KAPITEL 4

Infrastruktur

DNS ist für den Backup-Server und die ggf. eingesetzten Proxies sehr wichtig. Die Namensauflösung des FQDN sollte vorwärts wie rückwärts funktionieren. Dabei müssen der vCenter Server bzw. der SCVMM und alle beteiligten Hosts erkannt werden.

Möchte man die Datensicherung vom Host nicht über das Verwaltungsnetzwerk bekommen, sondern über ein extra dafür eingerichtetes schnelleres Netzwerk, so kann man auf allen Veeam-Komponenten die lokale Hosts-Datei dafür nutzen und somit die Namensauflösung über den DNS-Server umgehen.

vCenter Server, SCVMM und Hosts

In einer kleinen Umgebung reicht es, als Nächstes den SCVMM, den Hyper-V Cluster oder den vCenter Server anzugeben, den Backup-Speicher und Anmeldeinformationen der angegebenen Server sowie die administrativen Accounts für die Sicherung von speziellen Maschinen, wie Exchange, SQL, Active-Directory-Domaincontroller etc.

Haben Sie keinen SCVMM, Hyper-V Cluster oder vCenter Server, so können Sie auch den oder die Hosts hier eintragen. Wird ein Host aber vom SCVMM oder vCenter Server aus bedient, so sollte dieser Host nicht zusätzlich hier eingetragen werden.

Klicken Sie links unten in dem grauen Bereich auf »Backup Infrastructure« und dann im oberen Bereich links auf »Managed servers«. In dem nun folgenden Fenster (siehe Abbildung 4-1) wählen Sie den SCVMM oder vCenter Server aus, indem Sie auf »Microsoft Hyper-V« oder »VMware vSphere« klicken. Bei der Erstinstallation erscheint dieses Fenster automatisch.

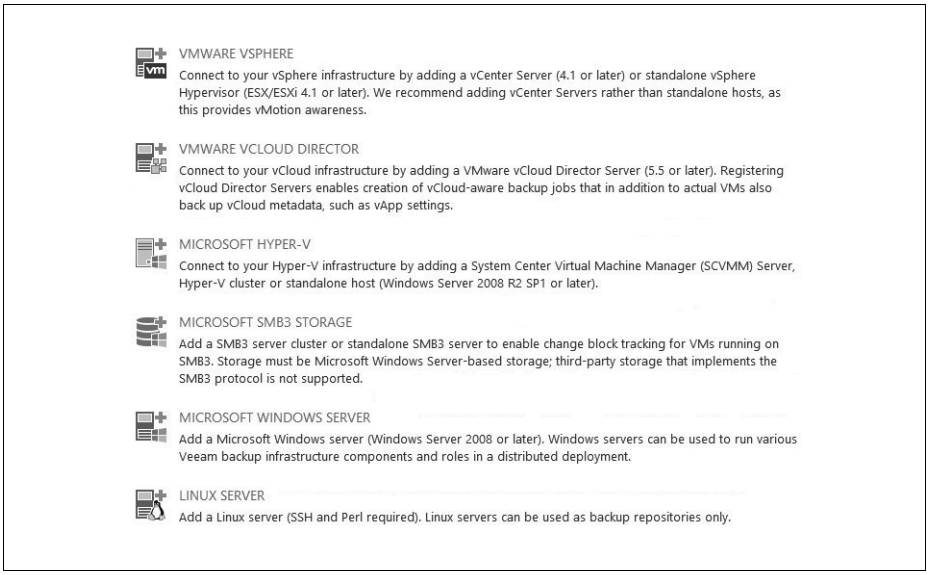

Abbildung 4-1: Virtuelle Infrastrukturkomponenten hinzufügen

Geben Sie den DNS-Namen des Management Servers an und klicken Sie auf »Next«. Im nächsten Fenster klicken Sie auf die Schaltfläche »Add« und geben dort die Domäne und den Namen des Zugriffsberechtigen an oder suchen Sie ihn über »Browse«. Vergessen Sie nicht, den Suchpfad auf die Domäne zu setzen und das Passwort einzutragen. Über den Link »Manage accounts« sehen Sie alle schon eingetragenen Benutzer und können diese ggf. entfernen, bearbeiten oder weitere hinzufügen. Anschließend versucht Veeam B&R eine Verbindung über den SSL Port 443 mit dem Server aufzubauen. Sehen Sie sich die Zusammenfassung an und klicken Sie auf »Finish«.

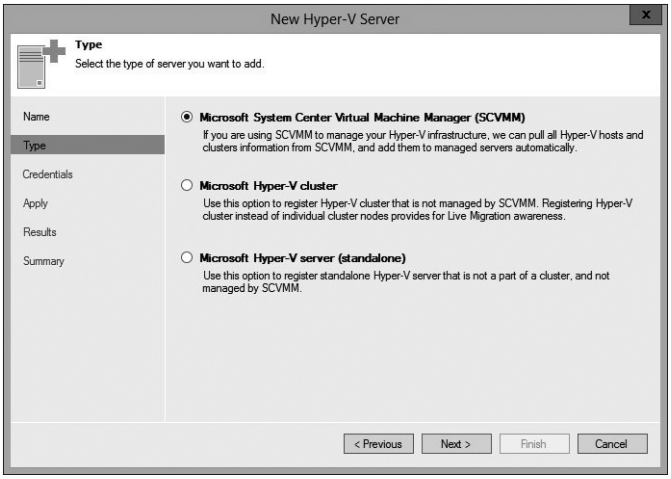

Abbildung 4-2: Hinzufügen weiterer Hypervisor

Sie können jetzt weitere SCVMM, vCenter Server oder auch alleinstehende Hosts (bei VMware: nur lizenzierte, keine kostenlosen) und einen Hyper-V Cluster nach Bedarf hinzufügen. Diese sollten aber nicht gleichzeitig auch zum hinzugefügten Management Server gehören, sonst wird eine VM doppelt gefunden.

Bei einem Windows-Server kann es sich hier nur um einen »Backup Proxy« oder ein »Backup Repository« handeln, bei einem Linux-Server nur um ein »Backup Repository«. Auf jedem weiteren Windows-Server werden der Veeam-Installer-Dienst und Veeam Transport installiert. Dafür müssen die Datei und die Druckerfreigabe aktiviert worden sein und ab Server 2012 ggf. die Ports in der Firewall freigeschaltet werden.

Repositories

Auf einem Backup-Speicher werden alle relevanten Dateien einer oder mehrerer VMs aus einem Backup Job abgespeichert. Ein solches Repository kann jeder Windows- oder Linux-Rechner, eine Windows-Freigabe oder auch eine oder mehrere lokale Festplatte(n) sein. Selbstverständlich können Sie die Daten auch auf ein NAS, SAN oder einem deduplizierenden Speicher ablegen, dieses sollte aber nicht gleichzeitig der Storage der virtuellen Infrastruktur sein, also auf dem die zu sichernden VMs liegen.

Klicken Sie unter »Backup Infrastructure« links oben auf den Eintrag »Backup Repositories« und dann auf »Add Repository«. In der Liste auf der rechten Seite ist der Standardspeicher bereits eingetragen, der aber meist nicht für große Daten-

mengen geeignet ist. Wählen Sie einen der vier zur Auswahl stehenden Typen aus, die nachfolgend beschrieben werden.

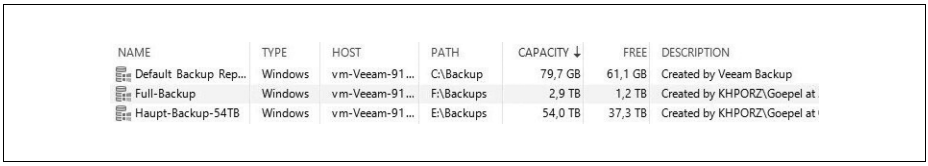

Abbildung 4-3: Datensicherungsspeicher angeben

Microsoft Windows Server

Geben Sie einen sprechenden Namen für den Speicher und ggf. eine Beschreibung an.

Ist es ein lokal angeschlossener Speicher, klicken Sie auf »Next« und wählen Sie ggf. die Schaltfläche »Populate«, um alle angeschlossenen Datenträger mit deren Kapazität und freiem Speicherplatz zu sehen.

Unter dem Punkt »Load control« können die maximal möglichen gleichzeitigen Tasks angegeben werden. Diese hängen von der Geschwindigkeit des jeweiligen Storage ab. Auch kann man die maximale Anzahl von Daten (in MByte pro Sekunde) angeben, damit der Datenspeicher nicht überfordert wird (meistens unnötig).

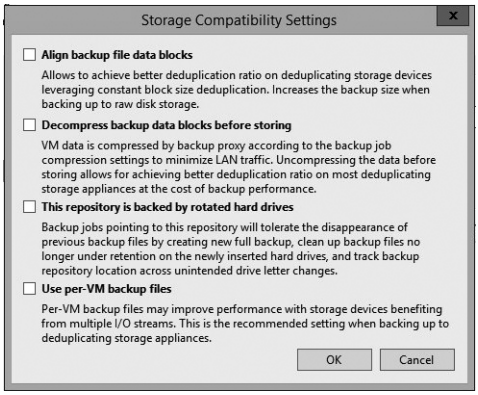

Abbildung 4-4: Erweiterte Einstellungen zum Repository

Hinter der Schaltfläche »Advanced« verbergen sich noch vier weitere Punkte:

- *Align backup file data blocks* bedeutet, dass bei Speichersystemen mit fester Blockgröße eine Ausrichtung der Daten an der 4-KByte-Grenze gemacht wird.

Damit kann zwar eine bessere Deduplizierung erreicht werden, aber auch eine höhere Fragmentierung und eine große Menge ungenutzten Speichers.

- *Decompress backup data blocks before storing* bedeutet, dass die Daten vor der Speicherung wieder ausgepackt werden. Veeam komprimiert die Daten vor der Übertragung auf einen Speicher, um die Performance zu steigern. Gepackte Daten lassen sich auf einem deduplizierten Speicher aber nicht so platzsparend ablegen.
- *This Repository is backed by rotated hard drives* bedeutet, dass die Speicherung der Daten z.B. auf verschiedenen externen Festplatten gemacht wird. Vergisst man diesen Punkt, so schlägt das übernächste Backup fehl, weil Veeam die vorherigen Daten nicht findet. Bei dieser Option wird immer ein Full Backup gemacht, wenn das letzte Medium nicht vorhanden ist bzw. ausgetauscht wurde. Das bedeutet auch, dass das Medium genug Platz für zwei Full Backups haben muss oder vor jedem Job geleert werden muss. Sind noch nutzbare Daten vorhanden, versucht der BS die bereits vorliegenden Blöcke zu nutzen und macht eine inkrementelle Sicherung. Diese beinhaltet alle Unterschiede zu den gefundenen Daten und kann je nach Stand der alten Sicherung sehr groß werden. Um vorherige Daten von dem Datenträger zu löschen, kann ein Skript genutzt oder es kann auch speziell für diesen Fall ein Eintrag in die Registry gesetzt werden (siehe Kapitel 15).
- *Use per-VM backup files* bedeutet, dass die Daten für einen deduplizierten Speicher optimiert abgelegt werden. Hierbei können mehrere I/O-Kanäle genutzt werden. Üblicherweise werden alle VMs in einem Job in einer einzelnen Datei auf das Repository geschrieben. Läuft nur jeweils ein Job für das Datastore, kann es sinnvoll sein, »Pro VM-Backup File« zu aktivieren, damit mehrere Streams die Übertragung zum Storage besser ausnutzen. Gerade auf einem deduplizierenden Store wird dies empfohlen, bei einem »Scale-out Repository« ist dies standardmäßig aktiv. Dafür sollte »Parallel Data Processing« aktiviert sein. Diese Option kann nicht für wechselnde Datenträger »This Repository is backed by rotated hard drives« eingesetzt werden, Data Deduplication ist dann nicht mehr pro Job, sondern pro VM. Als Lizenz braucht man hierfür Enterprise oder höher, sonst steht die Option nicht zur Verfügung, und Backups schlagen fehl, wenn die Lizenz nachträglich herabgestuft, also unter Enterprise eingespielt wird. Ändert man die Einstellungen nachträglich, so werden bestehende Backups auf dem Repository nicht geändert. Erst nach dem nächsten Full Backup (FB) ziehen die gemachten Einstellungen. Bei synthetischen Full Backups jedoch nicht; man kann hier aber ein manuelles FB starten, um die Änderungen zu aktivieren.

Bei den »Retention Points« wird ebenfalls der Job berücksichtigt, nicht die VM. Sind im Job drei VMs, wobei eine nur zwei Mal richtig gesichert wurde, die anderen fünf Mal, so werden bei der sechsten Sicherung trotzdem alle Wiederherstellungspunkte der drei VMs gelöscht!

vPower NFs kann im nächsten Abschnitt gewählt werden. Handelt es sich um den lokalen Server, so kann man hier auf »Next« klicken. Ist es aber ein entfernter Windows-Speicher, so sollte dort auch diese Komponente installiert werden (über Add Server). Über vPower NFS kann man aus dem Backup-Speicher heraus VMs direkt auf einem Host starten und später dann verschieben (Instant VM recovery).

Sind auf diesem Speicher noch ältere Sicherungen von Veeam, so können diese jetzt importiert werden (Kästchen anklicken).

Linux-Server

Haben Sie den zweiten Typ gewählt, so kann sein interner, ein an ihn direkt angeschlossener oder ein NFS-Speicher dafür in Frage kommen. Klicken Sie auf die Schaltfläche »Add new« und geben Sie den DNS-Namen oder die IP-Adresse des Servers ein. Ein SSH-Zugriff über den Port 22 muss dabei möglich und es muss über den Account ein Schreibzugriff erlaubt sein. Handelt es sich um einen alleinstehenden NFS Storage, so muss dort ggf. noch Pearl installiert werden.

Shared Folder

Eine Windows-Freigabe über SMB (Server-Message-Block-Protokoll) oder CIFS (Common Internet File System) wird über einen UNC-Pfad hinzugefügt, also z.B. `\\Servername\Freigabname`. Geben Sie ggf. hierfür notwendige Berechtigungen ein und überlegen Sie sich bei langsamen Verbindungen, ob ein zusätzlicher Gateway-Server (Proxy) dafür genutzt werden soll.

Deduplicating Storage Appliance

Wenn das hinzuzufügende Repository selbst dedupliziert, müssen Sie den letzten der vier Punkte auswählen, ansonsten schlägt die Sicherung darauf fehl. Unterstützt werden zurzeit Dell EMC Data Domain, ExaGrid und HP StoreOnce. Wählen Sie im nächsten Fenster Ihren Storage und füllen Sie die benötigten Felder entsprechend aus. Ist der Storage über Fibre Channel (FC) angeschlossen, so denken Sie zusätzlich an das Zoning für den Zugriff.

Archive Repositories

Erst ab der Version 10 werden sogenannte Archive Repositories für die Langzeitarchivierung als »Scale-out Repositories« angeboten – welche man statt der Sicherung auf Bandlaufwerke konfigurieren kann. Hierbei wird es möglich sein, Daten ab einem bestimmten Zeitpunkt (z.B. 30 Tage) dorthin verschieben zu lassen. Es ist also kein zusätzlicher Job mehr für diese Aufgabe notwendig.

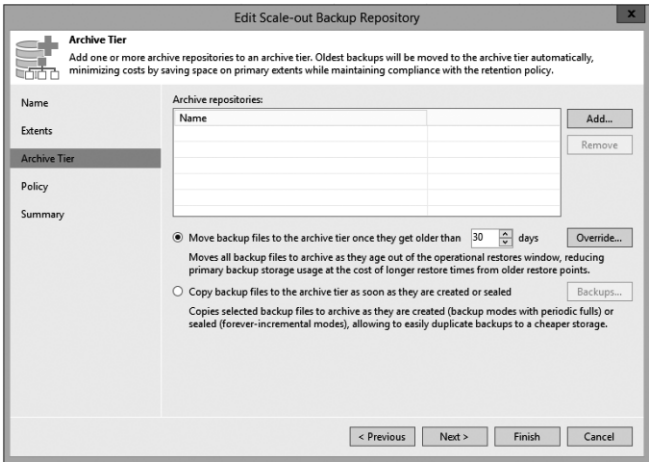

Abbildung 4-5: Scale-out Archive Repositories

Vorteile des Deduplizierungsspeichers

Die von Backup & Replication verwendete Deduplizierungs-Speichertechnologie wurde von Veeam selbst entwickelt und ist in die Anwendung integriert. Diese Technologie wertet auf dem Sicherungsspeicher vorhandene Blöcke aus, die in Wiederherstellungspunkten gespeichert werden, und überprüft, ob identische Abschnitte bereits vorhanden sind.

Speichern Sie gleiche Maschinen möglichst im selben Job, damit mehrere Sicherungsaufgaben über die Deduplizierungs-Speichertechnologie besser zusammengefasst und die Deduplizierungsraten maximiert werden. Sie müssen aber nicht alle gleichartigen VMs in derselben Sicherungsaufgabe zusammenfassen – die Deduplizierung funktioniert darüber aber deutlich besser.

Die Deduplizierung wird für alle gespeicherten virtuellen Maschinen ausgewertet, selbst wenn einige zurzeit nicht gesichert werden; es werden aber nur identische Blöcke innerhalb einer Sicherung berücksichtigt.

Es können Speicherplätze für die Sicherungen von fast beliebiger Größe angegeben werden, und die Anzahl ist jeweils nur auf das Betriebssystem beschränkt, auf dem Sie installieren.

Die Menge des benötigten Speichers für die Sicherungen variiert je nach der Menge an Festplattenspeicher, den die Deduplizierung durch die Ausführung von ähnlichen virtuellen Maschinen sparen kann.

Haben Sie als Repository einen deduplizierenden Storage gewählt, macht Veeam hier keine zusätzliche Deduplizierung.

Proxies

Bei der Installation des B&R-Servers wird dieser auch automatisch zu einem Backup Proxy. In größeren Umgebungen oder bei speziellen Anforderungen sollten zusätzliche Windows-Maschinen (physisch oder virtuell) als Proxy z. B. für einen Lastausgleich installiert werden. Der Backup Proxy befindet sich logisch zwischen der virtuellen Umgebung und dem Backup-Server und wird von diesem gesteuert.

Ein Backup Proxy wird auch als »Data Mover« bezeichnet und erhält die Daten, bearbeitet sie und transferiert diese auf den Zielspeicher. Ein Proxy entlastet den Backup-Server, da er die Daten für die Speicherung bereits vorbereitet. Je größer eine virtuelle Umgebung ist, umso mehr Backup Proxies sollte man einsetzen. Der »Transport Mode« wird beim Hinzufügen eines Servers meistens richtig erkannt: direkter Zugriff auf SAN, Virtual Appliance oder Netzwerk.

Den Transportmodus kann man nicht beim Backup Job auswählen, sondern nur beim Backup Proxy. Bei einem Job können Sie aber den jeweiligen Proxy mit eingestelltem Modus festlegen.

Möchte man über langsame Verbindungen einen Datenaustausch machen, so kann man hier auch die Bandbreite (Throttling) einstellen.

Die Installation des Proxies erfolgt vom Backup-Server aus und kann – je nach Bedarf – auf einem physischen oder virtuellen Windows-Rechner erfolgen.

Seine Aufgaben sind: VM-Daten vom Produktions-Storage zu holen, diese zu komprimieren und zu deduplizieren, ggf. zu verschlüsseln und anschließend an das Backup Repository oder an einen anderen Proxy (WAN-Strecken oder Replikation) zu senden.

Ein Proxy kann für verschiedene Aufgaben oder Zwecke eingesetzt werden:

- eine optimale Route zu einem verzweigten Netzwerk
- direkter Zugriff auf ein Storage
- von der Architektur her näher an den VMs
- etc.

Wenn Sie Lizenzen für einen Windows-Server einsparen wollen, können Sie auch eine Workstation Edition als Proxy nutzen. Nehmen Sie hier möglichst ein 64-Bit-Betriebssystem und entsprechenden RAM und Anzahl an CPUs. Die Anforderungen an einen Proxy sind dabei relativ gering: 200 MByte RAM pro zu verarbeitenden Task reichen mittlerweile aus. Haben Sie einen Proxy mit vielen CPUs, können Sie den »default compression level« auf »Optimal« einstellen, um Daten schneller übertragen zu können. Dabei wird die CPU-Last ca. um das Doppelte steigen, aber die Daten werden ca. um die Hälfte schrumpfen. Diese mit der Ver-

sion 9.5 eingesetzte Technik nennt sich »Advanced Data Fetcher« und entlastet die virtuelle Umgebung durch die Reduzierung von I/O-Operationen wesentlich.

Wenn Sie mehrere Proxies einsetzen, sollten Sie den Backup-Server nicht als Proxy und wenn möglich auch nicht als Repository laufen lassen. Dies lässt sich nachträglich in der Infrastruktur leicht erledigen.

On- und Off-Host Proxies

Nur unter Hyper-V gibt es den Unterschied zwischen diesen beiden Versionen des Proxies. Grob gesagt befindet sich der On-Host Proxy auf dem Hyper-V-Server, der Off-Host Proxy auf einem anderen Windows-Rechner.

Der Off-Host Proxy entlastet den Hyper-V-Server, indem er einen Volume-Snapshot auf dem Host initiiert, auf dem die zu sichernde VM liegt. Diesen Snapshot bindet er sich als Quelle direkt an, verarbeitet die Daten und transferiert diese zum Repository. Ist der Vorgang abgeschlossen, wird der Snapshot gelöst und anschließend gelöscht.

Achten Sie bei der Auswahl des Off-Host Proxies auf das Häkchen bei »Failover«, das gesetzt sein sollte (siehe Abbildung 4-6).

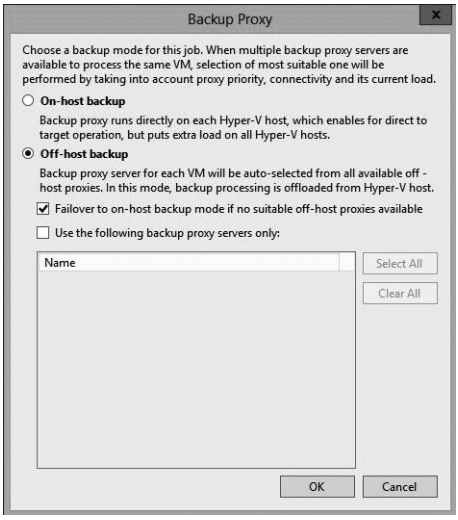

Abbildung 4-6: Hyper-V Off-Host Proxy

Auf einem Hyper-V Cluster mit CSV (Cluster Shared Volumes) darf ein Off-Host Proxy nicht zum Cluster gehören. Da der Snapshot dieselbe LUN-Signatur hat wie das Volume, muss er außerhalb des Clusters verarbeitet werden, ansonsten kann das Cluster ausfallen.

WAN Accelerators

Für eine WAN-Strecke wird eine Internetverbindung von 5 MBit/s benötigt. Bei der Enterprise-Plus-Version kann man dann sogenannte WAN Accelerators einsetzen, die ein besonderes Komprimierungsverfahren nutzen. Diese können den Datenverkehr um bis zum 50-fachen beschleunigen.

Die WAN Accelerator werden immer als Paar eingesetzt: einer an der Quellseite, der andere an der Zielseite, die die zu übertragenden Daten cachen und deduplizieren – deshalb sollte die Maschine genug Festplattenspeicher haben (üblicherweise 10 GByte pro eingesetztem Betriebssystem und zusätzlich 20 GByte pro TByte-Daten auf der Zielseite). Die Installation wird wie beim Proxy beschrieben direkt vom B&R-Server auf einer 64-Bit physischen oder virtuellen Windows-Maschine durchgeführt. Ein bereits bestehender Proxy oder ein Repository-Server kann diese Aufgabe auch zusätzlich übernehmen, wenn er mindestens 8 GByte RAM hat.

Wenn Sie einen Ziel- oder Quell-WAN-Beschleuniger zur Umgebung hinzufügen, sollten Sie bei den Bemerkungen (Description) unbedingt etwas eintragen, weil dieser Text, z.B. Quelle oder Ziel, auch bei der Auswahl bei einem Job erscheint – das macht die Arbeit einfacher.

Transportmodi

Um an die Daten der VMs zu kommen, gibt es drei verschiedene Möglichkeiten:

1. Direct Storage Access – direkter Zugriff auf das Storage über das jeweilige Protokoll (FC, FCoE, iSCSI, NFS)
2. Virtual Appliance – Anbinden der VM-Festplatte der zu sichernden VM an den eigenen SCSI-Adapter
3. Network – über das Netzwerk

Welcher der drei Modi genommen wird, entscheidet der Backup-Server oder Proxy selber, wobei man beim Backup Job dies auch einstellen bzw. erzwingen kann. Werden keine manuellen Einstellungen vorgenommen, so überprüft der Backup-Server die Möglichkeiten und entscheidet sich für das Beste in folgender Reihenfolge: Direct Storage Access, Virtual Appliance oder Network (NBD = Network Block Device).

Bei VMware erfolgt der Zugriff bei allen drei Möglichkeiten über die Softwareschnittstelle VADP (vSphere API for Data Protection), weshalb ein kostenloser ESXi hier nicht eingesetzt werden kann.

Direct Storage Access

Veeam Backup & Replication kann Daten direkt vom/zum Storage-System, auf dem die VMs oder Backups liegen, lesen und schreiben. Es wird weiterhin über das Protokoll SCSI (SAN), NFS (NAS) und SMB3 (Windows Freigabe) unterschieden, wie im Folgenden erklärt.

Direct SAN Access (DSA)

Diese Zugriffsart wird empfohlen, wenn die zu sichernden VM-Daten auf einem gemeinsamen SAN Volume liegen, welches über Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), Internet SCSI (iSCSI) angeschlossen ist oder auf einem gemeinsam genutzten DAS Storage (Direct Attached Storage, SAS oder SCSI) liegen. Bei diesen Zugriffen wird weder der Host noch das Netzwerk belastet, und die Übertragungsgeschwindigkeit ist meist deutlich höher als bei den anderen Möglichkeiten.

Dieser Modus kann für Backups, Replikationen, Wiederherstellung von VMs oder deren Dateien und Replica Failback eingesetzt werden.

Voraussetzungen für DSA

Um eine optimale Geschwindigkeit zu bekommen, sollte es sich bei der Maschine für DSA um eine physische Maschine handeln (iSCSI über eine VM ist nicht sinnvoll, weil dieses wiederum den Host belastet). Weiterhin muss diese über einen Hardware- oder Software-HBA (Host Bus Adapter) verfügen. SAN Volumes müssen für das Betriebssystem des Rechners sichtbar sein, es darf aber keine Initialisierung der Datastores erfolgen, weil diese sonst für die Hosts unbrauchbar wären. Veeam setzt die SAN-Berechtigung automatisch auf »Offline Shared«, um so eine Änderung zu verhindern. Für eine Wiederherstellung muss der Zugriff aber schreibend erlaubt werden. Überdenken Sie dabei die Berechtigungen für User auf so einem Gerät. Verwenden Sie lieber wenige, aber stärkere Proxies für diesen Zugriff.

Begrenzungen beim DAS

- Ein VMware vSAN kann hier nicht genutzt werden, hier muss einer der anderen beiden Modi zum Tragen kommen.
- Ebenfalls werden virtuelle Volumes (vVol) von Veeam nicht unterstützt. VMs werden über DSA nicht gesichert, wenn auch nur eine der VM-Platten auf so einem Storage liegt.
- Bei einer Replikation wird nur beim ersten Mal in diesem Modus geschrieben, gelesen wird immer so.
- Beim DSA werden nur Thick-, keine Thin-Provisioning-Festplatten berücksichtigt, wohl aber das »Thin Provisioning« vom Storage selber.

- Eine inkrementelle Wiederherstellung wird nicht unterstützt. Wenn man CBT (Changed Block Tracking) deaktiviert, funktioniert allerdings die Wiederherstellung, oder man nutzt einen der anderen beiden Modi.
- Ab vSphere 5.5 werden auch IDE- und SATA-Festplatten unterstützt, bei 5.1 und älter nur lesend – nicht schreibend.
- Die »Advanced Data Fetcher«(ADF)-Technologie (entlastet die VMware-Umgebung durch die Reduzierung von I/O-Operationen) kann hier nicht genutzt werden, außer es werden Snapshots vom Storage genommen (empfohlen).

Wenn Sie iSCSI-Verbindungen nutzen, sollten Sie zum einen die »TCP-Windows Size« in der Registry auf 65.500 setzen (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\GlobalMaxTcpWindowSize) und das »autotuning« deaktivieren: [netsh interface tcp show global] zum Anzeigen der Einstellungen, [netsh interface tcp set global autotuning = disable] zum Abschalten.

Direct NFS Access

Werden VMs auf einem NFS Storage betrieben, sollte für den Veeam Backup & Replication Server der direkte Zugriff auf die Volumes ermöglicht werden, um den ESXi Host zu entlasten (Microsoft unterstützt kein NFS-Protokoll). Veeam bringt einen optimierten nativen NFS Client mit, der für Backups, Replikationen, Quick Migration, VM Copy, vollständiges Wiederherstellen einer VM, Festplatten-Wiederherstellung und das Replica Failback genutzt wird. Im Gegensatz zum DAS wird hier die Advanced-Data-Fetcher-Technologie unterstützt. Gerade bei Hyper Converged Systems sollte diese Zugriffsart genutzt werden.

Es kann sowohl das Protokoll v.3.0 als auch v.4.1 genutzt werden. Sind am ESXi die NFS Volumes mit Namen statt IP-Adresse verbunden, muss der Backup-Server diese Namen auflösen können (ggf. eine lokale Hosts-Datei verwenden).

Direkter NFS Zugriff kann nicht verwendet werden, wenn die VM schon einen Snapshot hat, und bei der Replikation geht das Updaten nicht. Der Zugriff geht ebenfalls nicht, wenn VMware Tools quiescense beim Job aktiviert wurden. In allen Fällen, in denen der NFS Zugriff nicht funktioniert, werden die Daten übers Netzwerk übertragen.

Über die Einstellungen beim Proxy kann man den Transportmodus auswählen (siehe Bild). Der Proxy muss lesend und schreibend auf die NFS Volumes zugreifen können und Root-Rechte besitzen.

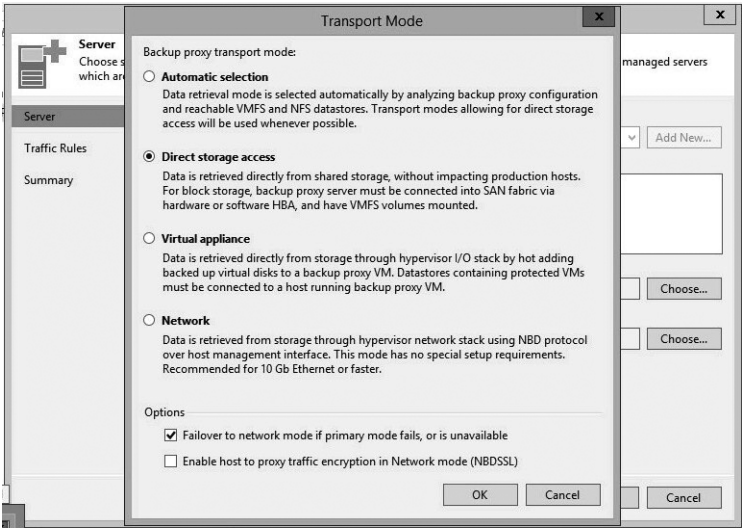

Abbildung 4-7: Wählbare Transportmodi

SMB3-Speicher

Unter Hyper-V können VMs auch auf einem Windows 2012 (oder höher) Cluster oder einer Standalone-Freigabe laufen, im Gegensatz zu VMware vSphere. Veeam unterstützt die Sicherung von diesen Speichern, weshalb sie (Microsoft SMB3 Server) zusätzlich zu den Hosts zur Bestandsliste hinzugefügt werden sollten. Anderenfalls kann das bereits oben beschriebene CBT-Verfahren nicht für diese VMs genutzt werden. Eine Ausnahme bildet dabei der Server 2016: Hier muss die Freigabe nicht hinzugefügt werden, sollte aber, damit man mehr Kontrolle (maximale Anzahl an Snapshots und die Latenz-Kontrolle) über diesen Storage bekommt.

Appliance-Modus

Der virtuelle Appliance-Modus ist nur bei vSphere vorhanden und nicht so effektiv wie die DSA-Modi, aber besser als der Netzwerkmodus. Dafür wird eine VM als Proxy eingesetzt, die sich die Festplatten der zu sichernden VMs lokal an seinen SCSI-Adapter mountet (HotAdd). Da die Daten direkt vom ESXi Storage kommen, ist es ähnlich wie bei DAS – nur dass der Stack vom Host verwendet wird. Dieser Modus kann für Backup, Replikation, VM Copy, Quick Migration, vollständige VM-Wiederherstellung, Festplatten-Wiederherstellung und Replica Failback genutzt werden. Gerade für das schnelle Wiederherstellen ganzer VMs wird dieser Modus empfohlen, zumal jede Storage-Art hier Unterstützung findet. Wenn möglich, sollte in großen Umgebungen pro Host – zumindest pro Cluster – je ein Proxy dafür eingesetzt werden.

Einschränkungen:

- Bei vSphere 5.1 und älter darf die VMDK-Datei nicht größer als 1,98 TByte sein.
- IDE-Festplatten werden nicht unterstützt.
- Für das HotAdd werden keine paravirtuellen SCSI-Adapter auf der Appliance unterstützt.
- Erst ab vSphere 6.0 werden SATA-Festplatten unterstützt.

Dieser Modus ist die einzige Möglichkeit für VMs, die auf vSAN Volumes liegen oder verschlüsselt sind.

Achten Sie darauf, dass Ihre Appliance keinen paravirtuellen SCSI-Adapter hat, da dieser für das HotAdd nicht unterstützt wird. Fügen Sie ggf. einen weiteren SCSI-Adapter zum Proxy hinzu. Überprüfen Sie auch regelmäßig, ob die Festplatten der zu sichernden VMs korrekt wieder gelöst wurden, sonst bleibt ein Snapshot zurück und die Platten müssen manuell konsolidiert werden. Bitte nicht bei NFS Storages einsetzen, nehmen Sie lieber Direct NFS Access oder setzen Sie den Registry Key »HKLM\Software\Veeam\Veeam Backup and Replication\EnableSameHostHotaddMode« (DWord, Wert 2) ein! Proxies sollten nicht geklont werden, das Ausrollen von Templates für diesen Zweck geht aber.

Netzwerkmodus

Diese Variante kann für jegliche Infrastruktur genutzt werden. Bei diesem Modus werden die Daten über den Host über das Netzwerk (NBD = Network-Block-Device-Protokoll) übertragen. Dieses ist die langsamste Möglichkeit für den Backup-Server, aber die einzige Art, wenn man einen physischen Proxy und lokale Platten auf dem Host hat. Die zu sichernden Daten werden nach dem Snapshot der VM vom Host gelesen und über das Netzwerk (Management Network = Verwaltungsdatenverkehr) an den Proxy geliefert. Der Host drosselt dabei die Übertragungsrate auf ca. 25 MByte/s bei 1-GBit-Adaptern für NBD und NBDSSL. Auch hier ist die ADF-Funktion nicht nutzbar.

Für kleine Übertragungsdaten und bei 10 GE (Gigabit Ethernet) ist das eine gute Möglichkeit, bei NFS Storages und für komplette Wiederherstellungen von VMs sollte es aber trotzdem nicht verwendet werden.

Veeam Backup & Replication kann mehrere Festplatten von VMs parallel verarbeiten, auch wenn diese auf unterschiedlichen Storages (SAN und lokal) liegen. Wichtig ist, dass man bei den Modi »Failover to network mode if primary transport modes fail or are not available« beim Proxy auswählt bzw. den Standard (angeklickt) lässt (siehe Abbildung 4-8).

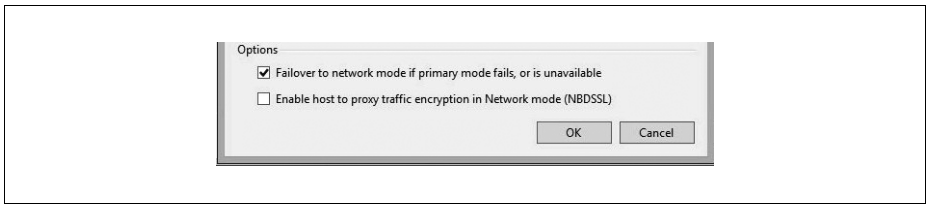

Abbildung 4-8: Rückfall zum Netzwerkmodus

Transportmodi-Übersicht

In der folgenden Tabelle 4-1 werden die einzelnen Modi nochmals zusammengefasst und verglichen:

Tabelle 4-1: Transport-Modi

	Direct SAN	SAN+BFSS	Direct NFS	HotAdd	NBD
ADF	nein	ja	ja	ja	nein
Geschwindigkeit	schnell	schneller	schneller	schneller	langsam
Beeinflussung	wenig	weniger	weniger	hoch	hoch
Zuverlässigkeit	gut	sehr gut	sehr gut	schlecht	sehr gut
Unterstützung	gut	sehr gut	sehr gut	gut	gut

Dabei bezeichnet SAN Storage Area Network (bei Fibre Channel und iSCSI), BFSS Backup From Storage Snapshots, NBD Network-Block-Device-Protokoll und ADF Advanced Data Fetcher, wie bereits oben beschrieben.

Menüeinstellungen

In dem Hauptmenü, welches links oben durch drei waagerechte Balken erreichbar ist, werden einige grundsätzliche Einstellungen zum Backup-Server eingerichtet. Vieles davon erreichen Sie auch an anderen Stellen – anderes jedoch nicht.

Der Punkt Upgrade ist ausgegraut, wenn es keine aktualisierte Version gibt. Nachrichten über fehlende Patches sehen Sie in der Konsole unter dem Eintrag »Backup Infrastructure« durch einen nur dann erscheinenden Punkt »Missing Updates«.

Manage Credentials

Nach einem Klick auf diese Option öffnet sich ein neues Fenster, in dem alle bisher eingetragenen Benutzer zentral angezeigt, gelöscht und bearbeitet werden können. Veeam selber trägt dort mindestens zwei Linux-User ein, die für das Wiederherstellen von Dateien unter Linux und für andere Aufgaben (z.B. Microsoft Azure) genutzt werden. Diese sollten Sie nur bearbeiten, wenn Sie sich sicher sind, dass sich die Anmeldedaten o. Ä. geändert haben.

Alle User, die während der Erstellung der Jobs hinzugefügt werden, erscheinen automatisch auch in diesem Fenster.

Credentials löschen

Wenn Sie einen User oder eine Gruppe entfernen wollen, so müssen alle Jobs, die diesen Account nutzen, vorher geändert werden. Klicken Sie dazu in dem Fenster auf den Benutzer oder die Gruppe und anschließend auf »Edit« oder »Remove«. Im nächsten Fenster sind alle Namen aufgelistet, bei denen Berechtigungen für diesen Account vergeben wurden. Dies kann der Zugriff auf den vCenter oder einen anderen Server sein, ein Job für »Application Aware Image Processing«, der SysAdmin für Oracle, eine SMB/CIFS-Freigabe, eine DataDomain, ein StorageOnce oder auch ein NAS-Laufwerk (Shared Folder). Sie müssen zunächst bei jedem der aufgelisteten Einträge andere Berechtigungen vergeben, bevor Sie die Credentials löschen können.

Manage Passwords

Dieser Punkt ist für die Aktualisierung oder Änderung der Passwörter bei Verschlüsselungen gedacht. Sollten Sie schon einen Job mit Verschlüsselung angelegt haben, so wird hier der Hinweis (Hint) und das Datum der letzten Änderung angezeigt. Sollten Sie die Verschlüsselung eingesetzt haben und das Passwort nicht mehr wissen, so kann diese Sicherung nicht mehr entschlüsselt werden. Beachten Sie auch die Ausnahmen, die ich hierzu in Kapitel 10 Enterprise Manager (weiter unten) geschrieben habe.

Manage Azure Accounts

Falls Sie Microsofts Cloud Azure nutzen, können Sie hier Angaben zum Azure Resource Manager hinzufügen. Dafür muss auf dem Server bereits die Azure PowerShell installiert sein. Bei älteren Verträgen oder zur Fehlersuche kann auch noch der klassische Zugriff eingerichtet (versucht) werden. Hierfür benötigen Sie dann die Konfigurationsdatei (subscription configuration file), aus dem Veeam die notwendigen Informationen ausliest.

General Options

Hier werden auf fünf Registerkarten allgemeine Einstellungen vorgenommen:

I/O Control

Das Häkchen bei »Enable parallel processing« ist standardmäßig gesetzt. Dadurch können mehrere Aufgaben gleichzeitig (parallel) verarbeitet werden.

Das Kästchen bei »Enable storage latency control« ist üblicherweise nicht angehakt. Dieser Punkt sollte auch nur genutzt werden, wenn der Datenspeicher häufig überfordert ist. Dann kann man Veeam dazu veranlassen, keine neuen

Aufgaben zum Storage zu senden, wenn die Wartezeit (Latenz) schon bei 20 ms angekommen ist, und/oder bereits laufende Prozesse werden ab 30 ms gedrosselt. Einzelne Repositories lassen sich nur mit der Enterprise-Plus-Lizenz einstellen.

E-Mail Settings

Möchte man E-Mail-Nachrichten bekommen, wenn die jeweiligen Jobs beendet wurden, so kann man hier die dafür notwendigen Einstellungen vornehmen – das lässt sich auch bei jedem Job manuell einstellen, falls man individuelle Informationen zugeschickt bekommen möchte. Setzen Sie das Häkchen bei »Enable e-mail notifications« und füllen Sie die benötigten Felder aus. Im Feld »Subject« stehen einige Platzhalter für das Ergebnis (Success, Warning oder Error), der Name des Jobs, die Anzahl der im Job enthaltenen Objekte und ggf. Fehler.

Im unteren Teil sind standardmäßig alle vier Kästchen angehakt. Das betrifft Meldungen bei Erfolg, Warnungen und Fehler sowie das Unterdrücken von Fehlernachrichten bis zum letzten Versuch. Überlegen Sie sich, ob Sie die Fehler schon beim ersten Fehlversuch bekommen möchten, und nehmen Sie das Häkchen dort ggf. raus.

SNMP Setting

Auf dieser Registerkarte können bis zu fünf Empfänger für SNMP Traps eingetragen werden. Unabhängig davon kann der Server natürlich auch über SNMP auf dem Port 161/162 abgefragt werden.

Notifications

Sowohl bei SNMP als auch bei E-Mail werden einstellbare Informationen gesendet, wenn der Backup Storage (Repository) weniger als 10% freien Speicherplatz aufweist und wenn das Volume der zu sichernden VM weniger als 10% freien Platz hat.

Wenn der Produktionsspeicher weniger als 5% Platz frei hat, wird die jeweilige VM nicht mehr gesichert, da durch Snapshots der Platz aufgebraucht werden könnte und damit alle darauf laufenden VMs stehen bleiben.

Wenn der Vertrag (Subscription) ausläuft, wird eine Nachricht gesendet und es wird regelmäßig nach Updates für das Produkt gesucht.

History

Hier kann man einstellen, wie viele Aufgaben (500 sessions) angezeigt und wie lange diese gespeichert werden (53 weeks).

Security

Auf der letzten Registerkarte kann man sich das selbst signierte Zertifikat des BS anschauen oder auch ein neues installieren. Für neu hinzukommende Linux-Server kann eingestellt werden, ob diesen generell oder ob nur bereits bekannten vertraut wird. Bei neuen Servern müsste man den »Fingerprint« hierüber importieren.

Users and Roles

Möchte man Benutzern oder Gruppen die Möglichkeit geben, selbstständig über die Oberfläche Informationen zu lesen, Jobs zu bearbeiten, zu starten usw., können hier Berechtigungen dafür vergeben werden. Es gibt vier vordefinierte Rollen, die einem lokalen Benutzer oder einer lokalen Gruppe – oder auch aus dem AD – zugewiesen werden können, damit er hier bestimmte Aufgaben übernehmen kann.

Der Restore Operator kann nur eine Wiederherstellung, der Backup Operator nur ein Backup initiieren, der Backup Viewer nur lesend zugreifen und der Backup Administrator hat alle Rechte. Auch können hier bestehende Einträge geändert und gelöscht werden.

Leider ist es hier nicht möglich, Berechtigungen auf einzelne Objekte oder Kategorien zu legen, und wer hier lesen darf, sieht alle Daten – auch verschlüsselte.

Network Traffic Rules

Über diesen Menüpunkt kann man Regeln für

- die Bandbreitenbeschränkungen einrichten, damit der Transfer nicht die produktiven Maschinen zu stark belastet;
- Datentransferverbindungen einschränken: Pro Job werden fünf gleichzeitige Verbindungen aufgebaut, bei mehreren parallel laufenden Jobs kann das das Netzwerk überlasten. Da bei jeder Datenübertragung CRC (Cyclic Redundancy Check) Checks zum Einsatz kommen, sind die Daten von Veeam aber immer konsistent;
- Datenverschlüsselungen einrichten, falls die Verbindung über eine unsichere Leitung läuft, sowie
- bevorzugte Netzwerkverbindungen einstellen: Hiermit kann festgelegt werden, über welchen Weg z. B. eine Wiederherstellung erfolgen soll, wenn das Produktionsnetzwerk nicht belastet werden darf.

Die hier gemachten Einstellungen können dann bei dem jeweiligen Job ausgewählt werden, da sie übergreifend zur Verfügung stehen. Zusätzlich kann bei den meisten Transfers ebenfalls so eine Regel erstellt werden.

Configuration Backup

An dieser Stelle kann man die Informationen über die angelegten Jobs mit allen Details einmal täglich auf einen Datenträger ablegen, um sie im Bedarfsfall auf einem neu erstellten BS wieder einlesen zu können. Weitere wichtige Details hierzu stehen unter Punkt 5.8.

Console

Hinter dem Menüpunkt »Console« verbirgt sich zum einen der Aufruf der angepassten PowerShell-Umgebung, die näher im Kapitel 13 erklärt wird, zum Zweiten kann hierüber das beliebte SSH-Tool PuTTy aufgerufen werden, mit dem man z.B. auf die Konsole eines ESXi Hosts oder auf andere Linux-Rechner kommen kann, und zuletzt ein Link zum Aufruf einer Remote-Desktop-Verbindung auf den Backup-Server selbst.

Da über das Microsoft RDP häufig vom lokalen Rechner Laufwerke, Drucker und die Zwischenablage an die entfernte Maschine durchgereicht wird, empfehle ich aus Sicherheitsgründen, auf dem BS den Zugriff über RDP zu unterbinden.

Color Theme

Wem die Farbgestaltung (helles Grün) von Veeam nicht zusagt, der kann die Console hierüber in eine von drei anderen Farben umgestalten.

License

Wie bereits unter Punkt 1.6 erwähnt, kann man hier Informationen zu den eingetragenen Lizenzen für die virtuelle Umgebung, die physischen Windows und Linux-Rechner bekommen, eine neue oder zusätzliche Lizenz eintragen (falls Sie einen EM im Einsatz haben, sollten Sie das dort zentral erledigen) und über die Schaltfläche »Manage« auch nicht mehr vorhandene Hosts austragen (Revoke).

Sobald eine VM von einem Host gesichert oder repliziert wird, wird er dieser Liste hinzugefügt. Tauschen Sie einen Hypervisor aus, so muss das hier über »Revoke« bekannt gemacht werden. Weiterhin haben Sie hier den Überblick über die eingetragenen Lizenzen, wie viele davon in Benutzung sind und wie viele noch übrig bleiben.

Help

Über den vorletzten Punkt können Sie die Online-Hilfe aufrufen. Dabei wird der Standardbrowser geöffnet und die Seite mit der Dokumentation aufgerufen.

Weiterhin gibt es hier die Möglichkeit, Log-Dateien für einen Job oder alle beteiligten Komponenten (BS, Proxy etc.) zu exportieren, die man anschließend dem Veeam-Support zur Verfügung stellen kann.

Der dritte Punkt gibt Aufschluss über die installierte Version, die Dauer des Support-Vertrages, den Lizenznehmer und bietet zwei zusätzliche Links zum Technischen Support und der Veeam Community. Mit einem Klick auf das Fenster schließt sich dieses wieder.