Praxishandbuch Veeam Backup & Replication 12
für VMware und Microsoft Hyper-V

KAPITEL 6

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 mit Veeam, 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 Job« und wählen Sie aus dem Dropdown-Menü die passende Option:

- Virtuelle Maschine von VMware vSphere oder Microsoft Hyper-V
- Windows Computer – physischer Windows-Server oder Workstation
- Linux Computer – physischer Linux-Server oder Workstation
- Mac Computer – Computer mit MacOS Betriebssystem
- Unix Computer – Computer mit Oracle Solaris oder IBM AIX
- Application – Anwendungen für Oracle RMAN, SAP HANA oder SAP on Oracle
- 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 sowie Datum und Uhrzeit der Erstellung eingetragen. Diese Informationen sieht man auch in der Liste aller Jobs, deshalb sollte man dort ggf. etwas Aussagekräftiges eintragen wie die Uhrzeit, wann der Job läuft, wie oft etc. Diese Liste könnte man dann z. B. nach der Startzeit sortieren.

Setzt man das Häkchen bei »High priority«, so werden die VMs in diesem Job als Nächstes gesichert – unabhängig davon, wie viele noch vor ihnen in der Warteschlange wären. Das ist sinnvoll, wenn dieser Job zu einem bestimmten Zeitpunkt gestartet werden muss.

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:

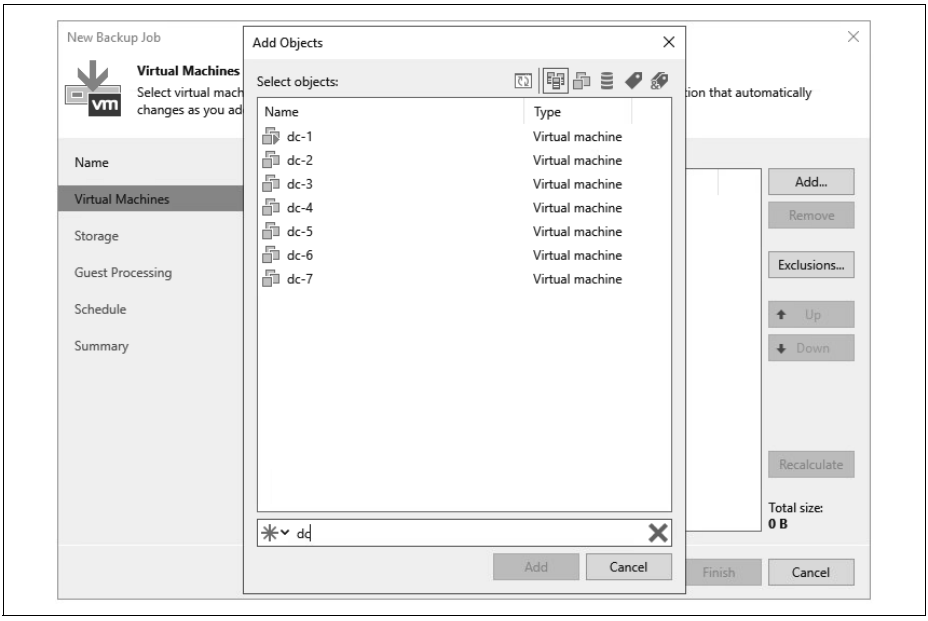


Abbildung 6-1: Auswahl der Objekte

Oben rechts in dem Fenster kann man über die Icons von links angefangen bei VMware:

1. die Ansicht aktualisieren,
2. die Ansicht »Hosts and Clusters«,
3. »VMs and Templates«,
4. »Datenspeicher und VMs«,
5. »VMs and Tags« oder
6. »Kombinationen von Tags«

auswählen.

Bei Hyper-V bedeuten die Icons:

1. die Ansicht aktualisieren
2. die Ansicht »Hosts and Clusters«
3. »Hosts and Volumes«
4. »VMs and Tags« (nur über SCVMM)
5. »VM Groups« (nur über SCVMM)

Bei »VMs and Tags«, also benutzerdefinierten Attribute, und beim letzten Icon »Tags combination« (nur die VMs, die alle ausgewählten Tags aufweisen) sollte man nach der ersten Sicherung überprüfen, ob das gewünschte Ergebnis erreicht wurde. Die Auswahl bei Tags ist nicht unbedingt immer zuverlässig.

Wenn man auf das blaue 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 6-2 dargestellt.

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.

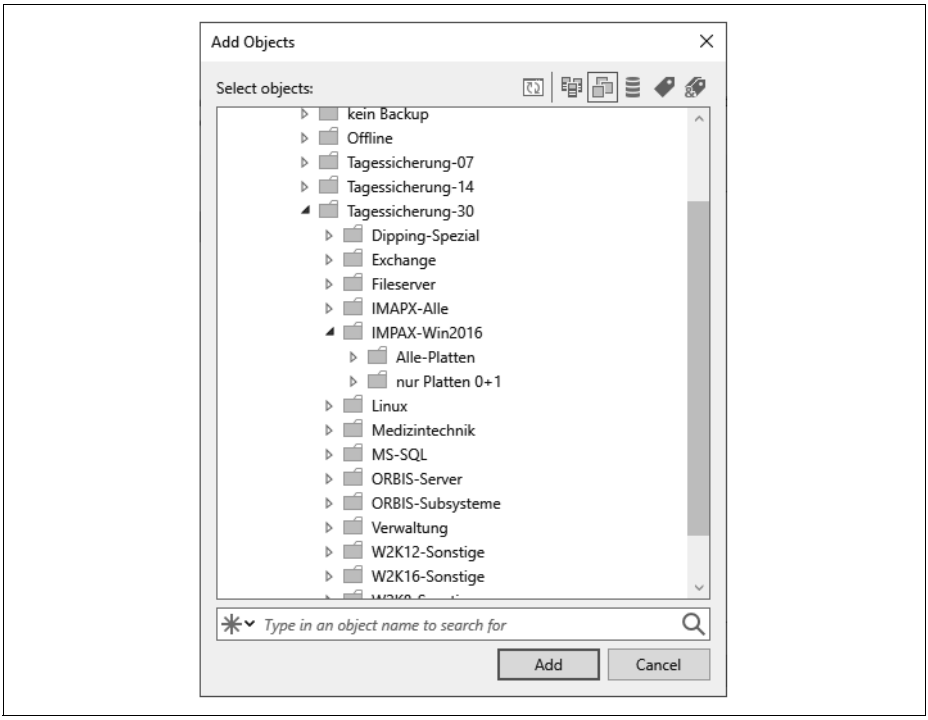


Abbildung 6-2: Ordnerstruktur für die Datensicherung

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 von den 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.

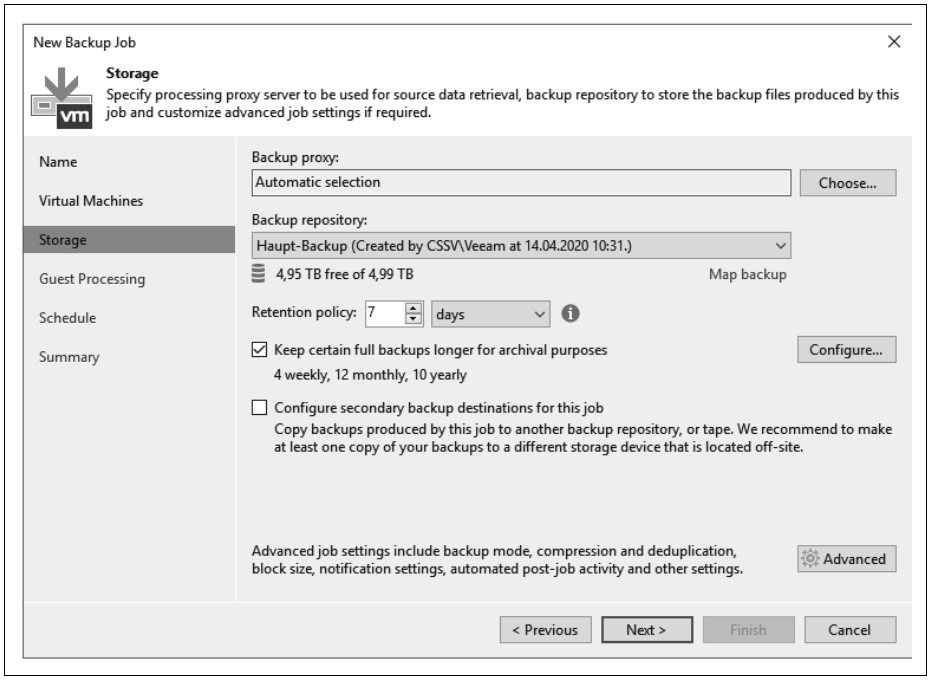


Abbildung 6-3: Backup-Job-Einstellungen

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 dem darunterliegenden Kästchen das 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.

Die Tage bei »Remove deleted VMs data after« sollten nicht unter »7« angegeben werden, weil es sonst bei einem vorübergehenden Ausfall der Infrastruktur zum Verlust aller Backups führen kann.

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« wird bzw. 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 Repositories 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 Blockgrößen im Dropdown-Feld ausgewählt werden. Dabei bedeutet
- »4 MB« (früher »Local target (large blocks)«), dass es sich um Storages handelt, auf denen die Dateien der Datensicherung größer als 16 TByte sind
- »1 MB« (früher »Local target«) einen lokalen Datenspeicher mit einer Übertragungsgeschwindigkeit ab 150 MByte/s. Dieses ist auch die richtige Einstellung für DAS und SAN.
- »512 KB« (früher »LAN target«) für Sicherungen auf NAS, Onsite Backup und Replikationen
- »256 KB« (früher WAN target«) für Backups über WAN-Strecken für Offsite-Sicherungen.

Der BS wird anhand dieser Einstellungen die jeweilige Komprimierung und Deduplizierung 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 12 ab Seite 177 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 Bemerkungen 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 »E-Mail-Settings« auf Seite 77).

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 »Guest Processing«.

Haben Sie das Einfrieren für die VMs in dem Job gewählt und aktivieren später zusätzlich das Kästchen 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 und VUL 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 auftauchen, wie in Abbildung 6-4 beispielhaft dargestellt.

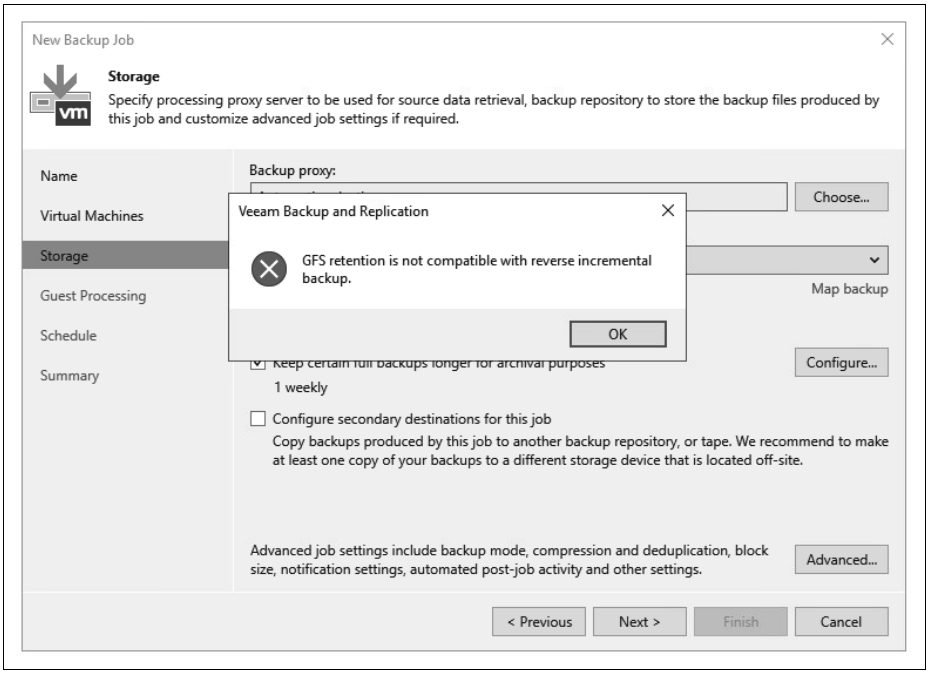


Abbildung 6-4: Konfigurationsfehler beim Backup Job

Hier wurde als Backup-Methode »Reverse incremental« oder »Incremental forever« (dann nur ein gelbes Dreieck) 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, SharePoint sowie bei PostgreSQL. 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 6-1 beschrieben:

Tabelle 6-1: 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 sowohl ohne als auch mit einer der genannten Anwendungen residieren, kann man für einzelne VMs das »application processing« hier deaktivieren, damit für diese das »quiescence« gilt.

Im unteren Teil bei »VSS Settings« 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.

Im letzten Abschnitt in diesem Fenster bei »Persistent guest agent« kann festgelegt werden, ob der spezielle Agent von Veeam dauerhaft in der zu sichernden Maschine verbleibt. Durch diese persistente Bereitstellung entfallen die Sicherheits- und Port-Anforderungen für die Injektion des Laufzeitprozesses.

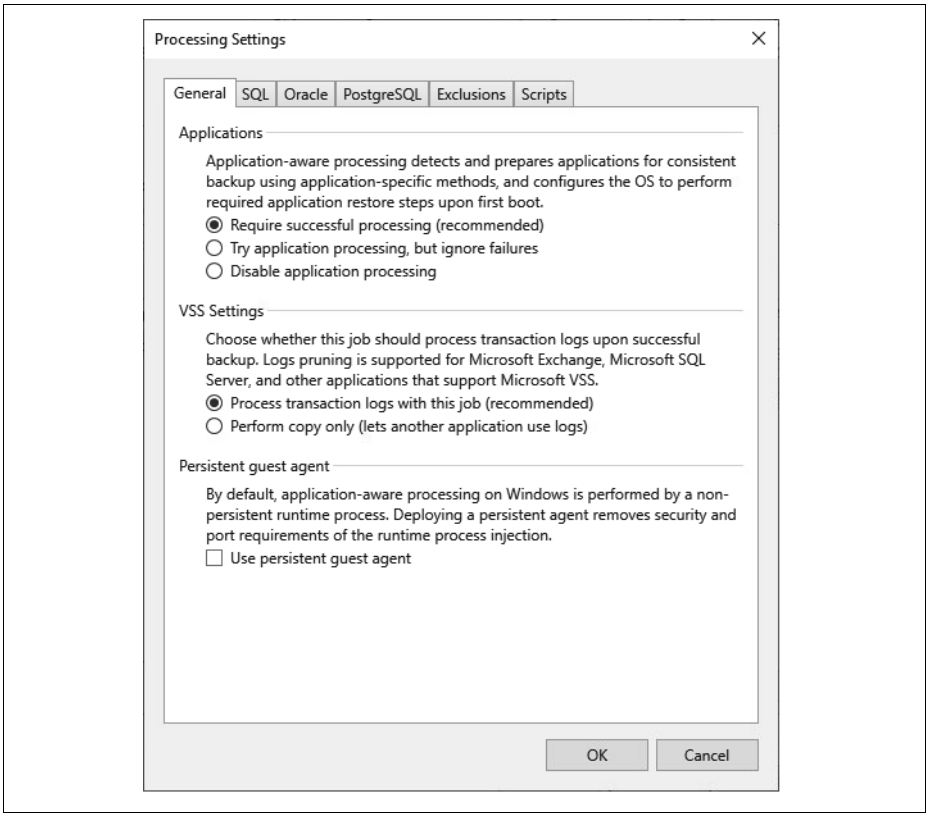


Abbildung 6-5: Erweiterte Einstellungen zu den Anwendungen

Auf den Registerkarten für »SQL«, »Oracle« und »PostgreSQL« 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 den Registerkarten »Oracle« und »PostgreSQL« kann man zusätzlich einen speziellen Benutzer mit Passwort angeben, der die notwendigen Rechte auf der Datenbank hat.

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 sollen 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 12). 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.

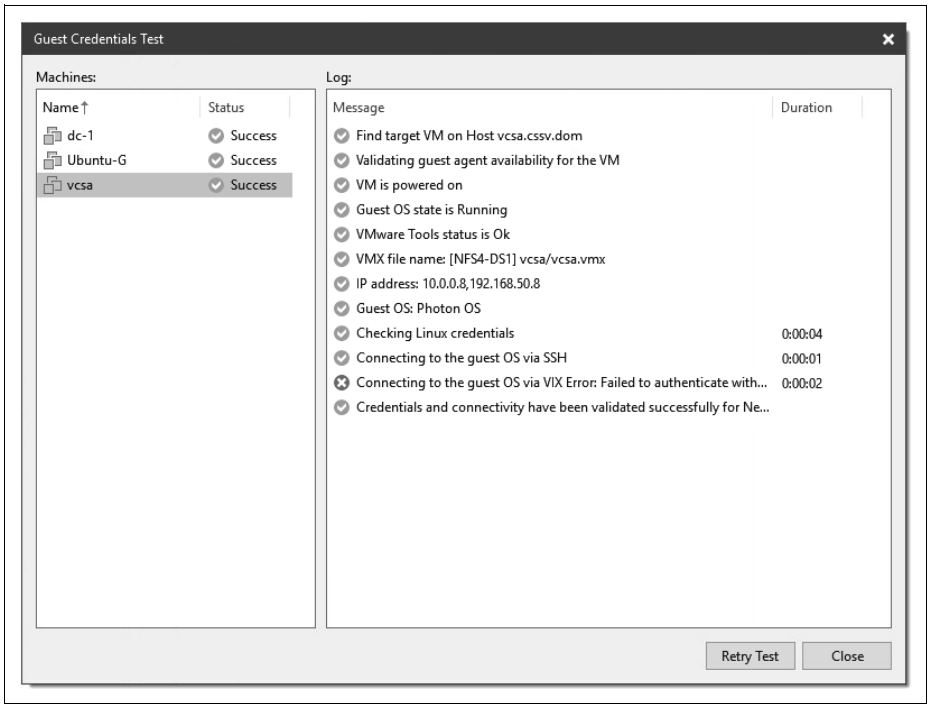


Abbildung 6-6: Anmeldedaten überprüfen

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 hotstandby, 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.

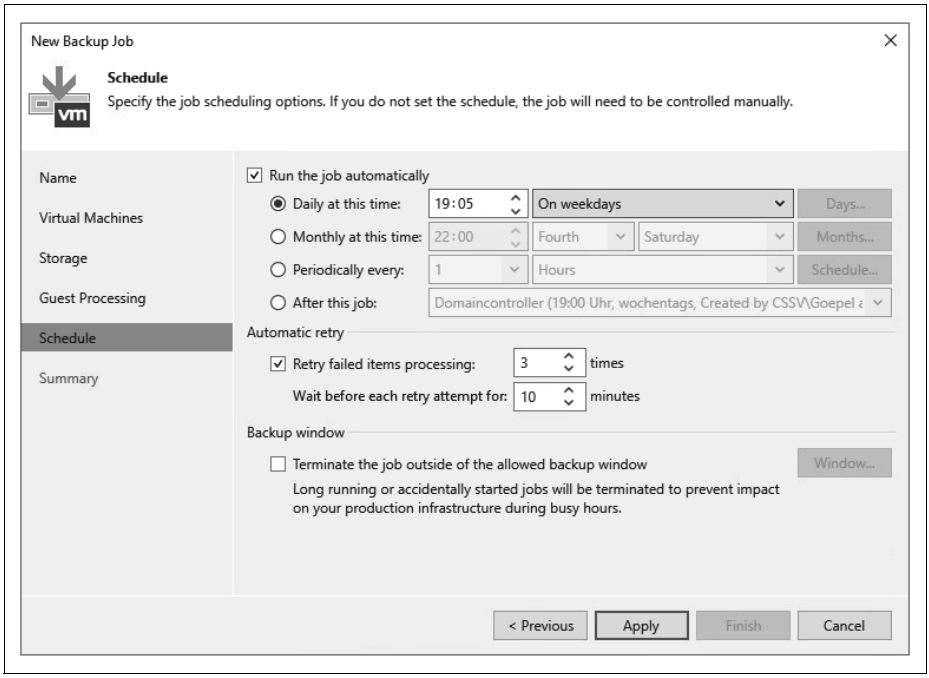
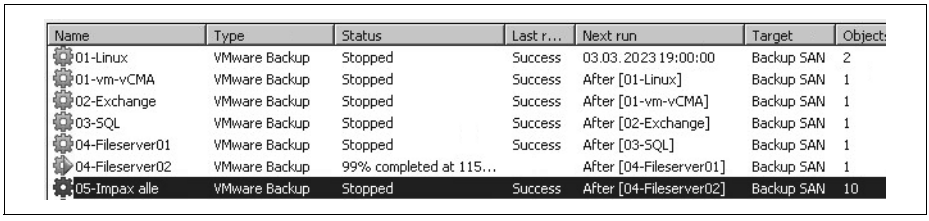


Abbildung 6-7: Auswahl der Sicherungsoptionen

In der Abbildung 6-8 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	03.03.2023 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 6-8: 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 bis 16:00 Uhr und ohne die Mittagspause.

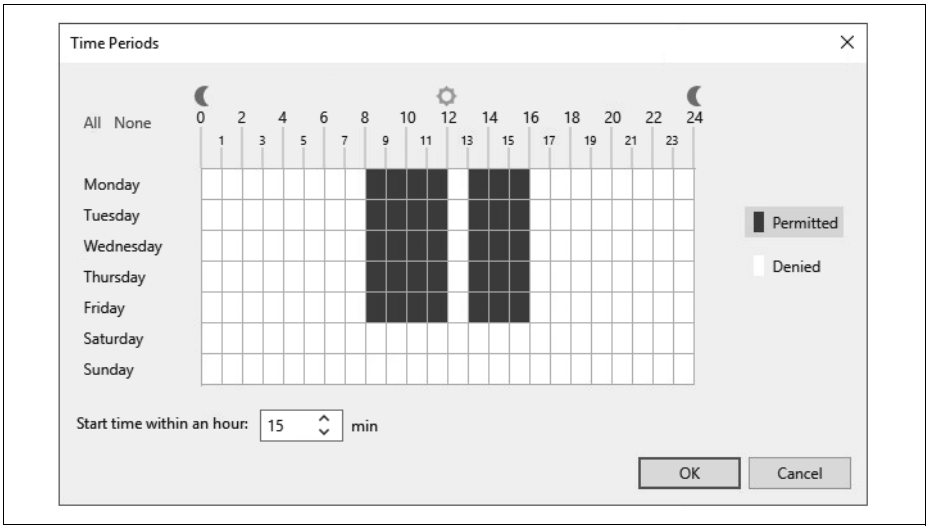


Abbildung 6-9: Sicherungen in Zeitintervallen

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 bis 11:15 Uhr und von 13:15 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 14 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: Domaincontroller — **Success**
19:00 Uhr, wochentags, Created by CSSV\Goepel at 03.03.2023 11:58. — 6 of 6 VMs processed

Dienstag, 7. März 2023 09:09:10

Success	6	**Start time**	09:09:10	**Total size**	590 GB	**Backup size**	395,8 MB
Warning	0	**End time**	09:12:31	**Data read**	3,7 GB	**Dedupe**	1,1x
Error	0	**Duration**	0:03:21	**Transferred**	391,9 MB	**Compression**	3,0x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
dc-3	Success	09:09:23	09:10:04	90 GB	0 B	109,3 KB	0:00:41	
dc-4	Success	09:09:23	09:10:05	90 GB	0 B	107,7 KB	0:00:42	
dc-7	Success	09:09:48	09:10:22	90 GB	0 B	18,6 KB	0:00:34	
dc-2	Success	09:09:23	09:10:45	150 GB	0 B	111 KB	0:01:22	
dc-6	Success	09:10:28	09:12:00	90 GB	0 B	109,4 KB	0:01:32	
dc-1	Success	09:09:23	09:12:25	80 GB	3,7 GB	391,4 MB	0:03:02	

Abbildung 6-10: Übersichts-Mail nach der Sicherung

Backup von verschlüsselten VMs

Bei VMware vSphere kann man 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.