KAPITEL 1

Backup im Allgemeinen

Backup und Recovery sind mit die wichtigsten Aufgaben, die bei einer produktiven Umgebung anfallen. Hierbei spielt es keine Rolle, ob es sich um die virtuelle Welt handelt oder ob physische Systeme gesichert werden müssen. Auch eine Probewiederherstellung sollte zu den regelmäßigen Aufgaben eines jeden Administrators gehören.

Leider zeigt sich in der Praxis, dass dieses wichtige Thema im produktiven Bereich nur allzu oft vernachlässigt wird. Einige Betriebe sind sogar vom Gesetzgeber her verpflichtet, Sicherungen einzurichten und bei Anfrage auch nachzuweisen, aber dieser Umstand ist vielen EDV-Mitarbeitern häufig unbekannt. Außerdem müssen einige Daten noch nach zehn oder gar dreißig Jahren auf Verlangen abrufbar sein.

Im Falle eines Falles muss man sich auf ein Backup verlassen können, und man sollte dieses auch regelmäßig durch ein Recovery überprüfen. Nur wer das oft übt, wird im Katastrophenfall oder in Stresssituationen richtig handeln und einen größeren Datenverlust zu verhindern wissen. In dieser Dokumentation finden Sie Erläuterungen zu allen wichtigen Vorgehens- und Hinweisen zu deren richtiger Verwendung.

Backup-Unterschiede zwischen den Welten

Wenn Sie Ihre physischen Maschinen mittels Agenten im Betriebssystem bisher auf Band oder Platte gesichert haben, können Sie das auch weiterhin tun, u. a. mit dieser Software. In der virtuellen Welt gibt es aber andere Möglichkeiten, die einem die Wiederherstellung eines Rechners deutlich erleichtern. Die bloßen Daten eines Rechners kann man erst wieder in eine fertig aufgesetzte Maschine mit installiertem Backup-Agenten zurückspielen. Welche Hardware und Treiber vorher in der physischen oder virtuellen Maschine waren, lässt sich nachträglich nicht immer zweifelsfrei bestimmen. Bei einer virtuellen Maschine (VM) können aber alle beteiligten Dateien auf ein Volume des Hypervisors zurückkopiert werden, und die Maschine ist sofort wieder einsatzbereit – ohne Umwege über eine Neuinstallation des Betriebssystems und Installation einer Backup-Software bzw. eines Agenten.

In letzter Zeit haben viele Hersteller recht gute Produkte für die Sicherung und Wiederherstellung für virtuelle Maschinen programmiert. Dabei gibt es sowohl kostenlose Produkte als auch Kaufversionen mit den unterschiedlichsten Ansätzen. Erfahrungen können Sie meist über voll funktionierende, zeitlich begrenzte Versionen sammeln und sich dann für ein Produkt entscheiden. Schauen Sie sich z.B. die Möglichkeiten an, die die Firmen Quest Software (ehemals Vizioncore, jetzt Dell, *www.quest.com/virtualization*), Veeam (*www.veeam.com/de*), Broadcom (ehemals Symantic Backup, *www.broadcom.com*) oder auch Acronis (*www.acronis.de*) bieten.

Die Ansätze der einzelnen Produkte sind zwar zum Teil sehr unterschiedlich, wichtig ist aber nur, dass Sie eine Software finden, mit der Sie einfach, schnell und unkompliziert diese Aufgabe erledigen können.

Sicherung des Hosts

Die Meinungen beim Backup eines ESXi- oder Hyper-V-Servers gehen weit auseinander. Muss der Host überhaupt gesichert werden, oder setzt man ihn einfach neu auf? Beides ist möglich!

Da beim neu installierbaren Hypervisor von VMware (ESXi) kein Betriebssystem mehr als Grundlage vorhanden ist, schlagen die üblichen Backup-Methoden wie bei Linux fehl. Welche Möglichkeiten gibt es dann überhaupt? Mit dem Befehl vicfg-cfgbackup.pl über vCLI o.Ä. können die wichtigsten Konfigurationsdateien des Hosts gesichert und wieder zurückgespielt werden. Bei der kostenlosen Version schlägt das Zurückspielen aber fehl, weil der Host sich nach dem Einspielen der Lizenz im schreibgeschützten Modus befindet bzw. die sonst üblichen Softwareschnittstellen geschlossen sind. Setzt man einen neuen ESXi auf, trägt man die Lizenz einfach erst nach dem Zurückspielen der Sicherung ein. Natürlich kann die Konfiguration aber auch per Hand nach einer Neuinstallation wieder eingepflegt werden. Probleme gibt es dann aber gegebenenfalls bei der neuen Identität, die den Zugriff auf einen externen Storage, z.B. wegen eines anderen IQN (iSCSI Qualified Name), verhindern kann.

Eine weitere Möglichkeit besteht darin, den Befehl vm-support aufzurufen. Dieser sammelt unter anderem auch die komplette Konfiguration. Die anschließend erstellte gepackte Datei kopiert man sich auf einen beliebigen Datenträger. Muss der Host neu installiert werden, so entfernt man aus dem Paket die nicht benötigten Verzeichnisse wie z.B. /proc und /vmfs und kopiert die restlichen Daten in die Originalverzeichnisse zurück. Wenn man anschließend den Server neu startet, ist die komplette Konfiguration wiederhergestellt.

Hat man ein Fibre-Channel- oder iSCSI-SAN, so kann man die Installation des Hosts auch dort vornehmen. Über zusätzliche Funktionen des Storage können natürlich auch diese Daten gesichert werden. Einen neuen Server lässt man ein-

fach vom SAN booten und braucht sich keinerlei weitere Gedanken über das Backup zu machen.

Bootet man den Host von einem USB-Stick oder einer Flash-Speicherkarte, so kann man diesen auch klonen. Das funktioniert auch im laufenden Betrieb, da der Host alle Daten im RAM vorhält.

Bei Hyper-V von Microsoft kann der Server (von 2008 R2 SP1 bis einschließlich 2016) direkt über Veeam Backup & Replication (B&R) gesichert werden.

Sicherung der VMs

Wie schon eingangs erwähnt, kann man bei der Sicherung von virtuellen Maschinen genauso verfahren wie bei physischen Systemen. Besser ist es jedoch, wenn eine Backup-Software die Dateien der VM von der jeweiligen Partition sichert. Dazu gehören bei VMware die Festplattendateien (*.vmdk und *-flat.vmdk), die Konfigurationsdateien (*.vmx und *.vmxf) sowie gegebenenfalls das BIOS (*.nvram, nur notwendig, wenn BIOS-Einstellungen geändert wurden) und bei Hyper-V die Konfigurationsdateien (XML bis 2008, ab 2016 binär mit Endung VMCX) sowie die Festplatte VHD oder AVHD. Haben Sie aktive Snapshots, müssen Sie diese ebenfalls berücksichtigen und zusätzlich die Snapshot-Datei (*.vmsd bzw. *.vsv) sichern. Auf jeden Fall ist es besser, wenn Sie die Snapshots vor der Sicherung entfernen bzw. übernehmen/löschen. Ab Windows Server 2016 spricht man von VM Checkpoints statt Snapshots, da sich hier etwas geändert hat. Der Einfachheit halber bleibe ich bei dem Terminus »Snapshots«.

Die meisten Softwarelösungen für diese Aufgabe machen vor dem Backup einen Snapshot der Maschine, weil dann die Festplattendatei ohne Probleme kopiert werden kann. Ist der Vorgang abgeschlossen, wird der dann aktuelle Zustand übernommen (der Snapshot wird gelöscht).

Achten Sie unbedingt auf die korrekte Rücknahme der Snapshots. Bei Problemen kann das jeweilige Volume schnell volllaufen. Schuld daran ist manchmal die VSS-Komponente (Volume Shadowcopy Service) in den VMware Tools. Ändern Sie dann die Einstellungen der Tools und wählen Sie VSS ab. Manchmal ist auch der Eintrag »`disk.EnableUUID = "TRUE"`« in der *.vmx-Datei schuld. Ändern Sie den Eintrag dann auf »FALSE«. Bei Microsoft Hyper-V Host unter 2008 R2 und früher lässt sich der VSS-Provider pro Volume einstellen. Sie können aber auch in der Jobkonfiguration das VSS abschalten.

Die Backup-Lösung für virtuelle Maschinen unter VMware und Microsoft Hyper-V namens Veeam Backup & Replication liegt nunmehr in der Version 10 vor und macht wie vorher einen sehr guten und stabilen Eindruck.

Dieses Produkt wurde in der Vergangenheit mehrfach ausgezeichnet, z.B. als Produkt des Jahres und »Best of vmworld«.

Ähnlich wie andere Datensicherungsanwendungen für VMs unterstützt Backup & Replication einen deduplizierten Speicher sowie eine Kompression vor der Übertragung auf das Sicherungsmedium, was die Netzwerkbelastung und den Storage-Bedarf deutlich verringert.

Eine sehr interessante Lösung ist die integrierte Near-CDP-Funktion (Near-Continuous Data Protection). Damit werden Änderungen an virtuellen Maschinen erkannt und die vorher erstellten Images (Replikate) laufend aktualisiert.

VMs können im Katastrophenfall direkt über den Datensicherungsspeicher gestartet werden – ein Zurückspielen der gesicherten VM auf einen schnelleren Storage kann dann später erfolgen. Auch lässt sich eine Art Sandbox (SureBackup) nutzen, um in einer abgeschotteten, gesicherten Umgebung ein Backup mit mehreren Maschinen zu überprüfen.

Selbstverständlich können auch über das File Level Restore einzelne Dateien aus der Sicherung wiederhergestellt und mittlerweile auch physische Windows- und Linux-Maschinen gesichert werden. Diese und viele weitere Produktmerkmale werden nachfolgend besprochen.

Veeam Software

Die Firma Veeam Software Group GmbH mit Hauptsitz in Baar (Schweiz) entwickelt Produkte für Datensicherung und Management in virtuellen Umgebungen. Sie wurde im Jahre 2006 gegründet, war zwischenzeitlich eine AG und wurde im Januar 2020 von dem amerikanischen Unternehmen Insight Partners übernommen. Die ersten vorgestellten Produkte waren Veeam Monitor und Veeam Reporter, die mittlerweile Bestandteil von Veeam ONE sind.

Das kostenlos angebotene Tool FASTSCP kam 2007 auf den Markt und ist jetzt die Grundlage der Datensicherung Backup & Replication, welche im Jahre 2008 erstmals angeboten wurde.

Die Firma bietet noch weitere interessante Tools an, über die Sie sich Informationen auf deren Website ansehen können.

Systemvoraussetzungen

Veeam Backup & Replication (B&R) kann ab VMware vSphere 5.5 bis zur aktuellen Version und für ESXi Hosts (ab 5.5) eingesetzt werden. Der freie, kostenlose ESXi Host wird nicht unterstützt. Bei Hyper-V werden sogar der freie und der Nano Server ab 2008 R2 SP1 unterstützt. Die Software wird als Dienst auf einem physischen oder virtuellen 64-Bit-Windows-Betriebssystem ab Windows 7 SP1 bis Windows Server 2019 installiert.

Als Hardwarevoraussetzung gilt eine 64-Bit-CPU mit mindestens 4GB RAM plus jeweils 500 MB für jeden gleichzeitig ausgeführten Backup-Job. Auf der Festplatte

werden 15 GB für die Installation und für den Katalog jeweils 10 GB für je 100 VMs benötigt. Netzwerktechnisch sollte es mindestens ein 1-GBit-Ethernet-Adapter sein und für eine WAN-Strecke minimal 1 MBit/s.

Ein Backup-Server (BS) kann bis zu 10.000 VMs sichern. Als Datenbank sollte es dann ein externer MS-SQL-Server 2014 (oder neuer) oder für bis zu 350 VMs auch die SQL-Express-Variante sein. Konfigurieren Sie den BS mit einem Sockel und mindestens vier Kernen sowie ausreichend RAM (siehe obigen Abschnitt), wenn es sich um eine virtuelle Maschine handelt. Beachten Sie dabei auch die physische Struktur Ihres Hypervisors.

Nutzen Sie für Ihre VMs für Windows 2012 R2 (oder höher) die interne Deduplizierung, sollten Sie Veeam Backup & Replication ebenfalls auf diesem Betriebssystem installieren und das Feature »Data Deduplication« aktivieren, sonst kann es bei der Dateiwiederherstellung dieser VMs zu Problemen kommen.

Installieren Sie den Backup-Server möglichst nicht auf Produktionsmaschinen wie Microsoft Hyper-V Server, DCs, Exchange- und andere besondere Anwendungsserver.

Unterstützung von VMs:

- Alle Typen und Versionen der VMs inkl. 62-TByte-vmdk-Festplatten werden unterstützt. Bei Hyper-V die Hardwareversion 5.0, 8.0 und 9.0, Generation 1 und 2, VHDX-Festplatten bis 64 TB.
- »Passthrough«-, RDM-Festplatten, unabhängige Disks (independent) und im OS angebundene iSCSI-Festplatten werden nicht gesichert. Ebenfalls werden gemountete Netzwerkfreigaben und externe Mountpoints nicht berücksichtigt.
- Alle Betriebssysteme in den VMware VMs und alle von Hyper-V gelisteten werden unterstützt.
- Die Veeam Explorer für bestimmte Anwendungen benötigen das Microsoft VSS, weswegen die Applikationen erst ab Windows Server 2008 berücksichtigt werden können. Windows Server 2003 und Nano Server werden nicht mehr unterstützt.
- Es sollten möglichst die neuesten SP (Service Packs) und Patches im Backup-Server installiert sein.
- Die Hyper-V-Integrationskomponenten sowie die VMware Tools müssen für Application Aware Processing und File Level Restore bei Windows und für das SureBackup installiert sein.

Die aktualisierte Veeam Backup & Replication Console, über die man aus der Ferne übers Netzwerk auf die Sicherungsumgebung zugreifen kann, braucht etwas weniger als die oben beschriebenen Werte. Ein 64-Bit-Betriebssystem ab Windows 7 SP1 muss es aber schon sein.

Lizenzierung

Sie sollten während der Installation des BS bereits Ihren Lizenz-Key angeben, sonst wird die Software in der kostenlosen Version (Community Edition) installiert. Das nachträgliche Einspielen oder Ändern der Lizenz ist zwar ohne Probleme möglich, jedoch müssten dann diverse Funktionen nachträglich manuell aktiviert werden.

Lizenziert wird hier für die VMs entweder pro CPU-Sockel der beteiligten Hosts oder pro Instanz, bei physischen Windows- oder Linux-Maschinen pro Server bzw. Workstation und jeweils ein oder drei Jahre Support und Subscription. Eine Verlängerungslizenz ist für deutlich geringere Kosten erhältlich. Zielhosts (für die Replikation oder Migration) brauchen nicht lizenziert zu werden. Eine 30-Tage-Testversion kann von der Internetseite *www.veeam.com/de* heruntergeladen werden. Sockellizenzen und Instanzen können auch kombiniert und gleichzeitig eingesetzt werden.

Pro Sockel

Dieses ist die alte Art der Lizenzierung und kann auch weiter genutzt werden. Dabei wird für jeden Prozessorsockel des Hypervisors (Microsoft oder VMware) je eine Lizenz benötigt. Wie viele virtuelle Maschinen auf den Hosts liegen und gesichert werden, spielt dabei keine Rolle. Zusätzlich werden bis zu sechs Instanzen dazugegeben, um z. B. physische Maschinen sichern zu können. Haben Sie nur vier Sockel der Hosts lizenziert, bekommen Sie auch nur vier Instanzen dazu.

Die gekauften Lizenzen werden automatisch den jeweiligen Hosts zugewiesen, sobald ein Sicherungsjob auf den Hypervisor verweist, auf dem die zu sichernde Maschine liegt. Das manuelle Eintragen eines Hosts zu der Liste ist nicht nötig und auch nicht möglich. Um nicht mehr benötigte Hosts von den zugewiesenen Lizenzen zu lösen und diese zum Beispiel einem neuen Host zuzuweisen, klicken Sie in der Oberfläche im Menü auf »Help – License«. In dem folgenden Fenster klicken Sie auf die Schaltfläche »Licensed Hosts«, dann werden die Server gelistet, denen eine Lizenz zugewiesen wurde. Klicken Sie den nicht mehr benötigten Host an und dann auf die Schaltfläche »Revoke«.

Pro Instanz

Veeam spricht hier von der universellen Lizenz (Veeam Universal Licensing), bei der jede Maschine, egal ob physisch oder virtuell, eine Lizenz benötigt. Darin enthalten sind auch Cloud-Maschinen, und der Umfang der Funktionen entspricht der Version Enterprise Plus.

Produkteditionen

Veeam Backup & Replication gibt es – zuzüglich der freien und der Essentials-Version – in drei verschiedenen Editionen: Standard, Enterprise und Enterprise Plus, die alle aus einer Installationsroutine kommen. Diese bieten natürlich unterschiedliche Funktionen, wie aus der folgenden (von Veeam übernommenen) Tabelle 1-1 ersichtlich ist.

Tabelle 1-1: Funktionen der Editionen

Veeam Backup & Replication	Community	Standard	Enterprise	Enterprise Plus
Backup				
Applikationskonsistente, imagebasierte Backups	ja	ja	ja	ja
VeeamZIP™	ja	ja	ja	ja
NAS-Backup	teilweise	teilweise	teilweise	ja
Veeam Cloud Tier			ja	ja
Proxy für die Interaktion mit Gastsystemen in ROBO-Umgebungen			ja	ja
Backup I/O Control			teilweise	ja
Backups aus Storage-Snapshots (1)				ja
Orchestrierung der Snapshots von Primärspeichersystemen (1)	ja	ja	ja	ja
Unterstützung von Nutanix AHV v2 Proxy	ja	ja	ja	ja
Speichern von Backups				
Integrierte Deduplizierung, Komprimierung und integrierter Ausschluss von Swap-Dateien	ja	ja	ja	ja
BitLooker™ und dateiselektive Verarbeitung auf Image-Ebene	ja	ja	ja	ja
Backup Copy Jobs	ja	ja	ja	ja
End-to-End-Verschlüsselung	teilweise	teilweise	ja	ja
Native Unterstützung von Bandsicherungen	teilweise	teilweise	teilweise	
Veeam Cloud Connect Backup		ja	ja	ja
Proxy-Affinität			ja	ja
Backup-Dateien pro VM für deduplizierenden Storage			ja	ja
Scale-out Backup Repository™			teilweise	ja
Integrierte WAN-Beschleunigung			teilweise	ja
Veeam-Plug-in für Oracle RMAN und SAP HANA				ja
Replikation				
Imagebasierte VM-Replikation	ja	ja	ja	ja
Unterstütztes Failover und Failback	ja	ja	ja	ja
Replikation aus Backups	ja	ja	ja	ja
Geplantes Failover	ja	ja	ja	ja
Veeam Cloud Connect Replication		ja	ja	ja
1-Click Failover-Orchestrierung			ja	ja

Tabelle 1-1: Funktionen der Editionen (Fortsetzung)

Veeam Backup & Replication	Community	Standard	Enterprise	Enterprise Plus
WIEDERHERSTELLUNG				
Wiederherstellung vollständiger VMs				
Vollständige Wiederherstellung einer VM	ja	ja	ja	ja
Instant VM Recovery®	ja	ja	ja	ja
Wiederherstellung von VM-Dateien und virtuellen Festplatten	ja	ja	ja	ja
Direct Restore to AWS, Microsoft Azure, Azure Stack	ja	ja	ja	ja
Wiederherstellung auf Dateiebene				
Instant File-Level Recovery	ja	ja	ja	ja
Wiederherstellung auf Objektebene				
Veeam Explorer™ for Storage Snapshots (1)	ja	ja	ja	ja
Veeam Explorer for Microsoft Active Directory	teilweise	teilweise	ja	ja
Veeam Explorer for Microsoft Exchange	teilweise	teilweise	ja	ja
Veeam Explorer for Microsoft SQL Server	teilweise	teilweise	ja	ja
Veeam Explorer for Microsoft SharePoint	teilweise	teilweise	ja	ja
Veeam Explorer for Oracle			ja	ja
Self-Service				
Portal für Helpdesk-Mitarbeiter für 1-Click Restore von Dateien und VMs			ja	ja
Portal für Helpdesk-Mitarbeiter für die Wiederherstellung von Microsoft-Exchange-Objekten			ja	ja
Datenbankwiederherstellungsportal für Microsoft-SQL-Datenbanken			ja	ja
Datenbankwiederherstellungsportal für Oracle-Datenbanken			ja	ja
Self-Service-Portal für die Wiederherstellung von Dateien				ja
Delegieren von Wiederherstellungsaufgaben				ja
VEEAM DATALABS				
Secure Restore	ja	ja	ja	ja
SureBackup®			ja	ja
SureReplica (2)			ja	ja
Staged Restore			ja	ja
On-Demand Sandbox™			ja	ja
On-Demand Sandbox für Storage Snapshots (2)				ja
MANAGEMENT				
Unterstützung für VMware vSphere und Microsoft Hyper-V	ja	ja	ja	ja
Integriertes Management für Veeam Agenten	ja	ja	ja	ja
vSphere Web Client-Plug-ins (2)		ja	ja	ja

Tabelle 1-1: Funktionen der Editionen (Fortsetzung)

Veeam Backup & Replication	Community	Standard	Enterprise	Enterprise Plus
Standalone-Konsole	ja	ja	ja	ja
Indizierung von Gastdateisystemen	teilweise	teilweise	ja	ja
Unterstützung von vCloud Director [2]	teilweise	teilweise	teilweise	ja
Veeam Backup Enterprise Manager – zentrale Management-Weboberfläche		teilweise	ja	ja
Rollenbasierte Zugriffskontrolle (RBAC) [2]				ja
WEITERE FEATURES				
Verschiedene Optionen für den Zugriff auf Speichersysteme	ja	ja	ja	ja
Changed Block Tracking	ja	ja	ja	ja
File Manager	ja	ja	ja	ja
Quick Migration [2]	ja	ja	ja	ja
Automatisierung von Aufgaben	teilweise	teilweise	teilweise	ja

[1] Einige Dateisysteme werden nur für VMware unterstützt.

[2] nur VMware

(*) Die Community Edition ist auf maximal 10 Lizenzen begrenzt.

Das Zusammenführen von Lizenzen wird im Abschnitt »Zusammenführen von Lizenzen« auf Seite 188 beschrieben.

Erklärung der wichtigsten Funktionen

Nachfolgend möchte ich die in Tabelle 1-1 aufgeführten Funktionen kurz erklären:

Applikationskonsistente, imagebasierte Backups
: Erstellung applikationskonsistenter, imagebasierter VM-Backups mit erweiterter anwendungsspezifischer Verarbeitung (einschließlich Kürzung der Transaktionsprotokolle)

VeeamZIP™
: Optimierung von Ad-hoc-Backups aktiver VMs für Archivierungszwecke

NAS-Backup
: Sicherung, Schutz und Wiederherstellung großer NAS-Dateiserver für die Formate SMB/CIFS und NFS. Backups direkt in Repositorys für kurz- und langfristige Speicherziele.

Veeam Cloud Tier
: Native Objektspeicher-Integration für lokalen Speicher, AWS, Microsoft Azure, IBM Cloud sowie verschiedene S3-kompatible Storage-Angebote. Sowohl Kopie- als auch Auslagerungsspeicher werden unterstützt.

Proxy für die Interaktion mit Gastsystemen in ROBO-Umgebungen
: Verringerung der Arbeitslast auf dem zentralen Backup-Server und einfachere Skalierbarkeit für große Unternehmen mit vielen Installationen in Außen-/Zweigstellen (Remote Office/Branch Office, ROBO) bei der anwendungsspezifischen Verarbeitung und Indizierung des Gastdateisystems

Backup I/O Control
: Ermöglicht die Festlegung der maximal zulässigen I/O-Latenz für Produktivspeichersysteme, um sicherzustellen, dass Backup und Replikation die Verfügbarkeit der Speichersysteme in der Produktivumgebung nicht beeinträchtigen. Die Enterprise Edition verfügt über eine globale Latenzeinstellung, während die Enterprise Plus Edition die Anpassung dieser Einstellung auf Ebene der einzelnen Speichersysteme ermöglicht.

Backups aus Storage-Snapshots
: Beliebig häufige Erstellung imagebasierter Backups und Replikate bei nur geringen oder keinerlei Auswirkungen auf die Produktivumgebung auf Basis von:

  - Cisco HyperFlex-Snapshots
  - Dell EMC VNX-, VNX2- und VNXe-Snapshots
  - HPE 3PAR StoreServ-, StoreVirtual- und StoreVirtual VSA-Snapshots
  - IBM Spectrum Virtualize FlashCopy
  - Lenovo Spectrum Virtualize FlashCopy
  - NetApp Data ONTAP-basiertem Storage, einschließlich FAS, FlexArray (V-Series) und Data ONTAP Edge
  - Nimble Storage CS Series- und AF Series-Snapshots
  - und weitere

Integrierte Deduplizierung, Komprimierung und integrierter Ausschluss von Swap-Dateien
: Verringerung des Speicherplatzbedarfs für Backups und des Netzwerk-Traffics durch integrierte Deduplizierung, verschiedene Komprimierungsoptionen zur Abstimmung der Speicherauslastung mit der Performance und Arbeitslast auf dem Backup Proxy sowie Verringerung der benötigten Backup-Speicherkapazitäten und Optimierung der Performance durch den Ausschluss von Swap-Dateien

BitLooker™ und dateiselektive Verarbeitung auf Image-Ebene
: Analyse der NTFS-Masterdateitabelle (MFT) zur Identifizierung der Blöcke, die zu gelöschten Dateien gehören, und Überspringen dieser Blöcke während der Verarbeitung auf Image-Ebene zur Verringerung der Größe der Backup-Datei und Bandbreitenauslastung bei der Replikation

Backup Copy Jobs
: Automatisches Kopieren aller oder ausgewählter VM-Backups an den gewünschten DR-Speicherort, einschließlich Überprüfung und Fehlerbehebung zur Sicherstellung der Verfügbarkeit und Zuverlässigkeit der Kopien

End-to-End-Verschlüsselung
: Absicherung von Backup-Daten und Netzwerkübertragungen mit End-to-End-Verschlüsselung (256-Bit-AES) ohne Beeinträchtigung der Datenreduktion durch die integrierte Komprimierung und WAN-Beschleunigung. Alle Editionen bieten eine quellseitige Verschlüsselung (während des Backups), bei der Übertragung (Netzwerk-Traffic) und bei der Speicherung (Bandsicherung). Die Enterprise- und Enterprise-Plus-Editionen bieten zudem Schutz bei Kennwortverlust.

Native Bandunterstützung
: Sicherung und Archivierung von Dateien und VM-Backups auf eigenständigen Bandlaufwerken sowie physischen und virtuellen Bandbibliotheken, die mit einem Microsoft-Windows-Server in der Umgebung verbunden sind. Alle Editionen unterstützen das Kopieren von Windows-, Linux- und VM-Backup-Dateien auf Band. Die Enterprise- und Enterprise-Plus-Editionen bieten außerdem eine umfassende Integration in Backup Jobs und Unterstützung für das vollständige Tracking von VMs und Wiederherstellungspunkten auf Band sowie in Media Vaults. Sie unterstützen außerdem globale Medienpools (mit mehreren Bandbibliotheken) und einen dedizierten Medienpooltyp für eine einfachere Aufbewahrung von GFS-Backups (Großvater, Vater, Sohn).

Veeam Cloud Connect Backup
: Übertragung von Backups an externe Speicherorte mit vollständig integrierter, schneller und zuverlässiger Sicherung und Wiederherstellung in die bzw. aus der Cloud über einen Service Provider

Proxy-Affinität
: Einfachere Job-Erstellung und Abbildung von Direktverbindungen zwischen Proxys und Backup-Repositorys

Backup-Dateien pro VM für deduplizierenden Storage
: Speichern von VMs in separaten Backup-Dateien für eine bessere Backup-Performance bei der Sicherung auf deduplizierendem Storage. Hierzu werden durch Parallelverarbeitung von VMs mehrere gleichzeitige Schreibdatenströme ermöglicht.

Scale-out Backup Repository™
: Bereitstellung einer Abstraktionsebene über den einzelnen Speichergeräten zur Erstellung eines virtuellen Backup-Speicherpools.

Mit der Enterprise Edition können Anwender ein Scale-out Backup Repository mit drei aktiven Erweiterungen und einer inaktiven Erweiterung (im Wartungsmodus) erstellen. Mit der Enterprise Plus Edition ist die Anzahl der Repositorys oder Erweiterungen nicht beschränkt.

Integrierte WAN-Beschleunigung
: Bis zu 50 x schnellere Übertragung von Backups an externe Speicherorte und Verringerung der Bandbreitenauslastung mit agentenlosen Backup Copy Jobs. Die Enterprise Edition unterstützt die integrierte WAN-Beschleunigung ausschließlich für Veeam-Cloud-Connect-Speicherziele. Die Enterprise Plus Edition unterstützt die integrierte WAN-Beschleunigung für beliebige Speicherziele.

Veeam-Plug-in für Oracle RMAN und SAP HANA
: Übertragung von SAP-HANA- und Oracle-RMAN-Backups in Veeam-Repositorys unter Verwendung nativer Backup- und Wiederherstellungsfunktionalitäten von SAP und Oracle. Version 10 bietet Verbesserungen wie Backup-Kopie-Verarbeitung, höhere Leistung und Backup-Parallelverarbeitung für Cluster.

Imagebasierte VM-Replikation
: Lokale Replikation von VMs für eine hohe Verfügbarkeit oder externe Replikation für Disaster Recovery

Unterstütztes Failover und Failback
: Rollback von Replikaten und Unterstützung bei Failover und Failback

Replikation aus Backups
: Direkte Erstellung von Replikaten aus VM-Backup-Dateien ohne Beeinträchtigung der Produktivumgebung

Geplantes Failover
: Einfachere Migration von Rechenzentren ohne Datenverlust

Veeam Cloud Connect Replication
: Gewährleistung einer hohen Verfügbarkeit unternehmenskritischer Anwendungen durch vollständig integrierte, schnelle und sichere cloudbasierte Disaster Recovery über einen DRaaS-Provider (Disaster Recovery as a Service)

1-Click-Failover-Orchestrierung
: Integrierte Orchestrierung von Failover-Plänen für ein einfaches 1-Click-Standort-Failover zur Minimierung ungeplanter Ausfallzeiten

Vollständige Wiederherstellung einer VM
: Wiederherstellung einer gesamten VM auf dem ursprünglichen oder einem anderen Host. Durch schnelle Rollbacks kann die Wiederherstellung auf geänderte Blöcke beschränkt werden.

Instant VM Recovery
: Schnelle Wiederherstellung von Services für Anwender, indem VMs direkt über eine Backup-Datei auf herkömmlichen Backup-Speichergeräten gestartet werden

Wiederherstellung von VM-Dateien und virtuellen Festplatten
: Wiederherstellung einzelner VM-Dateien (z.B. VMX) und virtueller Festplatten

Direct Restore to AWS, Microsoft Azure, Azure Stack
: Wiederherstellung oder Migration von lokalen Windows- oder Linux-basierten VMs, physischen Servern und Endgeräten in AWS und in die Microsoft Azure Cloud

Instant File Level Recovery
: Wiederherstellung von Dateien aus 19 gängigen Dateisystemen unter Windows, Linux, BSD, Mac OS, Novell, Solaris und Unix (3)

Veeam Explorer für Storage-Snapshots
: Wiederherstellung einzelner VMs, Gastdateien und Anwendungsobjekte aus:

  - Dell EMC VNX-, VNX2- und VNXe-Snapshots
  - Hewlett Packard Enterprise (HPE) 3PAR StoreServ-, StoreVirtual- und StoreVirtual VSA-Snapshots
  - IBM Spectrum Virtualize-Snapshots auf dem IBM SAN Volume Controller und der Storwize-Produktreihe
  - Lenovo V Series Spectrum Virtualize-Snapshots
  - NetApp-Data-ONTAP-basiertem Storage, einschließlich FAS,
  - FlexArray und Data ONTAP Edge
  - Nimble Storage CS Series- und AF Series-Snapshots

Veeam Explorer für Microsoft Active Directory
: Suche nach und Wiederherstellung von sämtlichen Objekttypen in Active Directory (AD) wie Benutzern, Gruppen, Computerkonten und Kontakten, einschließlich Wiederherstellung von Benutzer- und Computerkennwörtern. Alle Editionen unterstützen die Wiederherstellung einzelner Benutzer und Computerkonten über den Export ins LDIFDE-Format, die Wiederherstellung direkt in AD sowie die Wiederherstellung von Kennwörtern. Die Enterprise- und Enterprise-Plus-Editionen unterstützen die Wiederherstellung von Mehrfachauswahlen, Containern, Gruppenrichtlinienobjekten, in AD integrierten DNS-Datensätzen und Konfigurationspartitionsobjekten.

Veeam Explorer für Microsoft Exchange
: Sofortiger Einblick in Backups von Microsoft Exchange 2010, 2013 und 2016 für die Wiederherstellung einzelner Exchange-Objekte (z.B. E-Mails, Termine, Notizen und Kontakte), von Online-Archivpostfächern und dauerhaft

gelöschten Objekten. Umfassende e-Discovery-Features einschließlich einer Schätzung der Größe der Abfrageergebnisse und ausführlicher Export-Reports. Alle Editionen unterstützen die Wiederherstellung von Objekten aus Exchange-Postfächern über Speichern, Senden und PST-Export. Die Enterprise- und Enterprise-Plus-Editionen unterstützen eine Wiederherstellung im ursprünglichen Postfach.

Veeam Explorer für Microsoft SQL Server
: Problemlose Wiederherstellung einzelner SQL-Datenbanken auch ohne umfassende SQL-Kenntnisse und ohne Suche nach Datenbank- und Transaktionsprotokolldateien. Alle Editionen unterstützen den lokalen Export von SQL-Datenbankdateien eines bestimmten Zeitpunkts. Die Enterprise- und Enterprise-Plus-Editionen unterstützen agentenlose Transaktionsprotokolle zum Sichern und Zurückspielen sowie die Wiederherstellung von Datenbanken und SQL-Objekten (Tabellen, gespeicherten Prozeduren, Ansichten usw.) auf Transaktionsebene auf dem ursprünglichen oder einem anderen SQL-Server.

Veeam Explorer für Microsoft SharePoint
: Sofortiger Einblick in SharePoint-Backups mit erweiterten Features für die Suche, die eine schnelle Wiederherstellung von einzelnen SharePoint-Objekten und vollständigen Websites ermöglichen. Alle Editionen unterstützen die Wiederherstellung von SharePoint-Objekten über Speichern, Senden und Exportieren. Die Enterprise- und Enterprise-Plus-Editionen unterstützen auch die Wiederherstellung von vollständigen Websites sowie die Wiederherstellung am ursprünglichen Speicherort.

Veeam Explorer für Oracle
: Problemlose Wiederherstellung einzelner Oracle-Datenbanken auch ohne umfassende Oracle-Kenntnisse und ohne Suche nach Datenbank- und Transaktionsprotokolldateien. Die Enterprise- und Enterprise-Plus-Editionen ermöglichen eine agentenlose Sicherung von Transaktionsprotokollen, das Management von archivierten Protokollen und die Wiederherstellung von Datenbanken auf Transaktionsebene auf dem ursprünglichen oder einem anderen Oracle-Server.

Portal für Helpdesk-Mitarbeiter für 1-Click Restore von Dateien und VMs
: Wiederherstellung von Gastdateien und VMs mit einem Klick über eine Weboberfläche

Portal für Helpdesk-Mitarbeiter für die Wiederherstellung von Microsoft-Exchange-Objekten
: Wiederherstellung von Postfachobjekten im ursprünglichen Postfach mit einem Klick über eine Weboberfläche

Datenbankwiederherstellungsportal
: Wiederherstellung einzelner Datenbanken auf dem ursprünglichen Server oder einem anderen Oracle- oder SQL-Server mit einem Klick über eine Weboberfläche

Self-Service-Portal für die Wiederherstellung von Dateien
: Portal zur Dateiwiederherstellung mit automatischer VM-Erkennung und automatischer Delegierung basierend auf der Zugehörigkeit zur lokalen Administratorgruppe

Delegierung von Wiederherstellungsaufgaben
: Umfassende Self-Services für alle Wiederherstellungsfeatures der Weboberfläche durch Delegieren der Wiederherstellung einzelner VMs oder VM-Gruppen an bestimmte Benutzer oder Benutzergruppen wie lokale IT-Mitarbeiter, Anwender, Abteilungsmitglieder usw.

Secure Restore
: Überprüfung von Backups zur Verbesserung der Sicherheit und Verringerung von Unterbrechungen aufgrund von Schadsoftware durch optionale Virenscans in Echtzeit, Wiederherstellung auf einen sicheren, virenfreien Wiederherstellungspunkt, unabhängige Unterstützung für Windows Defender, ESET und Symantec Protection Engine sowie Möglichkeit der Erweiterung um Antiviren-Tools von weiteren Herstellern

SureBackup
: Automatisches Testen und Überprüfen der Wiederherstellbarkeit aller gesicherten VMs durch Ausführen der VM direkt über die Backup-Datei (keine Wiederherstellung der vollständigen VM erforderlich), einschließlich Unterstützung für benutzerdefinierte Anwendungstestskripte

SureReplica
: Automatisches Testen und Überprüfen der Wiederherstellbarkeit aller replizierten VMs, einschließlich Unterstützung für benutzerdefinierte Anwendungstestskripte

Staged Restore
: Optimierung des Prozesses zur Löschung sensibler Daten z.B. nach DSGVO (Recht auf Vergessenwerden) mit benutzerdefinierten Skripten und Automatisierung; Datentest in einer abgeschirmten simulierten Produktivumgebung vor der sicheren und schnellen Wiederherstellung im Produktivsystem

On-Demand Sandbox
: Ausführung einer oder mehrerer VMs direkt über ein Backup in einer isolierten Umgebung einschließlich Nutzung einer Kopie der Produktivumgebung für Fehlerbehebung, Tests und Schulungen ohne Beeinträchtigung des Geschäftsbetriebs

On-Demand Sandbox für Storage-Snapshots
: Schnelle Erstellung vollständig isolierter Kopien der Produktivumgebung auf der Grundlage von Storage-Snapshots für ein einfaches Testen und eine schnelle Fehlerbehebung

Unterstützung für VMware vSphere und Microsoft Hyper-V
: Unterstützung für VMware vSphere 5.5 oder höher und Microsoft Hyper-V 2008 R2 SP1 oder höher, Anzeige beider Hypervisoren über eine Konsole

Integriertes Management für Veeam Agent
: Beinhaltet eine einzige Managementkonsole, um die Verfügbarkeit von virtuellen, physischen und cloudbasierten Workloads zu gewährleisten, zentralisierte Bereitstellung von Backup-Agenten, Windows Server Failover Cluster Support sowie Reports zur Überwachung und Identifizierung geschützter und ungeschützter Agenten

vSphere Web Client-Plug-ins
: Ausführung von VeeamZIP und Quick Backup, Monitoring von Backups, einfache Identifizierung nicht gesicherter VMs und einfachere Kapazitätsplanung direkt über den vSphere Web Client

Standalone-Konsole
: Separate Installation der Konsole sowohl auf dem Backup-Server als auch auf Laptops und Desktops, sodass RDP-Sessions (Remote-Desktop-Protokoll) auf einem Backup-Server überflüssig werden

Indizierung von Gastdateisystemen
: Katalog mit Gastdateien für die unkomplizierte Suche nach einzelnen Dateien zur Wiederherstellung einer Datei ohne Kenntnis des genauen Speicherorts oder des Zeitpunkts ihrer Löschung. Alle Editionen stellen einen Katalog mit Gastdateien von Backups bereit, die derzeit auf Festplatte gespeichert sind. Die Enterprise- und Enterprise-Plus-Editionen beinhalten außerdem einen Katalog mit archivierten Backup-Dateien und ermöglichen durch die Integration in 1-Click Restore eine Wiederherstellung direkt über die Suchergebnisse.

Unterstützung von vCloud Director
: Sicherung von vApp- und VM-Metadaten und -Attributen sowie Wiederherstellung von vApps und VMs direkt in vCloud mit vollständiger Unterstützung von Fast-Provisioning-VMs. Alle Editionen ermöglichen einen integrierten Einblick in die vCloud-Director-Infrastruktur, Backups über VeeamZIP (einschließlich Backups von vApp- und VM-Metadaten und -Attributen) und die direkte Wiederherstellung in vCloud. Die Enterprise Edition unterstützt geplante inkrementelle Backup Jobs für vCloud-VMs sowie die Integration in das Portal des Kunden über RESTful API. Die Enterprise Plus Edition unterstützt Self-Services für die Sicherung und Wiederherstellung auf dem Mandanten über Enterprise Manager sowie die native vCloud-Director-Authentifizierung.

Veeam Backup Enterprise Manager – zentrale Management-Weboberfläche
: Webbasierte, konsolidierte Ansicht verteilter Umgebungen auf einer zentralen Konsole ohne Anmeldung auf den einzelnen Backup-Servern, einschließlich Erstellung eines Verbunds mehrerer Backup- Server, zentralem Reporting und konsolidierter Benachrichtigung. Alle Editionen bieten Features für das Monitoring und Reporting über mehrere Backup-Server hinweg sowie das Starten und Anhalten von Jobs. Die Enterprise- und Enterprise-Plus-Editionen bieten außerdem umfassende Features für das Job-Management und die Möglichkeit zur Wiederherstellung.

Rollenbasierte Zugriffskontrolle (RBAC)
: Zuweisen von Rollen und Berechtigungen für das Erstellen, Wiederherstellen und Überwachen von Backups an Nutzer, Steuerung von Backup-Speicherorten und -kontingenten

Verschiedene Optionen für den Zugriff auf Speichersysteme
: Backup und Replikation direkt von SAN- und NFS-Speichersystemen, über den I/O-Stack des Hypervisors oder über LAN

Changed Block Tracking
: Minimierung des Zeitaufwands für Backups und Unterstützung für häufigere Backups und Replikationen. Wird sowohl in VMware-vSphere- als auch in Microsoft-Hyper-V-Umgebungen unterstützt.

File Manager
: Integration des Dateimanagements (Veeam FastSCP™) in die Bedienerkonsole

Quick Migration
: Migration von VMware-VMs zwischen Hosts und Speichersystemen mit VMware vMotion, Storage vMotion und der von Veeam bereitgestellten Migrationstechnologie

Automatisierung von Aufgaben
: Alle Editionen unterstützen PowerShell. Die Enterprise Plus Edition unterstützt außerdem RESTful API.

KAPITEL 5

Jobkonfiguration

Jedes Backup, jede Replikation, jede Kopieraktion oder auch ein SureBackup wird über einen Job erledigt, der gespeichert und zeitmäßig geplant werden kann. Für das Anlegen eines Jobs steht jeweils ein Assistent zur Verfügung, der alle notwendigen und möglichen Schritte abfragt.

Im Folgenden werden die einzelnen Typen der Jobs und was man dort einstellen kann näher erklärt.

Backup Jobs

Das Backup einer bestehenden VM ist wohl der häufigste Fall einer Datensicherung, deshalb werde ich ihn hier zuerst besprechen. Bei den weiteren Möglichkeiten, einen Job anzulegen, ist vieles zum Backup Job gleich und wird dort nicht nochmals erwähnt.

Um einen Backup Job zu generieren, klicken Sie im unteren linken Teil auf »Home«, dann auf »Backup Jobs« und wählen Sie aus dem Dropdown-Menü die passende Option:

1. Virtuelle Maschine von VMware vSphere oder Microsoft Hyper-V
2. Windows Computer – physischer Windows-Server oder Workstation
3. Linux Computer – physischer Linux-Server oder Workstation
4. Netzwerkfreigaben auf Windows oder Linux, NFS-Ordner oder SMB3-Freigaben

Als Beispiel nehme ich hier »Virtual machine« von Microsoft und VMware.

Menüpunkt Name

Geben Sie im ersten Fenster einen sprechenden Namen für den Job an. Es empfiehlt sich, dort ggf. die VMs, die gesichert werden sollen, anzugeben. Das kann der Name der VMs sein, der Name eines Ressourcenpools, eines Ordners oder des

Betriebssystems etc. Wichtig ist, dass Sie die VM zum Wiederherstellen auch finden. Mit diesem Namen wird auf dem Repository ein Ordner erstellt, in dem die Backup-Dateien landen; diese Dateien haben ebenfalls den Namen des Jobs.

Unter Beschreibung (Description) werden der Ersteller des Jobs und das Datum der Erstellung eingetragen. Diese Informationen sieht man auch in der Liste aller Jobs, deshalb sollte man dort ggf. etwas Aussagekräftiges eintragen wie z.B. die Uhrzeit, wann der Job läuft. Diese Liste könnte man dann nach der Startzeit sortieren.

Menüpunkt Virtual Machines

Im nächsten Fenster können Sie über »Add« die gewünschten VMs zur Liste hinzufügen. In dem neuen Fenster ist es möglich, nach Namen oder Namensbestandteilen zu suchen:

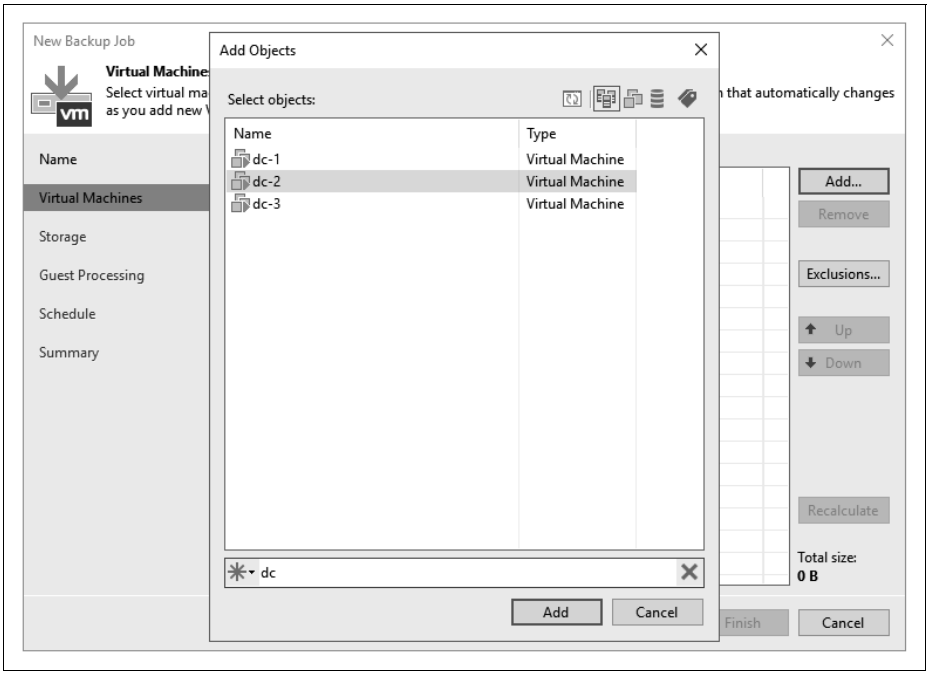


Abbildung 5-1: Auswahl der Objekte

Oben rechts in dem Fenster kann man über die fünf Icons von links angefangen die Ansicht aktualisieren, die Ansicht »Hosts and Clusters«, »VMs and Templates« sowie »Datenspeicher und VMs« auswählen. Bei Hyper-V bedeutet das vierte Icon »Hosts and Volumes«, bei vSphere das letzte Icon »VMs and Tags«, also benutzerdefinierte Attribute.

Wenn man auf das lila Sternchen unten links neben dem Eingabefeld klickt, kann man noch ein weiteres Kontextmenü aufklappen und darüber nach Objekten wie VMs, Ordner, Cluster, Hosts, Ressourcenpools und vApp (beides nur bei VMware), Host Group und SCVMM (beides nur bei Microsoft) suchen oder anzeigen lassen.

Viele meiner Kunden nutzen »Folder«, also eine Ordnerstruktur für die Datensicherung mit Veeam, weil so sichergestellt ist, dass eine neu angelegte oder auch wiederhergestellte VM automatisch in der Datensicherung ist – und nicht vergessen wird, wie in der Abbildung 5-2 dargestellt.

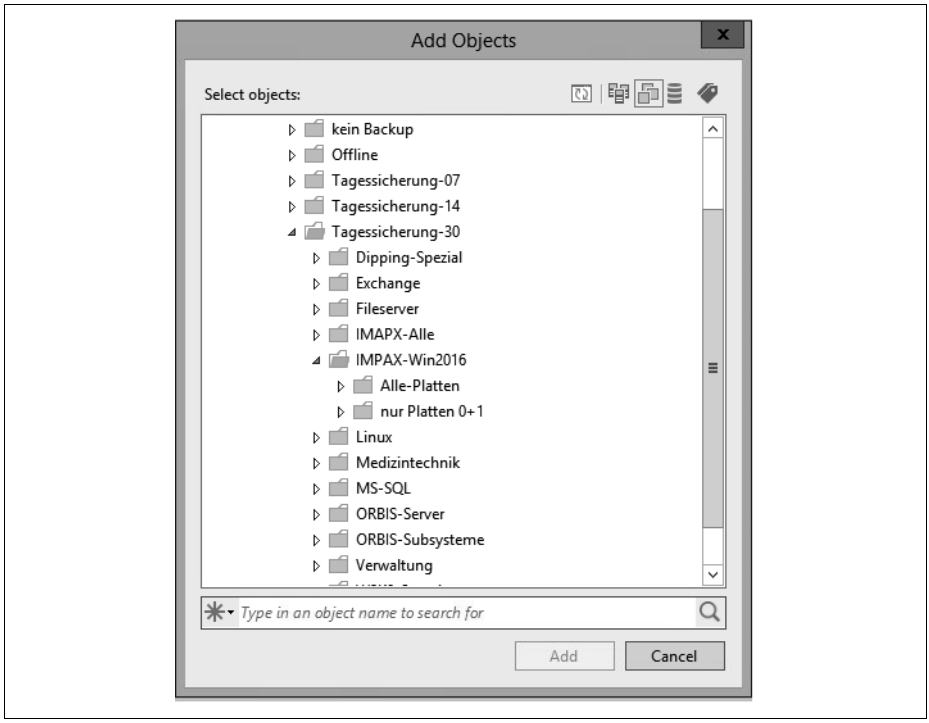


Abbildung 5-2: Ordnerstruktur für die Datensicherung

Hat man ein oder mehrere Objekte zum Sichern ausgewählt, können über die Schaltfläche »Exclusions« VMs, die sich in einem Ordner befinden, aber nicht gesichert werden sollen, ausgenommen werden (ggf. Kästchen bei »Show full hierarchy« anklicken). Für einzelne VMs können noch bestimmte Festplatten aus der Sicherung genommen oder auch Templates nur beim Full Backup gesichert werden.

Weiterhin kann man die Reihenfolge der VMs nachträglich ändern, damit die Sicherung auch wie gewünscht abläuft. Über die Schaltfläche »Recalculate« wird zum einen die Gesamtgröße der VMs und in der Spalte »Size« die jeweilige Größe

der zu sichernden Objekte angezeigt. Sollte dort bei einer VM der Wert »0« oder »N/A« auftauchen, wurde die ID der Maschine nicht gefunden (Veeam merkt sich die ID, nicht den Namen). Das passiert z. B., wenn die VM gelöscht und aus einer Datensicherung wiederhergestellt wurde, denn dann bekommt sie vom vCenter Server oder SCVMM eine neue ID.

Menüpunkt Storage

Im dritten Fenster »Storage« wählen Sie den Backup Proxy und den Sicherungsplatz (Backup Repository) aus und geben an, wie viele Wiederherstellungspunkte (Restore Points) oder wie viele Tage (days) auf dem Storage behalten werden sollen. Die ältesten Sicherungen werden dann automatisch gelöscht, wenn die Anzahl überschritten wird.

Der Backup Proxy wird vom BS meist automatisch richtig erkannt, und diese Einstellung sollte nur in Ausnahmefällen, z. B. bei WAN Accelerators oder in einer DMZ, geändert werden – dazu später mehr.

In dem Dropdown-Feld »Backup repository« können Sie die zuvor erstellten Speicherplätze auswählen. Achten Sie darauf, dass für den Job und alle Restore Points genügend Speicher zur Verfügung steht. Über den blauen Link »Map backup« können bereits vorhandene Sicherungen hinzugefügt werden, z. B. wenn man die Sicherungen auf einen anderen Storage verschoben hat oder Veeam neu aufsetzen musste.

Die »Restore Points« beziehen sich auf den Job, nicht auf die VMs im Job. Hat man beispielsweise einen Ordner mit drei VMs fünf Mal gesichert, wobei das Backup für eine VM drei Mal fehlschlug, hat man von dieser VM nach der eingestellten Zahl nur zwei Restore Points. Bleibt der Fehler, hat man nach fünf Sicherungen keine Wiederherstellungspunkte der nicht gesicherten VM! Das heißt auch, wenn die VM gelöscht wird, aber im Job verbleibt, fallen die Daten nach der eingestellten Wiederholung automatisch raus.

Beim Kästchen »Keep certain full backups longer for archival purposes« kann über die Schaltfläche »Configure« seit der Version 10 ein GFS(Grandfather, Father, Son)-Backup eingestellt werden, bei dem man Wochen-, Monats- und Jahressicherungen unabhängig der Restore Points länger aufbewahrt. Diese können während der eingestellten Laufzeit – also z. B. vier Wochen – nicht geändert oder gelöscht werden. Für das Monats-Backup wird üblicherweise das letzte Wochen-Backup genutzt und für das Jahres-Backup das letzte Monats-Backup des eingestellten Monats. Es wird also nicht nochmals ein zusätzliches Full Backup generiert, sondern nur das »Flag« dafür gesetzt.

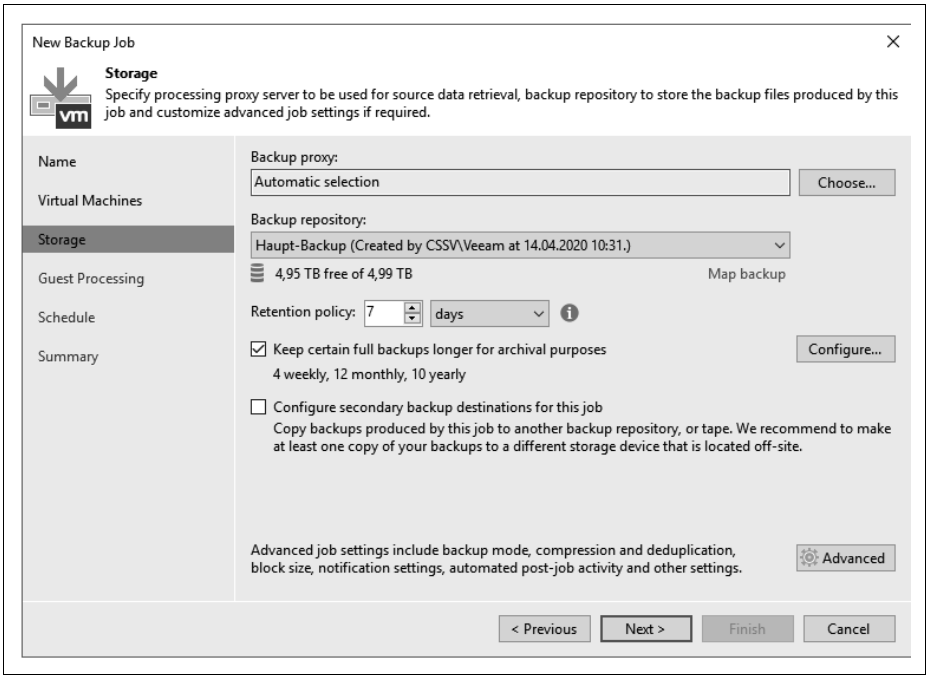


Abbildung 5-3: Backup-Job-Einstellungen

Bei »Configure secondary destinations for this job« kann man zusätzlich einen Tape Job oder einen Copy Job angeben, der nach der Datensicherung die gesicherten Dateien auf ein Bandlaufwerk oder einen anderen Datenspeicher kopieren soll. Dieser Job muss aber bereits angelegt sein, damit die Abhängigkeit zu dieser Sicherung sichergestellt ist.

Erweiterte Einstellungsmöglichkeiten zum Backup Job

Unter der Schaltfläche »Advanced« befinden sich weitere interessante Einstellungen, wie im Folgenden erklärt wird.

Auf der Registerkarte »Backup« kann man den Modus der Sicherung einstellen. Die einzelnen Modi habe ich bereits oben detailliert angesprochen. Der Modus »Incremental forever« wird eingestellt, indem man das Optionsfeld bei »Incremental (recommended)« anklickt und bei allen anderen Kästchen die Häkchen löscht. Überlegen Sie sich, ob Sie regelmäßig zusätzlich ein Full Backup erstellen lassen wollen oder ob Sie dafür einen eigenen Job generieren, um z.B. die Daten auf ein anderes Laufwerk abzulegen, was hier nicht ausgewählt werden kann.

Auf der Registerkarte »Maintenance« kann bei »Storage-level corruption guard« eine Überprüfung des Datenspeichers in regelmäßigen Abständen angegeben werden. Das ist sinnvoll, wenn man die Daten sehr lange dort liegen lässt. Veeam macht zwar bei jeder Sicherung eine Überprüfung, aber danach nicht mehr.

Unter »Full backup file maintenance« kann zum einen eine »Aufräumaktion« mit Defragmentierung und auch die Retention Policy für gelöschte oder aus dem Backup entfernte VMs eingestellt werden. Beachten Sie, dass hier Tage und nicht Wiederherstellungspunkte angegeben werden. Wenn man keine regelmäßigen Full Backups durchführen lässt, sollte man »Remove deleted VMs data after« anklicken und eine Anzahl an Tagen einstellen. Wenn die Zeit abgelaufen ist, werden die Daten bei der »Aufräumaktion« der VM als gelöscht markiert, also nicht wirklich vom Datenträger gelöscht, aber irgendwann überschrieben.

Auf der Registerkarte »Storage« können Einstellungen zum Datenspeicher ausgewählt werden. »Enable inline data deduplication« bewirkt, dass pro Job alle Redundanzen gelöscht werden, also weniger Speicher gebraucht wird (empfohlen). Bei »Exclude swap file blocks« werden die Auslagerungsdatei(en) der Maschinen nicht mit gesichert (empfohlen), und bei »Exclude deleted file blocks« werden gelöschte Dateien (Ausnahme die im Papierkorb) nicht mit gesichert. Die letzten beiden Funktionen betreffen nur VMs mit Microsoft-NTFS-Dateisystem.

Bei »Compression level« kann zwischen fünf Einstellungen gewählt werden, wobei ein höherer Kompressionsgrad Platz spart, aber auch meist eine längere Backup-Zeit bedingt.

- »None« sollte bei Repositorys gewählt werden, die selbst komprimieren oder deduplizieren,
- »Dedupe-friendly« belastet die CPU des Backup Proxys weniger,
- »Optimal« balanciert den Zeitbedarf mit der Kompressionsrate aus,
- »High« verringert die Größe um ca. 10%, benötigt aber deutlich mehr CPU-Performance und
- »Extreme« bietet die geringste Backup-Größe auf Kosten der Performance und Zeit.

Bei »Storage optimization« kann zwischen vier verschiedenen Punkten im Dropdown-Feld ausgewählt werden, auf welchen Datenspeicher das Backup landen wird. Dabei bedeutet »WAN« eine Geschwindigkeit mit bis zu 50 MBit/s, »LAN« üblicherweise 1 GBit/s und »Local target« einen lokalen Datenspeicher mit einer Übertragungsgeschwindigkeit ab 150 MByte/s. Das »Local target (large blocks)« wird hingegen häufig missverstanden: Hier handelt es sich um Storages, auf denen die Dateien der Datensicherung größer als 16 TByte sind. Der BS wird anhand dieser Einstellungen auch die jeweilige Blockgröße an die Übertragung anpassen.

Sollen die Backup-Daten verschlüsselt werden, kann unter »Enable backup file encryption« das Häkchen gesetzt und ein Passwort eingegeben werden. Haben Sie einen Enterprise Manager installiert und den BS dort hinterlegt, kann auch über den EM die Verschlüsselung bei verlorenem Passwort rückgängig gemacht werden. Den Vorgang dazu habe ich in Kapitel 11 ausführlich beschrieben.

Auf der Registerkarte Notifications können bei Bedarf Informationen zu einem Job per SNMP-Trap und/oder E-Mail verschickt sowie bei der VM in den Bemer-

kungen eingetragen werden. Dabei bedeutet die Option »Append«, dass jeweils das letzte Ergebnis an bestehende Eintragungen angehängt wird – nicht ältere Informationen zu den Jobs.

Bei mehreren Backup Jobs kann die Benachrichtigungseinstellung besser für alle Jobs zusammen unter dem Punkt »Options« aus dem Grundmenü eingestellt werden (siehe Abschnitt »General Options« auf Seite 53).

Auf der Registerkarte vSphere (nur bei VMware) bzw. Hyper-V (nur bei Microsoft) sollte bei bestimmten VMs das Einfrieren derselben ausgewählt werden, indem man das Häkchen bei »Enable VMware Tools quiescence« bzw. »Enable Hyper-V guest quiescence« setzt und dementsprechende Skripte einsetzt. Dies ist bei allen VMs angebracht, die spezielle Anwendungen (wie Datenbanken) hosten oder viele Transaktionen durchführen und nicht Microsoft als Betriebssystem nutzen. Bei Windows-VMs wird stattdessen der Dienst Volume Shadowcopy Service (VSS) genutzt. Beispiele für die Sicherung von Linux-Datenbanken habe ich weiter unten ausführlich beschrieben, wobei eine Oracle-Datenbank auf Linux nicht darunter fällt: diese wird über »Application aware processing« anders behandelt. Beachten Sie dazu auch den nächsten Abschnitt »Menüpunkt Guest Processing«.

Haben Sie das Einfrieren für die VMs in dem Job gewählt und aktivieren später zusätzlich das Käbfstchen bei »Application aware processing«, so wird der BS immer zuerst versuchen, die Anwendung zu erkennen, und das »quiescence« ignorieren.

Für eine schnellere inkrementelle Sicherung und für die Wiederherstellung einer VM oder deren Platten sollte das CBT-Verfahren (Changed Block Tracking) verwendet werden. Hier legt die Sicherungssoftware beim ersten Backup eine Datei pro Festplatte in den Ordner der VM mit der Endung *.ctk. Ab dann wird der Host die Adressen der geänderten Blöcke dort reinschreiben, damit bei der nächsten Sicherung der BS nur die geänderten Blöcke lesen und nicht die gesamte VM durchsuchen muss. Das beschleunigt die Sicherung immens. Bei Hyper-V auf 2016er-Maschinen lässt sich das nicht deaktivieren. Dort wird es RCT (Resilient Change Tracking) genannt. Voraussetzung ist dabei, dass alle Hosts die 2016er-Version oder höher haben, der Cluster-Level ebenfalls mindestens 2016 ist und die VM die Konfigurationsversion 8 oder höher hat. VMware-Maschinen müssen die Hardware Version 7 oder höher haben. Das CBT- oder RCT-Verfahren wird beim Full Backup automatisch wieder zurückgesetzt. Veeam nutzt bei VMs mit »Thin Provision«-Festplatten diese Funktion auch beim Full Backup. Hat eine VM einen Snapshot, so kann das Verfahren nicht angewendet werden.

Unter Hyper-V hat man hier zusätzlich den Schalter für Volume Snapshots. Hier können mehrere virtuelle Maschinen über einen einzigen Volume Snapshot gesichert werden. Dafür gibt es unter VMware die Registerkarte »Integration«, über

die mit der Lizenz Enterprise Plus ebenfalls Snapshots von einem unterstützten Datenspeicher anstatt über die VMware Tools gemacht werden können. Dieses Verfahren bremst die virtuelle Umgebung nicht aus, und die Daten kommen sehr schnell direkt über den Storage. Dafür muss der Backup-Server allerdings physisch sein und einen direkten Zugriff auf den jeweiligen Speicher über iSCSI, Fibre Channel oder Ähnliches haben. Beachten Sie auch das Kästchen bei »Failover to standard backup«, falls eine Sicherung über diesen Weg nicht erfolgen kann.

Auf der Registerkarte »Scripts« können Befehle oder Kommandos vor und/oder nach dem Job auf dem BS ausgeführt werden. Das lässt sich dann noch tageweise einstellen, also wann und wie oft das jeweilige Kommando laufen soll. Benötigen Sie allerdings Skripte innerhalb der zu sichernden VM, können Sie das unter dem nächsten Punkt »Guest Processing« einstellen.

Haben Sie Einstellungen unter »Advanced« verändert, lässt sich das für alle folgenden Jobs als Standard über die Schaltfläche »Save As Default« abspeichern.

Zurückgekehrt in das Fenster »Storage«, kann ggf. ein zusätzlicher Hinweis (gelbes Dreieck) auftauchen, wie in der Abbildung 5-4 beispielhaft dargestellt.

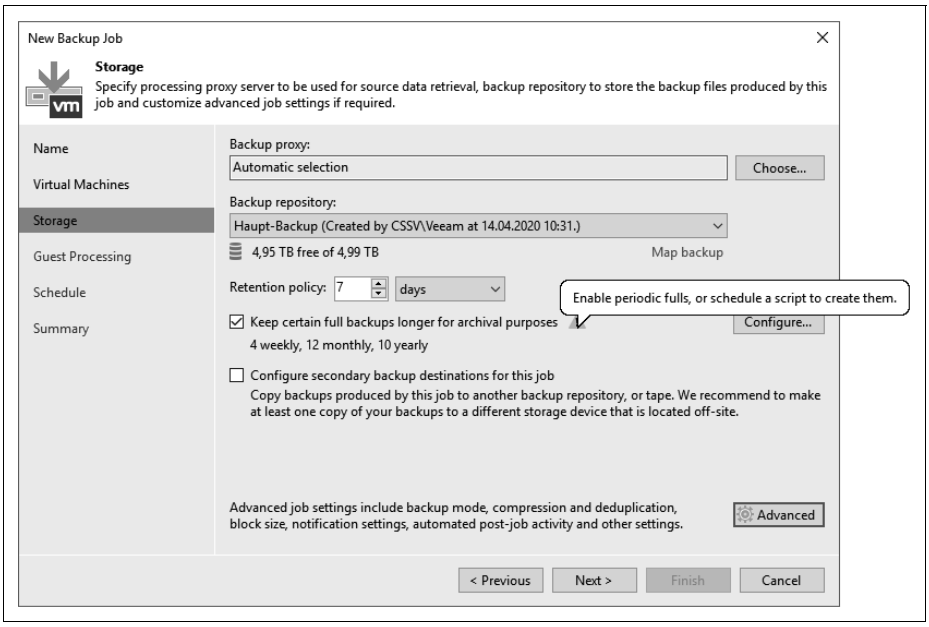


Abbildung 5-4: Konfigurationsfehler beim Backup Job

Hier wurde als Backup-Methode »Reverse incremental« oder »Incremental forever« gewählt, was mit der GFS-Sicherung nicht vereinbar ist, da keine regelmäßigen Full Backups angelegt werden, die eigentlich wöchentlich, monatlich oder jährlich zur Verfügung stehen müssten.

Menüpunkt Guest Processing

Im vierten Fenster »Guest Processing« können für bestimmte Anwendungen im Betriebssystem noch Einstellungen und Anmeldedaten hinterlegt werden. Das macht Sinn bei Domänencontrollern, MSSQL- und Oracle-Servern, Exchange-Servern sowie bei SharePoint. Mit dem angegebenen Account können die Daten auch einzeln wiederhergestellt werden, also einzelne Postfächer, Anlagen zu E-Mails, Tabellen aus Datenbanken, gelöschte Objekte aus Active Directory etc.

Um beim Backup die jeweilige VM in einen konsistenten Zustand zu bringen, hat man beim Job die Möglichkeit, das Häkchen bei »Enable application-aware processing« zu setzen oder unter »Storage – Advanced – vSphere« das »VMware Tools quiescence« anzuhaken. Die Funktionen der beiden Methoden werden in der nachfolgenden Tabelle 5-1 beschrieben:

Tabelle 5-1: Funktionen der beiden Methoden

Feature	VMware Tools/Hyper-V guest quiescence	application-aware processing
konsistentes Backup von Windows-VMs	ja	ja
Synchronisationstreiber für Linux-VMs	ja	nein
Unterstützung für spezielle Anwendungen	eingeschränkt	ja
Vorbereitung für spez. Anwendung vor VSS (z. B. Oracle)	nein	ja
Application Log Truncation (MS SQL, Exchange)	ja, in der VM platziert	ja, kann vom B&R-Server platziert werden
Fehlermeldungen	im Gast-OS	auf B&R-Server

In beiden Fällen wird also versucht, ein konsistentes Backup zu bekommen, wobei das Stilllegen über die Funktionen der Virtualisierungssoftware das Microsoft VSS nutzt und über Veeam in dem Betriebssystem der VM ein eigener Laufzeitprozess abhängig von der Anwendung gestartet wird.

Über die Schaltfläche »Applications« kommen Sie in ein weiteres Fenster, in dem die Objekte des jeweiligen Jobs in einer Tabelle aufgeführt sind. Wählen Sie eines der Objekte aus und klicken auf »Edit«, so öffnet sich ein neues Fenster, in dem bei Bedarf weitere Einstellungen vorgenommen werden können. Auf der ersten Registerkarte »General« unter »Applications« lässt sich eine von drei Möglichkeiten für den korrekten Ablauf einstellen. Hier sollte man nur in Ausnahmefällen von dem Standard (recommended) abweichen, es sei denn, man hat das Stilllegen der VMs vorher ausgewählt. Wie bereits oben angeführt, versucht der BS immer zuerst die Anwendung zu erkennen, und falls das nicht funktioniert, wird er dann erst über die VMware bzw. Hyper-V Tools die VM einfrieren. Für Jobs, in denen VMs mit und ohne einer der genannten Anwendungen sind, kann man für einzelne VMs das »application processing« hier deaktivieren, damit für diese das »quiescence« gilt.

Im unteren Teil bei »Transaction logs« kann auf das Abschneiden von Log-Dateien von SQL, Oracle und Exchange Einfluss genommen werden. Nach einer erfolgreichen Sicherung werden dann die Transaktions-Logs abgeschnitten, um Platz in der VM zu sparen. War die Sicherung nicht erfolgreich, wird dieser Prozess nicht durchgeführt und die Logs bleiben bestehen. Wichtig ist hierbei, dass die VMware Tools (bzw. Hyper-V integration components) korrekt installiert sind und die VSS-Erweiterung der Tools läuft. Soll eine in der Maschine integrierte Anwendung das machen, muss der untere Punkt (Perform copy only) angewählt werden. Das gilt auch, wenn in der VM ein anderes Tool die Transaktions-Logs wegschreibt.

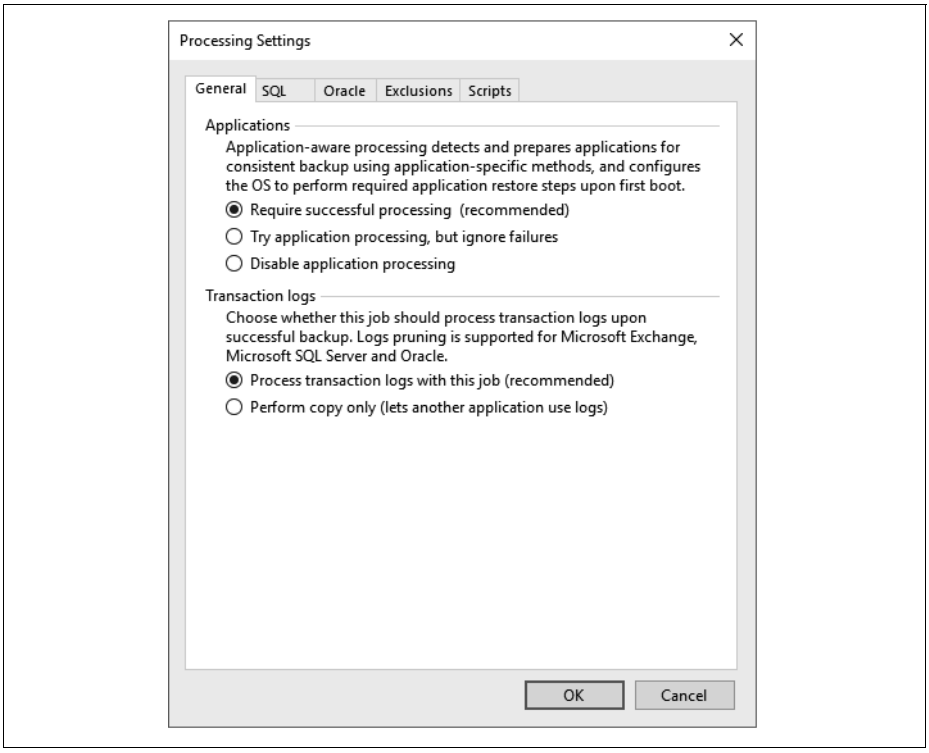


Abbildung 5-5: Erweiterte Einstellungen zu den Anwendungen

Auf den Registerkarten für »SQL« und »Oracle« hat man die Möglichkeit, die Log-Dateien in regelmäßigen Abständen zusätzlich zu sichern, damit sich ein konsistenter Zustand auch tagsüber in einstellbaren Intervallen sichern lässt. Sollten Sie diesen Punkt angeklickt haben, überlegen Sie sich, wann die Dateien nicht mehr benötigt werden – üblicherweise nach der nächsten oder übernächsten Sicherung. Hierbei werden im Grunde zwei Jobs angelegt: einer für die Sicherung der VM und einer für die Transaktions-Logs. Der Task für die Logs läuft ständig im Hintergrund und holt die Daten periodisch über eine eigene Laufzeitanwendung, z. B. alle 15 Minuten, ab. Diese Anwendung sichert im Betriebssystem der VM die

Daten in einem temporären Ordner und transferiert sie in regelmäßigen Abständen auf das Repository. Die Transaktions-Logs werden übrigens erst nach einer erfolgreichen Sicherung der VM geholt – solange bleibt der Job im Leerlauf.

Auf der Registerkarte »Oracle« kann man zusätzlich für den Benutzer SYSDBA die notwendigen Anmeldeinformationen hinterlegen.

Auf der Registerkarte »Exclusions« können sowohl Dateien als auch Ordner von der Sicherung einer einzelnen oder aller VMs mit NTFS als Dateisystem in dem Job ausgenommen werden. Hat man beispielsweise sehr viele große Dateien wie gepackte, Bilder und Filme, die nicht gesichert werden müssen, so kann dies Platz sparen, wird aber zu einer längeren Verarbeitungszeit führen. Im oberen Teil kann etwas ausgeschlossen werden, was dazu führt, dass die komplette VM gesichert wird, nur diese Daten nicht. Im unteren Teil wird eingetragen, was nur gesichert wird, also nicht die komplette VM, sondern nur diese(r) Ordner und Datei(en). Je mehr Einträge dort gemacht werden, umso länger dauert allerdings die Datensicherung – weil ständig nach den Ausnahmen gefiltert werden muss. Hierbei können auch Wildcards wie *, ? und Umgebungsvariablen wie %windir% und %homepath% genutzt werden.

Gerade bei einem Server, bei dem Dateien nur in einem Ordner öfter gesichert werden soll als die VM, ist die Funktion »Include« besser geeignet als ein »File Copy Job«. Achten Sie darauf, dass nur NTFS, nicht auch ReFS oder andere Dateisysteme unterstützt werden.

Auf der Registerkarte »Scripts« lassen sich noch Batch-Dateien für Windows-Anwendungen angeben, die keine Unterstützung durch VSS (Volume Shadowcopy Service) bieten, oder auch Shell-Skripte für Linux. Diese Dateien müssen sich auf dem lokalen System befinden (also z.B. dem Backup-Server) und sie müssen im Voraus fertiggestellt sein. Über solche Skripte könnte man zum Beispiel Dienste vor dem Snapshot (Pre-freeze script) stoppen und anschließend (Post-thaw script) wieder starten. Die Skripte müssen bei Linux die Endung *.sh haben und werden zur Laufzeit auf die VM über den SSH-Port 22 kopiert. Alternativ kann dies über die installierten VMware Tools mittels VMware-VIX-Kommunikation passieren. Achten Sie dabei auf das Häkchen bei »VMware Tools quiescence«.

Hat man als Sicherung Windows- und Linux-Maschinen in einem einzigen Job, so wird automatisch für Linux das Shell-Skript und für Windows die Batch-Datei genommen.

Das Häkchen bei »Enable guest file system indexing« ist für sehr große Datenmengen gedacht – typischerweise für Fileserver –, um schneller einzelne Dateien finden zu können. Ohne dieses Häkchen können trotzdem von fast jedem Dateisystem einzelne Dateien oder Ordner wiederhergestellt werden. Im Zusammenhang mit dem EM kann über mehrere BS in allen Sicherungen nach Dateien

gesucht werden, da der EM alle Indexe lokal speichert (Details zum EM in Kapitel 11). Wählen Sie ein Objekt in dem Fenster aus, so können Sie über die Schaltfläche »Edit« noch zusätzliche Angaben zu Ein- und Ausschlüssen machen, wobei die Voreinstellungen für Windows und Linux bereits sehr gut sind.

Hat man das Häkchen bei »Enable application-aware processing« oder bei der Indexierung gesetzt, muss man ebenfalls im Feld »Guest OS credentials« die notwendigen Anmeldedaten raussuchen oder hinzufügen (»Add ...«). Hat man mehrere VMs mit unterschiedlichen Anmeldedaten in einem Job, so können über die Schaltfläche »Credentials« für jedes Objekt individuelle Angaben gemacht werden. Haben Sie alle Accounts zugeordnet, so sollten Sie diese vorab über die Schaltfläche »Test Now« ausprobieren. In dem neuen Fenster werden alle Objekte aufgelistet und anschließend die Ergebnisse der Tests angezeigt. Sollte bei einem oder mehreren Einträgen eine Warnung stehen, so klicken Sie in die jeweilige Zeile auf der linken Seite, um Details in der rechten Hälfte dazu zu sehen.

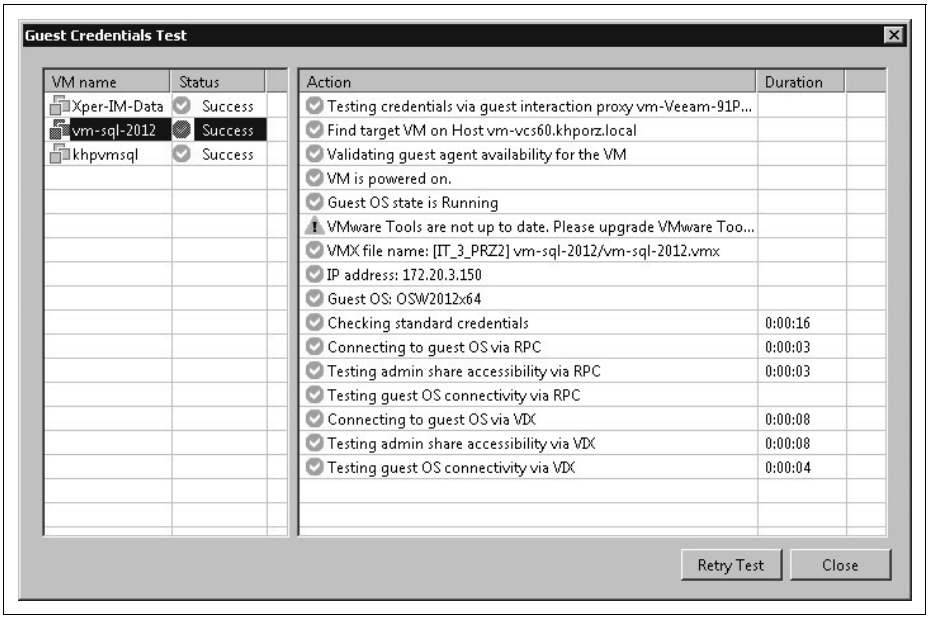


Abbildung 5-6: Anmeldedaten überprüfen

Sollte in der Spalte »Status« bereits eine Warnung stehen, liegt dies häufig an der Firewall auf der jeweiligen VM. Diese lässt üblicherweise keine Anmeldung und Installation eines Agenten über das Netzwerk zu. Funktioniert der Zugriff nicht über RPC, aber über VIX oder umgekehrt, wird ebenfalls eine Warnung angezeigt, die aber die Funktionalität der Aufgabe nicht beeinflusst – diese Warnung kann dann also ignoriert werden.

Exchange- und SQL-Knoten

Jegliche Konfigurationen von Exchange-DAG-Knoten (Database Availability Groups) und Microsoft SQL 2012 AlwaysOn Cluster (und höher), ob aktiv, passiv oder hot-standby, mit allen Datenbanken unterstützt der BS von Veeam. Die Transaktions-Logs werden auf allen beteiligten Servern gekürzt, ohne dass weitere Einstellungen dazu notwendig sind und egal ob es sich um einen aktiven oder passiven Knoten handelt. Da es bei einem Snapshot zu einer Verzögerung oder kurzen Unterbrechung bei der Kommunikation der Exchange-Knoten untereinander kommen kann, sollte man ggf. die Timeouts der beteiligten Server anpassen. Dafür gibt es einen ausführlichen Knowledge-Base-Artikel von Veeam: *https://www.veeam.com/kb1744*. Beachten Sie, dass möglichst alle beteiligten SQL-Server der AlwaysOn Availability Group und alle Exchange-DAG-Knoten in jeweils einem Backup Job enthalten sein sollten.

Menüpunkt Schedule

Im vorletzten Fenster »Schedule« kann man planen, wann und wie oft der Job laufen soll. Es ist sowohl möglich, eine Zeit, bestimmte Tage, Zeitabstände als auch andere Optionen zu nutzen.

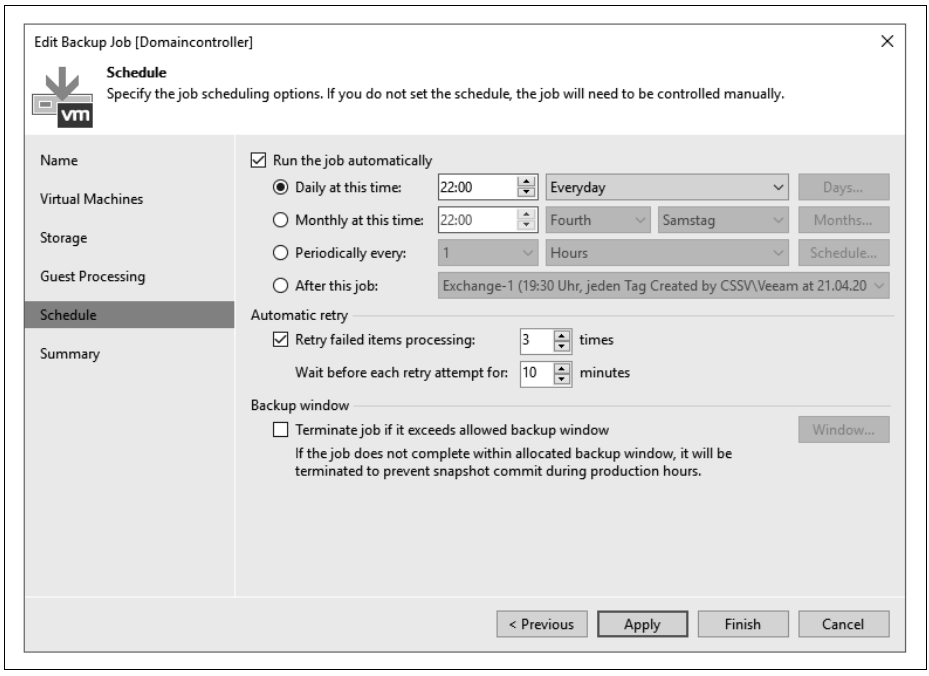
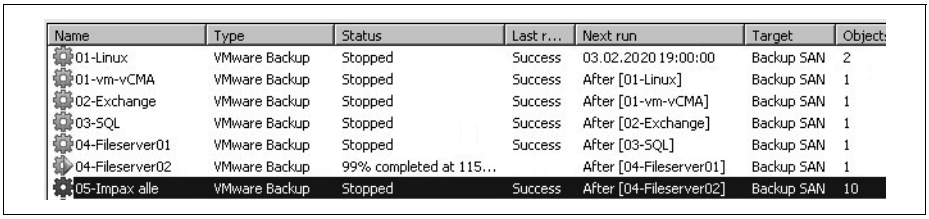


Abbildung 5-7: Auswahl der Sicherungsoptionen

In Abbildung 5-8 ist als Beispiel der Job direkt nach Beendigung des vorherigen Jobs geplant.



Name	Type	Status	Last r…	Next run	Target	Objects
01-Linux	VMware Backup	Stopped	Success	03.02.2020 19:00:00	Backup SAN	2
01-vm-vCMA	VMware Backup	Stopped	Success	After [01-Linux]	Backup SAN	1
02-Exchange	VMware Backup	Stopped	Success	After [01-vm-vCMA]	Backup SAN	1
03-SQL	VMware Backup	Stopped	Success	After [02-Exchange]	Backup SAN	1
04-Fileserver01	VMware Backup	Stopped	Success	After [03-SQL]	Backup SAN	1
04-Fileserver02	VMware Backup	99% completed at 115…		After [04-Fileserver01]	Backup SAN	1
05-Impax alle	VMware Backup	Stopped	Success	After [04-Fileserver02]	Backup SAN	10

Abbildung 5-8: Reihenfolge der Jobs

- *Daily at this time:* Hier lassen sich die Uhrzeit und die jeweiligen Tage, wann die Sicherung laufen soll, einstellen. Everyday bedeutet jeden Tag von Montag bis Sonntag, On week-days sichert von Montag bis Freitag und bei On these days können über die Schaltfläche »Days« die gewünschten Tage angeklickt werden.
- *Monthly at this time:* Hier wird einmal im Monat eine Sicherung gemacht, und man kann zwischen First, Second, Third, Fourth, Last und This day auswählen. Im dritten Dropdown-Feld wählt man den Wochentag aus, und über die Schaltfläche »Month« lassen sich die gewünschten Monate einstellen.
- *Periodically every:* Will man eine VM mehrmals täglich sichern, wählt man diese Option. Sie können periodisch Stunden und Minuten oder auch ständig (Continuously) auswählen. Bei der letzten Option wird ein Snapshot der VM gemacht, diese gesichert, der Snapshot gelöscht und ein erneuter Snapshot gemacht, wieder gesichert usw. Über die Schaltfläche »Schedule« kann noch ein Zeitfenster für die Sicherung gewählt werden, also z. B. nur wochentags in der Zeit von 8:00 Uhr bis 16:00 Uhr und ohne die Mittagspause.

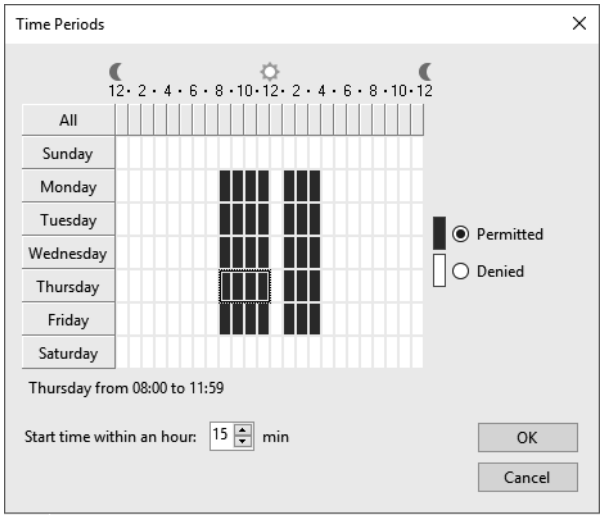


Abbildung 5-9: Sicherungen in Zeitintervallen

Achten Sie bei allen Einstellungen unter diesem Punkt auf die Anzahl der gewünschten Restore Points! Bei dem Beispiel im Screenshot werden z.B. ab 8:15 Uhr bis 11:15 Uhr und von 13:15 Uhr bis 15:15 Uhr Sicherungen gemacht, also pro Tag 7 und pro Woche 35. Brauchen Sie die Daten für zwei Wochen, so müssen Sie im dritten Fenster (Storage) insgesamt 70 Restore Points oder 10 Days ausgewählt haben.

In dem Feld »Automatic retry« ist üblicherweise eine dreifache Wiederholung mit jeweils 10 Minuten Pause eingestellt. Das lässt sich nach eigenen Bedürfnissen auch abändern.

In dem Feld »Backup window« kann eine Zeit ähnlich wie bei den periodischen Sicherungen eingestellt werden, damit eine noch laufende Datensicherung zu Beginn der Arbeitszeit abgebrochen wird. Tritt dies ein, werden alle noch nicht fertiggestellten Sicherungen von VMs gelöscht und bei der nächsten Datensicherung diese zuerst gesichert.

Menüpunkt Summary

Im letzten Fenster »Summary« steht nur noch die Übersicht zu dem Job – einstellen lässt sich hier nichts mehr. Klicken Sie auf »Finish«, nachdem Sie sich die Details zu dem Job angesehen haben, oder planen Sie den sofortigen Start des Jobs, indem Sie das Häkchen bei »Run the job when I click Finish« setzen.

Nach dem Backup Job kann man sich die Details zu der Sicherung anschauen und/oder auch per Mail als Bericht zusenden lassen.

Backup job: 115-Medizintechnik 1 — **Success**
Created by KHPORZ\Goepel at 07.04.2016 16:39. — 4 of 4 VMs processed

Mittwoch, 22. April 2020 20:00:17

Success	4	**Start time**	20:00:17	**Total size**	4,9 TB	**Backup size**	24,2 GB	
Warning	0	**End time**	20:13:37	**Data read**	40,5 GB	**Dedupe**	1,0x	
Error	0	**Duration**	0:13:19	**Transferred**	24,2 GB	**Compression**	1,6x	

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
khpvmmed	Success	20:01:33	20:11:00	1,3 TB	16,6 GB	6,4 GB	0:09:27	
khpvmmed02	Success	20:01:33	20:10:05	955 GB	1,7 GB	725,6 MB	0:08:31	
vm-steri-beli	Success	20:06:05	20:08:53	80 GB	1,7 GB	583,1 MB	0:02:47	
khpvmSchlaflabor	Success	20:06:05	20:13:13	2,6 TB	20,6 GB	16,5 GB	0:07:08	

Abbildung 5-10: Übersichts-Mail nach der Sicherung

Backup von verschlüsselten VMs

Seit kurzem kann man bei VMware vSphere virtuelle Maschinen aus Sicherheitsgründen verschlüsseln. Das Backup solcher VMs muss man ganz anders gestalten als bei herkömmlichen Maschinen. Logischerweise geht ein Backup über den »Direct Storage Access« sowie über Storage Snapshots nicht. Eine gute Möglichkeit bietet hier ein Veeam Proxy als verschlüsselte VM, da darüber der HotAdd-Modus ausführbar ist. Auch eine Sicherung übers Netzwerk (nur NBDSSL) kann erfolgen. Da Veeam das VDDK (Virtual Disk Development Kit) nutzt und die Daten hiermit unverschlüsselt gelesen werden, sollte man über eine Verschlüsselung der Backup-Dateien nachdenken – ggf. auch über eine verschlüsselte Übertragung zum Repository.

VeeamZIP

Mit VeeamZIP kann man schnell und unkompliziert Full Backups von einer oder mehreren laufenden oder ausgeschalteten VMs, ähnlich wie beim normalen Backup, erstellen. Als Speicherort kommt der lokale Rechner, der BS oder eine Freigabe in Betracht, und es braucht kein Job dafür erstellt zu werden. Die zu wählenden Optionen sind dabei sehr überschaubar: Speicherort, Aufbewahrungszeit (eine Woche bis drei Jahre), Verschlüsselung des Backups, Kompressionslevel und ggf. das Stilllegen. Nach der Sicherung werden diese unter »Home – Disk (VeeamZIP)« angezeigt, und man kann von dort auch die Wiederherstellung – ähnlich wie beim normalen Backup – starten.

Bei diesen Vorgängen wird keine »Bremse« für den zugrunde liegenden Storage verwendet. Eventuell noch andere laufende Task könnten dadurch in Mitleidenschaft gezogen werden.

Über »Inventory« wählen Sie Ihre Infrastruktur aus und erweitern die Einträge, bis die VM, der Ordner o.Ä. auf der rechten Seite erscheint. Über das Kontextmenü oder das Ribbon wählen Sie dann VeeamZIP aus, geben den gewünschten Speicherort an und wann dieses Backup gelöscht werden soll (siehe Abbildung 5-11).

Beachten Sie bitte, dass das letzte Kästchen für »Disable VMware Tools quiescence« angehakt werden muss, wenn Sie die VM nicht »einfrieren« wollen.

Wenn Sie das gleiche Backup nochmals vornehmen möchten, wählen Sie aus dem Kontextmenü »VeeamZIP to«, dann ist die Vorauswahl in dem Fenster wie beim letzten Mal.

KAPITEL 11

Enterprise Manager

Der Veeam Backup & Replication Enterprise Manager (EM) ist eine optionale Komponente, die man auf einem physischen oder virtuellen Windows-Rechner installieren kann. Das Tool, welches man über einen Browser ansteuert, lässt sich auch auf einen Backup-Server oder Proxy installieren. Meistens wird das Programm eingesetzt, wenn man mehrere Backup & Replication Server hat, da man hierüber alle Jobs sehen, konfigurieren, den Status einsehen und einen Report über alle B&R-Server bekommt. Mit dem EM kann man auch Dateien von einem Gastbetriebssystem in allen aktuellen und archivierten Backups suchen – über die gesamte Backup-Infrastruktur – und diese mit einem Klick wiederherstellen. Diese Komponente hat unter anderem einen Dienst, der den Index von VM-OS-Dateien von allen B&R-Servern holt, diese konsolidiert und in einen eigenen Katalog speichert. Aus diesem Katalog kann er sehr schnell die gewünschte Datei finden.

Installation

Die Komponenten für die Installation des EM befinden sich auf dem ISO, welches auch für die Installation des B&R-Servers genutzt wurde. Ab Windows 2012 kann man mit der rechten Maustaste draufklicken und »bereitstellen« wählen. Anschließend kann über die Datei setup.exe die Installation gestartet werden.

Wählt man einen bereits bestehenden Backup-Server, so wird die vorhandene Lizenz erkannt und muss nicht nochmals angegeben werden. Die Features, die man zur Auswahl hat, sind natürlich zum einen der EM (aktiv) und zum anderen ein »Cloud Connect Portal for Service Provider« (standardmäßig nicht aktiv), welches Nutzern einer weiteren Site die Möglichkeit gibt, ein vollständiges Failover zu initiieren.

Im nächsten Schritt werden die notwendigen Voraussetzungen überprüft und das Ergebnis wird im Fenster angezeigt (siehe Abbildung 11-1).

Da in dem Installationspaket die notwendigen Komponenten vorhanden sind, kann man über die Schaltfläche »Install« alles Notwendige nachinstallieren.

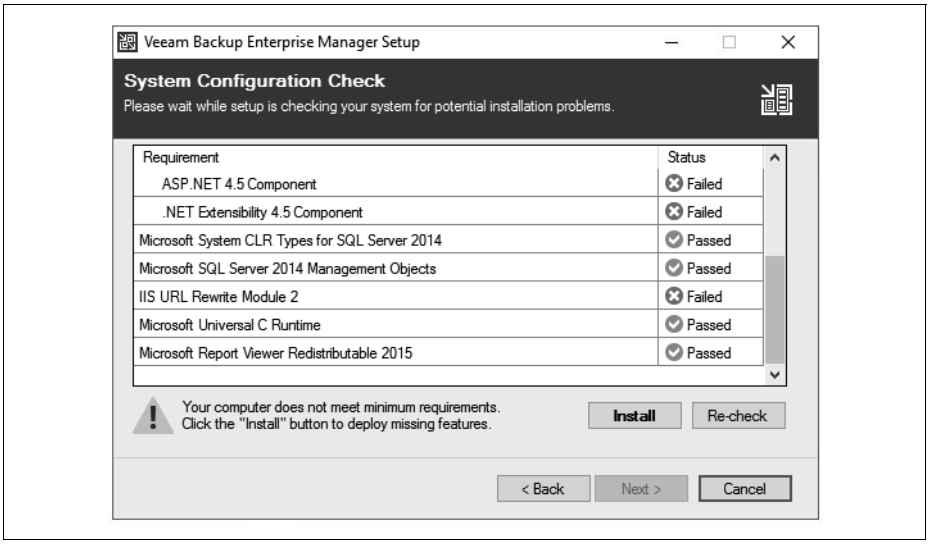


Abbildung 11-1: Fehlende Anwendungskomponenten

Der Dienst des EM kann mit lokalen Rechten oder denen eines Users laufen. Hier sollte man nur einen Unterschied machen, wenn der Rechner, auf dem die Installation stattfindet, nicht Mitglied einer Domäne ist.

Die Informationen des EM werden in einer Datenbank (VeeamBackupReporting) hinterlegt. Hat man eine kleine Umgebung, kann hierfür auch der lokale SQL-Server von Veeam (SQL-Express) genutzt werden.

Auf der nächsten Seite werden die notwendigen Netzwerk-Ports, das benötigte Zertifikat und ggf. eine sichere Verbindung über TLS 1.2 abgefragt.

Ist die Installation erfolgreich durchgelaufen, so hat man auf dem Desktop ein zusätzliches Symbol für den Enterprise Manager, über das man die Webseite für diesen auf dem Port 9443 (*https://Servername:9443/*) aufrufen kann, und ein Icon für »Veeam Self Service File Restore«, mit dem Dateien wiederhergestellt werden können. Leider sind die lokalen Anmeldedaten (Windows Session Authentication) beim Aufruf der Webseite nicht nutzbar, sodass man sich erneut authentifizieren muss. Klickt man bei dem Aufruf der Seite das Kästchen bei »Remain signed in« an, so sollen die Anmeldedaten gespeichert werden – was jedoch nicht immer funktioniert.

Konfiguration des Enterprise Managers

Nachdem die Oberfläche im Browser geöffnet wurde, sollte man sich zunächst um die erste Konfiguration kümmern. Klicken Sie dazu oben rechts auf »Configuration«. Hier sollte man zunächst den oder die Backup-Server über die Schaltfläche »Add« hinzufügen, auch wenn die Installation auf so einem Server stattgefunden

hat. Möchte man mehrere Backup-Server hinzufügen, muss man den Vorgang jeweils wiederholen und immer die Anmeldedaten des Backup-Servers angeben, da diese nicht als Auswahl zur Verfügung stehen – im Gegensatz zum Backup-Server, bei dem man diese aus einer Drop-Box auswählen kann. Backup-Proxys, Repositorys und Ähnliches werden hier nicht angegeben.

Hat man den oder die Backup-Server hinzugefügt, sammelt der EM zunächst Informationen über die Backup und Replication Jobs, die man sich ein paar Minuten später unter »Dashboard« für die letzten 24 Stunden oder auch sieben Tage ansehen kann.

Der vCenter Server wird meist automatisch erkannt, wenn man den oder die Backup-Server hinzugefügt hat (Hyper-V gehört noch nicht dazu). Hier gibt es die Möglichkeit, für den Web- und den HTML5-Client ein Plug-in zu installieren. Klicken Sie dafür zunächst auf den vCenter Server und dann auf die Schaltfläche »Check version ...«, geben Sie die Anmeldeinformationen an und warten Sie, bis der »Plug-in Status« von »Pending ...« auf »Not installed« wechselt.

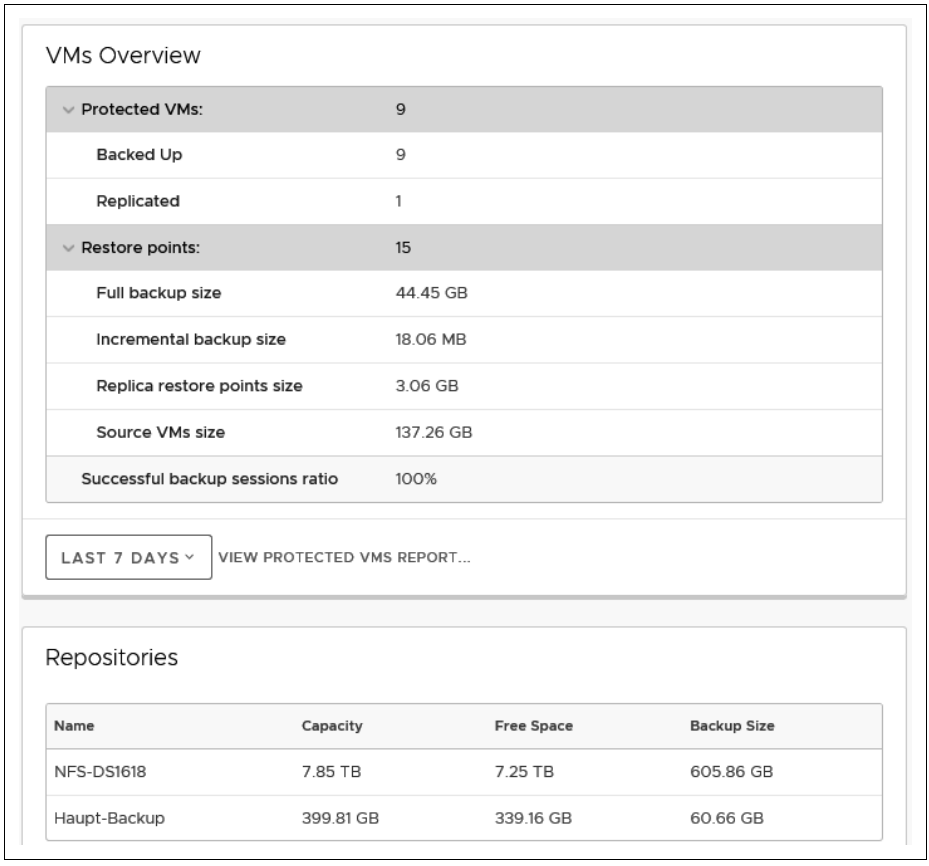


Abbildung 11-2: Plug-in-Informationen – Ausschnitt des vCenter Servers

Sollten Sie sich nicht anmelden können, überprüfen Sie, ob die letzten Updates installiert wurden. Anschließend können Sie auf den Button »Install« klicken, damit auf dem vCenter Server die Informationen zu Veeam B&R sichtbar werden. Nach einer kurzen Zeit sollte der Status des Plug-ins auf »Installed« wechseln und in der nächsten Spalte die Versionsnummer anzeigen.

Haben Sie sich direkt an dem vCenter Server mit genügend Berechtigungen angemeldet, so finden Sie beim Web-Client unter »Home« das Icon für Veeam Backup & Replication. Hierüber erhalten Sie eine Übersicht über den Status der Backups und Replikationen und können auch über einen neuen Eintrag im Kontextmenü eine VM über Veeam Zip sichern. Auf dem aktuellen HTML5-Client ist das Plug-in zunächst nicht sichtbar. Melden Sie sich erneut an, finden Sie es über die Schaltfläche »Menü« im Dropdown-Feld. Sollte dies nicht so sein, melden Sie sich am VMware Appliance Management (*https://vcsa:5480*) an und starten Sie die Dienste des Web- und vSphere-Client neu.

Die Links »View protected VMs report«, »View latest Backup Job status report« und »View Capacity Planning for Backup Repositories« leitet jeweils auf eine Informationsseite zu Veeam One weiter. Das Programm Veeam One ist ein Reporting-Tool, das in der Availability Suite enthalten ist und auch separat erworben werden kann.

Self-Service

Über den Self-Service kann der Backup-Administrator die Vorgänge für das VM-Backup und die Wiederherstellung an andere Benutzer delegieren, wenn diese in vSphere Berechtigungen an den jeweiligen VMs haben. Dazu zählt die Wiederherstellung von Dateien, Festplatten, Objekten etc. auch ohne administrativen Account (siehe auch Abschnitt »Veeam Self-Service FileRestore« auf Seite 149 und Abschnitt »Veeam Self-Service Backup« auf Seite 150).

Sessions

An dieser Stelle erhält man eine Auflistung über die eingesammelten Informationen der oder des Backup-Server(s). Die Daten werden üblicherweise alle 15 Minuten geholt und in die Datenbank des EM gespeichert und können hinterher über das Dashboard angesehen werden.

Das Intervall lässt sich nicht direkt an dieser Stelle ändern, sondern an dem ersten Eintrag auf der linken Spalte bei »Backup Servers«. Klicken Sie den gewünschten BS an und wählen Sie aus der Menüleiste »Schedule« aus. Hier kann der Zeitraum in Minuten und Stunden gewählt und auch auf die manuelle Methode gewechselt werden. In der Session-Liste können Sie auf den jeweiligen blauen Link (z. B. Success) klicken, um weitere Details zu dem Eintrag zu bekommen. Diese Liste lässt sich auch in eine XLSX-Datei exportieren.

Roles

Um sich am EM anmelden und damit arbeiten zu können, müssen Berechtigungen für User oder Gruppen eingetragen sein. Unter »Roles« können sehr granular Berechtigungen nach Bedarf für Personen eingetragen werden. Es ist zum Beispiel möglich, Berechtigungen zur Wiederherstellung von Dateien zu delegieren, ohne den Inhalt der Dateien sehen zu können.

Drei Rollen sind hier vorgegeben und können auch nicht ergänzt werden:

- Portal Administrator: anfänglich standardmäßig an die in der lokalen Administratorengruppe aufgeführten Benutzer und den Benutzer, der Veeam installiert hat. Über diese Rolle bekommt man Zugriff auf alle verfügbaren Operationen und Registerkarten der Oberfläche.
- Portal User: Zugriff auf Rechner aus dem Wiederherstellungsbereich auf den Registerkarten »Machines« und »Files«, ermöglicht ein »Quick Backup« für Rechner aus dem Wiederherstellungsbereich auf der Registerkarte »Machines«, Wiederherstellungsvorgänge gemäß den Delegationseinstellungen durchführen und Informationen über alle Backup-Server und Backup-Aufträge auf den Registerkarten »Dashboard«, »Reports« und »Jobs« anzeigen.
- Restore Operator: Zugriff auf Maschinen aus dem Wiederherstellungsbereich auf den Registerkarten »Machines« und »Files« und Wiederherstellungsvorgänge gemäß den Delegationseinstellungen durchführen.

Auf die Konfiguration des EM können die Mitglieder der letzten beiden Rollen nicht zugreifen. Damit Benutzer oder Gruppen aus dem AD ausgesucht werden können, muss der EM-Dienst die notwendigen Berechtigungen dafür haben. Ist der Rechner, auf dem der EM installiert ist, Mitglied der Domäne und der Dienst läuft als »Lokales Systemkonto«, gibt es keine Probleme.

Settings

Einige grundsätzliche Sicherheitseinstellungen für den EM können hier auf insgesamt sechs Registerkarten festgelegt werden:

- Search Catalog: Einstellungen über die Aktualisierungsrate des Kataloges und der Indexe
- Key Management: Das Konzept, die Begriffe und Verfahren der Datenver- und -entschlüsselung habe ich schon ausführlich beschrieben. Als Teil des Prozesses helfen Ihnen die EM-Schlüssel bei der Wiederherstellung verschlüsselter Daten im Falle eines verlorenen oder vergessenen Passworts, das zur Verschlüsselung verwendet wurde. Während der Installation von Enterprise Manager erzeugt das Setup automatisch einen neuen Schlüsselsatz, der einen öffentlichen Enterprise-Manager-Schlüssel und einen privaten Enterprise-

Manager-Schlüssel enthält. Siehe dazu auch Abschnitt »Verschlüsseltes Backup ohne Passwort wiederherstellen« auf Seite 151.

- SAML Authentication: Organisationen, die einen Single-Sign-On-Service in ihrer IT-Infrastruktur verwenden, können Benutzern den Zugriff auf den EM ohne Angabe eines Kennworts ermöglichen. Dazu muss der EM-Administrator SAML-Authentifizierungseinstellungen (Security Assertion Markup Language) konfigurieren. Dafür kann auch der EM selbst benutzt werden, indem er den »Identity Provider« darstellt. Die Anmeldung erfolgt anschließend über das Zertifikat.
- Directory Account: Hier kann ein administrativer AD-User hinterlegt werden, der die notwendigen Berechtigungen im Active Directory und Exchange hat, um Objekte aus den Postfächern direkt wiederherzustellen.
- Chart Settings: Bei Bedarf können Sie das Erscheinungsbild der Diagramme in der Hauptansicht (Dashboard) von Veeam Backup Enterprise Manager anpassen. Standardmäßig wird das unter dem gewählten Kontrollkästchen »Show backup window« angegebene Zeitintervall im Aktivitätsdiagramm hervorgehoben und das Intervall ist von 20:00 Uhr abends bis 8:00 Uhr morgens. Sie können das hervorgehobene Intervall so ändern, dass es mit Ihrem geplanten Sicherungsfenster korreliert, indem Sie die Start- und Stoppzeit bearbeiten. Wenn Sie das Sicherungsfenster in der Grafik nicht markieren möchten, deaktivieren Sie das Kontrollkästchen »Show backup window«.
- Session History: ermöglicht die Konfiguration von Aufbewahrungseinstellungen für die Indexdateien (Guest file system catalog) sowie für die Ereignishistorie (Event history). Hier gibt es einen Unterschied bei der Lizenz: Nur bei Enterprise und höher werden die Daten für die Indexe auch für archivierte Backups behalten.

Licensing

Hier können Informationen über eingetragene Lizenzen angesehen und neue Lizenzen für alle beteiligten Backup-Server eingetragen werden. Der EM sammelt Informationen über die Art der Lizenz, die auf den angeschlossenen BS installiert sind, sowie über die Anzahl der Instanzen in der Lizenz. Wenn der EM Datenbanken von Backup-Servern repliziert, synchronisiert er auch die Lizenzdaten (das heißt, er prüft, ob die auf dem BS installierte Lizenz mit der auf dem EM-Server installierten Lizenz übereinstimmt). Stimmen die Lizenzen nicht überein, wird die Lizenz auf dem Backup-Server automatisch mit der Lizenz auf dem Enterprise-Manager-Server aktualisiert. Sie können hier nicht die Lizenzen von Cloud- und lokalen BS gleichzeitig einspielen, sondern benötigen dafür unterschiedliche EM. Weitere Details zu Lizenzen habe ich unter Abschnitt »Lizenzierung« bereits aufgeführt.

Notifications

Um Benachrichtigungen vom EM zu bekommen, kann bei diesem Menüpunkt auf sechs Registerkarten das Notwendige eingestellt werden:

- Server Settings: Hier kann ein Mail-Server mit allen notwendigen Angaben eingetragen werden, damit der EM Benachrichtigungen als Zusammenfassung versenden kann.
- Job Summary: Um eine tägliche Zusammenfassung zu erhalten, können diese Felder ausgefüllt werden. Im Feld »Subject« wird bzw. werden eine oder mehrere Zahlen von 1 bis 6 eingetragen. Bei einem Klick auf das weiße »i« im blauen Kreis erfolgt eine Erklärung über die jeweiligen Zahlen. Ein Beispiel könnte folgender Eintrag sein: Fehler: %1, Warnungen: %2, Erfolg: %3. Die Parameter mit Prozent werden dabei automatisch aufgelöst und übermittelt.
- Lab Request: Sie können hier konfigurieren, dass Benachrichtigungs-E-Mails über Anfragen aus dem virtuellen Labor verschickt werden, die von Anwendern erstellt wurden, die Wiederherstellungen auf Objektebene der Universalanwendung (universal application item restore, U-AIR) durchführen müssen.
- Restore Operations: Werden Dateien wiederhergestellt (File Level Restore), so kann auch hier eine Nachricht vom EM aus versendet werden.
- License Information: Je nach installierter Lizenz (siehe Abschnitt »Lizenzierung« auf Seite 6) kann eine Benachrichtigung über das Ende des Support-Vertrages oder der Nutzung der Instanzen gesendet werden.
- Key Management: Alle Vorgänge bezüglich der Verschlüsselung können ebenfalls per Mail verschickt werden.

About

Hierüber bekommt man eine Anzeige über die Version des EM, des Katalogdienstes, der Softwareschnittstelle RESTful API und die URLs für den EM sowie das Self-Service Portal.

Menü des Enterprise Managers

Die acht Menüeinträge des EM und was man damit anfangen kann, möchte ich im Folgenden kurz erklären:

Dashboard

Die Übersichtsseite, die bei jedem Start der Oberfläche als Erstes angezeigt wird, liefert eine Zusammenfassung über die wichtigsten statistischen Daten und lässt sich für die letzten 24 Stunden oder die letzte Woche umschalten. Alle blauen Zahlen sind Links, die zu einer Registerkarte im Menü verzweigen.