BACKUP SWISS

Ihr Cloudpartner aus der Schweiz

Handbuch in der Version 7.9

Revision: 25/04/2019

Inhaltsverzeichnis

1 Über den Backup Service

Mit diesem Service können Sie physische und virtuelle Maschinen, Dateien und Datenbanken sichern und wiederherstellen – und dabei sowohl lokale Storages wie auch einen Cloud Storage verwenden.

Der Zugriff auf den Service erfolgt über eine Weboberfläche, die als Backup-Konsole (manchmal auch „Backup Console“, nach dem englischen Namen der Produkt-Komponente) bezeichnet wird.

2 Software-Anforderungen

2.1 Unterstützte Webbrowser

Die Weboberfläche unterstützt folgende Webbrowser:

- Google Chrome 29 (oder später)
- Mozilla Firefox 23 (oder höher)
- Opera 16 (oder höher)
- Windows Internet Explorer 10 (oder höher)
- Microsoft Edge 25 (oder höher)
- Safari 8 (oder höher), unter den Betriebssystemen macOS oder iOS ausgeführt

In anderen Webbrowsern (inkl. Safari-Browser, die unter anderen Betriebssystem laufen) wird möglicherweise die Benutzeroberfläche nicht korrekt angezeigt oder stehen einige Funktionen nicht zur Verfügung.

2.2 Unterstützte Betriebssysteme und Umgebungen

Agent für Windows

Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
Windows Server 2003 SP1/2003 R2 und höher – Standard und Enterprise Editionen (x86, x64)
Windows Small Business Server 2003/2003 R2
Windows Vista – alle Editionen
Windows Server 2008 – Standard, Enterprise, Datacenter und Web Editionen (x86, x64)
Windows Small Business Server 2008
Windows 7 – alle Editionen
Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation und Web Editionen
Windows MultiPoint Server 2010/2011/2012
Windows Small Business Server 2011 – alle Editionen
Windows 8/8.1 – alle Editionen (x86, x64), ausgenommen Windows RT-Editionen
Windows Server 2012/2012 R2 – alle Editionen
Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
Windows 10 – Home, Pro, Education, Enterprise und IoT Enterprise Editionen
Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers
Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers

Agent für SQL, Agent für Exchange und Agent für Active Directory

Jeder dieser Agenten kann auf einer Maschine installiert werden, die unter einem der oben aufgeführten Betriebssysteme läuft und eine unterstützte Version der entsprechenden Applikation ausführt.

Agent für Office 365

Windows Server 2008 – Standard, Enterprise, Datacenter und Web Editionen (nur x64)

Windows Small Business Server 2008

Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation und Web Editionen

Windows Small Business Server 2011 – alle Editionen

Windows 8/8.1 – alle Editionen (nur x64), ausgenommen Windows RT-Editionen

Windows Server 2012/2012 R2 – alle Editionen

Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (nur x64)

Windows 10 – Home, Pro, Education und Enterprise Editionen (nur x64)

Windows Server 2016 – alle Installationsoptionen (nur x64), mit Ausname des Nano Servers

Agent für Linux

Linux mit Kernel 2.6.9 bis 4.19.8 und glibc 2.3.4 (oder höher)

Zahlreiche x86- und x86_64-Linux-Distributionen, einschließlich:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29
- SUSE Linux Enterprise Server 10 und 11
- SUSE Linux Enterprise Server 12 – wird mit allen Dateisystemen außer Btrfs unterstützt
- Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 – sowohl Unbreakable Enterprise Kernel als auch Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5
- ClearOS 5.x, 6.x, 7, 7.1, 7.4
- ALT Linux 7.0

Bevor Sie das Produkt auf einem System installieren, das keinen RPM-Paketmanager verwendet (wie etwa ein Ubuntu-System), müssen Sie diesen Manager manuell installieren – beispielsweise durch Ausführung folgenden Befehls (als Benutzer 'root'): **`apt-get install rpm`**

Agent für Mac

OS X Mavericks 10.9

OS X Yosemite 10.10

OS X El Capitan 10.11

macOS Sierra 10.12

macOS High Sierra 10.13

macOS Mojave 10.14

Agent für VMware (Virtuelle Appliance)

Dieser Agent wird als eine virtuelle Appliance ausgeliefert, die auf einem ESXi-Host ausgeführt werden kann.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7

Agent für VMware (Windows)

Dieser Agent wird in Form einer Windows-Applikation ausgeliefert und kann unter jedem Betriebssystem ausgeführt werden, welches weiter oben für den Agenten für Windows aufgelistet wurde – mit folgenden Ausnahmen:

- 32-Bit-Betriebssysteme werden nicht unterstützt.
- Windows XP, Windows Server 2003/2003 R2 und Windows Small Business Server 2003/2003 R2 werden nicht unterstützt.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7

Agent für Hyper-V

Windows Server 2008 (nur x64) mit Hyper-V

Windows Server 2008 R2 mit Hyper-V

Microsoft Hyper-V Server 2008/2008 R2

Windows Server 2012/2012 R2 mit Hyper-V

Microsoft Hyper-V Server 2012/2012 R2

Windows 8, 8.1 (nur x64) mit Hyper-V

Windows 10 – Pro, Education und Enterprise Editionen mit Hyper-V

Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers

Microsoft Hyper-V Server 2016

Agent für Virtuozzo

Virtuozzo 6.0.10, 6.0.11, 6.0.12

2.3 Unterstützte Microsoft SQL Server-Versionen

- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

2.4 Unterstützte Microsoft Exchange Server-Versionen

- **Microsoft Exchange Server 2016** – alle Editionen.
- **Microsoft Exchange Server 2013** – alle Editionen, Kumulatives Update 1 und später.
- **Microsoft Exchange Server 2010** – alle Editionen, alle Service Packs. Die Wiederherstellung von Postfächern und Postfach-Elementen wird ab Service Pack 1 (SP1) unterstützt.
- **Microsoft Exchange Server 2007** – alle Editionen, alle Service Packs. Die Wiederherstellung von Postfächern und Postfachelementen wird nicht unterstützt.

2.5 Unterstützte Microsoft SharePoint-Versionen

Backup Service unterstützt folgende Microsoft SharePoint-Versionen:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*Um den SharePoint Explorer mit diesen Versionen verwenden zu können, benötigen Sie eine SharePoint-Wiederherstellungsfarm, an welche Sie die Datenbanken anfügen können.

Die Datenbanken, aus denen Sie Daten extrahieren, müssen von derselben SharePoint-Version stammen wie diejenige, wo der SharePoint Explorer installiert ist.

2.6 Unterstützte Virtualisierungsplattformen

Die nachfolgende Tabelle fasst zusammen, wie die verschiedenen Virtualisierungsplattformen unterstützt werden.

Plattform	Backup auf Hypervisor-Ebene (Backup ohne Agent)	Backup innerhalb eines Gastbetriebssystems
VMware		
VMware vSphere-Versionen: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 **VMware vSphere-Editionen:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual Server) VMware Workstation VMware ACE VMware Player		+
Microsoft		

Plattform	Backup auf Hypervisor-Ebene (Backup ohne Agent)	Backup innerhalb eines Gastbetriebssystems
Windows Server 2008 (x64) mit Hyper-V Windows Server 2008 R2 mit Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 mit Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) mit Hyper-V Windows 10 mit Hyper-V Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers Microsoft Hyper-V Server 2016	+	+
Microsoft Virtual PC 2004 und 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5		Nur vollständig virtualisierte Gäste (HVM)
Red Hat und Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		+
Kernel-based Virtual Machines (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Nur vollständig virtualisierte Gäste (HVM)
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x bis 20180425.x		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	(nur virtuelle Maschinen). Container werde nicht unterstützt)

Plattform	Backup auf Hypervisor-Ebene (Backup ohne Agent)	Backup innerhalb eines Gastbetriebssystems
Amazon		
Amazon EC2-Instanzen		+
Microsoft Azure		
Virtuelle Azure-Maschinen		+

* Bei diesen Editionen wird der HotAdd-Transport für virtuelle Laufwerke auf vSphere 5.0 (und später) unterstützt. Auf Version 4.1 können Backups langsamer laufen.

** Backups auf Hypervisor-Ebene werden nicht für vSphere Hypervisor unterstützt, da dieses Produkt den Zugriff auf die Remote-Befehlszeilenschnittstelle (Remote Command Line Interface, RCLI) auf den 'Nur Lesen'-Modus beschränkt. Der Agent arbeitet während des vSphere Hypervisor-Evaluierungszeitraums ohne Eingabe einer Seriennummer. Sobald Sie eine Seriennummer eingeben, hört der Agent auf zu funktionieren.

Einschränkungen

- **Fehlertolerante Maschinen**

  Der Agent für VMware sichert eine fehlertolerante Maschine nur dann, wenn die Fehlertoleranz in VMware vSphere 6.0 (und später) aktiviert wurde. Falls Sie ein Upgrade von einer früheren vSphere-Version durchgeführt haben, reicht es aus, wenn Sie die Fehlertoleranz für jede Maschine deaktivieren und aktivieren. Wenn Sie eine frühere vSphere-Version verwenden, installieren Sie einen Agenten im Gastbetriebssystem.

- **Unabhängige Laufwerke und RDM-Laufwerke**

  Der Agent für VMware kann keine RDM-Laufwerke (Raw Device Mapping) im physischen Kompatibilitätsmodus und keine unabhängigen Laufwerke sichern. Der Agent überspringt diese Laufwerke und fügt dem Log entsprechende Warnmeldungen hinzu. Sie können diese Warnmeldungen vermeiden, indem Sie unabhängige Laufwerke und RDM-Laufwerke im physischen Kompatibilitätsmodus von einem Backup-Plan ausschließen. Falls Sie diese Laufwerke sichern wollen, müssen Sie einen Agenten im Gastbetriebssystem installieren.

- **Pass-Through-Laufwerke (Durchleitungslaufwerke)**

  Der Agent für Hyper-V kann keine Pass-Through-Laufwerke sichern. Der Agent überspringt diese Laufwerke während des Backups und fügt dem Log entsprechende Warnmeldungen hinzu. Sie können diese Warnmeldungen vermeiden, indem Sie Pass-through-Laufwerke von einem Backup-Plan ausschließen. Falls Sie diese Laufwerke sichern wollen, müssen Sie einen Agenten im Gastbetriebssystem installieren.

- **iSCSI-Verbindung im Gast**

  Der Agent für VMware und der Agent für Hyper-V sichern keine LUN-Volumes, die über einen iSCSI-Initiator verbunden sind, der von innerhalb des Gastbetriebssystems aus arbeitet. Weil den ESXi- und Hyper-V-Hypervisoren solche Volumes nicht bekannt sind, werden die Volumes nicht in die Hypervisor-basierten Snapshots aufgenommen und daher ohne Vorwarnung vom Backup ausgeschlossen. Wenn Sie diese Volumes oder bestimmte Daten auf diesen Volumes sichern wollen, müssen Sie einen Agenten im Gastbetriebssystem installieren.

- **Hyper-V-Gast-Clustering**

  Mit dem Agenten für Hyper-V können keine virtuellen Hyper-V-Maschinen gesichert werden, die Knoten eines Windows Server-Failover-Clusters sind. Ein VSS-Snapshot auf Host-Ebene kann sogar das externe Quorum-Laufwerk temporär vom Cluster trennen. Wenn Sie diese Maschinen per Backup sichern wollen, müssen Sie die Agenten in den entsprechenden Gastbetriebssystemen installieren.

- **Linux-Maschinen, die logische Volumes enthalten (LVM)**

  Folgende Aktionen für Linux-Maschinen mit LVM werden vom Agenten für VMware und dem Agenten für Hyper-V nicht unterstützt:

  - P2V-Migration, V2P-Migration und V2V-Migration von Virtuozzo. Den Agenten für Linux verwenden, um Backups und Boot-Medien für Wiederherstellungen zu erstellen.
  - Eine virtuelle Maschine direkt aus einem Backup ausführen, welches durch den Agenten für Linux erstellt wurde.
- **Verschlüsselte virtuelle Maschinen** (mit VMware vSphere 6.5 eingeführt)
  - Verschlüsselte virtuelle Laufwerke werden im Backup in einem unverschlüsselten Zustand gespeichert. Falls die Verschlüsselung der entsprechenden Daten für Sie wichtig ist, können Sie bei der Erstellung eines Backup-Plans (S. 59) festlegen, dass die Backups selbst verschlüsselt werden.
  - Wiederhergestellte virtuelle Maschinen sind immer unverschlüsselt. Sie können die Verschlüsselung nach Abschluss der Wiederherstellung aber wieder manuell aktivieren.
  - Wenn Sie verschlüsselte virtuelle Maschinen per Backup sichern, empfehlen wir Ihnen, außerdem auch die virtuelle Maschine zu verschlüsseln, auf welcher der Agent für VMware ausgeführt wird. Ansonsten sind die ausgeführten Aktionen mit den verschlüsselten Maschinen möglicherweise langsamer als erwartet. Verwenden Sie den vSphere Webclient, um der Maschine des Agenten die **VM-Verschlüsselungsrichtlinie** zuzuweisen.
  - Verschlüsselte virtuelle Maschinen werden via LAN gesichert – und zwar auch dann, wenn Sie den SAN-Transportmodus für den Agenten konfiguriert haben. Der Agent wird stattdessen auf den NBD-Transportmodus zurückgreifen, weil VMware den SAN-Transportmodus beim Backup verschlüsselter virtueller Laufwerke nicht unterstützt.
- **Secure Boot** (mit VMware vSphere 6.5 eingeführt)

  Wenn eine virtuelle Maschine als neue virtuelle Maschine wiederhergestellt wurde, ist **Secure Boot** anschließend deaktiviert. Sie können die Option nach Abschluss der Wiederherstellung aber wieder manuell aktivieren.
- **ESXi-Konfigurations-Backups** werden nicht für VMware vSphere 6.7 unterstützt.

2.7 Kompatibilität mit Verschlüsselungssoftware

Daten, die auf *Dateiebene* von einer Verschlüsselungssoftware verschlüsselt werden, können ohne Beschränkung gesichert und wiederhergestellt werden.

Verschlüsselungssoftware, die Daten auf Laufwerksebene *Laufwerksebene* verschlüsseln, tun dies 'on the fly'. Daher sind die entsprechenden, in ein Backup aufgenommenen Daten nicht verschlüsselt. Programme zur Laufwerksverschlüsselung modifizieren häufig wichtige Systembereiche: Boot-Record oder Partitionstabellen oder Dateisystemtabellen. Diese Faktoren können daher Backup- und Recovery-Aktionen mit solchen Laufwerken sowie die Fähigkeit eines wiederhergestellten Systems beeinflussen, booten oder auf eine Secure Zone zugreifen zu können.

Daten, die mit folgenden Software-Produkten zur Laufwerksverschlüsselung verschlüsselt wurden, können per Backup gesichert werden:

- Microsoft BitLocker-Laufwerksverschlüsselung
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption.

Um zuverlässige Wiederherstellungen auf Laufwerksebene zu garantieren, sollten Sie allgemeinen Regeln sowie Software-spezifischen Empfehlungen folgen.

Allgemeine Installationsregel

Es wird dringend empfohlen, die Verschlüsselungssoftware vor der Installation der Backup Agenten einzurichten.

Verwendung der Secure Zone

Die Secure Zone darf keiner Laufwerksverschlüsselung unterzogen werden. Die Secure Zone kann nur folgendermaßen verwendet werden:

1. Installieren Sie zuerst die Verschlüsselungssoftware und dann den Agenten.
2. Erstellen Sie die Secure Zone.
3. Wenn Sie das Laufwerk oder dessen Volumes verschlüsseln, müssen Sie die Secure Zone von der Verschlüsselung ausschließen.

Allgemeine Backup-Regel

Sie können ein Laufwerk-Backup im Betriebssystem durchführen.

Software-spezifische Recovery-Prozeduren

Microsoft BitLocker-Laufwerksverschlüsselung

So stellen Sie ein System wieder her, das per BitLocker verschlüsselt wurde:

1. Booten Sie mit einem Boot-Medium.
2. Stellen Sie das System wieder her. Die wiederhergestellten Daten sind unverschlüsselt.
3. Booten Sie das wiederhergestellte System neu.
4. Schalten Sie die BitLocker-Funktion ein.

Falls Sie nur ein Volume eines mehrfach partitionierten Laufwerks wiederherstellen müssen, so tun Sie dies unter dem Betriebssystem. Eine Wiederherstellung mit einem Boot-Medium kann dazu führen, dass Windows das wiederhergestellte Volume (die Partition) nicht mehr erkennen kann.

McAfee Endpoint Encryption und PGP Whole Disk Encryption

Sie können ein verschlüsseltes System-Volume nur durch Verwendung eines Boot-Mediums wiederherstellen.

Falls das wiederhergestellte System nicht mehr bootet, erstellen Sie einen neuen Master Boot Record, wie in folgendem Artikel der Microsoft Knowledge Base beschrieben:
https://support.microsoft.com/kb/2622803

3 Unterstützte Dateisysteme

Ein Backup Agent kann jedes Dateisystem per Backup sichern, auf welches das Betriebssystem, auf dem der Agent installiert ist, zugreifen kann. Der Agent für Windows kann beispielsweise ein ext4-Dateisystem sichern und wiederherstellen, sofern ein entsprechender ext4-Treiber unter Windows installiert wurde.

Die nachfolgende Tabelle fasst die Dateisysteme zusammen, die gesichert und wiederhergestellt werden können (Boot-Medien unterstützen nur Wiederherstellungen). Angegebene Beschränkungen gelten sowohl für die Agenten als auch Boot-Medien.

Dateisystem	Unterstützt durch			Einschränkungen
	Agenten	Boot-Medien für Windows und Linux	Boot-Medien für Mac	
FAT16/32	Alle Agenten	+	+	Keine Beschränkungen
NTFS		+	+	
ext2/ext3/ext4		+	-	
HFS+	Agent für Mac	-	+	
APFS		-	+	▪ Wird ab macOS High Sierra 10.13 unterstützt ▪ Bei Wiederherstellungen zu einer anderen als der ursprünglichen (wie einer fabrikneuen) Maschine muss die ursprüngliche Laufwerkskonfigurationen manuell neu erstellt werden.
JFS	Agent für Linux	+	-	Kein Ausschluss von Dateien von einem Laufwerk-Backup
ReiserFS3		+	-	
ReiserFS4		+	-	▪ Kein Ausschluss von Dateien von einem Laufwerk-Backup ▪ Keine Größenänderung von Volumes während einer Wiederherstellung
ReFS	Alle Agenten	+	+	
XFS		+	+	
Linux Swap	Agent für Linux	+	-	Keine Beschränkungen

Dateisystem	Unterstützt durch			Einschränkungen
	Agenten	Boot-Medien für Windows und Linux	Boot-Medien für Mac	
exFAT	Alle Agenten	+ Sie können kein Boot-Medium für eine Wiederherstellung verwenden, wenn das Backup auf einem Laufwerk mit dem Dateisystem exFAT *gespeichert ist*	+	▪ Es werden nur Laufwerk-/Volume-Backups unterstützt ▪ Es können keine Dateien aus einem Backup ausgeschlossen werden ▪ Es können keine einzelnen Dateien aus einem Backup wiederhergestellt werden

Die Software schaltet automatisch auf den Sektor-für-Sektor-Modus um, wenn ein Laufwerk ein Dateisystem verwendet, welches nicht erkannt oder nicht unterstützt wird. Ein Sektor-für-Sektor-Backup ist für jedes Dateisystem möglich, welches:

- Block-basiert ist
- sich nur über ein Laufwerk erstreckt
- ein Standard-MBR-/GPT-Partitionierungsschema verwendet

Falls ein Dateisystem diese Anforderungen nicht erfüllt, wird ein Backup fehlschlagen.

4 Das Konto aktivieren

Wenn ein Administrator ein Konto für Sie erstellt, wird eine E-Mail-Nachricht an Ihre E-Mail-Adresse gesendet. Die Nachricht enthält folgende Informationen:

- **Einen Link zur Kontoaktivierung.** Klicken Sie auf den Link und definieren Sie das Kennwort für das Konto. Merken Sie sich Ihren Anmeldenamen, der auf der Kontoaktivierungsseite angezeigt wird.
- **Ein Link zur Anmeldeseite der Backup Console.** Verwenden Sie diesen Link, um zukünftig auf die Console zuzugreifen. Die Anmeldedaten (Anmeldename, Kennwort) sind mit denen des vorherigen Schrittes identisch.

5 Zugriff auf den Backup Service

Sie können sich am Backup Service anmelden, wenn Sie Ihr Konto aktiviert haben.

So melden Sie sich am Backup Service an

1. Rufen Sie die Anmeldeseite des Backup Service auf. Die Adresse der Anmeldeseite war in der Aktivierungs-E-Mail-Nachricht enthalten.
2. Geben Sie den Anmeldenamen ein und klicken Sie dann auf **Fortsetzen**.
3. Geben Sie das Kennwort ein und klicken Sie dann auf **Anmelden**.

4. Wenn Sie die Administrator-Rolle im Backup Service haben, klicken Sie auf **Backup & Disaster Recovery**.

   Benutzer, die keine Administrator-Rolle haben, melden sich direkt an der Backup-Konsole an.

Sie können die Sprache der Weboberfläche ändern, wenn Sie auf das Symbol 'Konto' in der oberen rechten Ecke klicken.

Wenn **Backup & Disaster Recovery** nicht der einzige Service ist, den Sie abonniert haben, können Sie über das Symbol  in der rechten oberen Ecke zwischen den Services umschalten. Administratoren können über das Symbol auch zum Management-Portal wechseln.

6 Die Installation der Software

6.1 Vorbereitung

Schritt 1:

Wählen Sie einen Agenten danach aus, welche Art von Daten Sie per Backup sichern wollen. Die nachfolgende Tabelle soll Ihnen durch eine Zusammenfassung aller relevanten Informationen bei dieser Entscheidung helfen.

Beachten Sie, dass der Agent für Windows zusammen mit dem Agenten für Exchange bzw. für SQL, für VMware, für Hyper-V oder für Active Directory installiert wird. Wenn Sie also beispielsweise den Agenten für SQL installieren, können Sie zudem auch immer ein Backup der kompletten Maschine (auf welcher der Agent installiert ist) erstellen.

Was möchten Sie sichern?	Welchen Agenten soll ich installieren?	Wo soll die Installation erfolgen?
Physische Maschinen		
Unter Windows laufende physische Maschinen	Agent für Windows	Auf der Maschine, die gesichert werden soll.
Physische Maschinen, auf denen Linux läuft	Agent für Linux	
Unter macOS laufende physische Maschinen	Agent für Mac	
Applikationen		
SQL-Datenbanken	Agent für SQL	Auf der Maschine, die den Microsoft SQL Server ausführt.
Exchange-Datenbanken	Agent für Exchange	Auf der Maschine, auf der die Postfachrolle des Microsoft Exchange Servers ausgeführt wird.
Microsoft Office 365-Postfächer	Agent für Office 365	Auf einer Windows-Maschine, die über eine Internetverbindung verfügt. Sie müssen – abhängig von der gewünschten Funktionalität – möglicherweise den Agenten für Office 365 installieren. Weitere Informationen dazu finden Sie im Abschnitt 'Office 365-Daten sichern' (S. 148).

Was möchten Sie sichern?	Welchen Agenten soll ich installieren?	Wo soll die Installation erfolgen?
Microsoft Office 365 OneDrive-Dateien und SharePoint Online-Websites	—	Diese Daten können nur von einem Agenten gesichert werden, in der Cloud installiert ist. Weitere Informationen finden Sie im Abschnitt 'Office 365-Daten sichern (S. 148)'.
G Suite Gmail-Postfächer, Google Drive-Dateien und Team Drive-Dateien	—	Diese Daten können nur von einem Agenten gesichert werden, in der Cloud installiert ist. Weitere Informationen finden Sie im Abschnitt 'G Suite sichern (S. 164)'.
Maschinen, auf denen die Active Directory Domain Services (Active Directory-Domänendienste) laufen	Agent für Active Directory	Auf dem Domain Controller.
Virtuelle Maschinen		
Virtuelle VMware ESXi-Maschinen	Agent für VMware (Windows)	Auf einer Windows-Maschine, die Netzwerkzugriff auf den vCenter Server und den Storage für virtuelle Maschinen hat.*
	Agent für VMware (Virtuelle Appliance)	Auf dem ESXi-Host.
Virtuelle Hyper-V-Maschinen	Agent für Hyper-V	Auf dem Hyper-V-Host.
Virtuelle Virtuozzo-Maschinen und -Container	Agent für Virtuozzo	Auf dem Virtuozzo-Host.
Virtuelle Maschinen, die auf Amazon EC2 gehostet werden	Wie bei den physischen Maschinen**	Auf der Maschine, die gesichert werden soll.
Virtuelle Maschinen, auf Windows Azure gehostet		
Virtuelle Citrix XenServer-Maschinen		
Red Hat Virtualization (RHV/RHEV)		
Kernel-based Virtual Machines (KVM)		
Virtuelle Oracle-Maschinen		
Virtuelle Nutanix AHV-Maschinen		
Mobilgeräte		
Mobilgeräte mit Android	Mobile App für Android	Auf dem Mobilgerät, das gesichert werden soll.
Mobilgeräte mit iOS	Mobile App für iOS	

*Sollte Ihr ESXi einen per SAN angeschlossenen Storage verwenden, 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 ESXi-Host und das LAN. Ausführliche Informationen finden Sie im Abschnitt 'Agent für VMware – LAN-freies Backup (S. 195)'.

**Eine virtuelle Maschine wird dann als 'virtuell' betrachtet, wenn Sie von einem externen Agenten gesichert wird. Sollte ein Agent dagegen in einem Gastsystem installiert sein, werden Backup- und Recovery-Aktionen genauso wie bei physischen Maschinen durchgeführt. Davon unabhängig wird die Maschine jedoch als virtuelle Maschine gezählt, wenn Sie Quotas für eine bestimmte Anzahl von Maschinen festlegen.

Schritt 2:

Überprüfen Sie die Systemanforderungen für die Agenten.

Agent	Durch den/die Agent(en) belegter Speicherplatz
Agent für Windows	550 MB
Agent für Linux	500 MB
Agent für Mac	450 MB
Agent für SQL	600 MB (50 MB + 550 MB Agent für Windows)
Agent für Exchange	750 MB (200 MB + 550 MB Agent für Windows)
Agent für Office 365	550 MB
Agent für Active Directory	600 MB (50 MB + 550 MB Agent für Windows)
Agent für VMware	700 MB (150 MB + 550 MB Agent für Windows)
Agent für Hyper-V	600 MB (50 MB + 550 MB Agent für Windows)
Agent für Virtuozzo	500 MB

Die typische Arbeitsspeicherbelegung beträgt 300 MB ('oberhalb' des Betriebssystems und anderer ausgeführter Applikationen). Der Speicherverbrauch kann – abhängig von der Art und Menge der Daten, die die Agenten verarbeiten – kurzzeitig auf bis zu 2 GB steigen.

Bei einer Wiederherstellung mit einem Boot-Medium oder einer Laufwerkswiederherstellung mit Neustart werden mindestens 1 GB Arbeitsspeicher benötigt.

Schritt 3:

Laden Sie das Setup-Programm herunter. Sie können die Download-Links ermitteln, indem Sie auf **Alle Geräte** –> **Hinzufügen** klicken.

Auf der '**Geräte hinzufügen**'-Seite werden die Webinstaller für jeden Agenten bereitgestellt, der unter Windows installiert wird. Ein Webinstaller ist eine kleine, ausführbare Datei, die das Setup-Hauptprogramm aus dem Internet herunterlädt und dieses als temporäre Datei speichert. Die temporäre Datei wird direkt nach der Installation wieder gelöscht.

Falls Sie die Setup-Programme lokal speichern möchten, müssen Sie ein Paket herunterladen, welches alle Agenten zur Installation unter Windows enthält. Nutzen Sie dafür den Link im unteren Bereich der Seite '**Geräte hinzufügen**'. Es gibt sowohl 32-Bit- wie auch 64-Bit-Pakete. Mit diesem Paket können Sie festlegen, welche Komponenten installiert werden sollen. Diese Pakete ermöglichen Ihnen außerdem, eine unbeaufsichtigte Installation (beispielsweise per Gruppenrichtlinie) durchzuführen. Dieses erweiterte Szenario ist im Abschnitt 'Agenten per Gruppenrichtlinie bereitstellen' beschrieben.

Um das Setup-Programm des Agenten für Office 365 herunterzuladen, klicken Sie in der oberen rechten Ecke zuerst auf das Kontosymbol und dann auf **Downloads** –> **Agent für Office 365**.

Die Installation unter Linux und macOS wird mithilfe herkömmlicher Setup-Programme durchgeführt.

Alle Setup-Programme benötigen eine Internetverbindung, um die Maschine im Backup Service registrieren zu können. Wenn es keine Internetverbindung gibt, schlägt die Installation fehl.

Schritt 4:

Stellen Sie vor der Installation sicher, dass die Firewalls und anderen Komponenten Ihres Netzwerksicherheitssystems (z.B. ein Proxy-Server) über folgende TCP-Ports eingehende und ausgehende Verbindungen erlauben:

- **443** und **8443** – diese Ports werden verwendet, um auf die Backup-Konsole zuzugreifen, die Agenten zu registrieren, Zertifikate herunterzuladen, Benutzer zu autorisieren und Dateien aus dem Cloud Storage herunterzuladen.
- **7770...7800** – die Agenten verwenden diese Ports, um mit dem Backup Management Server zu kommunizieren.
- **44445** – die Agenten verwenden diesen Port, um Daten bei Backup- und Recovery-Aktionen zu übertragen.

Falls in Ihrem Netzwerk ein Proxy-Server aktiv ist, sollten Sie sich im Abschnitt 'Proxy-Server-Einstellungen (S. 20)' darüber informieren, ob und wann Sie diese Einstellungen für jede Maschine konfigurieren müssen, die einen Backup Agenten ausführt.

Die minimale Internetverbindungsgeschwindigkeit, um den Agenten noch aus der Cloud verwalten zu können, beträgt 1 Mbit/s. Diese Geschwindigkeit sollte nicht mit der minimalen Übertragungsrate verwechselt werden, die benötigt wird, um Backups in die Cloud erstellen zu können. Berücksichtigen Sie dies, wenn Sie eine Internetanschlusstechnologie mit niedriger Bandbreite (wie ADSL) verwenden.

6.2 Proxy-Server-Einstellungen

Die Backup Agenten können ihre Daten auch über einen HTTP/HTTPS-Proxy-Server übertragen. Der Server muss durch einen HTTP-Tunnel arbeiten, ohne den HTTP-Verkehr zu scannen oder zu beeinflussen. Man-in-the-Middle-Proxies werden nicht unterstützt.

Da sich der Agent bei der Installation selbst in der Cloud registriert, müssen die Proxy-Server-Einstellungen während der Installation oder schon vorher bereitgestellt werden.

Unter Windows:

Wenn in Windows ein Proxy-Server konfiguriert ist (**Systemsteuerung** –> **Internetoptionen** –> **Verbindungen**), liest das Setup-Programm die entsprechenden Proxy-Server-Einstellungen aus der Registry aus und übernimmt diese automatisch. Sie können die Proxy-Einstellungen auch während der Installation eingeben oder sie im Voraus (wie nachfolgend beschrieben) festlegen. Wenn Sie die Proxy-Einstellungen nach der Installation ändern wollen, gehen Sie genauso vor.

So können Sie die Proxy-Server-Einstellungen in Windows spezifizieren

1. Erstellen Sie ein neues Text-Dokument und öffnen Sie dieses in einem Text-Editor (wie Notepad).
2. Kopieren Sie die nachfolgenden Zeilen und fügen Sie diese dann in die Datei ein:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Ersetzen Sie `proxy.company.com` mit dem Host-Namen/der IP-Adresse Ihres Proxy-Servers – und verwenden Sie `000001bb` als Hexadezimalwert für die Port-Nummer. Beispielsweise entspricht `000001bb` dem Port 443.
4. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie `proxy_login` und `proxy_password` mit den entsprechenden Anmeldedaten des Proxy-Servers. Wenn diese nicht der Fall ist, löschen Sie diese Zeilen aus der Datei.
5. Speichern Sie das Dokument als '**proxy.reg**'.
6. Führen Sie die Datei 'als Administrator' aus.
7. Bestätigen Sie, dass Sie die Änderung der Windows Registry wirklich ausführen wollen.
8. Sollte der Backup Agent bisher noch nicht installiert sein, können Sie die Installation jetzt durchführen. Gehen Sie alternativ folgendermaßen vor, um den Agenten neu zu starten:
   a. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie ein: **cmd**
   b. Klicken Sie auf **OK**.
   c. Führen Sie folgende Befehle aus:

```
net stop mms
net start mms
```

Unter Linux:

Starten Sie die Installationsdatei mit den Parametern **`--http-proxy-host=`**ADRESSE **`--http-proxy-port=`**PORT **`--http-proxy-login=`**ANMELDENAME **`--http-proxy-password=`**KENNWORT. Wenn Sie die Proxy-Einstellungen nach der Installation ändern wollen, verwenden Sie die unten beschriebene Prozedur.

So können Sie die Proxy-Server-Einstellungen in Linux ändern

1. Öffnen Sie die Datei **/etc/Acronis/Global.config** in einem Text-Editor.
2. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn die Proxy-Einstellungen während der Installation des Agenten spezifiziert wurden, suchen Sie nach dem folgenden Abschnitt:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADRESSE"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"ANMELDENAME"</value>
    <value name="Password" type="TString">"KENNWORT"</value>
</key>
```

   - Sie können die obigen Zeilen auch kopieren und in die Datei zwischen den Tags '**`<registry name="Global">...</registry>`**' einfügen.
3. Ersetzen Sie ADRESSE mit dem Host-Namen/der IP-Adresse des neuen Proxy-Servers – und PORT mit dem Dezimalwert der dazugehörigen Port-Nummer.
4. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie ANMELDENAME und KENNWORT mit den entsprechenden Anmeldedaten des Proxy-Servers. Wenn diese nicht der Fall ist, löschen Sie diese Zeilen aus der Datei.
5. Speichern Sie die Datei.
6. Starten Sie den Agenten neu, indem Sie den folgenden Befehl in einem beliebigen Verzeichnis ausführen:

```
sudo service acronis_mms restart
```

Unter macOS:

Sie können die Proxy-Einstellungen auch während der Installation eingeben oder sie im Voraus (wie nachfolgend beschrieben) festlegen. Wenn Sie die Proxy-Einstellungen nach der Installation ändern wollen, gehen Sie genauso vor.

So können Sie die Proxy-Server-Einstellungen in macOS spezifizieren

1. Erstellen Sie die Datei '**/Library/Application Support/Acronis/Registry/Global.config**' und öffnen Sie diese in einem Text-Editor (z.B. Text Edit).
2. Kopieren Sie die nachfolgenden Zeilen und fügen Sie diese dann in die Datei ein:

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. Ersetzen Sie `proxy.company.com` mit dem Host-Namen/der IP-Adresse Ihres Proxy-Servers – und verwenden Sie `443` als Dezimalwert für die Port-Nummer.
4. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie `proxy_login` und `proxy_password` mit den entsprechenden Anmeldedaten des Proxy-Servers. Wenn diese nicht der Fall ist, löschen Sie diese Zeilen aus der Datei.
5. Speichern Sie die Datei.
6. Sollte der Backup Agent bisher noch nicht installiert sein, können Sie die Installation jetzt durchführen. Gehen Sie alternativ folgendermaßen vor, um den Agenten neu zu starten:
   a. Gehen Sie zu **Programme** –> **Dienstprogramme** –> **Terminal**
   b. Führen Sie folgende Befehle aus:

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

6.3 Linux-Pakete

Um die benötigten Module dem Linux-Kernel hinzufügen zu können, benötigt das Setup-Programm folgende Linux-Pakete:

- Das Paket mit den Kernel-Headers oder Kernel-Quellen. Die Paketversion muss zur Kernel-Version passen.
- Das GNU Compiler Collection (GCC) Compiler System. Die GCC-Version muss dieselbe sein, mit der der Kernel kompiliert wurde.
- Das Tool 'Make'.
- Der Perl-Interpreter.
- Die Bibliotheken **`libelf-dev`**, **`libelf-devel`** oder **`elfutils-libelf-devel`**, um Kernels ab v4.15 zu erstellen, die mit dem Parameter CONFIG_UNWINDER_ORC=y konfiguriert wurden. Für einige Distributionen, wie z.B. Fedora 28, müssen diese separat von Kernel-Headern installiert werden.

Die Namen dieser Pakete variieren je nach Ihrer Linux-Distribution.

Unter Red Hat Enterprise Linux, CentOS und Fedora werden die Pakete normalerweise vom Setup-Programm installiert. Bei anderen Distributionen müssen Sie die Pakete installieren, sofern Sie noch nicht installiert sind oder nicht die benötigten Versionen haben.

Sind die erforderlichen Pakete bereits installiert?

Führen Sie folgende Schritte aus, um zu überprüfen, ob die Pakete bereits installiert sind:

1. Führen Sie folgenden Befehl aus, um die Kernel-Version und die erforderliche GCC-Version zu ermitteln:

   ```
   cat /proc/version
   ```

   Die Ausgabezeilen dieses Befehls sehen ungefähr so aus: **`Linux version 2.6.35.6`** und **`gcc version 4.5.1`**
2. Führen Sie folgenden Befehl aus, um zu ermitteln, ob das Tool 'Make' und der GCC-Compiler installiert sind:

   ```
   make -v
   gcc -v
   ```

   Stellen Sie für **gcc** sicher, dass die vom Befehl zurückgemeldete Version die gleiche ist, wie die **`gcc version`** in Schritt 1. Bei **make** müssen Sie nur sicherstellen, dass der Befehl ausgeführt wird.
3. Überprüfen Sie, ob für die Pakete zur Erstellung der Kernel-Module die passende Version installiert ist:
   - Führen Sie unter Red Hat Enterprise Linux, CentOS und Fedora folgenden Befehl aus:

     ```
     yum list installed | grep kernel-devel
     ```
   - Führen Sie unter Ubuntu folgende Befehle aus:

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   Stellen Sie in jedem Fall sicher, dass die Paketversionen die gleichen wie bei **`Linux version`** im Schritt 1 sind.
4. Mit folgendem Befehl können Sie überprüfen, ob der Perl-Interpreter installiert ist:

   ```
   perl --version
   ```

   Der Interpreter ist installiert, wenn Ihnen Informationen über die Perl-Version angezeigt werden.
5. Führen Sie unter Red Hat Enterprise Linux, CentOS und Fedora folgenden Befehl aus, um zu überprüfen, ob **`elfutils-libelf-devel`** installiert ist.

   ```
   yum list installed | grep elfutils-libelf-devel
   ```

   Die Bibliothek ist installiert, wenn Ihnen Informationen über die Bibliotheksversion angezeigt werden.

Installation der Pakete aus dem Repository

Die folgende Tabelle führt auf, wie Sie die erforderlichen Pakete in verschiedenen Linux-Distributionen installieren können.

Linux-Distribution	Paketnamen	Art der Installation
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Das Setup-Programm wird die Pakete unter Verwendung Ihres Red Hat-Abonnements automatisch herunterladen und installieren.

	perl	Führen Sie folgenden Befehl aus: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Das Setup-Programm wird die Pakete automatisch herunterladen und installieren.
	perl	Führen Sie folgenden Befehl aus: `yum install perl`
Ubuntu Debian	**linux-headers** **linux-image** **gcc** **make** **perl**	Führen Sie folgende Befehle aus: `sudo apt-get update` `sudo apt-get install linux-headers-`uname -r`` `sudo apt-get install linux-image-`uname -r`` `sudo apt-get install gcc-<Paketversion>` `sudo apt-get install make` `sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source
	gcc
	make
	perl
		`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

Die Pakete werden aus dem Repository der Distribution heruntergeladen und installiert.

Informieren Sie sich für andere Linux-Distribution in den Dokumentationen der Distribution, wie die exakten Namen der erforderlichen Pakete dort lauten und wie diese installiert werden.

Manuelle Installation der Pakete

Sie müssen die Pakete **manuell** installieren, falls:

- Die Maschine kein aktives Red Hat-Abonnement oder keine Internetverbindung hat.
- Das Setup-Programm kann die zu Ihrer Kernel-Version passenden Versionen von **kernel-devel** oder **gcc** nicht finden. Sollte das verfügbare **kernel-devel** neuer als Ihr Kernel sein, dann müssen Sie den Kernel aktualisieren oder die passende **kernel-devel**-Version manuell installieren.
- Sie haben die erforderlichen Pakete im lokalen Netzwerk und möchten keine Zeit für automatische Suche und Download aufbringen.

Beziehen Sie die Pakete aus Ihrem lokalen Netzwerk oder von der Webseite eines vertrauenswürdigen Drittherstellers – und installieren Sie diese dann wie folgt:

- Führen Sie unter Red Hat Enterprise Linux, CentOS oder Fedora folgenden Befehl als Benutzer 'root' aus:
  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```
- Führen Sie unter Ubuntu folgenden Befehl aus:
  ```
  sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

Beispiel: Manuell Installation der Pakete unter Fedora 14

Folgen Sie diesen Schritten, um die erforderlichen Pakete unter Fedora 14 auf einer 32-Bit-Maschine zu installieren:

1. Führen Sie folgenden Befehl aus, um die Kernel-Version und die erforderliche GCC-Version zu ermitteln:


```
cat /proc/version
```

Die Ausgabe dieses Befehls beinhaltet Folgendes:

```
Linux version 2.6.35.6-45.fc14.i686
gcc version 4.5.1
```

2. Besorgen Sie sich die Pakete für **kernel-devel** und **gcc**, die zu dieser Kernel-Version passen:

```
kernel-devel-2.6.35.6-45.fc14.i686.rpm
gcc-4.5.1-4.fc14.i686.rpm
```

3. Besorgen Sie sich das **make**-Paket für Fedora 14:

```
make-3.82-3.fc14.i686
```

4. Führen Sie folgende Befehle als Benutzer 'root' aus, um die Pakete zu installieren:

```
rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
rpm -ivh gcc-4.5.1.fc14.i686.rpm
rpm -ivh make-3.82-3.fc14.i686
```

Sie können all diese Pakete mit einem einzigen **rpm**-Befehl spezifizieren. Die Installation jeder dieser Pakete kann die Installation weiterer Pakete erfordern, um Abhängigkeiten aufzulösen.

6.4 Installation der Agenten

Unter Windows:

1. Überprüfen Sie, dass die Maschine mit dem Internet verbunden ist.
2. Melden Sie sich als Administrator an und starten Sie das Setup-Programm.
3. [Optional] Klicken Sie auf **Installationseinstellungen anpassen** und Sie können bei Bedarf die folgenden Änderungen vornehmen:
   - Falls Sie den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers überprüfen oder ändern wollen. Unter Windows wird ein verfügbarer Proxy-Server automatisch erkannt und verwendet.
   - Falls Sie den Installationspfad ändern wollen.
   - Falls Sie das Konto for den Agenten-Dienst ändern wollen.
4. Klicken Sie auf **Installieren**.
5. [Nur, wenn Sie den Agenten für VMware installieren] Spezifizieren Sie die Adresse und Anmeldedaten für den vCenter Server oder den eigenständigen ESXi-Host, dessen virtuelle Maschinen der Agent sichern soll – und klicken Sie dann auf **Fertig**. Wir empfehlen, dass Sie ein Konto verwenden, dem die Rolle **Administrator** zugewiesen ist. Alternativ können Sie auch ein Konto angeben, welches über die notwendigen Berechtigungen (S. 197) auf dem vCenter Server oder ESXi-Host verfügt.
6. [Nur, wenn Sie eine Installation auf einem Domain Controller durchführen] Spezifizieren Sie das Benutzerkonto, unter dem der Agenten-Dienst ausgeführt werden soll – und klicken Sie dann auf **Fertig**. Das Setup-Programm erstellt aus Sicherheitsgründen nicht automatisch neue Konten auf einem Domain Controller.
7. Warten Sie, bis die Registrierungsanzeige erscheint.
8. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Die Maschine registrieren**. Melden Sie sich im geöffneten Browserfenster an der Backup-Konsole an, überprüfen Sie die Registrierungsinformationen und klicken Sie dann auf **Registrierung bestätigen**.
   - Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die

Registrierungsschritte dann auf einer anderen Maschine durchführen. In diesem Fall müssen Sie den Registrierungscode in das Registrierungsformular eingeben. Der Registrierungscode ist für eine (1) Stunde gültig.

Alternativ können Sie das Registrierungsformular auch aufrufen, wenn Sie zuerst auf **Alle Geräte** –> **Hinzufügen** klicken, dann nach unten bis zu **Registrierung per Code** scrollen und anschließend auf **Registrieren** klicken.

Tipp: *Beenden Sie das Setup-Programm nicht, bevor Sie die Registrierung bestätigt haben! Um die Registrierung neu initiieren zu können, müssen Sie das Setup-Programm neu starten. Klicken Sie anschließend auf* ***Die Maschine registrieren****.*

Dadurch wird die Maschine dem Konto zugewiesen, welches zur Anmeldung an die Backup-Konsole verwendet wurde.

Unter Linux:

1. Überprüfen Sie, dass die Maschine mit dem Internet verbunden ist.
2. Starten Sie die Installationsdatei als Benutzer 'root'.

   Falls in Ihrem Netzwerk ein Proxy-Server aktiviert ist, spezifizieren Sie beim Ausführen der Datei den Host-Namen/die IP-Adresse und den Port des Servers im folgenden Format:
   --http-proxy-host=ADRESSE **--http-proxy-port=**PORT
   --http-proxy-login=ANMELDENAME **--http-proxy-password=**KENNWORT.
3. Aktivieren Sie die Kontrollkästchen derjenigen Agenten, die Sie installieren wollen. Folgende Agenten sind verfügbar:
   - **Agent für Linux**
   - **Agent für Virtuozzo**

   Der Agent für Virtuozzo kann nicht ohne den Agenten für Linux installiert werden.
4. Warten Sie, bis die Registrierungsanzeige erscheint.
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Die Maschine registrieren**. Melden Sie sich im geöffneten Browserfenster an der Backup-Konsole an, überprüfen Sie die Registrierungsinformationen und klicken Sie dann auf **Registrierung bestätigen**.
   - Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann auf einer anderen Maschine durchführen. In diesem Fall müssen Sie den Registrierungscode in das Registrierungsformular eingeben. Der Registrierungscode ist für eine (1) Stunde gültig.

   Alternativ können Sie das Registrierungsformular auch aufrufen, wenn Sie zuerst auf **Alle Geräte** –> **Hinzufügen** klicken, dann nach unten bis zu **Registrierung per Code** scrollen und anschließend auf **Registrieren** klicken.

   Tipp: *Beenden Sie das Setup-Programm nicht, bevor Sie die Registrierung bestätigt haben! Um die Registrierung erneut zu initiieren, müssen Sie das Setup-Programm neu starten. Wiederholen Sie anschließend die Installationsprozedur.*

Dadurch wird die Maschine dem Konto zugewiesen, welches zur Anmeldung an die Backup-Konsole verwendet wurde.

Troubleshooting-Informationen können Sie in folgender Datei finden:
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

Unter macOS:

1. Überprüfen Sie, dass die Maschine mit dem Internet verbunden ist.
2. Klicken Sie doppelt auf die Installationsdatei (.dmg).
3. Warten Sie, bis das Betriebssystem das Disk-Image für die Installation geladen hat.
4. Klicken Sie doppelt auf **Installieren**.
5. Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird, klicken Sie in der Menüleiste auf **Backup Agent**, dann auf **Proxy-Server-Einstellungen** und spezifizieren Sie anschließend den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers.
6. Geben Sie auf Nachfrage die Administrator-Anmeldedaten an.
7. Klicken Sie auf **Fortsetzen**.
8. Warten Sie, bis die Registrierungsanzeige erscheint.
9. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Die Maschine registrieren**. Melden Sie sich im geöffneten Browserfenster an der Backup-Konsole an, überprüfen Sie die Registrierungsinformationen und klicken Sie dann auf **Registrierung bestätigen**.
   - Klicken Sie auf **Registrierungsinfo anzeigen**. Im Setup-Programm werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann auf einer anderen Maschine durchführen. In diesem Fall müssen Sie den Registrierungscode in das Registrierungsformular eingeben. Der Registrierungscode ist für eine (1) Stunde gültig.

   Alternativ können Sie das Registrierungsformular auch aufrufen, wenn Sie zuerst auf **Alle Geräte** –> **Hinzufügen** klicken, dann nach unten bis zu **Registrierung per Code** scrollen und anschließend auf **Registrieren** klicken.

   Tipp: *Beenden Sie das Setup-Programm nicht, bevor Sie die Registrierung bestätigt haben! Um die Registrierung erneut zu initiieren, müssen Sie das Setup-Programm neu starten. Wiederholen Sie anschließend die Installationsprozedur.*

Dadurch wird die Maschine dem Konto zugewiesen, welches zur Anmeldung an die Backup-Konsole verwendet wurde.

6.5 Den Agenten für VMware (Virtuelle Appliance) von einer OVF-Vorlage aus bereitstellen

6.5.1 Bevor Sie beginnen

Systemanforderungen für den Agenten

Standardmäßig werden der virtuellen Appliance 4 GB RAM und 2 vCPUs zugeordnet, was für die meisten Aktionen optimal und ausreichend ist. Wir empfehlen, diese Ressourcen auf 8 GB RAM und 4 vCPUs zu erhöhen, wenn die Bandbreite der Backup-Übertragungen voraussichtlich 100 MB/Sek. übersteigt (z.B. in 10-Gigabit-Netzwerken), um die Backup-Performance zu verbessern.

Die eigenen virtuellen Laufwerke der Appliance belegen nicht mehr als 6 GB. Das Laufwerksformat (ob „Thick“ oder „Thin“) spielt keine Rolle und hat daher keinen Einfluss auf die Performance der Appliance.

Wie viele Agenten benötige ich?

Obwohl bereits eine virtuelle Appliance in der Lage ist, eine komplette vSphere-Umgebung zu sichern, hat es sich bewährt, je eine virtuelle Appliance pro vSphere-Cluster (oder pro Host, wenn es keine Cluster gibt) bereitzustellen. Dies ermöglicht schnellere Backups, weil die Appliance die gesicherten Laufwerke per HotAdd-Transport anschließen kann und der Backup-Verkehr daher von einem lokalen Laufwerk zu einem anderen weitergeleitet wird.

Es ist normal, sowohl die virtuelle Appliance als auch den Agenten für VMware (Windows) gleichzeitig zu verwenden, sofern diese mit demselben vCenter Server *oder* mit verschiedenen ESXi-Hosts verbunden sind. Vermeiden Sie Situationen, bei denen ein Agent direkt mit einem ESXi-Host und ein anderer Agent mit dem vCenter Server verbunden ist, der diesen ESXi-Host verwaltet.

Sie sollten keinen lokal angeschlossenen Storage verwenden (also Backups auf virtuellen Laufwerken speichern, die an die virtuelle Appliance angeschlossen sind), wenn Sie mehr als einen Agenten haben. Weitere Informationen und Überlegungen dazu finden Sie im Abschnitt 'Einen lokal angeschlossenen Storage verwenden (S. 30)'.

Automatischen DRS (Distributed Resource Scheduler) für den Agenten deaktivieren

Wenn die virtuelle Appliance in einem vSphere-Cluster bereitgestellt wird, sollten Sie überprüfen, dass für diesen die Funktion 'automatisches vMotion' deaktiviert ist. Aktivieren Sie in den DRS-Einstellungen des Clusters einzelne Automatisierungslevel für jede virtuelle Maschine und schalten Sie den **Automatisierungslevel** für die virtuelle Appliance auf **Deaktiviert**.

6.5.2 Deployment der OVF-Vorlage

1. Klicken Sie auf **Alle Geräte** –> **Hinzufügen** –> **VMware ESXi** –> **Virtuelle Appliance (OVF)**.

   Das .zip-Archiv wird zu Ihrer Maschine heruntergeladen.
2. Entpacken Sie das .zip-Archiv. Der Ordner enthält eine .ovf-Datei und zwei .vmdk-Dateien.
3. Stellen Sie sicher, dass die Maschine, die den vSphere Client ausführt, auf diese Dateien zugreifen kann.
4. Starten Sie den vSphere Client und melden Sie sich am vCenter Server an.
5. Führen ein Deployment der OVF-Vorlage durch.
   - Wählen Sie beim Konfigurieren des Storage den gemeinsam genutzten Datenspeicher (sofern vorhanden). Das Laufwerksformat (ob „Thick“ oder „Thin“) spielt keine Rolle und hat daher keinen Einfluss auf die Performance der Appliance.
   - Achten Sie beim Konfigurieren der Netzwerkverbindungen darauf, ein Netzwerk auszuwählen, das eine Internetverbindung zulässt, damit sich der Agent korrekt in der Cloud registrieren kann.

6.5.3 Die virtuelle Appliance konfigurieren

1. **Die virtuelle Appliance starten**

   Lassen Sie im vSphere-Client die **Bestandsliste** (Inventory) anzeigen, klicken Sie mit der rechten Maustaste auf den Namen der virtuellen Appliance und wählen Sie dann **Einschalten** (Power on). Wählen Sie die Registerlasche '**Konsole**'.
2. **Proxy-Server**

   Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird:

a. Drücken Sie zum Starten der Eingabeaufforderung die Tastenkombination Strg+Alt+F2, während Sie sich in der Benutzeroberfläche der virtuellen Appliance befinden.

b. Öffnen Sie die Datei **/etc/Acronis/Global.config** in einem Text-Editor.

c. Suchen Sie den folgenden Abschnitt:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"0"</value>
    <value name="Host" type="TString">"ADRESSE"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"ANMELDENAME"</value>
    <value name="Password" type="TString">"KENNWORT"</value>
</key>
```

d. Ersetzen Sie **0** durch **1**.

e. Ersetzen Sie ADRESSE mit dem Host-Namen/der IP-Adresse des neuen Proxy-Servers – und PORT mit dem Dezimalwert der dazugehörigen Port-Nummer.

f. Wenn Ihr Proxy-Server eine Authentifizierung benötigt, ersetzen Sie ANMELDENAME und KENNWORT mit den entsprechenden Anmeldedaten des Proxy-Servers. Wenn diese nicht der Fall ist, löschen Sie diese Zeilen aus der Datei.

g. Speichern Sie die Datei.

h. Führen Sie den Befehl **reboot** aus.

Ansonsten können Sie diesen Schritt überspringen.

3. **Netzwerkeinstellungen**

   Die Netzwerkverbindung des Agenten wird automatisch per DHCP (Dynamic Host Configuration Protocol) konfiguriert. Zur Änderung der Standardkonfiguration klicken Sie unter **Agentenoptionen** bei **eth0** auf **Ändern** und spezifizieren die gewünschten Netzwerkeinstellungen.

4. **vCenter/ESX(i)**

   Klicken Sie unter **Agentenoptionen**, in **vCenter/ESX(i)**, auf **Ändern** und spezifizieren Sie den Namen oder die IP-Adresse des vCenter-Servers. Der Agent kann daraufhin Backup- und Recovery-Aktionen mit jeder vom vCenter-Server verwalteten virtuellen Maschine durchführen.

   Falls Sie keinen vCenter-Server verwenden, dann spezifizieren Sie den Namen oder die IP-Adresse desjenigen ESXi-Hosts, dessen virtuelle Maschinen Sie sichern und wiederherstellen wollen. Normalerweise laufen Backups schneller ab, wenn der Agent solche virtuelle Maschinen sichert, die von seinem eigenen Host gehostet werden.

   Spezifizieren Sie die Anmeldedaten, die der Agent verwendet, um sich mit dem vCenter-Server oder ESXi zu verbinden. Wir empfehlen, dass Sie ein Konto verwenden, dem die Rolle **Administrator** zugewiesen ist. Alternativ können Sie auch ein Konto angeben, welches über die notwendigen Berechtigungen (S. 197) auf dem vCenter Server oder ESXi-Host verfügt.

   Sie können auf **Verbindung prüfen** klicken, um sicherzustellen, dass die Anmeldedaten korrekt sind.

5. **Management Server**

   a. Klicken Sie bei **Agent-Optionen** im **Management Server** auf den Befehl **Ändern**.

   b. Wählen Sie bei **Server-Name/IP** die Option **Cloud**. Die Software zeigt die Adresse des Backup Service an. Ändern Sie diese Adresse nicht, solange es keine anderslautenden Anweisungen gibt.

   c. Spezifizieren Sie unter **Benutzername** und **Kennwort** die Anmeldedaten für den Backup Service. Der Agent und die virtuellen Maschinen, die der Agent verwaltet, werden unter diesem Konto registriert.

6. **Zeitzone**

   Klicken Sie im Bereich **Zeitzone** unter **Virtuelle Maschine** auf **Ändern**. Stellen Sie durch die Auswahl Ihres Standortes sicher, dass alle geplanten Aktionen zur korrekten Zeit ausgeführt werden.

7. **[Optional] Lokale Storages**

   Sie können an die virtuelle Appliance ein zusätzliches Laufwerk anschließen, sodass der Agent für VMware seine Backups zu diesem lokal angeschlossenen Storage durchführen kann.

   Fügen Sie das Laufwerk hinzu, indem Sie die Einstellungen der virtuellen Maschine bearbeiten und dann auf '**Aktualisieren** klicken. Darauf wird der Link **Storage erstellen** verfügbar. Klicken Sie auf den Link, wählen Sie das Laufwerk und spezifizieren Sie eine Bezeichnung für dieses.

6.5.4 Einen lokal angeschlossenen Storage verwenden

Sie können an einen Agenten für VMware (Virtuelle Appliance) ein zusätzliches Laufwerk anschließen, sodass der Agent seine Backups zu diesem lokal angeschlossenen Storage durchführen kann. Mit diesem Ansatz wird Netzwerkverkehr zwischen dem Agenten und dem Backup-Speicherort vermieden.

Eine virtuelle Appliance, die auf demselben Host oder Cluster mit den gesicherten virtuellen Maschinen ausgeführt wird, hat direkten Zugriff auf den/die Datenspeicher, wo sich die Maschinen befinden. Das bedeutet, dass die Appliance die gesicherten Laufwerke per HotAdd-Transport anschließen kann und der Backup-Verkehr daher von einem lokalen Laufwerk zu einem anderen weitergeleitet wird. Wenn der Datenspeicher als **Festplatte/LUN** (statt per **NFS**) verbunden ist, wird das Backup komplett 'LAN-frei' sein. Bei einem NFS-Datenspeicher kommt es dagegen zum Netzwerkverkehr zwischen dem Datenspeicher und dem Host.

Die Verwendung eines lokal angeschlossenen Storages setzt voraus, dass der Agent immer dieselben Maschinen sichert. Falls die Maschinen stattdessen vom Management Server zwischen den Agenten verteilt werden, können die Backups einer Maschine über mehrere Storages zerstreut werden. Wir empfehlen, keinen lokal angeschlossenen Storage zu verwenden, wenn Sie mehr als einen Agenten haben.

Sie können den Storage zu einem bereits arbeitenden Agenten hinzufügen oder wenn Sie den Agenten über eine OVF-Vorlage bereitstellen (S. 28).

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 VMware (Virtuelle Appliance).
2. Fügen Sie das Laufwerk hinzu, indem Sie die Einstellungen der virtuellen Maschine bearbeiten. Die Laufwerksgröße muss mindestens 10 GB betragen.

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

So wählen Sie einen lokal angeschlossen Storage als Backup-Ziel

Wählen Sie beim Erstellen eines Backup-Plans (S. 36) unter **Backup-Ziel** die Option **Lokale Ordner** – Sie dann den mit dem lokal angeschlossenen Storage korrespondierenden Laufwerksbuchstaben an, beispielsweise **D:**.

6.6 Agenten per Gruppenrichtlinie bereitstellen

Sie können den Agenten für Windows durch Verwendung einer Gruppenrichtlinie zentral auf Maschinen installieren (oder bereitstellen), die Mitglieder einer Active Directory-Domain sind.

Dieser Abschnitt erläutert, wie Sie ein Gruppenrichtlinienobjekt einrichten, um Agenten auf Maschinen in einer kompletten Domain oder deren Organisationseinheit bereitzustellen.

Jedes Mal, wenn sich eine Maschine an der Domain anmeldet, stellt das entsprechende Gruppenrichtlinienobjekt sicher, dass der Agent installiert und registriert ist.

Voraussetzungen

Bevor Sie mit dem Deployment des Agenten fortfahren, sollten Sie sicherstellen, dass:

- Sie eine Active Directory-Domain mit einem Domain Controller haben, die unter Microsoft Windows Server 2003 oder später laufen.
- Sie innerhalb der Domain ein Mitglied der Gruppe **Domänen-Admins** Domain sind.
- Sie das Setup-Programm **Alle Agenten zur Installation unter Windows** heruntergeladen haben. Auf der Seite **Geräte hinzufügen** in der Backup Console der Download-Link verfügbar ist.

Schritt 1: Ein Registrierungstoken generieren

Ein Registrierungs-Token übermittelt Ihre Identität an das Setup-Programm, ohne dass dabei Ihre Anmeldedaten (Anmeldename, Kennwort) für die Backup-Konsole gespeichert werden. Dadurch können Sie eine beliebige Anzahl von Maschinen unter Ihrem Konto registrieren. Um mehr Sicherheit zu erreichen, hat ein Token eine begrenzte Lebensdauer.

So können Sie ein Registrierungstoken generieren

1. Melden Sie sich an der Backup-Konsole mit den Anmeldedaten desjenigen Kontos an, dem die Maschinen zugewiesen werden sollen.
2. Klicken Sie auf **Alle Geräte** –> **Hinzufügen**.
3. Scrollen Sie bis zu **Registrierungstoken** runter und klicken Sie dann auf **Generieren**.
4. Spezifizieren Sie die Token-Gültigkeitsdauer und klicken Sie anschließend auf **Token generieren**.
5. Kopieren Sie das Token oder notieren Sie es auf einem Zettel.

   Wenn Sie auf **Aktive Tokens verwalten** klicken, können Sie alle bereits generierten Tokens einsehen und verwalten.

Schritt 2: Die .mst-Transform-Datei erstellen und das Installationspaket erstellen

1. Melden Sie sich als Administrator an einer beliebigen Maschine in der Domain an.
2. Erstellen Sie einen freigegebenen Ordner, in dem die Installationspakete gespeichert werden sollen. Stellen Sie sicher, dass alle Domain-Benutzer auf diesen freigegebenen Ordner zugreifen können – beispielsweise indem Sie die vorgegebenen Freigabeeinstellungen für **Jeder** übernehmen.
3. Starten Sie das Setup-Programm.
4. Klicken Sie auf **.mst- und .msi-Dateien für eine unbeaufsichtigte Installation erstellen**.

5. Klicken Sie neben **Registrierungstoken** auf **Spezifizieren** und geben Sie dann das von Ihnen generierte Token ein.
6. Überprüfen oder ändern Sie die Installationseinstellungen, die der .mst-Datei hinzugefügt werden, und klicken Sie dann auf **Fortsetzen**.
7. Spezifizieren Sie bei **Speicherziel für die Dateien** den Pfad zu dem von Ihnen erstellten Ordner.
8. Klicken Sie auf **Generieren**.

Anschließend wird die .mst-Transform-Datei erstellt und werden die .msi- und .cab-Installationspakete in dem von Ihnen erstellten Ordner extrahiert.

Schritt 3: Die Gruppenrichtlinienobjekte aufsetzen

1. Melden Sie sich am Domain Controller als Domain-Administrator an. Sollte die Domain mehr als einen Domain Controller haben, so melden Sie sich an irgendeinem von diesen als Domain-Administrator an.
2. Falls Sie planen, den Agenten in einer Organisationseinheit bereitzustellen, stellen Sie sicher, dass diese Organisationseinheit in der Domain existiert. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie im **Startmenü** zu **Verwaltung** und klicken Sie auf **Active Directory-Benutzer und -Computer** (im Windows Server 2003) oder **Gruppenrichtlinienverwaltung** (im Windows Server 2008 oder höher).
4. Im Windows Server 2003:
   - Klicken Sie mit der rechten Maustaste auf den Namen der Domain oder Organisationseinheit und wählen Sie dann **Eigenschaften**. Klicken Sie im Dialogfenster auf die Registerlasche **Gruppenrichtlinien** und wählen Sie dann **Neu**.

   In Windows Server 2008 oder höher:
   - Klicken Sie mit der rechten Maustaste auf den Namen der Domain oder Organisationseinheit, klicken Sie danach auf **Gruppenrichtlinienobjekt hier erstellen und verknüpfen**.
5. Bezeichnen Sie das neue Gruppenrichtlinienobjekt als **Agent für Windows**.
6. Öffnen Sie das Gruppenrichtlinienobjekt **Agent für Windows** folgendermaßen, um es bearbeiten zu können:
   - Klicken Sie im Windows Server 2003 auf das Gruppenrichtlinienobjekt und dann auf den Befehl **Bearbeiten**.
   - Klicken Sie im Windows Server 2008 oder höher unter **Gruppenrichtlinienobjekte** mit der rechten Maustaste auf das Gruppenrichtlinienobjekt und dann auf den Befehl **Bearbeiten**.
7. Erweitern Sie im Snap-In 'Gruppenrichtlinienobjekt-Editor' den Eintrag **Computerkonfiguration**.
8. Im Windows Server 2003 und Windows Server 2008:
   - Erweitern Sie den Eintrag **Softwareeinstellungen**.

   In Windows Server 2012 oder höher:
   - Erweitern Sie **Richtlinien** –> **Softwareeinstellungen**.
9. Klicken Sie mit der rechten Maustaste auf **Softwareinstallation**, wählen Sie dort **Neu** und klicken Sie auf **Paket**.
10. Wählen Sie das .mis-Installationspaket des Agenten in dem eben von Ihnen erstellten, freigegebenen Ordner und klicken Sie dann auf **Öffnen**.
11. Klicken Sie im Dialogfenster **Software bereitstellen** auf **Erweitert** und bestätigen Sie dann mit **OK**.
12. Klicken Sie in der Registerkarte **Modifikationen** auf **Hinzufügen** und wählen Sie das .mst-Transform, welches Sie zuvor erstellt haben.

13. Klicken Sie auf **OK** und schließen Sie das Dialogfenster **Software bereitstellen**.

6.7 Update der Agenten

Sie können mit der Weboberfläche Agenten ab den folgenden Version per Update aktualisieren:

- Agent für Windows, Agent für VMware (Windows), Agent für Hyper-V: Version 11.9.191 (und höher)
- Agent für Linux: Version 11.9.191 (und höher)
- Andere Agenten: jede Version kann aktualisiert werden

Sie können die Version des Agenten ermitteln, wenn Sie die betreffende Maschine auswählen und dann auf den Befehl **Überblick** klicken.

Wenn Sie ältere Agenten-Versionen aktualisieren wollen, müssen Sie die neueste Agenten-Version manuell herunterladen und installieren. Sie können die Download-Links ermitteln, indem Sie auf **Alle Geräte** –> **Hinzufügen** klicken.

So führen Sie das Update eines Agenten über die Weboberfläche durch:

1. Klicken Sie auf **Einstellungen** –> **Agenten**.

   Die Software zeigt eine Liste der Maschinen an. Maschinen mit einer veralteten Agenten-Version sind mit einem orangefarbenen Ausrufezeichen gekennzeichnet.
2. Wählen Sie die Maschinen aus, auf denen Sie die Agenten aktualisieren wollen. Diese Maschinen müssen online sein.
3. Klicken Sie auf **Agent aktualisieren**.

So können Sie den Agenten für VMware (Virtuelle Appliance) per Update aktualisieren

1. Entfernen Sie den Agenten für VMware (Virtuelle Appliance) gemäß der Beschreibung im Abschnitt 'Agenten deinstallieren (S. 34)'. Löschen Sie in Schritt 5 den Agenten über **Einstellungen** –> **Agenten**, obwohl Sie planen, den Agenten erneut zu installieren.
2. Stellen Sie den Agenten für VMware (Virtuelle Appliance) gemäß der Beschreibung im Abschnitt 'Deployment der OVF-Vorlage (S. 28)' bereit.
3. Konfigurieren Sie den Agenten für VMware (Virtuelle Appliance) gemäß der Beschreibung im Abschnitt 'Agenten deinstallieren (S. 28)'.

   Wenn Sie den lokal angeschlossenen Storage wieder aufbauen wollen, gehen Sie in Schritt 7 folgendermaßen vor:

   a. Fügen Sie das Laufwerk, welches den lokalen Storage enthält, der virtuellen Appliance hinzu.
   b. Klicken Sie auf **Aktualisieren** –> **Storage erstellen** > **Mounten**.
   c. Die Software zeigt den ursprünglichen **Buchstaben** und die **Bezeichung** des Laufwerks an. Übernehmen Sie die Einstellungen, ohne diese zu ändern.
   d. Klicken Sie auf **OK**.

   Dadurch werden die Backup-Pläne, die auf den alten Agenten angewendet wurden, automatisch wieder auf den neuen Agenten angewendet.
4. Pläne mit aktiviertem applikationskonformen Backup erfordern eine erneute Eingabe der Anmeldedaten für das Gastbetriebssystem. Bearbeiten Sie diese Pläne und geben Sie die Anmeldedaten neu ein.
5. Pläne, mit denen die ESXi-Konfiguration gesichert wird, erfordern eine erneute Eingabe des Kennworts für das 'root'-Konto. Bearbeiten Sie diese Pläne und geben Sie das Kennwort neu ein.

6.8 Agenten deinstallieren

Unter Windows:

Wenn Sie einzelne Produktkomponenten (z.B. einen der Agenten oder den Backup Monitor) entfernen wollen, führen Sie das Setup-Programm '**Alle Agenten zur Installation unter Windows**' aus, wählen Sie die Option zur Änderung des Produktes und deaktivieren Sie dann das Kontrollkästchen derjenigen Komponente, die Sie entfernen wollen. Den Link für das Setup-Programm finden Sie auf der Seite **Downloads** (klicken Sie in der oberen rechten Ecke auf das Symbol für das Konto und dann auf **Downloads**).

Wenn Sie alle Produktkomponenten entfernen wollen, befolgen Sie die nachfolgend beschriebenen Schritte.

1. Melden Sie sich als Administrator an.
2. Gehen Sie zu **Systemsteuerung** und wählen Sie **Programme und Funktionen** (oder **Software** bei Windows XP) –> **Acronis Backup Agent** –> **Deinstallieren**.
3. [Optional] Aktivieren Sie das Kontrollkästchen **Protokolle (Logs) und Konfigurationseinstellungen entfernen**.

   Falls Sie vorhaben, den Agenten später erneut zu installieren, lassen Sie dieses Kontrollkästchen deaktiviert. Wenn Sie das Kontrollkästchen aktivieren, wird die Maschine möglicherweise in der Backup-Konsole dupliziert – und die Backups der alten Maschine werden nicht mehr mit der neuen Maschine assoziiert sein.
4. Bestätigen Sie Ihre Entscheidung.
5. Überspringen Sie diesen Schritt, falls Sie vorhaben, den Agenten später noch einmal erneut zu installieren. Klicken Sie anderenfalls in der Backup-Konsole auf **Einstellungen** –> **Agenten**, wählen Sie die Maschine aus, auf welcher der Agent installiert war und klicken Sie dann auf **Löschen**.

Unter Linux:

1. Führen Sie als Benutzer 'root' die Datei '**/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**' aus.
2. [Optional] Aktivieren Sie das Kontrollkästchen **Alle Spuren des Produkts (Logs, Tasks, Depots und Konfigurationseinstellungen) entfernen**.

   Falls Sie vorhaben, den Agenten später erneut zu installieren, lassen Sie dieses Kontrollkästchen deaktiviert. Wenn Sie das Kontrollkästchen aktivieren, wird die Maschine möglicherweise in der Backup-Konsole dupliziert – und die Backups der alten Maschine werden nicht mehr mit der neuen Maschine assoziiert sein.
3. Bestätigen Sie Ihre Entscheidung.
4. Überspringen Sie diesen Schritt, falls Sie vorhaben, den Agenten später noch einmal erneut zu installieren. Klicken Sie anderenfalls in der Backup-Konsole auf **Einstellungen** –> **Agenten**, wählen Sie die Maschine aus, auf welcher der Agent installiert war und klicken Sie dann auf **Löschen**.

Unter macOS:

1. Klicken Sie doppelt auf die Installationsdatei (.dmg).
2. Warten Sie, bis das Betriebssystem das Disk-Image für die Installation geladen hat.
3. Klicken Sie im Image doppelt auf **Deinstallieren**.
4. Geben Sie auf Nachfrage die Administrator-Anmeldedaten an.
5. Bestätigen Sie Ihre Entscheidung.

6. Überspringen Sie diesen Schritt, falls Sie vorhaben, den Agenten später noch einmal erneut zu installieren. Klicken Sie anderenfalls in der Backup-Konsole auf **Einstellungen** –> **Agenten**, wählen Sie die Maschine aus, auf welcher der Agent installiert war und klicken Sie dann auf **Löschen**.

Den Agenten für VMware (Virtuelle Appliance) entfernen

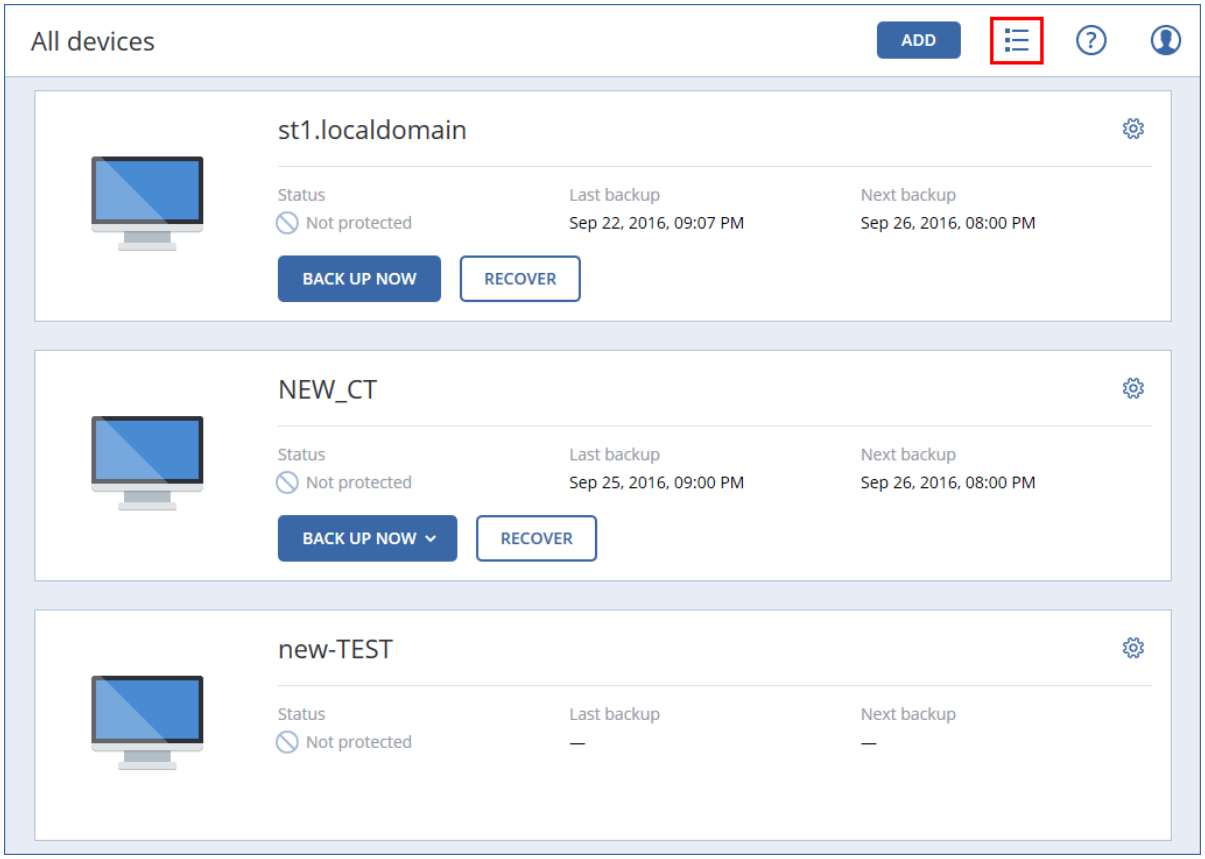
1. Starten Sie den vSphere Client und melden Sie sich am vCenter Server an.
2. Sollte die virtuelle Appliance (VA) eingeschaltet sein, dann klicken Sie mit der rechten Maustaste auf die VA. Klicken Sie anschließend auf die Befehle **Betrieb** –> **Ausschalten**. Bestätigen Sie Ihre Entscheidung.
3. Sollte die VA einen lokal angeschlossenen Storage auf einer virtuellen Festplatte verwenden und Sie die Daten dieser Festplatte bewahren wollen, dann gehen Sie folgendermaßen vor:
   a. Klicken Sie mit der rechten Maustaste auf die VA und wählen Sie **Einstellungen bearbeiten**.
   b. Wählen Sie die virtuelle Festplatte mit dem Storage und klicken Sie auf **Entfernen**. Klicken Sie unter **Optionen beim Entfernen** auf **Von der virtuellen Maschine entfernen**.
   c. Klicken Sie auf **OK**.

   Die Festplatte verbleibt als Ergebnis im Datenspeicher. Sie können die virtuelle Festplatte an eine andere VA anschließen.
4. Klicken Sie mit der rechten Maustaste auf die VA und wählen Sie **Von Festplatte löschen**. Bestätigen Sie Ihre Entscheidung.
5. Überspringen Sie diesen Schritt, falls Sie vorhaben, den Agenten später noch einmal erneut zu installieren. Alternativ können Sie in der Backup-Konsole auch Folgendes tun:
   a. Klicken Sie auf **Einstellungen** –> **Agenten**, wählen Sie die virtuelle Appliance aus und klicken Sie dann auf **Löschen**.
   b. Klicken Sie auf **Backups** –> **Speicherorte** und löschen Sie dann den Speicherort, der dem lokal angeschlossenen Storage entspricht.

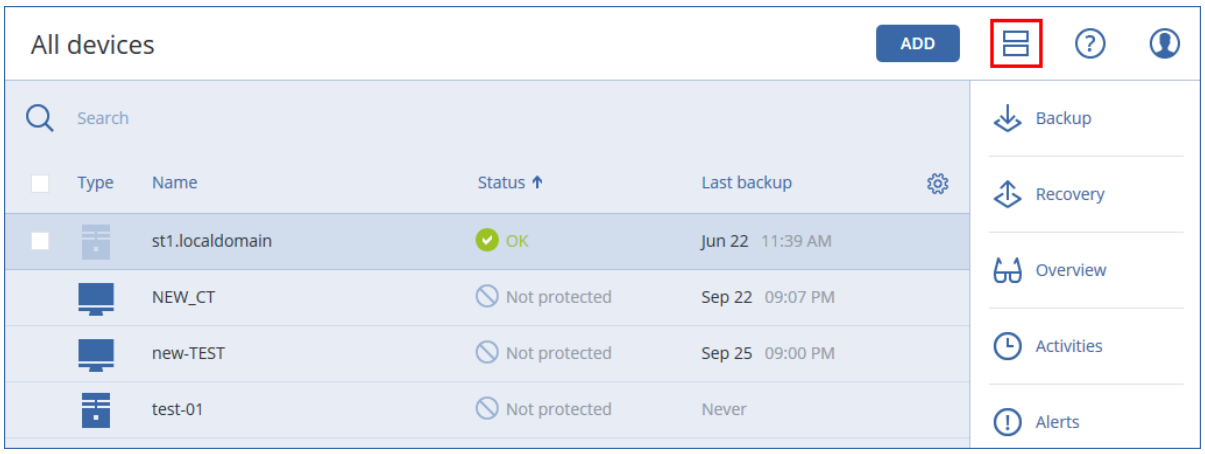
7 Die verschiedenen Ansichten der Backup Console

Die Backup Console verfügt über zwei Ansichten: eine einfache Ansicht und eine Tabellenansicht. Um zwischen den Ansichten umzuschalten, klicken Sie in der oberen rechten Ecke auf das entsprechende Symbol.

Die einfache Ansicht unterstützt lediglich eine kleine Anzahl von Maschinen.



Bei einer größeren Anzahl von Maschinen wird automatisch die Tabellenansicht aktiviert.



Beide Ansichten stellen ansonsten dieselben Funktionen und Operationen bereit. In diesem Dokument wird die Tabellenansicht verwendet, um den Zugriff auf die Operationen zu beschreiben.

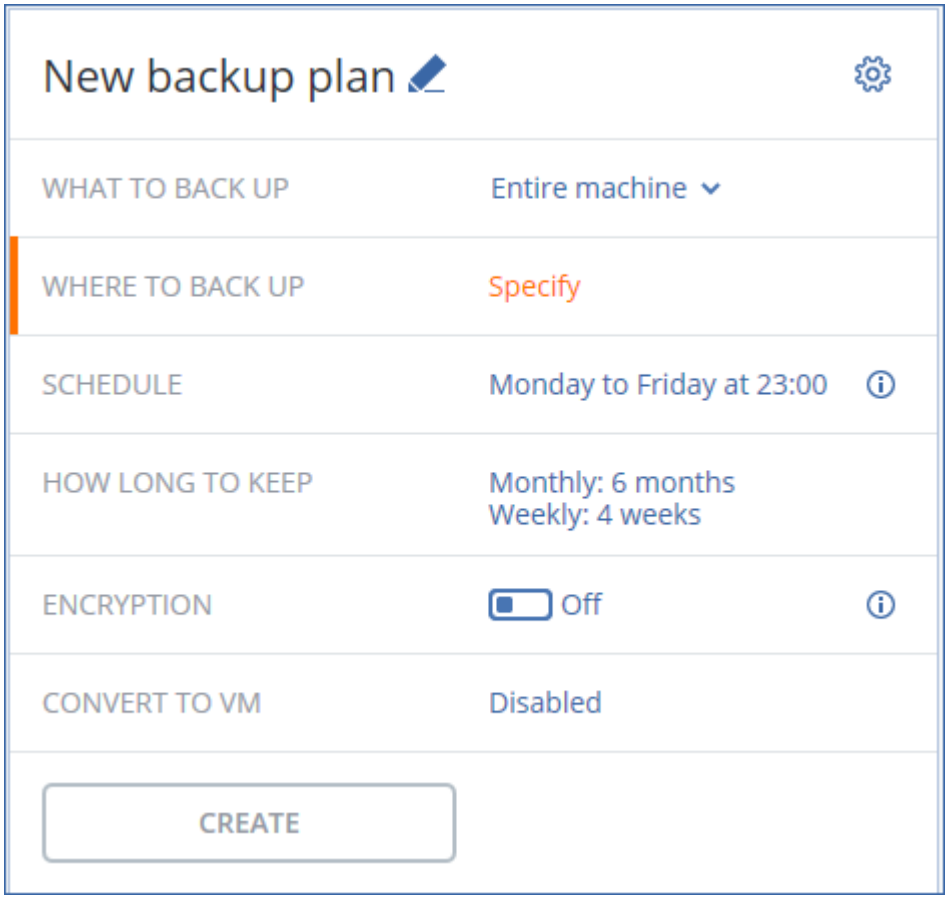
8 Backup

Ein Backup-Plan ist ein Satz mit Richtlinien für den Schutz der gegebenen Daten auf einer gegebenen Maschine.

Ein Backup-Plan kann zum Zeitpunkt seiner Erstellung (oder später) auf mehrere Maschinen angewendet werden.

So erstellen Sie den ersten Backup-Plan

1. Wählen Sie Maschinen, die Sie per Backup sichern wollen.
2. Klicken Sie auf **Backup**.
   Die Software zeigt eine neue Backup-Plan-Vorlage an.

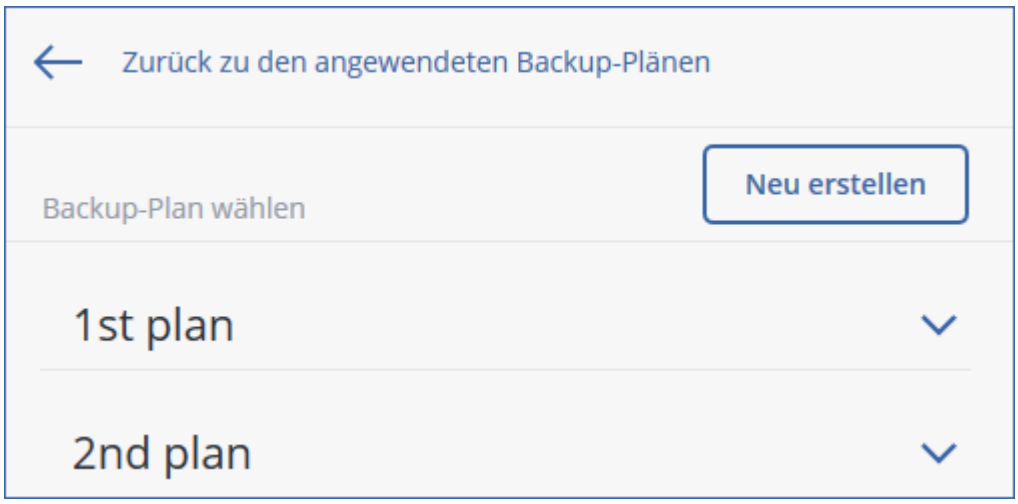


3. [Optional] Wenn Sie den Namen des Backup-Plans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. [Optional] Wenn Sie die Plan-Parameter ändern wollen, klicken Sie auf den entsprechenden Backup-Plan-Fensterbereich.
5. [Optional] Wenn Sie die Backup-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol.
6. Klicken Sie auf **Erstellen**.

So wenden Sie einen vorhandenen Backup-Plan an

1. Wählen Sie Maschinen, die Sie per Backup sichern wollen.
2. Klicken Sie auf **Backup**. Sollte auf die ausgewählten Maschinen bereits ein allgemeiner Backup-Plan angewendet worden sein, dann klicken Sie auf **Backup-Plan hinzufügen**.

Die Software zeigt die bisher erstellten Backup-Pläne an.



3. Wählen Sie den zu verwendenden Backup-Plan aus.
4. Klicken Sie auf **Anwenden**.

8.1 Backup-Plan-Spickzettel

Die nachfolgende Tabelle fasst alle verfügbaren Backup-Plan-Parameter zusammen. Verwenden Sie diese Tabelle, um einen Backup-Plan zu erstellen, der am besten zu Ihren Bedürfnissen passt.

Backup-Quelle	**Elemente für das Backup** **Auswahlmethoden**	**Backup-Ziel**	**Planung** **Backup-Schemata** **(nicht für die Cloud)**	**Aufbewahrungsdauer**
Laufwerke/Volumes (physische Maschinen)	Direkte Auswahl (S. 40) Richtlinienregeln (S. 40) Dateifilter (S. 70)	Cloud (S. 45) Lokaler Ordner (S. 45) Netzwerkordner (S. 45) NFS (S. 45)* Secure Zone (S. 45)**	Nur inkrementell (Einzeldatei) (S. 48) Nur vollständig (S. 48) Wöchentlich vollständig, täglich inkrementell (S. 48) Benutzerdefiniert (V-D-I) (S. 48)	Nach Backup-Alter (einzelne Regel/per Backup-Set) (S. 58) Nach Backup-Anzahl (S. 58) Unbegrenzt aufbewahren (S. 58)
Laufwerke/Volumes (virtuelle Maschinen)	Richtlinienregeln (S. 40) Dateifilter (S. 70)	Cloud (S. 45) Lokaler Ordner (S. 45) Netzwerkordner (S. 45) NFS (S. 45)*		
Dateien (nur physische Maschinen)	Direkte Auswahl (S. 42) Richtlinienregeln (S. 42) Dateifilter (S. 70)	Cloud (S. 45) Lokaler Ordner (S. 45) Netzwerkordner (S. 45) NFS (S. 45)* Secure Zone (S. 45)**	Nur vollständig (S. 48) Wöchentlich vollständig, täglich inkrementell (S. 48) Benutzerdefiniert (V-D-I) (S. 48)	

Backup-Quelle		Elemente für das Backup Auswahlmethoden	Backup-Ziel	Planung Backup-Schemata (nicht für die Cloud)	Aufbewahrungsdauer
ESXi-Konfiguration		Direkte Auswahl (S. 45)	Lokaler Ordner (S. 45) Netzwerkordner (S. 45) NFS (S. 45)*		
Websites (Dateien und MySQL-Datenbanken)		Direkte Auswahl (S. 181)	Cloud (S. 45)	—	
Systemzustand		Direkte Auswahl (S. 44)	Cloud (S. 45) Lokaler Ordner (S. 45) Netzwerkordner (S. 45)	Nur vollständig (S. 48) Wöchentlich vollständig, täglich inkrementell (S. 48) Benutzerdefiniert (V-I) (S. 48)	
SQL-Datenbanken		Direkte Auswahl (S. 136)			
Exchange-Datenbanken		Direkte Auswahl (S. 137)			
Microsoft Office 365	Postfächer (lokaler Agent für Office 365)	Direkte Auswahl (S. 150)	Cloud (S. 45) Lokaler Ordner (S. 45) Netzwerkordner (S. 45)	Nur inkrementell (Einzeldatei) (S. 48)	
	Postfächer (lokaler Agent für Office 365)	Direkte Auswahl (S. 153)	Cloud (S. 45)	—	
	OneDrive-Dateien	Direkte Auswahl (S. 157) Richtlinienregeln (S. 157)			
	SharePoint Online-Daten	Direkte Auswahl (S. 161) Richtlinienregeln (S. 161)			
G Suite	Gmail-Postfächer	Direkte Auswahl (S. 167)	Cloud (S. 45)	—	
	Google Drive-Dateien	Direkte Auswahl (S. 170) Richtlinienregeln (S. 170)			
	Team Drive-Dateien	Direkte Auswahl (S. 174) Richtlinienregeln (S. 174)			

* Backups zu NFS-Freigaben sind unter Windows nicht verfügbar.

** Eine Secure Zone kann nicht auf einem Mac erstellt werden.

8.2 Daten für ein Backup auswählen

8.2.1 Laufwerke/Volumes auswählen

Ein Backup auf Laufwerksebene (kurz 'Laufwerk-Backup') enthält eine Kopie der Daten eines Laufwerks/Volumes – und zwar in 'gepackter' Form. Sie können aus einem solchen Laufwerk-Backup sowohl einzelne Laufwerke/Volumes wie auch einzelne Dateien/Ordner wiederherstellen. Unter dem 'Backup einer kompletten Maschine' versteht man ein Backup, das alle Laufwerke der betreffenden Maschine enthält.

Es gibt zwei Möglichkeiten, wie Sie Laufwerke/Volumes auswählen können: direkt (manuell) auf jeder Maschine oder mithilfe von Richtlinienregeln. Es besteht die Möglichkeit, bestimmte Dateien durch die Festlegung von Dateifiltern (S. 70) von einem Laufwerk-Backup auszuschließen.

Direkte Auswahl

Eine direkte Auswahl ist nur für physische Maschinen verfügbar.

1. Wählen Sie bei **Backup-Quelle** die Option **Laufwerke/Volumes**.
2. Klicken Sie auf **Elemente für das Backup**.
3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Direkt**.
4. Aktivieren Sie für jede der im Backup-Plan enthaltenen Maschinen die entsprechenden Kontrollkästchen neben den zu sichernden Laufwerken/Volumes.
5. Klicken Sie auf **Fertig**.

Richtlinienregeln verwenden

1. Wählen Sie bei **Backup-Quelle** die Option **Laufwerke/Volumes**.
2. Klicken Sie auf **Elemente für das Backup**.
3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Richtlinienregeln verwenden**.
4. Wählen Sie eine der vordefinierten Regeln aus oder geben Sie Ihre eigenen Regeln ein (oder kombinieren Sie beides).

   Die Richtlinienregeln werden auf alle Maschinen angewendet, die im Backup-Plan enthalten sind. Wenn (beim Start des Backups) auf einer Maschine keine Daten gefunden werden, die den definierten Regeln entsprechen, so wird das Backup auf dieser Maschine fehlschlagen.
5. Klicken Sie auf **Fertig**.

Regeln für Windows, Linux und OS X

- Der Parameter **`[All volumes]`** wählt bei Maschinen, die unter Windows laufen, alle Volumes aus – und bei Maschinen, die unter Linux oder OS X laufen, alle gemounteten Volumes.

Regeln für Windows

- Ein Laufwerksbuchstabe (beispielsweise **C:**) wählt das Volume mit eben diesem Laufwerksbuchstaben aus.
- **`[Fixed Volumes (Physical machines)]`** wählt bei physischen Maschinen alle Volumes aus, die keine Wechselmedien sind. Fest eingebaute Volumes schließen auch solche Volumes ein, die auf SCSI-, ATAPI-, ATA-, SSA-, SAS- und SATA-Geräten sowie auf RAID-Arrays liegen.
- **`[BOOT+SYSTEM]`** wählt die System- und Boot-Volumes aus. Diese Kombination entspricht dem minimalen Datensatz, der für die Wiederherstellbarkeit eines Betriebssystems aus einem Backup notwendig ist.

- Der Parameter **[Disk 1]** wählt das erste Laufwerk der betreffenden Maschine aus (einschließlich aller Volumes auf diesem Laufwerk). Um ein anderes Laufwerk auszuwählen, müssen Sie nur die entsprechende Laufwerksnummer eingeben.

Regeln für Linux

- Der Parameter **/dev/hda1** wählt das erste Volume auf dem ersten IDE-Laufwerk aus.
- Der Parameter **/dev/sda1** wählt das erste Volume auf dem ersten SCSI-Laufwerk aus.
- Der Parameter **/dev/md1** wählt das erste Software-RAID-Laufwerk aus.

Verwenden Sie zur Auswahl anderer Basis-Volumes den Parameter **/dev/xdyN**, wobei:

- 'x' dem Laufwerkstyp entspricht
- 'y' der Laufwerksnummer entspricht ('a' für das erste Laufwerk, 'b' für das zweite usw.)
- 'N' der Volume-Nummer entspricht.

Um ein logisches Volume auswählen zu können, müssen Sie dessen Namen zusammen mit dem Namen der Volume-Gruppe spezifizieren. Um beispielsweise zwei logische Volumes namens **lv_root** und **lv_bin** sichern zu können – die zudem beide zur Volume-Gruppe **vg_meinemaschine** gehören – müssen Sie folgende Parameter spezifizieren:

```
/dev/vg_meinemaschine/lv_root
/dev/vg_meinemaschine/lv_bin
```

Regeln für OS X

- **[Disk 1]** wählt das erste Laufwerk der betreffenden Maschine aus (einschließlich aller Volumes auf diesem Laufwerk). Um ein anderes Laufwerk auszuwählen, müssen Sie nur die entsprechende Laufwerksnummer eingeben.

8.2.1.1 Was speichert das Backup eines Laufwerks oder Volumes?

Ein Laufwerk- bzw. Volume-Backup speichert das **Dateisystem** des entsprechenden Laufwerks bzw. Volumes 'als Ganzes'. Dabei werden auch alle zum Booten des Betriebssystems erforderlichen Informationen eingeschlossen. Aus solchen Backups können Laufwerke oder Volumes komplett wiederhergestellt werden – aber auch einzelne Dateien oder Ordner.

Wenn die Backup-Option (S. 80) '**Sektor-für-Sektor (Raw-Modus)**' aktiviert ist, werden in einem Laufwerk-Backup alle Sektoren des Laufwerks gespeichert. Das Sektor-für-Sektor-Backup kann verwendet werden, um Laufwerke mit nicht erkannten oder nicht unterstützten Dateisystemen sowie anderen proprietären Datenformaten zu sichern.

Windows

Ein Volume-Backup speichert alle Dateien und Ordner des gewählten Volumes, unabhängig von ihren Attributen (inkl. versteckter oder System-Dateien), den Boot-Record, die FAT (File Allocation Table) und – sofern vorhanden – auch das Stammverzeichnis (Root) und die Spur Null (Track Zero), inkl. Master Boot Record (MBR).

Ein Laufwerk-Backup speichert alle Volumes des betreffenden Laufwerks (inkl. versteckter Volumes wie Wartungs-Volumes von Herstellern) und die Spur Null (Track Zero) mit dem Master Boot Record (MBR).

Folgende Elemente sind *nicht* in einem Laufwerk- oder Volume-Backup enthalten (und genauso wenig in einem Backup auf Dateiebene):

- Die Auslagerungsdatei (pagefile.sys) und die Datei, die ein Abbild des Hauptspeichers ist, wenn der Computer in den Ruhezustand wechselt (hiberfil.sys). Nach einer Wiederherstellung werden die Dateien an passender Position mit einer Größe von Null erneut erzeugt.
- Wenn das Backup unter dem Betriebssystem durchgeführt wird (und nicht mit einem Boot-Medium oder durch Sicherung von virtuellen Maschinen auf Hypervisor-Ebene):
  - Windows Schattenspeicher (Shadow Storage). Der auf diesen verweisende Pfad wird über den Registry-Wert **VSS Default Provider** bestimmt, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup** gefunden werden kann. Das bedeutet, dass bei Betriebssystemen ab Windows Vista keine Windows-Systemwiederherstellungspunkte gesichert werden.
  - Wenn die Backup-Option (S. 81) **VSS (Volume Shadow Copy Service)** aktiviert ist, werden alle Dateien und Ordner, die im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** spezifiziert sind, nicht per Backup gesichert.

Linux

Ein Volume-Backup speichert alle Dateien und Verzeichnisse des gewählten Laufwerkes (unabhängig von ihren Attributen), einen Boot-Record und den Dateisystem-Super-Block.

Ein Laufwerk-Backup speichert alle Volumes des Laufwerks, inkl. der Spur Null (Track Zero) mit dem 'Master Boot Record' (MBR).

Mac

Ein Laufwerk oder Volume-Backup speichert alle Dateien und Verzeichnisse des ausgewählten Laufwerks oder Volumes – plus einer Beschreibung des Volume-Layouts.

Folgende Elemente werden dabei ausgeschlossen:

- System-Metadaten, wie etwa das Dateisystem-Journal und der Spotlight-Index.
- Der Papierkorb
- Time Machine-Backups

Laufwerke und Volumes auf einem Mac werden physisch auf Dateiebene gesichert. Bare Metal Recovery (Wiederherstellung auf fabrikneuer Hardware) von Laufwerk- und Volume-Backups ist möglich, aber der Backup-Modus 'Sektor-für-Sektor' ist nicht verfügbar.

8.2.2 Dateien/Verzeichnisse auswählen

Backups auf Dateiebene (kurz 'Datei-Backups') sind nur für physische Maschinen verfügbar.

Ein dateibasiertes Backup ist zur Wiederherstellung eines Betriebssystems nicht ausreichend geeignet. Verwenden Sie ein Datei-Backup, wenn Sie nur bestimmte Daten (beispielsweise ein aktuelles Projekt) sichern wollen. Sie können so die Backup-Größe verringern bzw. Speicherplatz sparen.

Es gibt zwei Möglichkeiten, wie Sie Dateien auswählen können: direkt (manuell) auf jeder Maschine oder mithilfe von Richtlinienregeln. Bei beiden Methoden können Sie die Auswahl durch die Festlegung von Dateifiltern (S. 70) noch verfeinern.

Direkte Auswahl

1. Wählen Sie bei **Backup-Quelle** die Option **Dateien/Ordner**.
2. Klicken Sie auf **Elemente für das Backup**.

3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Direkt**.
4. Für jede der im Backup-Plan enthaltenen Maschinen:
   a. Klicken Sie auf **Dateien und Ordner auswählen**.
   b. Klicken Sie auf **Lokaler Ordner** oder **Netzwerkordner**.

      Die Freigabe muss von der ausgewählten Maschine aus zugreifbar sein.
   c. Bestimmen Sie (über 'Durchsuchen') die gewünschten Dateien/Ordner oder geben Sie den Pfad manuell ein – und klicken Sie dann auf die Schaltfläche mit dem Pfeil. Spezifizieren Sie bei Aufforderung die Anmeldedaten (Benutzernamen, Kennwort), um auf den freigegebenen Ordner zugreifen zu können.

      Ein Backup von Ordnern mit anonymem Zugriff wird nicht unterstützt.
   d. Wählen Sie die gewünschten Dateien/Ordner aus.
   e. Klicken Sie auf **Fertig**.

Richtlinienregeln verwenden

1. Wählen Sie bei **Backup-Quelle** die Option **Dateien/Ordner**.
2. Klicken Sie auf **Elemente für das Backup**.
3. Wählen Sie bei **Elemente für das Backup auswählen** die Option **Richtlinienregeln verwenden**.
4. Wählen Sie eine der vordefinierten Regeln aus oder geben Sie Ihre eigenen Regeln ein (oder kombinieren Sie beides).

   Die Richtlinienregeln werden auf alle Maschinen angewendet, die im Backup-Plan enthalten sind. Wenn (beim Start des Backups) auf einer Maschine keine Daten gefunden werden, die den definierten Regeln entsprechen, so wird das Backup auf dieser Maschine fehlschlagen.
5. Klicken Sie auf **Fertig**.

Auswahlregeln für Windows

- Vollständiger Pfad zu einer Datei oder einem Ordner, beispielsweise **D:\Arbeit\Text.doc** oder **C:\Windows**.
- Templates:
  - Der Parameter **[All Files]** wählt alle Dateien auf allen Volumes der betreffenden Maschine aus.
  - Der Parameter **[All Profiles Folder]** wählt die Benutzerordner aller Benutzerprofile aus (üblicherweise **C:\Benutzer** (evtl. 'C:\Users' direkt im Dateisystem) oder **C:\Dokumente und Einstellungen**).
- Umgebungsvariablen:
  - Der Parameter **%ALLUSERSPROFILE%** wählt die Ordner der 'Gemeinsamen Daten' aller Benutzerprofile aus (üblicherweise **C:\ProgramData** oder **C:\Dokumente und Einstellungen\All Users**).
  - Der Parameter **%PROGRAMFILES%** wählt den Systemordner 'Programme' aus (beispielsweise **C:\Programme**).
  - Der Parameter **%WINDIR%** wählt den Systemordner von Windows aus (beispielsweise **C:\Windows**).

  Sie können auch andere Umgebungsvariablen oder eine Kombination von Umgebungsvariablen und Text verwenden. Geben Sie beispielsweise Folgendes ein, wenn Sie den Ordner 'Java' im Systemordner 'Programme' auswählen wollen: **%PROGRAMFILES%\Java**.

Auswahlregeln für Linux

- Vollständiger Pfad für eine Datei oder ein Verzeichnis. Beispiel: um **datei.txt** auf dem Volume **/dev/hda3** zu sichern, welches wiederum unter **/home/usr/docs** gemountet ist, können Sie entweder die Befehlszeile **/dev/hda3/datei.txt** oder **/home/usr/docs/datei.txt** spezifizieren.
  - **`/home`** wählt das Home-Verzeichnis der allgemeinen Benutzer aus.
  - **`/root`** wählt das Home-Verzeichnis des Benutzers 'root' aus.
  - Der Parameter **`/usr`** wählt das Verzeichnis für alle benutzerbezogenen Programme aus.
  - **`/etc`** wählt das Verzeichnis der Systemkonfigurationsdateien aus.
- Templates:
  - **`[All Profiles Folder]`** wählt **/home** aus Dies ist der Ordner, in dem sich standardmäßig alle Benutzerprofile befinden.

Auswahlregeln für macOS

- Vollständiger Pfad für eine Datei oder ein Verzeichnis.
- Templates:
  - **`[All Profiles Folder]`** wählt **/Users** aus Dies ist der Ordner, in dem sich standardmäßig alle Benutzerprofile befinden.

Beispiele:

- Um **datei.txt** auf Ihrem Desktop zu sichern, müssen Sie die Befehlszeile **/Users/<Benutzername>/Desktop/datei.txt** spezifizieren, wobei <Benutzername> für Ihren eigenen Benutzernamen steht.
- Spezifizieren Sie **/Users**, wenn Sie die Home-Verzeichnisse aller Benutzer sichern wollen.
- Spezifizieren Sie **/Applications**, wenn Sie das Verzeichnis sichern wollen, in dem alle Programme installiert sind.

8.2.3 Einen Systemzustand auswählen

Ein Backup des Systemzustands ist für Maschinen verfügbar, die unter Windows Vista oder einer neuere Windows-Version laufen.

Um einen Systemzustand sichern zu können, müssen Sie bei **Backup-Quelle** die Option **Systemzustand** auswählen.

Ein Backup des Systemzustands setzt sich aus Dateien folgender Windows-Komponenten/-Funktionen zusammen:

- Konfigurationsinformationen für die Aufgabenplanung
- VSS-Metadatenspeicher
- Konfigurationsinformationen für die Leistungsindikatoren
- MSSearch-Dienst
- Intelligenter Hintergrundübertragungsdienst (BITS)
- Die Registry
- Windows-Verwaltungsinstrumentation (WMI)
- Registrierungsdatenbank der Komponentendienste-Klasse

8.2.4 Eine ESXi-Konfiguration auswählen

Mit dem Backup einer ESXi-Host-Konfiguration können Sie einen ESXi-Host auf fabrikneuer Hardware wiederherstellen (Bare Metal Recovery). Die Wiederherstellung wird von einem Boot-Medium aus durchgeführt.

Evtl. auf dem Host laufende virtuelle Maschinen werden nicht in das Backup eingeschlossen. Sie können diese jedoch separat per Backup sichern und wiederherstellen.

Das Backup einer ESXi-Host-Konfiguration beinhaltet:

- Den Boot-Loader und die Boot-Bank-Partition des Hosts.
- Den Host-Zustand (virtuelle Netzwerk- und Storage-Konfiguration, SSL-Schlüssel, Server-Netzwerkeinstellungen und Informationen zu den lokalen Benutzern).
- Auf dem Host installierte oder bereitgestellte Erweiterungen und Patches.
- Protokolldateien.

Voraussetzungen

- SSH muss im **Sicherheitsprofil** der ESXi-Host-Konfiguration aktiviert sein.
- Sie müssen das Kennwort des 'root'-Kontos auf dem ESXi-Host kennen.

Einschränkungen

- ESXi-Konfigurations-Backups werden nicht für VMware vSphere 6.7 unterstützt.
- Eine ESXi-Konfiguration kann nicht in den Cloud Storage (als Backup-Ziel) gesichert werden.

So wählen Sie eine ESXi-Konfiguration aus

1. Gehen Sie zu **VMware** –> **Hosts und Cluster**.
2. Suchen Sie die gewünschten ESXi-Hosts über den Befehl 'Durchsuchen'.
3. Wählen Sie gefundenen ESXi-Hosts aus und klicken Sie auf **Backup**.
4. Wählen Sie bei **Backup-Quelle** die Option **ESXi-Konfiguration**.
5. Spezifizieren Sie bei **'root'-Kennwort für ESXi** das Kennwort für das jeweilige 'root'-Konto auf jedem der ausgewählten ESXi-Hosts – oder verwenden Sie dasselbe Kennwort für alle Hosts.

8.3 Ein Ziel auswählen

Klicken Sie auf **Backup-Ziel** und wählen Sie dann eine der folgenden Möglichkeiten:

- **Cloud Storage**

  Die Backups werden im Cloud-Datacenter gespeichert.

- **Lokale Ordner**

  Wenn Sie nur eine einzelne Maschine ausgewählt haben, dann bestimmen Sie auf der ausgewählten Maschine über 'Durchsuchen' den gewünschten Ordner – oder geben Sie den Ordnerpfad manuell ein.

  Wenn Sie mehrere Maschinen ausgewählt haben, geben Sie den Ordnerpfad manuell ein. Die Backups werden in genau diesem Ordner auf jeder der ausgewählten physischen Maschinen gespeichert – oder auf der Maschine, wo der Agent für virtuelle Maschinen installiert ist. Falls der Ordner nicht existiert, wird er automatisch erstellt.

- **Netzwerkordner**

  Dies ist ein Ordner, der per SMB/CIFS/DFS freigegeben ist.

Bestimmen Sie (per 'Durchsuchen') den gewünschten Freigabe-Ordner oder geben Sie den Pfad im folgenden Format manuell ein:

- Für SMB-/CIFS-Freigaben: `\\<Host-Name>\<Pfad>\` oder `smb://<Host-Name>/<Pfad>/`
- Für DFS-Freigabe: `\\<vollständiger DNS-Domain-Name>\<DFS-Stammverzeichnis>\<Pfad>`

  Beispielsweise: `\\beispiel.firma.com\freigabe\dateien`

Klicken Sie anschließend auf die Schaltfläche mit dem Pfeil. Spezifizieren Sie bei Aufforderung die Anmeldedaten (Benutzernamen, Kennwort), um auf den freigegebenen Ordner zugreifen zu können.

Backups zu einem Ordner mit anonymem Zugriff werden nicht unterstützt.

- **NFS-Ordner** (auf Maschinen verfügbar, die mit Linux oder macOS laufen)

  Bestimmen Sie (per 'Durchsuchen') den gewünschten NFS-Ordner oder geben Sie den Pfad im folgenden Format manuell ein:

  `nfs://<Host-Name>/<exportierter Ordner>:/<Unterordner>`

  Klicken Sie anschließend auf die Schaltfläche mit dem Pfeil.

  Ein NFS-Ordner, der per Kennwort geschützt ist, kann nicht als Backup-Ziel verwendet werden.

- **Secure Zone** (verfügbar, falls auf jeder der ausgewählten Maschinen eine Secure Zone verfügbar ist)

  Die 'Secure Zone' ist ein spezielles, geschütztes Volume (Partition), das auf einem Laufwerk der zu sichernden Maschine liegt. Dieses Volume bereits muss vor der Konfiguration eines entsprechenden Backups manuell erstellt worden sein. Weitere Informationen über die Erstellung einer Secure Zone, ihrer Vorteile und Beschränkungen finden Sie im Abschnitt 'Über die Secure Zone' (S. 46)'.

8.3.1 Über die Secure Zone

Die 'Secure Zone' ist ein spezielles, geschütztes Volume (Partition), das auf einem Laufwerk der zu sichernden Maschine liegt. Sie kann verwendet werden, um die Backups von Laufwerken oder Dateien der jeweiligen Maschine zu speichern.

Sollte das betreffende Laufwerk jedoch aufgrund eines physischen Fehlers ausfallen, gehen alle in der Secure Zone gespeicherten Backups verloren. Aus diesem Grund sollten Sie ein Backup nicht alleine nur in der Secure Zone speichern, sondern möglichst noch an einem oder sogar mehreren anderen Speicherorten. In Unternehmensumgebungen kann eine Secure Zone beispielsweise als praktischer Zwischenspeicher für Backups dienen, wenn ein normalerweise verwendeter Speicherort temporär nicht verfügbar ist (z.B. aufgrund einer fehlenden oder zu langsamen Daten- oder Netzwerkanbindung).

Wann ist die Verwendung einer Secure Zone sinnvoll?

Die Secure Zone:

- Ermöglicht es, bei einer Laufwerkswiederherstellung dasselbe Laufwerk als Recovery-Ziel zu verwenden, auf dem das entsprechende Laufwerk-Backup selbst gespeichert ist.
- Bietet eine kosteneffektive und praktische Methode, um Ihre Daten leicht gegen Software-Fehler, Virusangriffe und Bedienungsfehler abzusichern.
- Ermöglicht es, dass bei Backup- oder Recovery-Aktionen die gesicherten Daten nicht unbedingt auf einem anderen Medium liegen oder über eine Netzwerkverbindung bereitgestellt werden müssen. Diese Funktion ist besonders für Benutzer von Mobilgeräten nützlich.

- Eignet sich gut als primäres Backup-Ziel, wenn Backups per Replikation noch an anderen Speicherorten gesichert werden.

Beschränkungen

- Unter Mac OS X ist die Verwendung einer Secure Zone nicht möglich.
- Die Secure Zone kann nur als normale Partition auf einem Laufwerk vom Typ 'Basis' angelegt/verwendet werden. Sie kann weder auf einem dynamischen Datenträger liegen, noch als logisches Volume (einem per LVM verwalteten Volume) erstellt werden.
- Die Secure Zone verwendet FAT32 als Dateisystem. Da FAT32 eine Dateigrößenbeschränkung von 4 GB hat, werden größere Backups bei der Speicherung in der Secure Zone entsprechend aufgeteilt. Dies hat jedoch keinen Einfluss auf die Geschwindigkeit oder spätere Wiederherstellungsprozesse.
- Das Backup-Format 'Einzeldatei' (S. 206) wird von der Secure Zone nicht unterstützt. Wenn Sie einen Backup-Plan mit dem Backup-Schema '**Nur inkrementell (Einzeldatei)**' haben/erstellen und dort die Secure Zone als Backup-Ziel auswählen, wird das Backup-Schema automatisch auf **Wöchentlich vollständig, täglich inkrementell** geändert.

So erstellen Sie die Secure Zone

1. Entscheiden Sie sich, auf welchem Laufwerk Sie die Secure Zone erstellen wollen.
2. Starten Sie das Befehlszeilenwerkzeug und geben Sie den Befehl '**`acrocmd list disks`**' ein, damit Ihnen die Laufwerksnummern angezeigt werden.
3. Verwenden Sie den Befehl '**`create asz`**' des Werkzeugs '**`acrocmd`**'. Der Befehl versucht zuerst, den 'nicht zugeordneten' Speicherplatz des entsprechenden Laufwerks zu nutzen. Sollte es zu wenig 'nicht zugeordneten' Speicherplatz geben, wird stattdessen freier Speicherplatz von den spezifizierten Volumes verwendet. Weitere Details finden Sie im Abschnitt 'Wie die Erstellung der Secure Zone ein Laufwerk umwandelt'.

   Beispiele:

   - Es wird eine Secure Zone auf dem Laufwerk 1 der lokalen Maschine erstellt. Die Secure Zone wird mit einer bestimmten Standardgröße erstellt. Diese wird aus einem Durchschnittswert berechnet, der sich aus der maximal möglichen Größe (= komplett verfügbarer 'nicht zugeordneter' Speicherplatz) und der kleinstmöglichen Größe (ca. 50 MB) ergibt.

     ```
     acrocmd create asz --disk=1
     ```

   - Es wird eine kennwortgeschützte Secure Zone mit einer Größe von 100 GB auf Laufwerk 2 der lokalen Maschine erstellt. Sollte es zu wenig 'nicht zugeordneten' Speicherplatz geben, wird weiterer Speicherplatz vom zweiten Volume des Laufwerks übernommen.

     ```
     acrocmd create asz --disk=2 --volume=2-2 --asz_size=100gb --password=abc12345
     ```

   - Es wird eine Secure Zone mit einer Größe von 20 GB auf Laufwerk 1 einer Remote-Maschine erstellt.

     ```
     acrocmd create asz --host=192.168.1.2 --credentials=john,pass1 --disk=1
     --asz_size=20gb
     ```

   Eine ausführliche Beschreibung des Befehls '**`create asz`**' finden Sie in der 'Befehlszeilenreferenz'.

Wie die Erstellung der Secure Zone ein Laufwerk umwandelt

- Die Secure Zone wird immer am Ende des entsprechenden Laufwerks erstellt. Zur Berechnung des endgültigen Laufwerk-/Volume-Layouts wird das Programm zuerst solchen 'nicht zugeordneten' Speicherplatz verwenden, der am Ende des Laufwerks liegt (sofern verfügbar).

- Sollte der 'nicht zugeordnete' Speicherplatz am Ende des Laufwerks nicht ausreichen, jedoch zwischen den Volumes (Partitionen) noch weiterer 'nicht zugeordneter' Speicherplatz vorhanden sein, so werden die entsprechenden Volumes so verschoben, dass der benötigte 'nicht zugeordnete' Speicherplatz demjenigen am Endes des Laufwerkes hinzugefügt wird.
- Wenn der so zusammengestellte Speicherplatz immer noch nicht ausreicht, wird das Programm freien Speicherplatz von denjenigen Volumes entnehmen, die Sie dafür festgelegt haben. Die Größe dieser Volumes wird bei diesem Prozess entsprechend proportional verkleinert. Wenn dabei die Größe eines gesperrten Volumes geändert werden muss, ist ein Neustart erforderlich.
- Auf jedem Volume sollte jedoch eine gewisse Menge freier Speicherplatz vorhanden sein/bleiben, um weiter damit arbeiten zu können. Auf einem Volume mit Betriebssystem und Anwendungen müssen beispielsweise temporäre Dateien angelegt werden können. Ein Volume, dessen freier Speicherplatz weniger als 25 Prozent der Gesamtgröße des Volumes entspricht – oder durch den Prozess unter diesen Wert kommen würde – wird von der Software überhaupt nicht verkleinert. Nur wenn alle entsprechenden Volumes des Laufwerks mindestens 25 Prozent freien Speicherplatz haben, wird die Software mit der proportionalen Verkleinerung der Volumes fortfahren.

Daraus ergibt es sich, dass es normalerweise nicht ratsam ist, der Secure Zone die maximal mögliche Größe zuzuweisen. Am Ende haben Sie sonst auf keinem Volume mehr ausreichend freien Speicherplatz, was dazu führen kann, dass Betriebssystem und Anwendungen nicht mehr starten oder fehlerhaft arbeiten.

8.4 Planung

Planungen verwenden die Zeiteinstellungen (einschließlich der Zeitzone) des Betriebssystems, auf welchem der Agent installiert ist. Die Zeitzone des Agenten für VMware (Virtuelle Appliance) kann in der Benutzeroberfläche des Agenten (S. 28) konfiguriert werden.

Wenn beispielsweise in einem Backup-Plan eine Ausführung für 21:00 Uhr geplant ist und auf mehrere Maschinen in verschiedenen Zeitzonen angewendet wird, wird auf jeder Maschine das Backup um 21:00 Uhr der jeweiligen Ortszeit gestartet.

Die Planungsparameter hängen vom Backup-Ziel ab.

Wenn der Cloud Storage als Backup-Ziel dient

Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag. Sie können den Zeitpunkt bestimmen, an dem das Backup ausgeführt werden soll.

Wenn Sie die Backup-Häufigkeit ändern wollen, bewegen Sie einfach den entsprechenden grafischen Schieber – und spezifizieren Sie dann die gewünschte Backup-Planung.

Sie können die Backup-Planung so einstellen, dass die Ausführung nicht nach Zeit, sondern auf bestimmte Ereignisse hin erfolgt. Wählen Sie dazu in den Planungseinstellungen den gewünschten Ereignistyp aus. Weitere Informationen finden Sie im Abschnitt 'Planung nach Ereignissen (S. 50)'.

Wichtig: *Das erst Backup ist vom Typ 'vollständig' – was bedeutet, dass es die meiste Zeit benötigt. Alle nachfolgenden Backups sind inkrementell und benötigen deutlich weniger Zeit.*

Wenn andere Speicherorte als Backup-Ziel dienen

Sie können eines der vordefinierten Backup-Schemata verwenden oder ein benutzerdefiniertes Schema erstellen. Ein Backup-Schema ist derjenige Teil eines Backup-Plans, der die Backup-Planung und die Backup-Methode enthält.

Wählen Sie bei **Backup-Schema** eine der folgenden Möglichkeiten:

- [Nur für Laufwerk-Backups] **Nur inkrementell (Einzeldatei)**

  Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag. Sie können den Zeitpunkt bestimmen, an dem das Backup ausgeführt werden soll.

  Wenn Sie die Backup-Häufigkeit ändern wollen, bewegen Sie einfach den entsprechenden grafischen Schieber – und spezifizieren Sie dann die gewünschte Backup-Planung.

  Die Backups verwenden das neue Backup-Format 'Einzeldatei' (S. 206).

  Dieses Schema ist nicht verfügbar, wenn Sie die Secure Zone als Backup-Ziel verwenden.

- **Nur vollständig**

  Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag. Sie können den Zeitpunkt bestimmen, an dem das Backup ausgeführt werden soll.

  Wenn Sie die Backup-Häufigkeit ändern wollen, bewegen Sie einfach den entsprechenden grafischen Schieber – und spezifizieren Sie dann die gewünschte Backup-Planung.

  Alle Backups sind vom Typ 'vollständig'.

- **Wöchentlich vollständig, täglich inkrementell**

  Die standardmäßig Planung für die Durchführung von Backups ist 'täglich' und zwar von Montag bis Freitag. Sie können die Wochentage sowie den Zeitpunkt der Backup-Ausführung ändern.

  Einmal pro Woche wird ein Voll-Backup erstellt. Alle anderen Backups sind inkrementell. Der genaue Tag, an dem das Voll-Backup erstellt wird, wird durch die Option **Wöchentliches Backup** definiert (klicken Sie auf das Zahnradsymbol und dann auf die Befehle **Backup-Optionen** –> **Wöchentliches Backup**).

- **Benutzerdefiniert**

  Spezifizieren Sie die Planungen für die vollständigen, differentiellen und inkrementellen Backups.

  Beim Backup von SQL- und Exchange-Daten sowie eines Systemzustands ist die Option 'Differentielles Backup' nicht verfügbar.

Sie können jede Backup-Planung so konfigurieren, dass die Ausführung nicht nach Zeit, sondern auf bestimmte Ereignisse hin erfolgt. Wählen Sie dazu in den Planungseinstellungen den gewünschten Ereignistyp aus. Weitere Informationen finden Sie im Abschnitt 'Planung nach Ereignissen (S. 50)'.

Zusätzliche Planungsoptionen

Für jedes Ziel haben Sie folgende Einstellungsmöglichkeiten:

- Spezifizieren Sie die Backup-Startbedingungen, damit das geplante Backup nur ausgeführt wird, wenn bestimmte Bedingungen erfüllt sind. Weitere Informationen finden Sie im Abschnitt 'Startbedingungen (S. 52)'.
- Sie können einen Datumsbereich für die Planung festlegen, zu dem die entsprechende Operation ausgeführt werden soll. Aktivieren Sie das Kontrollkästchen **Den Plan in einem Datumsbereich ausführen** und spezifizieren Sie anschließend den gewünschten Datumsbereich.
- Sie können die Planung deaktivieren. Solange die Planung deaktiviert ist, werden die Aufbewahrungsregeln nicht angewendet – außer ein Backup wird manuell gestartet.
- Eine Verzögerung für den Ausführungszeitpunkt einführen. Der Verzögerungswert für jede Maschine wird zufällig bestimmt und reicht von Null bis einem maximalen, von Ihnen spezifizierten Wert. Sie können diese Einstellung bei Bedarf verwenden, wenn Sie mehrere Maschinen per Backup zu einem Netzwerkspeicherort sichern, um eine übermäßige Netzwerklast zu vermeiden.

  Klicken Sie auf das Zahnradsymbol und dann auf **Backup-Optionen** –> **Planung**. Wählen Sie die Option **Backup-Startzeiten in einem Zeitfenster verteilen** und spezifizieren Sie dann den

maximalen Verzögerungswert. Der Verzögerungswert für jede Maschinen wird bestimmt, wenn der Backup-Plan auf die Maschine angewendet wird – und er bleibt so lange gleich, bis Sie den Backup-Plan erneut bearbeiten und den maximalen Verzögerungswert ändern.

***Hinweis**: Diese Option ist standardmäßig aktiviert und der vorgegebene maximale Verzögerungswert beträgt 30 Minuten.*

- Klicken Sie auf **Mehr anzeigen**, um auf die folgenden Optionen zugreifen zu können.
  - **Task bei Neustart der Maschine ausführen, wenn die Maschine zur geplanten Zeit ausgeschaltet war** (standardmäßig deaktiviert)
  - **Standby- oder Ruhezustandsmodus während des Backups verhindern** standardmäßig aktiviert)

    Diese Option gilt nur für Maschinen, die unter Windows laufen.
  - **Aus Standby- oder Ruhezustandsmodus aufwecken, um ein geplantes Backup zu starten** (standardmäßig deaktiviert)

    Diese Option gilt nur für Maschinen, die unter Windows laufen. Diese Option ist nicht wirksam, wenn das Gerät ausgeschaltet ist, d.h. die Option macht keinen Gebrauch von der Wake-on-LAN-Funktionalität.

8.4.1 Planung nach Ereignissen

Wenn Sie einen Backup-Plan konfigurieren, können Sie in den Planungseinstellungen einen Ereignistyp festlegen. Das Backup wird gestartet, sobald das festgelegte Ereignisse eintritt.

Sie können eines der folgenden Ereignisse wählen:

- **Zeit seit letztem Backup**

  Dies ist die verstrichene Zeit seit Abschluss des letzten erfolgreichen Backups innerhalb desselben Backup-Plans. Sie können einen bestimmten Zeitraum definieren.
- **Wenn sich ein Benutzer am System anmeldet**

  Standardmäßig führt die Anmeldung eines beliebigen Benutzers dazu, dass das Backup ausgelöst wird. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.
- **Wenn sich ein Benutzer vom System abmeldet**

  Standardmäßig führt die Abmeldung eines beliebigen Benutzers dazu, dass das Backup ausgelöst wird. Sie können aber von 'Jeder Benutzer' zu einem bestimmten Benutzerkonto wechseln.

***Hinweis:** Das Backup wird nicht ausgeführt, wenn das System herunterfährt, weil 'Herunterfahren' nicht dasselbe wie 'Abmelden' ist.*

- **Beim Systemstart**
- **Beim Herunterfahren des Systems**
- **Bei Ereignis im Windows-Ereignisprotokoll**

  Sie müssen die Ereigniseigenschaften (S. 51) spezifizieren.

Die untere Tabelle zeigt die Ereignisse an, die für verschiedene Daten unter Windows, Linux und macOS verfügbar sind.

Backup-Quelle	Zeit seit letztem Backup	Wenn sich ein Benutzer am System anmeldet	Wenn sich ein Benutzer vom System abmeldet	Beim Systemstart	Beim Herunterfahren des Systems	Bei Ereignis im Windows-Ereignisprotokoll
Laufwerke/Volumes oder Dateien (physische Maschinen)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Laufwerke/Volumes (virtuelle Maschinen)	Windows, Linux	–	–	–	–	–
ESXi-Konfiguration	Windows, Linux	–	–	–	–	–
Office 365-Postfächer	Windows	–	–	–	–	Windows
Exchange-Datenbanken und -Postfächer	Windows	–	–	–	–	Windows
SQL-Datenbanken	Windows	–	–	–	–	Windows

8.4.1.1 Bei Ereignis im Windows-Ereignisprotokoll

Sie können ein Backup so planen, dass es automatisch gestartet wird, wenn ein bestimmtes Windows-Ereignis in eine der Protokolllisten **Anwendung**, **Sicherheit** oder **System** aufgenommen wird.

Angenommen, Sie wollen einen Backup-Plan aufstellen, der automatisch ein vollständiges Notfall-Backup Ihrer Daten durchführt, sobald Windows entdeckt, dass die Festplatte vor einem Ausfall steht.

Sie können die Ereignisse durchsuchen und Ereigniseigenschaften einsehen, wenn Sie das Snap-In **Ereignisanzeige** verwenden (welches auch über die **Computerverwaltung** verfügbar ist). Um die Windows-Protokolle für **Sicherheit** öffnen zu können, müssen Sie Mitglied in der Gruppe der **Administratoren** sein.

Ereigniseigenschaften

Protokollname

Spezifizieren Sie den Namen eines Protokolls. Wählen Sie den Namen einer Standard-Protokollliste (**Anwendung**, **Sicherheit** oder **System**) oder geben Sie den Namen einer Protokollliste ein – beispielsweise: **Microsoft Office Sitzungen**

Ereignisquelle

Spezifizieren Sie die Quelle des Ereignisses, welche typischerweise das Programm oder die Systemkomponente angibt, die das Ereignis verursachte – beispielsweise: **disk**

Ereignistyp

Geben Sie den Typ des Ereignisses an: **Fehler**, **Warnung**, **Informationen**, **Überprüfung erfolgreich** oder **Überprüfung fehlgeschlagen**.

Ereignis-Kennung:

Bezeichnet die Ereignis-Nummer, die üblicherweise die spezielle Art der Ereignisse unter Ereignissen derselben Quelle identifiziert.

So tritt z.B. ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **7** auf, wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, während ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **15** stattfindet, wenn eine Festplatte noch nicht zugriffsbereit ist.

Beispiel: 'Fehlerhafte Blöcke'-Notfall-Backup

Treten ein oder mehrere fehlerhafte Blöcke plötzlich auf einer Festplatte auf, so deutet das üblicherweise auf einen baldigen Ausfall der Festplatte hin. Angenommen, Sie wollen einen Backup-Plan erstellen, der die Daten einer Festplatte sichert, sobald eine solche Situation eintritt:

Wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, nimmt es ein Ereignis mit der Ereignis-Quelle **disk** und der Ereignis-Kennung **7** in die Protokollliste **System** auf; der Typ des Ereignisses ist **Fehler**.

Wenn Sie den Plan erstellen, geben Sie Folgendes im Bereich **Planung** ein bzw. wählen es aus:

- **Protokollname**: **System**
- **Ereignis-Quelle**: **Laufwerk**
- **Ereignis-Typ**: **Fehler**
- **Ereignis-Kennung**: **7**

Wichtig: *Um sicherzustellen, dass ein Backup trotz Vorhandensein von fehlerhaften Blöcken fertiggestellt wird, müssen Sie festlegen, dass das Backup die fehlerhaften Blöcke ignorieren soll. Zur Umsetzung gehen Sie in den* ***Backup-Optionen*** *zum Unterpunkt* ***Fehlerbehandlung*** *und aktivieren das Kontrollkästchen* ***Fehlerhafte Sektoren ignorieren****.*

8.4.2 Startbedingungen

Diese Einstellungen geben dem Scheduler mehr Flexibilität und ermöglichen es, ein Backup in Abhängigkeit von gewissen Bedingungen auszuführen. Bei mehreren Bedingungen müssen diese alle gleichzeitig erfüllt sein, damit das Backup starten kann. Startbedingungen gelten nicht, wenn ein Backup-Plan manuell gestartet wird.

Wenn Sie auf diese Einstellungen zugreifen wollen, klicken Sie auf **Mehr anzeigen**, wenn Sie die Planungseinstellungen für einen Backup-Plan konfigurieren.

Wie sich der Scheduler verhalten soll, wenn die Bedingung (oder eine von mehreren Bedingungen) nicht erfüllt ist, kann über die Backup-Option Backup-Startbedingungen (S. 67) definiert werden. Wenn die Bedingung(en) über einen zu langen Zeitraum nicht erfüllt wurde(n), könnte ein weiteres Aufschieben des Backups zu kritisch werden. Um zu bestimmen, was in so einem Fall passieren soll, können Sie ein Zeitintervall festlegen, nach dessen Ablauf des Backups auf jeden Fall ausgeführt wird – egal ob die Bedingung(en) erfüllt wurde(n) oder nicht.

Die untere Tabelle zeigt die Startbedingungen an, die für verschiedene Daten unter Windows, Linux und macOS verfügbar sind.

Backup-Quelle	Laufwerke/Volumes oder Dateien (physische Maschinen)	Laufwerke/Volumes (virtuelle Maschinen)	ESXi-Konfiguration	Office 365-Postfächer	Exchange-Datenbanken und -Postfächer	SQL-Datenbanken
Benutzer ist inaktiv (S. 53)	Windows	–	–	–	–	–

Der Host des Backup-Speicherorts ist verfügbar (S. 54)	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Benutzer sind abgemeldet (S. 54)	Windows	–	–	–	–	–
Entspricht dem Zeitintervall (S. 55)	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Akkubelastung senken (S. 55)	Windows	–	–	–	–	–
Nicht starten, wenn eine getaktete Verbindung besteht (S. 56)	Windows	–	–	–	–	–
Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht: (S. 56)	Windows	–	–	–	–	–
IP-Adresse des Gerätes überprüfen (S. 57)	Windows	–	–	–	–	–

8.4.2.1 Benutzer ist inaktiv

'Benutzer ist inaktiv' bedeutet, dass auf der Maschine ein Bildschirmschoner läuft oder die Maschine gesperrt ist.

Beispiel

Starte das Backup auf der Maschine täglich um 21:00 Uhr, möglichst, wenn der Benutzer inaktiv ist. Wenn der Benutzer um 23:00 Uhr immer noch aktiv, starte den Task trotzdem.

- Planung: Täglich, jeden Tag ausführen. Start um: **21:00**.
- Bedingung: **Benutzer ist inaktiv**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, **Backup trotzdem ausführen nach 2** Stunde(n).

Ergebnis:

(1) Wenn der Benutzer vor 21:00 Uhr inaktiv wird, so wird das Backup um 21:00 Uhr ausgeführt.

(2) Wenn der Benutzer zwischen 21:00 und 23:00 Uhr inaktiv wird, so wird das Backup sofort gestartet, nachdem der Benutzer inaktiv wurde.

(3) Wenn der Benutzer um 23 Uhr immer noch aktiv ist, wird das Backup um 23:00 Uhr gestartet.

8.4.2.2 Der Host des Backup-Speicherorts ist verfügbar

'Der Host des Backup-Speicherorts ist verfügbar' bedeutet, dass die Maschine, die den Backup-Zielspeicherort hostet, über das Netzwerk verfügbar ist.

Diese Bedinung gilt für Netzwerkordner, den Cloud Storage und Speicherorte, die von einem Storage Node verwaltet werden.

Diese Bedingung sagt nichts über die Verfügbarkeit des Speicherorts selbst aus – nur über die Verfügbarkeit des Hosts. Wenn beispielsweise der Host verfügbar ist, der Netzwerkordner auf diesem Host aber nicht freigegeben ist oder die Anmeldedaten für den Ordner nicht mehr gültig sind, trifft die Bedingung dennoch weiterhin zu.

Beispiel

Bestimmte Daten werden an jedem Arbeitstag um 21 Uhr zu einem Netzwerkordner gesichert. Wenn die Maschine, die den Ordner hostet, gerade nicht verfügbar ist (z.B. wegen Wartungsarbeiten), können Sie das Backup überspringen und bis zum nächsten geplanten Start am nächsten Werktag warten lassen.

- Planung: Täglich, Montag bis Freitag ausführen Start um: **21:00**.
- Bedingung: **Der Host des Backup-Speicherorts ist verfügbar**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und der Host verfügbar ist, wird das Backup sofort ausgeführt.

(2) Wenn es 21 Uhr wird, aber der Host nicht verfügbar ist, wird das Backup am nächsten Arbeitstag starten, sofern der Host dann verfügbar ist.

(3) Wenn der Host niemals an Werktagen um 21 Uhr verfügbar ist, wird das Backup niemals starten.

8.4.2.3 Benutzer sind abgemeldet

Ermöglicht Ihnen, ein Backup auf Warteposition zu setzen, bis sich alle Benutzer von Windows abgemeldet haben.

Beispiel

Starte das Backup jeden Freitag um 20:00 Uhr, möglichst, wenn alle Benutzer abgemeldet sind. Wenn einer der Benutzer um 23:00 Uhr immer noch angemeldet ist, starte das Backup trotzdem.

- Planung: Wöchentlich, immer freitags. Start um: **20:00**.
- Bedingung: **Benutzer sind abgemeldet**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, **Backup trotzdem ausführen nach 3** Stunde(n).

Ergebnis:

(1) Wenn alle Benutzer um 20:00 Uhr abgemeldet sind, wird das Backup um 20:00 Uhr gestartet.

(2) Wenn sich der letzte Benutzer zwischen 20:00 und 23:00 Uhr abmeldet, wird das Backup sofort ausgeführt, nachdem sich der Benutzer abgemeldet hat.

(3) Wenn ein Benutzer um 23 Uhr immer noch angemeldet ist, wird das Backup um 23:00 Uhr gestartet.

8.4.2.4 Entspricht dem Zeitintervall

Beschränkt die Startzeit für ein Backup auf ein bestimmtes Zeitintervall.

Beispiel

Eine Firma verwendet unterschiedliche Speicherorte auf demselben NAS-Gerät (Network Attached Storage), um Benutzerdaten und Server zu sichern. Ein Arbeitstag beginnt um 8:00 und endet um 17:00 Uhr. Benutzerdaten sollen jeweils gesichert werden, sobald ein Benutzer sich abmeldet – jedoch nicht vor 16:30 Uhr. Das Backup der Unternehmensserver erfolgt täglich um 23:00 Uhr. Die Benutzerdaten sollten daher alle möglichst vor diesem Zeitpunkt gesichert sein, damit genügend freie Netzwerkbandbreite verfügbar ist. Zur Kalkulation wird angenommen, dass das Backup der Daten eines Benutzers nicht mehr als je eine Stunde benötigt. Das letzte Benutzer-Backup sollte also spätestens um 22 Uhr starten. Daraus ergibt sich folgende Anweisung: Wenn ein Benutzer im vorgegebenen Zeitintervall noch angemeldet ist oder sich zu einer anderen Zeit abmeldet, werden die Daten des Benutzers nicht gesichert – also die Backup-Ausführung übersprungen.

- Ereignis: **Wenn sich ein Benutzer vom System abmeldet**. Spezifizieren Sie das Benutzerkonto: **Jeder Benutzer**.
- Bedingung: **Entspricht dem Zeitintervall**: von **16:30 Uhr** bis **22:00 Uhr**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

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

(2) Wenn sich der Benutzer zu einem anderen Zeitpunkt abmeldet, wird das Backup übersprungen.

8.4.2.5 Akkubelastung senken

Verhindert ein Backup, wenn das Gerät (Notebook oder Tablet) nicht an eine externe Stromquelle angeschlossen ist (sondern im Akkubetrieb läuft). In Abhängigkeit vom Wert der Option Backup-Startbedingungen (S. 67), wird das übersprungene Backup (nicht) gestartet, wenn das Gerät wieder an eine externe Stromquelle angeschlossen wird. Folgende Optionen sind verfügbar:

- **Nicht starten, wenn im Akkubetrieb**

  Ein Backup wird nur gestartet, wenn das Gerät mit einer externen Stromquelle verbunden ist.
- **Im Akkubetrieb starten, wenn Akkustand höher ist als:**

  Ein Backup wird gestartet, wenn das Gerät mit einer externen Stromquelle verbunden ist oder der Akkustand über dem spezifizierten Wert liegt.

Beispiel

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr. Wenn das Gerät nicht mit einer externen Stromquelle verbunden ist (beispielsweise, weil der Benutzer an einem späten Meeting teilnimmt), können Sie das Backup überspringen lassen, um Akkuladung zu sparen, und stattdessen darauf warten lassen, dass der Benutzer das Gerät wieder an eine externe Stromquelle anschließt.

- Planung: Täglich, Montag bis Freitag ausführen Start um: 21:00.
- Bedingung: **Akkubelastung senken**, **Nicht starten, wenn im Akkubetrieb**.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und das Gerät mit einer externen Stromquelle verbunden ist, wird das Backup sofort gestartet.

(2) Wenn es 21:00 Uhr wird und das Gerät im Akkubetrieb läuft, wird das Backup gestartet, sobald das Gerät wieder mit einer externen Stromquelle verbunden ist.

8.4.2.6 Nicht starten, wenn eine getaktete Verbindung besteht

Verhindert ein Backup (auch ein Backup zu einem lokalen Laufwerk), wenn das Gerät eine Internetverbindung verwendet, die von Windows als 'getaktet' eingestuft wird (z.B. eine Mobilfunkverbindung). Weitere Informationen über getaktete Verbindungen in Windows finden Sie in diesem Artikel:
https://support.microsoft.com/de-de/help/17452/windows-metered-internet-connections-faq.

Es gibt eine zusätzliche Maßnahme, um Backups über WLAN- bzw. Mobile Hotspots zu verhindern: Wenn Sie die Option **Nicht starten, wenn eine getaktete Verbindung besteht** aktivieren, wird automatisch auch die Option **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht** aktiviert. Folgende Netzwerknamen sind standardmäßig eingetragen: 'android', 'phone', 'mobile' und 'modem'. Sie können diese Namen aus der Liste löschen, wenn Sie auf das X-Zeichen klicken.

Beispiel

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr. Wenn das Gerät eine getaktete Internetverbindung verwendet (beispielsweise, weil der Benutzer auf einer Geschäftsreise ist), können Sie das Backup überspringen lassen, um Netzwerkverkehr/Gebühren zu sparen, und stattdessen auf den geplanten Start am nächsten Werktag warten lassen.

- Planung: Täglich, Montag bis Freitag ausführen Start um: 21:00.
- Bedingung: **Nicht starten, wenn eine getaktete Verbindung besteht**.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und das Gerät keine getaktete (aber eine andere) Internetverbindung verwendet, wird das Backup sofort gestartet.

(2) Wenn es 21:00 Uhr wird und das Gerät eine getaktete Internetverbindung verwendet, wird das Backup am nächsten Werktag gestartet.

(3) Wenn das Gerät werktags um 21:00 Uhr immer eine getaktete Internetverbindung verwendet, wird das Backup niemals gestartet.

8.4.2.7 Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht:

Verhindert ein Backup (auch ein Backup zu einem lokalen Laufwerk), wenn das Gerät mit einem der spezifizierten WLANs verbunden ist. Sie können als WLAN-Name die sogenannte SSID (Service Set Identifier) spezifizieren.

Die Sperre gilt für alle Netzwerke, die den angegebenen Namen als Teilzeichenfolge in ihrer SSID enthalten (unabhängig von Groß-/Kleinschreibung). Beispiel: wenn Sie 'phone' als Netzwerkname spezifizieren, wird das Backup nicht gestartet, wenn das Gerät mit einem WLAN mit einer der folgenden SSIDs verbunden ist: 'Peters iPhone', 'phone_wlan' oder 'mein_PHONE_wlan'.

Diese Bedingung ist nützlich, um Backups zu verhindern, wenn ein Gerät per WLAN-/Mobile Hotspot mit dem Internet verbunden ist.

Es gibt eine zusätzliche Maßnahme, um Backups über WLAN- bzw. Mobile Hotspots zu verhindern: Wenn Sie die Option **Nicht starten, wenn eine getaktete Verbindung besteht** aktivieren, wird automatisch auch die Option **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht** aktiviert. Folgende Netzwerknamen sind standardmäßig eingetragen: 'android', 'phone', 'mobile' und 'modem'. Sie können diese Namen aus der Liste löschen, wenn Sie auf das X-Zeichen klicken.

Beispiel

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr. Wenn das Gerät über einen WLAN-/Mobile Hotspot mit dem Internet verbunden ist (beispielsweise, weil das betreffende Notebook per Tethering-Modus mit einem Smartphone verbunden ist), können Sie das Backup überspringen lassen, um Netzwerkverkehr/Gebühren zu sparen, und stattdessen auf den geplanten Start am nächsten Werktag warten lassen.

- Planung: Täglich, Montag bis Freitag ausführen Start um: 21:00.
- Bedingung: **Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht**, **Netzwerkname**: `<SSID des Hotspot-Netzwerks>`.
- Backup-Startbedingungen: **Das geplante Backup überspringen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und die Maschine nicht mit dem spezifizierten Netzwerk verbunden ist, wird das Backup sofort gestartet.

(2) Wenn es 21:00 Uhr wird und die Maschine mit dem spezifizierten Netzwerk verbunden ist, wird das Backup am nächsten Werktag gestartet.

(3) Wenn die Maschine werktags um 21:00 Uhr immer mit dem spezifizierten Netzwerk verbunden ist, wird das Backup niemals gestartet.

8.4.2.8 IP-Adresse des Gerätes überprüfen

Verhindert ein Backup (auch ein Backup zu einem lokalen Laufwerk), wenn eine der Geräte-IP-Adressen innerhalb oder außerhalb des angegebenen IP-Adressbereichs liegt. Folgende Optionen sind verfügbar:

- **Starten, wenn außerhalb des IP-Bereichs**
- **Starten, wenn innerhalb des IP-Bereichs**

Sie können mit beiden Optionen mehrere Bereiche spezifizieren. Es werden nur IPv4-Adressen unterstützt.

Diese Bedingung ist nützlich, wenn sich ein Benutzer im Ausland befindet, um hohe Datenübertragungsgebühren zu vermeiden. Außerdem kann es helfen, Backups über eine VPN-Verbindung (Virtual Private Network) zu verhindern.

Beispiel

Das Backup erfolgt normalerweise immer werktags um 21:00 Uhr. Wenn sich ein Gerät per VPN-Tunnel mit dem Firmennetzwerk verbindet (z.B., weil der Benutzer von zu Hause aus arbeitet), können Sie das Backup überspringen lassen und darauf warten, bis der Benutzer mit seinem Gerät wieder im Büro ist.

- Planung: Täglich, Montag bis Freitag ausführen Start um: 21:00.

- Bedingung: **IP-Adresse des Gerätes überprüfen**, **Starten, wenn außerhalb des IP-Bereichs**, **Von**: `<Anfang des VPN-IP-Adressbereichs>`, **Bis**: `<Ende des VPN-IP-Adressbereichs>`.
- Backup-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und die IP-Adresse der Maschine nicht im spezifizierten Bereich liegt, wird das Backup sofort gestartet.

(2) Wenn es 21:00 Uhr wird und die IP-Adresse der Maschine im spezifizierten Bereich liegt, wird das Backup gestartet, sobald das Gerät eine 'nicht-VPN'-IP-Adresse erhält.

(3) Wenn die IP-Adresse der Maschine werktags um 21:00 Uhr immer im spezifizierten Bereich liegt, wird das Backup niemals gestartet.

8.5 Aufbewahrungsregeln

1. Klicken Sie auf **Aufbewahrungsdauer**.
2. Wählen Sie bei **Bereinigung** eine der folgenden Möglichkeiten:
   - **Nach Backup-Alter** (Standardeinstellung)

     Spezifizieren Sie, wie lange Backups, die von diesem Plan erstellt wurden, aufbewahrt werden sollen. Die Aufbewahrungsregeln werden standardmäßig für jedes Backup-Set (S. 206) separat spezifiziert. Um für alle Backups eine gemeinsame Regel verwenden zu können, müssen Sie auf **Auf einzelne Regel für alle Backup-Sets umschalten** klicken.
   - **Nach Backup-Anzahl**

     Spezifizieren Sie ein Maximum für die Anzahl an Backups, die aufbewahrt werden sollen.
   - **Backups unbegrenzt aufbewahren**

Was Sie zudem noch wissen sollten

- Wenn laut Backup-Schema und Backup-Format jedes Backup als separate Datei gespeichert wird, kann diese Datei solange nicht gelöscht werden, bis die 'Lebensdauer' aller von dieser Datei abhängigen (inkrementellen und differentiellen) Backups abgelaufen ist. Dies erfordert eine gewisse Menge an extra Speicherplatz, um solche Backups aufbewahren zu können, deren Löschung zurückgestellt wurde. Es kann daher auch vorkommen, dass die von Ihnen spezifizierten Werte für Backup-Alter, Backup-Größe und Backup-Anzahl überschritten werden.

  Diese Verhalten kann durch Verwendung der Backup-Option 'Backup-Konsolidierung (S. 65)' geändert werden.
- Aufbewahrungsregeln sind Bestandteil eines Backup-Plans. Sie werden nicht mehr auf die Backups einer Maschine angewendet, sobald der entsprechende Backup-Plan von dieser Maschine widerrufen oder gelöscht wird – oder die Maschine selbst aus dem Backup Service gelöscht wird. Wenn Sie die vom Backup-Plan erstellten Backups nicht mehr benötigen, können Sie diese löschen (wie im Abschnitt 'Backups löschen (S. 127)' beschrieben).

8.6 Replikation

Wenn Sie die Backup-Replikation aktivieren, wird jedes Backup direkt nach seiner Erstellung zu einem zweiten Speicherort kopiert. Falls frühere Backups nicht repliziert wurden (weil beispielsweise die Netzwerkverbindung verloren ging), wird die Software auch alle Backups replizieren, die nach der letzten erfolgreichen Replikation erschienen sind.

Replizierte Backups sind unabhängig von den Backups, die am ursprünglichen Speicherort verbleiben (und umgekehrt). Sie können Daten von jedem dieser Backups wiederherstellen, ohne Zugriff auf andere Speicherorte zu haben.

Anwendungsbeispiele

- **Verlässliches Disaster Recovery**

  Speichern Sie Ihre Backups sowohl 'on-site' (zur sofortigen Wiederherstellung) wie auch 'off-site' (um die Backups vor Ausfall des lokalen Speichers oder natürlichen Desastern zu schützen).
- **Den Cloud Storage nutzen, um Daten vor natürlichen Desastern zu schützen**

  Replizieren Sie die Backups zum Cloud Storage, indem lediglich geänderte Daten übertragen werden.
- **Nur die jüngsten Recovery-Punkte aufbewahren**

  Löschen Sie ältere Backups mithilfe von Aufbewahrungsregeln von einem schnellen Speicher, um den teuren Speicherplatz nicht übermäßig zu beanspruchen.

Unterstützte Speicherorte

Sie können ein Backup *von* jedem der nachfolgenden Speicherorte (als Quelle) replizieren:

- Einem lokalen Ordner
- Einem Netzwerkordner
- Einer Secure Zone

Sie können ein Backup *zu* jedem der nachfolgenden Speicherorte (als Ziel) replizieren:

- Einem lokalen Ordner
- Einem Netzwerkordner
- Dem Cloud Storage

So aktivieren Sie eine Backup-Replikation

1. Aktivieren Sie im Backup-Plan-Fensterbereich den Schalter **Backups replizieren**.

   Der Schalter wird nur dann angezeigt, wenn der unter **Backup-Ziel** gewählte Speicherort eine Replikation auch unterstützt.
2. Spezifizieren Sie bei **Replikationsziel** einen geeigneten Speicherort (wie im Abschnitt 'Ein Ziel auswählen (S. 45)' beschrieben).
3. Spezifizieren Sie bei **Aufbewahrungsdauer** die gewünschte Aufbewahrungsregel (wie im Abschnitt 'Aufbewahrungsregeln (S. 58)' beschrieben).

8.7 Verschlüsselung

Wir empfehlen Ihnen, alle Backups zu verschlüsseln, die im Cloud Storage gespeichert werden – insbesondere, wenn Ihr Unternehmen gesetzlichen Bestimmungen (zum Datenschutz u. Ä.) unterliegt.

Wichtig: *Falls Sie Ihr Kennwort verlieren, gibt es keine Möglichkeit, Ihre verschlüsselten Backups wiederherzustellen!*

Verschlüsselung in einem Backup-Plan

Die Verschlüsselung wird aktiviert, wenn Sie beim Erstellen eines Backup-Plans die entsprechenden Verschlüsselungseinstellungen spezifizieren. Nachdem ein Backup-Plan angewendet wurde, können die Verschlüsselungseinstellungen nicht mehr geändert werden. Erstellen Sie einen neuen Backup-Plan, wenn Sie andere Verschlüsselungseinstellungen verwenden wollen.

So spezifizieren Sie die Verschlüsselungseinstellungen ein einem Backup-Plan

1. Aktivieren Sie im Backup-Plan-Fensterbereich den Schalter **Verschlüsselung**.
2. Spezifizieren und bestätigen Sie das Verschlüsselungskennwort.
3. Wählen Sie einen der folgenden Verschlüsselungsalgorithmen:
   - **AES 128** – die Backups werden nach dem Advanced Encryption Standard (AES) und mit einer Tiefe von 128 Bit verschlüsselt.
   - **AES 192** – die Backups werden mit dem AES-Algorithmus und einer Tiefe von 192-Bit verschlüsselt.
   - **AES 256** – die Backups werden mit dem AES-Algorithmus und einer Tiefe von 256-Bit verschlüsselt.
4. Klicken Sie auf **OK**.

Verschlüsselung als Eigenschaft einer Maschine

Diese Option ist für Administratoren gedacht, die die Backups vieler Maschinen handhaben müssen. Falls Sie ein einzigartiges Verschlüsselungskennwort für jede Maschine benötigen oder die Verschlüsselung von Backups unabhängig von den Verschlüsselungseinstellungen des Backup-Plans erzwingen wollen, müssen Sie die Verschlüsselungseinstellungen individuell auf jeder Maschine speichern. Die Backups werden mit dem AES-Algorithmus und einer Tiefe von 256-Bit verschlüsselt.

Das Speichern von Verschlüsselungseinstellungen auf einer Maschine beeinflusst die Backup-Pläne folgendermaßen:

- **Bei Backup-Plänen, die bereits auf die Maschine angewendet wurden.** Wenn die Verschlüsselungseinstellungen in einem Backup-Plan anders sind, wird das Backup fehlschlagen.
- **Bei Backup-Plänen, die später auf die Maschine angewendet werden.** Die auf einer Maschine gespeicherten Verschlüsselungseinstellungen überschreiben die Verschlüsselungseinstellungen eines Backup-Plans. Jedes Backup wird verschlüsselt – selbst dann, wenn die Verschlüsselung in den Backup-Plan-Einstellungen deaktiviert ist.

Diese Option kann auf einer Maschine verwendet werden, auf welcher der Agent für VMware läuft. Sie sollten jedoch vorsichtig sein, wenn Sie mehr als einen Agenten für VMware mit demselben vCenter Server verbunden haben. Sie müssen dieselben Verschlüsselungseinstellungen für alle Agenten verwenden, weil es eine Art Lastverteilung (Load Balancing) zwischen ihnen gibt.

Nachdem die Verschlüsselungseinstellungen gespeichert wurden, können diese wie unten beschrieben geändert oder zurückgesetzt werden.

Wichtig: *Sollte ein Backup-Plan, der auf dieser Maschine ausgeführt wird, bereits Backups erstellt haben, so wird eine Änderung der Verschlüsselungseinstellungen bewirken, dass dieser Plan fehlschlagen wird. Wenn Sie weitere Backups erstellen wollen, müssen Sie daher einen neuen Backup-Plan erstellen.*

So speichern Sie die Verschlüsselungseinstellungen auf einer Maschine

1. Melden Sie sich als Administrator (unter Windows) oder als Benutzer 'root' (unter Linux) an.
2. Führen Sie folgendes Skript aus:
   - Unter Windows: `<Installationspfad>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<Verschlüsselungskennwort>`

     Wobei `<Installationspfad>` für den Installationspfad des Backup Agenten steht. Standardmäßig ist dies der Ordner '**%ProgramFiles%\BackupClient**'.
   - Unter Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<Verschlüsselungskennwort>`

So setzen Sie die Verschlüsselungseinstellungen auf einer Maschine zurück

1. Melden Sie sich als Administrator (unter Windows) oder als Benutzer 'root' (unter Linux) an.
2. Führen Sie folgendes Skript aus:
   - Unter Windows: `<Installationspfad>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     Wobei `<Installationspfad>` für den Installationspfad des Backup Agenten steht. Standardmäßig ist dies der Ordner '**%ProgramFiles%\BackupClient**'.
   - Unter Linux: **/usr/sbin/acropsh -m manage_creds --reset**

So ändern Sie die Verschlüsselungseinstellungen über den Backup Monitor

1. Melden Sie sich bei Windows oder macOS als Administrator an.
2. Klicken Sie im Infobereich der Taskleiste (Windows) oder in der Menüleiste (macOS) auf das Symbol für den **Backup Monitor**.
3. Klicken Sie auf das Zahnradsymbol.
4. Klicken Sie auf die Option **Verschlüsselung**.
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie den Befehl **Spezifisches Kennwort für diese Maschine festlegen**. Spezifizieren und bestätigen Sie das Verschlüsselungskennwort.
   - Wählen Sie den Befehl **Verschlüsselungseinstellungen des Backup-Plans verwenden**.
6. Klicken Sie auf **OK**.

Wie die Verschlüsselung arbeitet

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 der Backups benötigen, aber desto sicherer sind auch die Daten.

Der Codierungsschlüssel ist dann per AES-256 verschlüsselt, wobei ein SHA-256-Hash-Wert des Kennworts als Schlüssel dient. Das Kennwort selbst wird weder auf dem Laufwerk noch in den Backups gespeichert; stattdessen wird der Kennwort-Hash zur Verifikation verwendet. Mit dieser zweistufigen Methode sind die gesicherten Daten vor unberechtigtem Zugriff geschützt – ein verlorenes Kennwort kann daher auch nicht wiederhergestellt werden.

8.8 Ein Backup manuell starten

1. Wählen Sie eine Maschine aus, die über mindestens einen auf sie angewendeten Backup-Plan verfügt.
2. Klicken Sie auf **Backup**.
3. Sollten mehr als ein Backup-Plan auf die Maschine angewendet werden, dann wählen Sie den gewünschten Backup-Plan aus.
4. Klicken Sie im Backup-Plan-Fensterbereich auf **Jetzt ausführen**.

Der Backup-Fortschritt für die Maschine wird in der Spalte **Status** angezeigt.

8.9 Backup-Optionen

Wenn Sie die Backup-Optionen ändern wollen, klicken Sie auf das Zahnradsymbol neben dem Backup-Plan-Namen und dann auf das Element **Backup-Optionen**.

Welche Backup-Optionen verfügbar sind

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

- Der Umgebung, in welcher der Agent arbeitet (Windows, Linux, macOS).
- Der Art der zu sichernden Daten (Laufwerke, Dateien, virtuelle Maschinen, Applikationsdaten).
- Dem Backup-Ziel (Cloud Storage, lokaler Ordner, Netzwerkordner).

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

	Backup auf Laufwerksebene			**Backup auf Dateiebene**			**Virtuelle Maschinen**			**SQL und Exchange**
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Alarmmeldungen (S. 64)	+	+	+	+	+	+	+	+	+	+
Backup-Konsolidierung (S. 65)	+	+	+	+	+	+	+	+	+	-
Backup-Format (S. 66)	+	+	+	+	+	+	+	+	+	+
Backup-Validierung (S. 67)	+	+	+	+	+	+	+	+	+	+
Backup-Startbedingungen (S. 67)	+	+	-	+	+	-	+	+	+	+
CBT (Changed Block Tracking) (S. 68)	+	-	-	-	-	-	+	+	-	-
Komprimierungsgrad (S. 68)	+	+	+	+	+	+	+	+	+	+
Fehlerbehandlung (S. 69)										
Erneut versuchen, wenn ein Fehler auftritt	+	+	+	+	+	+	+	+	+	+
Während der Durchführung keine Meldungen bzw. Dialoge anzeigen (Stiller Modus)	+	+	+	+	+	+	+	+	+	+

	Backup auf Laufwerksebene			Backup auf Dateiebene			Virtuelle Maschinen			SQL und Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Fehlerhafte Sektoren ignorieren	+	+	+	+	+	+	+	+	+	-
Erneut versuchen, wenn bei der VM-Snapshot-Erstellung ein Fehler auftritt	-	-	-	-	-	-	+	+	+	-
Schnelles inkrementelles/differentielles Backup (S. 70)	+	+	+	-	-	-	-	-	-	-
Snapshot für Datei-Backups (S. 72)	-	-	-	+	+	+	-	-	-	-
Dateifilter (S. 70)	+	+	+	+	+	+	+	+	+	-
Protokollabschneidung (S. 72)	-	-	-	-	-	-	+	+	-	Nur SQL
LVM-Snapshot-Erfassung (S. 72)	-	+	-	-	-	-	-	-	-	-
Mount-Punkte (S. 73)	-	-	-	+	-	-	-	-	-	-
Multi-Volume-Snapshot (S. 74)	+	+	-	+	+	-	-	-	-	-
Performance (S. 74)	+	+	+	+	+	+	+	+	+	+
Physischer Datenversand (S. 75)	+	+	+	+	+	+	+	+	+	-
Vor-/Nach-Befehle (S. 76)	+	+	+	+	+	+	+	+	+	+
Befehle vor/nach der Datenerfassung (S. 78)	+	+	+	+	+	+	-	-	-	+
Planung (S. 80)										

	Backup auf Laufwerksebene			Backup auf Dateiebene			Virtuelle Maschinen			SQL und Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Startzeiten in einem Zeitfenster verteilen	+	+	+	+	+	+	+	+	+	+
Die Anzahl gleichzeitig ausgeführter Backups begrenzen	-	-	-	-	-	-	+	+	+	-
Sektor-für-Sektor-Backup (S. 80)	+	+	-	-	-	-	+	+	+	-
Aufteilen (S. 81)	+	+	+	+	+	+	+	+	+	+
Task-Fehlerbehandlung (S. 81)	+	+	+	+	+	+	+	+	+	+
VSS (Volume Shadow Copy Service) (S. 81)	+	-	-	+	-	-	-	+	-	+
VSS (Volume Shadow Copy Service) für virtuelle Maschinen (S. 82)	-	-	-	-	-	-	+	+	-	-
Wöchentliche Backups (S. 83)	+	+	+	+	+	+	+	+	+	+
Windows-Ereignisprotokoll (S. 83)	+	-	-	+	-	-	+	+	-	+

8.9.1 Alarmmeldungen

Keine erfolgreichen Backups für eine spezifizierte Anzahl aufeinanderfolgender Tage

Die Voreinstellung ist: **Deaktiviert**.

Diese Option bestimmt, ob eine Alarmmeldung generiert wird, wenn der Backup-Plan innerhalb des spezifizierten Zeitraums kein erfolgreiches Backup durchgeführt hat. Zusätzlich zu fehlgeschlagenen Backups zählt die Software hier auch Backups, die nicht planungsgemäß ausgeführt wurden (verpasste Backups).

Die Alarmmeldungen werden pro Maschine generiert und in der Registerkarte **Alarmmeldungen** angezeigt.

Sie können spezifizieren, ab wie vielen aufeinanderfolgenden Tagen ohne Backups eine Alarmmeldung generiert wird.

8.9.2 Backup-Konsolidierung

Diese Option bestimmt, ob Backups während einer Bereinigung konsolidiert oder komplette Backup-Ketten gelöscht werden sollen.

Die Voreinstellung ist: **Deaktiviert**.

Konsolidierung ist ein Prozess, bei dem zwei oder mehr aufeinander folgende, abhängige Backups zu einem einzelnen Backup kombiniert werden.

Eine Aktivierung dieser Option bewirkt, dass ein Backup, welches während einer Bereinigung gelöscht werden soll, zusammen mit dem nächsten abhängigen Backup (inkrementell oder differentiell) konsolidiert wird.

Bei deaktivierter Option wird das Backup solange aufbewahrt, bis alle abhängigen Backups gelöscht werden. Dieser hilft, die potenziell zeitaufwendige Konsolidierung zu vermeiden, benötigt aber extra Speicherplatz für von der Löschung zurückgestellte Backups. Das Alter oder die Anzahl der Backups kann daher die Werte überschreiten, die in den entsprechenden Aufbewahrungsregeln spezifiziert wurden.

Wichtig: *Beachten Sie, dass eine Konsolidierung nur eine bestimmte Art der Datenbereinigung ist, jedoch keine Alternative zu einer richtigen Löschung ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup vorlagen, die jedoch im aufbewahrten inkrementellen oder differentiellen Backup fehlten.*

Diese Option ist *nicht* wirksam, wenn einer der folgenden Umstände zutrifft:

- Der Cloud-Storage wird als Backup-Ziel verwendet.
- Als Backup-Schema wurde **Nur inkrementell (Einzeldatei)** festgelegt.
- Als Backup-Format (S. 66) wurde '**Version 12**' festgelegt.

Backups, die im Cloud Storage gespeichert sind, sowie Backups vom Typ 'Einzeldatei' (mit dem Backup-Format Version 11 oder Version 12) werden immer konsolidiert, da ihre innere Struktur eine schnelle und einfache Konsolidierung ermöglicht.

Wenn jedoch das Backup-Format 'Version 12' verwendet wird und mehrere Backup-Ketten vorliegen (jede Kette wird als separate .tibx-Datei gespeichert), dann funktioniert die Konsolidierung nur innerhalb der letzten Kette. Alle anderen Ketten werden als Ganzes gelöscht, mit Ausnahme der ersten Kette, die auf minimale Größe verkleinert wird, um die Metainformationen zu bewahren (ca. 12 KB). Diese Metainformationen sind erforderlich, um bei gleichzeitigen Lese- und Schreibaktionen für Datenkonsistenz zu sorgen. Die in diesen Ketten enthaltenen Backups verschwinden aus der Benutzeroberfläche, sobald die Aufbewahrungsregel angewendet wird. Diese Backups existieren jedoch physisch solange weiter, bis die gesamte Kette gelöscht wurde.

In allen anderen Fällen werden Backups, deren Löschung verschoben wurde, in der Benutzeroberfläche mit einem Mülleimer-Symbol () gekennzeichnet. Wenn Sie ein solches Backup löschen, indem Sie auf das X-Symbol klicken, wird die Konsolidierung durchgeführt.

8.9.3 Backup-Format

Die Option bestimmt das Format der Backups, die vom Backup-Plan erstellt werden. Sie können zwischen zwei Formaten wählen: dem neuen Format (**Version 12**), welches für schnelleres Backup und Recovery entwickelt wurde – und dem herkömmlichen Format (Legacy-Format, **Version 11**), welches aus Kompatibilitätsgründen und für besondere Einsatzzwecke bewahrt wurde.

Diese Option ist für Backups von Websites, Office 365-Daten und G Suite-Daten *nicht* verfügbar. Diese Backups werden immer im neuen Format erstellt.

Die Voreinstellung ist: **Automatische Auswahl**.

Sie können eine der folgenden Optionen wählen:

- **Automatische Auswahl**

  Version 12 wird verwendet, außer der Backup-Plan muss bestehende Backups erweitern, die mit früheren Produktversionen erstellt wurden.
- **Version 12**

  Ein für die meisten Fälle empfehlenswertes, neues Format für schnelles Backup und Recovery. Jede Backup-Kette (ein vollständiges oder differentielles Backup und alle davon abhängigen inkrementellen Backups) wird als einzelne .tibx-Datei gespeichert.
- **Version 11**

  Ein früheres Format ('Legacy-Format'), das in neuen Backup-Plänen verwendet werden kann, um bestehende Backups zu erweitern, die mit früheren Produktversionen erstellt wurden.

  Verwenden Sie dieses Format (mit jedem Backup-Schema – außer mit **Nur inkrementell (Einzeldatei)**) außerdem, wenn Sie vollständige, inkrementelle und differentielle Backups als separate Dateien vorliegen haben wollen.

Backup-Format und Backup-Dateien

Bei Backup-Speicherorten, die mit einem Datei-Manager durchsucht werden können (wie etwa lokale Ordner oder Netzwerklaufwerke), bestimmt das Backup-Format die Anzahl der Dateien und ihrer Erweiterung. Die folgende Tabelle listet die Dateien auf, die pro Maschine oder Postfach erstellt werden können.

	Nur inkrementell (Einzeldatei)	**Andere Backup-Schemata**
Backup-Format **Version 11**	Eine .tib-Datei und eine .xml-Metadaten-Datei	Mehrere .tib-Dateien und eine .xml-Metadaten-Datei (traditionelles Format)
Backup-Format **Version 12**	Eine .tibx-Datei pro Backup-Kette (ein vollständiges oder differentielles Backup und alle davon abhängigen inkrementellen Backups)	

Das Backup-Format ändern

Bei Laufwerk-Backups kann das Backup-Format nicht mehr geändert werden, nachdem der Backup-Plan angewendet wurde.

Bei Datei- und Datenbank-Backups kann das Backup-Format von **Version 11** auf **Version 12** geändert werden, nachdem der Backup-Plan angewendet wurde. Die umgekehrte Aktion ist jedoch nicht möglich.

Wenn Sie das Backup-Format ändern:

- Das nächste ausgeführte Backup wird ein Voll-Backup sein.

- Bei Backup-Speicherorten, die mit einem Datei-Manager durchsucht werden können (wie etwa lokale Ordner oder Netzwerklaufwerke), wird eine neue .tibx-Datei erstellt. Die neue Datei übernimmt den Namen der Originaldatei, jedoch um das Suffix **_v12A** erweitert.
- Aufbewahrungsregeln und Replikationen werden nur auf neue Backups angewendet.
- Die alten Backups werden nicht gelöscht, sondern bleiben über die Registerkarte **Backups** weiter verfügbar. Sie können Sie jedoch manuell löschen.
- Die alten Cloud Backups werden nicht auf die Quota **Cloud Storage** angerechnet.
- Die alten lokalen Backups werden solange auf die Quota **Lokales Backup** angerechnet, bis diese von Ihnen gelöscht werden.

8.9.4 Backup-Validierung

Validierung ist eine Aktion, mit der geprüft wird, ob es grundsätzlich möglich ist, dass Daten, die in einem Backup gespeichert sind, wiederhergestellt werden können. Wenn diese Option aktiviert ist, wird jedes von einem entsprechenden Backup-Plan erstellte Backup direkt nach seiner Erstellung validiert.

Die Voreinstellung ist: **Deaktiviert**.

Bei einer Validierung wird für jeden Datenblock, der aus dem entsprechenden Backup wiederhergestellt werden kann, eine Prüfsumme berechnet. Es gibt nur eine Ausnahmen, nämlich die Validierung von Datei-Backups, die im Cloud Storage gespeichert sind. Diese Backups werden validiert, indem die Konsistenz der im Backup gespeicherten Metadaten überprüft wird.

Eine Validierung ist ein zeitaufwendiger Prozess – das gilt auch für inkrementelle oder differentielle Backups, die ja normalerweise kleiner sind. Hintergrund ist, dass bei einer Validierungsaktion nicht nur diejenigen Daten überprüft werden, die in einem einzelnen Backup direkt gespeicherten sind, sondern auch alle weiteren Daten, die von diesem Backup ausgehend wiederherstellbar sind, weil dieses zu einer Backup-Kette gehört. Daher muss auch auf früher erstellte Backups (in einer Backup-Kette) zugegriffen werden können.

Obwohl eine erfolgreiche Validierung bedeutet, dass eine Wiederherstellung mit hoher Wahrscheinlichkeit möglich sein wird, werden nicht alle Faktoren überprüft, die den zukünftigen Recovery-Prozess beeinflussen können. Wenn Sie ein Betriebssystem per Backup gesichert haben und dieses zusätzlich testen wollen, empfehlen wir Ihnen, dass Sie mit einem Boot-Medium eine Testwiederherstellung auf ein freies, überzähliges Laufwerk durchführen. In einer ESXi- oder Hyper-V-Umgebungen können Sie eine entsprechende virtuelle Maschine auch direkt aus dem Backup heraus ausführen (S. 184).

8.9.5 Backup-Startbedingungen

Diese Option gilt nur für Windows- und Linux-Betriebssysteme.

Diese Option bestimmt, wie sich das Programm verhalten soll, wenn ein Backup eigentlich starten sollte (weil der vorgegebene Zeitpunkt erreicht ist oder das spezifizierte Startereignis eingetreten ist), die festgelegte Bedingung (oder eine von mehreren Bedingungen) jedoch nicht erfüllt ist. Weitere Informationen dazu finden Sie im Abschnitt 'Startbedingungen (S. 52)'.

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

Warten, bis die Bedingungen erfüllt sind

Mit dieser Einstellung beginnt der Scheduler, die Bedingungen zu überwachen, und startet das Backup, sobald die Bedingungen erfüllt sind. Wenn die Bedingungen nie erfüllt werden, wird das Backup auch nie gestartet.

Wenn die Bedingungen über einen zu langen Zeitraum nicht erfüllt wurden, könnte ein weiteres Aufschieben des Backups zu kritisch werden. Um zu bestimmen, was in so einem Fall passieren soll, können Sie ein Zeitintervall festlegen, nach dessen Ablauf des Backups auf jeden Fall ausgeführt wird – egal ob die Bedingung(en) erfüllt wurde(n) oder nicht. Aktivieren Sie das Kontrollkästchen **Backup trotzdem ausführen nach** und spezifizieren Sie den gewünschten Zeitraum. Das Backup wird gestartet, sobald die Bedingungen erfüllt sind ODER die festgelegte maximale Zeitverzögerung abgelaufen ist – je nachdem, welche dieser Vorgaben als erstes gültig wird.

Das geplante Backup überspringen

Ein Backup aufzuschieben kann unter gewissen Umständen inakzeptabel sein. Beispielsweise, wenn Sie Daten unbedingt zu einem ganz bestimmten Zeitpunkt sichern müssen. In so einem Fall kann es sinnvoll sein, ein Backup zu überspringen, statt darauf zu warten, dass Bedingungen erfüllt sind (insbesondere wenn die Backups relativ häufig durchgeführt werden).

8.9.6 CBT (Changed Block Tracking)

Diese Option gilt nur für Laufwerk-Backups von virtuellen Maschinen und von physischen Maschinen, die unter Windows laufen. Sie gilt außerdem auch für Backups von Microsoft SQL Server- und Microsoft Exchange Server-Datenbanken.

Voreinstellung ist: **Aktiviert**.

Diese Option bestimmt, ob CBT (Changed Block Tracking) verwendet werden soll, wenn ein inkrementelles oder differentielles Backup durchgeführt wird.

CBT ist eine Technologie, mit der Backup-Prozesse beschleunigt werden können. Dabei werden entsprechende Laufwerke oder Datenbanken kontinuierlich auf Blockebene überwacht, ob vorhandene Dateninhalte geändert wurden. Wenn dann ein Backup durchgeführt wird, können die zuvor bereits ermittelten Änderungen direkt im Backup gespeichert werden.

8.9.7 Komprimierungsgrad

Diese Option definiert den Grad der Komprimierung für die zu sichernden Daten. Folgende Stufen sind verfügbar: **Ohne**, **Normal**, **Hoch**.

Die Voreinstellung ist: **Normal**.

Ein höherer Komprimierungsgrad verlängert den Backup-Prozess, verkleinert aber den benötigten Backup-Speicherplatz.

Der optimale Komprimierungsgrad hängt von der Art der Daten ab, die gesichert werden sollen. So wird z.B. eine maximale Komprimierung die Größe einer Backup-Datei nicht wesentlich beeinflussen, wenn Dateien im Backup erfasst werden, die bereits stark komprimiert sind (wie .jpg-, .pdf- oder .mp3-Dateien). Andere Typen, wie z.B. doc- oder xls-Dateien, werden dagegen stark komprimiert.

8.9.8 Fehlerbehandlung

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

Erneut versuchen, wenn ein Fehler auftritt

Die Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 30. Abstand zwischen den Versuchen: 30 Sekunden.**

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

Wenn der Speicherort des Backups im Netzwerk nicht verfügbar/erreichbar ist, wird das Programm versuchen, den Ort alle 30 Sekunden erneut zu erreichen – jedoch nicht mehr als 30 Mal. Die Versuche werden aufgegeben, wenn entweder die Verbindung gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

Cloud Storage

Wenn Sie den Cloud Storage als Backup-Ziel auswählen, wird der Optionswert automatisch auf **Aktiviert** gesetzt. **Anzahl der Versuche: 300**. **Abstand zwischen den Versuchen: 30 Sekunden.**

Die tatsächliche Anzahl der Versuche ist in diesem Fall unbegrenzt. Die Zeitüberschreitung (Timeout), bevor das Backup als fehlgeschlagen gilt, wird dagegen folgendermaßen berechnet: (300 Sekunden + **Abstand zwischen den Versuchen**) * (**Anzahl der Versuche** + 1).

Beispiele:

- Mit den Standardwerten wird das Backup nach folgender Zeit fehlschlagen: 99330 Sekunden bzw. ca. 27,6 Stunden = (300 Sekunden + 30 Sekunden) * (300 + 1).
- Wenn Sie die **Anzahl der Versuche** auf 1 und den **Abstand zwischen den Versuchen** auf 1 Sekunde festlegen, wird das Backup nach folgender Zeit fehlschlagen: 602 Sekunden bzw. ca. 10 Minuten = (300 Sekunden + 1 Sekunde) * (1 + 1).

Wenn der berechnete Timeout-Wert 30 Minuten überschreitet und die Datenübertragung noch nicht gestartet wurde, wird die tatsächliche Zeitüberschreitung auf 30 Minuten gesetzt.

Während der Durchführung keine Meldungen bzw. Dialoge anzeigen (Stiller Modus)

Die Voreinstellung ist: **Aktiviert**.

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

Fehlerhafte Sektoren ignorieren

Die Voreinstellung ist: **Deaktiviert**.

Ist diese Option deaktiviert, dann wird der Backup-Aktivität jedes Mal der Status **Benutzereingriff erforderlich** zugewiesen, wenn das Programm auf einen fehlerhaften Sektor trifft. Wenn Sie z.B. vorhaben, die Informationen von einer 'sterbenden' Festplatte zu retten, aktivieren Sie diese

Funktion. Die restlichen Daten werden in diesem Fall noch gesichert und Sie werden das entstandene Laufwerk-Backup mounten und die noch gültigen Daten auf ein anderes Laufwerk kopieren können.

Erneut versuchen, wenn bei der VM-Snapshot-Erstellung ein Fehler auftritt

Die Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 3. Abstand zwischen den Versuchen: 5 Minuten.**

Wenn die Snapshot-Erfassung einer virtuellen Maschine fehlschlägt, versucht das Programm, die Aktion zu wiederholen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

8.9.9 Schnelles inkrementelles/differentielles Backup

Diese Option gilt für inkrementelle und differentielle Backups auf Dateiebene.

Die Voreinstellung ist: **Aktiviert**.

Inkrementelle oder differentielle Backups erfassen nur jeweils geänderte Daten. Um das Backup-Verfahren zu beschleunigen, ermittelt das Programm, ob eine Datei geändert wurde oder nicht – und zwar anhand von Dateigröße und Zeitstempel der jeweils letzten Änderung. Ist diese Funktion ausgeschaltet, so vergleicht das Programm die Quelldateien und die Dateien, die bereits im Backup gespeichert sind, stattdessen anhand des kompletten Dateiinhaltes.

8.9.10 Dateifilter

Dateifilter definieren, welche Dateien und Ordner während des Backup-Prozesses übersprungen werden sollen.

Dateifilter stehen, sofern nicht anders angegeben, für Backups auf Laufwerk- und Dateiebene zur Verfügung.

So aktivieren Sie Dateifilter

1. Wählen Sie die Daten für das Backup aus.
2. Klicken Sie neben dem Namen des Backup-Plans auf das Zahnradsymbol und anschließend auf den Befehl **Backup-Optionen**.
3. Wählen Sie **Dateifilter**.
4. Verwenden Sie eine der nachfolgend beschriebenen Optionen.

Dateien ausschließen, die bestimmte Kriterien erfüllen

Es gibt zwei Optionen, die auf gegensätzliche Weise funktionieren.

- **Nur Dateien ins Backup einschließen, die folgende Kriterien erfüllen**

  Beispiel: Falls Sie festlegen, dass die komplette Maschine gesichert werden soll, und dann den Eintrag '**C:\Datei.exe**' in den Filterkriterien spezifizieren, wird nur diese Datei im Backup gesichert.

  Hinweis: *Dieser Filter wirkt sich nicht auf Datei-Backups aus, wenn* ***Version 11*** *beim* ***Backup-Format*** *(S. 66) ausgewählt ist und das Backup-Ziel NICHT der Cloud Storage ist.*

- **Dateien vom Backup ausschließen, die folgende Kriterien erfüllen**

Beispiel: Falls Sie festlegen, dass die komplette Maschine gesichert werden soll, und dann den Eintrag '**C:\Datei.exe**' in den Filterkriterien spezifizieren, wird genau diese (und nur diese) Datei beim Backup übersprungen.

Es ist auch möglich, beide Optionen gemeinsam zu verwenden. Die letzte Option überschreibt die vorhergehende, was bedeutet: falls Sie '**C:\Datei.exe**' in beiden Feldern spezifizieren, wird die Datei beim Backup übersprungen.

Kriterien

- **Vollständiger Pfad**

  Spezifizieren Sie den vollständigen Pfad zu der Datei oder dem Ordner, indem Sie mit dem Laufwerksbuchstaben (bei Backups unter Windows) oder dem Stammverzeichnis (bei Backups unter Linux oder macOS) beginnen.

  Sowohl unter Windows wie auch unter Linux/macOS können Sie in den Datei- bzw. Ordnerpfaden einen normalen Schrägstrich (Slash) verwenden (Beispiel: **C:/Temp/Datei.tmp**). Unter Windows können Sie zudem den herkömmlichen, nach links geneigten Schrägstrich (Backslash) verwenden (Beispiel: **C:\Temp\Datei.tmp**).

- **Name**

  Spezifizieren Sie den Namen der Datei oder des Ordners (Beispiel: **Dokument.txt**). Es werden alle Dateien und Ordner mit diesem Namen ausgewählt.

Bei den Kriterien wird die Groß-/Kleinschreibung *nicht* beachtet. Wenn Sie beispielsweise **C:\Temp** spezifizieren, wird **C:\TEMP**, **C:\temp** usw. ausgewählt.

Sie können ein oder mehrere Platzhalterzeichen (*, ** und ?) in dem Kriterium verwenden. Diese Zeichen können innerhalb des vollständigen Pfades und im Namen der Datei oder des Ordners verwendet werden.

Der Asterisk (*) ersetzt null bis mehrere Zeichen in einem Dateinamen. So beinhaltet beispielsweise das Kriterium **Dok*.txt** Dateien wie **Dok.txt** und **Dokument.txt**.

Der doppelte Asterisk (**) ersetzt null bis mehrere Zeichen in einem Dateinamen und Pfad (Schrägstriche eingeschlossen). Beispielweise schließt das Kriterium ****/Docs/**.txt** alle txt-Dateien in allen Unterordnern von allen Ordnern mit der Bezeichnung **Docs** ein.

Das Fragezeichen (?) steht für exakt ein Zeichen in einem Dateinamen. Beispielsweise schließt das Kriterium **Dok?.txt** Dateien wie **Dok1.txt** und **Doks.txt** ein – während Dateien wie **Dok.txt** oder **Dok11.txt** ausgeschlossen werden.

Versteckte Dateien und Ordner ausschließen

Aktivieren Sie dieses Kontrollkästchen, um Dateien und Ordner zu überspringen, die mit dem Attribut **Versteckt** gekennzeichnet sind (bei Windows-typischen Dateisystemen) – oder die mit einem Punkt (.) beginnen (bei Linux-typischen Dateisystemen wie Ext2 und Ext3). Bei Ordnern mit dem Attribut 'Versteckt' wird der gesamte Inhalt ausgeschlossen (einschließlich solcher Dateien, die nicht versteckt sind).

Systemdateien und Systemordner ausschließen

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

Tipp: *Sie können die Attribute von Dateien oder Ordnern über ihre Datei- bzw. Ordner-Eigenschaften oder den Kommandozeilenbefehl 'attrib' überprüfen. Weitere Informationen finden Sie im Hilfe und Support-Center von Windows.*

8.9.11 Snapshot für Datei-Backups

Diese Option gilt nur für Backups auf Dateiebene.

Diese Option definiert, ob die Dateien bei einem Backup nacheinander gesichert oder mithilfe eines einmaligen Daten-Snapshots erfasst werden.

Hinweis: *Dateien, die auf Netzwerkfreigaben gespeichert sind, werden immer nacheinander gesichert.*

Die Voreinstellung ist:

- Wenn nur Maschinen zum Backup ausgewählt wurden, die unter Linux laufen: **Keinen Snapshot erstellen.**
- Ansonsten: **Snapshot erstellen, sofern möglich.**

Sie können eine der folgenden Optionen wählen:

- **Snapshot erstellen, sofern möglich**

  Dateien direkt sichern, sofern kein Snapshot möglich ist.
- **Snapshot immer erstellen**

  Der Snapshot ermöglicht es, alle Dateien zu sichern – auch solcher, die mit einem exklusiven Zugriff geöffnet sind. Die gesicherten Dateien haben alle den gleichen Backup-Zeitpunkt. Wählen Sie diese Einstellung nur, wenn diese Faktoren kritisch sind, d.h. ein Backup der Dateien ohne den vorhergehenden Snapshot keinen Sinn macht. Wenn kein Snapshot erstellt werden kann, wird das Backup fehlschlagen.
- **Keinen Snapshot erstellen**

  Dateien immer direkt sichern. Der Versuch, Dateien zu sichern, die per exklusivem Zugriff geöffnet sind, führt hier zu einem Fehler. Außerdem ist die Backup-Zeit der Dateien nicht gleich.

8.9.12 Protokollabschneidung

Diese Option gilt für Backups von Microsoft SQL Server-Datenbanken und für Laufwerk-Backups mit aktiviertem Microsoft SQL Server-Applikations-Backup.

Diese Option bestimmt, ob die SQL-Transaktionsprotokolle nach einem erfolgreichen Backup abgeschnitten werden.

Die Voreinstellung ist: **Aktiviert**.

Wenn diese Option aktiviert ist, kann eine Datenbank nur auf einen Zeitpunkt zurückgesetzt (wiederhergestellt) werden, zu dem es ein von der Software erstelltes Backup gibt. Deaktivieren Sie diese Option, wenn Sie die Transaktionsprotokolle mithilfe der integrierten Backup-Engine des Microsoft SQL Servers sichern. Sie können die Transaktionsprotokolle nach der Wiederherstellung anwenden – und damit eine Datenbank auf einen beliebigen Zeitpunkt zurücksetzen (wiederherstellen).

8.9.13 LVM-Snapshot-Erfassung

Diese Option gilt nur für physische Maschinen.

Diese Option gilt für Laufwerk-Backups von Volumes, die vom Linux Logical Volume Manager (LVM) verwaltet werden. Solche Volumes werden auch als 'logische Volumes' bezeichnet.

Diese Option definiert, wie der Snapshot eines logischen Volumes erfasst wird. Die Backup-Software kann dies eigenständig tun oder den Linux Logical Volume Manager (LVM) beanspruchen.

Die Voreinstellung ist: **Durch die Backup-Software**.

- **Durch die Backup-Software**. Die Snapshot-Daten werden überwiegend im RAM gehalten. Das Backup ist schneller und es wird kein nicht zugeordneter Speicherplatz auf der Volume-Gruppe benötigt. Wir empfehlen die Voreinstellung daher nur zu ändern, falls es ansonsten zu Problemen beim Backup von logischen Volumes kommt.
- **Durch den LVM**. Der Snapshot wird auf 'nicht zugeordnetem' Speicherplatz der Volume-Gruppe gespeichert. Falls es keinen 'nicht zugeordneten' Speicherplatz gibt, wird der Snapshot durch die Backup-Software erfasst.

8.9.14 Mount-Punkte

Diese Option ist nur unter Windows und für ein Datei-basiertes Backup wirksam, dessen Datenquelle gemountete Volumes oder freigegebene Cluster-Volumes enthält.

Diese Option ist nur wirksam, wenn Sie einen Ordner als Backup-Quelle auswählen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. (Ein Mount-Punkt ist ein Ordner, an den ein zusätzliches Volume logisch angebunden ist).

- Wenn ein solcher Ordner (oder ein übergeordneter Ordner) als Backup-Quelle ausgewählt wird – und die Option **Mount-Punkte** aktiviert wurde – dann werden alle auf dem gemounteten Volume liegenden Dateien in das Backup aufgenommen. Wenn die Option **Mount-Punkte** deaktiviert wurde, bleibt der Mount-Punkt im Backup leer.

  Bei der Wiederherstellung eines übergeordneten Ordners hängt die Frage, ob auch der Inhalt des Mount-Punktes wiederhergestellt wird (oder nicht) davon ab, ob die Option **Mount-Punkte** für die Recovery-Aktion (S. 103) aktiviert oder deaktiviert wurde.
- Wenn Sie den Mount-Punkt direkt auswählen oder einen Ordner innerhalb des gemounteten Volumes, dann werden die gewählten Ordner wie herkömmliche Ordner betrachtet. Sie werden unabhängig vom Status der Backup-Option **Mount-Punkte** gesichert – genauso, wie sie unabhängig vom Status der entsprechenden Recovery-Option **Mount-Punkte**für die Recovery-Aktion (S. 103) wiederhergestellt werden.

Voreinstellung ist: **Deaktiviert**.

Tipp: *Sie können virtuelle Maschinen vom Typ Hyper-V sichern, die auf einem freigegebenen Cluster-Volume liegen, indem Sie die benötigten Dateien oder das komplette Volume per Datei-basiertem Backup sichern. Fahren Sie die virtuellen Maschinen herunter, um zu gewährleisten, dass sie in einem konsistenten Zustand gesichert werden.*

Beispiel

Angenommen, der Ordner **C:\Daten1** ist der Mount-Punkt für ein gemountetes Volume. Das Volume enthält die Verzeichnisse **Ordner1** und **Ordner2**. Sie erstellen einen Backup-Plan zur Datei-basierten Sicherung Ihrer Daten.

Wenn Sie das Volume C per Kontrollkästchen auswählen und dafür die Option **Mount-Punkte** aktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup auch die Verzeichnisse **Ordner1** und **Ordner2** enthalten. Wenn Sie die gesicherten Daten dann später wiederherstellen, sollten Sie an die

entsprechende, gewünschte Einstellung der Option **Mount-Punkte** für die Recovery-Aktionen (S. 103) denken.

Wenn Sie das Volume C per Kontrollkästchen auswählen und die Option **Mount-Punkte** jedoch deaktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup leer sein.

Wenn Sie die Verzeichnisse **Daten1**, **Ordner1** oder **Ordner2** direkt selbst per Kontrollkästchen zum Backup auswählen, werden diese markierten Ordner wie herkömmliche Ordners in Backup aufgenommen – unabhängig vom Status der Option **Mount-Punkte**.

8.9.15 Multi-Volume-Snapshot

Diese Option gilt nur für Backups von physischen Maschinen, die mit Windows oder Linux laufen.

Diese Option gilt für Laufwerk-Backups. Diese Option gilt auch für Backups auf Dateiebene, wenn diese unter Verwendung eines Snapshots erstellt werden. (Die Option Snapshot für Datei-Backups (S. 72) bestimmt, ob bei einem solchen Backup ein Snapshot benutzt wird oder nicht.)

Diese Option bestimmt, ob die Snapshots bei mehreren Volumes gleichzeitig oder nacheinander erfasst werden sollen.

Die Voreinstellung ist:

- Wenn mindestens eine Maschine, die mit Windows läuft, zum Backup ausgewählt wurde: **Aktiviert**.
- Ansonsten: **Deaktiviert**.

Wenn diese Option aktiviert ist, werden die Snapshots aller zu sichernden Volumes gleichzeitig erstellt. Verwenden Sie diese Option, um ein zeitkonsistentes Backup von Daten zu erstellen, die über mehrere Volumes verteilt sind (z.B. für eine Oracle-Datenbank).

Wenn diese Option deaktiviert ist, werden die Snapshots der Volumes nacheinander erfasst. Falls sich die Daten also über mehrere Volumes erstrecken, werden diese zu unterschiedlichen Zeiten gesichert. Das resultierende Backup ist daher möglicherweise nicht konsistent.

8.9.16 Performance

Prozesspriorität

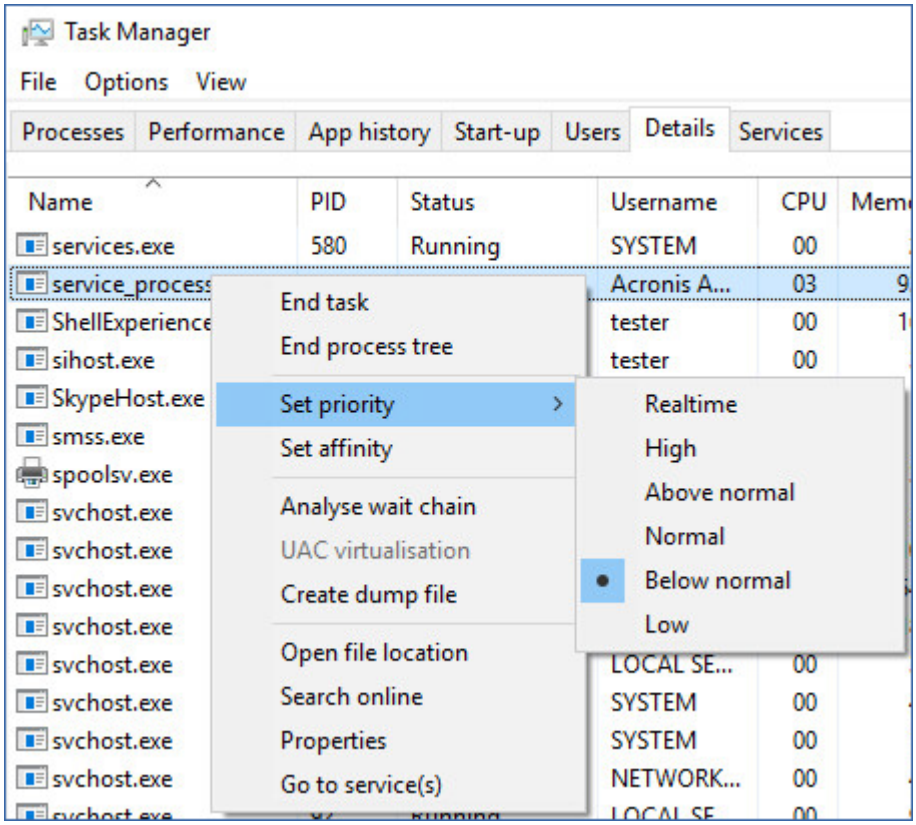
Diese Option bestimmt, welche Priorität dem Backup-Prozess innerhalb des Betriebssystems zugewiesen wird.

Die verfügbaren Einstellungen sind: **Niedrig**, **Normal**, **Hoch**.

Voreinstellung ist: **Niedrig** (unter Windows, entspricht **Niedriger als normal**).

Die Priorität eines Prozesses, der in einem System ausgeführt wird, bestimmt, wie viele CPU-und System-Ressourcen ihm zugewiesen werden. Durch das Herabsetzen der Backup-Priorität stehen mehr Ressourcen für andere Applikationen zur Verfügung. Das Heraufsetzen der Backup-Priorität kann den Backup-Prozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren (wie etwa der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk).

Diese Option bestimmt die Priorität des Backup-Prozesses (**service_process.exe**) unter Windows und die Priorität ('niceness') des Prozeses (**service_process**) unter Linux und OS X.



Die Ausgabegeschwindigkeit beim Backup

Mit dieser Option können Sie Geschwindigkeit begrenzen, mit der die Backup-Daten auf die Festplatte geschrieben werden (Backup-Ziel ist ein lokaler Ordner) – oder mit der die Backup-Daten durch ein Netzwerk übertragen werden (Backup-Ziel ist eine Netzwerkfreigabe oder ein Cloud Storage).

Voreinstellung ist: **Deaktiviert**.

Wenn die Option aktiviert ist, können Sie eine maximal erlaubte Ausgabegeschwindigkeit in KB/Sekunde festlegen.

8.9.17 Physischer Datenversand

Diese Option gilt, wenn als Backup-Ziel der Cloud Storage verwendet wird und das Backup-Format (S. 66) mit **Version 12** festgelegt ist.

Diese Option gilt für Laufwerk- und Datei-Backups, die von einem Agenten für Windows, Agenten für Linux, Agenten für Mac, Agenten für VMware, Agenten für Hyper-V und Agenten für Virtuozzo erstellt wurden.

Diese Option bestimmt, ob das erste Voll-Backup, welches durch einen entsprechenden Backup-Plan erstellt wurde, auf einer Festplatte gespeichert und dann über den Service 'Physische Datenversand' (Physical Data Shipping) in den Cloud Storage übertragen wird. Alle dazugehörigen, nachfolgenden inkrementellen Backups können dann über das Netzwerk/Internet durchgeführt werden.

Die Voreinstellung ist: **Deaktiviert.**

Über den Service 'Physische Datenversand'

Die Weboberfläche für den Service 'Physische Datenversand' ist nur für Administratoren verfügbar.

Eine ausführliche Anleitung, wie Sie den Service 'Physischer Datenversand' und das entsprechende Auftragserstellungstool verwenden, finden Sie in der Anleitung für Administratoren zum 'Physischen Datenversand'. Sie können auf dieses Dokument zugreifen, wenn Sie Weboberfläche für den Service 'Physische Datenversand' auf das Fragezeichen-Symbol klicken.

Ein Überblick zum Ablauf des physischen Datenversandes

1. Erstellen Sie einen neuen Backup-Plan. Aktivieren Sie in diesem Plan die Backup-Option **Physischer Datenversand**.

   Sie können das Backup direkt auf dem für den Versand verwendeten Laufwerk erstellen lassen – oder zuerst in einen lokalen Ordner oder Netzwerkordner speichern und das Backup anschließend auf das Laufwerk kopieren.

   ***Wichtig**: Wenn das anfängliche Voll-Backup erstellt wurde, müssen alle nachfolgenden Backups weiterhin mit demselben Backup-Plan durchgeführt werden. Jeder andere Backup-Plan, selbst wenn er die gleichen Parameter und die gleiche Maschine verwenden sollte, benötigt einen neuen/anderen physischen Datenversand.*

2. Nachdem das anfängliche Backup abgeschlossen wurde, können Sie über die Weboberfläche für den Service 'Physischer Datenversand' das Auftragserstellungstool herunterladen, um mit diesem die Bestellung durchzuführen.

   Sie können auf diese Weboberfläche zugreifen, wenn Sie sich am Management-Portal anmelden. Klicken Sie dort dann zuerst auf **Überblick** –> **Nutzung** – und anschließend unter **Physischer Datenversand** auf den Befehl **Service verwalten**.

3. Verpacken Sie das Laufwerk sorgfältig und versenden Sie es dann per Post an das entsprechende Datacenter.

   ***Wichtig**: Stellen Sie sicher, dass Sie die Verpackungsanweisungen befolgen, wie sie in der Anleitung für Administratoren zum 'Physischen Datenversand' beschrieben sind.*

4. Sie können den Auftragsstatus über die Weboberfläche für den Service verfolgen. Beachten Sie, dass alle nachfolgenden Backups solange noch fehlschlagen werden, bis das anfängliche Voll-Backup vom Festplattenlaufwerk in den Cloud Storage hochgeladen wurde.

8.9.18 Vor-/Nach-Befehle

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

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

Befehl vor dem Backup	Backup	Befehl nach Backup

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

- Löschen Sie bestimmte temporäre Dateien von der Festplatte, bevor ein Backup gestartet wird.
- Konfiguration Sie das Antivirenprodukt eines Drittanbieters so, dass es vor jedem Start des Backups ausgeführt wird.
- Kopieren Sie Backups selektiv zu einem anderen Speicherort. Diese Option kann nützlich sein, weil die in einem Backup-Plan konfigurierte Replikation *jedes* Backup zu den nachfolgenden Speicherorten kopiert.

Der Agent führt die Replikation *nach* Ausführung des Nach-Backup-Befehls aus.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern, wie z.B. 'Pause'.

8.9.18.1 Befehl vor dem Backup

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

1. Aktivieren Sie den Schalter **Einen Befehl vor dem Backup ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

Kontrollkästchen	**Auswahl**			
Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Backup erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Backup nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Backup nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Backup gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

8.9.18.2 Befehlsausführung nach dem Backup

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn ein Backup erfolgreich abgeschlossen wurde.

1. Aktivieren Sie den Schalter **Einen Befehl nach dem Backup ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus.
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei ausgeführt werden soll.

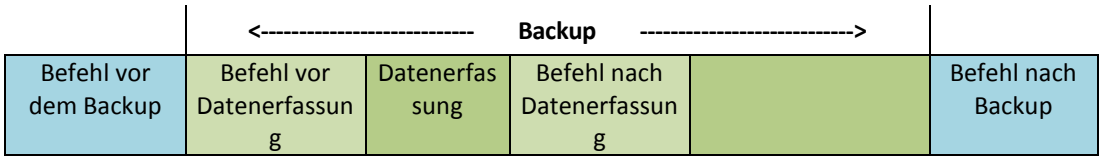
4. Geben bei Bedarf im Feld **Argumente** eventuell benötigte Parameter für die Befehlsausführung ein.
5. Aktivieren Sie das Kontrollkästchen **Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls besonders wichtig für Sie ist. Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Sollte die Befehlsausführung fehlschlagen, erhält der Backup-Status den Wert '**Fehler**'.

   Wenn das Kontrollkästchen deaktiviert ist, hat das Ergebnis der Befehlsausführung keinen Einfluss darauf, ob die Backup-Ausführung als erfolgreich oder fehlgeschlagen eingestuft wird. Sie können das Ergebnis der Befehlsausführung in der Registerkarte **Aktivitäten** überwachen.
6. Klicken Sie auf **Fertig**.

8.9.19 Befehle vor/nach der Datenerfassung

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

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.



Wenn die Option Volume Shadow Copy Service (VSS) (S. 81) aktiviert ist, werden die Ausführung der Befehle und die Aktionen von Microsofts VSS folgendermaßen eingeordnet:

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

Mithilfe der Befehle vor/nach der Datenerfassung können Sie Datenbanken, die nicht mit VSS kompatibel sind, vor der Datenerfassung anhalten und nach der Datenerfassung wieder fortsetzen. Da die Datenerfassung nur einige Sekunden benötigt, werden die Datenbanken oder Applikationen nur für kurze Zeit pausiert.

8.9.19.1 Befehl vor Datenerfassung

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

1. Aktivieren Sie den Schalter **Einen Befehl vor der Datenerfassung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

Kontrollkästchen	Auswahl			
Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Datenerfassung erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Datenerfassung nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Datenerfassung nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Datenerfassung gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

8.9.19.2 Befehl nach Datenerfassung

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

1. Aktivieren Sie den Schalter **Einen Befehl nach der Datenerfassung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

Kontrollkästchen	Auswahl			
Backup scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Backup erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Backup nur fortsetzen, nachdem der Befehl erfolgreich	Backup nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder	Nicht verfügbar	Backup gleichzeitig mit Befehlsausführung fortsetzen, unabhängig vom

	durchgeführt wurde.	Misserfolg der Ausführung.		Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

8.9.20 Planung

Mit dieser Option können Sie festlegen, ob Backups nach Planung oder mit einer Verzögerung starten sollen – und wie viele virtuelle Maschinen gleichzeitig gesichert werden.

Die Voreinstellung ist: **Backup-Startzeiten in einem Zeitfenster verteilen. Maximale Verzögerung:: 30 Minuten.**

Sie können eine der folgenden Optionen wählen:

- **Alle Backups genau nach Planung starten**

  Die Backups von physischen Maschinen werden wie im Plan definiert gestartet. Virtuelle Maschinen werden nacheinander gesichert.
- **Startzeiten in einem Zeitfenster verteilen**

  Die Backups von physischen Maschinen werden mit einer Verzögerung (bezogen auf die geplante Zeit) gestartet. Der Verzögerungswert für jede Maschine wird zufällig bestimmt und reicht von Null bis einem maximalen, von Ihnen spezifizierten Wert. Sie können diese Einstellung bei Bedarf verwenden, wenn Sie mehrere Maschinen per Backup zu einem Netzwerkspeicherort sichern, um eine übermäßige Netzwerklast zu vermeiden. Der Verzögerungswert für jede Maschinen wird bestimmt, wenn der Backup-Plan auf die Maschine angewendet wird – und er bleibt so lange gleich, bis Sie den Backup-Plan erneut bearbeiten und den maximalen Verzögerungswert ändern.

  Virtuelle Maschinen werden nacheinander gesichert.
- **Die Anzahl gleichzeitig ausgeführter Backups begrenzen**

  Diese Option ist nur dann verfügbar, wenn ein Backup-Plan auf mehrere virtuelle Maschinen angewendet wird. Diese Option definiert, wie viele virtuelle Maschinen ein Agent gleichzeitig sichern kann, wenn er den gegebenen Backup-Plan ausführt.

  Falls ein Agent gemäß eines Backup-Plans ein gleichzeitiges Backup mehrerer Maschinen starten muss, wird dieser zwei Maschinen auswählen. (Zur Optimierung der Backup-Performance versucht der Agent Maschinen zuzuweisen, die auf verschiedenen Storages gespeichert sind). Sobald eines der beiden Backups abgeschlossen ist, wählt der Agent eine dritte Maschine und so weiter.

  Sie können die Anzahl der virtuellen Maschinen ändern, die ein Agent gleichzeitig sichern soll. Der maximale Wert ist 10. Wenn der Agent jedoch mehrere Backup-Pläne ausführt, die sich zeitlich überlappen, werden die in deren Optionen angegebenen Zahlen addiert. Sie können die Gesamtzahl der virtuellen Maschinen (S. 200), die ein Agent gleichzeitig sichern kann, begrenzen – unabhängig davon, wie viele Backup-Pläne ausgeführt werden.

  Die Backups von physischen Maschinen werden wie im Plan definiert gestartet.

8.9.21 Sektor-für-Sektor-Backup

Die Option gilt nur für Backups auf Laufwerksebene.

Diese Option definiert, ob von einem Laufwerk/Volume eine exakte Kopie auf physischer Ebene erstellt werden soll.

Die Voreinstellung ist: **Deaktiviert**.

Wenn diese Option aktiviert ist, werden beim Backup eines Laufwerks/Volumes alle vorhandenen Sektoren gesichert – einschließlich der Sektoren von 'nicht zugeordnetem' und 'freiem' Speicherplatz. Das resultierende Backup wird die gleiche Größe wie das gesicherte Laufwerk haben (sofern die Option 'Komprimierungsgrad (S. 68)' auf **Ohne** eingestellt ist). Die Software schaltet automatisch auf den Sektor-für-Sektor-Modus um, wenn ein Laufwerk ein Dateisystem verwendet, das nicht erkannt oder nicht unterstützt wird.

8.9.22 Aufteilen

Diese Option gilt für die Backup-Schemata **Nur vollständig**, **Wöchentlich vollständig, täglich inkrementell** und **Benutzerdefiniert**.

Mit dieser Option können Sie festlegen, ob und wie große Backups in kleinere Dateien aufgeteilt werden sollen.

Die Voreinstellung ist: **Automatisch**.

Es stehen folgende Einstellungen zur Verfügung:

- **Automatisch**

  Das Backup wird aufgeteilt, wenn es die maximale Dateigröße überschreitet, die vom Dateisystem des Zielspeicherortes/Datenträgers noch unterstützt wird.
- **Feste Größe**

  Geben Sie die gewünschte Dateigröße manuell ein oder wählen Sie diese mit dem Listenfeld aus.

8.9.23 Task-Fehlerbehandlung

Diese Option bestimmt, wie sich das Programm verhalten soll, wenn die geplante Ausführung eines Backup-Plans fehlschlägt. Diese Option gilt nicht, wenn ein Backup-Plan manuell gestartet wird.

Wenn diese Option aktiviert ist, wird das Programm versuchen, die Ausführung des Backup-Plans zu wiederholen. Sie können festlegen, wie oft und mit welchem Zeitintervall die Ausführung wiederholt werden soll. Die Versuche werden aufgegeben, wenn die Aktion gelingt – oder die festgelegte Anzahl der Versuche erreicht ist (je nachdem, was zuerst eintritt).

Die Voreinstellung ist: **Deaktiviert**.

8.9.24 VSS (Volume Shadow Copy Service)

Diese Option gilt nur für Windows-Betriebssysteme.

Diese Option definiert, ob ein VSS-Provider (Volume Shadow Copy Service) die VSS-konforme Applikationen benachrichtigen muss, dass ein Backup startet. Dies gewährleistet, dass die von den entsprechenden Applikationen verwendeten und dann im Backup gespeicherten Daten in einem konsistenten Zustand gesichert werden. Beispielsweise, dass alle Datenbanktransaktionen in dem Augenblick abgeschlossen werden, in dem die Backup-Software den Snapshot erfasst. Die Datenkonsistenz gewährleistet dann wiederum, dass die Applikationen auch in einem korrekten Zustand wiederhergestellt werden können und somit unmittelbar nach der Wiederherstellung einsatzbereit sind.

Die Voreinstellung ist: **Aktiviert**. **Snapshot Provider automatisch auswählen**.

Sie können eine der folgenden Optionen wählen:

- **Snapshot Provider automatisch auswählen**

  Automatisch zwischen Hardware Snapshot Provider, Software Snapshot Provider und Microsoft Software Shadow Copy Provider (Microsoft-Softwareschattenkopie-Anbieter) wählen.
- **Microsoft Software Shadow Copy Provider verwenden**

  Wir empfehlen, diese Option beim Backup von Applikationsservern (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint oder Active Directory) zu verwenden.

Deaktivieren Sie diese Option, wenn Ihre Datenbank nicht VSS-kompatibel ist. Snapshots werden zwar schneller erfasst, aber die Datenkonsistenz von Applikationen, deren Transaktionen zum Zeitpunkt des Snapshots nicht vollendet sind, kann nicht garantiert werden. Mit definierbaren Befehlen vor/nach der Datenerfassung (S. 78) können Sie sicherstellen, dass die Daten in einem konsistenten Zustand gesichert wurden. Spezifizieren Sie z.B. einen Befehl vor der Datenerfassung, der diese Datenbank anhält und alle Cache-Speicher leert, um zu sichern, dass alle Transaktionen vollendet sind – und ergänzen Sie Befehle nach der Datenerfassung, damit die Datenbank nach der Snapshot-Erstellung den Betrieb wieder aufnimmt.

Hinweis: *Wenn diese Option aktiviert ist, werden alle Dateien, die im Registry-Schlüssel '**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**' spezifiziert sind, nicht per Backup gesichert. Es werden insbesondere keine offline Outlook-Datendateien (.ost) gesichert, da diese im Wert '**OutlookOST**' dieses Schlüssels spezifiziert sind.*

VSS-Voll-Backup aktivieren

Falls diese Option aktiviert ist, werden die Protokolle des Microsoft Exchange Servers und anderer VSS-konformer Applikationen (mit Ausnahme des Microsoft SQL Servers) nach jedem erfolgreichen vollständigen, inkrementellen oder differentiellen Laufwerk-Backup abgeschnitten.

Die Voreinstellung ist: **Deaktiviert**.

Lassen Sie diese Option in folgenden Fällen deaktiviert:

- Falls Sie den Agenten für Exchange oder eine Dritthersteller-Software zum Backup von Exchange Server-Daten verwenden. Hintergrund ist, dass die Protokollabschneidung die aufeinanderfolgenden Transaktionsprotokoll-Backups beeinträchtigt.
- Falls Sie eine Dritthersteller-Software zum Backup der SQL Server-Daten verwenden. Hintergrund ist, dass die Dritthersteller-Software das resultierende Laufwerk-Backup als sein eigenes Voll-Backup ansehen wird. Als Folge wird das nächste differentielle Backup der SQL Server-Daten fehlschlagen. Die Backups werden solange fehlschlagen, bis die Dritthersteller-Software das nächste eigene Voll-Backup erstellt.
- Falls andere VSS-kompatible Applikationen auf der Maschine laufen und es aus irgendwelchen Gründen notwendig ist, deren Protokolle zu behalten.

Eine Aktivierung dieser Option bewirkt kein Abschneiden von Microsoft SQL Server-Protokollen. Wenn Sie das SQL Server-Protokoll nach einem Backup abschneiden lassen wollen, müssen Sie die Backup-Option 'Protokollabschneidung (S. 72) aktivieren.

8.9.25 VSS (Volume Shadow Copy Service) für virtuelle Maschinen

Diese Option definiert, ob die virtuellen Maschinen mit stillgelegten (quiesced) Snapshots erfasst werden sollen. Um einen stillgelegten Snapshot zu erfassen, wendet die Backup-Software den VSS (Volumenschattenkopiedienst) innerhalb der virtuellen Maschine an – und zwar mithilfe der VMware Tools oder der Hyper-V-Integrationsdienste.

Die Voreinstellung ist: **Aktiviert**.

Eine Aktivierung dieser Option bewirkt, dass die Transaktionen aller VSS-konformen Applikationen, in einer virtuellen Maschine laufen, abgeschlossen werden, bevor der Snapshot erfasst wird. Falls ein stillgelegter Snapshot (nach einer in der Option 'Fehlerbehandlung (S. 69)' spezifizierten Anzahl von Neuversuchen) fehlschlägt und die Option 'Applikations-Backup' deaktiviert ist, wird ein 'nicht stillgelegter' (non-quiesced) Snapshot erstellt. Sollte die Option 'Applikations-Backup' aktiviert sein, wird das Backup fehlschlagen.

Sollte die Option deaktiviert sein, wird ein 'nicht stillgelegter' (non-quiesced) Snapshot erstellt. Die Maschine wird dann in einem 'crash-konsistenten' Zustand gesichert.

8.9.26 Wöchentliche Backups

Diese Option bestimmt, welche Backups in Aufbewahrungsregeln und Backup-Schemata als 'wöchentlich' betrachtet werden. Ein 'wöchentliches' Backup ist dasjenige Backup, das als erstes in einer Woche erstellt wird.

Die Voreinstellung ist: **Montag**.

8.9.27 Windows-Ereignisprotokoll

Diese Option gilt nur für Windows-Betriebssysteme.

Diese Option definiert, ob die Agenten für alle Backup-Aktionen entsprechende Ereigniseinträge im Windows-Anwendungsereignisprotokoll hinterlegen sollen. Sie können die Protokolleinträge über die Windows-Ereignisanzeige einsehen, die per Eingabebefehl (eventvwr.exe) oder per Menü (**Systemsteuerung** –> **Verwaltung** –> **Ereignisanzeige**) aufgefrufen werden kann. Sie können die Ereignisse filtern, die geloggt werden.

Die Voreinstellung ist: **Deaktiviert**.

9 Recovery

9.1 Spickzettel für Wiederherstellungen

Die nachfolgende Tabelle fasst alle verfügbaren Recovery-Methoden zusammen. Verwenden Sie diese Tabelle, um diejenige Recovery-Methode zu finden, die am besten zu Ihren Bedürfnissen passt.

Recovery-Quelle	Recovery-Methode
Physische Maschine (Windows oder Linux)	Weboberfläche verwenden (S. 85) Boot-Medium verwenden (S. 90)
Physische Maschine (Mac)	Boot-Medium verwenden (S. 90)
Virtuelle Maschine (VMware oder Hyper-V)	Weboberfläche verwenden (S. 88) Boot-Medium verwenden (S. 90)
Virtuelle Maschine oder Container (Virtuozzo)	Weboberfläche verwenden (S. 88)
ESXi-Konfiguration	Boot-Medium verwenden (S. 99)
Dateien/Ordner	Weboberfläche verwenden (S. 94) Dateien aus dem Cloud Storage herunterladen (S. 95) Boot-Medium verwenden (S. 97) Dateien aus lokalen Backups extrahieren (S. 98)
Systemzustand	Weboberfläche verwenden (S. 99)
SQL-Datenbanken	Weboberfläche verwenden (S. 139)

Recovery-Quelle		Recovery-Methode
Exchange-Datenbanken		Weboberfläche verwenden (S. 142)
Exchange-Postfächer		Weboberfläche verwenden (S. 144)
Websites		Weboberfläche verwenden (S. 183)
Microsoft Office 365	Postfächer (lokaler Agent für Office 365)	Weboberfläche verwenden (S. 151)
	Postfächer (lokaler Agent für Office 365)	Weboberfläche verwenden (S. 154)
	OneDrive-Dateien	Weboberfläche verwenden (S. 158)
	SharePoint Online-Daten	Weboberfläche verwenden (S. 162)
G Suite	Postfächer	Weboberfläche verwenden (S. 168)
	Google Drive-Dateien	Weboberfläche verwenden (S. 171)
	Team Drive-Dateien	Weboberfläche verwenden (S. 175)

Hinweis für Mac-Benutzer

- Ab Mac OS X 10.11 El Capitan werden bestimmte System-Dateien/-Ordner/-Prozesse mit dem erweiterten Datei-Attribut 'com.apple.rootless' gekennzeichnet und so besonders geschützt. Diese Funktion zur Wahrung der Systemintegrität wird auch SIP (System Integrity Protection) genannt. Zu den geschützten Dateien gehörten vorinstallierte Applikationen sowie die meisten Ordner in /system, /bin, /sbin, /usr.

  Solchermaßen geschützte Dateien und Ordner können bei einer Recovery-Aktion nicht überschrieben werden, wenn die Wiederherstellung unter dem Betriebssystem selbst ausgeführt wird. Wenn es notwendig ist, diese geschützten Dateien zu überschreiben, müssen Sie die Wiederherstellung stattdessen mit einem Boot-Medium durchführen.
- Ab macOS Sierra 10.12 können selten verwendete Dateien mit der Funktion 'In iCloud speichern' in die Cloud verschoben werden. Von diesen Dateien werden im Dateisystem kleine 'Fußabdrücke' gespeichert. Bei einem Backup werden dann diese Datenfußabdrücke statt der Originaldateien gesichert.

  Wenn Sie einen solchen Datenfußabdruck an ursprünglichen Speicherort wiederherstellen, wird er mit der iCloud synchronisiert und die Originaldatei ist wieder verfügbar. Wenn Sie einen Datenfußabdruck an einem anderen Speicherort wiederherstellen, ist keine Synchronisierung möglich und ist die Originaldatei daher nicht verfügbar.

9.2 Ein Boot-Medium erstellen

Ein Boot-Medium ist eine CD, eine DVD, ein USB-Stick oder ein anderes Wechselmedium, welches Ihnen ermöglicht, den Agenten ohne die Hilfe des eigentlichen Betriebssystems auszuführen. Der Haupteinsatzzweck eines bootfähigen Mediums besteht in der Möglichkeit, ein System wiederherzustellen, welches nicht mehr starten (booten) kann.

Wir empfehlen dringend, dass Sie ein Boot-Medium erstellen und dieses testen, sobald Sie das erste Mal ein Backup auf Laufwerksebene erstellt haben. Es hat sich außerdem bewährt, nach jedem größeren Update des Backup Agenten auch ein neues Medium zu erstellen.

Zur Wiederherstellung von Windows oder Linux können Sie dasselbe Medium verwenden. Um macOS wiederherstellen zu können, müssen Sie ein separates Medium auf einer Maschine erstellen, die unter macOS läuft.

So erstellen Sie ein bootfähiges Medium unter Windows oder Linux

1. Laden Sie die ISO-Datei des Boot-Mediums herunter. Wählen Sie zum Herunterladen der Datei eine Maschine aus – und klicken Sie dann auf **Wiederherstellen** > **Weitere Wiederherstellungsmöglichkeiten...** > **ISO-Image herunterladen**.
2. [Optional] Kopieren, drucken oder notieren Sie sich das Registrierungs-Token, das von der Backup-Konsole angezeigt wird.

   Mit diesem Token können Sie von einem Boot-Medium aus direkt auf den Cloud Storage zugreifen, ohne Ihre Anmeldedaten eingeben zu müssen. Dies ist notwendig, wenn Sie sich nicht selbst direkt an der Cloud anmelden können, sondern stattdessen eine Drittanbieter-Authentifizierung verwenden.
3. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Brennen Sie die ISO-Datei auf eine CD/DVD.
   - Erstellen Sie einen bootfähigen USB-Stick mit der ISO-Datei. Um einen USB-Stick grundsätzlich bootfähig zu machen, können Sie eines (von vielen) kostenlos im Internet verfügbaren Freeware-Tools verwenden.

     Verwenden Sie beispielsweise `ISO to USB` oder RUFUS, falls Sie eine UEFI-Maschine booten wollen – oder `Win32DiskImager`, wenn Sie eine BIOS-Maschine haben. Unter Linux können Sie das Utility `dd` verwenden.
   - Mounten Sie die ISO-Datei als CD-/DVD-Laufwerk für diejenige virtuelle Maschine, die Sie wiederherstellen wollen.

So können Sie ein Boot-Medium unter macOS erstellen

1. Klicken Sie auf einer Maschine, auf welcher der Agent für Mac installiert ist, im Menü **Programme** auf den Eintrag **Rescue Media Builder**.
2. Die Software zeigt Ihnen die angeschlossenen Wechsellaufwerke/Wechselmedien an. Wählen Sie dasjenige aus, welches Sie bootfähig machen wollen.

   Warnung: *Alle Daten auf diesem Laufwerk werden gelöscht.*
3. Klicken Sie auf **Erstellen**.
4. Warten Sie, bis die Software das bootfähige Medium erstellt hat.

9.3 Recovery einer Maschine

9.3.1 Physische Maschinen

Dieser Abschnitt erläutert, wie Sie physische Maschinen mithilfe der Weboberfläche wiederherstellen können.

Für die Wiederherstellung folgender Systeme müssen Sie ein Boot-Medium (statt der Weboberfläche) verwenden:

- OS X
- Ein beliebiges Betriebssystem, das auf fabrikneuer Hardware (Bare Metal Recovery) oder zu einer Offline-Maschine wiederhergestellt werden soll

Die Wiederherstellung eines Betriebssystems erfordert immer einen Neustart (Reboot) des Systems. Sie können wählen, ob die Maschine automatisch neu gestartet werden soll – oder ob Ihr der Status **Benutzereingriff erforderlich** zugewiesen werden soll. Das wiederhergestellte System geht automatisch online.

So stellen Sie eine physische Maschine wieder her

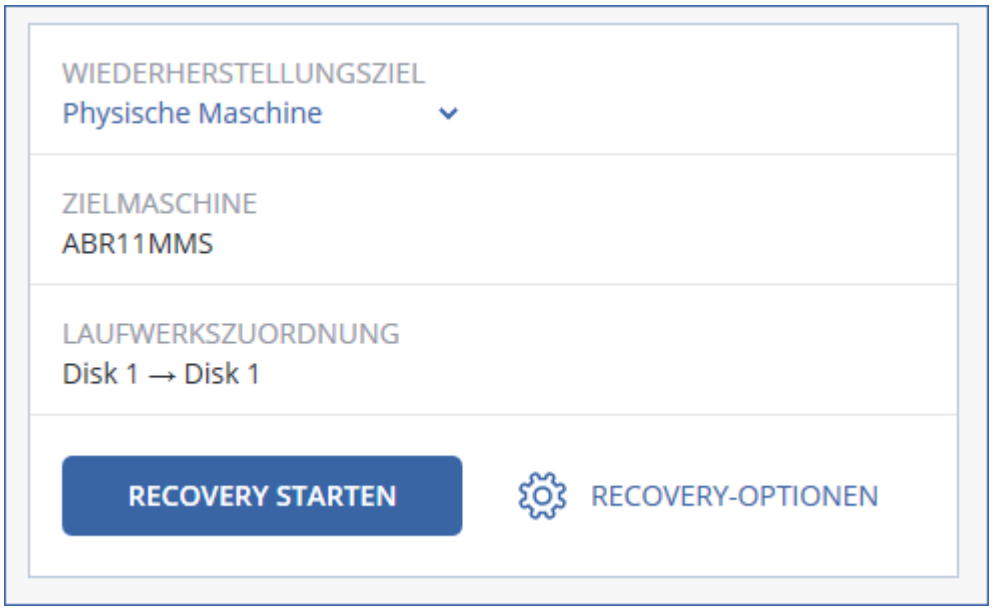
1. Wählen Sie die Maschine, die per Backup gesichert wurde.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:

   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Zielmaschine, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).
   - Stellen Sie die Maschine so wieder her, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 90)' beschrieben ist.
4. Klicken Sie auf **Recovery** –> **Komplette Maschine**.

   Die Software weist die Laufwerke im Backup automatisch den Laufwerken der Zielmaschine zu.

   - Wenn Sie eine andere physische Maschine als Recovery-Ziel verwenden wollen, klicken Sie auf **Zielmaschine** und wählen Sie dann eine Zielmaschine aus, die online ist.
   - Sollte die Laufwerkszuordnung fehlschlagen, können Sie die Maschine auch so wiederherstellen, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 90)' beschrieben ist. Mit dem Medium können Sie die Auswahl der wiederherzustellenden Laufwerke und die Zuordnung der Laufwerke manuell durchführen.



5. Klicken Sie auf **Recovery starten**.
6. Bestätigen Sie, dass die Daten auf den Laufwerken durch die Datenversionen überschrieben werden sollen, die im Backup vorliegen. Bestimmen Sie, ob ein automatischer Neustart der Maschine erfolgen soll.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

9.3.2 Physische Maschinen als virtuelle Maschinen wiederherstellen

Dieser Abschnitt erläutert, wie Sie eine physische Maschine über die Weboberfläche als virtuelle Maschine wiederherstellen können. Damit Sie diese Aktion ausführen können, muss mindestens ein Agent für VMware oder ein Agent für Hyper-V installiert und registriert sein.

Weiter Informationen zu P2V-Migrationen finden Sie im Abschnitt 'Migration von Maschinen (S. 194)'.

So können Sie eine physische Maschine als virtuelle Maschine wiederherstellen

1. Wählen Sie die Maschine, die per Backup gesichert wurde.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:

   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).
   - Stellen Sie die Maschine so wieder her, wie es im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 90)' beschrieben ist.
4. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
5. Wählen Sie unter **Wiederherstellungsziel** die Option **Virtuelle Maschine**.
6. Klicken Sie auf **Zielmaschine**.
   a. Bestimmen Sie den Hypervisor (**VMware ESXi** oder **Hyper-V**).

      Für die Aktion muss mindestens ein Agent für VMware oder ein Agent für Hyper-V installiert sein.

   b. Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll. Die Option 'Neue Maschine' ist vorteilhafter, da hier die Laufwerkskonfiguration im Backup nicht mit der Laufwerkskonfiguration der Zielmaschine exakt übereinstimmen muss.

   c. Wählen Sie den Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Zielmaschine aus.

   d. Klicken Sie auf **OK**.
7. [Optional] Wenn Sie eine neue Maschine als Recovery-Ziel verwenden, können Sie außerdem noch Folgendes tun:
   - Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V – und bestimmten Sie dann den Datenspeicher (Storage) für die neue virtuelle Maschine.

- Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.

8. Klicken Sie auf **Recovery starten**.
9. Wenn Sie eine vorhandene virtuelle Maschine als Recovery-Ziel verwenden, müssen Sie noch bestätigen, dass deren Laufwerke überschrieben werden.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

9.3.3 Virtuelle Maschine

Während der Wiederherstellung zu einer virtuellen Maschine muss diese gestoppt sein. Die Software stoppt die entsprechende Maschine ohne weitere Benutzeraufforderung. Wenn die Wiederherstellung abgeschlossen wurde, müssen Sie die Maschine manuell wieder starten.

Dieses Verhalten kann durch die Verwendung der Recovery-Option für die VM-Energieverwaltung geändert werden (klicken Sie dazu auf **Recovery-Optionen** –> **VM-Energieverwaltung**).

So stellen Sie eine virtuelle Maschine wieder her

1. Wählen Sie eine der nachfolgenden Varianten:
   - Wählen Sie eine zu sichernde Maschine, klicken Sie auf **Recovery** und wählen Sie dann einen Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).
2. Klicken Sie auf **Recovery** –> **Komplette Maschine**.
3. Wenn die Wiederherstellung auf einer physischen Maschine durchführen wollen, wählen Sie bei **Wiederherstellungsziel** das Element **Physische Maschine**. Ansonsten können Sie diesen Schritt überspringen.

Eine Wiederherstellung auf einer physischen Maschine ist nur dann möglich, wenn die Laufwerkskonfiguration im Backup exakt mit der Laufwerkskonfiguration der Zielmaschine übereinstimmt.

Falls dies zutrifft, fahren Sie mit Schritt 4 im Abschnitt 'Physische Maschine (S. 85)' fort. Falls dies nicht zutrifft, empfehlen wir Ihnen, eine V2P-Migration mithilfe eines Boot-Mediums (S. 90) durchzuführen.

4. Die Software wählt automatisch die ursprüngliche Maschine als Zielmaschine aus.

   Wenn Sie die Wiederherstellung auf eine andere virtuelle Maschine durchführen wollen, müssen Sie auf **Zielmaschine** klicken und dann Folgendes tun:

   a. Wählen Sie den Hypervisor (**VMware ESXi**, **Hyper-V** oder **Virtuozzo**).

      Nur virtuelle Virtuozzo-Maschinen können zu Virtuozzo wiederhergestellt werden. Weiter Informationen zu V2V-Migrationen finden Sie im Abschnitt 'Migration von Maschinen (S. 194)'.

   b. Bestimmen Sie, ob eine neue oder eine vorhandene Maschine als Recovery-Ziel verwendet werden soll.

   c. Wählen Sie den Host und eine vorhandene Maschine – oder spezifizieren Sie einen Namen für die neue Maschine.

   d. Klicken Sie auf **OK**.

5. [Optional] Wenn Sie eine neue Maschine als Recovery-Ziel verwenden, können Sie außerdem noch Folgendes tun:

   - Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V und Virtuozzo – und bestimmten Sie dann den Datenspeicher (Storage) für die neue virtuelle Maschine.
   - Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.

6. Klicken Sie auf **Recovery starten**.

7. Wenn Sie eine vorhandene virtuelle Maschine als Recovery-Ziel verwenden, müssen Sie noch bestätigen, dass deren Laufwerke überschrieben werden.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

9.3.4 Laufwerke mithilfe eines Boot-Mediums wiederherstellen

Genau Informationen über die Erstellung eines bootfähigen Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen (S. 84)'.

So stellen Sie Laufwerke mithilfe eines Boot-Mediums wieder her

1. Booten Sie die Zielmaschine mit einem Boot-Medium.
2. [Nur bei Wiederherstellung eines Macs] Wenn Sie APFS-formatierte Laufwerke/Volumes zu einer anderen als der ursprünglichen (wie einer fabrikneuen) Maschine wiederherstellen, müssen Sie die ursprüngliche Laufwerkskonfiguration manuell neu erstellen:
   a. Klicken Sie auf **Festplattendienstprogramm**.
   b. Stellen Sie die ursprüngliche Laufwerkskonfiguration wieder her. Anweisungen dazu finden Sie unter https://support.apple.com/guide/disk-utility/welcome.
   c. Klicken Sie auf **Festplattendienstprogramm** > **Festplattendienstprogramm beenden**.
3. Klicken Sie entweder auf **Diese Maschine lokal verwalten** oder zweimal auf **Rescue Bootable Media** (abhängig vom verwendeten Typ des Mediums).
4. Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird, klicken Sie auf **Extras** –> **Proxy-Server** und spezifizieren Sie dann den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers. Ansonsten können Sie diesen Schritt überspringen.
5. [Optional] Klicken Sie bei der Wiederherstellung von Windows oder Linux auf **Tools** –> **Medium im Backup Service registrieren** und spezifizieren Sie dann das Registrierungstoken, das Sie beim Download des Mediums erhalten haben. Wenn Sie dies tun, müssen Sie keine Anmeldedaten oder keinen Registrierungscode eingeben, um auf den Cloud Storage zuzugreifen (wie in Schritt 8 beschrieben).
6. Klicken Sie innerhalb der Willkommensseite auf **Recovery**.
7. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
8. Spezifizieren Sie den Backup-Speicherort:
   - Wählen Sie das Element **Cloud Storage**, um Dateien aus dem Cloud Storage wiederherzustellen. Geben Sie die Anmeldedaten des Kontos ein, dem die gesicherte Maschine zugewiesen wird.

     Bei der Wiederherstellung von Windows oder Linux haben Sie die Möglichkeit, einen Registrierungscode anzufordern und diesen statt der Anmeldeinformationen zu verwenden. Klicken Sie auf **Registrierungscode verwenden** –> **Den Code anfordern**. In der Software werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann auf einer anderen Maschine durchführen. Der Registrierungscode ist für eine (1) Stunde gültig.
   - Um eine Wiederherstellung von einem lokalen Ordner oder einem Netzwerkordner aus durchzuführen, wählen Sie den entsprechenden Ordner über das Element **Lokale Ordner** oder **Netzwerkordner** aus.

   Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.
9. Wählen Sie das Backup, aus dem die Daten wiederhergestellt werden sollen. Geben Sie das Kennwort für das Backup an, falls Sie dazu aufgefordert werden.
10. Wählen Sie bei **Backup-Inhalte** die wiederherzustellenden Laufwerke. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.

11. Die Software ordnet unter **Recovery-Ziel** die ausgewählten Laufwerke automatisch den Ziellaufwerken zu.

    Falls die Zuordnung erfolglos ist oder falls Sie mit dem Zuordnungsergebnis unzufrieden sind, können Sie die Laufwerke auch manuell zuordnen.

    Eine Änderung des Laufwerk-Layouts kann die Bootfähigkeit des Betriebssystems beeinflussen. Verwenden Sie möglichst das ursprüngliche Laufwerkslayout der Maschine, außer Sie sind sich über das Ergebnis der Änderung absolut sicher.

12. [Bei einer Wiederherstellung von Linux] Falls die gesicherte Maschine logische Volumes hatte (LVM) und Sie die ursprüngliche LVM-Struktur nachbilden wollen:
    a. Stellen Sie sicher, dass die Anzahl der Laufwerke der Zielmaschine und jede Laufwerkskapazität der der ursprünglichen Maschine entspricht oder diese übersteigt – und klicken Sie dann auf **RAID/LVM anwenden**.
    b. Überprüfen Sie die Volume-Struktur und klicken Sie dann auf **RAID/LVM anwenden** um sie zu erstellen.
13. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
14. Wählen Sie **OK**, um die Wiederherstellung zu starten.

9.3.5 Universal Restore verwenden

Moderne Betriebssysteme behalten normalerweise ihre Bootfähigkeit, wenn sie auf abweichender Hardware (beinhaltet auch VMware- und Hyper-V-Maschinen) wiederhergestellt werden. Falls ein Betriebssystem nach einer Wiederherstellung dennoch nicht mehr bootet, können Sie das Tool 'Universal Restore' verwenden, um diejenigen Treiber und Module zu aktualisieren, die das Betriebssystem zum Starten auf der neuen Hardware/Maschine benötigt.

Universal Restore kann für Windows und Linux verwendet werden.

So verwenden Sie Universal Restore

1. Booten Sie die Maschine mithilfe eines Boot-Mediums.
2. Klicken Sie auf den Befehl **Universal Restore anwenden**.
3. Sollte es mehrere Betriebssysteme auf der Maschine geben, dann wählen Sie dasjenige System aus, welches von Universal Restore angepasst werden soll.
4. [Nur bei Windows] Konfigurieren Sie die 'Erweiterten Einstellungen' (S. 91).
5. Klicken Sie auf **OK**.

9.3.5.1 Universal Restore unter Windows

Vorbereitung

Treiber vorbereiten

Bevor Sie Universal Restore auf ein Windows-Betriebssystem anwenden, sollten Sie sicherstellen, dass Sie über die passenden Treiber für den neuen Festplatten-Controller und den Chipsatz des Mainbords verfügen. Diese Treiber sind für den Start des Betriebssystem unerlässlich. Verwenden Sie (sofern vorhanden) die Treiber-CD/-DVD, die der Hardware-Hersteller Ihrem Computer/Mainboard beigelegt hat – oder laden Sie benötigten Treiber von der Website des Herstellers herunter. Die Treiber sollten die Dateierweiterung *.inf verwenden. Wenn Sie die Treiber im Format *.exe, *.cab oder *.zip herunterladen, extrahieren Sie diese mit einer entsprechenden Dritthersteller-Anwendung.

Eine empfehlenswerte Vorgehensweise ist es, die benötigten Treiber (für die in Ihrer Organisation verwendete Hardware) an einem zentralen Aufbewahrungsort ('Repository') zu speichern und dabei nach Gerätetyp oder Hardware-Konfiguration zu sortieren. Sie können eine Kopie des Treiber-Repositorys zur leichteren Verwendung auch auf DVD oder USB-Stick vorhalten. Suchen Sie daraus die benötigten Treiber aus, um diese dem bootfähigen Medium hinzufügen zu können. Erstellen Sie dann für jeden Ihrer Server ein benutzerdefiniertes Boot-Medium mit den benötigten Treibern (und der benötigten Netzwerk-Konfiguration). Alternativ können Sie den Pfad zum Repository auch bei jeder Verwendung von Universal Restore spezifizieren.

Überprüfen Sie, dass auf die Treiber in der bootfähigen Umgebung zugegriffen werden kann.

Überprüfen Sie, dass Sie beim Arbeiten mit dem bootfähigen Medium auf das Gerät mit den Treibern zugreifen können. Ein WinPE-basiertes Medium sollte dann zum Einsatz kommen, wenn ein Gerät unter Windows verfügbar ist, von einem Linux-basierten Medium aber nicht erkannt wird.

Universal Restore-Einstellungen

Automatische Suche nach Treibern

Spezifizieren Sie, wo das Programm nach Treibern für die Hardware-Abstraktionsschicht (HAL, Hardware Abstraction Layer) sowie für Festplatten-Controller und Netzwerkkarten suchen soll:

- Befinden sich die Treiber auf einem Datenträger (CD/DVD) des Herstellers oder einem anderen Wechselmedium, dann aktivieren Sie **Wechselmedien durchsuchen**.
- Liegen die Treiber in einem Netzwerkordner oder auf einem bootfähigen Medium, so spezifizieren Sie den Pfad zu diesem Ordner durch Anklicken von **Ordner durchsuchen**.

Zusätzlich wird Universal Restore den Standardspeicherort (Ordner) für Treiber durchsuchen. Dessen genaue Position ist über den Registry-Wert **DevicePath** definiert, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** gefunden werden kann. Üblicherweise befindet sich dieser Speicherordner im Unterverzeichnis 'WINDOWS/inf'.

Universal Restore führt im spezifizierten Ordner und seinen Unterordnern eine rekursive Suche durch, ermittelt dann unter allen verfügbaren Festplatten-Controller- und HAL-Treibern diejenigen, die am besten geeignet sind, und installiert diese Treiber schließlich im System. Universal Restore sucht außerdem nach Treibern für Netzwerkkarten. Der Pfad zu einem gefundenen Treiber wird dem Betriebssystem dann von Universal Restore mitgeteilt. Falls die Hardware über mehrere Netzwerkkarten verfügt, versucht Universal Restore, die Treiber für alle Karten zu konfigurieren.

Auf jeden Fall zu installierende Massenspeichertreiber

Sie benötigen diese Einstellung falls:

- Die Hardware einen speziellen Massenspeicher-Controller verwendet – z.B. einen RAID- (insbesondere NVIDIA RAID) oder Fibre Channel-Adapter.
- Sie ein System zu einer virtuellen Maschine migriert haben, die einen SCSI-Festplatten-Controller verwendet. Verwenden Sie diejenigen SCSI-Treiber, die zusammen mit Ihrer Virtualisierungssoftware ausgeliefert werden. Alternativ können Sie die neueste Treiberversion vermutlich auch von der Website des betreffenden Software-Herstellers herunterladen.
- Falls die automatische Suche nach Treibern nicht hilft, das System zu booten.

Spezifizieren Sie die entsprechenden Treiber, indem Sie auf den Befehl **Treiber hinzufügen** klicken. Treiber, die hier definiert werden, werden auch dann (mit entsprechenden Warnmeldungen) installiert, wenn das Programm einen besseren Treiber findet.

Der Universal Restore-Prozess

Klicken Sie auf **OK**, nachdem Sie die benötigten Einstellungen spezifiziert haben.

Falls Universal Restore an den angegebenen Speicherorten keinen kompatiblen Treiber findet, zeigt es eine Eingabeaufforderung für das Problemgerät an. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

- Fügen Sie den Treiber einem der zuvor spezifizierten Speicherorte hinzu und klicken Sie dann auf **Wiederholen**.
- Klicken Sie auf **Ignorieren**, falls Sie sich nicht mehr an den Speicherort erinnern können, damit der Prozess fortgesetzt wird. Sollte das Ergebnis nicht zufriedenstellend sein, dann wenden Sie Universal Restore erneut an. Spezifizieren Sie bei Konfiguration der Aktion den benötigten Treiber.

Sobald Windows bootet, wird es die Standardprozedur zur Installation neuer Hardware initialisieren. Der Treiber für die Netzwerkkarte wird ohne weitere Nachfrage installiert, sofern er eine passende Microsoft Windows-Signatur hat. Anderenfalls verlangt Windows eine Bestätigung, dass der unsignierte Treiber installiert werden soll.

Danach können Sie die Netzwerk-Verbindung konfigurieren und weitere Treiber spezifizieren (beispielsweise für die Grafikkarte und USB-Geräte).

9.3.5.2 Universal Restore unter Linux

Universal Restore kann auf Linux-Betriebssysteme mit der Kernel-Version 2.6.8 (oder höher) angewendet werden.

Wenn Universal Restore auf ein Linux-Betriebssystem angewendet wird, aktualisiert es ein temporäres Dateisystem, das auch als 'Initial RAM-Disk' (initrd) bekannt ist. Dadurch wird gewährleistet, dass das Betriebssystem auch auf neuer, abweichender Hardware booten kann.

Universal Restore kann dieser 'Initial RAM-Disk' benötigte Module für die neue Hardware hinzufügen (einschließlich Gerätetreiber). Es findet die benötigten Module normalerweise im Verzeichnis **/lib/modules**. Falls Universal Restore ein benötigtes Modul nicht finden kann, schreibt es den Dateinamen des Moduls in das Log.

Universal Restore kann unter Umständen die Konfiguration des GRUB-Boot-Loaders ändern. Dies kann beispielsweise notwendig sein, um die Bootfähigkeit des Systems zu gewährleisten, falls die neue Maschine ein anderes Volume-Layout als die ursprüngliche hat.

Universal führt keine Änderungen am Linux-Kernel durch!

Zur ursprünglichen 'Initial RAM-Disk' zurücksetzen

Sie können bei Bedarf zur ursprünglichen 'Initial RAM-Disk' zurücksetzen.

Die 'Initial RAM-Disk' ist auf der Maschine in Form einer Datei gespeichert. Bevor Universal Restore die 'Initial RAM-Disk' zum ersten Mal aktualisiert, speichert es diese als Kopie ab – und zwar im gleichen Verzeichnis. Der Name dieser Kopie entspricht dem Dateinamen, ergänzt um den Suffix **_acronis_backup.img**. Diese Kopie wird auch dann nicht überschrieben, wenn Sie Universal Restore mehrmals ausführen (beispielsweise nachdem Sie fehlende Treiber hinzugefügt haben).

Sie können folgendermaßen vorgehen, um zur ursprünglichen 'Initial RAM-Disk' zurückzukehren:

- Benennen Sie die Kopie passend um. Führen Sie beispielsweise einen Befehl, der ungefähr so aussieht:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img
initrd-2.6.16.60-0.21-default
```

- Spezifizieren Sie die Kopie in der Zeile **initrd** der GRUB-Boot-Loader-Konfiguration.

9.4 Dateien wiederherstellen

9.4.1 Dateien über die Weboberfläche wiederherstellen

1. Wählen Sie diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie den gewünschten Recovery-Punkt aus. Beachten Sie dabei, dass Recovery-Punkte nach Speicherorten gefiltert werden.

   Falls es sich bei der ausgewählten Maschine um eine physische Maschine handelt und diese offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der folgenden Möglichkeiten vor:

   - [Empfohlen] Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Zielmaschine, die online ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).
   - Laden Sie die Dateien aus dem Cloud Storage herunter (S. 95).
   - Verwenden Sie ein bootfähiges Medium (S. 97).
4. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.
5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.

   Hinweis: *Für Laufwerk-Backups, die im Cloud Storage gespeichert sind, ist keine Suchfunktion verfügbar.*
6. Wählen Sie die Dateien, die Sie wiederherstellen wollen.
7. Falls Sie die Dateien als .zip-Archiv speichern wollen, müssen Sie zuerst auf **Download** klicken, dann den Zielspeicherort für die Daten bestimmen und schließlich auf **Speichern** klicken. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.

   Ein Download ist nicht möglich, weil die Gesamtgröße der ausgewählten Dateien 100 MB überschreitet oder weil in Ihrer Auswahl Ordner enthalten sind.
8. Klicken Sie auf **Recovery**.

   Wählen Sie bei **Recovery zu** eine der folgenden Möglichkeiten:

   - Die ursprüngliche Maschine, auf der sich die Dateien im Backup befunden haben, die Sie wiederherstellen wollen (sofern auf der Maschine ein Agent installiert ist).
   - Die Maschine, auf welcher ein Agent für VMware, ein Agent für Hyper-V oder ein Agent für Virtuozzo installiert ist (sofern die Dateien von einer virtuellen ESXi-, Hyper-V- oder Virtuozzo-Maschine stammen).

   Dies ist die Zielmaschine für die Wiederherstellung. Sie können bei Bedarf auch eine andere Maschine auswählen.

9. Wählen Sie bei **Pfad** das gewünschte Ziel für die Wiederherstellung. Sie können eine der folgenden Optionen wählen:
   - Der ursprüngliche Speicherort (bei Wiederherstellung zur ursprünglichen Maschine)
   - Ein lokaler Ordner auf der Zielmaschine
   - Ein Netzwerkordner, auf von der Zielmaschine aus verfügbar ist.
10. Klicken Sie auf **Recovery starten**.
11. Wählen Sie eine der folgenden Optionen zum Überschreiben:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

9.4.2 Dateien aus dem Cloud Storage herunterladen

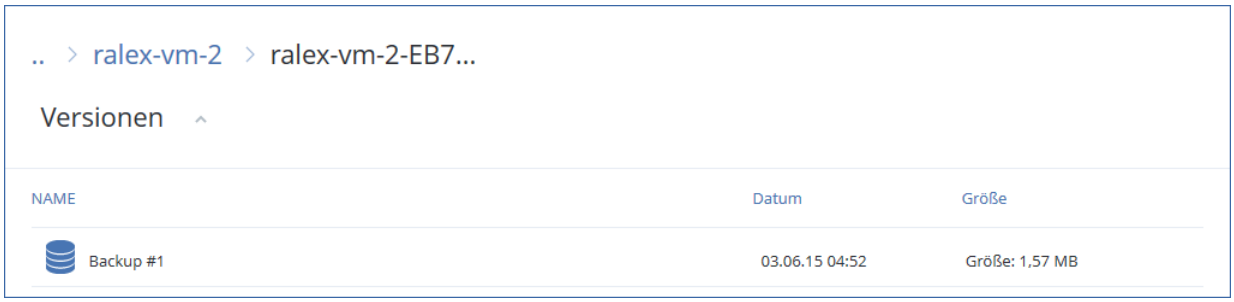
Sie können den Cloud Storage durchsuchen, die Inhalte von Backups einsehen und benötigte Dateien herunterladen.

Einschränkungen

- Die Backups von SQL-Datenbanken, Exchange-Datenbanken und eines Systemzustands können nicht durchsucht werden.
- Für ein optimales Download-Erlebnis sollten Sie nicht mehr als 100 MB gleichzeitig herunterladen. Um größere Datenmengen schnell aus der Cloud abzurufen, verwenden Sie die Prozedur zur Wiederherstellung von Dateien (S. 94).

So laden Sie Dateien aus dem Cloud Storage herunter

1. Wählen Sie eine Maschine, die per Backup gesichert wurde.
2. Klicken Sie auf **Recovery** –> **Weitere Wiederherstellungsmöglichkeiten...** –> **Dateien herunterladen**.
3. Geben Sie die Anmeldedaten des Kontos ein, dem die gesicherte Maschine zugewiesen wird.
4. [Beim Durchsuchen von Laufwerk-Backups] Klicken Sie unter **Versionen** auf dasjenige Backup, dessen Dateien Sie wiederherstellen wollen.



[Beim Durchsuchen von Datei-Backups] Sie können den Backup-Zeitpunkt im nächsten Schritt auswählen (unter dem Zahnradsymbol, das rechts neben der ausgewählten Datei liegt). Standardmäßig werden die Dateien des letzten (jüngsten) Backups wiederhergestellt.

5. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien abzurufen.

6. Aktivieren Sie die Kontrollkästchen derjenigen Elemente, die Sie wiederherstellen müssen – und klicken Sie dann auf **Download**.

   Falls Sie eine einzelne Datei auswählen, wird diese 'wie vorliegend' heruntergeladen. Anderenfalls werden die ausgewählten Daten in eine .zip-Datei archiviert.
7. Wählen Sie den Ort, wo die Daten abgelegt werden sollen und klicken Sie auf **Speichern**.

9.4.3 Eine Datei mit ASign signieren

ASign ist ein Service, der es ermöglicht, dass mehrere Personen eine per Backup gesicherte Datei elektronisch unterschreiben (signieren) können. Diese Funktion ist nur für Backups auf Dateiebene verfügbar, die im Cloud Storage gespeichert sind.

Es kann nur je eine Dateiversion gleichzeitig signiert werden. Wenn eine Datei also zu mehreren Zeitpunkten gesichert wurde, müssen Sie die gewünschte Version bestimmten, die signiert werden soll – und nur diese Version wird dann signiert.

ASign kann beispielsweise verwendet werden, um folgende Dateien elektronisch zu signieren:

- Miet- oder Leasing-Verträge
- Kaufverträge
- Kaufvereinbarungen für Wertgegenstände
- Kreditverträge
- Berechtigungsscheine
- Finanzdokumente
- Versicherungsdokumente
- Haftungsverzichtserklärungen
- Gesundheitsdokumente
- Forschungsunterlagen
- Authentizitätzertifikate für Produkte
- Geheimhaltungsvereinbarungen
- Schriftliche Angebote
- Vertraulichkeitsvereinbarungen

- Vereinbarungen mit unabhängigen Vertragspartnern

So können Sie eine Dateiversion signieren

1. Wählen Sie die gewünschte Datei aus, wie es in den Schritten 1-6 des Abschnitts 'Dateien über die Weboberfläche wiederherstellen (S. 94)' beschrieben ist.
2. Überprüfen Sie im linken Fensterbereich, dass der korrekte Zeitpunkt (Datum, Uhrzeit) ausgewählt wurde.
3. Klicken Sie auf **Diese Dateiversion signieren**.
4. Spezifizieren Sie das Kennwort für das Cloud Storage-Konto, unter dem das Backup gespeichert wurde. Der Anmeldename des Kontos wird im Eingabeaufforderungsfenster angezeigt.

   Die Benutzeroberfläche des ASign Service wird in einem Webbrowser-Fenster geöffnet.
5. Fügen Sie bei Bedarf weitere Unterzeichner hinzu, indem Sie deren E-Mail-Adressen spezifizieren. Nach dem Versenden der Einladungen können keine weiteren Unterzeichner mehr hinzugefügt oder entfernt werden. Überprüfen Sie daher, dass auch wirklich alle Personen in der Liste sind, deren Signatur erforderlich ist.
6. Klicken Sie auf **Zum Signieren einladen**, damit die Einladung an die Unterzeichner versendet wird.

   Jeder Unterzeichner erhält eine E-Mail-Nachricht mit der Signatur-Aufforderung. Wenn alle angeforderten Unterzeichner die Datei signiert haben, wird diese noch vom Notary Service beglaubigt und signiert.

   Sie erhalten jeweils Benachrichtigungen, wenn ein Unterzeichner die Datei signiert hat und wenn der komplette Prozess abgeschlossen wurde. Sie können auf die ASign-Webseite zugreifen, indem Sie in einer der E-Mail-Nachrichten, die Sie erhalten, auf **Details anzeigen** klicken.
7. Gehen Sie nach Abschluss des Prozesses zur ASign-Webseite und klicken Sie auf **Dokument abrufen**, um ein .pdf-Dokument herunterzuladen, welches folgende Informationen enthält:
   - Eine Signaturzertifikatsseite mit den zusammengestellten Signaturen.
   - Eine Audit-Trail-Seite mit einem Verlauf folgender Aktivitäten: wann die Einladung an die Unterzeichner gesendet wurde, wann der Unterzeichner die Datei signiert hat usw.

9.4.4 Dateien mit einem Boot-Medium wiederherstellen

Genau Informationen über die Erstellung eines bootfähigen Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen (S. 84)'.

So stellen Sie Dateien mithilfe eines Boot-Mediums wieder her

1. Booten Sie die Zielmaschine mit dem Boot-Medium.
2. Klicken Sie entweder auf **Diese Maschine lokal verwalten** oder zweimal auf **Rescue Bootable Media** (abhängig vom verwendeten Typ des Mediums).
3. Falls in Ihrem Netzwerk ein Proxy-Server verwendet wird, klicken Sie auf **Extras** –> **Proxy-Server** und spezifizieren Sie dann den Host-Namen/die IP-Adresse, den Port und die Anmeldedaten des Proxy-Servers. Ansonsten können Sie diesen Schritt überspringen.
4. [Optional] Klicken Sie bei der Wiederherstellung von Windows oder Linux auf **Tools** –> **Medium im Backup Service registrieren** und spezifizieren Sie dann das Registrierungstoken, das Sie beim Download des Mediums erhalten haben. Wenn Sie dies tun, müssen Sie keine Anmeldedaten oder keinen Registrierungscode eingeben, um auf den Cloud Storage zuzugreifen (wie in Schritt 7 beschrieben).
5. Klicken Sie innerhalb der Willkommensseite auf **Recovery**.
6. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.

7. Spezifizieren Sie den Backup-Speicherort:
   - Wählen Sie das Element **Cloud Storage**, um Dateien aus dem Cloud Storage wiederherzustellen. Geben Sie die Anmeldedaten des Kontos ein, dem die gesicherte Maschine zugewiesen wird.

     Bei der Wiederherstellung von Windows oder Linux haben Sie die Möglichkeit, einen Registrierungscode anzufordern und diesen statt der Anmeldeinformationen zu verwenden. Klicken Sie auf **Registrierungscode verwenden** –> **Den Code anfordern**. In der Software werden der Registrierungslink und Registrierungscode angezeigt. Sie können diese kopieren und die Registrierungsschritte dann auf einer anderen Maschine durchführen. Der Registrierungscode ist für eine (1) Stunde gültig.
   - Um eine Wiederherstellung von einem lokalen Ordner oder einem Netzwerkordner aus durchzuführen, wählen Sie den entsprechenden Ordner über das Element **Lokale Ordner** oder **Netzwerkordner** aus.

   Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.
8. Wählen Sie das Backup, aus dem die Daten wiederhergestellt werden sollen. Geben Sie das Kennwort für das Backup an, falls Sie dazu aufgefordert werden.
9. Wählen Sie bei **Backup-Inhalte** das Element **Ordner/Dateien**.
10. Wählen Sie Daten, die Sie wiederherstellen wollen. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.
11. Spezifizieren Sie bei **Recovery-Ziel** einen gewünschten Ordner. Optional können Sie neuere Dateiversionen vor Überschreibung schützen oder einige Dateien von der Wiederherstellung ausschließen.
12. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
13. Wählen Sie **OK**, um die Wiederherstellung zu starten.

9.4.5 Dateien aus lokalen Backups extrahieren

Sie können Backups nach bestimmten Inhalten durchsuchen und gewünschte Dateien extrahieren.

Anforderungen

- Diese Funktionalität steht nur unter Windows und bei Verwendung des Windows Datei-Explorers zur Verfügung.
- Auf der Maschine, von der aus Sie ein Backup durchsuchen wollen, muss ein Backup Agent installiert sein.
- Folgende, im Backup gesicherte Dateisysteme werden dabei unterstützt: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS oder HFS+.
- Das Backup selbst muss entweder in einem lokalen Ordner oder in einer Netzwerkfreigabe (SMB/CIFS) gespeichert sein.

So extrahieren Sie Dateien aus einem Backup

1. Verwenden Sie den Windows Datei-Explorer, um den Speicherort des Backups aufzurufen.
2. Klicken Sie doppelt auf die Backup-Datei. Die Dateinamen basieren auf folgender Vorlage:

   `<Maschinenname> - <Backup-Plan-GUID>`
3. Sollte das Backup verschlüsselt sein, dann geben Sie das entsprechende Kennwort ein. Ansonsten können Sie diesen Schritt überspringen.

   Der Windows Datei-Explorer zeigt die Recovery-Punkte an.
4. Klicken Sie doppelt auf einen gewünschten Recovery-Punkt.

   Der Windows Datei-Explorer zeigt die im Backup gespeicherten Daten an.

5. Wählen Sie den gewünschten Ordner aus.
6. Kopieren Sie die benötigten Dateien zu einem beliebigen Ordner im Dateisystem.

9.5 Einen Systemzustand wiederherstellen

1. Wählen Sie diejenige Maschine, deren Systemzustand Sie wiederherstellen wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie einen Systemzustand-Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.
4. Klicken Sie auf **Systemzustand wiederherstellen**.
5. Bestätigen Sie, dass der vorliegende Systemzustand mit der Version überschrieben werden soll, die im Backup vorliegt.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

9.6 Eine ESXi-Konfiguration wiederherstellen

Um eine ESXi-Konfiguration wiederherstellen zu können, benötigen Sie ein Linux-basiertes Boot-Medium. Genau Informationen über die Erstellung eines bootfähigen Mediums finden Sie im Abschnitt 'Ein Boot-Medium erstellen (S. 84)'.

Wenn Sie für die Wiederherstellung einer ESXi-Konfiguration einen anderen als den ursprünglichen Host als Ziel verwenden wollen und der ursprüngliche ESXi-Host noch mit dem vCenter Server verbunden ist, sollten Sie diesen ursprünglichen Host vom vCenter Server trennen und entfernen, um unerwartete Probleme bei der Wiederherstellung zu vermeiden. Wenn Sie den ursprünglichen Host gemeinsam mit dem wiederhergestellten Host weiter behalten/verwenden wollen, können Sie ihn nach Abschluss der Wiederherstellung wieder hinzufügen.

Evtl. auf dem Host laufende virtuelle Maschinen werden nicht in das ESXi-Konfigurations-Backup eingeschlossen. Sie können diese jedoch separat per Backup sichern und wiederherstellen.

So stellen Sie eine ESXi-Konfiguration wieder her

1. Booten Sie die Zielmaschine mit dem Boot-Medium.
2. Klicken Sie auf **Diese Maschine lokal verwalten**.
3. Klicken Sie innerhalb der Willkommensseite auf **Recovery**.
4. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
5. Spezifizieren Sie den Backup-Speicherort:
   - Wählen Sie den gewünschten Ordner unter **Lokale Ordner** oder **Netzwerkordner** aus.

   Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen.
6. Wählen Sie bei **Anzeigen** das Element **ESXi-Konfiguration**.
7. Wählen Sie das Backup, aus dem die Daten wiederhergestellt werden sollen. Geben Sie das Kennwort für das Backup an, falls Sie dazu aufgefordert werden.
8. Klicken Sie auf **OK**.
9. Bei **Für neue Datenspeicher zu verwendende Laufwerke** gehen Sie folgendermaßen vor:
   - Wählen Sie bei **ESXi wiederherstellen zu** dasjenige Laufwerk, auf dem die Host-Konfiguration wiederhergestellt werden soll. Wenn Sie den ursprünglichen Host als Ziel für die Wiederherstellung der Konfiguration verwenden, wird das ursprüngliche Laufwerk standardmäßig vorausgewählt.

- [Optional] Wählen Sie bei **Für neue Datenspeicher verwenden** die Laufwerke, auf denen die neuen Datenspeicher erstellt werden sollen. Beachten Sie, dass dabei alle (möglicherweise bereits vorhandenen) Daten auf den ausgewählten Laufwerken verloren gehen. Falls Sie die virtuellen Maschinen in den vorhandenen Datenspeichern bewahren wollen, wählen Sie kein Laufwerk aus.

10. Falls Sie Laufwerke für neue Datenspeicher auswählen, bestimmen Sie auch die Methode, wie diese erstellt werden sollen. Verwenden Sie dazu die Befehle **Einen Datenspeicher auf allen ausgewählten Laufwerken erstellen: Einen Datenspeicher pro Laufwerk erstellen** oder **Einen Datenspeicher auf allen ausgewählten Laufwerken erstellen**.
11. [Optional] Ändern Sie gegebenenfalls bei **Netzwerkzuordnung**, wie die automatische Zuordnung die (im Backup vorliegenden) virtuellen Switche den physischen Netzwerkadaptern zugeordnet hat.
12. [Optional] Klicken Sie auf **Recovery-Optionen**, um zusätzliche Einstellungen zu spezifizieren.
13. Wählen Sie **OK**, um die Wiederherstellung zu starten.

9.7 Recovery-Optionen

Wenn Sie die Recovery-Optionen ändern wollen, klicken Sie während der Konfiguration der Wiederherstellung auf **Recovery-Optionen**.

Verfügbarkeit der Recovery-Optionen

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

- Der Umgebung, in welcher der Agent seine Recovery-Aktionen durchführt (Windows, Linux, macOS oder ein Boot-Medium).
- Die Art der wiederherzustellenden Daten (Laufwerke, Dateien, virtuelle Maschinen, Applikationsdaten).

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

	Laufwerke			**Dateien**				**Virtuelle Maschinen**	**SQL und Exchange**
	Windows	Linux	Boot-Medium	Windows	Linux	macOS	Boot-Medium	ESXi, Hyper-V und Virtuozzo	Windows
Backup-Validierung (S. 101)	+	+	+	+	+	+	+	+	+
Zeitstempel für Dateien (S. 102)	-	-	-	+	+	+	+	-	-
Fehlerbehandlung (S. 101)	+	+	+	+	+	+	+	+	+
Dateifilter (Ausschluss) (S. 102)	-	-	-	+	+	+	+	-	-
Dateisicherheitseinstellungen (S. 102)	-	-	-	+	-	-	-	-	-
Flashback (S. 103)	+	+	+	-	-	-	-	+	-

	Laufwerke			Dateien				Virtuelle Maschinen	SQL und Exchange
	Windows	Linux	Boot-Medium	Windows	Linux	macOS	Boot-Medium	ESXi, Hyper-V und Virtuozzo	Windows
Wiederherstellung mit vollständigem Pfad (S. 103)	-	-	-	+	+	+	+	-	-
Mount-Punkte (S. 103)	-	-	-	+	-	-	-	-	-
Performance (S. 103)	+	+	-	+	+	+	-	+	+
Vor-/Nach-Befehle (S. 104)	+	+	-	+	+	+	-	+	+
SID ändern (S. 105)	+	-	-	-	-	-	-	-	-
VM-Energieverwaltung (S. 106)	-	-	-	-	-	-	-	+	-
Windows-Ereignisprotokoll (S. 106)	+	-	-	+	-	-	-	Nur Hyper-V	+

9.7.1 Backup-Validierung

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

Die Voreinstellung ist: **Deaktiviert**.

Die Validierung berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Es gibt nur eine Ausnahmen, nämlich die Validierung von Datei-Backups, die im Cloud Storage gespeichert sind. Diese Backups werden validiert, indem die Konsistenz der im Backup gespeicherten Metadaten überprüft wird.

Eine Validierung ist ein zeitaufwendiger Prozess (auch bei inkrementellen oder differentiellen Backups, die normalerweise kleiner sind). Hintergrund ist, dass die Aktion nicht einfach nur die tatsächlich in dem betreffenden Backup enthaltenen Daten validiert, sondern alle Daten, die ausgehend von diesem Backup wiederherstellbar sind. Dies erfordert unter Umständen auch einen Zugriff auf zuvor erstellte (abhängige) Backups.

9.7.2 Fehlerbehandlung

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

Erneut versuchen, wenn ein Fehler auftritt

Die Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 30. Abstand zwischen den Versuchen: 30 Sekunden.**

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

Während der Durchführung keine Meldungen bzw. Dialoge anzeigen (Stiller Modus)

Die Voreinstellung ist: **Deaktiviert**.

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

9.7.3 Zeitstempel für Dateien

Diese Option gilt nur für die Wiederherstellung von Dateien.

Diese Option bestimmt, ob wiederhergestellte Dateien den ursprünglichen Zeitstempel aus dem Backup übernehmen – oder ob ihnen das Datum/die Zeit des aktuellen Wiederherstellungszeitpunkts zugewiesen wird.

Wenn diese Option aktiviert ist, werden den Dateien die aktuelle Zeit und das aktuelle Datum zugewiesen.

Die Voreinstellung ist: **Aktiviert**.

9.7.4 Dateifilter (Ausschluss)

Diese Option gilt nur für die Wiederherstellung von Dateien.

Diese Option definiert, welche Dateien und Ordner während eines Recovery-Prozesses übersprungen und so von der Liste der wiederherzustellenden Elemente ausgeschlossen werden.

Hinweis: *Ausschließungen überschreiben eine mögliche Auswahl von wiederherzustellenden Datenelementen. Falls Sie beispielsweise festlegen, dass die Datei 'MeineDatei.tmp' wiederhergestellt werden soll und Sie aber zudem alle .tmp-Dateien ausschließen, dann wird 'MeineDatei.tmp' nicht wiederhergestellt.*

9.7.5 Dateisicherheitseinstellungen

Diese Option gilt, wenn Sie Dateien aus Laufwerk- und Datei-Backups von NTFS-formatierten Volumes wiederherstellen.

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

Die Voreinstellung ist: **Aktiviert**.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Zugriffsrechte aus dem Backup beibehalten sollen – oder ob sie die NTFS-Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

9.7.6 Flashback

Diese Option gilt – ausgenommen beim Mac – für die Wiederherstellung von Laufwerken und Volumes auf physischen und virtuellen Maschinen.

Diese Option funktioniert nur, wenn das Volume-Layout des gerade wiederhergestellten Laufwerks exakt mit dem des Ziellaufwerks übereinstimmt.

Wenn diese Option aktiviert ist, werden nur solche Daten wiederhergestellt, hinsichtlicher derer sich das Backup und das Ziellaufwerk unterscheiden. Dadurch kann die Wiederherstellung von physischen und virtuellen Maschinen beschleunigt werden. Der Datenvergleich erfolgt auf Blockebene.

Wenn Sie eine physische Maschine wiederherstellen, ist die Voreinstellung: **Deaktiviert**.

Wenn Sie eine virtuelle Maschine wiederherstellen, ist die Voreinstellung: **Aktiviert**.

9.7.7 Wiederherstellung mit vollständigem Pfad

Diese Option gilt nur, wenn Daten aus einem Datei-Backup wiederhergestellt werden.

Wenn diese Option aktiviert wird, erhalten die Dateien am Zielspeicherort wieder ihren vollständigen (ursprünglichen) Pfad.

Die Voreinstellung ist: **Deaktiviert**.

9.7.8 Mount-Punkte

Diese Option gilt nur unter Windows und wenn Daten aus einem Datei-Backup wiederhergestellt werden.

Aktivieren Sie diese Option, um Dateien und Ordner wiederherzustellen, die auf gemounteten Volumes gespeichert waren und mit aktivierter Option 'Mount-Punkte (S. 73)' gesichert wurden.

Die Voreinstellung ist: **Deaktiviert**.

Diese Option ist nur wirksam, wenn Sie einen Ordner wiederherstellen wollen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. Wenn Sie einen Ordner innerhalb des Mount-Punktes oder den Mount-Punkt selbst für eine Recovery-Aktion wählen, werden die gewählten Elemente unabhängig vom Wert der Option '**Mount-Punkte**' wiederhergestellt.

Hinweis: *Beachten Sie, dass für den Fall, dass das Volume zum Recovery-Zeitpunkt nicht gemountet ist, die Daten direkt zu demjenigen Ordner wiederhergestellt werden, der zum Backup-Zeitpunkt der Mount-Punkt war.*

9.7.9 Performance

Diese Option bestimmt, welche Priorität dem Recovery-Prozess innerhalb des Betriebssystems zugewiesen wird.

Die verfügbaren Einstellungen sind: **Niedrig**, **Normal**, **Hoch**.

Voreinstellung ist: **Normal**.

Die Priorität eines Prozesses, der in einem System ausgeführt wird, bestimmt, wie viele CPU-und System-Ressourcen ihm zugewiesen werden. Durch ein Herabsetzen der Recovery-Priorität werden mehr Ressourcen für andere Applikationen freigeben. Das Heraufsetzen der Recovery-Priorität kann den Wiederherstellungsprozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig

laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren wie der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk.

9.7.10 Vor-/Nach-Befehle

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

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

- Starten Sie den Befehl **Checkdisk**, damit logische Fehler im Dateisystem, physische Fehler oder fehlerhafte Sektoren vor Beginn oder nach Ende der Recovery-Aktion gefunden und behoben werden.

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

Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.

9.7.10.1 Befehl vor Recovery

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

1. Aktivieren Sie den Schalter **Einen Befehl vor der Wiederherstellung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. 'Pause').
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
5. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
6. Klicken Sie auf **Fertig**.

Kontrollkästchen	**Auswahl**			
Wiederherstellung scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Wiederherstellung erst ausführen, wenn die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Recovery nur durchführen, nachdem der Befehl erfolgreich ausgeführt	Recovery nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder	Nicht verfügbar	Recovery gleichzeitig mit Befehlsausführung durchführen, unabhängig vom

	wurde. Wiederherstellung scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Misserfolg der Ausführung.		Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

9.7.10.2 Befehl nach Recovery

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

1. Aktivieren Sie den Schalter **Einen Befehl nach der Wiederherstellung ausführen**.
2. Geben Sie im Feld **Befehl** ein Kommando ein oder wählen Sie eine vorbereitete Stapelverarbeitungsdatei aus dem Dateisystem aus.
3. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
4. Tragen Sie, sofern erforderlich, in das Feld **Argumente** entsprechende Parameter für die Befehlsausführung ein.
5. Aktivieren Sie das Kontrollkästchen **Wiederherstellung scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls besonders wichtig für Sie ist. Der Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Sollte die Befehlsausführung fehlschlagen, erhält der Recovery-Status den Wert '**Fehler**'.

   Wenn das Kontrollkästchen deaktiviert ist, hat das Ergebnis der Befehlsausführung keinen Einfluss darauf, ob die Recovery-Ausführung als erfolgreich oder fehlgeschlagen eingestuft wird. Sie können das Ergebnis der Befehlsausführung in der Registerkarte **Aktivitäten** überwachen.
6. Klicken Sie auf **Fertig**.

Hinweis: *Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.*

9.7.11 SID ändern

Diese Option ist gültig, wenn Sie Windows 8.1/Windows Server 2012 R2 (oder früher) wiederherstellen.

Diese Option gilt nicht, wenn eine Wiederherstellung zu einer virtuellen Maschine (als Ziel) mit einem Agenten für VMware oder einem Agenten für Hyper-V durchgeführt wird.

Die Voreinstellung ist: **Deaktiviert**.

Die Software kann eine eindeutige SID (Computer Security Identifier) für das wiederhergestellte Betriebssystem erstellen. Sie benötigen diese Option nur, wenn Sie die Betriebsfähigkeit von Dritthersteller-Software sicherstellen müssen, die von der Computer-SID abhängt.

Eine Änderung der SID auf einem bereitgestellten oder wiederhergestellten System wird von Microsoft offiziell nicht unterstützt. Wenn Sie diese Option verwenden, tun Sie dies also auf eigenes Risiko hin.

9.7.12 VM-Energieverwaltung

Diese Optionen gelten nur, wenn eine Wiederherstellung zu einer virtuellen Maschine (als Ziel) durchgeführt wird und dafür ein Agent für VMware, ein Agent für Hyper-V oder ein Agent für Virtuozzo verwendet wird.

Virtuelle Zielmaschinen bei Start der Wiederherstellung ausschalten

Die Voreinstellung ist: **Aktiviert**.

Eine vorhandene Maschine kann nicht als Wiederherstellungsziel verwendet werden, solange sie online ist. Mit dieser Option wird die Zielmaschine automatisch ausgeschaltet, sobald die Wiederherstellung startet. Möglicherweise vorhandene/aktive Benutzer werden dabei von der Maschine getrennt und nicht gespeicherte Daten gehen verloren.

Deaktivieren Sie das Kontrollkästchen für diese Option, wenn Sie die virtuelle Maschinen vor der Wiederherstellung manuell ausschalten wollen.

Virtuelle Zielmaschine nach Abschluss der Wiederherstellung einschalten

Die Voreinstellung ist: **Deaktiviert**.

Wenn eine Maschine (aus einem Backup) zu einer anderen Maschine wiederhergestellt wird, kann es passieren, dass das Replikat der vorhandenen Maschine anschließend im Netzwerk erscheint. Sie können dies vermeiden, wenn Sie die wiederhergestellte Maschine manuell einschalten, nachdem Sie die notwendigen Vorsichtsmaßnahmen getroffen haben.

9.7.13 Windows-Ereignisprotokoll

Diese Option gilt nur für Windows-Betriebssysteme.

Diese Option definiert, ob die Agenten für alle Recovery-Aktionen entsprechende Ereigniseinträge im Windows-Anwendungsereignisprotokoll hinterlegen sollen. Sie können die Protokolleinträge über die Windows-Ereignisanzeige einsehen, die per Eingabebefehl (eventvwr.exe) oder per Menü (**Systemsteuerung** –> **Verwaltung** –> **Ereignisanzeige**) aufgefrufen werden kann. Sie können die Ereignisse filtern, die geloggt werden.

Die Voreinstellung ist: **Deaktiviert**.

10 Disaster Recovery

Die Disaster Recovery-Funktionalität ermöglicht es Ihnen, eine virtuelle Maschine (VM) in der Cloud zu besitzen. Bei einem Desaster kann der Workload umgehend von der betroffenen/beschädigten Maschine auf eine entsprechende Cloud-VM umgeschaltet werden, was auch Failover genannt wird.

Damit die Cloud-Maschine in Ihr lokales TCP/IP-Netzwerk (LAN) eingebunden ist, müssen Sie Ihr LAN über einen sicheren VPN-Tunnel in die Cloud erweitern. Das lässt sich einfach durch Installation einer VPN-Appliance umsetzen, die in zwei Ausführungen mitgeliefert wird: eine für VMware ESXi und eine für Hyper-V.

Sobald die VPN-Verbindung konfiguriert und die VM in der Cloud erstellt wurde, können Sie direkt von der Backup-Konsole aus auf diese VM zugreifen. Alternativ können Sie sich auch per RDP oder SSH mit der VM verbinden.

Die Disaster Recovery-Funktionalität ist nur für Administratoren auf Firmenebene verfügbar. Die Administratoren sind dafür verantwortlich, den Benutzerzugriff auf die Cloud-VM einzurichten und die entsprechenden Benutzer zu instruieren, wie diese bei einem Desaster auf die Cloud-VM zugreifen können.

Kostenpflichtige, per Quotas kontrollierbare Ressourcen

Bei einer VM in der Cloud müssen Sie sich keine Gedanken mehr über verfügbare Ersatz-Hardware machen. Aber Sie müssen die Computing-Ressourcen bezahlen, die die VM während ihrer Ausführung belegt bzw. verbraucht. Dazu gehören CPU- und Arbeitsspeicher-Ressourcen (als 'Berechnungspunkte' bestimmt); der von den VM-Dateien belegte Speicherplatz im Datenspeicher sowie eine öffentliche IP-Adresse (sofern benötigt).

Der Speicherplatz im Datenspeicher wird hier auch als 'Disaster Recovery Storage' bezeichnet. Dieser schnelle Storage ist teurer als herkömmlicher Cloud Storage, in dem die Backups gespeichert werden. Die Kosten für den Disaster Recovery Storage beinhalten auch die Kosten für die Infrastruktur, die für die Disaster Recovery-Funktionalität erforderlich ist.

Recovery-Server

Die Cloud-VM kann eine Kopie Ihres lokalen Servers sein, basierend auf den Server-Backups, die in der Cloud gespeichert sind. Diese Maschine wird als **Recovery-Server** bezeichnet.

Ein Recovery-Server ist die meiste Zeit inaktiv. Sie starten ihn nur, wenn Sie einen Testlauf durchführen wollen oder eine Failover-Aktion erforderlich ist. Da der Server nur dann und damit in dieser relativ kurzen Zeit CPU- und RAM-Ressourcen verbraucht, zahlen Sie überwiegend für den Cloud Storage (zur Backup-Aufbewahrung) und dafür, dass ein gewisser Disaster Recovery Storage für Sie reserviert wird. Weitere Vorteile eines Recovery-Servers sind:

- Es sind keine tieferen Kenntnisse über die Software erforderlich, die auf dem Server installiert ist.
- Langzeit-Datenaufbewahrung. Sie können einen Wiederherstellungspunkt auswählen, der Jahre zurückliegt, um entsprechende Datenänderungen einzusehen oder auf gelöschte Daten zuzugreifen.
- Zusätzliche Wiederherstellungsfähigkeiten. Sie können die Maschine komplett wiederherstellen oder eine granulare Wiederherstellung aus demselben Backup durchführen, das zum Disaster Recovery verwendet wird.

Primäre Server

Ein weiterer Cloud-VM-Typ wird als **primärer Server** bezeichnet. Dabei handelt es sich einfach um einen zusätzlichen Server in Ihrem Netzwerk. Der Service ermöglicht Ihnen, eine virtuelle Maschine auf Basis einer der bereitgestellten Vorlagen zu erstellen. Die weitere Wartung des Servers liegt dann in Ihrer Verantwortlichkeit.

Ein primärer Server wird üblicherweise verwendet, um Echtzeit-Datenreplikationen zwischen Servern durchzuführen, die wichtige Applikationen ausführen. Sie richten die Replikation selbst ein, indem Sie die internen Tools der jeweiligen Applikation verwenden. Beispielsweise kann eine Active Directory- oder SQL-Replikation zwischen lokalen Servern und dem primären Server konfiguriert werden.

Alternativ kann ein primärer Server auch in eine AlwaysOn-Verfügbarkeitsgruppe (AAG) oder Datenbankverfügbarkeitsgruppen (DAG) aufgenommen werden.

Beide Methoden erfordern weitreichende Kenntnisse der jeweiligen Applikation und der dazugehörigen Administratorrechte. Ein primärer Server verbraucht fortlaufend Computing-Ressourcen (Berechnungspunkte) und benötigt Speicherplatz im schnellen Disaster Recovery Storage. Zudem sind gewisse Wartungsaktivitäten auf Ihrer Seite erforderlich: Überwachung der Replikation, Installation von Software-Updates, Durchführung von Backups. Die Vorteile sind minimale RPOs und RTOs bei minimaler Belastung der Produktionsumgebung (im Vergleich zum Backup kompletter Server in der Cloud).

Einschränkungen

Für folgende Systeme oder Umstände wird kein Disaster Recovery unterstützt:

- Für Virtuelle Virtuozzo-Maschinen und -Container
- Für Mac-Maschinen
- Für Linux-Maschinen mit logischen Volumes (LVM) oder Volumes, die mit dem XFS-Dateisystem formatiert sind oder Laufwerke ohne eine Partitionstabelle.
- Für Windows-Maschinen mit dynamischen Datenträgern
- Wenn die Backups der ursprünglichen Maschine verschlüsselt sind

Ein Recovery-Server hat eine Netzwerkschnittstelle. Wenn die ursprüngliche mehrere Netzwerkschnittstellen hat, wird nur eine davon emuliert.

Cloud-Server werden nicht verschlüsselt.

10.1 Software-Anforderungen

Unterstützte Betriebssysteme

Der Schutz mit einem Recovery-Server wurde mit folgenden Betriebssystemen getestet:

- Centos 6.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers

Windows-Desktop-Betriebssysteme werden aufgrund von Microsoft-Produktbedingungen nicht unterstützt.

Eine korrekte Funktion der Software mit anderen Windows-Betriebssystemen und Linux-Distributionen ist möglich, wird jedoch nicht garantiert.

Unterstützte Virtualisierungsplattformen

Der Schutz von virtuellen Maschinen mit einem Recovery-Server wurde mit folgenden Virtualisierungsplattformen getestet:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 mit Hyper-V
- Windows Server 2012/2012 R2 mit Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM)
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2
- Virtuelle Azure-Maschinen

Die VPN-Appliance wurde mit folgenden Virtualisierungsplattformen getestet:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 mit Hyper-V
- Windows Server 2012/2012 R2 mit Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausname des Nano Servers
- Microsoft Hyper-V Server 2016

Eine korrekte Funktion der Software mit anderen Virtualisierungsplattformen und Versionen ist möglich, wird jedoch nicht garantiert.

10.2 Eine VPN-Verbindung konfigurieren

Bevor Sie einen primären Server oder Recovery-Server erstellen können, müssen Sie eine VPN-Verbindung zur Cloud-Recovery-Site eingerichtet haben. Die VPN-Verbindung verwendet zwei virtuelle Maschinen:

- Eine VPN-Appliance, die sich lokal auf Ihren Systemen befindet.
- Einen VPN-Server, der sich auf der Cloud-Recovery-Site befindet.

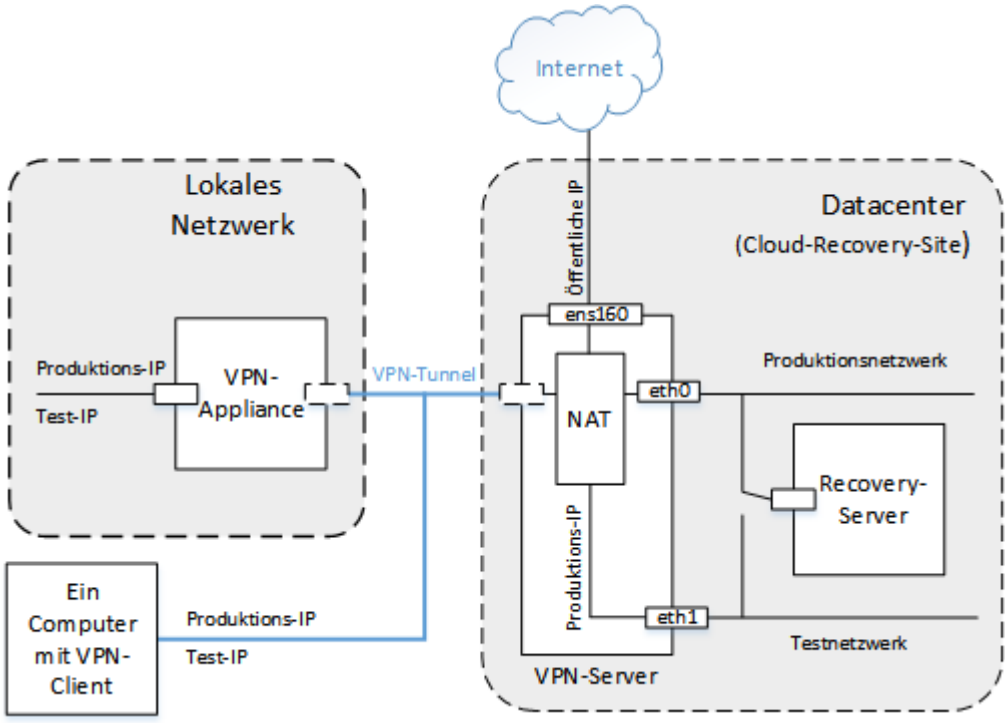
Die VPN-Appliance ermöglicht eine Verbindung zwischen der Cloud-Recovery-Site und Ihrem lokalen Netzwerk (LAN). Für den Fall, dass das lokale Netzwerk einmal ausfällt, benötigen Sie die Möglichkeit, sich direkt mit dem VPN-Server zu verbinden.

Das nachfolgende Diagramm erläutert die Verbindungsmöglichkeiten zur Cloud-Recovery-Site und die Übersetzung von IP-Adressen in den Failover- und Test-Failover-Modi.

- Im Failover-Modus ist (wie abgebildet) ein Recovery-Server mit dem Produktionsnetzwerk verbunden und ihm wurde die Produktions-IP-Adresse zugewiesen.
- Im Test-Failover-Modus ist ein Recovery-Server mit dem isolierten Test-Netzwerk verbunden und ihm wurde ebenfalls die Produktions-IP-Adresse zugewiesen. Um jedoch auf den Server per VPN

zugreifen zu können, müssen Sie die Test-IP-Adresse verwenden. Der VPN-Server ersetzt die Test-IP-Adresse durch die Produktions-IP-Adresse innerhalb des Testnetzwerks.

- Sollte der Recovery-Server eine öffentliche IP-Adresse haben, dann wird diese ebenfalls im Failover- und Test-Failover-Modus in die Produktions-IP-Adresse übersetzt.



10.2.1 Anforderungen für die VPN-Appliance

Systemanforderungen

- 1 CPUs
- 1 GB RAM
- 8 GB Festplattenspeicherplatz

Ports

- TCP 443 (ausgehend) – für VPN-Verbindungen
- TCP 80 (ausgehend) – für automatische Updates der Appliance (S. 112)

Stellen Sie sicher, dass Ihre Firewalls und anderen Komponenten des Netzwerk-Sicherheitssystems Verbindungen zu allen IP-Adressen über diese Ports zulassen.

10.2.2 Verbindung über die VPN-Appliance

Die VPN-Appliance erweitert Ihr lokales Netzwerk (LAN) über einen sicheren VPN-Tunnel in die Cloud. Eine solche Verbindung wird oft auch als S2S-Verbindung (Site-to-Site) bezeichnet.

So können Sie eine Verbindung über die VPN-Appliance einrichten

1. Klicken Sie auf **Geräte** –> **Cloud-Recovery-Site**.
2. Klicken Sie auf der Willkommensseite auf **Start**.

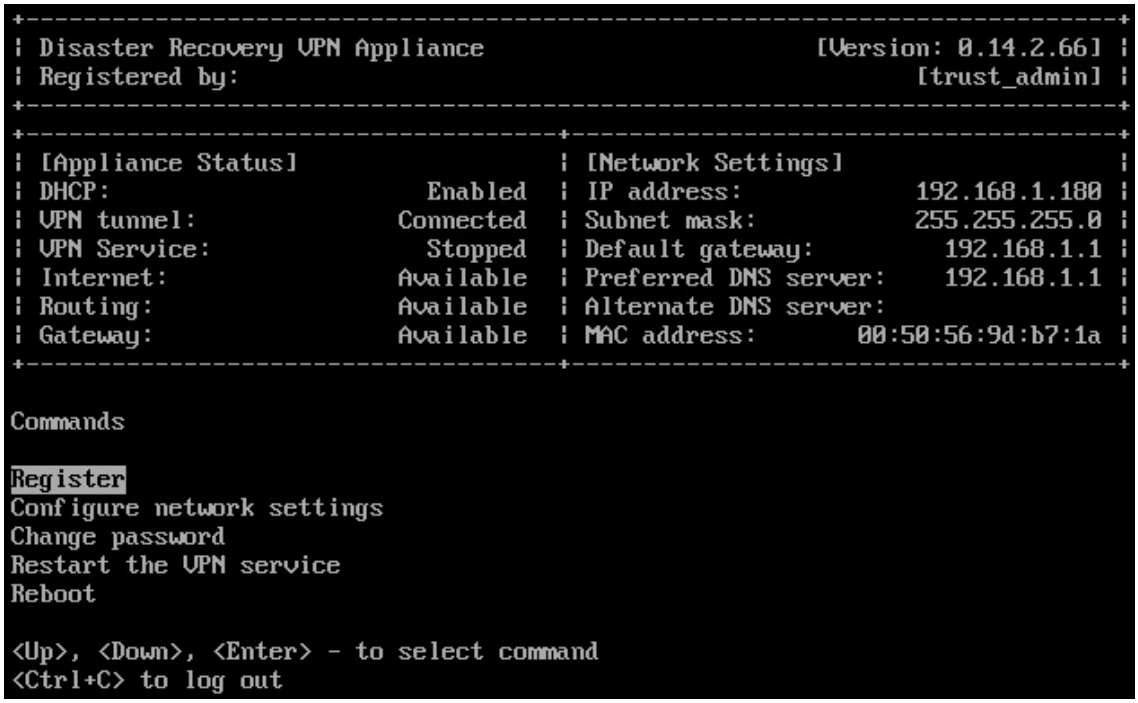
   Das System beginnt damit, den VPN-Server in der Cloud bereitzustellen. Dies kann einige Zeit benötigen. Währenddessen können Sie zum nächsten Schritt weitergehen.

Hinweis: *Der VPN-Server wird kostenlos bereitgestellt. Er wird gelöscht, wenn die Disaster Recovery-Funktionalität nicht verwendet wird (d.h., wenn sieben Tage lang kein primärer oder Recovery-Server in der Cloud vorhanden ist).*

3. Laden Sie je nach der von Ihnen verwendeten Virtualisierungsplattform die entsprechende VPN-Appliance für VMware vSphere oder Microsoft Hyper-V herunter.
4. Stellen Sie die Appliance bereit und verbinden Sie diese mit dem Produktionsnetzwerk.

   Überprüfen Sie in vSphere, dass für alle virtuellen Switche, die die VPN-Appliance mit dem Produktionsnetzwerk verbinden, der **Promiscuous-Modus** aktiviert ist und auf **Akzeptieren** eingestellt ist. Sie können im vSphere Client mit folgender Befehlssequenz auf diese Einstellungen zugreifen: Host auswählen –> **Übersicht** –> **Netzwerk** > Switch auswählen –> **Einstellungen bearbeiten...** > **Sicherheit**.

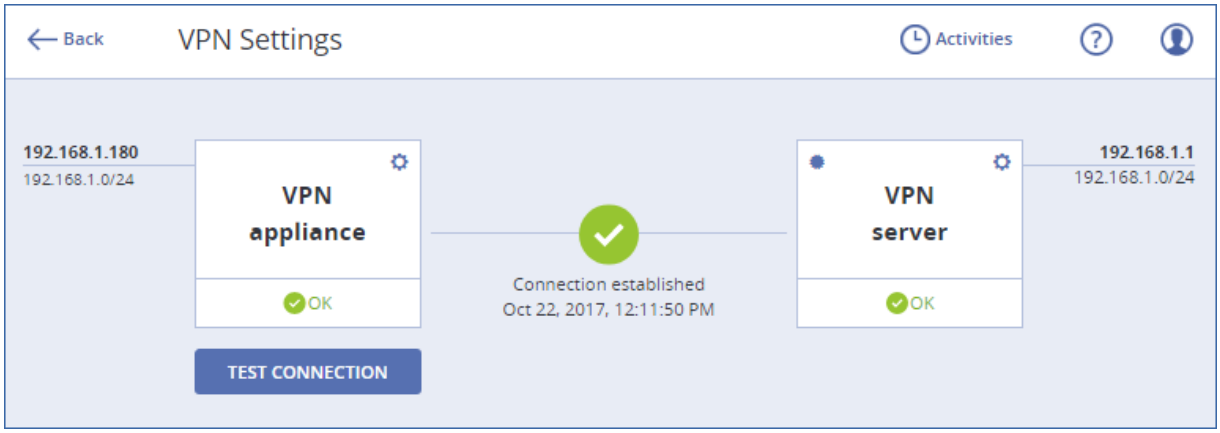
   Erstellen Sie in Hyper-V eine virtuelle Maschine der Generation 1 mit 1,024 MB Arbeitsspeicher. Wir empfehlen außerdem, dass Sie für diese Maschine die Option 'Dynamischer Arbeitsspeicher' aktivieren. Gehen Sie, sobald die Maschine erstellt wurde, zu **Einstellungen** –> **Hardware** –> **Netzwerkkarte** –> **Erweiterte Features** – und aktivieren Sie dort das Kontrollkästchen **Spoofing von MAC-Adressen aktivieren**.
5. Schalten Sie die Appliance ein.
6. Öffnen Sie die Appliance-Konsole und melden Sie sich mit der Benutzernamen-/Kennwort-Kombination 'admin/admin' an.



7. [Optional] Ändern Sie das Kennwort.
8. [Optional] Ändern Sie die Netzwerkeinstellungen. Sie können dem Gerät bei Bedarf eine statische IP-Adresse zuweisen.
9. Registrieren Sie die Appliance im Backup Service, indem Sie die Anmeldedaten des Firmenadministrators verwenden.

   Diese Anmeldedaten werden nur einmal verwendet, um das Zertifikat abzurufen. Die Datacenter-URL ist vordefiniert.

Die Appliance verbindet sich mit dem VPN-Server. Wenn die Konfiguration abgeschlossen wurde, zeigt die Appliance als Status '**OK**' an.



So können Sie die VPN-Verbindung testen

1. Klicken Sie auf **Geräte** –> **Cloud-Recovery-Site**.
2. Klicken Sie auf **VPN-Einstellungen**.
3. Überprüfen Sie, dass als Status für die VPN-Appliance und den VPN-Server '**OK**' angezeigt wird.
4. Klicken Sie auf **Test**.

   Die VPN-Appliance überprüft die Verbindung zum VPN-Server. Ihnen wird eine Liste der durchgeführten Teste angezeigt und welche Ergebnisse diese hatten.

10.2.3 Aktionen mit der VPN-Appliance

In der Backup-Konsole (unter **Geräte** –> **Cloud-Recovery-Site** –> **VPN-Einstellungen**) können Sie:

- Die Appliance verbinden/trennen
- Die Registrierung der Appliance aufheben

Wenn Sie auf diese Einstellungen zugreifen wollen, klicken Sie in der Abbildung der VPN-Appliance auf das Zahnradsymbol.

In der Appliance-Konsole können Sie:

- Das Kennwort für die Appliance ändern
- Die Netzwerkeinstellungen einsehen und ändern
- Das Registrierungskonto registrieren/ändern (durch Wiederholung der Registrierung)
- Den VPN-Dienst neu starten
- Die Appliance neu booten
- Zur Fehlersuche einen Ping an eine Netzwerkadresse senden

Ein Update der VPN-Appliance durchführen

Die VPN-Appliance sucht selbst einmal täglich automatisch nach Updates. Wenn eine neue Version gefunden wird, wird das Update automatisch durchgeführt, ohne dass der VPN-Dienst gestoppt oder neu gestartet werden müsste.

10.2.4 Point-to-Site-Verbindung

Die VPN-Appliance ermöglicht eine Verbindung zwischen der Cloud-Recovery-Site und Ihrem lokalen Netzwerk (LAN). Für den Fall, dass das lokale Netzwerk einmal ausfällt, benötigen Sie die Möglichkeit,

sich direkt mit der Cloud-Recovery-Site zu verbinden. Eine solche Verbindung wird meist als Point-to-Site-Verbindung (P2S, Punkt-zu-Standort) bezeichnet, im Gegensatz ein einer Site-to-Site-Verbindung (S2S, Standort-zu-Standort).

So können Sie Anmeldedaten (Benutzername, Kennwort) für die Point-to-Site-Verbindung festlegen

1. Klicken Sie in der Backup-Konsole (unter **Geräte** –> **Cloud-Recovery-Site** –> **VPN-Einstellungen**) in der Abbildung der VPN-Appliance auf das Zahnradsymbol.
2. Klicken Sie auf **Anmeldedaten ändern**.
3. Geben Sie den Benutzernamen ein.
4. Geben Sie das Kennwort ein.
5. Bestätigen Sie das Kennwort.
6. Klicken Sie auf **OK**.

So können Sie eine Point-to-Site-Verbindung aufbauen

1. Installieren Sie den OpenVPN-Client auf derjenigen Maschine, die Sie mit der Cloud-Recovery-Site verbinden möchten.

   Folgende OpenVPN-Client-Versionen werden unterstützt: 2.4.0 und höher.
2. Klicken Sie in der Backup-Konsole auf **Geräte** –> **Cloud-Recovery-Site** –> **VPN-Einstellungen**.
3. Klicken Sie in der linken oberen Ecke des VPN-Servers auf das Zahnradsymbol.
4. Klicken Sie auf **Konfiguration für OpenVPN herunterladen**.
5. Importieren Sie die Konfiguration in die OpenVPN-Einstellungen.
6. Geben Sie beim Verbindungsaufbau die Anmeldedaten ein, die Sie wie oben beschrieben eingerichtet haben.

10.2.5 Point-to-Site-Verbindungsparameter

Klicken Sie in der Backup-Konsole (unter **Geräte** –> **Cloud-Recovery-Site** –> **VPN-Einstellungen**) in der Abbildung der VPN-Appliance auf das Zahnradsymbol. Die Software zeigt den Benutzernamen an, der für die Point-to-Site-Verbindung festgelegt wurde, und die nachfolgenden Menüpunkte an.

Konfiguration für OpenVPN herunterladen

Mit diesem Befehl wird die Konfigurationsdatei für den OpenVPN-Client heruntergeladen. Diese Datei ist erforderlich, um eine Point-to-Site-Verbindung zur Cloud-Recovery-Site (S. 112) aufzubauen.

Anmeldedaten ändern

Mit diesem Befehl können Sie den Benutzernamen und/oder das Kennwort ändern, die für die Point-to-Site-Verbindung verwendet werden.

Dies ist in folgenden Fällen erforderlich:

- Bei der ersten Konfiguration der Point-to-Site-Verbindung (S. 112).
- Zur Durchführung einer regelmäßigen Kennwortänderung (gemäß der in Ihrem Unternehmen festgelegten Sicherheitsrichtlinien).
- Um für einige Benutzer (z.B. ehemalige Mitarbeiter) den Zugriff auf die Cloud-Recovery-Site einzuschränken.

Nachdem die Anmeldedaten geändert wurden, müssen Sie die betreffenden Benutzer darüber informieren, dass diese andere Anmeldedaten verwenden müssen.

Konfigurationsdatei neu generieren

Sie können die Konfigurationsdatei für den OpenVPN-Client neu generieren.

Dies ist in folgenden Fällen erforderlich:

- Wenn das VPN-Client-Zertifikat bald abläuft. Um das Ablaufdatum einzusehen, klicken Sie in der Abbildung des VPN-Servers auf das (i)-Symbol.
- Wenn Sie annehmen, dass die Konfigurationsdatei kompromittiert sein könnte.

Sobald die Konfigurationsdatei aktualisiert wurde, ist keine Verbindung mehr über die alte Konfigurationsdatei möglich. Stellen Sie sicher, dass die neue Datei an alle Benutzer verteilt wird, die die Point-to-Site-Verbindung verwenden dürfen.

10.3 Mit einem Recovery-Server arbeiten

10.3.1 Einen Recovery-Server erstellen

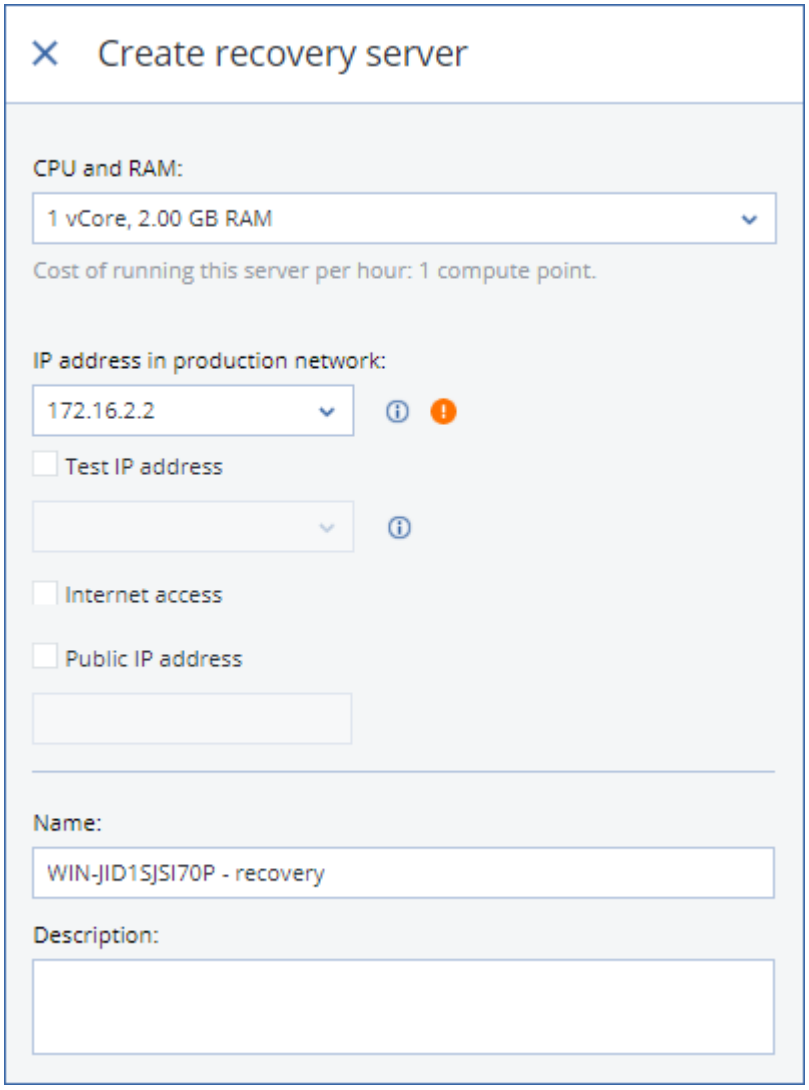
Voraussetzungen

- Sie müssen einer Maschine, die Sie sichern wollen, einen Backup-Plan zuweisen.
  - Sie können die komplette Maschine sichern oder nur diejenigen Laufwerke, die zum Booten und zur Bereitstellung notwendiger Dienste erforderlich sind.
  - Als Backup-Ziel muss der Cloud Storage ausgewählt sein.
  - Die Backup-Verschlüsselung muss deaktiviert sein.
  - Wir empfehlen, dass Sie den Backup-Plan mindestens einmal vor Erstellung des Recovery-Servers ausführen, um sicherzustellen, dass die Cloud Backups erfolgreich erstellt wurden.
- Es muss eine VPN-Verbindung zur Cloud-Recovery-Site eingerichtet sein.

So können Sie einen Recovery-Server erstellen

1. Wählen Sie die Maschine aus, die Sie sichern wollen.

2. Klicken Sie zuerst auf **Disaster Recovery** und dann auf **Recovery-Server erstellen**.



3. Bestimmen Sie die Anzahl der virtuellen CPU-Kerne und die Größe des Arbeitsspeichers.

   Beachten Sie die Berechnungspunkte neben jeder Option. Die Anzahl der Berechnungspunkte spiegelt wieder, wie viel die Ausführung des Recovery-Servers pro Stunde kostet.

4. Spezifizieren Sie die IP-Adresse, die der Server im Produktionsnetzwerk haben wird. Standardmäßig ist die IP-Adresse der ursprünglichen Maschine vorgegeben.

   Hinweis: *Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.*

5. [Optional] Aktivieren Sie das Kontrollkästchen **IP-Adresse testen** und spezifizieren Sie dann die IP-Adresse.

   Dies ermöglicht es, dass Sie sich während eines Test-Failovers per RDP oder SSH mit dem Recovery-Server verbinden können. Im Test-Failover-Modus wird der VPN-Server mithilfe des NAT-Protokolls die Test-IP-Adresse gegen die Produktions-IP-Adresse ersetzen.

   Wenn Sie das Kontrollkästchen deaktiviert lassen, können Sie sich während eines Test-Failovers nur über die Konsole mit dem Server verbinden.

   Hinweis: *Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.*

   Sie können eine der vorgeschlagenen IP-Adressen verwenden oder eine andere eingeben.

6. [Optional] Aktivieren Sie das Kontrollkästchen **Internetzugriff**.

   Dies ermöglicht es dem Recovery-Server, sich während eines Failovers (auch im Testmodus) mit dem Internet zu verbinden.
7. [Optional] Aktivieren Sie das Kontrollkästchen **Öffentliche IP-Adresse**.

   Wenn der Recovery-Server über eine öffentliche IP-Adresse verfügt, ist er während eines Failovers (auch im Testmodus) aus dem Internet verfügbar. Wenn Sie das Kontrollkästchen deaktiviert lassen, wird der Server nur in Ihrem Produktionsnetzwerk verfügbar sein.

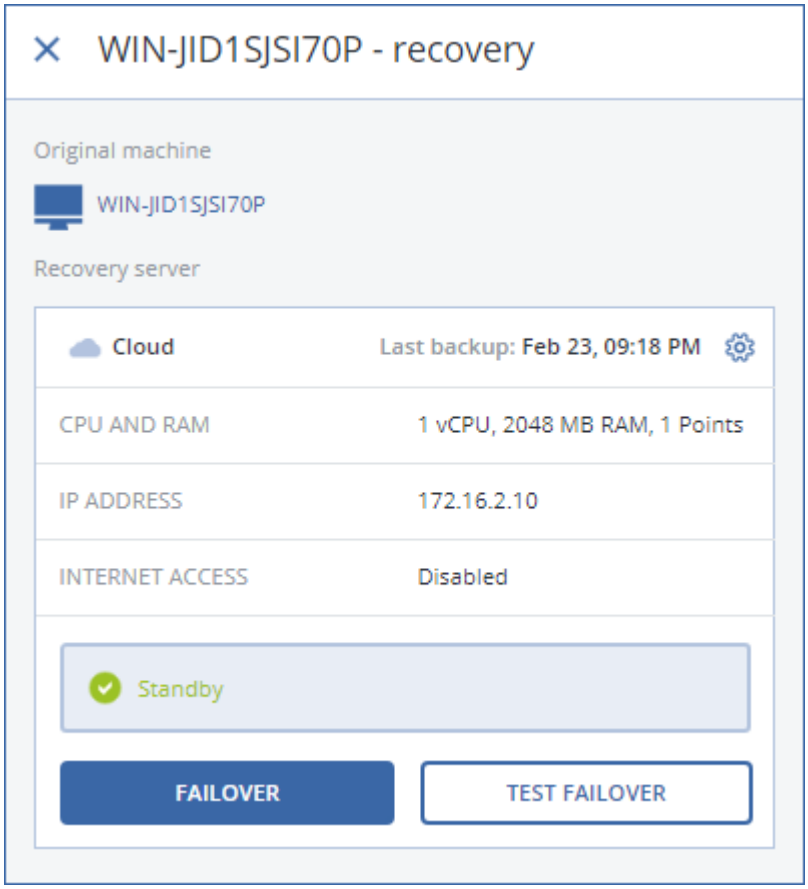
   Die öffentliche IP-Adresse wird angezeigt, nachdem Sie die Konfiguration abgeschlossen haben. Für eingehende Verbindungen zu den öffentlichen IP-Adressen sind folgende offene Ports verfügbar:

   TCP: 80, 443, 8088, 8443

   UDP: 1194

   Wenn Sie andere offene Ports benötigen, kontaktieren Sie den Support.
8. [Optional] Ändern Sie den Namen des Recovery-Servers.
9. [Optional] Geben Sie eine Beschreibung für den Recovery-Server ein.
10. Klicken Sie auf **Fertig**.

Der Recovery-Server wird in der Backup-Konsole im Bereich **Cloud-Recovery-Site** angezeigt. Sie können auf seine Einstellungen auch zugreifen, wenn Sie die ursprüngliche Maschine auswählen und dann auf **Disaster Recovery** klicken.



10.3.2 So funktioniert ein Failover

Eine Failover-Aktion basiert auf der Funktion 'VM von Backup ausführen (S. 184)'.

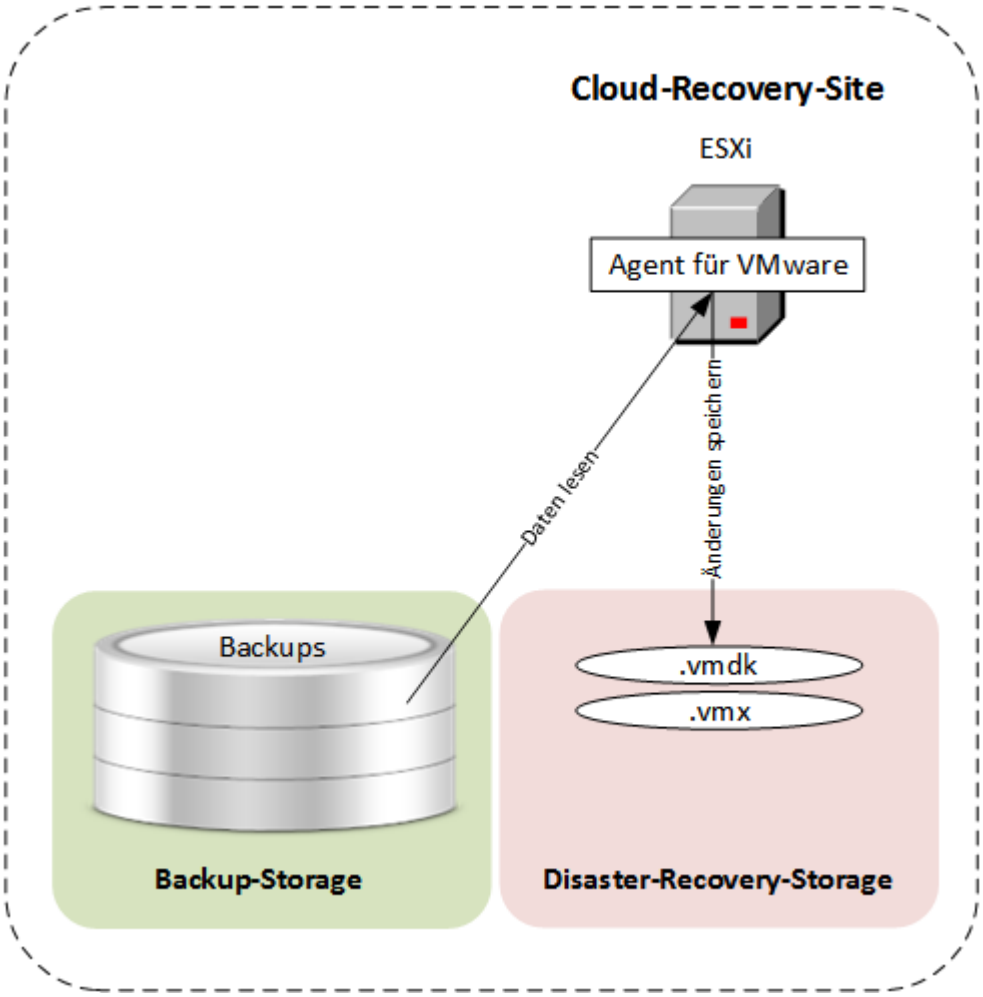
Die Aussage „ein Recovery-Server startet“ bedeutet, dass eine virtuelle Maschine mit vordefinierten Parametern aus einem (von möglicherweise mehreren) Backups der ursprünglich gesicherten Maschine gestartet wird.

Bei einem **Test-Failover** wird die virtuelle Maschine nicht finalisiert. Das bedeutet, dass der Agent die Inhalte der virtuellen Laufwerke direkt aus dem Backup auslesen kann, also die verschiedenen Bereiche des Backups per wahlfreien Zugriff verfügbar sind. Der Server arbeitet daher möglicherweise langsamer, belegt dafür aber nur wenig Speicherplatz im Datenspeicher (dem Disaster-Recovery Storage).

Bei einem **tatsächlichen Failover** wird die virtuelle Maschine schnellstmöglich finalisiert, um die beste Performance zu erreichen. Sobald der Recovery-Server gestartet ist, ändert sich dessen Stadium auf **Finalisierung**. Dieser Prozess überträgt die virtuellen Laufwerke des Servers aus dem Backup zum Disaster Recovery Storage. Tatsächlich läuft die Wiederherstellung der virtuellen Maschine ab, während die Maschine ausgeführt wird. Aufgrund dieses Prozesses arbeitet der Server möglicherweise langsamer. Wenn die Finalisierung abgeschlossen ist, erreicht der Server wieder eine normale Performance. Das Server-Stadium wird auf **Failover** geändert.

Wenn auf dem Recovery-Server ein Backup-Agent ist, wird der Agenten-Dienst gestoppt, um unerwünschte Aktivitäten (wie Backup-Starts oder das Senden veralteter Statusmeldungen an den Backup-Dienst) zu vermeiden.

Die folgende Abbildung verdeutlicht die Ausführung eines Recovery-Servers (inkl. der entsprechenden Storage-Nutzung).



10.3.3 Einen Failover testen

Einen Failover zu testen bedeutet, einen Recovery-Server in einem Test-VLAN zu starten, welches von Ihrem Produktionsnetzwerk isoliert ist. Sie können mehrere Recovery-Server gleichzeitig testen, um deren Interaktion zu überprüfen. Innerhalb des Testnetzwerks kommunizieren die Server über ihre Produktions-IP-Adressen. Die Server können jedoch keine TCP- oder UDP-Verbindungen zu den Maschinen in Ihrem lokalen Netzwerk (LAN) aufbauen.

Obwohl Failover-Tests optional sind, empfehlen wir Ihnen, diese doch so häufig durchzuführen, wie Sie es unter Berücksichtigung der Faktoren Kosten und Sicherheit passend finden. Bewährt hat sich die Erstellung eines sogenannten Runbooks. Das ist eine Zusammenstellung von Anweisungen, die beschreibt, wie die Produktionsumgebung in die Cloud übertragen wird.

So können Sie einen Test-Failover ausführen

1. Wählen Sie die ursprüngliche Maschine oder den Recovery-Server aus, für die/den Sie den Test durchführen wollen.
2. Klicken Sie auf **Disaster Recovery**.

   Die Beschreibung des Recovery-Servers wird angezeigt.
3. Klicken Sie auf **Failover testen**.
4. Wählen Sie den gewünschten Recovery-Punkt und klicken Sie dann auf **Failover testen**.

   Wenn der Recovery-Server gestartet ist, ändert sich dessen Stadium auf '**Failover wird getestet**'.
5. Testen Sie den Recovery-Server mit einer der nachfolgenden Methoden:
   - Klicken Sie in der Backup-Konsole auf **Geräte** –> **Cloud-Recovery-Site**, wählen Sie den Recovery-Server aus und klicken Sie abschließend im rechten Fensterbereich auf **Konsole**.
   - Verbinden Sie sich per RDP oder SSH mit dem Recovery-Server und verwenden Sie dabei die Test-IP-Adresse, die Sie bei der Erstellung des Recovery-Servers spezifiziert haben. Testen Sie die Verbindung sowohl innerhalb als auch außerhalb des Produktionsnetzwerks (wie im Abschnitt 'Point-to-Site-Verbindung (S. 112)' beschrieben).
   - Führen Sie ein Skript im Recovery-Server aus.

     Dieses Skript kann beispielsweise den Anmeldebildschirm überprüfen, ob Applikationen gestartet wurden, ob eine Internetverbindung besteht oder ob sich andere Maschinen mit dem Recovery-Server verbinden können.
   - Wenn der Recovery-Server auf das Internet zugreifen kann und eine öffentliche IP hat, können Sie auch TeamViewer verwenden.
6. Klicken Sie, wenn der Test abgeschlossen ist, in der Backup-Konsole auf **Test stoppen**.

   Der Recovery-Server wird gestoppt. Alle Änderungen am Recovery-Server, die während des Test-Failovers erfolgten, werden verworfen.

10.3.4 Einen Failover durchführen

Ein Failover ist ein Prozess, bei dem ein Workload von Ihren lokalen Systemen (on-premise) in die Cloud verschoben wird. Der Begriff wird außerdem auch für das Stadium verwendet, wenn der Workload in der Cloud bleibt.

Wenn Sie einen Failover initiieren, startet der Recovery-Server im Produktionsnetzwerk. Alle Backup-Pläne werden von der ursprünglichen Maschine widerrufen. Es wird automatisch ein neuer Backup-Plan erstellt und dem Recovery-Server zugewiesen.

So können Sie einen Failover durchführen

1. Stellen Sie sicher, dass die ursprüngliche Maschine nicht mehr im Netzwerk verfügbar ist.

2. Wählen Sie in der Backup-Konsole die ursprüngliche Maschine aus – oder den Recovery-Server, der dieser Maschine zugeordnet ist.
3. Klicken Sie auf **Disaster Recovery**.

   Die Beschreibung des Recovery-Servers wird angezeigt.
4. Klicken Sie auf **Failover**.
5. Wählen Sie den gewünschten Recovery-Punkt und klicken Sie dann auf **Failover**.

   Wenn der Recovery-Server gestartet ist, ändert sich dessen Stadium auf **Finalisierung** und nach einer gewissen Zeit auf **Failover.** Es ist wichtig zu verstehen, dass der Server in beiden Stadien verfügbar ist, trotz der rotierenden Fortschrittsanzeige. Weitere Details finden Sie im Abschnitt 'So funktioniert ein Failover (S. 116)'.
6. Überprüfen Sie, dass der Recovery-Server gestartet ist, indem Sie sich dessen Konsole anzeigen lassen. Klicken Sie auf **Geräte** –> **Cloud-Recovery-Site**, wählen Sie den Recovery-Server aus und klicken Sie abschließend im rechten Fensterbereich auf **Konsole**.
7. Stellen Sie sicher, dass der Recovery-Server über die Produktions-IP-Adresse verfügbar ist, die Sie bei Erstellung des Recovery-Servers spezifiziert haben.

Sobald der Recovery-Server finalisiert ist, wird automatisch ein neuer Backup-Plan erstellt und dem Recovery-Server zugewiesen. Bis auf einige Einschränkungen basiert dieser Backup-Plan auf demjenigen Backup-Plan, der zu Erstellung des Recovery-Servers verwendet wurde. Sie können in diesem Plan nur die Planung und Aufbewahrungsregeln ändern. Weitere Informationen dazu finden Sie im Abschnitt 'Backup der Cloud-Server (S. 121)'.

Die einzige Möglichkeit, aus dem Failover-Zustand herauszukommen, ist eine Failback-Aktion durchzuführen.

10.3.5 Einen Failback durchführen

Ein Failback ist ein Prozess, bei dem ein Workload aus der Cloud zurück zu Ihren lokalen Systemen verschoben wird.

Während der Prozess läuft, ist der Server, der verschoben wird, nicht verfügbar. Die Länge dieses Wartungsfensters entspricht in etwa der Dauer einer Backup-Ausführung und einer sich daran anschließenden Wiederherstellung des Servers.

So können Sie einen Failback durchführen

1. Wählen Sie den Recovery-Server aus, der sich im **Failover**-Stadium befindet.
2. Klicken Sie auf **Disaster Recovery**.

   Die Beschreibung des Recovery-Servers wird angezeigt.
3. Klicken Sie auf **Failback vorbereiten**.

   Der Recovery-Server wird gestoppt und als Backup zum Cloud Storage gesichert. Warten Sie, bis das Backup erfolgreich abgeschlossen wurde.

   Anschließend sind zwei Aktionen verfügbar: **Failback abbrechen** und **Failback ausführen**. Wenn Sie auf **Failback abbrechen** klicken, wird der Recovery-Server wieder gestartet und der Failover fortgesetzt.
4. Stellen Sie den Server aus diesem Backup auf einer physischen oder virtuellen Maschine in Ihrer lokalen Infrastruktur (on-premise) wieder her.
   - Wenn Sie ein Boot-Medium verwenden, sollten Sie die Anleitung im Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 90)' befolgen. Stellen Sie sicher, dass Sie sich mit dem Konto in der Cloud anmelden, für welches der Server registriert ist – und dass Sie dann das neueste Backup auswählen.

- Wenn die Zielmaschine online ist oder es sich um eine virtuelle Maschine (VM) handelt, können Sie die Backup-Konsole verwenden. Wählen Sie in der Registerkarte **Backups** den Cloud Storage aus. Wählen Sie bei der Option **Von dieser Maschine aus durchsuchen** die physische Zielmaschine aus oder die Maschine, auf welcher der Agent läuft (wenn die Zielmaschine eine VM ist). Die ausgewählte Maschine muss für dasselbe Konto registriert sein, für welches auch der Server registriert ist. Suchen Sie das neueste Backup des Servers, klicken Sie auf die Option **Komplette Maschine wiederherstellen** – und konfigurieren Sie dann die Recovery-Parameter. Ausführliche Informationen dazu finden Sie im Abschnitt 'Eine Maschine wiederherstellen (S. 85)'.

Überprüfen Sie, dass die Wiederherstellung abgeschlossen wurde und die wiederhergestellte Maschine korrekt funktioniert.

5. Gehen Sie in der Backup-Konsole wieder zurück zum Recovery-Server und klicken Sie auf **Failback ausführen**.

   Der Recovery-Server und die Recovery-Punkte werden für einen nächsten Failover bereit sein. Wenn Sie neue Recovery-Punkte erstellen wollen, müssen Sie dem neuen lokalen Server einen Backup-Plan zuweisen.

10.4 Mit einem primären Server arbeiten

10.4.1 Einen primären Server erstellen

Voraussetzungen

- Es muss eine VPN-Verbindung zur Cloud-Recovery-Site eingerichtet sein.

So können Sie einen primären Server erstellen

1. Klicken Sie auf **Geräte** –> **Cloud**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie eine Vorlage für die neue virtuelle Maschine aus.
4. Bestimmen Sie die Anzahl der virtuellen CPU-Kerne und die Größe des Arbeitsspeichers.

   Beachten Sie die Berechnungspunkte neben jeder Option. Die Anzahl der Berechnungspunkte spiegelt wieder, wie viel die Ausführung des primären Servers pro Stunde kostet.
5. Spezifizieren Sie die IP-Adresse, die der Server im Produktionsnetzwerk haben wird. Als Standardeinstellung wird die erste freie IP-Adresse aus Ihrem Produktionsnetzwerk verwendet.

   Hinweis: *Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.*
6. [Optional] Aktivieren Sie das Kontrollkästchen **Internetzugriff**.

   Dadurch wird dem primären Server ermöglicht, auf das Internet zuzugreifen.
7. [Optional] Aktivieren Sie das Kontrollkästchen **Öffentliche IP-Adresse**.

   Wenn der primäre Server über eine öffentliche IP-Adresse verfügt, ist er aus dem Internet verfügbar. Wenn Sie das Kontrollkästchen deaktiviert lassen, wird der Server nur in Ihrem Produktionsnetzwerk verfügbar sein.

   Die öffentliche IP-Adresse wird angezeigt, nachdem Sie die Konfiguration abgeschlossen haben. Für eingehende Verbindungen zu den öffentlichen IP-Adressen sind folgende offene Ports verfügbar:

   TCP: 80, 443, 8088, 8443

   UDP: 1194

   Wenn Sie andere offene Ports benötigen, kontaktieren Sie den Support.

8. [Optional] Ändern Sie die Größe der virtuellen Festplatte. Wenn Sie mehr als eine Festplatte benötigen, müssen Sie auf **Laufwerk hinzufügen** klicken und dann die Größe des neuen Laufwerks festlegen.
9. Geben Sie dem primären Server einen Namen.
10. [Optional] Geben Sie eine Beschreibung für den primären Server ein.
11. Klicken Sie auf **Fertig**.

Der primäre Server wird im Produktionsnetzwerk verfügbar gemacht. Sie können den Server über seine Konsole, über RDP, SSH oder den TeamViewer verwalten.

10.4.2 Aktionen mit einem primären Server

Der primäre Server wird in der Backup-Konsole im Bereich **Cloud-Recovery-Site** angezeigt.

Sie können den Server starten bzw. stoppen, wenn Sie im rechten Fensterbereich auf **Start** bzw. **Stopp** klicken.

Wenn Sie die primären Server-Einstellungen bearbeiten wollen, müssen Sie zuerst den Server stoppen, dann auf **Info** klicken und anschließend auf **Bearbeiten**.

Wenn Sie dem primären Server einen Backup-Plan zuweisen wollen, klicken Sie auf **Backup**. Daraufhin wird Ihnen ein vordefinierter Backup-Plan angezeigt, indem Sie nur die Planung und Aufbewahrungsregeln ändern können. Weitere Informationen dazu finden Sie im Abschnitt 'Backup der Cloud-Server (S. 121)'.

10.5 Backup der Cloud-Server

Primäre Server und Recovery-Server werden von dem Agenten für VMware gesichert, der auf der Cloud-Recovery-Site installiert ist. In der ersten Version ist dieses Backup funktionell noch beschnitten, wenn man es gegen die Backup-Funktionalität von lokalen Agenten vergleicht. Diese Beschränkungen sind aber nur temporär und werden mit zukünftigen Versionen aufgehoben.

- Der einzig mögliche Backup-Speicherort ist der Cloud Storage.
- Ein Backup-Plan kann nicht auf mehrere Server gleichzeitig angewendet werden. Jeder Server muss seinen eigenen Backup-Plan haben, auch wenn alle Backup-Pläne ansonsten die gleichen Einstellungen haben.
- Auf einen Server kann nur je ein Backup-Plan angewendet werden.
- Applikationskonforme Backups werden nicht unterstützt.
- Es ist keine Verschlüsselung verfügbar.
- Es sind keine Backup-Optionen verfügbar.

Wenn Sie einen primären Server löschen, werden auch dessen Backups gelöscht.

Ein Recovery-Server wird nur im Failover-Stadium per Backup gesichert. Seine Backups setzen die Backup-Sequenz des ursprünglichen Servers fort. Wenn ein Failback durchgeführt wird, kann der ursprüngliche Server diese Backup-Sequenz fortsetzen. Die Backups des Recovery-Servers können also nur manuell gelöscht werden – oder weil Aufbewahrungsregeln angewendet werden. Wenn ein Recovery-Server gelöscht wird, werden seine Backups immer aufbewahrt.

10.6 Runbooks verwenden

Ein Runbook ist eine Zusammenstellung von Anweisungen, die beschreibt, wie die Produktionsumgebung in die Cloud übertragen wird. Sie können Runbooks in der Backup-Konsole erstellen. Wenn Sie auf die Registerkarte **Runbooks** zugreifen wollen, wählen Sie die Befehle **Disaster Recovery** –> **Runbooks**.

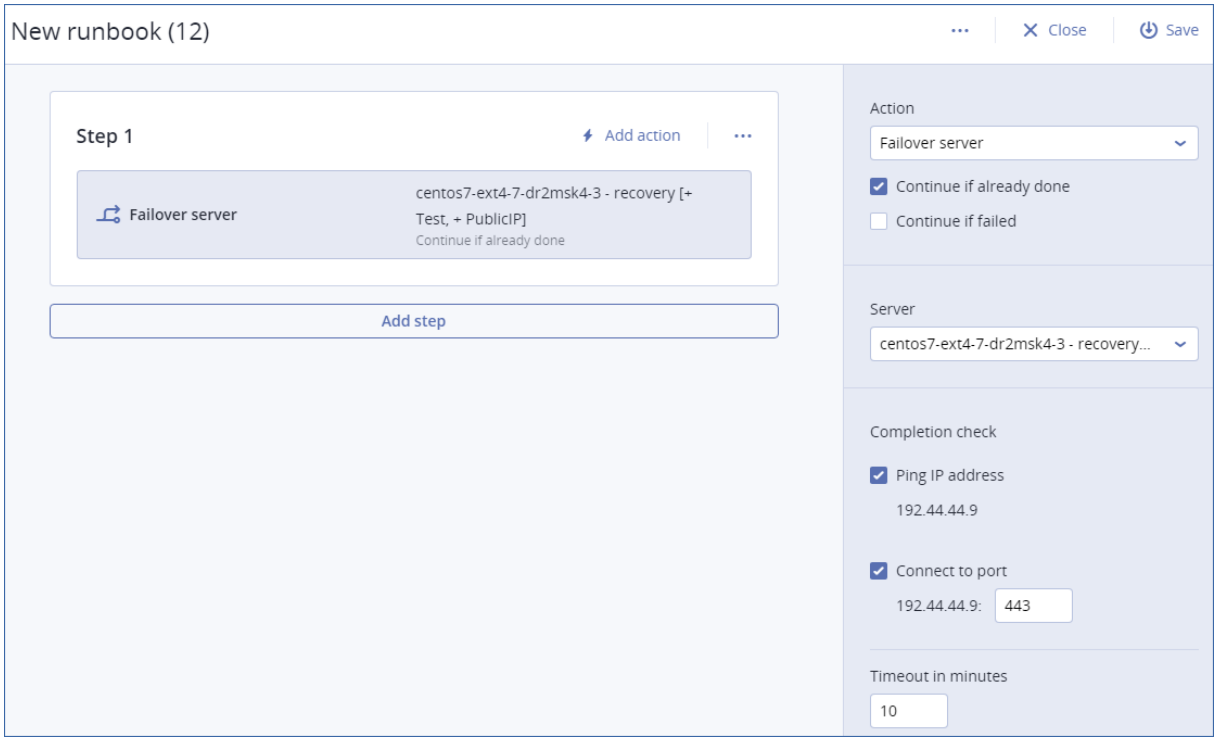
Warum sollte ich Runbooks verwenden?

Mit Runbooks können Sie:

- Ein Failover von einem oder mehreren Servern automatisieren
- Das Failover-Ergebnis automatisch überprüfen, indem Sie die Server-IP anpingen und die Verbindung zu dem von Ihnen spezifizierten Port überprüfen
- Die Reihenfolge der Aktionen mit den Servern festlegen, die verteilte Applikationen ausführen
- Manuelle Aktionen in den Workflow einbinden
- Die Integrität Ihrer Disaster Recovery-Lösung überprüfen, indem Sie die entsprechenden Runbooks im Testmodus ausführen

10.6.1 Ein Runbook erstellen

Klicken Sie zum Erstellen eines Runbooks auf **Runbook erstellen** –> **Schritt hinzufügen** –> **Aktion hinzufügen**. Sie können die Aktionen und Schritte per Drag&Drop verschieben. Vergessen Sie nicht, dem Runbook einen eindeutigen Namen zu geben. Wenn Sie ein längeres Runbook erstellen, sollten Sie zwischenzeitlich immer mal wieder auf **Speichern** klicken. Klicken Sie auf **Schließen**, wenn Sie fertig sind.



Schritte und Aktionen

Ein Runbook besteht aus Schritten, die nacheinander ausgeführt werden. Ein Schritt besteht aus Aktionen, die gleichzeitig gestartet werden. Eine Aktion kann bestehen aus:

- Eine Operation kann mit einem Cloud Server durchgeführt werden (**Server-Failover ausführen**, **Server starten**, **Server stoppen**, **Server-Failback ausführen**). Hinweis: normalerweise wird der Begriff 'Aktion(en)' in der Benutzerdokumentation und Bernutzeroberfläche für den hier verwendeten Begriff 'Operation(en)' verwendet bzw. zwischen diesen beiden nicht unterschieden. Für diesen Abschnitt über Runbooks wird zwischen den beiden Begriffen unterschieden. Im übrigen Verlauf der Dokumentation werden die hier genannten 'Operation(en)' ansonsten als Aktionen bezeichnet. Um diese Operation zu definieren, müssen Sie zuerst die Operation auswählen, dann den Cloud Server und dann die Parameter für die Operation.
- Eine manuelle Operation, die Sie verbal beschreiben müssen. Sobald die Operation abgeschlossen wurde, muss ein Benutzer auf die Bestätigungsschaltfläche klicken, damit das Runbook fortgesetzt werden kann.
- Die Ausführung eines anderen Runbooks. Um diese Operation zu definieren, müssen Sie das entsprechende Runbook auswählen.

  Ein Runbook kann nur eine (1) Ausführung eines bestimmten Runbooks enthalten. Wenn Sie beispielsweise die Aktion 'Runbook A ausführen' hinzugefügt haben, können Sie zwar die Aktion 'Runbook B ausführen' hinzufügen, aber keine weitere Aktion 'Runbook A ausführen'.

***Hinweis**: In dieser Produktversion muss ein Benutzer einen Failback manuell durchführen. Ein Runbook zeigt die Eingabeaufforderung an, wenn dies erforderlich ist.*

Aktionsparameter

Alle Operationen mit Cloud Servern haben folgende Parameter:

- **Fortsetzen, wenn bereits durchgeführt** (standardmäßig aktiviert)

  Dieser Parameter definiert das Runbook-Verhalten, wenn die erforderliche Operation bereits durchgeführt wurde (weil beispielsweise ein Failover bereits durchgeführt wurde oder ein Server bereits ausgeführt wird). Wenn dieser Parameter aktiviert wurde, gibt das Runbook eine Warnung aus und fährt mit der Ausführung fort. Wenn der Parameter deaktiviert wurde, schlägt die Operation und damit dann auch das Runbook fehl.
- **Fortsetzen, wenn fehlgeschlagen** (standardmäßig deaktiviert)

  Dieser Parameter definiert das Runbook-Verhalten, wenn die erforderliche Operation fehlschlägt. Wenn dieser Parameter aktiviert wurde, gibt das Runbook eine Warnung aus und fährt mit der Ausführung fort. Wenn der Parameter deaktiviert wurde, schlägt die Operation und damit dann auch das Runbook fehl.

Fertigstellungsprüfung

Sie können für die Aktionen **Server-Failover ausführen** und **Server Starten** eine Fertigstellungsprüfung hinzufügen, um sicherzustellen, dass der entsprechende Server verfügbar ist und die benötigen Services bereitgestellt sind. Wenn eine dieser Prüfungen scheitert, wird die Aktion als fehlgeschlagen betrachtet.

- **IP-Adresse anpingen**

  Die Software wird die Produktions-IP-Adresse des Cloud Servers solange anpingen, bis der Server antwortet oder es zu einem Timeout kommt (je nachdem, was zuerst eintritt).
- **Mit Port verbinden** (standardmäßig 443)

  Die Software wird versuchen, sich über die Produktions-IP-Adresse und den von Ihnen spezifizierten Port mit dem Cloud Server zu verbinden, bis die Verbindung hergestellt ist oder es zu einem Timeout kommt (je nachdem, was zuerst eintritt). Auf diese Weise können Sie überprüfen, ob die Applikation, die auf dem angegebenen Port lauscht, auch ausgeführt wird.

Der vorgegebene Timeout-Wert beträgt 10 Minuten. Sie können diesen bei Bedarf ändern.

10.6.2 Aktionen mit Runbooks

Um auf die Liste der Aktionen zuzugreifen, bewegen Sie den Mauszeiger auf ein Runbook und klicken Sie auf das Symbol mit den drei Punkten. Wenn ein Runbook nicht ausgeführt wird, sind folgenden Aktionen verfügbar:

- **Ausführen**
- **Bearbeiten**
- **Klonen**
- **Löschen**

Ein Runbook ausführen

Jedes Mal, wenn Sie auf **Ausführen** klicken, werden Sie zur Eingabe von Ausführungsparametern aufgefordert. Diese Parameter gelten für alle Failover- und Failback-Operationen, die im Runbook enthalten sind. Diejenigen Runbooks, die mit der Operation **Runbook ausführen** spezifiziert werden, erben diese Parameter vom Haupt-Runbook.

- **Failover- und Failback-Modus**

  Wählen Sie, ob Sie einen Test-Failover (Standardvorgabe) oder einen tatsächlichen (Produktions-)Failover ausführen möchten. Der Failback-Modus entspricht dem gewählten Failover-Modus.

- **Failover-Recovery-Punkt**

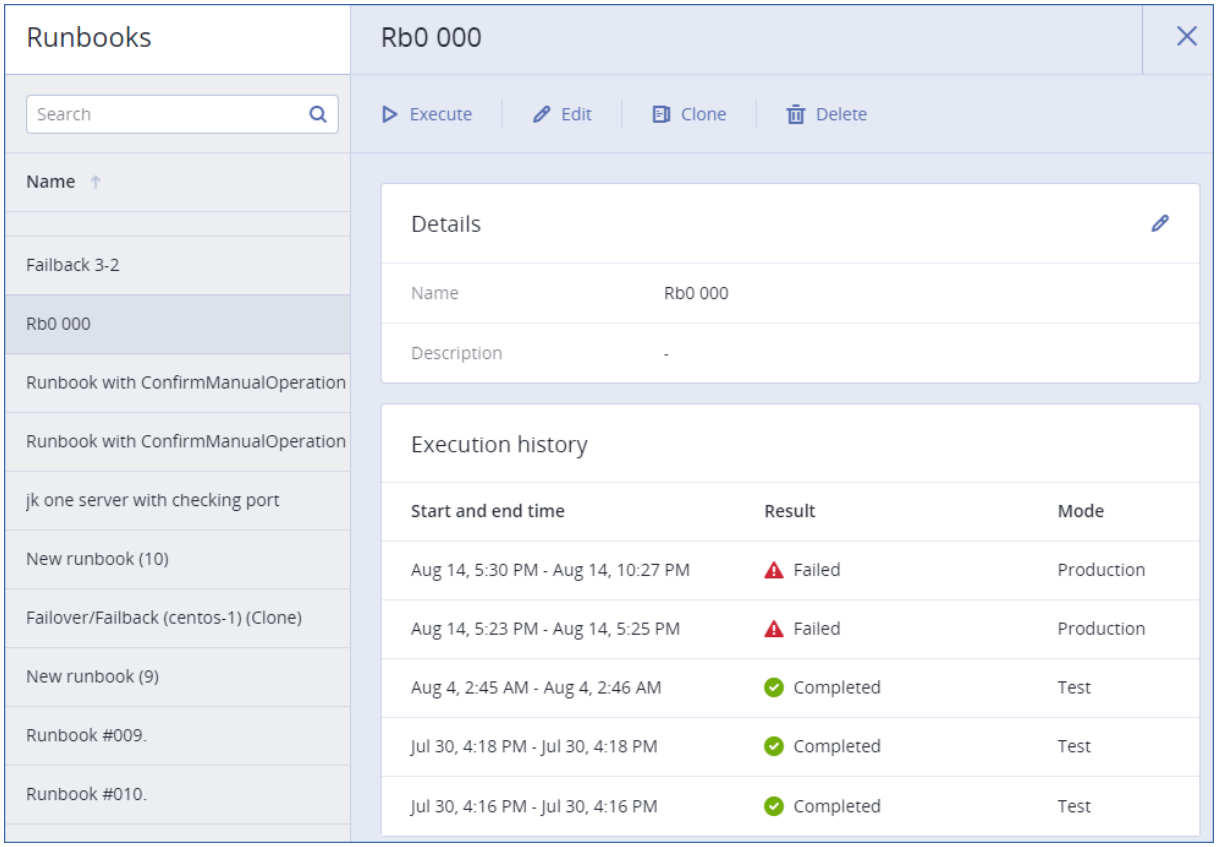
  Wählen Sie den neuesten Recovery-Punkt (Standardvorgabe) oder wählen Sie einen bestimmten Zeitpunkt in der Vergangenheit. Bei letzterem werden für jeden Server diejenigen Recovery-Punkte ausgewählt, die dem spezifizierten Zeitpunkt am nächsten liegen.

Eine Runbook-Ausführung stoppen

Sie können während einer Runbook-Ausführung den Befehl **Stopp** aus der Liste der verfügbaren Aktionen wählen. Die Software wird alle bereits gestarteten Aktionen abschließen – außer solche Aktionen, die eine Benutzerinteraktion erfordern.

Den Ausführungsverlauf anzeigen

Wenn Sie ein Runbook in der Registerkarte **Runbooks** auswählen, wird Ihnen die Software Details und einen Ausführungsverlauf zu diesem Runbook anzeigen. Klicken Sie auf eine Zeile, die zu einer bestimmten Ausführung gehört, um das entsprechende Ausführungsprotokoll einzusehen.



11 Aktionen mit Backups

11.1 Die Registerkarte 'Backups'

Die Registerkarte **Backups** ermöglicht den Zugriff auf alle Backups – inklusive der Backups von Offline-Maschinen und solchen Maschinen, die nicht mehr für den Backup Service registriert sind.

Backups, die an einem freigegebenen Speicherort (wie SMB- oder NFS-Freigaben) gespeichert sind, können von allen Benutzern gesehen werden, die mindestens über Leserechte für diesen Speicherort verfügen.

Im Cloud Storage haben Benutzer jedoch immer nur Zugriff auf Ihre jeweils eigenen Backups. Ein Administrator kann die Backups eines jeden Kontos einsehen, welches zu einer gegebenen Abteilung oder einer Firma und deren Untergruppen gehört. Dieses Konto wird indirekt über den Befehl **Von dieser Maschine aus durchsuchen** ausgewählt. Die Registerkarte **Backups** zeigt die Backups all derjenigen Maschinen an, die jemals für dasselbe Konto registriert wurden, da diese Maschine registriert ist.

Backups, die vom *Cloud* Agenten für Office 365 erstellt wurden, sowie Backups von G Suite-Daten werden nicht im Speicherort '**Cloud Storage**' angezeigt, sondern in einem separaten Bereich namens **Cloud-Applikationen-Backups**.

Backup-Speicherorte, die in Backup-Plänen verwendet werden, werden automatisch in der Registerkarte **Backups** aufgeführt. Wenn Sie einen benutzerdefinierten Ordner (z.B. einen USB-Stick) zur Liste der Backup-Speicherorte hinzufügen wollen, müssen Sie auf **Durchsuchen** klicken und dann den gewünschten Ordnerpfad spezifizieren.

Wenn Sie einige Backups über einen Datei-Manager (wie dem Windows Explorer) hinzugefügt oder entfernt haben, klicken Sie auf das Zahnradsymbol neben dem Speicherortsnamen und anschließend auf **Aktualisieren**.

Ein Backup-Speicherort (mit Ausnahme des Cloud Storage) verschwindet aus der Registerkarte **Backups**, wenn alle Maschinen, die je zu diesem Speicherort gesichert wurden, aus dem Backup Service gelöscht wurden. Dadurch wird sichergestellt, dass Sie für Backups, die an diesem Speicherort aufbewahrt wurden, nicht weiter bezahlen müssen. Sobald ein neues Backup zu diesem Speicherort erfolgt, wird der Speicherort mit allen darin gespeicherten Backups wieder neu hinzugefügt.

So wählen Sie einen Recovery-Punkt über die Registerkarte 'Backups'

1. Wählen Sie auf der Registerkarte **Backups** den Speicherort aus, wo die Backups gespeichert sind.

   Die Software zeigt all diejenigen Backups an, für die Ihr Konto am ausgewählten Speicherort die Berechtigung zur Anzeige hat. Die Backups werden in Gruppen zusammengefasst. Die Gruppennamen basieren auf folgender Vorlage:

   `<Maschinenname> - <Backup-Plan-Name>`
2. Wählen Sie eine Gruppe, von der die Daten wiederhergestellt werden sollen.
3. [Optional] Klicken Sie auf **Ändern** (neben dem Befehl **Von dieser Maschine aus durchsuchen**) und wählen Sie dann eine andere Maschine aus. Einige Backups können nur von bestimmten Agenten durchsucht werden. Sie müssen beispielsweise eine Maschine auswählen, auf der ein Agent für SQL läuft, um die Backups von Microsoft SQL Server-Datenbanken durchsuchen zu können.

   Wichtig: *Beachten Sie, dass die Maschine, die über* ***Von dieser Maschine aus durchsuchen*** *festgelegt wird, auch das Standardziel für die Wiederherstellung der Backups einer physischen Maschine ist. Nachdem Sie einen Recovery-Punkt ausgewählt und auf* ***Recovery*** *geklickt haben, sollten Sie die Einstellung '****Zielmaschine****' doppelt überprüfen, um sicherzustellen, dass Sie die Wiederherstellung auch wirklich zu genau dieser Maschine durchführen wollen. Wenn Sie das Recovery-Ziel ändern wollen, müssen Sie über den Befehl* ***Von dieser Maschine aus durchsuchen*** *eine andere Maschine spezifizieren.*
4. Klicken Sie auf **Backups anzeigen**.
5. Wählen Sie den gewünschten Recovery-Punkt aus.

11.2 Volumes aus einem Backup mounten

Indem Sie die Volumes eines Laufwerk-Backups (Images) mounten, können Sie auf diese Volumes so zugreifen, als wären es physische Laufwerke. Volumes werden im 'Nur Lesen'-Modus gemountet.

Anforderungen

- Diese Funktionalität steht nur unter Windows und bei Verwendung des Windows Datei-Explorers zur Verfügung.
- Auf der Maschine, auf der Sie das Mounten durchführen, muss der Agent für Windows installiert sein.
- Das im Backup vorliegende Dateisystem muss von der Windows-Version, die auf der Maschine läuft, unterstützt werden.
- Das Backup selbst muss entweder in einem lokalen Ordner, in einer Netzwerkfreigabe (SMB/CIFS) oder in einer Secure Zone gespeichert sein.

So mounten Sie ein Volume aus einem Backup

1. Verwenden Sie den Windows Datei-Explorer, um den Speicherort des Backups aufzurufen.
2. Klicken Sie doppelt auf die Backup-Datei. Die Dateinamen basieren auf folgender Vorlage:
   `<Maschinenname> - <Backup-Plan-GUID>`
3. Sollte das Backup verschlüsselt sein, dann geben Sie das entsprechende Kennwort ein. Ansonsten können Sie diesen Schritt überspringen.

   Der Windows Datei-Explorer zeigt die Recovery-Punkte an.
4. Klicken Sie doppelt auf einen gewünschten Recovery-Punkt.

   Der Windows Datei-Explorer zeigt die im Backup gespeicherten Volumes an.

   ***Tipp**: Wenn Sie auf ein Volume doppelt klicken, können Sie dessen Inhalte einsehen/durchsuchen. Sie können Dateien/Ordner aus dem Backup zu einem beliebigen Ordner im Dateisystem kopieren.*
5. Klicken Sie mit der rechten Maustaste auf das zu mountende Volume und klicken Sie dann auf **Im 'Nur Lesen'-Modus mounten**.
6. Sollte das Backup in einer Netzwerkfreigabe gespeichert sein, müssen Sie bei Bedarf die entsprechenden Anmeldedaten angeben, um auf die Freigabe zugreifen zu können. Ansonsten können Sie diesen Schritt überspringen.

   Das ausgewählte Volume wird von der Software gemountet. Dem Volume wird dabei standardmäßig der erste freie Laufwerksbuchstabe zugewiesen.

So trennen Sie ein Volume wieder (unmounting)

1. Gehen Sie im Windows Datei-Explorer zur obersten Ebene des Verzeichnisbaums (das Element '**Computer**' bzw. unter Windows 8.1 (und später) '**Dieser PC**').
2. Klicken Sie mit der rechten Maustaste auf das gemountete Volume.
3. Klicken Sie auf **Trennen**.

   Das Mounten des ausgewählten Volumes wird von der Software aufgehoben und das entsprechende Laufwerk vom Dateisystem getrennt.

11.3 Backups löschen

So löschen Sie die Backups einer Maschine, die online und in der Backup-Konsole aufgeführt sind

1. Wählen Sie auf der Registerkarte **Alle Geräte** eine Maschine aus, deren Backups Sie löschen wollen.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie den Speicherort aus, an dem sich die zu löschen Backups befinden.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Zum Löschen eines einzelnen Backups müssen Sie das entsprechende Backup auswählen und dann auf das X-Symbol klicken.
   - Um alle Backups am ausgewählten Speicherort zu löschen, klicken Sie auf **Alle löschen**.
5. Bestätigen Sie Ihre Entscheidung.

So löschen Sie die Backups einer bestimmten Maschine

1. Wählen Sie auf der Registerkarte **Backups** den Speicherort, an dem Sie die Backups löschen wollen.

   Die Software zeigt all diejenigen Backups an, für die Ihr Konto am ausgewählten Speicherort die Berechtigung zur Anzeige hat. Die Backups werden in Gruppen zusammengefasst. Die Gruppennamen basieren auf folgender Vorlage:

`<Maschinenname> - <Backup-Plan-Name>`

2. Wählen Sie eine Gruppe aus.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein einzelnes Backup löschen wollen, klicken Sie auf **Backups anzeigen**, wählen Sie anschließend das zu löschende Backup aus und klicken Sie dann auf das X-Symbol.
   - Um die ausgewählte Gruppe zu löschen: klicken Sie auf **Löschen**.
4. Bestätigen Sie Ihre Entscheidung.

So können Sie Backups direkt aus dem Cloud Storage löschen

1. Melden Sie sich, wie im Abschnitt 'Dateien aus dem Cloud Storage herunterladen (S. 95)' beschrieben, am Cloud Storage an.
2. Klicken Sie auf den Namen der Maschine, deren Backups Sie löschen wollen.

   Die Software zeigt eine oder mehrere Backup-Gruppen an.
3. Klicken Sie auf das Zahnradsymbol, das zu der Backup-Gruppe gehört, die Sie löschen möchten.
4. Klicken Sie auf **Entfernen**.
5. Bestätigen Sie die Aktion.

Vorgehensweise, wenn Sie lokale Backups mit einem Datei-Manager gelöscht haben

Wir empfehlen, dass Sie Backups nach Möglichkeit nur über die Backup-Konsole löschen. Wenn Sie lokale Backups dennoch mit einem Datei-Manager (wie dem Windows Explorer) gelöscht haben, gehen Sie folgendermaßen vor:

1. Klicken Sie auf der Registerkarte **Backups** auf das Zahnradsymbol neben dem Speicherortsnamen.
2. Klicken Sie auf **Aktualisieren**.

Auf diese Weise teilen Sie dem Backup Service mit, dass die lokale Storage-Nutzung geringer geworden ist.

12 Aktionen mit Backup-Plänen

Weitere Informationen über die Erstellung eines Backup-Plans finden Sie im Abschnitt 'Backup (S. 36)'.

So bearbeiten Sie einen Backup-Plan

1. Wenn Sie den Backup-Plan für alle Maschinen (auf die er angewendet wird) bearbeiten wollen, wählen Sie eine dieser Maschinen aus. Alternativ können Sie auch die Maschinen auswählen, für die Sie den Backup-Plan bearbeiten wollen.
2. Klicken Sie auf **Backup**.
3. Wählen Sie den Backup-Plan aus, den Sie bearbeiten wollen.
4. Klicken Sie neben dem Namen des Backup-Plans auf das Zahnradsymbol und anschließend auf den Befehl **Bearbeiten**.
5. Wenn Sie die Plan-Parameter ändern wollen, klicken Sie auf den entsprechenden Backup-Plan-Fensterbereich.
6. Klicken Sie auf **Änderungen speichern**.
7. Wenn Sie den Backup-Plan für alle Maschinen (auf die er angewendet wird) ändern wollen, klicken Sie auf **Änderungen auf diesen Backup-Plan anwenden**. Klicken Sie alternativ auf **Einen neuen Backup-Plan nur für die ausgewählten Geräte erstellen**.

So widerrufen Sie die Anwendung einen Backup-Plans auf bestimmte Maschinen

1. Wählen Sie die Maschinen aus, für die Sie die Anwendung des Backup-Plans widerrufen wollen.
2. Klicken Sie auf **Backup**.
3. Falls mehrere Backup-Pläne auf die Maschinen angewendet werden, wählen Sie denjenigen Backup-Plan aus, dessen Anwendung Sie widerrufen wollen.
4. Klicken Sie neben dem Namen des Backup-Plans auf das Zahnradsymbol und anschließend auf den Befehl **Widerrufen**.

So löschen Sie einen Backup-Plan

1. Wählen Sie irgendeine Maschine aus, auf die der zu löschende Backup-Plan angewendet wird.
2. Klicken Sie auf **Backup**.
3. Falls mehrere Backup-Pläne auf die Maschinen angewendet werden, wählen Sie denjenigen Backup-Plan aus, den Sie löschen wollen.
4. Klicken Sie neben dem Namen des Backup-Plans auf das Zahnradsymbol und anschließend auf den Befehl **Löschen**.

   Der Backup-Plan wird daraufhin zuerst auf allen Maschinen widerrufen und dann vollständig von der Weboberfläche gelöscht.

13 Mobilgeräte sichern

Verwenden Sie die Backup-App, um Daten auf Ihren Mobilgeräten zu sichern und wiederherzustellen.

Unterstützte Mobilgeräte

- Smartphones oder Tablets mit Betriebssystem Android 4.1 (oder höher).
- iPhones, iPads und iPods mit Betriebssystem iOS 8 oder höher.

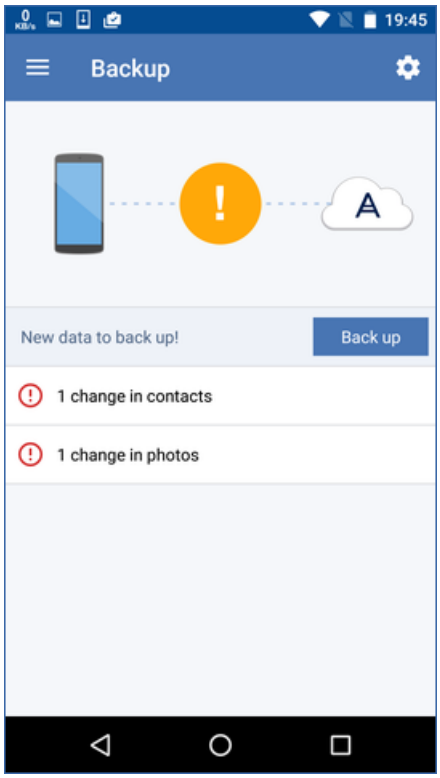
Was Sie per Backup sichern können

- Kontakte
- Fotos
- Videos
- Kalender
- Textnachrichten (nur bei Android-Geräten)
- Erinnerungen (nur bei iOS-Geräte)

Was Sie wissen sollten

- Sie können Ihre Daten nur zum Cloud Storage (als Ziel) sichern.

- Die App zeigt Ihnen bei jedem Start eine Übersicht von zwischenzeitlich erfolgten Datenänderungen an. Diese können Sie auf Wunsch dann mit einem manuellen Backup sichern.



- Standardmäßig ist die Funktionalität '**Kontinuierliches Backup**' eingeschaltet. In diesem Modus sucht die Backup-App alle sechs Stunden nach Datenänderungen und führt automatisch ein Backup aus, sofern solche Änderungen gefunden wurden. Sie können das kontinuierliche Backup ganz ausschalten oder (in den Einstellungen der App) die Beschränkung '**Nur beim Aufladen**' aktivieren.
- Auf die gesicherten Daten können Sie anschließend von jedem Mobilgerät aus zugreifen, welches für Ihr Konto registriert ist. Dies ist hilfreich, wenn Sie Daten beispielsweise von einem alten auf ein neues Mobilgerät übertragen wollen. Bei Kontakten und Fotos ist es möglich, diese von einem Android-Gerät (Quelle) auf einem iOS-Gerät (Ziel) wiederherzustellen – und umgekehrt. Mithilfe der Backup-Konsole können Sie Fotos, Videos und Kontakte außerdem auch auf einen Computer herunterladen.
- Daten, die von Mobilgeräten gesichert wurden, welche für Ihr Konto registriert sind, sind auch nur über Ihr Konto verfügbar. Keine andere Person kann Ihre Daten einsehen oder wiederherstellen.
- In der Backup-App können Sie Daten immer nur jeweils vom letzten (jüngsten) Backup aus wiederherstellen. Wenn Sie Daten aus einem älteren Backup wiederherstellen wollen, müssen Sie die Backup-Konsole verwenden (auf einem Computer oder Tablet).
- Auf die Backups von Mobilgeräten werden keine Aufbewahrungsregeln angewendet.
- Wenn während des Backups in dem Gerät eine SD-Karte vorhanden ist, werden auch die dort gespeicherten Daten mitgesichert. Bei einer Wiederherstellung werden diese Daten auch auf der SD-Karte wiederhergestellt, sofern diese vorhanden ist. Wenn nicht, werden diese Daten auf dem internen Speicher des Mobilgerätes wiederhergestellt.
- Für Daten auf dem internen Gerätespeicher und auf einer SIM-Karte des Gerätes gilt gleichermaßen: egal, wo diese Daten ursprünglichen gespeichert waren, sie werden immer auf dem internen Gerätespeicher wiederhergestellt.

Schritt-für-Schritt-Anleitungen

So erhalten Sie die Backup-App

1. Öffnen Sie auf dem Mobilgerät einen Webbrowser und geben Sie die URL der Backup Console ein.
2. Melden Sie sich mit Ihrem Konto an.
3. Klicken Sie auf **Alle Geräte** –> **Hinzufügen**.
4. Wählen Sie unter **Mobilgeräte** den Gerätetyp.

   Abhängig vom Gerätetyp werden Sie entweder zum Apple App Store oder zum Google Play Store weitergeleitet.
5. [Nur auf iOS-Geräten] Klicken Sie auf **Laden**.
6. Klicken Sie auf **Installieren**, damit die Backup-App eingerichtet wird.

So können Sie ein iOS-Gerät per Backup sichern

1. Öffnen Sie die Backup-App.
2. Melden Sie sich mit Ihrem Konto an.
3. Wählen Sie die Datenkategorien aus, die Sie sichern wollen. Standardmäßig sind alle Kategorien ausgewählt.
4. Tippen Sie auf **Backup jetzt**.
5. Erlauben Sie, dass die App auf Ihre persönlichen Daten zugreifen darf. Datenkategorien, auf die Sie den Zugriff verweigert haben, werden nicht mitgesichert.

Das Backup wird gestartet.

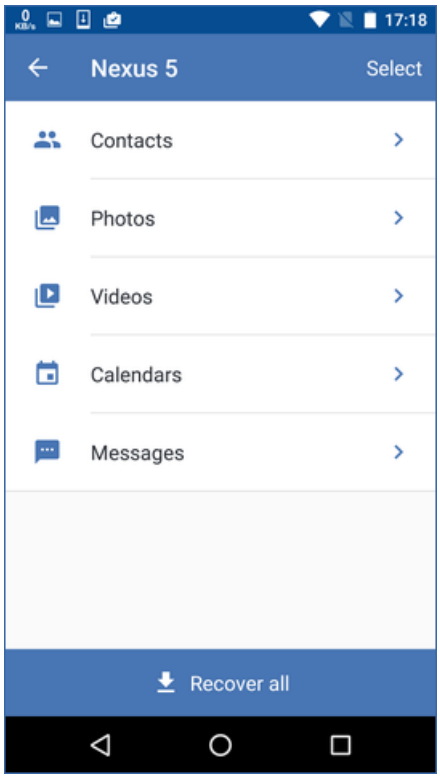
So starten Sie eine Sicherung auf einem Android-Gerät

1. Öffnen Sie die Backup-App.
2. Melden Sie sich mit Ihrem Konto an.
3. [Unter Android 6.0 und höher] Erlauben Sie, dass die App auf Ihre persönlichen Daten zugreifen darf. Datenkategorien, auf die Sie den Zugriff verweigert haben, werden nicht mitgesichert.
4. [Optional] Spezifizieren Sie die Datenkategorie, die Sie sichern wollen. Tippen Sie dazu zuerst auf das Zahnradsymbol und dann auf die Schieber derjenigen Datenkategorien, die vom Backup ausgeschlossen werden sollen. Tippen Sie abschließend auf den Pfeil für 'Zurück'.
5. Tippen Sie auf **Backup**.

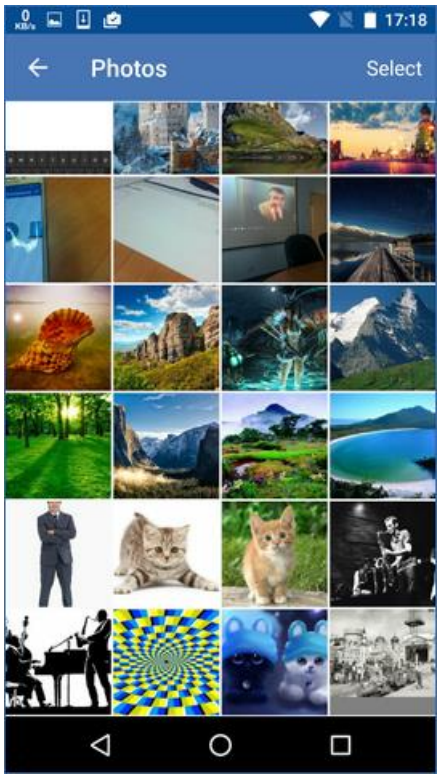
So können Sie Daten auf einem Mobilgerät wiederherstellen

1. Öffnen Sie die Backup-App.
2. Wischen Sie nach rechts und tippen Sie auf **Zugriff und Recovery**.
3. Tippen Sie auf den Gerätenamen.
4. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie alle gesicherten Daten wiederherstellen wollen, müssen Sie auf **Alle wiederherstellen** tippen. Es sind keine weiteren Aktionen erforderlich.
   - Wenn Sie eine oder mehrere Datenkategorien wiederherstellen wollen, müssen Sie auf **Auswahl** tippen und dann die Kontrollkästchen der gewünschten Datenkategorien aktivieren. Tippen Sie auf den Befehl **Recovery**. Es sind keine weiteren Aktionen erforderlich.

- Wenn Sie eines oder mehrere Datenelemente wiederherstellen wollen, die zu einer bestimmten Datenkategorie gehören, müssen Sie auf die betreffende Datenkategorie tippen. Fahren Sie mit den nachfolgenden Schritten fort.



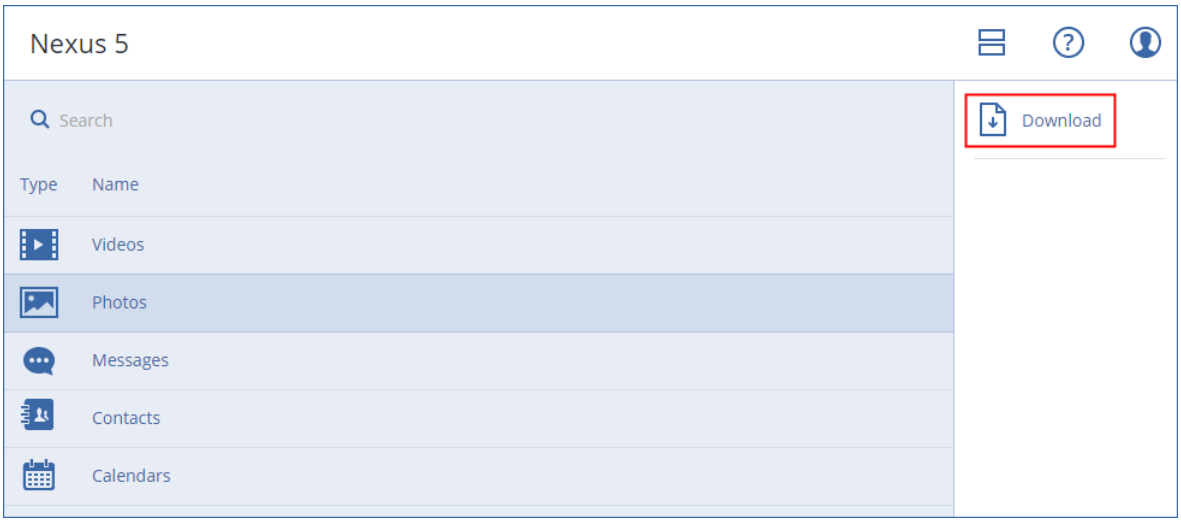
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein einzelnes Datenelement wiederherstellen wollen, müssen Sie dieses antippen.
   - Wenn Sie mehrere Datenelemente wiederherstellen wollen, müssen Sie auf **Auswahl** tippen und dann die Kontrollkästchen der gewünschten Elemente aktivieren.



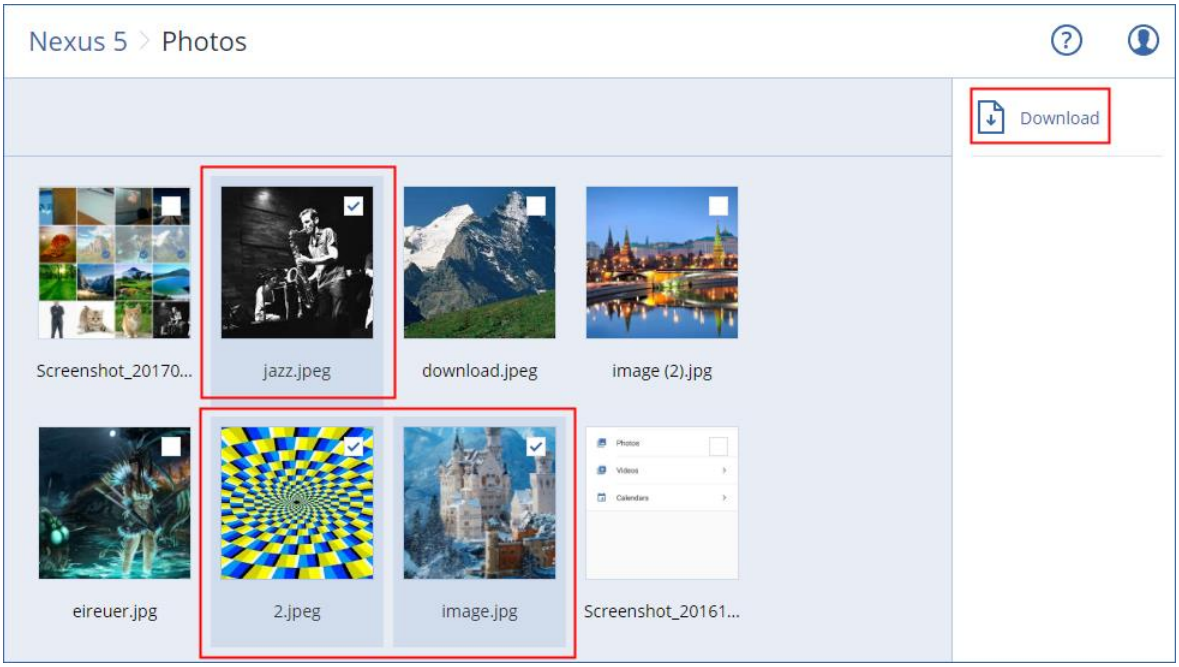
6. Tippen Sie auf den Befehl **Recovery**.

So können Sie mit der Backup-Konsole auf Daten zugreifen

1. Öffnen Sie auf einem Computer einen Webbrowser und geben Sie die URL der Backup Console ein.
2. Melden Sie sich mit Ihrem Konto an.
3. Wählen Sie bei **Alle Geräte** den Namen Ihres Mobilgerätes aus – und klicken Sie dann auf **Recovery**.
4. Wählen Sie den gewünschten Recovery-Punkt aus.
5. Gehen Sie nach einer der folgenden Möglichkeiten vor:
   - Wenn Sie alle Fotos, Videos oder Kontakte herunterladen wollen, müssen Sie die entsprechende Datenkategorie auswählen. Klicken Sie auf **Download**.



   - Wenn Sie bestimmte Fotos, Videos oder Kontakte herunterladen wollen, müssen Sie auf die entsprechende Datenkategorie klicken und dann die Kontrollkästchen der gewünschten Datenelemente aktivieren. Klicken Sie auf **Download**.



- Wenn Sie eine Vorschau von einer Textnachricht, einem Foto oder einem Kontakt ansehen wollen, müssen Sie auf die entsprechende Datenkategorie klicken und dann auf das gewünschte Datenelement.

Weitere Informationen finden Sie unter http://www.acronis.com/redirector/products/atimobile/docs/?lang=de. Diese Hilfeinformationen sind ebenfalls in der Backup-App verfügbar (tippen Sie dazu im Menü der App auf **Einstellungen** –> **Hilfe**).

14 Applikationen sichern

Microsoft SQL Server und Microsoft Exchange Server sichern

Es gibt zwei Methoden, wie Sie diese Applikationen per Backup schützen können:

- **Datenbank-Backup**

  Hierbei handelt es sich um ein Datei-Backup der Datenbanken und der Metadaten, die mit den Datenbanken assoziiert sind. Die Datenbanken können zu einer aktiven Applikation oder als Dateien wiederhergestellt werden.

- **Applikationskonformes Backup**

  Hierbei handelt es sich um ein Laufwerk-Backup, bei dem außerdem die Metadaten der Applikationen eingesammelt werden. Diese Metadaten ermöglichen es, dass die Applikationsdaten (im Backup) durchsucht und wiederhergestellt werden können, ohne dass dafür das komplette Laufwerk/Volume wiederhergestellt werden müsste. Das Laufwerk/Volume kann natürlich auch komplett wiederhergestellt werden. Das bedeutet, dass eine einzelne Lösung und ein einzelner Backup-Plan gleichermaßen die Anwendungsbereiche 'Disaster Recovery' und 'Data Protection' abdecken kann.

Microsoft SharePoint sichern

Eine Microsoft SharePoint-Farm besteht aus Front-End-Webservern (die die SharePoint-Dienste ausführen), Datenbankservern (die den Microsoft SQL Server ausführen) und – optional – bestimmte Applikationsserver, die die Front-End-Webserver von einigen SharePoint-Diensten entlasten. Einige Front-End- und Applikationsserver können identisch sein.

So sichern Sie eine komplette SharePoint-Farm:

- Sichern Sie alle Datenbank-Server mit einem applikationskonformen Backup.
- Sichern Sie alle einzelnen Front-End- und Applikationsserver mit einem herkömmlichem Laufwerk-Backup.

Die Backups aller Server sollten mit derselben Planung durchgeführt werden.

Wenn Sie nur die Inhalte sichern wollen, können Sie die Inhaltsdatenbanken separat sichern.

Einen Domain-Controller sichern

Eine Maschine, auf der die Active Directory Domain Services (Active Directory-Domänendienste) laufen, kann per applikationskonformem Backup geschützt werden. Falls eine Domain mehr als zwei Domain-Controller enthält und Sie einen davon wiederherstellen, wird eine 'nicht autorisierte' Wiederherstellung durchgeführt und so ein USN-Rollback nach der Wiederherstellung vermieden.

Applikationen wiederherstellen

Die nachfolgende Tabelle gibt einen Überblick über alle Recovery-Methoden, die zur Wiederherstellung von Applikationen verfügbar sind.

	Von einem Datenbank-Backup	Von einem applikationskonformen Backup	Von einem Laufwerk-Backup
Microsoft SQL Server	Datenbanken zu einer aktiven SQL Server-Instanz (S. 139) Datenbanken als Dateien (S. 139)	Komplette Maschine (S. 85) Datenbanken zu einer aktiven SQL Server-Instanz (S. 139) Datenbanken als Dateien (S. 139)	Komplette Maschine (S. 85)
Microsoft Exchange Server	Datenbanken zu einem aktiven Exchange Server (S. 142) Datenbanken als Dateien (S. 142) Granulares Recovery zu einem aktiven Exchange Server (S. 144)	Komplette Maschine (S. 85) Datenbanken zu einem aktiven Exchange Server (S. 142) Datenbanken als Dateien (S. 142) Granulares Recovery zu einem aktiven Exchange Server (S. 144)	Komplette Maschine (S. 85)
Microsoft SharePoint-Datenbank-Server	Datenbanken zu einer aktiven SQL Server-Instanz (S. 139) Datenbanken als Dateien (S. 139) Granulares Recovery mithilfe des SharePoint Explorers	Komplette Maschine (S. 85) Datenbanken zu einer aktiven SQL Server-Instanz (S. 139) Datenbanken als Dateien (S. 139) Granulares Recovery mithilfe des SharePoint Explorers	Komplette Maschine (S. 85)
Microsoft SharePoint-Front-End-Webserver	-	-	Komplette Maschine (S. 85)
Active Directory-Domänendienste	-	Komplette Maschine (S. 85)	-

14.1 Voraussetzungen

Bevor Sie das applikationskonforme Backup konfigurieren, sollten Sie sicherstellen, dass die nachfolgend aufgeführten Voraussetzungen erfüllt sind.

Verwenden Sie zum Überprüfen des VSS-Writer-Stadiums den Befehl '**`vssadmin list writers`**'.

Allgemeine Voraussetzungen

Für Microsoft SQL Server müssen folgende Voraussetzungen erfüllt sein:

- Mindestens eine Microsoft SQL Server-Instanz ist gestartet.
- Der SQL Writer für VSS ist aktiviert.

Für Microsoft Exchange Server müssen folgende Voraussetzungen erfüllt sein:

- Der Microsoft Exchange-Informationsspeicherdienst ist gestartet.
- Windows PowerShell ist installiert. Für Exchange 2010 (und höher) muss es mindestens Windows PowerShell-Version 2.0 sein.
- Microsoft .NET Framework ist installiert.

  Für Exchange 2007 muss es mindestens Microsoft .NET Framework-Version 2.0 sein.

  Für Exchange 2010 (und höher) muss es mindestens Microsoft .NET Framework-Version 3.5 sein.
- Der Exchange Writer für VSS ist aktiviert.

Auf einem Domain Controller müssen folgende Voraussetzungen erfüllt sein:

- Der Active Directory Writer für VSS ist aktiviert.

Zur Erstellung eines Backup-Plans müssen folgende Voraussetzungen erfüllt sein:

- Für physische Maschinen ist die Backup-Option 'Volume Shadow Copy Service (VSS) (S. 81)' aktiviert.
- Für virtuelle Maschinen ist die Backup-Option 'VSS (Volume Shadow Copy Service) für virtuelle Maschinen (S. 82)' aktiviert.

Zusätzliche Anforderungen für applikationskonforme Backups

Überprüfen Sie bei Erstellung eines Backup-Plans, dass die '**Komplette Maschine**' zum Backup ausgewählt wurde.

Falls die Applikationen auf virtuellen Maschinen laufen, die über den Agenten für VMware gesichert werden, müssen folgende Voraussetzungen erfüllt sein:

- Die zu sichernden virtuellen Maschinen erfüllen die Anforderungen für applikationskonsistentes Stilllegen (Quiescing), wie sie im folgenden VMware Knowledge Base-Artikel erläutert sind: https://pubs.vmware.com/vsphere-6-5/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkBkupVadp.9.6.html
- Die VMware Tools sind auf den Maschinen installiert und aktuell.
- Die Benutzerkontensteuerung (UAC) ist auf jeder der Maschinen deaktiviert. Wenn Sie die Benutzerkontensteuerung (UAC) nicht ausschalten wollen, müssen Sie die Anmeldedaten eines integrierten Domain-Administrators (DOMAIN\Administrator) bereitstellen, wenn Sie das Applikations-Backup aktivieren.

14.2 Datenbank-Backup

Bevor Sie ein Datenbank-Backup durchführen, sollten Sie sicherstellen, dass die unter 'Voraussetzungen (S. 135)' aufgeführten Anforderungen erfüllt sind.

Wählen Sie die Datenbanken so wie nachfolgend beschrieben aus – und spezifizieren Sie dann nach Bedarf (S. 38) die anderen Einstellungen des Backup-Plans.

14.2.1 SQL-Datenbanken auswählen

Das Backup einer SQL-Datenbank enthält die entsprechenden Datenbankdateien (.mdf, .ndf), Protokolldateien (.ldf) und andere zugeordnete Dateien. Die Dateien werden mithilfe des SQL-Writer-Dienstes gesichert. Der Dienst muss dann laufen, wenn der Volume Shadow Copy Service (VSS, Volumenschattenkopie-Dienst) ein Backup oder eine Wiederherstellung anfordert.

Die SQL-Transaktionsprotokolle werden nach jedem erfolgreichen Backup abgeschnitten. Die SQL-Protokollabschneidung kann in den Backup-Plan-Optionen (S. 72) deaktiviert werden.

So wählen Sie SQL-Datenbanken aus

1. Klicken Sie auf **Microsoft SQL**.

   Es werden die Maschinen angezeigt, auf denen der Agent für SQL installiert ist.
2. Bestimmen Sie (per 'Durchsuchen') die Daten, die Sie sichern wollen.

   Klicken Sie doppelt auf eine Maschine, damit Ihnen die dort vorliegenden SQL Server-Instanzen angezeigt werden. Klicken Sie doppelt auf eine Instanz, damit Ihnen die dort vorliegenden Datenbanken angezeigt werden.
3. Wählen Sie Daten aus, die Sie sichern wollen. Sie können eine komplette Instanz oder einzelne Datenbanken auswählen.
   - Wenn Sie eine komplette SQL Server-Instanz auswählen, werden alle aktuellen Datenbanken und auch alle Datenbanken, die der ausgewählten Instanz zukünftig hinzugefügt werden, per Backup gesichert.
   - Wenn Sie die gewünschten Datenbanken direkt auswählen, werden dagegen nur diese Datenbanken gesichert.
4. Klicken Sie auf **Backup**. Geben Sie bei Aufforderung die benötigten Anmeldedaten ein, um auf die SQL Server-Daten zugreifen zu können. Das Konto muss auf der betreffenden Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder der Gruppe **Administratoren** sein – und auf jeder Instanz, die Sie sichern wollen, ein Mitglied der **SysAdmin**-Rolle.

14.2.2 Exchange Server-Daten auswählen

Die nachfolgende Tabelle gibt Ihnen einen Überblick über die Microsoft Exchange Server-Daten, die Sie für ein Backup verwenden können – und die (mindestens benötigten) Benutzerrechte, die zum Sichern dieser Daten erforderlich sind.

Exchange-Version	Datenelemente	Benutzerrechte
2007	Speichergruppen	Mitglied in der Rollengruppe **Exchange-Organisationsadministratoren**
2010/2013/2016	Datenbanken	Mitglied in der Rollengruppe **Serververwaltung**.

Ein Voll-Backup enthält alle ausgewählten Exchange Server-Daten.

Ein inkrementelles Backup enthält die geänderten Datenblöcke der Datenbankdateien, die Prüfpunktdateien und eine kleinere Anzahl von Protokolldateien, die neuer als der korrespondierende Datenbank-Prüfpunkt sind. Da im Backup alle Änderungen an den Datenbankdateien enthalten sind, ist es nicht notwendig, alle Transaktionsprotokoll-Datensätze seit dem letzten (vorherigen) Backup zu sichern. Es muss nur dasjenige Protokoll nach einer Wiederherstellung zurückgespielt werden, welches neuer (jünger) als der Prüfpunkt ist. Dies ermöglicht eine schneller Wiederherstellung und gewährleistet ein erfolgreiches Datenbank-Backup auch bei aktivierter Umlaufprotokollierung.

Die Transaktionsprotokolldateien werden nach jedem erfolgreichen Backup abgeschnitten.

So wählen Sie Exchange-Server-Daten aus

1. Klicken Sie auf **Microsoft Exchange**.

   Es werden diejenigen Maschinen angezeigt, auf denen der Agent für Exchange installiert ist.
2. Bestimmen Sie (per 'Durchsuchen') die Daten, die Sie sichern wollen.

   Klicken Sie doppelt auf eine Maschine, damit Ihnen die dort vorliegenden Datenbanken (Speichergruppen) angezeigt werden.

3. Wählen Sie Daten aus, die Sie sichern wollen. Geben Sie bei Aufforderung die Anmeldedaten an, die für den Datenzugriff notwendig sind.
4. Klicken Sie auf **Backup**.

14.3 Applikationskonformes Backup

Applikationskonformes Backup auf Laufwerksebene ist für physische Maschinen und für virtuelle ESXi-Maschinen verfügbar.

Wenn Sie eine Maschine sichern, auf der ein Microsoft SQL Server, Microsoft Exchange Server oder die Active Directory Domain Services (Active Directory-Domänendienste) ausgeführt werden, können Sie mit der Option **Applikations-Backup** einen zusätzlichen Schutz für die Daten dieser Applikationen aktivieren.

Wann ist ein applikationskonformes Backup sinnvoll?

Mit einem applikationskonformen Backup können Sie Folgendes sicherstellen:

1. Die Applikationen werden in einem konsistenten Zustand gesichert und sind daher nach der Wiederherstellung der Maschine auch direkt verfügbar.
2. Sie können SQL- und Exchange-Datenbanken, Exchange-Postfächer und Exchange-Postfachelemente wiederherstellen, ohne die komplette Maschine wiederherstellen zu müssen.
3. Die SQL-Transaktionsprotokolle werden nach jedem erfolgreichen Backup abgeschnitten. Die SQL-Protokollabschneidung kann in den Backup-Plan-Optionen (S. 72) deaktiviert werden. Die Exchange-Transaktionsprotokolle werden nur auf virtuellen Maschinen abgeschnitten. Sie können die Option 'VSS-Voll-Backup' (S. 81) aktivieren, falls Sie wollen, dass die Exchange-Transaktionsprotokolle auf einer physischen Maschine abgeschnitten werden.
4. Falls eine Domain mehr als zwei Domain-Controller enthält und Sie einen davon wiederherstellen, wird eine 'nicht autorisierte' Wiederherstellung durchgeführt und so ein USN-Rollback nach der Wiederherstellung vermieden.

Was ist erforderlich, um applikationskonformes Backup verwenden zu können?

Auf einer physischen Maschine muss neben dem Agenten für Windows auch der Agent für SQL und/oder der Agent für Exchange installiert sein.

Auf einer virtuellen Maschine ist die Installation eines Agenten nicht erforderlich, weil die Maschine hier üblicherweise über den Agenten für VMware (Windows) gesichert wird.

Der Agent für VMware (Virtuelle Appliance) kann applikationskonforme Backups erstellen, aber keine Applikationsdaten aus diesen Backups wiederherstellen. Wenn Sie Applikationsdaten aus Backups wiederherstellen wollen, die von diesem Agenten erstellt wurden, benötigen Sie den Agenten für VMware (Windows), den Agenten für SQL oder den Agenten für Exchange auf einer Maschine, die auf den Speicherort zugreifen kann, wo die Backups vorliegen. Wenn Sie die Wiederherstellung von Applikationsdaten konfigurieren wollen, wählen Sie zuerst den gewünschten Recovery-Punkt auf der Registerkarte **Backups** aus und dann bei **Von dieser Maschine aus durchsuchen** die entsprechende Maschine.

Weitere Anforderungen finden Sie in den Abschnitten 'Voraussetzungen (S. 135)' und 'Erforderliche Benutzerrechte (S. 139)'.

14.3.1 Erforderliche Benutzerrechte

Ein applikationskonformes Backup enthält die Metadaten von VSS-kompatiblen Applikationen, die auf dem Laufwerk vorliegen. Um auf diese Metadaten zugreifen zu können, benötigt der Agenten ein Konto mit passenden Berechtigungen, die nachfolgend aufgeführt sind. Wenn Sie ein applikationskonformes Backup aktivieren, werden Sie aufgefordert, ein solches Konto zu spezifizieren.

- Für SQL Server:

  Das Konto muss auf der betreffenden Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder der Gruppe **Administratoren** sein – und auf jeder Instanz, die Sie sichern wollen, ein Mitglied der **SysAdmin**-Rolle.
- Für Exchange Server:

  Exchange 2007: Das Konto muss Mitglied in der Rollengruppe **Exchange-Organisationsadministratoren** sein.

  Exchange 2010 und höher: Das Konto muss Mitglied in der Rollengruppe **Organisationsverwaltung** sein.
- Für Active Directory:

  Das Konto muss ein Domain-Administrator sein.

14.4 SQL-Datenbanken wiederherstellen

Dieser Abschnitt beschreibt die Wiederherstellung von Datenbank-Backups und applikationskonformen Backups.

Sie können SQL-Datenbanken zu einer SQL Server-Instanz wiederherstellen, sofern der Agent für SQL auf derjenigen Maschine installiert ist, auf welcher die Instanz läuft. Sie müssen außerdem Anmeldedaten für ein Konto angeben, welches auf der Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder der Gruppe **Administratoren** ist – und zudem auf der Zielinstanz ein Mitglied der **SysAdmin**-Rolle ist.

Sie können die Datenbanken alternativ auch als Dateien wiederherstellen. Das kann nützlich sein, falls Sie Daten zur Überwachung oder weiteren Verarbeitung durch Drittthersteller-Tools extrahieren müssen. Wie Sie SQL-Datenbankdateien an eine SQL Server-Instanz anfügen, ist im Abschnitt 'SQL Server-Datenbanken anfügen (S. 141)' erläutert.

Falls Sie lediglich den Agenten für VMware (Windows) verwenden, ist nur eine Recovery-Methode verfügbar, nämlich Datenbanken als Dateien wiederherzustellen. Eine Wiederherstellung von Datenbanken über den Agenten für VMware (Virtual Appliance) ist nicht möglich.

Systemdatenbanken werden grundsätzlich auf die gleiche Weise wie Benutzerdatenbanken wiederhergestellt. Die Besonderheiten bei der Wiederherstellung einer Systemdatenbank sind im Abschnitt 'Systemdatenbanken wiederherstellen (S. 141)' beschrieben.

So stellen Sie SQL-Datenbanken wieder her

1. Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **Microsoft SQL**. Ansonsten können Sie diesen Schritt überspringen.
2. Wählen Sie diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.

3. Klicken Sie auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:

   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für SQL installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung der SQL-Datenbanken verwendet.
5. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen, klicken Sie auf **SQL-Datenbanken wiederherstellen**.
   - Wenn Sie eine Wiederherstellung aus einem applikationskonformen Backup durchführen, klicken Sie auf **Recovery** –> **SQL-Datenbanken**.
6. Wählen Sie Daten, die Sie wiederherstellen wollen. Klicken Sie doppelt auf eine Instanz, damit Ihnen die dort vorliegenden Datenbanken angezeigt werden.
7. Wenn Sie die Datenbanken als Dateien wiederherstellen wollen, klicken Sie auf **Als Dateien wiederherstellen**. Wählen Sie anschließend einen lokalen Ordner oder Netzwerkordner aus, in dem die Dateien gespeichert werden sollen – und klicken Sie dann auf **Recovery**. Ansonsten können Sie diesen Schritt überspringen.
8. Klicken Sie auf **Recovery**.
9. Die Datenbanken werden standardmäßig zu den ursprünglichen Datenbanken wiederhergestellt. Falls die ursprüngliche Datenbank nicht existiert, wird sie automatisch neu erstellt. Sie können auch eine andere SQL Server-Instanz (die auf derselben Maschine läuft) auswählen, auf welcher die Datenbanken wiederhergestellt werden sollen.

   So stellen Sie eine Datenbank als eine andere Datenbank auf derselben Instanz wieder her:

   a. Klicken Sie auf den Datenbanknamen.
   b. Wählen Sie bei **Recovery zu** die Option **Neue Datenbank**.
   c. Spezifizieren Sie den Namen für die neue Datenbank.
   d. Spezifizieren Sie den Pfad für die neue Datenbank und den Pfad für die Protokolle. Der von Ihnen spezifizierte Ordner darf keine ursprüngliche Datenbank oder Protokolldateien enthalten.
10. [Optional] Um das Datenbankstadium nach der Wiederherstellung zu ändern, müssen Sie auf den Datenbanknamen klicken und dann einen der folgenden Stadien auswählen:
    - **Verwendungsbereit (Mit RECOVERY wiederherstellen)** (Standardeinstellung)

      Die Datenbank ist nach Abschluss der Wiederherstellung direkt einsatzbereit. Benutzer haben vollen Zugriff auf sie. Die Software wird für alle Transaktionen der wiederhergestellten Datenbank ein Rollback ausführen, für die kein 'Commit' ausgeführt wurde und die in den Transaktionsprotokollen gespeichert sind. Sie können keine zusätzlichen Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen.
    - **Nicht betriebsbereit (Mit NORECOVERY wiederherstellen)**

      Die Datenbank ist nach Abschluss der Wiederherstellung nicht betriebsbereit. Benutzer haben keinen Zugriff auf sie. Die Software behält alle nicht übernommenen Transaktionen

(ohne 'Commit') der wiederhergestellten Datenbank. Sie können zusätzliche Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen und auf diese Weise den notwendigen Recovery-Punkt erreichen.

- **Schreibgeschützt (Mit STANDBY wiederherstellen)**

  Benutzer haben nach Abschluss der Wiederherstellung einen 'Nur Lesen'-Zugriff auf die Datenbank. Die Software wird alle nicht übernommenen Transaktionen (ohne 'Commit') rückgängig machen. Die Rückgängigaktionen werden jedoch in einer temporären Standby-Datei gespeichert, sodass die Recovery-Effekte zurückgestellt werden werden können.

  Dieser Wert wird primär verwendet, um den Zeitpunkt eines SQL Server-Fehlers zu ermitteln.

11. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

14.4.1 Systemdatenbanken wiederherstellen

Alle Systemdatenbanken einer Instanz werden gleichzeitig wiederhergestellt. Bei der Wiederherstellung von Systemdatenbanken führt die Software einen automatischen Neustart der Zielinstanz im Einzelbenutzermodus aus. Nach Abschluss der Wiederherstellung startet die Software die Instanz neu und stellt andere Datenbanken (sofern vorhanden) wieder her.

Weitere Punkte, die bei der Wiederherstellung von Systemdatenbanken beachtet werden sollten:

- Systemdatenbanken können nur zu einer Instanz wiederhergestellt werden, die dieselbe Version wie die ursprüngliche Instanz hat.
- Systemdatenbanken können nur im Stadium 'Verwendungsbereit' (ready to use) wiederhergestellt werden.

Die master-Datenbank wiederherstellen

Zu den Systemdatenbanken gehört auch die sogenannte **master**-Datenbank. Die **master**-Datenbank erfasst allgemeine Informationen über alle Datenbanken einer Instanz. Die **master**-Datenbank in einem Backup enthält daher genau die Informationen über die Datenbanken, die zum Zeitpunkt des Backups in der Instanz vorlagen. Nach der Wiederherstellung der **master**-Datenbank müssen Sie möglicherweise Folgendes tun:

- Datenbanken, die in der Instanz aufgetaucht sind, nachdem das Backup erstellt wurde, sind für die Instanz nicht sichtbar. Um diese Datenbanken zurück in die Produktion zu bringen, müssen Sie diese manuell mithilfe des Microsoft SQL Server Management Studios an die Instanz anschließen.
- Datenbanken, die nach Erstellung des Backups gelöscht wurden, werden in der Instanz als offline angezeigt. Löschen Sie diese Datenbanken mithilfe des SQL Server Management Studios.

14.4.2 SQL Server-Datenbanken anfügen

Dieser Abschnitt beschreibt, wie Sie eine Datenbank im SQL Server mithilfe des SQL Server Management Studios anfügen können. Es kann immer nur eine Datenbank gleichzeitig angefügt werden.

Das Anfügen einer Datenbank erfordert eine der folgenden Berechtigungen: **Datenbank erstellen**, **Beliebige Datenbank erstellen** oder **Beliebige Datenbank ändern**. Normalerweise verfügt auf der Instanz die Rolle **SysAdmin** über diese Berechtigungen.

So fügen Sie eine Datenbank an

1. Führen Sie Microsoft SQL Server Management Studio aus.
2. Verbinden Sie sich mit der benötigten SQL Server-Instanz und erweitern Sie dann die Instanz.
3. Klicken Sie mit der rechten Maustaste auf **Datenbanken** und klicken Sie dann auf **Anfügen**.
4. Klicken Sie auf **Hinzufügen**.
5. Lokalisieren und Wählen Sie im Dialogfenster **Datenbankdateien suchen** die .mdf-Datei der Datenbank.
6. Stellen Sie im Bereich **Datenbankdetails** sicher, dass die restlichen Datenbankdateien (.ndf- und .ldf-Dateien) gefunden werden.

   Details: SQL Server-Datenbankdateien werden möglicherweise nicht automatisch gefunden, falls:

   - Sie sich nicht am Standardspeicherort befinden – oder sie nicht im selben Ordner wie die primäre Datenbankdatei (.mdf) sind. Lösung: Spezifizieren Sie den Pfad zu den benötigten Dateien manuell in der Spalte **Aktueller Dateipfad**.
   - Sie haben einen unvollständigen Satz an Dateien wiederhergestellt, der die Datenbank bildet. Lösung: Stellen Sie die fehlenden SQL Server-Datenbankdateien aus dem Backup wieder her.
7. Klicken Sie, wenn alle Dateien gefunden sind, auf **OK**.

14.5 Exchange-Datenbanken wiederherstellen

Dieser Abschnitt beschreibt die Wiederherstellung von Datenbank-Backups und applikationskonformen Backups.

Sie können Exchange Server-Daten zu einem aktiv laufenden Exchange Server wiederherstellen. Dies kann der ursprüngliche Exchange Server sein – oder ein Exchange Server mit derselben Version, der auf einer Maschine mit demselben vollqualifizierten Domain-Namen (FQDN) läuft. Der Agent für Exchange muss auf der Zielmaschine installiert sein.

Die nachfolgende Tabelle gibt Ihnen einen Überblick über die Exchange Server-Daten, die Sie für eine Wiederherstellung verwenden können – und die (mindestens benötigten) Benutzerrechte, die zur Wiederherstellung dieser Daten erforderlich sind.

Exchange-Version	Datenelemente	Benutzerrechte
2007	Speichergruppen	Mitglied in der Rollengruppe **Exchange-Organisationsadministratoren**.
2010/2013/2016	Datenbanken	Mitglied in der Rollengruppe **Serververwaltung**.

Sie können die Datenbanken (Speichergruppen) alternativ auch als Dateien wiederherstellen. Die Datenbankdateien werden (zusammen mit den Transaktionsprotokolldateien) aus dem Backup in einem von Ihnen spezifizierten Ordner extrahiert. Das kann nützlich sein, falls Sie Daten für eine Überwachung oder zur weiteren Verarbeitung durch Tools von Drittherstellern extrahieren müssen – oder wenn eine Wiederherstellung aus irgendeinem Grund fehlschlägt und Sie nach einem Workaround suchen, die Datenbanken manuell zu mounten (S. 143).

Falls Sie lediglich den Agenten für VMware (Windows) verwenden, ist nur eine Recovery-Methode verfügbar, nämlich Datenbanken als Dateien wiederherzustellen. Eine Wiederherstellung von Datenbanken über den Agenten für VMware (Virtual Appliance) ist nicht möglich.

So stellen Sie Exchange-Daten wieder her

Wir werden bei dieser Prozedur die Datenbanken und Speichergruppen einheitlich nur als 'Datenbanken' bezeichnen.

1. Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen wollen, klicken Sie auf **Microsoft Exchange**. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.
2. Wählen Sie diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
3. Klicken Sie auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Andere Wiederherstellungsmöglichkeiten verwenden:

   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird als Zielmaschine für die Wiederherstellung der Exchange-Daten verwendet.
5. Klicken Sie auf **Recovery** –> **Exchange-Datenbanken**.
6. Wählen Sie Daten, die Sie wiederherstellen wollen.
7. Wenn Sie die Datenbanken als Dateien wiederherstellen wollen, klicken Sie auf **Als Dateien wiederherstellen**. Wählen Sie anschließend einen lokalen Ordner oder Netzwerkordner aus, in dem die Dateien gespeichert werden sollen – und klicken Sie dann auf **Recovery**. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.
8. Klicken Sie auf **Recovery**. Geben Sie auf Nachfrage die Anmeldedaten für den Exchange Server an.
9. Die Datenbanken werden standardmäßig zu den ursprünglichen Datenbanken wiederhergestellt. Falls die ursprüngliche Datenbank nicht existiert, wird sie automatisch neu erstellt.

   So stellen Sie eine Datenbank zu einer anderen Datenbank wieder her:

   a. Klicken Sie auf den Datenbanknamen.
   b. Wählen Sie bei **Recovery zu** die Option **Neue Datenbank**.
   c. Spezifizieren Sie den Namen für die neue Datenbank.
   d. Spezifizieren Sie den Pfad für die neue Datenbank und den Pfad für die Protokolle. Der von Ihnen spezifizierte Ordner darf keine ursprüngliche Datenbank oder Protokolldateien enthalten.
10. Klicken Sie auf **Recovery starten**.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

14.5.1 Exchange-Server-Datenbanken mounten

Sie können die Datenbanken nach Wiederherstellung der Datenbankdateien dadurch wieder online bringen, dass Sie sie mounten. Das Mounten wird mithilfe der Exchange-Verwaltungskonsole, dem Exchange-System-Manager oder der Exchange-Verwaltungsshell durchgeführt.

Die wiederhergestellte Datenbank wird sich im Stadium 'Dirty Shutdown' befinden. Eine Datenbank, die sich im Zustand 'Dirty Shutdown' befindet, kann vom System gemountet werden, falls sie zu ihrem ursprünglichen Speicherort wiederhergestellt wurde (vorausgesetzt, die Information über die ursprüngliche Datenbank ist im Active Directory vorhanden). Wenn Sie eine Datenbank zu einem anderen Speicherort wiederherstellen (beispielsweise eine neue Datenbank oder die

Wiederherstellungsdatenbank), dann kann die Datenbank solange gemountet werden, bis Sie sie mithilfe des Befehls **`Eseutil /r <Enn>`** in das Stadium 'Clean Shutdown' bringen. **`<Enn>`** gibt das Protokolldatei-Präfix für die Datenbank an (bzw. die Speichergruppe, welche die Datenbank enthält), auf die Sie die Transaktionsprotokolldateien anwenden müssen.

Das Konto, welches Sie zum Anfügen einer Datenbank verwenden, muss an eine Exchange-Server-Administratorrolle und an eine lokalen Administratorengruppe des Zielservers delegiert sein.

Weitere Details zum Mounten von Datenbanken finden Sie in folgenden Artikeln:

- Exchange 2010 oder höher: http://technet.microsoft.com/de-de/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/de-de/library/aa998871(v=EXCHG.80).aspx

14.6 Exchange-Postfächer und Postfachelemente wiederherstellen

Dieser Abschnitt beschreibt die Wiederherstellung von Exchange-Postfächern und Postfachelementen aus Datenbank-Backups und applikationskonformen Backups.

Überblick

Granulares Recovery kann zu einem Microsoft Exchange Server 2010 Service Pack 1 (SP1) oder höher durchgeführt werden. Die im Quell-Backup gespeicherten Datenbanken dürfen für ein granulares Recovery von jeder unterstützten Exchange-Version stammen.

Granulares Recovery kann vom Agenten für Exchange oder vom Agent for VMware (Windows) durchgeführt werden. Der als Ziel verwendete Exchange Server und die Maschine, auf welcher der Agent läuft, müssen derselben Active Directory-Gesamtstruktur (Forest) angehören.

Folgende Elemente können wiederhergestellt werden:

- Postfächer (ausgenommen archivierte Postfächer)
- Öffentliche Ordner
- Öffentlicher Ordner-Elemente
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalenderereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Anmerkungen

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Wenn bei einer Postfach-Wiederherstellung ein vorhandenes Postfach als Ziel ausgewählt wird, werden alle dort vorliegenden Elemente, die übereinstimmende IDs haben, überschrieben.

Bei einer Wiederherstellung von Postfachelementen werden keinerlei Elemente überschrieben. Die Postfachelemente werden immer in einem Ordner (des Zielpostfaches) mit der Bezeichnung **Wiederhergestellte Elemente** gespeichert.

Anforderungen an Benutzerkonten

Ein von einem Backup aus wiederhergestelltes Postfach muss ein assoziiertes Benutzerkonto im Active Directory haben.

Benutzerpostfächer und deren Inhalte können nur dann wiederhergestellt werden, wenn die mit ihnen assoziierten Benutzerkonten *aktiviert* sind. Raum-, Geräte- oder freigegebene Postfächer können nur dann wiederhergestellt werden, wenn ihre assoziierten Benutzerkonten *deaktiviert* sind.

Ein Postfach, welches die oberen Bedingungen nicht erfüllt, wird während einer Wiederherstellung übersprungen.

Falls einige Postfächer übersprungen werden, die Wiederherstellung mit dem Status 'Mit Warnungen' abgeschlossen. Sollten alle Postfächer übersprungen werden, schlägt die Wiederherstellung fehl.

14.6.1 Postfächer wiederherstellen

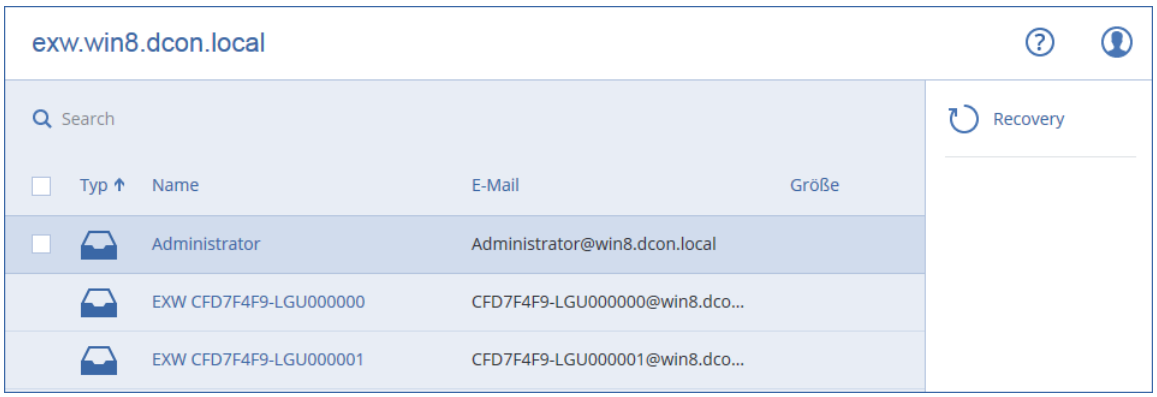
1. Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen wollen, klicken Sie auf **Microsoft Exchange**. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.
2. Wählen Sie diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
3. Klicken Sie auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Andere Wiederherstellungsmöglichkeiten verwenden:

   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird dann die Wiederherstellung durchführen (statt der ursprünglichen Maschine, die offline ist).
5. Klicken Sie auf **Recovery** –> **Exchange-Postfächer**.
6. Wählen Sie die Postfächer aus, die Sie wiederherstellen wollen.

   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.



7. Klicken Sie auf **Recovery**.
8. Klicken Sie auf **Zielmaschine mit Microsoft Exchange Server**, wenn Sie die Zielmaschine auswählen oder ändern wollen. Mit diesem Schritt können Sie eine Maschine als Recovey-Ziel verwenden, auf der kein Agent für Exchange läuft.

   Spezifizieren Sie den vollqualifizierten Domain-Namen (FQDN) einer Maschine, auf welcher die Rolle '**Clientzugriff**' des Microsoft Exchange Servers aktiviert ist. Die Maschine muss zu derselben Active Directory-Gesamtstruktur (Forest) gehören wie die Maschine, welche die Wiederherstellung durchführt.

   Geben Sie bei Aufforderung die Anmeldedaten eines Kontos ein, welches für den Zugriff auf die Maschine verwendet werden soll. Die Anforderungen für dieses Konto sind im Abschnitt 'Erforderliche Benutzerrechte (S. 147)' aufgeführt.
9. [Optional] Klicken Sie auf **Datenbank zur Neuerstellung fehlender Postfächer**, wenn Sie die automatisch ausgewählte Datenbank ändern wollen.
10. Klicken Sie auf **Recovery starten**.
11. Bestätigen Sie Ihre Entscheidung.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

14.6.2 Postfachelemente wiederherstellen

1. Wenn Sie eine Wiederherstellung aus einem Datenbank-Backup durchführen wollen, klicken Sie auf **Microsoft Exchange**. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.
2. Wählen Sie diejenige Maschine aus, auf der sich die wiederherzustellenden Daten ursprünglich befunden haben.
3. Klicken Sie auf **Recovery**.
4. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.

   Falls die Maschine offline ist, werden keine Recovery-Punkte angezeigt. Andere Wiederherstellungsmöglichkeiten verwenden:

   - Sollte sich das Backup im Cloud Storage oder einem freigegebenen Storage befinden (d.h., dass andere Agenten auf diesen zugreifen können), dann klicken Sie zuerst auf den Befehl **Maschine auswählen**. Wählen Sie anschließend eine Maschine aus, die online ist und auf welcher der Agent für Exchange oder der Agent für VMware installiert ist, und dann den gewünschten Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).

   Die in einer der oberen Aktionen zum Durchsuchen ausgewählte Maschine wird dann die Wiederherstellung durchführen (statt der ursprünglichen Maschine, die offline ist).
5. Klicken Sie auf **Recovery** –> **Exchange-Postfächer**.
6. Klicken Sie auf dasjenige Postfach, in dem sich die wiederherzustellenden Elemente ursprünglich befunden haben.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

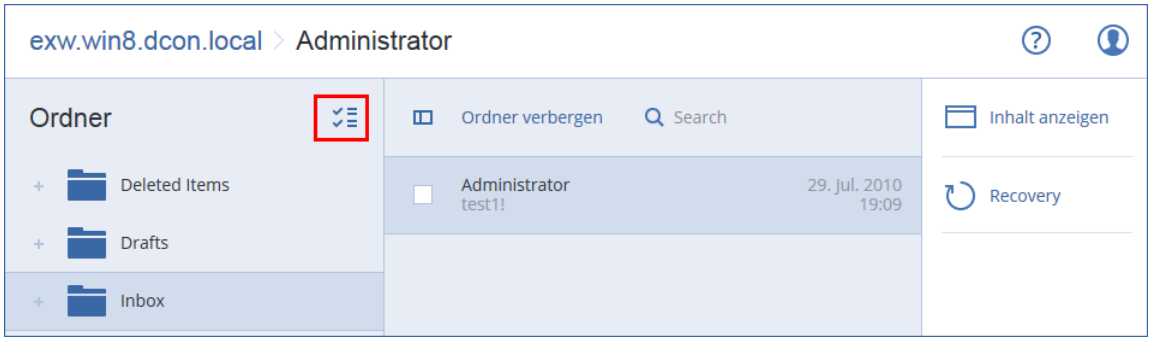
   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
   - Für Ereignisse: Suche per Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

Bei Auswahl einer E-Mail-Nachricht können Sie auf **Inhalt anzeigen** klicken, damit Ihnen die Nachricht (inkl. Anhänge) angezeigt wird.

Tipp: *Sie können eine angehängte Datei herunterladen, indem Sie auf ihren Namen klicken.*

Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol zum Wiederherstellen von Ordnern.



8. Klicken Sie auf **Recovery**.
9. Klicken Sie auf **Zielmaschine mit Microsoft Exchange Server**, wenn Sie die Zielmaschine auswählen oder ändern wollen. Mit diesem Schritt können Sie eine Maschine als Recovey-Ziel verwenden, auf der kein Agent für Exchange läuft.

   Spezifizieren Sie den vollqualifizierten Domain-Namen (FQDN) einer Maschine, auf welcher die Rolle '**Clientzugriff**' des Microsoft Exchange Servers aktiviert ist. Die Maschine muss zu derselben Active Directory-Gesamtstruktur (Forest) gehören wie die Maschine, welche die Wiederherstellung durchführt.

   Geben Sie bei Aufforderung die Anmeldedaten eines Kontos ein, welches für den Zugriff auf die Maschine verwendet werden soll. Die Anforderungen für dieses Konto sind im Abschnitt 'Erforderliche Benutzerrechte (S. 147)' aufgeführt.
10. Bei **Zielpostfach** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht existiert oder Sie eine andere als die ursprüngliche Maschine als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
11. Klicken Sie auf **Recovery starten**.
12. Bestätigen Sie Ihre Entscheidung.

Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt.

14.6.3 Erforderliche Benutzerrechte

Um auf Postfächer zugreifen zu können, benötigt der Agent für Exchange ein Konto mit passenden Berechtigungen. Sie werden aufgefordert, dieses Konto zu spezifizieren, wenn Sie Aktionen mit Postfächern konfigurieren.

Die Mitgliedschaft des Kontos in der Rollengruppe **Organisationsverwaltung** ermöglicht den Zugriff auf alle Postfächer (auch solche, die in Zukunft erstellt werden).

Die mindestens erforderlichen Benutzerrechte sind:

- Das Konto muss Mitglied in der Rollengruppe **Empfängerverwaltung** sein.
- Das Konto muss die Verwaltungsrolle **ApplicationImpersonation** für alle Benutzer oder Benutzergruppen aktiviert haben, auf deren Postfächer der Agent zugreifen wird.

Genauere Informationen zur Konfiguration der Verwaltungsrolle **ApplicationImpersonation** finden Sie im folgenden Microsoft Knowledge Base-Artikel: https://msdn.microsoft.com/de-de/library/office/dn722376.aspx.

15 Office 365-Daten sichern

Warum sollten Sie Office 365-Daten per Backup sichern?

Microsoft Office 365 ist zwar ein Set von Cloud-Diensten, ein regelmäßiges Backup bietet aber eine zusätzliche Schutzebene gegen Anwenderfehler und böswillige Angriffe. Sie können gelöschte Elemente auch dann noch aus einem Backup wiederherstellen, wenn die offizielle Office 365-Aufbewahrungsdauer abgelaufen ist. Zusätzlich können Sie eine lokale Kopie Ihrer Exchange Online-Postfächer speichern, falls Sie dies aufgrund von gesetzlichen oder firmeninternen Vorschriften tun müssen.

Agent für Office 365

Abhängig von der gewünschten Funktionalität können Sie den Agenten für Office 365 lokal installieren, den in der Cloud installieren Agenten verwenden – oder beides. Die nachfolgende Tabelle fasst die Funktionalität des lokalen und Cloud-basierten Agenten zusammen.

	Lokaler Agent für Office 365	**Cloud Agent für Office 365**
Datenelemente, die per Backup gesichert werden können	**Exchange Online:** Benutzer und freigegebene Postfächer	▪ **Exchange Online**: Benutzerpostfächer, freigegebene Postfächer und Gruppenpostfächer ▪ **OneDrive**: Benutzer-Dateien und -Ordner ▪ **SharePoint Online**: klassische Website-Sammlungen, Gruppen-(Team)-Websites, Kommunikations-Websites, einzelne Datenelemente
Backup von Archivpostfächern (**In-Situ-Archiv**)	Nein	Ja
Backup-Planung	Benutzerdefiniert (S. 48)	Kann nicht geändert werden. Jeder Backup-Plan wird täglich zur gleichen Tageszeit ausgeführt.*
Backup-Speicherorte	Cloud Storage, lokaler Ordner, Netzwerkordner	Nur Cloud Storage
Automatischer Schutz für neue Office 365-Benutzer, -Gruppen, -Websites	Nein	Ja, indem Sie einen Backup-Plan auf die Gruppen **Alle Benutzer**, **Alle Gruppen**, **Alle Websites** anwenden.
Mehr als eine Office 365-Organisation sichern	Nein	Ja
Granulares Recovery	Ja	Ja

	Lokaler Agent für Office 365	Cloud Agent für Office 365
Wiederherstellung zu einem anderen Benutzer innerhalb einer Organisation	Ja	Ja
Wiederherstellung zu einer anderen Organisation	Nein	Ja
Wiederherstellung zu einem lokalen Microsoft Exchange Server	Nein	Nein
Maximale Anzahl von Elementen, die ohne Performanceverlust gesichert werden können	Wenn Sie den Cloud Storage als Backup-Ziel verwenden: 5000 Postfächer pro Unternehmen Wenn andere Speicherorte als Backup-Ziel dienen: 2000 Postfächer pro Backup-Plan (ohne Beschränkung der Anzahl der Postfächer pro Unternehmen)	5000 gesicherte Elemente (Postfächer, OneDrives oder Websites) pro Unternehmen

* Da ein Cloud Agent mehrere Kunden bedient, bestimmt der Agent die Startzeit für jeden Backup-Plan selbst, um eine gleichmäßige Auslastung über den Tag und die gleiche Service-Qualität für alle Kunden zu gewährleisten.

Beschränkung

Eine automatische Erstellung von Benutzern, Gruppen oder Websites während einer Wiederherstellung ist nicht möglich. Wenn Sie z.B. eine gelöschte SharePoint Online-Website wiederherstellen wollen, erstellen Sie zuerst manuell eine neue Website und spezifizieren Sie diese Website dann als Ziel für eine Wiederherstellung.

Erforderliche Benutzerrechte

Im Backup Service

Jeder Agent für Office 365, ob lokal oder Cloud-basiert, muss unter dem Konto eines Kunden-Administrators registriert sein.

In Microsoft Office 365

Ihrem Konto muss die Rolle 'globaler Administrator' in Microsoft Office 365 zugewiesen sein.

- Der lokale Agent wird sich mit diesem Konto bei Office 365 anmelden. Damit der Agent auf die Inhalte aller Postfächer zugreifen kann, wird diesem Konto die Verwaltungsrolle **ApplicationImpersonation** zugewiesen. Wenn Sie das Kontokennwort ändern, müssen Sie auch das Kennwort in der Backup-Konsole aktualisieren (wie unter 'Die Office 365-Zugriffsanmeldedaten ändern (S. 152)' beschrieben).
- Der Cloud Agent meldet sich nicht bei Office 365 an. Der Agent erhält die notwendigen Berechtigungen direkt von Microsoft Office 365. Sie müssen die Gewährung dieser Berechtigungen nur einmal bestätigen, wenn Sie als globaler Administrator angemeldet sind. Der Agent speichert Ihre Kontoanmeldedaten nicht und verwendet diese beim Durchführen von Backups und Wiederherstellungen nicht. Eine Änderung des Kontokennworts in Office 365 hat keinen Einfluss auf den Betrieb des Agenten.

15.1 Den lokal installierten Agenten für Office 365 verwenden

15.1.1 Eine Microsoft Office 365-Organisation hinzufügen

So können Sie eine Microsoft Office 365-Organisation hinzufügen

1. Melden Sie sich als Firmenadministrator an der Backup-Konsole an.
2. Klicken Sie in der rechten oberen Ecke auf das Symbol für 'Konto' und anschließend auf die Befehle **Downloads** –> **Agent fü Office 365**.
3. Laden Sie den Agenten herunter und installieren Sie ihn auf einer Windows-Maschine, die mit dem Internet verbunden ist.
4. Klicken Sie nach Abschluss der Installation auf **Geräte** –> **Microsoft Office 365** – und geben Sie dann die Anmeldedaten des globalen Office 365-Administrators ein.

   ***Wichtig:**: Innerhalb einer Organisation (Firmen-Gruppe) darf es nur einen lokal installierten Agenten für Office 365 geben.*

Als Ergebnis erscheinen die Datenelemente Ihres Unternehmens/Ihrer Organisation in der Backup-Konsole auf der Seite **Microsoft Office 365**.

15.1.2 Exchange Online-Postfächer sichern

Welche Elemente können per Backup gesichert werden?

Sie können Benutzerpostfächer und freigegebene Postfächer sichern. Gruppen- und Archivpostfächer (**In-Situ-Archiv**) können nicht gesichert werden.

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:

- Postfächer
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalenderereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Anmerkungen

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Wenn bei einer Postfach-Wiederherstellung ein vorhandenes Postfach als Ziel ausgewählt wird, werden alle dort vorliegenden Elemente, die übereinstimmende IDs haben, überschrieben.

Bei einer Wiederherstellung von Postfachelementen werden keinerlei Elemente überschrieben. Stattdessen wird der vollständige Pfad zu einem Postfachelement im Zielordner neu erstellt.

15.1.2.1 Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann nach Bedarf (S. 38) die anderen Einstellungen des Backup-Plans.

So wählen Sie Postfächer aus

1. Klicken Sie auf **Microsoft Office 365**.
2. Melden Sie sich bei Aufforderung als globaler Administrator an Microsoft Office 365 an.
3. Wählen Sie die Postfächer aus, die Sie per Backup sichern wollen.
4. Klicken Sie auf **Backup**.

15.1.2.2 Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wählen Sie das wiederherzustellende Postfach und klicken Sie dann auf **Recovery**.

   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backups' (S. 125) aus – und klicken Sie dann auf **Backups anzeigen**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.
4. Klicken Sie auf **Recovery** –> **Postfach**.
5. Bei **Zielpostfach** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

   Das ursprüngliche Postfach wird automatisch vorausgewählt. Sollte dieses Postfach nicht existieren, müssen Sie das Zielpostfach spezifizieren.
6. Klicken Sie auf **Recovery starten**.

Postfachelemente wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wählen Sie dasjenige Postfach aus, in dem sich die wiederherzustellenden Elemente ursprünglich befunden haben – und klicken Sie dann auf **Recovery**.

   Sie können die Postfächer nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   Falls das Postfach gelöscht wurde, wählen Sie es in der Registerkarte 'Backups' (S. 125) aus – und klicken Sie dann auf **Backups anzeigen**.
3. Wählen Sie einen Recovery-Punkt. Beachten Sie dabei, dass Recovery-Punkte nach Speicherort gefiltert werden.
4. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
5. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
   - Für Ereignisse: Suche per Titel und Datum.
   - Für Tasks: Suche per Betreff und Datum.
   - Für Kontakte: Suche per Name, E-Mail-Adresse und Telefonnummer.

   Bei Auswahl einer E-Mail-Nachricht können Sie auf **Inhalt anzeigen** klicken, damit Ihnen die Nachricht (inkl. Anhänge) angezeigt wird.

   Tipp: *Sie können eine angehängte Datei herunterladen, indem Sie auf ihren Namen klicken.*

Wenn eine E-Mail-Nachricht ausgewählt wurde, können Sie auf **Als E-Mail senden** klicken, damit die Nachricht an eine bestimmte E-Mail-Adresse gesendet wird. Als Absender der Nachricht wird die E-Mail-Adresse Ihres Administrator-Kontos verwendet.

Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 

6. Klicken Sie auf **Recovery**.
7. Bei **Zielpostfach** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

   Das ursprüngliche Postfach wird automatisch vorausgewählt. Sollte dieses Postfach nicht existieren, müssen Sie das Zielpostfach spezifizieren.
8. Klicken Sie auf **Recovery starten**.
9. Bestätigen Sie Ihre Entscheidung.

Die Postfachelemente werden immer in einem Ordner (des Zielpostfaches) mit der Bezeichnung **Wiederhergestellte Elemente** gespeichert.

15.1.2.3 Die Office 365-Zugriffsanmeldedaten ändern

Sie können die Zugriffsanmeldedaten für Office 365 ändern, ohne den Agenten neu installieren zu müssen.

So ändern Sie die Anmeldedaten für Office 365

1. Klicken Sie auf **Geräte** –> **Microsoft Office 365**.
2. Klicken Sie auf **Anmeldedaten spezifizieren**.
3. Geben Sie die Anmeldedaten des globalen Office 365-Administrators ein und klicken Sie dann auf **OK**.

   Der Agent wird sich mit diesem Konto bei Office 365 anmelden. Damit der Agent auf die Inhalte aller Postfächer zugreifen kann, wird diesem Konto die Verwaltungsrolle **ApplicationImpersonation** zugewiesen.

15.2 Den Cloud Agenten für Office 365 verwenden

15.2.1 Eine Microsoft Office 365-Organisation hinzufügen

So können Sie eine Microsoft Office 365-Organisation hinzufügen

1. Melden Sie sich als Firmenadministrator an der Backup-Konsole an.
2. Klicken Sie auf **Geräte** –> **Hinzufügen** –> **Microsoft Office 365 Business**.
3. Wählen Sie das von Ihrer Organisation/Firma verwendete Microsoft Datacenter aus.

   Die Software leitet Sie zur Microsoft Office 365-Anmeldeseite weiter.
4. Melden Sie sich mit den Anmeldedaten des globalen Office 365-Administrators an.

   Microsoft Office 365 zeigt eine Liste der Berechtigungen an, die erforderlich sind, um die Daten Ihres Unternehmens sichern und wiederherstellen zu können.
5. Bestätigen Sie, dass Sie dem Backup Service diese Berechtigungen gewähren wollen.

Als Ergebnis erscheinen die Datenelemente Ihres Unternehmens in der Backup-Konsole auf der Seite **Microsoft Office 365**.

Tipps zur weiteren Nutzung

- Der Cloud Agent führt die Synchronisierung mit Office 365 alle 24 Stunden durch, beginnend mit dem Zeitpunkt, ab dem das Unternehmen dem Backup Service hinzugefügt wurde. Wenn Sie einen Benutzer, eine Gruppe oder eine Website hinzufügen oder entfernen, wird diese Änderung nicht sofort in der Backup-Konsole angezeigt. Wenn Sie die Synchronisierung des Cloud Agenten mit Office 365 erzwingen wollen, wählen Sie die entsprechende Organisation auf der **Microsoft Office 365**-Seite aus und klicken Sie dann auf **Aktualisieren**.
- Wenn Sie den Gruppen **Alle Benutzer**, **Alle Gruppen** oder **Alle Websites** einen Backup-Plan zugewiesen haben, werden die neu hinzugefügten Elemente erst dann in das Backup aufgenommen, wenn die Synchronisierung durchgeführt wurde.
- Gemäß den Microsoft-Richtlinien bleibt ein Benutzer, eine Gruppe oder eine Website, nachdem diese aus der Office 365-Benutzeroberfläche entfernt wurden, noch für einige weitere Tage per API verfügbar. Während dieser Tage wird das entfernte Element in der Backup-Konsole als inaktiv (ausgegraut) dargestellt und nicht per Backup gesichert. Wenn das entfernte Element auch nicht mehr per API verfügbar ist, verschwinden es ganz aus der Backup-Konsole. Dessen Backups können (sofern vorhanden) unter **Backups** –> **Cloud-Applikationen-Backups** gefunden werden.

15.2.2 Exchange Online-Postfächer sichern

Welche Elemente können per Backup gesichert werden?

Sie können Benutzerpostfächer, freigegebene Postfächer und Gruppenpostfächer sichern. Außerdem können Sie optional auch die Archivpostfächer (**In-Situ-Archiv**) der ausgewählten Postfächer sichern.

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:

- Postfächer
- E-Mail-Ordner
- E-Mail-Nachrichten
- Kalendereereignisse
- Aufgaben
- Kontakte
- Journal-Einträge
- Anmerkungen

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Sie können bei der Wiederherstellung von Postfächern und Postfachelementen auswählen, ob die Elemente am Zielort überschrieben werden sollen (oder nicht).

15.2.2.1 Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann nach Bedarf (S. 38) die anderen Einstellungen des Backup-Plans.

So können Sie Exchange Online-Postfächer auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.

3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Postfächer aller Benutzer und alle freigegegenen Postfächer zu sichern (einschließlich solcher Postfächer, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Benutzerpostfächer oder freigegebene Postfächer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Postfächer Sie sichern wollen, und klicken Sie dann auf **Backup**.
   - Um alle Gruppenpostfächer zu sichern (einschließlich der Postfächer von Gruppen, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Gruppenpostfächer sichern wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie die Gruppen aus, deren Postfächer Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Backup-Plan-Fensterbereich:
   - Überprüfen Sie, dass das Element **Postfächer** bei **Backup-Quelle** ausgewählt ist.
   - Wenn Sie keine Archivpostfächer sichern wollen, deaktivieren Sie den Schalter **Archivpostfach**.

15.2.2.2 Postfächer und Postfachelemente wiederherstellen

Postfächer wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie ein Benutzerpostfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie den Benutzer aus, dessen Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
   - Wenn Sie ein freigegebenes Postfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie das freigegebene Postfach aus, welches Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
   - Wenn Sie ein Gruppenpostfach wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie die Gruppe aus, deren Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.
   - Wenn der Benutzer, die Gruppe oder das freigegebene Postfach zuvor gelöscht wurde, können Sie das Element im Bereich **Cloud-Applikationen-Backups** in der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die Postfächer enthalten, wählen Sie* ***Postfächer*** *bei* ***Nach Inhalt filtern****.*
5. Klicken Sie auf **Recovery** –> **Komplettes Postfach**.

6. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
7. Bei **Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

   Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
8. Klicken Sie auf **Recovery starten**.
9. Wählen Sie eine dieser Überschreiben-Optionen:
   - **Vorhandene Elemente überschreiben**
   - **Vorhandene Elemente nicht überschreiben**
10. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

Postfachelemente wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie Elemente aus einem Benutzerpostfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie denjenigen Benutzer aus, in dessen Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Elemente aus einem freigegebenen Postfach wiederherstellen wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie dasjenige freigegebene Postfach aus, in welchem sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Elemente aus einem Gruppenpostfach wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie diejenige Gruppe aus, in deren Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn der Benutzer, die Gruppe oder das freigegebene Postfach zuvor gelöscht wurde, können Sie das Element im Bereich **Cloud-Applikationen-Backups** in der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die Postfächer enthalten, wählen Sie* ***Postfächer*** *bei* ***Nach Inhalt filtern****.*
5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Elemente abzurufen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

- Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger und Datum.
- Für Ereignisse: Suche nach Titel und Datum.
- Für Tasks: Suche per Betreff und Datum.
- Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.

7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen. Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 

   Zusätzlich haben Sie auch folgende Möglichkeiten:

   - Klicken Sie bei der Auswahl eines Elements auf **Inhalt anzeigen**, um die Inhalte (inklusive Anhänge) einsehen zu können. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
   - Klicken Sie bei der Auswahl einer Nachricht oder eines Kalenderelements auf **Als E-Mail senden**, wenn Sie das Element an eine spezifizierte E-Mail-Adresse versenden wollen. Sie können den Absender bestimmen und einen Text schreiben, der dem weitergeleiteten Element hinzugefügt wird.
   - Nur bei einem unverschlüsselten Backup, wenn Sie die Suchfunktion verwendet und ein einzelnes Element in den Suchergebnissen ausgewählt haben: klicken Sie auf **Versionen anzeigen**, um die Version des Elements auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.

8. Klicken Sie auf **Recovery**.
9. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
10. Bei **Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
11. [Nur bei Wiederherstellung zu einem Benutzerpostfach oder freigegebenen Postfach] Bei **Pfad** können Sie den Zielordner im Zielpostfach einsehen oder ändern. Standardmäßig ist der Ordner **Wiederhergestellte Elemente** vorausgewählt.

    Gruppenpostfachelemente werden immer im Ordner **Posteingang** wiederhergestellt.
12. Klicken Sie auf **Recovery starten**.
13. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Elemente überschreiben**
    - **Vorhandene Elemente nicht überschreiben**
14. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.2.3 OneDrive-Dateien sichern

Welche Elemente können per Backup gesichert werden?

Sie können ein komplettes OneDrive sichern – oder auch nur einzelne Dateien und Ordner.

Dateien werden inklusive ihrer Freigabeberechtigungen gesichert. Erweiterte Berechtigungsstufen (**Entwerfen**, **Vollzugriff**, **Mitwirken**) werden nicht mitgesichert.

Welche Elemente können wiederhergestellt werden?

Sie können ein komplettes OneDrive wiederherstellen oder beliebige einzelne Dateien/Ordner, die gesichert wurden.

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Freigabeberechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

Freigabelinks für Dateien und Ordner werden nicht wiederhergestellt.

15.2.3.1 OneDrive-Dateien auswählen

Wählen Sie die Dateien wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Backup-Plans nach Bedarf (S. 38).

So können Sie OneDrive-Dateien auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Dateien aller Benutzer zu sichern (einschließlich solcher Benutzer, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie die Dateien einzelner Benutzer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Dateien Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Backup-Plan-Fensterbereich:
   - Überprüfen Sie, dass das Element **OneDrive** bei **Backup-Quelle** ausgewählt ist.
   - Wählen Sie bei **Elemente für das Backup** eine der folgenden Möglichkeiten:
     - Übernehmen Sie die Voreinstellung **[Alle]** (alle Dateien).
     - Spezifizieren Sie die zu sichernden Dateien und Ordner an, indem Sie deren Namen oder Pfade hinzufügen.

       Sie können Platzhalterzeichen (*, ** und ?) verwenden. Ausführlichere Informationen über die Verwendung von Pfaden und Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.
     - Spezifizieren Sie Dateien und Ordner für das Backup, indem Sie diese per 'Durchsuchen' auswählen.

       Der Link **Durchsuchen** ist nur verfügbar, wenn ein Backup-Plan für einen einzelnen Benutzer erstellt wird.
   - [Optional] Klicken Sie bei **Elemente für das Backup** auf **Ausschlusskriterien anzeigen**, um zu spezifizieren, ob und welche Dateien und Ordner während des Backup-Prozesses übersprungen werden sollen.

Dateiausschlusskritieren überschreiben eine vorherige Dateiauswahl, d.h., wenn Sie in beiden Feldern dieselbe Datei spezifizieren, wird diese Datei beim anschließenden Backup übersprungen.

15.2.3.2 OneDrive und OneDrive-Dateien wiederherstellen

Ein komplettes OneDrive wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen OneDrive Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die OneDrive-Dateien enthalten, wählen Sie* ***OneDrive*** *bei* ***Nach Inhalt filtern****.*
5. Klicken Sie auf **Recovery** –> **Kompletter OneDrive-Ordner**.
6. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
7. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer anzeigen lassen, ändern oder spezifizieren.

   Der ursprüngliche Benutzer wird automatisch vorausgewählt. Wenn dieser Benutzer nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer spezifizieren.
8. Bestimmen Sie, ob Sie auch die Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
11. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

OneDrive-Dateien wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.

3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen OneDrive-Dateien Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die OneDrive-Dateien enthalten, wählen Sie* ***OneDrive*** *bei* ***Nach Inhalt filtern****.*
5. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
7. Wählen Sie die Dateien, die Sie wiederherstellen wollen.

   Wenn das Backup unverschlüsselt ist und Sie eine einzelne Datei ausgewählt haben, können Sie auf **Versionen anzeigen** klicken, um eine bestimmte Dateiversion auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Wenn Sie eine Datei herunterladen wollen, müssen Sie diese auswählen, auf **Download** klicken, den Zielspeicherort für die Datei bestimmen und schließlich auf **Speichern** klicken. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.
9. Klicken Sie auf **Recovery**.
10. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

    Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
11. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer anzeigen lassen, ändern oder spezifizieren.

    Der ursprüngliche Benutzer wird automatisch vorausgewählt. Wenn dieser Benutzer nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer spezifizieren.
12. Bei **Pfad** können Sie den Zielordner im OneDrive des Zielbenutzers einsehen oder ändern. Standardmäßig ist der ursprüngliche Speicherort vorausgewählt.
13. Bestimmen Sie, ob Sie auch die Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
14. Klicken Sie auf **Recovery starten**.
15. Wählen Sie eine der folgenden Optionen zum Überschreiben:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**

16. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.2.4 SharePoint Online-Websites sichern

Welche Elemente können per Backup gesichert werden?

Sie können klassische SharePoint Website-Sammlungen, Gruppen-(Team)-Websites und Kommunikations-Websites sichern. Sie können außerdem einzelne Unterwebsites, Listen und Bibliotheken für ein Backup auszuwählen.

Folgende Elemente werden bei einem Backup *übersprungen*:

- Die Website-Einstellungen für **Aussehen und Verhalten** (mit Ausnahme von **Titel, Beschreibung und Logo**).
- Seitenkommentare und Seitenkommentar-Einstellungen (Kommentare **An**/**Aus**).
- Die Website-Einstellungen **Websitefeatures**.
- Webpartseiten und Webparts, die in Wiki-Seiten eingebettet sind (aufgrund von Beschränkungen der SharePoint Online API).
- OneNote-Dateien (aufgrund von Beschränkungen der SharePoint Online API).
- Externe Daten und verwaltete Metadatentypen von Spalten.
- Die Standard-Website-Sammlung 'domain-my.sharepoint.com'. Dies ist eine Sammlung, in der sich alle OneDrive-Dateien der Benutzer der Organisation/desUnternehmens befinden.
- Der Inhalt des Papierkorbs.

Einschränkungen

- Titel und Beschreibungen von Webseiten/Unterwebsites/Listen/Spalten werden während eines Backups abgeschnitten, wenn der Titel/Beschreibungsumfang größer als 10000 Byte ist.

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Website-Backup wiederhergestellt werden:

- Die komplette Website
- Unterwebsites
- Listen
- Listenelemente
- Dokumentbibliotheken
- Dokumente
- Listenelement-Anhänge
- Website-Seiten und Wiki-Seiten

Sie können eine Suchfunktion verwenden, um bestimmte Elemente zu finden.

Elemente können zur ursprünglichen oder einer nicht-ursprünglichen Website wiederhergestellt werden. Der Pfad zu einem wiederhergestellten Element ist derselbe wie der ursprüngliche Pfad. Wenn der Pfad nicht existiert, wird er automatisch erstellt.

Sie können wählen, ob die Elemente bei der Wiederherstellung ihre ursprünglichen Freigabeberechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen des übergeordneten Ojekts übernehmen sollen, in dem sie wiederhergestellt werden.

Folgende Elemente können nicht wiederhergestellt werden:

- Unterwebsites, die auf dem Template **Visio-Prozessrepository** beruhen.
- Listen der folgenden Typen: **Umfrageliste**, **Aufgabenliste**, **Bildbibliothek**, **Links**, **Kalender**, **Diskussionsrunde**, **Externe** und **Interne Tabelle**.
- Listen, für die mehrere Inhaltstypen aktiviert wurden.

15.2.4.1 SharePoint Online-Daten auswählen

Wählen Sie die Daten wie nachfolgend beschrieben aus – und spezifizieren Sie die anderen Einstellungen des Backup-Plans je nach Bedarf (S. 38).

So können Sie SharePoint Online-Daten auswählen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um alle klassichen SharePoint-Websites in der Organisation zu sichern (einschließlich solcher Websites, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Website-Sammlung**, wählen Sie **Alle Website-Sammlungen** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne klassische Websites sichern wollen, erweitern Sie den Knoten **Website-Sammlung**, wählen Sie **Alle Website-Sammlungen**, wählen Sie die Website aus, die Sie sichern wollen, und klicken Sie dann auf **Backup**.
   - Um alle Gruppen-Websites zu sichern (einschließlich der Websites, die erst in der Zukunft erstellt werden), erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Gruppen-Websites sichern wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie die Gruppen aus, deren Websites Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Backup-Plan-Fensterbereich:
   - Überprüfen Sie, dass das Element **SharePoint-Websites** bei **Backup-Quelle** ausgewählt ist.
   - Wählen Sie bei **Elemente für das Backup** eine der folgenden Möglichkeiten:
     - Übernehmen Sie die Voreinstellung **[Alle]** (alle Elemente der ausgewählten Websites).
     - Spezifizieren Sie die zu sichernden Unterwebsites, Listen und Bibliotheken, indem Sie deren Namen oder Pfade hinzufügen.

       Wenn Sie eine Unterwebsite oder eine Toplevel-Website-Liste/Bibliothek sichern wollen, spezifizieren Sie deren Anzeigenamen im folgenden Format: `/anzeigename/**`

       Wenn Sie eine Unterwebsite-Liste/Bibliothek sichern wollen, spezifizieren Sie deren Anzeigenamen im folgenden Format: `/unterwebsite anzeigename/liste anzeigename/**`

       Die Anzeigenamen der Unterwebsites, Listen und Bibliotheken werden auf der Seite **Website-Inhalte** einer SharePoint-Website oder -Unterwebsite angezeigt.
     - Spezifizieren Sie Unterwebsites für das Backup, indem Sie diese per 'Durchsuchen' auswählen.

       Der Link **Durchsuchen** ist nur verfügbar, wenn ein Backup-Plan für eine einzelne Website erstellt wird.

- [Optional] Klicken Sie bei **Elemente für das Backup** auf **Ausschlusskriterien anzeigen**, um zu spezifizieren, ob und welche Unterwebsites, Listen und Bibliotheken während des Backup-Prozesses übersprungen werden sollen.

  Elementausschlusskritieren überschreiben eine vorherige Elementauswahl, d.h., wenn Sie in beiden Feldern dieselbe Unterwebsite spezifizieren, wird diese Unterwebsite beim anschließenden Backup übersprungen.

15.2.4.2 SharePoint Online-Daten wiederherstellen

1. Klicken Sie auf **Microsoft Office 365**.
2. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie Daten aus einem Gruppen-Website wiederherstellen wollen, erweitern Sie den Knoten **Gruppen**, wählen Sie **Alle Gruppen**, wählen Sie diejenige Gruppe aus, deren Website die wiederherzustellenden Elemente ursprünglich enthalten hat, und klicken Sie dann auf **Recovery**.
   - Wenn Sie Daten aus einem klassischen Website wiederherstellen wollen, erweitern Sie den Knoten **Website-Sammlungen**, wählen Sie **Alle Website-Sammlungen**, wählen Sie diejenige Website aus, in der sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.
   - Wenn die Website zuvor gelöscht wurde, können Sie diese im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Gruppen und Websites auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die SharePoint-Websites enthalten, wählen Sie* ***SharePoint-Websites*** *bei* ***Nach Inhalt filtern****.*
5. Klicken Sie auf **SharePoint-Dateien wiederherstellen**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Datenelemente abzurufen.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen.

   Wenn das Backup unverschlüsselt ist, Sie die Suchfunktion verwendet und dann eine einzelne Datei in den Suchergebnissen ausgewählt haben, können Sie auf **Versionen anzeigen** klicken, um eine bestimmte Elementversion auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Wenn Sie ein Element herunterladen wollen, müssen Sie dieses auswählen, auf **Download** klicken, den Zielspeicherort für das Element bestimmen und schließlich auf **Speichern** klicken. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.
9. Klicken Sie auf **Recovery**.

10. Wenn dem Backup Service mehrere Office 365-Organisationen hinzugefügt wurden, klicken Sie auf **Office 365-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

    Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
11. Bei **Zu Website wiederherstellen** können Sie die gewünschte Ziel-Website anzeigen lassen, ändern oder spezifizieren.

    Standardmäßig ist die ursprüngliche Website vorausgewählt. Wenn diese Website nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie die Ziel-Website spezifizieren.
12. Bestimmen Sie, ob Sie auch die Freigabeberechtigungen der wiederhergestellten Elemente mit wiederherstellen wollen.
13. Klicken Sie auf **Recovery starten**.
14. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
15. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

15.2.5 Upgrade des Cloud Agenten

In diesem Abschnitt wird beschrieben, wie Sie ein Upgrade auf die aktuelle Version der Backup-Lösung für Microsoft Office 365 durchführen können. Diese Version unterstützt OneDrive- und SharePoint Online-Backups und bietet eine verbesserte Performance bei Backups und Wiederherstellungen.

Die Upgrade-Verfügbarkeit hängt davon ab, welches Datacenter verfügbar ist und welche Einstellungen Ihr Service-Provider vorgenommen hat. Wenn das Upgrade verfügbar ist, wird in der Backup-Konsole oben auf der Registerkarte **Microsoft Office 365 (v1)** eine Benachrichtigung angezeigt.

Der Upgrade-Prozess

Während des Upgrades werden die Benutzer Ihrer Office 365-Organisation der neuen Backup-Lösung hinzugefügt. Die Backup-Pläne werden migriert und auf die entsprechenden Benutzer angewendet.

Früher erstellte Backups werden von einem Speicherort in der Cloud zu einem anderen kopiert. Die kopierten Backups werden auf der Registerkarte **Backups** in einem separaten Bereich namens **Cloud-Applikationen-Backups** angezeigt, während die ursprünglichen Backups im Speicherort **Cloud Storage** verbleiben. Nach Abschluss des Upgrade-Prozesses werden die ursprünglichen Backups aus dem Speicherort **Cloud Storage** gelöscht.

Das Upgrade kann mehrere Stunden oder sogar Tage dauern – in Abhängigkeit von der Anzahl der Benutzer im Unternehmen, der Anzahl der Backups und der Zugriffsgeschwindigkeit auf Office 365. Während des Upgrades können aber weiterhin Wiederherstellungen aus früher erstellten Backups durchgeführt werden. Jedoch gehen alle Backups und Backup-Pläne, die während des Upgrades erstellt werden, verloren.

Für den unwahrscheinlichen Fall, dass es zu einem Upgrade-Fehler kommt, bleibt die Backup-Lösung voll funktionsfähig. Das Upgrade kann dann vom Fehlerzeitpunkt aus neu gestartet werden.

So können Sie den Upgrade-Prozess starten

1. Klicken Sie auf **Microsoft Office 365 (v1)**.
2. Klicken Sie in der Benachrichtigung im oberen Fensterbereich auf den Befehl **Upgrade**.
3. Bestätigen Sie, dass Sie den Upgrade-Prozess wirklich starten wollen.
4. Wählen Sie das von Ihrer Organisation/Firma verwendete Microsoft Datacenter aus.

   Die Software leitet Sie zur Microsoft Office 365-Anmeldeseite weiter.
5. Melden Sie sich mit den Anmeldedaten des globalen Office 365-Administrators an.

   Microsoft Office 365 zeigt eine Liste der Berechtigungen an, die erforderlich sind, um die Daten Ihres Unternehmens sichern und wiederherstellen zu können.
6. Bestätigen Sie, dass Sie dem Backup Service diese Berechtigungen gewähren wollen.

   Sie werden zur Backup-Konsole umgeleitet und der Upgrade-Prozess wird gestartet. Der Verlauf des Upgrades wird im Fensterbereich **Microsoft Office 365** –> **Aktivitäten** angezeigt.

16 G Suite-Daten sichern

Was bedeutet die Sicherung von G Suite?

- Cloud-zu-Cloud-basiertes Backup & Recovery von G Suite-Benutzerdaten (Gmail-Postfächer, Kalender, Kontakte, Google Drives) und G Suite Team Drives.
- Granulares Recovery von E-Mails, Dateien, Kontakten und anderen Datenelementen.
- Unterstützung für mehrere G Suite-Organisationen und organisationsübergreifende Wiederherstellungen.
- Optionale Beglaubigung (Notarization) von gesicherten Dateien mithilfe der Blockchain-Datenbank von Ethereum. Wenn die Beglaubigungsfunktion aktiviert ist, können Sie überprüfen und belegen, ob und dass Ihre gesicherten Dateien seit Erstellung des dazugehörigen Backups authentisch und unverändert geblieben sind.
- Optionale Volltextsuche. Wenn diese Funktion aktiviert wird, können Sie E-Mail-Nachrichten nach ihren Inhalten durchsuchen.
- Pro Unternehmen können bis zu 5000 Elemente (Postfächer, Google Drives und Team Drives) ohne Performanceverlust gesichert werden.

Erforderliche Benutzerrechte

Wenn Sie Ihre G Suite-Organisation dem Backup Service hinzufügen wollen, müssen Sie als Super Admin angemeldet sein.

Das Super Admin-Kennwort wird nirgendwo gespeichert und wird weder für Backups noch Wiederherstellungen verwendet. Wenn Sie dieses Kennwort in G Suite ändern, hat dies keinen Einfluss auf die Backup Service-Operationen.

Wenn der Super Admin, der die G Suite-Organisation hinzugefügt hat, aus G Suite gelöscht wird oder eine Admin-Rolle mit weniger Rechten erhält, werden die Backups mit einer Fehlermeldung wie 'Zugriff verweigert' fehlschlagen. In diesem Fall müssen Sie die im Abschnitt 'Eine G Suite-Organisation hinzufügen (S. 165)' erläuterte Prozedur wiederholen und gültige Super Admin-Anmeldedaten spezifizieren. Zur Vermeidung dieser Situation empfehlen wir, dass Sie einen dedizierten Super Admin-Benutzer für Backup- und Wiederherstellungszwecke anlegen.

Im Backup Service müssen Sie ein Firmenadministrator sein. Abteilungsadministratoren oder Benutzer können keine Backups oder Wiederherstellungen von G Suite durchführen.

Über die Backup-Planung

Da der Cloud Agent mehrere Kunden bedient, bestimmt der Agent die Startzeit für jeden Backup-Plan selbst, um eine gleichmäßige Auslastung über den Tag und die gleiche Service-Qualität für alle Kunden zu gewährleisten.

Jeder Backup-Plan wird täglich zur gleichen Tageszeit ausgeführt.

Einschränkungen

Eine Suche in verschlüsselten Backups wird nicht unterstützt.

16.1 Eine G Suite-Organisation hinzufügen

Eine G Suite-Organisation hinzufügen

1. Melden Sie sich als Firmenadministrator an der Backup-Konsole an.
2. Klicken Sie auf **Geräte** –> **Hinzufügen** –> **G Suite**.
3. Befolgen Sie die von der Software angezeigten Instruktionen:
   a. Klicken Sie auf **Marketplace öffnen**.
   b. Melden Sie sich mit den Anmeldedaten des Super Admins an.
   c. Klicken Sie auf **Domain installieren**.
   d. Bestätigen Sie die Domain-weite Installation.

      G Suite zeigt eine Liste der Berechtigungen an, die erforderlich sind, um die Daten Ihrer Organisation sichern und wiederherstellen zu können.
   e. Bestätigen Sie, dass Sie dem Backup Service diese Berechtigungen gewähren wollen.
   f. Schließen Sie die Installationsprozedur ab.
   g. Klicken Sie auf **Starten**.

Sie werden zurück zur Backup-Konsole geleitet. Die Datenelemente Ihrer Organisation werden in der Backup-Konsole auf der Seite **G Suite** angezeigt.

Tipps zur weiteren Nutzung

- Der Cloud Agent führt die Synchronisierung mit G Suite alle 24 Stunden durch – von dem Zeitpunkt an, ab dem das Unternehmen dem Backup Service hinzugefügt wurde. Wenn Sie einen Benutzer oder ein Team Drive hinzufügen oder entfernen, wird diese Änderung nicht sofort in der Backup-Konsole angezeigt. Wenn Sie die Synchronisierung des Cloud Agenten mit G Suite erzwingen wollen, wählen Sie die entsprechende Organisation auf der **G Suite**-Seite aus und klicken Sie dann auf **Aktualisieren**.
- Wenn Sie den Gruppen **Alle Benutzer** oder **Alle Team Drives** einen Backup-Plan zugewiesen haben, werden die neu hinzugefügten Elemente erst dann in das Backup aufgenommen, wenn die Synchronisierung durchgeführt wurde.
- Gemäß den Google-Richtlinien bleibt ein Benutzer oder ein Team Drive, nachdem dieser/dieses aus der G Suite-Benutzeroberfläche entfernt wurde, noch für einige weitere Tage per API verfügbar. Während dieser Tage wird das entfernte Element in der Backup-Konsole als inaktiv (ausgegraut) dargestellt und nicht per Backup gesichert. Wenn das entfernte Element auch nicht mehr per API verfügbar ist, verschwinden es ganz aus der Backup-Konsole. Dessen Backups können (sofern vorhanden) unter **Backups** –> **Cloud-Applikationen-Backups** gefunden werden.

16.2 Gmail-Daten sichern

Welche Elemente können per Backup gesichert werden?

Sie können die Postfächer von Gmail-Benutzern per Backup sichern. Ein Postfach-Backup beinhaltet auch die Daten von Kalendern und Kontakten. Optional können Sie auch die freigegebenen Kalender sichern.

Folgende Elemente werden bei einem Backup *übersprungen*:

- Die Kalender **Geburtstage**, **Erinnerungen** und **Tasks**.
- Ordner, die an Kalendereereignisse angehängt sind
- Der Ordner **Verzeichnis** in den Kontakten.

Folgende Kalenderelemente werden aufgrund von Beschränkungen der Google Calender API *übersprungen*:

- Terminvereinbarungen (Appointment Slots)
- Das Konferenzfeld eines Ereignisses
- Die Kalendereinstellung **Ganztätige Ereignisbenachrichtigungen**
- Die Kalendereinstellung **Automatisch Einladungen hinzufügen** (in Kalendern für Räume oder Gemeinschafsbereiche)

Folgende Kontaktelemente werden aufgrund von Beschränkungen der Google People API *übersprungen*:

- Der Ordner **Weitere Kontakte**
- Die externen Profile eines Kontaktes (**Verzeichnis-Profil**, **Google-Profil**)
- Das Kontaktfeld **Speichern unter**

Welche Elemente können wiederhergestellt werden?

Folgende Elemente können aus einem Postfach-Backup wiederhergestellt werden:

- Postfächer
- E-Mail-Ordner (nach der Terminologie von Google 'Labels' genannt. **Labels** werden in der Backup-Software als Ordner dargestellt, um die Konsistenz mit anderen Datendarstellungen zu gewährleisten.)
- E-Mail-Nachrichten
- Kalendereereignisse
- Kontakte

Sie können die Suchfunktion verwenden, um bestimmte Elemente in einem Backup zu finden – außer das Backup ist verschlüsselt. Eine Suche in verschlüsselten Backups wird nicht unterstützt.

Sie können bei der Wiederherstellung von Postfächern und Postfachelementen auswählen, ob die Elemente am Zielort überschrieben werden sollen (oder nicht).

Einschränkungen

- Kontaktfotos können nicht wiederhergestellt werden
- Das Kalenderelement **Außer Haus** wird aufgrund von Beschränkungen der Google Calender API als reguläres Kalendereereignis wiederhergestellt.

16.2.1 Postfächer auswählen

Wählen Sie die Postfächer wie nachfolgend beschrieben aus – und spezifizieren Sie dann nach Bedarf (S. 38) die anderen Einstellungen des Backup-Plans.

So können Sie Gmail-Postfächer auswählen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Postfächer aller Benutzer zu sichern (einschließlich solcher Postfächer, die erst in der Zukunft erstellt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie einzelne Benutzerpostfächer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Postfächer Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Backup-Plan-Fensterbereich:
   - Überprüfen Sie, dass das Element **Gmail** bei **Backup-Quelle** ausgewählt ist.
   - Wenn Sie Kalender sichern möchten, die für die ausgewählten Benutzer freigegeben wurden, aktivieren Sie den Schalter **Freigegebene Kalender einbeziehen**.
   - Entscheiden Sie, ob Sie die gesicherten E-Mail-Nachrichten per Volltextsuche (S. 167) durchsuchen wollen. Sie finden diese Option, wenn Sie zuerst auf das Zahnradsymbol klicken – und dann auf **Backup-Optionen** –> **Volltextsuche**.

16.2.1.1 Volltextsuche

Diese Option bestimmt, ob die Inhalte von E-Mail-Nachrichten vom Cloud-Agenten indiziert werden.

Die Voreinstellung ist: **Aktiviert**.

Wenn diese Option aktiviert ist, werden die Nachrichteninhalte indiziert und Sie können Nachrichten nach ihrem Inhalten durchsuchen. Ansonsten können Sie die Nachrichten nur nach Betreff, Absender, Empfänger oder Datum durchsuchen.

***Hinweis**: Eine Suche in verschlüsselten Backups wird nicht unterstützt.*

Der Indizierungsprozess hat keinen Einfluss auf die Backup-Performance, da diese Prozesse jeweils von unterschiedlichen Software-Komponenten durchgeführt werden. Die Indizierung des ersten (vollständigen) Backups kann einige Zeit benötigen, daher kann es zu einer Verzögerung zwischen der Backup-Fertigstellung und der anschließenden Anzeige der Inhalt in den Suchergebnissen kommen.

Der Index belegt 10-30 Prozent des Speicherplatzes, der für die Postfach-Backups belegt wird. Wenn Sie den exakten Wert erfahren wollen, klicken Sie auf **Backups** –> **Cloud-Applikationen-Backups** und sehen Sie sich die Spalte **Indexgröße** an. Wenn Sie Speicherplatz sparen wollen, können Sie die Volltextsuche deaktivieren. Der Wert in der Spalte **Indexgröße** wird dann nach dem nächsten Backup auf eine wenige Megabyte reduziert. Diese minimale Menge an Metadaten ist notwendig, um nach Betreff, Absender, Empfänger oder Datum suchen zu können.

Wenn Sie die Volltextsuche wieder aktivieren, indiziert die Software alle Backups, die zuvor durch den Backup-Plan erstellt wurden. Dies wird ebenfalls einige Zeit benötigen.

16.2.2 Postfächer und Postfachelemente wiederherstellen

16.2.2.1 Postfächer wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen Postfach Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die Postfächer enthalten, wählen Sie **Gmail** bei **Nach Inhalt filtern**.*
5. Klicken Sie auf **Recovery** –> **Komplettes Postfach**.
6. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt werden, klicken Sie auf **G Suite-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
7. Bei **Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

   Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
8. Klicken Sie auf **Recovery starten**.
9. Wählen Sie eine dieser Überschreiben-Optionen:
   - **Vorhandene Elemente überschreiben**
   - **Vorhandene Elemente nicht überschreiben**
10. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

16.2.2.2 Postfachelemente wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie denjenigen Benutzer aus, in dessen Postfach sich die wiederherzustellenden Elemente ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

Sie können Benutzer und Gruppen auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die Postfächer enthalten, wählen Sie* ***Gmail*** *bei* ***Nach Inhalt filtern****.*

5. Klicken Sie auf **Recovery** –> **E-Mail-Nachrichten**.
6. Wählen Sie den gewünschten Ordner aus. Wenn das Backup unverschlüsselt ist, können Sie die Suchfunktion verwenden, um eine Liste der gewünschten Datenelemente abzurufen.

   Folgende Suchoptionen sind verfügbar. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

   - Für E-Mail-Nachrichten: Suche per Betreff, Absender, Empfänger, Datum, Name eines Anhangs und Nachrichteninhalt. Die letzten beiden Optionen sind nur dann verfügbar, wenn die Option **Volltextsuche** während des Backups aktiviert war. Die Sprache eines zu durchsuchenden Nachrichtenfragments kann als weiterer Parameter angegeben werden.
   - Für Ereignisse: Suche nach Titel und Datum.
   - Für Kontakte: Suche nach Namen, E-Mail-Adresse und Telefonnummer.
7. Wählen Sie die Elemente aus, die Sie wiederherstellen wollen. Wenn Sie Ordner auswählen wollen, klicken Sie auf das Symbol 'Ordner wiederherstellen'. 

   Zusätzlich haben Sie auch folgende Möglichkeiten:

   - Klicken Sie bei der Auswahl eines Elements auf **Inhalt anzeigen**, um die Inhalte (inklusive Anhänge) einsehen zu können. Klicken Sie auf den Namen einer angehängten Datei, um diese herunterzuladen.
   - Nur bei einem unverschlüsselten Backup, wenn Sie die Suchfunktion verwendet und ein einzelnes Element in den Suchergebnissen ausgewählt haben: klicken Sie auf **Versionen anzeigen**, um die Version des Elements auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Klicken Sie auf **Recovery**.
9. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
10. Bei **Zu Postfach wiederherstellen** können Sie das gewünschte Zielpostfach anzeigen lassen, ändern oder spezifizieren.

    Das ursprüngliche Postfach wird automatisch vorausgewählt. Wenn dieses Postfach nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie das Zielpostfach spezifizieren.
11. Bei **Pfad** können Sie den Zielordner im Zielpostfach einsehen oder ändern. Standardmäßig ist der ursprüngliche Ordner vorausgewählt.
12. Klicken Sie auf **Recovery starten**.
13. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Elemente überschreiben**
    - **Vorhandene Elemente nicht überschreiben**
14. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

16.3 Google Drive-Dateien sichern

Welche Elemente können per Backup gesichert werden?

Sie können ein komplettes Google Drive sichern – oder auch nur einzelne Dateien und Ordner. Optional können Sie auch Dateien sichern, die für Google Drive-Benutzer freigegeben wurden.

Dateien werden inklusive ihrer Freigabeberechtigungen gesichert.

Folgende Elemente werden bei einem Backup *übersprungen*:

- Eine freigegebene Datei – wenn der Benutzer Zugriff als Kommentator oder Betrachter auf die Datei hat und der Dateibesitzer die Optionen zum Herunterladen, Drucken und Kopieren für Kommentatoren und Betrachter deaktiviert hat.
- Der Ordner **Computer** (vom Backup & Sync-Client erstellt)

Einschränkungen

- Von den Google-spezifischen Dateiformaten werden nur Google Docs, Google Tabellen, Google Präsentationen und Google Zeichnungen gesichert.

Welche Elemente können wiederhergestellt werden?

Sie können ein komplettes Google Drive wiederherstellen oder beliebige einzelne Dateien/Ordner, die gesichert wurden.

Sie können die Suchfunktion verwenden, um bestimmte Elemente in einem Backup zu finden – außer das Backup ist verschlüsselt. Eine Suche in verschlüsselten Backups wird nicht unterstützt.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Freigabeberechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

Einschränkungen

- Kommentare in Dateien werden nicht wiederhergestellt.
- Freigabelinks für Dateien und Ordner werden nicht wiederhergestellt.
- Die **Eigentümer-Einstellungen** für freigegebene Dateien (**Bearbeiter dürfen weder die Zugriffsberechtigung ändern noch neue Personen hinzufügen** und **Optionen zum Herunterladen, Drucken und Kopieren für Kommentatoren und Betrachter deaktivieren**) können während einer Wiederherstellung nicht geändert werden.
- Die Eigentümerschaft für eine freigegebene Datei kann während einer Wiederherstellung nicht geändert werden, wenn die Option **Bearbeiter dürfen weder die Zugriffsberechtigung ändern noch neue Personen hinzufügen** für diesen Ordner aktiviert ist. Diese Einstellung verhindert, dass die Google Drive API die Ordnerberechtigungen auflistet. Die Eigentümerschaft von Dateien in dem Ordner wird korrekt wiederhergestellt.

16.3.1 Google Drive-Dateien auswählen

Wählen Sie die Dateien wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Backup-Plans nach Bedarf (S. 38).

So können Sie Google Drive-Dateien auswählen

1. Klicken Sie auf **G Suite**.

2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Dateien aller Benutzer zu sichern (einschließlich solcher Benutzer, die erst in der Zukunft angelegt werden), erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie die Dateien einzelner Benutzer sichern wollen, erweitern Sie den Knoten **Benutzer**, wählen Sie **Alle Benutzer**, wählen Sie die Benutzer aus, deren Dateien Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Backup-Plan-Fensterbereich:
   - Überprüfen Sie, dass das Element **Google Drive** bei **Backup-Quelle** ausgewählt ist.
   - Wählen Sie bei **Elemente für das Backup** eine der folgenden Möglichkeiten:
     - Übernehmen Sie die Voreinstellung **[Alle]** (alle Dateien).
     - Spezifizieren Sie die zu sichernden Dateien und Ordner an, indem Sie deren Namen oder Pfade hinzufügen.

       Sie können Platzhalterzeichen (*, ** und ?) verwenden. Ausführlichere Informationen über die Verwendung von Pfaden und Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.
     - Spezifizieren Sie Dateien und Ordner für das Backup, indem Sie diese per 'Durchsuchen' auswählen.

       Der Link **Durchsuchen** ist nur verfügbar, wenn ein Backup-Plan für einen einzelnen Benutzer erstellt wird.
   - [Optional] Klicken Sie bei **Elemente für das Backup** auf **Ausschlusskriterien anzeigen**, um zu spezifizieren, ob und welche Dateien und Ordner während des Backup-Prozesses übersprungen werden sollen.

     Dateiausschlusskritieren überschreiben eine vorherige Dateiauswahl, d.h., wenn Sie in beiden Feldern dieselbe Datei spezifizieren, wird diese Datei beim anschließenden Backup übersprungen.
   - Wenn Sie die Dateien sichern möchten, die für die ausgewählten Benutzer freigegeben wurden, aktivieren Sie den Schalter **Freigegebene Dateien einbeziehen**.
   - Wenn Sie für alle zu sichernden Dateien die Beglaubigungsfunktion aktivieren wollen, aktivieren Sie den Schalter **Beglaubigung (Notarization)**. Weitere Informationen zu diesem Thema finden Sie im Abschnitt 'Beglaubigung (Notarization) (S. 177)'.

16.3.2 Google Drive und Google Drive-Dateien wiederherstellen

16.3.2.1 Ein komplettes Google Drive wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen Google Drive Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

Sie können Benutzer auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.

4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die Google Drive-Dateien enthalten, wählen Sie* ***Google Drive*** *bei* ***Nach Inhalt filtern****.*

5. Klicken Sie auf **Recovery** –> **Komplettes Laufwerk**.
6. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
7. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer oder das Ziel-Team Drive anzeigen lassen, ändern oder spezifizieren.

   Der ursprüngliche Benutzer wird automatisch vorausgewählt. Wenn dieser Benutzer nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer oder das Ziel-Team Drive spezifizieren.

   Wenn das Backup freigegebene Dateien enthält, werden die Dateien im Stammverzeichnis des Ziellaufwerks (Ziel-Team Drive) wiederhergestellt.
8. Bestimmen Sie, ob Sie auch die Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine dieser Überschreiben-Optionen:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
11. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

16.3.2.2 Google Drive-Dateien wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Benutzer**, wählen Sie die Option **Alle Benutzer**, wählen Sie den Benutzer, dessen Google Drive-Dateien Sie wiederherstellen wollen, und klicken Sie dann auf **Recovery**.

   Wenn der Benutzer zuvor gelöscht wurde, können Sie diesen im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können Benutzer auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.

   Tipp: *Wenn Sie nur Recovery-Punkte sehen wollen, die Google Drive-Dateien enthalten, wählen Sie* ***Google Drive*** *bei* ***Nach Inhalt filtern****.*

5. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
7. Wählen Sie die Dateien, die Sie wiederherstellen wollen.

   Wenn das Backup unverschlüsselt ist und Sie eine einzelne Datei ausgewählt haben, können Sie auf **Versionen anzeigen** klicken, um eine bestimmte Dateiversion auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Wenn Sie eine Datei herunterladen wollen, müssen Sie diese auswählen, auf **Download** klicken, den Zielspeicherort für die Datei bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
9. Klicken Sie auf **Recovery**.
10. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

    Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
11. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer oder das Ziel-Team Drive anzeigen lassen, ändern oder spezifizieren.

    Der ursprüngliche Benutzer wird automatisch vorausgewählt. Wenn dieser Benutzer nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer oder das Ziel-Team Drive spezifizieren.
12. Bei **Pfad** können Sie den Zielordner im Google Drive des Zielbenutzers oder im Ziel-Team Drive einsehen oder ändern. Standardmäßig ist der ursprüngliche Speicherort vorausgewählt.
13. Bestimmen Sie, ob Sie auch die Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
14. Klicken Sie auf **Recovery starten**.
15. Wählen Sie eine der folgenden Optionen zum Überschreiben:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
16. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

16.4 Team Drive-Dateien sichern

Welche Elemente können per Backup gesichert werden?

Sie können ein komplettes Google Drive sichern – oder auch nur einzelne Dateien und Ordner.

Dateien werden inklusive ihrer Freigabeberechtigungen gesichert.

Einschränkungen

- Ein Team Drive ohne Mitglieder kann aufgrund von Beschränkungen der Google Drive API nicht gesichert werden.

- Von den Google-spezifischen Dateiformaten werden nur Google Docs, Google Tabellen, Google Präsentationen und Google Zeichnungen gesichert.

Welche Elemente können wiederhergestellt werden?

Sie können ein komplettes Team Drive wiederherstellen oder beliebige einzelne Dateien/Ordner, die gesichert wurden.

Sie können die Suchfunktion verwenden, um bestimmte Elemente in einem Backup zu finden – außer das Backup ist verschlüsselt. Eine Suche in verschlüsselten Backups wird nicht unterstützt.

Sie können wählen, ob die Dateien bei der Wiederherstellung ihre ursprünglichen Freigabeberechtigungen aus dem Backup beibehalten sollen – oder ob sie die Berechtigungen desjenigen Ordner übernehmen sollen, in dem sie wiederhergestellt werden.

Folgende Elemente werden nicht wiederhergestellt:

- Freigabeberechtigungen für eine Datei, die für einen Benutzer außerhalb der Organisation freigegeben wurde, werden nicht wiederhergestellt, wenn im als Ziel verwendeten Team Drive der Dateizugriff für Personen außerhalb der Organisation deaktiviert ist.
- Freigabeberechtigungen für eine Datei, die für einen Benutzer freigegeben wurde, der kein Mitglied des als Ziel verwendeten Team Drive ist, werden nicht wiederhergestellt, wenn die Option **Freigabe für Nichtmitglieder** im als Ziel verwendeten Team Drive deaktiviert ist.

Einschränkungen

- Kommentare in Dateien werden nicht wiederhergestellt.
- Freigabelinks für Dateien und Ordner werden nicht wiederhergestellt.

16.4.1 Team Drive-Dateien auswählen

Wählen Sie die Dateien wie nachfolgend beschrieben aus – und spezifizieren Sie dann die anderen Einstellungen des Backup-Plans nach Bedarf (S. 38).

So können Sie Team Drive-Dateien auswählen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Benutzerdaten Sie sichern wollen. Ansonsten können Sie diesen Schritt überspringen.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Um die Dateien aller Team Drives zu sichern (einschließlich solcher Team Drives, die erst in der Zukunft erstellt werden), erweitern Sie den Knoten **Team Drives**, wählen Sie **Alle Team Drives** und klicken Sie dann auf **Gruppen-Backup**.
   - Wenn Sie die Dateien einzelner Team Drives sichern wollen, erweitern Sie den Knoten **Team Drives**, wählen Sie **Alle Team Drives**, wählen Sie diejenigen Team Drives aus, die Sie sichern wollen, und klicken Sie dann auf **Backup**.
4. Im Backup-Plan-Fensterbereich:
   - Wählen Sie bei **Elemente für das Backup** eine der folgenden Möglichkeiten:
     - Übernehmen Sie die Voreinstellung **[Alle]** (alle Dateien).
     - Spezifizieren Sie die zu sichernden Dateien und Ordner an, indem Sie deren Namen oder Pfade hinzufügen.

Sie können Platzhalterzeichen (*, ** und ?) verwenden. Ausführlichere Informationen über die Verwendung von Pfaden und Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.

- Spezifizieren Sie Dateien und Ordner für das Backup, indem Sie diese per 'Durchsuchen' auswählen.

  Der Link **Durchsuchen** ist nur verfügbar, wenn ein Backup-Plan für ein einzelnes Team Drive erstellt wird.

- [Optional] Klicken Sie bei **Elemente für das Backup** auf **Ausschlusskriterien anzeigen**, um zu spezifizieren, ob und welche Dateien und Ordner während des Backup-Prozesses übersprungen werden sollen.

  Dateiausschlusskritieren überschreiben eine vorherige Dateiauswahl, d.h., wenn Sie in beiden Feldern dieselbe Datei spezifizieren, wird diese Datei beim anschließenden Backup übersprungen.

- Wenn Sie für alle zu sichernden Dateien die Beglaubigungsfunktion aktivieren wollen, aktivieren Sie den Schalter **Beglaubigung (Notarization)**. Weitere Informationen zu diesem Thema finden Sie im Abschnitt 'Beglaubigung (Notarization) (S. 177)'.

16.4.2 Team Drive und Team Drive-Dateien wiederherstellen

16.4.2.1 Ein komplettes Team Drive wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Team Drives**, wählen Sie die Option **Alle Team Drives**, wählen Sie das wiederherzustellende Team Drive aus und klicken Sie dann auf **Recovery**.

   Wenn das Team Drive zuvor gelöscht wurde, können Sie diese im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können die Team Drives nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Recovery** –> **Komplettes Team Drive**.
6. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

   Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
7. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer oder das Ziel-Team Drive anzeigen lassen, ändern oder spezifizieren. Wenn Sie einen Benutzer angeben, werden die Daten zu dem Google Drive dieses Benutzers wiederhergestellt.

   Standardmäßig ist das ursprüngliche Team Drive vorausgewählt. Wenn dieses Team Drive nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer oder das Ziel-Team Drive spezifizieren.
8. Bestimmen Sie, ob Sie auch die Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
9. Klicken Sie auf **Recovery starten**.
10. Wählen Sie eine dieser Überschreiben-Optionen:

- **Vorhandene Dateien überschreiben**
- **Vorhandene Datei überschreiben, wenn diese älter ist**
- **Vorhandene Dateien nicht überschreiben**

11. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

16.4.2.2 Team Drive-Dateien wiederherstellen

1. Klicken Sie auf **G Suite**.
2. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, wählen Sie diejenige Organisation aus, deren Backup-Daten Sie wiederherstellen möchten. Ansonsten können Sie diesen Schritt überspringen.
3. Erweitern Sie den Knoten **Team Drives**, wählen Sie die Option **Alle Team Drives**, wählen Sie dasjenige Team Drive aus, in dem sich die wiederherzustellenden Dateien ursprünglich befunden haben, und klicken Sie dann auf **Recovery**.

   Wenn das Team Drive zuvor gelöscht wurde, können Sie diese im Bereich **Cloud-Applikationen-Backups** der Registerkarte 'Backups' (S. 125) auswählen und dann auf **Backups anzeigen** klicken.

   Sie können die Team Drives nach einem Namen durchsuchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
4. Wählen Sie einen Recovery-Punkt.
5. Klicken Sie auf **Wiederherstellen** –> **Dateien/Ordner**.
6. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Ausführlichere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.

   Die Suchfunktion ist nicht verfügbar, wenn das Backup verschlüsselt ist.
7. Wählen Sie die Dateien, die Sie wiederherstellen wollen.

   Wenn das Backup unverschlüsselt ist und Sie eine einzelne Datei ausgewählt haben, können Sie auf **Versionen anzeigen** klicken, um eine bestimmte Dateiversion auszuwählen, die Sie wiederherstellen wollen. Sie können jede Backup-Version auswählen, auch wenn diese vor oder nach dem eigentlichen, zuvor ausgewählten Recovery-Punkt liegt.
8. Wenn Sie eine Datei herunterladen wollen, müssen Sie diese auswählen, auf **Download** klicken, den Zielspeicherort für die Datei bestimmen und schließlich auf **Speichern** klicken. Ansonsten können Sie diesen Schritt überspringen.
9. Klicken Sie auf **Recovery**.
10. Wenn dem Backup Service mehrere G Suite-Organisationen hinzugefügt wurden, klicken Sie auf **G Suite-Organisation**, um die Zielorganisation einsehen, ändern oder spezifizieren zu können.

    Die ursprüngliche Organisation wird automatisch vorausgewählt. Wenn diese Organisation nicht mehr im Backup Service registriert ist, müssen Sie die Zielorganisation spezifizieren.
11. Bei **Zu Laufwerk wiederherstellen** können Sie den gewünschten Zielbenutzer oder das Ziel-Team Drive anzeigen lassen, ändern oder spezifizieren. Wenn Sie einen Benutzer angeben, werden die Daten zu dem Google Drive dieses Benutzers wiederhergestellt.

    Standardmäßig ist das ursprüngliche Team Drive vorausgewählt. Wenn dieses Team Drive nicht mehr existiert oder Sie eine andere als die ursprüngliche Organisation als Ziel ausgewählt haben, müssen Sie den Zielbenutzer oder das Ziel-Team Drive spezifizieren.

12. Bei **Pfad** können Sie den Zielordner im Google Drive des Zielbenutzers oder im Ziel-Team Drive einsehen oder ändern. Standardmäßig ist der ursprüngliche Speicherort vorausgewählt.
13. Bestimmen Sie, ob Sie auch die Freigabeberechtigungen der Dateien mit wiederherstellen wollen.
14. Klicken Sie auf **Recovery starten**.
15. Wählen Sie eine der folgenden Optionen zum Überschreiben:
    - **Vorhandene Dateien überschreiben**
    - **Vorhandene Datei überschreiben, wenn diese älter ist**
    - **Vorhandene Dateien nicht überschreiben**
16. Klicken Sie auf **Fertig stellen**, um Ihre Entscheidung zu bestätigen.

16.5 Beglaubigung (Notarization)

Mit der Beglaubigungsfunktion können Sie überprüfen und belegen, ob und dass Ihre gesicherten Dateien seit dem Backup authentisch und unverändert geblieben sind Wir empfehlen die Nutzung dieser Funktion, wenn Sie wichtige Dateien (wie rechtlich relevante Dokumente) sichern, deren Authentizität Sie später einmal überprüfen wollen/müssen.

Die Beglaubigungsfunktion ist nur für Backups von Google Drive-Dateien und G Suite Team Drive-Dateien verfügbar.

So können Sie die Beglaubigungsfunktion verwenden

Wenn Sie die Beglaubigungsfunktion für alle zum Backup ausgewählten Dateien aktivieren wollen, müssen Sie beim Erstellen des entsprechenden Backup-Plans den Schalter **Beglaubigung (Notarization)** einschalten.

Wenn Sie eine Wiederherstellung konfigurieren, werden die beglaubigten Dateien durch ein spezielles Symbol gekennzeichnet. Das bedeutet, dass Sie die Authentizität dieser Dateien überprüfen können.

Und so funktioniert es

Der Agent berechnet während eines Backups die Hash-Werte der zu sichernden Dateien, baut einen Hash-Baum auf (basierend auf der Ordnerstruktur), speichert diesen Hash-Baum mit im Backup und sendet dann das Wurzelverzeichnis (root) des Hash-Baums an den Notary Service. Der Notary Service speichert das Wurzelverzeichnis des Hash-Baums in der Blockchain-Datenbank von Ethereum. Damit wird sichergestellt, dass dieser Wert nicht mehr geändert werden kann.

Wenn die Authentizität einer Datei überprüft werden soll, berechnet der Agent den Hash-Wert der Datei und vergleicht diesen dann mit dem Hash-Wert, der im Hash-Baum innerhalb des Backups gespeichert ist. Sollten diese Hash-Werte nicht übereinstimmen, wird die Datei als 'nicht authentisch' eingestuft. Im anderen Fall ist die Authentizität der Datei durch den Hash-Baum garantiert.

Um zu verifizieren, dass der Hash-Baum selbst nicht kompromittiert wurde, sendet der Agent den Wert des Hash-Baum-Wurzelverzeichnisses an den Notary Service. Der Notary Service vergleicht diesen Wert mit dem, der in der Blockchain-Datenbank gespeichert ist. Wenn die Hash-Werte übereinstimmen, ist die ausgewählte Datei garantiert authentisch. Falls nicht, zeigt die Software über eine Nachricht an, dass die Datei nicht authentisch ist.

16.5.1 Die Authentizität von Dateien mit dem Notary Service überprüfen

Falls die Beglaubigungsfunktion (Notarization) während eines Backups aktiviert wurde, können Sie später bei Bedarf die Authentizität einer gesicherten Datei überprüfen.

So können Sie die Authentizität von Dateien überprüfen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn Sie die Authentizität einer Google Drive-Datei überprüfen wollen, müssen Sie die Datei wie in Schritt 1-7 des Abschnitts 'Google Drive-Dateien wiederherstellen (S. 172)' beschrieben auswählen.
   - Wenn Sie die Authentizität einer G Suite Team Drive-Datei überprüfen wollen, müssen Sie die Datei wie in Schritt 1-7 des Abschnitts 'Team Drive-Dateien wiederherstellen (S. 176)' beschrieben auswählen.
2. Überprüfen Sie, dass die ausgewählte Datei mit dem folgenden Symbol gekennzeichet ist:  . Das bedeutet, dass die Datei 'beglaubigt' (notarized) ist.
3. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Klicken Sie auf **Verifizieren**.

     Die Software überprüft die Authentizität der Datei und zeigt das Ergebnis an.
   - Klicken Sie auf **Zertifikat abrufen**.

     Ein Zertifikat, das die Dateibeglaubigung bestätigt, wird in einem Webbrowser-Fenster geöffnet. In dem Fenster werden außerdem Anweisungen angezeigt, wie Sie die Dateiauthentizität manuell überprüfen können.

17 Active Protection

Active Protection kann ein System vor Ransomware und Krypto-Mining-Malware schützen. Ransomware verschlüsselt Dateien und verlangt ein Lösegeld für die Bereitstellung des Codierungsschlüssels. Krypto-Mining-Malware führt mathematische Berechnungen im Hintergrund durch, um digitale Krypto-Währungen zu 'schürfen', und stiehlt auf diese Weise Rechenleistung und Netzwerkressourcen vom betroffenen System.

Active Protection ist derzeit nur für Maschinen verfügbar, die unter Windows (Version 7 und höher) oder Windows Server (Version 2008 R2 und höher) laufen. Auf der zu schützenden Maschine muss der Agent für Windows laufen.

Active Protection ist für Agenten ab Version 12.0.4290 verfügbar. Die Aktualisierung von Agenten wird im Abschnitt 'Update der Agenten (S. 33)' erläutert.

Und so funktioniert es

Active Protection überwacht die auf der geschützten Maschine laufenden Prozesse in Echtzeit. Wenn ein fremder Prozess versucht, Dateien auf der Maschine zu verschlüsseln oder eine digitale Krypto-Währung zu berechnen („schürfen“), generiert Active Protection eine Alarmmeldung und führt bestimmte, weitere Aktionen aus, sofern diese zuvor über eine entsprechende Konfiguration spezifiziert wurden.

Zusätzlich verhindert die Selbstschutzfunktion (Self-Protection), dass die Prozesse, Registry-Einträge, ausführbaren Dateien und Konfigurationsdateien der Backup-Software selbst sowie vorhandene Backups, die in lokalen Ordnern gespeichert sind, verändert werden können.

Active Protection verwendet eine verhaltensbasierte Heuristik, um schädliche Prozesse zu erkennen. Dazu vergleicht Active Protection die von einem Prozess ausgeführten Aktionsketten (z.B. Ereignisse im Dateisystem) mit Aktionsketten, die in einer Referenzdatenbank mit bekannten schädlichen Verhaltensmustern gespeichert sind. Mit diesem Ansatz kann Active Protection auch neue (bisher unbekannte) Malware anhand typischer Verhaltensmuster als Schadsoftware erkennen.

Active Protection-Einstellungen

Um durch die heuristische Analyse belegte Ressourcen zu minimieren und sogenannte Falsch-Positiv-Erkennungen zu vermeiden, können Sie folgende Einstellungen festlegen, wenn ein vertauenswürdiges Programm als Ransomware eingestuft wird:

- Vertrauenswürdige Prozesse, die niemals als Ransomware eingestuft werden. Prozesse, die von Microsoft signiert wurden, werden immer als vertrauenswürdig eingestuft.
- Schädliche Prozesse, die immer als Ransomware eingestuft werden. Solange Active Protection auf der Maschine aktiviert ist, können diese Prozesse nicht gestartet werden.
- Ordner, die nicht auf Dateiänderungen überwacht werden.

Spezifizieren Sie den vollständigen Pfad zur ausführbaren Datei des Prozesses (mit dem Laufwerksbuchstaben beginnend). Beispiel: **`C:\Windows\Temp\er76s7sdkh.exe`**.

Sie können die Platzhalterzeichen (* und ?) verwenden, um Ordner zu spezifizieren. Der Asterisk (*) ersetzt null bis mehrere Zeichen. Das Fragezeichen (?) steht für exakt ein Zeichen. Umgebungsvariablen (wie etwa %AppData%) können nicht verwendet werden.

Active Protection-Plan

Alle Einstellungen für Active Protection sind im Active Protection-Plan enthalten. Dieser Plan kann auf mehrere Maschinen angewendet werden.

In einer Organisation kann es nur einen Active Protection-Plan geben (Firmen-Gruppe). Nur Firmen-Administratoren und Administratoren der höheren Ebene dürfen den Plan anwenden, bearbeiten oder widerrufen.

Den Active Protection-Plan anwenden

1. Bestimmen Sie die Maschinen, für die Active Protection aktiviert werden soll.
2. Klicken Sie auf **Active Protection**.
3. [Optional] Klicken Sie auf **Bearbeiten**, um folgende Einstellungen anzupassen:
   - Wählen Sie bei **Aktion bei Erkennung** diejenige Aktion aus, die die Software durchführen soll, wenn eine Ransomware-Aktivität erkannt wurde. Klicken Sie anschließend auf **Fertig**. Sie können eine der folgenden Optionen wählen:
     - **Nur benachrichtigen**

       Die Software erstellt eine Alarmmeldung über den Prozess.
     - **Den Prozess stoppen** (Standard)

       Die Software erstellt eine Alarmmeldung und hält den Prozess an.
     - **Aus Cache wiederherstellen**

       Die Software erstellt eine Alarmmeldung, stoppt den Prozess und setzt die erfolgten Dateiänderungen mithilfe des Service-Caches zurück.

- Spezifizieren Sie bei **Schädliche Prozesse** diejenigen Prozesse, die immer als Ransomware eingestuft werden. Klicken Sie anschließend auf **Fertig**.
- Spezifizieren Sie bei **Vertrauenswürdige Prozesse** diejenigen Prozesse, die niemals als Ransomware eingestuft werden. Klicken Sie anschließend auf **Fertig**. Prozesse, die von Microsoft signiert wurden, werden immer als vertrauenswürdig eingestuft.
- Spezifizieren Sie bei **Ausgeschlossene Ordner** eine Liste derjenigen Ordner, die nicht auf Änderungen an Dateien überwacht werden. Klicken Sie anschließend auf **Fertig**.
- Deaktivieren Sie den Schalter für **Selbstschutz**.

  Die Selbstschutzfunktion (Self-Protection) verhindert, dass die Prozesse, Registry-Einträge, ausführbaren Dateien und Konfigurationsdateien der Backup-Software selbst sowie Backups, die in lokalen Ordnern gespeichert sind, verändert werden können. Wir raten davon ab, diese Funktion zu deaktivieren.
- Ändern Sie die **Schutzoptionen** (S. 180).

4. Wenn Sie die Einstellungen verändern, klicken Sie anschließend auf **Änderungen speichern**. Die Änderungen werden auf alle Maschinen angewendet, auf denen Active Protection aktiviert wurde.
5. Klicken Sie auf **Anwenden**.

17.1 Schutzoptionen

Backups

Diese Option ist nur dann wirksam, wenn im Active Protection-Plan die Option **Selbstschutz** aktiviert ist.

Diese Option gilt für Dateien mit den Endungen .tibx, .tib sowie .tia und die in lokalen Ordnern vorliegen.

Mit dieser Option können Sie Prozesse spezifizieren, die berechtigt sind, Backup-Dateien zu modifizieren, auch wenn diese Dateien per Selbstschutz-Funktion grundsätzlich geschützt sind. Dies kann nützlich sein, wenn Sie Backup-Dateien löschen oder per Skript zu einem anderen Speicherort verschieben wollen.

Die Voreinstellung ist: **Aktiviert**.

Wenn diese Option aktiviert ist, können die Backup-Dateien nur von solchen Prozessen modifiziert werden, die vom Hersteller der Backup-Software signiert wurden. Dadurch kann die Software Aufbewahrungsregeln anwenden und Backups löschen, wenn ein Benutzer dies über die Weboberfläche anfordert. Andere Prozesse, egal ob diese verdächtig sind oder nicht, können die Backups nicht modifizieren.

Wenn Sie diese Option deaktivieren, können Sie auch anderen Prozessen erlauben, Backups zu modifizieren. Spezifizieren Sie den vollständigen Pfad zur ausführbaren Datei des Prozesses (mit dem Laufwerksbuchstaben beginnend).

Krypto-Mining-Schutz

Diese Option bestimmt, ob Active Protection mögliche Krypto-Mining-Malware erkennt.

Die Voreinstellung ist: **Deaktiviert**.

Wenn eine Krypto-Mining-Aktivität erkannt wird, wird die ausgewählte **Aktion bei Erkennung** durchgeführt (mit Ausnahme der Wiederherstellung von Dateien aus dem Cache, da es hier nichts zum Wiederherstellen gibt).

Krypto-Mining-Malware kann die Performance nützlicher Applikationen beeinträchtigen, die Stromrechnung erhöhen, Systemabstürze oder sogar Hardware-Schäden (durch übermäßige Nutzung) verursachen. Wir empfehlen, Krypto-Mining-Malware zur Liste der **Schädlichen Prozesse** hinzuzufügen, um deren Ausführung zu unterbinden.

Zugeordnete Laufwerke

Diese Option bestimmt, ob auch Netzwerkordner durch die die Active Protection-Funktion geschützt werden sollen, die als lokale Laufwerke zugeordnet (gemountet) sind.

Diese Option gilt für Ordner, die per SMB oder NFS freigegeben/zugeordnet wurden.

Die Voreinstellung ist: **Aktiviert**.

Wenn sich eine Datei ursprünglich auf einem solchen Netzlaufwerk befand, kann diese nicht an ihrem ursprünglichen Speicherort wiederhergestellt werden, wenn die Datei aufgrund des Befehls **Aus Cache wiederherstellen** aus dem Cache extrahiert wird. Stattdessen wird die Datei aus dem Caceh in demjenigen Ordner wiederhergestellt, der in den Einstellungen der Option spezifiziert wurde. Der vorgegebene Ordner ist: **C:\ProgramData\Acronis\Restored Network Files**. Falls es diesen Ordner nicht gibt, wird er automatisch erstellt. Wenn Sie diesen Pfad ändern wollen, dürfen Sie nur einen lokalen Ordner spezifizieren. Netzwerkordner werden nicht unterstützt (gilt auch für Ordner von Netzwerklaufwerken)

18 Websites und Webhosting-Server schützen

18.1 Websites schützen

Eine Website kann als Folge eines unberechtigten Zugriffs oder eines Malware-Angriffs beschädigt werden. Erstellen Sie ein Backup Ihrer Website, wenn Sie diese (nach bzw. aufgrund einer Beschädigung) leicht auf einen fehlerfreien Zustand zurücksetzen wollen.

Was benötige ich, um eine Website sichern zu können?

Sie müssen auf die Website über das SFTP- oder SSH-Protokoll zugreifen können. Es ist nicht notwendig, einen Agenten zu installieren. Sie müssen Ihre Website einfach nur so hinzufügen, wie es später in diesem Abschnitt beschrieben ist.

Welche Elemente können per Backup gesichert werden?

Sie können folgende Elemente sichern:

- **Dateien mit Website-Inhalten**

  Alle Dateien, die über das Konto verfügbar sind, welches Sie für die SFTP- oder SSH-Verbindung spezifiziert haben.
- **Verknüpfte Datenbanken (sofern vorhanden), auf MySQL-Servern gehostet.**

  Alle Datenbanken, die über das von Ihnen spezifizierten MySQL-Konto verfügbar sind.

Wenn Ihre Website Datenbanken verwendet, sollten Sie die Dateien und Datenbanken gemeinsam per Backup sichern, damit Sie diese in einem konsistenten Zustand wiederherstellen können.

Einschränkungen

- Der einzig verfügbare Speicherort für ein Website-Backup ist der Cloud Storage.
- Ein Backup-Plan kann nicht auf mehrere Websites angewendet werden. Jede Website muss ihren eigenen Backup-Plan haben, selbst wenn alle Backup-Pläne ansonsten die gleichen Einstellungen haben.
- Es kann nur ein Backup-Plan auf eine Website angewendet werden.
- Es sind keine Backup-Optionen verfügbar.

18.1.1 Eine Website per Backup sichern

So können Sie eine Website hinzufügen und ihr Backup konfigurieren

1. Klicken Sie auf **Geräte** –> **Hinzufügen**.
2. Klicken Sie auf **Website**.
3. Konfigurieren Sie die folgenden Zugriffseinstellungen für die Website:
   - Geben Sie bei **Website-Name** eine (von Ihnen erstellte) Bezeichnung für Ihre Website ein. Dieser Name wird in der Backup-Konsole angezeigt.
   - Spezifizieren Sie bei **Host** den Namen und die IP-Adresse des Hosts, die für den Zugriff auf die Website per SFTP oder SSH verwendet werden sollen. Beispielsweise `mein.server.com` oder `10.250.100.100`
   - Spezifizieren Sie bei **Port** die Port-Nummer.
   - Spezifizieren Sie bei **Benutzername** und **Kennwort** die Anmeldedaten des Kontos, welches für den Zugriff auf die Website per SFTP oder SSH verwendet werden soll.

     ***Wichtig**: Es werden nur die Dateien per Backup gesichert, die über das spezifizierte Konto verfügbar sind.*

     Statt eines Kennworts können Sie auch Ihren privaten SSH-Schlüssel spezifizieren. Aktivieren Sie dafür das Kontrollkästchen **Privaten SSH-Schlüssel statt Kennwort verwenden** und spezifizieren Sie dann den entsprechenden Schlüssel.
4. Klicken Sie auf **Weiter**.
5. Wenn Ihre Website MySQL-Datenbanken verwendet, konfigurieren Sie die Zugriffseinstellungen für diese Datenbanken. Anderenfalls können Sie auf **Überspringen** klicken.
   a. Wählen Sie bei **Verbindungsart**, wie auf die Datenbanken aus der Cloud zugegriffen werden soll:
      - **Per SSH vom Host** – Es wird über den Host auf die Datenbanken zugegriffen, der in Schritt 3 spezifiziert wurde.
      - **Direkte Verbindung** – Es wird direkt auf die Datenbanken zugegriffen. Wählen Sie diese Einstellung nur, wenn die Datenbanken auch über das Internet verfügbar sind.

   b. Spezifizieren Sie bei **Host** den Namen oder die IP-Adresse des Hosts, auf dem der entsprechende MySQL-Server ausgeführt wird.

   c. Spezifizieren Sie bei **Port** die Port-Nummer für die TCP/IP-Verbindung zum Server. Die Standardportnummer ist 3306.

   d. Spezifizieren Sie bei **Benutzername** und **Kennwort** die Anmeldedaten für das MySQL-Konto.

      ***Wichtig**: Es werden nur die Datenbanken per Backup gesichert, die über das spezifizierte Konto verfügbar sind.*

   e. Klicken Sie auf **Erstellen**.

6. Die Software zeigt eine neue Backup-Plan-Vorlage an. Ändern Sie (bei Bedarf) die Einstellungen und klicken Sie dann auf **Anwenden**.

So können Sie die Verbindungseinstellungen ändern

1. Wählen Sie die Website unter **Geräte** –> **Websites** aus.
2. Klicken Sie auf **Überblick**.
3. Klicken Sie auf das Stiftsymbol neben der Website oder neben den Datenbank-Verbindungseinstellungen.
4. Nehmen Sie alle notwendigen Änderungen vor und klicken Sie dann auf **Speichern**.

So können Sie einen Backup-Plan bearbeiten

1. Wählen Sie die Website unter **Geräte** –> **Websites** aus.
2. Klicken Sie auf **Backup**.
3. Klicken Sie neben dem Namen des Backup-Plans auf das Zahnradsymbol und anschließend auf den Befehl **Bearbeiten**.
4. Nehmen Sie alle notwendigen Änderungen vor und klicken Sie dann auf **Änderungen speichern**.

18.1.2 Eine Website wiederherstellen

So können Sie eine Website wiederherstellen

1. Wählen Sie bei **Geräte** –> **Websites** diejenige Website aus, die Sie wiederherstellen wollen.

   Sie können die gewünschte Website auch per Namen suchen. Platzhalterzeichen (Wildcards) werden nicht unterstützt.
2. Klicken Sie auf **Recovery**.
3. Wählen Sie den gewünschten Recovery-Punkt aus.
4. Klicken Sie auf **Recovery** und bestimmen Sie, welche Elemente Sie wiederherstellen wollen: **Dateien/Ordner** oder **SQL-Datenbanken** (sofern vorhanden).

   Um sicherzustellen, dass Ihre Website anschließend in einem konsistenten Zustand ist, sollten Sie sowohl die Dateien als auch Datenbanken wiederherstellen (in beliebiger Reihenfolgen).
5. Befolgen Sie in Abhängigkeit von Ihrer Wahl eine der nachfolgend beschriebenen Prozeduren.

So können Sie die Website-Dateien/-Ordner wiederherstellen

1. Wechseln Sie zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden. Weitere Informationen über die Verwendung von Platzhalterzeichen finden Sie im Abschnitt 'Dateifilter (S. 70)'.
2. Wählen Sie die Dateien, die Sie wiederherstellen wollen.
3. Um die Dateien als .zip-Datei abzuspeichern, müssen Sie auf **Download** klicken, dann den Zielspeicherort für die Daten bestimmen und schließlich auf **Speichern** klicken. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.
4. Klicken Sie auf **Recovery** und bestätigen Sie dann die Aktion.

   Die ausgewählten Dateien und Ordner werden an ihrem ursprünglichen Speicherort wiederhergestellt.

So können Sie die Datenbanken wiederherstellen

1. Wählen Sie Datenbanken, die Sie wiederherstellen wollen.
2. Um die Datenbanken als .zip-Datei abzuspeichern, müssen Sie auf **Download** klicken, dann den Zielspeicherort für die Dateien bestimmen und schließlich auf **Speichern** klicken. Wenn Sie dies nicht wollen, können Sie diesen Schritt überspringen.

3. Klicken Sie auf **Recovery** und bestätigen Sie dann die Aktion.

   Die ausgewählten Datenbanken werden am ursprünglichen Speicherort wiederhergestellt.

18.2 Webhosting-Server schützen

Webhosting-Administratoren, die die Plattformen Plesk oder cPanel verwenden, können diese Plattformen in den Backup Service integrieren.

Nach der Integration kann ein Administrator Folgendes tun:

- Einen kompletten Plesk- oder cPanel-Server per Laufwerk-Backup zum Cloud Storage sichern
- Den kompletten Server (inkl. aller Websites) wiederherstellen
- Für Plesk: granulare Wiederherstellungen von Websites, einzelnen Dateien, Postfächern oder Datenbanken durchführen
- Für cPanel: granulare Wiederherstellungen von Websites, einzelnen Dateien, Postfächern, E-Mail-Filtern, E-Mail-Weiterleitungen, Datenbanken und Konten durchführen
- Self-Service-Recovery für Plesk- und cPanel-Kunden aktivieren

Die Integration erfolgt über die Backup Service-Erweiterung. Wenn Sie die Erweiterung für Plesk oder cPanel benötigen, wenden Sie sich an den Anbieter des Backup Service.

Unterstützte Plesk- und cPanel-Versionen

- Plesk für Linux 17.0 und höher
- Jede cPanel-Version mit PHP 5.6 und höher

Quotas

Jeder per Backup gesicherte Plesk- oder cPanel-Server wird auf die Quota **Webhosting-Server** angerechnet. Wenn diese Quota deaktiviert ist oder die Überschreitungsgrenze für diese Quota erreicht ist, passiert Folgendes:

- Bei einem physischen Server wird die Quota **Server** verwendet. Wenn diese Quota deaktiviert ist oder die Überschreitungsgrenze für diese Quota erreicht ist, wird das Backup fehlschlagen.
- Bei einem virtuellen Server wird die Quota **Virtuelle Maschinen** verwendet. Wenn diese Quota deaktiviert ist oder die Überschreitungsgrenze für diese Quota erreicht ist, wird die Quota **Server** verwendet. Wenn diese Quota deaktiviert ist oder die Überschreitungsgrenze für diese Quota erreicht ist, wird das Backup fehlschlagen.

19 Spezielle Aktionen mit virtuellen Maschinen

19.1 Eine virtuelle Maschine aus einem Backup heraus ausführen (Instant Restore)

Sie können eine virtuelle Maschine aus einem Laufwerk-Backup heraus ausführen, welches ein Betriebssystem enthält. Mit dieser Aktion, die auch 'sofortige Wiederherstellung' oder 'Instant Recovery' genannt wird, können Sie einen virtuellen Server innerhalb von Sekunden hochfahren. Die virtuellen Laufwerke werden direkt aus dem Backup heraus emuliert und belegen daher keinen Speicherplatz im Datenspeicher (Storage). Zusätzlicher Speicherplatz wird lediglich benötigt, um Änderungen, die an den virtuellen Laufwerken durchgeführt werden, zu speichern.

Wir empfehlen, eine solche temporäre virtuelle Maschine für einen Zeitraum von bis zu drei Tagen auszuführen. Danach können Sie sie vollständig entfernen oder in eine reguläre virtuelle Maschine konvertieren (durch 'Finalisieren'), ohne dass es dabei zu einer Ausfallzeit kommt.

Solange die temporäre virtuelle Maschine vorhanden ist bzw. verwendet wird, können keine Aufbewahrungsregeln auf das Backup angewendet werden, welches die Maschine als Grundlage verwendet. Backups der ursprünglichen Maschine können weiterhin ungestört ausgeführt werden.

Anwendungsbeispiele

- **Disaster Recovery**

  Bringen Sie die Kopie einer ausgefallenen Maschine in kürzester Zeit online.
- **Ein Backup testen**

  Führen Sie eine Maschine von einem Backup aus und überprüfen Sie, ob das Gastbetriebssystem und Applikationen korrekt funktionieren.
- **Auf Applikationsdaten zugreifen**

  Verwenden Sie, während eine Maschine ausgeführt wird, die integrierten Verwaltungswerkzeuge der Applikation und extrahieren Sie erforderliche Daten.

Voraussetzungen

- Mindestens ein Agent für VMware oder Agent für Hyper-V muss für den Backup Service registriert sein.
- Das Backup kann in einem Netzwerkordner oder einem lokalen Ordner auf derjenigen Maschine gespeichert werden, auf welcher der Agent für VMware oder Agent für Hyper-V installiert ist. Wenn Sie einen Netzwerkordner verwenden, muss dieser von der entsprechenden Maschine aus verfügbar sein. Eine virtuelle Maschine kann auch direkt von einem Backup heraus ausgeführt werden, welches im Cloud Storage gespeichert ist. Dies ist jedoch langsamer, weil für diese Aktion intensive wahlfreie Lesezugriffe auf das Backup notwendig sind.
- Das Backup muss eine komplette Maschine enthalten oder doch zumindest alle Volumes, die zur Ausführung des Betriebssystems notwendig sind.
- Es können sowohl die Backups von physischen wie auch virtuellen Maschinen verwendet werden. Die Backups von Virtuozzo-*Containern* können nicht verwendet werden.
- Backups, die logische Linux-Volumes (LVMs) enthalten, müssen mit dem Agenten für VMware oder Agenten für Hyper-V erstellt werden. Die virtuelle Maschine muss denselben Typ wie die Originalmaschine (ESXi oder Hyper-V) haben.

19.1.1 Eine Maschine ausführen

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wählen Sie eine zu sichernde Maschine, klicken Sie auf **Recovery** und wählen Sie dann einen Recovery-Punkt.
   - Wählen Sie einen Recovery-Punkt auf der Registerkarte 'Backups' (S. 125).
2. Klicken Sie auf **Als VM ausführen**.

Die Software wählt den Host und die anderen benötigten Parameter automatisch aus.

3. [Optional] Klicken Sie auf **Zielmaschine** und ändern Sie den Typ der virtuellen Maschine (ESXi oder Hyper-V), den Host oder den Namen der virtuellen Maschine.
4. [Optional] Klicken Sie auf **Datenspeicher** für ESXi oder **Pfad** für Hyper-V – und bestimmten Sie dann den Datenspeicher für die neue virtuelle Maschine.

   Während die Maschine ausgeführt wird, werden die (möglichen) Änderungen gesammelt, die an den virtuellen Laufwerken erfolgen. Stellen Sie sicher, dass der ausgewählte Datenspeicher genügend freien Speicherplatz hat.
5. [Optional] Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers und die Netzwerkverbindungen der virtuellen Maschine zu ändern.
6. [Optional] Bestimmen Sie den Betriebszustand der VM (**An**/**Aus**).
7. Klicken Sie auf **Jetzt ausführen**.

Als Ergebnis dieser Aktion wird die Maschine in der Weboberfläche mit einem dieser Symbole angezeigt:  oder 

. Von solchen virtuellen Maschinen kann kein Backup erstellt werden.

19.1.2 Eine Maschine löschen

Wir raten davon ab, eine temporäre virtuelle Maschine direkt in vSphere/Hyper-V zu löschen. Dies kann zu Fehlern in der Weboberfläche führen. Außerdem kann das Backup, von dem die Maschine ausgeführt wurde, für eine gewisse Zeit gesperrt bleiben (es kann nicht von Aufbewahrungsregeln gelöscht werden).

So löschen Sie eine virtuelle Maschine, die aus einem Backup heraus ausgeführt wird.

1. Wählen Sie auf der Registerkarte **Alle Geräte** eine Maschine aus, die aus einem Backup heraus ausgeführt wird.

2. Klicken Sie auf **Löschen**.

Die Maschine wird von der Weboberfläche entfernt. Sie wird außerdem auch aus der vSphere- oder Hyper-V-Bestandsliste (Inventory) und dem Datenspeicher (Storage) entfernt. Alle Änderungen an den Daten der Maschine, die während ihrer Ausführungen erfolgten, gehen verloren.

19.1.3 Eine Maschine finalisieren

Wenn eine virtuelle Maschine aus einem Backup heraus ausgeführt wird, werden auch die Inhalte der virtuellen Laufwerke direkt aus dem Backup entnommen. Sollte daher während der Ausführung die Verbindung zum Backup-Speicherort oder dem Backup Agenten verloren gehen, geht auch der Zugriff auf die Maschine verloren und kann die Maschine beschädigt werden.

Wenn es sich um eine ESXi-Maschine handelt, können Sie diese in eine 'dauerhafte' Maschine umwandeln. Das bedeutet, alle virtuellen Laufwerke der Maschine zusammen mit allen Änderungen, die während ihrer Ausführung aufgetreten sind, zu dem Datenspeicher wiederherzustellen, auf dem diese Änderungen gespeichert werden. Dieser Prozess wird 'Finalisieren' genannt.

Das Finalisieren erfolgt, ohne dass es zu einem Ausfall der Maschine kommt. Die virtuelle Maschine wird also während des Finalisierens *nicht* ausgeschaltet.

So finalisieren Sie eine virtuelle Maschine, die aus einem Backup heraus ausgeführt wird.

1. Wählen Sie auf der Registerkarte **Alle Geräte** eine Maschine aus, die aus einem Backup heraus ausgeführt wird.
2. Klicken Sie auf **Finalisieren**.
3. [Optional] Spezifizieren Sie einen neuen Namen für die Maschine.
4. [Optional] Den Laufwerk-Provisioning-Modus ändern. Standardeinstellung ist **Thin**.
5. Klicken Sie auf **Finalisieren**.

Der Name der Maschine wird sofort geändert. Der Recovery-Fortschritt wird auf der Registerkarte **Aktivitäten** angezeigt. Sobald die Wiederherstellung fertiggstellt wurde, wird das Symbol der Maschine zu dem für eine reguläre virtuelle Maschine geändert.

Das sollten Sie über die Finalisierung wissen

Finalisierung vs. normale Wiederherstellung

Der Finalisierungsprozess ist aus folgenden Gründen langsamer als eine normale Wiederherstellung:

- Während einer Finalisierung greift der Agent per Zufallszugriff auf unterschiedliche Teile des Backups zu. Wenn eine komplette Maschine wiederhergestellt wird, liest der Agent die Daten nacheinander aus dem Backup aus.
- Wenn die virtuelle Maschine während der Finalisierung ausgeführt wird, liest der Agent die Daten aus dem Backup häufiger aus, um beide Prozesse gleichzeitig aufrechtzuerhalten. Während einer normalen Wiederherstellung wird die virtuelle Maschine gestoppt.

Die Finalisierung von Maschinen, die aus Cloud Backups ausgeführt werden

Die Finalisierungsgeschwindigkeit hängt – aufgrund des intensiven Zugriffs auf die Backup-Daten – stark von der Verbindungsbandbreite zwischen dem Backup-Speicherort und dem Agenten ab. Die Finalisierung von Backups, die in der Cloud liegen, ist langsamer als von lokalen Backups. Wenn die Internetverbindung sehr langsam oder sogar instabil ist, kann die Finalisierung einer Maschine, die aus einem Cloud-Backup ausgeführt wird, fehlschlagen. Falls Sie die Wahl haben, empfehlen wir Ihnen daher, virtuelle Maschinen möglichst aus lokalen Backups auszuführen, wenn Sie eine Finalisierung planen.

19.2 Replikation von virtuellen Maschinen

Die Möglichkeit zur Replikation ist nur für virtuelle VMware ESXi-Maschinen verfügbar.

Unter Replikation wird (hier) ein Prozess verstanden, bei dem von einer virtuellen Maschine zuerst eine exakte Kopie (Replikat) erstellt wird – und dieses Replikat dann mit der ursprünglichen Maschine fortlaufend synchronisiert wird. Wenn Sie eine wichtige virtuelle Maschine replizieren, haben Sie immer eine Kopie dieser Maschine in einem startbereiten Zustand verfügbar.

Eine Replikation kann entweder manuell oder auf Basis einer (von Ihnen spezifizierten) Planung gestartet werden. Die erste Replikation ist vollständig, was bedeutet, dass die komplette Maschine kopiert wird. Alle nachfolgenden Replikationen erfolgen dann inkrementell und werden mithilfe von 'CBT (Changed Block Tracking)' (S. 192) durchgeführt (außer diese Option wird extra deaktiviert).

Replikation vs. Backup

Anders als bei geplanten Backups wird bei einem Replikat immer nur der letzte (jüngste) Zustand der virtuellen Maschine aufbewahrt. Ein Replikat belegt Platz im Datenspeicher, während für Backups ein kostengünstigerer Storage verwendet werden kann.

Das Aktivieren eines Replikats geht jedoch deutlich schneller als eine klassische Wiederherstellung aus einem Backup – und ist auch schneller als die Ausführung einer virtuellen Maschine aus einem Backup. Ein eingeschaltetes Replikat arbeitet schneller als eine VM, die aus einem Backup ausgeführt wird, und es muss kein Agent für VMware geladen werden.

Anwendungsbeispiele

- **Sie replizieren virtuelle Maschinen zu einem Remote-Standort.**

  Die Replikation ermöglicht Ihnen, teilweise oder vollständige Datacenter-Ausfälle zu überstehen, indem Sie die virtuellen Maschinen von einem primären zu einem sekundären Standort klonen. Als sekundärer Standort wird üblicherweise eine entfernt gelegene Einrichtung verwendet, die normalerweise nicht von denselben Störereignissen (Katastrophen in der Umgebung, Infrastrukturprobleme etc.) wie der primäre Standort betroffen wird/werden kann.

- **Sie replizieren virtuelle Maschinen innerhalb eines Standortes (von einem Host/Datenspeicher zu einem anderen).**

  Eine solche Onsite-Replikation kann zur Gewährleistung einer hohen Verfügbarkeit und für Disaster Recovery-Szenarien verwendet werden.

Das können Sie mit einem Replikat tun

- **Ein Replikat testen** (S. 190)

  Das Replikat wird für den Test eingeschaltet. Verwenden Sie den vSphere Client oder andere Tools, um die korrekte Funktion des Replikats zu überprüfen. Die Replikation wird angehalten, solange der Test läuft.

- **Failover auf ein Replikat** (S. 190)

  Bei einem Failover wird der Workload der ursprünglichen virtuellen Maschine auf ihr Replikat verschoben. Die Replikation wird angehalten, solange die Failover-Aktion läuft.

- **Das Replikat sichern**

  Backup und Replikation erfordern beide einen Zugriff auf virtuelle Laufwerke, wodurch wiederum der Host, auf dem die virtuelle Maschine läuft, in seiner Performance beeinflusst wird. Wenn Sie von einer virtuellen Maschine sowohl Backups als auch ein Replikat haben wollen, der Produktions-Host dadurch aber nicht zusätzlich belastet werden soll, dann replizieren Sie die Maschine zu einem anderen Host. Dieses Replikat können Sie anschließend per Backup sichern.

Einschränkungen

Folgende Arten von virtuellen Maschinen können nicht repliziert werden:

- Fehlertolerante Maschinen, die auf ESXi 5.5 (und niedriger) laufen.
- Maschine, die aus Backups ausgeführt werden.
- Die Replikate von virtuellen Maschinen.

19.2.1 Einen Replikationsplan erstellen

Ein Replikationsplan muss für jede Maschine individuell erstellt werden. Es ist nicht möglich, einen vorhandenen Plan auf andere Maschinen anzuwenden.

So erstellen Sie einen Replikationsplan

1. Wählen Sie eine virtuelle Maschine aus, die repliziert werden soll.
2. Klicken Sie auf **Replikation**.

   Die Software zeigt eine Vorlage für den neuen Replikationsplan an.
3. [Optional] Wenn Sie den Namen des Replikationsplans ändern wollen, klicken Sie auf den vorgegebenen Standardnamen.
4. Klicken Sie auf **Zielmaschine** – und gehen Sie dann folgendermaßen vor:
   a. Bestimmen Sie, ob ein neues Replikat erstellt werden oder ein bereits vorhandenes Replikat der Maschine verwendet werden soll.
   b. Wählen Sie den ESXi-Host und spezifizieren Sie einen Namen für das neue Replikat – oder wählen Sie eine bereits vorhandenes Replikat aus.

      Der Standardname für ein neues Replikat ist **[Name der ursprünglichen Maschine]_replica**.
   c. Klicken Sie auf **OK**.
5. [Nur bei Replikation zu einer neuen Maschine] Klicken Sie auf **Datenspeicher** und bestimmten Sie dann den Datenspeicher für die neue virtuelle Maschine.
6. [Optional] Klicken Sie auf **Planung**, wenn Sie die Planung für die Replikation ändern wollen.

   Die Replikation erfolgt standardmäßig einmal am Tag – und zwar von Montag bis Freitag. Sie können den genauen Zeitpunkt festlegen, an dem die Replikation ausgeführt werden soll.

   Wenn Sie die Replikationsfrequenz ändern wollen, bewegen Sie einfach den entsprechenden grafischen Schieber – und spezifizieren Sie dann die gewünschte Planung.

   Sie außerdem noch Folgendes tun:

   - Sie können einen Datumsbereich für die Planung festlegen, zu dem die entsprechende Operation ausgeführt werden soll. Aktivieren Sie das Kontrollkästchen **Den Plan in einem Datumsbereich ausführen** und spezifizieren Sie anschließend den gewünschten Datumsbereich.
   - Sie können die Planung deaktivieren. In diesem Fall kann die Replikation manuell gestartet werden.
7. [Optional] Klicken Sie auf das Zahnradsymbol, wenn Sie die Replikationsoptionen (S. 192) anpassen wollen.
8. Klicken Sie auf **Anwenden**.
9. [Optional] Wenn Sie den Plan manuell ausführen wollen, klicken im Fensterbereich für die Planung auf **Jetzt ausführen**.

Wenn ein Replikationsplan ausgeführt wird, erscheint das virtuelle Maschinen-Replikat in der Liste '**Alle Geräte**' und wird mit diesem Symbol gekennzeichnet: 

19.2.2 Ein Replikat testen

So bereiten Sie ein Replikat für einen Test vor

1. Wählen Sie ein Replikat aus, das getestet werden soll.
2. Klicken Sie auf **Replikat testen**.
3. Klicken Sie auf **Test starten**.
4. Bestimmen Sie, ob das eingeschaltete Replikat mit dem Netzwerk verbunden werden soll. Die Standardvorgabe ist, dass das Replikat nicht mit dem Netzwerk verbunden wird.
5. [Optional] Falls Sie das Replikat mit dem Netzwerk verbinden wollen, müssen Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen** aktivieren, damit die ursprüngliche Maschine angehalten wird, bevor das Replikat eingeschaltet wird.
6. Klicken Sie auf **Start**.

So stoppen Sie den Test eines Replikats

1. Wählen Sie das Replikat aus, welches gerade getestet wird.
2. Klicken Sie auf **Replikat testen**.
3. Klicken Sie auf **Test stoppen**.
4. Bestätigen Sie Ihre Entscheidung.

19.2.3 Ein Failover auf ein Replikat durchführen

So führen Sie ein Failover von einer Maschine auf ein Replikat durch

1. Wählen Sie ein Replikat aus, auf welches das Failover erfolgen soll.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Failover**.
4. Bestimmen Sie, ob das eingeschaltete Replikat mit einem Netzwerk verbunden werden soll. Als Standardvorgabe wird das Replikat mit demselben Netzwerk wie die ursprüngliche Maschine verbunden.
5. [Optional] Falls Sie das Replikat mit dem Netzwerk verbinden wollen, müssen Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen** deaktivieren, wenn die ursprüngliche Maschine online bleiben soll.
6. Klicken Sie auf **Start**.

Während sich das Replikat im Failover-Stadium befindet, können Sie eine der folgenden Aktionen wählen:

- **Failover stoppen** (S. 191)

  Stoppen Sie das Failover, wenn die ursprüngliche Maschine repariert wurde. Das Replikat wird ausgeschaltet. Die Replikation wird fortgesetzt.
- **Permanentes Failover auf das Replikat durchführen** (S. 191)

  Diese sofortige Aktion entfernt die 'Replikat'-Kennzeichnung von der virtuellen Maschine, sodass diese nicht mehr als Replikationsziel verwendet werden kann. Wenn Sie die Replikation wieder aufnehmen wollen, bearbeiten Sie den Replikationsplan, um diese Maschine als Quelle auszuwählen.

- **Failback** (S. 191)

  Führen Sie ein Failback aus, falls Sie ein Failover zu einer Site gemacht haben, die nicht für den Dauerbetrieb gedacht ist. Das Replikat wird zu der ursprünglichen oder einer neuen virtuellen Maschine wiederhergestellt. Sobald die Wiederherstellung zu der ursprünglichen Maschine abgeschlossen ist, wird diese eingechaltet und die Replikation fortgesetzt. Wenn Sie die Wiederherstellung zu einer neuen Maschine durchgeführt haben, bearbeiten Sie den Replikationsplan, um diese Maschine als Quelle auszuwählen.

19.2.3.1 Ein Failover stoppen

So stoppen Sie einen Failover-Vorgang

1. Wählen Sie ein Replikat, das sich im Failover-Stadium befindet.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Failover stoppen**.
4. Bestätigen Sie Ihre Entscheidung.

19.2.3.2 Ein permanentes Failover durchführen

So führen Sie ein permanentes Failover durch

1. Wählen Sie ein Replikat, das sich im Failover-Stadium befindet.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Permanentes Failover**.
4. [Optional] Ändern Sie den Namen der virtuellen Maschine.
5. [Optional] Aktivieren Sie das Kontrollkästchen **Ursprüngliche virtuelle Maschine stoppen**.
6. Klicken Sie auf **Start**.

19.2.3.3 Ein Failback durchführen

So führen Sie ein Failback von einem Replikat durch

1. Wählen Sie ein Replikat, das sich im Failover-Stadium befindet.
2. Klicken Sie auf **Replikat-Aktionen**.
3. Klicken Sie auf **Failback vom Replikat**.

   Die Software wählt automatisch die ursprüngliche Maschine als Zielmaschine aus.
4. [Optional] Klicken Sie auf **Zielmaschine** – und gehen Sie dann folgendermaßen vor:
   a. Bestimmen Sie, ob das Failback zu einer neuen oder einer bereits vorhandenen Maschine durchgeführt werden soll.
   b. Wählen Sie den ESXi-Host und spezifizieren Sie einen Namen für die neue Maschine – oder wählen Sie eine bereits vorhandene Maschine aus.
   c. Klicken Sie auf **OK**.
5. [Optional] Wenn Sie eine neue Maschine als Failback-Ziel verwenden, können Sie außerdem noch Folgendes tun:
   - Klicken Sie auf **Datenspeicher**, um den Datenspeicher für die virtuelle Maschine festzulegen.
   - Klicken Sie auf **VM-Einstellungen**, um die Größe des Arbeitsspeichers, die Anzahl der Prozessoren und die Netzwerkverbindungen für die virtuelle Maschine zu ändern.
6. [Optional] Klicken Sie auf **Recovery-Optionen**, wenn Sie die Failback-Optionen (S. 192) ändern wollen.
7. Klicken Sie auf **Recovery starten**.

8. Bestätigen Sie Ihre Entscheidung.

19.2.4 Replikationsoptionen

Wenn Sie die Replikationsoptionen ändern wollen, klicken Sie auf das Zahnradsymbol neben dem Namen des Replikationsplans und dann auf das Element **Replikationsoptionen**.

Changed Block Tracking (CBT)

Diese Option entspricht im Wesentlichen der Backup-Option 'CBT (Changed Block Tracking) (S. 68)'.

Laufwerk-Provisioning

Diese Option definiert die Laufwerk-Provisioning-Einstellungen für das Replikat.

Die Voreinstellung ist: **Thin Provisioning**.

Folgende Werte sind verfügbar: **Thin Provisioning**, **Thick Provisioning**, **Ursprüngliche Einstellung behalten**.

Fehlerbehandlung

Diese Option entspricht im Wesentlichen der Backup-Option 'Fehlerbehandlung (S. 69)'.

Vor-/Nach-Befehle

Diese Option entspricht im Wesentlichen der Backup-Option 'Vor-/Nach-Befehle (S. 76)'.

VSS (Volume Shadow Copy Service) für virtuelle Maschinen

Diese Option entspricht im Wesentlichen der Backup-Option 'VSS (Volume Shadow Copy Service) für virtuelle Maschinen (S. 82)'.

19.2.5 Failback-Optionen

Wenn Sie die Failback-Optionen ändern wollen, klicken Sie während der Failbackup-Konfiguration auf **Recovery-Optionen**.

Fehlerbehandlung

Diese Option entspricht im Wesentlichen der Recovery-Option 'Fehlerbehandlung (S. 101)'.

Performance

Diese Option entspricht im Wesentlichen der Recovery-Option 'Performance (S. 103)'.

Vor-/Nach-Befehle

Diese Option entspricht im Wesentlichen der Recovery-Option 'Vor-/Nach-Befehle (S. 104)'.

VM-Energieverwaltung

Diese Option entspricht im Wesentlichen der Recovery-Option 'VM-Energieverwaltung (S. 106)'.

19.2.6 Seeding eines anfänglichen Replikats

Um die Replikation zu einem Remote-Standort zu beschleunigen und Netzwerkbandbreite einzusparen, können Sie ein Replikat-Seeding durchführen.

Wichtig: *Um ein Replikat-Seeding durchführen zu können, muss der Agent für VMware (Virtuelle Appliance) auf dem ESXi-Zielhost ausgeführt werden.*

So führen Sie das Seeding eines anfänglichen Replikats durch

1. Gehen Sie nach einer der nachfolgenden Möglichkeiten vor:
   - Wenn die ursprüngliche Maschine ausgeschaltet werden kann, tun Sie dies – und springen sie dann zu Schritt 4.
   - Wenn die ursprüngliche virtuelle Maschine nicht ausgeschaltet werden kann, fahren Sie mit dem nächsten Schritt fort.
2. Erstellen Sie einen Replikationsplan (S. 189).

   Wählen Sie beim Erstellen des Plans bei **Zielmaschine** die Option **Neues Replikat** sowie den ESXi, der die ursprüngliche Maschine hostet.
3. Führen Sie den Plan einmal aus.

   Auf dem ursprünglichen ESXi wird ein Replikat erstellt.
4. Exportieren Sie die Dateien der virtuellen Maschine (oder des Replikats) auf ein externes Festplattenlaufwerk.
   a. Verbinden Sie das externe Laufwerk mit der Maschine, auf welcher der vSphere Client ausgeführt wird.
   b. Verbinden Sie den vSphere Client mit dem ursprünglichen vCenter/ESXi.
   c. Wählen Sie das neu erstellte Replikat in der Bestandsliste (Inventory) aus.
   d. Klicken Sie auf **Datei** –> **Exportieren** –> **OVF-Vorlage exportieren**.
   e. Spezifizieren Sie im **Verzeichnis** den entsprechenden Ordner auf dem externen Laufwerk.
   f. Klicken Sie auf **OK**.
5. Senden Sie das Festplattenlaufwerk zum Remote-Standort.
6. Importieren Sie das Replikat in den ESXi-Zielhost.
   a. Verbinden Sie das externe Laufwerk mit der Maschine, auf welcher der vSphere Client ausgeführt wird.
   b. Verbinden Sie den vSphere Client mit dem Ziel-vCenter/-ESXi.
   c. Klicken Sie auf **Datei** –> **OVF-Vorlage bereitstellen**.
   d. Spezifizieren Sie bei **Von einer Datei oder URL bereitstellen** die Vorlage, die Sie in Schritt 4 exportiert haben.
   e. Schließen Sie die Import-Prozedur ab.
7. Bearbeiten Sie den Replikationsplan, den Sie in Schritt 2 erstellt haben. Wählen Sie bei **Zielmaschine** die Option **Vorhandenes Replikat** und wählen Sie dann das importierte Replikat aus.

Die Software wird daraufhin die Aktualisierung des Replikats fortsetzen. Alle Replikationen werden inkrementell sein.

19.3 Virtualisierungsumgebungen verwalten

Sie können vSphere-, Hyper-V- und Virtuozzo-Umgebungen in ihrer nativen Darstellung anzeigen lassen. Sobald der entsprechende Agent installiert und registriert ist, werden die Registerkarten **VMware**, **Hyper-V** oder **Virtuozzo** unter **Geräte** angezeigt.

Über die Registerkarte **VMware** können Sie die Zugriffsanmeldedaten für einen vCenter Server oder eigenständigen ESXi-Host ändern, ohne den Agenten neu installieren zu müssen.

So ändern Sie die Zugriffsanmeldedaten für einen vCenter Server oder eigenständigen ESXi-Host

1. Klicken Sie bei **Geräte** auf **VMware**.
2. Klicken Sie auf **Hosts und Cluster**.
3. Wählen Sie in der '**Hosts und Cluster**'-Liste (rechts neben dem '**Hosts und Cluster**'-Verzeichnisbaum) denjenigen vCenter Server oder eigenständigen ESXi-Host aus, der bei der Installation des Agenten für VMware spezifiziert wurde.
4. Klicken Sie auf **Überblick**.
5. Klicken Sie unter **Anmeldedaten** auf den Benutzernamen.
6. Spezifizieren Sie die neuen Anmeldedaten und klicken Sie abschließend auf **OK**.

19.4 Migration von Maschinen

Sie können eine Maschine migrieren, wenn Sie ihr Backup zu einer anderen (also nicht der ursprünglichen) Maschine wiederherstellen.

Die nachfolgende Tabelle fasst alle verfügbaren Migrationsoptionen zusammen.

Maschinentyp im Backup:	**Verfügbare Recovery-Ziele**				
	Physische Maschine	Virtuelle ESXi-Maschine	Virtuelle Hyper-V-Maschine	Virtuelle Virtuozzo-Maschine	Virtuozzo-Container
Physische Maschine	+	+	+	-	-
Virtuelle VMware ESXi-Maschine	+	+	+	-	-
Virtuelle Hyper-V-Maschine	+	+	+	-	-
Virtuelle Virtuozzo-Maschine	+	+	+	+	-
Virtuozzo-Container	-	-	-	-	+

Anleitungen zur Durchführung von Migrationen finden Sie in folgenden Abschnitten:

- Physisch-zu-virtuell (P2V) – 'Physische Maschinen als virtuelle Maschinen wiederherstellen (S. 87)'
- Virtuell-zu-virtuell (V2V) – 'Virtuelle Maschine (S. 88)'
- Virtuell-zu-physisch (V2P) – 'Virtuelle Maschine (S. 88)' oder 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen (S. 90)'

Obwohl es möglich ist, V2P-Migrationen von der Weboberfläche aus durchzuführen, empfehlen wir für bestimmte Fälle die Verwendung eines Boot-Mediums. Sie können das Boot-Medium auch für eine Migration zu ESXi oder Hyper-V verwenden.

Mit dem Boot-Medium können Sie Folgendes tun:

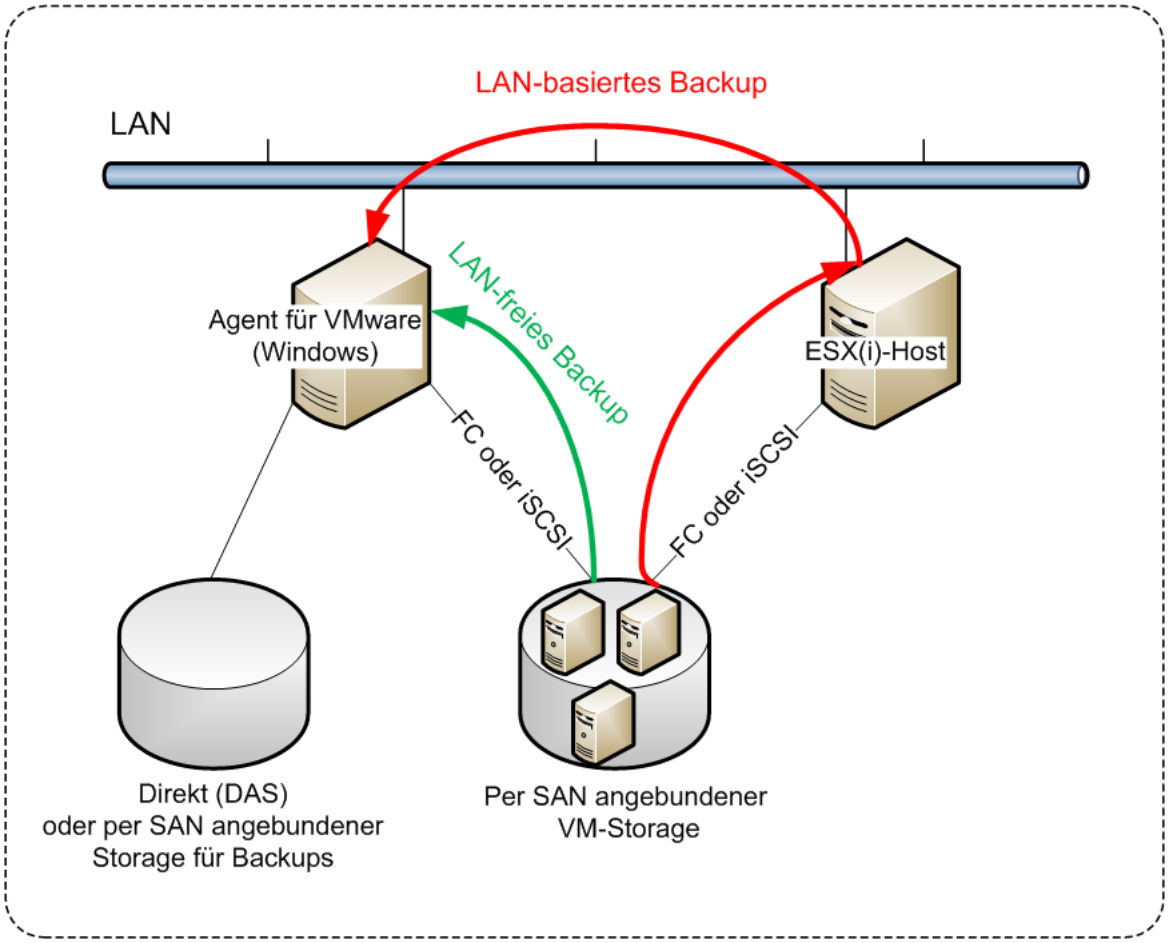
- Einzelne Laufwerke oder Volumes für die Wiederherstellung auswählen.

- Die Laufwerke im Backup manuell bestimmten Laufwerken der Zielmaschine zuweisen.
- P2V-Migration, V2P-Migration oder V2V-Migration von Virtuozzo auf einer Linux-Maschine mit logischen Volumes (LVM) durchführen. Den Agenten für Linux verwenden, um Backups und Boot-Medien für Wiederherstellungen zu erstellen.
- Treiber für bestimmte Hardware bereitstellen, die für die Bootfähigkeit des Systems notwendig sind.

19.5 Agent für VMware – LAN-freies Backup

Sollte Ihr ESXi einen per SAN angeschlossenen Storage verwenden, 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 ESXi-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 Maschine des Agenten oder auf einem per SAN angebundenen Storage speichern.



So ermöglichen Sie dem Agenten, auf einen Datenspeicher direkt zuzugreifen

1. Installieren Sie den Agenten für VMware auf einer Windows-Maschine, die Netzwerkzugriff auf den vCenter Server hat.

2. Verbinden Sie die LUN (Logical Unit Number), die den Datenspeicher für die Maschine hostet. Beachten Sie dabei:
   - Verwenden Sie dasselbe Protokoll (z.B. iSCSI oder FC), das auch zur Datenspeicher-Verbindung mit dem ESXi verwendet wird.
   - Die LUN *darf nicht* initialisiert werden und muss als 'Offline'-Laufwerk in der **Datenträgerverwaltung** erscheinen. Falls Windows die LUN initialisiert, kann sie beschädigt und damit unlesbar für VMware vSphere werden.

Als Ergebnis wird der Agent den SAN-Transportmodus nutzen, um auf die virtuelle Laufwerke zuzugreifen. Das bedeutet, es werden nur die blanken ('raw') LUN-Sektoren über iSCSI/FC gelesen, ohne dass das VMFS-Dateisystem erkannt wird (welches von Windows nicht unterstützt wird).

Einschränkungen

- In vSphere 6.0 (und höher) kann der Agent den SAN-Transportmodus nicht verwenden, wenn sich einige der VM-Laufwerke auf einem „VMware Virtual Volume“ (VVol) befinden und einige nicht. Die Backups solcher virtuellen Maschinen werden daher fehlschlagen.
- Verschlüsselte virtuelle Maschinen, die mit VMware vSphere 6.5 eingeführt wurden, werden via LAN gesichert – und zwar auch dann, wenn Sie den SAN-Transportmodus für den Agenten konfiguriert haben. Der Agent wird stattdessen auf den NBD-Transportmodus zurückgreifen, weil VMware den SAN-Transportmodus beim Backup verschlüsselter virtueller Laufwerke nicht unterstützt.

Beispiel

Falls Sie ein iSCSI-SAN verwenden, konfigurieren Sie den iSCSI-Initiator auf einer unter Windows laufenden Maschine, auf welcher der Agent für VMware installiert ist.

So konfigurieren Sie die SAN-Richtlinie

1. Melden Sie sich als Administrator an, öffnen Sie die Eingabeaufforderung, geben Sie den Befehl '**`diskpart`**' ein und drücken Sie dann auf die **Eingabetaste**.
2. Geben Sie **`san`** und drücken Sie die **Eingabetaste**. Überprüfen Sie, dass **SAN-Richtlinie: Offline – Alle** angezeigt wird.
3. Falls ein anderer Wert für die SAN-Richtlinie eingestellt ist:
   a. Geben Sie den Befehl **`san policy=offlineall`** ein.
   b. Drücken Sie die **Eingabetaste**.
   c. Führen Sie Schritt 2. aus, um zu überprüfen, dass die Einstellung korrekt angewendet wurde.
   d. Starten Sie die Maschine neu.

So konfigurieren Sie einen iSCSI-Initiator

1. Gehen Sie zu **Systemsteuerung** –> **Verwaltung** –> **iSCSI-Initiator**.

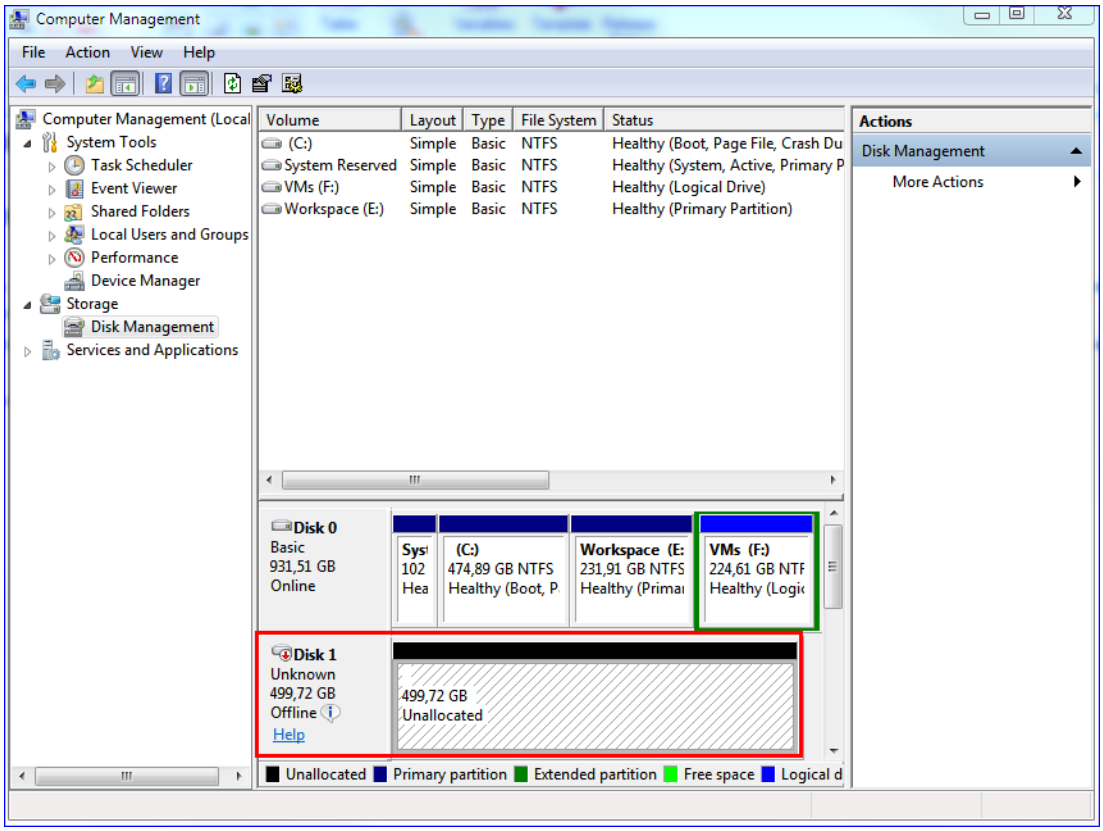
   Tipp: *Wenn Sie das Systemsteuerungsmodul **Verwaltung** nicht finden können, müssen Sie evtl. die Ansicht der **Systemsteuerung** von **Start** oder **Kategorie** auf eine andere Ansicht umstellen – oder die Suchfunktion verwenden.*

2. Wenn Sie den Microsoft iSCSI-Initiator das erste Mal aufrufen, müssen Sie bestätigen, dass Sie den Microsoft iSCSI-Initiator-Dienst starten wollen.
3. Geben Sie in der Registerkarte **Ziele** den vollqualifizierten Domain-Namen (FQDN) oder die IP-Adresse des SAN-Zielgerätes ein und klicken Sie dann auf **Schnell verbinden**.
4. Wählen Sie die LUN aus, die den Datenspeicher hostet, und klicken Sie dann auf **Verbinden**.

Sollte die LUN nicht angezeigt werden, dann überprüfen Sie, dass die Zonenzuweisung auf dem iSCSI-Ziel der Maschine, die den Agenten ausführt, ermöglicht, auf die LUN zuzugreifen. Die Maschine muss in die Liste der erlaubten iSCSI-Initiatoren auf diesem Ziel aufgenommen sein.

5. Klicken Sie auf **OK**.

Die betriebsbereite SAN-LUN sollte in der **Datenträgerverwaltung** so wie im unterem Screenshot angezeigt werden.



19.6 Agent für VMware – notwendige Berechtigungen

Damit ein Agent für VMware auf allen Hosts und Clustern, die von einem vCenter Server verwaltet werden, Aktionen durchführen kann, muss er über entsprechende Berechtigungen auf dem vCenter Server verfügen. Falls der Agent lediglich auf einem bestimmten ESXi-Host arbeiten soll, müssen Sie dem Agenten dieselben Berechtigungen auf diesem Host zuweisen.

Spezifizieren Sie das Konto mit den benötigten Berechtigungen, wenn Sie den Agenten für VMware installieren oder konfigurieren. Informationen darüber, wie Sie das Konto auch zu einem späteren Zeitpunkt noch ändern können, finden Sie im Abschnitt 'Virtualisierungsumgebungen verwalten (S. 193)'.

		Aktion			
Objekt	**Recht**	**Backup einer VM**	**Recovery zu einer neuen VM**	**Recovery zu einer existierenden VM**	**VM von Backup ausführen**
Kryptografische Operationen (ab vSphere 6.5)	**Laufwerk hinzufügen**	+*			

		Aktion			
Objekt	**Recht**	**Backup einer VM**	**Recovery zu einer neuen VM**	**Recovery zu einer existierenden VM**	**VM von Backup ausführen**
	Direktzugriff	+*			
Datenspeicher	**Speicher zuteilen**		+	+	+
	Datenspeicher durchsuchen				+
	Datenspeicher konfigurieren	+	+	+	+
	Dateivorgänge auf niedriger Ebene				+
Global	**Lizenzen**	+	+	+	+
	Methoden deaktivieren	+	+	+	
	Methoden aktivieren	+	+	+	
Host > Konfiguration	**Konfiguration für Speicherpartition**				+
Host > Lokale Operationen	**VM erstellen**				+
	VM löschen				+
	Virtuelle Maschine neu konfigurieren				+
Netzwerk	**Netzwerk zuweisen**		+	+	+
Ressource	**Virtuelle Maschine zu Ressourcenpool zuweisen**		+	+	+
Virtuelle Maschine –> Konfiguration	**Vorhandenes Laufwerk hinzufügen**	+	+		+
	Neues Laufwerk hinzufügen		+	+	+
	Gerät hinzufügen oder entfernen		+		+
	Erweitert	+	+	+	
	CPU-Anzahl ändern		+		
	Festplattenänderungsverfolgung	+		+	
	Festplatten-Lease	+		+	
	Arbeitsspeicher		+		
	Laufwerk entfernen	+	+	+	+
	Umbenennen		+		

		Aktion			
Objekt	**Recht**	**Backup einer VM**	**Recovery zu einer neuen VM**	**Recovery zu einer existierenden VM**	**VM von Backup ausführen**
	Anmerkung festlegen				+
	Einstellungen		+	+	+
Virtuelle Maschine –> Gastbetriebssystem	**Programmausführung im Gastbetriebssystem**	+**			
	Gastvorgangsabfragen	+**			
	Änderungen des Gastbetriebssystems	+**			
Virtuelle Maschine –> Interaktion	**Ticket zur Steuerung durch Gast abrufen** (in vSphere 4.1 und 5.0)				+
	CD-Medien konfigurieren		+	+	
	Gastbetriebssystem-Verwaltung über VIX API (in vSphere 5.1 und höher)				+
	Ausschalten			+	+
	Einschalten		+	+	+
Virtuelle Maschine –> Bestandsliste	**Aus vorhandener erstellen**		+	+	+
	Neu erstellen		+	+	+
	Registrieren				+
	Entfernen		+	+	+
	Registrierung aufheben				+
Virtuelle Maschine –> Provisioning	**Laufwerkszugriff zulassen**		+	+	+
	Lesezugriff auf Festplatte zulassen	+		+	
	Download virtueller Maschine zulassen	+	+	+	+
Virtuelle Maschine –> Status	**Snapshot erstellen**	+		+	+
	Snapshot entfernen	+		+	+

		Aktion			
Objekt	**Recht**	**Backup einer VM**	**Recovery zu einer neuen VM**	**Recovery zu einer existierenden VM**	**VM von Backup ausführen**
vApp	**Virtuelle Maschine hinzufügen**				+

* Diese Berechtigung ist nur zum Backup von verschlüsselten Maschinen erforderlich.

** Diese Berechtigung ist nur für applikationskonforme Backups erforderlich.

19.7 Virtuelle Windows Azure- und Amazon EC2-Maschinen

Um eine virtuelle Windows Azure- oder Amazon EC2-Maschine sichern zu können, müssen Sie einen Backup Agenten auf der entsprechenden Maschine installieren. Backup- und Recovery-Aktionen werden hier genauso wie bei physischen Maschinen durchgeführt. Davon unabhängig wird die Maschine jedoch als virtuelle Maschine gezählt, wenn Sie Quotas für eine bestimmte Anzahl von Maschinen festlegen.

Der Unterschied zu einer physischen Maschine ist, dass virtuelle Windows Azure- und Amazon EC2-Maschinen nicht mit einem Boot-Medium gebootet werden können. Wenn Sie bei einer Wiederherstellung eine neue virtuelle Windows Azure- und Amazon EC2-Maschine als Ziel verwenden wollen, gehen Sie wie nachfolgend beschrieben vor.

So stellen Sie eine Maschine als virtuelle Windows Azure- oder Amazon EC2-Maschine wieder her

1. Erstellen Sie in Windows Azure oder Amazon EC2 eine neue virtuelle Maschine von einem Image/Template. Die neue Maschine muss dieselbe Laufwerkskonfiguration wie die Maschine haben, die Sie wiederherstellen wollen.
2. Installieren Sie den Agenten für Windows oder den Agenten für Linux auf der neuen Maschine.
3. Stellen Sie die Maschine aus dem Backup nach der Anleitung im Abschnitt 'Physische Maschine (S. 85)' wieder her. Wählen Sie die neue Maschine als Zielmaschine aus, wenn Sie die Wiederherstellung konfigurieren.

19.8 Die Gesamtzahl der gleichzeitig gesicherten virtuellen Maschinen begrenzen

Die Backup-Option **Planung** (S. 80) bestimmt, wie viele virtuelle Maschinen ein Agent gleichzeitig sichern kann, wenn er den gegebenen Backup-Plan ausführt.

Wenn sich mehrere Backup-Pläne zeitlich überschneiden, werden die Zahlen, die in deren Backup-Optionen spezifiziert wurden, addiert. Auch wenn die resultierende Gesamtzahl vom Programm auf 10 begrenzt ist, können überlappende Pläne die Backup-Performance beeinträchtigen und sowohl den Host als auch den Storage für die virtuellen Maschinen überlasten.

Sie können die Gesamtzahl der virtuellen Maschinen, die ein Agent für VMware oder Agent für Hyper-V gleichzeitig sichern kann, noch weiter reduzieren.

So können Sie die Gesamtzahl der virtuellen Maschinen begrenzen, die ein Agent für VMware (Windows) oder Agent für Hyper-V gleichzeitig sichern kann

1. Erstellen Sie auf der Maschine, die den Agenten ausführt, ein neues Text-Dokument und öffnen Sie dieses in einem Text-Editor (wie Notepad).
2. Kopieren Sie die nachfolgenden Zeilen und fügen Sie diese dann in die Datei ein:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Ersetzen Sie `00000001` mit dem Hexadezimalwert der Begrenzung, die Sie festlegen wollen. Beispiele: `00000001` ist 1 und `0000000A` ist 10.
4. Speichern Sie das Dokument als Datei mit dem Namen '**proxy.reg**'.
5. Führen Sie die Datei 'als Administrator' aus.
6. Bestätigen Sie, dass Sie die Änderung der Windows Registry wirklich ausführen wollen.
7. Gehen Sie dann folgendermaßen vor, um den Agenten neu zu starten:
   a. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie ein: **cmd**
   b. Klicken Sie auf **OK**.
   c. Führen Sie folgende Befehle aus:

```
net stop mms
net start mms
```

So können Sie die Gesamtzahl der virtuellen Maschinen begrenzen, die der Agent für VMware (Virtuelle Appliance) sichern kann

1. Drücken Sie zum Starten der Eingabeaufforderung die Tastenkombination Strg+Umschalt+F2, während Sie sich in der Benutzeroberfläche der virtuellen Appliance befinden.
2. Öffnen Sie die Datei **/etc/Acronis/MMS.config** in einem Text-Editor (wie **vi**).
3. Suchen Sie den folgenden Abschnitt:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Ersetzen Sie `10` mit dem Dezimalwert der Begrenzung, die Sie festlegen wollen.
5. Speichern Sie die Datei.
6. Führen Sie den Befehl **`reboot`** aus, um den Agenten neu zu starten.

20 Benutzerkonten und Organisationseinheiten (Abteilungen)

Die Verwaltung von Benutzerkonten und Organisationseinheiten (Abteilungen) erfolgt über das Management-Portal. Auf dieses können Sie zugreifen, indem Sie nach der Anmeldung am Backup Service auf **Management-Portal** klicken. Alternativ können Sie in der rechten oberen Ecke auch auf das Symbol  klicken und anschließend auf **Management-Portal**. Nur Benutzer mit administrativen Berechtigungen können auf das Portal zugreifen.

Weitere Informationen über die Verwaltung von Benutzerkonten und Unternehmenseinheiten finden Sie in der Management-Portal-Administrator-Anleitung. Sie können auf dieses Dokument zugreifen, wenn Sie im Management-Portal auf das Fragezeichen-Symbol klicken.

Dieser Abschnitt enthält zusätzliche Informationen zur Verwaltung des Backup Service.

20.1 Quotas

Mit Quotas können Sie einschränken, ob und wie Benutzer den Service verwenden können. Um Quotas festlegen zu können, müssen Sie in der Registerkarte **Benutzer** den gewünschten Benutzer auswählen und anschließend im Bereich **Quotas** auf das Stiftsymbol klicken.

Wenn eine Quota überschritten wird, wird an den Benutzer (bzw. seine E-Mail-Adresse) eine entsprechende Benachrichtigung gesendet. Wenn Sie keine Quota-Überschreitung festlegen, wird die Quota als 'weich' angesehen. Das bedeutet, dass keine Beschränkungen für die Nutzung des Backup Service gelten.

Sie können außerdem Quota-Überschreitungen spezifizieren. Eine Überschreitung erlaubt es dem Benutzer, die Quota um den spezifizierten Wert zu überschreiten. Wird die Überschreitungsgrenze erreicht, werden Nutzungsbeschränkungen auf den Backup Service angewendet.

MSPs (Managed Service Provider) können auf ähnliche Weise außerdem Quotas für ihre Kundenfirmen spezifizieren.

20.1.1 Backup

Sie können die Cloud Storage-Quota, die Quota für lokale Backups und die maximale Anzahl an Maschinen/Geräten/Websites spezifizieren, die ein Benutzer sichern darf. Folgende Quotas sind verfügbar.

Quotas für Geräte

- **Workstations**
- **Server**
- **Virtuelle Maschinen**
- **Mobilgeräte**
- **Webhosting-Server**
- **Websites**

Ein(e) Maschine/Gerät/Website wird als 'geschützt' betrachtet, wenn auf diese(s) mindestens ein Backup-Plan angewendet wird. Ein Mobilgerät wird nach Durchführung des ersten Backups als 'geschützt' betrachtet.

Wenn die Überschreitungsgrenze für eine bestimmte Anzahl von Geräten erreicht ist, kann der Benutzer keinen weiteren Geräten mehr einen Backup-Plan zuweisen.

Quotas für Cloud-Datenquellen

- **Office 365-Arbeitsplätze**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Dem Unternehmen kann es gestattet werden, **Postfächer**, **OneDrive**-Dateien oder beides zu sichern. Firmenadministratoren können die Quota und Nutzungsinformationen im Management-Portal einsehen, jedoch keine Quota für einen Benutzer festlegen.

- **Office 365 SharePoint Online**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Diese Quota (de)aktiviert die Möglichkeit, SharePoint Online-Websites zu sichern. Wenn diese Quota aktiviert ist, können beliebig viele SharePoint Online-Websites gesichert werden. Firmenadministratoren können zwar nicht die Quota im Management-Portal einsehen, aber den Speicherplatz in den Nutzungsberichten einsehen, der von den SharePoint Online-Backups belegt wird.
- **G Suite-Arbeitsplätze**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Der Firma kann es erlaubt werden, **Gmail**-Postfächer (inkl. Kalender und Kontakte), **Google Drive**-Dateien oder beides zu sichern. Firmenadministratoren können die Quota und Nutzungsinformationen im Management-Portal einsehen, jedoch keine Quota für einen Benutzer festlegen.
- **G Suite Team Drive**

  Diese Quota wird vom Service-Provider auf die komplette Firma angewendet. Diese Quota (de)aktiviert die Möglichkeit, G Suite Team Drives zu sichern. Wenn diese Quota aktiviert ist, können beliebig viele Team Drives gesichert werden. Firmenadministratoren können zwar nicht die Quota im Management-Portal einsehen, aber den Speicherplatz in den Nutzungsberichten einsehen, der von den SharePoint Online-Backups belegt wird.

Ein Office 365-Arbeitsplatz gilt als geschützt, solange mindestens ein Backup-Plan auf das Postfach oder OneDrive-Laufwerk des Benutzers oder angewendet wird. Ein G Suite-Arbeitsplatz gilt als geschützt, solange mindestens ein Backup-Plan auf das Postfach oder das Google Drive-Laufwerk des Benutzers angewendet wird.

Wenn die Überschreitungsgrenze für eine bestimmte Anzahl von Arbeitsplätzen erreicht ist, kann ein Firmenadministrator keinen weiteren Arbeitsplätzen mehr einen Backup-Plan zuweisen.

Quotas für Storage

- **Lokales Backup**

  Die Quota '**Lokales Backup**' beschränkt die Gesamtgröße der lokalen Backups, die mithilfe der Cloud-Infrastruktur erstellt werden können. Für diese Quota kann keine Überschreitung festgelegt werden.
- **Cloud-Ressourcen**

  Die Quota **Cloud-Ressourcen** kombiniert die Quota für Backup Storage und die Quotas für Disaster Recovery. Die Backup Storage-Quota begrenzt die Gesamtgröße der Backups, die im Cloud Storage gespeichert sind. Wird die Backup Storage-Quota-Überschreitungsgrenze erreicht, werden weitere Backups fehlschlagen.

20.1.2 Disaster Recovery

Diese Quotas werden vom Service-Provider auf die komplette Firma angewendet. Firmenadministratoren können die Quotas und Nutzungsinformationen im Management-Portal einsehen, jedoch keine Quotas für bestimmte Benutzer festlegen.

- **Disaster Recovery Storage**

  Dieser Storage wird von primären Servern und Recovery-Servern verwendet. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server oder Recovery-Server erstellt oder Laufwerke zu vorhandenen primären Servern hinzufügt/erweitert werden. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, kann kein Failover initiiert oder ein gestoppter Server gestartet werden. Die Ausführung laufender Server wird aber fortgesetzt.

Wenn die Quota deaktiviert wird, werden alle Server gelöscht. Die Registerkarte **Cloud-Recovery-Site** wird nicht mehr in der Backup-Konsole angezeigt.

- **Berechnungspunkte**

  Diese Quote begrenzt die CPU- und RAM-Ressourcen, die die primären Server und Recovery-Server während eines Abrechnungszeitraums verbrauchen dürfen. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, werden alle primären Server und Recovery-Server heruntergefahren. Diese Server können erst wieder verwendet werden, wenn der nächste Abrechnungszeitraum beginnt. Der vorgegebene Abrechnungszeitraum ist ein voller Kalendermonat.

  Wenn die Quota deaktiviert ist, können die Server überhaupt nicht verwendet werden (unabhängig vom Abrechnungszeitraum).

- **Öffentliche IP-Adressen**

  Mit dieser Quota wird die Anzahl der öffentlichen IP-Adressen beschränkt, die primären Servern und Recovery-Servern zugewiesen werden können. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine öffentlichen IP-Adressen mehr für weitere Server aktiviert werden. Sie können einem Server die Verwendung öffentlicher IP-Adressen verbieten, wenn Sie in den Server-Einstellungen das Kontrollkästchen **Öffentliche IP-Adressen** deaktivieren. Anschließend können Sie einem anderen Server die Verwendung einer öffentlichen IP-Adresse (die normalerweise nicht dieselbe ist) erlauben.

  Wenn die Quota deaktiviert wird, hören alle Server auf, öffentliche IP-Adressen zu verwenden, und sind anschließend nicht mehr über das Internet erreichbar.

- **Cloud Server**

  Diese Quota ermöglicht es, die Gesamtzahl der primären Server und Recovery-Server zu beschränken. Wenn die Überschreitungsgrenze für diese Quota erreicht ist, können keine primären Server oder Recovery-Server erstellt werden.

  Wenn die Quota deaktiviert wird, sind die Server zwar noch in der Backup-Konsole sichtbar, aber die einzige auf sie anwendbare Aktion ist **Löschen**.

- **Internetzugriff**

  Diese Quota (de)aktiviert den Internetzugriff für primäre Server und Recovery-Server.

  Wenn die Quota deaktiviert wird, verlieren die primären Server und Recovery-Server sofort ihre Internetverbindung. Der Schalter **Internetzugriff** in den Server-Eigenschaften wird zurückgesetzt und deaktiviert.

20.2 Benachrichtigungen

Um die Benachrichtigungseinstellungen für einen Benutzer ändern zu können, müssen Sie in der Registerkarte **Benutzer** den gewünschten Benutzer auswählen und anschließend im Bereich **Einstellungen** auf das Stiftsymbol klicken. Es stehen folgende Benachrichtigungseinstellungen zur Verfügung:

- **Benachrichtigungen über Quota-Überbenutzung** (standardmäßig aktiviert)

  Die Benachrichtigungen zu überschrittenen Quotas.

- **Geplante Nutzungsberichte**

  Die nachfolgend beschriebenen Nutzungsberichte, die am ersten Tag eines jeden Monats gesendet werden.

- **Benachrichtigungen über Fehler**, **Benachrichtigungen über Warnungen** und **Benachrichtigungen über erfolgreiche Aktionen** (standardmäßig deaktiviert)

Die Benachrichtigungen über die Ausführungsergebnisse von Backup-Plänen und die Ergebnisse von Disaster Recovery-Aktionen für jedes Gerät.

- **Tägliche Zusammenfassung über aktive Alarmmeldungen** (standardmäßig aktiviert)

  Die Zusammenfassung informiert Sie über fehlgeschlagene Backups, verpasste Backups und andere Probleme. Die Zusammenfassung wird um 10:00 Uhr morgens (nach der Zeit des Datacenters) versendet. Wenn zum betreffenden Zeitpunkt keine Probleme vorliegen, wird auch keine Zusammenfassung gesendet.

Alle Benachrichtigungen werden an die E-Mail-Adresse gesendet, die für den entsprechenden Benutzer spezifiziert wurde.

20.3 Nutzungsberichte

Ein Bericht über die Nutzung des Backup Service enthält folgende Daten über eine Firma oder Abteilung:

- Die Größe von Backups pro Abteilung, pro Benutzer, pro Gerätetyp.
- Die Anzahl von geschützten Geräten pro Abteilung, pro Benutzer, pro Gerätetyp.
- Der Preis pro Abteilung, pro Benutzer, pro Gerätetyp.
- Die Gesamtgröße der Backups.
- Die Gesamtzahl der geschützten Geräte.
- Der Gesamtpreis.

21 Problembehebung (Troubleshooting)

Dieser Abschnitt beschreibt, wie Sie ein Agenten-Protokoll (Log) als .zip-Datei speichern können. Falls ein Backup aus unbekannten Gründen fehlschlägt, hilft diese Datei den Mitarbeitern des technischen Supports, das Problem zu identifizieren.

So stellen Sie Logs zusammen

1. Wählen Sie die Maschine aus, deren Protokolle (Logs) Sie sammeln wollen.
2. Klicken Sie auf **Aktivitäten**.
3. Klicken Sie auf **Systeminformationen sammeln**.
4. Spezifizieren Sie bei Aufforderung durch Ihren Webbrowser, wo die Datei gespeichert werden soll.

22 Glossar

B

Backup-Format 'Einzeldatei'

Ein neues Backup-Format, in dem das anfängliche Voll-Backup sowie die nachfolgenden inkrementellen Backups gemeinsam in Form einer einzigen .tib- oder tibx-Datei (statt einer Kette von Dateien) gespeichert werden. Dieses Format nutzt die Geschwindigkeit der inkrementellen Backup-Methode und vermeidet dabei gleichzeitig deren größten Nachteil: das schwierige Löschen veralteter Backups. Die Software kennzeichnet diejenigen Blöcke, die von veralteten Backups verwendet werden, als 'frei' und schreibt neue Backups in diese neuen Blöcke. Dies führt zu einer extrem schnellen Bereinigung, bei gleichzeitig minimalem Ressourcenbeanspruchung.

Das Backup-Format 'Einzeldatei' ist nicht verfügbar, wenn als Backup-Ziel ein Storage (wie beispielsweise ein Bandlaufwerk) verwendet wird, der keine wahlfreien Lese- und Schreib-Zugriffe (Random Access Read and Write) zulässt.

Backup-Set

Eine Gruppe von Backups, auf die eine einzelne Aufbewahrungsregel angewendet werden kann.

Beim Backup-Schema '**Benutzerdefiniert**' entsprechen die Backup-Sets den Backup-Methoden (**Vollständig**, **Differentiell** und **Inkrementell**).

In allen anderen Fällen sind die Backups-Sets **Monatlich**, **Täglich**, **Wöchentlich** und **Stündlich**.

- Ein 'monatliches' Backup ist dasjenige Backup, das als erstes in einem bestimmten Monat erstellt wird.
- Ein 'wöchentliches' Backup ist das erste Backup, welches an demjenigen Wochentag erstellt wird, wie er über die Option **Wöchentliches Backup** festgelegt wurde (klicken Sie auf das Zahnradsymbol und dann auf die Befehle **Backup-Optionen** –> **Wöchentliche Backups**).

  Wenn ein 'wöchentliches' Backup das erste Backup ist, welches seit Anbruch eines Monats erstellt wurde, so wird dieses Backup als 'monatliches' Backup betrachtet. In diesem Fall wird ein wöchentliches Backup an dem ausgewählten Tag der nächsten Woche erstellt.
- Ein 'tägliches' Backup ist das erste Backup, welches seit Anbruch eines Tages erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines 'monatlichen' oder 'wöchentlichen' Backups.
- Ein 'stündliches' Backup ist das erste Backup, welches seit Anbruch einer Stunde erstellt wird – es sei denn, dieses Backup fällt unter die Definition eines 'monatlichen', 'wöchentlichen' oder 'täglichen' Backups.

D

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum letzten vorangegangenen Voll-Backup (S. 207). Sie benötigen den Zugriff auf das entsprechende Voll-Backup, um die Daten aus einem differentiellen Backup wiederherzustellen.

I

Inkrementelles Backup

Ein Backup, das Datenänderungen in Bezug zum letzten Backup speichert. Um Daten von einem inkrementellen Backup wiederherstellen zu können, müssen Sie auch Zugriff auf andere Backups (in derselben Backup-Kette) haben.

V

Voll-Backup

Selbstständiges Backup, das alle Daten enthält, die für die Sicherung gewählt wurden. Sie benötigen kein weiteres Backup, um die Daten aus einem Voll-Backup wiederherzustellen.