Acronis

Acronis Backup 12.5

OPTIMALE VORGEHENSWEISEN
(BEST PRACTICES)

Version: 28.06.2018

Inhaltsverzeichnis

1 Einführung

Über diese Anleitung

Dieses Dokument beschreibt optimale Vorgehensweisen und Empfehlungen für den Einsatz von Acronis Backup in einer Reihe von typischen Umgebungen. Dadurch möchten wir Ihnen helfen, gängige Probleme zu vermeiden, zu denen es im Zusammenhang mit falsch konfigurierten Implementierungen kommen kann.

Die Empfehlungen für jede Umgebung sind in sich abgeschlossen. Sie können also einfach auswählen, welche Empfehlungen am besten zu Ihrem Szenario passt.

Die Empfehlungen zu 'Wiederherstellungen', der Abschnitt 'Sonstige Empfehlungen' und die Anhänge sind nicht für die beschriebenen Umgebungen spezifisch. Sie sollten von jedem, der diese Anleitung verwendet, befolgt werden.

Zielgruppe

Diese Anleitung richtet sich an Backup-Administratoren und andere Berater, die Acronis Backup verwalten.

Die meisten Abschnitte dieser Anleitung setzen voraus, dass Sie bereits praktische Erfahrungen mit Acronis Backup haben, und dienen daher als „erweiterte Bedienungsanleitung“. Das bedeutet, dass Sie unter Umständen die dazugehörigen Grundlageninformationen in der allgemeinen Benutzeranleitung von Acronis Backup nachschlagen müssen.

Die Informationen in dieser Anleitung basieren auf den Erfahrungen von Acronis Spezialisten, die bei der Lösung von Kundenproblemen mit Acronis Backup 12.5 Update 2 (und früheren Versionen) gesammelt wurden. Sie erzielen die besten Ergebnisse, wenn Sie nicht nur einzelnen, sondern allen Empfehlungen folgen, die zu Ihrem Umgebungstyp gehören.

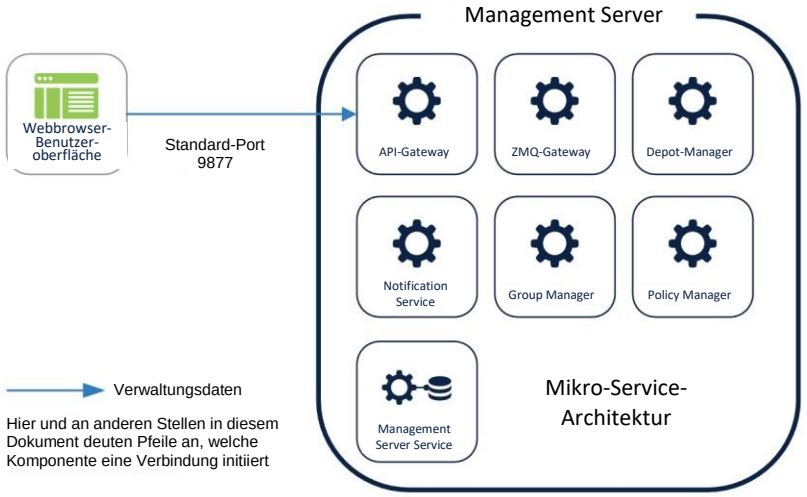
- Einzelne und isolierte Maschinen (S. 11)
- Kleine Umgebungen (S. 21)
- Typische KMUs (S. 35)
- Große Umgebungen (S. 50)

2 Acronis Backup – Komponenten und Architektur

Acronis Backup besteht aus den folgenden installierbaren Komponenten:

Management Server

Der Acronis Management Server besteht aus einer Reihe von Diensten (als Teil von Komponentennamen auch „Services“ genannt), die für die Verwaltung von Acronis Backup und für die Bereitstellung der webbasierten Benutzeroberfläche zuständig sind. Diese Dienste verwalten Agenten, Gruppen und Backup-Pläne, senden Benachrichtigungen, sammeln Daten, erstellen und speichern Berichte etc. Eine vollständige Liste der Dienste und ihrer Funktionen finden Sie im Anhang A (S. 77). Der Management Server wird üblicherweise zuerst installiert und dient dann als Einstiegspunkt in die Verwaltung Ihrer Acronis Backup Infrastruktur. An Backup-, Recovery- oder anderen Aktionen ist er jedoch nicht selbst beteiligt.



Komponenten zur Remote-Installation

Dies ist ein Archiv aller Installationskomponenten, die im vollständigen Installationspaket von Acronis Backup enthalten sind. Sie müssen dies installieren, um vom Acronis Management Server aus die Remote-Bereitstellung von Agenten anstoßen zu können. Wenn Sie keine Remote-Installationsfunktionalität über die Produkt-Benutzeroberfläche benötigen, sollten Sie diese Komponente nicht installieren, um Speicherplatz einzusparen.

Monitoring Service

Diese Komponente stellt Datenzusammenstellungen, die Berichtsdatenbank sowie die Berichts- und Dashboard-Funktionalität im Produkt zur Verfügung. Sie kann derzeit nur als Add-on für den Management Server installiert werden.

Das System sammelt nur dann Überwachungsdaten, wenn dieser Dienst läuft. Wenn Sie den Dienst erst später installieren, ist Ihr Berichtsdatensatz also unvollständig.

Wenn diese Komponente nicht installiert ist, werden die Berichts- und Dashboard-Funktionen in der Produkt-Benutzeroberfläche ausgeblendet.

Backup-Agenten

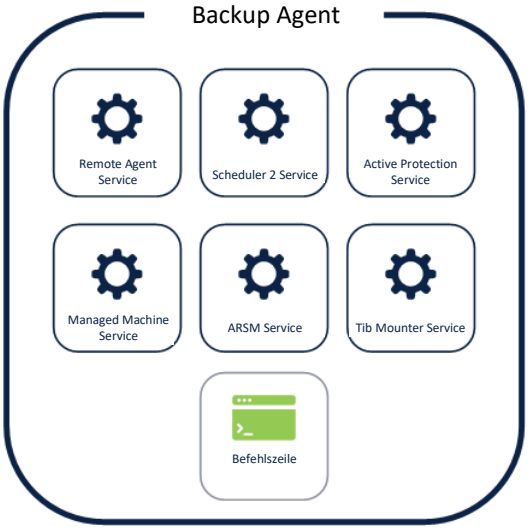
Auch die Acronis Backup Agenten werden als Dienste installiert. Sie sind für die Durchführung von spezifischen Backup-, Wiederherstellungs-, Replikations- und anderen Aufgaben auf den zu sichernden Maschinen verantwortlich. Sie werden normalerweise auf jedem zu sichernden Gerät installiert und werden anschließend auf dem Acronis Management Server hinzugefügt.

Die Acronis Agenten können jedoch komplett unabhängig arbeiten. Sie benötigen keine konstante Kommunikation mit dem Management Server, um ihre planmäßigen Backup-Aktionen durchzuführen. Es ist auch möglich, einen Agenten isoliert zu installieren und dabei ganz auf den Management Server zu verzichten (S. 14). In diesem Fall muss der Agent jedoch über die Kommandozeile verwaltet werden.

Es werden verschiedene Typen von Agenten verwendet, um unterschiedliche Datenquellen zu sichern. Sie verwenden jedoch dieselbe Architektur, Kommunikationsprotokolle und den größten Teil der Funktionalität.

Eine Liste der derzeit verfügbaren Agenten ist weiter unten aufgelistet. Die Liste wird bei jeder neuen Datenquelle erweitert, die Acronis mit zukünftigen Updates unterstützen wird.

- Agent für Windows
- Agent für Linux
- Agent für Mac
- Agent für VMware (Windows)
- Agent für VMware (Virtuelle Appliance)
- Agent für Hyper-V
- Agent für Exchange
- Agent für Office 365
- Agent für Oracle



Bootable Media Builder

Dieses eigenständige, benutzeroberflächenbasierte Tool wird verwendet, um die beiden unterschiedlichen Arten von Acronis Boot-Medien zu erstellen: das standardmäßige Linux-basierte Boot-Medium oder das WinPE-basierte Boot-Medium.

Normalerweise müssen Sie nur eine Instanz dieses Tools auf einer Ihrer Maschinen installieren. Denn auf dieser Maschine erstellte Boot-Medien funktionieren auch auf anderen Maschinen.

Ein Acronis Boot-Medium kann komplett eigenständig verwendet werden und verfügt über eine Backup- und Recovery-Funktionalität, die von einem Agenten bereitgestellt wird, der den weiter oben beschriebenen Agenten sehr ähnlich ist. Mit einem solchen Medium können Sie ein System auch auf fabrikneuer Hardware wiederherstellen. Alles was Sie dazu benötigen, ist das Boot-Medium und die Datei, die das jeweilige Backup enthält.

Backup Monitor

Diese Komponente wird zusammen mit einem Agenten installiert. Sie ermöglicht vom Infobereich der Taskleiste aus oder über die Menüleiste des Betriebssystems eine grundlegende Interaktion mit dem Agenten. Mit dem Backup Monitor können Sie auf der Maschine, auf welcher der Agent installiert ist, ein laufendes Backup direkt überwachen oder stoppen.

Storage Node

Diese Komponente ermöglicht es, einen verwalteten zentralen Speicherort (Storage) zu erstellen und zu verwalten, der von den Agenten dann als Backup-Ziel verwendet werden kann. Ein solcher verwalteter Storage ist notwendig, um Katalogisierungen, Deduplizierungen und zentrale Band-Backups nutzen zu können.

Katalogdienst

Der Catalog Service (auch Katalogdienst genannt) indiziert Ihre Backups, damit Sie in den Backups nach Dateien suchen und diese dann direkt wiederherstellen können. Er ist nur für die Suchfunktion erforderlich, aber nicht, um Dateien an sich wiederherstellen zu können.

PXE Server

Dieser Dienst wird zusammen mit dem Bootable Media Builder verwendet und ermöglicht Ihnen, eine Maschine über das Netzwerk booten zu können.

Architekturüberblick

Acronis Backup 12.5 und Acronis Data Cloud, die Acronis Cloud-Plattform, teilen sich eine gemeinsame Architektur und Code-Basis. Über die Acronis Cloud-Plattform können Service Provider ihren Kunden Backup- und andere Data Protection-Dienste anbieten. In unseren skalierbaren Datenzentren – die derzeit über 100 Petabyte an Daten von Acronis Partnern und Tausenden von Acronis Kunden speichern – laufen also die gleichen Management-Komponenten, die zu Beginn dieses Abschnitts aufgeführt wurden. Der wesentliche Unterschied besteht darin, dass die in der Cloud verwendeten Dienste von einem dedizierten Team auf einem komplexen Server-Netzwerk in unseren Datenzentren bereitgestellt und gewartet werden. Während die Komponenten bei Acronis Backup 12.5 in Form eines einfachen Ein-Klick-Installationspakets bereitgestellt werden.

Der große Cloud-Service-Umfang der Cloud-Plattform hat viele Architekturentscheidungen bestimmt, die Acronis Backup 12.5 zugrunde liegen. Ein Beispiel wäre der Wechsel von monolithischen Diensten mit RPC-Verbindungen in früheren Produkten zu der neuen, flexibleren Mikro-Service-Architektur, bei der Kommunikationen über eine RESTful API erfolgen. Und auch die Entscheidung, für die Konsole eine webbasierte Benutzeroberfläche zu verwenden, wurde getroffen, weil dies gleichzeitig auch die beste Option ist, um eine Benutzeroberfläche für Cloud-Dienste bereitzustellen.

Auch Kunden von Acronis Backup 12.5, die eine lokale Bereitstellung verwenden, profitieren von der neuen Skalierbarkeit und Stabilität auf großem Maßstab. Statt wie früher Hunderte von Endgeräten zu verwalten, kann der neue Management Server nun Tausende von Agenten effektiv verwalten – und das sogar mit relativ bescheidener Hardware.

Das schnelle Wachstum unserer Cloud Services-Plattform erfordert eine ständige Weiterentwicklung der zugrunde liegenden Architektur. Da unsere Cloud-Plattform und Acronis Backup 12.5 auf einer gemeinsamen Architektur beruhen, unterliegen beide auch denselben Änderungen in diesen Bereichen.

Die Änderungen bleiben für den Endanwender transparent. Beachten Sie jedoch, dass diese Anleitung mit jedem größeren Update von Acronis Backup 12.5 aktualisiert wird. Der in Anhang A (S. 77) aufgeführte frühere **Remote Agent** Service wird beispielsweise verworfen.

2.1 Resource Usage Calculator (Ressourcennutzungsrechner)

Als Ergänzung zu dieser Anleitung haben wir einen Ressourcennutzungsrechner (Resource Usage Calculator, vorerst nur in Englisch verfügbar) auf Basis einer Excel-Tabellenkalkulation erstellt. Wir werden in diesem Dokument öfter auf diesen Rechner verweisen. Der Rechner wird Ihnen bei der Hardware-Auslegung für größere Umgebungen helfen. Und außerdem, die Storage-Anforderungen abzuschätzen, die Sie in Bezug auf die von Ihnen festgelegten Aufbewahrungsfristen benötigen – und die Zeit, um die entsprechenden Datenmengen im Netzwerk zu übertragen.

Wir werden den Rechner regelmäßig aktualisieren, wenn entsprechende Kundenrückmeldungen und neuen Daten vorliegen. Sie können die jeweils neueste Version des Rechners unter folgender Adresse finden: https://go.acronis.com/resource-usage-calculator

Wenn Sie den Rechner verwenden wollen, geben Sie zuerst im Tabellenblatt 'About Environment' die Werte ein, die die Größe Ihrer Umgebung beschreiben. Machen Sie dann im Tabellenblatt 'About Backup Policy' Angaben dazu, welchen Backup-Plan, Storage und welches Backup-Fenster Sie verwenden wollen. Überprüfen Sie anschließend die resultierenden Empfehlungen auf den weiteren Tabellenblättern. Wenn Sie sich nicht sicher sind, ob Sie Funktionen wie Katalogisierung oder Deduplizierung verwenden wollen, studieren Sie die zu Ihrer Umgebung gehörenden Empfehlungen durch, die in den nachfolgenden Abschnitten erläutert werden.

2.2 Lizenzierung

2.2.1 Richtlinie

Die Acronis Backup 12.5 Lizenzierungsrichtlinie ist einfach und direkt:

- Es gibt Dauerlizenzen oder Abonnement-Lizenzen.
- Die Lizenzierung bezieht sich jeweils (alternativ) auf die Anzahl der: physischen Maschinen, virtuellen Hosts, Office 365-Postfächer, Cloud-Instanzen.
  - Es sind keine Lizenzen erforderlich, um Komponenten zu installieren.
  - Die Lizenzen werden nach der Installation – entweder automatisch oder manuell – jeweils einem bestimmten Agenten zugewiesen.
  - Eine Lizenz muss zugewiesen werden, um einen neuen Backup-Plan bereitstellen oder einen vorhandenen Backup-Plan ausführen zu können.
- Es gibt zwei Arten von Lizenzen, abhängig von der Produkt-Edition: **Standard** und **Advanced**:
  - **Standard** dient der Sicherung einzelner Maschinen (S. 11) und kleiner Umgebungen (S. 21).
  - **Advanced** enthält eine Reihe von Funktionen zur Sicherung von KMUs (kleine und mittlere Unternehmen) (S. 35) und großen Umgebungen (S. 50).
  - Die Lizenzen werden zudem nach dem Betriebssystem unterteilt, welches Sie verwenden, um eine Lizenz zuzuweisen.
- **Standard-Lizenzen**:
  - Acronis Backup 12.5 Workstation – kann Maschinen zugewiesen werden, die mit einer Desktop-Version von Windows (XP, Vista, 7-10) oder macOS laufen.
  - Acronis Backup 12.5 Server – kann jedem unterstützten Betriebssystem zugewiesen werden.
  - Acronis Backup 12.5 Windows Server Essentials – kann einem Windows Server
  - Essentials oder einem ähnlichen System zugewiesen werden.
  - Acronis Backup 12.5 Virtual Host – kann einem Hypervisor zugewiesen werden, der Ihre VMs ausführt.
  - Acronis Backup 12.5 Office 365 – kann Office 365-Postfächern zugewiesen werden (nur als Abonnement verfügbar).
- **Advanced-Lizenzen**:
  - Acronis Backup 12.5 Advanced Workstation – kann Maschinen zugewiesen werden, die mit einer Desktop-Version von
  - Windows (XP, Vista, 7-10) oder macOS laufen.
  - Acronis Backup 12.5 Advanced Server – kann jedem unterstützten Betriebssystem zugewiesen werden.
  - Acronis Backup 12.5 Advanced Virtual Host – kann einem Hypervisor zugewiesen werden, der Ihre
  - VMs ausführt.
  - Acronis Backup 12.5 Advanced Office 365 – kann Office 365-Postfächern zugewiesen werden
  - (nur als Abonnement verfügbar).
  - Acronis Backup 12.5 Advanced Universal License – kann jedem physischen Host oder Hypervisor zugewiesen werden (nur als Dauerlizenz verfügbar).
- Cloud-Speicherplatz in den Acronis Datenzentren ist Abonnement-basiert und wird separat lizenziert.

2.2.2 Lizenz Server

Jede Management Server-Installation enthält einen Lizenz Server. Diese Komponente speichert die Lizenzen in eigenen verschlüsselten Dateien und überprüft regelmäßig die Zuweisung und Gültigkeit der Lizenzen, die dem LizenzServer hinzugefügt wurden. Lizenzen werden nach einer Installation hinzugefügt. Das bedeutet, dass sich die Installationsdatei und der Installationsprozess bei unterschiedlichen Lizenzen nicht ändern. Es ist derzeit noch nicht möglich, einen einzelnen Lizenz Server für mehrere Management Server zu registrieren. Diese Funktionalität wird aber in einer zukünftigen Versionen von Acronis Backup verfügbar sein.

Wenn eine Maschine einem Management Server hinzugefügt wird, wird die Maschine immer über den entsprechenden Lizenz Server lizenziert. Jedes Mal, wenn ein Agent online geht (mindestens aber einmal täglich), wird die Lizenz-Zuweisung für jeden Agenten, der auf dem Management Server registriert ist, überprüft und erneuert.

Wenn diese Überprüfung 30 Tage lang fehlschlägt (z.B., weil die Maschine an einem externen Ort war und sich in dieser Zeit nicht mit dem Management Server verbinden konnte), deaktiviert der Agent die Backup-Funktionalität für diese Maschine.

Wenn Sie isolierte Maschinen verwenden, die mit keinem Management Server verbunden sind, kann der Agent dennoch separat über die Befehlszeile lizenziert werden (S. 14). In diesem Fall muss die Maschine über die Befehlszeile auch verwaltet werden, da die Benutzeroberfläche ein Funktionsbestandteil des Management Servers ist.

Ein Agent kann nicht „selbst-lizenziert“ sein und gleichzeitig durch den Management Server verwaltet werden.

2.2.3 Standard- und Advanced-Lizenzen auf einem Management Server verwenden

Die gleichzeitige Verwendung von Standard- und Advanced-Lizenzen auf einer einzigen Management Server-Installation wird von uns nicht empfohlen.

Es ist zwar technisch möglich, Standard- und Advanced-Lizenzen auf ein und demselben Management Server hinzuzufügen, aber die Benutzererfahrung ist nicht für dieses Szenario optimiert. Denn es kann passieren, dass Sie unwissentlich Backup-Pläne erstellen können, die dann bei der Ausführung aufgrund fehlender Lizenzen fehlschlagen.

Sie sollten Standard-Lizenzen verwenden, wenn Sie bis zu fünf Maschinen haben und keine Advanced-Funktionalität (https://www.acronis.com/de-de/business/overview/compare-products/) benötigen.

Verwenden Sie Advanced-Lizenzen, wenn Sie eine größere Umgebung haben oder erweiterte Funktionen wie „Backup auf Bänder“ oder „Prozessauslagerungen auf andere Hosts“ benötigen.

3 Einzelne und isolierte Maschinen

Beschreibung der Umgebung

Eine „Einzelmaschinen-Installation“ ist eine Installation, bei der die Verwaltung lokal erfolgt – also auf derselben Maschine, die auch per Backup gesichert wird. Dieses Szenario trifft zu, wenn Sie nur eine einzige Maschine sichern wollen. Auch bei größeren Umgebungen, die nur aus isolierten Maschinen bestehen, welche nicht remote verwaltet werden können.

Wenn Sie die Benutzeroberfläche der Webkonsole verwenden wollen, um die Backups auf der Maschine lokal zu verwalten, muss der Management Server zusammen mit dem Agenten auf derselben Maschine installiert werden. In diesem Fall kann eine isolierte Maschine unter Linux oder Windows laufen. Aber nicht unter macOS, weil für den Mac keine Management-Komponenten verfügbar sind.

Eine weitere Option besteht darin, diese Maschine über unseren Management Server in der Cloud zu verwalten. Dafür benötigt die Maschine jedoch eine Internetverbindung, was nicht immer der Fall ist.

Als letzte Option kann eine einzelne Maschine auch allein über die Befehlszeile verwaltet werden. Bei diesem Szenario müssen weder Management-Komponenten installiert werden, noch ist eine Netzwerkverbindung erforderlich. Dafür steht Ihnen keine Benutzeroberfläche zur Verwaltung Ihrer Backups zur Verfügung. Und auch die übrige Verwaltung muss über Skripte und die Befehlszeile erfolgen.

Diese Option ist nur für Maschinen mit Dauerlizenzen verfügbar, da Sie einer einzelnen isolierten Maschine über die Befehlszeile keine Abonnement-Lizenz zuweisen können.

3.1 Vorbereitungen für die Bereitstellung

Dieser Abschnitt behandelt die Anforderungen und Empfehlungen, die bei einer Bereitstellung von Acronis Backup 12.5 für Umgebungen mit einzelnen oder isolierten Maschinen beachtet werden müssen.

3.1.1 Software-Anforderungen für einzelne und isolierte Maschinen

Neben der Voraussetzung, dass Ihr System unterstützt werden muss, gibt es keine weiteren speziellen Anforderungen.

Die vollständigen Systemanforderungen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#36626.html.

Wenn Sie Ihre einzelne Maschine vom Betriebssystem aus verwalten, sollten Sie sicherstellen, dass Sie die Anforderungen des Management Servers einhalten, die die Anforderungen des Agenten übersteigen. Beispielsweise wird der Mac für die Management Server-Komponenten nicht unterstützt.

Wenn Sie die Maschine nur über die Befehlszeile verwalten wollen, befolgen Sie den Abschnitt über den Agenten https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#36983.html.

3.1.2 Hardware-Anforderungen und Dimensionierung

Die minimalen Hardware-Anforderungen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#36552.html.

Beachten Sie: wenn Sie die lokale Verwaltung über den Management Server durchführen wollen, müssen Sie die Anforderungen des Agenten um die des Management Server erweitern (da letztere höher sind).

3.1.3 Bereitstellungstyp

Die Bereitstellungsempfehlungen für die Sicherung einer einzelnen Maschine versus einer isolierten Maschine (eine Maschine, die keinen Internet- oder LAN-Anschluss hat) unterscheiden sich.

3.1.3.1 Einzelne verbundene Maschine

Wenn die Maschine eine Internetverbindung hat, empfehlen wir, das Cloud-Bereitstellungsmodell zu verwenden. Denn dies ist die einfachste Möglichkeit, ein Backup zu erstellen. In diesem Fall wird die Benutzeroberfläche und die Verwaltung von den Management Server-Komponenten bereitgestellt, die in den Acronis Datenzentren installiert sind. Das erspart Ihnen die Notwendigkeit, die Komponenten selbst installieren zu müssen. Ihre einzelne Maschine wird über das Internet mit dem Management Server in der Cloud in Verbindung treten.

Beachten Sie aber, dass einige der erweiterten Funktionen von Acronis Backup 12.5 derzeit beim Cloud-Bereitstellungsmodell noch nicht verfügbar sind. Die Verfügbarkeit für Cloud-Bereitstellungen erfolgt in zukünftigen Produktversionen. Eine vollständige Liste mit allen Funktionen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#38760.html.

Wenn Sie eine dieser erweiterten Funktionen oder eine direktere Kontrolle über die Management-Komponenten benötigen, müssen Sie diese zusammen mit dem Backup Agenten installieren.

Wenn die Ressourcen dieser Maschine nur sehr begrenzt sind, können Sie auf die Verwaltungsoberfläche auch verzichten. Installieren Sie stattdessen einfach nur den Agenten und verwenden Sie die Befehlszeile, um Backups über Skripte zu erstellen.

3.1.3.2 Isolierte Maschinen

Wenn Sie mehrere isolierte Maschinen sichern wollen, die nicht mit dem Internet oder untereinander verbunden werden können, empfehlen wir, dass Sie nur den Agenten installieren und dann dessen Befehlszeilenschnittstelle verwenden, um die Verwaltung durchzuführen.

Dieser Ansatz hat den Vorteil, dass Sie dasselbe Skript auf allen Maschinen verwenden können, um den Backup-Prozess zu automatisieren – statt jede Maschine einzeln über die Benutzeroberfläche des jeweiligen Agenten verwalten zu müssen.

Eine Beschreibung der verfügbaren Befehle finden Sie in der Befehlszeilenreferenz https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5_Command_Line_Reference/index.html#37072.html.

Sie können natürlich auch auf jeder isolierten Maschine den vollständigen Management Server installieren. Dies ist angebracht, wenn jede Maschine direkt von ihrem Benutzer verwaltet werden soll oder wenn Ihnen die Nutzung der Befehlszeile nicht zusagt.

3.2 Komponenten und Installation

3.2.1 Management-Komponenten

Installieren Sie die Management-Komponenten nur, wenn Sie Ihre einzelne Maschine mit einer webbasierten Benutzeroberfläche verwalten wollen, die auf derselben Maschine läuft.

In diesem Fall empfehlen wir Ihnen, folgende Komponenten zu installieren:

- **Management Server** – wird zur Darstellung der Benutzeroberfläche benötigt.

- **Bootable Media Builder** – muss auf mindestens einer Maschine in Ihrer Umgebung installiert werden, damit Sie eine Notfallwiederherstellung (Disaster Recovery) durchführen können, wenn das System der Maschine nicht mehr bootfähig ist.

Die unteren Komponenten werden für diesen Umgebungstyp nicht empfohlen.

- **Monitoring Service**
  Diese Komponente ermöglicht Dashboards und Berichte in der Benutzeroberfläche des Management Servers. Zwar sind Echtzeit-Dashboards und planbare Berichte bei der Verwaltung größerer Umgebungen unverzichtbar, bei einer einzelnen Maschine sind sie jedoch nicht erforderlich.
- **Komponenten zur Remote-Installation** (nur für Windows)
  Mit dieser Komponente können Sie die Remote-Installation von Windows-Agenten von der Benutzeroberfläche des Produkts aus anstoßen. Diese Funktion ist nicht relevant, wenn Sie eine einzelne Maschine verwenden.
- **Acronis Storage Node**
  Diese Komponente wird nur verwendet, wenn Sie eine größere Menge von Maschinen per Backup zu einem einzelnen, zentralen Storage sichern wollen. Bei einer einzelnen Maschine wird sie nicht verwendet.
- **Catalog Service (Katalogdienst)**
  Diese Funktion wird nur im Zusammenhang mit einem Storage Node verwendet und dient dazu, darüber verwaltete Backups durchsuchen zu können.

3.2.2 Backup Agenten

Backup Agenten müssen auf jeder Maschine installiert werden, die Sie mit einer Data Protection-Funktion schützen wollen.

Anweisungen zur Installation der verschiedenen Agenten finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#36415.html.

Der Backup Agent allein reicht aus, um alle Backup- und Recovery-Aktionen durchzuführen (sofern Sie ihn verwalten können).

Die Verwaltung kann über die Befehlszeile erfolgen, die immer zusammen mit einem Agenten installiert wird.

3.2.3 Empfohlene Installationsprozedur

Ausführliche Installationsanweisungen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#36428.html.

Bei einer Installation unter Linux sollten Sie sicherstellen, dass zuvor auf der Maschine alle erforderlichen Linux-Pakete installiert wurden – siehe: https://www.acronis.com/de-de/support/documentation/AcronisBackup_11.7/#22619.html.

3.2.3.1 Verwaltung über die Benutzeroberfläche

Nachfolgend finden Sie unsere Empfehlungen, wenn Sie den Agenten über die Webkonsole verwalten wollen:

1. Registrieren Sie Ihr Produkt in Ihrem Acronis Konto. Ausführliche Anweisungen dazu finden Sie hier: https://kb.acronis.com/content/4834
2. Laden Sie die vollständige Installationsdatei herunter, die für Ihr jeweiliges Betriebssystem (Windows oder Linux) passend ist. Sie können die Dateien immer direkt aus Ihrem Konto herunterladen, nachdem Sie die Registrierung durchgeführt haben.
3. Installieren Sie den Acronis Management Server, den Backup Agent und den Bootable Media Builder auf der Maschine.
4. Importieren Sie die Lizenz und weisen Sie diese zu.
5. Konfigurieren Sie Ihre Speicherorte (Storages).
6. Konfigurieren Sie Ihre Backup-Pläne und wenden Sie diese an.

3.2.3.2 Verwaltung über die Befehlszeile

Nachfolgend finden Sie unsere Empfehlungen, wenn Sie die Befehlszeile zur Verwaltung verwenden wollen.

1. Registrieren Sie Ihr Produkt in Ihrem Acronis Konto. Ausführliche Anweisungen dazu finden Sie hier: https://kb.acronis.com/content/4834
2. Laden Sie die vollständige Installationsdatei herunter, die für Ihr jeweiliges Betriebssystem (Windows oder Linux) passend ist. Sie können die Dateien immer direkt aus Ihrem Konto herunterladen, nachdem Sie die Registrierung durchgeführt haben.
3. Starten Sie die Installationsdatei, indem Sie den Parameter '**`--skip-registration`**' verwenden.
4. Wählen Sie den Backup Agenten für die Installation und optional den Bootable Media Builder (sofern Sie letzteren noch auf keiner anderen Maschine installiert haben).
5. Weisen Sie dem Agenten mit dem Befehl '**`acrocmd add license --key=<LIZENZSCHLÜSSEL>`**' eine Lizenz zu.
6. Erstellen Sie mithilfe der Befehlszeile Ihre Backups.

3.3 Backup-Plan-Empfehlungen

3.3.1 Backup-Quelle

In der Regel werden Sie wohl komplette Maschinen sichern – und dabei bestimmte Ausschlussregeln verwenden, damit keine unerwünschten Dateien in das Backup aufgenommen werden.

Sie können Laufwerke (Partitionen), einzelne Dateien und Ordner oder Dateikategorien anhand von Dateierweiterungen ausschließen. Beispielsweise können Sie bei der Sicherung eines Notebooks oder Desktop-Rechners alle .avi-Dateien vom Backup ausschließen.

Für unterschiedliche Backup-Quellen sind jeweils unterschiedliche Backup-Pläne erforderlich (zumindest je einer für jede unterschiedliche Art von Backup-Quelle).

Beispiel: wenn Sie monatlich ein Backup Ihrer kompletten Maschine erstellen wollen und täglich ein Backup Ihrer wichtigsten Dateien, dann benötigen Sie auf dieser Maschine zwei separate Backup-Pläne.

3.3.2 Backup-Ziel

Für einzelne Maschinen gibt es üblicherweise zwei wesentliche Speicheroptionen:

- Sie können alle Backups direkt auf der Maschine selbst speichern. Beispielsweise kann jede Maschine ihr Volume C:\ (Quelle) auf ihrem Laufwerk D:\ (Ziel) speichern – oder auf einem angeschlossenen USB-Laufwerk.
- Sie können alle Backups im Netzwerk speichern. Wir empfehlen ein handelsübliches NAS-Gerät oder eine Netzwerkfreigabe. In beiden Fällen sollte der bereitgestellte Speicherplatz ausreichend sein, um Ihre Backup-Daten über die erforderliche Aufbewahrungsdauer aufnehmen zu können. Nutzen Sie den Ressourcennutzungsrechner (S. 8), um die ungefähre Backup-Größe unter Berücksichtigung Ihrer Umgebung und Aufbewahrungsfristen zu berechnen.

3.3.3 Planung

Die empfohlene Backup-Planung hängt üblicherweise von der Datenmenge auf Ihren zu sichernden Geräten und den vorgegebenen RPO-Zielen (Recovery Point Objective) ab. Solange das aktuell ausgeführte Backup genügend Zeit zur Fertigstellung hat, bevor das nächste Backup startet, sollten Sie keine Probleme haben.

Allerdings nimmt ein Backup eine beträchtliche Menge an Ressourcen von der zu sichernden Maschine in Anspruch, was laufende Produktions-Workloads beeinflussen kann (insbesondere wenn die Belastung hoch ist).

Unsere Erfahrung zeigt, dass eine gute, allgemein empfehlenswerte Planung darin besteht, jeden Tag zur Nachtzeit (nach Betriebsschluss) ein inkrementelles Backup durchzuführen – und über das Wochenende ein Voll-Backup.

Es wird allgemein empfohlen, weitere Tasks (wie Replikation oder Validierung) ebenfalls für das Wochenende zu planen – sofern nach Abschluss der Backups dafür noch genügend Zeit vorhanden ist.

3.3.4 Aufbewahrungszeiten

Aufbewahrungsfristen basieren oft auf externen Richtlinien oder Compliance-Regeln. Sie können die zu erwartende Größe der Backups für die Aufbewahrungsdauer mithilfe des Ressourcennutzungsrechners (S. 8) abschätzen.

Wenn der als primäres Backup-Ziel verwendete Storage nicht genügend groß sein sollte, können Sie spezielle Replikationstasks planen, um die Daten zur Langzeitaufbewahrung auf einen anderen, billigeren Storage zu verschieben.

Sie können Ihre Backups beispielsweise in die Acronis Cloud replizieren oder einen Band-basierten Storage zur Langzeitaufbewahrung verwenden.

3.3.5 Replikation, Konvertierung und Validierung

Wenn die Größe der zu sichernden Daten es zulässt, dass Sie zusätzlich zum Backup-Task noch weitere Datenverarbeitungsaufgaben in das Backup-Fenster einbinden, sollten Sie diese Optionen ebenfalls direkt im Backup-Plan konfigurieren.

Wenn die Datenmenge zu groß ist und nur das Backup in das Backup-Fenster passt, sollten Sie separate Pläne erstellen, die Aufgaben wie Replikation oder Validierung außerhalb der Stoßzeiten (wie am Wochenende) durchführen.

3.3.6 Weitere Empfehlungen

Benachrichtigungen, Alarmmeldungen und Berichte

Der empfohlene Weg, den Status Ihrer Backups mit minimalem Aufwand zu verwalten, besteht darin, folgende Benachrichtigungen festzulegen:

- Aktivieren Sie das Kontrollkästchen **Tägliche Zusammenfassung über aktive Alarmmeldungen** in den Benachrichtigungseinstellungen
- Bestimmen Sie, zu welcher Zeit Sie die Benachrichtigungen bevorzugt überprüfen wollen. Die Standardvorgabe ist 10:00 Uhr.
- Deaktivieren Sie alle anderen Kontrollkästchen.

Diese Einstellung bedeutet, dass Sie täglich eine einzige E-Mail erhalten, die dann leicht und schnell zu überprüfen ist. Wenn alles in Ordnung ist, erhalten Sie eine E-Mail, die diese Einstellung explizit bestätigt. Wenn es beispielsweise in der zurückliegenden Nacht Probleme mit Ihren Backups gegeben hat, erhalten Sie eine Liste mit Warnmeldungen, in der das/die Problem(e) klar angegeben sind.

Wenn Sie noch mehr Kontrolle wollen, können Sie einzelne Alarmbenachrichtigungen für kritische Benachrichtigungen konfigurieren. Dadurch können Sie sicherstellen, dass Sie direkt eine E-Mail erhalten, sobald auf Ihrer Maschine ein Problem auftritt.

Beachten Sie, dass Alarmbenachrichtigungen standardmäßig gesendet werden, sobald ein Alarm aktiviert wird. Jeder Alarm auf jedem Agenten für jeden Plan generiert eine E-Mail.

Dateiformat

Verwenden Sie wann immer möglich das Standard-Backup-Format 'Version 12'.
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#38763.html.

Active Protection

Active Protection ist derzeit nur für Maschinen mit Windows 7 (und höher) sowie Windows Server 2008 R2 (und höher) verfügbar. Der Agent für Windows muss auf der Maschine installiert sein.

Wir empfehlen, Active Protection auf allen Maschinen zu aktivieren, sofern diese nicht unter zu knappen CPU-Ressourcen leiden.

Bei starken Dateizugriffen bewirkt Active Protection üblicherweise einen CPU-Overhead von einigen wenigen CPU-Prozenten im System.

3.4 Überlegungen in puncto Storage

NAS

Die einfachste Storage-Lösung für einzelne Maschinen ist ein NAS-Gerät oder ähnliche Netzwerkfreigaben, wo die Backups aller Maschinen in der Umgebung gespeichert werden.
Sie müssen dabei insbesondere beachten, dass auf dem zugrundeliegenden Storage-Gerät genügend Speicherplatz vorhanden ist. Sie können den Ressourcennutzungsrechner (S. 8) verwenden, um die benötigte Speicherplatzgröße einzuschätzen. Der empfohlene minimale Speicherplatz berechnet sich aus der Größe aller Backups (für Ihre Aufbewahrungszeit) + der Größe eines Voll-Backups von allen Maschinen.

USB- oder internes Laufwerk

Eine weitere empfehlenswerte Storage-Option besteht darin, jede Maschine ihre Backups zu einem externen USB-Laufwerk oder einem speziellen internen Backup-Laufwerk erstellen zu lassen.

Externer Storage (Offsite-Storage)

Es ist besonders wichtig, dass Sie mindestens eine Kopie Ihrer Daten an einem externen Ort (Offsite-Storage) vorliegen haben. Wir empfehlen die Verwendung der Replikationsfunktion, um eine solche Offsite-Kopie in Ihrem eigenen Acronis Cloud Storage zu speichern. Ihre Offsite-Backups werden dabei in einem unserer sicheren Datenzentren gespeichert, welches sich in Ihrem Land/Ihrer Region befindet.

Dies ist die einfachste Möglichkeit, um Ihre Daten sicher in einem Offsite-Storage zu speichern. Aufgrund beschränkter Internet-Upload-Bandbreiten, Compliance-Gründen, Kostenerwägungen usw. ist die Option aber wohl nicht für jeden passend.

In diesem Fall empfehlen wir, die Backups zuerst zu einem externen USB-Laufwerk oder Bandlaufwerk zu replizieren. Und die entsprechenden Speichermedien dann regelmäßig an einem sicheren externen Ort zu hinterlegen.

3.4.1 Wechsellaufwerke

In kleineren Umgebungen ist es oft üblich, Backups auf externen Wechsellaufwerken erstellen zu lassen und die entsprechenden Speichermedien regelmäßig auszutauschen.

Dies funktioniert mit Acronis Backup 12.5 nicht sofort „out of the box“, weil wir die Backup-Metadaten immer direkt in den Backups selbst speichern. Denn dieser Ansatz bietet den großen Vorteil, dass Ihre Backups damit komplett portabel sind: Sie können ein Backup beispielsweise auf einem USB-Stick speichern, durch die ganze Welt zu einem komplett anderen Ort versenden und dort wiederherstellen, ohne dass Sie etwas über die ursprüngliche Umgebung wissen müssen.

Ohne einen speziellen Mechanismus, der die wichtigen Metadaten zwischen verschiedenen Wechseldatenträgern synchronisiert, verursacht ein Backup-Plan, der einen solchen Storage-Typ als Ziel verwendet, eine Vielzahl von Problemen bei der Backup-Erstellung und -Aufbewahrung. Ein solcher Mechanismus ist aber für zukünftige Updates geplant.

Eine derzeit schon funktionierende Methode für dieses Szenario ist in unserer Knowledge Base (unter https://kb.acronis.com/content/58372) beschrieben.
Diese Methode ist eher eine Zwischen- als eine ideale Lösung. Aber bis wir Wechsellaufwerke mit dem beschriebenen Mechanismus unterstützen, ist es die beste Möglichkeit.

3.4.2 Bandgeräte

Acronis ist bestrebt, die Unterstützung für Bandgeräte fortzusetzen und auszuweiten.

Eine Liste von getesteten und unterstützten Bandgeräten finden Sie in der Hardware-Kompatibilitätsliste für Bandlaufwerke
(https://go.acronis.com/acronis-backup-advanced-tape-hcl).

Wenn Sie die Kompatibilität Ihres eigenen Bandgerätes testen wollen, können Sie das Bandkompatibilitätstool verwenden
(https://kb.acronis.com/content/57237).

Wenn das Tool ein Problem findet, kontaktieren Sie bitte den Acronis Support, damit das Problem zu unserer Entwicklungsabteilung weitergeleitet und gelöst werden kann.

Ein Agent kann Backups direkt zu einem Bandlaufwerk erstellen. Wenn Sie eine einzelne oder isolierte Maschine haben und Band-Backups erstellen wollen, müssen Sie das Bandlaufwerk direkt an der Maschine anschließen, auf welcher der Agent installiert ist.

3.4.2.1 Bandverwaltungsdatenbank

Die Informationen über alle Bandgeräte, Bänder und Backup-Inhalte werden in der Bandverwaltungsdatenbank gespeichert, die sich wiederum auf der Maschine befindet, an welcher das Bandgerät angeschlossen ist.

Der Standardpfad für die Datenbank ist:

- Windows 7, Windows Server 2008 und höher:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database
- Linux:
  /var/lib/Acronis/BackupAndRecovery/ARSM/Database

Die Datenbankgröße hängt von der Zahl der auf den Bändern gespeicherten Backups ab – wobei etwa 10 MB auf einhundert Backups kommen. Mit einigen wenigen Maschinen ist dies –auch mit längeren Aufbewahrungszeiten – kein Problem.

Sie sollten jedoch sicherstellen, dass Sie genügend Speicherplatz für diese Datenbank auf Ihrem System haben. Falls Sie unsicher sind, sollten Sie vor dem Start des ersten Band-Backups den Pfad entsprechend überprüfen.

So verlagern Sie die Datenbank unter Windows:

1. Stoppen Sie den Dienst '**Removable Storage Management**'.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Ermitteln Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings**.
4. Spezifizieren Sie den Pfad zum neuen Speicherort im Registry-Wert `ArsmDmlDbProtocol`. Der String darf bis zu 32765 Zeichen enthalten.
5. Starten Sie den Dienst '**Removable Storage Management**' wieder.

So verlagern Sie die Datenbank unter Linux:

1. Stoppen Sie den Dienst '**acronis_rsm**'.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Öffnen Sie die Konfigurationsdatei **/etc/Acronis/ARSM.config** in einem Text-Editor.
4. Suchen Sie nach folgender Zeile: `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Ändern Sie den Pfad unter dieser Ziele.
6. Speichern Sie die Datei.
7. Starten Sie den Dienst '**acronis_rsm**' wieder.

Sie dürfen die Band-Datenbank nicht löschen! Denn dies würde erfordern, dass all Bänder erneut gescannt werden müssen, um die darauf gespeicherten Backups wieder verwendbar zu machen. Und dies ist ein sehr zweitaufwendiger und fehleranfälliger Prozess.

3.4.2.2 Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren

Diese Option ist standardmäßig deaktiviert. Wenn Sie diese Option in den Bandverwaltungseinstellungen Ihres Backup-Plans aktivieren, können Sie aus Image-Backups, die auf Ihren Bändern gespeichert sind, auch einzelne Dateien wiederherstellen.

Beachten Sie, dass Sie sich diese Funktionalität mit hohen Speicherplatzkosten erkaufen. Wenn die Funktionalität aktiviert ist, erstellt die Software bei jedem Backup zusätzliche Dateien auf einem Festplattenlaufwerk der Maschine, an der das Bandgerät angeschlossen ist. Datei-Recovery von Laufwerk-Backups ist möglich, solange diese zusätzlichen Dateien intakt sind. Die Dateien werden automatisch gelöscht, wenn das Band, auf dem die entsprechenden Backups gespeichert sind, gelöscht, entfernt oder überschrieben wird.

Diese zusätzlichen Dateien befinden sich an diesem Speicherort:

- In Windows 7, Windows Server 2008 und höher:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation
- In Linux:
  /var/lib/Acronis/BackupAndRecovery/TapeLocation

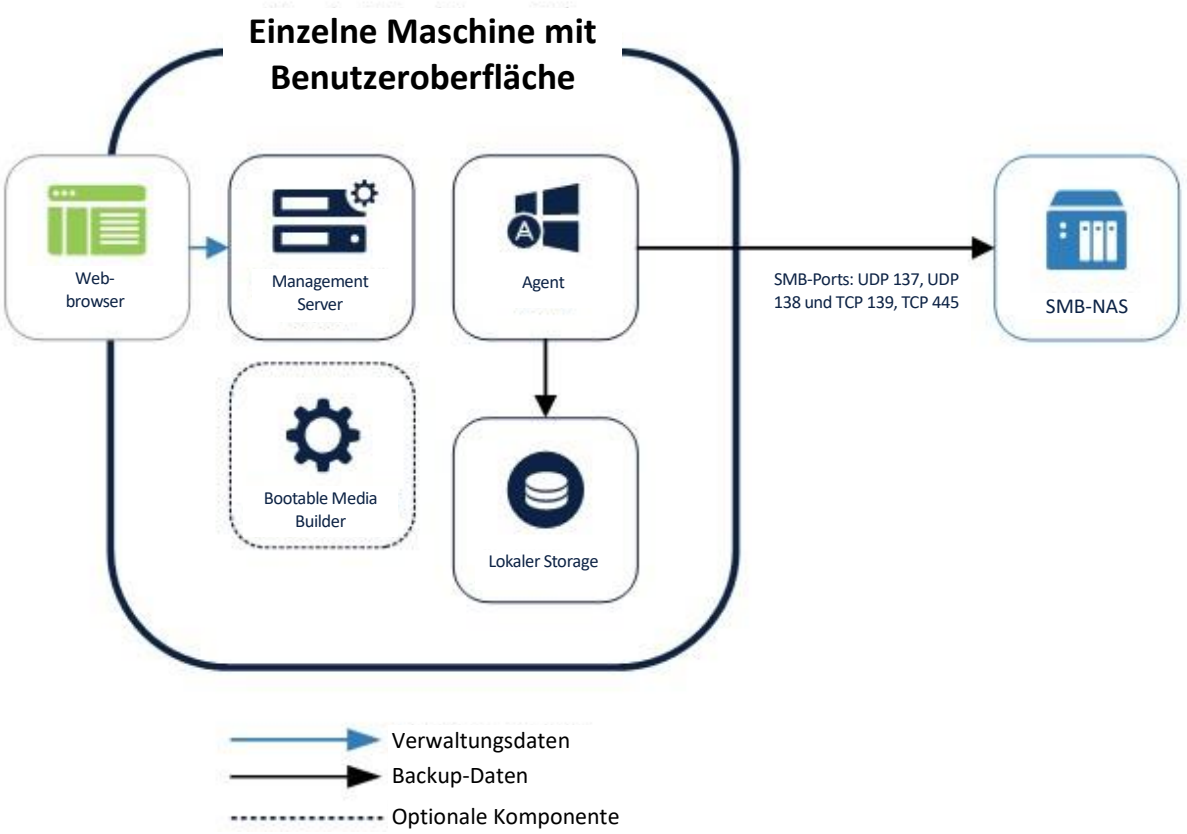
Der von diesen zusätzlichen Dateien belegte Speicherplatz hängt von der Anzahl der Dateien im entsprechenden Backup ab. Beim Voll-Backup eines Laufwerks mit ungefähr 20.000 Dateien (typisches Laufwerk-Backup einer Workstation) belegen die zusätzlichen Dateien ca. 150 MB. Ein einzelnes Voll-Backup eines Servers mit 250.000 Dateien kann etwa 700 MB an zusätzlichen Dateien erzeugen.

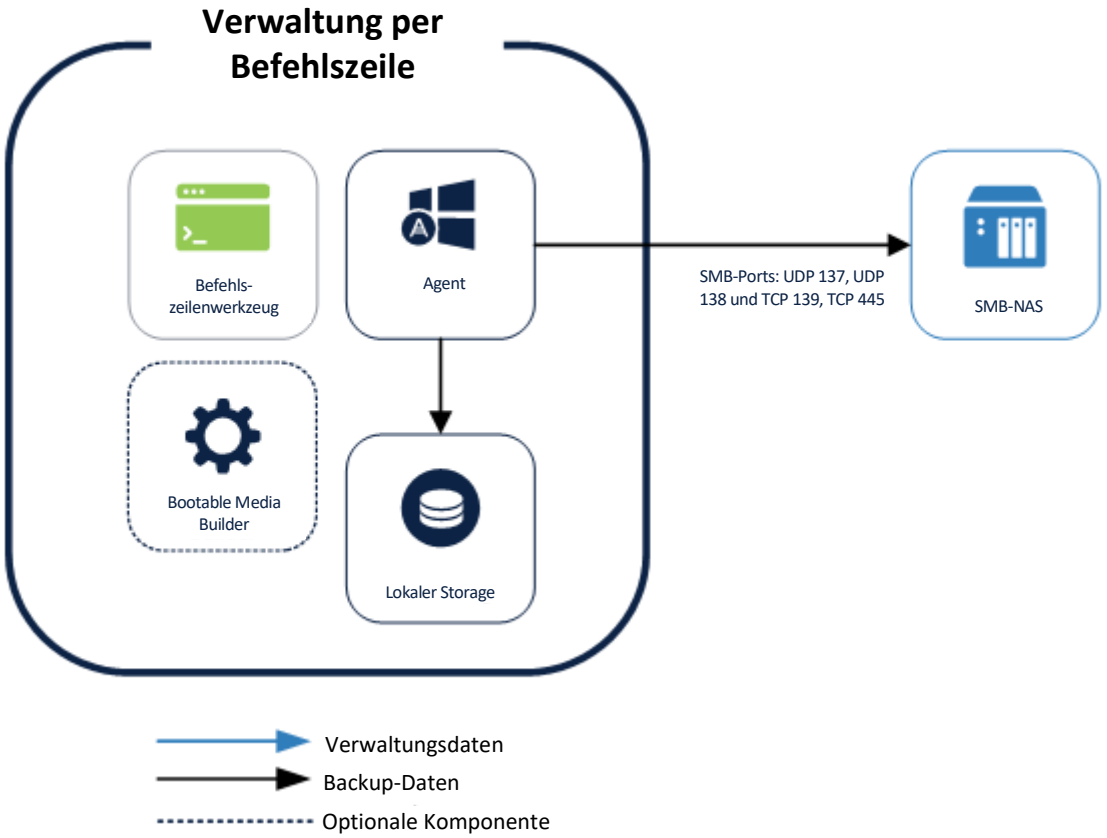
Auch in kleinen Umgebungen kann die Größe dieser Dateien schnell auf Dutzende von Gigabyte anwachsen.

Wir empfohlen daher, dass Sie diese Option deaktiviert lassen, wenn Sie die Option nicht unbedingt benötigen. Wenn doch, sollten Sie sicherstellen, dass der verwendete Speicherort oder Storage Node von der Speicherplatzgröße auf diese zusätzlichen Dateien ausgelegt ist.

3.5 Netzwerkdiagramme und Ports

Das vollständige Netzwerkdiagramm können Sie im Anhang B (S. 82) finden.
Nachfolgend finden Sie die Netzwerkdiagramme für einzelne und isolierte Maschinen.





4 Kleine Umgebung

Beschreibung der Umgebung

Kleine Umgebungen bestehen aus:

- 2-10 Maschinen in einem einzelnen Netzwerk ohne dedizierte Backup-Server-Hardware
- 1 Hypervisor oder Cluster

Für eine erfolgreiche Bereitstellung in einer solchen Umgebung ist es entscheidend, dass Sie eine einzelne Maschine auswählen, die als Backup Server fungiert und Ihnen die Benutzeroberfläche bereitstellt. Alle anderen Maschinen werden von diesem zentralen Punkt aus über die Webkonsole verwaltet. Für den Backup Server sollte üblicherweise eine leistungsfähigere physische oder virtuelle Maschine verwendet werden. Bei dieser Lösung entfällt die Notwendigkeit, alle Komponenten auf jeder Maschine installieren zu müssen. Und der administrative Aufwand zur Verwaltung der Umgebung wird drastisch gesenkt.

Auf der Maschine des Backup Servers selbst muss kein Server-Betriebssystem installiert sein. Dennoch können Sie mit dem Backup Server natürlich Windows- oder Linux-Server per Backup sichern.

4.1 Vorbereitungen für die Bereitstellung

Dieser Abschnitt behandelt die Anforderungen und Empfehlungen, die bei einer Bereitstellung von Acronis Backup 12.5 in kleinen Umgebungen beachtet werden müssen.

4.1.1 Empfohlene Software-Anforderungen für kleine Umgebungen

Die nachfolgende Liste enthält die Betriebssysteme, die Sie für eine Installation des Management Servers in einer kleinen Umgebung verwenden können.

Obwohl Sie den Management Server auch unter Linux installieren können, empfehlen wir, ein Standard-Windows-Betriebssystem zu verwenden – entweder (ohne Präferenz) einen Windows Server oder eine Desktop-Version.

Windows

Windows Server 2008 – Standard, Enterprise und Datacenter Editionen (x86, x64)
Windows Small Business Server 2008
Windows 7 – alle Editionen (x86, x64)
Windows Server 2008 R2 – Standard, Enterprise, Datacenter und Foundation 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 2008/2008 R2/2012/2012 R2/2016
Windows 10 – Home, Pro, Education, Enterprise und IoT Enterprise Editionen
Windows Server 2016 – alle Installationsoptionen, mit Ausname des Nano Servers

4.1.2 Hardware-Anforderungen und Dimensionierung

Obwohl die Hardware-Anforderungen für eine zentrale Verwaltung mit der Größe Ihrer Umgebung zunehmen, ist diese Zunahme vernachlässigbar, wenn sich um 10-20 zu sichernden Geräte handelt.

Die minimalen Hardware-Anforderungen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#36552.html.

Ausführlichere Empfehlungen zu der für den Betrieb Ihrer Backup-Infrastruktur erforderlichen Hardware finden Sie auch in unserem Ressourcennutzungsrechner (S. 8).

4.1.3 Bereitstellungstyp

Der Acronis Backup 12.5 Management Server kann als physischer Server, virtuelle Maschine, Acronis Backup Appliance und schließlich als Cloud-Plattform bereitgestellt werden, um Ihre lokale Backup-Infrastruktur zu verwalten.

Abhängig von der Konfiguration Ihrer Umgebung, können Sie hier die Empfehlungen für den Bereitstellungstyp finden, den Sie verwenden wollen.

4.1.3.1 Rein physische Umgebung

Wenn Ihre Umgebung nur aus physischen Maschinen besteht (wie einige Server und dazugehörige Workstations), empfehlen wir eine der beiden nachfolgenden Vorgehensweisen:

1. Bestimmen Sie eine dieser Maschinen in Ihrer Umgebung dazu, als Backup Server zu fungieren. Auch wenn unser Management Server auf geringe Ressourcen-Nutzung ausgelegt ist, sollten Sie keinen stärker beschäftigten Produktionsserver als Backup Server wählen. Jede Maschine mit konstanter Netzwerkverbindung und passender Hardware ist für die Aufgabe ausreichend.
   Sie sollten aber sicherstellen, dass die als Backup-Server verwendete Maschine kein mobiles/tragbares Gerät (wie ein Notebook) ist, welches öfter vom Netzwerk getrennt werden könnte. Die Maschine sollte eine konstante, feste IP-Adresse haben bzw. zugewiesen bekommen.
2. Wählen Sie das Cloud-Bereitstellungsmodell. Dabei verwenden Sie an sich denselben Management Server, der aber über die weltweiten Acronis Datenzentren bereitgestellt wird. Sie müssen in diesem Fall also keine eigene Instanz installieren. Ihre Maschinen werden über das Internet mit dem Management Server in der Cloud in Verbindung treten.

Beachten Sie aber, dass einige der erweiterten Funktionen von Acronis Backup 12.5 derzeit beim Cloud-Bereitstellungsmodell noch nicht verfügbar sind. Die Verfügbarkeit für Cloud-Bereitstellungen erfolgt in zukünftigen Produktversionen. Eine vollständige Liste mit allen Funktionen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#38760.html.

4.1.3.2 Rein virtuelle Umgebung

Wenn Sie einen einzelnen Hypervisor (oder ein einzelnes Cluster) per Backup sichern wollen, empfehlen wir die Bereitstellung von Acronis Backup 12.5 als Acronis Backup Appliance (ab Update 2 verfügbar). Weitere Informationen dazu finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/en-us/support/documentation/AcronisBackup_12.5/#37789.html.

4.1.3.3 Hybride Umgebung (physisch/virtuell)

In diesem Fall sind alle drei Bereitstellungstypen gleichwertig:

1. Installation auf einer Ihrer physischen Maschinen.
2. Bereitstellung als Acronis Backup Appliance.
3. Verwendung des Cloud-Bereitstellungsmodells.

Die passende Wahl hängt davon ab, was in Ihrer Umgebung verfügbar ist.

Wenn Ihr Hypervisor beispielsweise ständig überlastet ist und Sie eine freie physische Maschine verfügbar haben, wäre Option 1 die beste Wahl.

Wenn Sie dagegen einen sehr begrenzten Speicherplatz, aber einen leistungsfähigen Hypervisor haben, sollten Sie Option 2 wählen.

Die Cloud-Bereitstellung ist die beste Option, wenn Sie keine der weiter oben aufgeführten erweiterten Funktionen benötigen.

4.2 Komponenten und Installation

4.2.1 Management-Komponenten

Wenn Sie sich für die Bereitstellung auf einer physischen Maschine entscheiden, sollten Sie anhand der nachfolgenden Empfehlungen bestimmen, welchen Komponenten auf dem Server installiert werden sollen, den Sie für die Verwaltung der Backup-Tasks einsetzen wollen. Da dies normalerweise keine dedizierte Maschine in einer kleinen Umgebung sein wird, sind die unteren Empfehlungen mehr auf niedrigen Ressourcenverbrauch statt auf Bequemlichkeit ausgelegt.

Folgende Komponenten werden empfohlen:

- **Management Server** – ist erforderlich
- **Bootable Media Builder** – muss auf mindestens einer Maschine in Ihrer Umgebung installiert sein und ist neben dem Management Server eine gute Wahl

Die nachfolgenden Komponenten sind meistens nicht nur nicht erforderlich, sondern normalweise auch nicht empfehlenswert:

- **Monitoring Service**
  Diese Komponente ermöglicht Dashboards und Berichte in der Benutzeroberfläche des Management Servers. Zwar sind Echtzeit-Dashboards und planbare Berichte bei der Verwaltung größerer Umgebungen unverzichtbar, bei kleineren Umgebungen sind sie jedoch nicht erforderlich. Zudem verursacht die Erfassung, Speicherung und Anzeige der Berichtsdaten einen nicht unerheblichen Overhead.
- **Komponenten zur Remote-Installation** (nur für Windows)
  Mit dieser Komponente können Sie die Remote-Installation von Windows-Agenten von der Benutzeroberfläche des Produkts aus anstoßen. Diese Komponente benötigt 2 GB und mehr an freien Speicherplatz auf Ihrem System-Volume. Sie sollten sie nur installieren, wenn Sie auf dem System-Volume der Management Server-Maschine über genügend Speicherplatz verfügen und Sie zusätzlich die bequeme Möglichkeit nutzen wollen, Agenten remote installieren zu können.
- **Acronis Storage Node**
  Diese Komponente ist nur erforderlich, wenn Sie Ihre Maschinen per Backup auf einem einzelnen, zentralen Bandlaufwerk sichern wollen. In allen anderen Fällen sollten Sie diese Komponente nicht installieren.
  Die nachfolgenden Komponenten sollten Sie in kleinen Umgebungen **nicht installieren**:
- **Catalog Service**
  Der Katalogdienst dient nur dazu, verwaltete Backups durchsuchen zu können. Dies kann sehr nützlich sein, wenn Benutzer bestimmte Dateien anfragen und Sie diese in den Backups finden wollen. Eine Volltextsuche in den Backups (nach bestimmten Dokumenteninhalten) wird mit einem zukünftigen Update von Acronis Backup 12.5 eingeführt werden.

4.2.2 Backup Agenten

Backup Agenten müssen in jedem Teil Ihrer Umgebung installiert werden, die Sie sichern wollen. Anweisungen zur Installation der verschiedenen Agenten finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#36415.html.

Physische Maschinen

Wir empfehlen, dass Sie den Agenten direkt auf dem Betriebssystem installieren, das auf einer physischen Maschine läuft.

Umgebungen mit virtuellen Maschinen

Dies bedeutet in der Regel, dass Sie einen oder mehrere Agenten installieren, die direkt mit dem Hypervisor kommunizieren, auf dem diese Maschinen ausgeführt werden.

Wir empfehlen folgende Vorgehensweisen:

Hyper-V-Umgebungen

Installieren Sie den Agenten für Hyper-V auf jedem Hyper-V-Host, der in Ihrer Infrastruktur läuft. Die Agenten müssen auch dann auf jedem Host installiert werden, wenn die Hosts in einem Cluster verbunden sind.

Wenn Sie Ihre VMs auf SMB3-Netzwerkfreigaben speichern wollen, sollten Sie nicht vergessen, die Windows-Funktion 'VSS für SMB-Freigaben' zu aktivieren. Ohne diese Einstellung werden Ihre Backups fehlschlagen.

Weitere Informationen (in Englisch) finden Sie hier:
https://blogs.technet.microsoft.com/clausjor/2012/06/14/vss-for-smb-file-shares/

VMware vSphere-Umgebungen

Sie können eine oder mehrere virtuelle Appliances direkt als VM bereitstellen und/oder einen Agenten für VMware (Windows) installieren. Die virtuelle Appliance ist eine Acronis Linux-Instanz (eine von Acronis erstellte spezielle, kleine Linux-Distribution), auf der ein Standard-Agent für VMware läuft.

- Die Standardempfehlung ist, eine virtuelle Appliance auf jedem ESXi-Host in Ihrer virtuellen Umgebung zu installieren.
- Die Installation auf einer physischen Windows-Maschine wird empfohlen, wenn Sie Offloaded- oder LAN-freie Backups durchführen wollen.
  - Offloaded Backup
    - Wird verwendet, wenn Ihre produktiven ESX(i)-Hosts so stark ausgelastet sind, dass eine Ausführung der virtuellen Appliances nicht wünschenswert ist.
  - 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. Ausführliche Informationen zum LAN-freien Backup finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#37873.html .

Beachten Sie, dass Sie einen Agenten direkt innerhalb einer bestimmten virtuellen Maschine installieren können. Dafür ist keine eigene Lizenz erforderlich.

Dies eignet sich für Szenarien, bei denen kein agentenloses Backup von virtuellen Maschinen unterstützt wird – wie z.B.:

- Virtuelle Laufwerkskonfigurationen (wie RAW-Laufwerke), für die es keine Snapshot-Unterstützung gibt;
- Hypervisor (wie Xen oder RHEV), für die es keine Unterstützung für agentenloses Backup gibt.

4.2.2.1 Dimensionierung für Agent für VMware/Hyper-V

Agenten für VMware/Hyper-V (ob als virtuelle Appliance oder auf einem Windows-System installiert) sind die einzigen Agenten, deren Anforderungen mit der Umgebungsgröße skalieren. Die typischen Mindestanforderungen sind wie folgt:

RAM

- 1 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über 16 GB oder weniger gesamten Arbeitsspeicher verfügt
- 2 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über bis zu 64 GB Arbeitsspeicher verfügt bzw. gleichzeitig 2 bis 4 Maschinen sichert
- 4 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über mehr als 64 GB Arbeitsspeicher verfügt und gleichzeitig 4 bis 10 Maschinen sichert

CPU

- 2 CPU-Threads werden immer empfohlen
- 2 Kerne (4 Threads), wenn gleichzeitig bis zu 5 VMs gesichert werden
- 4 Kerne (8 Threads), wenn gleichzeitig bis zu 10 VMs gesichert werden

4.2.2.2 Überlegungen in puncto DNS-Konfiguration

Die richtige Konfiguration des Domain Name Systems (DNS) ist bei virtuellen Backups sehr wichtig und die häufigste Ursache für zahlreiche Fehler und Probleme. Die Hostnamen diverser Acronis- und VMware-Komponenten müssen über mehrere physische/virtuelle Netzwerke hinweg untereinander korrekt aufgelöst werden können.

Der VMware Agent muss folgende Namen auflösen können:

- den Management Server-Hostnamen
- jeden ESX(i)-Hostnamen
- den vCenter-Hostnamen

Jede der oberen Komponenten muss außerdem in der Lage sein, die Namen der anderen untereinander auflösen zu können. Wenn die Namensauflösung nicht korrekt funktioniert, werden Sie verschiedene Kategorien von Fehlern sehen – von Bereitstellungsproblemen bis zu Backup-Fehlern.

Um diese Fehler zu vermeiden, sollten Sie unseren Empfehlungen folgen:

Wenn Sie in einer Acronis Lösung einen vCenter Server hinzufügen, wird unser Produkt versuchen, auf jedem Host in Ihrer vSphere-Umgebung eine virtuelle Appliance zu installieren. Weitere Informationen dazu finden Sie in der offiziellen Benutzeranleitung:
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#36631.html.

Damit diese automatische Bereitstellung funktioniert, ist es wichtig, dass die Domain-Namen-Auflösung zwischen dem Acronis Management Server und den Gastbetriebssystemen der VMs (die in Ihren ESX(i)-Hosts ausgeführt werden) funktioniert. Das ist notwendig, um sicherstellen zu können, dass der Acronis Agent für VMware (Virtuelle Appliance) nach der Bereitstellung mit einem konfiguriertem DNS-Server in der Lage ist, sich mit dem Acronis Management Server zu verbinden (über dessen Hostnamen). Um Ihnen dabei zu helfen, haben wir mit Update 2 ein Feld eingeführt, mit dem Sie festlegen können, wie sich die Komponenten mit dem Server verbinden sollen – über den Hostnamen oder über die IP-Adresse.

Wir empfehlen, dass Sie statt dem Hostnamen die IP-Adresse auswählen, die der Agent zur Verbindung mit dem Management Server verwenden soll.

Sobald die Appliance für VMware bereitgestellt wurde, sollten Sie die DNS-Auflösung zwischen dem Agenten und den anderen Komponenten überprüfen:

1. Öffnen Sie einen vSphere Client und bauen Sie eine Verbindung zu einem ESX(i)-Host oder vCenter auf.
2. Navigieren Sie zu der virtuellen Appliance, öffnen Sie die Registerkarte **Konsole** und drücken Sie dann die Tastenkombination **Strg**+**Alt**+**F2**, um auf der Appliance in den Befehlszeilenmodus zu wechseln (den Sie mit der Tastenkombination **Alt**+**F1** wieder verlassen können).
3. Geben Sie einen Ping-Befehl ein, um den ESXi-Hostnamen und den vCenter-Namen von der virtuellen Appliance aus aufzulösen:
   `ping Hostname_des_ESXi`
   `ping Hostname_des_vCenters`.
4. Wenn der Ping-Befehl für den Hostnamen nicht erfolgreich ist, haben Sie ein DNS-Namensauflösungsproblem, weswegen VM-Backups von diesem Agenten auch nicht funktionieren werden.

*Wenn der **Port 25** gesperrt ist, wird der **`ping`**-Befehl nicht korrekt funktionieren. Sie können dann stattdessen andere Befehle verwenden – wie **`nslookup`**. Es ist nicht so wichtig, welchen Befehl genau Sie wählen, solange Sie damit überprüfen können, ob eine Verbindung über den Hostnamen erfolgt.*

Sie können das Problem beheben, indem Sie das Netzwerk in der Appliance und in Ihrer virtuellen Umgebung korrekt konfigurieren. Als Workaround können Sie auf jeder Appliance auch die Datei 'hosts' bearbeiten.
Das Bearbeiten der Datei 'hosts' funktioniert folgendermaßen:

1. Öffnen Sie die Konsole der virtuellen Appliance mit folgender Tastenkombination: **Strg**+**Alt**+**F2**.
2. Öffnen Sie die Datei 'hosts' mit folgendem Befehl:
   `vi /etc/hosts`
3. Drücken Sie die Taste **i**, um in den Bearbeitungsmodus zu wechseln.
4. Geben Sie die IP-Adresse und den aufzulösenden Namen des Servers in folgendem Format ein:
   `XXX.XXX.XXX.XXX Hostname`
5. Speichern Sie die Änderungen, indem Sie die Taste **Esc** drücken, geben Sie dann **`:wq`** ein
6. Drücken Sie die **Eingabetaste**.
7. Verlassen Sie die Konsole mit der Tastenkombination **Alt**+**F1**.

4.2.2.3 Prozessauslagerung auf andere Hosts (Off-Host-Verarbeitung)

Eine sehr wichtige neue Funktion von Acronis Backup 12.5 Advanced ist die Fähigkeit von Acronis Agenten, neben Backups noch eine Reihe anderen Datenverarbeitungstasks ausführen zu können. Jeder dieser Tasks kann auf Basis einer eigenen Planung laufen und ist komplett unabhängig von den eigentlichen Backups. Zu den verfügbaren Tasks gehören:

- Backup-Replikation
- Validierung
- Bereinigung
- Konvertierung zu VM
- VM-Replikation

Diese Funktionalität ist unerlässlich, um Backup-Daten im größeren Umfang so zu verwalten, dass alle Anforderungen eines Backup-Plans erfüllt werden, ohne dass das begrenzte Backup-Fenster überschritten wird. In kleineren Umgebungen ist sie jedoch weniger wichtig. Mit dieser Funktionalität können Sie Ihre Backups beispielsweise an den Wochenenden direkt von einem Storage zu einem anderen Storage replizieren lassen, ohne dass dabei die Backup-Agenten selbst einbezogen werden.

In kleineren Umgebungen ist diese Funktionalität normalerweise nicht erforderlich, da das Verhältnis zwischen Datenmenge und Netzwerkbandbreite hier normalerweise viel kleiner ist. Sie kann aber auch hier praktisch sein – beispielsweise, wenn die Backup-Daten wöchentlich oder monatlich zu einem Offsite-Storage (wie die Acronis Cloud) repliziert werden sollen.

4.2.3 Empfohlene Installationsprozedur

Ausführliche Installationsanweisungen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#36428.html.

Bei einer Installation unter Windows sollten Sie sicherstellen, dass zuvor auf der Maschine alle erforderlichen Linux-Pakete installiert wurden – siehe: https://www.acronis.com/de-de/support/documentation/AcronisBackup_11.7/#22619.html.

Nachfolgend finden Sie unsere Empfehlungen für kleinere Umgebungen:

1. Registrieren Sie Ihr Produkt in Ihrem Acronis Konto. Ausführliche Anweisungen dazu finden Sie hier: https://kb.acronis.com/content/4834
2. Laden Sie die vollständige Installationsdatei herunter, die für Ihr jeweiliges Betriebssystem (Windows oder Linux) passend ist.
   Sie können die Dateien immer direkt aus Ihrem Konto herunterladen, nachdem Sie die Registrierung durchgeführt haben.
3. Installieren Sie den Acronis Management Server, den Backup Agent und den Bootable Media Builder auf der Maschine, die Sie als Backup Server ausgewählt haben.
4. Konfigurieren Sie Ihre Speicherorte (Storages).
5. Beginnen Sie mit der Bereitstellung der Backup Agenten.
   a. Sie können eine automatische Installation aus dem Produkt heraus erfolgen lassen („Push-Installation“), wenn die **Komponenten zur Remote-Installation** installiert sind.
   b. Ansonsten müssen Sie die Installationsdatei manuell auf jeder Maschine installieren, die gesichert werden soll. Beachten Sie, dass die Agenten für Linux und Mac derzeit noch immer manuell installiert werden müssen (auf jeder Maschine, die gesichert werden soll). Die Push-Installationsfunktion für diese Systeme wird mit einem zukünftigen Update von Acronis Backup eingeführt.
6. Konfigurieren Sie Ihre Backup-Pläne und wenden Sie diese an.
7. **[Optional]** Konfigurieren Sie Off-Host-Datenverarbeitungspläne, wenn Sie Backups beispielsweise wöchentlich/monatlich replizieren und validieren wollen.

4.3 Backup-Plan-Empfehlungen

4.3.1 Backup-Quelle

In der Regel werden Sie wohl komplette Maschinen sichern – und dabei bestimmte Ausschlussregeln verwenden, damit keine unerwünschten Dateien in das Backup aufgenommen werden.

Sie können Laufwerke (Partitionen), einzelne Dateien und Ordner oder Dateikategorien anhand von Dateierweiterungen ausschließen. Beispielsweise können Sie bei der Sicherung eines Notebooks oder Desktop-Rechners alle .avi-Dateien vom Backup ausschließen. Ausschlusskritierien und andere Backup-Optionen basieren immer auf einem Backup-Plan. Wenn Sie also für verschiedene Maschinen unterschiedliche Ausschlusskriterien benötigen, müssen Sie auch mehrere Pläne erstellen.

Für unterschiedliche Backup-Quellen sind jeweils unterschiedliche Backup-Pläne erforderlich (zumindest je einer für jede unterschiedliche Art von Backup-Quelle).

Wenn Sie beispielsweise wenig Speicherplatz haben, können Sie einen Backup-Plan zur Sicherung einer kompletten Maschine erstellen und diesen auf Ihren Produktionsserver anwenden. Und mit einem zweiten Backup-Plan, den Sie auf persönliche Desktop-Rechner anwenden, können Sie den Benutzerordner auf jeder Maschine sichern. Dazu müssen Sie bei der Backup-Plan-Erstellung nur die Auswahlregel **[Alle Benutzerprofile]** verwenden.

4.3.2 Backup-Ziel

Für kleine Umgebungen gibt es üblicherweise zwei wesentliche Speicheroptionen:

- Sie können alle Backups direkt auf der Maschine des Agenten selbst speichern.
  Beispielsweise kann jede Maschine ihr Volume **C:** auf ihrem Volume **D:** (Ziel) speichern – oder auf einem angeschlossenen USB-Laufwerk.
  Für diese Szenarien gibt es keine besonderen Empfehlungen.
  Dies hat den Vorteil einer geringeren Netzwerkauslastung, jedoch auf Kosten eines höheren Verwaltungsaufwands (denn jeder Speicherplatz muss einzeln angesprochen werden).
  Diese Option ist empfehlenswert, wenn Sie keine zentrale Netzwerkfreigabe oder kein NAS-Gerät haben, wo Sie Ihre Backups speichern können.
- Sie können alle Backups zentral speichern.
  Wir empfehlen ein handelsübliches NAS-Gerät oder eine Netzwerkfreigabe. In beiden Fällen sollte der bereitgestellte Speicherplatz ausreichend sein, um Ihre Backup-Daten über die erforderliche Aufbewahrungsdauer aufnehmen zu können.
  Nutzen Sie den Ressourcennutzungsrechner (S. 8), um die ungefähre Backup-Größe unter Berücksichtigung Ihrer Umgebung und Aufbewahrungsfristen zu berechnen.

4.3.3 Planung

Solange die Netzwerkverbindung zwischen Ihren Geräten (Backup-Quelle) und Ihrem Backup Storage (Backup-Ziel) nicht furchtbar unzureichend ist (weil Sie beispielsweise einen Dateiserver mit 6 TB haben, der nur über eine 10-MBit-Verbindung mit einem NAS-Gerät verbunden ist), wird die Netzwerkgeschwindigkeit keinen nennenswerten Einfluss auf das Backup haben. Das bedeutet, dass die empfohlene Backup-Planung üblicherweise von der Datenmenge auf Ihren zu sichernden Geräten und den vorgegebenen RPO-Zielen (Recovery Point Objective) abhängt. Solange das aktuell ausgeführte Backup genügend Zeit zur Fertigstellung hat, bevor das nächste Backup startet, sollten Sie keine Probleme haben.

Allerdings nimmt ein Backup eine beträchtliche Menge an Ressourcen von der zu sichernden Maschine in Anspruch, was laufende Produktions-Workloads beeinflussen kann (insbesondere wenn die Belastung hoch ist).

Unsere Erfahrung zeigt, dass eine gute, allgemein empfehlenswerte Planung darin besteht, jeden Tag zur Nachtzeit (nach Betriebsschluss) ein inkrementelles Backup durchzuführen – und über das Wochenende ein Voll-Backup.

Es wird allgemein empfohlen, weitere Tasks (wie Replikation oder Validierung) ebenfalls für das Wochenende zu planen – obwohl das für kleinere Umgebungen nicht so kritisch ist.

4.3.4 Aufbewahrungszeiten

Aufbewahrungsfristen basieren oft auf externen Richtlinien oder Compliance-Regeln. Sie können die zu erwartende Größe der Backups für die Aufbewahrungsdauer mithilfe des Ressourcennutzungsrechners (S. 8) abschätzen.

Wenn der als primäres Backup-Ziel verwendete Storage nicht genügend groß sein sollte, können Sie spezielle Replikationstasks planen, um die Daten zur Langzeitaufbewahrung auf einen anderen, billigeren Storage zu verschieben.

Sie können Ihre Backups beispielsweise in die Acronis Cloud replizieren oder einen Band-basierten Storage zur Langzeitaufbewahrung verwenden.

4.3.5 Replikation, Konvertierung und Validierung

Wenn Sie vermeiden wollen, dass ausgeführte Backups Ihre Maschinen und Ihr Netzwerk stärker beeinflussen, sollten Sie keine Replikations- oder Validierungsoptionen in Ihren Backup-Plänen festlegen.

Stattdessen können Sie separate „Mini-Pläne“ erstellen, die Aufgaben wie Replikation oder Validierung eigenständig außerhalb der Stoßzeiten (etwa am Wochenende) durchführen. Es ist normalerweise am bequemsten, wenn Sie festlegen, dass der auf dem Management Server installierte Agent diese Aktionen ausführt.

Wenn die Mehrfachtasks (wie Backup + Replikation + Validierung) aber während der Nacht abgeschlossen werden können, ohne dass Ihre Produktion negativ beeinflusst wird, spricht auch nichts dagegen, diese zusätzlichen Tasks mit in den Backup-Plan aufzunehmen. Und es ist dann natürlich auch bequemer, die Tasks auf diese Art gemeinsam zu verwalten.

Dies gilt auch bei Szenarien, bei denen jeder Agent ein Backup zu seinem eigenen lokalen Speicherort erstellt. In diesem Fall müssen die zusätzlichen Datenverarbeitungstasks (wie Validierung) in denselben Backup-Plan integriert werden.

4.3.6 Weitere Empfehlungen

Benachrichtigungen, Alarmmeldungen und Berichte

Normalerweise ist es notwendig, dass Sie den Status Ihrer Backups genau im Auge behalten. Kleine Umgebungen haben normalerweise aber keine betriebskritische Hardware und kein dediziertes IT-Team, um auftretende Backup-Probleme schnellstmöglich zu lösen.

Den meisten Anwendern reicht es aus, mit einer gewissen Sicherheit davon ausgehen zu können, dass das tägliche Backup korrekt funktionieren wird.

Der empfohlene Weg, den Status Ihrer Backups mit minimalem Aufwand zu verwalten, besteht darin, folgende Benachrichtigungen festzulegen:

- Aktivieren Sie das Kontrollkästchen **Tägliche Zusammenfassung über aktive Alarmmeldungen** in den Benachrichtigungseinstellungen
- Bestimmen Sie, zu welcher Zeit Sie die Benachrichtigungen bevorzugt überprüfen wollen. Die Standardvorgabe ist 10:00 Uhr.
- Deaktivieren Sie alle anderen Kontrollkästchen.

Diese Einstellung bedeutet, dass Sie täglich eine einzige E-Mail erhalten, die dann leicht und schnell zu überprüfen ist. Wenn alles in Ordnung ist, erhalten Sie eine E-Mail, die diese Einstellung explizit bestätigt. Wenn es beispielsweise in der zurückliegenden Nacht Probleme mit Ihren Backups gegeben hat, erhalten Sie eine Liste mit Warnmeldungen, in der das/die Problem(e) klar angegeben sind.

Wenn Sie noch mehr Kontrolle wollen, können Sie einzelne Alarmbenachrichtigungen für kritische Benachrichtigungen konfigurieren. Dadurch können Sie sicherstellen, dass Sie direkt eine E-Mail erhalten, sobald auf Ihrer Maschine ein Problem auftritt.

Beachten Sie, dass Alarmbenachrichtigungen standardmäßig gesendet werden, sobald ein Alarm aktiviert wird. Jeder Alarm auf jedem Agenten für jeden Plan generiert eine E-Mail.

Dateiformat

Verwenden Sie wann immer möglich das Standard-Backup-Format 'Version 12'.
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#38763.html.

Active Protection

Active Protection ist derzeit nur für Maschinen mit Windows 7 (und höher) sowie Windows Server 2008 R2 (und höher) verfügbar. Der Agent für Windows muss auf der Maschine installiert sein.

Wir empfehlen, Active Protection auf allen Maschinen zu aktivieren, sofern diese nicht unter zu knappen CPU-Ressourcen leiden.

Bei starken Dateizugriffen bewirkt Active Protection üblicherweise einen CPU-Overhead von einigen wenigen CPU-Prozenten im System.

4.4 Überlegungen in puncto Storage

NAS

Die einfachste Storage-Lösung für einzelne Maschinen ist ein NAS-Gerät oder ähnliche Netzwerkfreigaben, wo die Backups aller Maschinen in der Umgebung gespeichert werden.
Sie müssen dabei insbesondere beachten, dass auf dem zugrundeliegenden Storage-Gerät genügend Speicherplatz vorhanden ist. Sie können den Ressourcennutzungsrechner (S. 8) verwenden, um die benötigte Speicherplatzgröße einzuschätzen. Der empfohlene minimale Speicherplatz berechnet sich aus der Größe aller Backups (für Ihre Aufbewahrungszeit) + der Größe eines Voll-Backups von allen Maschinen.

USB- oder internes Laufwerk

Eine weitere empfehlenswerte Storage-Option besteht darin, jede Maschine ihre Backups zu einem externen USB-Laufwerk oder einem speziellen internen Backup-Laufwerk erstellen zu lassen.

Externer Storage (Offsite-Storage)

Es ist besonders wichtig, dass Sie mindestens eine Kopie Ihrer Daten an einem externen Ort (Offsite-Storage) vorliegen haben. Wir empfehlen die Verwendung der Replikationsfunktion, um eine solche Offsite-Kopie in Ihrem eigenen Acronis Cloud Storage zu speichern. Ihre Offsite-Backups werden dabei in einem unserer sicheren Datenzentren gespeichert, welches sich in Ihrem Land/Ihrer Region befindet.

Dies ist die einfachste Möglichkeit, um Ihre Daten sicher in einem Offsite-Storage zu speichern. Aufgrund beschränkter Internet-Upload-Bandbreiten, Compliance-Gründen, Kostenerwägungen usw. ist die Option aber wohl nicht für jeden passend.

In diesem Fall empfehlen wir, die Backups zuerst zu einem externen USB-Laufwerk oder Bandlaufwerk zu replizieren. Und die entsprechenden Speichermedien dann regelmäßig an einem sicheren externen Ort zu hinterlegen.

4.4.1 Deduplizierung

Verwenden Sie keine Deduplizierung. In kleinen Umgebungen gleicht der geringe Gewinn, der hier durch die Deduplizierung erzielt werden kann, die zusätzliche Hardware-Belastung nicht aus.

4.4.2 Wechsellaufwerke

In kleineren Umgebungen ist es oft üblich, Backups auf externen Wechsellaufwerken erstellen zu lassen und die entsprechenden Speichermedien regelmäßig auszutauschen.

Dies funktioniert mit Acronis Backup 12.5 nicht sofort „out of the box“, weil wir die Backup-Metadaten immer direkt in den Backups selbst speichern. Denn dieser Ansatz bietet den großen Vorteil, dass Ihre Backups damit komplett portabel sind: Sie können ein Backup beispielsweise auf einem USB-Stick speichern, durch die ganze Welt zu einem komplett anderen Ort versenden und dort wiederherstellen, ohne dass Sie etwas über die ursprüngliche Umgebung wissen müssen.

Ohne einen speziellen Mechanismus, der die wichtigen Metadaten zwischen verschiedenen Wechseldatenträgern synchronisiert, verursacht ein Backup-Plan, der einen solchen Storage-Typ als Ziel verwendet, eine Vielzahl von Problemen bei der Backup-Erstellung und -Aufbewahrung. Ein solcher Mechanismus ist aber für zukünftige Updates geplant.

Eine derzeit schon funktionierende Methode für dieses Szenario ist in unserer Knowledge Base unter dieser Adresse beschrieben:
https://kb.acronis.com/content/58372.
Diese Methode ist eher eine Zwischen- als eine ideale Lösung. Aber bis wir Wechsellaufwerke mit dem beschriebenen Mechanismus unterstützen, ist es die beste Möglichkeit.

4.4.3 Bandgeräte

Acronis ist bestrebt, die Unterstützung für Bandgeräte fortzusetzen und auszuweiten.

Eine Liste von getesteten und unterstützten Bandgeräten finden Sie in der Hardware-Kompatibilitätsliste für Bandlaufwerke (https://go.acronis.com/acronis-backup-advanced-tape-hcl).

Wenn Sie die Kompatibilität Ihres eigenen Bandgerätes testen wollen, können Sie das Bandkompatibilitätstool verwenden (https://kb.acronis.com/content/57237).

Wenn das Tool ein Problem findet, kontaktieren Sie bitte den Acronis Support, damit das Problem zu unserer Entwicklungsabteilung weitergeleitet und gelöst werden kann.

Ein Agent kann Backups direkt zu einem Bandlaufwerk erstellen. Wenn Sie eine einzelne oder isolierte Maschine haben und Band-Backups erstellen wollen, müssen Sie das Bandlaufwerk direkt an der Maschine anschließen, auf welcher der Agent installiert ist.

4.4.3.1 Storage Nodes für Bänder

Der Acronis Storage Node wird benötigt, wenn Sie eine größere Menge von Maschinen per Backup auf (ein oder mehrere) Bandlaufwerke sichern wollen. Das Bandgerät muss dafür an die Maschine des Storage Nodes angeschlossen sein.

Wenn Sie mehrere eigenständige Bandlaufwerke haben oder lediglich eine einzelne Maschine per Backup auf Band sichern wollen, empfehlen wir, dass Sie das Bandlaufwerk direkt an die zu sichernde(n) Maschine(n) anschließen – und folglich auf Verwendung des Storage Nodes zu verzichten.

4.4.3.2 Bandverwaltungsdatenbank

Die Informationen über alle Bandgeräte, Bänder und Backup-Inhalte werden in der Bandverwaltungsdatenbank gespeichert, die sich wiederum auf der Maschine befindet, an welcher das Bandgerät angeschlossen ist.

Der Standardpfad für die Datenbank ist:

- Windows 7, Windows Server 2008 und höher:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database
- Linux:
  /var/lib/Acronis/BackupAndRecovery/ARSM/Database

Die Datenbankgröße hängt von der Zahl der auf den Bändern gespeicherten Backups ab – wobei etwa 10 MB auf einhundert Backups kommen. Mit einigen wenigen Maschinen ist dies –auch mit längeren Aufbewahrungszeiten – kein Problem.

Sie sollten jedoch sicherstellen, dass Sie genügend Speicherplatz für diese Datenbank auf Ihrem System haben. Falls Sie unsicher sind, sollten Sie vor dem Start des ersten Band-Backups den Pfad entsprechend überprüfen.

So verlagern Sie die Datenbank unter Windows:

1. Stoppen Sie den den Dienst '**Removable Storage Management**'.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Ermitteln Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings**.
4. Spezifizieren Sie den Pfad zum neuen Speicherort im Registry-Wert `ArsmDmlDbProtocol`. Der String darf bis zu 32765 Zeichen enthalten.
5. Starten Sie den den Dienst '**Removable Storage Management**' wieder.

So verlagern Sie die Datenbank unter Linux:

1. Stoppen Sie den Dienst '**acronis_rsm**'.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Öffnen Sie die Konfigurationsdatei **/etc/Acronis/ARSM.config** in einem Text-Editor.
4. Suchen Sie nach folgender Zeile: `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Ändern Sie den Pfad unter dieser Ziele.
6. Speichern Sie die Datei.
7. Starten Sie den Dienst '**acronis_rsm**' wieder.

Sie dürfen die Band-Datenbank nicht löschen! Denn dies würde erfordern, dass all Bänder erneut gescannt werden müssen, um die darauf gespeicherten Backups wieder verwendbar zu machen. Und dies ist ein sehr zweitaufwendiger und fehleranfälliger Prozess.

4.4.3.3 Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren

Diese Option ist standardmäßig deaktiviert. Wenn Sie diese Option in den Bandverwaltungseinstellungen Ihres Backup-Plans aktivieren, können Sie aus Image-Backups, die auf Ihren Bändern gespeichert sind, auch einzelne Dateien wiederherstellen.

Beachten Sie, dass Sie sich diese Funktionalität mit hohen Speicherplatzkosten erkaufen. Wenn die Funktionalität aktiviert ist, erstellt die Software bei jedem Backup zusätzliche Dateien auf einem Festplattenlaufwerk der Maschine, an der das Bandgerät angeschlossen ist. Datei-Recovery von Laufwerk-Backups ist möglich, solange diese zusätzlichen Dateien intakt sind. Die Dateien werden automatisch gelöscht, wenn das Band, auf dem die entsprechenden Backups gespeichert sind, gelöscht, entfernt oder überschrieben wird.

Diese zusätzlichen Dateien befinden sich an diesem Speicherort:

- In Windows 7, Windows Server 2008 und höher:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation
- In Linux:
  /var/lib/Acronis/BackupAndRecovery/TapeLocation

Der von diesen zusätzlichen Dateien belegte Speicherplatz hängt von der Anzahl der Dateien im entsprechenden Backup ab. Beim Voll-Backup eines Laufwerks mit ungefähr 20.000 Dateien (typisches Laufwerk-Backup einer Workstation) belegen die zusätzlichen Dateien ca. 150 MB. Ein einzelnes Voll-Backup eines Servers mit 250.000 Dateien kann etwa 700 MB an zusätzlichen Dateien erzeugen.

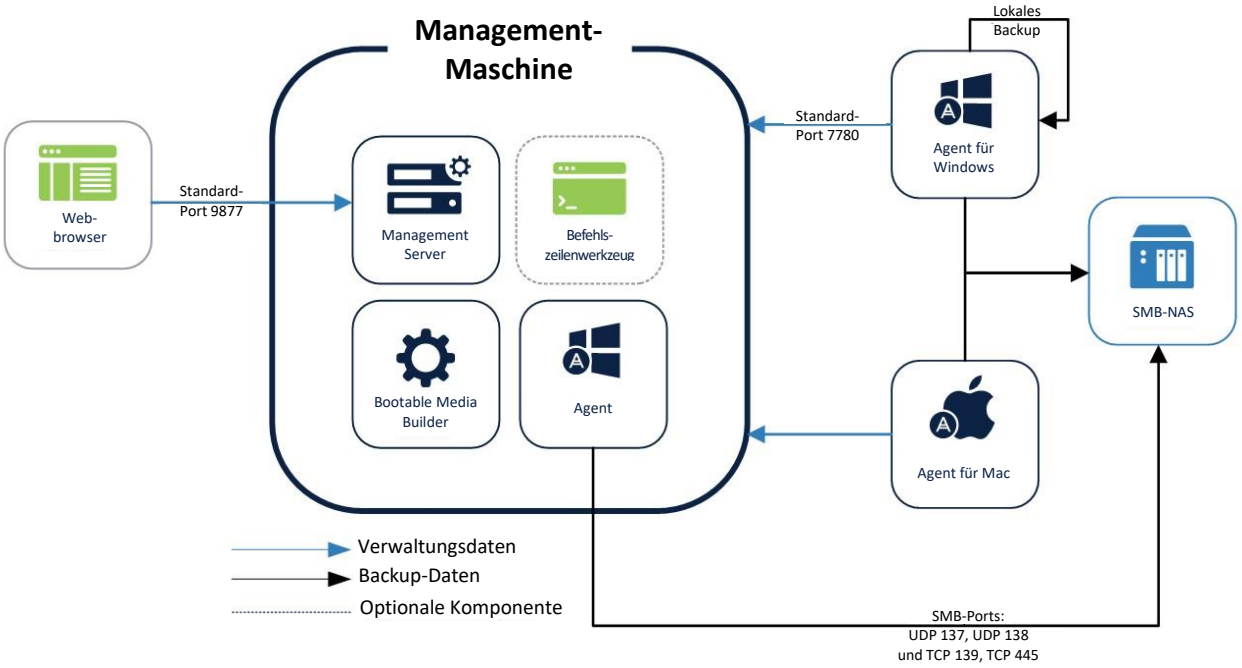
Auch in kleinen Umgebungen kann die Größe dieser Dateien schnell auf Dutzende von Gigabyte anwachsen.

Wir empfohlen daher, dass Sie diese Option deaktiviert lassen, wenn Sie die Option nicht unbedingt benötigen. Wenn doch, sollten Sie sicherstellen, dass der verwendete Speicherort oder Storage Node von der Speicherplatzgröße auf diese zusätzlichen Dateien ausgelegt ist.

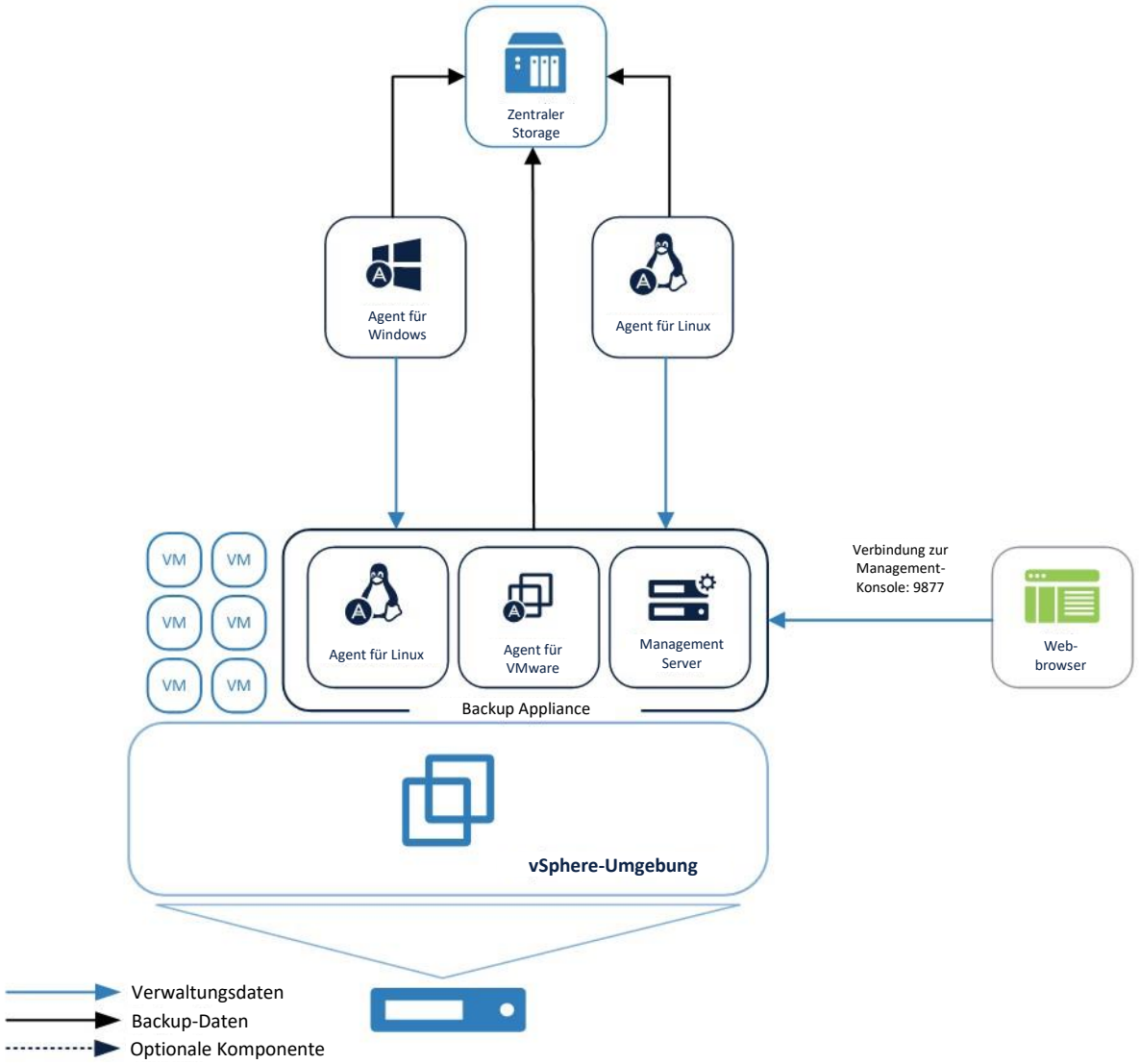
4.5 Netzwerkdiagramme und Ports

Das vollständige Netzwerkdiagramm können Sie im Anhang B (S. 82) finden.

Nachfolgend finden Sie das Netzwerkdiagramm für kleine Umgebungen.



Nachfolgend finden Sie das Netzwerkdiagramm, wenn Sie nur die Acronis Backup Appliance verwenden wollen.



5 Typische KMUs

Beschreibung der Umgebung

Wir definieren typische KMUs (kleine und mittlere Unternehmen) hier folgendermaßen:

- Einige Dutzend bis ca. einhundert physische Server
  - Davon 2-3 Linux-Server
- 1 Hypervisor, zumeist in einem 2-Host-Cluster mit einigen hundert virtuellen Maschinen (VMs)
- Eine Reihe von Produktions-Applikationen, für die granulare Wiederherstellungen möglich sein sollten

KMU-Umgebungen müssen sich zudem oft an bestimmte gesetzliche oder unternehmenseigene Richtlinien halten – beispielsweise: zwingend erforderliche externe Backup-Kopien, Replikationen, Validierungen etc. Mit Acronis Backup 12.5 wurde eine neue Funktion namens '*Prozessauslagerung auf andere Hosts (Off-Host-Verarbeitung)*' eingeführt, die die Durchführung solcher zusätzlicher Tasks in KMU-Umgebungen deutlich erleichtert.

5.1 Vorbereitungen für die Bereitstellung

Dieser Abschnitt behandelt die Anforderungen und Empfehlungen, die bei einer Bereitstellung von Acronis Backup 12.5 in KMU-Umgebungen beachtet werden müssen.

5.1.1 Empfohlene Software-Anforderungen für KMU-Umgebungen

Die nachfolgende Liste enthält die Betriebssysteme, die Sie für eine Installation des Management Servers in einer KMU-Umgebung verwenden können.

Bei KMU-Umgebungen, die überwiegend auf Windows basieren, empfehlen wir, den Management Server auf Windows Server 2012 R2 (oder höher) zu installieren. Grundsätzlich ist es aber auch möglich, eine Maschine mit einer älteren Windows-Version oder mit Linux zu verwenden.

Windows

Windows Server 2008 – Standard, Enterprise und Datacenter Editionen (x86, x64)
Windows Small Business Server 2008
Windows 7 – alle Editionen (x86, x64)
Windows Server 2008 R2 – Standard, Enterprise, Datacenter und Foundation 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 2008/2008 R2/2012/2012 R2/2016
Windows 10 – Home, Pro, Education, Enterprise und IoT Enterprise Editionen
Windows Server 2016 – alle Installationsoptionen, mit Ausname des Nano Servers
Obwohl es nicht zwingend erforderlich ist, ein Windows Server-Betriebssystem zu verwenden, ist es für mittlere und größere Umgebungen aus Gründen der Skalierbarkeit, Sicherheit und Stabilität dennoch ratsam.

5.1.2 Management Server-Datenbank

Der Acronis Management Server verwendet standardmäßig ein SQLite-Datenbank-Backend, um seine Daten in Windows- und Linux-Umgebungen zu speichern. Die Wahl dieser Standarddatenbank ist für die meisten KMU-Umgebungen überwiegend ausreichend.

Wenn Ihnen die Zuverlässigkeit der Datenbank wichtig ist oder eine Unternehmensrichtlinie die Verwendung dedizierter Microsoft SQL-Instanzen vorschreibt, können Sie während der Installation festlegen, dass eine Microsoft SQL-Datenbank verwendet werden soll (S. 51).

Bei Linux empfehlen wir die Verwendung einer PostgreSQL-Datenbank. Deren Konfiguration ist in folgendem Knowledge Base-Artikel erläutert: https://kb.acronis.com/content/60395.

Die integrierte Unterstützung und Installation von PostgreSQL-Datenbanken unter Linux wird mit einem zukünftigen Update von Acronis Backup eingeführt.

Die Empfehlungen und Dimensionierung des Microsoft SQL Servers finden Sie im Abschnitt über große Umgebungen (S. 50).

SQLite kann dennoch installiert und lokal für einige andere Dienste verwendet werden, wird dann aber nicht die Datenbank für das Hauptprodukt enthalten.

5.1.3 Hardware-Anforderungen und Dimensionierung

Die Hardware-Anforderungen für die zentralen Management-Komponenten skalieren mit der Anzahl der zu verwaltenden Geräte (insbesondere bei Umgebungen mit über 200 Maschinen).

Der Management Server ist gut optimiert und wenig CPU- bzw. RAM-abhängig. Daher sollte jeder halbwegs moderne Server für eine KMU-Umgebung geeignet sein. Der Management Server reagiert jedoch empfindlich auf den I/O-Durchsatz des Storage-Subsystems, das von den verschiedenen Datenbanken der Management Server-Dienste verwendet wird. Dies liegt daran, dass die Sicherungen hunderter Geräte auch Hunderte bis Tausende von IOPs (Eingabe-/Ausgabe-Aktionen pro Sekunde) erzeugen können, weswegen Standard-Festplatten als Storage-Hardware schnell zum Flaschenhals werden können.

Wir empfehlen daher, dass Sie performante SSD-Laufwerke (mit hoher IOPS-Leistung) für den Management Server verwenden, wenn Sie Umgebungen mit Hunderten von Geräten sichern müssen.

Ausführlichere Empfehlungen zu der für den Betrieb Ihrer Backup-Infrastruktur erforderlichen Hardware finden Sie auch in unserem Ressourcennutzungsrechner (S. 8).

5.1.4 Bereitstellungstyp

Der Acronis Backup 12.5 Management Server kann als physischer Server, virtuelle Maschine, Acronis Backup Appliance und schließlich als Cloud-Plattform bereitgestellt werden, um Ihre lokale Backup-Infrastruktur zu verwalten.

Obwohl die IOPS-Leistung des Server-Storage-Subsystems für KMU-Umgebungen nicht so kritisch ist, bleibt sie auch hier ein wichtiger Faktor. Wir empfehlen daher allgemein, dass Sie einen physischen Server verwenden, da dies die einfachste Lösung ist, um die Storage-Subsystem-Performance zu optimieren.

Wenn Ihr Hypervisor ein ausreichend schnelles virtuelles Laufwerkssubsystem (mit mehr als 100 IOPS) bereitstellen kann, können Sie den Management Server auch auf einer virtuellen Maschine oder als Acronis Backup Appliance installieren.

Beim Acronis Backup Cloud-Bereitstellungsmodell wird der gleiche Acronis Backup 12.5 Management Server verwendet – er wird lediglich von einem Acronis Datenzentrum aus bereitgestellt. Die Agenten werden über das Internet mit dem Management Server in der Cloud verbunden. Dieses Bereitstellungsmodell empfiehlt sich aber nicht als Hauptszenario für große Umgebungen, weil einige neue Funktionen, die speziell in großen Umgebungen verwendet werden, nur bei lokaler Bereitstellungen verfügbar sind.

Die Verfügbarkeit für Cloud-Bereitstellungen erfolgt in zukünftigen Produktversionen.

5.2 Komponenten und Installation

5.2.1 Management-Komponenten

Folgende Komponenten müssen auf dem Server installiert sein, der für die Backup-Verwaltung zuständig ist:

- **Management Server**
- **Monitoring Service**

In einigen Fällen ist es empfehlenswert, die nachfolgenden Komponenten ebenfalls auf demselben Server zu installieren.

- **Komponenten zur Remote-Installation** (nur für Windows)
  Mit dieser Komponente können Sie die Remote-Installation von Windows-Agenten von der Benutzeroberfläche des Produkts aus anstoßen. Wenn Sie die Agenten mithilfe einer Gruppenrichtlinie installieren wollen, wird diese Komponente nicht benötigt.
- **Backup Agent**
  Mit dieser Komponente können Sie den Management Server selbst sichern.
  Da der Management Server für die Backup-Funktion der Agenten nicht zwingend notwendig ist, können Sie diesen Schritt prinzipiell überspringen. Sie müssen jedoch die komplette Konfiguration neu installieren und wiederholen (was bei großen Umgebungen einige Zeit dauern kann), wenn der Server ausfällt und Sie kein Backup von diesem haben. Empfehlungen zur Selbstsicherung des Management Servers finden Sie in einem unteren Abschnitt.
  - Es gibt derzeit keine Möglichkeit, die Konfiguration des Management Servers zu importieren oder zu exportieren.
    Diese Funktionalität wird mit einem zukünftigen Update von Acronis Backup eingeführt.
  - Es gibt keine bereits integrierte Möglichkeit, einen Management Server-Cluster aufzubauen.
  - Zur Sicherung des Management Servers benötigen Sie eine Lizenz, die dem Betriebssystem entsprechen muss, welches Sie für den Management Server verwenden.

Die folgenden Komponenten müssen installiert werden, aber nicht unbedingt parallel zum Management Server. Wenn es bequemer für Sie ist, können die nachfolgenden Komponenten auf jeder Maschine installiert werden, auf der ein lizenzierter Agent läuft:

- **Bootable Media Builder**
- **Microsoft SQL-Datenbank** (für Umgebungen mit mehr als 900 Agenten)

Für die nachfolgenden Komponenten sollte dedizierte Hardware verwendet werden – jedoch nur, wenn Ihre Backup-Pläne und/oder Ihr Storage-Typ dies erfordert.

Über den Ressourcennutzungsrechner (S. 8) erhalten Sie Empfehlungen zur Installation und der benötigten Anzahl dieser Komponenten.

- **Acronis Storage Node**
  Diese Komponente wird benötigt, wenn Sie verwaltete Backup-Speicherorte verwenden wollen. Diese sind erforderlich, wenn Sie die Deduplizierungsfunktion oder den Backup-Katalog verwenden wollen und/oder eine zentrale Bandspeicherung planen. In allen anderen Fällen ist der Storage Node nicht notwendig und wird auch nicht empfohlen.
- **Catalog Service**
  Der Katalogdienst dient nur dazu, verwaltete Backups durchsuchen zu können. Dies kann sehr nützlich sein, wenn Benutzer bestimmte Dateien anfragen und Sie diese in den Backups finden wollen. Eine Volltextsuche in den Backups (nach bestimmten Dokumenteninhalten) wird mit einem zukünftigen Update von Acronis Backup 12.5 eingeführt werden.
  Wenn Sie den Inhalt Ihrer Backup-Archive nicht indizieren wollen, sollten Sie den Katalogdienst nicht installieren.

5.2.2 Backup Agenten

Backup Agenten müssen in jedem Teil Ihrer Umgebung installiert werden, die Sie sichern wollen. Anweisungen zur Installation der verschiedenen Agenten finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#36415.html.

Physische Maschinen

Wir empfehlen, dass Sie den Agenten direkt auf dem Betriebssystem installieren, das auf einer physischen Maschine läuft.

Umgebungen mit virtuellen Maschinen

Dies bedeutet in der Regel, dass Sie einen oder mehrere Agenten installieren, die direkt mit dem Hypervisor kommunizieren, auf dem diese Maschinen ausgeführt werden.

Wir empfehlen folgende Vorgehensweisen:

Hyper-V-Umgebungen

Installieren Sie den Agenten für Hyper-V auf jedem Hyper-V-Host, der in Ihrer Infrastruktur läuft. Die Agenten müssen auch dann auf jedem Host installiert werden, wenn die Hosts in einem Cluster verbunden sind.

Wenn Sie Ihre VMs auf SMB3-Netzwerkfreigaben speichern wollen, sollten Sie nicht vergessen, die Windows-Funktion 'VSS für SMB-Freigaben' zu aktivieren. Ohne diese Einstellung werden Ihre Backups fehlschlagen.

Weitere Informationen (in Englisch) finden Sie hier:
https://blogs.technet.microsoft.com/clausjor/2012/06/14/vss-for-smb-file-shares/

VMware vSphere-Umgebungen

Sie können eine oder mehrere virtuelle Appliances direkt als VM bereitstellen und/oder einen Agenten für VMware (Windows) installieren. Die virtuelle Appliance ist eine Acronis Linux-Instanz (eine von Acronis erstellte spezielle, kleine Linux-Distribution), auf der ein Standard-Agent für VMware läuft.

- Die Standardempfehlung ist, eine virtuelle Appliance auf jedem ESXi-Host in Ihrer virtuellen Umgebung zu installieren. Dies erfolgt automatisch, wenn Sie ein vCenter zu Ihrem Management Server hinzufügen, sofern das DNS richtig konfiguriert ist (S. 39).
- Die Installation auf einer physischen Windows-Maschine wird empfohlen, wenn Sie Offloaded- oder LAN-freie Backups durchführen wollen.
  - Offloaded Backup (Ausgelagertes Backup)
    Wird verwendet, wenn Ihre produktiven ESX(i)-Hosts so stark ausgelastet sind, dass eine zusätzliche Ausführung der virtuellen Appliances nicht wünschenswert ist.
  - 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. Ausführliche Informationen zum LAN-freien Backup finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#37873.html.

Beachten Sie, dass Sie einen Agenten direkt innerhalb einer bestimmten virtuellen Maschine installieren können. Dafür ist keine eigene Lizenz erforderlich.

Dies eignet sich für Szenarien, bei denen kein agentenloses Backup von virtuellen Maschinen unterstützt wird – wie z.B.:

- Virtuelle Laufwerkskonfigurationen (wie RAW-Laufwerke), für die es keine Snapshot-Unterstützung gibt;
- Hypervisor (wie Xen oder RHEV), für die es keine Unterstützung für agentenloses Backup gibt.

5.2.2.1 Dimensionierung für Agent für VMware/Hyper-V

Agenten für VMware/Hyper-V (ob als virtuelle Appliance oder auf einem Windows-System installiert) sind die einzigen Agenten, deren Anforderungen mit der Umgebungsgröße skalieren. Die typischen Mindestanforderungen sind wie folgt:

RAM

- 1 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über 16 GB oder weniger gesamten Arbeitsspeicher verfügt
- 2 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über bis zu 64 GB Arbeitsspeicher verfügt bzw. gleichzeitig 2 bis 4 Maschinen sichert
- 4 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über mehr als 64 GB Arbeitsspeicher verfügt und gleichzeitig 4 bis 10 Maschinen sichert

CPU

- 2 CPU-Threads werden immer empfohlen
- 2 Kerne (4 Threads), wenn gleichzeitig bis zu 5 VMs gesichert werden
- 4 Kerne (8 Threads), wenn gleichzeitig bis zu 10 VMs gesichert werden

5.2.2.2 Überlegungen in puncto DNS-Konfiguration

Die richtige Konfiguration des Domain Name Systems (DNS) ist bei virtuellen Backups sehr wichtig und die häufigste Ursache für zahlreiche Fehler und Probleme. Die Hostnamen diverser Acronis- und VMware-Komponenten müssen über mehrere physische/virtuelle Netzwerke hinweg untereinander korrekt aufgelöst werden können.

Der VMware Agent muss folgende Namen auflösen können:

- den Management Server-Hostnamen
- jeden ESX(i)-Hostnamen
- den vCenter-Hostnamen

Jede der oberen Komponenten muss außerdem in der Lage sein, die Namen der anderen untereinander auflösen zu können. Wenn die Namensauflösung nicht korrekt funktioniert, werden Sie verschiedene Kategorien von Fehlern sehen – von Bereitstellungsproblemen bis zu Backup-Fehlern.

Um diese Fehler zu vermeiden, sollten Sie unseren Empfehlungen folgen:

Wenn Sie in einer Acronis Lösung einen vCenter Server hinzufügen, wird unser Produkt versuchen, auf jedem Host in Ihrer vSphere-Umgebung eine virtuelle Appliance zu installieren. Weitere Informationen dazu finden Sie in der offiziellen Benutzeranleitung:
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#36631.html.

Damit diese automatische Bereitstellung funktioniert, ist es wichtig, dass die Domain-Namen-Auflösung zwischen dem Acronis Management Server und den Gastbetriebssystemen der VMs (die in Ihren ESX(i)-Hosts ausgeführt werden) funktioniert. Das ist notwendig, um sicherstellen zu können, dass der Acronis Agent für VMware (Virtuelle Appliance) nach der Bereitstellung mit einem konfiguriertem DNS-Server in der Lage ist, sich mit dem Acronis Management Server zu verbinden (über dessen Hostnamen). Um Ihnen dabei zu helfen, haben wir mit Update 2 ein Feld eingeführt, mit dem Sie festlegen können, wie sich die Komponenten mit dem Server verbinden sollen – über den Hostnamen oder über die IP-Adresse.

Wir empfehlen, dass Sie statt dem Hostnamen die IP-Adresse auswählen, die der Agent zur Verbindung mit dem Management Server verwenden soll.

Sobald die Appliance für VMware bereitgestellt wurde, sollten Sie die DNS-Auflösung zwischen dem Agenten und den anderen Komponenten überprüfen:

1. Öffnen Sie einen vSphere Client und bauen Sie eine Verbindung zu einem ESX(i)-Host oder vCenter auf.
2. Navigieren Sie zu der virtuellen Appliance, öffnen Sie die Registerkarte **Konsole** und drücken Sie dann die Tastenkombination **Strg**+**Alt**+**F2**, um auf der Appliance in den Befehlszeilenmodus zu wechseln (den Sie mit der Tastenkombination **Alt**+**F1** wieder verlassen können).
3. Geben Sie einen Ping-Befehl ein, um den ESXi-Hostnamen und den vCenter-Namen von der virtuellen Appliance aus aufzulösen:
   `ping Hostname_des_ESXi`
   `ping Hostname_des_vCenters`.
4. Wenn der Ping-Befehl für den Hostnamen nicht erfolgreich ist, haben Sie ein DNS-Namensauflösungsproblem, weswegen VM-Backups von diesem Agenten auch nicht funktionieren werden.

*Wenn der **Port 25** gesperrt ist, wird der **`ping`**-Befehl nicht korrekt funktionieren. Sie können dann stattdessen andere Befehle verwenden – wie **`nslookup`**. Es ist nicht so wichtig, welchen Befehl genau Sie wählen, solange Sie damit überprüfen können, ob eine Verbindung über den Hostnamen erfolgt.*

Sie können das Problem beheben, indem Sie das Netzwerk in der Appliance und in Ihrer virtuellen Umgebung korrekt konfigurieren. Als Workaround können Sie auf jeder Appliance auch die Datei 'hosts' bearbeiten.
Das Bearbeiten der Datei 'hosts' funktioniert folgendermaßen:

1. Öffnen Sie die Konsole der virtuellen Appliance mit folgender Tastenkombination: **Strg**+**Alt**+**F2**.
2. Öffnen Sie die Datei 'hosts' mit folgendem Befehl:
   `vi /etc/hosts`
3. Drücken Sie die Taste **i**, um in den Bearbeitungsmodus zu wechseln.
4. Geben Sie die IP-Adresse und den aufzulösenden Namen des Servers in folgendem Format ein:
   `XXX.XXX.XXX.XXX Hostname`
5. Speichern Sie die Änderungen, indem Sie die Taste **Esc** drücken, geben Sie dann **`:wq`** ein
6. Drücken Sie die **Eingabetaste**.
7. Verlassen Sie die Konsole mit der Tastenkombination **Alt**+**F1**.

5.2.2.3 Prozessauslagerung auf andere Hosts (Off-Host-Verarbeitung)

Eine sehr wichtige neue Funktion von Acronis Backup 12.5 Advanced ist die Fähigkeit von Acronis Agenten, neben Backups noch eine Reihe anderen Datenverarbeitungstasks ausführen zu können. Jeder dieser Tasks kann auf Basis einer eigenen Planung laufen und ist komplett unabhängig von den eigentlichen Backups. Zu den verfügbaren Tasks gehören:

- Backup-Replikation
- Validierung
- Bereinigung
- Konvertierung zu VM
- VM-Replikation

Diese Funktionalität ist unerlässlich, um Backup-Daten so zu verwalten, dass alle Anforderungen eines Backup-Plans erfüllt werden, ohne dass das begrenzte Backup-Fenster überschritten wird. Sie können mit dieser Funktionalität beispielsweise einen Agenten auf Ihrem Backup Storage Server installieren und Archive validieren/bereinigen, ohne die Netzwerkbandbreite und die Backup-Zeiten zu beeinflussen. Oder Sie können Ihre Backups an den Wochenenden direkt von einem Storage zu einem anderen replizieren lassen.

5.2.3 Empfohlene Installationsprozedur

Ausführliche Installationsanweisungen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#36428.html.

Bei einer Installation unter Windows sollten Sie sicherstellen, dass zuvor auf der Maschine alle erforderlichen Linux-Pakete installiert wurden – siehe: https://www.acronis.com/de-de/support/documentation/AcronisBackup_11.7/#22619.html.

Nachfolgend finden Sie unsere Empfehlungen für KMU-Umgebungen:

1. Registrieren Sie Ihr Produkt in Ihrem Acronis Konto. Ausführliche Anweisungen dazu finden Sie hier: https://kb.acronis.com/content/4834
2. Laden Sie die vollständige Installationsdatei herunter, die für Ihr jeweiliges Betriebssystem (Windows oder Linux) passend ist.
   Sie können die Dateien immer direkt aus Ihrem Konto herunterladen, nachdem Sie die Registrierung durchgeführt haben.
3. Installieren Sie den Acronis Management Server, den Backup Agenten, den Monitoring Service, den Bootable Media Builder und die Komponenten zur Remote-Installation auf Ihrem Backup Server.
4. Installieren Sie den Storage Node oder den Katalogdienst (sofern benötigt) auf den Servern, die an Ihre Storage-Infrastruktur angebunden sind, und registrieren Sie diese auf Ihrem Management Server.
5. Richten Sie Ihre Gruppen ein.
6. Konfigurieren Sie Ihre Speicherorte (Storages).
   - Installieren Sie einen separaten Agenten auf oder in der Nähe des Speicherorts (möglichst nah im Netzwerk).
     Dieser Agent wird für Off-Host-Datenverarbeitungstasks (wie Bereinigung, Validierung und Replikationen zu anderen Storages) verwendet.
7. Konfigurieren Sie Ihre Backup-Pläne und wenden Sie diese auf die Gruppen an.

8. Beginnen Sie mit der Bereitstellung der Backup Agenten.
   a. Wir empfehlen normalerweise, Gruppenrichtlinien zu verwenden, um große Mengen von Agenten automatisch zu verteilen.
   b. Sie können die automatische Installation aber auch vom Produkt aus anstoßen (Push-Installation). Beachten Sie, dass die Agenten für Linux und Mac derzeit noch immer manuell installiert werden müssen (auf jeder Maschine, die gesichert werden soll). Die Push-Installationsfunktion für diese Systeme wird mit einem zukünftigen Update von Acronis Backup eingeführt.
   c. Agenten können während der Installation zu administrativen Einheiten hinzugefügt werden, wenn Sie das entsprechende Konto angeben.
9. Wenden Sie Backup-Pläne auf solche Maschinen an, die noch nicht über Gruppen abgedeckt sind.
10. Stellen Sie die Agenten in der Nähe der Speicherorte bereit (möglichst nah im Netzwerk). Diese Agenten werden für Off-Host-Datenverarbeitungstasks verwendet.
11. Erstellen Sie Off-Host-Pläne (Validierungs-, Bereinigungs-, Replikations- und Konvertierungspläne), um Ihre Daten außerhalb von Backup-Fenstern und Netzwerken zu verwalten, damit keine Ressourcen auf geschützten Maschinen beeinträchtigt werden.

5.3 Backup-Plan-Empfehlungen

5.3.1 Backup-Quelle

In der Regel werden Sie wohl komplette Maschinen sichern – und dabei bestimmte Ausschlussregeln verwenden, damit keine unerwünschten Dateien in das Backup aufgenommen werden.

Sie können Laufwerke (Partitionen), einzelne Dateien und Ordner oder Dateikategorien anhand von Dateierweiterungen ausschließen.

Beispielsweise können Sie alle .avi-Dateien in Ihren Backup-Plänen ausschließen, die auf Gruppen angewendet werden, mit denen Notebooks gesichert werden.

5.3.2 Backup-Ziel

Für KMU-Umgebungen gibt es üblicherweise zwei wesentliche Speicheroptionen:

- Sie können alle Backups direkt auf oder in der Nähe der Endpunkt-Agenten selbst speichern lassen. Beispielsweise kann jede Maschine ihr Volume C:\ (Quelle) auf ihrem Volume D:\ (Ziel) speichern. Für diese Szenarien gibt es keine besonderen Empfehlungen. Dies hat den Vorteil einer geringeren Netzwerkauslastung, jedoch auf Kosten eines höheren Verwaltungsaufwands (denn jeder Speicherplatz muss einzeln angesprochen werden). Diese Option ist empfehlenswert, wenn Sie Wiederherstellungen im großen Umfang durchführen müssen, bei denen Hunderte oder Tausende von Maschinen gleichzeitig und mit minimaler Auswirkung auf die Produktion wieder betriebsbereit gemacht werden müssen. Weitere Informationen finden Sie im Abschnitt mit den Empfehlungen für Wiederherstellungen.
- Sie können alle Backups zentral speichern.
  Bei große Umgebungen sind dafür mehrere Netzwerksegmente mit eigenem Storage und/oder schnelle Netzwerkverbindungen zu diesem Storage notwendig. Vergleichen Sie dazu den Abschnitt mit den „Überlegungen in puncto Storage“ (S. 45).
  Wenn Backups zentral gespeichert werden, sollten alle Datenverarbeitungstasks (wie Validierung oder Replikation) von einem dedizierten Agenten durchgeführt werden, der an diesen Storage angebunden ist.

5.3.3 Planung

Ihr Netzwerk ist zumeist der wichtigste Engpass für Ihre Backups. nur eine begrenzte Anzahl von Backups kann gleichzeitig in einem Subnetz-Segment ausgeführt werden, ohne dieses zu überlasten.

Daher muss die Backup-Planung zwischen Ihren RPO-Anforderungen (Recovery Point Objectives), der insgesamt zu sichernden Datenmenge und der Netzwerkbandbreite, die zur Übertragung dieser Daten verfügbar ist, abgewogen werden. Bei typischen KMU-Größen (ein paar Dutzend Geräte, einige Terabyte an Daten, ein Backup-Plan mit täglichen inkrementelle Backups) sind normalerweise keine besonderen Überlegungen notwendig.

Wenn Ihre Umgebung jedoch eher größer ist, ein stark belastetes Netzwerk hat oder Sie aus anderen Gründen Ihre Umgebung nicht mit einem einzigen Backup-Schema abdecken können, empfiehlt es sich, die Backup-Umgebung in sinnvolle benutzerdefinierte Gruppen aufzuteilen. Weitere Informationen zum Erstellen von Gruppen finden Sie in der Produktdokumentation.

Jede Gruppe sollte diejenige Anzahl von Agenten enthalten, die notwendig sind, um das Backup innerhalb des zugewiesenen Backup-Fensters abschließen zu können. Bei der Umsetzung dieser Aufgabe hilft Ihnen der Ressourcennutzungsrechner (S. 8).

Es gibt weitere Faktoren, die die Backup-Zeit über die erwartete Netzwerkbandbreite hinaus verlängern. So kann beispielsweise die Erfassung der Applikations-Metadaten bei einem applikationskonformen VM-Backup eine längere Zeit benötigen, wenn es ein Problem mit der Quellapplikation gibt. Sie sollten daher das erste Backup von Ihrer Gruppe überwachen, um sicherzustellen, dass es keine deutlichen Ausreißer gibt.

Das empfohlene Backup-Schema ist **Nur inkrementell**, weil die Anzahl der Voll-Backups dabei auf ein Minimum (nämlich nur das erste) reduziert wird.

Eine weitere Option besteht darin, das Backup direkt auf jeder zu sichernden Ressource zu speichern. In diesem Fall bedarf es für die Planung keiner besonderen Überlegungen, da sich das Backup nicht mehr auf das Netzwerk auswirken wird.

Beide Methoden funktionieren gleich gut und sind mehr von Ihren Wiederherstellungsszenarien und dem verfügbaren Speicherplatz abhängig.

5.3.4 Aufbewahrungszeiten

Aufbewahrungsfristen basieren oft auf externen Richtlinien oder Compliance-Regeln. Sie können die zu erwartende Größe der Backups für die Aufbewahrungsdauer mithilfe des Ressourcennutzungsrechners (S. 8) abschätzen.

Wenn der als primäres Backup-Ziel verwendete Storage nicht genügend groß sein sollte, können Sie spezielle Replikationstasks planen, um die Daten zur Langzeitaufbewahrung auf einen anderen, billigeren Storage zu verschieben.

Sie können Ihre Backups beispielsweise in die Acronis Cloud replizieren oder einen Band-basierten Storage verwenden.

Wenn Sie einen sehr großen zentralen Storage für Ihre Backups verwenden, empfehlen wir dringend, keine Aufbewahrungsregeln in Ihrem Backup-Plan zu verwenden. Legen Sie für das Backup die Aufbewahrungseinstellung **Backups unbegrenzt behalten** fest. Der Grund ist, dass alle Bereinigungsaufgaben, die Sie direkt mit in den Backup-Plan integrieren, von jedem dieser Backup Agenten selbst ausgeführt werden, sobald das Backup abgeschlossen wurde. Diese Vorgehensweise führt zu einer beträchtlichen Belastung der Agenten und des Netzwerks, wenn Tausende von Agenten versuchen, sofort nach einem Backup auch noch eine Bereinigung durchzuführen.

Installieren Sie stattdessen auf dem Storage (oder so nah wie möglich zu diesem) einen separaten Agenten, für den Sie einen eigenen **Bereinigungsplan** festlegen. Diese Bereinigungen werden dann von diesem einzelnen Agenten nach je eigenen Plänen ausgeführt, wobei nur eine minimale bis keine Netzwerklast verursacht wird.

5.3.5 Replikation, Konvertierung und Validierung

Ähnlich wie bei der Bereinigungsprozedur gilt : legen Sie keine Replikations- oder Validierungsoptionen mit in einem Backup-Plan fest, der einen zentralen Storage als Ziel verwendet.

Stattdessen können Sie separate „Mini-Pläne“ erstellen, die Aufgaben wie Replikation oder Validierung eigenständig außerhalb der Stoßzeiten durchführen.

Der Agent, der diese ausgelagerten Aktionen (Off-Host-Prozesse) durchführt, sollte möglichst nah im Netzwerk zum Storage installiert werden, über die maximale Bandbreite verfügen und vorzugsweise direkt auf dem Storage selbst ausgeführt werden.

Dies gilt nicht bei Szenarien, bei denen jeder Agent ein Backup zu seinem eigenen lokalen Speicherort erstellt. In diesem Fall müssen die zusätzlichen Datenverarbeitungstasks (wie Validierung) in denselben Backup-Plan integriert werden.

5.3.6 Weitere Empfehlungen

Benachrichtigungen, Alarmmeldungen und Berichte

Um den administrativen Aufwand für die Handhabung dieser Informationen zu reduzieren, sollten Sie folgende Tipps beachten:

- Deaktivieren Sie alle nicht benötigten Alarmtypen in Ihrer Umgebung.
  Wenn Sie beispielsweise Notebooks oder andere Mobilgeräte sichern, ist die Alarmmeldung **Backup-Status ist unbekannt** normalerweise nicht sonderlich nützlich. Denn dieser Alarmtyp wird ständig ausgelöst, wenn Mitarbeiter das Netzwerk verlassen und die Agenten daher nicht mehr unter Kontrolle des Management Server sind.

- Zudem können Sie für bestimmte Alarmmeldungen die Priorität erhöhen oder senken.

  Diese Änderungen gelten auf der Ebene des kompletten Management Servers und können derzeit noch nicht pro Benutzer oder Organisationseinheit angepasst werden. Diese Funktionalität wird mit einem zukünftigen Update von Acronis Backup 12.5 eingeführt.

- Benachrichtigungen werden normalweise gesendet, sobald ein Alarm aktiviert wurde.
  Jeder Alarmkontext ist für den jeweiligen Agenten und Plan spezifizisch, für den er aktiviert wurde. Wenn derselbe Plan also bei zwei Agenten fehlschlägt oder derselbe Agent zwei verschiedene Planfehler hat, werden zwei Alerts generiert und zwei Benachrichtigungen gesendet. Bei einer Skalierung auf Dutzende Agenten würden gängige Fehler (wie Netzwerkstörungen) also Dutzende von Benachrichtigungen durch dasselbe Problem bedeuten.
  Wir empfehlen daher, „Benachrichtigungen pro Alarm“ nur für die wichtigsten Alarmtypen und nur bei solchen Plänen einzustellen, die wichtige Infrastrukturen abdecken und sofortige Reaktionen bei Fehlern verlangen. Nutzen Sie bei weniger wichtigen Maschinen stattdessen Sie die täglichen geplanten Alarmberichte und die Berichtsfunktionen, um einen täglichen Überblick über den Maschinenstatus zu erhalten.
- Verwenden Sie den Alarm '**Keine erfolgreichen Backups für eine spezifizierte Anzahl aufeinanderfolgender Tage**' in den Backup-Plan-Optionen.
  Dieser Alarm wird nur aktiviert, wenn für ein Gerät nach einer bestimmten Anzahl von Tagen kein erfolgreiches Backup erstellt werden konnte. Dies ist ein nützlicher Weg, um bei Maschinen, bei denen ein einzelnes verpasstes Backup nicht so kritisch ist, die Backup-Fehler eines einzelnen Tages zu ignorieren.

Fehler-Behandlungen und -Wiederholungen

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen (beispielsweise, wenn kein Netzwerk mehr verfügbar ist). Die Standardvorgabe sind 30 erneute Versuche in Intervallen von 30 Sekunden (über 15 Minuten). Für kleinere Backup-Jobs ist das nicht weiter kritisch. Aber wenn Sie Backups von großen Maschinengruppen parallel ausführen, kann dies das Backup-Fenster schon signifikant beeinflussen. Sie können den Wert daher auf 10 Neuversuche mit 30-Sekunden-Intervallen senken.

Dateiformat

Verwenden Sie wann immer möglich das Standard-Backup-Format 'Version 12' (https://www.acronis.com/en-us/support/documentation/AcronisBackup_12.5/#38763.html).

Active Protection

Active Protection ist derzeit nur für Maschinen mit Windows 7 (und höher) sowie Windows Server 2008 R2 (und höher) verfügbar. Der Agent für Windows muss auf der Maschine installiert sein.

Wir empfehlen, Active Protection auf allen Maschinen zu aktivieren, sofern diese nicht unter zu knappen CPU-Ressourcen leiden.
Bei starken Dateizugriffen bewirkt Active Protection üblicherweise einen CPU-Overhead von einigen wenigen CPU-Prozenten im System.

Selbstsicherung des Management Server

Stellen Sie sicher, dass auch der Management Server selbst von einem Backup-Plan gesichert wird.

Er muss nicht unbedingt gesichert werden, da Sie Ihre komplette Umgebung auch per Disaster Recovery wiederherstellen können, indem Sie isoliert unsere Boot-Medien verwenden. Aber ohne ein Backup des Management Servers müssen Sie diesen neu installieren, alle Agenten wieder hinzufügen und die komplette Konfiguration nach der Wiederherstellung Ihrer gesicherten Geräte neu durchführen.

Wenn Sie ein Backup des Management Server haben, stehen Ihnen außerdem noch weitere Optionen zur Verfügung – beisspielsweise können Sie das als virtuelle Maschine ausführen oder in eine virtuelle Standby-Maschine konvertieren, um Wiederherstellungsprozesse zu beschleunigen (vgl. die Empfehlungen zu Wiederherstellungen (S. 67)).

5.4 Überlegungen in puncto Storage

Wie weiter oben erwähnt, ist eine wichtige Überlegung die Bandbreite Ihres zentralen Storage im Hinblick auf die Anzahl der gleichzeitigen Backups, die diesen Storage als Speicherziel verwenden.

Über den Ressourcennutzungsrechner (S. 8) können Sie abschätzen, wie viele Storage-Segmente Sie auf Basis von vorgegebenen Netzwerkbandbreiten und Backup-Fenstern benötigen, um all Ihre Maschinen per Voll-Backup zu sichern.

5.4.1 Deduplizierung

Die Deduplizierung erfolgt bei Acronis Backup 12.5 immer „an der Quelle“ – was bedeutet, dass die Hash-Berechnung vom Agenten durchgeführt wird und somit keine Daten, die bereits in einem Backup vorhanden sind, erneut über das Netzwerk gesendet werden. Dies ist eine großartige Möglichkeit, sowohl den Speicherbedarf als auch die Netzwerkbandbreite zu senken, insbesondere wenn Sie Backups von Maschinen erstellen, die relativ ähnliche Daten enthalten.

Beachten Sie, dass eine Deduplizierung ein komplexer Prozess ist, den Sie sich mit der Notwendigkeit für einen relativ leistungsfähigen Storage-Server und dem Verzicht auf bestimmte Funktionen erkaufen müssen. Die derzeit wichtigste fehlende Funktion ist die Unterstützung des Version-12-Backup-Formats, was jedoch mit einem zukünftigen Update eingeführt werden wird.

Wenn Sie die Deduplizierungsfunktion verwenden wollen, sollten Sie mehr über die Deduplizierungstechnologie und die dazugehörigen empfohlenen Vorgehensweisen im entsprechenden Abschnitt des offiziellen Benutzerhandbuchs informieren:
https://www.acronis.com/en-us/support/documentation/AcronisBackup_12.5/#7143.html.

Deduplizierung ist dann am sinnvollsten, wenn Sie viele Maschinen per Backup sichern wollen und diese Maschinen zu einem beträchtlichen Prozentsatz identische Daten haben. Oder wenn Sie Backups auf einem Storage speichern müssen, der nur per WAN/Internet oder einer anderen Verbindung mit geringer Bandbreite verfügbar ist.

Bei KMU-Umgebungen ist das eher selten der Fall, weshalb es hier meistens empfehlenswert ist, auf eine Deduplizierung zu verzichten.

Deduplizierung und Replikation

Die allgemeine Empfehlung lautet, dass eine Replikation immer **zu** einem deduplizierten Speicherort erfolgen sollte – und niemals **von** einem deduplizierten Speicherort aus.

Dies ist darin begründet, dass Replikationen bei Acronis Backup keine einfachen Kopien der Archivdaten sind, sondern eher erneuten Backups („Re-Backups“) als Kopiervorgängen entsprechen. Wenn Sie also eine Replikation zu einem deduplizierten Speicherort durchführen, werden – genau wie bei einem Backup – nur einmalige Daten (ohne Duplikate) übertragen. Dies ist ein großer Vorteil, wenn Sie z.B. lokale Backups durchführen und diese dann zu einem externen deduplizierten Speicherort replizieren.

Dies bedeutet auch, dass Daten, die von einem deduplizierten Speicherort aus repliziert werden, während dieser Replikation rekonstituiert werden. Oder mit anderen Worten: die resultierende Datei ist nicht mehr dedupliziert und kann unabhängig vom Deduplizierungsdienst auf dem Storage Node verwendet werden.

Dieser Datenrekonstitutionsprozess verursacht einigen Overhead für die Replikationsaktion und würde dementsprechend länger dauern, wenn Sie eine Replikation von einen nicht-deduplizierten Speicherort durchführen. Dies erschwert Skalierungen, insbesondere wenn das Ziel eine Bandbibliothek ist und daher anfällig für Verzögerungen ist.

5.4.2 Bandgeräte

Acronis ist bestrebt, die Unterstützung für Bandgeräte fortzusetzen und auszuweiten.

Eine Liste von getesteten und unterstützten Bandgeräten finden Sie in der Hardware-Kompatibilitätsliste für Bandlaufwerke (https://go.acronis.com/acronis-backup-advanced-tape-hcl).

Wenn Sie die Kompatibilität Ihres eigenen Bandgerätes testen wollen, können Sie das Bandkompatibilitätstool verwenden (https://kb.acronis.com/content/57237).

Wenn das Tool ein Problem findet, kontaktieren Sie bitte den Acronis Support, damit das Problem zu unserer Entwicklungsabteilung weitergeleitet und gelöst werden kann.

Ein Agent kann Backups direkt zu einem Bandlaufwerk erstellen. Wenn Sie eine einzelne oder isolierte Maschine haben und Band-Backups erstellen wollen, müssen Sie das Bandlaufwerk direkt an der Maschine anschließen, auf welcher der Agent installiert ist.

5.4.2.1 Storage Node für Bänder

Der Acronis Storage Node wird benötigt, wenn Sie eine größere Menge von Maschinen per Backup auf (ein oder mehrere) Bandlaufwerke sichern wollen. Das Bandgerät muss dafür an die Maschine des Storage Nodes angeschlossen sein.

Wenn Sie sowohl Bänder als auch Deduplizierung verwenden wollen, empfehlen wir, für jeden Storage einen eigenen Storage Node zu installieren, da Sie mit einem Management Server praktisch unbegrenzt viele Storage Nodes verwalten können.

5.4.2.2 Bandverwaltungsdatenbank

Die Informationen über alle Bandgeräte, Bänder und Backup-Inhalte werden in der Bandverwaltungsdatenbank gespeichert, die sich wiederum auf der Maschine befindet, an welcher das Bandgerät angeschlossen ist.Der Standardpfad für die Datenbank ist:

- Windows 7, Windows Server 2008 und höher:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database
- Linux:
  /var/lib/Acronis/BackupAndRecovery/ARSM/Database

Die Datenbankgröße hängt von der Zahl der auf den Bändern gespeicherten Backups ab – wobei etwa 10 MB auf einhundert Backups kommen. Mit einigen wenigen Maschinen ist dies –auch mit längeren Aufbewahrungszeiten – kein Problem.

Sie sollten jedoch sicherstellen, dass Sie genügend Speicherplatz für diese Datenbank auf Ihrem System haben. Falls Sie unsicher sind, sollten Sie vor dem Start des ersten Band-Backups den Pfad entsprechend überprüfen.

So verlagern Sie die Datenbank unter Windows:

1. Stoppen Sie den den Dienst '**Removable Storage Management**'.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Ermitteln Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings**.
4. Spezifizieren Sie den Pfad zum neuen Speicherort im Registry-Wert `ArsmDmlDbProtocol`. Der String darf bis zu 32765 Zeichen enthalten.
5. Starten Sie den den Dienst '**Removable Storage Management**' wieder.

So verlagern Sie die Datenbank unter Linux:

1. Stoppen Sie den Dienst '**acronis_rsm**'.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Öffnen Sie die Konfigurationsdatei **/etc/Acronis/ARSM.config** in einem Text-Editor.
4. Suchen Sie nach folgender Zeile: `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Ändern Sie den Pfad unter dieser Ziele.
6. Speichern Sie die Datei.
7. Starten Sie den Dienst '**acronis_rsm**' wieder.

Sie dürfen die Band-Datenbank nicht löschen! Denn dies würde erfordern, dass all Bänder erneut gescannt werden müssen, um die darauf gespeicherten Backups wieder verwendbar zu machen. Und dies ist ein sehr zweitaufwendiger und fehleranfälliger Prozess.

5.4.2.3 Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren

Diese Option ist standardmäßig deaktiviert. Wenn Sie diese Option in den Bandverwaltungseinstellungen Ihres Backup-Plans aktivieren, können Sie aus Image-Backups, die auf Ihren Bändern gespeichert sind, auch einzelne Dateien wiederherstellen.

Beachten Sie, dass Sie sich diese Funktionalität mit hohen Speicherplatzkosten erkaufen. Wenn die Funktionalität aktiviert ist, erstellt die Software bei jedem Backup zusätzliche Dateien auf einem Festplattenlaufwerk der Maschine, an der das Bandgerät angeschlossen ist. Datei-Recovery von Laufwerk-Backups ist möglich, solange diese zusätzlichen Dateien intakt sind. Die Dateien werden automatisch gelöscht, wenn das Band, auf dem die entsprechenden Backups gespeichert sind, gelöscht, entfernt oder überschrieben wird.

Diese zusätzlichen Dateien befinden sich an diesem Speicherort:

- In Windows 7, Windows Server 2008 und höher:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation
- In Linux:
  /var/lib/Acronis/BackupAndRecovery/TapeLocation

Der von diesen zusätzlichen Dateien belegte Speicherplatz hängt von der Anzahl der Dateien im entsprechenden Backup ab. Beim Voll-Backup eines Laufwerks mit ungefähr 20.000 Dateien (typisches Laufwerk-Backup einer Workstation) belegen die zusätzlichen Dateien ca. 150 MB. Ein einzelnes Voll-Backup eines Servers mit 250.000 Dateien kann etwa 700 MB an zusätzlichen Dateien erzeugen.

Auch in kleinen Umgebungen kann die Größe dieser Dateien schnell auf Dutzende von Gigabyte anwachsen.

Wir empfohlen daher, dass Sie diese Option deaktiviert lassen, wenn Sie die Option nicht unbedingt benötigen. Wenn doch, sollten Sie sicherstellen, dass der verwendete Speicherort oder Storage Node von der Speicherplatzgröße auf diese zusätzlichen Dateien ausgelegt ist.

5.4.2.4 Bandsätze

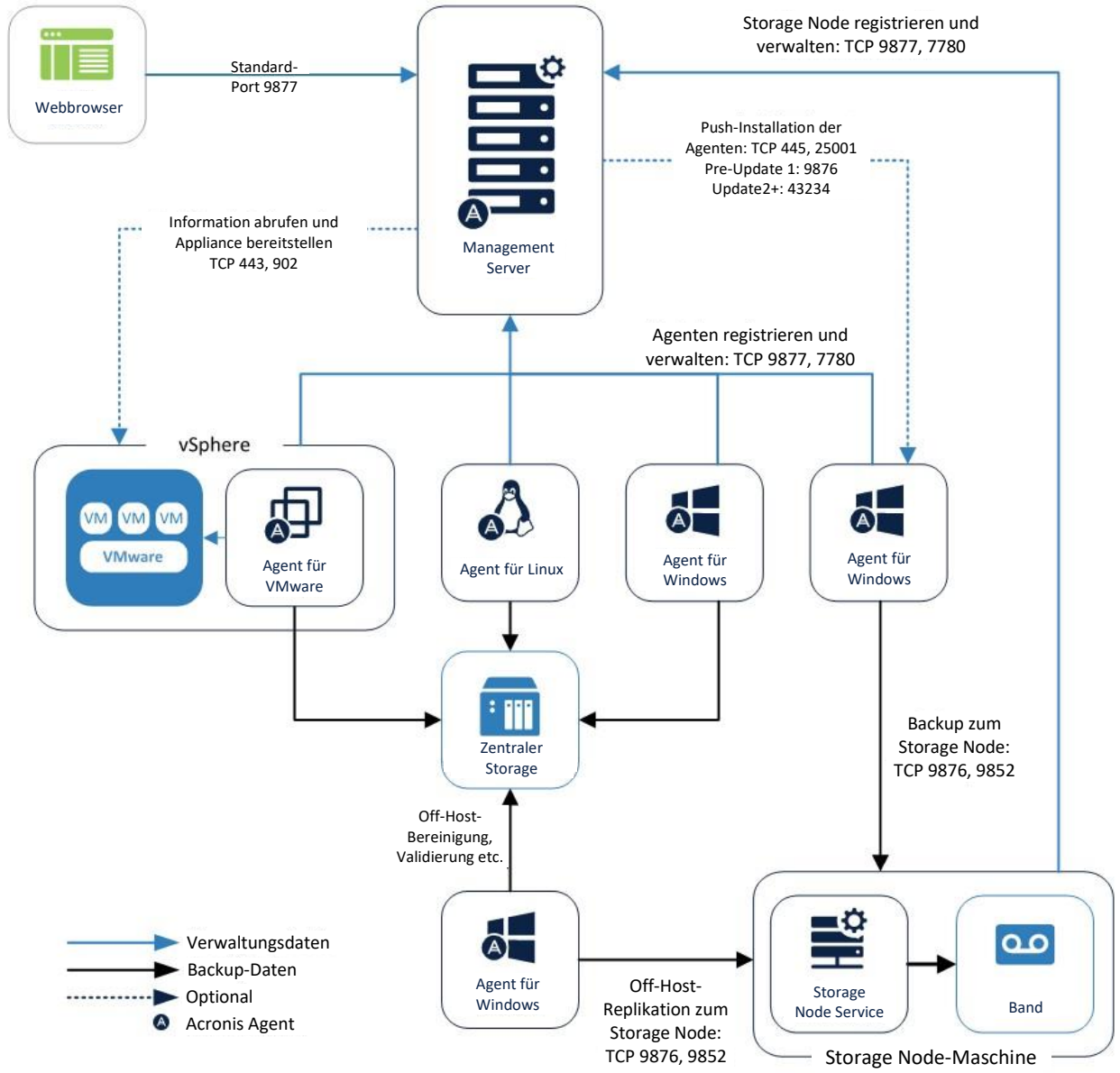
Sie können in Acronis Backup 12.5 Bandsätze erstellen, um flexibler zu verwalten, welche Geräte ihre Backups zu welchen Bändern erstellen – und unter welchen Bedingungen dies geschehen soll. Beispielsweise können Sie an jedem einzelnen Werktag ein bestimmtes Band verwenden und am Wochenende wiederum einen anderen Satz von Bändern.

Weitere Informationen finden Sie in diesem Knowledge Base-Artikel über Bandsätze:
https://kb.acronis.com/content/59315.

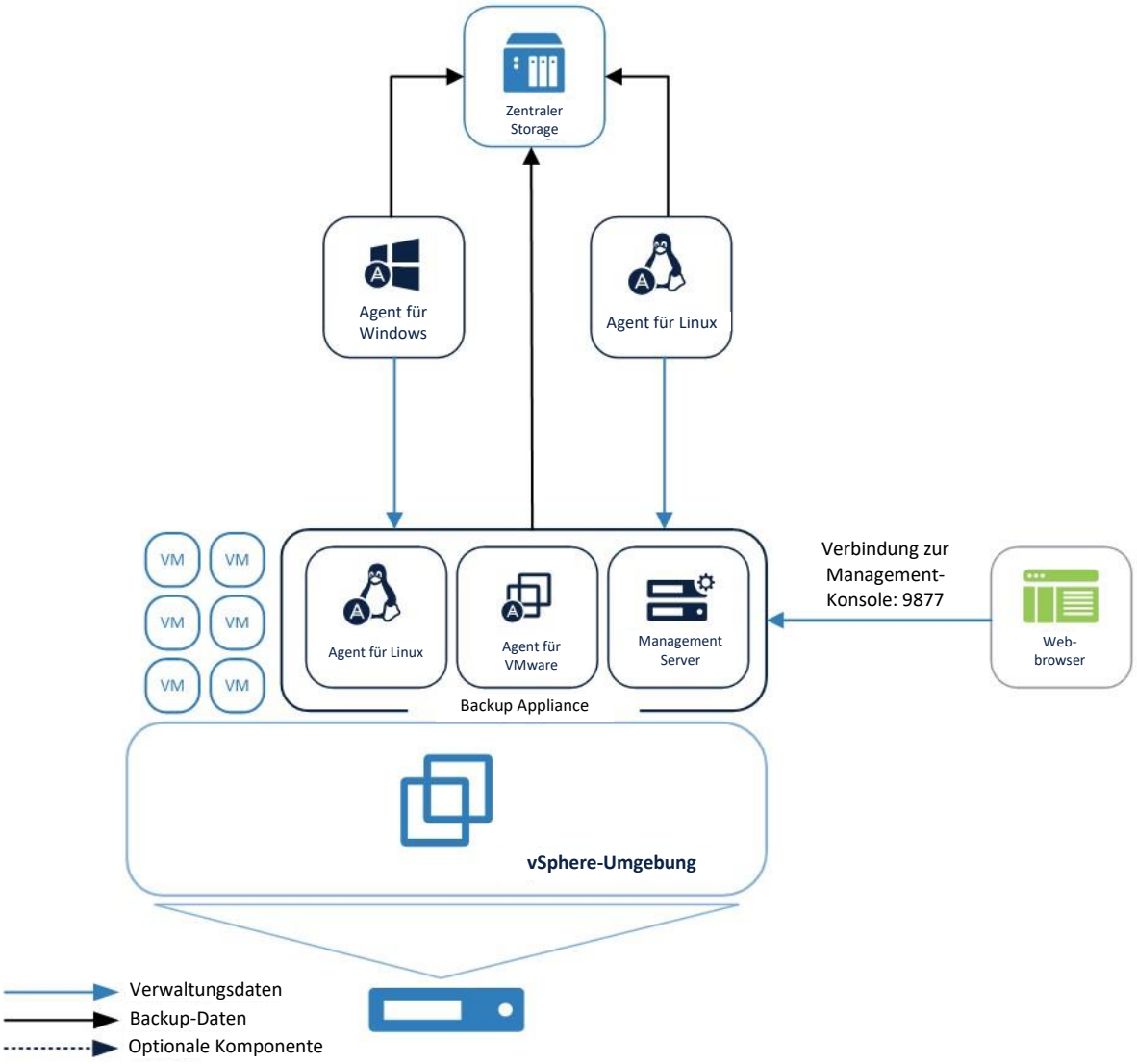
5.5 Netzwerkdiagramme und Ports

Das vollständige Netzwerkdiagramm können Sie im Anhang B (S. 82) finden.

Nachfolgend finden Sie das Netzwerkdiagramm für typische KMU-Umgebungen.



Nachfolgend finden Sie das Netzwerkdiagramm, wenn Sie nur die Acronis Backup Appliance verwenden wollen.



6 Große Umgebungen

Beschreibung der Umgebung

Solche Umgebungen bestehen aus Hunderten von Maschinen, die mit einer dedizierten Backup-Infrastruktur gesichert werden müssen.

Der Knackpunkt bei diesen Umgebungen ist, dass die gleichzeitige Sicherung von Hunderten von Maschinen jedes Netzwerk überlastet und diese sehr langsam macht. Um dies zu vermeiden, müssen die Management-Komponenten auf geeigneter dedizierter Hardware installiert und die Backup-Pläne sorgfältig in puncto Zeitplanung verwaltet werden.

Ab Update 3.1 kann Acronis Backup bis zu 4.000 Agenten pro Management Server unterstützen, wenn dieser entsprechend unseren Empfehlungen konfiguriert wurde.

6.1 Vorbereitungen für die Bereitstellung

Dieser Abschnitt behandelt die Anforderungen und Empfehlungen, die bei einer Bereitstellung von Acronis Backup 12.5 in großen Umgebungen beachtet werden müssen.

6.1.1 Empfohlene Software-Anforderungen für große Umgebungen

Die nachfolgende Liste enthält die Betriebssysteme, die Sie für eine Installation des Management Servers in einer KMU-Umgebung verwenden können.

Bei Umgebungen, die überwiegend auf Windows basieren, empfehlen wir, den Management Server auf Windows Server 2012 R2 (oder höher) zu installieren. Grundsätzlich ist es aber auch möglich, eine Maschine mit einer älteren Windows-Version oder mit Linux zu verwenden.

Beachten Sie außerdem, dass Sie unter Linux keine administrativen Einheiten erstellen können.

Windows

Windows Server 2008 – Standard, Enterprise und Datacenter Editionen (x86, x64)
Windows Small Business Server 2008
Windows 7 – alle Editionen (x86, x64)
Windows Server 2008 R2 – Standard, Enterprise, Datacenter und Foundation 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 2008/2008 R2/2012/2012 R2/2016
Windows 10 – Home, Pro, Education, Enterprise und IoT Enterprise Editionen
Windows Server 2016 – alle Installationsoptionen, mit Ausname des Nano Servers
Obwohl es nicht zwingend erforderlich ist, ein Windows Server-Betriebssystem zu verwenden, ist es für große Umgebungen aus Gründen der Skalierbarkeit, Sicherheit und Stabilität dennoch ratsam.

Linux

Linux mit Kernel 2.6.23 bis 4.15 und glibc 2.3.4 (oder höher)
Verschiedene x86_64-Linux-Distributionen, inklusive:
Red Hat Enterprise Linux 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5
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
Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24
SUSE Linux Enterprise Server 11, 12
Debian 5.x, 6.x, 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, 9.0, 9.1, 9.2, 9.3, 9.4
CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4
Oracle Linux 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5 – sowohl Unbreakable Enterprise Kernel als auch Red Hat Compatible Kernel
CloudLinux 6.x, 7, 7.1
ALT Linux 7.0

6.1.2 Management Server-Datenbank

Der Acronis Management Server verwendet standardmäßig ein SQLite-Datenbank-Backend, um seine Daten in Windows- und Linux-Umgebungen zu speichern.

Für größere Umgebungen empfehlen wir, dass Sie statt der standardmäßigen SQLite-Datenbank eine robustere und sicherere Lösung verwenden.

- Bei Windows empfehlen wir, dass Sie während der Installation die Microsoft SQL-Datenbank auswählen.
- Bei Linux empfehlen wir die Verwendung einer PostgreSQL-Datenbank. Deren Konfiguration ist in folgendem Knowledge Base-Artikel erläutert: https://kb.acronis.com/content/60395.

6.1.2.1 Microsoft SQL-Datenbank-Empfehlungen

Wir empfehlen folgende Konfiguration, wenn Sie Tausende von Agenten auf einem Microsoft SQL-Backend für die Datenbank ausführen:

- 8 CPU-Kerne
- 32 GB RAM
- 100 GB freier Speicherplatz für die Datenbank-Instanz

Um eine maximale Performance zu erreichen, sollte die Microsoft SQL-Instanz auf dem gleichen Server wie der Management Server ausgeführt werden und **SSPI** zur Authentifizierung verwendet werden.

6.1.3 Hardware-Anforderungen und Dimensionierung

Die Hardware-Anforderungen für die meisten peripheren Acronis Backup 12.5-Komponenten (die Backup-Agenten eingeschlossen) ändern sich nicht bei einer Skalierung. Unabhängig davon, wie viele Agenten installiert sind: die individuellen Anforderungen für jeden Agenten hängen von der Menge der Daten ab, die auf jeder Maschine gesichert werden und nicht von der Gesamtzahl der Agenten.

Die Hardware-Anforderungen für die zentralen Management-Komponenten skalieren mit der Anzahl der zu verwaltenden Geräte (insbesondere bei Umgebungen mit über 200 Maschinen).

Der Management Server ist nur wenig CPU- bzw. RAM-abhängig, daher ist der Schlüsselfaktor für große Umgebungen der I/O-Durchsatz des Storage-Subsystems, das von den verschiedenen Datenbanken der Management Server-Dienste verwendet wird.

Dies liegt daran, dass die Backups in großen Umgebungen Hunderte bis Tausende von IOPs (Eingabe-/Ausgabe-Aktionen pro Sekunde) erzeugen, weswegen Standard-Festplatten als Storage-Hardware schnell zum Flaschenhals werden können.

Wir empfehlen daher, dass Sie performante Laufwerke (wie SSDs, mit hoher IOPS-Leistung) für den Management Server in großen Umgebungen verwenden.

Ausführlichere Empfehlungen zu der für den Betrieb Ihrer Backup-Infrastruktur erforderlichen Hardware finden Sie auch in unserem Ressourcennutzungsrechner (S. 8).

6.1.4 Bereitstellungstyp

Der Acronis Backup 12.5 Management Server kann als physischer Server, virtuelle Maschine, Acronis Backup Appliance und schließlich als Cloud-Plattform bereitgestellt werden, um Ihre lokale Backup-Infrastruktur zu verwalten.

Bei große Umgebungen ist es aufgrund der Hardware-Anforderungen und der IOPS-Last auf dem Laufwerk-Subsystem empfehlenswert, einen physischen Server zu verwenden.

Beim Acronis Backup Cloud-Bereitstellungsmodell wird der gleiche Acronis Backup 12.5 Management Server verwendet – er wird lediglich von einem Acronis Datenzentrum aus bereitgestellt. Die Agenten werden über das Internet mit dem Management Server in der Cloud verbunden. Dieses Bereitstellungsmodell empfiehlt sich aber nicht als Hauptszenario für große Umgebungen, weil einige neue Funktionen, die speziell in großen Umgebungen verwendet werden, nur bei lokaler Bereitstellungen verfügbar sind. Die Verfügbarkeit für Cloud-Bereitstellungen erfolgt in zukünftigen Produktversionen.

6.1.5 Anpassungen nach dem Deployment für große Umgebungen

Wenn Sie mehr als 1.000 Ressourcen hinzufügen möchten, empfehlen wir, das Aktualisierungsintervall für die Berichtsdaten anzupassen, um die Auslastung für den Management Server zu verringern.

Das Intervall steuert, wie häufig Widget-Daten zu Storage, Gruppenmitgliedschaft und Lizenznutzung aktualisiert werden. Dies ist ein Kompromiss zwischen CPU-Belastung und Aktualisierungsintervall für die Berichtsdaten.

Wenn mehr als 2.000 Ressourcen geschützt werden sollen, wird ein Intervall von einer Stunde empfohlen. Das kann folgendermaßen erfolgen:

1. Öffnen Sie die Konfigurationsdatei für den Monitoring Service.
   Unter Windows: `%PROGRAMDATA%\Acronis\MonitoringServer\config.ini`
   In Linux: `/var/lib/Acronis/MonitoringServer/config.ini`
2. Suchen Sie die Zeilen unten:
```
; Intervall zur Sammlung von Kennzahlen für Depots in Sekunden (standardmäßig 1 Minute)
; vault_collection_interval = 60
; Intervall zur Sammlung von Kennzahlen für Gruppen in Sekunden (standardmäßig 1 Minute)
; group_collection_interval = 60
; Intervall zur Sammlung von Kennzahlen für Depots in Sekunden (standardmäßig 1 Minute)
; license_collection_interval = 60
```
3. Heben Sie die Kommentierungskennzeichnung auf und legen Sie die tatsächlichen Werte auf 3600 fest (1 Stunde in Sekunden)
```
; Intervall zur Sammlung von Kennzahlen für Depots in Sekunden (standardmäßig 1 Minute)
vault_collection_interval = 3600
; Intervall zur Sammlung von Kennzahlen für Gruppen in Sekunden (standardmäßig 1 Minute)
group_collection_interval = 3600
; Intervall zur Sammlung von Kennzahlen für Depots in Sekunden (standardmäßig 1 Minute)
license_collection_interval = 3600
```

6.2 Komponenten und Installation

6.2.1 Management-Komponenten

Folgende Komponenten müssen auf dem Server installiert sein, der für die Backup-Verwaltung zuständig ist:

- **Management Server**
- **Monitoring Service**

In einigen Fällen ist es empfehlenswert, die nachfolgenden Komponenten ebenfalls auf demselben Server zu installieren.

- **Komponenten zur Remote-Installation** (nur für Windows)
  Mit dieser Komponente können Sie die Remote-Installation von Windows-Agenten von der Benutzeroberfläche des Produkts aus anstoßen. Wenn Sie die Agenten mithilfe einer Gruppenrichtlinie installieren wollen, wird diese Komponente nicht benötigt.
- **Backup Agent**
  Mit dieser Komponente können Sie den Management Server selbst sichern.
  Da der Management Server für die Backup-Funktion der Agenten nicht zwingend notwendig ist, können Sie diesen Schritt prinzipiell überspringen. Sie müssen jedoch die komplette Konfiguration neu installieren und wiederholen (was bei großen Umgebungen einige Zeit dauern kann), wenn der Server ausfällt und Sie kein Backup von diesem haben. Empfehlungen zur Selbstsicherung des Management Servers finden Sie in einem unteren Abschnitt.
  Es gibt derzeit keine Möglichkeit, die Konfiguration des Management Servers zu importieren oder zu exportieren.
  - Diese Funktionalität wird mit einem zukünftigen Update von Acronis Backup eingeführt.
  - Es gibt keine bereits integrierte Möglichkeit, einen Management Server-Cluster aufzubauen.
  - Zur Sicherung des Management Servers benötigen Sie eine Lizenz, die dem Betriebssystem entsprechen muss, welches Sie für den Management Server verwenden.
  -
  .

Die folgenden Komponenten müssen installiert werden, aber nicht unbedingt parallel zum Management Server. Wenn es bequemer für Sie ist, können die nachfolgenden Komponenten auf jeder Maschine installiert werden, auf der ein lizenzierter Agent läuft:

- **Bootable Media Builder**
- **Microsoft SQL-Datenbank** (für Umgebungen mit mehr als 900 Agenten)

Für die nachfolgenden Komponenten sollte dedizierte Hardware verwendet werden – jedoch nur, wenn Ihre Backup-Pläne und/oder Ihr Storage-Typ dies erfordert.

Über den Ressourcennutzungsrechner (S. 8) erhalten Sie Empfehlungen zur Installation und der benötigten Anzahl dieser Komponenten.

- **Acronis Storage Node**
  Diese Komponente wird benötigt, wenn Sie verwaltete Backup-Speicherorte verwenden wollen. Diese sind erforderlich, wenn Sie die Deduplizierungsfunktion oder den Backup-Katalog verwenden wollen und/oder eine zentrale Bandspeicherung planen. In allen anderen Fällen ist der Storage Node nicht notwendig und wird auch nicht empfohlen.
- **Catalog Service**
  Der Katalogdienst dient nur dazu, verwaltete Backups durchsuchen zu können. Dies kann sehr nützlich sein, wenn Benutzer bestimmte Dateien anfragen und Sie diese in den Backups finden wollen. Eine Volltextsuche in den Backups (nach bestimmten Dokumenteninhalten) wird mit einem zukünftigen Update von Acronis Backup 12.5 eingeführt werden.
  Wenn Sie den Inhalt Ihrer Backup-Archive nicht indizieren wollen, sollten Sie den Katalogdienst nicht installieren.

6.2.2 Backup Agenten

Backup Agenten müssen in jedem Teil Ihrer Umgebung installiert werden, die Sie sichern wollen. Anweisungen zur Installation der verschiedenen Agenten finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#36415.html.

Physische Maschinen

Wir empfehlen, dass Sie den Agenten direkt auf dem Betriebssystem installieren, das auf einer physischen Maschine läuft.

Umgebungen mit virtuellen Maschinen

Dies bedeutet in der Regel, dass Sie einen oder mehrere Agenten installieren, die direkt mit dem Hypervisor kommunizieren, auf dem diese Maschinen ausgeführt werden.

Wir empfehlen folgende Vorgehensweisen:

Hyper-V-Umgebungen

Installieren Sie den Agenten für Hyper-V auf jedem Hyper-V-Host, der in Ihrer Infrastruktur läuft. Die Agenten müssen auch dann auf jedem Host installiert werden, wenn die Hosts in einem Cluster verbunden sind.

Wenn Sie Ihre VMs auf SMB3-Netzwerkfreigaben speichern wollen, sollten Sie nicht vergessen, die Windows-Funktion 'VSS für SMB-Freigaben' zu aktivieren. Ohne diese Einstellung werden Ihre Backups fehlschlagen.

Weitere Informationen (in Englisch) finden Sie hier:
https://blogs.technet.microsoft.com/clausjor/2012/06/14/vss-for-smb-file-shares/

VMware vSphere-Umgebungen

Sie können eine oder mehrere virtuelle Appliances direkt als VM bereitstellen und/oder einen Agenten für VMware (Windows) installieren. Die virtuelle Appliance ist eine Acronis Linux-Instanz (eine von Acronis erstellte spezielle, kleine Linux-Distribution), auf der ein Standard-Agent für VMware läuft.

- Die Standardempfehlung ist, eine virtuelle Appliance auf jedem ESXi-Host in Ihrer virtuellen Umgebung zu installieren.
- Die Installation auf einer physischen Windows-Maschine wird empfohlen, wenn Sie Offloaded- oder LAN-freie Backups durchführen wollen.
  - Offloaded Backup
    - Wird verwendet, wenn Ihre produktiven ESX(i)-Hosts so stark ausgelastet sind, dass eine Ausführung der virtuellen Appliances nicht wünschenswert ist.
  - 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. Ausführliche Informationen zum LAN-freien Backup finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#37873.html.

Beachten Sie, dass Sie einen Agenten direkt innerhalb einer bestimmten virtuellen Maschine installieren können. Dafür ist keine eigene Lizenz erforderlich.

Dies eignet sich für Szenarien, bei denen kein agentenloses Backup von virtuellen Maschinen unterstützt wird – wie z.B.:

- Virtuelle Laufwerkskonfigurationen (wie RAW-Laufwerke), für die es keine Snapshot-Unterstützung gibt;
- Hypervisor (wie Xen oder RHEV), für die es keine Unterstützung für agentenloses Backup gibt.

6.2.2.1 Dimensionierung für Agent für VMware/Hyper-V

Agenten für VMware/Hyper-V (ob als virtuelle Appliance oder auf einem Windows-System installiert) sind die einzigen Agenten, deren Anforderungen mit der Umgebungsgröße skalieren. Die typischen Mindestanforderungen sind wie folgt:

RAM

- 1 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über 16 GB oder weniger gesamten Arbeitsspeicher verfügt
- 2 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über bis zu 64 GB Arbeitsspeicher verfügt bzw. gleichzeitig 2 bis 4 Maschinen sichert
- 4 GB zusätzlicher freier Arbeitsspeicher für den Agenten, wenn Ihr Hypervisor-Host über mehr als 64 GB Arbeitsspeicher verfügt und gleichzeitig 4 bis 10 Maschinen sichert

CPU

- 2 CPU-Threads werden immer empfohlen
- 2 Kerne (4 Threads), wenn gleichzeitig bis zu 5 VMs gesichert werden
- 4 Kerne (8 Threads), wenn gleichzeitig bis zu 10 VMs gesichert werden

6.2.2.2 Überlegungen in puncto DNS-Konfiguration

Die richtige Konfiguration des Domain Name Systems (DNS) ist bei virtuellen Backups sehr wichtig und die häufigste Ursache für zahlreiche Fehler und Probleme. Die Hostnamen diverser Acronis- und VMware-Komponenten müssen über mehrere physische/virtuelle Netzwerke hinweg untereinander korrekt aufgelöst werden können.

Der VMware Agent muss folgende Namen auflösen können:

- den Management Server-Hostnamen
- jeden ESX(i)-Hostnamen
- den vCenter-Hostnamen

Jede der oberen Komponenten muss außerdem in der Lage sein, die Namen der anderen untereinander auflösen zu können. Wenn die Namensauflösung nicht korrekt funktioniert, werden Sie verschiedene Kategorien von Fehlern sehen – von Bereitstellungsproblemen bis zu Backup-Fehlern.

Um diese Fehler zu vermeiden, sollten Sie unseren Empfehlungen folgen:

Wenn Sie in einer Acronis Lösung einen vCenter Server hinzufügen, wird unser Produkt versuchen, auf jedem Host in Ihrer vSphere-Umgebung eine virtuelle Appliance zu installieren. Weitere Informationen dazu finden Sie in der offiziellen Benutzeranleitung:
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#36631.html.

Damit diese automatische Bereitstellung funktioniert, ist es wichtig, dass die Domain-Namen-Auflösung zwischen dem Acronis Management Server und den Gastbetriebssystemen der VMs (die in Ihren ESX(i)-Hosts ausgeführt werden) funktioniert.

Das ist notwendig, um sicherstellen zu können, dass der Acronis Agent für VMware (Virtuelle Appliance) nach der Bereitstellung mit einem konfiguriertem DNS-Server in der Lage ist, sich mit dem Acronis Management Server zu verbinden (über dessen Hostnamen). Um Ihnen dabei zu helfen, haben wir mit Update 2 ein Feld eingeführt, mit dem Sie festlegen können, wie sich die Komponenten mit dem Server verbinden sollen – über den Hostnamen oder über die IP-Adresse.

Wir empfehlen, dass Sie statt dem Hostnamen die IP-Adresse auswählen, die der Agent zur Verbindung mit dem Management Server verwenden soll.

Sobald die Appliance für VMware bereitgestellt wurde, sollten Sie die DNS-Auflösung zwischen dem Agenten und den anderen Komponenten überprüfen:

1. Öffnen Sie einen vSphere Client und bauen Sie eine Verbindung zu einem ESX(i)-Host oder vCenter auf.
2. Navigieren Sie zu der virtuellen Appliance, öffnen Sie die Registerkarte **Konsole** und drücken Sie dann die Tastenkombination **Strg**+**Alt**+**F2**, um auf der Appliance in den Befehlszeilenmodus zu wechseln (den Sie mit der Tastenkombination **Alt**+**F1** wieder verlassen können).
3. Geben Sie einen Ping-Befehl ein, um den ESXi-Hostnamen und den vCenter-Namen von der virtuellen Appliance aus aufzulösen:
   `ping Hostname_des_ESXi`
   `ping Hostname_des_vCenters`.
4. Wenn der Ping-Befehl für den Hostnamen nicht erfolgreich ist, haben Sie ein DNS-Namensauflösungsproblem, weswegen VM-Backups von diesem Agenten auch nicht funktionieren werden.

*Wenn der **Port 25** gesperrt ist, wird der **`ping`**-Befehl nicht korrekt funktionieren. Sie können dann stattdessen andere Befehle verwenden – wie **`nslookup`**. Es ist nicht so wichtig, welchen Befehl genau Sie wählen, solange Sie damit überprüfen können, ob eine Verbindung über den Hostnamen erfolgt.*

Sie können das Problem beheben, indem Sie das Netzwerk in der Appliance und in Ihrer virtuellen Umgebung korrekt konfigurieren. Als Workaround können Sie auf jeder Appliance auch die Datei 'hosts' bearbeiten.
Das Bearbeiten der Datei 'hosts' funktioniert folgendermaßen:

1. Öffnen Sie die Konsole der virtuellen Appliance mit folgender Tastenkombination: **Strg**+**Alt**+**F2**.
2. Öffnen Sie die Datei 'hosts' mit folgendem Befehl:
   `vi /etc/hosts`
3. Drücken Sie die Taste **i**, um in den Bearbeitungsmodus zu wechseln.
4. Geben Sie die IP-Adresse und den aufzulösenden Namen des Servers in folgendem Format ein:
   `XXX.XXX.XXX.XXX Hostname`
5. Speichern Sie die Änderungen, indem Sie die Taste **Esc** drücken, geben Sie dann **`:wq`** ein
6. Drücken Sie die **Eingabetaste**.
7. Verlassen Sie die Konsole mit der Tastenkombination **Alt**+**F1**.

6.2.2.3 Prozessauslagerung auf andere Hosts (Off-Host-Verarbeitung)

Eine sehr wichtige neue Funktion von Acronis Backup 12.5 Advanced ist die Fähigkeit von Acronis Agenten, neben Backups noch eine Reihe anderen Datenverarbeitungstasks ausführen zu können. Jeder dieser Tasks kann auf Basis einer eigenen Planung laufen und ist komplett unabhängig von den eigentlichen Backups. Zu den verfügbaren Tasks gehören:

- Backup-Replikation
- Validierung
- Bereinigung
- Konvertierung zu VM
- VM-Replikation

Diese Funktionalität ist unerlässlich, um die Backup-Daten im großen Umgebungen so zu verwalten. Sie können mit dieser Funktionalität beispielsweise einen Agenten auf Ihrem Backup Storage Server installieren und Archive validieren/bereinigen, ohne die Netzwerkbandbreite und die Backup-Zeiten zu beeinflussen. Oder Sie können Ihre Backups an den Wochenenden direkt von einem Storage zu einem anderen replizieren lassen.

6.2.3 Empfohlene Installationsprozedur

Ausführliche Installationsanweisungen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#36428.html.

Bei einer Installation unter Windows sollten Sie sicherstellen, dass zuvor auf der Maschine alle erforderlichen Linux-Pakete installiert wurden – siehe: https://www.acronis.com/de-de/support/documentation/AcronisBackup_11.7/#22619.html.

Nachfolgend finden Sie unsere Empfehlungen für große Umgebungen:

1. Registrieren Sie Ihr Produkt in Ihrem Acronis Konto. Ausführliche Anweisungen dazu finden Sie hier: https://kb.acronis.com/content/4834
2. Laden Sie die vollständige Installationsdatei herunter, die für Ihr jeweiliges Betriebssystem (Windows oder Linux) passend ist.
   Sie können die Dateien immer direkt aus Ihrem Konto herunterladen, nachdem Sie die Registrierung durchgeführt haben.
3. Installieren Sie den Acronis Management Server, den Backup Agenten, den Monitoring Service, den Bootable Media Builder und die Komponenten zur Remote-Installation auf Ihrem Backup Server.
4. Installieren Sie den Storage Node oder den Katalogdienst (sofern benötigt) auf den Servern, die an Ihre Storage-Infrastruktur angebunden sind, und registrieren Sie diese auf Ihrem Management Server.
5. Richten Sie Ihre Gruppen, Benutzer und Einheiten ein (vgl. Sie die unteren Empfehlungen).
6. Konfigurieren Sie Ihre Speicherorte (Storages).
   Installieren Sie einen separaten Agenten auf oder in der Nähe des Speicherorts (möglichst nah im Netzwerk). Dieser Agent wird für Off-Host-Datenverarbeitungstasks (wie Bereinigung, Validierung und Replikationen zu anderen Storages) verwendet.
7. Konfigurieren Sie Ihre Backup-Pläne und wenden Sie diese auf die Gruppen an.
8. Beginnen Sie mit der Bereitstellung der Backup Agenten.
   a. Wir empfehlen normalerweise, Gruppenrichtlinien zu verwenden, um große Mengen von Agenten automatisch zu verteilen.
   b. Sie können die automatische Installation aber auch vom Produkt aus anstoßen (Push-Installation). Beachten Sie, dass die Agenten für Linux und Mac derzeit noch immer manuell installiert werden müssen (auf jeder Maschine, die gesichert werden soll). Die Push-Installationsfunktion für diese Systeme wird mit einem zukünftigen Update von Acronis Backup eingeführt.
   c. Agenten können während der Installation zu administrativen Einheiten hinzugefügt werden, wenn Sie das entsprechende Konto angeben.
9. Wenden Sie Backup-Pläne auf solche Maschinen an, die noch nicht über Gruppen abgedeckt sind.
10. Stellen Sie die Agenten in der Nähe der Speicherorte bereit (möglichst nah im Netzwerk). Diese Agenten werden für Off-Host-Datenverarbeitungstasks verwendet.
11. Erstellen Sie Off-Host-Pläne (Validierungs-, Bereinigungs-, Replikations- und Konvertierungspläne), um Ihre Daten außerhalb von Backup-Fenstern und Netzwerken zu verwalten, damit keine Ressourcen auf geschützten Maschinen beeinträchtigt werden.

6.3 Backup-Plan-Empfehlungen

6.3.1 Backup-Quelle

In der Regel werden Sie wohl komplette Maschinen sichern – und dabei bestimmte Ausschlussregeln verwenden, damit keine unerwünschten Dateien in das Backup aufgenommen werden.

Sie können Laufwerke (Partitionen), einzelne Dateien und Ordner oder Dateikategorien anhand von Dateierweiterungen ausschließen.

Beispielsweise können Sie alle .avi-Dateien in Ihren Backup-Plänen ausschließen, die auf Gruppen angewendet werden, mit denen Notebooks gesichert werden.

6.3.2 Backup-Ziel

Für große Umgebungen gibt es üblicherweise zwei wesentliche Speicheroptionen:

- Sie können alle Backups direkt auf oder in der Nähe der Endpunkt-Agenten selbst speichern lassen. Beispielsweise kann jede Maschine ihr Volume C:\ (Quelle) auf ihrem Volume D:\ (Ziel) speichern. Für diese Szenarien gibt es keine besonderen Empfehlungen. Dies hat den Vorteil einer geringeren Netzwerkauslastung, jedoch auf Kosten eines höheren Verwaltungsaufwands (denn jeder Speicherplatz muss einzeln angesprochen werden). Diese Option ist empfehlenswert, wenn Sie Wiederherstellungen im großen Umfang durchführen müssen, bei denen Hunderte oder Tausende von Maschinen gleichzeitig und mit minimaler Auswirkung auf die Produktion wieder betriebsbereit gemacht werden müssen. Weitere Informationen finden Sie im Abschnitt mit den Empfehlungen für Wiederherstellungen.
- Sie können alle Backups zentral speichern.
  Bei große Umgebungen sind dafür mehrere Netzwerksegmente mit eigenem Storage und/oder schnelle Netzwerkverbindungen zu diesem Storage notwendig. Vergleichen Sie dazu den unteren Abschnitt mit den „Überlegungen in puncto Storage“ (S. 61).
  Wenn Backups zentral gespeichert werden, sollten alle Datenverarbeitungstasks (wie Validierung oder Replikation) von einem dedizierten Agenten durchgeführt werden, der an diesen Storage angebunden ist.

6.3.3 Planung

In großen Umgebungen ist das Netzwerk zumeist der wichtigste Engpass für Ihre Backups: nur eine begrenzte Anzahl von Backups kann gleichzeitig in einem Subnetz-Segment ausgeführt werden, ohne dieses zu überlasten.

Der üblicherweise empfohlene Weg, um mit diesen physischen Beschränkungen umzugehen, besteht darin, die Backup-Umgebung in sinnvolle benutzerdefinierte Gruppen aufzuteilen. Weitere Informationen zum Erstellen von Gruppen finden Sie in der Produktdokumentation.

Jede Gruppe sollte diejenige Anzahl von Agenten enthalten, die notwendig sind, um das Backup innerhalb des zugewiesenen Backup-Fensters abschließen zu können. Bei der Umsetzung dieser Aufgabe hilft Ihnen der Ressourcennutzungsrechner (S. 8).

Es gibt weitere Faktoren, die die Backup-Zeit über die erwartete Netzwerkbandbreite hinaus verlängern. So kann beispielsweise die Erfassung der Applikations-Metadaten bei einem applikationskonformen VM-Backup eine längere Zeit benötigen, wenn es ein Problem mit der Quellapplikation gibt. Sie sollten daher das erste Backup von Ihrer Gruppe überwachen, um sicherzustellen, dass es keine deutlichen Ausreißer gibt.

Das empfohlene Backup-Schema ist **Nur inkrementell**, weil die Anzahl der Voll-Backups dabei auf ein Minimum (nämlich nur das erste) reduziert wird.

Eine weitere Option besteht darin, das Backup direkt auf jeder zu sichernden Ressource zu speichern. In diesem Fall bedarf es für die Planung keiner besonderen Überlegungen, da sich das Backup nicht mehr auf das Netzwerk auswirken wird.

Beide Methoden funktionieren gleich gut und sind mehr von Ihren Wiederherstellungsszenarien und dem verfügbaren Speicherplatz abhängig.

6.3.4 Aufbewahrungszeiten

Aufbewahrungsfristen basieren oft auf externen Richtlinien oder Compliance-Regeln. Sie können die zu erwartende Größe der Backups für die Aufbewahrungsdauer mithilfe des Ressourcennutzungsrechners (S. 8) abschätzen.

Wenn der als primäres Backup-Ziel verwendete Storage nicht genügend groß sein sollte, können Sie spezielle Replikationstasks planen, um die Daten zur Langzeitaufbewahrung auf einen anderen, billigeren Storage zu verschieben.

Sie können Ihre Backups beispielsweise in die Acronis Cloud replizieren oder die Acronis Storage-Lösung in Ihrem eigenen Datenzentrum einsetzen.

Wenn Sie einen sehr großen zentralen Storage für Ihre Backups verwenden, empfehlen wir dringend, keine Aufbewahrungsregeln in Ihrem Backup-Plan zu verwenden. Legen Sie für das Backup die Aufbewahrungseinstellung **Backups unbegrenzt behalten** fest.

Der Grund ist, dass alle Bereinigungsaufgaben, die Sie direkt mit in den Backup-Plan integrieren, von jedem dieser Backup Agenten selbst ausgeführt werden, sobald das Backup abgeschlossen wurde. Diese Vorgehensweise führt zu einer beträchtlichen Belastung der Agenten und des Netzwerks, wenn Tausende von Agenten versuchen, sofort nach einem Backup auch noch eine Bereinigung durchzuführen.

Installieren Sie stattdessen auf dem Storage (oder so nah wie möglich zu diesem) einen separaten Agenten, für den Sie einen eigenen **Bereinigungsplan** festlegen. Diese Bereinigungen werden dann von diesem einzelnen Agenten nach je eigenen Plänen ausgeführt, wobei nur eine minimale bis keine Netzwerklast verursacht wird.

6.3.5 Replikation, Konvertierung und Validierung

Ähnlich wie bei der Bereinigungsprozedur gilt: legen Sie keine Replikations- oder Validierungsoptionen mit in einem Backup-Plan fest, der einen zentralen Storage als Ziel verwendet.

Stattdessen können Sie separate „Mini-Pläne“ erstellen, die Aufgaben wie Replikation oder Validierung eigenständig außerhalb der Stoßzeiten durchführen.

Der Agent, der diese ausgelagerten Aktionen (Off-Host-Prozesse) durchführt, sollte möglichst nah im Netzwerk zum Storage installiert werden, über die maximale Bandbreite verfügen und vorzugsweise direkt auf dem Storage selbst ausgeführt werden.

Dies gilt nicht bei Szenarien, bei denen jeder Agent ein Backup zu seinem eigenen lokalen Speicherort erstellt. In diesem Fall müssen die zusätzlichen Datenverarbeitungstasks (wie Validierung) in denselben Backup-Plan integriert werden.

6.3.6 Weitere Empfehlungen

Benachrichtigungen, Alarmmeldungen und Berichte

Sogar sehr stabile Umgebungen neigen dazu, täglich viele Fehler zu verarbeiten, wenn die Zahl der gesicherten Geräte in die Tausende geht.

Um den administrativen Aufwand für die Handhabung dieser Informationen zu reduzieren, sollten Sie folgende Tipps beachten:

- Deaktivieren Sie alle nicht benötigten Alarmtypen in Ihrer Umgebung.
  Wenn Sie beispielsweise Notebooks oder andere Mobilgeräte sichern, ist die Alarmmeldung **Backup-Status ist unbekannt** normalerweise nicht sonderlich nützlich. Denn dieser Alarmtyp wird ständig ausgelöst, wenn Mitarbeiter das Netzwerk verlassen und die Agenten daher nicht mehr unter Kontrolle des Management Server sind.
  Zudem können Sie für bestimmte Alarmmeldungen die Priorität erhöhen oder senken.

  Diese Änderungen gelten auf der Ebene des kompletten Management Servers und können derzeit noch nicht pro Benutzer oder Organisationseinheit angepasst werden. Diese Funktionalität wird mit einem zukünftigen Update von Acronis Backup 12.5 eingeführt.

- Benachrichtigungen werden normalerweise direkt gesendet, sobald ein Alarm aktiviert wird. Jeder Alarmkontext ist für den jeweiligen Agenten und Plan spezifizisch, für den er aktiviert wurde.
  Wenn derselbe Plan also bei zwei Agenten fehlschlägt oder derselbe Agent zwei verschiedene Planfehler hat, werden zwei Alerts generiert und zwei Benachrichtigungen gesendet. Bei einer Skalierung auf Dutzende Agenten würden gängige Fehler (wie Netzwerkstörungen) also Dutzende von Benachrichtigungen durch dasselbe Problem bedeuten.
  Wir empfehlen daher, „Benachrichtigungen pro Alarm“ nur für die wichtigsten Alarmtypen und nur bei solchen Plänen einzustellen, die wichtige Infrastrukturen abdecken und sofortige Reaktionen bei Fehlern verlangen. Nutzen Sie bei weniger wichtigen Maschinen stattdessen Sie die täglichen geplanten Alarmberichte und die Berichtsfunktionen, um einen täglichen Überblick über den Maschinenstatus zu erhalten.
- Verwenden Sie den Alarm '**Keine erfolgreichen Backups für eine spezifizierte Anzahl aufeinanderfolgender Tage**' in den Backup-Plan-Optionen.
  Dieser Alarm wird nur aktiviert, wenn für ein Gerät nach einer bestimmten Anzahl von Tagen kein erfolgreiches Backup erstellt werden konnte. Dies ist ein nützlicher Weg, um bei Maschinen, bei denen ein einzelnes verpasstes Backup nicht so kritisch ist, die Backup-Fehler eines einzelnen Tages zu ignorieren.

Einheiten

Wenn mehrere Personen für die Verwaltung der Backup-Umgebung zuständig sind, sollten Sie sicherstellen, dass die Umgebung in Organisationseinheiten unterteilt wird, wie es in folgendem Abschnitt des Benutzerhandbuchs erläutert ist:
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/index.html#39305.html.

Fehler-Behandlungen und -Wiederholungen

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen (beispielsweise, wenn kein Netzwerk mehr verfügbar ist). Die Standardvorgabe sind 30 erneute Versuche in Intervallen von 30 Sekunden (über 15 Minuten). Für kleinere Backup-Jobs ist das nicht weiter kritisch. Aber wenn Sie Backups von großen Maschinengruppen parallel ausführen, kann dies das Backup-Fenster schon signifikant beeinflussen. Sie können den Wert daher auf 10 Neuversuche mit 30-Sekunden-Intervallen senken.

Dateiformat

Verwenden Sie wann immer möglich das Standard-Backup-Format 'Version 12' (https://www.acronis.com/en-us/support/documentation/AcronisBackup_12.5/#38763.html).

Active Protection

Active Protection ist derzeit nur für Maschinen mit Windows 7 (und höher) sowie Windows Server 2008 R2 (und höher) verfügbar. Der Agent für Windows muss auf der Maschine installiert sein.

Wir empfehlen, Active Protection auf allen Maschinen zu aktivieren, sofern diese nicht unter zu knappen CPU-Ressourcen leiden.
Bei starken Dateizugriffen bewirkt Active Protection üblicherweise einen CPU-Overhead von einigen wenigen CPU-Prozenten im System.

Selbstsicherung des Management Server

Stellen Sie sicher, dass auch der Management Server selbst von einem Backup-Plan gesichert wird.

Er muss nicht unbedingt gesichert werden, da Sie Ihre komplette Umgebung auch per Disaster Recovery wiederherstellen können, indem Sie isoliert unsere Boot-Medien verwenden. Aber ohne ein Backup des Management Servers müssen Sie diesen neu installieren, alle Agenten wieder hinzufügen und die komplette Konfiguration nach der Wiederherstellung Ihrer gesicherten Geräte neu durchführen.

Wenn Sie ein Backup des Management Server haben, stehen Ihnen außerdem noch weitere Optionen zur Verfügung – beispielsweise können Sie das als virtuelle Maschine ausführen oder in eine virtuelle Standby-Maschine konvertieren, um Wiederherstellungsprozesse zu beschleunigen (vgl. die Empfehlungen zu Wiederherstellungen (S. 67)).

6.4 Überlegungen in puncto Storage

Wie weiter oben erwähnt, ist eine wichtige Überlegung für große Umgebung die Bandbreite Ihres zentralen Storage im Hinblick auf die Anzahl der gleichzeitigen Backups, die diesen Storage als Speicherziel verwenden.

Über den Ressourcennutzungsrechner (S. 8) können Sie abschätzen, wie viele Storage-Segmente Sie auf Basis von vorgegebenen Netzwerkbandbreiten und Backup-Fenstern benötigen, um all Ihre Maschinen per Voll-Backup zu sichern.

6.4.1 Deduplizierung

Die Deduplizierung erfolgt bei Acronis Backup 12.5 immer „an der Quelle“ – was bedeutet, dass die Hash-Berechnung vom Agenten durchgeführt wird und somit keine Daten, die bereits in einem Backup vorhanden sind, erneut über das Netzwerk gesendet werden. Dies ist eine großartige Möglichkeit, sowohl den Speicherbedarf als auch die Netzwerkbandbreite zu senken, insbesondere wenn Sie Backups von Maschinen erstellen, die relativ ähnliche Daten enthalten.

Beachten Sie, dass eine Deduplizierung ein komplexer Prozess ist, den Sie sich mit der Notwendigkeit für einen relativ leistungsfähigen Storage-Server und dem Verzicht auf bestimmte Funktionen erkaufen müssen. Die derzeit wichtigste fehlende Funktion ist die Unterstützung des Version-12-Backup-Formats, was jedoch mit einem zukünftigen Update eingeführt werden wird.

Wenn Sie die Deduplizierungsfunktion verwenden wollen, sollten Sie mehr über die Deduplizierungstechnologie und die dazugehörigen empfohlenen Vorgehensweisen im entsprechenden Abschnitt des offiziellen Benutzerhandbuchs informieren:
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#7143.html.

Deduplizierung ist dann am sinnvollsten, wenn Sie viele Maschinen per Backup sichern wollen und diese Maschinen zu einem beträchtlichen Prozentsatz identische Daten haben. Oder wenn Sie Backups auf einem Storage speichern müssen, der nur per WAN/Internet oder einer anderen Verbindung mit geringer Bandbreite verfügbar ist.

Deduplizierung und Replikation

Die allgemeine Empfehlung lautet, dass eine Replikation immer **zu** einem deduplizierten Speicherort erfolgen sollte – und niemals **von** einem deduplizierten Speicherort aus.

Dies ist darin begründet, dass Replikationen bei Acronis Backup keine einfachen Kopien der Archivdaten sind, sondern eher erneuten Backups („Re-Backups“) als Kopiervorgängen entsprechen. Wenn Sie also eine Replikation zu einem deduplizierten Speicherort durchführen, werden – genau wie bei einem Backup – nur einmalige Daten (ohne Duplikate) übertragen. Dies ist ein großer Vorteil, wenn Sie z.B. lokale Backups durchführen und diese dann zu einem externen deduplizierten Speicherort replizieren.

Dies bedeutet auch, dass Daten, die von einem deduplizierten Speicherort aus repliziert werden, während dieser Replikation rekonstituiert werden. Oder mit anderen Worten: die resultierende Datei ist nicht mehr dedupliziert und kann unabhängig vom Deduplizierungsdienst auf dem Storage Node verwendet werden.

Dieser Datenrekonstitutionsprozess verursacht einigen Overhead für die Replikationsaktion und würde dementsprechend länger dauern, wenn Sie eine Replikation von einen nicht-deduplizierten Speicherort durchführen. Dies erschwert Skalierungen, insbesondere wenn das Ziel eine Bandbibliothek ist und daher anfällig für Verzögerungen ist.

6.4.2 Bandgeräte

Acronis ist bestrebt, die Unterstützung für Bandgeräte fortzusetzen und auszuweiten.

Eine Liste von getesteten und unterstützten Bandgeräten finden Sie in der Hardware-Kompatibilitätsliste für Bandlaufwerke
(https://go.acronis.com/acronis-backup-advanced-tape-hcl).

Wenn Sie die Kompatibilität Ihres eigenen Bandgerätes testen wollen, können Sie das Bandkompatibilitätstool verwenden
(https://kb.acronis.com/content/57237).

Wenn das Tool ein Problem findet, kontaktieren Sie bitte den Acronis Support, damit das Problem zu unserer Entwicklungsabteilung weitergeleitet und gelöst werden kann.

Ein Agent kann Backups direkt zu einem Bandlaufwerk erstellen. Wenn Sie eine einzelne oder isolierte Maschine haben und Band-Backups erstellen wollen, müssen Sie das Bandlaufwerk direkt an der Maschine anschließen, auf welcher der Agent installiert ist.

6.4.2.1 Storage Node für Bänder

Der Acronis Storage Node wird benötigt, wenn Sie eine größere Menge von Maschinen per Backup auf (ein oder mehrere) Bandlaufwerke sichern wollen. Das Bandgerät muss dafür an die Maschine des Storage Nodes angeschlossen sein.

Wenn Sie sowohl Bänder als auch Deduplizierung verwenden wollen, empfehlen wir, für jeden Storage einen eigenen Storage Node zu installieren, da Sie mit einem Management Server praktisch unbegrenzt viele Storage Nodes verwalten können.

6.4.2.2 Bandverwaltungsdatenbank

Die Informationen über alle Bandgeräte, Bänder und Backup-Inhalte werden in der Bandverwaltungsdatenbank gespeichert, die sich wiederum auf der Maschine befindet, an welcher das Bandgerät angeschlossen ist.

Der Standardpfad für die Datenbank ist:

- Windows 7, Windows Server 2008 und höher:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database
- Linux:
  /var/lib/Acronis/BackupAndRecovery/ARSM/Database

Die Datenbankgröße hängt von der Zahl der auf den Bändern gespeicherten Backups ab – wobei etwa 10 MB auf einhundert Backups kommen. Mit einigen wenigen Maschinen ist dies –auch mit längeren Aufbewahrungszeiten – kein Problem.

Sie sollten jedoch sicherstellen, dass Sie genügend Speicherplatz für diese Datenbank auf Ihrem System haben. Falls Sie unsicher sind, sollten Sie vor dem Start des ersten Band-Backups den Pfad entsprechend überprüfen.

So verlagern Sie die Datenbank unter Windows:

1. Stoppen Sie den den Dienst '**Removable Storage Management**'.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Ermitteln Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings**.
4. Spezifizieren Sie den Pfad zum neuen Speicherort im Registry-Wert `ArsmDmlDbProtocol`. Der String darf bis zu 32765 Zeichen enthalten.
5. Starten Sie den den Dienst '**Removable Storage Management**' wieder.

So verlagern Sie die Datenbank unter Linux:

1. Stoppen Sie den Dienst '**acronis_rsm**'.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Öffnen Sie die Konfigurationsdatei **/etc/Acronis/ARSM.config** in einem Text-Editor.
4. Suchen Sie nach folgender Zeile: `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Ändern Sie den Pfad unter dieser Ziele.
6. Speichern Sie die Datei.
7. Starten Sie den Dienst '**acronis_rsm**' wieder.

Sie dürfen die Band-Datenbank nicht löschen! Denn dies würde erfordern, dass all Bänder erneut gescannt werden müssen, um die darauf gespeicherten Backups wieder verwendbar zu machen. Und dies ist ein sehr zweitaufwendiger und fehleranfälliger Prozess.

6.4.2.3 Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren

Diese Option ist standardmäßig deaktiviert. Wenn Sie diese Option in den Bandverwaltungseinstellungen Ihres Backup-Plans aktivieren, können Sie aus Image-Backups, die auf Ihren Bändern gespeichert sind, auch einzelne Dateien wiederherstellen.

Beachten Sie, dass Sie sich diese Funktionalität mit hohen Speicherplatzkosten erkaufen. Wenn die Funktionalität aktiviert ist, erstellt die Software bei jedem Backup zusätzliche Dateien auf einem Festplattenlaufwerk der Maschine, an der das Bandgerät angeschlossen ist. Datei-Recovery von Laufwerk-Backups ist möglich, solange diese zusätzlichen Dateien intakt sind. Die Dateien werden automatisch gelöscht, wenn das Band, auf dem die entsprechenden Backups gespeichert sind, gelöscht, entfernt oder überschrieben wird.

Diese zusätzlichen Dateien befinden sich an diesem Speicherort:

- In Windows 7, Windows Server 2008 und höher:
  %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation
- In Linux:
  /var/lib/Acronis/BackupAndRecovery/TapeLocation

Der von diesen zusätzlichen Dateien belegte Speicherplatz hängt von der Anzahl der Dateien im entsprechenden Backup ab. Beim Voll-Backup eines Laufwerks mit ungefähr 20.000 Dateien (typisches Laufwerk-Backup einer Workstation) belegen die zusätzlichen Dateien ca. 150 MB. Ein einzelnes Voll-Backup eines Servers mit 250.000 Dateien kann etwa 700 MB an zusätzlichen Dateien erzeugen.

Auch in kleinen Umgebungen kann die Größe dieser Dateien schnell auf Dutzende von Gigabyte anwachsen.

Wir empfohlen daher, dass Sie diese Option deaktiviert lassen, wenn Sie die Option nicht unbedingt benötigen. Wenn doch, sollten Sie sicherstellen, dass der verwendete Speicherort oder Storage Node von der Speicherplatzgröße auf diese zusätzlichen Dateien ausgelegt ist.

6.4.2.4 Bandsätze

Sie können in Acronis Backup 12.5 Bandsätze erstellen, um flexibler zu verwalten, welche Geräte ihre Backups zu welchen Bändern erstellen – und unter welchen Bedingungen dies geschehen soll. Beispielsweise können Sie an jedem einzelnen Werktag ein bestimmtes Band verwenden und am Wochenende wiederum einen anderen Satz von Bändern.

Weitere Informationen finden Sie in diesem Knowledge Base-Artikel über Bandsätze:
https://kb.acronis.com/content/59315.

6.4.3 Acronis Storage (neu in Update 2)

Acronis Storage ist eine Software-Defined-Storage-Lösung, mit der Sie einen sicheren, unternehmensgerechten Storage – wie ein SAN (Storage Area Network) oder NAS (Network Attached Storage) – leicht und schnell aus preiswerter, handelsüblicher Hardware und Netzwerk-Equipment aufbauen können.

Acronis Storage ist für die Speicherung großer Datenmengen optimiert und bietet Datenredundanz (Replikation und Lösch-Codierung), Hochverfügbarkeit, Selbstreparaturfähigkeiten und Storage-Sharing.

Benutzerdaten werden bei Acronis Storage auf organisierten Server-Clustern in Form von Datensegmenten (Chunks) mit fester Größe gespeichert. Um die hohe Verfügbarkeit der Benutzerdaten zu gewährleisten, werden die Datensegmente automatisch repliziert und über die im Cluster verfügbaren Server verteilt.

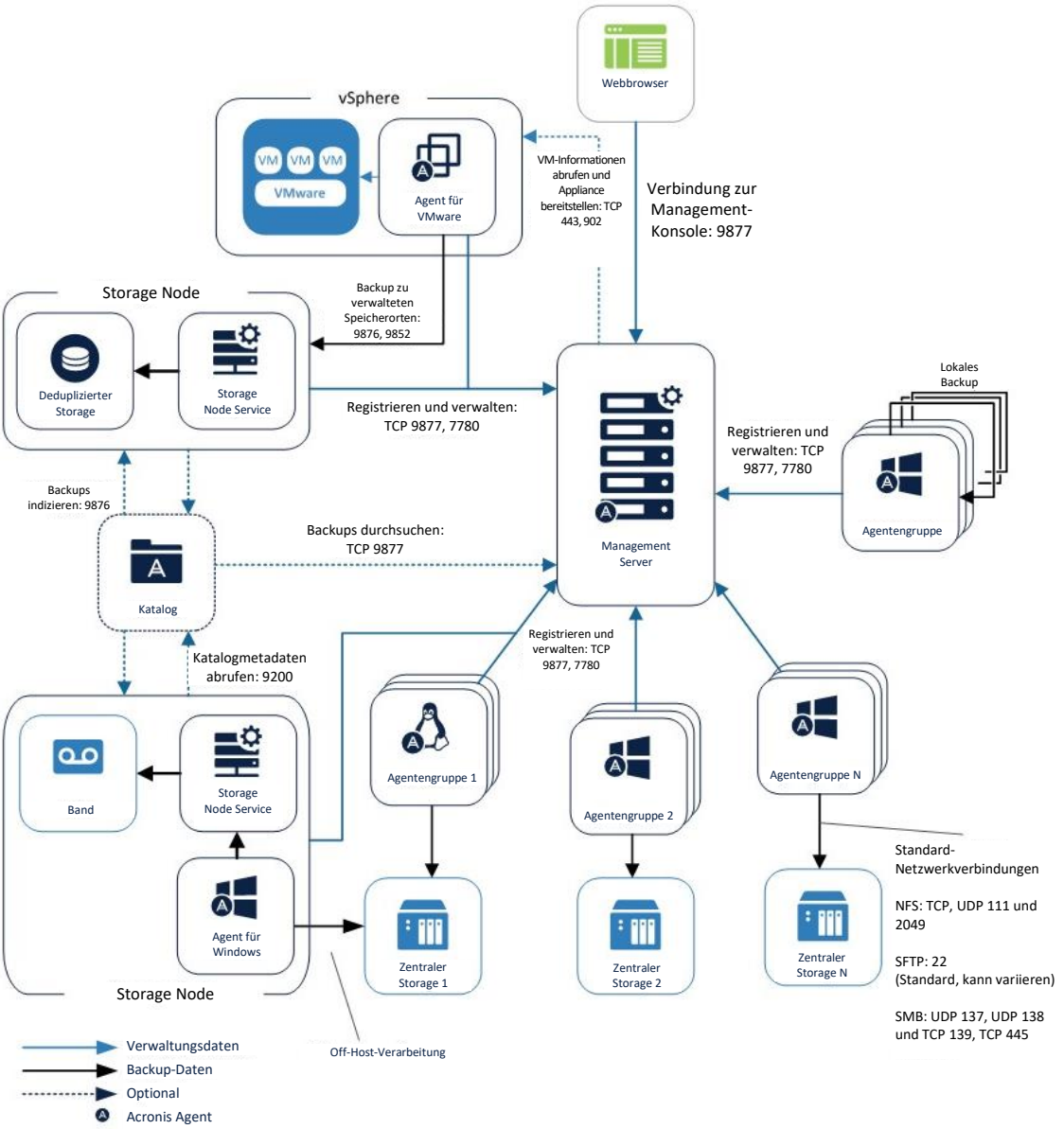
Ab Acronis Backup 12.5 Update 2 können Sie Acronis Storage-Cluster als Backup-Ziel für Ihre eigenen lokalen Sicherungen verwenden, indem Sie einen Acronis Storage Gateway im Produkt registrieren.

Genau die gleiche Storage-Lösung wird in den Acronis Datenzentren für unsere Cloud Backups verwendet und hat sich dabei auch unter Skalierungsanforderungen als zuverlässig erwiesen. Wenn Sie sich bisher noch für keine Storage-Lösung entschieden haben, ist Acronis Storage gerade zur Speicherung von Backups in großen Umgebungen eine klare Empfehlung.

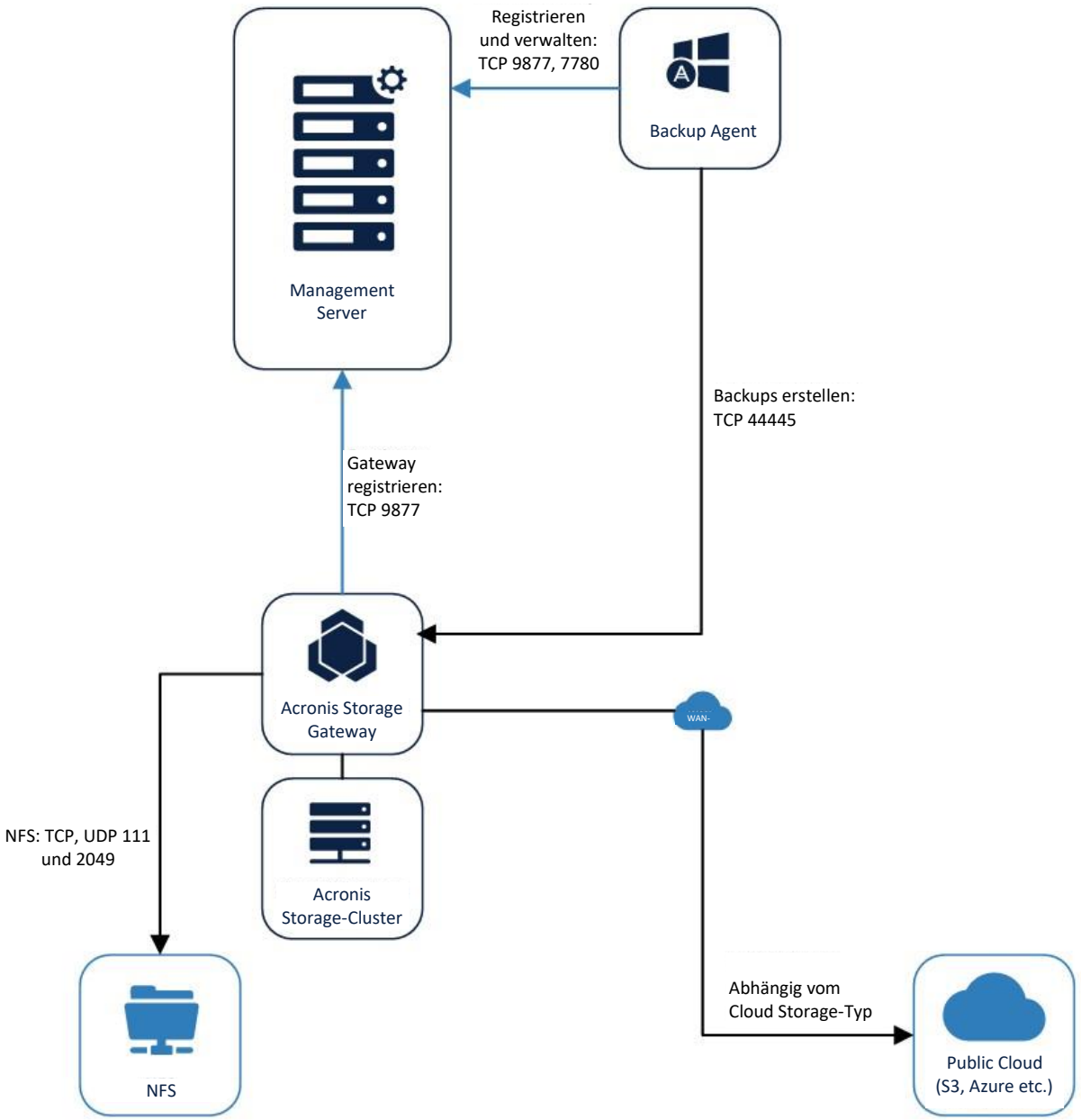
6.5 Netzwerkdiagramme und Ports

Das vollständige Netzwerkdiagramm können Sie im Anhang B (S. 82) finden.

Nachfolgend finden Sie das Netzwerkdiagramm für große Umgebungen.



Nachfolgend finden Sie das Netzwerkdiagramm für Acronis Storage.



7 Empfehlungen zu Wiederherstellungen

In diesem Abschnitt finden Sie einige allgemeine Empfehlungen und Szenarien zur Wiederherstellung Ihrer Umgebung.

Wenn es eine Empfehlung in diesem Dokument gibt, die Sie unbedingt befolgen sollten, dann lautet diese: testen und dokumentieren Sie immer Ihre Disaster Recovery-Prozedur! Sie sollten für diese Tests bevorzugt (aber nicht zwingenderweise) dieselbe Hardware wie auf den Produktionsmaschinen verwenden. Ein Wiederherstellungstest auf einer virtuellen Maschine, die unabhängig von Ihrer Umgebung läuft, ist immer noch besser, als die Prozedur gar nicht zu testen.

7.1 Boot-Medien

Die bootfähige Umgebung von Acronis, die von einem Boot-Medium ausgeführt wird, ist ein sehr leistungsfähiges Tool und die Basis der meisten Wiederherstellungsszenarien, die Sie mit Acronis umsetzen können.

Die Standardausführung dieser bootfähigen Umgebung ist eine von Acronis erstellte spezielle, kleine Linux-Distribution. Diese Distribution enthält einen Agenten mit demselben Funktionsumfang wie jeder andere installierbare Agent, unsere eigenen Dateisystemtreiber und eine Benutzeroberfläche.

Diese Umgebung kann direkt aus dem Produkt heraus verwendet werden. Wenn Sie beispielsweise von der Webkonsole aus das System-Image einer laufenden Maschine wiederherstellen wollen, läuft folgender Prozess ab:

Ein Image der bootfähigen Umgebung wird auf der wiederherzustellenden Maschine an einem temporären Ort gespeichert.
Zusammen mit der bootfähigen Umgebung werden auch die Wiederherstellungsbefehle geschrieben. Diese Befehle werden ausgeführt, nachdem die bootfähige Umgebung gebootet wurde.
Das System auf der Maschine wird angewiesen, beim nächsten Neustart die bootfähige Umgebung zu starten, und danach wird die Maschine neu gebootet.

Eine Variante der bootfähigen Umgebung ist der **Acronis Startup Recovery Manager** (ASRM). Wenn Sie diesen aktivieren, können Sie die entsprechende Maschine mit unserer Linux-Umgebung starten, wenn Sie während des Bootvorgangs die Taste F11 drücken. Weitere Informationen dazu finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/en-us/support/documentation/AcronisBackup_12.5/#38872.html.

Das übliche Szenario sieht so aus, dass Sie ein Boot-Medium erstellen, von dem aus die bootfähige Umgebung dann ausgeführt wird. Dabei handelt es sich beispielsweise um eine herkömmliche beschreibbare CD (oder das ISO-Image für eine solche Boot-CD), einen USB-Stick oder einen PXE Server. Um ein solches Boot-Medium zu erstellen, können Sie entweder den Acronis Bootable Media Builder verwenden – oder ein von uns vorbereitetes ISO-Image direkt aus Ihrem Acronis Konto herunterladen.

7.1.1 Das Boot-Medium testen

Sie sollten das Boot-Medium unbedingt zuerst auf Ihrer üblichen Hardware testen, bevor Sie es tatsächlich zur Wiederherstellung Ihres Systems verwenden. Wenn Sie in Ihrem Büro fünf unterschiedliche Maschinentypen haben, sollten Sie diese alle mit dem Boot-Medium testen. Dabei müssen Sie drei Dinge testen:

1. Überprüfen Sie, ob Sie auf der Maschine die bootfähige Umgebung mit dem Medium starten können. Wenn nicht: erstellen Sie das Medium neu und wiederholen Sie dann den Test.
   Probleme mit der Bootfähigkeit sind meistens auf ein beschädigtes Medium oder andere Fehler beim Erstellungsprozess zurückzuführen.

2. Überprüfen Sie, ob in der bootfähigen Umgebung alle lokalen Laufwerke richtig erkannt werden. RAID-Geräte sollten beispielsweise nicht auf der Ebene der zugrundeliegenden Laufwerksstruktur angezeigt werden, sondern als Laufwerksverbund mit zugreifbaren Inhalten.
3. Stellen Sie sicher, dass Sie über das Boot-Medium auf Ihre Backup-Dateien zugreifen können, die auf anderen Laufwerken/Storages liegen.

Der Grund dafür ist einfach: es könnte sein, dass die bootfähige Umgebung auf dem Medium Ihre Hardware nicht unterstützt. Das passiert nur selten, aber sollte doch von Ihnen überprüft werden. Und zwar möglichst als eine der ersten Maßnahmen, nachdem Sie Ihre Backups erstellt haben.

Die Erstellung einer eigenen Linux-Distribution ermöglicht uns eine beispiellose Flexibilität und Funktionalität. Jedoch zu dem Nachteil, dass die mögliche Hardware-Unterstützung durch die Verfügbarkeit von Open Source-Linux-Treibern beschränkt wird. Da es kein allgemeines Plug-&-Play-Treiber-Modell für Linux gibt, müssen alle benötigten Hardware-Treiber vor der Erstellung der bootfähigen Umgebung kompiliert werden.

Es gibt auch Hersteller, die überhaupt keine Linux-Treiber für ihre Hardware bereitstellen. Die entsprechende Hardware können auch wir dann mit unserer bootfähigen Linux-Umgebung nicht unterstützen.

Wenn es zu Problemen mit der bootfähigen Umgebung kommt, liegt es meistens an der Verwendung neuerer Hardware, für die wir noch keine Unterstützung integrieren konnten. Obwohl wir unsere Linux-Umgebung regelmäßig mit neuen Treibern aktualisieren, ist es für einen unabhängigen Drittanbieter wie uns unmöglich, die stets neu erscheinende Hardware immer zu 100% abzudecken.

Sollte Ihr Boot-Medium daher mit Ihrer Hardware einmal nicht funktionieren, kontaktieren Sie bitte den Acronis Support, damit das Problem zu unserer Entwicklungsabteilung weitergeleitet und gelöst werden kann. Eventuell gibt es auch bereits eine neuere Version der Linux-Umgebung, die Ihre Hardware unterstützt. Oder wir können eine neue Version erstellen, falls dies möglich ist. Wie Sie den Support kontaktieren können, finden Sie in diesem Knowledge Base-Artikel: https://kb.acronis.com/content/56079.

7.1.2 WinPE-Umgebung

Statt der standardmäßigen Linux-Umgebung können Sie auch eine Microsoft WinPE-Umgebung als Boot-Medium erstellen. Der Acronis Bootable Media Builder wird dann einen Standardprozess initiieren, um ein bootfähiges WinPE-Image auf Basis des Windows ADK (Assessment & Deployment Kit) zu erstellen. Der entsprechende Prozess ist in diesem englischsprachigen Microsoft Knowledge Base-Artikel beschrieben: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/winpe-create-usb-bootable-drive.

Während der Erstellung des WinPE-Standardmediums installiert der Media Builder dann auch einen Acronis Agenten (inkl. Benutzeroberfläche), damit dieser auf dem resultierenden Medium verfügbar ist.

Für die meisten Einsatzfälle empfehlen wir das Standard-Linux-Medium, da wir dieses unter vollständiger Kontrolle haben und auftretende Probleme daher auch am besten lösen können. Wenn unsere Linux-Umgebung beispielsweise auf Ihrem System nicht booten kann, können unsere Entwickler das Problem gut analysieren und beheben. Wenn dagegen die WinPE-Umgebung auf Ihrem System nicht bootet, können unsere Entwickler gar nichts tun, da dieses Medium allein unter der Kontrolle von Microsoft steht.

Der wichtigste Vorteil der WinPE-Umgebung besteht darin, dass diese alle Hardware-Treiber unterstützt, die auch für die Standard-Windows-Desktop-Betriebssysteme verfügbar sind. Neue Treiber können während der Medium-Erstellung einfach eingebunden werden. Da es für fast alle Hardware auch Treiber für Microsoft Windows gibt, kann man mit einem WinPE-Medium Treiberprobleme lösen, die man sonst mit der Linux-Umgebung hätte.

Vor diesem Hintergrund empfehlen wir, dass Sie in folgenden Fällen ein WinPE-Medium verwenden:

- Wenn Sie bereits ein WinPE-basiertes Medium haben, welches Sie für andere Zwecke verwenden. Wenn Ihre Techniker beispielsweise bereits ein leistungsstarkes WinPE-Medium mit bestimmten Plug-ins und Tools zur Wartung Ihrer Systeme verwenden, können Sie dieses Medium durch die Integration des Acronis Agenten noch leistungsfähiger machen.

- Wenn Sie Hardware verwenden, für die Ihr Hersteller keine Linux-Treiber bereitstellt. Ein Beispiel wäre der Dell PERC S300 RAID-Controller.
- Wenn die Hardware-Konfiguration auf Ihren zu sichernden Systemen zu vielseitig ist oder sich zu oft ändert. In diesem Fall kann es sinnvoller sein, ein einziges WinPE-Medium zu erstellen, dem Sie alle erforderlichen Treiber für alle Maschinen hinzufügen können.

7.1.3 Boot-Medium-Aktionen automatisieren

Acronis Backup 12.5 bietet die leistungsfähige neue Möglichkeit, Boot-Medium-Aktionen (wie Backup und Recovery) per Skript zu automatisieren und diese Skripts während der Medium-Erstellung einzubinden. Damit können Sie physische Disaster Recovery-Abläufe automatisieren und einige interessante Szenarien umsetzen, die später in diesem Abschnitt beschrieben werden.

Wenn Sie Ihre Umgebung mit einer typischen Hardware- und Backup-Plan-Vorlage sichern, können Sie mit einem skriptbasierten Boot-Medium Ihre komplette Disaster Recovery-Prozedur formalisieren.

Damit können Sie nicht nur Ihre Wiederherstellungsabläufe besser testen (was immer ratsam ist), sondern auch bestimmte Faktoren (wie RTOs) optimieren sowie die Schulung Ihrer Mitarbeiter erleichtern. Mit einem optimal skriptgesteuerten Medium kann die Wiederherstellung einer einzelnen Maschine so vereinfacht werden, dass sie selbst von Personen ohne jede Kenntnis über Acronis Produkte durchgeführt werden kann.

Wie Sie Ihr Boot-Medium mit automatisierbaren Aktionen erweitern können, wird in der offiziellen Benutzeranleitung erläutert:
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#39737.html.

7.1.4 Boot-Medien registrieren

Acronis Backup 12.5 bietet eine weitere nützliche Funktion, um einzigartige Backup & Recovery-Szenarien zu ermöglichen: Sie können über die Webkonsole mit dem Agent auf dem Boot-Medium genauso aus der Ferne interagieren, als würde es sich um einen normalen Agenten für Windows oder Linux handeln. Und im Wesentlichen sind die Linux-Agenten ja auch gleich.

Ein Beispiel: Sie haben eine öffentliche Workstation oder einen Schulungs-PC und müssen diesen regelmäßig über ein Master-Image wiederherstellen. Bei einem solchen Szenario sollten Sie das verwendete Boot-Medium auf unserem Management Server registrieren.

Sie finden das registrierte Medium dann auf der Registerkarte '**Boot-Medium**' unter '**Geräte**' und können daher vom Management Server aus mit dem Agenten auf dem Medium auf die gleiche Art interagieren wie mit jedem anderen Agenten auch. Sie können beispielsweise Backup-Planungen auf dem Medium erstellen, Wiederherstellung aus der Ferne konfigurieren und ausführen oder den Status von Aktivitäten überprüfen, die bereits auf dem Medium ausgeführt wurden.

Jedes Medium wird eindeutig anhand eines Hash-Werts identifiziert, der aus der/den MAC-Adresse(n) der Maschine (die mit dem Medium gebootet wurde) generiert wird. Sie können also auf Basis einer CD oder eines USB-Sticks beliebig viele Maschinen booten, von denen jede im Management Server eindeutig über eine ID identifiziert wird. Und diese ID bleibt – egal wie oft die Maschine gebootet wird – solange konstant, wie die Netzwerkkarte der Maschine nicht geändert wird.

Diese Empfehlung gilt auch, wenn Sie Backups erstellen müssen, ohne dass Sie etwas auf dem Betriebssystem installieren wollen/können. Beispielsweise, wenn Sie ein nicht unterstütztes altes Betriebssystem wie Windows NT verwenden. Weitere Informationen dazu finden Sie im Abschnitt 'Sonstige Empfehlungen' (S. 74).

Anweisungen zur Registrierung von Boot-Medien finden Sie in der offiziellen Benutzeranleitung:
https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#39308.html.

7.2 Wiederherstellungsszenarien

7.2.1 Einfache Wiederherstellungen

Einfache Wiederherstellungsszenarien und die damit verbundenen grundlegenden Funktionen werden in der offiziellen Produktdokumentation erläutert. Für diese Szenarien gibt es eine grundlegende Empfehlung: Testen Sie Ihre Wiederherstellungsprozedur, bevor eine tatsächliche Wiederherstellung notwendig wird. Eine Übersicht aller einfachen Wiederherstellungsszenarien finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#36648.html.

Befolgen Sie diese Anweisungen, wenn Sie regelmäßig einzelne physische Maschinen/VMs/Dateien/Applikationen wiederherstellen müssen.

7.2.2 Massenwiederherstellungen

Dieses Szenario beschreibt die empfohlene Konfiguration, wenn Sie eine größere Menge von Maschinen gleichzeitig wiederherstellen müssen. Beispiel: Ihr Unternehmen wird mit einem Virus angegriffen, der sich schnell ausbreitet. Dieser Angriff würde nicht gestoppt, wenn Sie die Maschinen nur einzeln nacheinander wiederherstellen würden.

Bei diesem Szenario wird außerdem vorausgesetzt, dass Ihre komplette Hardware funktioniert und am üblichen Ort verfügbar ist. Anders sind Situationen, in denen Sie alles verlieren und Sie daher ein Disaster Recovery in einem externen Datenzentrum durchführen müssen. Ein solches standortweites Disaster Recovery-Szenario wird weiter unten erläutert (S. 71).

Eine Massenwiederherstellung sollte möglichst nicht über das Netzwerk durchgeführt werden. Das Netzwerk wird bei der gleichzeitigen Wiederherstellung vieler Maschine nicht nur schnell zum Flaschenhals, sondern sollte bei einem Malware-Angriff auch als eine der ersten Maßnahmen ausgeschaltet werden, um weitere Ausbreitungen zu verhindern.

Sie können auch physische Maschinen in großen Mengen und ohne Netzwerkzugriff wiederherstellen, wenn Sie folgenden Empfehlungen folgen:

- Konfigurieren Sie Ihre Backup-Pläne so, dass auf jeder Maschine auch ein Backup zu einem lokalen Speicherort erstellt wird.
  - Dafür sollten Sie die Aufbewahrungsregeln so einstellen, dass nur jeweils das neueste Backup lokal aufbewahrt wird, da Sie keinen vollständigen Backup-Verlauf auf jeder Maschine benötigen.
  - Die Backups sollten zu einem zentralen Storage repliziert werden. Alternativ können Sie auch einen zweiten Backup-Plan erstellen, der zu einem anderen Zeitpunkt mit anderen Parametern ausgeführt wird. Die lokalen Backup-Kopien werden verwendet, um alle lokalen Maschinen schnellstmöglich wiederherstellen zu können. Mit den zentralen Backup-Kopien werden dagegen einzelne Maschinen wiederhergestellt, die ausgefallen sind.
- Sie können optional auch ein skriptgesteuertes Boot-Medium erstellen, um die Wiederherstellung der Maschine aus diesem einzelnen lokalen Backup zu automatisieren. Dadurch können Sie viel Zeit und Arbeitskraft einsparen.
- Bei einem Disaster können Sie jede Maschine mit einem Boot-Medium starten. Da das benötigte Backup lokal gespeichert ist, können Sie beliebig viele Maschinen parallel starten. Jede Maschine wird Ihre eigene Wiederherstellung durchführen, ohne andere Maschinen zu beeinflussen.
  Das ist die schnellste Möglichkeit für ein gleichzeitiges Disaster Recovery von beliebig vielen physischen Maschinen.

7.2.3 Standortweites Disaster Recovery

Dieses Szenario enthält Empfehlungen, wie Sie sich vor Situationen schützen können, bei denen Ihre komplette Umgebung ausfällt und Sie diese aus Offsite-Backups wiederherstellen müssen. Solche Disaster ereignen sich zwar wesentlich seltener als Festplattenausfälle, aber wenn es dazu kommt, sind die Konsequenzen weit schlimmer.

Das größte Problem bei der Wiederherstellung einer kompletten Umgebung hängt mit der vorhandenen Hardware zusammen, auf der diese Umgebung läuft. Denn Backups allein reichen für eine Wiederherstellung nicht aus, wenn es keinen Standort/keine Hardware mehr gibt, wohin die Backups wiederhergestellt werden können.

Idealerweise sollten Sie einen separaten Disaster Recovery-Standort haben, der in ausreichender Entfernung vom primären Produktionsstandort liegt und genügend Hardware-Ressourcen hat, um darauf Ihre wiederhergestellte Produktionsumgebung auszuführen. An diesem Standort sollten Sie zudem einmal im Jahr Disaster Recovery-Übungen durchführen.

Eine solche Lösung ist jedoch ziemlich kostspielig. Eine gute Alternative ist ein virtueller Disaster Recovery-Standort, der über ausreichende VMware-Hypervisor-Ressourcen verfügt, um die wichtigsten Produktions-Workloads zu übernehmen, bis der Hauptstandort wieder online ist. Selbst wenn Sie einen physischen Disaster Recovery-Standort haben, ist ein guter ESXi-Host oder -Cluster sehr empfehlenswert, um die Wiederherstellung zu beschleunigen.

Die aktuelle Version von Acronis Backup 12.5 bietet mehr Funktionen für VMware als für andere Virtualisierungsplattformen. Wenn Sie den Hypervisor für Ihren Disaster Recovery-Standort wählen können, sollten Sie VMware verwenden.

Zudem können Sie ein Offsite-Disaster-Recovery auf Cloud-Servern ausführen, was den großen Vorteil bietet, dass Sie nicht in Standby-Hardware investieren müssen.

Acronis bietet einen eigenen Cloud-basierten Disaster Recovery Service:
https://www.acronis.com/de-de/business/disaster-recovery-service/

7.2.4 Allgemeine Empfehlungen für Disaster Recovery

Egal wo sich Ihr Disaster Recovery-Standort befindet und wie er genau aussieht – es gibt eine Reihe von allgemeinen Empfehlungen, die Sie bei der Konzeption und Ausführung Ihrer Disaster Recovery-Szenarien beachten sollten.

Die Empfehlungen richten sich nach dem Storage-Typ für Ihre Offsite-Backups, denn die Wiederherstellungsabläufe hängt davon ab, wo die Backups vorliegen und welche Vorbereitungen notwendig sind.

7.2.4.1 Normaler unverwalteter oder Festplatten-Storage

An solchen Speicherorten werden die Backup-Metadaten von Acronis Backup 12.5 zusammen mit den tatsächlichen Backups gespeichert. Das macht die Archive portabel und den jeweiligen Disaster Recovery-Prozess einfach.

Von portablen USB-Festplatten in kleinen Umgebungen bis zu SFTPs oder großen verteilten SANs – Sie können über den Management Server, ein Boot-Medium oder einen Agenten auf Ihre Backups zugreifen.

Wenn Ihre Umgebung nicht sehr groß ist und die Offsite-Backups auf Festplatten vorliegen, die zum physischen DR-Speicherort transportiert werden können, ist das empfohlene Wiederherstellungsprozedur die gleiche, wie es im Abschnitt „Massenwiederherstellungen“ (S. 70) beschrieben ist. Schließen Sie einfach das entsprechende Laufwerk, auf dem Ihre Backups gespeichert sind, an die jeweilige Maschine an, starten Sie ein Boot-Medium und führen Sie die Wiederherstellung aus – wobei das angeschlossene Laufwerk als Quelle und das interne Laufwerk der Maschine als Ziel dient.

Bei größeren physischen Umgebungen mit nicht verwalteten Speicherorten sollten Sie folgende Vorgehensweise befolgen:

- Stellen Sie den Management Server aus einem entsprechenden Backup wieder her.
- Fügen Sie dem Management Server den Speicherort hinzu, auf dem sich das/die Backup(s) befinden.
- Starten Sie jede wiederherzustellende Maschine mit einem Boot-Medium und registrieren Sie dieses auf dem Management Server.
- Starten Sie die verschiedenen Wiederherstellungsprozeduren remote vom Management Server aus, sobald die Maschinen in dessen Benutzeroberfläche angezeigt werden.
- Wenn Sie die Wiederherstellung zu mehreren Personen ausführen können, warten Sie nicht, bis der Management Server online ist und beginnen Sie mit der Registrierung der Boot-Medium-Agenten. Starten Sie parallele Wiederherstellungen mithilfe mehrfacher Kopien des Boot-Mediums.

Beachten Sie, dass die Maschine nach ihrer Wiederherstellung im Management Server nicht notwendigerweise als online angezeigt wird. Der wiederhergestellte Agent wird weiterhin versuchen, die alte Adresse und den alten Host-Namen zu erreichen. Sie können den Agenten nach der Wiederherstellung neu registrieren, um dessen Backup-Verwaltung in der Disaster-Recovery-Umgebung fortzusetzen – oder Sie stellen sicher, dass der wiederhergestellte Management Server denselben Namen und dieselbe Adresse wie der alte verwendet.

Wenn Sie einen vSphere/ESXi-Host an Ihrem Disaster Recovery-Standort haben, ist der grundlegende Workflow etwas anders:

- Zuerst empfehlen wir, dass Sie im Voraus eine VM-Kopie Ihres Management-Servers speichern. Sie können eine solche Kopie erstellen, indem Sie eine normale '**Zu VM konvertieren**'-Aktion zu Ihrem Offsite-Standort durchführen – mit Ihrem Hypervisor als Ziel.
- Sie beginnen dann die Disaster Recovery-Prozedur damit, dass Sie einfach diese VM des Management Servers aktivieren.
- Sobald diese VM läuft, können Sie den Offsite-Backup-Storage hinzufügen oder aktualisieren.
- Registrieren Sie den vSphere/ESXi-Host auf dem Management Server, der in dieser virtuellen Umgebung läuft.
- Um die wichtigste Infrastruktur wiederherzustellen, verwenden Sie die Option '**VM von Backup ausführen**', damit die entsprechenden Systeme innerhalb weniger Minuten als virtuelle Maschinen betriebsbereit sind. Durch die Ausführung der Maschine als VM werden die Daten nicht zurück zum Datenspeicher kopiert. Sie wird einfach vom System gemountet und direkt verwendet. Diese laufende VM kann ohne Ausfallzeiten in die Produktion verschoben werden – eine einzigartige Funktion von Acronis Backup 12.5.
- Die anderen, weniger wichtigen Maschinen können dann mit den weiter oben beschriebenen Methoden wiederhergestellt werden.

7.2.4.2 Verwaltete Speicherorte (inklusive Deduplizierung)

Verwaltete Speicherorten sind dahingehend besonders, dass bei ihnen die Backup-Metadaten auf dem Acronis Storage Node gespeichert werden. Dies ist besonders bei der Deduplizierung wichtig, da diese Metadaten für Wiederherstellungen erforderlich sind und deren erneute Generierung viel Zeit benötigt.

Für externe verwaltete Speicherorte bedeutet dies, dass Sie den Storage Node unbedingt am selben externen Standort wie das Storage-Medium vorhalten sollten und dass Sie diesen Storage Node dann über das Internet/WAN registrieren sollten.

Wenn Sie diese empfohlene Konfiguration verwenden, gelten weiterhin die Standardprozeduren (S. 71) – bis auf eine einfache Änderung:

- Nachdem Sie den Management Server wiederhergestellt haben, müssen Sie den Storage Node auf dem wiederhergestellten Server erneut registrieren.
  Auf die Backups kann genauso zugegriffen werden als würden Sie vom lokalen Management Server verwaltet, da der Storage Node eigenständig (in sich geschlossen) ist.

Beachten Sie, dass Sie außerdem auf jeden Storage Node-Speicherort direkt mit einem Boot-Medium zugreifen können (statt über den Management Server gehen zu müssen). Geben Sie im Wiederherstellungsfenster einfach '**`bsp://storage.node.address/`**' als Speicherortpfad ein. Wobei '**`bsp`**' für „Backup Storage Protocol“ steht. Es ist das Protokoll von Acronis, das vom Storage Node zur Kommunikation mit den Agenten verwendet wird.

7.2.4.3 Zu externen Standorten gesendete Bänder

Band-Metadaten werden ebenfalls auf dem Storage Node gespeichert. Diese Band-Indexdaten werden benötigt, um die entsprechenden Backups wiederherstellen zu können. Dies bedeutet: da es Tage dauern kann, eine große Anzahl von Bändern erneut zu scannen, bevor Sie die Metadaten neu generieren und dann verwenden können, ist es für diese Art von Umgebung besonders wichtig, vorbereitet zu sein, wenn Sie mehr als nur ein paar Server sichern wollen.

Der entscheidende Vorbereitungsschritt bei diesem Szenario ist einfach: Stellen Sie sicher, dass das Backup der Storage Node-Banddatenbank am selben Speicherplatz vorliegt wie der externe Band-Storage. Jedes Mal, wenn Sie Bänder zu dem externen Standort schicken, sollten Sie auch eine aktualisierte Backup-Kopie des Storage Nodes mitsenden. Das Backup kann auf Band oder einem anderen Medium gespeichert werden. Es ist beispielsweise eine gute Alternative, eine Kopie in der Cloud aufzubewahren, sofern Ihr Zweitstandort über einen Internetzugriff verfügt. Da Sie nur eine Kopie des Systems und dessen Metadaten benötigen, sollte das Backup des Storage Nodes nicht viel Speicherplatz belegen.

Wenn Sie das Storage Node-Backup zusammen mit den anderen versendeten Bändern ebenfalls auf Band speichern, sollten Sie sicherstellen, dass Sie dieses Band passend beschriften.

- Sie beginnen die Wiederherstellungsprozedur damit, dass Sie dieses Backup des Storage Nodes mithilfe eines Boot-Mediums zu einer neuen Maschine wiederherstellen. Dazu gehört auch das Einscannen des Bandes vom Boot-Medium aus, wodurch die gespeicherten Wiederherstellungspunkte dann in der Benutzeroberfläche des Boot-Mediums verfügbar werden.
- Wenn der Storage Node zusammen mit der Banddatenbank wiederhergestellt wurde, können Sie die weiteren Bänder verwenden, ohne dass diese gescannt werden müssen, wodurch Sie viele Stunden an Zeit spart.
- Sobald der Storage Node wieder betriebsbereit ist, können Sie mit der im oberen Abschnitt über verwaltete Speicherorte beschriebenen Prozedur weiterverfahren.

8 Sonstige Empfehlungen

Dieser Abschnitt enthält eine Reihe unterschiedlicher Empfehlungen, die nicht an keine besonderen Umgebungsdetails gebunden sind.

8.1 Nicht unterstützte Betriebssysteme sichern

Dieser Abschnitt gilt auch für unterstützte Betriebssysteme, auf denen Sie – aus Sicherheits- oder anderen Gründen – keinen Agenten installieren können.

Die Image-Backups von Acronis Backup 12.5 werden auf der unteren Blockebene von Laufwerken erstellt. Das bedeutet, dass Sie auch ein nicht unterstütztes Betriebssystem mit einem unterstützten Dateisystem sichern können, solange der Agent, der dieses Backup ausführt, mit diesem Dateisystem umgehen kann.

Mit „nicht unterstützten“ Systemen meinen wir alle Betriebssysteme, unter denen kein Agent installiert werden kann. Meistens liegt das daran, dass die derzeitige Version des Agenten bestimmte Bibliotheken benötigt, die für die alten Systeme nicht mehr verfügbar sind. Wir bemühen uns sehr, auch ältere Systeme weiter zu unterstützen. So sind wir beispielsweise eine der wenigen Lösungen, bei der Sie einen Agenten noch unter Windows XP installieren können. Aber natürlich können wir das nicht unbegrenzt lange tun.

Wie weiter oben erwähnt (S. 67) steht Ihnen aber immer die bootfähige Umgebung mit ihrem eigenständigen Agenten zur Verfügung. Dieser Agent ist vollständig von dem Betriebssystem unabhängig, das auf dem zu sichernden Laufwerk installiert ist. Solange dieser Agent das betreffende Dateisystem sichern kann, können Sie das Backup durchführen, ohne irgendetwas installieren zu müssen.

Ja, Sie können sogar nicht unterstützte Dateisysteme sichern, wenn Sie die Backup-Option '**Sektor-für-Sektor**' verwenden. Dafür muss nur eine Voraussetzung erfüllt sein: es darf kein „verteiltes“ Dateisystem sein, sondern muss auf „Blockgeräten“ basieren. Denn bei dieser Methode wird jeder Block des ursprünglichen Laufwerks kopiert – was den freien Speicherplatz mit einschließt.

Wenn Sie ein solches System sichern wollen, gehen Sie folgendermaßen vor:

1. Booten Sie das System mit unserem Boot-Medium und registrieren Sie dieses auf dem Management Server (wie im Abschnitt über die „Empfehlungen zu Wiederherstellungen“ (S. 67) beschrieben).
2. Erstellen Sie einen Backup-Plan auf dem Boot-Medium.
3. Booten Sie die Maschine neu und führen Sie den Backup-Plan dann aus, wenn ein Backup erstellt werden soll. Es ist derzeit nicht möglich, die Maschine auf Basis einer Planung direkt vom Produkt aus neu zu booten. Dieser Prozess kann daher nicht vollständig aus Acronis Backup 12.5 heraus automatisiert werden.

8.2 Tragbare Geräte sichern

In Bezug auf die Sicherung von tragbaren Geräten wie Laptops und Notebooks gibt es einige Besonderheiten. Sie können beispielsweise die Backup-Ausführung unterbinden, wenn das Gerät mit einem VPN oder Mobilfunknetzwerk (getaktete Verbindung) verbunden ist.

Um solche Szenarien besser zu unterstützen, wurden mit Acronis Backup 12.5 Update 2 einige neue Planungsoptionen und Backup-Startbedingungen eingeführt.

Neue Planungsoptionen:

- Eine Maschine kann für ein Backup aus dem Energiesparmodus aufgeweckt werden
- Während eines Backups kann der Standby- oder Ruhezustandsmodus verhindert werden
- Eine Option, die die Ausführung verpasster Backups beim Start einer Maschine verhindert

Neue Backup-Startbedingungen:

- Nicht starten, wenn im Akkubetrieb
- Im Akkubetrieb starten, wenn Akkustand höher ist als:
- Nicht starten, wenn eine getaktete Verbindung besteht
- Nicht starten, wenn eine Verbindung mit folgenden WLANs besteht:
- IP-Adresse des Gerätes überprüfen

Sie können diese Bedingungen verwenden, wenn Sie zentrale Backup-Richtlinien für Ihre Laptops, Notebooks oder Tablets erstellen.

Eine ausführliche Beschreibung dieser Optionen finden Sie in der offiziellen Benutzeranleitung: https://www.acronis.com/de-de/support/documentation/AcronisBackup_12.5/#37575.html.

8.3 Per Skript festgelegter Speicherort

Mit dieser leistungsfähigen Funktion können Sie den Backup-Speicherort per Parameter festlegen. Wenn Sie beispielsweise viele Maschinen sichern müssen, können Sie bestimmen, dass jede Maschine einen bestimmten lokalen Ordner, der den Namen der Maschine erhält, als Backup-Ziel verwendet.

Bei einem solchen Fall sollten Sie kein Backup für jede Maschine erstellen, sondern ein Skript verwenden, mit dem sich die verschiedenen Speicherorte alle über einen einzigen Plan auflösen lassen. Die Skripte können in JScript oder VBScript geschrieben werden. Wenn der Backup-Plan bereitgestellt wird, führt die Software das Skript auf jeder Maschine aus. Die Skript-Ausgabe für jede Maschine sollte eine Zeichenkette sein, die den jeweiligen Ordnerpfad (lokal oder Netzwerkpfad) enthält. Falls ein entsprechender Ordner nicht existiert, wird er automatisch erstellt. Jeder Ordner wird auf der Registerkarte **Backups** als separater Backup-Speicherort angezeigt. Spezifizieren Sie für Netzwerkordner die Zugriffsanmeldedaten mit den Lese-/Schreibberechtigungen.

Beispiel: das fogende JScript-Skript gibt den Backup-Speicherort für eine Maschine im Format '**\\bkpsrv\<machine name>**' aus:

```
WScript.echo("\\\\bkpsrv\\" +
WScript.CreateObject("WScript.Network").ComputerName);
```

Als Ergebnis dieser Aktion werden die Backups einer jeden Maschine in einem Ordner gleichen Namens auf dem Server **bkpsrv** gespeichert.

9 Komprimierung und Verschlüsselung

9.1 Komprimierung

Acronis Backup 12.5 verwendet einen neuen Komprimierungsalgorithmus namens Zstandard (bzw. Zstd).

Selbst bei „normaler“ Einstellung für die Komprimierung bietet dieser neue Algorithmus bessere Komprimierungsgrade und Geschwindigkeiten als zuvor mit Zlib bei höheren Einstellungen.

Grundsätzlich empfehlen wir bei Acronis, die Standardeinstellungen für die Komprimierung zu verwenden, da damit der beste Ausgleich aus Speicherplatzeinsparungen und Backup-Performance erreicht wird.

9.2 Verschlüsselung

Die Verschlüsselungseinstellungen werden beim Erstellen eines Backup-Plans festgelegt und können später nicht mehr geändert werden. Wenn Sie andere Verschlüsselungseinstellungen verwenden möchten, müssen Sie einen neuen Backup-Plan erstellen.

Es stehen drei Verschlüsselungsstufen zur Verfügung:

- AES 128
- AES 192
- AES 256

Die Verschlüsselungsstufe ist ein Kompromiss zwischen Sicherheit und Backup-Performance des Agenten. Die Verschlüsselung auf einer höheren Stufe verbraucht mehr Zeit und CPU-Ressourcen.

Beachten Sie, dass auch eine geringe Verschlüsselungsstufe Auswirkungen auf die Backup-Zeiten hat. Unsere Empfehlungen:

- Verschlüsseln Sie immer Backups, die an einen Offsite-Standort gesendet oder in der Cloud gesichert werden.
- Verschlüsseln Sie Backups, die vertrauliche Daten enthalten, z. B. Krankenunterlagen oder Kundendaten.

Beachten Sie, dass für alle Recovery-Aktionen verschlüsselter Backups ein Kennwort erforderlich ist. Wenn das Kennwort verloren geht, ist keine Wiederherstellung möglich.

Sie können Verschlüsselung auch als Maschinen-Eigenschaft verwenden. Weitere Details finden Sie in unserer Dokumentation unter https://www.acronis.com/en-us/support/documentation/AcronisBackup_12.5/#37608.html.

10 Anhang A. Services (Dienste)

10.1 Agent-Dienste (Windows)

Name	Verwendung	Prozess	Datenbank (C:\ProgramData\Acronis)	Logs (C:\ProgramData\Acronis)	Vom Dienst verwendeter Port
Acronis Remote Agent Service	Älterer Dienst zur Verbindung zwischen den Acronis Komponenten	agent.exe	N/A	N/A	9876
Acronis Scheduler2 Service	Führt geplante Tasks auf bestimmte Ereignisse hin aus	schedul2.exe Unterprozess: schedhlp.exe	N/A	\Acronis\Schedule2	8081
Acronis Active Protection Service	Ermöglicht Schutz vor Ransomware	active_protection_service.exe	\ActiveProtection	\ActiveProtection\Logs	6109
Acronis Removable Storage Management Service	Zur Verwaltung von Bandgeräten	arsm.exe	\BackupAndRecovery\ARSM\Database	\BackupAndRecovery\ARSM	9852 43239
Acronis Managed Machine Service	Bietet Funktionalität für Backup, Recovery, Replikationen, Aufbewahrung, Validierung	mms.exe Unterprozess: service_process.exe	\BackupAndRecovery\MMSData\DML	\BackupAndRecovery\MMS	
Tib Mounter Service	Ermöglicht es, tib-Dateien zu mounten und durchsuchen	tib_mounter_service.exe	N/A	\TibMounterServiceLogs	

10.2 Management Server-Dienste (Windows)

Name	Verwendung	Prozess	Datenbank (C:\ProgramData\Acronis)	Logs (C:\ProgramData\Acronis)	Vom Dienst verwendeter Port
Acronis Remote Agent Service	Älterer Dienst zur Verbindung zwischen den Acronis Komponenten	agent.exe	N/A	N/A	9876
Acronis Scheduler2 Service	Führt geplante Tasks auf bestimmte Ereignisse hin aus	schedul2.exe, untergeordneter Prozess: schedhlp.exe	N/A	\ServiceManager\Logs	8081
Acronis Service Manager Service	Stellt die Funktionalität für die Acronis Management Server-Dienste bereit	asm.exe	N/A	\ServiceManager\Logs	30500 9851
		Untergeordnete Prozesse:			
		api_gateway.exe	N/A	\ApiGateway\Logs	9877
		task_manager.exe	\TaskManager\	\TaskManager\Logs	30677
		policy_manager.exe	\PolicyManager\	\PolicyManager\Logs	30676
		vault_manager.exe	\VaultManager\	\VaultManager\Logs	9221
		catalog_manager.exe	\CatalogManager\	\CatalogManager\Logs	9222
		account_server.exe	\AccountServer\	\AccountServer\Logs	30678
		group_manager.exe	\GroupManager\	\GroupManager\group_manager.log	30680
		scheduler.exe	\Scheduler	N/A	
		acronis_license_service.exe	N/A	\LicenseServer\Logs	30443
		acronis_notification_service.exe	N/A	\NotificationService\Logs	30572
		tracer.exe	N/A	\ServiceManager\Logs	
Acronis Web Server	Für die Ausführung der Backup-Konsole verantwortlich	ams_web_service.exe	N/A	\WebServer\Logs	30679
Acronis ZeroMQ Gateway Service	Kommunikation zwischen Agenten und Management Server	zmqgw.exe	N/A	\ZmqGw	7780 7755 7756 7765
Acronis Management Server Service	Zentrale Verwaltung der Acronis Agenten	ManagementServer.exe	\Acronis\AMS	\Acronis\AMS\logs	
Acronis Monitoring Service	Zusammenstellen und Anzeigen von Berichtsdaten	acronis_monitoring_service.exe	\MonitoringServer\am-database\metrics	\MonitoringServer\Logs	30444

10.3 Acronis Storage Node- und Backup Agent-Dienste (auf der Acronis Storage Node-Maschine) (Windows)

Name	Verwendung	Prozess	Datenbank (C:\ProgramData\Acronis)	Logs (Protokolle): (C:\ProgramData\Acronis)	Vom Dienst verwendeter Port
Acronis Storage Node Service	Verwaltet die Aktionen in verwalteten Speicherorten	StorageServer.exe	N/A	\BackupAndRecovery\ASN\logs	
Acronis Catalog Browser Service	Zeigt die in allen verwalteten Speicherorten gesicherten Daten an	catalog_browser.exe	\BackupAndRecovery\ASN\DmlDatabase	\CatalogBrowser\Logs	
Elasticsearch 2.4.0 (elasticsearch-service - x64)	Zum Indizieren und Durchsuchen von Daten in Backups	elasticsearch-service-x64.exe	\ElasticSearch\Data	\ElasticSearch\Logs	

10.4 Dienst-Konten

Die meisten der oben aufgeführten Dienste werden unter den Konten 'Lokales System' oder 'Netzwerkdienst' installiert und ausgeführt.

Sie können aber auch eigenen Dienstbenutzer spezifizieren – und zwar für diese drei Dienste des Produktes:

1. der Acronis Managed Machine Service auf dem Agenten
2. der Acronis Management Server Service auf dem Management Server
3. der Acronis Storage Node Service auf dem Storage Node

Standardmäßig wird der Managed Machine Service auf dem Agenten unter dem Konto **Lokales System** installiert und ausgeführt. Der Management Server Service bzw. der Storage Node Service werden von unserem Installer mit einem neu erstellten Benutzer installiert, der **AMS User** bzw. **ASN User** genannt wird.

Sie können den Dienstbenutzer aber während der Installation ändern, wenn Sie die Option **Folgendes Konto verwenden** auswählen. Diese Option ist zwingend erforderlich, wenn Sie auf einem Domain Controller installieren, da das Installationsprogramm auf diesem aus Sicherheitsgründen keine neuen Konten erstellen kann.

Neue Konten werden mit einem zufälligen GUID-Kennwort erstellt.

Den Benutzern werden bei der Installation folgende Berechtigungen zugewiesen:

Acronis Managed Machine Service

- Mitglied in der Gruppe der Sicherungs-Operatoren und Administratoren.
  Die Mitgliedschaft in der Gruppe der Administratoren erfolgt nur dann, wenn es ein neuer Benutzer ist. Bereits vorhandenen Benutzern wird diese Mitgliedschaft nicht gewährt.
- Es wird die Berechtigung **Vollzugriff** auf den Ordner '%PROGRAMDATA%\Acronis' (bei Windows XP und Server 2003: '%ALLUSERSPROFILE%\Application Data\Acronis') und dessen Unterordner gewährt.
- Es wird die Berechtigung **Vollzugriff** auf bestimmte Registry-Schlüssel im folgenden Schlüssel gewährt: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis.
- Diese Benutzerrechte werden zugewiesen:
  - Als Dienst anmelden.
  - Anpassen von Speicherkontingenten für einen Prozess.
  - Ersetzen eines Tokens auf Prozessebene.
  - Verändern der Firmwareumgebungsvariablen.

Acronis Management Server Service

- Mitgliedschaft in den Gruppen 'Acronis ApiGatewayUsers' und 'Acronis Centralized Admins'.
  Diese Gruppen werden während der Installation erstellt und zur Gruppen- und Benutzerverwaltung im Produkt verwendet.
- Es wird die Berechtigung **Vollzugriff** auf den Ordner '%PROGRAMDATA%\Acronis' (bei Windows XP und Server 2003: '%ALLUSERSPROFILE%\Application Data\Acronis') und dessen Unterordner gewährt.
- Es wird die Berechtigung **Vollzugriff** auf bestimmte Registry-Schlüssel im folgenden Schlüssel gewährt: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis.
- Diese Benutzerrechte werden zugewiesen:
  - Als Dienst anmelden.

Acronis Storage Node Service

- Mitglied in der Gruppe der Sicherungs-Operatoren, Administratoren, Acronis Centralized Admins, Acronis Remote Users.
  Die Mitgliedschaft in der Gruppe der Administratoren erfolgt nur dann, wenn es ein neuer Benutzer ist. Bereits vorhandenen Benutzern wird diese Mitgliedschaft nicht gewährt.
  Die Gruppen Acronis Centralized Admins und Acronis Remote Users werden während der Installation erstellt.
- Es wird die Berechtigung 'Vollzugriff' auf den Ordner '%PROGRAMDATA%\Acronis' (bei Windows XP und Server 2003: '%ALLUSERSPROFILE%\Application Data\Acronis') und dessen Unterordner gewährt.
- Es wird die Berechtigung 'Vollzugriff' auf bestimmte Registry-Schlüssel im folgenden Schlüssel gewährt: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis.
- Diese Benutzerrechte werden zugewiesen:
  - Als Dienst anmelden.

Die Gruppe 'Acronis Remote Users' ist veraltet und wird bei zukünftigen Updates entfernt. Wenn Sie Update 2 oder höher ausführen, können Sie die Gruppe auch manuell entfernen.

10.5 Services und Komponenten (Linux)

Ports, die mit **(i)** gekennzeichnet sind, lauschen auf 'localhost' nur und müssen nicht geöffnet werden.

Name des Services	Verwendung	Prozess	/etc/init.d Skript	Vom Dienst verwendeter Port	Komponente
Acronis Remote Agent Service	Älterer Service, der die Konnektivität zwischen den Acronis Komponenten ermöglicht	/usr/lib/Acronis/Agent/acronisagent	acronis_agent	9876	Acronis Agent für Linux
Acronis Removable Storage Management Service	Zur Verwaltung von Bandgeräten	/usr/lib/Acronis/ARSM/arsm	acronis_rsm	zufällig (i)	Acronis Agent für Linux
Acronis Service Manager Service	Stellt die Funktionalität für die Acronis Management Server-Dienste bereit	usr/lib/Acronis/ServiceManager/asm	acronis_asm	-	Acronis Management Server
		ASM – untergeordnete Dienste/Prozesse:			
		/usr/lib/Acronis/ApiGateway/api_gateway		9877	
		/usr/lib/Acronis/WebServer/acronis_web_service		30679(i)	
		/usr/lib/Acronis/TaskManager/task_manager		30677(i)	
		/usr/lib/Acronis/PolicyManager/policy_manager		30676(i)	
		/usr/lib/Acronis/VaultManager/vault_manager		30691(i)	
		/usr/lib/Acronis/CatalogManager/catalog_manager		30692(i)	
		/usr/lib/Acronis/AccountServer/account_server		30678(i)	
		/usr/lib/Acronis/GroupManager/group_manager		30680(i)	
		/usr/lib/Acronis/Scheduler/scheduler		30681(i)	
		/usr/lib/Acronis/LicenseServer/acronis_license_service-bin		30443(i)	
		/usr/lib/Acronis/NotificationService/acronis_notification_service		30572(i)	
		/usr/lib/Acronis/UpdateService/update_service		46471(i)	
Acronis Managed Machine Service	Stellt die Funktionalitäten für Backup, Recovery, Replikation, Aufbewahrung, Validierung bereit	/usr/lib/Acronis/BackupAndRecovery/mms	acronis_mms	43234 9850	Acronis Agent für Linux
Acronis ZMQ Gateway Service	Ermöglicht die Kommunikation zwischen den Agenten und dem Management Server	/usr/lib/Acronis/ZmqGw/zmqgw	acronis_zmqgw	7780 7765(i) 7756(i) 7755(i)	Acronis Management Server
Acronis Management Server Service	Zentrale Verwaltung der Acronis Agenten	/usr/lib/Acronis/AMS/ManagementServer	acronis_ams	9851 30500(i)	Acronis Management Server
Acronis Monitoring Service	Berichtsdaten zusammenstellen und anzeigen	/usr/lib/Acronis/MonitoringServer/acronis_monitoring_service	acronis_monitoring_service	30444(i)	Acronis Management Server

10.6 Speicherung der Anmeldedaten

Anmeldedaten werden im Dateisystem im Ordner **C:\ProgramData** gespeichert. Sie werden mit dem Algorithmus AES-256-CBC verschlüsselt. Der Codierungsschlüssel wird für jeweils für folgende Dienste erstellt:

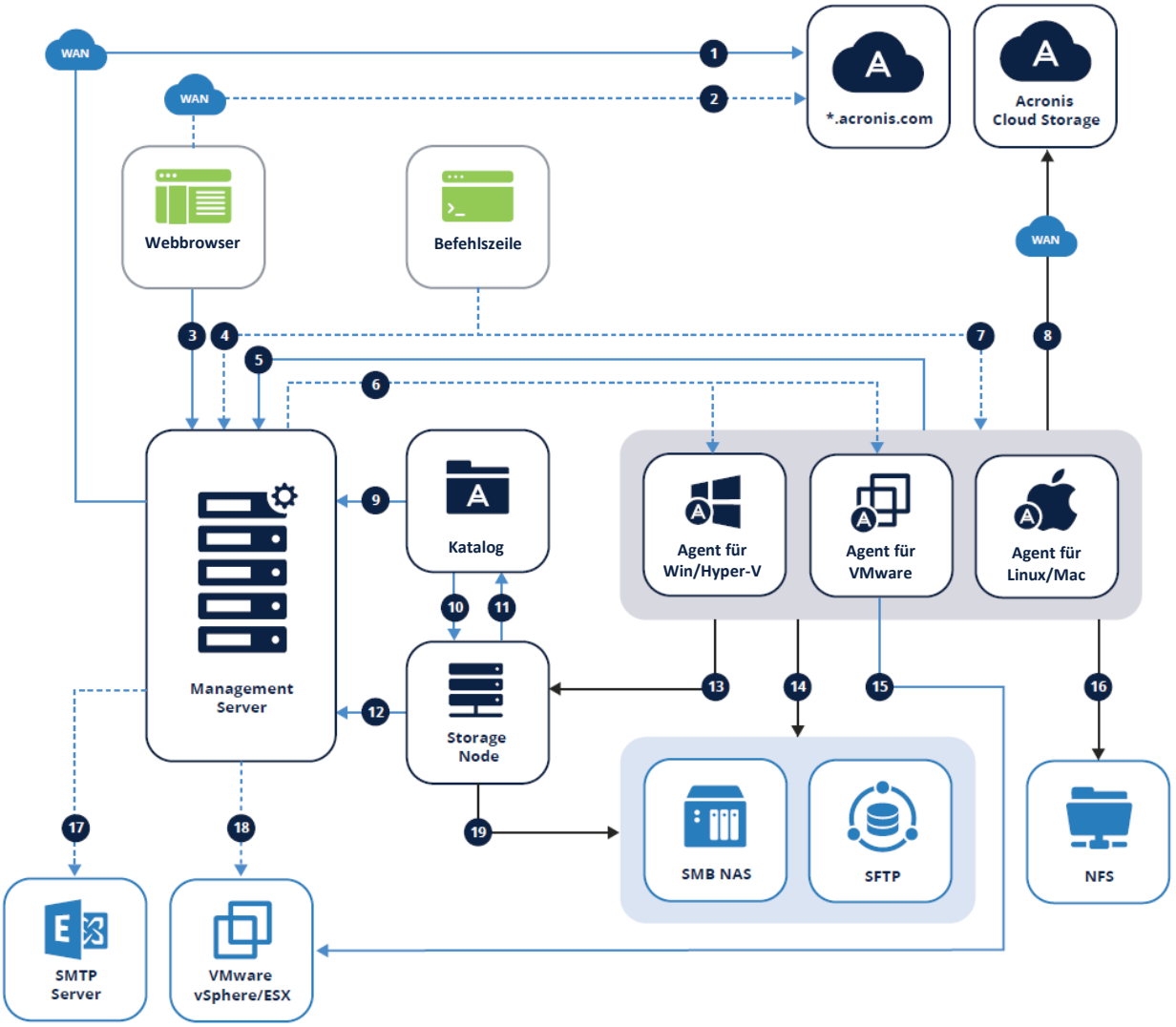
- Acronis Management Server Service
- Managed Machine Service
- Acronis Storage Node Service

Wenn alle drei Dienste auf demselben Server installiert sind, verwendet jeder seinen eigenen Anmeldedatenspeicher und Codierungsschlüssel.

Dieser Schlüssel wird folgendermaßen generiert:

- Während des Installationsvorgangs wird ein zufälliger hochentropischer „Maschinenschlüssel“ generiert.
- Auf Basis dieses Maschinenschlüssels wird dann der eigentliche Codierungsschlüssel mithilfe eines Algorithmus abgeleitet, der in der Anmeldedatenspeicher-Applikation implementiert ist.

11 Anhang B. Netzwerkdiagramm und Ports



Die Bildbeschreibung finden Sie auf der nächsten Seite.

Legende

Die Pfeilrichtung zeigt an, welche Komponente die Verbindung initiiert. Beachten Sie, dass alle Ports vom Typ 'TCP' sind (außer es ist anders angegeben).

1.	Installationskomponenten herunterladen: 80 zu dl.acronis.com	**12.**	- ASN verwalten: 7780 ZMQ - ASN registrieren und Tasks verwalten: TCP 9877
2.	Abonnement-Lizenzen synchronisieren: 443 zu account.acronis.com	**13.**	Backup zu verwaltetem Speicherort: 9876,9852
3.	Umgebung verwalten: 9877	**14.**	- SMB: UDP 137, UDP 138 und TCP 139, TCP 445 - SFTP: 22 (Standard, kann geändert werden)
4.	Zugriff über Remote-Befehlszeile (acrocmd, acropsh): 9851	**15.**	VM-Backups erstellen: 443, 902
5.	- Agent registrieren: 9877* - Agent verwalten: 7780 ZMQ - Lizenzen synchronisieren: 9877	**16.**	NFS: TCP, UDP 111 und 2049
6.	Remote-Installation: **U1 und früher**: 445, 25001, 9876 **U2+**: 445, 25001, 43234	**17.**	Berichte und E-Mails senden: SMTP (25, 465, 587 etc.)
7.	Zugriff über Remote-Befehlszeile (acrocmd, acropsh): 9850	**18.**	Appliance bereitstellen: 443, 902
8.	Backups zum Acronis Cloud Storage erstellen: 443, 8443, 44445, 5060	**19.**	- SMB: UDP 137, UDP 138 und TCP 139, TCP 445 - SFTP: 22 (Standard, kann geändert werden)
9.	Backups suchen und durchsuchen: 9877		
10.	Backups indizieren: 9876		
11.	Katalog-Metadaten empfangen: 9200		

*Vergleiche die untere Einschränkung.

Während der Maschinen-Registrierung eingegebene Anmeldedaten

Bei Update 2 und früheren Versionen werden die Anmeldedaten, die während der Maschinen-Registrierung eingegeben wurden, nicht verschlüsselt über das Netzwerk übertragen. Sie dienen lediglich der korrekten Identifizierung der Organisationseinheit, in welcher der Agent registriert werden soll. Sie können das Kennwort daher auch leer lassen, wenn Sie es nicht mögen, dass es unverschlüsselt über das Netzwerk übertragen wird. Dieses Vorgehen wird bei zukünftigen Updates geändert werden.

Ports

In diesem Abschnitt werden die unterschiedlichen Ports aufgelistet, die zur Kommunikation zwischen den verschiedenen Acronis Komponenten geöffnet sein sollten – und zwar sowohl innerhalb des Netzwerks als auch für den Netzwerkverkehr nach außen. Es handelt sich um dieselben Ports wie im oberen Diagramm, nur dass sie hier noch einmal nach Komponenten aufgelistet sind.

Beachten Sie, dass alle Kommunikationen zwischen den Diensten einer einzelnen Komponente ebenfalls über Netzwerkverbindungen erfolgen. Diese Dienste lauschen ausschließlich auf der 'localhost'-Adresse. Diese internen Ports sind hier nicht aufgeführt, da sie nicht in der Firewall geöffnet und nicht im Netzwerk geändert werden müssen. Sie können diese Informationen in der entsprechenden Spalte der Tabellen im Anhang A (S. 77) finden.

Obwohl die internen Ports den Datenverkehr nicht beeinflussen, können sie dennoch einen Konflikt verursachen, wenn eine andere Applikation auf demselben Port lauscht. Sie können die von den Acronis Diensten verwendeten internen Ports normalerweise ändern – und zwar über die .json-Konfigurationsdatei des jeweiligen Dienstes, die Sie in dessen Verzeichnis finden: ***c:\Program Files\Acronis\[Dienstname]\[Dienstname].json***

Management Server

Folgende Ports sollten immer auf dem Management Server für die eingehenden Verbindungen der verschiedenen Komponenten geöffnet sein:

- TCP 9877
- TCP 7780

Folgende Ports sind optional, wenn Sie per Remote-Befehlszeile auf den Management Server zugreifen wollen:

- TCP 9851

Backup Agenten

Für ihre reguläre Backup- und Recovery-Funktionalität benötigen die Agenten keine offenen Ports. Sie können optional die folgenden Ports für Remote-Installationen und Remote-Zugriffe über die Befehlszeile öffnen:

- TCP 445, 25001, 9876 (Remote-Installation für U1 und früher)
  TCP 445, 25001, 43234 (Remote-Installation für U2 und später)
- TCP 9850 (Zugriff über die Remote-Befehlszeile)

Storage Node

Der Storage Node benötigt zur Kommunikation mit Agenten, dass folgende eingehende Ports offen sind:

- TCP 9876, 9852

Folgende Ports müssen zur Kommunikation mit dem Katalog offen sein (sofern dieser separat installiert ist):

- TCP 9876

Katalog

Wenn der Katalog separat installiert ist, muss er eingehende Verbindungen von allen Storage Nodes auf diesem Port annehmen können:

- TCP 9200

Ausgehende WAN-Verbindungen

Wenn Sie die Acronis Cloud-Funktionalität verwenden, muss die Firewall ausgehende Verbindungen zu den folgenden Ports zulassen:

- TCP 80 (Installationsdateien über die Benutzeroberfläche herunterladen)
- TCP 443 (Lizenzen mit account.acronis.com synchronisieren – für Abonnementlizenzen erforderlich)
- TCP 443, 8443, 44445, 5060 (Backups zum Acronis Cloud Storage erstellen)

Dritthersteller-Komponenten

Die Acronis Produkte müssen für bestimmte Funktionalitäten auch mit externen Komponenten kommunizieren können: Ihr SMTP-Server muss beispielsweise Verbindungen vom Management Server annehmen können, um die E-Mail-Benachrichtigungsfunktionalität verwenden zu können. Der nachfolgende Abschnitt listet die am häufigsten verwendeten Komponenten und deren Ports auf:

- **VMware**: TCP 443, 902 (müssen für alle Verbindungen von Acronis Komponenten offen sein, die mit vSphere/ESX kommunizieren)
- **SMTP**: Zu den Standardports gehören: TCP 25, 465, 587 etc. (vom AMS zum Mail-Server, der Port kann geändert werden)
- **NFS**: TCP, UDP 111 und 2049 (von Agenten zum NFS-Host)
- **SMB**: UDP 137, UDP 138 und TCP 139, TCP 445 (von Agenten zu SMB-Freigaben)
- **SFTP**: Standardport: TCP 22 (kann in der Server-Konfiguration geändert werden)

Urheberrechtserklärung

Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch einzelne oder mehrere U.S.-Patentnummern abgedeckt und geschützt:
7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234 sowie schwebende Patentanmeldungen.