hinzufügen, der Teil eines vCenters ist 106
17.5.4 Anmeldedaten 106
17.5.5 ESX(i)-Host entfernen 107
17.6 Einstellungen verwalten 108
17.6.1 Online Backup-Proxy verwalten 108
17.6.2 Kennwort für Agenten verwalten 109

18 Optimale Vorgehensweisen 110
18.1 Backups von virtuellen Maschinen auf einer Netzwerkfreigabe erstellen 110
18.2 Wiederherstellen eines Virtuelle-Maschinen-Backups an einem neuen Speicherort 111
18.3 Recovery von Dateien und Ordnern 111
19 Support 112
19.1 Technischer Support 112
19.2 Fehlerbehebung (Troubleshooting) 112
20 Glossar 113

1 Einführung in Acronis vmProtect 8

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 8 – Überblick

Acronis vmProtect 8 ist eine umfassende Backup- und Recovery-Lösung für VMware vSphere™-Umgebungen. Sie ermöglicht Organisationen das Erstellen von Backups kompletter virtueller ESX(i)-Maschinen ohne Einsatz des Agenten sowie die Wiederherstellung kompletter Maschinen oder einzelner Dateien und Ordner.

2.1 Funktionen von Acronis vmProtect 8

Mit der preisgekrönten Imaging-Technologie von Acronis erstellt Acronis vmProtect 8 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(i)-Host wiederherstellen. Eine der wichtigsten neuen Funktionen ist die Möglichkeit, eine virtuelle Maschine ohne Wiederherstellung direkt aus dem Backup zu starten – und so die VM nach einem Ausfall in nur wenigen Sekunden wieder betriebsbereit zu machen.

Weitere neue Funktionen sind z.B.:

- Die Auswahlmöglichkeit zwischen virtueller Appliance und Windows-basierter Installation
- Webbasierte und einfach zu bedienende Benutzeroberfläche
- LAN-freies Backup mit Direktzugriff auf freigegebenen Storage
- Schnelle Wiederherstellung durch sofortiges Ausführen einer VM von einem Backup auf einem vorhandenen ESX(i)-Host
- Neues, erweitertes 'Nur inkrementell'-Speicherformat für Backups
- Gleichzeitige Backups mehrerer virtueller Maschinen
- Unterstützung für die vApp- und Ressourcenpool-Einstellungen für Backup bzw. Recovery
- Unterstützung von Changed Block Tracking (CBT)
- Desaster-Recovery-Plan

Die wichtigsten Vorteile von Acronis vmProtect 8 sind:

1. **Einfach zu bedienen:** Acronis vmProtect 8 kann entweder als virtuelle Appliance bereitgestellt oder auf einer Windows-Maschine installiert und über die brandneue webbasierte Schnittstelle verwaltet werden. Dank der Erfahrungen von Acronis im Design intuitiver Schnittstellen sowie der Fokussierung auf VMware ist eine Benutzeroberfläche entstanden, die einen sofortigen Einsatz ohne großes Lesen bzw. Suchen in der Programmdokumentation ermöglicht und kritische Fehler bei der Bedienung oder Konfiguration verhindert.
2. **Mehr Funktionalität:** Zusätzlich zu den Standardfunktionen Backup und Wiederherstellung bietet vmProtect 8 einzigartige Funktionalität wie beispielsweise: Das Ausführen einer virtuellen Maschine direkt von einem Backup; eine unbegrenzte Anzahl von P2V-Konvertierungen; Backups zum Cloud-basierten Acronis Online Storage; Industriestandard 256-Bit-Verschlüsselung zum Schutz der Backups.
3. **Geringe TCO (Total Cost of Ownership):** Die Anschaffungskosten für vmProtect 8 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

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 Agenten installiert haben, können Sie folgende Aktionen ausführen:

- 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 des Backups online ('läuft'), offline ('gestoppt') oder 'angehalten' sein oder zwischen diesen Stadien umschalten.

Während der Wiederherstellung auf eine virtuelle 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. 33) und 'Backups von virtuellen Maschinen wiederherstellen' (S. 56).

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

4.1 Voraussetzungen

4.1.1 Unterstützte Betriebssysteme

Acronis vmProtect 8 unterstützt folgende Betriebssysteme:

- Windows XP Professional SP2 (x64), SP3 (x86)
- 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 8
- Windows Server 2008 – Standard, Enterprise, Foundation Editionen (x86, x64).
- Windows Small Business Server 2008
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation Editionen.
- Windows Small Business Server 2011
- Windows Server 2012

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 8	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 8 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 8 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 8 unterstützen:

- VMware vSphere (Virtual Infrastructure)
- Server-Typen: ESX und ESXi
- Versionen: 4.1, 5.0, 5.1.
- Editionen/Lizenzen
  - VMware vSphere Standard (der Hot-Add-Backup-Modus wird nur unter vSphere 5.0+ unterstützt).
  - VMware vSphere Advanced
  - VMware vSphere Enterprise
  - VMware vSphere Enterprise Plus

- VMware vSphere Standard (der Hot-Add-Backup-Modus wird nur unter vSphere 5.0+ unterstützt).
- VMware vSphere Essentials Plus (der Hot-Add-Backup-Modus wird nur unter vSphere 5.0+ unterstützt).

VMware vSphere Hypervisor (Free ESXi) wird NICHT unterstützt.

Die ESX(i) Version 4.0-Umgebung wird mit Einschränkungen unterstützt; so werden beispielsweise die Funktionen Exchange-Server-Backup-Extraktion (S. 64) und ESXi-Konfigurations-Backup (S. 79) nicht unterstützt.

Die Acronis vmProtect 8-Funktion 'Exchange-Server-Backup extrahieren (S. 64)' unterstützt Microsoft Exchange ab Version 2003 SP2 und höher. Die Funktion Exchange-Server-Backup-Extraktion von Acronis vmProtect 8 unterstützt KEINE Exchange-Datenbanken, die sich auf auf dynamischen Laufwerken von Windows (LDM) befinden.

Acronis vmProtect 8 unterstützt bei den gesicherten virtuellen Maschinen folgende Dateisysteme: NTFS/FAT16/FAT32/ext2/ext3/ext4/ReFS. Bei anderen VM-Dateisystemen wird der Backup-Modus 'Sektor-für-Sektor' verwendet, was bedeutet, dass für solche Archive keine granuläre Wiederherstellung möglich ist (es können also nur komplette VMs wiederhergestellt werden). Beispiele für nicht unterstützte Dateisysteme sind LVM-Volumes von Linux (oder dynamische Datenträger von Windows). Sie werden im Sektor-für-Sektor-Backup-Modus gesichert.

Beachten Sie, dass folgende Umgebungen für Backup- und Recovery-Aktionen NICHT unterstützt werden:

- RDM-Laufwerke (Raw Device Mapping)
- Fehlertoleranz-VMs

Außerdem können unabhängige virtuelle Laufwerke NICHT gesichert werden, während die virtuelle Maschine eingeschaltet ist. Schalten Sie eine solche VM vor dem Backup aus.

Um den problemlosen Betrieb der Acronis vmProtect 8 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

Zur korrekten Nutzung der Webkonsole mit dem IE 8 sollten Sie Ihre Internet-Einstellungen überprüfen. Die Einstellung unter **Extras** –> **Internetoptionen** –> Registerlasche **Sicherheit** –> **Internet** –> **Sicherheitsstufe** sollte nicht auf 'Hoch' stehen. Die Sicherheitsstufe in der Registerlasche **Datenschutz** sollte auf 'Mittelhoch' oder niedriger eingestellt sein.

Zur korrekten Nutzung der Webkonsole mit dem IE 9 sollten Sie Ihre Internet-Einstellungen überprüfen. Die Option **Extras** –> **Internetoptionen** –> **Erweitert** –> '**Verschlüsselte Seiten nicht auf dem Datenträger speichern**' muss deaktiviert sein. Anderenfalls wird die Funktion **Datei-Recovery** nicht korrekt arbeiten.

4.1.3 So installieren Sie die VMWare Tools

Acronis vmProtect 8 erfordert die Installation von VMware Tools auf den virtuellen Maschinen, die gesichert werden sollen. Nur so lässt sich eine einwandfreie Stilllegung des Dateisystems gewährleisten (VSS-Unterstützung verwenden) und die Möglichkeit, Dateien oder Ordner auszuschließen, aktivieren. So installieren Sie die VMware Tools:

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

Beachten Sie, dass für die Funktion **VM von Backup ausführen** ein VMkernel-Netzwerk auf dem ESX(i)-Server konfiguriert sein muss. Dazu gehen Sie im vSphere Client über **Konfiguration** –> **Netzwerk** und fügen den VMkernel-Verbindungstyp zu den vSwitch-Eigenschaften hinzu.

4.1.4 Berechtigungen für Backup und Recovery von VMs

Sobald der Acronis vmProtect 8 Agent auf einer Windows-Maschine installiert oder auf einem ESX(i)-Host bereitgestellt wurde, sollten Sie zuerst die Konfiguration der durch diesen Agenten verwalteten ESX(i)-Hosts/vCenter durchführen. Der Umfang der verfügbaren Aktionen hängt von den Berechtigungen ab, die ein Benutzer (von Ihnen spezifiziert, beim Hinzufügen eines ESX(i)-Hosts/vCenters in der vmProtect 8 Agent Web Console: **Konfigurieren** –> **ESX(i)-Hosts**) auf dem vCenter Server hat. Es stehen nur solche Aktionen zur Verfügung, die dieser Benutzer ausführen darf. Die unteren Tabellen enthalten die Berechtigungen, die für Backup und Recovery von virtuellen ESX(i)-Maschinen sowie für ein Virtual Appliance-Deployment benötigt werden.

Berechtigungen auf einem vCenter Server oder ESX(i)-Host

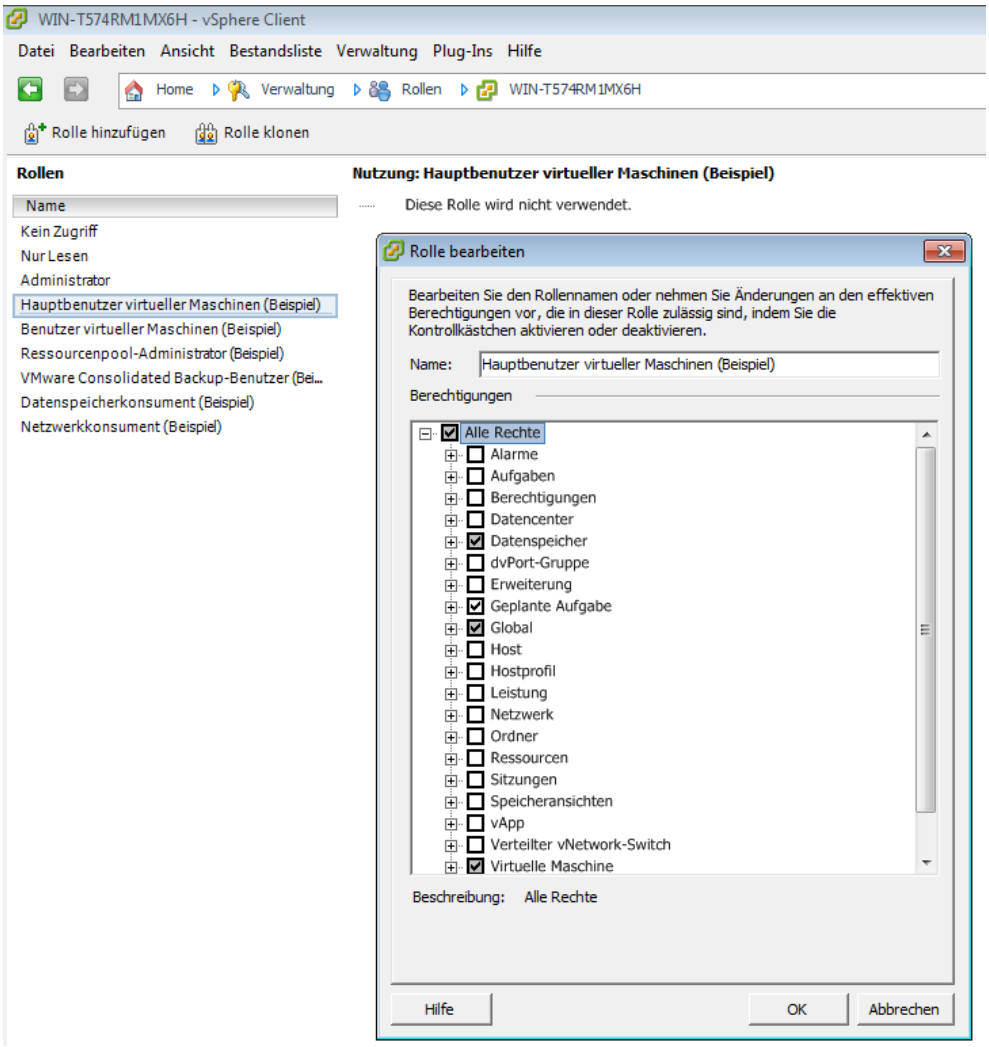
Die untere Tabelle erläutert die Berechtigungen, die der Benutzer eines vCenter-Servers haben muss, um Aktionen auf allen vCenter-Hosts und -Clustern ausführen zu können.

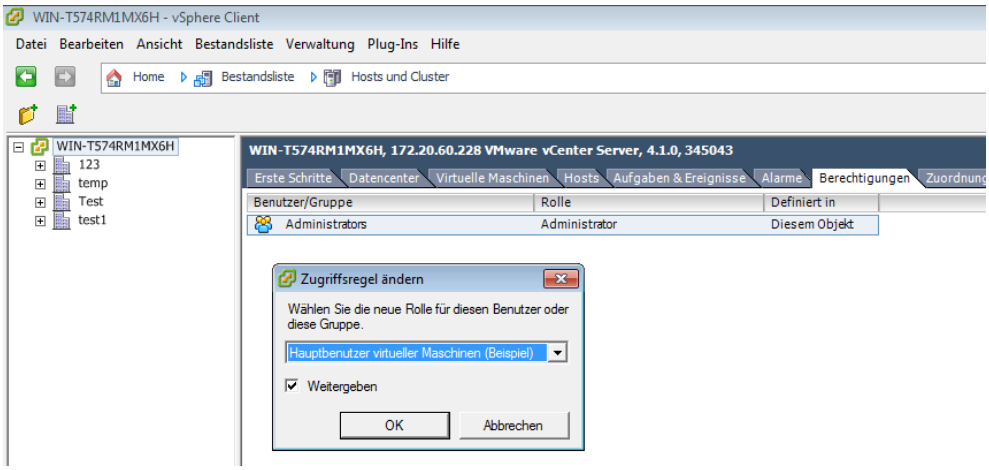
Um festzulegen, dass ein Benutzer nur auf einem bestimmten ESX-Host arbeiten kann, weisen Sie dem Anwender auf dem Host dieselben Berechtigungen zu. Zusätzlich wird die Berechtigung **Global** –> **Lizenzen** benötigt, um die virtuellen Maschinen eines speziellen ESX-Host sichern zu können.

		Aktion				
Objekt	**Recht**	**Backup einer VM**	**Laufwerk einer VM sichern**	**Recovery zu einer neuen VM**	**Recovery zu einer existierenden VM**	**VA-Deployment**
Datenspeicher	**Speicher zuteilen**			+	+	+
	Datenspeicher durchsuchen					+
	Dateivorgänge auf niedriger Ebene					+

Global	**Lizenzen**	+ (nur auf ESX-Host benötigt)	+ (nur auf ESX-Host benötigt)	+	+	
Netzwerk	**Netzwerk zuweisen**			+	+	+
Ressource	**Virtuelle Maschine zu Ressourcenpool zuweisen**			+	+	+
Virtuelle Maschine –> Konfiguration	**Vorhandene Festplatte hinzufügen**	+	+	+		
	Neues Festplatte hinzufügen			+	+	+
	Gerät hinzufügen oder entfernen			+		+
	CPU-Anzahl ändern			+		
	Arbeitsspeicher			+		
	Festplatte entfernen	+	+	+	+	
	Umbenennen			+		
	Einstellungen				+	
Virtuelle Maschine –> Interaktion	**CD-Medien konfigurieren**			+		
	Konsoleninteraktion					+
	Ausschalten				+	+
	Einschalten			+	+	+
Virtuelle Maschine –> Bestandsliste	**Aus vorhandener erstellen**			+	+	
	Neu erstellen			+	+	+
	Entfernen			+	+	+
Virtuelle Maschine –> Provisioning	**Festplattenzugriff zulassen**			+	+	
Virtuelle Maschine –> Status	**Snapshot erstellen**	+	+		+	+
	Snapshot entfernen	+	+		+	+

Die Rollen-Berechtigungen können über den vSphere Client, der mit einem ESX(i)-Host/vCenter verbunden ist, über **Administration** –> **Rollen** konfiguriert werden. Danach können Sie den spezifischen Benutzer zur Verbindung mit dem vCenter und mit einer bestimmten Rolle festlegen (über die Registerkarte **Berechtigungen**, wie in den unteren Bildern gezeigt).





4.2 Installationsoptionen

Zuerst müssen Sie die Acronis vmProtect 8-Software installieren, die Verbindung mit dem ESX(i)-Host konfigurieren und die Anmeldedaten für die Acronis vmProtect 8-Webkonsole einrichten.

Beim Start des Acronis vmProtect 8-Installationspaketes erscheint das Installationsmenü. Acronis vmProtect 8 bietet drei grundsätzliche Installationsoptionen an:

- **Acronis vmProtect 8 als virtuelle Appliance auf einem ESX(i)-Host installieren**
- **Acronis vmProtect 8 als Windows Agenten installieren**
- **Installationsdateien extrahieren**

Die **erste Option** erlaubt Ihnen das Installieren der Software auf einem Remote-ESX(i)-Host (siehe Acronis vmProtect 8 als virtuelle Appliance auf einem ESX(i)-Host installieren (S. 17)).

Mit der **zweiten Option** können Sie die Acronis vmProtect 8-Software auf einem lokalen Rechner installieren (siehe Acronis vmProtect 8 als Windows Agenten installieren (S. 18).

Mit der **dritten Option** können Sie die Installationsdateien extrahieren (siehe Installationsdateien extrahieren (S. 20)) und Acronis vmProtect 8 entweder remote bereitstellen oder manuell mit Hilfe von Standard-Installationswerkzeugen lokal installieren. Sie können diese Option wählen, 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.

Das Deployment der Acronis vmProtect 8 Virtual Appliance auf einem ESX(i)-Host ist aus mehreren Gründen der Installation von Acronis vmProtect 8 als Windows Agent vorzuziehen. Diese Gründe sind folgende:

1. Sie erhalten LAN-freie Backups ohne zusätzlichen Einrichtungsaufwand (es ist nicht erforderlich, den FC/iSCSI-Speicher mit der Windows-Maschine zu verbinden, auf der der Agent läuft).
2. Die virtuelle Appliance nutzt Hot-Add (Anbindung von virtuellen Laufwerken an die virtuelle Appliance während des Backups), welches gewöhnlich die schnellste Methode ist, um Lesezugriff auf VM-Daten zu erhalten.
3. Bei der virtuellen Appliance bestehen keine Probleme mit der Software-Kompatibilität (wie z.B. NFS Server oder andere Dienste von Drittherstellern, die die Ports blockieren können).
4. Die virtuelle Appliance lässt sich leichter pflegen und benötigt auch keine spezielle Windows-Maschine. Sie ist bei einer vollständig virtualisierten Infrastruktur auf jeden Fall die bessere Alternative.
5. Die virtuelle Appliance lässt sich leichter und schneller installieren.

Der Nachteil der virtuellen Appliance besteht darin, dass der Backup-Prozess die CPU- und Arbeitsspeicherleistung des ESX(i)-Hosts beansprucht; das kann in einer stark ausgelasteten Umgebung problematisch sein. Wenn in einem solchen Fall ein physikalischer Rechner als Konsole für die Verwaltung aller Funktionen von vmProtect 8 zur Verfügung steht, können Sie sich für die lokale Installation des Acronis vmProtect 8 Windows Agenten entscheiden.

4.2.1 Acronis vmProtect 8 als virtuelle Appliance auf einem ESX(i)-Host installieren

Sie können die Acronis vmProtect 8-Software auch direkt auf einem ESX(i)-Host installieren. Dieser Prozess einer Remote-Installation der Acronis vmProtect 8 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 8, 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 8 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 8-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.

   Sollten Sie das vCenter in diesem Schritt spezifizieren, dann können Sie die Option **vCenter-Integration aktivieren** über das entsprechende Kontrollkästchen auswählen.
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 8-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 8-Komponenten erfolgreich bereitgestellt wurden, wird die Seite 'Deployment wurde erfolgreich abgeschlossen' angezeigt. Markieren Sie hier das Kontrollkästchen, um die Acronis vmProtect 8 Web Console (im Standardbrowser) auszuführen und eine Verbindung zur neu bereitgestellten Acronis vmProtect 8 Virtual Appliance herzustellen. Klicken Sie auf **Schließen**. Standardmäßig sind Login und Kennwort für die Acronis vmProtect 8 Web Console admin/root. Beachten Sie: Es wird dringend empfohlen, das Kennwort nach der Erstanmeldung auf der Seite **Konfigurieren** –> **Kennwort für Agenten** zu ändern (weitere Informationen finden Sie im Abschnitt Kennwort für Agenten verwalten (S. 109)). Mit den Standard-Anmeldedaten erfolgt die Anmeldung automatisch. Wenn Sie den Wert des Kennworts für Agenten verändert haben, erscheint bei der Verbindung mit der Webkonsole das Standard-Anmeldefenster.

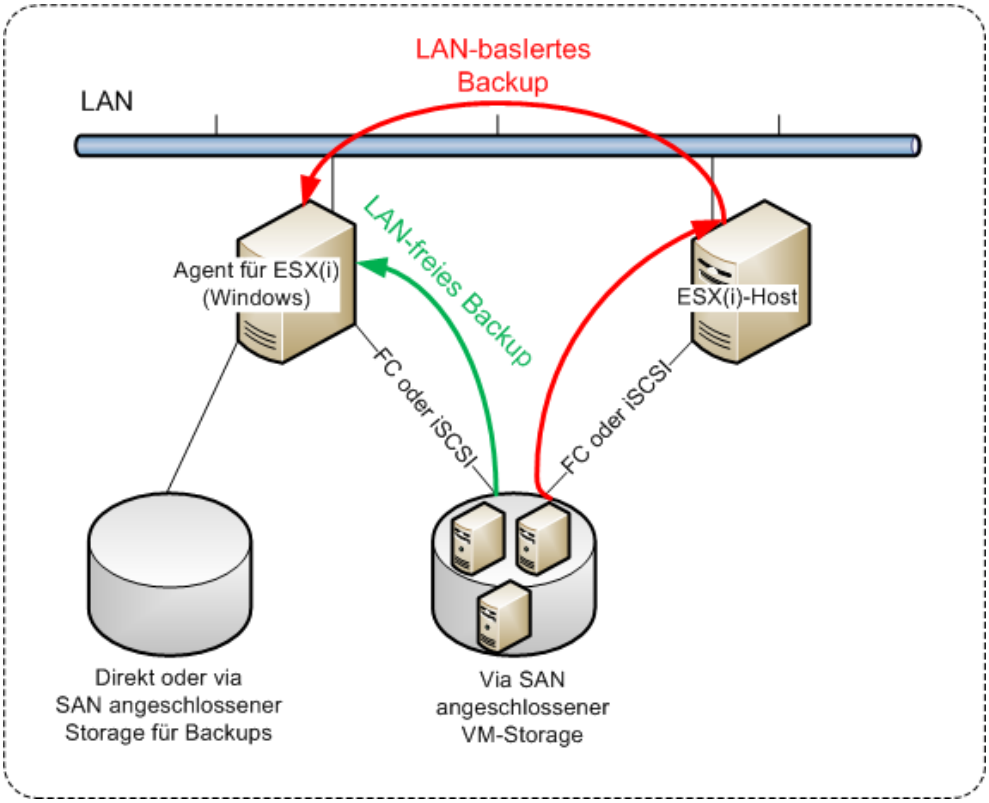
Bei Auftreten eines Problems wird die virtuelle Appliance (bzw. die Teile, die bereits während der Installation bereitgestellt wurden) automatisch vom ESX(i) entfernt. Die Seite **Installation der vmProtect 8-Komponenten fehlgeschlagen** wird angezeigt. Hier wird eine Zusammenfassung der installierten und nicht installierten Komponenten angezeigt. Der Link **Log anzeigen** öffnet ein Pop-up-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. 112) auf.

4.2.2 Acronis vmProtect 8 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 8 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 8 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 8, 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 8 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 8 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 8 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 8 im Zielordner

C:\Programme\Acronis bzw. C:\Programme (x86)\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 8 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 8-Komponenten erfolgreich installiert wurden, wird die Seite 'Installation wurde abgeschlossen' angezeigt. Aktivieren Sie, falls gewünscht, das Kontrollkästchen, um die Acronis vmProtect 8-Webkonsole auszuführen und klicken Sie auf **Schließen**.

Wenn die Installationsprozedur fehlschlägt und alle oder einige Acronis vmProtect 8-Komponenten aus irgendeinem Grund nicht installiert werden konnten, wird die Seite 'Installation der vmProtect 8-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. 112) auf.

4.2.3 Installationsdateien extrahieren

Das Acronis vmProtect 8-Installationspaket bietet Ihnen die Möglichkeit, die Installationsdateien auf Ihren Rechner zu extrahieren und dann manuell auszuführen und mithilfe von Standardwerkzeugen zu installieren.

Klicken Sie im Hauptmenü für die Acronis vmProtect 8-Installation auf den Eintrag **Installationsdateien extrahieren**. Wählen Sie die Komponenten aus, die als separate Installationsdateien auf dem Rechner gespeichert werden sollen:

- AcronisESXAppliance.ovf und zwei vmdk-Dateien – Installationsdateien für die Acronis Virtual Appliance.
- vmProtectAgent.msi – die Hauptinstallationsdatei für den Acronis vmProtect 8 Windows Agenten.
- vmProtectExchangeBackupAgent.msi – die Installationsdatei für den Acronis vmProtect 8 Exchange Backup Agenten. Dieser Agent kann innerhalb eines Gast-Betriebssystems installiert

werden, in dem die Benutzerkontensteuerung (UAC) aktiviert ist. Er ist dazu gedacht, UAC-Beschränkungen zu überwinden, um vmProtect 8 Exchange Backup-Optionen zu ermöglichen. Nach der Installation stellt der Dienst des **Acronis vmProtect 8 Exchange Backup Agenten** einen Kommunikationskanal mit dem Acronis vmProtect 8 Agenten bereit.

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 Verbindungseinstellungen des ESX(i)-Hosts

Detaillierte Informationen über das Einrichten und die Konfiguration der Anmeldedaten für eine Verbindung mit dem ESX(i)-Host finden Sie im Abschnitt ESX(i)-Hosts verwalten (S. 104).

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 das Element **Lokale Ordner** und wählen Sie das lokal angeschlossene Speicherlaufwerk, beispielsweise D:\.

Dieselbe Vorgehensweise gilt für das Wiederherstellen von Dateien und andere Aktionen mit Backups.

4.3 Deinstallation von Acronis vmProtect

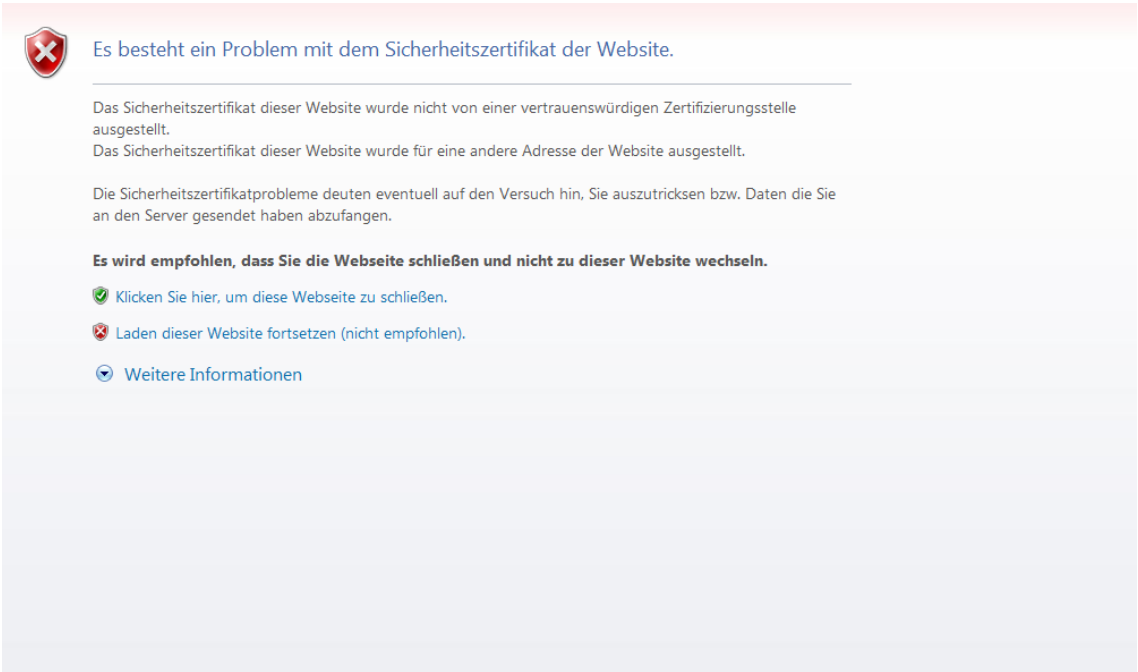
Um den Acronis vmProtect Windows Agenten zu deinstallieren, verwenden Sie das Standardtool von Windows, **Programme hinzufügen oder entfernen**.

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

5 Erste Schritte

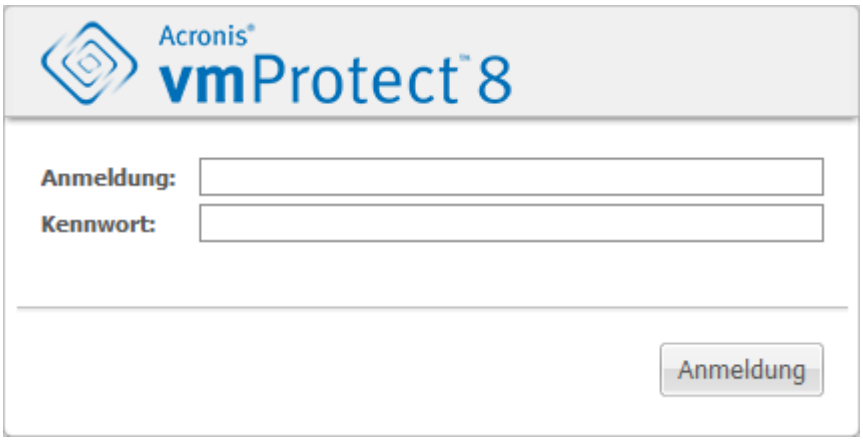
Sobald Sie Acronis vmProtect 8 installiert haben bzw. die Acronis vmProtect 8 Virtual Appliance bereitgestellt ist, können Sie die Acronis vmProtect 8 Web Console ausführen. Die Webkonsole öffnet sich im Standard-Webbrowser.

Beachten Sie, dass der (agentenseitig installierte) Acronis vmProtect 8-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 Ihres Browsers.



Fehlermeldung zum Zertifikat

Wenn sich die Webkonsole im Webbrowser öffnet, wird zunächst ein Anmeldefenster angezeigt, in dem Sie die Anmeldedaten für Acronis vmProtect 8 eintragen müssen. Bei der auf einer virtuellen Appliance basierten Installation sind das Login und Kennwort standardmäßig **admin/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 8 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(i)-Host-Bereich (S. 104) 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(i)-Hosts werden Lizenzen noch nicht automatisch an diesen gebunden. Daher müssen Sie als Nächstes die Lizenzen auf der Lizenzenseite (S. 101) einrichten.
- Nach dem Einrichten der ESX(i)-Hosts und Lizenzen können Sie den Assistenten 'Neuer Backup-Task' (S. 33) ausführen, der Sie durch alle Schritte des Backup-Prozesses führt.

5.1 Dashboard-Verwaltung

Wenn Sie Acronis vmProtect 8 installiert haben und starten (d.h. eine Verbindung zur Acronis vmProtect 8-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 Ihr vCenter, die 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 8-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 8 zur Verfügung stehen, ist es ein sehr nützliches Tool für schnelle operative Entscheidungen.

Zum Dashboard wechseln Sie, indem Sie auf das Acronis vmProtect 8 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.

Aufgaben

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** (**Ansicht** –>**Tasks**) wechseln.

Task-Statistiken

Der Bereich **Task-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.

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. 96)).

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 Registerkarten im Menüband

Über das Menüband oben im Bildschirm können Sie die Software verwalten und alle Bedienfunktionen ausführen. Die grundlegenden Acronis vmProtect 8-Funktionen, auf die über das obere Menü Zugriff besteht, sind in den folgenden Abschnitten beschrieben.

Das Acronis vmProtect 8-Menüband hat drei Hauptregisterkarten: Die Registerkarten **Aktionen**, **Ansicht** und **Konfigurieren**. Eine vierte Acronis-Registerkarte erscheint dynamisch, je nach der aktuell ausgewählten **Ansicht** oder **Konfigurieren**-Aktion.

Ansicht 'Dashboard'

Die in der Menübandleiste immer verfügbare Schaltfläche **Startseite** führt zur Ansicht **Dashboard**. Die Konfiguration des Dashboards wird im Abschnitt 'Dashboard-Verwaltung (S. 24)' beschrieben.

1) Registerkarte 'Aktionen'

Die erste Registerkarte, **Aktionen**, enthält die Basisfunktionen von Acronis vmProtect 8; von hier aus können Sie folgende Basis-Tasks starten:

a. Backup-Task

Über die Schaltfläche **Backup** starten Sie den Assistenten **Neuer Backup-Task**. Die Einstellungen für den Assistenten sind im Abschnitt 'Backups virtueller Maschinen erstellen' (S. 33) beschrieben.

b. Replikations-Task

Über die Schaltfläche **Replikation** starten Sie den Assistenten **Neuer Replikations-Task**. Die Einstellungen für den Assistenten sind im Abschnitt 'Neuer Replikations-Task' (S. 48) beschrieben.

c. Recovery-Task

Über die Schaltfläche **Recovery** starten Sie den Assistenten **Neuer Recovery-Task**. Die Einstellungen für den Assistenten sind im Abschnitt 'Backup virtueller Maschinen wiederherstellen' (S. 56) beschrieben.

d. Task 'Exchange extrahieren'

Über die Schaltfläche **Exchange-Recovery** starten Sie den Assistenten zum **Extrahieren von Exchange Server-Elementen**. Die Einstellungen für den Assistenten sind im Abschnitt 'Exchange-Server-Backup-Extraktion' (S. 64) beschrieben.

c. Task 'VM von Backup ausführen'

Über die Schaltfläche **VM von Backup ausführen** starten Sie den entsprechenden Assistenten. Die Einstellungen für den Assistenten sind im Abschnitt 'VM von Backup ausführen' (S. 70) beschrieben.

f. Datei-Recovery-Task

Über die Schaltfläche **Datei-Recovery** starten Sie den 'Datei-Recovery'-Assistenten. Die Einstellungen für den Assistenten sind im Abschnitt 'Datei-Recovery' (S. 75) beschrieben.

g. Validierungstask

Über die Schaltfläche **Validieren** starten Sie einen neuen Validierungstask. Der Task ist im Abschnitt 'Backup validieren' (S. 94) beschrieben.

h. Task für ESXi-Konfigurations-Backup

Über die Schaltfläche **ESXi-Konfigurations-Backup** starten Sie den Assistenten **Neuer ESXi-Backup-Task**. Die Einstellungen für den Assistenten sind im Abschnitt 'Abschnitt 'Bare Metal Recovery von ESXi-Hosts' (S. 79)' beschrieben.

2) Registerkarte 'Ansicht'

Die zweite Registerkarte, **Ansicht**, enthält die wichtigsten Datenansichten für Acronis vmProtect 8 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. 85) beschrieben.

b. Ansicht 'Recovery-Punkte'

Dieser Link öffnet die Ansicht **Recovery-Punkte**. Die Verwaltung der Recovery-Punkte wird im Abschnitt 'Recovery-Punkte verwalten' (S. 89) beschrieben.

c. Ansicht 'Replikate'

Dieser Link öffnet die Ansicht **Replikate**. Die Verwaltung von replizierten VMs ist im Abschnitt 'Replizierte VMs verwalten' (S. 51) beschrieben.

d. Ansicht 'Gemountete VM(s)'

Dieser Link öffnet die Ansicht **Gemountete VM(s)**. Die Verwaltung gemounteter virtueller Maschinen wird im Abschnitt 'Gemountete VMs verwalten (S. 96)' beschrieben.

e. Ansicht 'Logs anzeigen'

Dieser Link öffnet die Ansicht **Logs anzeigen**. Die Log-Verwaltung wird im Abschnitt 'Logs verwalten' (S. 98) beschrieben.

3) Registerkarte 'Konfigurieren'

Die dritte Registerkarte, **Konfigurieren**, enthält die wichtigsten Werkzeuge für die Konfiguration von Acronis vmProtect 8; hier können Sie die Standardeinstellungen für einfache Backup- bzw. Recovery-Aktionen und andere Einstellungen vornehmen.

a. ESX(i)-Hosts

Dieser Link öffnet die Seite zur Verwaltung von **ESX(i)-Hosts**. Die Verwaltung von ESX(i)-Hosts ist im Abschnitt 'ESX(i)-Hosts verwalten' (S. 104) beschrieben.

b. Lizenzen

Dieser Link öffnet die Seite **Lizenzen** verwalten. Die Lizenzverwaltung wird im Abschnitt 'Lizenzen verwalten' (S. 101) beschrieben.

c. Einstellungen

Die Einstellungen für das **Online Backup-Abonnement** und den **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 Registerkarte **Konfigurieren** enthält außerdem zwei Links zu den **Standardeinstellungen für Backup** und **Recovery**. Eine detaillierte Beschreibung der Backup- bzw. Recovery-Einstellungen sowie weiterer Einstellungen finden Sie im Abschnitt 'Einstellungen verwalten' (S. 108).

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) Die dynamische Registerkarte von vmProtect 8

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

a. Ansicht –> Recovery-Punkte

Wenn die Ansicht **Recovery-Punkte** ausgewählt ist, erscheint die Registerkarte **Recovery-Punkte** im Menüband. Die Seite zur Verwaltung der **Recovery-Punkte** wird im Abschnitt 'Recovery-Punkte verwalten' (S. 89) beschrieben.

b. Ansicht –> Replikate

Wenn die Ansicht **Replikate** ausgewählt ist, erscheint die Registerkarte **Replikate** im Menüband. Die Seite zur Verwaltung der **Replikate** ist im Abschnitt 'Replikate verwalten' (S. 48) beschrieben.

c. Ansicht –> Gemountete VM(s)

Wenn die Ansicht **Gemountete VM(s)** ausgewählt ist, erscheint die Registerkarte **Gemountete VM(s)** im Menüband. Die Seite **Gemountete VM(s)** wird im Abschnitt 'Gemountete VMs verwalten (S. 96)' beschrieben.

d. Ansicht –> Logs anzeigen

Wenn die Ansicht **Logs anzeigen** ausgewählt ist, erscheint die Registerkarte **Logs** im Menüband. Die Seite zur Verwaltung der **Logs** wird im Abschnitt 'Logs verwalten' (S. 98) 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.

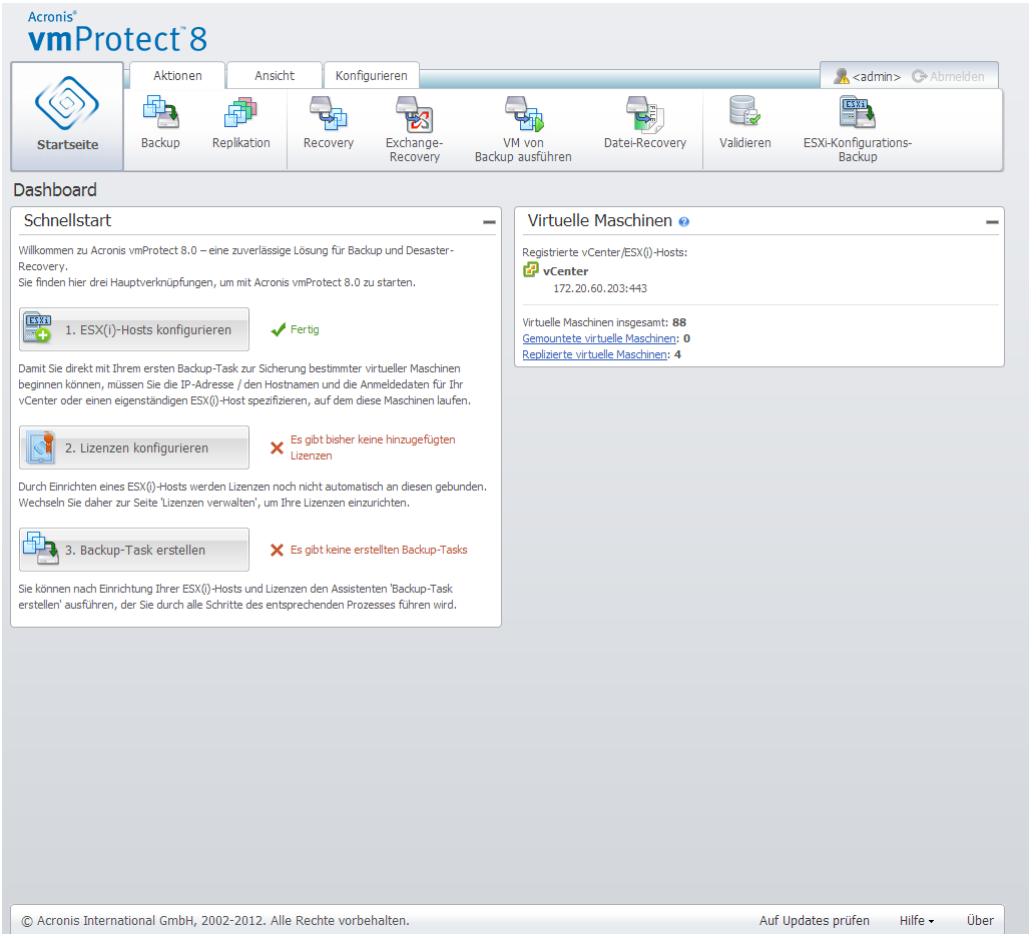
6 vCenter-Integration

Das wichtigste Werkzeug für die Verwaltung der virtuellen Infrastruktur von vSphere ist der VMware vSphere Client. Obwohl der VMware vSphere Client keine eigene Backup- und Recovery-Funktion bietet, ist es nicht immer sinnvoll, ein anderes Tool für das Verwalten dieser wichtigen Aktionen einzusetzen. Acronis vmProtect 8 hat nun eine vCenter-Integration, mit der einfache Backup- und Recovery-Aktionen direkt aus dem VMware vSphere Client heraus ausgeführt werden können, ohne Einsatz der Acronis vmProtect 8 Weboberfläche.

Die Integration mit dem vCenter ist nur möglich, wenn ein vCenter im Acronis vmProtect 8 Agenten registriert ist. Ohne ein registriertes vCenter ist eine solche Integration nicht möglich. Die Integration wird automatisch deaktiviert, wenn ein vCenter aus der Konfiguration des Acronis vmProtect 8 Agenten entfernt wird.

Die Acronis vmProtect 8 vCenter-Integration kann von der vmProtect 8 Web-Oberfläche oder vom vCenter Plug-in Manager aus manuell aktiviert und deaktiviert werden. Um die vCenter-Integration zu aktivieren, gehen Sie zu **Konfigurieren** –> **ESX(i) Hosts** und aktivieren bei Hinzufügen eines neuen vCenters das Kontrollkästchen **vCenter-Integration aktivieren** oder klicken Sie auf die Schaltfläche **vCenter-Integration aktivieren**. Klicken Sie zum Ausschalten der Funktion auf **vCenter-Integration deaktivieren**. Das Anmeldefenster von Acronis vmProtect 8 zeigt die IP-Adresse des Agenten an, in dem die Integration aktiviert wurde.

Die Integration ist bei vSphere-Clients, die mit dem vCenter verbunden sind, unter **Bestandliste** (Inventory) –> **Lösungen und Anwendungen** (Solutions and Applications) -> **Acronis vmProtect 8.0** verfügbar.



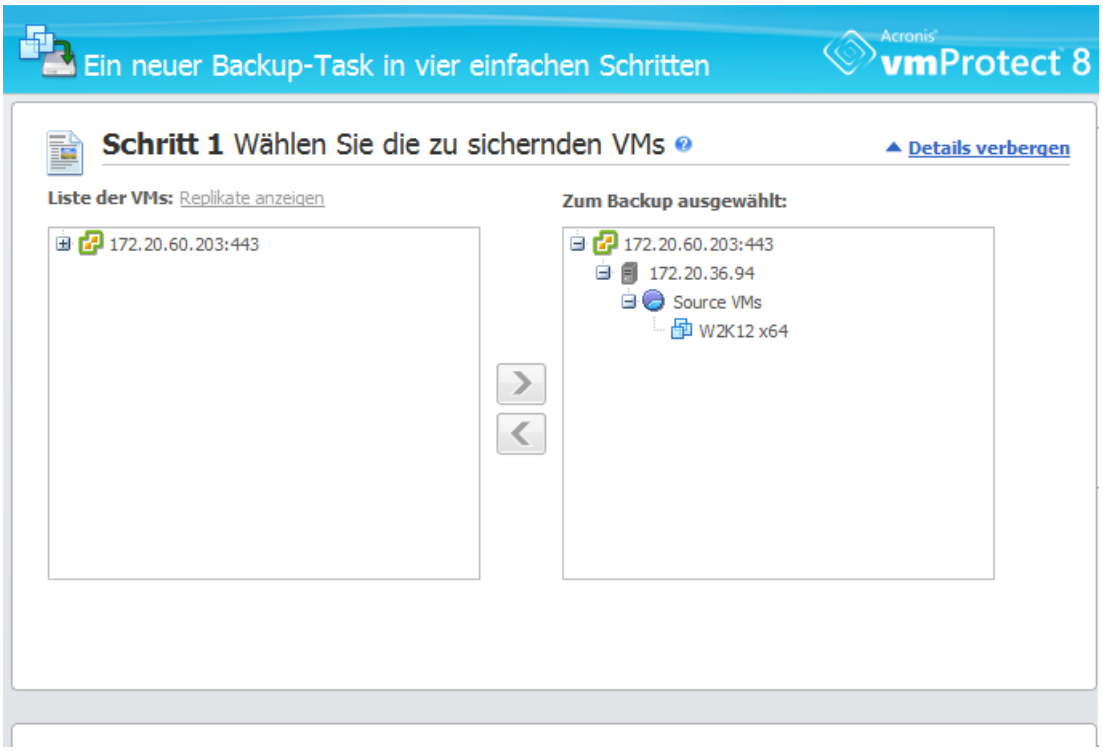
So funktioniert die vCenter-Integration

Mit der vCenter-Integration können Sie direkt von der VMware vSphere-Oberfläche aus Tasks für Backup, Recovery, Replikation etc. erstellen und deren Fortschritt überwachen.

Wählen Sie ein beliebiges Element – virtuelle Maschine, vApp bzw. Ressourcenpool, oder ESX(i)-Host bzw. Cluster – im Verzeichnisbaum der VMware vSphere. Klicken Sie mit der rechten Maustaste auf das ausgewählte Element, um das Kontextmenü zu öffnen. Das Kontextmenü enthält die Optionen **Acronis vmProtect 8 Backup** und **Acronis vmProtect 8 Recovery**. Bei Auswahl einer dieser Optionen öffnet sich das Acronis Pop-up-Fenster und der Assistent für Backup bzw. Recovery wird aktiviert, der Sie beim Erstellen und sofortigen Ausführen eines Backup- bzw. Recovery-Tasks unterstützt.

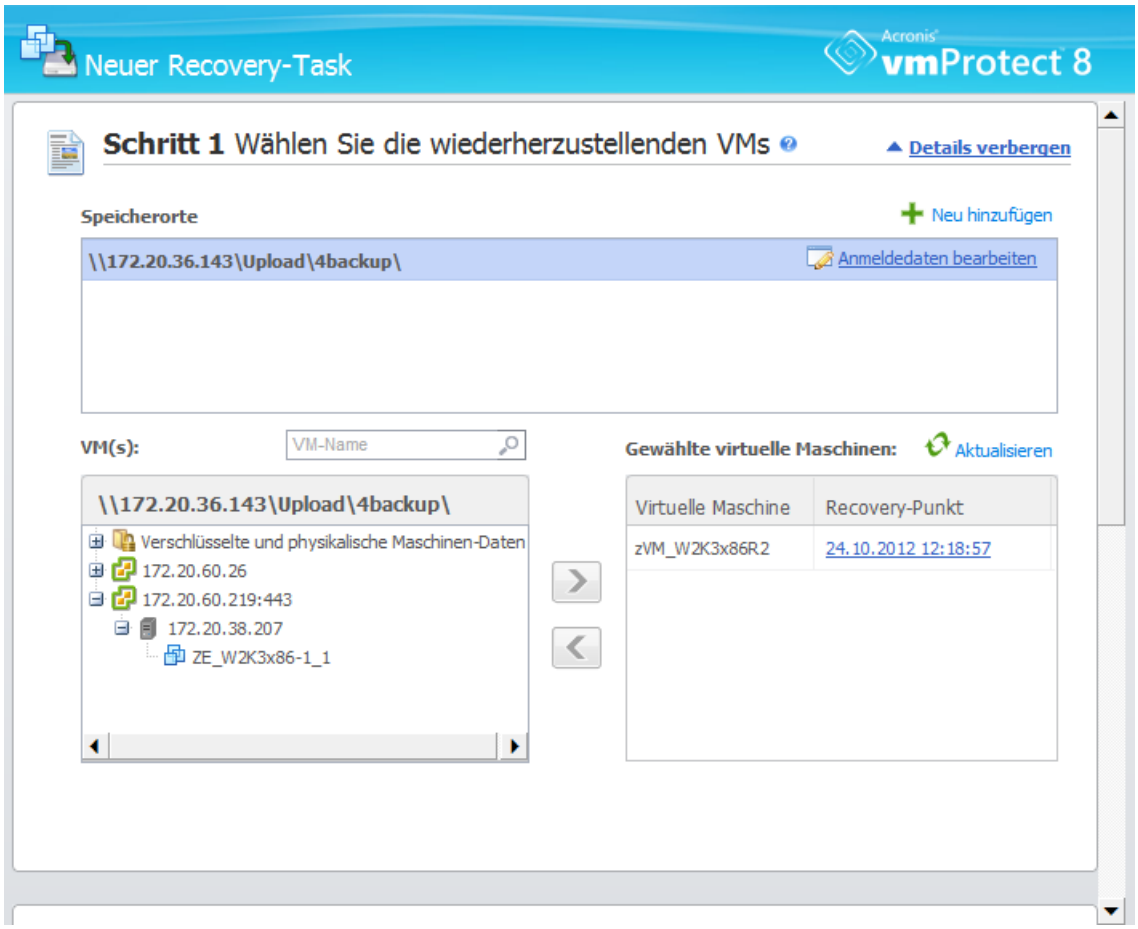
Die Assistenten für Backup und Recovery (einschließlich der Backup- und Recovery-Einstellungen) in der VMware vSphere-Oberfläche sehen genau so aus wie in Acronis vmProtect 8.

Der Standard-Assistent **Neuer Backup-Task** besteht aus vier Schritten, die im Detail im Abschnitt 'Backups virtueller Maschinen erstellen' (S. 33) beschrieben sind. Im ersten Schritt des Assistenten in VMware vSphere ist im **Acronis Backup**-Fenster die mit der rechten Maustaste ausgewählte VM bereits eingetragen; Sie können die Standardauswahl aber auch ändern.



vCenter-Integration, Neuer Backup-Task, Schritt 1

Der Standard-Assistent **Neuer Recovery-Task** besteht aus drei Schritten, die im Detail im Abschnitt 'Ein Backup virtueller Maschinen wiederherstellen' (S. 56) beschrieben sind. Im ersten Schritt des Assistenten in VMware vSphere ist im **Acronis Recovery**-Fenster die mit der rechten Maustaste ausgewählte VM bereits eingetragen. Der neueste Recovery-Punkt am zuerst gefundenen **letzten Speicherort** ist vorausgewählt.



vCenter-Integration, Neuer Recovery-Task, Schritt 1

Beachten Sie, dass Sie in der Ansicht **VMs und Vorlagen** des vSphere-Clients nicht mit Ordnern arbeiten können. Es werden im Acronis-Kontextmenü nur die Eintragungen für virtuelle Maschinen angezeigt.

Beachten Sie, dass die vCenter-Integration von einem speziellen vmProtect 8 Agenten verwaltet wird. Wenn dieser Agent vom vCenter aus nicht erreichbar ist, werden auch die über die Kontextmenüs verfügbaren Funktionen nicht richtig arbeiten.

VMware vSphere und Acronis vmProtect 8 Synchronisierung

Wenn das vCenter aktiviert ist, werden alle im VMware vSphere Client ausgeführten Aktionen in der Acronis vmProtect 8 Oberfläche gespiegelt. Diese synchronisierten Aktionen sind: neue Tasks und Task-Fortschritt. Im Bereich **Letzte Tasks** wird der Fortschritt der Tasks für Backup/Recovery/etc. angezeigt, die über das Kontextmenü im VMware vSphere Client ausgeführt werden. Wenn Sie über den entsprechenden Eintrag des Kontextmenüs im VMware vSphere Client Daten an einem neuen Speicherort sichern oder von einem neuen Speicherort wiederherstellen, werden die letzten Speicherorte in vmProtect 8 ebenfalls aktualisiert.

Analog dazu werden alle mit Acronis vmProtect 8 ausgeführten Tasks für Backup/Recovery/etc. als **Tasks** im VMware vSphere Client registriert.

7 Backups von virtuellen Maschinen erstellen

Klicken Sie im Bereich **Schnellstart** des Dashboards auf **Backup-Task erstellen** oder klicken Sie auf der Registerkarte **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:

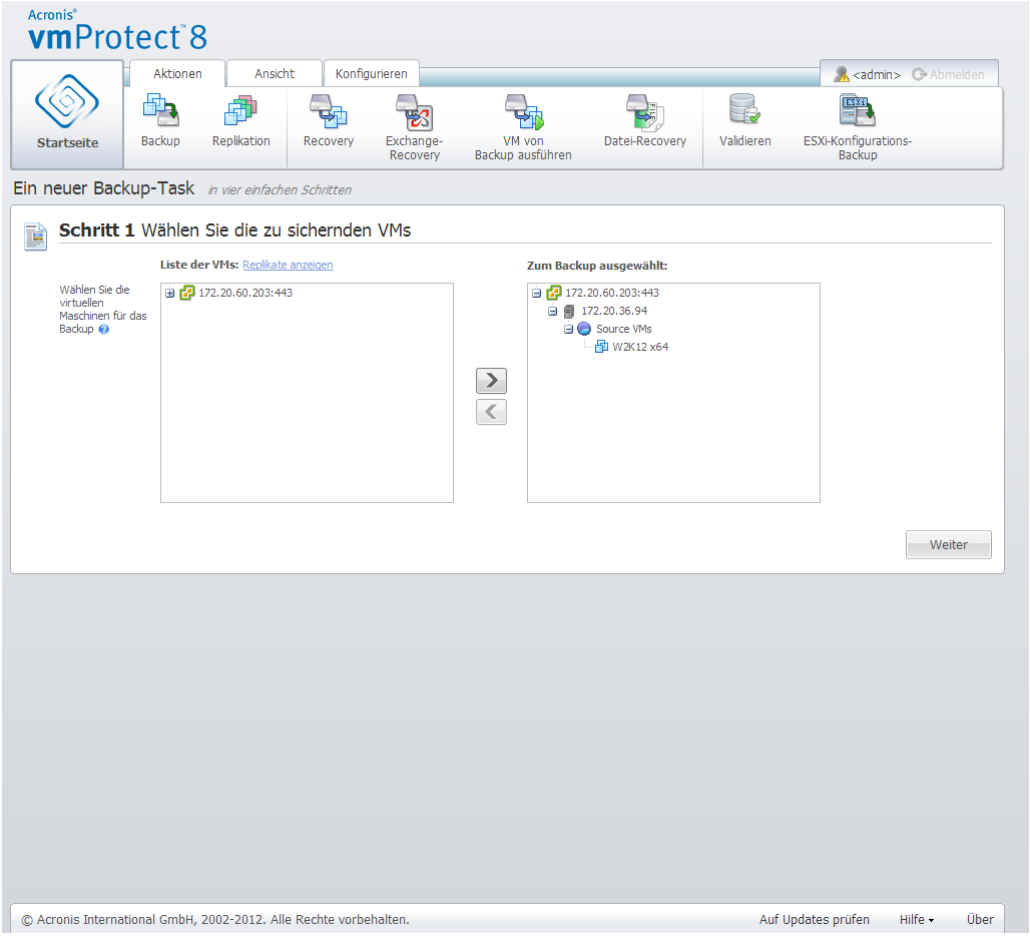
- Wählen Sie die zu sichernden VMs.
- Zeitpunkt des Backups
- Backup-Ort
- Art des Backups

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

7.1 Wählen Sie die zu sichernden VMs

Im ersten Schritt wählen Sie die zu sichernden virtuellen Maschinen (oder vApps) aus. Auf der linken Seite werden alle vom Acronis vmProtect 8 Agenten verwalteten ESX(i)-Hosts/vCenter 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(i)-Host auf der Seite **Konfigurieren** –> **ESX(i)-Hosts** hinzugefügt haben.

Die Auswahl der virtuellen Maschinen (oder vApps) erfolgt mit Hilfe der Schaltflächen **>** und **<** durch Verschieben von der linken in die rechte Seite. 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.



Assistent 'Neuer Backup-Task', Schritt 1 'Wählen Sie die zu sichernden VMs'

Zum Backup dynamischer Maschinen-Gruppen wählen Sie im Verzeichnisbaum das übergeordnete Element (z.B. den ESX(i)-Host oder VMs-Ordner) und verschieben es mit der 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.

Sie können außerdem VM-Replikate per Backup sichern (siehe den Abschnitt 'Replikation (S. 48)'). Klicken Sie dazu über der Liste der VMs auf die Schaltfläche **Replikate anzeigen** und wählen Sie das zu sichernde VM-Replikat. Beachten Sie, dass es nicht empfohlen wird, eine Replikation zu und ein Backup von einem VM-Replikat gleichzeitig durchzuführen. Sie sollten bei der Konfiguration der Planungen also vorsichtig sein.

Klicken Sie auf **Weiter**, wenn Sie die zu sichernden VMs ausgewählt haben, um den ersten Schritt abzuschließen und fortzufahren.

7.2 Backup-Zeitpunkt

Im zweiten 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'). Der Standardwert ist 'Backup erstellen alle 1 Wochen am So, Mo, Di, Mi, Do, Fr, Sa um 12 Uhr.' Hier können Sie den Standardwert ändern oder 'Keine Planung, Ausführung bei Bedarf' wählen, so dass der Backup-Task nicht planmäßig ausgeführt wird. Er wird entweder direkt nach der Erstellung des Backup-Tasks gestartet oder manuell aus der Ansicht **Tasks**.

Legen Sie fest, wie oft die Daten gesichert werden sollen. Acronis vmProtect 8 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-Ausführung während des Tages...** 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: **22:00:00 Uhr**.

'Werktags'-Planung

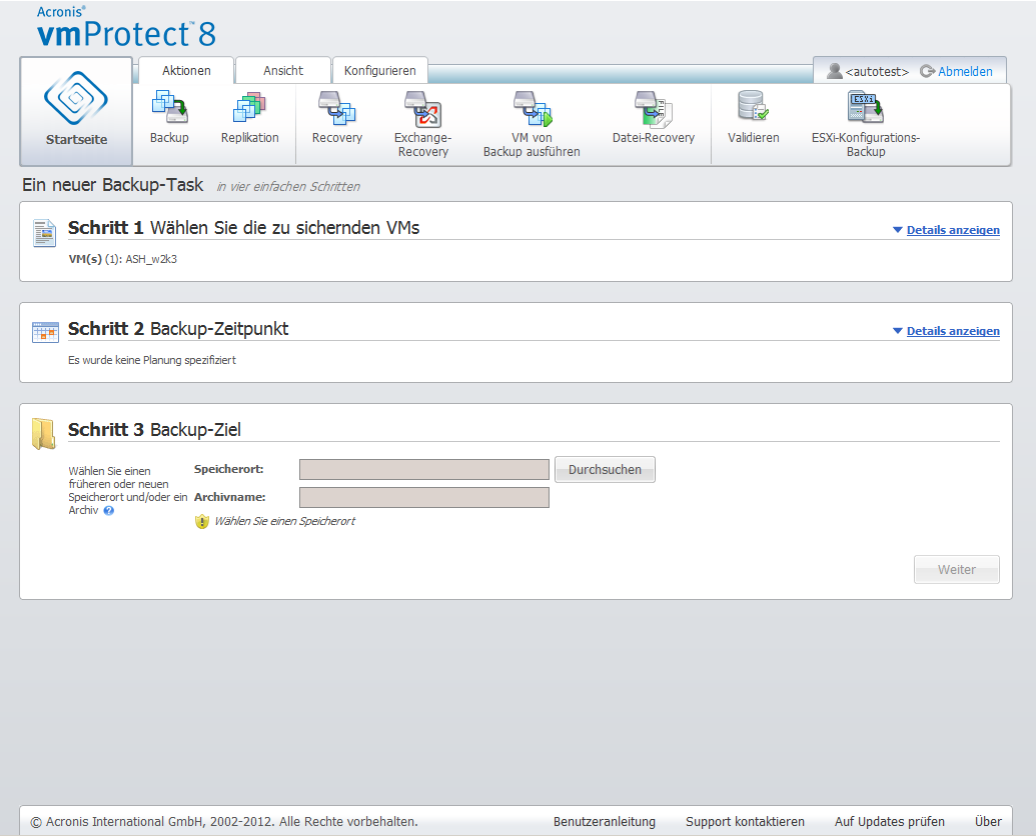
Den Task jede Woche an Werktagen ausführen: von Montag bis Freitag. Während eines Werktags startet der Task nur einmal, um 21:00 Uhr. Die Parameter der Planung werden wie folgt eingestellt:

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.

7.3 Backup-Ziel

Im dritten 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 'Neuer Backup-Task', Schritt 3 '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
- Letzte Speicherorte.
- Lokale Ordner
- Netzwerkordner
- FTP-Server
- SFTP-Server

Falls Ihr vmProtect 8 Agent keine hinzugefügte Lizenz hat, ist das einzige wählbare Backup-Ziel der Acronis Online Backup Storage.

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 Dialog 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 der Acronis vmProtect 8 Online Backup Storage möglicherweise in Ihrer Region nicht verfügbar ist. Weitere Informationen finden Sie unter http://www.acronis.de/my/backup-recovery-online/.

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 Durchsuchen des Verzeichnisbaums können Sie einen Pfad im entsprechenden Feld **Speicherort** unten eingeben und diesen Speicherort dann mit einem Klick auf **Start** 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.

Wählen Sie den Archivtyp für das neue Backup. Acronis vmProtect 8 kann Daten in zwei unterschiedlichen Archivtypen sichern – in einem Standard-Archiv (Legacy-Modus) oder einem Archiv im Modus 'Nur inkrementell'.

Wählen Sie für das Archiv im Legacy-Modus die Option **Jedes Backup in separater Datei speichern** (*Weitere Informationen finden Sie im Abschnitt 'Backup-Schema für mehrere Dateien (Legacy-Modus)'* (S. 9)). Oder wählen Sie die Option **Alle Backups in einer Datei speichern** (empfohlene Vorgehensweise). Das Archiv hat dann das neue, verbesserte Format 'Nur inkrementell' (*Weitere Informationen finden Sie im Abschnitt 'Backup-Schema für eine Datei (Modus 'Nur inkrementell)'* (S. 10)).

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

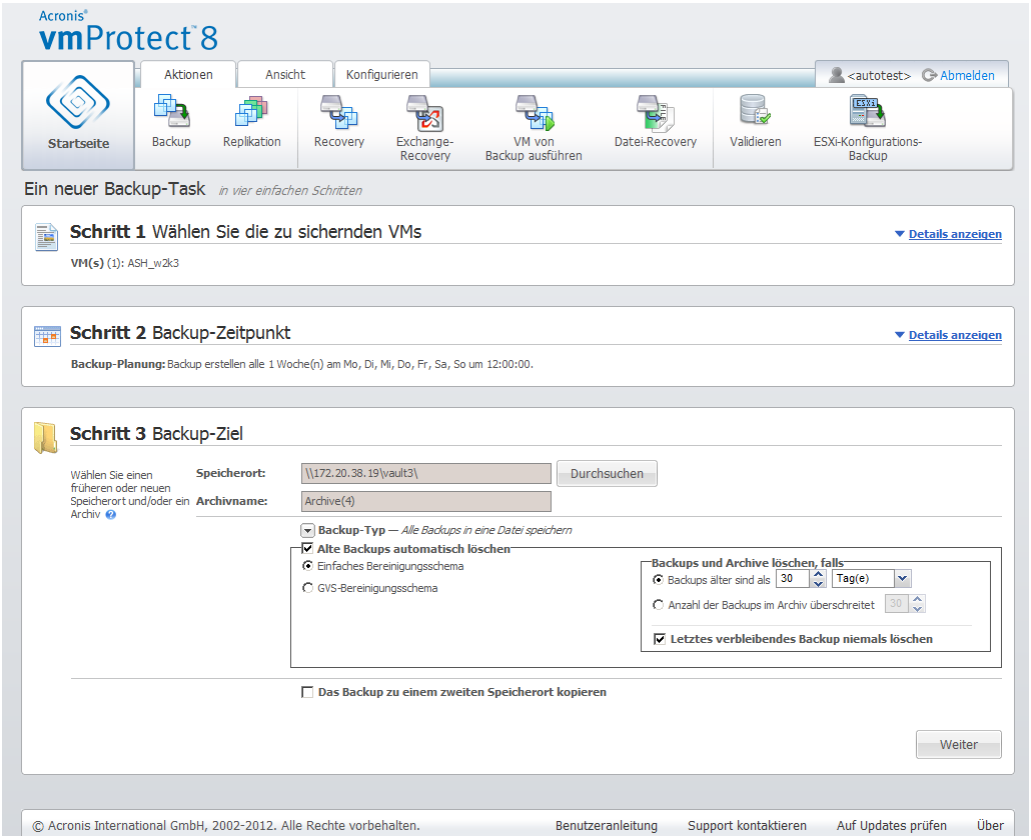
Aktivieren Sie das Kontrollkästchen **Alte Backups automatisch löschen**, um Aufbewahrungsregeln zur Verwaltung der Backups im Archiv festzulegen. Die verfügbaren Optionen hängen vom Setup der Planung im vorhergehenden Schritt (*Abbschnitt 'Backup-Zeitpunkt'*) und dem gewählten Archiv-Format ab. So steht beispielsweise das Bereinigungsschema 'Großvater-Vater-Sohn' (GVS) für ungeplante Backup-Tasks nicht zur Verfügung. Die Auswahl 'Erstelle Voll-Backups alle: <...> ist für die Option 'Alle Backups in einer Datei' 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.

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.

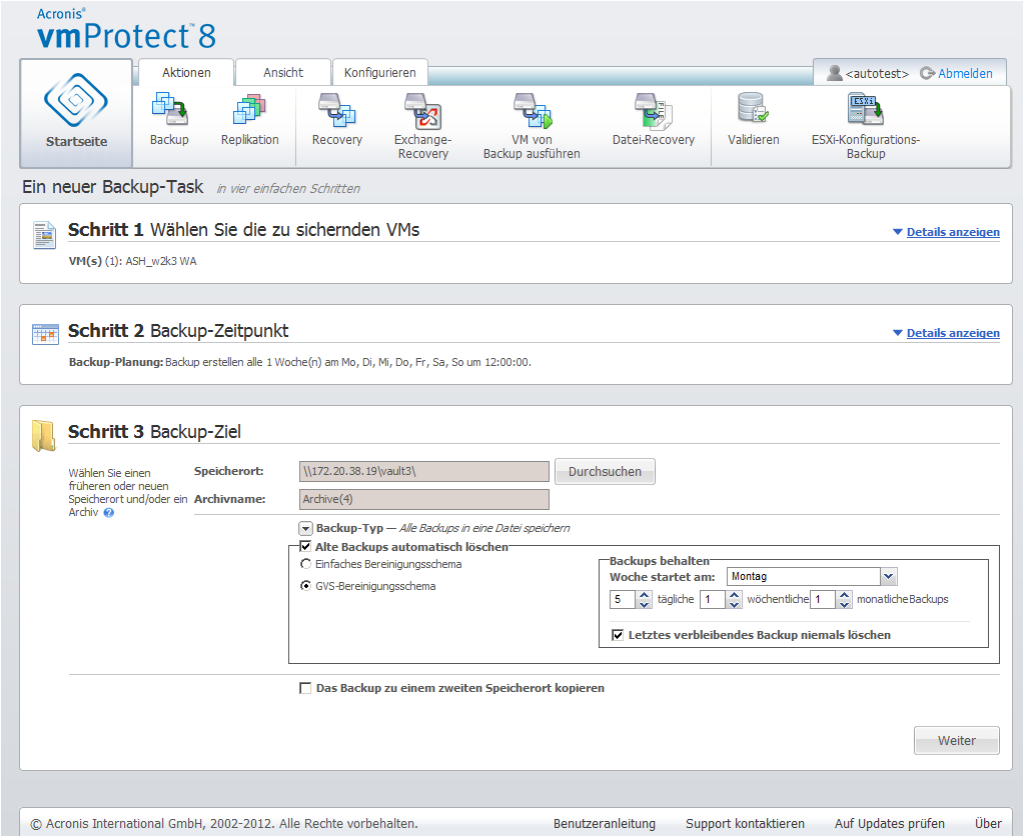


Assistent 'Backup erstellen', Schritt 3, 'Backup-Ziel', Einfaches Bereinigungsschema, 'Veraltete Backups löschen'

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. 10) 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 3, 'Backup-Ziel', 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, falls**' '**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 einen Backup-Task auf eine Gruppe virtueller Maschinen anwenden, aber eine dieser Maschinen vom ESX(i)-Host gelöscht wurde und 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.

Sie können Ihre VM-Umgebung schützen, indem Sie Ihre Backups an unterschiedlichen Orten speichern. Der Backup-Task speichert standardmäßig alle Backup-Archive zu einem einzelnen Storage. Sie können den Task aber dazu konfigurieren, die erstellten Backups zu einem anderen Archive-Storage (am zweiten Speicherort) zu kopieren.

Aktivieren Sie das Kontrollkästchen **Das Backup zu einem zweiten Speicherort kopieren**.

Die folgenden Einstellungen ermöglichen Ihnen, die Optionen für 'Backup kopieren' zu konfigurieren. Wählen Sie den zweiten Speicherort, an dem Ihre Backups ebenfalls gespeichert werden sollen und dann den **Archivnamen**. Klicken Sie auf 'Durchsuchen' und wählen Sie aus der Liste der verfügbaren Speicherorte den gewünschten.

Wählen Sie aus dem Listenfeld **Kopie-Zeitpunkt**, ob Sie möchten, dass das Backup sofort nach jeder Backup-Erstellung zum zweiten Speicherort kopiert werden soll. Alternativ können Sie auch spezifische Tage angeben, an denen Ihre Backup-Kopie durchgeführt werden soll, abweichend von den Tagen der eigentlichen Backup-Planung. In diesem Fall können Sie außerdem die Option **Alle verpassten Recovery-Punkte kopieren** oder **Nur zuletzt erstellte Recovery-Punkte kopieren** aktivieren.

Die Option **Nur zuletzt erstellte Recovery-Punkte kopieren** kann hilfreich sein, wenn der gewählte erste Speicherort manchmal nicht verfügbar ist. Sollte die Option **Alle verpassten Recovery-Punkte kopieren** ausgewählt sein und die Aufbewahrungsregeln für den ersten Storage auf dem Hauptspeicherort ausgeführt werden, dann löscht die Software die Recovery-Punkte, die gemäß dieser Regeln entfernt werden sollen – und das auch dann, wenn diese Recovery-Punkte nicht zum zweiten Speicherort kopiert wurden. Wenn die Aufbewahrungsregeln daher ausgeführt werden, wird also nicht überprüft, ob die Recovery-Punkte bereits zum zweiten Speicherort kopiert wurden (oder nicht).

Standardmäßig sind der Backup-Typ und die Bereinigungsregeln für die kopierten Backups identisch zu den entsprechenden primären Backup-Einstellungen. Mittlerweile können Sie wählen, ob Sie andere Einstellungen spezifizieren wollen, beispielsweise, einen anderen Backup-Typs zu verwenden oder die Optionen der Aufbewahrungsregeln zu ändern.

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

7.4 Art des Backups

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

7.4.1 Exchange-aware Backup-Einstellungen

Bevor Sie einen **Exchange-Server-Backup extrahieren**, muss das Backup so konfiguriert sein, dass es 'Exchange-aware' ist. Wählen Sie aus der Liste der VMs auf der linken Seite die VM(s), auf der bzw. denen der MS Exchange Server läuft, und geben Sie die **Anmeldedaten für den Domain-Administrator** an. Sie können mehrere VMs mit Exchange hinzufügen.

Sie können auch die Option **Exchange Server-Transaktionsprotokolle automatisch nach dem Backup abschneiden** wählen. Mit Auswahl dieser Option wird die Exchange Server-Datenbank gesichert, einschließlich aller während des Backups erfolgten Datenbank-Updates. Standardmäßig ist diese Option deaktiviert.

Beachten Sie, dass Sie mit Aktivierung des Exchange-aware Backups Gast-Betriebssystem-Anmeldedaten für die gewählte(n) VM(s) bereitstellen müssen, die den MS Exchange-Server ausführen. Das bedeutet, dass Sie einen Benutzer mit Domain-Administrator-Berechtigungen spezifizieren müssen. Die mit dem Windows 2008 Server eingeführte Technik zur Benutzerkontensteuerung (User Account Control, UAC) wird nicht direkt von Acronis vmProtect 8 unterstützt, da das Produkt auf die Daten der VMs im 'Agenten-losen'-Zustand

zugreift. Sollte also für den von Ihnen spezifizierten Benutzer die Benutzerkontensteuerung aktiviert sein, dann schlagen wir folgende mögliche Lösungen vor (je eine ist zulässig):

1. Deaktivieren Sie die Benutzerkontensteuerung für den spezifizierten Benutzer. Die Benutzerkontensteuerung kann beispielsweise über eine Domain-Gruppenrichtlinie (de)aktiviert werden.
2. Spezifizieren Sie einen anderen Benutzer, für den die Benutzerkontensteuerung deaktiviert ist. Sie können beispielsweise ein integriertes Domain-Administrator-Konto verwenden, für das die Benutzerkontensteuerung standardmäßig deaktiviert ist.
3. Installieren Sie einen kleinen 'Exchange Backup Agent' (10 MB) innerhalb der VM. Durchführung: Führen Sie das Installationspaket von Acronis vmProtect 8 aus, wählen Sie im Menü die Option **Komponenten extrahieren**, extrahieren Sie auf diese Weise den Exchange Backup Agent als '.msi-Komponente' und installieren Sie den Agenten auf dem Exchange-Server, auf dem die Benutzerkontensteuerung (UAC) aktiviert ist. Danach können Sie unabhängig vom UAC-Status jeden Domain-Benutzer mit Domain-Administrator-Berechtigungen verwenden.

Obwohl vmProtect 8 keine Cluster-kompatible Software ist, können Sie dennoch Exchange-aware Backups von Exchange-Cluster-Knoten erstellen (Versionen ab Exchange 2003 SP2+ werden unterstützt). Während des Backups kann Acronis vmProtect 8 die Exchange-Datenbanken sichern, die zu diesem Zeitpunkt für diese VM (Exchange-Cluster-Knoten) verfügbar sind. Es gibt viele verschiedene Arten von Exchange-Clustern (SCC, CCR, DAG), die alle bestimmte Eigenschaften haben; Sie sollten vor allem aber sicher gehen, dass die VM, mit der Sie unter Verwendung der 'Exchange-aware'-Option das Backup durchführen, auch tatsächlich auf die Daten aus den Exchange-Datenbanken zugreifen kann. Dieselbe Vorgehensweise betrifft auch die Option 'Abschneiden von Transaktionsprotokolldateien'; sie gilt nur für Datenbanken, auf die Zugriff besteht.

So ist es beispielsweise unerheblich, welcher Knoten eines Exchange 2010-DAG-Clusters gesichert wird; jeder Knoten kann aktive Datenbanken und passive Datenbanken (d.h. Replikate von Datenbanken auf anderen Knoten) hosten und es werden all diese Datenbanken zuverlässig gesichert, da sie von allen Knoten aus erreichbar sind. Beachten Sie, dass in einem solchen Fall die Protokolldateien für aktive und passive Datenbanken abgeschnitten werden.

Ausgenommen von dieser Regel sind SCC-Cluster; hier befindet sich die Datenbank auf einem freigegebenen Storage und ist daher für die Funktion 'vStorage API' nicht erreichbar, mit der auf die VM-Daten zugegriffen werden soll. SCC-Cluster werden NICHT unterstützt.

Wenn Sie die Exchange-Datenbank aus dem Backup extrahieren und zum Zeitpunkt der Fehlfunktion wiederherstellen wollen – also die Datenbank mit der Sicherungskopie ersetzen und darüber die Transaktionsprotokolle wiederherstellen –, müssen Sie auf jeden Fall die neueste Version der Datenbank extrahieren, damit die vorhandenen Transaktionsprotokolle auf diese Kopie angewandt werden können. Wenn eines der Transaktionsprotokolle in der Kette fehlt, ist keine Wiederherstellung möglich.

7.4.2 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. 94)).

Falls Sie Ihren Backup-Task dazu konfiguriert haben, die Backups zu einem zweiten Speicherort zu kopieren, dann können Sie hier wählen, ob die Backups am zweiten Speicherort validiert werden sollen oder nicht.

7.4.3 Andere Einstellungen

Klicken Sie auf **Weitere Optionen**, um das Fenster mit den zusätzlichen Einstellungen zu öffnen. Diese Optionen sind im Abschnitt 'Optionen' (S. 42) beschrieben.

7.4.4 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.

7.5 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.

7.5.1 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 AES-Algorithmus arbeitet im 'Cipher Block Chaining Mode' (CBC) und verwendet einen zufällig erstellten Schlüssel mit einer benutzerdefinierten Größe von 128, 192 oder 256 Bit. Je größer der Schlüssel, desto länger wird das Programm zur Verschlüsselung benötigen, aber desto sicherer sind auch die Daten.

7.5.2 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, für die Ausschlusskriterien festgelegt werden können.

Diese Option ist nur bei Backups virtueller Maschinen mit NTFS- und FAT-Dateisystemen wirksam. Sie wirkt sich insbesondere bei allen ausgeschalteten VMs (mit FAT- und NTFS-Dateisystemen) aus, sowie bei eingeschalteten VMs, auf denen als Betriebssystem Windows Server 2003 oder höher läuft. Für diese Option müssen außerdem VMware Tools auf der Ziel-VM laufen.

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 **Dateien ausschließen, die die folgenden Kriterien erfüllen**: *.tmp, *.~, *.bak

7.5.3 Komprimierungsgrad

Die Option **Komprimierungsgrad** definiert den Grad der Komprimierung für die zu sichernden Daten. Der Standardwert für diese Option ist **Normal**.

Der optimale Komprimierungsgrad 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 entstehende Größe des Backup-Archivs wird maximal sein.
- **Normal**. Dieser Komprimierungsgrad wird in den meisten Fällen empfohlen.
- **Hoch**. Die Größe des Backups 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 Volumes zu verringern.

7.5.4 Fehlerbehandlung

Mit diesen Optionen können Sie festlegen, wie eventuell auftretende Fehler beim Backup 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.

7.5.5 Desaster-Recovery-Plan

Das Desaster-Recovery-Szenario sieht vor, dass unterschiedliche Personen für das Verwalten von Backup- und Recovery-Prozessen verantwortlich sind. Daher weiß die Person, die eine Wiederherstellung ausführt, möglicherweise nicht genau, wo sich die Images befinden, zu welchen Maschinen sie gehören, usw. Mit Acronis vmProtect 8 können Sie einen **Desaster-Recovery-Plan (DRP)** erstellen, der Schritt für Schritt in einfachen Anweisungen erklärt, wie die Daten nach einem Systemausfall aus dem Backup-Archiv wiederhergestellt werden können. Der **Desaster-Recovery-Plan** kann per E-Mail an bestimmte Benutzer versandt oder an einem bestimmten Speicherort bzw. in einem bestimmten Ordner gespeichert werden.

Der **Desaster-Recovery-Plan** wird vom Acronis Agenten generiert und nach Erstellen des ersten Backups versandt. Bei Änderungen am Backup-Task oder erheblichen Änderungen an den Backup-Inhalten wird ein neuer **Desaster-Recovery-Plan** versandt.

Der Standardwert für den Parameter **Desaster-Recovery-Plan** ist 'Deaktiviert'.

In den **Standardeinstellungen für Backups** können Sie den **Desaster-Recovery-Plan** für alle Backup-Tasks aktivieren. Gehen Sie zu **Konfigurieren** –> **Backup-Einstellungen** und klicken Sie auf **Desaster-Recovery-Plan**. In Schritt 4 des Assistenten **Neuer Backup-Task** können Sie auch DRP für einzelne Backup-Tasks einrichten. Klicken Sie auf **Weitere Optionen** und gehen Sie zum Bereich **Desaster-Recovery-Plan**.

Aktivieren Sie den DRP durch Anklicken des Kontrollkästchens **Desaster-Recovery-Plan senden**. Konfigurieren Sie die Optionen für den DRP wie folgt:

- Tragen Sie die Empfänger-E-Mail in das Eingabefeld E-Mail-Adressen ein. Sie können auch mehrere, durch Semikolons getrennte E-Mail-Adressen eingeben.
- Geben Sie eine E-Mail-**Betreffzeile** ein. Die Standard-Betreffzeile ist **Acronis vmProtect 8 Benachrichtigung von der Acronis Appliance**.
- Geben Sie die Adresse des Postausgangsservers (SMTP) in das Feld **SMTP-Server** ein.
- Tragen Sie die **Port**-Adresse des Postausgangsservers ein. Standardmäßig ist der Port auf 25 gesetzt.

- Wenn der SMTP-Server eine Authentifizierung benötigt, dann geben Sie **Benutzernamen** und **Kennwort** in den entsprechenden Feldern an.
- Tragen Sie den Namen des E-Mail-Absenders in das Eingabefeld **Von** ein.
- Wählen Sie, falls erforderlich, die Option **Verschlüsselung verwenden** und als Verschlüsselungstyp SSL oder TLS.
- Mit einem Klick auf **Test-Mail senden** können Sie überprüfen, ob der **Desaster-Recovery-Plan** mit den angegebenen Einstellungen korrekt versandt wird.

Aktivieren Sie das Kontrollkästchen **Desaster-Recovery-Plan zum folgenden Speicherort hochladen**, um eine Kopie des DRP aufzubewahren, und klicken Sie dann auf **Durchsuchen**.

7.5.6 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** – damit eine Benachrichtigung gesendet wird, wenn der Backup-Task erfolgreich abgeschlossen wurde.
- **Wenn das Backup fehlschlägt** – damit eine Benachrichtigung erfolgt, wenn der Backup-Task nicht erfolgreich war.
- **Vollständiges Log zur Benachrichtigung hinzufügen** – um das vollständige Log zu erhalten.

Geben Sie eine oder mehrere E-Mail-Adressen ein, an die die Benachrichtigungen geschickt werden. Die Adressen werden im Feld **E-Mail-Adressen** eingegeben, per Semikolon 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, der die Nachricht verschickt. Wenn Sie dieses Feld leer lassen, werden die Nachrichten so konstruiert, 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** – Damit das Ereignis-Log der Backup-Aktionen an die spezifizierten SNMP-Manager gesendet wird.
  Typ der zu übermittelnden Ereignisse – 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 – geben 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.

SNMP-Objekte

Acronis vmProtect 8 stellt die folgenden Simple Network Management Protocol (SNMP)-Objekte für SNMP-Verwaltungsanwendungen zur Verfügung:

- Typ des Ereignisses

  Objekt-Identifier (OID): 1.3.6.1.4.1.24769.100.200.1.0

  Syntax: OctetString

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

  Objekt-Identifier (OID): 1.3.6.1.4.1.24769.100.200.2.0

  Syntax: OctetString

  Der Wert enthält die Textbeschreibung des Ereignisses (identische Darstellung wie in den Meldungen der Ereignisanzeige von Acronis vmProtect 8).

Beispiele für Varbind-Werte:

1.3.6.1.4.1.24769.100.200.1.0:Information

1.3.6.1.4.1.24769.100.200.2.0:I0064000B

Unterstützte Aktionen

Acronis vmProtect 8 **unterstützt nur TRAP-Aktionen**. Es ist nicht möglich, Acronis vmProtect 8 unter Verwendung von GET- und SET-Anforderungen zu verwalten. Das bedeutet, dass Sie einen SNMP-TRAP-Receiver verwenden müssen, um TRAP-Meldungen zu empfangen.

Weitere Informationen

http://kb.acronis.com/content/11851

Über die Testnachricht

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

Die Parameter der Testnachricht lauten folgendermaßen:

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

7.5.7 Erweiterte Einstellungen

1) Deduplizierung

Mit dieser Option aktivieren bzw. deaktivieren Sie die Deduplizierung für das vom Backup-Task erstellte Archiv. 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 die duplizierten 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: Aktiviert.

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 8 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 Sie möchten, dass dieser Modus zur Dateiübertragung verwendet wird.

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

7.6 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. 85)).

8 Replikation

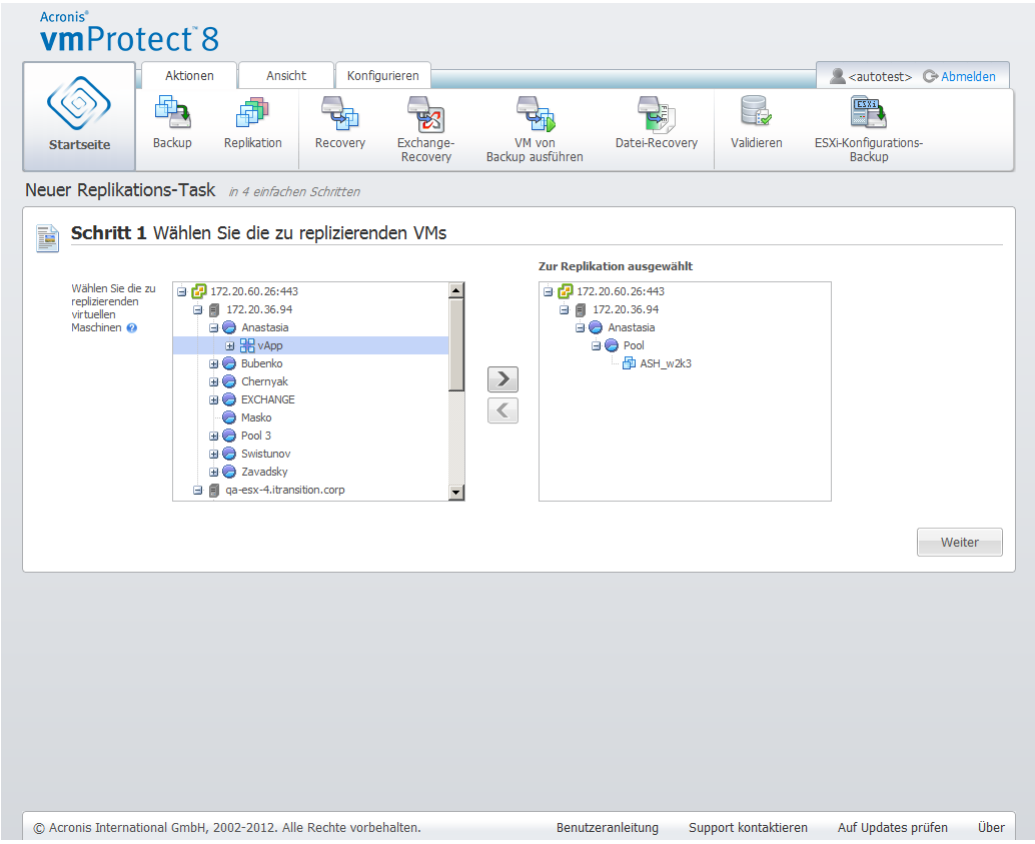
8.1 Neuer Replikations-Task

Mit der Replikations-Funktion können Sie die wichtigsten VMs klonen und bei einem Ausfall kritische Dienste schnell wieder starten. Klicken Sie zum Ausführen des **neuen Replikations-Tasks** auf **Aktionen** –> **Replikation**.

8.1.1 Wählen Sie die zu replizierenden VMs

Im ersten Schritt des Assistenten **Neuer Replikations-Task** wählen Sie die virtuellen Maschinen aus, die repliziert werden sollen. Auf der linken Seite werden alle vorhandenen, vom Acronis vmProtect 8 Agenten verwalteten ESX(i)-Hosts/vCenter sowie eine Liste der virtuellen Maschinen angezeigt. Ist die zu replizierende virtuelle Maschine nicht in der Liste, stellen Sie sicher, dass Sie den entsprechenden ESX(i)-Host auf der Seite **Konfigurieren** –> **ESX(i)-Hosts** hinzugefügt haben.

Die Auswahl der virtuellen Maschinen erfolgt mit Hilfe der Schaltflächen **>** und **<** sowie durch Verschieben von der linken auf die rechte Seite. Die Liste auf der rechten Seite zeigt dann alle für die Replikation ausgewählten virtuellen Maschinen. Mit der Schaltfläche **>** fügen Sie VMs zur Liste hinzu, mit der Schaltfläche **<** entfernen Sie die VMs aus der Liste.



Neuer Replikations-Task', Schritt 1 'Wählen Sie die zu replizierenden VMs'

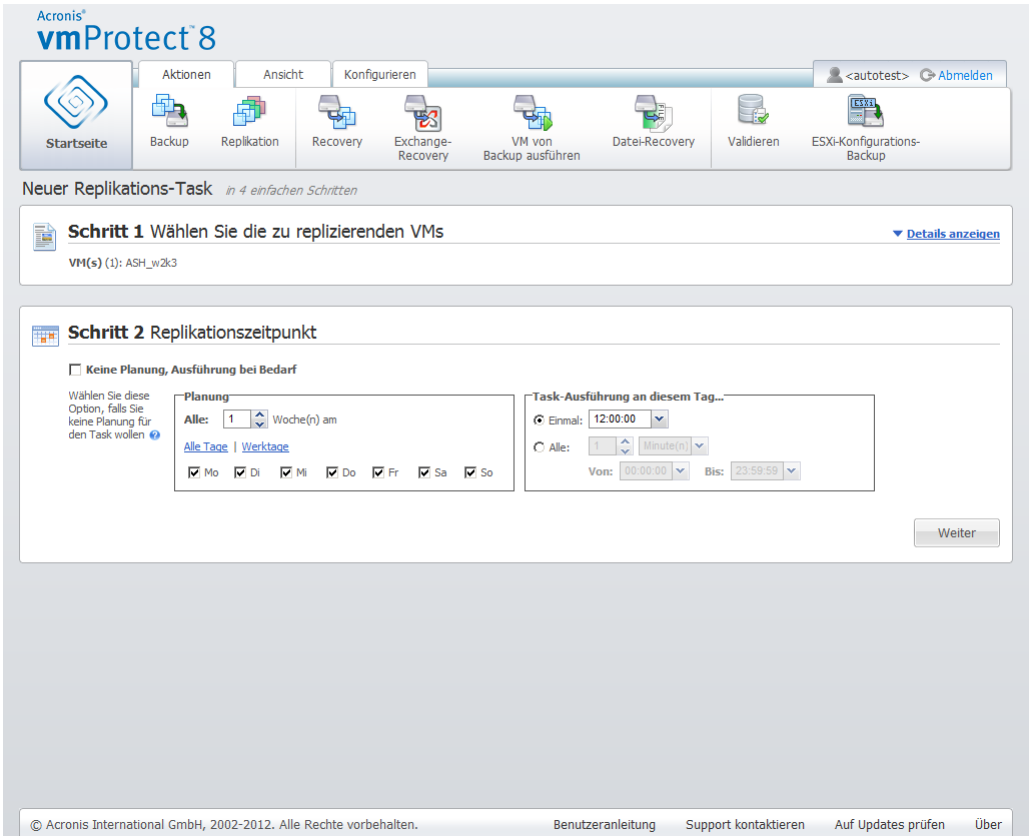
Zum Backup dynamischer Maschinen-Gruppen wählen Sie im Verzeichnisbaum das übergeordnete Element (z.B. den ESX(i)-Host oder VMs-Ordner) und verschieben es mit der Schaltfläche **>** in die rechte Liste. So werden alle zu dieser Gruppe gehörenden Maschinen automatisch in die

Backup-Liste aufgenommen. Der aktuelle Replikations-Task repliziert Maschinen, die in der Gruppe neu erstellt werden, automatisch mit.

Wählen Sie mindestens eine VM für die Replikation aus. Klicken Sie nach der Auswahl auf **Weiter**, um den ersten Schritt abzuschließen und fortzufahren.

8.1.2 Replikationszeitpunkt

Im zweiten Schritt des Assistenten **Neuer Replikations-Task** legen Sie die Planung für die Replikation der virtuellen Maschinen fest. Es stehen Ihnen zwei Optionen zur Verfügung – das Erstellen eines einzelnen Replikations-Tasks ('Keine Planung, Ausführung bei Bedarf') und die wöchentliche Planung. Der Standardwert ist 'Replikate erstellen alle 1 Wochen am So, Mo, Di, Mi, Do, Fr, Sa um 12 Uhr.' In diesem Schritt können Sie den Standardwert ändern oder 'Keine Planung, Ausführung bei Bedarf' wählen, so dass der Replikations-Task nicht planmäßig ausgeführt wird. Er wird entweder direkt nach der Erstellung gestartet oder manuell aus der Ansicht **Tasks**.



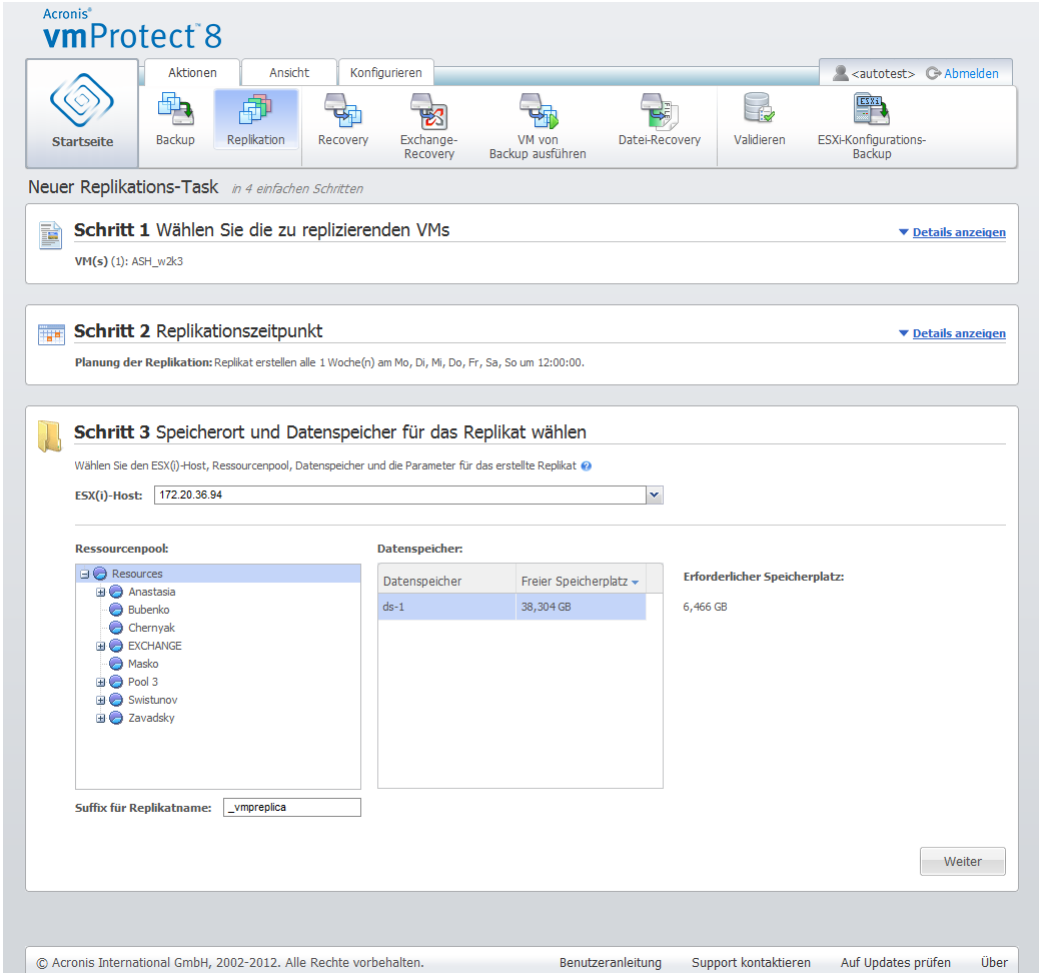
Neuer Replikations-Task', Schritt 2 'Zeitpunkt der Replikation'

Die Planung von Replikations-Tasks funktioniert genau wie die Planung von Backup-Tasks. Detaillierte Informationen zu den Planungs-Optionen sowie Planungsbeispiele finden Sie im Abschnitt 'Backup-Zeitpunkt' (S. 34).

Klicken Sie auf **Weiter**, wenn Sie die Planung des Replikations-Tasks abgeschlossen haben, um zum nächsten Schritt im Assistenten zu gelangen.

8.1.3 Speicherort und Datenspeicher für das Replikat wählen

Im dritten Schritt des Assistenten **Neuer Replikations-Task** bestimmen Sie den Speicherort und Datenspeicher für die VM-Replikate. Zuerst wählen Sie einen **ESX(i)-Host** im Listenfeld aus. Wählen Sie dann den **Ressourcenpool** auf dem Ziel-ESX-Host und den **Zieldatenspeicher** aus.



Neuer Replikations-Task, Schritt 3 'Speicherort und Datenspeicher für das Replikat auswählen'

Bestimmen Sie das **Suffix für den Replikatnamen**, das bei Erstellen des VM-Replikats verwendet werden soll. Der Standardname für Replikate ist "%Maschinen_Name%_vmpreplica", wobei "%Maschinen_Name%" der ursprüngliche Name der zu replizierenden VM ist und "_vmpreplica" das **Suffix für den Replikatnamen**. Falls eine VM dieses Namens bereits existiert, erscheint eine Warnmeldung mit der Aufforderung, das Namenssuffix zu ändern.

Treffen Sie eine Auswahl und klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.

8.1.4 Optionen für Replikations-Task

Im vierten Schritt des Assistenten **Neuer Replikations-Task** vergeben Sie einen Namen für den Replikations-Task. Beachten Sie, dass die Zeichen [ ] { } ; , . in Task-Namen nicht erlaubt sind.

Klicken Sie auf **Weitere Optionen...**, um den Replikations-Task zu konfigurieren. Folgende Optionen sind verfügbar:

1) E-Mail-Benachrichtigungen

2) SNMP-Benachrichtigungen

Weitere Informationen finden Sie im Abschnitt 'Benachrichtigungen' (S. 45).

3) CBT-Replikation**.**

Diese Option im Abschnitt **Erweiterte Einstellungen** legt fest, ob die Funktion Changed Block Tracking (CBT) von VMware bei den virtuellen Maschinen, die sie unterstützen, verwendet werden soll. Die Standardeinstellung für CBT-Replikation ist: Aktiviert.

CBT-Replikation überwacht alle Änderungen an Blöcken in der virtuellen Maschine. So wird die benötigte Zeit zur Replikaten erheblich reduziert. Die Zeit wird eingespart, weil Acronis vmProtect 8 nicht überprüfen muss, welche Blöcke seit dem letzten Backup verändert wurden. Diese Information kommt von der VMware-API.

4) Provisioning-Modus

Geben Sie an, welcher Provisioning-Modus auf den Ziel-VM-Replikaten verwendet werden soll. Die möglichen Modi sind **Thin Provisioning**, **Thick Provisioning**, **Flat Provisioning**, **Wie ursprünglich**. Standardmäßig wird der Modus **Thin Provisioning** verwendet. Der Modus Flat Provisioning wird für ESXi Version 5.0 verwendet.

Wenn Sie auf die Schaltfläche **Speichern** klicken, wird der Task mit den von Ihnen festgelegten Parametern gespeichert und erscheint in der Ansicht **Tasks**. Wenn Sie auf die Schaltfläche **Speichern und Ausführen** klicken, wird der Task gespeichert und umgehend ausgeführt.

8.2 Replizierte VMs verwalten

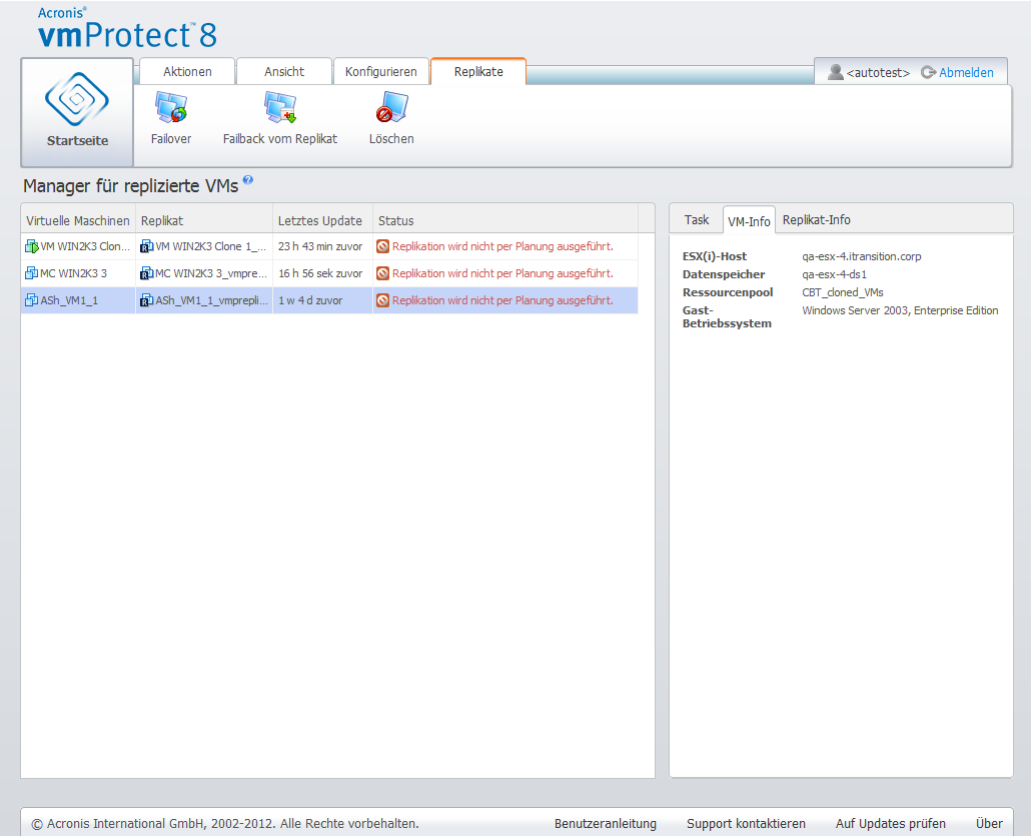
8.2.1 Manager für replizierte VMs

Auf der Seite Replikate (**Ansicht** –> **Replikate**) werden alle erstellten Replikate angezeigt, die auf den zum Acronis vmProtect 8 Agenten hinzugefügten ESX(i)-Hosts gefunden werden. Hier können Sie die Replikate auch verwalten.

Die Liste der Replikate enthält Informationen zu den ursprünglichen, replizierten virtuellen Maschinen, ihren Replikaten, zum Zeitpunkt des letzten Updates und zu ihrem Status (Replikation geplant/nicht geplant). Wählen Sie ein VM-Replikat, um detaillierte Informationen anzuzeigen.

Auf der rechten Seite der Registerkarte **VM Info** wird eine Zusammenfassung der Informationen über die ursprüngliche VM für das ausgewählte Replikat angezeigt:

- **ESX(i) Host**-Informationen
- **Datenspeicher**-Informationen
- **Ressourcenpool**, in dem die ursprüngliche VM gespeichert ist
- **Gast-VM**-Informationen



Manager für replizierte VMs

Auf der Registerkarte **Replikat-Info** wird eine Zusammenfassung der Informationen zum ausgewählten Replikat angezeigt:

- **ESX(i) Host**-Informationen
- **Datenspeicher**-Informationen
- **Ressourcenpool**, in dem die ursprüngliche VM gespeichert ist

Hier können Sie auch die grundlegenden Aktionen **Failover** und **Failback vom Replikat** ausführen. Die nachfolgenden Abschnitte beschreiben diese grundlegenden Aktionen im Detail.

8.2.2 Failover

Eine replizierte virtuelle Maschine können Sie nach dem Absturz durch Ausführen eines VM-Replikats schnell neu starten (Failover). Mit Hilfe der **Failover**-Funktion sind kritische Dienste in kürzester Zeit wieder einsatzbereit, sogar bevor die ausgefallene VM wiederhergestellt ist.

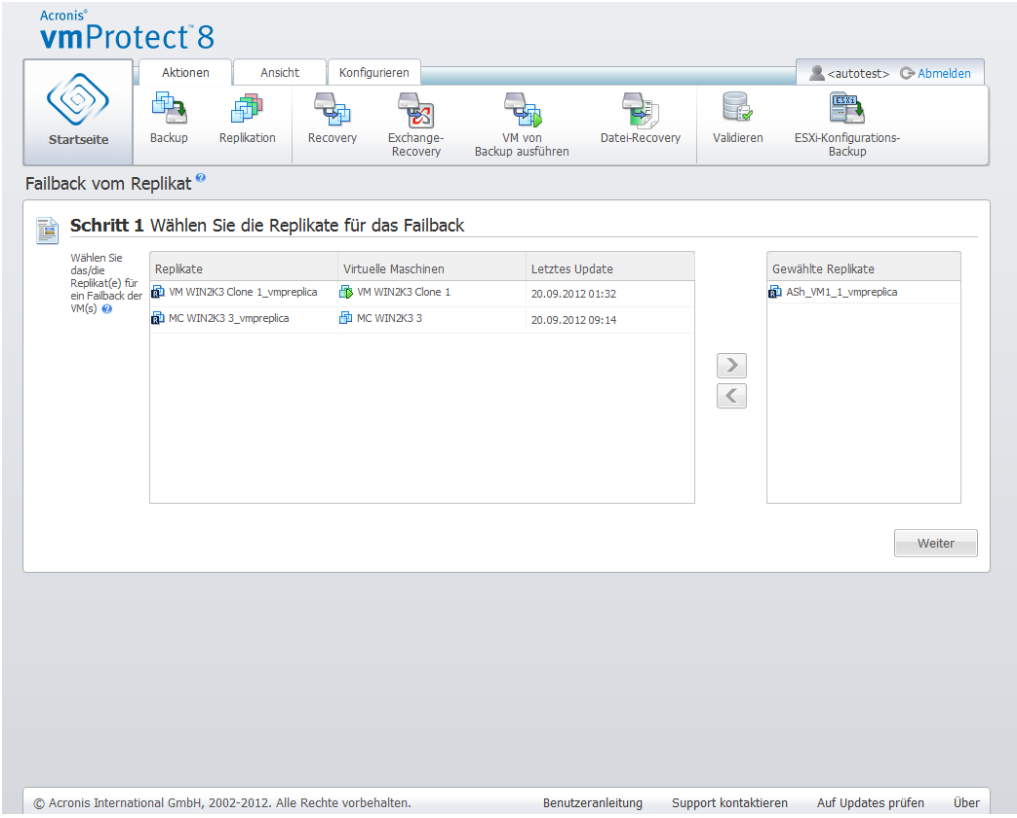
Wählen Sie das VM-Replikat, das gestartet werden soll, und klicken Sie auf die Schaltfläche **Failover** im Menüband. Legen Sie im Listenfeld fest, ob das Netzwerk auf dem VM-Replikat verwendet werden soll. Wenn die ursprüngliche VM läuft, können Sie die Option **Ursprüngliche VM vor Failover stoppen** wählen. Klicken Sie auf **Ausführen**.

Failover

8.2.3 Failback-VM vom Replikat

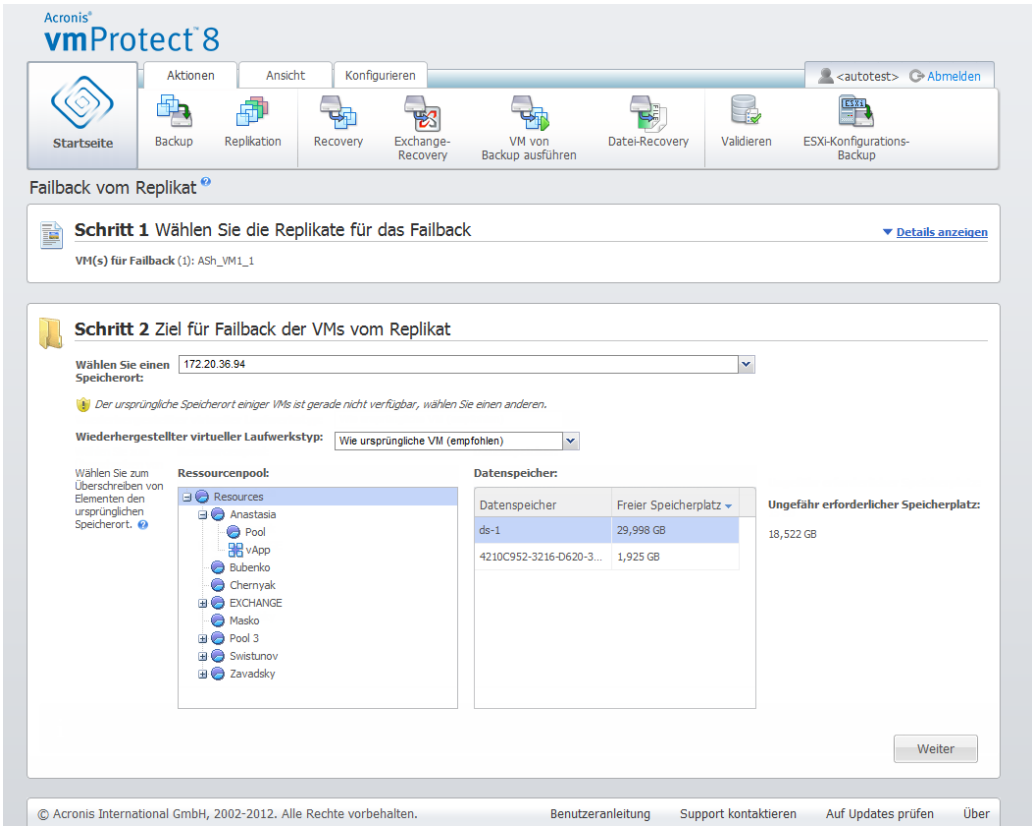
Beim Failback (Wiederherstellen einer VM vom Replikat) können Sie Ihre ursprüngliche VM mit Hilfe des VM-Replikats wiederherstellen. Diese Vorgehensweise bietet sich auch an, wenn Sie das VM-Replikat nach Beginn der **Failover**-Aktion anhalten und die Änderungen am ursprünglichen oder an einem neuen Speicherort speichern. Klicken Sie auf **Failback vom Replikat**, um den Assistenten zu starten.

Wählen Sie im ersten Schritt des Assistenten, **Failback vom Replikat**, mit Hilfe des Rechts-/Links-Steuerelements die Replikate, aus denen die VMs wiederhergestellt werden sollen, und klicken Sie auf **Weiter**.



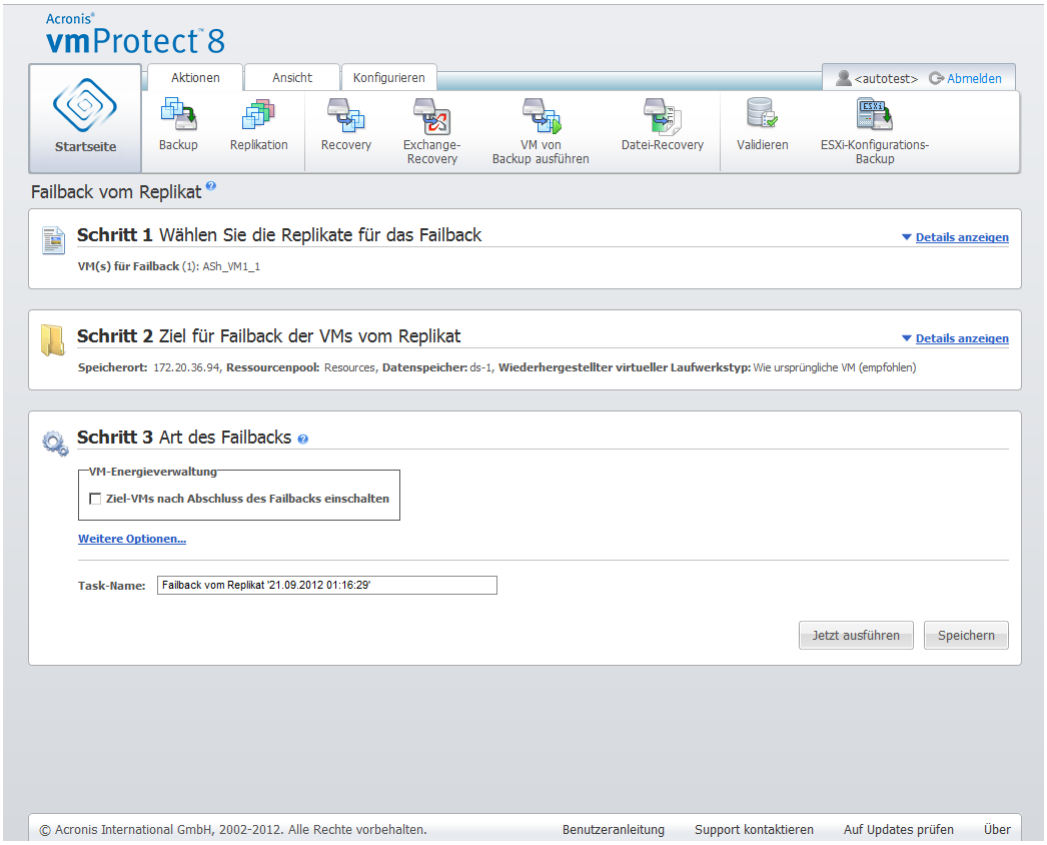
Failback vom Replikat, Schritt 1 'Replikate für das Failback auswählen'

Wählen Sie im zweiten Schritt, **Ziel für Failback der VMs vom Replikat**, den Speicherort der VMs. Sie können entweder den ursprünglichen Speicherort auswählen und die ursprünglichen VMs überschreiben oder für die wiederherzustellenden virtuellen Maschinen einen neuen Namen generieren. Sie können auch einen neuen Speicherort wählen. Klicken Sie nach Auswahl des Speicherorts auf **Weiter**.



Failback vom Replikat, Schritt 2 'Ziel für Failback der VMs vom Replikat'

Wählen Sie im dritten Schritt, **Art des Failbacks**, die Optionen für den Recovery-Task. Aktivieren Sie im Bereich **VM-Energieverwaltung** die Kontrollkästchen für **Ziel-VMs bei Start des Failbacks ausschalten** und **Ziel-VMs nach Abschluss des Failbacks einschalten** sowie andere Optionen. Vergeben Sie einen Task-Namen.



Failback vom Replikat, Schritt 3 'Art des Failbacks'

Wenn Sie auf die Schaltfläche **Speichern** klicken, werden alle Task-Parameter gespeichert. In der Ansicht **Tasks** wird der von Ihnen erstellte Task **Failback vom Replikat** angezeigt. Wenn Sie auf die Schaltfläche **Speichern und Ausführen** klicken, wird der Task gespeichert und umgehend ausgeführt.

Wenn das VM-Replikat läuft, stellt der Task **VM-Failback vom Replikat** die ursprüngliche VM wieder her, ohne das VM-Replikat anzuhalten. Erst wenn das Failback abgeschlossen ist, wird das VM-Replikat angehalten. Schließlich stellt der Task **VM-Failback vom Replikat** Änderungen, die während des Failbacks am VM-Replikat vorgenommen wurden, in der ursprünglichen (neuen) VM wieder her. So lassen sich Ausfallzeiten auf ein Minimum reduzieren und die VM in einem Zustand wiederherstellen, der dem Zustand des Replikats am nächsten kommt.

8.2.4 VM-Replikat löschen

Um das Replikat einer virtuellen Maschine zu löschen, wählen Sie es aus der Liste aus und klicken auf die Schaltfläche **Löschen** im Menüband.

9 Backups von virtuellen Maschinen wiederherstellen

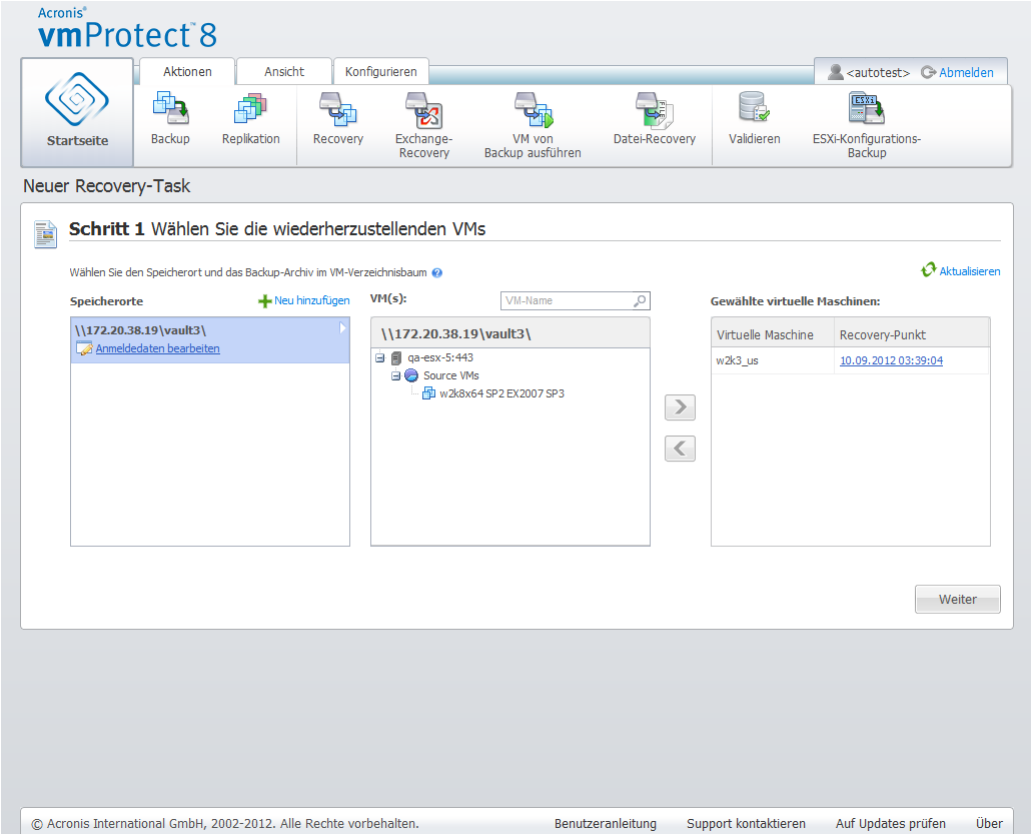
Klicken Sie in der Registerkarte **Aktionen** im Hauptmenü auf **Recovery**, um eine oder mehrere gesicherte virtuelle Maschinen wiederherzustellen. Der Assistent für **Neuer Recovery-Task** öffnet sich im Hauptarbeitsbereich und fordert Sie auf, die für den Recovery-Task erforderlichen Informationen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

- Wählen Sie die wiederherzustellenden VMs.
- Recovery-Ziel
- Art der Wiederherstellung.

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

9.1 Wählen Sie die wiederherzustellenden VMs

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.



Assistent 'Neuer Backup-Task', Schritt 1 'Wählen Sie die wiederherzustellenden VMs'

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

Falls sich am gewählten Speicherort durch Kennwort geschützte Archive oder Archive physikalischer Maschinen befinden, werden diese in einer separaten Liste unter **Verschlüsselte und physikalische Maschinen-Daten** angezeigt. Um Daten aus diesen Archiven wiederherstellen zu können, müssen Sie im Pop-up-Fenster **Kennwort** das entsprechende Kennwort 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 **<** sowie durch Verschieben von der linken auf die rechte Seite. Die Liste auf der rechten Seite zeigt dann alle für die Wiederherstellung ausgewählten virtuellen Maschinen. Mit der Schaltfläche **>** fügen Sie VMs zur Liste hinzu, mit der Schaltfläche **<** entfernen Sie die VMs aus der Liste. Diese Liste enthält die ausgewählten virtuellen Maschinen und ihre neuesten verfügbaren Recovery-Punkte, d.h. die Zeitpunkte, auf die Sie zurücksetzen können.

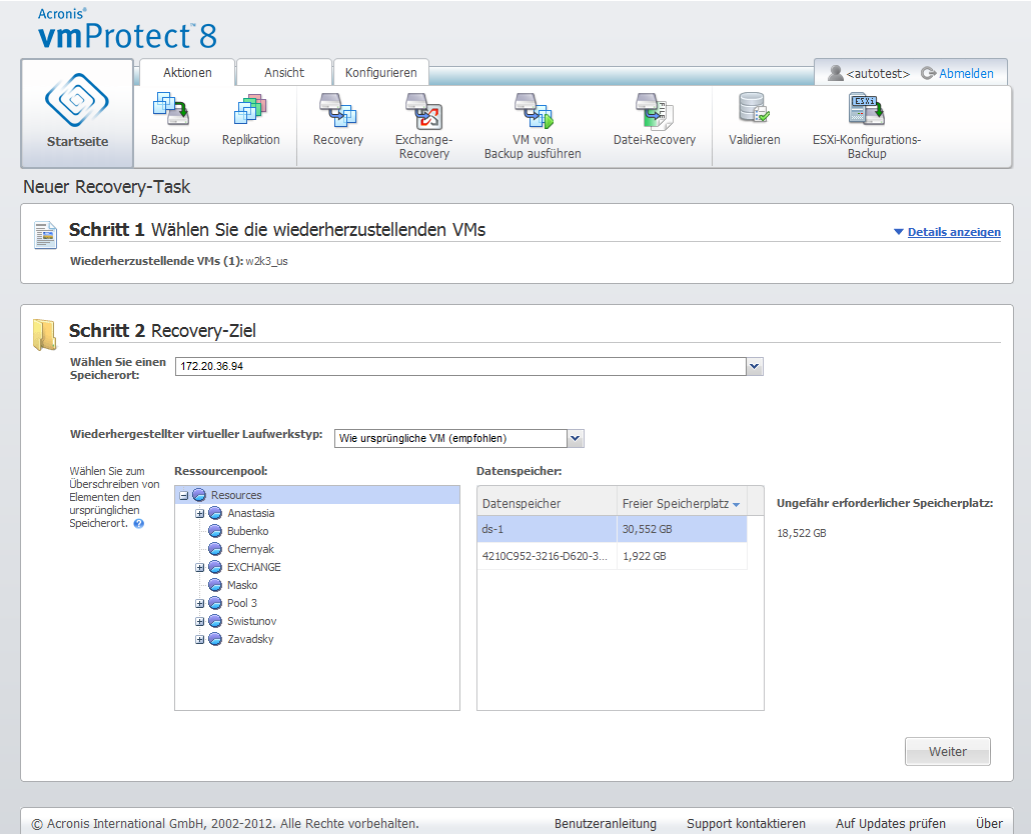
Standardmäßig wird der neueste Recovery-Punkt einer virtuellen Maschine voreingestellt. Klicken Sie auf den Recovery-Punkt, um ihn zu ändern. Im sich öffnenden Fenster können Sie dann einen anderen Recovery-Punkt wählen.

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.

Wählen Sie die wiederherzustellenden VMs und klicken Sie auf **Weiter**, um den ersten Schritt des Assistenten abzuschließen und fortzufahren.

9.2 Recovery-Ziel

Im zweiten Schritt des Assistenten 'Backup-wiederherstellen-Task' entscheiden Sie, wohin Sie die ausgewählten virtuellen Maschinen wiederherstellen.



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

Zunächst bestimmen Sie mit dem Listenfeld **Speicherort auswählen** den gewünschten Zielort für den Recovery-Task. Legen Sie fest, ob die ausgewählten virtuellen Maschinen an ihrem ursprünglichen Speicherort wiederhergestellt werden sollen oder auf einem anderen ESX(i)-Host bzw. Datenspeicher. Die Liste zeigt nur die vom Acronis vmProtect 8 Agenten verwalteten ESX(i)-Hosts an. Ist der gewünschte ESX(i)-Host nicht in der Liste, stellen Sie sicher, dass er in der Ansicht **Konfigurieren** –> **ESX(i)-Hosts** hinzugefügt wird.

Wird das Kontrollkästchen **Ursprünglicher Speicherort** zur Wiederherstellung der VM(s) ausgewählt, dann können Sie die Verwendung des Modus 'Inkrementelle Wiederherstellung' veranlassen, indem Sie das Kontrollkästchen **Inkrementelle Wiederherstellung verwenden** aktivieren. Die 'Inkrementelle Wiederherstellung' überprüft und nutzt nur solche Blöcke zur Wiederherstellung, die auf der ursprünglichen VM verändert wurden – anstatt die kompletten Daten der virtuellen Maschine wiederherzustellen. Dieser Modus hilft Ihnen, die Wiederherstellungsgeschwindigkeit bei Verwendung langsamer Backup-Speicherorte (wie dem Acronis Online Storage) oder langsamer Verbindungen zu steigern, indem die Menge der zu übertragenden Daten reduziert wird.

Beachten Sie, dass der Modus 'Inkrementelle Wiederherstellung' nur dann verwendet werden kann, wenn die Wiederherstellung 'über' die ursprüngliche VM durchgeführt wird, die auch zur Erstellung des Backups verwendet wurde. Sollte die Wiederherstellung zu einem neuen Speicherort erfolgen oder die ursprüngliche VM fehlen, dann wird eine vollständige Wiederherstellung durchgeführt.

Bei einer Wiederherstellung am **Ursprünglicher Speicherort** erscheint die wiederhergestellte VM möglicherweise nicht am selben Speicherort, an dem sie sich zum Zeitpunkt der Erstellung des Recovery-Punktes befand (und automatisch die bestehende VM überschreibt). Das ist der Fall, wenn die ausgewählte VM (definiert durch den Recovery-Punkt) zu einem anderen Host bzw. Datenspeicher, ESX(i)-Host, Ressourcenpool oder einer anderen 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

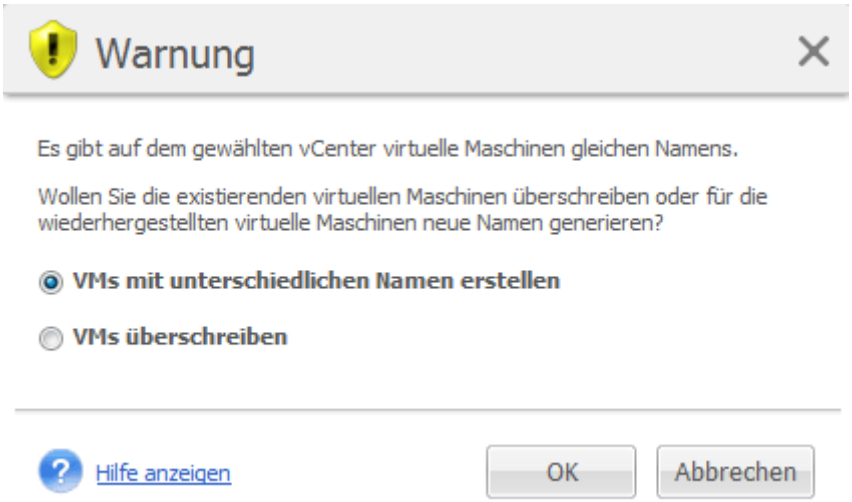
Recovery-Punktes in der vApp1, wurde aber zwischenzeitlich zur vApp2 migriert. Dann wird diese VM in der vApp2 wiederhergestellt und überschreibt die existierende VM.

Sobald der ESX(i)-Host definiert ist, wird automatisch eine Liste der verfügbaren Ressourcenpools und Datenspeicher erstellt, in der Sie den genauen Zielspeicherort für die wiederhergestellten virtuellen Maschinen festlegen.

Definieren Sie außerdem über das entsprechende Listenfeld das Format der wiederhergestellten virtuellen Laufwerke – **Wie ursprüngliche VM (empfohlen)**, **'Thick Provisioning'-Laufwerk** oder **'Thin Provisioning'-Laufwerk**. 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 Maschinen auf dem Datenspeicher wiederhergestellt werden, der bei diesem Schritt des Recovery-Assistenten festgelegt wird, jede von ihnen zu einer neuen VM.



Assistent 'Neuer Recovery-Task', Schritt 2 'Recovery-Ziel', Bestätigungsdialog 'Existierende VM überschreiben'

Falls sich auf dem ausgewählten ESX(i)-Host oder Datenspeicher virtuelle Maschinen desselben Namens befinden, werden Sie aufgefordert zu bestätigen, dass die existierenden VMs überschrieben werden sollen. 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 bei Start der Wiederherstellung ausschalten** aktiviert haben müssen (*siehe Abschnitt 'VM-Energieverwaltung'* (S. 62)).

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

'[Ursprünglicher_Name_der_VM]_DATUM'

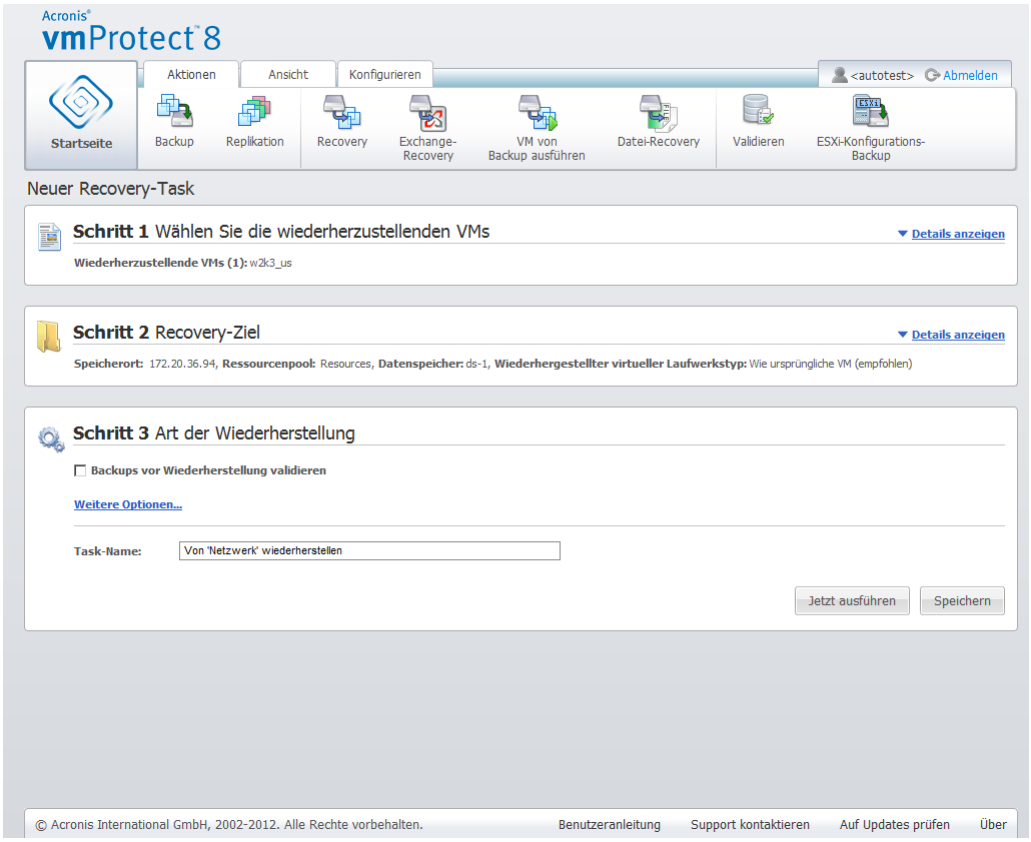
wobei 'Ursprünglicher_Name_der_VM' der ursprüngliche Name der wiederhergestellten virtuellen Maschine ist und DATUM das aktuelle Datum. War der Name der wiederhergestellten VM zum Beispiel 'VM_ursprünglich', wird sie nach der Wiederherstellung 'VM_ursprünglich_25.05.2011' benannt.

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

9.3 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. 94)). Über **Weitere Optionen...** können Sie die Einstellungen des Recovery-Tasks anpassen.



Assistent 'Neuer Recovery-Task', 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** sichern 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.

9.4 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).

9.4.1 Benachrichtigungen

1) E-Mail-Benachrichtigungen

Mit dieser Option richten Sie die E-Mail-Benachrichtigungen über wesentliche Ereignisse während eines Backups 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 die Wiederherstellung fehlschlägt** – die Benachrichtigung erfolgt, wenn Wiederherstellung nicht erfolgreich war.
- **Vollständiges Log zur Benachrichtigung hinzufügen** – um das vollständige Log zu erhalten.

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, der die Nachricht verschickt. Wenn Sie dieses Feld leer lassen, werden die Nachrichten so konstruiert, 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 bei der Wiederherstellung einzeln senden** – um ein Ereignis-Log der Wiederherstellung an spezifizierte SNMP-Manager zu schicken.
  Ereignistypen, die geschickt werden – Wählen Sie die Ereignistypen, die geschickt 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.

9.4.2 Fehlerbehandlung

Mit diesen Optionen geben Sie vor, wie bei der Wiederherstellung 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.

Aktivieren Sie das Kontrollkästchen **Alle Task-Aktionen bei einem Fehler abbrechen**, wenn beispielsweise mehrere, miteinander verbundene VMs wiederhergestellt werden sollen. Es werden dann alle Recovery-Aktionen abgebrochen, sobald eine VM nicht wiederhergestellt werden kann.

9.4.3 VM-Energieverwaltung

Ziel-VMs nach Abschluss der Wiederherstellung einschalten

Mit dieser Option konfigurieren Sie die Energieverwaltung der virtuellen Maschinen nach Ausführen des Recovery-Tasks.

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 anzuschalten.

9.4.4 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 Sie möchten, dass dieser Modus zur Dateiübertragung verwendet wird.

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

9.4.5 Recovery-Einstellungen für den Exchange Server

Bevor Sie die **Exchange-Server-Backup-Extraktion** ausführen, müssen die **Standardeinstellungen für die Exchange-Extraktion** konfiguriert werden. Das Extrahieren von Postfächern oder Postfachinhalten erfordert das temporäre Mounten einer spezifizierten VM aus einem Backup heraus. Öffnen Sie die Registerkarte **Exchange-Einstellungen** und geben Sie die Parameter zum Mounten der VM an.

- ESX(i)-Host
- Ressourcenpool
- Datenspeicher

9.5 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. 85)).

10 Exchange-Server-Backup-Extraktion

Gelegentlich ist es notwendig, aus dem Laufwerk-Backup einer virtuellen Maschine mit installiertem Microsoft Exchange Server nur die Exchange-Daten zu extrahieren. Mit der Funktion **Exchange Server-Elemente extrahieren** können Sie:

- komplette Exchange-Datenbanken aus VM-Backups extrahieren
- Exchange-Daten (Postfächer, Postfachelemente) aus VM-Backups extrahieren

Beachten Sie: Bevor Sie den Assistenten zum Extrahieren von Exchange-Elementen ausführen, müssen die Backups so konfiguriert sein, dass sie 'Exchange-aware' sind. Optional können Sie bestimmen, dass Transaktionsprotokolle nach dem Backup abgeschnitten werden sollen. (Weitere Informationen finden Sie in der Benutzeranleitung im Abschnitt 'Exchange-aware Backup-Einstellungen' (S. 40)).

Klicken Sie in der Registerkarte **Aktionen** auf die Hauptmenüschaltfläche **Exchange-Recovery**, um die gewünschten Exchange-Elemente aus einem Backup-Archiv zu extrahieren. Der Assistent zum **Extrahieren von Exchange-Server-Elementen** besteht aus mehreren Schritten, die erforderlich sind, um die Aktion abzuschließen. Die Schritte für den Assistenten zum Extrahieren von Exchange-Datenbanken, Exchange-Postfächern und Postfach-Inhalten sind in den folgenden Abschnitten beschrieben.

10.1 Datenbanken extrahieren

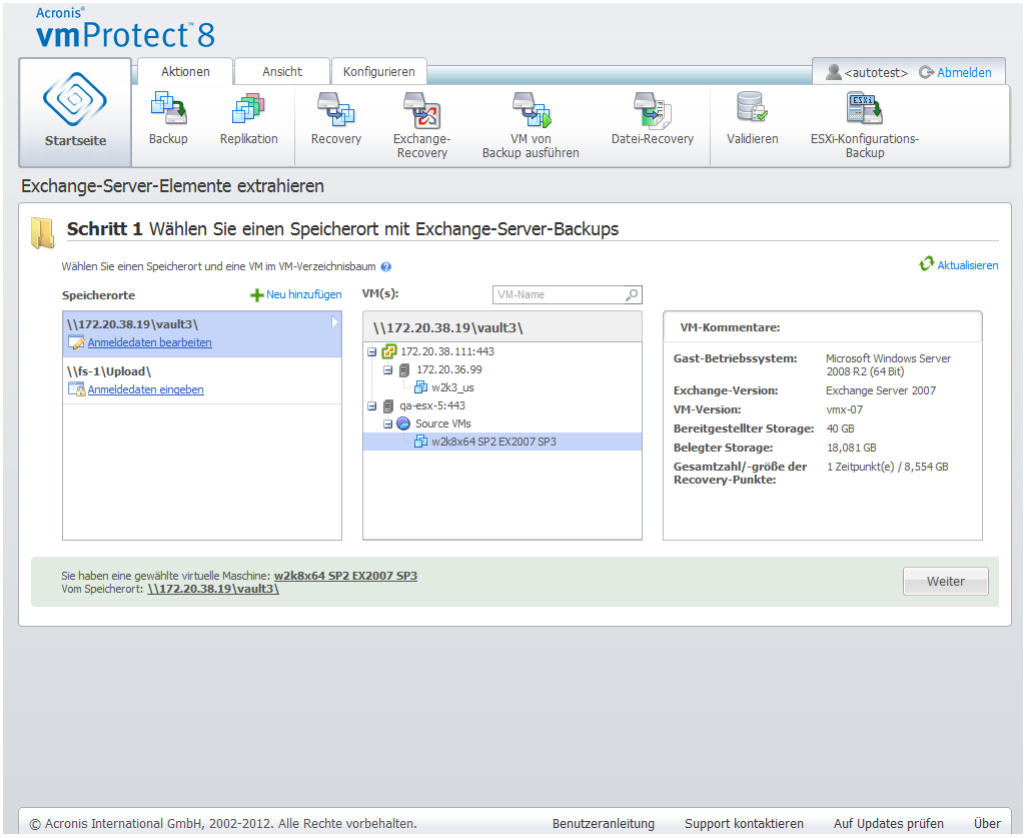
Bei der Extraktion von Datenbanken können Sie die MS Exchange Server-Datenbanken im Format .edb extrahieren und auf einer Netzwerkfreigabe speichern.

Das Wiederherstellen von Datenbanken zu einem spezifizierten Ordner bedeutet, dass die Datenbankdateien zusammen mit den Transaktionsprotokolldateien aus dem Backup zu einem von Ihnen spezifizierten Ordner extrahiert werden. Das ist hilfreich, wenn Daten für eine Überprüfung oder weitere Bearbeitung durch Tools von Drittherstellern extrahiert werden müssen oder wenn Sie nach einer Möglichkeit suchen, die Datenbanken manuell zu mounten.

Um eine Exchange-Datenbank zu extrahieren, müssen Sie die folgenden vier Schritte abschließen:

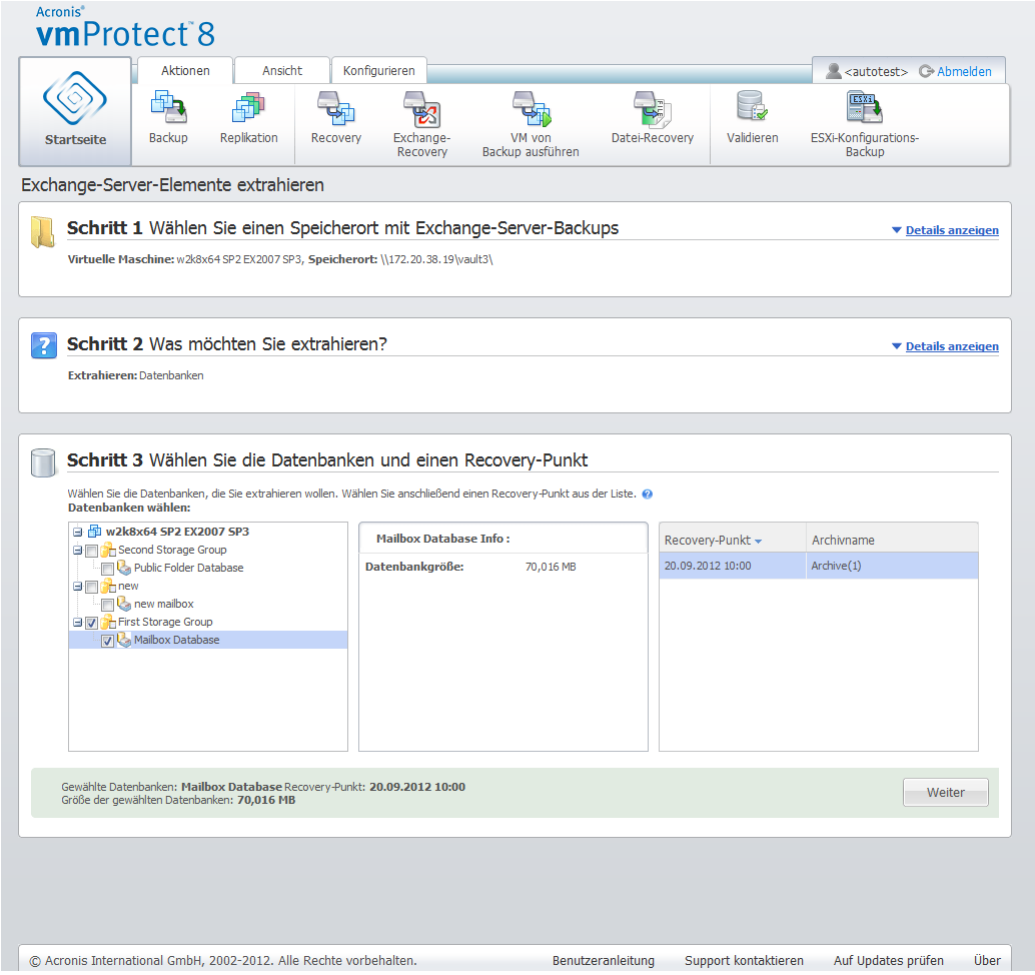
1. **Wählen Sie einen Speicherort für die Exchange-Server-Backups**.
2. **Was möchten Sie extrahieren?** (**Datenbanken**)
3. **Wählen Sie die Datenbanken und einen Recovery-Punkt aus**.
4. **Wählen Sie einen Backup-Ort für die Datenbanken.**

Im ersten Schritt wählen Sie einen Speicherort und eine VM mit Exchange-Server-Backups. Auf der linken Seite wird die Liste der Backup-Speicherorte angezeigt. Der ausgewählte Speicherort wird nach Exchange VM-Backups durchsucht und diese werden im mittleren Bereich angezeigt. Wählen Sie die VM, aus der Datenbanken extrahiert werden sollen. Auf der rechten Seite wird eine Zusammenfassung angezeigt. Klicken Sie auf **Weiter**.



Exchange Server-Elemente extrahieren, Speicherort mit Exchange Server-Backups auswählen

Wählen Sie im zweiten Schritt **Datenbanken** aus. Im dritten Schritt wählen Sie auf der linken Seite die Exchange Server-Datenbanken aus einer Liste aus und auf der rechten Seite einen Recovery-Punkt. Standardmäßig wird der neueste Recovery-Punkt vorausgewählt. Hier werden die Informationen zum ausgewählten Recovery-Punkt, der Datenbank und ihrer Größe angezeigt. Klicken Sie auf **Weiter**.



Exchange Server-Elemente extrahieren, Datenbanken und Recovery-Punkt auswählen

Klicken Sie anschließend auf **Durchsuchen** und wählen Sie den Zielordner aus, in dem das Datenbank-Archiv gespeichert werden soll. Klicken Sie auf **Abschluss**, um die Extraktion zu starten.

Die extrahierten Datenbanken sind im Zustand **Dirty Shutdown** und können nicht gemountet werden. Um die Datenbanken zu mounten, müssen Sie sie mit dem Befehl **Eseutil /r <Enn>** in den Zustand **Clean Shutdown** bringen. **<Enn>** gibt den Logdatei-Präfix für die Datenbank an (bzw. die Speichergruppe, welche die Datenbank enthält), auf die Sie die Transaktionsprotokolldateien anwenden müssen. Anweisungen zur Durchführung finden Sie unter:

- http://technet.microsoft.com/de-de/library/dd876926.aspx
- http://technet.microsoft.com/de-de/library/aa998340(EXCHG.80).aspx

10.2 Postfächer extrahieren

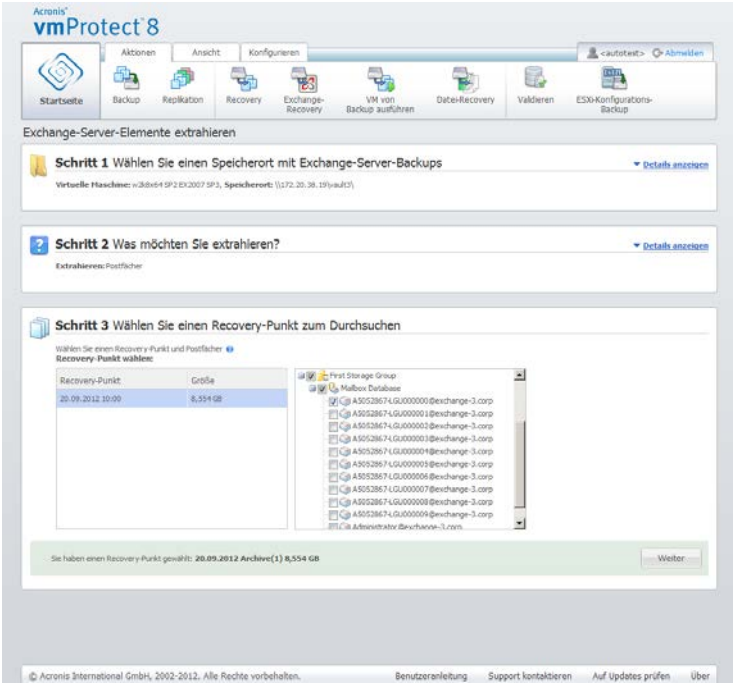
Bei der Extraktion von **Postfächern** können Sie mit folgenden Schritten bestimmte Postfächer auf dem Microsoft Exchange Server extrahieren:

1. **Wählen Sie einen Speicherort für die Exchange-Server-Backups**.
2. **Was möchten Sie extrahieren?** (**Postfächer**)
3. **Wählen Sie einen Recovery-Punkt zum Durchsuchen und ein Postfach bzw. mehrere Postfächer aus**.
4. **Wählen Sie einen Speicherort für die ausgewählten Elemente**.

Im ersten Schritt wählen Sie einen Speicherort und eine VM mit Exchange Server-Backups. Auf der linken Seite wird die Liste der Backup-Speicherorte angezeigt. Der ausgewählte Speicherort wird nach Exchange VM-Backups durchsucht und diese werden im mittleren Bereich angezeigt. Wählen Sie die VM, aus der die Postfächer extrahiert werden sollen. Auf der rechten Seite wird eine Zusammenfassung angezeigt. Klicken Sie auf **Weiter**.

Wählen Sie im zweiten Schritt **Postfächer** aus. Wenn ein weiterer Task zum **Extrahieren von Exchange-Elementen** aktiv ist, erscheint ein Bestätigungsdialog mit entsprechender Warnmeldung. Um mit der aktuellen Suche nach Exchange-Elementen fortzufahren, muss der andere aktive Task angehalten werden. Bestätigen Sie, dass der andere Task angehalten werden soll, um fortzufahren.

Wählen Sie im dritten Schritt auf der linken Seite einen Recovery-Punkt. Standardmäßig wird der neueste Recovery-Punkt vorausgewählt. Durchsuchen Sie auf der rechten Seite den Exchange-Server und wählen Sie das zu extrahierende Postfach bzw. die Postfächer. Klicken Sie auf **Weiter**.



Exchange Server-Elemente extrahieren, Recovery-Punkt für die Suche auswählen

Klicken Sie im letzten Schritt auf **Durchsuchen**, um den Zielordner auszuwählen, in dem die ausgewählten Elemente gespeichert werden sollen, und klicken Sie auf **Abschluss**, um die Extraktion zu starten. Nach Fertigstellen des Assistenten wird der Extraktions-Task erstellt und in der Ansicht **Tasks** angezeigt (**Ansicht** –> **Tasks**). Hier können Sie den Fortschritt des Tasks verfolgen und auf den Task bezogene Statistiken einsehen. Beachten Sie, dass es nicht möglich ist, diesen Task-Typ zu bearbeiten.

Um Postfächer zu extrahieren muss eine temporäre virtuelle Maschine direkt vom ausgewählten Recovery-Punkt des Backups gestartet werden; das kann einige Minuten dauern. Sie können den Fortschritt der Mounting-Aktion verfolgen. Sollte das Mounten fehlschlagen, können Sie dies im Log sehen und den Task abbrechen.

Beachten Sie, dass diese temporäre VM 15 Minuten lang gemountet bleibt. Wenn Sie den Assistenten zum **Extrahieren von Exchange Server-Elementen** verlassen und dann neu starten, können Sie **Damit fortfahren, den zuvor ausgewählten Recovery-Punkt zu durchsuchen**.

Die ausgewählten **Postfächer** werden am angegebenen Zielspeicherort als selbstextrahierendes (.exe) Acronis vmProtect 8-Archiv gespeichert. Sie können Datei auf einer beliebigen Maschine

ausführen, auf der Microsoft Outlook (2003+) installiert ist, um die E-Mails und anderen Elemente im .pst-Format zu extrahieren.

Beim Entpacken der Daten aus dem Archiv können Sie die zu extrahierenden Inhalte auswählen und einen Ordner angeben, in den sie extrahiert werden sollen. Klicken Sie auf **Extrahieren**, um die Aktion zu starten. Die Daten werden in eine .pst-Datei extrahiert, die in Microsoft Outlook geöffnet werden kann (**Datei** –> **Öffnen**). Beachten Sie, dass auf der Maschine, auf der Sie die Daten extrahieren, Microsoft Outlook installiert sein muss (da MAPI benötigt wird).

10.3 Postfachinhalte extrahieren

Bei der Extraktion von **Postfachinhalten** können Sie mit folgenden Schritten Postfächer durchsuchen und bestimmte Inhalte – Ordner und Elemente – extrahieren:

1. **Wählen Sie einen Speicherort für die Exchange-Server-Backups**.
2. **Was möchten Sie extrahieren?** (**Postfachinhalte**)
3. **Wählen Sie die zu extrahierenden Postfächer oder einen Recovery-Punkt zum Durchsuchen aus**.
4. **Wählen Sie die zu extrahierenden Ordner oder Elemente aus**.
5. **Wählen Sie einen Speicherort für die ausgewählten Elemente**.

Im ersten Schritt wählen Sie einen Speicherort und eine VM mit Exchange Server-Backups. Auf der linken Seite wird die Liste der Backup-Speicherorte angezeigt. Der ausgewählte Speicherort wird nach Exchange VM-Backups durchsucht und diese werden im mittleren Bereich angezeigt. Wählen Sie die VM, aus der die Postfächer und Postfachinhalte extrahiert werden sollen. Auf der rechten Seite wird eine Zusammenfassung angezeigt. Klicken Sie auf **Weiter**.

Wählen Sie im zweiten Schritt **Postfachinhalte** aus.

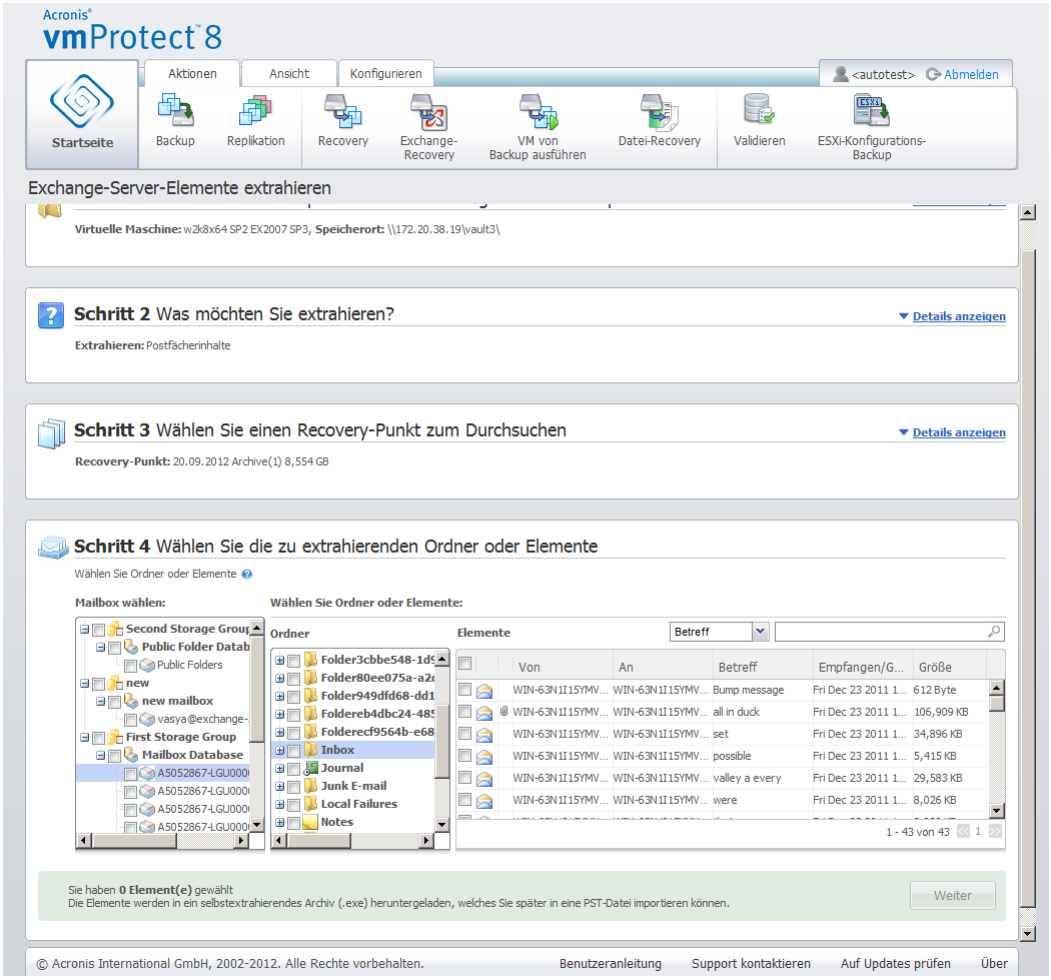
Wählen Sie im dritten Schritt auf der linken Seite einen Recovery-Punkt. Standardmäßig wird der neueste Recovery-Punkt vorausgewählt.

Klicken Sie im vierten Schritt auf **E-Mails durchsuchen**, um die zu extrahierenden Postfachinhalte auszuwählen. Zum Durchsuchen der Postfachinhalte muss eine temporäre virtuelle Maschine direkt vom ausgewählten Recovery-Punkt des Backups gestartet werden; das kann einige Minuten dauern. Sie können den Fortschritt der Mounting-Aktion verfolgen. Nach erfolgreichem Abschluss können Sie die Postfachinhalte auswählen. Sollte das Mounten fehlschlagen, können Sie dies im Log sehen und den Task abbrechen.

Beachten Sie, dass diese temporäre VM 10 Minuten lang gemountet bleibt. Wenn Sie den Assistenten zum **Extrahieren von Exchange Server-Elementen** verlassen und dann neu starten, können Sie **Damit fortfahren, den zuvor ausgewählten Recovery-Punkt zu durchsuchen**.

Die Auswahl von Postfachinhalten im vierten Schritt gestaltet sich wie folgt. Auf der linken Seite wird die Liste der verfügbaren Postfächer angezeigt. Wenn Sie ein Postfach auswählen, werden alle Inhalte in Form von Ordnern und Elementen angezeigt. Wählen Sie alle Elemente aus, die extrahiert werden sollen. Sie können auch Elemente aus anderen Postfächern auswählen. Klicken Sie auf **Weiter**, wenn Sie damit fertig sind.

Klicken Sie im letzten Schritt auf **Durchsuchen**, um den Zielordner auszuwählen, in dem die ausgewählten Elemente gespeichert werden sollen, und klicken Sie auf **Abschluss**, um die Extraktion zu starten. Ein Fenster mit Informationen zur Extraktion der Elemente wird angezeigt.



Exchange Server-Elemente extrahieren, Zielspeicherort für die Elemente auswählen

Die ausgewählten **Postfächer und Postfachinhalte** werden am angegebenen Zielspeicherort als selbstextrahierendes (.exe) Acronis vmProtect 8-Archiv gespeichert. Sie können Datei auf einer beliebigen Maschine ausführen, auf der Microsoft Outlook (2003+) installiert ist, um die E-Mails und anderen Elemente im .pst-Format zu extrahieren.

Beim Entpacken der Daten aus dem Archiv können Sie die zu extrahierenden Inhalte auswählen und einen Ordner angeben, in den sie extrahiert werden sollen. Klicken Sie auf **Extrahieren**, um die Aktion zu starten. Die Daten werden in eine .pst-Datei extrahiert, die in Microsoft Outlook geöffnet werden kann (**Datei –> Öffnen**). Beachten Sie, dass auf der Maschine, auf der Sie die Daten extrahieren, Microsoft Outlook installiert sein muss (da MAPI benötigt wird).

11 VM von Backup ausführen

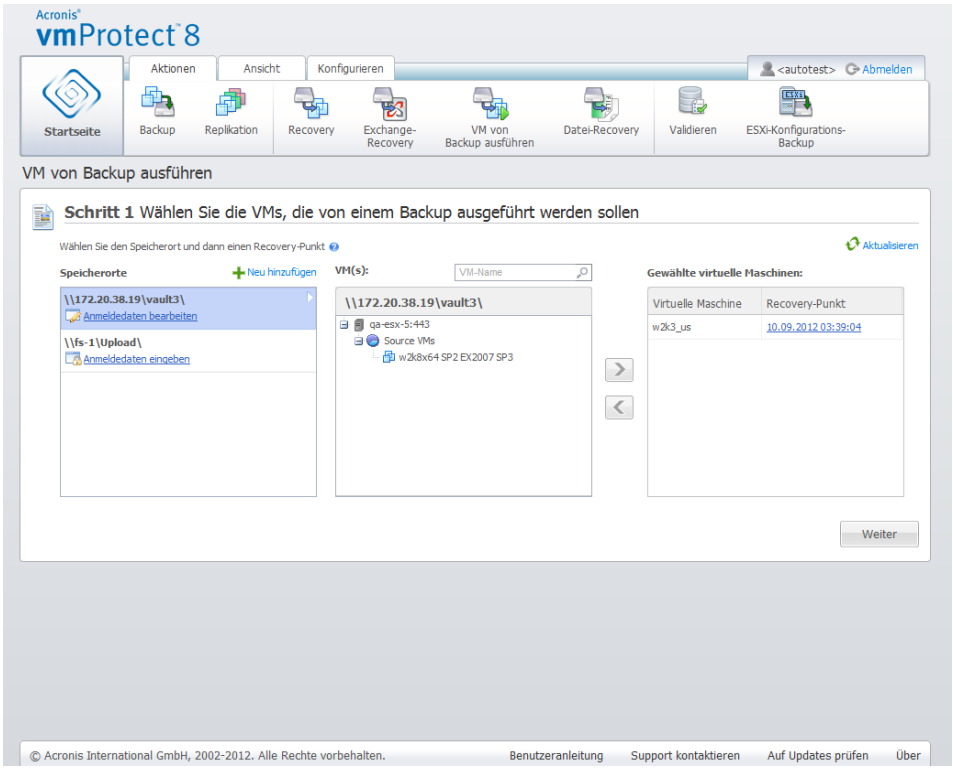
Klicken Sie auf **VM von Backup ausführen** (in der Registerkarte **Aktionen** des Hauptmenüs), um eine zuvor gesicherte virtuelle Maschine zu mounten, ohne sie zuvor wiederherzustellen. Der **VM von Backup ausführen**-Assistent öffnet sich im Hauptarbeitsbereich und fordert Sie auf, für die Wiederherstellung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

- Wählen Sie die VMs, die von einem Backup ausgeführt werden sollen.
- Ort der VM-Ausführung.
- Erweiterte Einstellungen

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

11.1 Wählen Sie die VMs, die von einem Backup ausgeführt werden sollen

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 'Wählen Sie die VMs, die von einem Backup ausgeführt werden sollen'

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.

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. 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 **<** sowie durch Verschieben von der linken auf die rechte Seite. Die Liste auf der rechten Seite zeigt dann alle zum Mounten ausgewählten virtuellen Maschinen. Mit der Schaltfläche **>** fügen Sie VMs zur Liste hinzu, mit der Schaltfläche **<** entfernen Sie die VMs aus der Liste. Die so aufgebaute Liste enthält die ausgewählten virtuellen Maschinen und ihre neuesten verfügbaren Recovery-Punkte, d.h., die Zeitpunkte, auf die Sie zurücksetzen können.

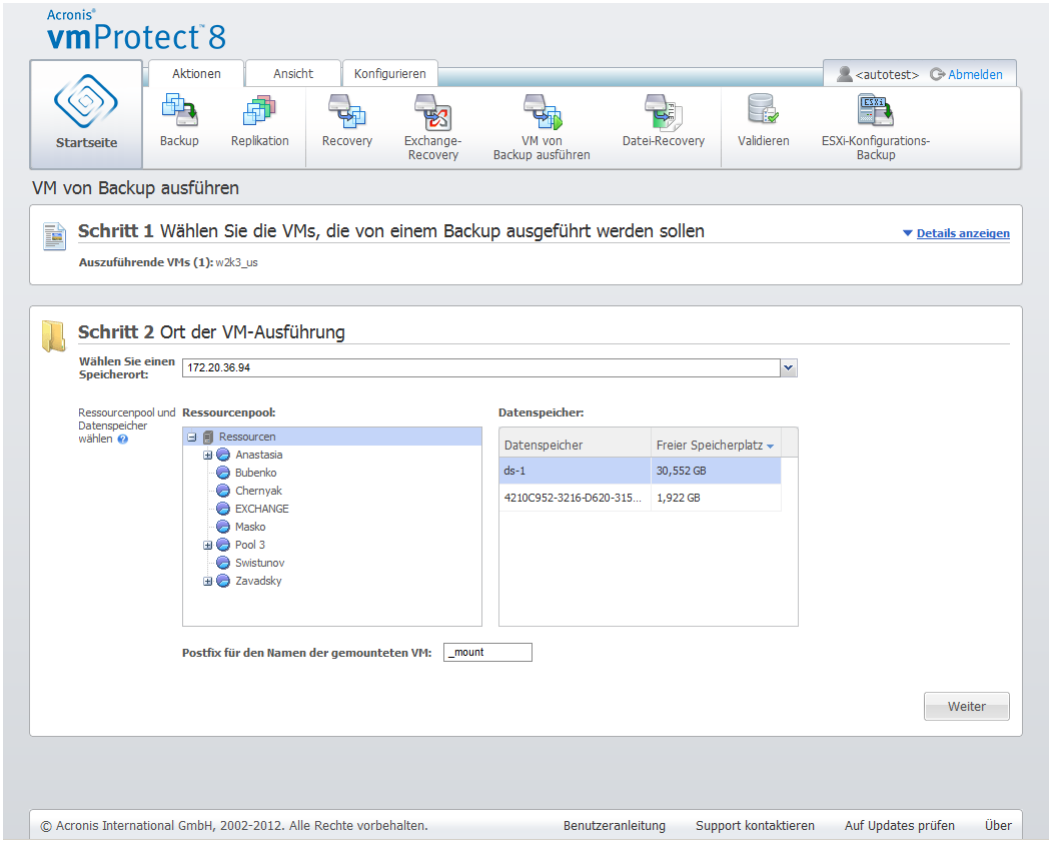
Standardmäßig wird der neueste Recovery-Punkt einer virtuellen Maschine voreingestellt. Klicken Sie auf den Recovery-Punkt, um ihn zu ändern. Im sich öffnenden Fenster können Sie dann einen anderen Recovery-Punkt wählen.

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.

Wählen Sie die wiederherzustellenden VMs und klicken Sie auf **Weiter**, um den ersten Schritt des Assistenten abzuschließen und fortzufahren.

11.2 Ort der VM-Ausführung

Im zweiten Schritt entscheiden Sie, wo die ausgewählten virtuellen Maschinen ausgeführt werden sollen.



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

Zunächst bestimmen Sie über das Listenfeld **Speicherort auswählen** den ESX(i)-Host, auf den Sie die ausgewählten VMs mounten wollen. Die Liste zeigt nur die vom Acronis vmProtect Agenten verwalteten ESX(i)-Hosts an. Ist der gewünschte ESX(i)-Host nicht in der Liste, stellen Sie sicher, dass er in der Ansicht **Konfigurieren** –> **ESX(i)-Hosts** hinzugefügt wird.

Sobald der ESX(i)-Host bestimmt ist, wird automatisch eine Liste mit den verfügbaren Ressourcenpools aufgebaut, in der Sie den genauen Speicherort für die gemounteten virtuellen Maschinen festlegen können. Die Wahl des Datenspeichers ist erforderlich, um zu definieren, wo die an den gemounteten virtuellen Maschinen vorgenommenen Änderungen gespeichert werden.

Beachten Sie, dass beim Mounten mehrerer virtueller Maschinen alle am selben Ziel gespeichert werden, das bei diesem Schritt des Assistenten **VM von Backup ausführen** festgelegt wird, jede von ihnen in einem separaten Ressourcenpool. Die an diesen VMs vorgenommenen Änderungen werden in einem eindeutigen Verzeichnis auf dem ausgewählten Datenspeicher gespeichert.

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(i)-Host auszuführen, insbesondere wenn die ursprüngliche VM dort bereits läuft. Die gemountete VM wird auf Basis folgender Konvention benannt:

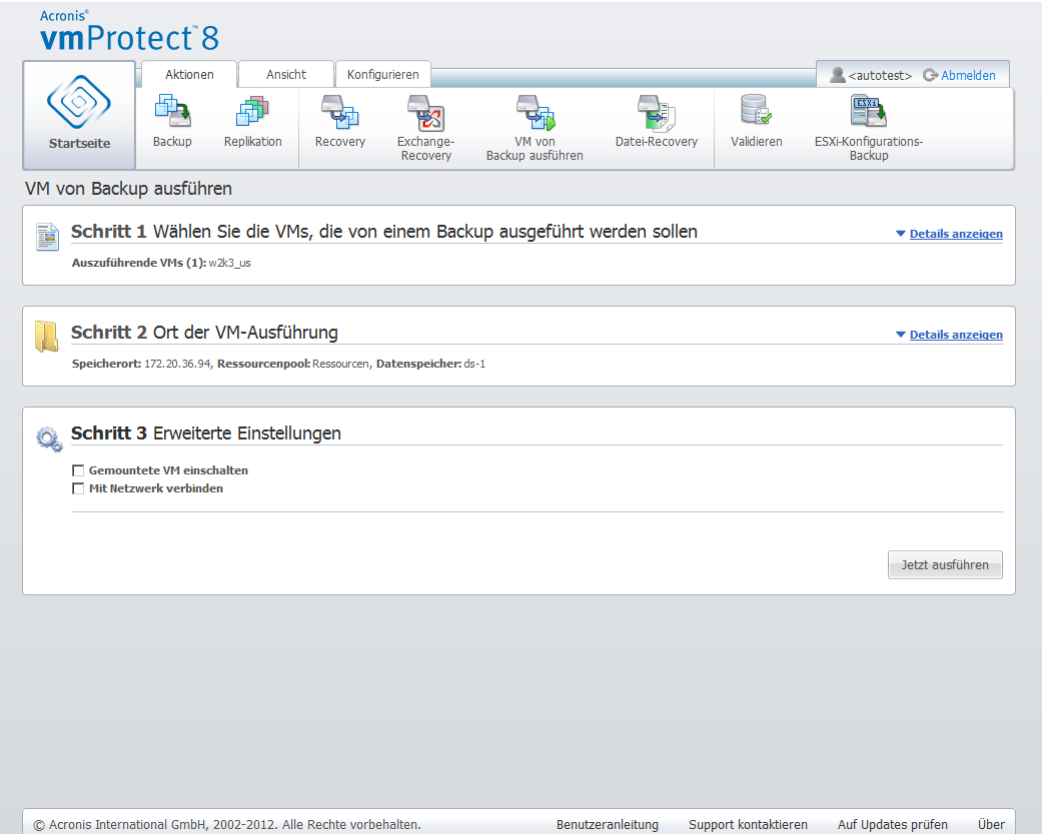
'[Ursprünglicher_Name_der_VM]_mount'

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 zum letzten Schritt zu gelangen.

11.3 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**.

11.4 Verwalten der 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.

Zusätzlich zur Option **Trennen** gibt es noch die Option **Trennen und Speichern**; damit wird die gemountete VM heruntergefahren und beim Anhalten der Maschine ein inkrementelles Backup der Änderungen erstellt. Beachten Sie, dass das Herunterfahren (Ausschalten) erzwungen wird, wenn die Maschine fünf Minuten lang nicht angehalten werden kann.

12 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 8 Management Console ausgeführt wird. (Der Dialog ist derselbe, der beim Speichern einer Internetseite mit dem Befehl **Datei** –> **Speichern unter** angezeigt wird).

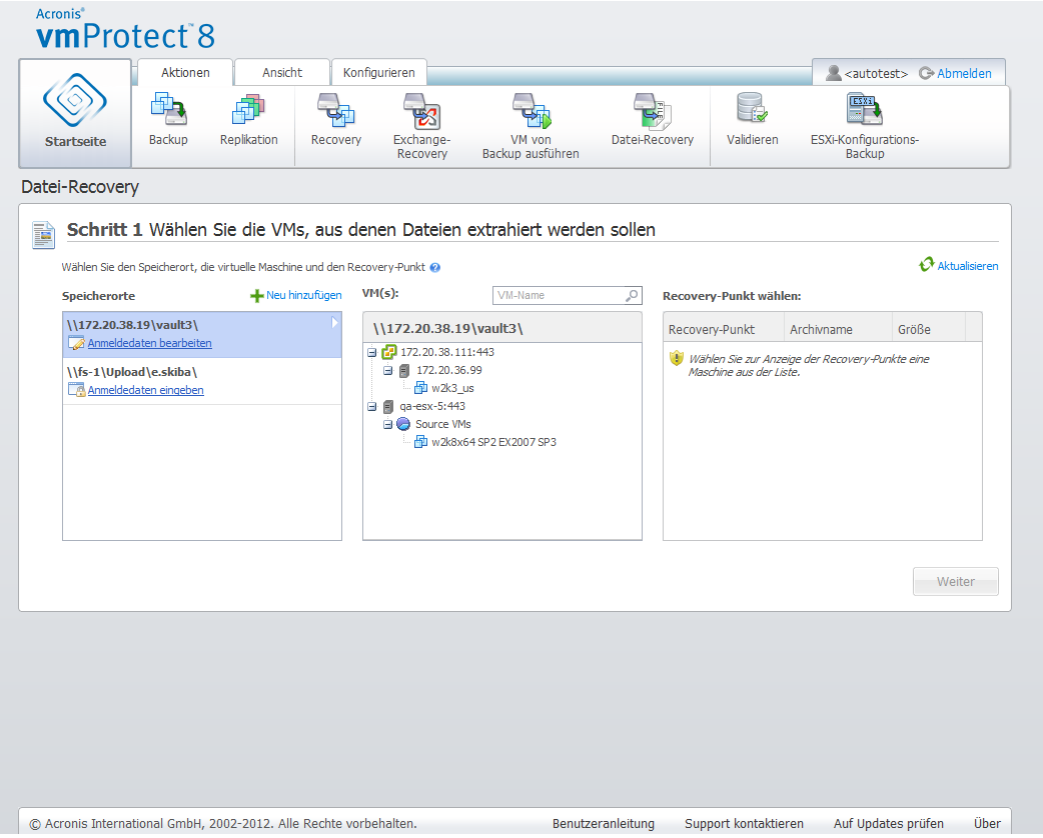
Klicken Sie auf **Datei-Recovery** auf der **Startseite** im Hauptmenü, um eine oder mehrere gesicherte Dateien wiederherzustellen. Der **Datei-Recovery**-Assistent öffnet sich im Hauptarbeitsbereich und fordert Sie auf, für die Wiederherstellung der Dateien die erforderlichen Informationen bereitzustellen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

- Wählen Sie die VMs, aus denen Dateien extrahiert werden sollen.
- Recovery-Punkt durchsuchen

Beachten Sie: Die Funktion 'Datei-Recovery' ist nicht für Backups verfügbar, die auf dem Acronis Online Backup Storage gespeichert sind. Sie können von diesem Backup-Storage-Typ nur die Wiederherstellung kompletter VMs durchführen.

12.1 Wählen Sie die VMs, aus denen Dateien extrahiert werden sollen

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



'Datei-Recovery'-Assistent, Schritt 1 „Wählen Sie die VMs, aus denen Dateien extrahiert werden sollen“

Sollten sich am gewählten Speicherort kennwortgeschützte Archive oder Archive physikalischer Maschinen befinden (verschlüsselte Daten und Daten von physikalischen Maschinen), dann müssen Sie das Kennwort angeben, um Ihre Daten aus diesen Archiven wiederherstellen zu können.

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.

12.2 Recovery-Punkt durchsuchen

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.

Acronis vmProtect 8 **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 kennen. Sie können die Dateien und Verzeichnisse in der Liste mit Hilfe von Suchkriterien filtern, so dass nur solche Elemente angezeigt werden, die diesen so genannten „Dateimasken“ entsprechen.

Dabei können Sie die Wildcards '*' und '?' als Dateimaske benutzen, z.B.: „C:\Finanzen*.*“

Sie können die Suchergebnisse 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.

Beachten Sie, dass eine erfolgreiche **Datei-Recovery** nicht möglich ist, wenn ein Dateiname unzulässige Zeichen enthält: * : ? « < > | / \. Verwenden Sie zum Wiederherstellen solcher Dateien die Aktion **VM von Backup ausführen**.

13 P2V-Migration

13.1 So führen Sie eine P2V-Migration aus

Zur Reduzierung der Hardware-Anforderungen ist oft eine Migration von physikalischen zu virtuellen Maschinen erforderlich. Um eine physikalische zu einer virtuellen Maschine zu migrieren (P2V), booten Sie die physikalische Maschine mit einem bootfähige Medium, erstellen ein Voll-Backup und führen dann die Wiederherstellung zu einer virtuellen Maschine durch.

Führen Sie folgende Schritte aus, um eine P2V-Migration durchzuführen:

1. Erstellen Sie ein bootfähiges Acronis Medium. Laden Sie den Acronis Bootable Media Builder für Acronis vmProtect 8 aus dem Bereich Meine Produkte und Downloads Ihres Kontos auf der Acronis-Website herunter. Installieren Sie ihn.
2. Booten Sie die physikalische Maschine, die Sie für die P2V-Migration benötigen, vom bootfähigen Acronis Medium.
3. Erstellen Sie ein Voll-Backup der physikalischen Maschine.
4. Führen Sie die Acronis vmProtect 8 Webkonsole aus, stellen Sie eine Verbindung zum Acronis Agenten her und klicken Sie auf der Registerkarte **Aktionen** auf **Wiederherstellen**.
5. Wählen Sie das erstellte Backup und den ESX(i)-Host, auf dem das Backup wiederhergestellt werden soll.

14 ESXi-Hosts auf fabrikneuer Hardware wiederherstellen (Bare Metal Recovery)

Acronis vmProtect 8 bietet mit dem Wiederherstellen eines ESXi-Hosts auf fabrikneuer Hardware (Bare Metal Recovery, BMR) eine einzigartige Funktion, welche die Wiederherstellungszeit auf ein Minimum reduziert, wenn der ESXi-Server abstürzt, nicht startet oder nach einem Patch-Update nicht mehr richtig arbeitet. Mit dieser Funktion können Binärdateien und Patches für den ESXi-Server sowie ESXi-Konfigurationen und fehlende VMs nach der Wiederherstellung und dem Neustart des ESXi-Servers wiederhergestellt werden ('fehlende VMs' sind in den Backups vorhanden, fehlen aber in den Datenspeichern; VMs sollten separat gesichert werden).

Bare Metal Recovery unterstützt nur die Versionen 4.1 und 5.0 von VMware ESXi; sie unterstützt nicht ESX.

Beachten Sie: Eine Wiederherstellung der ESXi-Host-Konfiguration kann nur auf lokale Laufwerke durchgeführt werden. Eine Wiederherstellung auf an das System angeschlossene USB-Laufwerke wird nicht unterstützt.

Die folgenden Abschnitte beschreiben, wie Sie Backup und Wiederherstellung einer **ESXi-Host-Konfiguration** einrichten.

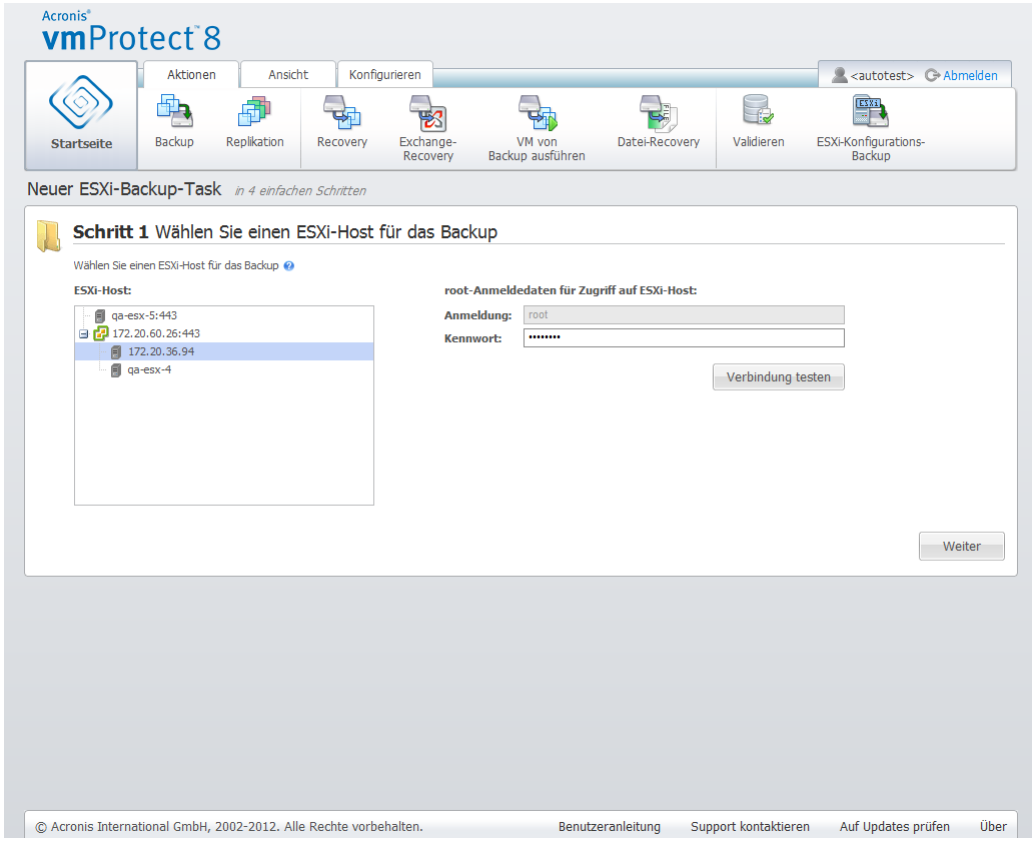
14.1 Backup einer ESXi-Host-Konfiguration

Das **Backup einer ESXi-Konfiguration** in Acronis vmProtect 8 unterscheidet sich vom Backup einer virtuellen Maschine.

Beim Backup einer ESXi-Host-Konfiguration wird die Aktivierung des SSH-Zugriffs für den ESXi-Host erzwungen, d.h., die Konfiguration wird automatisch angepasst, um die Sicherung einer ESXi-Konfiguration zu ermöglichen.

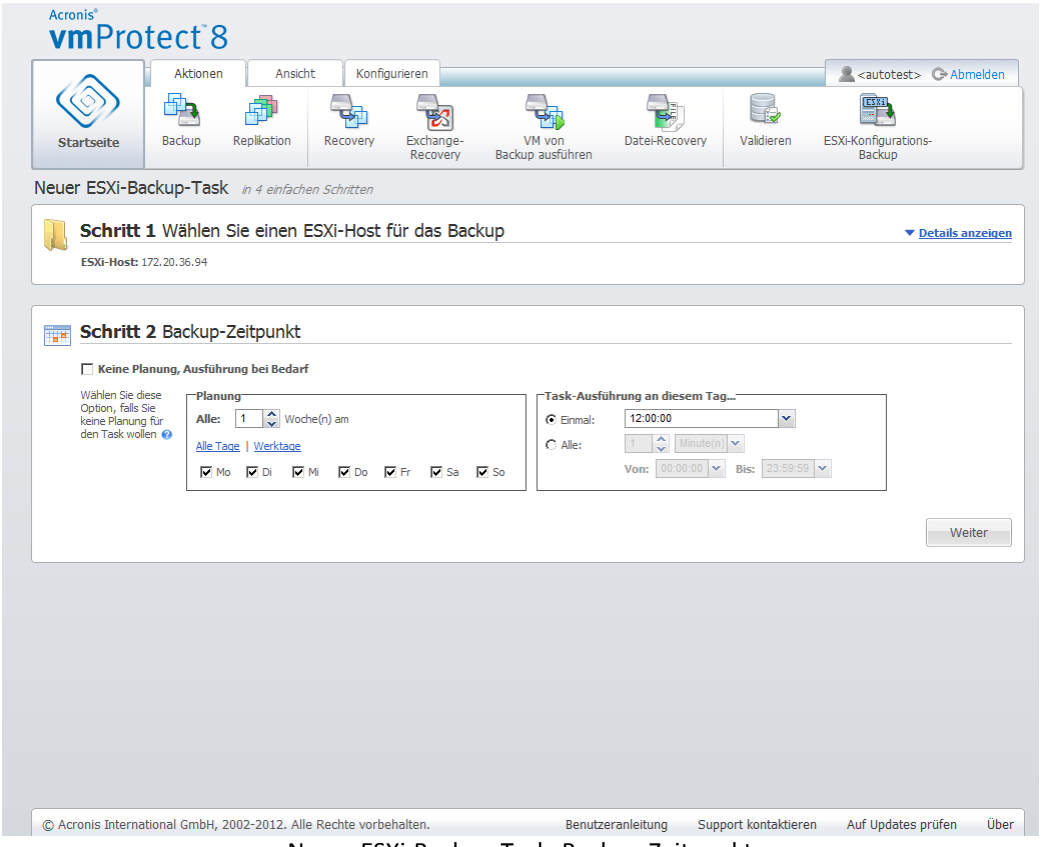
Um das Backup einer ESXi-Host-Konfiguration zu erstellen, führen Sie den Assistenten **Neuer ESX(i)-Backup-Task** aus; klicken Sie dazu auf **Aktionen** –> **ESXi-Konfigurations-Backup**. Wählen Sie im ersten Schritt des Assistenten **Neuer ESXi-Backup-Task** (**Wählen Sie einen ESXi-Host für Backup**) den ESXi-Host aus, dessen Konfiguration per Backup gesichert werden soll. Wählen Sie den ESXi-Host aus der Liste aller ESXi-Hosts bzw. des vCenters aus, die der Acronis vmProtect 8 Agenten verwaltet. Ist der gesuchte Host nicht in der Liste der **ESXi-Hosts**, stellen Sie sicher, dass er auf der Seite **Konfigurieren** –> **ESX(i)-Hosts** hinzugefügt wird. Beachten Sie, dass **ESXi-Backups** nur ESXi-Server unterstützen. ESX-Server können nicht für ein Backup ausgewählt werden.

Geben Sie nach Auswahl des ESXi-Host die 'root'-Anmeldedaten (Login/Kennwort) für den Zugriff ein. Um ein Backup der ESXi-Binärdateien und -Patches zu erstellen, wird eine SSH-Verbindung mit dem ESXi-Server aufgebaut. Dafür sind die root-Anmeldedaten erforderlich. Sie können auf **Verbindung testen** klicken, um die Gültigkeit der Anmeldedaten zu überprüfen. Klicken Sie auf **Weiter**.



Neuer ESXi-Backup-Task, Wählen Sie einen ESXi-Host für das Backup

Im zweiten Schritt (**Zeitpunkt des Backups**) bestimmen Sie, wann das Backup ausgeführt werden soll. Die Optionen im BMR-Backup-Scheduler sind identisch mit denen im VM-Backup-Assistenten.



Neuer ESXi-Backup-Task, Backup-Zeitpunkt

Wählen Sie im dritten Schritt (**Backup-Ziel**) den Archivnamen und den Speicherort, wo Ihr ESXi-Konfigurations-Backup-Archiv hinterlegt wird. Klicken Sie auf **Durchsuchen**; wählen Sie im Fenster, das sich öffnet, einen der nachfolgend aufgelisteten Speicherorte und klicken Sie dann auf **OK**:

- **Lokale Ordner**
- **Netzwerkordner**
- **FTP-Server**
- **SFTP-Server**

ESXi-Backups werden nur entsprechend dem Backup-Schema für mehrere Dateien (Archiv im Legacy-Modus) (S. 9) erstellt. Die Option **Alle Backups in einer Datei speichern (empfohlen)** ist deaktiviert.

Aktivieren Sie das Kontrollkästchen **Alte Backups automatisch löschen**, um Bereinigungsregeln einzurichten. Die Details zu diesen Einstellungen sind im Abschnitt 'Backup-Ziel (S. 35)' erläutert.

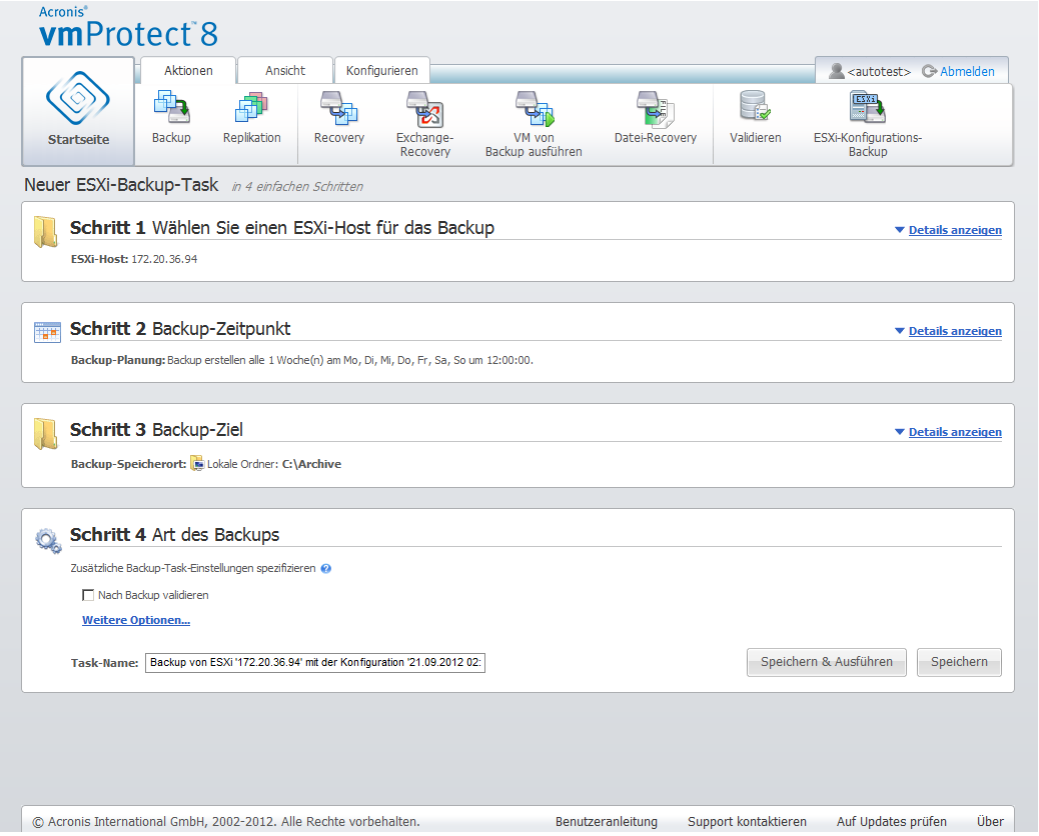
Aktivieren Sie das Kontrollkästchen **Das Backup zu einem zweiten Speicherort kopieren**. Die folgenden Einstellungen ermöglichen Ihnen, die Optionen für 'Backup kopieren' zu konfigurieren. Wählen Sie den zweiten Speicherort, an dem Ihre Backups ebenfalls gespeichert werden sollen und dann den **Archivnamen**. Klicken Sie auf 'Durchsuchen' und wählen Sie aus der Liste der verfügbaren Speicherorte den gewünschten.

Wählen Sie aus dem Listenfeld **Kopie-Zeitpunkt**, ob Sie möchten, dass das Backup sofort nach jeder Backup-Erstellung zum zweiten Speicherort kopiert werden soll. Alternativ können Sie auch spezifische Tage angeben, an denen Ihre Backup-Kopie durchgeführt werden soll, abweichend von den Tagen der eigentlichen Backup-Planung. In diesem Fall können Sie außerdem die Option **Alle verpassten Recovery-Punkte kopieren** oder **Nur zuletzt erstellte Recovery-Punkte kopieren** aktivieren.

Die Option **Nur zuletzt erstellte Recovery-Punkte kopieren** kann hilfreich sein, wenn der gewählte erste Speicherort manchmal nicht verfügbar ist. Sollte die Option **Alle verpassten Recovery-Punkte kopieren** ausgewählt sein und die Aufbewahrungsregeln für den ersten Storage auf dem Hauptspeicherort ausgeführt werden, dann löscht die Software die Recovery-Punkte, die gemäß dieser Regeln entfernt werden sollen – und das auch dann, wenn diese Recovery-Punkte nicht zum zweiten Speicherort kopiert wurden. Wenn die Aufbewahrungsregeln daher ausgeführt werden, wird also nicht überprüft, ob die Recovery-Punkte bereits zum zweiten Speicherort kopiert wurden (oder nicht).

Standardmäßig sind der Backup-Typ und die Bereinigungsregeln für die kopierten Backups identisch zu den entsprechenden primären Backup-Einstellungen. Mittlerweile können Sie wählen, ob Sie andere Einstellungen spezifizieren wollen, beispielsweise die Optionen für die Bereinigungsregeln zu ändern.

Aktivieren Sie im letzten Schritt (**Art des Backups**) bei Bedarf das Kontrollkästchen **Nach Backup validieren**. Klicken Sie auf **Weitere Optionen...**, um das Fenster mit den zusätzlichen Einstellungen zu öffnen. Diese Optionen sind in der Benutzeranleitung im Abschnitt Backup-Optionen (S. 42) beschrieben. Beachten Sie, dass folgende Optionen nicht zur Verfügung stehen: **Schutz des Archivs**, **Zusätzliche Einstellungen** –> **Deduplizierung**, **Zusätzliche Einstellungen** –> **CBT-Backup**.



Neuer ESXi-Backup-Task, Art des Backups

Zum Fertigstellen des Assistenten **Neuer ESXi-Backup-Task** müssen Sie einen Namen für den Task vergeben. Beachten Sie, dass die Zeichen [ ] { } ; , . in Task-Namen nicht erlaubt sind. Die Standardbezeichnung für den Task ist 'Backup der ESXi-Konfiguration [Datum/Zeit]'.

Wenn Sie auf die Schaltfläche **Speichern** klicken, wird der **neue ESXi-Backup-Task** mit den von Ihnen festgelegten Parametern gespeichert und erscheint in der Ansicht **Tasks**. Wenn Sie auf die Schaltfläche **Speichern und Ausführen** klicken, wird der Task gespeichert und umgehend ausgeführt.

14.2 Recovery einer ESXi-Host-Konfiguration

Durch das Wiederherstellen einer ESXi-Host-Konfiguration (BMR-Recovery) kann der ESXi-Server schnell wiederhergestellt werden, z.B. wenn er abgestürzt ist und sich nicht booten lässt. Mit dem Assistenten **ESXi-Host-Recovery** können Sie die Wiederherstellung einer früheren Konfiguration des ESXi-Hosts einrichten, die in einem bereits erstellten Backup gespeichert ist. Mit Hilfe des Assistenten können Sie lokale Datenspeicher (auf lokalen Laufwerken erstellte Datenspeicher) überprüfen und neu konfigurieren sowie vSwitches, die zuvor physikalischen NICs zugeordnet waren, neu zuordnen. Weiterhin können Sie bestimmen, welche Backup-Speicherorte für das Wiederherstellen der fehlenden VMs verwendet werden sollen, nachdem der ESXi-Host wiederhergestellt wurde und bootet.

Auf den Assistenten **ESXi-Host-Recovery** können Sie nur über die Benutzeroberfläche eines bootfähigen Acronis Mediums zugreifen. Ein solches Medium können Sie mit dem Acronis Bootable Media Builder erstellen. Hierfür gibt es ein separates Installationspaket. Sie können diese Funktion nicht über die Web-Oberfläche des Acronis vmProtect 8 Agenten ausführen.

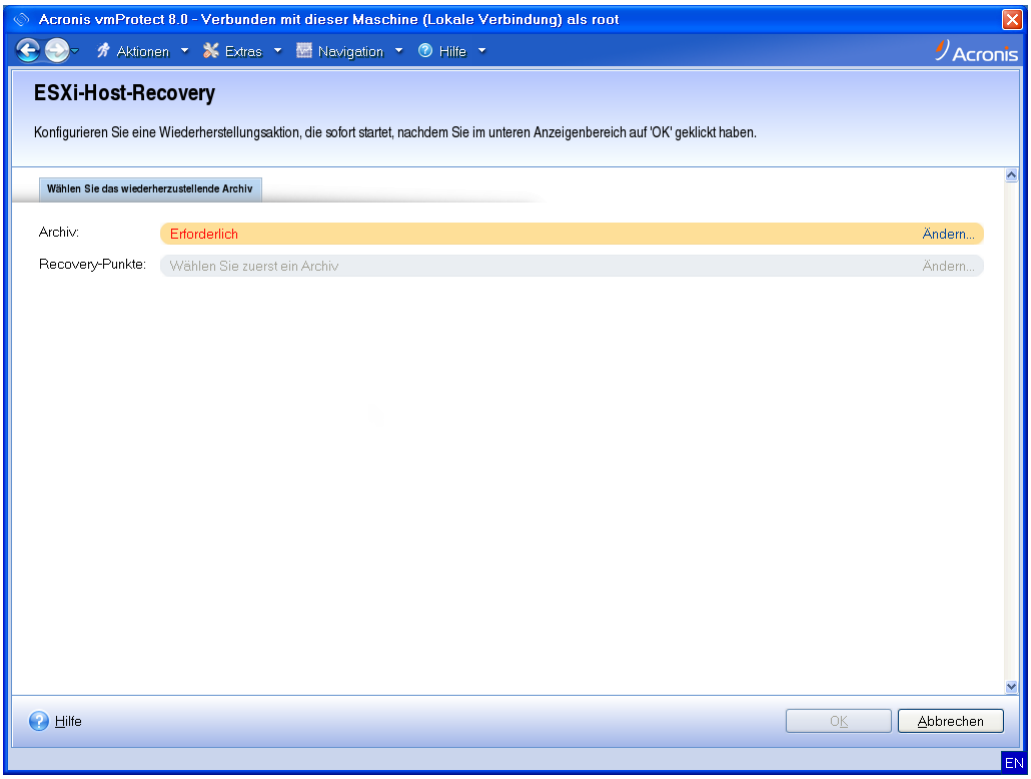
Wählen Sie im ersten Schritt das **Archiv** und den wiederherzustellenden **Recovery-Punkt** aus. Öffnen Sie das Pop-up-Fenster und wählen Sie den Speicherort aus, an dem das Backup-Archiv der

ESXi-Host-Konfiguration gespeichert ist. Wählen Sie dann das **Archiv** mit dem **ESXi-Host-Backup**. Nach Auswahl des Archivs ist standardmäßig der neueste Recovery-Punkt vorausgewählt. Sie können die Standardvorauswahl aber auch ändern.

Im zweiten Schritt müssen Sie die **vmProtect 8 Backup-Speicherorte auswählen**. Aktivieren Sie das Kontrollkästchen für den Backup-Speicherort und geben Sie im Fenster die Anmeldedaten ein. Es werden alle Speicherorte aufgelistet. Ausgewählte Speicherorte werden grau und nicht ausgewählte Speicherorte gelb angezeigt.

Die Speicherorte werden entsprechend den im Backup-Archiv einer ESXi-Host-Konfiguration vorhandenen Inhalten aufgelistet, in dem die Informationen über die Backup-Speicherorte der VMs gespeichert sind (Pfad für die **letzten Speicherorte**). In diesem Schritt können Sie neue Speicherorte hinzufügen. All diese Speicherorte werden für die Wiederherstellung von VM-Backups verwendet, wenn der ESXi-Host wieder läuft. Die Speicherorte können außerdem mit einem Kennwort geschützt werden; diese Anmeldedaten werden nach Wiederherstellen des ESXi-Servers für den Datenzugriff benötigt, wenn Acronis vmProtect 8 mit der Wiederherstellung der fehlenden VMs beginnt. Nur die folgenden Speicherorte stehen in diesem Schritt zur Auswahl:

- **Netzwerkordner**
- **FTP-Server**
- **SFTP-Server**



ESXi-Host-Konfiguration wiederherstellen

Beachten Sie, dass die VMs nach Wiederherstellen der ursprünglichen ESXi-Server-Konfiguration nicht automatisch wiederhergestellt werden, wenn Sie hier nicht die Backup-Speicherorte der VMs auswählen. In diesem Fall müssen Sie die fehlenden VMs manuell wiederherstellen.

Beachten Sie außerdem, dass unvorhersehbare Probleme auftreten können, wenn Sie die ESXi-Host-Konfiguration auf einer neuen Maschine wiederherstellen, während der ursprüngliche ESXi-Host aktiv ist und von einem vCenter verwaltet wird. Entfernen Sie vor der Wiederherstellung

den ursprünglichen ESXi-Host aus dem vCenter und fügen Sie ihn nach der Wiederherstellung wieder hinzu.

Im dritten Schritt müssen Sie die **lokalen Datenspeicher konfigurieren**. Da der ursprüngliche ESXi-Server fehlerhaft werden kann oder das Systemlaufwerk und der Datenspeicher verloren gehen können, unterscheidet sich die Zielkonfiguration möglicherweise von der des ursprünglichen Servers.

In der Liste werden die gefundenen Festplatten und ihre Größe angezeigt. Hier können Sie sehen, welche Datenspeicher bereits auf den gefundenen Festplatten vorhanden sind. Wenn ein Datenspeicher auf den Festplatten dem Datenspeicher in der ursprünglichen (im Backup der ESXi-Konfiguration gespeicherten) Konfiguration entspricht, wird sein Name in grün angezeigt. Wenn ein Datenspeicher gefunden wird, jedoch nicht der ursprünglichen Konfiguration entspricht, wird sein Name in gelb angezeigt. Wenn der gefundene Datenspeicher für die Erstellung eines neuen Datenspeichers bereinigt wird, wird sein Name in rot angezeigt. Aktivieren Sie das Kontrollkästchen **Für neue Datenspeicher verwenden**, um die Festplatte für die Erstellung eines neuen Datenspeichers zu verwenden.

Der neue Datenspeicher wird auf allen, in diesem Schritt ausgewählten Laufwerken erstellt; vorhandene Daten auf diesen Laufwerken werden dabei überschrieben. Sie sollten daher Ihre Auswahl sorgfältig prüfen.

Im vierten Schritt müssen Sie ein **virtuelles Netzwerk konfigurieren**. Dieser Schritt ist erforderlich für die Zuordnung der vSwitches im Backup der ESXi-Konfiguration, das auf physikalischen NICs wiederhergestellt wird. Sie können das Backup einer ESXi-Konfiguration auf demselben Server oder auf abweichender Hardware wiederherstellen. Mit diesem Schritt ist Folgendes möglich:

- Standardmäßig wird eine automatische Zuordnung verwendet. Die aktuelle Hardware wird nach NICs durchsucht, um diese dann automatisch den vSwitches im Backup der ESXi-Konfiguration zuzuordnen. Sie können die automatische Zuordnung der vSwitches überprüfen und sie, falls erforderlich, neu zuordnen.
- Während der Wiederherstellung des ESXi können Sie überprüfen, ob das Kabel an vmnicX angeschlossen ist oder nicht.

Klicken Sie, nachdem Sie alle Schritte ausgeführt haben, auf **OK**, um die Wiederherstellung zu starten. Bei der Wiederherstellung passiert nun Folgendes:

1. Mit der ersten Festplatte (gemäß der BIOS-Reihenfolge) werden die ESXi-Systempartitionen erstellt und dann bootet das System neu in die ESXi-Umgebung.
2. Beim Starten führt der ESXi-Server ein spezielles Skript aus, das die vSwitches und Datenspeicher entsprechend den im Recovery-Assistenten für die ESXi-Konfiguration angegebenen Einstellungen konfiguriert.
3. Der Acronis vmProtect 8 Agent (Virtual Appliance) wird in dem neu erstellten Datenspeicher bereitgestellt. Dann stellt der Agent die fehlenden virtuellen Maschinen aus den im Recovery-Assistenten für die ESXi-Konfiguration angegebenen Backup-Speicherorten wieder her. Außerdem durchsucht er die Backup-Speicherorte nach VMs auf dem ursprünglichen ESXi-Host, die nach dem Backup der ESXi-Konfiguration gesichert wurden, und stellte diese virtuelle Maschinen wieder her.

- Eine virtuelle Maschine wird als 'fehlend' bezeichnet, wenn sie in keinem der Datenspeicher gefunden wird, die der wiederhergestellte ESXi-Host aktuell erkennt.
- Die virtuellen Maschinen werden in allen erkannten Datenspeichern wiederhergestellt und füllen diese allmählich, wobei mindestens 10% Speicherplatz frei bleiben.

15 Tasks verwalten

Klicken Sie im Hauptmenü auf der Registerkarte **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/Validierung etc. zu erstellen, gehen Sie zur Registerkarte **Startseite** in der Hauptsymbolleiste).

Die Seite präsentiert eine allgemeine Liste aller im Acronis vmProtect 8 Agenten erstellter Tasks. Die Liste der Tasks enthält Aktionen zu Backup, Recovery, Validierung etc., die über die entsprechenden Bereiche in der Registerkarte **Startseite** der Hauptsymbolleiste erstellt worden sind.

Die Task-Liste stellt folgende Informationen über den Task bereit:

- **Task-Name** – der Unique Task Identifier.
- **Task-Typ** – *Backup*, *Recovery*, *Validierung*, *etc.*
- **Letzte Abschlusszeit** – Zeit, die seit der letzten Task-Fertigstellung verstrichen ist.
- **Nächster Task** – der Zeitpunkt, wann der Task ausgeführt wird oder *Manuell*.
- **Status** – *Inaktiv* oder *Wird ausgeführt*.

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

Alle bisher ausgeführten Tasks zeigen zudem den Status des letzten Ergebnis – **Erfolgreich abgeschlossen** (letzte Ausführung war erfolgreich), **Warnung** (der Task wurde bei der letzten Ausführung mit Warnungen beendet) oder **Fehler** (der Task ist bei der letzten Ausführung fehlgeschlagen). Sie können die Logs zum Task einsehen, indem Sie auf den Status des letzten Ergebnis klicken. Für noch nicht ausgeführte Tasks werden weder ein Status angegeben, noch Angaben im Feld **Letzte Abschlusszeit** gemacht.

Sie können die Tasks sortieren, indem Sie das entsprechende Sortierungskriterium aus dem Listenfeld in der rechten, oberen Ecke wählen. Eine auf- oder absteigende Sortierung der Tasks ist möglich nach **Erstellungszeit**, **Letzte Abschlusszeit**, **Letztes Ergebnis**, **Name**, **Nächste Startzeit**, **Status** und **Task-Typ**.

Auf der Seite zur Verwaltung der **Tasks** stehen Ihnen über die entsprechenden Schaltflächen für jeden Task der Liste die Aktionen **Ausführen**, **Abbrechen**, **Bearbeiten** oder **Löschen** zur Verfügung (*siehe die nachfolgenden Abschnitte*).

Sie können die Detailinformationen für jeden Task der Liste überprüfen, indem Sie die Registerkarten **Zusammenfassung** und **Quelle und Ziel** einsehen (*siehe den Abschnitt* '*Task-Details ansehen* (S. 86)').

15.1 Einen Task ausführen

Sie können den ausgewählten inaktiven Task starten, indem Sie auf die Schaltfläche **Ausführen** klicken. Nach dem Starten wird der Status des Tasks von '**Inaktiv**' auf '**Läuft**' geändert, mit Anzeige des Fortschrittsbalkens sowie der prozentualen Fertigstellung des Tasks.

Beachten Sie, dass Sie nur die Task-Logs anzeigen lassen können (*siehe den Abschnitt* '*Taks-Logs ansehen* (S. 86)') oder den aktiven Task **abbrechen** können (*siehe den Abschnitt* '*Einen Task abbrechen* (S. 86)'). Die anderen Schaltflächen **Ausführen**, **Bearbeiten** und **Löschen** sind deaktiviert. Um einen aktiven Task bearbeiten oder löschen zu können, müssen Sie ihn erst stoppen.

15.2 Einen Task abbrechen

Sie können den ausgewählten aktiven Task unterbrechen, indem Sie auf die Schaltfläche **Abbrechen** klicken. Sie werden aufgefordert, die Aktion zu bestätigen. Ist die Bestätigung erfolgt, wird der aktive Task sofort gestoppt und wechselt in das Stadium 'Inaktiv'.

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

15.3 Einen Task bearbeiten

Sie können den ausgewählten Task ändern, indem Sie auf die Schaltfläche **Bearbeiten** klicken. Je nach Typ des Tasks gelangen Sie in den entsprechenden Bereich der Registerkarte **Aktionen** – Backup, Recovery, Validierung, etc. Hier finden Sie alle Schritte der jeweiligen Assistenten für Backup/Recovery/Validierung etc., die Sie abgeschlossen, während Sie den entsprechenden Task erstellt 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. 33)'*,* '*Backups von virtuellen Maschinen wiederherstellen* (S. 56)'*,* '*Backups validieren* (S. 94)' *etc.*).

15.4 Einen Task löschen

Sie können den ausgewählten Task entfernen, indem Sie auf die Schaltfläche **Löschen** klicken. Sie werden aufgefordert, die Aktion zu bestätigen. Nach erfolgter Bestätigung wird der Task sofort gelöscht.

15.5 Task-Logs ansehen

Sie können die Logs des ausgewählten Task einsehen, indem Sie auf den Status des letzten Ergebnis klicken. Sie gelangen zur Ansicht **Logs** (**Ansicht** –> **Logs anzeigen**), wo Sie alle Logs für den aktuellen Task finden (*siehe Abschnitt 'Logs verwalten'* (S. 98)).

15.6 Task-Details ansehen

Indem Sie einen Task in der Liste auswählen, können Sie sich Detailinformationen zu diesem in den Registerkarten **Zusammenfassung** sowie **Quelle und Ziel** anzeigen lassen. Beachten Sie, dass die Registerkarten je nach Typ des Tasks (Backup, Recovery, Validierung etc.) variierende Informationen enthalten. Die nachfolgenden Abschnitte beschreiben den Inhalt der Registerkarten für einen entsprechenden Backup-Task.

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

Startzeitpunkt: 06/29/2012 12:49
Verbleibende Zeit: 41 Sek.
Letzte Abschlusszeit: N/A
Letztes Ergebnis: Noch nicht ausgeführt
Übertragene Byte: 1,219 GB

Backup: N/A
Geschwindigkeit: 8,053 Mb/s
Planung: Nicht verfügbar

Der rechts liegende Bereich **Optionen** zeigt die Einstellungen des aktuell ausgewählten Tasks. Dieser Bereich zeigt nur solche Optionen an, die von den Standardeinstellungen abweichen. Entsprechen alle Task-Optionen den Standardeinstellungen, dann meldet dieser Bereich lediglich '**Optionen: Standard**', ohne spezifische Werte anzuzeigen. Hier ein Beispiel:

Schutz des Archivs: An
Archivverschlüsselungsalgorithmus: AES 128
Anzahl der Versuche: 10
Abstand zwischen den Versuchen: 1 Minute(n)
Deduplizierung: Aus
CBT-Backup: An
FTP im Modus 'Aktiv' verwenden: An
Nach Backup validieren: An

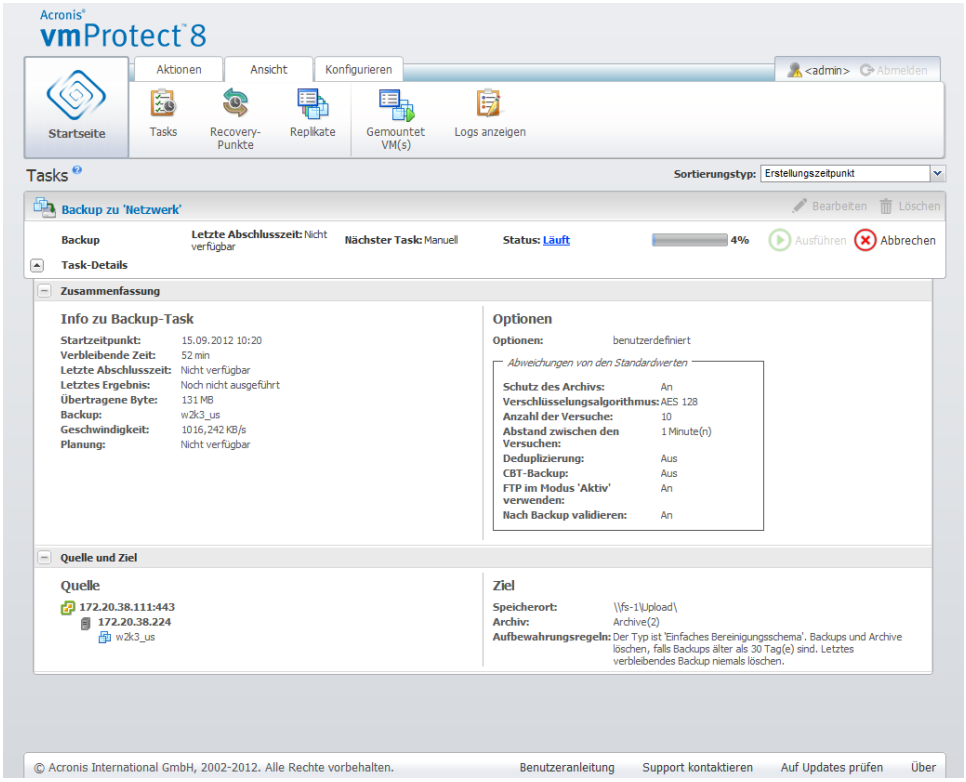
Die Registerkarte **Quelle und Ziel** im Bereich **Quelle** auf der linken Seite präsentiert den Verzeichnisbaum der ESX(i)-Hosts+vApps/VMs, die im Backup-Task enthalten sind. Dieser Verzeichnisbaum wird dynamisch aufgebaut. Ist ein kompletter ESX(i)-Host für das Backup vorgesehen, wird (in derselben Liste) der Baum für den aktuellen Status der Maschinen angezeigt, so wie bei VMware IC. Rechts vom ESX(i)-Host ist gekennzeichnet, dass die gesamte Gruppe gesichert wird (Markierung 'Alle virtuellen Maschinen'). Hier ein Beispiel:

ESX Host 1 'Alle virtuellen Maschinen':
Small_vm

ESX-Host 2:
AcronisESXAppliance (10.250.40.30)

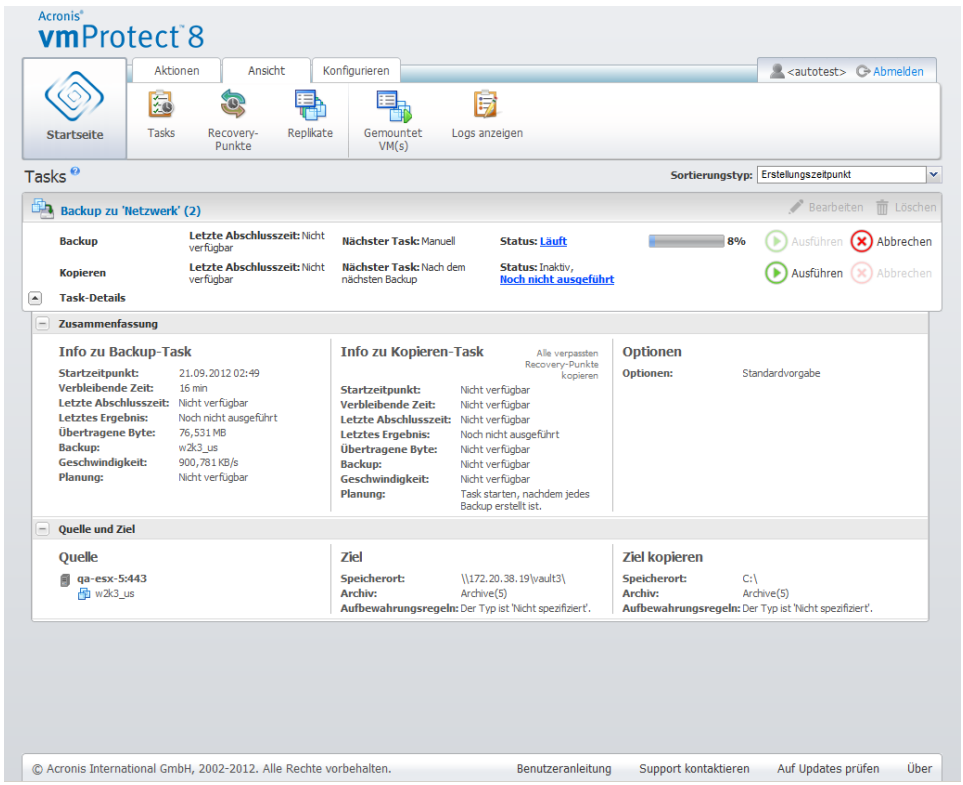
Der rechts liegende Bereich **Ziel** gibt Informationen über den Speicherort des gesicherten Archivs. Hier ein Beispiel:

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



Tasks verwalten, Task-Details ansehen, Registerkarte 'Zusammenfassung', Registerkarte 'Quelle und Ziel'

Falls der Backup-Task mit der Option **Das Backup zu einem zweiten Speicherort kopieren** konfiguriert wurde, dann werden in der Registerkarte 'Zusammenfassung' der Task-Details sowohl die Bereiche **Info zu Backup-Task** wie auch **Info zu Kopieren-Task** angezeigt (wie in der unteren Abbildung zu sehen).



Tasks verwalten, Task-Details ansehen, Info zu Backup- und Kopie-Task

16 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 eine virtuelle Maschine 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:

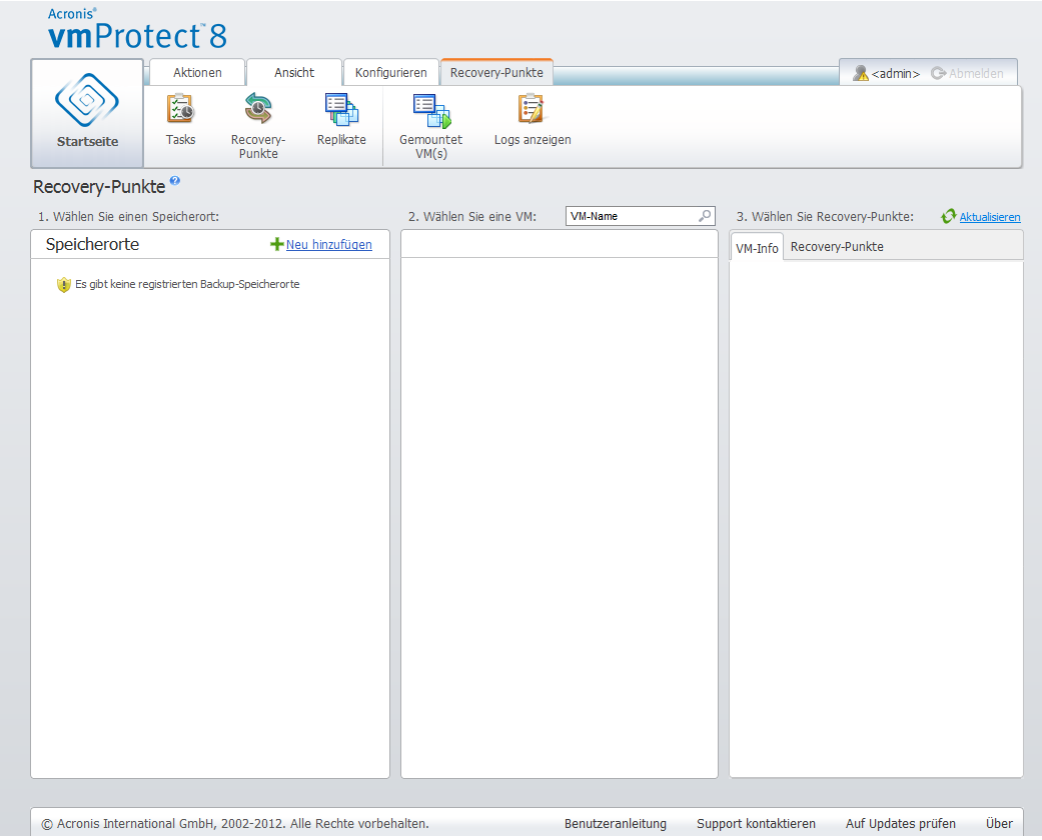
- die Backup-Speicherorte
- den Katalog virtueller Maschinen und
- die Liste der Recovery-Punkte.

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 mit den virtuellen Maschinen, die in den Archiven am gewählten Speicherort vorhanden sind. 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'

16.1 Einen Backup-Speicherort hinzufügen

Sie können Backup-Speicherorte direkt aus der Liste **Speicherorte** entfernen oder ihr hinzufügen. Ein Klick auf den Link **Neu hinzufügen** oben öffnet das Fenster **Speicherort hinzufügen**.

Beachten Sie, dass die Aktion 'Entfernen' Archive nicht physikalisch vom Speicherort entfernt, sondern nur den Speicherort aus der Acronis vmProtect 8-Konfiguration löscht. Alle Backups im Speicherort bleiben intakt und werden wieder sichtbar, wenn Sie diese über den entsprechenden Link erneut **Neu hinzufügen**. Das Entfernen oder Hinzufügen von Speicherorten kann notwendig sein, 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 Verzeichnisbaum oder durch Eingabe seines vollständigen Pfads im Feld **Speicherort** auswählen.

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 das Dialogfenster zur Eingabe der

Anmeldedaten. Nach dem Anmelden zeigt dieser Bereich den Inhalt des ausgewählten Speicherorts an, d.h. die hier vorhandenen Archive.

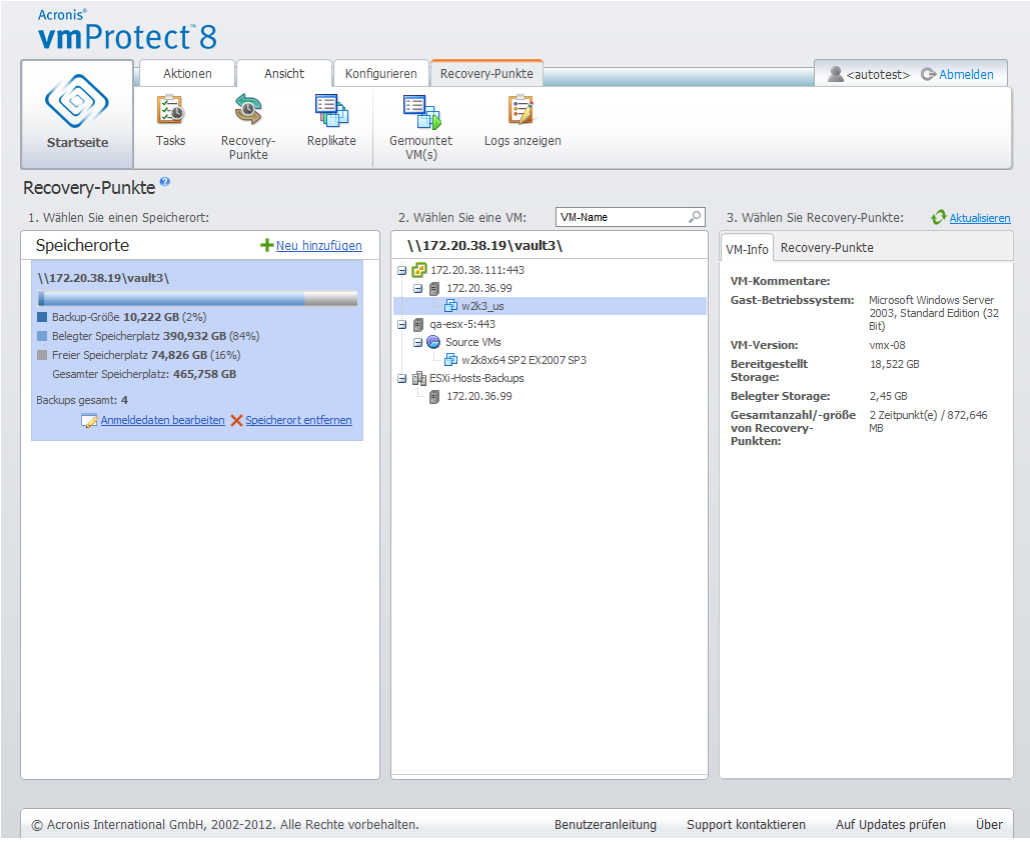
Alternativ zum Durchsuchen des Verzeichnisbaums können Sie den Pfad im entsprechenden Feld **Speicherort** eingeben und diesen Speicherort mit einem Klick auf **Start** durchsuchen. Auch hier erscheint im rechten Bereich dasselbe Dialogfenster, das zur Authentifizierung nach Login und Kennwort fragt.

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.

16.2 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 sich am gewählten Speicherort durch Kennwort geschützte Archive oder Archive physikalischer Maschinen befinden, werden diese in einer separaten Liste unter **Verschlüsselte und physikalische Maschinen-Daten** angezeigt. Um Daten aus diesen Archiven anzuzeigen, müssen Sie im Pop-up-Fenster **Kennwort** das entsprechende Kennwort eingeben.



Recovery-Punkte verwalten

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.

16.3 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 **Recovery-Punkte-Liste** können Sie zu den **Recovery-Punkte-Details** wechseln (siehe Abschnitt Registerkarte 'Zusammenfassung' (S. 92)).

Nach Auswahl eines bestimmten Recovery-Punktes in der Liste, können Sie alle im Abschnitt 'Aktionen mit ausgewählten Elementen' (S. 92) beschriebenen Aktionen durchführen.

16.4 Registerkarte 'Zusammenfassung'

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

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

16.5 Aktionen mit ausgewählten Elementen

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

- **Recovery**
- **Exchange-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. 92) beschrieben).

16.5.1 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. 56) beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

16.5.2 Exchange-Recovery

Klicken Sie im Menüband auf **Exchange-Recovery**, um die Exchange-Daten mit dem Assistenten **Extrahieren von Exchange Server-Elementen** aus dem gewählten Recovery-Punkt zu extrahieren. Im Assistenten sind die im Abschnitt 'Exchange-Server-Backup-Extraktion (S. 64)' beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

16.5.3 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. 70) beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

16.5.4 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. 75) beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

16.5.5 Validieren

Durch einen Klick auf **Validieren** im Menüband führen Sie die Backup-Validierung mit dem neuen Validierungstask durch. Im Validierungsassistenten sind die im Abschnitt 'Backups validieren' (S. 94) beschriebenen Einstellungen des ausgewählten Recovery-Punktes bereits eingetragen.

16.5.6 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.

Beachten Sie, dass in einem Archiv mit Legacy-Modus (S. 9) 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. 10) 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.

17 Andere Aktionen

17.1 Backups validieren

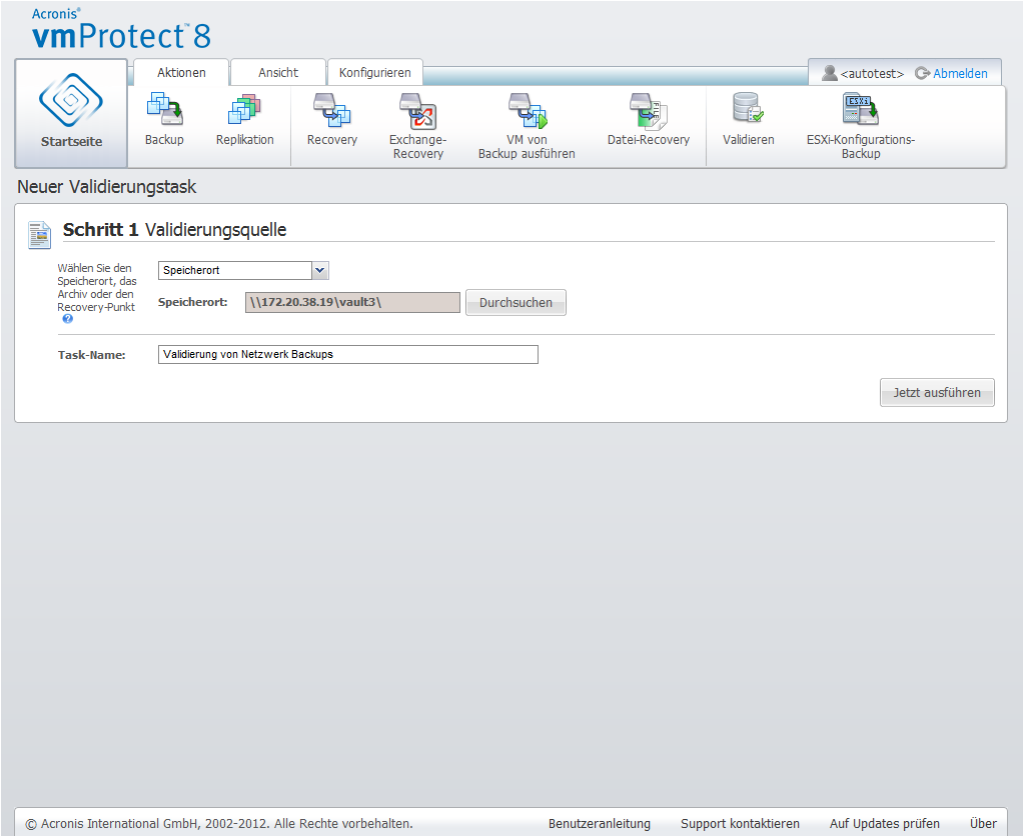
Die Validierung überprüft die Möglichkeit der Datenwiederherstellung aus einem Backup. Beachten Sie, dass eine erfolgreiche Validierung zwar eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, aber nicht alle Faktoren geprüft werden, die eine Wiederherstellung beeinflussen.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

Mit Acronis vmProtect 8 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.

17.1.1 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 granuläre 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'.



Neuer Validierungs-Task Validierungsquelle. Speicherort.

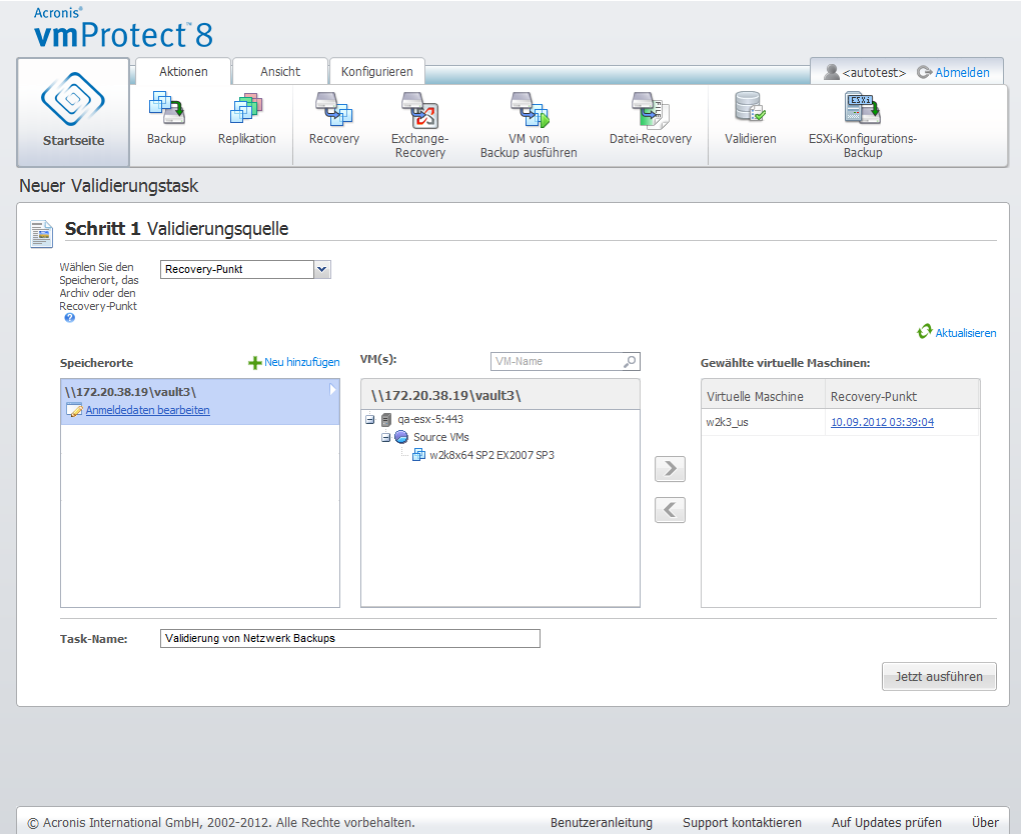
Archiv – Die Validierung eines Archivs überprüft die Integrität aller Backups (Recovery-Punkte) in dem spezifizierten Archiv. Im Allgemeinen ist diese Prozedur schneller als das Validieren des gesamten Speicherorts. Trotzdem ist es langsamer als das Validieren eines spezifischen Recovery-Punktes im Archiv.

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

Bestimmen Sie nach Auswahl des zu validierenden Elementtyps 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).

Sie können einen Verzeichnisbaum mit den virtuellen Maschinen sehen, die in den am gewählten Speicherort gesicherten Archiven enthalten sind – und können dann jede dieser virtuellen Maschinen auswählen, indem Sie sie 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 Assistenten 'Validierungstask erstellen' abzuschließen, müssen Sie einen Namen für den Task vergeben. Beachten Sie, dass die Zeichen [ ] { } ; . im Task-Namen nicht zulässig sind.



Neuer Validierungs-Task Validierungsquelle. Recovery-Punkt.

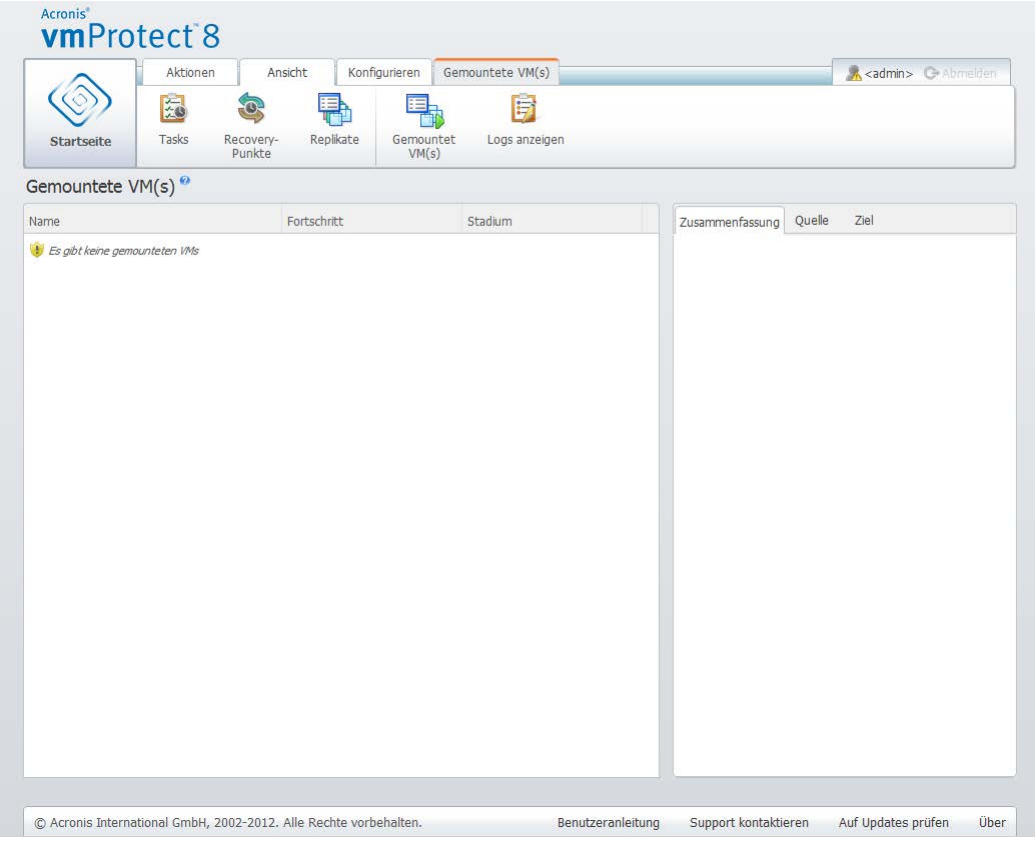
Wenn Sie auf **Jetzt ausführen** klicken, werden die ausgewählten Elemente validiert und der Fortschritt des neu erstellten Validierungstasks in der Ansicht **Tasks** angezeigt. Sein Ergebnis erscheint in den Ansichten **Dashboard** und **Logs anzeigen**.

17.2 Gemountete VMs verwalten

Klicken Sie in der Registerkarte **Ansicht** im Hauptmenüband von Acronis vmProtect 8 auf **Gemountete VMs**, um die Seite **Gemountete VMs** zu öffnen.

17.2.1 Liste 'Gemountete VMs'

Die Ansicht **Gemountete VMs** gibt einen Überblick über die virtuellen Maschinen, die gegenwärtig gemountet sind oder von einem Backup auf einem ESX(i)-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. 70)), 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).

17.2.2 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 Registerkarten wechseln können, um zusätzliche Details zu prüfen.

Nach Auswahl 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 Registerkartenansicht. Es gibt drei Registerkarten – 'Zusammenfassung', 'Quelle' und 'Ziel' ('Zusammenfassung' ist die Standardregisterkarte).

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

Startzeit, -datum: 20:11 11.05.2011

Die Registerkarte **Quelle** zeigt den Baum der gemounteten ESX(i)-Hosts sowie vApps und VMs an. Hier ein Beispiel für den Inhalt der Registerkarte **Quelle**:

Speicherort: \\Backups\
Archiv: Archivname

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

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

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

17.2.3 VMs trennen

Die kontextabhängige Symbolleiste in der Ansicht 'Gemountete VMs' hat zwei Schaltflächen, **Trennen** sowie **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**.

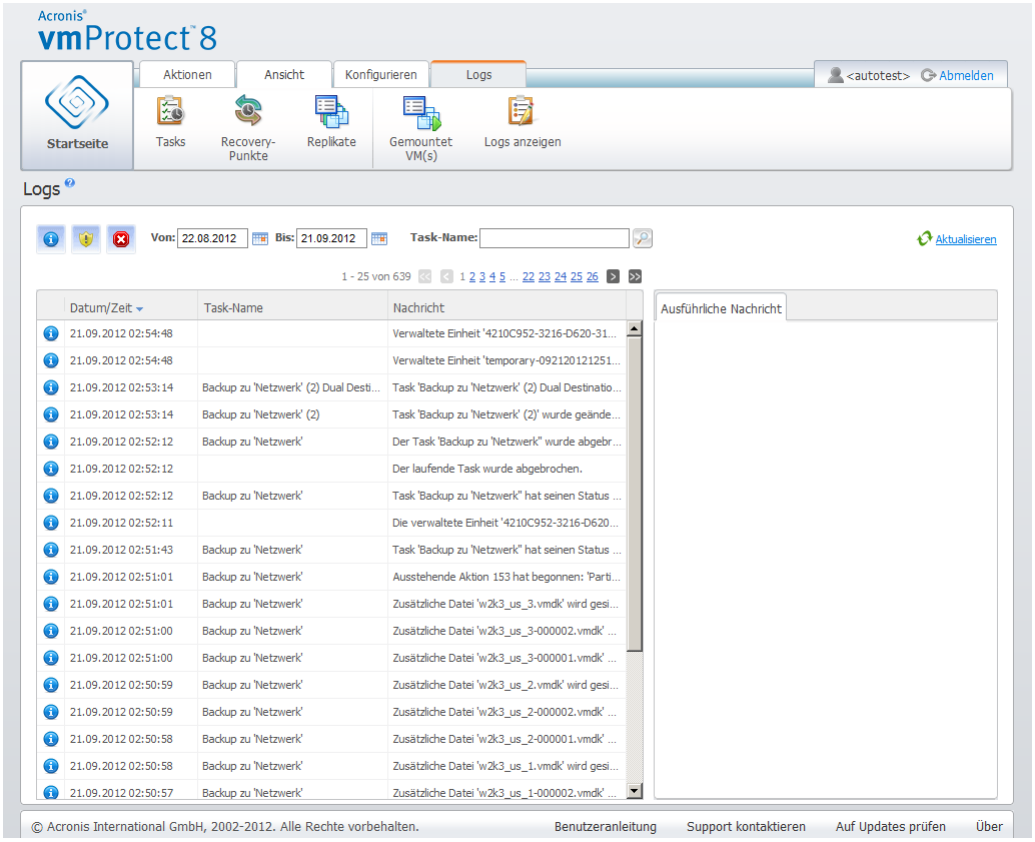
Durch die Aktion **Trennen und Speichern** wird die Maschine nicht mehr vom Backup ausgeführt und alle an der Maschine vorgenommenen Änderungen werden ins Archiv aufgenommen, wodurch ein neuer Recovery-Punkt hinzugefügt wird. Beachten Sie dass der Recovery-Punkt ohne eine 'Exchange-aware'-Option erstellt wird.

17.3 Logs verwalten

Klicken Sie in der Registerkarte **Ansicht** im Hauptmenüband von Acronis vmProtect 8 auf **Logs anzeigen**, um die Seite **Logs** zu öffnen.

17.3.1 Liste der Logs

Die Ansicht **Logs anzeigen** enthält eine Liste aller Ereignisse auf dem Acronis vmProtect 8-Agenten. Dazu gehören Backup und Recovery, Ausführen der VM von einem Backup und andere Tasks sowie Systemmeldungen, beispielsweise das Herstellen einer Verbindung zu verwalteten ESX(i)-Hosts bzw. vCentern.



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.

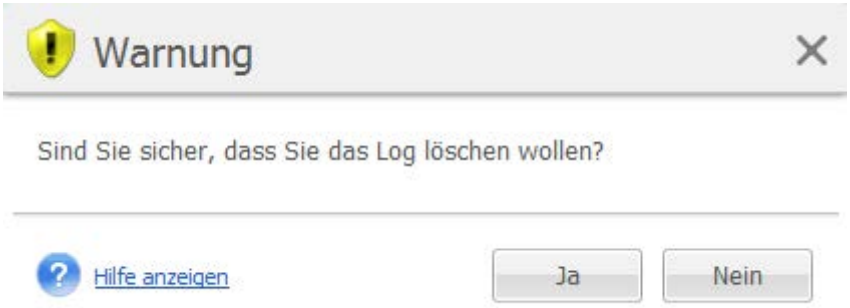
- Ereignis-Flags (Erfolg, Warnung oder Fehler)
- Datum/Zeit
- Task-Name

Das Anklicken eines Log-Ereignisses in der Liste öffnet eine detaillierte Meldung für dieses Log im rechten Fenster. Der Link **Für mehr Informationen** öffnet die Acronis Knowledge Base in einem neuen Browser-Fenster. Dieser Link ist nur für Log-Ereignisse des Typs 'Fehler' verfügbar.

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.

17.3.2 Logs bereinigen

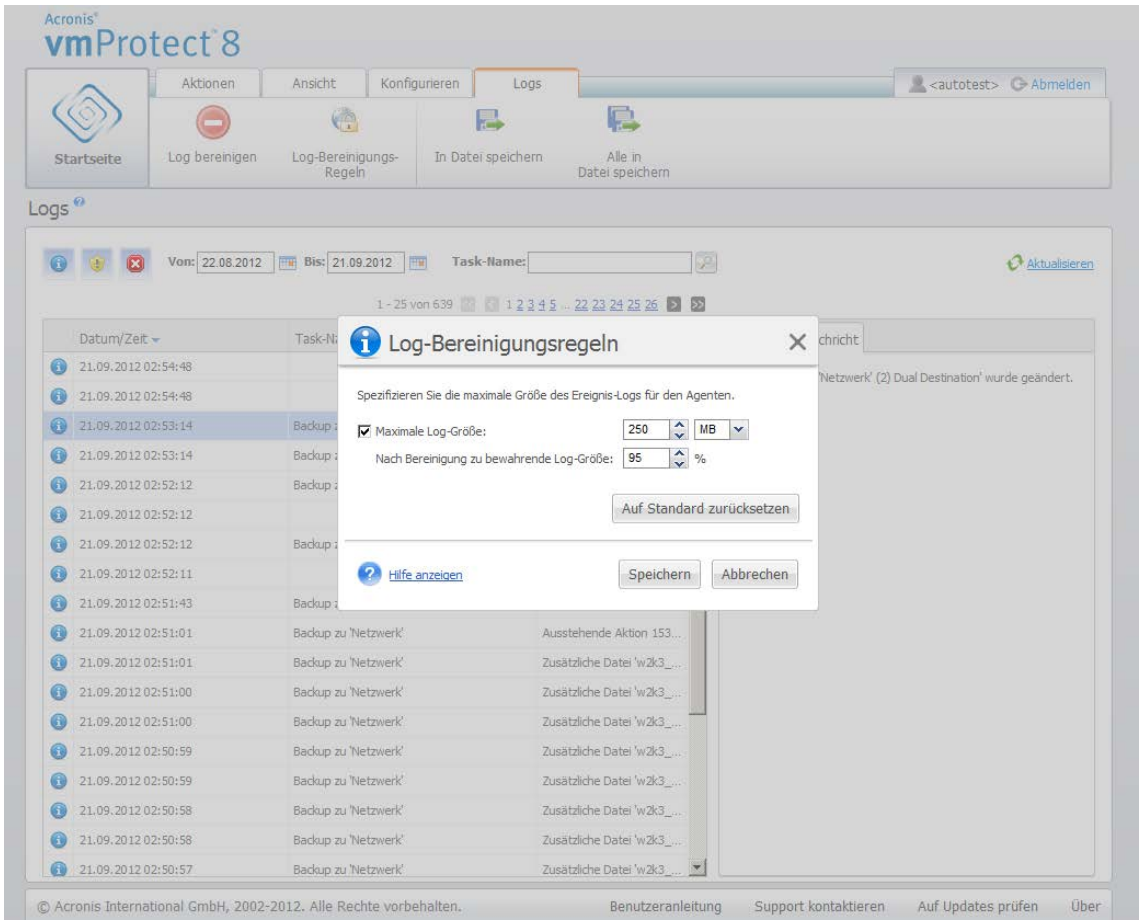
Klicken Sie auf **Logs bereinigen** in der Hauptsymbolleiste, um alle Log-Einträge zu löschen. Diese Aktion löscht alle Einträge im Acronis vmProtect 8-Log. Es erscheint die Warnmeldung 'Sind Sie sicher, dass Sie das Log löschen möchten?', um die Löschaktion zu bestätigen. Nach erfolgter Bestätigung werden alle Log-Einträge gelöscht.



Dialog 'Log bereinigen'.

17.3.3 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 8-Agenten bereinigt wird.



Dialog '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 (beispielsweise unter Windows XP/2003 Server %ALLUSERSPROFILE%\Anwendungsdaten\Acronis\vmProtect\VMMS\LogEvents).

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

Die Standardwerte für die **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.

17.3.4 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.

17.4 Lizenzen verwalten

Klicken Sie auf der Registerkarte **Konfigurieren** im Hauptmenüband von Acronis vmProtect 8 auf **Lizenzen**, um die Seite **Lizenzen** zu öffnen.

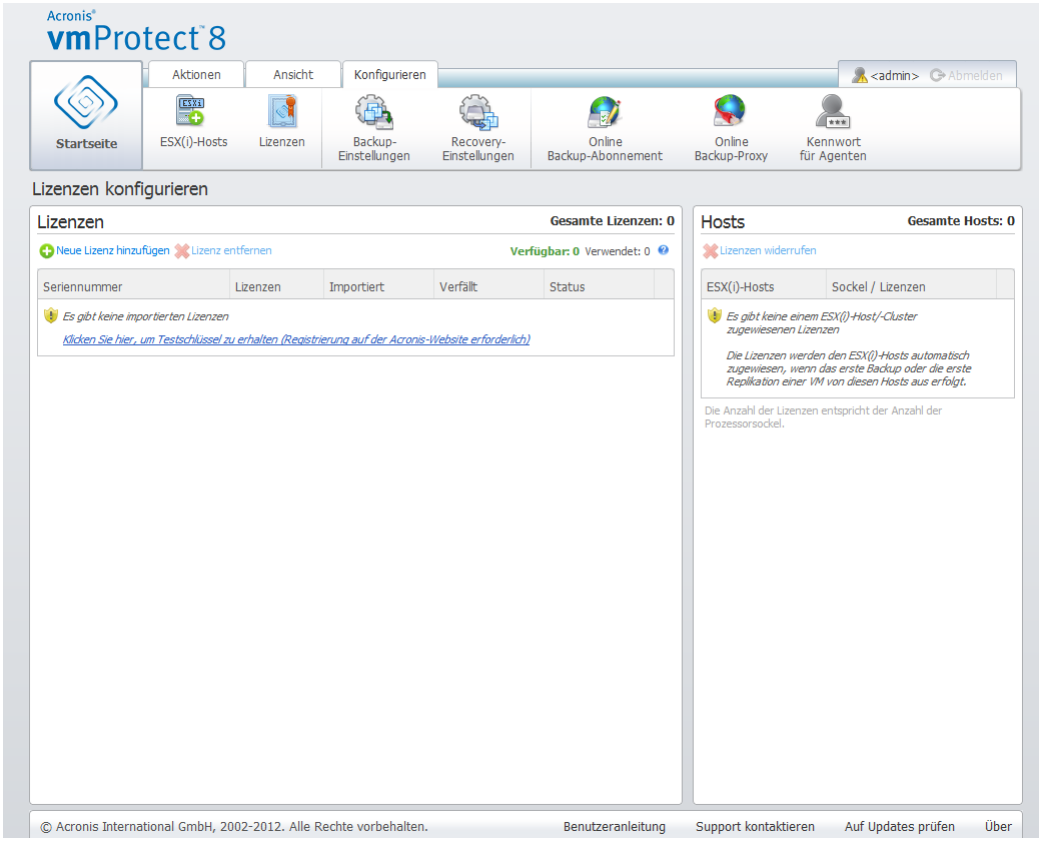
Die Ansicht **Lizenzen** gibt einen Überblick über die in den vmProtect 8 Agenten importierten Lizenzen. Hier können Sie über die entsprechenden Schaltflächen in der Symbolleiste die Lizenz-Seriennummern **hinzufügen** oder die Anbindung der Lizenzen an ESX-Hosts **entfernen**. Das Entfernen der Lizenzbindung gibt diese wieder frei.

Gemäß dem vmProtect 8-Lizenzschema ist für jede CPU auf dem verwalteten ESX(i)-Host bzw. Cluster eine eigene Lizenz erforderlich.

Beim ersten Ausführen von Acronis vmProtect 8 sind an keinen ESX(i)-Host oder Cluster Lizenzen gebunden. Ohne eine Lizenzbindung können Sie VMs nur zum Acronis Online Backup Storage als Backup-Ziel sichern. Eine neue Lizenz kann wie nachfolgend beschrieben hinzugefügt werden.

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.

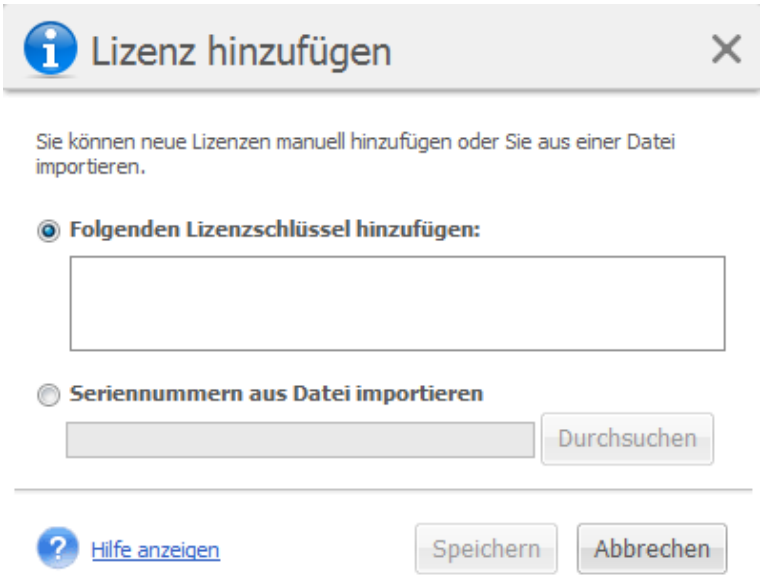
Die linke Seite enthält die Liste der ESX(i)-Hosts bzw. Cluster, an die Lizenzen gebunden sind. Die Anbindung der Lizenzen an ESX(i)-Hosts oder Cluster erfolgt bei der ersten Ausführung eines Backups oder einer Wiederherstellung mit virtuellen Maschinen, die auf diesem Host laufen. Bei einem Cluster 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(i)-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(i)-Host oder Cluster eingesetzt werden.



Seite 'Lizenzen verwalten', Lizenz-Liste

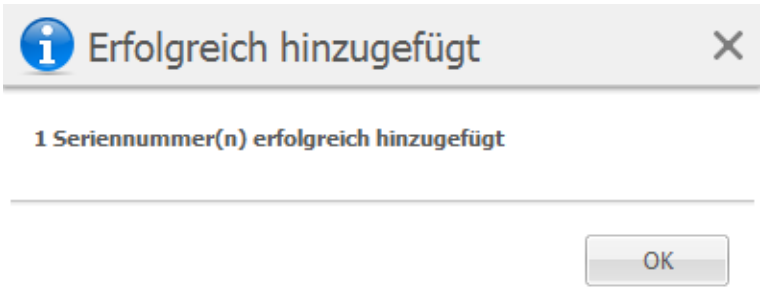
17.4.1 Lizenz hinzufügen

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'.

17.4.2 Fehler beim Hinzufügen von Lizenzen

Das Hinzufügen einer Lizenz kann aus folgenden Gründen fehlschlagen:

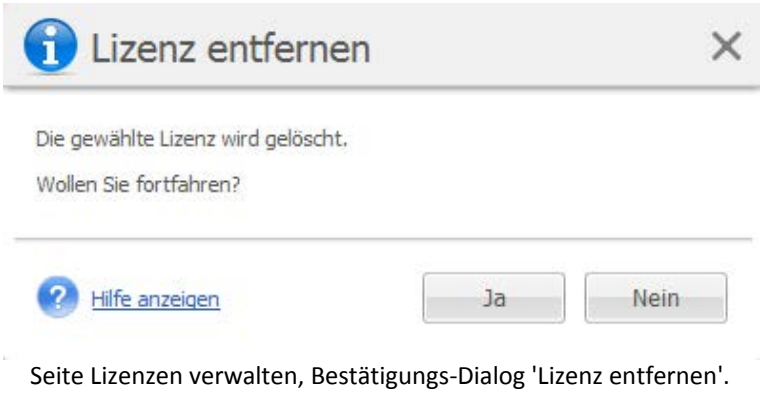
- Die Lizenz wurde bereits importiert
- Die Lizenz ist nicht korrekt.

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. 112).

17.4.3 Lizenz bzw. ESX(i)-Host entfernen

Wählen Sie einen ESX(i)-Host oder ein Cluster in der Liste aus und klicken Sie auf **Entfernen**. Die Lizenzzuweisung wird für den gewählten ESX(i)-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'.

17.4.4 Verfügbare Lizenzen

Es gibt mehrere Lizenztypen, die von Acronis vmProtect 8 verwendet werden können:

- Acronis vmProtect 6/7-Standard-Lizenzen
- Acronis vmProtect 8-Upgrade-Lizenzen
- Acronis vmProtect 8-Standard-Lizenzen
- Acronis vmProtect-Test-Lizenzen

Acronis vmProtect 8 verwendet ein 'pro Sockel'-Lizenzschema, bei dem jeder CPU-Sockel eines ESX(i)-Hosts eine Lizenz von Acronis vmProtect 8 erfordert. Diese Lizenzen werden dem ESX(i)-Host

beim ersten Backup zugewiesen oder bei der ersten Replikation einer VM von diesem ESX(i)-Host. Sollte dieser Host Teil eines VMware Clusters sein, dann werden die Lizenzen auch allen anderen ESX(i)-Hosts zugewiesen, die in diesem Cluster enthalten sind.

Alle Seriennummern mit ihren Details und ihrem jeweiligem Status werden gemäß ihres Lizenztyps aufgelistet.

Acronis vmProtect 8 verwendet entweder Acronis vmProtect 8-Standard-Lizenzen oder Acronis vmProtect 8-Upgrade-Lizenzen. Damit Sie Acronis vmProtect 8-Upgrade-Lizenzen hinzufügen können, muss eine ausreichende Anzahl von Acronis vmProtect 6/7-Standard-Lizenzen bereits registriert sein – anderenfalls schlägt das Hinzufügen der Acronis vmProtect 8-Upgrade-Lizenzen fehl.

Die Anzahl der verfügbaren Lizenzen zeigt an, wie viele Lizenzen (vmProtect 8-Standard-Lizenzen und vmProtect 8-Upgrade-Lizenzen) immer noch verwendet werden können, um sie den ESX(i)-Hosts zuzuweisen. Verwendete Lizenzen sind Lizenzen, die bereits ihren entsprechenden ESX(i)-Hosts zugewiesen wurden. Die Gesamtzahl der Lizenzen ist die Zahl der verwendeten zusammen mit der Zahl der verfügbaren. Die Anzahl der Lizenzen ohne Upgrade entspricht den vmProtect 6/7-Standard-Lizenzen, für die keine vmProtect 8-Upgrade-Lizenzen hinzugefügt wurden.

17.5 ESX(i)-Hosts verwalten

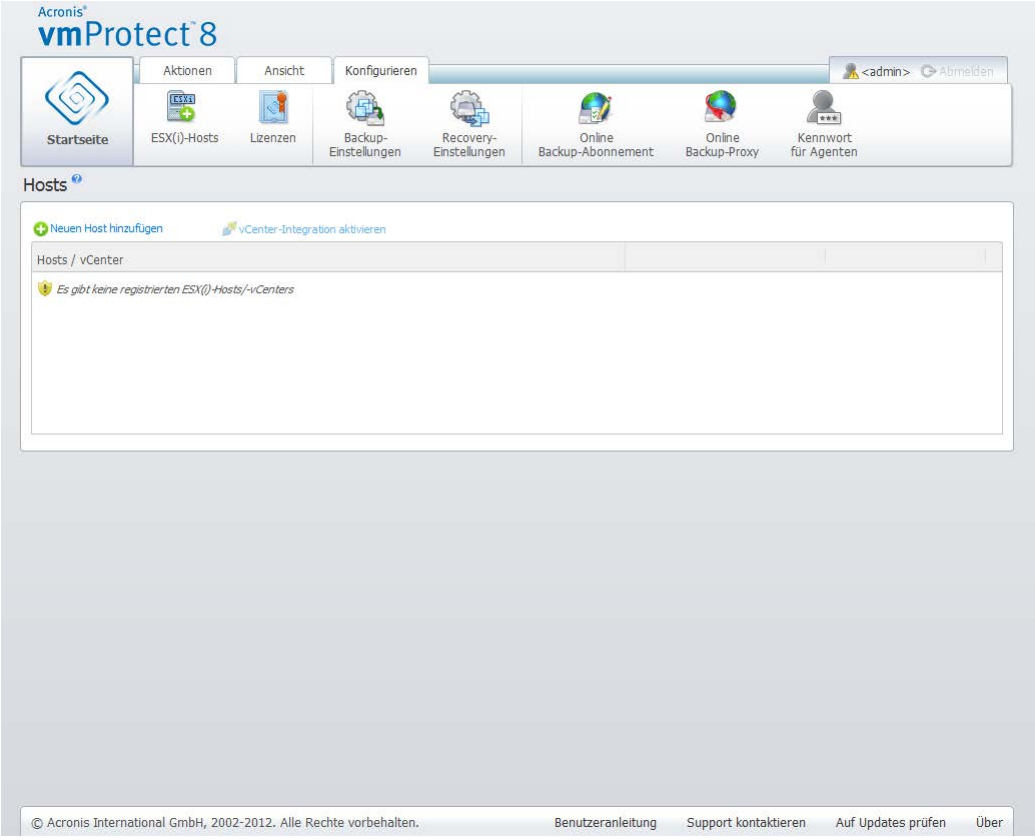
Klicken Sie auf der Registerkarte **Konfigurieren** im Hauptmenüband von Acronis vmProtect 8 auf **ESX(i)-Hosts**, um die Seite **ESX(i)-Hosts** zu öffnen.

17.5.1 Liste der ESX(i)-Hosts

Die Ansicht **Hosts** bietet einen Überblick und eine Schnittstelle zur Verwaltung der ESX(i)-Hosts bzw. des vCenters, die in den Einstellungen des vmProtect 8 Agenten registriert sind. Über die Schaltflächen im Menüband können Sie andere ESX(i)-Hosts zu der Liste hinzufügen oder aus der Liste entfernen.

Beim ersten Ausführen von Acronis vmProtect 8 gibt es keine registrierten ESX(i)-Hosts oder Cluster. Auf dieser Seite können Sie, wie unten beschrieben, neue ESX(i)-Hosts hinzufügen.

Nach Hinzufügen erscheint der ESX(i)-Host bzw. das vCenter in der Liste der Hosts.



Seite 'ESX(i)-Hosts konfigurieren', Liste der Hosts.

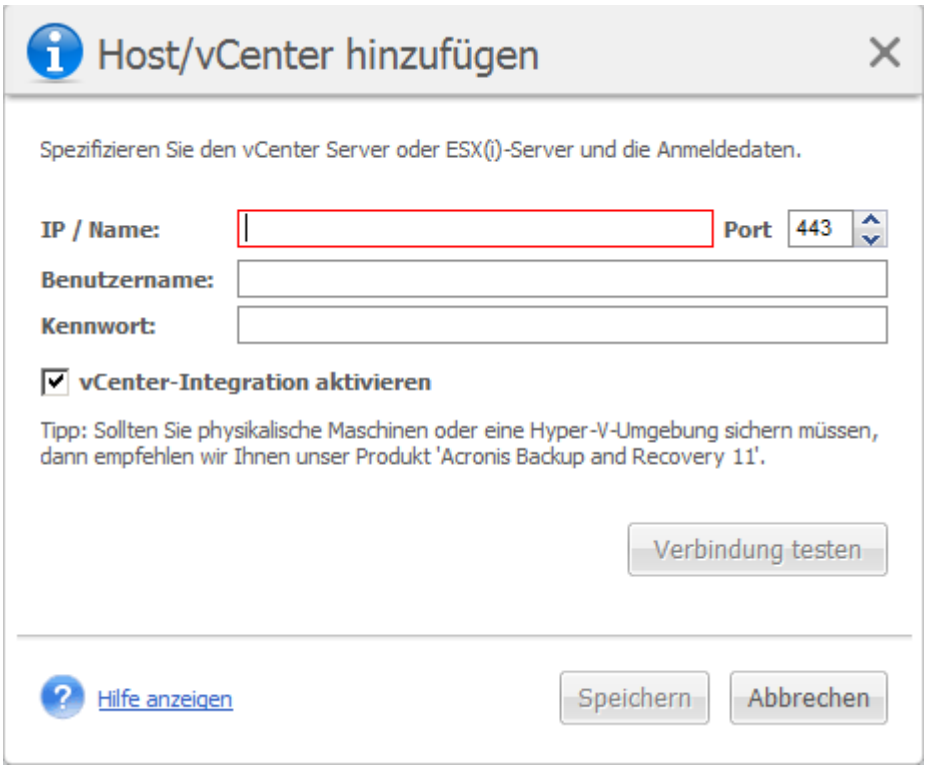
Das Hinzufügen eines ESX(i)-Hosts oder vCenters beinhaltet nicht automatisch die Anbindung der Lizenzen. Diese erfolgt erst, wenn Sie mit einer der auf diesem Host laufenden virtuellen Maschinen einen Backup- oder Recovery-Task ausführen. Nach Hinzufügen eines ESX(i)-Hosts oder vCenters können Sie mit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

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

Für eine erfolgreiche Verwaltung eines ESX(i)-Hosts oder vCenters ist die Eingabe von Anmeldedaten erforderlich. Die Anmeldedaten können Sie hier eingeben; sie bleiben solange erhalten, bis Sie den ESX(i)-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(i)-Host bzw. das vCenter in der Liste aus und klicken Sie auf der rechten Seite auf **Anmeldedaten bearbeiten**.

17.5.2 ESX(i)-Host hinzufügen

Um einen ESX(i)-Host bzw. ein vCenter hinzuzufügen, müssen Sie die IP-Adresse oder den Hostnamen sowie die Anmeldedaten angeben, um auf den gewünschten ESX(i)-Host oder das vCenter zuzugreifen. Sie können außerdem den benutzerdefinierten Port spezifizieren. 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(i)-Host oder das vCenter hinzuzufügen.



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

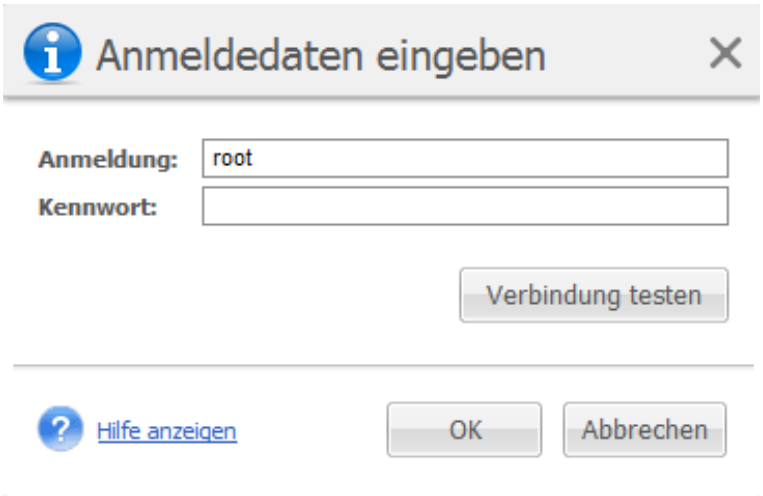
17.5.3 ESX(i)-Host hinzufügen, der Teil eines vCenters ist

Wenn Sie kein vCenter sondern einen ESX(i)-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(i)-Host vorgenommenen Änderungen zu verfolgen. Das kann unvorhersehbare Auswirkungen haben. Wenn Sie zum Beispiel eine VM von einem Backup ausführen, werden beim Trennen die temporären Dateien nicht vom ESX(i)-Host gelöscht, weil das vCenter sie sperrt. Darum wird dringend empfohlen, statt einzelner ESX(i)-Hosts das vCenter hinzuzufügen.

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

17.5.4 Anmeldedaten

Falls zum Beispiel Ihr Unternehmen aus Sicherheitsgründen wechselnde Kennwörter verlangt, macht dies das Ändern der Anmeldedaten erforderlich. Wählen Sie den ESX(i)-Host bzw. das vCenter in der Liste aus, klicken Sie auf **Anmeldedaten bearbeiten** und geben Sie Login und Kennwort für die Verbindung zum ESX(i)-Host bzw. vCenter ein. Wenn Sie Acronis vmProtect in einer Domain-Umgebung ausführen, muss der Benutzername im Format Domain\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(i)-Host oder das vCenter hinzuzufügen.



Seite ESX(i)-Hosts verwalten, Dialog 'Anmeldedaten eingeben'

17.5.5 ESX(i)-Host entfernen

Das Entfernen eines ESX(i)-Hosts aus der Acronis vmProtect 8-Konfiguration kann erforderlich werden, wenn keine weiteren Backup- bzw. Recovery-Aktionen über die auf diesem ESX(i)-Host laufenden virtuellen Maschinen durchgeführt werden sollen. Die diesem Host zugewiesenen Lizenzen werden nicht automatisch entfernt. Um die Lizenzbindung aufzuheben, gehen Sie zur Seite Konfigurieren –> Lizenzen (S. 101).

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

„Sie sind dabei, einen ESX(i)-Host bzw. ein vCenter zu entfernen, obwohl mit den auf diesem Host laufenden virtuellen Maschinen Backup- oder Recovery-Tasks verbunden sind. Diese Tasks funktionieren möglicherweise nicht mehr richtig. Wollen Sie fortfahren?“

Mit der Auswahl **Ja** verschwinden alle Acronis vmProtect 8-Tasks, die auf die virtuellen Maschinen angewendet werden, die auf diesem ESX(i)-Host bzw. vCenter laufen. Falls der Task virtuelle Maschinen von anderen ESX(i)-Hosts einschließt, wird er automatisch modifiziert, um die unnötigen virtuellen Maschinen aus der Task-Konfiguration zu entfernen. Es verbleiben also nur die virtuellen Maschinen, die von den weiterhin registrierten ESX(i)-Hosts verwaltet werden.

Seite ESX(i)-Hosts verwalten, Dialog 'Host entfernen'

17.6 Einstellungen verwalten

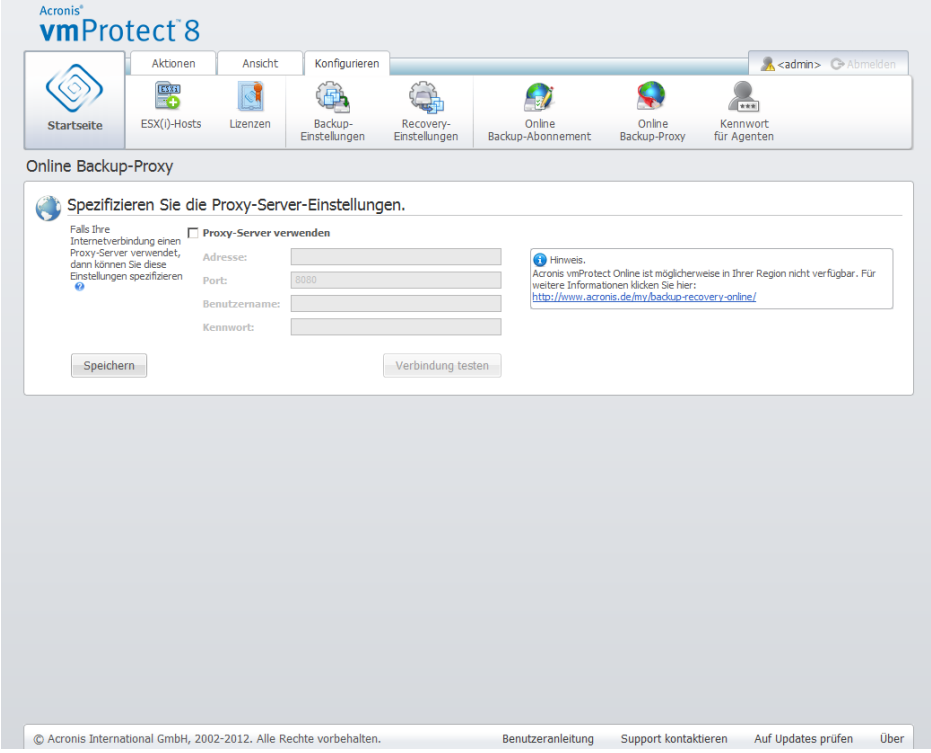
17.6.1 Online Backup-Proxy verwalten

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 der Acronis vmProtect Online Backup Storage nur HTTP- und HTTPS-Proxy-Server unterstützt.



Einstellungen konfigurieren, 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 Internetdienstanbieter um Unterstützung.

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

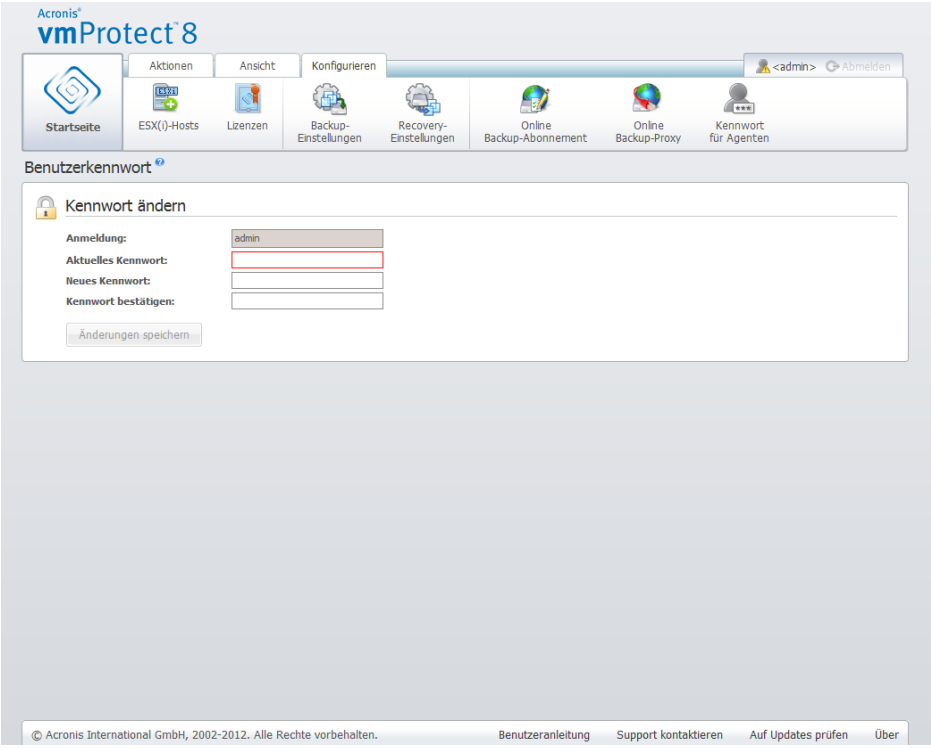
- Microsoft Internet Explorer: Klicken Sie im Menü **Extras** auf den Befehl **Internetoptionen**. Klicken Sie in der Registerkarte **Verbindungen** auf den Befehl **LAN-Einstellungen**.
- Mozilla Firefox: Klicken Sie im Menü **Extras** (zu erreichen über die **Firefox**-Schaltfläche oder über die Alt-Taste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

17.6.2 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. 17) installiert ist. Für die Verbindung mit dem Windows Agent (S. 18) 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

18 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. ESX(i)-Host hinzufügen

Um Backups zu erstellen und andere Aktionen auszuführen, müssen Sie zunächst die IP-Adresse bzw. den Host-Namen und die Anmeldedaten für das vCenter oder den einzelnen ESX(i)-Host angeben, auf dem die virtuellen Maschinen laufen. Klicken Sie im Bereich **Schnellstart** des **Dashboards** auf **ESX(i)-Hosts konfigurieren** oder gehen Sie zur Ansicht **ESX(i)-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(i)-Hosts verwalten' (S. 104).

2. Lizenzen hinzufügen

Durch Einrichten eines ESX(i)-Hosts werden Lizenzen noch nicht 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. 101).

Sie können anschließend mit dem Backup der virtuellen Infrastruktur beginnen.

18.1 Backups von virtuellen Maschinen auf einer Netzwerkfreigabe erstellen

Betrachten wir zunächst, wie Sie ein Backup von mehreren virtuellen Maschinen (beispielsweise fünf) erstellen und diese zu einer Netzwerkfreigabe sichern.

Nachdem Sie die **ESX(i)-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 Bereich **Schnellstart** des Dashboards auf **Backup-Task erstellen** – oder klicken Sie in der Registerkarte **Startseite** (des Hauptmenüs) 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. 33).

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 von Ihnen gewünschte Aktion aus. Sie können den Fortschritt des Tasks sowohl in der Ansicht **Dashboard** wie auch der Ansicht **Tasks** (**Ansicht** –> **Tasks**) der Benutzeroberfläche von Acronis vmProtect 8 verfolgen.

18.2 Wiederherstellen eines Virtuelle-Maschinen-Backups an einem neuen Speicherort

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

Dazu müssen Sie den Assistenten **Backup-Task wiederherstellen** ausführen, der Sie durch alle Schritte der Wiederherstellung führt. Klicken Sie in der Registerkarte **Startseite** im Hauptmenü auf **Recovery**. Führen Sie dann alle Schritte des Assistenten aus. Weitere Informationen finden Sie im Abschnitt 'Backups von virtuellen Maschinen wiederherstellen' (S. 56).

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 die Wiederherstellung und beenden Sie dann den Assistenten. Klicken Sie auf **Jetzt ausführen** um die Maschine sofort wiederherzustellen oder speichern Sie den Task, um die Wiederherstellung später auszuführen.

18.3 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 Assistenten zur **Datei-Recovery** aus, indem Sie in der Registerkarte **Startseite** im Hauptmenü auf **Datei-Recovery** klicken. Im ersten Schritt des Assistenten zur Datei-Recovery 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 zur **Datei-Recovery** finden Sie im Abschnitt 'Datei-Recovery' (S. 75).

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 Registerkarte **Ansicht** und klicken Sie auf **Recovery-Punkte**. Wählen Sie das Stadium 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**.

19 Support

19.1 Technischer Support

Maintenance- und Support-Programm

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

19.2 Fehlerbehebung (Troubleshooting)

Wenn Sie bei der Verwendung von Acronis vmProtect 8 Probleme haben oder Sie sich an den Technischen Support von Acronis wenden, schicken Sie uns die gespeicherten Logs der durchgeführten Aktionen. Gehen Sie zur Seite **Logs** (S. 98) und klicken Sie auf **Alle in Datei speichern** (S. 101).

Weitere Informationen darüber, wie Sie den Acronis Support erreichen, finden Sie unter http://www.acronis.com/support/.

20 Glossar

A

Agent (Acronis vmProtect 8 Agent)

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

Acronis vmProtect 8 enthält den Agenten für das Backup virtueller Maschinen, die sich auf einem VMware ESX(i) Virtualisierungs-Server befinden, mit dem der Agent verbunden ist. Jeder Agent kann mehrere ESX(i)-Hosts oder ein vCenter verwalten. Die optimale Vorgehensweise ist, statt spezifischer ESX(i)-Hosts, die vom vCenter verwaltet werden, das vCenter selbst auf dem Agenten zu registrieren. Sonst wird vMotion (S. 122) 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(i)-Host.

Archiv

Siehe Backup-Archiv (S. 114).

Archiv-Format 'Nur inkrementell'

Ein Archiv (S. 113)-Format der neuen Generation, das mehrere Backups (S. 113) von verschiedenen virtuellen Maschinen enthalten kann. Alle Backups in diesem Archiv werden im inkrementellen Modus (S. 118) 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. 114) in Form eines einzelnen Recovery-Punktes (S. 119) in einem Archiv. (S. 114) 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 8 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. 113), die von einem Backup-Task (S. 114) erstellt und verwaltet werden. Ein Legacy-Modus-Archiv kann mehrere Voll-Backups (S. 122) enthalten, aber auch inkrementelle (S. 118) und differentielle Backups (S. 116). Ein Archiv im Nur inkrementell (S. 113)-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. 120), Sichten des Inhalts, Mounten und Löschen von Backups) sollten nur mit Acronis vmProtect 8 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. 114) wie zum Beispiel der Schutz des Archivs, der Ausschluss von Quelldateien oder der Komprimierungsgrad. Backup-Optionen sind Bestandteil eines Backup-Tasks (S. 114).

Backup-Schema

Teil eines Backup-Tasks (S. 114), der die Backup-Planung sowie [optional] Aufbewahrungsregeln und eine Planung zur Bereinigung (S. 115) enthält. Beispielsweise: Führe ein Voll-Backup (S. 122) monatlich am letzten Tag des Monats um 10 Uhr und ein inkrementelles Backup (S. 118) an Sonntagen um 22 Uhr aus (für Archive (S. 113) 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. 113)-Modus durchgeführt, ist es nicht erforderlich, den Typ (vollständig oder inkrementell) zu definieren.

Acronis vmProtect 8 ermöglicht den Einsatz bekannter optimierter Backup-Schemata wie zum Beispiel GVS (S. 117), 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. 113) 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. 113) anhand spezifizierter Parameter konfiguriert ist (Backup-Optionen (S. 114)).

Bereinigung

Löschen von Backups (S. 113) aus einem Backup-Archiv (S. 114), 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. 114) 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. 35).

Bootable Agent

Ein bootfähiges Notfallwerkzeug, das die Backup-Funktionalität des Acronis vmProtect 8-Agenten (S. 113) enthält. Es ist typisch für die P2V (S. 119)-Migration. Der bootfähige Agent basiert auf einem Linux-Kernel. Eine Maschine kann mit Hilfe eines bootfähigen Mediums (S. 115) 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. 115) enthält.

Acronis vmProtect 8 verwendet bootfähige Medien für das Sichern einer physikalischen Maschine, um dann eine P2V (S. 119)-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 8 kann Deduplizierung auf alle Backup-Archive (S. 114) im Format Legacy-Modus (S. 119) oder 'Nur-inkrementell' (S. 113) anwenden. Das reduziert den für Archive benötigten Speicherplatz, den Backup-Datentransfer sowie die Netzwerkauslastung während der Backup-Erstellung.

Deduplizierung von Acronis vmProtect 8 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. 122). 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. 113) und Agent (S. 118) auf dem Agenten (S. 113) ausgeführt wird.

Distributed Resource Scheduler (DRS)

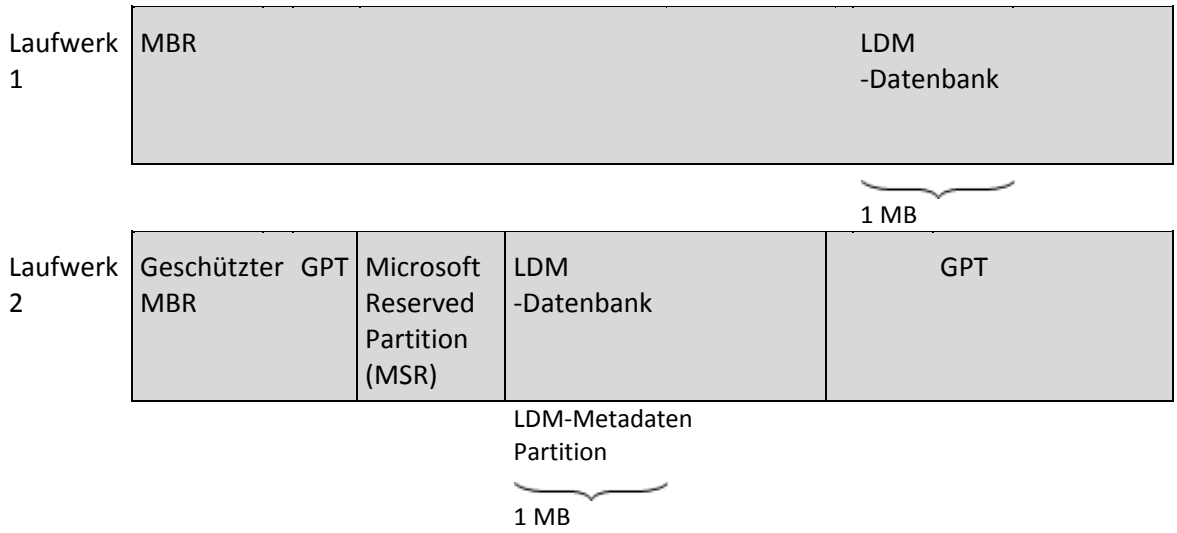
Eine spezifische Funktion des VMware vCenter, die mit Hilfe von vMotion (S. 122) eine automatische Lastverteilung bei einem ESX-Cluster vornimmt.

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/de-de/library/bb457110.aspx

816307 Empfohlene Verfahrensweisen für die Verwendung dynamischer Datenträger auf Windows Server 2003-Computern http://support.microsoft.com/kb/816307/de

Dynamisches Volume

Volume, das sich auf einem dynamischen Laufwerk (S. 116) oder genauer auf einer Laufwerksgruppe (S. 118) 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 8 die logischen dynamischen Volumes anstelle der gesamten dynamischen Laufwerks-Struktur.

G

GVS (Großvater-Vater-Sohn)

Ein gängiges Backup-Schema (S. 114), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 114) und der Anzahl an Recovery-Punkten (S. 119) 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. 113), welches Datenänderungen in Bezug zum letzten Backup speichert. Sie müssen auf andere Backups des gleichen Archivs (S. 113) zugreifen können, um Daten aus einem inkrementellen Backup wiederherstellen zu können.

K

Konsole (Acronis vmProtect 8 Management Console)

Die Konsole ist eine vom Acronis vmProtect 8-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 Acronis vmProtect 8-Agenten (S. 113) ist und 9876 der Port. Wenn der Administrator eine direkte Internetverbindung zwischen Konsole und Agent herstellt, arbeitet er mit direkter Verwaltung (S. 116).

L

Laufwerksgruppe

Anzahl dynamischer Laufwerke (S. 116), 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. 114).

M

Maschine (virtuelle Maschine)

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

Media Builder

Spezielles Werkzeug zur Erstellung bootfähiger Medien (S. 115).

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. 115) erstellen;
- Wiederherstellung des Backups zu einer virtuellen Umgebung (ESX(i)-Server).

R

Recovery-Punkt

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

Registrierte Maschine

Eine vom Acronis vmProtect 8 Agenten verwaltete virtuelle Maschine. Alle virtuellen Maschinen, die sich auf einem registrierten ESX(i)-Host oder vCenter befinden, werden automatisch registriert und können vom Acronis vmProtect 8 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 8 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 8 verwendet die Universal Restore Technology vor allem für Szenarien bei P2V (S. 119)-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. 113) 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. 114). Richtlinien definieren, wann und wie oft eine Validierung durchzuführen ist und ob das gesamte Archiv (S. 113) 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 8 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) dient der zentralen Verwaltung von VMware vSphere-Umgebungen und bietet IT-Administratoren damit deutlich leistungsfähigere Funktionen zur Steuerung von virtuellen Umgebungen (verglichen mit anderen Verwaltungsplattformen).

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

Bei Acronis vmProtect 8 wird das vCenter als Container für die virtuelle ESX-Infrastruktur angesehen, inklusive Datacenter, ESX-Hosts usw.

Verschlüsseltes Archiv

Ein Backup-Archiv (S. 114), das nach dem Advanced Encryption Standard (AES) verschlüsselt ist. Ist die Verschlüsselungsoption und ein Kennwort für das Archiv in den Backup-Optionen (S. 114) definiert, dann wird jedes zum Archiv gehörende Backup vom Agenten (S. 113) 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. 113), das alle für ein Backup ausgewählten Daten enthält. Um die Daten aus einem Voll-Backup wiederherzustellen, benötigen Sie kein weiteres Backup.