# **Bachelor Thesis**

"Ein Datensicherungssystem für die virtuelle Umgebung im Rechenzentrum der Berufsakademie Glauchau"

Vorgelegt am: 28. August 2015

Von: Kevin Haberland

Dietrich-Bonhoeffer Straße 37

08371, Glauchau

**Studiengang:** Technische Informatik

Studienrichtung: Daten- und Kommunikationstechnik

**Seminargruppe:** TI 2012

Matrikelnummer: 4001092

**Praxispartner:** SMI Computersysteme GmbH

Wehrstraße 13d 08371, Glauchau

Gutachter: Dipl.-Ing. Holger Schell

(SMI Computersysteme GmbH)

Dipl.-Inf. Falk Puschmann

(Staatliche Studienakademie Glauchau)

| Sperrvermerk  |
|---|
| Die vorliegende Bachelor-Thesis mit dem Thema "Ein Datensicherungssystem für die virtuelle Umgebung im Rechenzentrum der Berufsakademie Glauchau" beinhaltet interne und vertrauliche Informationen des Unternehmens. |
| Die Einsicht der Arbeit ist lediglich den zugewiesenen Gutachtern und den<br>befugten Mitgliedern des Prüfungsausschusses gestattet. Die Veröffentlichung   |
| des Dokuments wird sowohl im Ganzen, als auch in Auszügen, untersagt.   |

II

# Inhaltsverzeichnis

| Speri | rverme  | rk    |  | I    |
|-------|---------|-------|--|------|
| Inhal | tsverze | eichr | nis  | III  |
| Abbil | dungsv  | verze | eichnis  | V    |
| Tabe  | llenver | zeic  | hnis   | V    |
| Abkü  | rzungs  | sverz | eichnis  | . VI |
| 1 E   | inführ  | ung.  |  | 1    |
| 1.1   | Anr     | merk  | ung  | 1    |
| 1.2   | Pro     | jektr | notivation   | 1    |
| 1.3   | Gru     | undla | agen   | 1    |
| 1     | .3.1    | Beg   | griffe   | 1    |
|       | 1.3.1   | .1    | Backup   |      |
|       | 1.3.1   | .2    | Replikation  | 2    |
| 1     | .3.2    | Bac   | kupmethoden  | 2    |
|       | 1.3.2   | 2.1   | Vollbackup   | 2    |
|       | 1.3.2   | 2.2   | Differentielles Backup                                   |      |
|       | 1.3.2   | 2.3   | Vorwärts-inkrementelles Backup                           | 3    |
|       | 1.3.2   | 2.4   | Rückwärts-inkrementelles Backup                          |      |
|       | 1.3.2   | 2.5   | Synthetisch volles Backup                                | 5    |
| 1     | .3.3    | Prin  | nzipien der Backuprotation                               | 6    |
|       | 1.3.3   | 3.1   | FIFO   | 6    |
|       | 1.3.3   | 3.2   | Generationenprinzip                                      | 6    |
|       | 1.3.3   | _     | Türme von Hanoi  |      |
| 1     | .3.4    | Die   | 3-2-1-Regel  | 7    |
| 1     | .3.5    | Anf   | orderungen an Backups und Replikationen                  | 7    |
|       | 1.3.5   | 5.1   | Geringer Speicherplatzbedarf                             |      |
|       | 1.3.5   | 5.2   | Schnelles und sicheres Anlegen/Zurückspielen von Backups |      |
|       | 1.3.5   | -     | Sicherung auf externe Standorte                          |      |
| 1     | .3.6    | Vee   | eam Backup & Replication                                 |      |
|       | 1.3.6   | 5.1   | Einführung   | 9    |
|       | 1.3.6   | 5.2   | Architektur des Programms                                | 9    |
| 2 V   |         |       | ungen  |      |
| 2.1   | Situ    |       | n an der BA Glauchau                                     |      |
| 2     | 2.1.1   |       | Struktur der BA Glauchau                                 |      |
| 2.2   |         |       | hannel als Übertragungsmedium                            |      |
| 2.3   | Ers     |       | ng eines Konzeptes zur Realisierung der Datensicherungen |      |
| 2     | 2.3.1   |       | überlegungen   |      |
| 2     | 2.3.2   |       | tellung des Zeitplanes für die Anlegung der Backups      |      |
| 2     | 2.3.3   | Mö    | glichkeiten zur Implementierung einer Replikation        | . 14 |
| 2 4   | Διισ    | swah  | ol des Transportmodus für VBR                            | 15   |

|   | 2.4.1    | Einführung  | 15 |
|---|----------|---|----|
|   | 2.4.2    | Direct SAN Access Mode                                  | 15 |
|   | 2.4.2    | .1 Erklärung  | 15 |
|   | 2.4.2    | .2 Voraussetzungen                                      | 15 |
|   | 2.4.2    | 3.  |    |
|   | 2.4.3    | Virtual Appliance Mode                                  |    |
|   | 2.4.3    | .1 Erklärung  | 16 |
|   | 2.4.3    | .2 Voraussetzungen                                      | 16 |
|   | 2.4.3    | .3 Einschränkungen                                      | 16 |
|   | 2.4.4    | Network Mode  |    |
|   | 2.4.4    | .1 Erklärung  | 17 |
| 3 | Vergleid | ch von Datensicherungssystemen für virtuelle Umgebungen | 18 |
|   |          | führung   |    |
|   | 3.2 Anf  | orderungen an ein Datensicherungssystem für VMs         |    |
|   | 3.2.1    | Zusammenarbeit mit den Virtualisierungsprogramm         |    |
|   | 3.2.2    | Anzahl und Dauer einzelner Wiederherstellungsoptionen   |    |
|   | 3.2.3    | Wiederherstellung einzelner Anwendungsobjekte           |    |
|   | 3.2.4    | Abhängigkeit von Agenten                                |    |
|   | 3.2.5    | Unterstützte Dateiformate                               |    |
|   | 3.2.6    | Verfahren des Programms mit überschüssigen Daten        |    |
|   | 3.2.7    | Zusammenarbeit mit Drittanbieter-Software               |    |
|   | 3.2.8    | Aufwand der Einrichtung und Support                     |    |
|   | 3.2.9    | Kostenpunkt bzw. Preis-Leistungsverhältnis              |    |
|   | 3.3 Vor  | stellung der zu vergleichenden Backupsysteme            |    |
|   | 3.3.1    | Acronis Backup für VMware                               | 22 |
|   | 3.3.1    | .1 Einführung   | 22 |
|   | 3.3.1    | .2 Features   | 22 |
|   | 3.3.1    | .3 Lizenzierung (Acronis Backup für VMware)             | 23 |
|   | 3.3.2    | StorageCraft ShadowProtect 5                            | 23 |
|   | 3.3.2    | .1 Einführung   | 23 |
|   | 3.3.2    | .2 Features   | 24 |
|   | 3.3.2    | .3 Lizenzierung   | 24 |
|   | 3.3.3    | Veeam Backup & Replication v8                           | 25 |
|   | 3.3.3    | .1 Features   | 25 |
|   | 3.3.3    | .2 Lizenzierung   | 26 |
|   | 3.4 Zus  | ammenfassung  | 27 |
|   | 3.5 Faz  | it des Vergleichs                                       | 28 |
| 4 | Einricht | ung von Veeam Backup & Replication v8                   | 29 |
|   | 4.1 Hin  | zufügen der zu sichernden Server                        | 29 |
|   | 4.2 Ein  | richten des Backup-Proxys                               | 29 |

| 4.3      | Eini   | richten des Backup-Repositories                         | 31 |
|----------|--------|---|----|
| 4.4      | Eini   | richtung der Backup-Jobs                                | 32 |
| 4.5      | Eini   | richtung der Replikations-Jobs                          | 34 |
| 4.6      | Eini   | richtung von Sicherungen auf Bandlaufwerken (Tape-Jobs) | 39 |
| 4.7      | Opt    | imierung des Datenflusses                               | 40 |
| 4.8      | Eini   | richtung der "SureBackup"-Funktion                      | 41 |
| 4.8      | 3.1    | Einführung  | 41 |
| 4.8      | 3.2    | Einrichtung der "Application Group"                     | 42 |
| 4.8      | 3.3    | Einrichtung des "virtual Labs"                          | 43 |
| 4.8      | 3.4    | Einrichtung des "SureBackup"-Jobs                       | 45 |
| 4.9      | Sys    | temwiederherstellung im Katastrophenfall                | 46 |
| 4.9      | 9.1    | Manuelle Ausführung eines Replica-Failovers             | 46 |
| 4.9      | 9.2    | Vollständige Wiederherstellung eines Backups            | 46 |
| 4.9      | 9.3    | Wiederherstellung einzelner Dateien                     | 48 |
| 4.9      | 9.4    | Wiederherstellung einer Bandsicherung                   | 48 |
| 4.9      | 9.5    | Instant-VM-Recovery                                     | 49 |
| •        | 4.9.5  | .1 Ausführung einer Instant-VM-Recovery                 | 49 |
| 4.9      | 9.6    | Migration einer Instant-VM in die Produktion            | 50 |
| 5 Sc     | hluss  | wort  | 52 |
| Literatu | urverz | zeichnis  | 53 |
| Eidess   | taatli | che Erklärung   | 55 |
| These    |        |   | 56 |

# Abbildungsverzeichnis

| Abbildung 1: Vollbackup  | 3  |
|--|----|
| Abbildung 2: Differentielles Backup                              | 3  |
| Abbildung 3: (Vorwärts-)Inkrementelles Backup                    | 4  |
| Abbildung 4: Rückwärts-inkrementelles Backup                     | 5  |
| Abbildung 5: Synthetisches Vollbackup                            | 6  |
| Abbildung 6: Generationenprinzip                                 | 7  |
| Abbildung 7: IT-Struktur der BA Glauchau                         | 11 |
| Abbildung 8: Optimierung der Versandroute für Sicherungen        | 41 |
| Tabellenverzeichnis  |    |
| Tabelle 1: Vergleich von Backunsystemen für virtuelle Umgehungen | 27 |

# Abkürzungsverzeichnis

**AES** Advanced Encryption Standard

API Application Programming Interface

**BA** Berufsakademie

(k/M/G/T)B Kilo- / Mega- / Giga- / Tera-Byte

**CBT** Changed Block Tracking

**CIFS** Common Internet File System

**DAS** Direct Attached Storage

**DHCP** Dynamic Host Configuration Protocol

**DNS** Domain Name System

**DVS** Distributed virtual switch (Veeam Technologie)

**ESX(i)** Elastic Sky X (VMware Hypervisor)

**FIFO** First In, First Out

**FLIR** File Level Item Recovery (Veeam Technologie)

**FTP** File Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

I/O Input / Output

**IDE** Integrated Drive Electronics

IP Internet Protocol

(i)SCSI (internet) Small Computer System Interface

IT Informationstechnik

**LAN** Local Area Network

**LUN** Logical Unit Number

**NFS** Network File System

**OS** Operating System (Betriebssystem)

SP 2, SP 3 Service Pack 2/3

**SAN** Storage-Area-Network

**SMB, SMB3** Server Message Block (Version 3)

**SPF** Shadow Protect File

(Dateiformat für Sicherungen von ShadowProtect 5)

**SQL** Structured Query Language

**U-AIR** Universal Application Item Recovery (Veeam Technologie)

**USV** Unterbrechungsfreie Stromversorgung

**VADP** vStorage APIs for Data Protection (VMware Technologie)

VBR(v8) Veeam Backup & Replication v8

VHD(X) Virtual Hard Disk (Extended) (Dateiformat)

VM Virtuelle Maschine

**VMDK** Virtual Machine Disk

**VMFS** Virtual Machine File System

(v)NIC (virtual) Network Interface Card

VSS Volume Shadow Copy Service

**WAN** Wide Area Network

# 1 Einführung

## 1.1 Anmerkung

In dem hier vorliegenden Dokument wird der Name des Programmes "Veeam Backup & Replication v8" ggf. mit den Kürzeln "VBR", "VBRv8" oder mit "Veeam" umschrieben.

# 1.2 Projektmotivation

Nach der Umstellung einiger IT-Komponenten der Staatlichen Studienakademie Glauchau wird nun nach einer Sicherungslösung der dort vorhandenen, virtuellen IT-Infrastruktur gesucht. Diese Lösung sollte über automatisierte Sicherungs- und Wiederherstellungsoptionen verfügen, welche auf virtuelle Maschinen von VMware zugeschnitten sind. Des Weiteren soll sie ggf. die Replikation einiger systemkritischer Komponenten zum Erreichen einer gewissen Verfügbarkeit ermöglichen und steuern können.

Für den Fall eines Katastrophenszenarios soll somit ein weitgehender Verlust von Daten vermieden oder ihm zumindest entgegengewirkt werden.

In diesem Dokument wird die Situation der Berufsakademie genauer erläutert und auf die Funktionen und Handhabung der dafür installierten Sicherungs-Suite eingegangen. Des Weiteren werden Vorschläge zur Erweiterung und Optimierung der Datensicherung gebracht, sowie ein Vergleich zwischen einigen ausgewählten Backupprogrammen für virtuelle Systeme und VBR vorgenommen.

#### 1.3 Grundlagen

#### 1.3.1 Begriffe

#### 1.3.1.1 Backup

Als Backup wird eine Sonderform einer exakten Kopie eines Datenbestandes verstanden. Diese werden in der Regel für einen späteren Wiederherstellungsfall auch über längere Zeiträume hinweg gesichert und sollten entsprechend der 3-2-1-Regel erstellt werden.

Mit ihnen soll eventuellem Datenverlust im Katastrophenfall entgegengewirkt werden.

Ein Beispiel für ein Backup wäre ein gesicherter Datenbestand einer Datenbank zu einem vorherigen Zeitpunkt. Bei Ausfall der Datenbankstruktur können die Daten auf den Zeitpunkt der Erstellung des Backups zurückgesetzt werden.

#### 1.3.1.2 Replikation

Unter Replikation versteht man das Erstellen von Datenkopien, dessen Inhalt mit dem Original synchronisiert wird.

Sie dienen in der Regel zur schnelleren Bereitstellung von Ersatzdiensten und der Erreichung eines gewissen Grades der High-Availability.

Ein Beispiel hierfür wäre das Replizieren eines Servers, welcher DHCP und DNS-Dienste zur Verfügung stellt. Bei Ausfall dieses Servers, kann ein redundanter Server, auf welchem die Replikation stattfand, den synchronisierten Datenbestand des Originals nutzen, um dessen Aufgabe schnellstmöglich zu übernehmen.

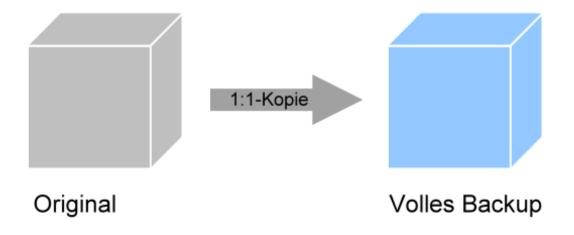
#### 1.3.2 Backupmethoden

#### 1.3.2.1 Vollbackup

Das wohl simpelste und in der Regel langsamste Verfahren zur Erstellung von Backups ist das Vollbackup. Hierbei wird eine einfache Kopie eines Datenbestandes (z.B. einer Festplattenpartition) angelegt.

Der Vorteil des Verfahrens ist einerseits seine geringe Beanspruchung von Rechenleistung während des Anlegens. Des Weiteren ist diese Art von Backup völlig autonom und benötigt kein anderes Backup zur Wiederherstellung der Daten.

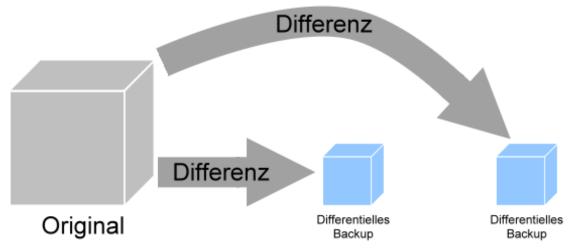
Ein großer Nachteil der Vollbackups ist jedoch der hohe Speicherbedarf, im Vergleich zu anderen Verfahren, vor allem bei Anlegen mehrerer Backups in regelmäßigen Zeitabständen.



# 1.3.2.2 Differentielles Backup

Ein differentielles Backup ist ein platzsparenderes Verfahren, welches nur die Änderungen zum zuletzt angelegten Vollbackup sichert. Daten, die zum Erstellungszeitpunkt keinen Unterschied zum letzten Vollbackup aufweisen werden somit nicht noch einmal gesichert.

Vorteil dieses Verfahrens ist der (in der Regel) geringere Speicherbedarf und Zeitaufwand bei der Erstellung von Backups, welcher jedoch auf Kosten zusätzlich benötigter Rechenleistung beim Erstellen und Wiederherstellen des Backups fällt. Als zusätzlicher Nachteil muss die Funktionalität des Vollbackups sichergestellt werden. Ist dieses als Basis fehlerbehaftet, so können ggf. nicht alle Daten wiederhergestellt werden.



**Abbildung 2: Differentielles Backup** 

#### 1.3.2.3 Vorwärts-inkrementelles Backup

Inkrementelle Backups sind eine Weiterführung des Prinzips der differentiellen Backups, in denen nicht die Änderungen zum letzten Vollbackup, sondern lediglich die Änderungen zum letzten inkrementellen Backup gesichert werden.

Dies birgt gegenüber differentiellen Backups den Vorteil, dass noch weniger Speicherplatz in Anspruch genommen wird.

Genau wie differentielle Backups, sind jedoch auch inkrementelle Backups von der Vollständigkeit und Funktionalität anderer Backups abhängig, was hier eine noch stärkere Bedeutung hat. Hierbei muss nicht nur die Integrität des letzten Vollbackups, sondern auch aller inkrementellen Backups bis zum gewünschten Zeitpunkt sichergestellt sein.

Der notwendige Aufwand beim Zurücksichern der Daten steigt hierbei mit zunehmender Anzahl inkrementeller Backups zwischen dem Vollbackup und dem gewünschten Wiederherstellungszeitpunkt an. Dies bedeutet einen höheren Aufwand beim Zurücksetzen der Daten auf einen aktuelleren Zeitpunkt, da das volle Backup um mehr inkrementelle Änderungen ergänzt werden muss.

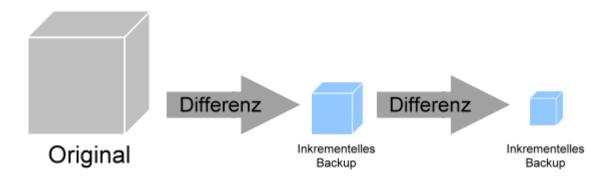


Abbildung 3: (Vorwärts-)Inkrementelles Backup

# 1.3.2.4 Rückwärts-inkrementelles Backup

Dieses Verfahren bietet eine Möglichkeit den Wiederherstellungsprozess zu beschleunigen, auf Kosten der Erstellungsdauer.

Hierbei wird nach jedem inkrementellen Backup ein synthetisch volles Backup generiert, welches für eine schnelle Wiederherstellung der aktuellsten Daten verwendet werden kann.

Im Gegensatz zu vorwärts-inkrementellen Backups steigt der Aufwand der Wiederherstellung hier an, wenn man zeitlich frühere Zustände wiederherstellt.

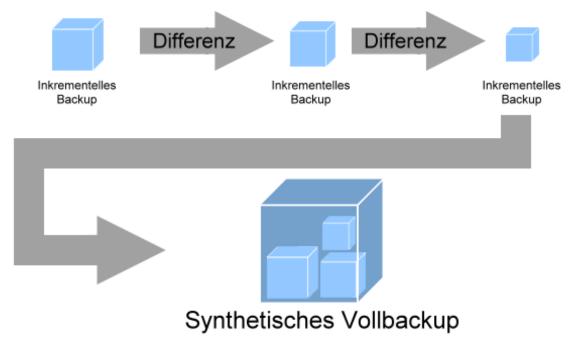


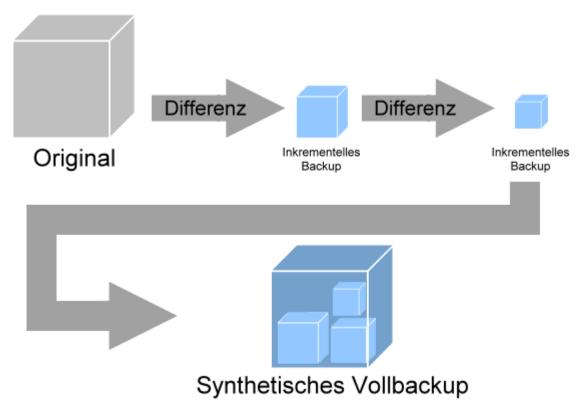
Abbildung 4: Rückwärts-inkrementelles Backup

#### 1.3.2.5 Synthetisch volles Backup

Synthetisch volle Backups unterscheiden sich vom Wiederherstellungsprozess nicht im Vergleich zu Vollbackups. Jedoch gibt es hier Unterschiede in der Erstellungsweise. Während Vollbackups direkt die Daten vom Datenträger lesen, werden synthetische Vollbackups auf Basis eines Vollbackups und darauffolgenden differentiellen oder inkrementellen Sicherungen generiert. Dabei werden die Daten des vollen Backups um die differentiellen bzw. inkrementellen Änderungen ergänzt.

Dieses Verfahren birgt den Vorteil, zum Erstellen des Backups nur das Speichermedium zu belasten, welches das Backup beherbergt, anstelle des Produktionsspeichers.

Als Nachteil besteht die Tatsache, dass sämtliche Inkremente funktionstüchtig und verfügbar sein müssen, damit das synthetische Backup ordnungsgemäß erstellt werden kann.



**Abbildung 5: Synthetisches Vollbackup** 

### 1.3.3 Prinzipien der Backuprotation

#### 1.3.3.1 FIFO

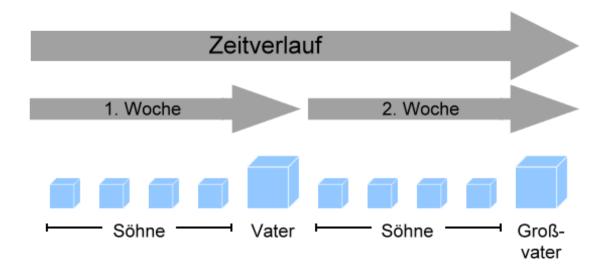
Das "First in, first out" (FIFO)-Prinzip, ist das wohl simpelste Prinzip der Backuprotationen. Hier werden jeweils die ersten (und damit ältesten) Backups gelöscht, sobald die Anzahl der zu behaltenden Sicherungspunkte überschritten wird. Die Reihenfolge der Backups wird hierbei gänzlich vom Erstellungszeitpunkt der Backups bestimmt.

#### 1.3.3.2 Generationenprinzip

Das Generationenprinzip ist ein weiteres Konzept, bei dem Backups für bestimmte Intervalle einbehalten werden. So z.B. werden täglich inkrementelle Backups angelegt, welche z.B. am Wochenende zu synthetisch vollen Backups zusammengefasst werden. Am Ende des Monats wird ein weiteres Vollbackup angelegt. Somit hat man im Verlaufe eines Monats:

- fünf inkrementelle, tägliche Backups (Backup 1. Generation, oder "Söhne")
- drei volle, wöchentliche Backups (Backup 2. Generation, oder "Väter")
- ein volles, monatliches Backup (Backup 3. Generation, oder "Großvater").

Diese Backupkette kann beliebig weiter fortgesetzt werden, z.B. mit jährlichen Backups (Backup 4. Generation, "Urgroßvater").



**Abbildung 6: Generationenprinzip** 

#### 1.3.3.3 Türme von Hanoi

Das Prinzip der "Türme von Hanoi" basiert auf dem Knobelspiel gleichen Namens. Bei diesem Spiel soll ein Stapel von Ringen, welcher der Größe nach sortiert ist, auf den letzten von drei Stäben erneut angeordnet werden sollen, ohne dass während des Prozesses ein größerer Ring auf einen kleineren abgelegt wird.

Das Prinzip dieses Spieles findet bei mehreren Gebieten der Informatik Anwendung – so auch bei Backups.

Jeder Ring des Turms stellt ein bestimmtes Speichermedium dar. Die Bewegung eines Ringes im Spiel ist hierbei analog der Auswahl des jeweiligen Speichermediums für das nächste Backup.

#### 1.3.4 Die 3-2-1-Regel

Die 3-2-1-Regel stellt eine Richtlinie zur Erstellung von sicheren Backups dar. Nach dieser Regel sollten drei Sicherungen, auf mindestens 2 verschiedenen Medien, mit einer weiteren Sicherung abseits der Produktion angelegt werden. Somit wird sichergestellt, dass zu jedem Zeitpunkt genügend Sicherungen zur Wiederherstellung zur Verfügung stehen, sollte es zu einem Katastrophenfall kommen.

### 1.3.5 Anforderungen an Backups und Replikationen

In nahezu allen Einsatzbereichen in denen die Informationstechnik Anwendung findet, werden Daten gespeichert, die bei Bedarf wiederhergestellt werden müssen. Dies betrifft z.B. insbesondere Banken, Webservices und Verkaufs- bzw. Lieferportale. In diesen Gebieten spielen Backups eine besonders wertvolle Rolle, da deren Produktion von den vorhandenen Datenbeständen abhängig ist.

Im Zuge dessen stellen sich für Backups bestimmte Anforderungen heraus, welche in den folgenden Punkten genauer erläutert werden sollen.

## 1.3.5.1 Geringer Speicherplatzbedarf

Eins der wohl wichtigsten Kriterien ist die Einnahme eines möglichst geringen Speicherplatzes pro Backup, um sicherstellen zu können, dass möglichst viele Wiederherstellungspunkte zur Verfügung stehen und ggf. eine langzeitige Archivierung der Daten ermöglicht werden kann.

Erreicht werden kann dies durch den Einsatz von Komprimierungsverfahren, De-Duplizierungsverfahren oder einer Kombination dieser. Komprimierung bedeutet hierbei lediglich die Um-Kodierung der Daten in ein kompakteres Format auf Kosten des Erstellungs- und Wiederherstellungsaufwandes. De-Duplizierung hingegen ist die Vermeidung der erneuten Sicherung von Daten, welche bereits zur Wiederherstellung verfügbar sind, um eine übermäßige Redundanz von Daten zu verhindern.

Eine weitere Möglichkeit bietet der Einsatz gewisser platzsparender Verfahren, wie z.B. differentielle und inkrementelle Backups. In Zusammenhang damit kann auch der gezielte Einsatz von Backup-Rotationsverfahren wie dem Generationenprinzip dazu beitragen, dass über größere Zeiträume hinweg mehr Speicherplatz zur Verfügung steht.

# 1.3.5.2 Schnelles und sicheres Anlegen/Zurückspielen von Backups

Für sämtliche Firmen ist es von größter Bedeutung, in Extremfällen, vorhandene Sicherung schnellstmöglich wiederherstellen zu können, sodass der Betrieb mit minimaler Auszeit wiederaufgenommen werden kann und entstandene finanzielle Verluste minimiert werden können.

Doch auch der Sicherungsprozess sollte schnell vollendet sein, damit die zu sichernden Daten zur Wiederherstellung verfügbar sind und die zur Sicherung genutzten Ressourcen wieder frei gegeben werden können.

Für eine schnelle Sicherung können Komprimierungsverfahren eingesetzt werden, um den Datentransfer über das Netzwerk zu beschleunigen. Die Paketheader sollten ebenfalls möglichst klein sein, um auf Dauer das Netzwerk nicht unnötig stark zu belasten.

Des Weiteren sollte die Möglichkeit geboten werden, Sicherungen nicht nur auf ein Speichermedium anlegen zu können, welches über ein Netzwerk angebunden ist, sondern ebenfalls direkt angeschlossene Medien zu unterstützen. Somit entfällt der

Versand von Sicherungsdaten über das Netzwerk (und die damit verbundene Erstellung von Netzwerkpaketen).

All diese Punkte, auch wenn von äußerst hoher Priorität, verlieren jedoch sämtliche Bedeutung, wenn diese aufgrund eines fehlerhaften Backups nicht wiederhergestellt werden können. Aufgrund dessen sollte es, wenn möglich ohne unnötige Belastung der Produktionsmaschinen, möglich sein, angelegte Datensicherungen auf Funktionalität und Integrität zu überprüfen. Vor allem bei virtuellen Maschinen bedeutet dies nicht nur die Überprüfung der Backup-Datei über eine Checksumme oder ähnlichem, sondern ebenfalls die Funktionalität der Maschine an sich, da es (vor allem bei großen Datenmengen) zu Fehlern kommen kann, bei denen ein fehlerhafter Datenbestand dennoch zufälligerweise die korrekte Checksumme generiert.

## 1.3.5.3 Sicherung auf externe Standorte

Um der 3-2-1-Regel gerecht werden zu können, sollten sich Backups ebenfalls auf externe Standorte sichern lassen können.

Hierzu ist die Unterstützung des Datenversandes über das WAN von Nöten, sowie die Implementierung von Komprimierungs- und De-Duplizierungsverfahren, um die Transferdauer zu minimieren.

# 1.3.6 Veeam Backup & Replication

#### 1.3.6.1 Einführung

"Veeam Backup & Replication v8" ist eine speziell für virtuelle Maschinen konzipierte Backuplösung und wurde von Veeam Software entwickelt.

Sie verfügt über zahlreiche Features zur Sicherung, Wiederherstellung und Replikation virtueller Maschinen auf Basis von VMware oder Hyper-V.

Des Weiteren verfügt das Programm über eine virtuelle Umgebung, in der angelegte Sicherungen auf ihre Funktionalität überprüft werden können.

Auf die vorhandenen Features sowie das Lizenzmodell wird im Punkt "Vorstellung der zu vergleichenden Backupprogramme" detaillierter eingegangen.

#### 1.3.6.2 Architektur des Programms

Veeams Backuplösung lässt sich in drei hauptsächliche Komponenten zerlegen, welche jeweils über unterschiedliche Aufgabenbereiche verfügen.

Das Backup-Repository ist der Speicherort der Backups und der Replikationen. Er beinhaltet, neben den gesicherten Daten auch weitere Metadaten über diese und deren VM. Diese Daten werden z.B. seitens des Backup-Proxys zur De-Duplizierung genutzt, indem festgestellt wird, ob sich eine zu sichernde Datei bereits auf dem Repository befindet und daher kein weiteres Mal gesendet werden muss.

Der Backup-Proxy ist eine Hilfsinstanz, welche die Daten der zu sichernden VM auf ein festgelegtes Repository weiterleitet. Dabei kümmert sich der Proxy ebenfalls um die Komprimierung der Daten und deren De-Duplizierung, im Falle einer Datensicherung über das WAN. Er kann für höhere Effizienz auch auf einer dedizierten, physischen Maschine installiert werden.

Dies ist stets dann von Interesse, wenn auf dem Veeam-Server selbst nur geringfügige Ressourcen zur Verfügung stehen oder auf eine starke Komprimierung zurückgegriffen wird und der Backupprozess möglichst schnell vollendet werden soll.

Der Veeam-Server, welcher die zu verwendende Nutzeroberfläche zur Erstellung und Wiederherstellung von Backups darstellt, ist ebenfalls die Komponente, welche die angelegten Jobs verwaltet und nach angelegten Zeitplan startet. Er verknüpft dabei den Backup-Proxy mit dem Backup-Repository, indem dieser dem Backup-Proxy einen Zielspeicher beim Anlegen und Wiederherstellen von Backups übermittelt. Mit ihm können u.a. auch Server hinzugefügt und administriert, sowie Zugangsdaten verwaltet und Copy-Jobs angelegt werden.

# 2 Vorbetrachtungen

#### 2.1 Situation an der BA Glauchau

#### 2.1.1 IT-Struktur der BA Glauchau

Die staatliche Berufsakademie Glauchau verfügt über mehrere physische Server mit mehreren virtuellen Maschinen. Die für die Sicherung relevanten Komponenten sind auf drei Räumlichkeiten verteilt:

In Raum 316, dem Serverraum, befindet sich der Veeam Backup-Server samt Backup-Proxy und einigen virtuellen, jedoch nicht produktiven, virtuellen Maschinen. Der hier installierte Veeam-Server ist zuständig für das Management und die Konfiguration der Backup- und Replikations-Jobs, sowie der SureBackup-Funktion.

Der Keller des Laborgebäudes beinhaltet zwei Blade-Center mit mehreren, virtuellen Produktionsmaschinen.

Zwischen dem Serverraum und dem Laborgebäude existieren zwei Speichersysteme, welche über eine Hardware-seitige, synchrone Spiegelung gespiegelt werden.

Das Storage-System mit einem Bandlaufwerk, welches das Backup-Repository des VBR-Systems darstellt, befindet sich im Raum 307 des Hauptgebäudes.

Sämtliche Komponenten sind über 8 Gigabit Fibre-Channel-Verbindungen verknüpft.

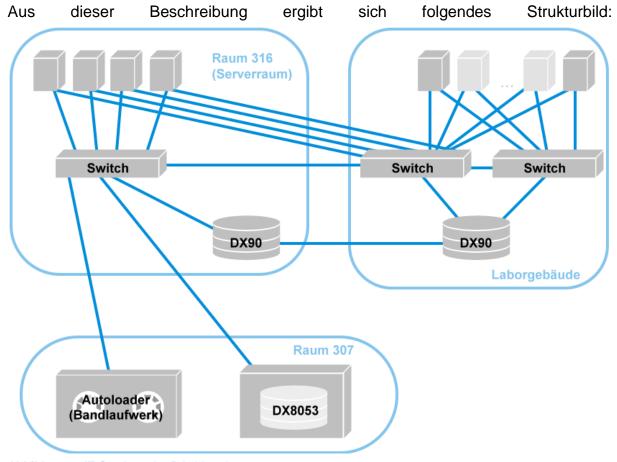


Abbildung 7: IT-Struktur der BA Glauchau

# 2.2 Fibre-Channel als Übertragungsmedium

In der BA Glauchau wurde anstatt anderer Verbindungsarten, wie iSCSI, Fibre-Channel (FC) gewählt, um die Übertragung der Daten zwischen den Komponenten zu beschleunigen.

Dies hat bestimmte Gründe, die auf der Funktionsweise von Fibre-Channel beruhen.

Das gewählte Übertragungsmedium dieser Technologie ist, wie der Name bereits sagt, Glasfaser. Über die Glasfasern werden nun statt elektrischer Signale Lichtsignale versendet. Diese sind nicht nur wesentlich schneller, sondern auch resistent gegen elektromagnetische Einflüsse, welche sich in Kupferadern zumeist in Form von Crosstalk (Übersprechen) als Störungen bemerkbar machen.

Mit der neuen Übertragungstechnologie folgt ebenfalls ein erneuerter Protokollstack. Dieser besteht aus fünf Schichten und ist damit im Vergleich zum Stack des Ethernets kleiner, womit weniger Verarbeitungsschritte pro Versand durchgeführt werden müssen.

Da das Protokoll von Fibre Channel sehr flexibel ist, unterstützt es auch den Versand von SCSI-Paketen, womit es die Anbindung eines Storage-Systems über Glasfaser ermöglicht.

Diese Eigenschaft wird an der BA Glauchau ausgenutzt um einen schnelleren Transfer der Sicherungsdaten über Glasfaser auf das Speichersystem zu bewerkstelligen.

# 2.3 Erstellung eines Konzeptes zur Realisierung der Datensicherungen

# 2.3.1 Vorüberlegungen

Auf Basis der Anforderungen an Backup (siehe 1.3.5.) soll im Folgenden ein Konzept erstellt werden, wie die Datensicherungen und Replikationen an der Berufsakademie in Glauchau auszuführen sind.

Wichtig in sämtlichen Backupprozessen ist es, den laufenden Betrieb nicht zu behindern bzw. gar anzuhalten. Die Zeitpläne für Backups und Replikationen, sowie der hier zu implementierenden SureBackup-Funktion sind also so zu legen, dass sie möglichst außerhalb der Nutzungszeiten liegen.

In der Regel finden keine weiteren Vorlesungen nach 18:00 Uhr mehr statt. Auch die Bibliothek hat dabei geschlossen und der Großteil des Personals ist außer Haus. Eine Ausnahme hierfür bilden die Bewohner des Wohnheims, welche das Gelände annahmeweise, jedoch nicht zwingenderweise, erst am Wochenende kurzfristig verlassen.

Ein weiterer Punkt ist die Zeitplanung bezüglich mehrerer Jobs. Um sich bei der Sicherung nicht gegenseitig zu behindern, sollte den einzelnen Maschinen ein Zeitfenster gegeben werden, in den jeweils keine andere Sicherung stattfindet.

Da bei dieser Konstellation Server in verschiedene Prioritätsklassen aufgeteilt werden können, kommt ein weiterer, wichtiger Gedanke zum Tragen: die Reihenfolge der Sicherungen. Um die negativen Auswirkungen eines eventuellen Datenverlustes so weit wie möglich zu minimieren, sollte sichergestellt werden, dass die Server, ihrer Priorität nach absteigend, gesichert werden. Des Weiteren sollte darauf geachtet werden, dass während der Backups die zur Verfügung gestellten Ressourcen optimal ausgenutzt werden.

So z.B. könnten mehrere Jobs gleichzeitig ausgeführt werden, sollten nicht alle Ressourcen ausgelastet sein. Hierbei ist jedoch auch die obere Grenze der Optimierung zu beachten: Werden letztendlich mehr Ressourcen benötigt als zur Verfügung stehen, wird das System "überlastet". Die kann dazu führen, dass mehrere Jobs mehr Zeit zur Fertigstellung in Anspruch nehmen als sonst. Bei einem Ausfall des Systems während der (verlängerten) Sicherungszeit kann es dadurch zu größeren Verlusten kommen, als bei einzelnen Sicherungen.

Um die 3-2-1-Regel erfüllen zu können, sollten zusätzliche Sicherungen auf Band vorgenommen werden. Dies wird hier durch den Autoloader im Raum 307 ermöglicht. Eine Sicherung über WAN auf einen externen Standort bzw. einen zur Verfügung gestellten Cloud-Speicher kann jedoch wahrscheinlich nicht erfolgen. Dazu müsste eine externe Speicherquelle, abseits der BA, zur Verfügung stehen oder ein Cloud-Speicher reserviert werden, welcher unter Umständen zu viel finanzielle Mittel beansprucht. Daher wird eine solche Sicherung wahrscheinlich ausgelassen. Da jedoch ein Verlust der Daten den eigentlichen Betrieb der Berufsakademie nicht zu einem völligen Stillstand führen würde, ist dies im vorliegenden Fall ggf. noch verantwortbar.

Das Generationenprinzip lässt sich mit der hier installierten Software ebenfalls erfüllen. Dabei können zu den täglich inkrementellen Sicherungen wichtiger Maschinen eine wöchentliche volle Sicherung vorgenommen werden, ggf. mit einer zusätzlichen, monatlichen Sicherung auf z.B. Band.

#### 2.3.2 Erstellung des Zeitplanes für die Anlegung der Backups

Für die Berufsakademie in Glauchau sollten die wichtigsten Server täglich inkrementell gesichert werden. Dafür eignet sich der Startzeitpunkt ab 20:00, nach dem das Gebäude verlassen sein sollte. Zu empfehlen ist hierbei eine parallele Sicherung der Maschinen, sodass die Ressourcen optimal für die Datensicherungsjobs genutzt

werden können. Wie viele Maschinen dabei parallel verarbeitet werden sollten, kann über die Aufnahme der benötigten Ressourcen während eines einzelnen Jobs geschehen. Anhand der Werte lässt sich dann ableiten, wie viele weitere VMs gesichert werden können, ohne die physikalische Maschine oder das Netzwerk zu überlasten, wenn überhaupt.

Am Ende der Woche, z.B. an Freitagen oder Samstagen, sollte anschließend jeweils ein synthetisch volles Backup durchgeführt werden. Hierbei kann zusätzlich jedes synthetisch volle Backup am letzten Wochenende eines jeden Monats auf Band gesichert werden. Damit würde es ein Backup 3. Generation darstellen und somit das Generationenprinzip erfüllen.

Weniger priorisierte Maschinen sollten lediglich wöchentlich gesichert werden. Dabei reicht eine einfache volle Sicherung aus. Sollte der Speicherplatz begrenzt sein, kann ggf. auf eine differentielle Sicherung mit regelmäßiger, erneuter Vollsicherung nach einem größeren Zeitraum ausgewichen werden.

Diese Sicherung könnten beiderseits auf Samstage und Sonntage verteilt werden. Aufgrund der geringeren Priorität der Daten ist hier die Erfüllung des Generationenprinzips bis zur 3. Generation jedoch nicht notwendig.

Gibt es unter Umständen VMs, deren Inhalt nahezu nie genutzt oder geändert wird, so reicht es diese manuell, bei Bedarf zu sichern. Selbst ein automatischer Job würde in einigen Fällen kaum neue Änderungen, wenn überhaupt sichern, womit sich der Aufwand kaum lohnt.

#### 2.3.3 Möglichkeiten zur Implementierung einer Replikation

Da "Veeam Backup & Replication" Mechanismen zur Replikation anbietet, sollten mögliche Umstände in Betracht gezogen werden, bei welchen die Implementierung dieser Johnenswert erscheint.

Da der Sinn der Replikation in einem schnellen Ersatz eines Servers liegt, sollte sie für Maschinen eingesetzt werden, deren Betrieb für die interne Organisation wichtig ist und auf die regelmäßig und häufig zugegriffen wird. Beispiele hierfür wären Datenbanken, welche zur Anmeldung z.B. am FTP-Server benötigt werden.

Da es im Laborgebäude noch einige freie ESX(i)-Hosts gibt, lassen sich diese zum Aufsetzen der Replikation nutzen.

Die genaue Vorgehensweise für eine mögliche Implementierung solch einer Replikation wird im Punkt 4.5. genauer erklärt.

# 2.4 Auswahl des Transportmodus für VBR

#### 2.4.1 Einführung

Der Transportmodus bestimmt über die Methodik, wie die Daten der einzelnen VMs auf das Repository geladen werden. Die Auswahl des richtigen Transportmodus ist von der Netzwerkstruktur des Sicherungssystems abhängig und bestimmt über die Effizienz und Geschwindigkeit der Backup-Jobs.

Veeam bietet hierfür entsprechend drei Transportmodi an:

- Direct SAN Access Mode
- Virtual Appliance Mode
- Network Mode

Diese Modi nutzen allesamt "VMware vStorage APIs for Data Protection" (VADP) und verfügen, je nach Szenario, über spezielle Vor- und Nachteile.

#### 2.4.2 Direct SAN Access Mode

#### 2.4.2.1 Erklärung

Dieser Modus eignet sich besonders für virtuelle Maschinen, dessen Speicher sich auf VMFS SAN LUNs befinden, welche direkt über Fibre Channel oder iSCSI mit dem jeweiligen ESX(i)-Host verbunden ist.

In diesem Modus wird VADP verwendet, um die Daten über Fibre Channel oder iSCSI über das SAN zu übertragen. Dabei werden der ESX(i)-Host und das lokale Netzwerk (LAN) umgangen, womit keine weitere Last auf den Host gelegt wird. Das macht diese Methode zur schnellsten der drei Varianten.

#### 2.4.2.2 Voraussetzungen

Damit diese Methode anwendbar ist, muss der Backup-Proxy direkten Zugriff auf den Produktionsspeicher haben, entweder über einen Hardware- oder einen Softwareadapter. Des Weiteren muss die SAN-Verbindung konfiguriert sein. Trifft eine oder beide Bedingungen nicht zu, so scheitert der Transport über diesen Modus.

#### 2.4.2.3 Einschränkungen

Diese Methode kann nicht bei virtuellen Maschinen eingesetzt werden, welche auf einem virtuellen SAN residieren. Hierfür muss eine der anderen beiden Methoden gewählt werden. Auch kann sie nicht eingesetzt werden, wenn mindestens eine Festplatte der VM ein virtuelles Volume ist.

Bei Replikationen funktioniert dieser Job nur beim Erstdurchlauf. Für alle darauf folgenden Durchläufe wird automatisch der Virtual Appliance oder der Netzwerkmodus verwendet.

Bei Wiederherstellungen allgemein funktioniert dieser Modus nur bei thick disks und kann aufgrund von Limitierungen seitens VMware nicht für inkrementelle Wiederherstellungen genutzt werden.

Auch wenn dieser Modus für die BA Glauchau am geeignetsten wäre, so gibt es noch einige Fragen zu klären, in Bezug auf die virtuellen Maschinen, um wirklich sicherstellen zu können, dass dieser Modus geeignet wird. Bis dahin sollte der Netzwerk-Modus verwendet werden (siehe 2.4.4.).

#### 2.4.3 Virtual Appliance Mode

#### 2.4.3.1 Erklärung

Wurde der Backup-Proxy einer virtuellen Maschine zugewiesen, so wird der Virtual Appliance Modus empfohlen.

Hierbei nutzt Veeam die HotAdd-Funktion von VMware, um die Speicher während des Betriebs der VM über SCSI zu verbinden. Somit werden Daten direkt von und auf den Speicher gelesen bzw. beschrieben, ohne dabei das Netzwerk zu belasten.

#### 2.4.3.2 Voraussetzungen

Für den Einsatz dieser Methode muss der Backup-Proxy auf einer virtuellen Maschine installiert sein. Des Weiteren muss der Proxy Zugriff auf das Dateisystem des Hosts haben, um die zu verwaltenden virtuellen Maschinen auslesen zu können. Auch müssen sowohl der Proxy, als auch der Veeam Server über die neuste Version der VMware Tools verfügen.

# 2.4.3.3 Einschränkungen

Die maximale Festplattengröße darf bei vSphere-Umgebungen der Version 5.1 und kleiner eine Größe von 1,98 TB nicht überschreiten. Bei der Nutzung von VMFS 3 Datastores muss die Blockgröße auf 1, 2, 4 oder 8 MB festgelegt werden, damit größere Platten gemounted werden können.

Zu guter Letzt wird das Sichern und Wiederherstellen von IDE Festplatten in diesem Modus gar nicht und für SATA-Festplatten nur ab vSphere Version 6 unterstützt.

#### 2.4.4 Network Mode

# 2.4.4.1 Erklärung

Der Netzwerk-Modus wird im Allgemeinen nicht empfohlen. Da der Datentransfer über das LAN stattfindet, belastet er nicht nur das Netzwerk, sondern ist somit auch verhältnismäßig langsam. Er wird, in der Regel nur als Rückfall-Methode verwendet oder wenn keine andere Methode anwendbar ist.

Dieser Modus hat jedoch den Vorteil, dass er in jeder Konfiguration eingesetzt werden kann und außer einer funktionsfähigen Netzwerkverbindung keine weiteren Voraussetzungen getroffen werden müssen.

# 3 Vergleich von Datensicherungssystemen für virtuelle Umgebungen

## 3.1 Einführung

Viele Firmen bieten bereits Backup-Programme an, welche nicht nur physikalische, sondern auch virtuelle Systeme unterstützen. Eine Auswahl dieser Programme soll nun zusammen mit "Veeam Backup & Replication v8" getestet werden.

Ziel der Tests ist es:

- herauszufinden ob Veeam tatsächlich der Konkurrenz überlegen ist
- herauszufinden ob ein zukünftiges Umschwenken auf ein anderes Produkt angebracht wäre
- eine grobe Übersicht über verfügbare Backupprogramme und deren Fähigkeiten zu schaffen

Um dieses Ziel zu erreichen werden die Programme auf folgende Punkte verglichen:

- Funktionsumfang des Programmes, einschließlich Backup- und Wiederherstellungsoptionen
- Unterstützte Gast-Betriebssysteme und virtuelle Umgebungen
- Erfüllung der 3-2-1-Regel und des Generationenprinzips
- Preis-/Leistungsumfang bzw. Lizenzierung
- Erfüllung weiterer Anforderungen für die BA Glauchau

# 3.2 Anforderungen an ein Datensicherungssystem für VMs

Bevor sich für ein bestimmtes Datensicherungsprodukt entschieden werden kann, sollten gewisse Anforderungen bestimmt und die zur Auswahl zur Verfügung stehenden Programme daraufhin geprüft werden. Diese Anforderungen beziehen sich im Allgemeinen auf die Thematiken Sicherheit, Kompatibilität und Features. Somit soll abgewogen werden können, wie effizient sich Desaster mit dem jeweiligen Programm bewältigen lassen.

Als Richtlinie sollte man sich hierfür folgenden Punkten bewusst werden:

#### 3.2.1 Zusammenarbeit mit den Virtualisierungsprogramm

Hierbei soll geklärt werden, inwiefern das Sicherungsprogramm auf die Fähigkeiten des genutzten Hypervisors zurückgreift. So z.B. sollten die Sicherungsprogramme in der Lage sein die angelegten VMs zu erkennen, deren virtuelle Festplatten zu beschreiben, und sie für die Dauer eines Sicherungsprozesses stillzulegen.

# 3.2.2 Anzahl und Dauer einzelner Wiederherstellungsoptionen

Eine der wichtigsten Fragen, welche zu beantworten wäre, betrifft die Optionen für Sicherung und Wiederherstellung sowie deren Dauer.

Das Programm sollte in der Lage sein, alle gängigen Backupverfahren (voll, inkrementell, differentiell) zu unterstützen und des Weiteren Möglichkeiten bieten um gewisse Prinzipien, wie die 3-2-1-Regel oder das Generationenprinzip, umzusetzen.

Auch ist es von großem Nutzen, wenn gewisse Features, wie z.B. Veeams "Instant-VM-Recovery" existieren, welche es in Notsituationen erlauben, Ersatzserver besonders schnell aus Backups zur Verfügung zu stellen.

#### 3.2.3 Wiederherstellung einzelner Anwendungsobjekte

Um den Wiederherstellungsprozess einzelner Datenobjekte zu beschleunigen und zu vereinfachen, sollten ebenfalls Funktionen bereitgestellt werden um das Rücksichern einzelner Datenbankobjekte (z.B. Microsoft Exchange), insbesondere aber einzelner Dateien zu ermöglichen. Solche Funktionalitäten können den gesamten Wiederherstellungsprozess beschleunigen, da nicht das gesamte Backup, sondern nur gewisse Teile dessen zurückgeschrieben werden.

Ein weiteres, nützliches Feature wäre die sofortige Wiederherstellung einer ausgefallenen VM entweder über Replikation oder einem angelegten Backup. Dies gewährleistet eine minimale Auszeit des Systems.

### 3.2.4 Abhängigkeit von Agenten

In vielen Sicherungssystemen werden Agenten verwendet, um den Datentransfer- und Austausch zwischen den Server und den virtuellen Maschinen zu gewährleisten. Diese müssen jedoch möglicherweise auf jeder zu sichernden VM installiert und gepflegt werden, was den administrativen Aufwand erheblich erhöhen kann.

Es ist daher wichtig, sich darüber zu informieren, ob (und wenn ja, wie viele) Agenten für den ordnungsgemäßen Betrieb des Systems benötigt werden.

#### 3.2.5 Unterstützte Dateiformate

Die unterstützten Dateiformate eines Datensicherungssystems spielen vor allem in Katastrophenfällen eine bedeutende Rolle. Wenn das interne IT-System ausfällt, muss sichergestellt sein, dass das Dateiformat der Sicherung von dem zur Wiederherstellung des Backups zur Verfügung stehenden Backupsystem eingelesen werden kann. Alternativ würde es ebenfalls ausreichen, wenn die Verfügbarkeit und

Funktionalität desselben Programms garantiert werden kann, welches das zu rücksichernde Programm erstellt hatte.

Es gibt einige offene Formate, wie z.B. VMDK oder VHD, welche für das Sichern und Rücksichern verwendet werden können. Diese Formate können von verschiedenen Programmen eingelesen werden und erlauben damit auch eine Wiederherstellung des Systems über ein anderes Sicherungssystem, im Falle, dass das ursprünglich genutzte System ebenfalls nicht verfügbar ist (da es z.B. im selben Katastrophenfall ebenfalls beschädigt wurde), oder bereits auf ein anderes System gewechselt wurde.

Programmspezifische Formate binden ihre Kunden an den jeweiligen Hersteller bzw. das jeweilige Produkt und erschweren den Umstieg auf ein anderes System somit erheblich, da ansonsten die alten Backupformate u.U. nicht mehr eingelesen werden können.

#### 3.2.6 Verfahren des Programms mit überschüssigen Daten

Als überschüssige Daten auf einer VM kann man solche beschreiben, bei denen mit hoher Wahrscheinlichkeit davon ausgegangen werden kann, dass diese für den Betrieb nicht benötigt werden. Solche Daten sind z.B. abgelaufene Gast-Dateisysteme, exakte Kopien anderer Datenbestände oder übermäßig groß zugewiesener Speicher.

Diese braucht das Sicherungssystem nicht zu sichern und kann somit Platz einsparen. Das Backupsystem muss also in der Lage sein, solch überflüssige Bestände zu erkennen und zu filtern, sowie den sonst eingenommenen Speicherplatz unnötiger Duplikate z.B. über De-Duplizierungsmechanismen, einzugrenzen.

#### 3.2.7 Zusammenarbeit mit Drittanbieter-Software

Auch wenn nicht unbedingt notwendig für den eigentlichen Betrieb, kann sich die Kompatibilität der Backuplösung mit Programmen von Drittanbietern als sehr nützlich erweisen.

Durch z.B. das zur Verfügung stellen von Schnittstellen seitens des Sicherungssystems können Anwendungen zum Einsatz gebracht werden, welche die Funktionen des Systems verbessern oder erweitern können. So könnten z.B. ältere Backup-Systeme mit dem Neuen verknüpft werden, um diese in den Gesamt-Sicherungsprozess einbinden zu können oder auch stärker spezialisierte Programme zur De-Duplizierung, Komprimierung oder Überwachung des Storage-Systems zu Einsatz gebracht werden.

#### 3.2.8 Aufwand der Einrichtung und Support

Um den administrativen Aufwand möglichst gering zu halten, sollten die Prozesse zur Erstellung und Bearbeitung von Backup- und Replikationsjobs genauer erforscht werden. So können z.B. die Integration und die Pflege von Agenten den Managementaufwand erheblich steigern. Auch kann ein unnötig umständlicher oder zeitaufwändiger Prozess zur Erstellung von Jobs oder der Konfiguration anderer Funktionen unnötig viel Zeit in Anspruch nehmen.

Eventuell verfügbare Funktionen, wie das Definieren von Job-Vorlagen oder ein simpler, konsistenter Aufbau der Menüs für das Jobmanagement können dem entgegenwirken.

#### 3.2.9 Kostenpunkt bzw. Preis-Leistungsverhältnis

Für die meisten Firmen, insbesondere für Privatunternehmen oder Unternehmen im mittelständischen Bereich, spielt der Kostenpunkt der Lösung eine bedeutende Rolle, da hierbei zumeist für die Beschaffung eines Backupsystems nur ein kleines Budget zur Verfügung gestellt wird. Diese Kosten setzen sich dabei aus mehreren Teilkosten zusammen.

Das Lizenzierungsmodell der Lösung steht hierbei meist mit im Vordergrund. Dieses Modell kann z.B. über eine zeitliche Gültigkeit des Programmes oder eine Beschränkung der erlaubten Anzahl an Installationen und Anwendungen entscheiden. Neben den verschiedenen Lizenzierungsansätzen können wiederrum auch verschiedene Editionen des Programms zur Verfügung stehen, welche dann z.B. über die folgenden Punkte bestimmen könnten:

- Auf wie vielen weiteren Servern (im Vergleich zu anderen Editionen), darf das Programm installiert werden?
- Wie viele virtuelle Maschinen dürfen (im Vergleich zu anderen Editionen) hiermit gesichert bzw. verwaltet werden?
- Über welche weiteren Funktionen verfügt die Edition?
- Welche Klasse von Support und welche Garantien stehen dem Nutzer zur Verfügung?

Neben der Lizenz müssen jedoch auch, vor allem bei der erstmaligen Einführung einer Backuplösung, Kosten für die Anschaffung, Installation und Wartung neuer, benötigter Hardware in Betracht gezogen werden.

Diese Kosten könnten u.a. durch folgende Punkte entstehen:

- Kauf eines dedizierten Servers f
   ür das Backupprogramm
- Kauf von weiteren Speichermedien, wie Festplatten oder Bandmedien
- Kauf eines Autoloaders f
   ür Bandmedien
- Ständiger Nachkauf neuer Speichermedien für fortführende Archivierung

- Wartungskosten f
  ür die neue Hardware
- ggf. Beschaffung weiteren Zubehörs wie z.B. einer USV
- Langzeitkosten für den laufenden Support

Diese Punkte sind nicht für alle IT-Systeme von Nöten und variieren in ihrem Umfang, abhängig von den jeweiligen Anforderungen. Auch können ggf. noch weitere Kostenpunkte aufgrund spezieller Anforderungen seitens des zu verwendenden Sicherungssystems oder seitens der Wünsche des Kunden entstehen.

# 3.3 Vorstellung der zu vergleichenden Backupsysteme

# 3.3.1 Acronis Backup für VMware

# 3.3.1.1 Einführung

"Acronis Backup for VMware" ist die Antwort der Acronis International GmbH, wenn es um Sicherungen von VMware-basierten, virtuellen Infrastrukturen geht. Neben dieser, existieren jedoch auch weitere Angebote welche jeweils Unterstützung für Hyper-V, Citrix XenServer, Red Hat Enterprise Virtualization und Oracle VMs bieten.

#### *3.3.1.2 Features*

Diese Softwarelösung ist direkt in VMware integriert und setzt für die Installation ein Windows-Betriebssystem der Version XP (mit SP 3 auf x86- bzw. SP2 auf x64-Archtiektur) oder höher voraus. Für die Unterstützung von Linux-Systemen wird eine separate Lösung angeboten.

Die Software arbeitet größtenteils agentenlos. Lediglich bei der Installation der Software auf eine physikalische Maschine wird ein Agent benötigt.

Zur Erstellung von Backups unterstützt Acronis Backup for VMware sämtliche, gängige Methoden. Somit lassen sich volle, differentielle, inkrementelle und synthetisch volle Backups erstellen. Des Weiteren bietet die Lösung alle notwendigen Mittel zur Realisierung des FIFO- und des Generationenprinzips an.

Zur Erfüllung der 3-2-1-Regel stellt Acronis die Möglichkeit zur Verfügung, die Daten (gegen Aufpreis) in die Cloud zu sichern.

Bei der Anlegung von Backup-Jobs bietet Acronis vielerlei erweiterte Konfigurationsmöglichkeiten an. So lassen sich Backups komprimieren, verschlüsseln (AES mit 128, 192 oder 256Bit Tiefe) oder mit Passwort schützen. Um inkrementelle Backupvorgänge zu beschleunigen, lässt sich Changed Block Tracking aktivieren. Zur Beschleunigung des Datentransfers stehen De-Duplizierungsmechanismen zur Verfügung. Zu guter Letzt lassen sich automatische Benachrichtigungen an die

Administratoren bei Fertigstellung eines Jobs versenden. Es wird sogar die Möglichkeit geboten, nach dem ersten Backup automatisch einen Backup-Recovery-Plan an alle Mitarbeiter zu verteilen.

Replikationen werden ebenfalls unterstützt und weisen einige, bereits in Backup-Jobs vorhandene Funktionen, wie die automatischen Benachrichtigungen oder das CBT auf. Damit der Betrieb bei Ausfall des Originals schnell wieder aufgenommen werden kann, verfügt die Software über die Möglichkeit des Failover- (Übernahme der Dienste durch eine replizierte VM) und Failback-Managements (Wiederherstellung der Original-VM durch das Replikat).

Wiederherstellungen stellen ebenfalls eine große Stärke des Programms dar.

Neben ganzer VMs und einzelner Dateien lassen sich ebenfalls Microsoft SQL Datenbanken auf Laufwerksebene zurücksichern. Selbst die Extraktion einzelner Microsoft Exchange Objekte und Postfächer (sowie individuelle Einträge oder Datenbanken) sind möglich. Die Wiederherstellung von SharePoint Server-Daten wird ebenfalls unterstützt.

Sollte eine schwerwiegende Katastrophe stattfinden, lassen sich auch virtuelle Maschinen, direkt aus den Backups heraus starten und als Ersatz betreiben.

Durch die Möglichkeit die Konfiguration des ESXi-Hosts zu sichern, stellt eine Bare-Metal-Recovery ebenfalls keine Herausforderung dar.

#### 3.3.1.3 Lizenzierung (Acronis Backup für VMware)

Eine Lizenz der Software gilt für einen zeitlich unbegrenzten Raum und wird pro Prozessor (auf dem physischen Host) mit unbegrenzter Anzahl an VMs 369€ verrechnet. Für die Speicherung auf die Cloud bietet Acronis, in 500 GB-Schritten, bis zu 3 TB Cloud-Speicher von 499€ bis maximal 1849€ an.

### 3.3.2 StorageCraft ShadowProtect 5

### 3.3.2.1 Einführung

ShadowProtect 5 ist eine der Backuplösungen des Hauses StorageCraft. Es unterstützt, genau wie die Programme von Acronis, VMware, Hyper-V, Red Hat Enterprise Virtualization, Citrix Xen-Server und virtuelle Maschinen von Oracle.

Zur Installation setzt es Windows ab der Version 2000 voraus und es bietet die Möglichkeit, das Programm auch über Remote-Zugriff (z.B. vom Smartphone aus) zu steuern.

#### 3.3.2.2 Features

Es lassen sich hier volle, differentielle, inkrementelle und durch die Zusammenführung von Images, synthetisch volle Backups erstellen. Diese können manuell oder per Zeitplan erstellt werden.

Eine automatische Benachrichtigung über E-Mail lässt sich bei Bedarf ebenfalls einrichten.

Im Unterschied zu den anderen Kandidaten stellt ShadowProtect 5 nur Sicherungen der Volumes als Sektor-für-Sektor-Kopien her. Somit lässt sich nicht eine gesamte virtuelle Maschine, sondern nur dessen Festplatteninhalt sichern.

Die gesicherten Dateien lassen sich mit einem Image-Konvertierungs-Tool in verschiedene Formate als SPF-, VHD-, VHDX-, VMDK-Datei umwandeln. Somit kann die Sicherung ggf. auch auf anderen Plattformen wiederhergestellt werden.

Die Wiederherstellung erfolgt somit auf Dateiebene. Dazu bietet ShadowProtect einen Manager zum mounten der Sicherung an. Das Volume wird hierbei als gewöhnliches System-Volume angezeigt. Somit kann manuell dessen Inhalt durchsucht und der gewünschte Inhalt zurückgeholt werden.

Für die direkte Wiederherstellung einer Maschine aus einem Backup steht die Funktion "VirtualBoot" zur Verfügung. Für diese Funktion wird VirtualBox von Oracle verwendet, um die virtuelle Maschine, zusammen mit den gesicherten Volumes aufzusetzen.

Ein Test der Integrität der Sicherungen lässt sich nur über die ImageReady-Funktion ausführen, welche z.B. den Befehl "chkdsk" ausführen kann, um das Dateisystem auf Fehler zu prüfen. Auch ist es in der Lage ein Microsoft Exchange Server-Backup bereitzustellen und dessen Dateien auf Integrität überprüfen.

Der Funktionsumfang von ShadowProtect 5 ist, verglichen mit Acronis und Veeam, doch recht arg. Es existieren keine dedizierten Replikationsfunktionen oder mit De-Duplizierung gestützte Sicherungsmöglichkeiten auf die Cloud oder über WAN. Eine Möglichkeit zur Komprimierung der Sicherungen fehlt ebenfalls.

Einzig und allein das Konvertierungs-Tool zur Umwandlung der Images stellt hier ein einzigartiges Feature dar.

#### 3.3.2.3 Lizenzierung

Die Lizenz für ShadowProtect 5 ist vergleichsweise preisintensiv. Mit 395\$ (ca. 350,55€ ¹) pro virtueller Maschine lässt sich diese nur einmal wiederherstellen, bevor die Lizenz erlischt. Um mehrere Wiederherstellungen durchzuführen, können Lizenzen

in einer Sammelbestellung (Bundle) gekauft werden. Angeboten werden hierbei bis zu 50 Maschinen für einen Preis von 7750\$ (ca. 6877,88€ ¹).

Der Support wird ebenfalls in Bundles angeboten, da eine Lizenz für den Support nur für einen Supportfall gültig ist. Diese müssen jedoch extra dazugekauft werden. Die Supportlizenzen reichen vom Einzelkauf für 50\$ für Desktop- (ca. 44,37€ ¹) und 300\$ (ca. 266,24€ ¹) für Enterprise Editionen, bis hin zu 5 Supportfällen für 225\$ (ca. 226,30€ ¹) für Desktop- und 1375\$ (ca. 1220,27€ ¹) für Enterprise- Editionen.

# 3.3.3 Veeam Backup & Replication v8

Veeam Backup & Replication v8 ist die derzeit aktuellste Version von Veeam Softwares Backup & Replication-Reihe. Die agentenlose Software wurde speziell für virtuelle Maschinen konzipiert und bietet viele Funktionen zur automatisierten Sicherung und Wiederherstellung, selbst über das WAN an.

Jedoch unterstützt das Programm lediglich VMware und Hyper-V-Umgebungen, was den Anwendungsraum stark eingrenzt.

#### *3.3.3.1 Features*

In Sachen Backup, bietet Veeam nicht nur voll, differentiell, inkrementell und synthetisch voll an, sondern auch rückwärts-inkrementell, ein Verfahren, was die Wiederherstellungszeit der aktuellsten Versionen bei inkrementellen Backups beschleunigen soll. Diese können sowohl manuell, als auch über zeitgesteuerte Jobs ausgeführt werden. Zusammen mit der Möglichkeit, Backups und Replikationen über das WAN oder über die Cloud zu sichern, erlaubt die Software die Erfüllung der 3-2-1-Regel. Auch das FIFO und das Generationenprinzip lassen sich vollständig umsetzen. Sämtliche erstellte VMs lassen sich für den Datentransfer und zur Speicherung komprimieren. Die Integrierte WAN-Beschleunigung und De-Duplizierung beschleunigen ebenfalls den Versand über das Netzwerk. CBT und automatisierte Benachrichtigungen lassen sich ebenfalls aktivieren.

Replikation wird (wie der Name des Programmes bereits sagt) ebenfalls unterstützt. Failover-, sowie Failback sind hier feste Bestandteile der Lösung. Mit der Erstellung eines Failover Plans, lassen sich ganze Gruppen von VMs wieder in Betrieb nehmen. Wie auch bei Backups werden hier Changed Block Tracking und Komprimierung unterstützt.

Bei der Wiederherstellung gibt es ebenfalls zahlreiche Möglichkeiten. Virtuelle Maschinen lassen sich komplett wiederherstellen. Auch einzelne Dateien auf

-

<sup>&</sup>lt;sup>1</sup> Der Preis wurde über die Google-Währungsumrechnung ermittelt und bezieht ich auf den Wechselkurs vom 21. August 2015.

beliebigen Gastsystemen lassen sich direkt aus den Backups heraus extrahieren. Des Weiteren unterstützt die Software ebenfalls die Wiederherstellung einzelner Microsoft Exchange und SharePoint-Objekte, sowie SQL-Datenbanken.

Mit Instant-VM-Recovery lässt sich, in Notsituationen, eine VM direkt aus einem Backup heraus starten und kann dadurch mit minimaler Ausfallzeit einen Ersatzserver bereitstellen.

Lediglich eine Bare-Metal-Recovery lässt sich aufgrund einer fehlenden Funktion zur Sicherung des Hosts durchführen.

Zum Test der Sicherungen auf Funktionalität bietet das Programm das sogenannte "SureBackup"-System an. Hierbei wird eine isolierte Testumgebung aufgebaut, bei dem das Backup bei einem ESXi-Host registriert gestartet und auf Verfügbarkeit und Bootbarkeit getestet wird. Durch die Möglichkeit, eigene Skripte in das System zu integrieren, können diese Tests so komplex und umfangreich werden, wie der Kunde es benötigt.

#### 3.3.3.2 Lizenzierung

Eine Lizenz für "Veeam Backup & Replication" ist zeitlich unbegrenzt und wird pro Sockel bestimmten Preisen, pro Edition vertrieben.

Zur Verfügung stehen die Standard, Enterprise und Enterprise Plus Editionen, welche unterschiedliche Features beinhalten.

Die individuellen Preise (pro Sockel) lauten wie folgt:

Standard Edition: 620€

• Enterprise Edition: 1100€

Enterprise Plus Edition: 1680€

Der Support ist für Europa in allen drei Editionen für das erste Jahr kostenlos.

Alternativ lassen sich auch Abonnement-basierte Lizenzen erwerben. Diese gelten entweder für ein, zwei, oder drei Jahre. Nach Ablauf der Lizenz wird sowohl der Support als auch die Nutzung des Programms abgeschaltet. Sie kann bei Bedarf verlängert, oder gegen eine einmalige Lizenz eingetauscht werden.

Die Preise für die Editionen variieren auch hier und es gelten damit die folgenden Preise pro Jahr:

Standard Edition: 395€

Enterprise Edition: 635€

Enterprise Plus Edition: 1010€

# 3.4 Zusammenfassung

Zusammenfassend werden hier noch einmal die Ergebnisse tabellarisch in einer Übersicht aufgeführt:

|                          | Veeam          | Acronis        | StorageCraft  |
|--------------------------|----------------|----------------|---------------|
|                          | Backup &       | Backup für     | ShadowProtect |
|                          | Replication v8 | <b>VM</b> ware | Version 5     |
| Backupmethoden           |                |                |               |
| - Voll                   | ✓              | ✓              | ✓             |
| - Synthetisch voll       | ✓              | ✓              | ✓             |
| - Differentiell          | ✓              | ✓              | ✓             |
| - Inkrementell           | ✓              | ✓              | ✓             |
| - Rückwärts inkrementell | ✓              | ×              | ×             |
| Rotationsmethoden        |                |                |               |
| - FIFO                   | ✓              | ✓              | ✓             |
| - GVS-Schema             | ✓              | ✓              | ×             |
| - Türme von Hanoi        | ✓              | ✓              | ×             |
| Replikation              | ✓              | ✓              | ×             |
| Komprimierung            | ✓              | ✓              | ×             |
| De-Duplizierung          | ✓              | ✓              | ×             |
| Sicherung über WAN       | ✓              | ×              | ×             |
| Sicherung auf Cloud      | √ *1           | <b>√</b> *2    | <b>√</b> *2   |
| Test der Backups         | <b>√</b> *1    | <b>√</b>       | ✓             |
| Wiederherstellung        |                |                |               |
| einzelner Objekte        |                |                |               |
| - MS SQL Support         | <b>√</b> *3    | $\checkmark$   | <b>√</b> *4   |
| - MS Exchange Objekte    | <b>√</b> *3    | ✓              | ×             |
| - MS Share Point         | <b>√</b> *3    | ✓              | ×             |
| Agenten-frei             | ✓              | <b>√</b> *5    | ×             |
| Backup ESXi-Host-Konfig. | ×              | ✓              | ×             |
| Bare-Metal-Recovery      | ×              | ✓              | ×             |
| Desaster Recovery Plans  | ×              | ✓              | ×             |
| Benachrichtigungssystem  | ✓              | ✓              | ✓             |

<sup>\*1</sup> Erst ab Enterprise Edition und höher

Tabelle 1: Vergleich von Backupsystemen für virtuelle Umgebungen

<sup>\*2</sup> Separate Lizenz

<sup>\*3</sup> Wiederherstellung an den ursprünglichen Ort erst ab der Enterprise Edition und höher

<sup>\*4</sup> Überprüfung einzelner Objekte, jedoch keine individuelle Objektwiederherstellung

<sup>\*5</sup> Installation auf physikalischen Servern nur mit Agenten möglich, sonst ohne

#### 3.5 Fazit des Vergleichs

Im direkten Vergleich sieht man schnell, dass das Produkt von StorageCraft, zumindest vom Funktionsumfang her, nicht mit denen von Veeam und Acronis mithalten kann. Daher eignet sich dieses Produkt am ehesten für kleine Firmen, mit eingeschränkter, virtueller Infrastruktur, bei denen mit nur wenigen Ausfällen zu rechnen ist und High-Availability keine sonderliche Rolle spielt. Durch die Support-Lizenzierung pro Fall lässt sich, im Verlaufe der Zeit ggf. Geld sparen, solang dieser nicht benötigt wird.

Solang sich jedoch auch andere Alternativen darbieten, sollte aufgrund der hohen Kosten auf dieses Programm möglichst verzichtet werden.

Interessant hingegen ist der Vergleich zwischen VBR und "Acronis Backup for VMware". Beide Lösungen bieten ein ähnlich großes Repertoire an Werkzeugen zur Bewältigung zahlreicher sicherungsbezogener Probleme.

Während VBRv8 mit seiner agentenlosen Funktionsweise, sowie rückwärtsinkrementeller und WAN-gestützter Sicherung einige Vorteile gegenüber dem Produkt von Acronis besitzt, so lässt sich doch keine Bare-Metal-Recovery durchführen. Auch stellt es keine mögliche Option dar, wenn eine Plattform außer VMware oder Hyper-V verwendet wird.

Da sich die Lizenzierungsmethoden zwischen ihnen stark ähneln und auch der Preis nahezu im selben Bereich liegt (Vergleich der Standard-Version von VBR), lässt sich hierbei kein definitiv günstigeres Programm feststellen.

Es bliebe jedoch noch weiter zu untersuchen, ob sich ggf. doch ein Umschwenken von Veeam auf Acronis für jetzige, oder zukünftige Kunden und Interessenten lohnt.

# 4 Einrichtung von Veeam Backup & Replication v8

# 4.1 Hinzufügen der zu sichernden Server

Bevor die Backup- und Replikations-Jobs überhaupt definiert werden können, müssen vorerst alle der von Veeam zu verwaltenden Server hinzugefügt werden.

Im "Backup Infrastructure"-Menü befindet sich der Menüpunkt "Managed Servers". Nach Auswahl dieses Punktes kann anschließend mit einem Klick auf die obere, linke Fensterecke via "Add Server" der Assistent zum Hinzufügen von Servern aufgerufen werden.

Als erstes steht die Auswahl des korrekten Server-Typs bevor. Dabei werden VMware vSphere und vCloud Director, sowie Hyper-V-, SMB3-, Linux und Windowsserver unterstützt.

Nach Auswahl des Typs und Angabe eines Namens und optionaler Beschreibung für den Server erfolgt nun die Angabe der Zugangsdaten für diesen Server. Die Zugangsdaten müssen einem Konto des Servers mit administrativen Rechten angehören.

Wurden noch keine Zugangsdaten zu Veeam hinzugefügt, kann dies über den Link "Manage accounts" nachgeholt werden.

VBR nutzt standardmäßig den Port 443 (HTTPS) um mit den Servern zu kommunizieren. Wurde eine nutzerdefinierte Änderung am Server diesbezüglich vorgenommen, muss diese Einstellung dementsprechend angepasst werden.

Beim Hinzufügen eines ESX-Hosts steht ein weiterer Konfigurationsschritt für eine SSH unterstützte Konsolenverbindung zur Verfügung. Des Weiteren lassen sich Ports für Kopier- und Copy-Job-Prozesse festlegen. Standardmäßig stehen hierfür die Ports 2500-5000 zur Verfügung. Bei kleineren Infrastrukturen kann die Portreichweite jedoch auch beschränkt werden, um z.B. lediglich 15 gleichzeitige Jobs zuzulassen.

Mit diesen Schritten ist die Serverkonfiguration vollendet. Hinzufügen lassen sich die Server in der zusammenfassenden Übersicht im letzten Schritt über einen Klick auf "Finish".

# 4.2 Einrichten des Backup-Proxys

Für den Datentransfer von der zu sichernden VM zu dem gewünschten Backup-Repository muss der Backup-Proxy eingerichtet werden. Dafür kann man im Menü "Backup Infrastructure" mit einen Klick auf den Button "Add Proxy" den Einrichtungsassistenten aufrufen. Alternativ kann dieser auch mit einem Rechtsklick auf "Backup Proxies" und anschließender Auswahl von "Add VMware Backup-Proxy" gestartet werden.

Der erste Schritt ist die Auswahl des Servers, welcher den Proxy betreiben soll. Wird der gewünschte Server nicht in der Liste der Backup-Proxys aufgezeigt, so wurde dieser noch nicht hinzugefügt (siehe 4.2.).

In der Text-Box unter "Proxy Description" lässt sich optional eine Beschreibung des Proxys eintragen, um bei Betrieb mehrerer Proxys den Überblick zu erhalten.

Der Transportmodus wird unter "Transport Mode" angegeben.

Das Programm versucht im Normalfall den optimalen Modus automatisch zu bestimmen.

Bei Auswahl der Option "Direct SAN Access" oder "Virtual Appliance" kann über die Option "Failover to network mode if primary transport modes fail or are unavailable" ein Failover auf den Netzwerkmodus aktiviert werden, sollte ein Job fehlschlagen.

Bei Auswahl des Netzwerkmodus lässt sich optional eine SSL-Verschlüsselung aktivieren, wenn die Option "Encrypt LAN traffic in the network mode (SSL)" ausgewählt wurde.

Veeam versucht standardmäßig automatisch sämtliche Datastores zu erkennen. Dies ist auch als Voreinstellung unter "Connected datastores" aufgeführt. Wünscht man jedoch, ganz bestimmte Datastores zu nutzen, können diese per Klick auf "Choose", rechts daneben, manuell ausgewählt werden.

Unter "Max. concurrent tasks" lässt sich die Anzahl gleichzeitig ablaufender Jobs für den Proxy festlegen. Diese Zahl sollte gleich der Anzahl der zur Verfügung stehenden Prozessorkerne sein. Das bedeutet, wenn zwei Kerne zur Verfügung stehen, sollten auch nur maximal zwei gleichzeitige Jobs ausgeführt werden.

Mit diesen Einstellungen wäre Schritt eins der Einrichtung des Proxys abgeschlossen.

Der zweite Schritt erlaubt es, Einstellungen bezüglich der Nutzung des Netzwerkes vorzunehmen. Das beinhaltet sowohl eine Begrenzung des maximal erlaubten Datendurchsatzes, sowohl als auch ein zeitliches Fenster welches erlaubte Nutzungszeiten definiert. All diese Einstellungen können für bestimmte Ziel-Adressen und -Adressbereiche definiert werden.

Der letzte Schritt gestattet nochmals eine zusammenfassende Einsicht über die vorgenommenen Einstellungen. Hier sollten diese noch einmal verifiziert werden, bevor die Einrichtung über einen Klick auf "Finish" abgeschlossen wird.

# 4.3 Einrichten des Backup-Repositories

Als letzte der drei Hauptkomponenten wird nun noch der Backup-Proxy eingerichtet. Im Menü "Backup Infrastructure" kann der Assistent entweder über einen Linksklick (oben links) auf "Add Repository", oder einem Rechtsklick auf den Punkt "Backup Repositories" mit anschließender Auswahl der Option "Add Backup Repository" gestartet werden.

Als nächstes ist das Repository als einer der folgenden Typen zu definieren:

- Microsoft Windows server with local or directly attached storage
- Linux server with local, directly attached or mounted NFS storage
- Shared folder using CIFS (SMB) protocol
- Deduplicating storage appliance

Nach Auswahl des Typs erfolgt der nächste Schritt zur Serverwahl.

Die konkrete Speicherpartition wird im Schritt "Repository" angegeben.

Neben der Wahl der Partition, lassen sich auch hier, wie beim Backup-Proxy, die Anzahl der maximal zulässigen, gleichzeitigen Aufträge unter "Limit maximum concurrent tasks" und die maximale Datenrate unter "Limit combined data rate to" begrenzen, wenn nötig.

Unter "Advanced" gibt es einige, weitere, interessante Optionen.

Für den Fall, dass De-Duplizierungstechniken eingesetzt werden, lassen sich Sämtliche Datenblöcke des angelegten Backups mithilfe der Option "Align backup file data blocks" auf eine feste Blockgröße von 4kb begrenzen. Diese Option sorgt für bessere De-Duplizierung, jedoch auf Kosten der Fragementierung und eventueller Platzverschwendung.

Ein weiteres Mittel, um De-Duplizierung zu erhöhen ist die Dekomprimierung der Daten, bevor sie auf das Medium gespeichert werden. Mit einem Haken in die Checkbox "Decompress backup data blocks before storing", lässt sich diese Funktion aktivieren. Zu beachten ist hierbei, dass diese Option nur sinnvoll ist, wenn die Backupdaten vor dem Transfer komprimiert werden.

Der nächste Schritt, "vPower NSF", ist vor allem für die SureBackup-Funktion von äußerster Bedeutung. vPowerNSF ist ein Windows Service, der einen Server als NSF-Server agieren lässt. Über diese Funktionen kann ein Backup direkt als virtuelle

Maschine aus dem Repository in einen ESX(i)-Host geladen werden, was die Grundlage von Funktionen wie der "File-Level Item Recovery" (FLIR), "Instant-VM-Recovery", "Universal Aplication-Item Recovery" (U-AIR) und der SureBackup-Funktion ist. Werden diese Funktionen verwendet, muss diese Option aktiviert sein, damit sie reibungslos funktionieren.

Zu guter Letzt lassen sich wieder alle vorgenommenen Konfigurationen noch einmal einsehen und überprüfen. Mit der Betätigung von "Finish" werden diese anschließend übernommen.

# 4.4 Einrichtung der Backup-Jobs

Die Aufgabe der Backup-Jobs ist die Automatisierung des Erstellens nutzerdefinierter Backups zu vorgegebenen Zeiten. Solche Jobs lassen sich über den Einrichtungsassistenten im Menü "Backup & Replication" erstellen. Gestartet werden kann dieser mit einem Klick auf "Backup Job" in der oberen, linken Ecke des Fensters, oder mit einem Rechtsklick auf "Backup" im Unterpunkt "Jobs" und anschließender Auswahl der Option "VMware" oder "Hyper-V".

Als erstes werden wieder ein Name und eine Beschreibung gefordert. Der Name sollte dabei aussagekräftig und kurz sein, um einzelne Jobs schneller unterscheiden und zuordnen zu können.

Im zweiten Schritt wird nun der zu sichernde VM-Container gewählt, welcher alle zu sichernden virtuellen Maschinen beinhaltet. Wird nach der Konfiguration des Jobs eine VM in den Container hinzugefügt, so aktualisiert sich automatisch der Backup-Job, sodass ab sofort auch die neue Maschine mit gesichert wird.

Sollen bestimmte VMs aus dem Sicherungsprozess ausgeschlossen werden, so lassen sich diese in die "Exclusions"-Liste eintragen. Dazu betätigt man rechts den Button "Exclusions…" und fügt die auszuschließenden Server der Liste hinzu.

Anstatt eines Containers lassen sich die Server auch einzeln hinzufügen. Dies ist notwendig, wenn man die Backup-Reihenfolge manuell festlegen möchte. Jedoch ist dies mit dem Hinzufügen von Containern nicht möglich, da diese die Liste zugehöriger virtueller Maschinen zufällig generieren und es damit keine festgelegte Reihenfolge gibt.

Im Abschnitt "Storage" werden nun ein Backup-Proxy für den Datentransfer von der VM und ein zuständiges Backup-Repository ausgewählt. Der Backup-Proxy wird per Voreinstellung automatisch gewählt. Dabei überprüft Veeam den Transportmodus, die Konnektivität und die derzeitige Last aller verfügbaren VMs, um den geeignetsten Kandidaten für einen auszuführenden Backup-Job zu bestimmen.

Optional kann auch eine feste Menge bestimmter Proxys festgelegt werden. Für die Zwecke der BA Glauchau, genügt jedoch bereits die automatische Auswahl.

Unter "Backup Repository" muss das Repository angegeben werden, auf den die virtuellen Maschinen gesichert werden sollen.

Die Anzahl der vorzubehaltenden Sicherungspunkte lässt sich mit der Option "Restore Points to keep on disk" genau festlegen.

Sollen die Daten während des Jobs gleichzeitig auf ein weiteres, getrenntes Medium kopiert werden, muss die Option "Configure secondary destinations for this job" aktiviert werden, womit der Schritt "Secondary Target" freigeschalten wird.

Der "Advanced..."-Button des "Storage"-Schritts erweiterte bietet wichtige, Einstellungen z.B. die Angabe der Backupmethode, an, wie Benachrichtigungsoptionen für Administratoren und Einstellungen zum Komprimierungsgrad.

Im 8. Schritt kann nun das sekundäre Speicherziel festgelegt werden, solang die Option "Secondary Target" im vorherigen Menüschritt aktiviert wurde. Hier kann der Job an einen Backup-To-Tape-Job oder einen Backup-Copy-Job gebunden werden, welcher letztendlich die Spiegelung des anzulegenden Backups übernimmt.

"Guest Processing" ist die nächste Sektion, in der Microsofts VSS-Technologie, sowie das indizieren von Dateien aus Gastsystemen aktiviert werden können. "Enable application-aware image processing" nutzt VSS, um Applikationen stillzulegen, um einen reibungslosen Sicherungsvorgang zu gewährleisten. Diese Option ist für sämtliche Server, deren Services keinen hohen Echtzeitanforderungen entsprechen, höchstens zu empfehlen.

"Enable guest-file system indexing" generiert einen Katalog von Dateien aus Gastsystemen. Dieser Katalog wird für den Dateiexplorer und dem 1-Click-Restore von individuellen Dateien benötigt. Diese Features existieren jedoch nur im Umfang des "Enterprise Managers", welcher hier keine Anwendung findet. Daher bleibt diese Einstellung inaktiv.

Neben den VSS und Gastsystem-Einstellungen müssen des Weiteren die Zugangsdaten eines Nutzerkontos auf der VM definiert werden. Dieses Nutzerkonto muss über administrative Rechte auf der virtuellen Maschine verfügen, damit Veeam uneingeschränkten Zugriff auf die Daten zum Lesen und Schreiben hat.

Im nächsten Schritt wird der Zeitplan für den Job festgelegt. Hier wird definiert zu welchen Tagen und Zeiten das Backup angelegt werden darf. Hier kann ein Job auch

direkt an einen anderen angehangen werden. Damit wird der angehangene Job sofort nach Vollendung des angegebenen Jobs ausgeführt.

Des Weiteren kann hier die Anzahl der Neuversuche bei Scheitern eines Jobs und die Wartezeit vor einem Neuversuch definiert werden.

Im letzten Menü können alle Einstellungen nochmals eingesehen und mit "Finish" bestätigt werden.

# 4.5 Einrichtung der Replikations-Jobs

Auch wenn noch keine konkreten Pläne für eine Replikation bestehen, so gibt es dennoch einige Beispiele, bei denen sich eine Replikation eines häufig genutzten Servers zur Erreichung von Availability lohnen könnte.

Für den Fall der Einrichtung eines solchen Systems soll im Folgenden eine Beschreibung zur Einrichtung dessen beschrieben werden.

Die Konfiguration eines solchen Jobs ist im Vergleich zu anderen recht umfangreich. Der Assistent zur Konfiguration eines solchen Jobs befindet sich im Menü "Backup & Replication" und kann unter "Jobs" über das Menü "Replication" für VMware oder Hyper-V gestartet werden.

Im ersten Schritt erfolgt wieder die Angabe eines Namens für den Job und eine optionale Beschreibung. Zusätzlich befinden sich hier aber noch drei weitere Einstellungsmöglichkeiten, die jeweils einen zusätzlichen Konfigurationsschritt im Konfigurationsmenü freischalten.

Zu einem wäre dies das sogenannte "Replica Seeding", welches über den Punkt "Low connection bandwidth (enable replica seeding)" ein- oder ausgeschalten werden kann. Replica seeding reduziert die Netzwerklast, indem es Veeam erlaubt ein bereits vorhandenes Backup als Basis der Replikation zu verwenden. Aufgrund dessen müssen nur noch inkrementelle Änderungen zum dortigen Zustand über das Netzwerk versendet werden, was die Datenmenge stark minimiert.

"Separate virtual networks (enable network mapping)" erlaubt das Anlegen einer Mapping-Tabelle, um die Last auf das Netzwerk ebenfalls zu verringern.

Um die IP-Adressen von Replikaten automatisch anzupassen, für den Fall, dass Adress-Schemata im Produktions- und Replikationsstandort nicht übereinstimmen, kann ein sogenanntes "Re-IP" vorgenommen werden. Zu Konfiguration dieser Funktionalität muss "Different IP addressing scheme (enable re-IP)" aktiviert sein.

Per Klick auf "Next" gelangt man in den nächsten Schritt, indem die Auswahl der zu replizierenden Maschinen stattfindet. Hier können sowohl einzelne VMs als auch

ganze Cluster repliziert werden. Bei der Cluster-Replikation werden neu in den Cluster hinzugefügte, virtuelle Maschinen, automatisch in den Backup-Job einbezogen.

Gegebenenfalls kann die Datenquelle über einen Klick auf "Source..." festgelegt werden. Hier können die Daten entweder von der VM selbst bezogen werden. Dies belastet jedoch das Produktionssystem und sollte, wenn möglich, gemieden werden. Andererseits lässt sich der Zustand der Maschine auch über dessen angelegtes Backup auf einem Repository beziehen. Hier können eine oder mehrere Speicherziele ausgewählt werden.

Zu beachten ist hierbei der Unterschied zu Replica-Seeding: Beim Seeding wird nur das initiale Replikat auf Basis des Backups erstellt. Alle weiteren, inkrementellen Änderungen erfolgen über den Bezug der Daten von der Produktions-VM an sich. Bei Auswahl einer Datenquelle jedoch, werden auch alle weiteren Backups nur von dem Repositorien bezogen. Daher setzt diese Option für einen ordnungsgemäßen Replikationsvorgang einen Backup-Job voraus.

Mit "Exclude..." können virtuelle Maschinen, oder einzelne Festplatten ausgewählt werden, welche vom Replikationsvorgang ausgeschlossen werden sollen. Dies ist nützlich, wenn ein ganzer Cluster repliziert werden soll, mit der Ausnahme einiger, weniger VMs.

Wie bei Backups kann auch hier über die Buttons "Up" und "Down" die Reihenfolge hinzugefügter Maschinen geändert werden, um z.B. systemkritische VMs als erstes zu replizieren.

Im "Destination"-Schritt des Assistenten wird der Zielort festgelegt. Hierbei müssen der entsprechende Host oder Cluster, ein Ressourcen-Pool, ggf. der Ordner für virtuelle Maschinen, sowie der Datastore bestimmt werden. Diese Einstellungen können für die Gesamtheit der zu replizierenden VMs oder vereinzelt pro Maschine (über "Choose…") vorgenommen werden.

Standardmäßig nutzt Veeam zum Speichern der VM-Daten thin disks. Falls die originale VM jedoch thick disks nutzt, kann dies über einen Klick auf "Pick datastore for selected virtual disks" geändert werden. Mit einem Klick auf "Add VM" wird der Explorer zur Auswahl der virtuellen Maschinen geöffnet. Nun muss die hinzugefügte Maschine ausgewählt werden, woraufhin sich das Format unter "Disk Type" ändern lässt.

Der darauffolgende Menüpunkt bestimmt über das Netzwerk-Mapping. Hierbei muss das Mapping für alle zu verbindenden Netzwerke, von Produktions- zu Replikationsstandort vorgenommen werden.

Durch Konfiguration des Mappings wird es Veeam ermöglicht, die IP-Adresse eines Replikates im Replikations-Netzwerk auf das Produktionsnetzwerk zu legen. Dadurch muss, im Falle eines Failovers, keine manuelle Anpassung der Verbindung des Replikates zum Produktionsnetz mehr erfolgen.

Diese Optionen sind nur verfügbar, wenn im Schritt "Name" die Option für Netzwerk-Mapping aktiviert wurde.

Wurde die Option "Different IP addressing scheme" im ersten Schritt des Assistenten ausgewählt, steht nun die "Re-IP"-Konfiguration zur Verfügung. Durch die Definition von Adress-Schemata-Regeln wird es Veeam ermöglicht die Replikations-VM mit der Produktions-VM zu verbinden, wenn sich die Adress-Schemata unterscheiden.

Die Adress-Reichweiten lassen sich in den Feldern "IP address" mit Ziffern von 1 bis 9 und dem "\*"-Zeichen definieren. So z.B. definiert die Eingabe "192.168.\*.\*" mit der Subnetzmaske "255.255.0.0" die Adressbereiche von 192.168.0.1 bis 192.168.255.254 in einem Klasse B Netzwerk.

Wurden die bis zu dem Punkt notwendigen Einstellungen vorgenommen, so erfolgt nun die die Konfiguration des Jobs an sich. Anzugeben sind hierbei in erster Line das Repository zur Speicherung von Checksummern gelesener Datenblöcke, um den inkrementellen Replikationsprozess zu beschleunigen.

Um das Replikat vom Original unterscheiden zu können, muss ein Suffix angegeben werden, welcher an dessen Namen angehangen wird.

Mit der "Restore points to keep"-Option wird die Anzahl zu erhaltender Wiederherstellungspunkte festgelegt.

Neben diesen Einstellungen, gibt es unter "Advanced" weitere Konfigurationsmöglichkeiten.

Unter "Traffic" kann die Menge des Netzwerkverkehrs angepasst werden. Dabei kann angegeben werden, ob Pagefile-Blöcke auf Windows basierenden Maschinen in den Bearbeitungsprozess einbezogen, oder ausgeschlossen werden sollen. Um sie einzubeziehen, muss die Option "Exclude swap file block from processing" deaktiviert werden. Aufgrund der stark dynamischen Natur dieser Daten ist dies nur zu empfehlen, wenn eine Echtzeit-Replikation durchgeführt wird.

Die Komprimierung der Daten vor dem Versand kann für eine geringere Last auf dem Übertragungskanal sorgen. Jedoch ist dies nur möglich, wenn diese zwischen zwei Backup-Proxys transferiert werden. Bei nur einem Proxy wird keine Dekomprimierung angewandt.

Um die Blockgröße der Replikationsdaten zu optimieren, muss unter "Storage optimization" der entsprechende Speichertyp ausgewählt werden. Da Veeam die Images beim Lesevorgang in Blöcke fester Größe aufteilt, hat dies Auswirkungen auf die Geschwindigkeit der Jobs. Da ebenfalls Metadaten zu jedem Block gespeichert werden, wird der Datastore bei geringeren Blockgrößen stärker belastet.

"Local target (16 TB + backup files)" kann verwendet werden, um Replikationsdaten von 16 TB oder mehr zuzulassen. Dabei wird eine Blockgröße von 8MB verwendet.

Für SAN, DAS oder direkt angeschlossenen Speichern sollte die Option "Local Target" mit einer Blockgröße von 1MB verwendet werden. Dies erlaubt es SAN, größere Datenblöcke mit einmal zu Verarbeiten und verringert somit die dafür notwendige Zeit. Jedoch sinkt hierbei die Effizienz der De-Duplizierung, da die Chance auf identische Blöcke mit zunehmender Größe sinkt. Allerdings stellt diese Methode aufgrund der großen Datenblöcke das beste Leistungsverhältnis der Jobs her.

Für Speicherziele im lokalen Netzwerk wird "LAN target" verwendet. Mit einer Blockgröße von 512 kB steigt zwar die De-Duplizierungsrate im Vergleich zu "Local target", jedoch sinkt damit auch die Performanz der Jobs.

Externe, über das WAN verbundene Ziele, sollten hierbei als "WAN target" festgelegt werden. Im Vergleich zu "LAN target" verringert sich hierbei die Block-Größe um die Hälfte und die De-Duplizierung ist am effizientesten. Jedoch bietet dieses Verfahren die schlechteste Replikations-Performanz.

Der "Notification"-Tab erlaubt die Konfiguration automatisierter E-Mail Nachrichten an Administratoren im Falle von Erfolg, Problemen oder gänzlichem Scheitern des Jobs. Diese Nachrichten können für jeden vorgenommenen Versuch des Jobs gesendet werden. Jedoch erlaubt die Funktion "Suppress notification until the last entry" eine Unterdrückung des Versands bis auf den letzten Versuch.

Die Adressen der gewünschten Empfänger sind mit einem Semikolon getrennt unter das Feld bei "Send email notifications to the following recipents" einzutragen.

Im Tab "vSphere" befindet sich die Funktion, I/O-Prozesse virtuelle Maschinen während des Replikationsprozesses anzuhalten, um ein konsistentes Abbild zu erhalten. Des Weiteren kann hier die Verfolgung geänderter Datenblöcke (CBT) aktiviert werden. Dies wird höchstens empfohlen, jedoch nur solang die VM noch über keine Snapshots verfügt, da diese Funktion sonst nicht aktiviert wird.

Unter "Storage Integration" lassen sich, anstelle von VMware-Snapshots Storage-Snapshots verwenden. Dies kann die Image Erstellung beschleunigen. Für den Fall einer Fehlkonfiguration oder einer gescheiterten Sicherung, kann über "Failover to standard backup" ein Failover zu nativen Methoden aktiviert werden.

Zu guter Letzt kann man noch, im "Advanced" Tab, Einstellungen zur Integritätsüberprüfung von Storage Metadaten und vor oder nach dem Job durchzuführenden Skripten vornehmen.

Im Schritt "Data Transfer" sind u.a. die Backup Proxys zum Datentransfer festzulegen. Der Quell-Proxy liegt dabei auf Seiten der Produktion, während sich der Ziel-Proxy beim Speicherzielort der Replikation befindet.

Im Falle einer Nutzung der WAN-Beschleunigung muss jeweils ein Beschleuniger an der Produktion und ein Beschleuniger am Ziel angegeben werden. Dafür muss jedoch die Option "Through build-in WAN accelerators" augewählt worden sein.

Sollte keine WAN-Beschleunigung zum Einsatz kommen, muss die Option "Direct" ausgewählt werden.

Wenn die Option für Replica-Seeding aktiviert wurde, so ist der "Seeding"-Schritt verfügbar.

In diesem Menü wird zuerst das Backup-Repository ausgewählt, von welchem das Backup ("Seed") bezogen werden soll.

Verfügt die Replikations-Seite bereits ein Replikat der VM, so kann dieses gemappt werden, um die zu versendende Menge an VM-Daten zu verringern. Veeam sichert hierbei nur noch die veränderten Daten im Vergleich zum bereits bestehenden Replikat. Um den Job an das Replikat zu verknüpfen muss vorerst die Funktion "Map replicas to exising VMs" aktiviert werden. Anschließend kann die Liste mit einem Klick auf "Detect" automatisch aktualisiert werden, woraufhin alle vorhandenen Replikate und deren Original-VMs aufgelistet werden sollten. Ist dies nicht der Fall, kann das Mapping manuell über "Edit" durchgeführt werden.

Für die Sicherstellung konsistenter Sicherungen ist der Schritt "Guest Processing" von besonderer Bedeutung. Hier werden drei Optionen angeboten:

- Application-aware image processing
- Transaction log handling
- pre-freeze and post-thaw scripts

Application-aware image processing nutzt, wie bei Backups, Microsofts VSS-Technologie, um Backups auf einen konsistenten Zustand zu bringen. Hierbei gibt es jedoch drei zusätzliche Optionen, welche das Verhalten des Jobs währenddessen

bestimmen. Einerseits kann vom Nutzer verlangt werden, dass die Volumenschattenkopie erfolgreich verlaufen sein muss, bevor der Job fortgeführt wird. Andererseits können auftretende Fehler entweder ignoriert, oder die Stilllegung durch VSS gänzlich deaktiviert werden.

Mit "Transaction logs" kann Veeam Transaktions-Logs von Microsoft-SQL Servern kürzen, um Speicher freizugeben. Ansonsten wächst die Größe des Logs weiter an und kann unter Umständen viel Speicherplatz belegen. Wenn anwendbar, sollte diese Option ausgewählt werden.

Skripts zur Ausführung vor und nach Ausführung der Replikation können im "Scripts"-Tab definiert werden. Dies ermöglicht die Ausführung nutzerdefinierter Tests zur Sicherstellung der Funktionalität des replizierten Systems. Ein solcher Test wird als erfolgreich angesehen, wenn er den Integer-Wert "0" zurückgibt.

Der letzte Schritt, "Schedule" erlaubt die Konfiguration des Zeitplanes des Jobs. Dabei lässt sich dieser entweder in regelmäßigen Intervallen, oder nach Abschluss eines bestimmten Jobs ausführen. Die Einstellungsmöglichkeiten sind analog zu denen eines Backup-Jobs.

Wie auch bei Backups lassen sich hier die Anzahl der Neuversuche und die Wartezeit vor jedem Versuch festlegen.

Mit "Create" und anschließendem "Finish" lässt sich dieser Job anwenden.

## 4.6 Einrichtung von Sicherungen auf Bandlaufwerken (Tape-Jobs)

Um eine Sicherung auf Band durchzuführen muss ein Tape-Job angelegt werden. Dieser kann im Menü "Backup & Replication" mit rechtsklick auf "Jobs" über "Tape Job" und "Backup" erstellt werden.

Nach der Angabe einer Beschreibung und einem Namen für den Job, erfolgt im zweiten Schritt die Verknüpfung des Tape-Jobs mit einem bestehenden Backup-Job. Dazu muss lediglich der gewünschte Job aus der Liste hinzugefügt werden.

Im nächsten Schritt, ist der Medien-Pool für die Sicherungen zu definieren. Dieser muss für virtuelle, volle Backups angegeben werden. Für inkrementelle Backups jedoch kann optionaler weise ein zweiter Pool hinzugefügt werden. Dafür muss die Option "Process incremental backup files" aktiviert sein.

Veeam erstellt automatisch virtuelle, volle Backups auf Bandsicherungen.

Mit "Schedule" kann der Zeitplan für diese virtuellen, vollen Backups angegeben werden.

In den Archivierungsoptionen im nächsten Menü kann die Hardwarekomprimierung aktiviert werden. Außerdem lässt sich bestimmen, ob das Band nach erfolgreicher Beendigung des Jobs automatisch ausgeworfen werden soll oder nicht.

Über "Export current media set once the job finishes" lassen sich Bänder, die zu dem angegebenen Media Set gehören in den Import bzw. Export-Slot verlegen.

Mit "Advanced" öffnen sich weitere Optionen. Diese beinhalten Benachrichtigungseinstellungen und Optionen zum automatischen Ausführen von Skripts.

Der Zeitplan lässt sich nun unter "Job Schedule" einrichten. Der Tape-Job kann entweder per Zeitplan, oder automatisch nach Vollendung des verknüpften Backup-Jobs erfolgen. Des Weiteren lässt sich die Wartezeit einstellen, über die der Job hinweg angehalten werden soll, im Falle dass ein Backup-Prozess noch im Gange ist.

Damit sind alle Konfigurationsschritte vorgenommen. Mit "Finish" können die Einstellungen übernommen werden. Wurde die Option "Run the job when I click Finish" aktiviert, wird der Job nach der Übernahme sofort gestartet.

# 4.7 Optimierung des Datenflusses

Anhand der IT-Struktur könnte es nach der Einrichtung aller Komponenten dazu kommen, dass während eines Backup-Jobs VM-Daten nicht direkt vom Laborgebäude zum Storage im Raum 307, sondern vorerst über den Serverraum (in dem sich der Veeam-Server befindet) geleitet werden. Dies muss vorerst optimiert werden, sodass sich die folgende Situation ergibt (siehe nächste Seite):

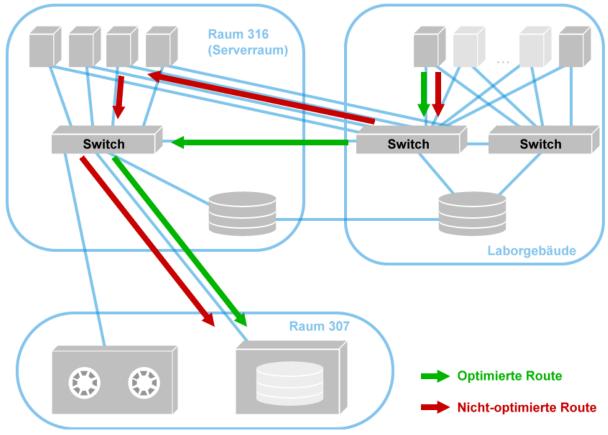


Abbildung 8: Optimierung der Versandroute für Sicherungen

Der Veeam Backup-Proxy leitet Daten von der Quelle, über sich selbst zum Zielort. Da jedoch kein weiter ESX(i)-Host auf dem direkten Verbindungsweg zwischen dem Laborgebäude und Raum 307 besteht, lässt sich dies nicht direkt auf die Struktur übertragen. Jedoch kann alternativ ein Backup-Proxy in einem der Hosts des Laborgebäudes aufgesetzt werden.

Findet nun ein Backup statt, informiert der Veeam Server den Proxy über die Quelle und das Ziel. Da der Proxy nach einer direkten Verbindung zwischen sich selbst und dem Zielort sucht, sollte dieser die von uns gewünschte Route nutzen, anstatt den Weg über den Veeam Server.

# 4.8 Einrichtung der "SureBackup"-Funktion

# 4.8.1 Einführung

Die SureBackup-Funktion ist eine von Veeam entwickelte Technologie, die es erlaubt, ein angelegtes Backup einer virtuellen Maschine direkt als Image in einen ESX(i)-Host zu laden.

Dabei wird eine abgeschirmte Umgebung erstellt, in der die VM ausgeführt und getestet wird. Um dies zu bewerkstelligen, nutzt Veeam insgesamt drei Komponenten: Eine "Application Group", ein "virtual Lab" und den "SureBackup"-Job.

# 4.8.2 Einrichtung der "Application Group"

Die Application Group ist eine Ansammlung an VMs, welche zusammen in einer virtuellen Umgebung für Testzwecke gestartet werden sollen. Diese Ansammlung beinhaltet die zu testende VM und sämtliche andere Maschinen, auf die sie für ihre Funktionalität angewiesen ist (wie z.B. einen DHCP-, DNS-, oder Datenbankserver).

Eine neue Application Group kann über den entsprechenden Einrichtungsassistenten erstellt werden. Dieser befindet sich in der Sektion "Backup Infrastructure" unter "Application Group" im Punkt "SureBackup". Mit einem Rechtsklick auf diesen kann via "Add App Group" eine Gruppe einerseits, wie in diesem Fall, für VMware- oder auch für Hyper-V-Hosts erstellt werden.

Das neu geöffnete Fenster zum Einrichten der Gruppe benötigt nur wenige Menüschritte zur Fertigstellung.

Nach Angabe eines passenden Namens und einer optionalen Beschreibung, erfolgt im zweiten Menüschritt die Angabe der zu startenden VMs samt einiger Angaben zu den Arten der auszuführenden Tests.

Die Maschinen lassen sich aus einem Backup oder der Infrastruktur hinzufügen.

Mit den Buttons "Move Up" und "Move Down" lässt sich deren Bootreihenfolge bestimmen. Dies ist von Nöten, wenn es Server gibt, auf dessen Dienste die zu testende(n) VM(s) angewiesen sind.

Nach dem Hinzufügen der einzelnen Server werden ihnen nun konkrete Rollen zugeteilt. Dadurch kann Veeam bereits speziell für die angegebene Rolle vordefinierte Tests durchführen. Dies geschieht über die Auswahl der VM in der Liste und einem anschließenden Klick auf "Edit". Im sich daraufhin öffnenden "Verification Options"-Fenster kann man nun im Tab "Role" eine der folgenden vordefinierten Rollen festlegen:

- DNS-Server
- Domain Controller
- Global Catalog
- Mail Server
- SQL Server
- Web Server

Unter dem Tab "Startup Options" können die maximale Größe des für den Tests allokierten Arbeitsspeichers, die maximal zulässige Boot-Zeit der Maschine sowie Startzeit der Applikationen und Bedingungen festsetzen, bei denen eine VM als erfolgreich gestartet betrachtet wird.

Sollten erweiterte Tests notwendig sein, können VB-Skripts im Tab "Test Scripts" in den Verifizierungstest integriert werden.

Nach erfolgreicher Konfiguration können die vorgenommenen Einstellungen anschließend mit "Finish", im letzten Schritt, übernommen werden.

# 4.8.3 Einrichtung des "virtual Labs"

Unter demselben "SureBackup"-Menüpunkt, wie bei der Einrichtung der Application Group kann auch hierfür unter "Virtual Labs" und "Add Virtual Labs" ein neues Labor angelegt werden.

Nach Start des Assistenten muss wieder ein Name für das Labor angegeben werden. Dieser Name sollte, wenn möglich, so gewählt werden, dass sich einfache Rückschlüsse auf die verwendete(n) Application Group(s) ziehen lassen können. Sollten spezielle Bedingungen gelten, können diese im Beschreibungsfeld vermerkt werden.

Im ersten Konfigurationsschritt muss ein Host für das virtual Lab ausgewählt werden, welcher die zu testende Maschine lädt und die Tests an ihr ausführt. Dieser Host sollte jedoch über ausreichend Arbeitsspeicher verfügen, da die Tests sehr ressourcenintensiv sein können.

Im nächsten Schritt muss ein Datastore zum Speichern sogenannter "Redo Logs" bestimmt werden. Redo Logs sind Hilfsdateien, welche vorgenommene Änderungen im Vergleich zum Backup der VM, zur temporären Bearbeitung der Maschine, beinhalten. Diese werden nach Durchführung der Tests automatisch wieder gelöscht.

Für eine automatische Verifizierung der Backups in dem Labor muss die Option "Use proxy appliance in this virtual lab" aktiviert und eingerichtet sein. Ohne sie können nur Heartbeat-Tests durchgeführt werden. Die Überprüfung und Wiederherstellung einzelner Dateien ist dann auch nur über die Konsole möglich.

Nach der Einrichtung des Proxys stehen nun zahlreiche Netzwerk-bezogene Einstellungen zur Konfiguration zur Verfügung.

Zu einem muss der Netzwerkmodus des Labs definiert werden. Dazu stehen drei Optionen zur Auswahl:

- Basic single-host (automatic configuration)
- Advanced single-host (manual configuration)
- Advanced multi-host (manual configuration)

Die "Basic single-host"-Methode eignet sich für Konfigurationen, bei denen sich alle Maschinen der Application Group, inklusive der zu testenden VM und dem Veeam Backup Server im selben Netzwerk befinden. In diesem Fall nimmt Veeam sämtliche Einstellungen selbst vor und startet das Labor auf dem vorweg konfigurierten Host. Auch wenn diese Methode sehr einfach zu konfigurieren ist, so legt sie zusätzliche Rechenlast auf den Host.

Im Falle, dass sich die VMs in verschiedenen Netzwerken, jedoch demselben Host befinden, muss die Option "Advanced single-host" gewählt werden. Mit dieser Methode werden zusätzliche Konfigurationsoptionen eröffnet. Eine automatische Ermittlung der Parameter durch Veeam ist hierbei nicht mehr möglich. Stattdessen, müssen alle Einstellungen zu den isolierten Netzwerken manuell vorgenommen werden. Auch hier wird zusätzliche Rechenlast auf den Host gelegt.

Am komplexesten ist "Advanced multi-host". Bei dieser Konfiguration handelt es sich um Zusammenstellungen, bei denen die Maschinen nicht nur in verschiedenen Netzwerken, sondern gar auf verschiedenen Servern befindlich sind.

Um eine Verbindung zwischen ihnen herstellen zu können kommt Veeams Distributed virtual switch (DVS) zum Einsatz. Dieser Switch stellt die zentrale Verwaltungsstelle zwischen den VMs und den isolierten Netzwerken dar.

Da diese Funktion jedoch die Enterprise Plus Edition von Veeam voraussetzt, kann sie in diesem Projekt nicht angewandt werden.

Wurde im Schritt "Networking" die Option "advanced networking" ausgewählt, so steht der Menüschritt "Isolated Networks" zur Verfügung. Hier werden die isolierten Netzwerke erstellt und einem Produktionsnetzwerk zugeteilt.

Ebenfalls nur dann verfügbar, wenn die Option "advanced networking" aktiviert wurde, ist der Schritt "Network Settings". Hier werden die erstellten, isolierten Netzwerke auf die Adressen des Produktionsnetzwerkes gemappt. Durch dieses Mapping können nun Datenpakete aus dem isolierten Netzwerk heraus zum Produktionsnetzwerk weitergeleitet werden. Um dies zu erreichen, kommt eine virtuelle Network Interface Card (vNIC) für jedes erstellte, isolierte Netzwerk zum Einsatz. Bei dessen Konfiguration muss das entsprechende Netzwerk ausgewählt werden. Anschließend wird die IP-Adresse (samt Subnetzmaske) angegeben, auf die es umgeleitet werden soll.

Zusätzlich kann bei fortgeschrittenen Einstellungen, im nächsten Menüschritt, statisches IP-Adress-mapping konfiguriert werden. Hierzu reichen lediglich die

Auswahl des zu mappenden Netzwerkes und die Angabe der IP im isolierten Netzwerk und einer von außen erreichbaren IP.

Aus Übersichtsgründen kann optional eine Beschreibung der Mapping-Regel angegeben werden.

Somit ist die Einrichtung des virtual Labs abgeschlossen. Nach nochmaliger Überprüfung der Einstellungen können diese mit "Finish" übernommen werden.

# 4.8.4 Einrichtung des "SureBackup"-Jobs

Der SureBackup-Job definiert den Zeitplan für die SureBackup-Tests und startet diese entsprechend der Konfiguration.

Unter "Backup & Replication" befindet sich im Kontextmenü unter "Jobs" der Punkt "SureBackup", unter welchem sich ein SureBackup-Job für beide Hypervisor-Plattformen erstellen lässt.

Bei der Angabe des Namens im ersten Schritt sollte dieser so gewählt werden, dass sich ggf. Rückschlüsse auf die involvierten Application Groups und dem virtual Lab schließen lassen. Alternativ kann dafür auch das "Description"-Field verwendet werden.

Im zweiten Schritt muss das zu startende virtual Lab ausgewählt werden, welches die Tests laut dem Job ausführen soll. Hier werden ebenfalls nochmals Informationen zu der Anzahl der involvierten und derzeit ausgeführten VMs, sowie dem Host und dem spezifizierten Datastore aufgelistet.

Per Klick auf "Next" gelangt man in das Menu "Application Group" in dem die für den Test zu startende Gruppe an Maschinen festgelegt wird. Normalerweise wird die Application-Group nach Abschluss der Tests heruntergefahren. Jedoch lässt sich diese Funktion auch deaktivieren, indem man unter "Keep the application group running once the job completes" einen Haken setzt. Dies ist sinnvoll, wenn zusätzliche Verifizierung oder eine Wiederherstellung einzelner Dateien durch den Nutzer erwünscht ist.

Die Verknüpfung der Tests an einen Backup- oder Replication-Job wird im nächsten Schritt durchgeführt. Über den "Add"-Button können Backup- und Replication-Jobs hinzugefügt werden, welche mithilfe dieses SureBackup-Jobs getestet werden sollen. Dazu muss die Option "Link jobs" aktiviert sein.

Mit "Process simultaneously up to xx VMs" kann die Anzahl an gleichzeitig stattfindenden Tests definiert werden.

Wird die Option "Link jobs" nicht aktiviert und kein Backup oder Replizierung verknüpft, so startet Veeam nur die virtuellen Maschinen der "Application Group" und verifiziert

diese. Damit also die virtuelle Maschine eines Backups getestet wird, muss diese Option aktiviert sein und der entsprechende Job verknüpft werden.

# 4.9 Systemwiederherstellung im Katastrophenfall

# 4.9.1 Manuelle Ausführung eines Replica-Failovers

Im Falle einer Situation, bei der ein Failover eines Replikats sattfinden soll, dieses jedoch nicht automatisch ausgeführt wurde, kann ein schnelles, manuelles Failover durchgeführt werden.

Dazu muss in "Restore Wizard" der Punkt "Failover to replica" gewählt werden.

Im neu geöffneten Assistenten, muss nun lediglich die betroffene VM, der gewünschte Wiederherstellungspunkt und ein Grund hierfür angegeben werden.

Das Failover wird anschließend mit einem Klick auf "Finish" durchgeführt.

# 4.9.2 Vollständige Wiederherstellung eines Backups

Im Falle eines kompletten Ausfalls einer virtuellen Maschine lässt sich diese über ein Backup auf einen früheren Stand zurücksetzen. Dies kann bei Veeam über den "Restore Wizard" bewerkstelligt werden. Hierbei ist der Punkt "Entire VM (including registration)" zu wählen.

Mit "Next" öffnet sich der "Full VM Restore Wizard", bei dem als Erstes die zu widerherzustellende Maschinen auszuwählen sind. Diese können über "Add VM" in die Liste hinzugefügt werden.

Der Wiederherstellungspunkt lässt sich unter "Point…" auswählen.

Danach folgt die Angabe des Wiederherstellungsmodus. Hierbei lässt sich die Sicherung auf einen beliebigen anderen oder ihren originalen Ursprungsort zurückspielen.

Letzteres schaltet die "Quick rollback"-Funktion frei. Mit ihr werden mithilfe von CBT lediglich die geänderten Blöcke der inkrementellen Backups zurückgespielt, anstatt die gesamte, volle Sicherung. Dies ist bei Verlusten oder Fehlern auf Gastbetriebssystems-Ebene zu empfehlen. Wurde die VM auf Hardwareebene beschädigt, sollte diese Option deaktiviert und die gesamte VM wiederhergestellt werden.

Um die Maschine an einen anderen Ort oder mit geänderten Einstellungen zurückzusichern, wählt man die Option "Restore to a new location or with different settings" aus. Quick rollback steht hierbei jedoch nicht mehr zur Verfügung.

In beiden Fällen lässt sich zur Wiederherstellung ein beliebiger Backup-Proxy mit dem Link "Pick proxy to use" bestimmen. Wird kein Proxy explizit angegeben, wählt Veeam automatisch einen angemessenen Proxy aus.

Bei Wiederherstellung an einen anderen Ort müssen nun noch die nächsten fünf Schritte durchlaufen werden. Der erste dieser Schritte ist die Auswahl eines neuen Hosts, auf welchem die VM ausgeführt werden soll. Dazu muss in der Liste jeweils das entsprechende Backup (bzw. die VM) ausgewählt werden und über einen Klick auf "Host" ein ESX(i)-Host zugewiesen werden. Diese Einstellung lässt sich auch für mehrere Maschinen gleichzeitig vornehmen, indem man mehrere Maschinen gleichzeitig markiert, bevor die Zuweisung über "Host" erfolgt.

Analog zum Verfahren der Host-Zuweisung erfolgt nun die Zuweisung der Maschinen zu jeweiligen Ressourcen-Pools. Das Verfahren ist das gleiche, wobei hier anstatt eines "Host"-Buttons ein "Pool"-Button zur Verwendung bereitsteht.

Der "Datastore"-Schritt verlangt anschließend die Auswahl eines Datastores für jede einzelne VM. Hierbei lassen sich diese über "Datastore…" zuweisen. Über den Button "Disk Type…" lässt sich bestimmen, ob thick disks oder thin disks verwendet werden sollen. Thick disks belegen auf dem physischen Host den gesamten zugewiesenen Speicher, wohingegen Thin disks nur so viel Speicher belegen, wie gerade für den Betrieb der VM nötig ist. Bei letzterem wird Speicher bei weiterer Belegung der virtuellen Festplatte erst dynamisch allokiert. Damit kommt es nicht zur Speicherverschwendung auf dem physikalischen Speicher durch ungenutzte Kapazitäten der virtuellen Platte.

Im nächsten Schritt lässt sich der Name und Ordner der neu anzulegenden VMs definieren. Dies geschieht über die Auswahl der jeweiligen VM und anschließendem Klick auf "New Name" bzw. Folder. Im "New Name"-Menü lässt sich neben den Namen auch ein nutzerdefinierter Suffix oder Präfix definieren.

Um das Netzwerk der neuen virtuellen Maschine an das Produktionsnetzwerk zu binden, kann nun ein Netzwerk-Mapping vorgenommen werden. Mit Auswahl der VMs und einem Klick auf "Network…" lassen sich das Ziel und Quellnetzwerk jeweils festlegen. Soll eine VM mit gar keinem Netzwerk verbunden werden, genügt die Betätigung der "Disconnected"-Schaltfläche.

Der Schritt "Restore" ist verfügbar unabhängig davon, ob die gewählte Sicherung an ihren Ursprungsort zurückgesetzt werden soll, oder nicht. Hierbei ist lediglich ein Grund für die Wiederherstellung, für spätere Referenz, anzugeben.

Als letztes erfolgt eine zusammenfassende Übersicht über die vorgenommenen Einstellungen. Diese können per "Finish" übernommen werden.

# 4.9.3 Wiederherstellung einzelner Dateien

Das Zurücksichern einzelner Dateien oder auch "File Level Item Recovery" (FLIR), wird stets dann eingesetzt, wenn nicht das gesamte Backup, sondern nur ein gewisser Teil dessen auf Dateiebene zurückgespielt werden soll.

Diese Funktion ist für sämtliche Betriebssysteme anwendbar, erlaubt es jedoch Dateien nur an ihren ursprünglichen Ort, oder dem Veeam-Server zu speichern.

Diese Funktion ist Teil des Recovery-Assistenten und lässt sich daher über diesem, mit einem Klick auf "Guest files (Windows)", für Windows-basierte Maschinen, oder "Guest files (other OS)", für andere Betriebssysteme nutzen.

Zuerst steht hierbei die Auswahl der virtuellen Maschine bevor, dessen Daten wiederhergestellt werden sollen.

In den anschließenden Schritten müssen der Wiederherstellungspunkt ausgewählt und ein Wiederherstellungsgrund angegeben werden.

Nach Fertigstellung öffnet sich ein visuell an den Windows-Explorer angelehnter Dateibrowser, in dem das Dateisystem der Maschine durchsucht und erwünschte Dateien zurückgesichert werden können. Mit einem Rechtsklick auf einen Ordner oder einer Datei können diese per "Restore" an ihren ursprünglichen Ort zurückkopiert werden. Mit "Copy To…" hingegen lässt sich die Datei auf der Maschine des Veeam-Servers speichern.

Seit Version 8 von VBR lassen sich die Dateien auch über "Restore" → "Keep" mit einem automatisch angehangenen "RESTORE"-Präfix an ihren originalen Speicherort sichern. Dabei wird jedoch die derzeitige Datei auf dem Zielort nicht überschrieben.

Zum Schreiben der Datei auf den Zielort, nutzt Veeam automatisch den Account, welcher im jeweiligen Backup-Job angegeben wurde. Hat dieser keine ausreichenden Berechtigungen, so wird der Nutzer zur Angabe der korrekten Nutzerkontendaten aufgefordert.

## 4.9.4 Wiederherstellung einer Bandsicherung

Eine Bandsicherung lässt sich entweder auf ein Repository zurücksichern, oder kann auch direkt eine ausgefallene VM ersetzen. Die ersten Schritte sind in beiden Fällen sehr ähnlich.

Hierzu muss wieder der "Restore Wizard" aufgerufen werden. Für die Wiederherstellung eines Backups in einem Repository wählt man die Option "Restore backup from tape to repository". Möchte man eine VM direkt wiederherstellen nutzt man "Restore entire VM" unter "Tape".

In beiden Fällen sind in den ersten beiden Schritten jeweils das Backup und über "Point…" der Wiederherstellungszeitpunkt zu wählen.

Für den Fall der Wiederherstellung ins Repository lässt sich im nächsten Schritt das jeweilige Ziel auswählen. Das Backup kann dabei auf ein Repository, lokal auf dem Computer oder einem verbundenen Speicher im Netzwerk zurückgesichert werden. Wurde das Ziel ausgewählt kann die Rücksicherung mit "Next" und anschließendem "Finish" gestartet werden.

Für die Wiederherstellung der virtuellen Maschine muss lediglich das Ziel-Repository ausgewählt werden. Anschließend erfolgen die restlichen Schritte eines "Full VM Restores". Die Vorgehensweise ist dieselbe wie bei der Wiederherstellung einer gesamten VM (siehe 4.9.2.).

#### 4.9.5 Instant-VM-Recovery

#### 4.9.5.1 Ausführung einer Instant-VM-Recovery

Die Instant-VM-Recovery ist die Funktion, die beim Ausfall von systemkritischen Komponenten verwendet werden kann, um schnell einen Ersatz via Backup zur Verfügung zu stellen.

Anstatt hier die Daten aus einem Backup auf den Zielhost zu schreiben, wird die Maschine direkt aus dem Backup heraus auf einem designierten ESXi-Host registriert und gestartet. Hierbei kommt Veeams vPower-Technologie zum Einsatz.

Um solch eine Wiederherstellung durchzuführen wird der Recovery-Assistent gestartet. Im "Home"-Tab lässt sich dieser mit einem Klick auf "Restore" öffnen. Daraufhin wählt man die Option "Instant VM Recovery" an und gelangt mit einem Klick auf "Next" in das Setup für "Instant Recovery".

Nachdem im ersten Schritt die wiederherzustellende Maschine ausgewählt wurde, muss im nächsten Punkt der Wiederherstellungszeitpunkt bestimmt werden. Hierbei werden in der Liste alle zurzeit zur Verfügung stehenden Backups, samt ihrer Erstellungszeit und des Typs angezeigt.

Wurde ein bestimmtes Backup gewählt gilt es nun, die Methode des Rückspiel-Prozesses zu spezifizieren. Es stehen dazu zwei Optionen zur Verfügung.

Einerseits lässt sich die VM an ihrem originalen Standort, samt ihrer originalen Einstellungen wiederherstellen. Diese Methode eignet sich eher für zeitkritische Wiederherstellungen, da man hierbei die Konfigurationsschritte "Destination" und "Datastore" überspringt.

Um die Maschine jedoch an einem anderen Host oder mit modifizierten Einstellungen wiederherzustellen, kann man andererseits die zweite Option wählen. Bei ihrer Auswahl stehen zwei weitere Schritte zur Konfiguration zur Verfügung.

Der erste dieser beiden Schritte, "Destination", bestimmt über den Zielort, an dem die VM wiederhergestellt werden soll. Dazu müssen ein geeigneter Server, ein Ressourcen-Pool sowie ein neuer Name für die anzulegende Maschine bestimmt werden.

Wurde dies getan, muss im nächsten Schritt ein Datastore für das Speichern von "Redo Logs", ähnlich wie beim Test der Sicherungen via SureBackup, angegeben werden. Da in diesem Falle zu erwarten ist, dass die VM länger im laufenden Betrieb verbleibt als bei SureBackup-Verifizierungen, sollte hier insbesondere Acht auf den noch verfügbaren Speicher gegeben werden.

Um den Grund dieser Aktion später nachvollziehen zu können, kann im Schritt "Restore Reason" ein Grund zur Wiederherstellung angegeben werden. Dieser sollte möglichst kurz und aussagekräftig gewählt werden.

Der letzte Schritt bietet noch zwei Optionen an, welche es dem Programm erlauben die VM automatisch hochzufahren und mit dem Netzwerk zu verbinden. Sollte eine, oder beide dieser Funktionen nicht erwünscht sein, können diese schlichtweg mit einem Entfernen des Hakens deaktiviert werden.

Mit Vollendung dieses Schrittes wird die virtuelle Maschine nun auf dem angegebenen Host registriert und (soweit angegeben) gestartet. Damit erscheint nun diese Maschine in der Liste unter "Instant Recovery". Zu beachten ist hierbei, dass sie damit noch nicht in das Produktionssystem integriert wurde, sondern als temporärer Ersatz in Hintergrund betrieben wird.

Mit einem Rechtsklick auf die VM in der Liste lässt sich diese über die Punkte "Migrate to production" in das System migrieren und mit "Stop publishing" stoppen und löschen.

# 4.9.6 Migration einer Instant-VM in die Produktion

Beim Versuch der Migration startet Veeam die "Quick Migration". Mit ihr kann eine über "Instant-Recovery" erstellte VM in das Produktionssystem integriert werden. Sie kann

auch verwendet werden, um eine virtuelle Maschine auf einen anderen Host umzuziehen.

Im ersten Schritt müssen die zu migrierenden Maschinen ausgewählt werden.

Der darauffolgende Punkt befasst sich mit der Auswahl des Migrationsziels. Hierbei muss in erster Linie der Host bzw. der Cluster ausgewählt werden, auf den die Maschinen registriert werden sollen. Als zweites müssen der Ressourcen-Pool, VM-Ordner sowie der Datastore festgelegt werden. Dies kann für alle Maschinen gleich oder unterschiedlich, per Klick auf die jeweiligen "Pick xx"-Buttons eingestellt werden.

Im letzten Schritt muss schließlich ein Quell- und ein Ziel-Backup-Proxy spezifiziert werden, um den Transfer der VM-Daten vom jetzigen Standort der VM zu ihrem Zielort zu bewerkstelligen. Verbleibt die zu migrierende Maschine an ihrem Standort (z.B. nach einer Instant-VM-Recovery), so kann als Quell- und Ziel-Proxy derselbe Backup-Proxy eingetragen werden.

Nach dieser Einstellung besteht nun noch die Wahl der Migrationsmethode. Standardmäßig wird Veeam Quick Migration verwendet, um die Migration durchzuführen. Wird die Option "Force Veeam quick migration" jedoch deaktiviert, versucht das Programm VMotion von VMware für diesen Prozess zu verwenden. Sollte dies jedoch nicht möglich sein (aufgrund einer z.B. fehlenden VMware vSphere Lizenz), wird auf native Methoden zurückgegriffen.

Im letzten Schritt kann der Vorgang gestartet werden. Wurde Veeams Quick Migration verwendet, kann die Quellmaschine automatisch (nach erfolgreichem Abschluss) durch Aktivierung von "Delete source VM files uppon successful quick migration" gelöscht werden. Anderenfalls muss dies nachgeholt werden, wenn es nicht bereits von den alternativen Methoden selbst durchgeführt wurde.

# 5 Schlusswort

Mit der hier vorliegenden Architektur bietet "Veeam Backup & Replication" ein angemessenes Sicherungssystem für sämtliche Bedürfnisse der Sicherung an.

Da die konkrete Implementierung leider noch nicht vorgenommen wurde, lassen sich bis jetzt nur Vermutungen zu einer möglichen, erfolgreichen Implementierung des Systems vornehmen.

Dennoch bleibt zu sagen, dass VBR aufgrund seiner Flexibilität eine sehr hohe Wahrscheinlichkeit für den Erfolg des Projektes bietet. Dies gilt nicht nur für die initiale Einführung, sondern auch für eventuelle Erweiterungen der IT-Struktur in der Zukunft.

# Literaturverzeichnis

# **Literaturquellen (PDF)**

# "Fibre Channel Fundamentals", Tom Weimer

Aufgerufen am: 20. Juli 2015

Quelle: <a href="http://www.unylogix.com/data\_storage/raid\_san/PDFs/White\_Pa">http://www.unylogix.com/data\_storage/raid\_san/PDFs/White\_Pa</a>

per\_Fibre\_Channel\_Fundamentals.pdf

# "Handbuch für das Backup virtueller Maschinen", VMware Inc.

Aufgerufen am: 20. Juli 2015

Quelle: <a href="http://tu-">http://tu-</a>

<u>dresden.de/die\_tu\_dresden/zentrale\_einrichtungen/zih/dienste/a\_rbeitsumgebung/datensicherung/dateien/vi3\_vm\_backup\_de.pdf</u>

# "Sieben Fragen, die Sie sich vor dem Kauf einer VM-Sicherungslösung stellen sollten", Quantum Corp.

Aufgerufen am: 06. Juli 2015 Stand des Dokuments: Januar 2012

Quelle: <a href="https://iq.quantum.com/exLink.asp?7912688OL18N53I44">https://iq.quantum.com/exLink.asp?7912688OL18N53I44</a>

<u>644656</u>

#### Online-Quellen

#### Backupkonzepte

- <a href="http://www.ee-solutions.de/backup-loesungen/backupkonzepte.html">http://www.ee-solutions.de/backup-loesungen/backupkonzepte.html</a>
- http://www.msxfaq.de/konzepte/backupkonzepte.htm
- https://de.wikipedia.org/wiki/Datensicherung
- <a href="http://www.windowspro.de/wolfgang-sommergut/vergleich-backup-strategien-fuer-virtuelle-maschinen">http://www.windowspro.de/wolfgang-sommergut/vergleich-backup-strategien-fuer-virtuelle-maschinen</a>

#### Fibre Channel / SCSI

- http://www.tecchannel.de/storage/san/465690/fibre\_channel\_funktion\_und\_techn ologie/index.html
- http://www.itwissen.info/definition/lexikon/Fibre-Channel-FC-fibre-channel.html

#### **Veeam Backup & Replication v8**

- http://www.veeam.com
  - o <a href="http://www.veeam.com/vmware-vsphere-solutions.html">http://www.veeam.com/vmware-vsphere-solutions.html</a>
  - http://www.veeam.com/buy-veeam-backup-replication.html
  - https://www.veeam.com/faq.html
  - o <a href="https://www.veeam.com/backup-licensing-faq.html">https://www.veeam.com/backup-licensing-faq.html</a>
  - http://helpcenter.veeam.com/backup/80/vsphere/

# Acronis Backup für VMware

- http://www.acronis.com
  - http://www.acronis.com/de-de/business/overview/compare-products/
  - <a href="http://www.acronis.com/de-de/business/backup/virtual-machine/">http://www.acronis.com/de-de/business/backup/virtual-machine/</a>
  - http://www.acronis.com/de-de/business/licensing-faq/
  - http://www.acronis.com/de-de/support/documentation/
    - http://www.acronis.com/de-de/download/docs/avmp9/userguide/

#### **Storagecraft Shadow Protect 5**

- https://buy.storagecraft.com/
  - https://buy.storagecraft.com/StorageCraft-ShadowProtect-Virtual-Server-Bundles-C33.aspx
- https://www.storagecraft.com/
  - https://www.storagecraft.com/de/produkte/shadowprotect-virtual
  - https://www.storagecraft.com/support/node/12798

# Eidesstaatliche Erklärung

| Ich, Ke | Kevin Haberland, erkläre hiermit ehrenwörtlic   | ch, dass:                          |
|---------|---|------------------------------------|
| 1.      | . ich meine Bachelor-Thesis mit dem Thema   | a                                  |
|         | "Ein Datensicherungssystem für die virtuel<br>Berufsakademie Glauchau"  | le Umgebung im Rechenzentrum de    |
|         | ohne fremde Hilfe angefertigt habe,   |                                    |
| 2.      | . dass ich die Übernahme wörtlicher Z<br>Verwendung der Gedanken anderer Auto<br>innerhalb der Arbeit gekennzeichnet habe | oren an den entsprechenden Steller |
| 3.      | . dass ich meine Bachelor-Thesis bei keine  | r anderen Prüfung vorgelegt habe.  |
| Ich bir | in mir bewusst, dass eine falsche Erklärung   | rechtliche Folgen haben wird.      |
|         |   |                                    |
|         |   |                                    |
| Ort, E  | Datum Unte  | rschrift                           |

#### These

Die Auswahl des Programmes "Veeam Backup & Replication v8" erfüllt die Anforderungen der Berufsakademie Glauchau und eignet sich somit für die Sicherung der dort vorhandenen, virtuelle Infrastruktur.

Wie sich anhand des Vergleiches von VBR mit anderen Sicherungsprogrammen gezeigt hat, erfüllt die Software nicht nur die Anforderungen zur möglichen Implementierung in das System, sondern auch den gestellten Sicherungsanforderungen.

Backups lassen sich sowohl auf dem Bandlaufwerk, als auch auf Festplatte speichern und die Architektur ist mit der Infrastruktur vollkommen kompatibel.

Mit den zur Verfügung stehenden Mitteln und Konfigurationsmöglichkeiten bietet Veeam nicht nur eine Möglichkeit der sicheren Erstellung von Backups, sondern ebenfalls Raum für eine Erweiterung der bestehenden Infrastruktur durch mögliche Replikationen oder Sicherungen über WAN.